

<https://student.fbtuit.uz/test/result/268190> 1/4

1. Solovey Shtrassen testi qanday turdagi tublikka testlovchi algoritm hisoblanadi?

☐ aniqlashtirilgan testlar tarkibiga kiruvchi algoritm

2. Steganografiya ma'lumotni qanday maxfiylashtiradi?

☐ maxfiy xabarni soxta xabar ichiga berkitish orqali

3. Pollard usuli qanday matematik muammoni yechadi?

☐ Faktorlash

4. DES shifrlash algoritmda har bir raunda necha bitli raund kalitlaridan foydalaniladi?

☐ 48

5. Quyidagi ifodani qiymatini toping.  $-19 \bmod 26$

☐ 6

6. RC4 shifrlash algoritmi simmetrik turga mansub bo'lsa, unda nechta kalitdan foydalaniladi?

☐ 1

7. RC4 shifrlash algoritmi qaysi turga mansub?

☐ oqimli shifrlar

8. Ochiq kalitli El-Gamal shifrlash algoritmi bardoshliligi qanday matematik muammo turiga asoslangan?

☐ faktorlash murakkabligiga

9. A5/1 oqimli shifrlash algoritmda Y registr uzunligi nechi bitga teng?

☐ 22

<https://student.fbtuit.uz/test/result/268190> 2/4

10. A5/1 shifrlash algoritmi simmetrik turga mansub bo'lsa, unda nechta kalitdan foydalaniladi?

☐ 1

11. O'rniga qo'yish shifrlash algoritmlari qanday sinfga bo'linadi?

☐ bir qiymatli va ko'p qiymatli shifrlash

12. Mantiqiy XOR amalining asosi qanday hisoblashga asoslangan?

☐ mod2 bo'yicha qo'shishga

13. .... shifrlar blokli va oqimli turlarga ajratiladi

☐ simmetrik

14. Ochiq kalitli shifrlash algoritmi keltirilgan qatorni toping?

☐ DES

15. Quyidagi ifodani qiymatini toping.  $-17 \bmod 11$

❑ 6

16. AES shifrlash algoritmi simmetrik turga mansub bo'lsa, unda nechta kalitdan foydalaniladi?

❑ 1

17. SHA1 xesh algoritmda nechta 32 bitli statik qiymatdan foydalanadi?

❑ 5

18. A5/1 shifrlash algoritmi bu?

❑ oqimli shifrlash algoritmi

09.05.2023, 00:49 Kriptogrifiya2 fanidan Oraliq nazorat | HEMIS Student axborot tizimi

<https://student.fbtuit.uz/test/result/268190> 3/4

19. RC4 oqimli shifrlash algoritmi asosan qayerda qo'llaniladi?

❑ simsiz aloqa vositalaridagi mavjud WEP protokolidagi

20. Ochiq kalitli RSA shifrlash algoritmda "d" shaxsiy kalit, "e" ochiq kalit bo'lsa shifrlash formulasi to'g'ri ko'rsatilgan qatorni belgilang?

❑  $C = M^d \pmod{\varphi(N)}$

21. DES shifrlash algoritmi bu?

❑ blokli shifrlash algoritmi

22. AES algoritmda shifrlash kalitining uzunligi necha bitga teng?

❑ 128, 156, 256 bit

23. Kompyuter davriga tegishli shifrlarni aniqlang?

❑ DES, AES shifri

24. Ferma testi qanday turdagi tublikka testlovchi algoritm hisoblanadi?

❑ taqribiy testlar tarkibiga kiruvchi algoritm

25. Ochiq kalitli RSA shifrlash algoritmi bardoshliligi qanday matematik muammo turiga asoslangan?

❑ faktorlash murakkabligiga

26. RSA algoritmining mualliflarini ko'rsating

❑ R. Rivest, K. Hellman, L. Adleman

27. Ochiq kalitli Rabin shifrlash algoritmi bardoshliligi qanday matematik muammo turiga asoslangan?

09.05.2023, 00:49 Kriptogrifiya2 fanidan Oraliq nazorat | HEMIS Student axborot tizimi

<https://student.fbtuit.uz/test/result/268190> 4/4

❑ elliptik egri chiqizlarda faktorizatsiyalash murakkabligiga

28. OpenSSL nima?

❑ Secure Sockets Layer (SSL) va kriptografiya vositalarini amalga oshiruvchi asosiy dasturdir

29. Vernam shifrlash algoritmda shifr matn C=101 ga, kalit K=111 ga teng bo'lsa shifr matn

qiymati qanday bo'ladi?

☐ 010

30. Vernam shifrlash algoritmi asosi qaysi mantiqiy hisoblashga asoslangan

☐ XOR

1. Kolliziya hodisasi deb nimaga aytiladi?

☐ ikki xil matn uchun bir xil xesh qiymat chiqishi

2. Quyidagi modulli ifodani qiymatini toping.  $(125 \cdot 45) \bmod 10$ .

☐ 5

3. Konfidensiallikni ta'minlash bu -?

☐ ruxsat etilmagan "o'qishdan" himoyalash

4. Sesar shifrlash usuli qaysi akslantirishga asoslangan?

☐ o'rniga qo'yish

5. ERI algoritmlari qanday muolajalardan iborat?

☐ imzoni shakllantirish, imzoni tekshirish

6. Mantiqiy XOR amalining asosi qanday hisoblashga asoslangan?

☐ mod2 bo'yicha qo'shishga

7. Ximoyalanuvchi ma'lumot boshqa bir ma'lumotni ichiga yashirish orqali maxfiyligini ta'minlaydigan usul qaysi?

☐ steganografiya

8. Vernam shifrlash algoritmi asosi qaysi mantiqiy hisoblashga asoslangan

☐ XOR

9. Faqat tub son keltirilgan qatorni toping?

☐ 3, 5

10. DES shifrlash algoritmidan har bir raunda necha bitli raund kalitlaridan foydalaniladi?

☐ 48

11. Dastlabki ma'lumotni bevosita shifrlash va deshifrlash uchun zarur manba ... deb ataladi

☐ Kalit

12. Rijndael algoritmi S-box uzunligi necha bit?

☐ 128

13. RSA algoritmidan p, q tub sonlar bo'lsa, modul qiymati N qanday topiladi?

☐  $N=p \cdot q$

14. Quyidagi ifoda nechta yechimga ega?  $3^x \equiv 2 \pmod{7}$ .

☐ bitta yechimga ega

15. A5/1 shifri qaysi turga mansub?

☐ oqimli shifrlar

16. Qaysi algoritm o'rtada turgan odam hujumiga bardoshsiz hisoblanadi?

☐ Diffie-Hellman

17. Vernam shifrlash algoritmidagi ochiq matn  $M=101$  ga, kalit  $K=111$  ga teng bo'lsa shifrlanган matn qiymati qanday bo'ladi?

☐ 010

18. Kompyuter davriga tegishli shifrlarni aniqlang?

☐ DES, AES shifri

19. Assimetrik kriptotizimlarda necha kalitdan foydalaniladi?

☐ 2 ta

20. RC/4 shifri qaysi turga mansub?

☐ oqimli shifrlar

21. RSA algoritmidagi matematik murakkablikni qanday usul orqali bartaraf qilish mumkin?

☐ Pollard usuli

22. Faktorlash muammosini yechishning Pollard usulida eng kichik polinom qanday tanlanadi?

☐  $x^2+1$

23. Qaysi algoritm har bir qadamda bir bayt qiymatni shifrlaydi?

☐ RC4

24. Faktorlash muammosini yechishning Pollard usulida funksiya argumenti boshlangich qiymati nechiga teng bo'ladi?

☐ 2

25. OpenSSL nima?

☐ Secure Sockets Layer (SSL) va kriptografiya vositalarini amalga oshiruvchi asosiy dasturdir

26. RSA shifrlash algoritmidagi qaysi parametrlar ochiq holda e'lon qilinadi?

☐ ochiq kalit –  $e$ , hamda modul qiymati -  $N$

27. Chastotalar tahlili hujumi qanday amalga oshiriladi?

☐ shifrlanган matnda qatnashgan harflar sonini aniqlash orqali

28. Kalit – bu?

☐ kalit – matnlarni shifrlash va deshifrlash uchun kerak bo'lgan axborot

29. GSM tarmog'ida foydalaniluvchi shifrlash algoritmi nomini ko'rsating?

☐ A5/1

30. AES shifrlash algoritmidagi 128 bitli ma'lumot bloki qanday o'lchamdagi jadvalga solinadi?

☐ 4x4

[Question] ГОСТ Р 34.10-94 qanday standart hisoblanadi? ERI standarti kodlash standarti steganografik standart shifrlash standarti Correct1 [Question] O'zDSt 1092:2009 qanday standart hisoblanadi? ERI standarti shifrlash standarti kodlash standarti steganografik standart Correct1 [Question] DSA qanday standart hisoblanadi? ERI standarti shifrlash standarti kodlash standarti steganografik standart Correct1 [Question] Seans kalitli hamda seans kalitsiz rejimlarda ishldigan standartni ko'rsating? O'zDSt 1092:2009 ECDSA-2000 ГОСТ Р 34.10-94 DSA Correct1 [Question] ГОСТ Р 34.10-94 standarti qaysi davlat standarti hisoblanadi? Rossiya O'zbekiston AQSH Kanada Correct1 [Question] O'zDSt 1092:2009 standarti qaysi davlat standarti hisoblanadi? O'zbekiston AQSH Rossiya Kanada Correct1 [Question] ECDSA-2000 qaysi davlat standarti hisoblanadi? AQSH Rossiya O'zbekiston Kanada Correct1 [Question] Raqamli imzoni shakllantirish muolajasi qaysi algoritmgaga tegishli? ERI algoritmgaga kodlash algoritmgaga shifrlash algoritmgaga steganografiya algoritmgaga Correct1 [Question] Elektron hujjatni mualliflikdan bosh tortmasligini qaysi amal orqali amalga oshiriladi? ERI orqali amalga oshiriladi kodlash orqali amalga oshiriladi autentifikatsiya orqali amalga oshiriladi shifrlash algoritmi orqali amalga oshiriladi Correct1 [Question] Elektron hujjat yaxlitligini (o'zgarmasligini) tekshirish qaysi amal orqali amalga oshiriladi? ERI orqali amalga oshiriladi kodlash orqali amalga oshiriladi shifrlash algoritmi orqali amalga oshiriladi autentifikatsiya orqali amalga oshiriladi Correct1 [Question] Elektron hujjat manbaini haqiqiyligini qaysi amal orqali amalga oshiriladi? ERI orqali amalga oshiriladi shifrlash algoritmi orqali amalga oshiriladi kodlash orqali amalga oshiriladi autentifikatsiya orqali amalga oshiriladi Correct1 [Question] 1 ga va o'ziga bo'linadigan sonlar qanday sonlar hisoblanadi? tub sonlar murakkab sonlar toq sonlar juft sonlar Correct1 [Question] Elliptik egriz chiqizlarda nuqtalar usitda qanday ammalar bajariladi? nuqtalarni qo'shish va nuqtalarni ikkilantirish nuqtalarni qo'shish va nuqtalarni ko'paytirish nuqtalarni qo'shish va nuqtalarni bo'lish nuqtalarni ayirish va nuqtalarni ko'paytirish Correct1 [Question] Sonlarni tublikka tekshiruvchi ehtimollikka asoslangan algoritmlar keltirilgan qatorni ko'rsating? Ferma, Solovey Shtrassen, Rabbi-Milner Ferma, Solovey Shtrassen, Eyler Eyler, Solovey Shtrassen, Rabbi-Milner Ferma, Eyler, Rabbi-Milner Correct1 [Question] Sonlarni tublikka tekshiruvchi algoritmlar qanday sinfga bo'linadi? aniqlashtirilgan va ehtimolli testlar aniqlashtirilgan va taqribiy testlar taqribiy va ehtimolli testlar aniqlashtirilgan, ehtimolli va taqribiy testlar Correct1 [Question] Sonlarni tublikka tekshiruvchi algoritmlar necha sinfga bo'linadi? 2 3 4 5 Correct1 [Question] Rabbi-Milner testi qanday turdagi tublikka testlovchi algoritmi hisoblanadi? ehtimollik testlar tarkibiga kiruvchi algoritmi aniqlashtirilgan testlar tarkibiga kiruvchi algoritmi taqribiy testlar tarkibiga kiruvchi algoritmi tublikka teslovchi algoritmi hisoblanmaydi Correct1 [Question] Solovey Shtrassen testi qanday turdagi tublikka testlovchi algoritmi hisoblanadi? ehtimollik testlar tarkibiga kiruvchi algoritmi aniqlashtirilgan testlar tarkibiga kiruvchi algoritmi taqribiy testlar tarkibiga kiruvchi algoritmi tublikka teslovchi algoritmi hisoblanmaydi Correct1 [Question] Ferma testi qanday turdagi tublikka testlovchi algoritmi hisoblanadi? ehtimollik testlar tarkibiga kiruvchi algoritmi aniqlashtirilgan testlar tarkibiga kiruvchi algoritmi taqribiy testlar tarkibiga kiruvchi algoritmi tublikka teslovchi algoritmi hisoblanmaydi Correct1 [Question] Kriptotizimlar kalitlar soni bo'yicha qanday turga bo'linadi? simmetrik va assimetrik simmetrik va bitta kalitli 3 kalitli kriptotizimlar assimetrik va 2 ta kalitli Correct1 [Question] Kriptotizimlar kalitlar soni bo'yicha nechta turga bo'linadi? 2 3 4 5 Correct1 [Question] Faqat simmetrik algoritmi keltirilgan qatorni ko'rsating? AES RSA El-Gamal Barcha javoblar to'g'ri Correct1 [Question] Kriptografiya bu -? axborotni o'zgartirish vositalari va usullarini o'rganadigan fan axborot mazmunidan beruxsat erkin foydalanishdan muhofazalash axborotni buzishning oldini olish axborot almashtirish vosita va usullari bilan shug'ullanadigan fa Correct1 [Question] Shifrlash

orqali ma'lumotning qaysi xususiyati ta'minlanadi? maxfiyligi butunliligi ishonchliligi foydalanuvchanliligi Correct1 [Question] Ochiq kalitli shifrlash algoritmi keltirilgan qatorni toping? El-Gamal AES DES RC4 Correct1 [Question] Ochiq kalitli shifrlash algoritmi keltirilgan qatorni toping? RSA AES DES RC4 Correct1 [Question] RSA algoritmining mualliflarini ko'rsating R. Rayvest, A. Shamir, L. Adleman Diffi va M. Xellman R. Rayvest, K. Xellman, L. Adleman L. Adleman, El Gamal, K. Shnorr Correct1 [Question] Kriptotahlil nima bilan shug'ullanadi? kalit yoki algoritmi bilmagan holda shifrlangan ma'lumotga mos k ochiq ma'lumotlarni shifrlash masalalarining matematik uslublari maxfiy kodlarni yaratish bilan maxfiy kodlar orqali ma'lumotlarni yashirish bilan Correct1 [Question] Sonlarni tublikka tekshirish algoritmlari nechta sinfga bo'linadi? ikkita sinfga uchta sinfga bitta sinfga sinflarga bo'linmaydi Correct1 [Question] Qanday sonlar tub sonlar hisoblanadi? 1 va o'ziga bo'linadigan sonlarlar barcha toq sonlar juft bo'lmagan sonlar 2 ga bo'linmaydigan sonlar Correct1 [Question] Ochiq kalitli kriptotizimlarda asosan qanday turdagi sonlar bilan ishlaydi? tub sonlar bilan kasr sonlar bilan chekli maydonda kasr sonlar faqat manfiy sonlar Correct1 [Question] Ochiq kalitli kriptotizimda, qaysi kalit orqali ma'lumot rasshifrovkalanadi? maxfiy kalit orqali ochiq kalit orqali ma'lumot shifrlanmaydi ushbu tizimda kalitdan foydalanilmaydi Correct1 [Question] Ochiq kalitli kriptotizimlarda qaysi kalit orqali ma'lumot shifrlanadi? ochiq kalit orqali maxfiy kalit orqali ushbu tizimda kalitdan foydalanilmaydi ma'lumot shifrlanmaydi Correct1 [Question] Ochiq kalitni kriptotizimlarda nechta kalitdan foydalanadi? ikkita bitta uchta kalitdan foydalanilmaydi Correct1 [Question] Kalit bardoshliligi bu - ? eng yaxshi ma'lum algoritmi bilan kalitni topish murakkabligidir eng yaxshi ma'lum algoritmi yordamida yolg'on axborotni ro'kach qi nazariy bardoshlilik amaliy bardoshlilik Correct1 [Question] Kerkxofs printsipli nimadan iborat? kriptografik tizim faqat kalit noma'lum bo'lgan taqdirdagina maxfiy kriptografik tizim faqat yopiq bo'lgan taqdirdagina maxfiylik ta' kriptografik tizim faqat kalit ochiq bo'lgan taqdirdagina maxfiy kriptografik tizim faqat ikkita kalit ma'lum bo'lgan taqdirdagina Correct1 [Question] Assimetrik kriptotizimlarda nechta kalitdan foydalaniladi? 2 ta 3 ta 4 ta kalit ishlatilmaydi Correct1 [Question] Ochiq kalitli kriptotizimlarda qanday turdagi kalitlardan foydalanadi? ochiq va maxfiy kalitlardan maxfiy kalitlar juftidan maxfiy kalitni uzatishni talab etmaydi ochiq kalitni talab etmaydi Correct1 [Question] Simmetrik kriptotizimlardagi qanday muammoni ochiq kalitli kriptotizimlar bartaraf etdi? maxfiy kalitni uzatish muammosini kalitni generatsiyalash muammosini ochiq kalitni uzatish muammosini kalitlar juftini hosil qilish muammosini Correct1 [Question] Kriptotizimlar kalitlar soni bo'yicha qanday turga bo'linadi? simmetrik va assimetrik turlarga simmetrik va bir kalitli turlarga 3 kalitli turlarga assimetrik va 2 kalitli turlarga Correct1 [Question] Kriptotizimlar kalitlar soni bo'yicha nechta turga bo'linadi? 2 4 6 8 Correct1 [Question] Ochiq kalitli kriptotizimlar ma'lumotni qanday xususiyatini taminlaydi? maxfiyligini butunligini foydalanuvchanligini ma'lumotni autentifikatsiyasini Correct1 [Question] Kriptologiya so'zining ma'nosi? cryptos – maxfiy, logos – ilm cryptos – kodlash, logos – ilm cryptos – kripto, logos – yashiraman cryptos – maxfiy, logos – kalit Correct1 [Question] Kriptologiya nechta yo'nalishga bo'linadi? 2 14 16 18 Correct1 [Question] Ochiq kalitli kriptotizimlar kim tomonidan kashf qilingan? U.Diffie va M.Hellman Rivest va Adlman Shamir va Rivest U.Diffie va Rivest Correct1 [Question] Shifrlash orqali ma'lumotning qaysi xususiyati ta'minlanadi? maxfiyligi butunliligi ishonchliligi foydalanuvchanligi Correct1 [Question] Kriptotahlil nima bilan shug'ullanadi? maxfiy kodlarni buzish bilan maxfiy kodlarni yaratish bilan shifrlash uslublarini bilmagan holda shifrlangan ma'lumotni asl h maxfiy kodlar orqali ma'lumotlarni yashirish bilan Correct1 [Question] Kriptografiya nima bilan shug'ullanadi? maxfiy kodlarni yaratish bilan maxfiy kodlarni buzish bilan maxfiy kodlar orqali ma'lumotlarni yashirish bilan shifrlash uslublarini

bilmagan holda shifrlangan ma'lumotni asl h Correct1 [Question] Kriptologiya nima bilan shug'ullanadi? maxfiy kodlarni yaratish va buzish ilmi bilan maxfiy kodlarni buzish bilan maxfiy kodlarni yaratish bilan maxfiy kodlar orqali ma'lumotlarni yashirish bilan Correct1 [Question] Kriptologiya qanday yo'nalishlarga bo'linadi? kriptografiya va kriptotahlil kriptografiya va kriptotizim kripto va kriptotahlil kriptotizim Correct1 [Question] Ochiq kalitli El-Gamal shifrlash algoritmda "p" tub son bo'lsa maxfiy kalit qanday tanlanadi? (p-1) bilan o'zaro tub bo'lgan (1,p-1) intervaldagi butun son p bilan o'zaro tub bo'lgan (1,p-1) intervaldagi butun son (1,p-1) intervaldagi tub son (p-1) bilan o'zaro tub bo'lgan (1,p) intervaldagi butun son Correct1 [Question] Ochiq kalitli RSA shifrlash algoritmda "p=7" tub son bo'lsa Eyler funskiyasi  $\varphi(p)$  qanday qiymat qaytaradi? 6 7  $\varphi(7)$   $\varphi(6)$  Correct1 [Question] Ochiq kalitli RSA shifrlash algoritmda "p" tub son bo'lsa Eyler funskiyasi  $\varphi(p)$  qanday qiymat qaytaradi? p-1 p  $\varphi(p)$   $\varphi(p-1)$  Correct1 [Question] Ochiq kalitli RSA shifrlash algoritmda "d" shaxsiy kalit, "e" ochiq kalit bo'lsa shifrlash formulasi to'g'ri ko'rsatilgan qatorni belgilang?  $C=M^e \pmod N$   $C=M^e \pmod{\varphi(N)}$   $C=M^d \pmod{\varphi(N)}$   $C=M^d \pmod N$  Correct1 [Question] Ochiq kalitli RSA shifrlash algoritmda "e" ochiq kalit, "d" shaxsiy kalit bo'lsa d shifrlash formulasi to'g'ri ko'rsatilgan qatorni belgilang?  $M=C^d \pmod N$   $M=C^d \pmod{\varphi(N)}$   $M=C^e \pmod N$   $M=C^e \pmod{\varphi(N)}$  Correct1 [Question] Ochiq kalitli RSA shifrlash algoritmda qaysi parametrlar ochiq holda e'lon qilinadi? N,e e N,d d Correct1 [Question] Ochiq kalitli RSA shifrlash algoritmda maxfiy kalit qanday topiladi?  $e*d=1 \pmod{\varphi(p*q)}$  taqqoslamadan  $e*d=1 \pmod N$   $e*d=1 \pmod{\varphi(p-1)}$   $e*d=1 \pmod{\varphi((p-1)(q-1))}$  Correct1 [Question] Ochiq kalitli RSA shifrlash algoritmda ochiq kalit "e" qanday topiladi?  $\varphi(N)$  bilan o'zaro tub va undan kichik bo'lgan son tanlanadi  $\varphi(N)$  dan kichik tub son tanlanadi  $\varphi(N)$  dan katta tub son tanlanadi  $\varphi(N)$  ning tub ko'paytuvchilaridan biri tanlanadi Correct1 [Question] Faktorlash muammosini yechishning Pollard usulida funksiya argumenti boshlangich qiymati nechiga teng bo'ladi? 2 1 3 0 Correct1 [Question] Faktorlash muammosini yechishning Pollard usulida eng kichik polinom qanday tanlanadi?  $x^2+1$   $x+1$   $x^2$  Correct1 [Question] Faktorlash muammosini yechishning Pollard usulida tanlanadigan funksiya qanday ko'rinishda bo'ladi? kvadratik polinom chiziqli polinom kubik polinom funksiya argumentiga bog'liq emas Correct1 [Question] Agar sonlarni tublikka tekshirishning Rabin-Miller testida beshta tublikka guvohi mavjud bo'lsa tekshirilayotgan sonni tub bo'lishi ehtimoli nechiga teng?  $1-2^{-5}$   $1-(1/2)$   $1-2^{-5}$   $1-5^{-2}$  Correct1 [Question] Agar sonlarni tublikka tekshirishning Ferma testida uchta tublikka guvohi mavjud bo'lsa tekshirilayotgan sonni tub bo'lishi ehtimoli nechiga teng?  $1-2^{-3}$   $1-(1/2)$   $1-2^{-3}$   $1-3^{-2}$  Correct1 [Question] Agar sonlarni tublikka tekshirishning Solovay-Shtraassen testida ikkita tublikka guvohi mavjud bo'lsa tekshirilayotgan sonni tub bo'lishi ehtimoli nechiga teng?  $1-2^{-2}$   $1-(1/2)$   $1-2^{-2}$   $1-(1/(2^{-2}))$  Correct1 [Question] "murakkabligiga guvoh" termini qaysi algoritmlarda ishlatiladi sonlarni tublikka tekshirish algoritmlarida shifrlash algoritmlarida kodlash algoritmlarida steganografik algoritmlarda Correct1 [Question] "soxta tublikka guvoh" termini qaysi algoritmlarda ishlatiladi sonlarni tublikka tekshirish algoritmlarida shifrlash algoritmlarida steganografik algoritmlarda kodlash algoritmlarida Correct1 [Question] "Pseudotub" termini qaysi algoritmlarda ishlatiladi sonlarni tublikka tekshirish algoritmlarida shifrlash algoritmlarida steganografik algoritmlarda kodlash algoritmlarida Correct1 [Question] Qanday sonlar murakkab sonlar deyiladi? ko'paytuvchilarga ajraladigan sonlar murakkab sonlar deyiladi ko'paytuvchilarga ajralmaydigan sonlar murakkab sonlar deyiladi ko'paytuvchilarga ajralmaydigan toq sonlar sonlar murakkab sonlar ko'paytuvchilarga ajraladigan juft sonlar murakkab sonlar deyiladi Correct1 [Question] RSA algoritmi qaysi tizimga mansub? Ochiq kalitli tizimlar Maxfiy kalitli tizimlar Xesh-funksiyalar Tasodifiy sonlar generatori Correct1 [Question] Sonlarni tublikka tekshirishda qaysi

algoritm Karlmaykl sonlarida ham to'g'ri ishlay di? Ferma algoritmda Solovey Shtrassen  
 algoritmda Rabin-Milner algoritmda Eyler algoritmda Correct1 [Question] Sonlarni tublikka  
 tekshirishda qaysi algoritm samarali hisoblanadi? Rabin Milner Solovey Shtrassen Ferma Eyler  
 Correct1 [Question] Qaysi algoritm o'rtada turgan odam hujumiga bardoshsiz hisoblanadi? Diffie-  
 Hellman RSA ElGamal DSA Correct1 [Question] Diffie-Hellman algoritmi qanday hujumga  
 bardoshsiz hisoblanadi? o'rtada turgan odam hujumiga chastotalar tahlili hujumiga yon kanal  
 tahlili hujumiga to'liq tanlash hujumiga Correct1 [Question] RSA shifrlash algoritmda qaysi  
 parametrlar ochiq holda e'lon qilinadi? ochiq kalit – e, hamda modul qiymati - N maxfiy kalit – d,  
 hamda modul qiymati - N ochiq kalit – e, hamda tub sonlar – p,q maxfiy kalit – d, hamda tub  
 sonlar – p,q Correct1 [Question] Qaysi kalit orqali ERI qo'yiladi? shaxsiy kalit orqali ochiq kalit  
 orqali kalit ishtirok etmaydi ikkala kalit birgalikda ishtirok etadi Correct1 [Question]  
 O'zbekistonning qanday ERI standarti mavjud? O'zDSt 1092:2009 DSA ECDSA-2000 GOCT P 34.10-  
 94 Correct1 [Question] O'zbekistonning nechta ERI standarti mavjud? 1 ta 2 ta 3 ta mavjud emas  
 Correct1 [Question] Amerikaning qanday ERI standarti mavjud? DSA va ECDSA-2000 DSA va GOCT  
 P 34.10-94 ECDSA-2000 va GOCT P 34.10-94 GOCT P 34.10-94 va O'zDSt 1092:2009 Correct1  
 [Question] Amerikaning nechta ERI standarti mavjud? 2 ta 1 ta 3 ta mavjud emas Correct1  
 [Question] RSA algoritmda p, q tub sonlar bo'lsa, modul qiymati N qanday topiladi?  $N=p*q$   $N=p/q$   
 $N=q/p$   $N=p-q$  Correct1 [Question] Karlmaykl sonlari qaysi tublikka tekshiruvchi algoritmlarda doim  
 bajariladi? Ferma testida Solovey-Shtrassen testida Eyler testida Rabbin testida Correct1  
 [Question] Faktorlash murakkabligiga asoslangan algoritm keltirilgan qatorni ko'rsating? RSA El-  
 Gamal Diffie-Hellman DSA Correct1 [Question] Diskret logarifmlash murakkabligiga asoslangan  
 algoritm keltirilgan qatorni ko'rsat ing? Diffie-Hellman, EL-Gamal algoritmi RSA algoritmi EL-Gamal  
 algoritmi Diffie-Hellman algoritmi Correct1 [Question] RSA shifrlash algoritmda tanlangan p va q  
 sonlarga qanday talab qo'yiladi? tub bo'lishi o'zaro tub bo'lishi butun son bo'lishi toq son bo'lishi  
 Correct1 [Question] O'zDSt 1092:2009 ERI standarti birinchi algoritmi qanday rejimlarda ishlaydi?  
 kalitli va kalitsiz ochiq kalitli va maxfiy kalitli ochiq va maxfiy 1 ta asosiy rejimi mavjud Correct1  
 [Question] Ochiq kalitli kriptotizimlarda elektron hujjatlarga qo'yilgan imzoni tekshirish qay si kalit  
 orqali amalga oshiriladi? ochiq kalit orqali maxfiy kalit orqali imzo qo'yilishi kalitga bog'liq emas  
 imzo qo'lda qo'yiladi Correct1 [Question] Ochiq kalitli kriptotizimlarda elektron hujjatlarga imzo  
 qo'yish qaysi kalit orqali amalga oshiriladi? shaxsiy kalit orqali ochiq kalit orqali imzo qo'yilishi  
 kalitga bog'liq emas imzo qo'lda qo'yiladi Correct1 [Question] ERI algoritmlari qanday  
 muolajalalardan iborat? imzoni shakllantirish, imzoni tekshirish imzoni shakllantirish, imzo qo'yish  
 va imzoni tekshirish imzoni shakllantirish va imzo qo'yish imzo qo'yish Correct1 [Question] ERI  
 algoritmlari nechta muolajadan iborat? ikkita bitta asosiy uchta to'rtta Correct1 [Question] Faqat  
 tub son keltirilgan qatorni toping? 2, 5 5, 25 16, 3 3, 21 Correct1 [Question] Diffie-Hellman qanday  
 algoritm hisoblanadi? kalitlarni ochiq taqsimlash algoritmi ochiq kalitli shifrlash algoritmi diskret  
 logarifmlash murakkabligiga asoslangan shifrlash algoritm faktorlash murakkabligiga asoslangan  
 kalitlarni ochiq taqsimlash Correct1 [Question] Diffie-Helman algoritmi qanday matematik  
 murakkablikka asoslanadi? diskret logarifmlash murakkabligiga faktorlash murakkabligiga elliptik  
 egri chiziqda diskret logarifmlash murakkabligiga elliptik egri chiziqda faktorlash murakkabligiga  
 Correct1 [Question] Ochiq kalitli El-Gamal shifrlash algoritmi qanday matematik murakkablikka  
 asoslanad i? diskret logarifmlash murakkabligiga faktorlash murakkabligiga elliptik egri chiziqda  
 diskret logarifmlash murakkabligiga elliptik egri chiziqda faktorlash murakkabligiga Correct1  
 [Question] Ochiq kalitli RSA shifrlash algoritmi bardoshliligi qanday matematik muammo turiga  
 asoslangan? faktorlash murakkabligiga diskret logarifmlash murakkabligiga elliptik egri chiziqda



faktorizatsiyalash murakkabligiga elliptik egri chiziqlarda faktorizatsiyalash murakkabligiga

Correct1 [Question] Sonlarni tublikka tekshirishning ehtimolli algoritmlariga quyidagilarning qaysilari kiradi? Ferma, Rabbi-Milner, Poklinton testlari Rabbi-Milner, Solovey-Shtrassen, Pollard testlari Ferma, Solovey-Shtrassen, Pollard testlari Rabbi Milner, Poklinton, Pollard testlari

Correct1 [Question] Ehtimolli testlar sonlarni tublikka tekshirishda qanday natijani beradi? tekshirilayotgan son tub yoki tubmasligi haqida ehtimollik bilan tekshirilayotgan son tub yoki tubmasligi haqida kafolatlangan ani tekshirilayotgan son tub yoki tubmasligi haqida tasodifiy ravishd tekshirilayotgan son tub yoki tubmasligini 0 va 1 qiymatlarga qar

Correct1 [Question] Faqat tub son keltirilgan qatorni toping? 3, 5 5, 15 16, 2 3, 18

Correct1 [Question] Ochiq kalitli kriptotizimlarning bardoshligini ta'minlashda qanday murakkab muammo turiga asoslanadi? faktorlash, diskret logarifmlash, elliptik egri chiziqda diskret faktorlash, diskret logarifmlash faktorlash, diskret logarifmlash, elliptik egri chiziqda faktoriz faktorlash, diskret logarifmlash, modulyar arifmetikaga

Correct1 [Question] Ochiq kalitli kriptotizimlarning matematik asosi nimaga asoslangan? oson hisoblanadigan bir tomonlama funksiyalarga modulyar arifmetikaga faktorizatsiyalashga diskret logarifmlashga

Correct1 [Question] Ochiq kalitli kriptotizimlar qanday turdagi matematik murakkablikka asoslangan algo ritmlarga bo'linadi? faktorizatsiyalash va diskret logarifmlash algoritmlariga modulyar arifmetika murakkabligiga asoslangan algoritmlarga diskret logarifmlash murakkabligiga asoslangan algoritmiga faktorizatsiyalash murakkabligiga asoslangan algoritmiga

Correct1 [Question] FOCT P 34.10-94 qanday standart hisoblanadi? ERI standarti kodlash standarti steganografik standart shifrlash standarti

Correct1 [Question] O'zDSt 1092:2009 qanday standart hisoblanadi? ERI standarti shifrlash standarti kodlash standarti steganografik standart

Correct1 [Question] DSA qanday standart hisoblanadi? ERI standarti shifrlash standarti kodlash standarti steganografik standart

Correct1 [Question] Seans kalitli hamda seans kalitsiz rejimlarda ishlidigan standartni ko'rsating? O'zDSt 1092:2009 ECDSA-2000 FOCT P 34.10-94 DSA

Correct1 [Question] FOCT P 34.10-94 standarti qaysi davlat standarti hisoblanadi? Rossiya O'zbekiston AQSH Kanada

Correct1 [Question] O'zDSt 1092:2009 standarti qaysi davlat standarti hisoblanadi? O'zbekiston AQSH Rossiya Kanada

Correct1 [Question] ECDSA-2000 qaysi davlat standarti hisoblanadi? AQSH Rossiya O'zbekiston Kanada

Correct1 [Question] Raqamli imzoni shakllantirish muolajasi qaysi algoritmga tegishli? ERI algoritmiga kodlash algoritmiga shifrlash algoritmiga steganografiya algoritmiga

Correct1 [Question] Elektron hujjatni mualliflikdan bosh tortmasligini qaysi amal orqali amalga oshiriladi? ERI orqali amalga oshiriladi kodlash orqali amalga oshiriladi autentifikatsiya orqali amalga oshiriladi shifrlash algoritmi orqali amalga oshiriladi

Correct1 [Question] Elektron hujjat yaxlitligini (o'zgarmasligini) tekshirish qaysi amal orqali amalga oshiriladi? ERI orqali amalga oshiriladi kodlash orqali amalga oshiriladi shifrlash algoritmi orqali amalga oshiriladi autentifikatsiya orqali amalga oshiriladi

Correct1 [Question] Elektron hujjat manbaini haqiqiylikini qaysi amal orqali amalga oshiriladi? ERI orqali amalga oshiriladi shifrlash algoritmi orqali amalga oshiriladi kodlash orqali amalga oshiriladi autentifikatsiya orqali amalga oshiriladi

Correct1 [Question] 1 ga va o'ziga bo'linadigan sonlar qanday sonlar hisoblanadi? tub sonlar murakkab sonlar toq sonlar juft sonlar

Correct1 [Question] Elliptik egri chiziqlarda nuqtalar usitda qanday ammalar bajariladi? nuqtalarni qo'shish va nuqtalarni ikkilantirish nuqtalarni qo'shish va nuqtalarni ko'paytirish nuqtalarni qo'shish va nuqtalarni bo'lish nuqtalarni ayirish va nuqtalarni ko'paytirish

Correct1 [Question] Sonlarni tublikka tekshiruvchi ehtimollikka asoslangan algoritmlar keltirilgan qatorni ko'rsating? Ferma, Solovey Shtrassen, Rabbi-Milner Ferma, Solovey Shtrassen, Eyler Eyler, Solovey Shtrassen, Rabbi-Milner Ferma, Eyler, Rabbi-Milner

Correct1 [Question] Sonlarni tublikka tekshiruvchi algoritmlar

qanday sinfga bo'linadi? aniqlashtirilgan va ehtimolli testlar aniqlashtirilgan va taqribiy testlar taqribiy va ehtimolli testlar aniqlashtirilgan, ehtimolli va taqribiy testlar Correct1 [Question]

Sonlarni tublikka tekshiruvchi algoritmlar necha sinfga bo'linadi? 2 3 4 5 Correct1 [Question]

Rabbi-Milner testi qanday turdagi tublikka testlovchi algoritm hisoblanadi? ehtimollik testlar tarkibiga kiruvchi algoritm aniqlashtirilgan testlar tarkibiga kiruvchi algoritm taqribiy testlar tarkibiga kiruvchi algoritm tublikka teslovchi algoritm hisoblanmaydi Correct1 [Question]

Solovey Shtrassen testi qanday turdagi tublikka testlovchi algoritm hisoblanadi? ehtimollik testlar tarkibiga kiruvchi algoritm aniqlashtirilgan testlar tarkibiga kiruvchi algoritm taqribiy testlar tarkibiga kiruvchi algoritm tublikka teslovchi algoritm hisoblanmaydi Correct1 [Question]

Ferma testi qanday turdagi tublikka testlovchi algoritm hisoblanadi? ehtimollik testlar tarkibiga kiruvchi algoritm aniqlashtirilgan testlar tarkibiga kiruvchi algoritm taqribiy testlar tarkibiga kiruvchi algoritm tublikka teslovchi algoritm hisoblanmaydi Correct1 [Question]

Kriptotizimlar kalitlar soni bo'yicha qanday turga bo'linadi? simmetrik va assimetrik simmetrik va bitta kalitli 3 kalitli kriptotizimlar assimetrik va 2 ta kalitli Correct1 [Question]

Kriptotizimlar kalitlar soni bo'yicha nechta turga bo'linadi? 2 3 4 5 Correct1 [Question]

Faqat simmetrik algoritm keltirilgan qatorni ko'rsating? AES RSA El-Gamal Barcha javoblar to'g'ri Correct1 [Question]

Kriptografiya bu -? axborotni o'zgartirish vositalari va usullarini o'rganadigan fan axborot mazmunidan beruxsat erkin foydalanishdan muhofazalash axborotni buzishning oldini olish axborot almashtirish vosita va usullari bilan shug'ullanadigan fa Correct1 [Question]

Shifrlash orqali ma'lumotning qaysi xususiyati ta'minlanadi? maxfiyligi butunliligi ishonchliligi foydalanuvchanliligi Correct1 [Question]

Ochiq kalitli shifrlash algoritmi keltirilgan qatorni toping? El-Gamal AES DES RC4 Correct1 [Question]

Ochiq kalitli shifrlash algoritmi keltirilgan qatorni toping? RSA AES DES RC4 Correct1 [Question]

RSA algoritmining mualliflarini ko'rsating R. Rayvest, A. Shamir, L. Adleman Diffi va M. Xellman R. Rayvest, K. Xellman, L. Adleman L. Adleman, El Gamal, K. Shnorrr Correct1 [Question]

Kriptotahlil nima bilan shug'ullanadi? kalit yoki algoritmni bilmagan holda shifrlangan ma'lumotga mos k ochiq ma'lumotlarni shifrlash masalalarining matematik uslublari maxfiy kodlarni yaratish bilan maxfiy kodlar orqali ma'lumotlarni yashirish bilan Correct1 [Question]

Sonlarni tublikka tekshirish algoritmlari necha sinfga bo'linadi? ikkita sinfga uchta sinfga bitta sinfga sinflarga bo'linmaydi Correct1 [Question]

Qanday sonlar tub sonlar hisoblanadi? 1 va o'ziga bo'linadigan sonlarlar barcha toq sonlar juft bo'lmagan sonlar 2 ga bo'linmaydigan sonlar Correct1 [Question]

Ochiq kalitli kriptotizimlarda asosan qanday turdagi sonlar bilan ishlaydi? tub sonlar bilan kasr sonlar bilan chekli maydonda kasr sonlar faqat manfiy sonlar Correct1 [Question]

Ochiq kalitli kriptotizimda, qaysi kalit orqali ma'lumot rasshifrovkalanadi? maxfiy kalit orqali ochiq kalit orqali ma'lumot shifrlanmaydi ushbu tizimda kalitdan foydalanilmaydi Correct1 [Question]

Ochiq kalitli kriptotizimlarda qaysi kalit orqali ma'lumot shifrlanadi? ochiq kalit orqali maxfiy kalit orqali ushbu tizimda kalitdan foydalanilmaydi ma'lumot shifrlanmaydi Correct1 [Question]

Ochiq kalitni kriptotizimlarda nechta kalitdan foydalanadi? ikkita bitta uchta kalitdan foydalanilmaydi Correct1 [Question]

Kalit bardoshliligi bu -? eng yaxshi ma'lum algoritm bilan kalitni topish murakkabligidir eng yaxshi ma'lum algoritm yordamida yolg'on axborotni ro'kach qi nazariy bardoshlilik amaliy bardoshlilik Correct1 [Question]

Kerkxofs printsipi nimadan iborat? kriptografik tizim faqat kalit noma'lum bo'lgan taqdirdagina maxf kriptografik tizim faqat yopiq bo'lgan taqdirdagina maxfiylik ta' kriptografik tizim faqat kalit ochiq bo'lgan taqdirdagina maxfiyl kriptografik tizim faqat ikkita kalit ma'lum bo'lgan taqdirdagina Correct1 [Question]

Assimetrik kriptotizimlarda necha kalitdan foydalaniladi? 2 ta 3 ta 4 ta kalit ishlatilmaydi Correct1 [Question]

Ochiq kalitli kriptotizimlarda qanday turdagi kalitlardan foydalanadi? ochiq va maxfiy kalitlardan maxfiy kalitlar juftidan maxfiy

kalitni uzatishni talab etmaydi ochiq kalitni talab etmaydi Correct1 [Question] Simmetrik kriptotizimlardagi qanday muammoni ochiq kalitli kriptotizimlar bartaraf etdi? maxfiy kalitni uzatish muammosini kalitni generatsiyalash muammosini ochiq kalitni uzatish muammosini kalitlar juftini hosil qilish muammosini Correct1 [Question] Kriptotizimlar kalitlar soni bo'yicha qanday turga bo'linadi? simmetrik va assimetrik turlarga simmetrik va bir kalitli turlarga 3 kalitli turlarga assimetrik va 2 kalitli turlarga Correct1 [Question] Kriptotizimlar kalitlar soni bo'yicha necha turga bo'linadi? 2 4 6 8 Correct1 [Question] Ochiq kalitli kriptotizimlar ma'lumotni qanday xususiyatini taminlaydi? maxfiyligini butunligini foydalanuvchanligini ma'lumotni autentifikatsiyasini Correct1 [Question] Kriptologiya so'zining ma'nosi? cryptos – maxfiy, logos – ilm cryptos – kodlash, logos – ilm cryptos – kripto, logos – yashiraman cryptos – maxfiy, logos – kalit Correct1 [Question] Kriptologiya necha yo'nalishga bo'linadi? 2 14 16 18 Correct1 [Question] Ochiq kalitli kriptotizimlar kim tomonidan kashf qilingan? U.Diffie va M.Hellman Rivest va Adlman Shamir va Rivest U.Diffie va Rivest Correct1 [Question] Shifrlash orqali ma'lumotning qaysi xususiyati ta'minlanadi? maxfiyligi butunligi ishonchliligi foydalanuvchanligi Correct1 [Question] Kriptotahlil nima bilan shug'ullanadi? maxfiy kodlarni buzish bilan maxfiy kodlarni yaratish bilan shifrlash uslublarini bilmagan holda shifrlangan ma'lumotni asl h maxfiy kodlar orqali ma'lumotlarni yashirish bilan Correct1 [Question] Kriptografiya nima bilan shug'ullanadi? maxfiy kodlarni yaratish bilan maxfiy kodlarni buzish bilan maxfiy kodlar orqali ma'lumotlarni yashirish bilan shifrlash uslublarini bilmagan holda shifrlangan ma'lumotni asl h Correct1 [Question] Kriptologiya nima bilan shug'ullanadi? maxfiy kodlarni yaratish va buzish ilmi bilan maxfiy kodlarni buzish bilan maxfiy kodlarni yaratish bilan maxfiy kodlar orqali ma'lumotlarni yashirish bilan Correct1 [Question] Kriptologiya qanday yo'nalishlarga bo'linadi? kriptografiya va kriptotahlil kriptografiya va kriptotizim kripto va kriptotahlil kriptoanaliz va kriptotizim Correct1 [Question] Ochiq kalitli El-Gamal shifrlash algoritmda "p" tub son bo'lsa maxfiy kalit qanday tanlanadi? (p-1) bilan o'zaro tub bo'lgan (1,p-1) intervaldagi butun son p bilan o'zaro tub bo'lgan (1,p-1) intervaldagi butun son (1,p-1) intervaldagi tub son (p-1) bilan o'zaro tub bo'lgan (1,p) intervaldagi butun son Correct1 [Question] Ochiq kalitli RSA shifrlash algoritmda "p=7" tub son bo'lsa Eyler funskiyasi  $\varphi(p)$  qanday qiymat qaytaradi? 6 7  $\varphi(7)$   $\varphi(6)$  Correct1 [Question] Ochiq kalitli RSA shifrlash algoritmda "p" tub son bo'lsa Eyler funskiyasi  $\varphi(p)$  qanday qiymat qaytaradi? p-1 p  $\varphi(p)$   $\varphi(p-1)$  Correct1 [Question] Ochiq kalitli RSA shifrlash algoritmda "d" shaxsiy kalit, "e" ochiq kalit bo'lsa shifrlash formulasi to'g'ri ko'rsatilgan qatorni belgilang?  $C=M^e \pmod N$   $C=M^e \pmod {\varphi(N)}$   $C=M^d \pmod {\varphi(N)}$   $C=M^d \pmod N$  Correct1 [Question] Ochiq kalitli RSA shifrlash algoritmda "e" ochiq kalit, "d" shaxsiy kalit bo'lsa d eshifrlash formulasi to'g'ri ko'rsatilgan qatorni belgilang?  $M=C^d \pmod N$   $M=C^d \pmod {\varphi(N)}$   $M=C^e \pmod N$   $M=C^e \pmod {\varphi(N)}$  Correct1 [Question] Ochiq kalitli RSA shifrlash algoritmda qaysi parametrlar ochiq holda e'lon qilinadi? N,e e N,d d Correct1 [Question] Ochiq kalitli RSA shifrlash algoritmda maxfiy kalit qanday topiladi?  $e*d=1 \pmod {\varphi(p*q)}$  taqqoslamadan  $e*d=1 \pmod N$   $e*d=1 \pmod {\varphi(p-1)}$   $e*d=1 \pmod {\varphi((p-1)(q-1))}$  Correct1 [Question] Ochiq kalitli RSA shifrlash algoritmda ochiq kalit "e" qanday topiladi?  $\varphi(N)$  bilan o'zaro tub va undan kichik bo'lgan son tanlanadi  $\varphi(N)$  dan kichik tub son tanlanadi  $\varphi(N)$  dan katta tub son tanlanadi  $\varphi(N)$  ning tub ko'paytuvchilaridan biri tanlanadi Correct1 [Question] Faktorlash muammosini yechishning Pollard usulida funksiya argumenti boshlangich qiymati nechiga teng bo'ladi? 2 1 3 0 Correct1 [Question] Faktorlash muammosini yechishning Pollard usulida eng kichik polinom qanday tanlanadi?  $x^2+1$   $x+1$   $x^2$  Correct1 [Question] Faktorlash muammosini yechishning Pollard usulida tanlanadigan funksiya qanday ko'rinishda bo'ladi? kvadratik polinom chiziqli polinom kubik polinom funksiya argumentiga bog'liq emas Correct1 [Question] Agar

sonlarni tublikka tekshirishning Rabin-Miller testida beshta tublikka guvohi mavjud bo'lsa tekshirilayotgan sonni tub bo'lishi ehtimoli nechiga teng?  $1-2^{(-5)}$   $1-(1/2)$   $1-2^5$   $1-5^{(-2)}$  Correct1

[Question] Agar sonlarni tublikka tekshirishning Ferma testida uchta tublikka guvohi mavjud bo'lsa tekshirilayotgan sonni tub bo'lishi ehtimoli nechiga teng?  $1-2^{(-3)}$   $1-(1/2)$   $1-2^3$   $1-3^{(-2)}$  Correct1

[Question] Agar sonlarni tublikka tekshirishning Solavey-Shtrassen testida ikkita tublikka guvohi mavjud bo'lsa tekshirilayotgan sonni tub bo'lishi ehtimoli nechiga teng?  $1-2^{(-2)}$   $1-(1/2)$   $1-2^2$   $1-(1/(2^{(-2)}))$  Correct1

[Question] “murakkabligiga guvoh” termini qaysi algoritmlarda ishlatiladi sonlarni tublikka tekshirish algoritmlarida shifrlash algoritmlarida kodlash algoritmlarida steganografik algoritmlarda Correct1

[Question] “soxta tublikka guvoh” termini qaysi algoritmlarda ishlatiladi sonlarni tublikka tekshirish algoritmlarida shifrlash algoritmlarida steganografik algoritmlarda kodlash algoritmlarida Correct1

[Question] “Psevdotub” termini qaysi algoritmlarda ishlatiladi sonlarni tublikka tekshirish algoritmlarida shifrlash algoritmlarida steganografik algoritmlarda kodlash algoritmlarida Correct1

[Question] Qanday sonlar murakkab sonlar deyiladi? ko'paytuvchilarga ajraladigan sonlar murakkab sonlar deyiladi ko'paytuvchilarga ajralmaydigan sonlar murakkab sonlar deyiladi ko'paytuvchilarga ajralmaydigan toq sonlar sonlar murakkab sonlar ko'paytuvchilarga ajraladigan juft sonlar murakkab sonlar deyiladi Correct1

[Question] RSA algoritmi qaysi tizimga mansub? Ochiq kalitli tizimlar Maxfiy kalitli tizimlar Xesh-funksiyalar Tasodifiy sonlar generatori Correct1

[Question] Sonlarni tublikka tekshirishda qaysi algoritm Karlmaykl sonlarida ham to'g'ri ishlaydi? Ferma algoritmidagi Solovey Shtrassen algoritmidagi Rabin-Milner algoritmidagi Eyler algoritmidagi Correct1

[Question] Sonlarni tublikka tekshirishda qaysi algoritm samarali hisoblanadi? Rabin Milner Solovey Shtrassen Ferma Eyler Correct1

[Question] Qaysi algoritm o'rtada turgan odam hujumiga bardoshsiz hisoblanadi? Diffie-Hellman RSA ElGamal DSA Correct1

[Question] Diffie-Hellman algoritmi qanday hujumga bardoshsiz hisoblanadi? o'rtada turgan odam hujumiga chastotalar tahlili hujumiga yon kanal tahlili hujumiga to'liq tanlash hujumiga Correct1

[Question] RSA shifrlash algoritmidagi qaysi parametrlar ochiq holda e'lon qilinadi? ochiq kalit – e, hamda modul qiymati - N maxfiy kalit – d, hamda modul qiymati - N ochiq kalit – e, hamda tub sonlar – p,q maxfiy kalit – d, hamda tub sonlar – p,q Correct1

[Question] Qaysi kalit orqali ERI qo'yiladi? shaxsiy kalit orqali ochiq kalit orqali kalit ishtirok etmaydi ikkala kalit birgalikda ishtirok etadi Correct1

[Question] O'zbekistonning qanday ERI standarti mavjud? O'zDSt 1092:2009 DSA ECDSA-2000 GOCT P 34.10-94 Correct1

[Question] O'zbekistonning nechta ERI standarti mavjud? 1 ta 2 ta 3 ta mavjud emas Correct1

[Question] Amerikaning qanday ERI standarti mavjud? DSA va ECDSA-2000 DSA va GOCT P 34.10-94 ECDSA-2000 va GOCT P 34.10-94 GOCT P 34.10-94 va O'zDSt 1092:2009 Correct1

[Question] Amerikaning nechta ERI standarti mavjud? 2 ta 1 ta 3 ta mavjud emas Correct1

[Question] RSA algoritmidagi p, q tub sonlar bo'lsa, modul qiymati N qanday topiladi?  $N=p*q$   $N=p/q$   $N=q/p$   $N=p-q$  Correct1

[Question] Karlmaykl sonlari qaysi tublikka tekshiruvchi algoritmlarda doim bajariladi? Ferma testida Solovey-Shtrassen testida Eyler testida Rabin testida Correct1

[Question] Faktorlash murakkabligiga asoslangan algoritm keltirilgan qatorni ko'rsating? RSA El-Gamal Diffie-Hellman DSA Correct1

[Question] Diskret logarifmlash murakkabligiga asoslangan algoritm keltirilgan qatorni ko'rsating? Diffie-Hellman, El-Gamal algoritmi RSA algoritmi El-Gamal algoritmi Diffie-Hellman algoritmi Correct1

[Question] RSA shifrlash algoritmidagi tanlangan p va q sonlarga qanday talab qo'yiladi? tub bo'lishi o'zaro tub bo'lishi butun son bo'lishi toq son bo'lishi Correct1

[Question] O'zDSt 1092:2009 ERI standarti birinchi algoritmi qanday rejimlarda ishlaydi? kalitli va kalitsiz ochiq kalitli va maxfiy kalitli ochiq va maxfiy 1 ta asosiy rejimi mavjud Correct1

[Question] Ochiq kalitli kriptotizimlarda elektron hujjatlarga qo'yilgan imzoni tekshirish qaysi kalit

orqali amalga oshiriladi? ochiq kalit orqali maxfiy kalit orqali imzo qo'yilishi kalitga bog'liq emas imzo qo'lda qo'yiladi Correct1 [Question] Ochiq kalitli kriptotizimlarda elektron hujjatlarga imzo qo'yish qaysi kalit orqali amalga oshiriladi? shaxsiy kalit orqali ochiq kalit orqali imzo qo'yilishi kalitga bog'liq emas imzo qo'lda qo'yiladi Correct1 [Question] ERI algoritmlari qanday muolajalardan iborat? imzoni shakllantirish, imzoni tekshirish imzoni shakllantirish, imzo qo'yish va imzoni tekshirish imzoni shakllantirish va imzo qo'yish imzo qo'yish Correct1 [Question] ERI algoritmlari nechta muolajadan iborat? ikkita bitta asosiy uchta to'rtta Correct1 [Question] Faqat tub son keltirilgan qatorni toping? 2, 5 5, 25 16, 3 3, 21 Correct1 [Question] Diffie-Hellman qanday algoritm hisoblanadi? kalitlarni ochiq taqsimlash algoritmi ochiq kalitli shifrlash algoritmi diskret logarifmlash murakkabligiga asoslangan shifrlash algoritm faktorlash murakkabligiga asoslangan kalitlarni ochiq taqsimlash Correct1 [Question] Diffie-Helman algoritmi qanday matematik murakkablikka asoslanadi? diskret logarifmlash murakkabligiga faktorlash murakkabligiga elliptik egri chiziqda diskret logarifmlash murakkabligiga elliptik egri chiziqda faktorlash murakkabligiga Correct1 [Question] Ochiq kalitli El-Gamal shifrlash algoritmi qanday matematik murakkablikka asoslanadi? diskret logarifmlash murakkabligiga faktorlash murakkabligiga elliptik egri chiziqda diskret logarifmlash murakkabligiga elliptik egri chiziqda faktorlash murakkabligiga Correct1 [Question] Ochiq kalitli RSA shifrlash algoritmi bardoshliligi qanday matematik muammo turiga asoslangan? faktorlash murakkabligiga diskret logarifmlash murakkabligiga elliptik egri chiziqlarda faktorizatsiyalash murakkabligiga elliptik egri chiziqlarda faktorizatsiyalash murakkabligiga Correct1 [Question] Sonlarni tublikka tekshirishning ehtimolli algoritmlariga quyidagilarning qaysilari kiradi? Ferma, Rabbi-Milner, Poklington testlari Rabbi-Milner, Solovey-Shtrassen, Pollard testlari Ferma, Solovey-Shtrassen, Pollard testlari Rabbi Milner, Poklington, Pollard testlari Correct1 [Question] Ehtimolli testlar sonlarni tublikka tekshirishda qanday natijani beradi? tekshirilayotgan son tub yoki tubmasligi haqida ehtimollik bilan tekshirilayotgan son tub yoki tubmasligi haqida kafolatlangan ani tekshirilayotgan son tub yoki tubmasligi haqida tasodifiy ravishd tekshirilayotgan son tub yoki tubmasligini 0 va 1 qiymatlarga qar Correct1 [Question] Faqat tub son keltirilgan qatorni toping? 3, 5 5, 15 16, 2 3, 18 Correct1 [Question] Ochiq kalitli kriptotizimlarning bardoshligini ta'minlashda qanday murakkab muammo turiga asoslanadi? faktorlash, diskret logarifmlash, elliptik egri chiziqda diskret faktorlash, diskret logarifmlash faktorlash, diskret logarifmlash, elliptik egri chiziqda faktoriz faktorlash, diskret logarifmlash, modulyar arifmetikaga Correct1 [Question] Ochiq kalitli kriptotizimlarning matematik asosi nimaga asoslangan? oson hisoblanadigan bir tomonlama funksiyalarga modulyar arifmetikaga faktorizatsiyalashga diskret logarifmlashga Correct1 [Question] Ochiq kalitli kriptotizimlar qanday turdagi matematik murakkablikka asoslangan algo ritmlarga bo'linadi? faktorizatsiyalash va diskret logarifmlash algoritmlariga modulyar arifmetika murakkabligiga asoslangan algoritmlarga diskret logarifmlash murakkabligiga asoslangan algoritmiga faktorizatsiyalash murakkabligiga asoslangan algoritmiga Correct1 [Question] RSA algoritmidan qanday maqsadda foydalaniladi? Shifrlash va elektron raqamli imzo Autentifikatsiya va xeshlash Shifrlash Elektron raqamli imzo Correct1 [Question] El Gamal algoritmidan qanday maqsadda foydalaniladi? Shifrlash va elektron raqamli imzo Autentifikatsiya va xeshlash Shifrlash Elektron raqamli imzo Correct1 [Question] DSSda qaysi algoritmdan foydalanilgan? Toxir El Gamal algoritmi K. Shnorr RSA ESIGN Correct1 [Question] DSA algoritmidan qanday maqsadda foydalaniladi? Elektron raqamli imzo Autentifikatsiya Shifrlash Xeshlash Correct1 [Question] EC DSA elektron raqamli imzo algoritmi qanday matematik murakkablik asosida yaratilgan? Elliptik egri chiziqli diskret logarifm Diskret logarifmlashni hisoblash Tub ko'paytuvchilarga ajratish Chiziqli algebratik tenglamalar sistemasini yechish

Correct1 [Question] Elektron raqamli imzo algoritmlari bardoshligini yanada oshirishda qanday funksiyalardan foydalaniladi? Xesh-funksiya Matematik funksiya Bir tomonlama funksiya Logarifmik funksiya Correct1 [Question] ГОСТ Р 34. 10-2001 elektron raqamli imzo algoritmda qaysi xesh-funksiyadan foydalaniladi? ГОСТ Р 34.11-94 O'z DSt 1106 A5 SHA-256 Correct1 [Question] Sonlarni tublikka tekshirishning Solovey-Shtrassen testida Lejandr simvoli qiymati qanday aniqlanadi? (a/p) (p/a) (p-1)/2 (a-1)/2 Correct1 [Question] Sonlarni tublikka tekshirishning Solovey-Shtrassen testida qanday simvoldan foydalanadi? Lejandr simvolidan Karlmaykl simvolidan Eyler simvolidan Lukas simvolidan Correct1 [Question] Elektron raqamli imzo bo'yicha birinchi O'z DSt 1092 qaysi korxona tomonidan ishlab chiqilgan? UNICON.UZ INFOCOM UZTELECOM O'zR axborot texnologiyalari va kommunikatsiyalarini rivojlanti Correct1 [Question] O'z DSt 1092 standarti qanday matematik murakkablik asosida yaratilgan? Parametrlil algebra Elliptik egri chiziqli diskret logarifm Diskret logarifmlashni hisoblash Tub ko'paytuvchilarga ajratish Correct1 [Question] O'z DSt 1092 standartida qanday amallardan foydalanilgan? Parametr bilan ko'paytirish, parametr bilan darajaga ko'tarish, Ko'paytirish, darajaga ko'tarish, teskarilash Qo'shish ayirish ko'paytirish, bo'lish Qo'shish, bo'lish, ayirish, darajaga ko'tarish Correct1 [Question] Umumiy bo'luvchi bu - Berilgan a va v sonlarni bo'luvchi butun son Berilgan a va v sonlarga karrali son Tub son O'zaro tub son Correct1 [Question] Eng katta umumiy bo'luvchi qanday belgilanadi? EKUB(a, b) EKUD EKUK EKUK(a,b) Correct1 [Question] Faktorlash – bu Berilgan sonning tub ko'paytuvchilarini topish Sonlar nazariyasining eng dastlabki masalalaridan biri Berilgan sonni biror amal yoki xususiyatga ko'ra uning tashkil et Berilgan to'plamni uning tashkil etuvchilari orqali ifodalanishi Correct1 [Question] Xeshlash algoritmlaridan qaysi xususiyatni ta'minlashda foydalaniladi? Butunlik Maxfiylik Foydalanuvchanlik Autentifikatsiya Correct1 [Question] AQSH ning elektron raqamli imzo standartini ko'rsating DSS DSA RSA ESIGN Correct1 [Question] DES shifrlash algoritmi... Simmetrik blokli shifr. Ochiq kalitli shifr. Assimetrik shifr. Ikki kalitli shifr. Correct1 [Question] Faktorlash muammosi ifodalangan qatorni ko'rsating?  $N=p \cdot q$ ;  $Y=(g^a) \bmod p$ ;  $N=\text{SQRT}(P)$ ;  $Y=g^a$ ; Correct1 [Question] 17 soni bilan o'zaro tub bo'lgan sonlarni ko'rsating? 16, 18 12, 34 14, 51 17 dan tashqari barcha sonlar Correct1 [Question] Qaysi algoritm Karlmaykl sonlarini murakkab son sifatida aniqlaydi? Solovey-Shtrassen algoritmi Ferma algoritmi Rabin Miller algoritmi RSA algoritmi Correct1 [Question] Eyler kriteriyasidan qaysi algoritmda foydalanadi? Solovey-Shtrassen algortmida Ferma algoritmda Rabin Miller algoritmda RSA algoritmda Correct1 [Question] Elliptik egri chiziqlarda funksiya koeffitsientlari a, b qiymati qanday shartni qanoatlantirishi kerak?  $4 \cdot a^3 + 27 \cdot b^2 \neq 0$   $4 \cdot a^2 + 27 \cdot b^2 \neq 0$   $4 \cdot a^3 + 27 \cdot b^3 \neq 0$   $4 \cdot a^2 + 27 \cdot b^3 \neq 0$  Correct1 [Question] 13 soni bilan o'zaro tub bo'lgan sonlarni ko'rsating? 5, 7 12, 26 14, 39 13 dan tashqari barcha sonlar Correct1 [Question] Agar RSA algoritmi uchun  $p=3$  va  $q=7$  bo'lsa,  $n$  va  $\varphi(n)$  ni hisoblang? 21, 12 21, 21 12, 21 12, 12 Correct1 [Question] Ochiq kalitli RSA shifrlash algoritmda " $p=11$ " tub son bo'lsa Eyler funksiyasi  $\varphi(p)$  qanday qiymat qaytaradi? 10 8 6 4 Correct1 [Question]  $-19 \bmod 11$  nechiga teng? 3 5 4 2 Correct1 [Question]  $143 \bmod 17$  nechiga teng? 7 6 5 8 Correct1 [Question] 2 lik sanoq tizimida 0101 soniga 1111 sonini 2 modul bo'yicha qo'shing? 1010 101 1111 1001 Correct1 [Question] Sonlarni tublikka tekshirishning Solovey-Shtrassen testida Lejandr simvoli qanday qiymatlarni qabul qilishi mumkin? 0,-1,1 0,1 0,-1 1, -1 Correct1 [Question] Sonlarni tublikka tekshirishning Solovey-Shtrassen testida qanday simvoldan foydalanadi? Lejandr simvolidan Karlmaykl simvolidan Eyler simvolidan Lukas simvolidan Correct1 [Question] Sonlarni tublikka tekshirishning Solovey-Shtrassen testida qanday taqqoslamadan foydalanadi?  $a^{((p-1)/2)} = (a/p) \bmod p$   $a^{((p-1)/2)} = 1 \bmod p$   $a^{((p-1)/2)} \neq (a/p) \bmod p$   $a^{((p-1)/2)} \neq 1 \bmod p$  Correct1 [Question] Sonlarni tublikka

tekshirishning Ferma testida qanday taqqoslama bajarilganda tekshirilayotgan son murakkab bo'ladi?  $a^{n-1} \equiv 1 \pmod{n}$   $a^{n-1} \equiv 1 \pmod{n}$   $a^{(n-1)} \equiv 1 \pmod{n}$   $a^{(n-1)} \equiv 1 \pmod{n}$  Correct1 [Question] Sonlarni tublikka tekshirishning Ferma testida qanday taqqoslamadan foydalaniladi?  $a^{n-1} \equiv 1 \pmod{n}$   $a^{(n-1)} \equiv 1 \pmod{n}$   $a^{(n)} \equiv 1 \pmod{n}$   $a^{n-1} \equiv 1 \pmod{n}$  Correct1 [Question] Sonlarni tublikka tekshirishning Solovay-Shtraassen testida qanday kriteriyadan foydalaniladi? Eyler kriteriyasidan Karlmaykl sonlari kriteriyasidan Murakkab sonlar kriteriyasidan Tub sonlar kriteriyasidan Correct1 [Question] O'zDSt 1092:2009 ERI standarti ikkinchi algoritmi qanday murakkablikka asoslanadi? elliptik egri chiziqlarda diskret logarifmlash murakkabligiga diskret logarifmlash murakkabligiga faktorizatsiyalash murakkabligiga elliptik egri chiziqlarda faktorizatsiyalash murakkabligiga Correct1 [Question] O'zDSt 1092:2009 ERI standarti birinchi algoritmi qanday murakkablikka asoslanadi? daraja parametr muammosiga diskret logarifmlash muammosiga faktorizatsiyalash muammosiga elliptik egri chiziqlarda faktorizatsiyalash murakkabligiga Correct1 [Question] DSA ERI standarti qanday murakkablikka asoslanadi? diskret logarifmlash masalasini murakkabligiga faktorizatsiyalash masalasi murakkabligiga elliptik egri chiziqlarga asoslangan diskret logarifmlash masalasi elliptik egri chiziqlarga asoslangan faktorizatsiyalash masalasi Correct1 [Question] O'zDSt 1092:2009 standarti bu? ERI standarti Shifrlash standarti Xesh funksiya standarti Kalitni generatsiyalash standarti Correct1 [Question] Ochiq kalitli kriptotizimlarga asoslangan ERI algoritmlarida kalitlar juftini qaysi tomon hosil qiladi? kalitlar juftini ma'lumot yuboruvchi tomon hosil qiladi kalitlar juftini ma'lumot qabul qiluvchi tomon hosil qiladi kalitlar juftini har bir foydalanuvchining o'zi hosil qiladi uchinchi ishonchli tomon hosil qiladi Correct1 [Question] ERI algoritmlari qanday turdagi masalalarni yechishga imkon beradi? ma'lumot yaxlitligini tekshirish, ma'lumot manbani autentifikatsiya ma'lumot yaxlitligini tekshirish, ma'lumot manbani autentifikatsiya ma'lumot manbani autentifikatsiyalash hamda rad etishdan himoyalash ma'lumot yaxlitligini tekshirish, rad etishdan himoyalash Correct1 [Question] Qanday algoritm yordamida diskret logarifmlash muammosini bartaraf etiladi? Polig-Hellman algoritmi Diffie-Hellman algoritmi Pollard algoritmi Eyler-Ferma algoritmi Correct1 [Question] Ochiq kalitli kriptotizimlarga asoslangan kalitlarni taqsimlovchi Diffie-Hellman algoritmi vazifasi nima? umumiy maxfiy kalitni hosil qilish ochiq va yopiq kalitlar juftini hosil qilish maxfiy kalitni uzatishni talab etmaydi ochiq kalitlarni hosil qilish Correct1 [Question] Ochiq kalitli RSA shifrlash algoritmidagi "e" ochiq kalit bo'lsa shifrlash formulasi to'g'ri ko'rsatilgan qatorni belgilang?  $C = M^e \pmod{N}$   $C = M^e \pmod{(N)}$   $C = M^d \pmod{(N)}$   $C = M^d \pmod{N}$  Correct1 [Question] Ochiq kalitli RSA shifrlash algoritmidagi "d" maxfiy kalit bo'lsa rasshifrovkalash formulasi to'g'ri ko'rsatilgan qatorni belgilang?  $M = C^d \pmod{N}$   $M = C^d \pmod{(N)}$   $M = C^e \pmod{N}$   $M = C^e \pmod{(N)}$  Correct1 [Question] Nosimmetrik kriptografiya asosida birinchi bo'lib elektron raqamli imzo bo'yicha milliy standart yaratgan davlat? AQSh Germaniya Rossiya Koreya Correct1 [Question] Aniqlashtirilgan testlar sonlarni tublikka tekshirishda qanday natijani beradi? tekshirilayotgan son tub yoki tubmasligi haqida kafolatlangan aniqlashtirilgan son tub yoki tubmasligi haqida tasodifiy ravishda tekshirilayotgan son tub yoki tubmasligi haqida ehtimollik bilan tekshirilayotgan son tub yoki tubmasligini 0 va 1 oraliqidagi qiymat Correct1 [Question] Malumotni shifrlash va deshifrlashda turli kalitlardan foydalanuvchi algoritmi qanday? El-Gamal AES DES RC4 Correct1 [Question] "A" va "B" foydalanuvchilar maxfiy tarzda ma'lumot almashmoqchi, "A" foydalanuvchi qabul qilgan ma'lumotni rasshifrovkalash uchun qaysi kalitdan foydalanadi? o'zining maxfiy kalitidan foydalanadi o'zining ochiq kalitidan foydalanadi "B" foydalanuvchining maxfiy kalitidan foydalanadi "B" foydalanuvchining ochiq kalitidan foydalanadi Correct1 [Question] "A" va "B" foydalanuvchilar maxfiy tarzda ma'lumot almashmoqchi, "A" foydalanuvchi ma'lumotni

shifrlab yuborish uchun qaysi kalitdan foydalanadi? "B" foydalanuvchining ochiq kalitidan foydalanadi o'zining ochiq kalitidan foydalanadi "B" foydalanuvchining maxfiy kalitidan foydalanadi o'zining maxfiy kalitidan foydalanadi Correct1 [Question] Quyida keltirilgan qaysi standart ochiq kalitli infratuzilmalar uchun mo'ljallangan? X.509 standarti DSA standarti ECDSA standarti RSA standarti Correct1 [Question] X.509 standarti nima uchun mo'ljallangan? ochiq kalitli infratuzilmalar uchun raqamli imzo uchun maxfiy kalit uchun ochiq kalit uchun Correct1 [Question] Tashkilot imzosi nimada aks etishi kerak? raqamli sertifikatda shifrlashda kodlashda raqamli imzoda Correct1 [Question] Foydalanuvchi ochiq kaliti nimada aks etishi kerak? raqamli sertifikatda raqamli imzoda shifrlashda kodlashda Correct1 [Question] Foydalanuvchi nomi haqidagi ma'lumotlar nimada aks etishi kerak? raqamli sertifikatda raqamli imzoda shifrlashda kodlashda Correct1 [Question] Raqamli sertifikat qanday parametrlarni o'z ichiga oladi? foydalanuvchi nomini, uning ochiq kalitini va tashkilot imzosini foydalanuvchi nomini, uning maxfiy kalitini va tashkilot imzosini foydalanuvchi maxfiy hamda ochiq kalitini va tashkilot imzosini foydalanuvchi maxfiy hamda ochiq kalitini Correct1 [Question] Ochiq kalit kafolati deganda nima tushiniladi? ochiq kalit domenda bo'lishi va hammaga ko'rinishi tushiniladi maxfiy kalit domenda bo'lishi va hammaga ko'rinishi tushiniladi ochiq kalit domenda bo'lishi va hammadan sir saqlanishi tushiniladi maxfiy kalit domenda bo'lishi va hammadan sir saqlanishi tushiniladi Correct1 [Question] Shaxsiy kalitni maxfiyligini saqlash deganda nima tushiniladi? kalitni boshqarish davomida tomonlardan maxfiy tarzda saqlanishi kalitni to'g'riligiga kafolat berilishi kalitlarni butunligini ta'minlanishi kalitni raqamli sertifikat bilan maxfiyligini ta'minlanishi Correct1 [Question] Ochiq kalitni taqsimlash jarayoni qaysi tizimga tegishli ochiq kalitlar infratuzilmasiga autentifikatsiya tizimlariga simmetrik kriptotizimlarga identifikatsiya tizimlariga Correct1 [Question] Ochiq kalitni identifikatsiyalash jarayoni qaysi tizimga tegishli ochiq kalitlar infratuzilmasiga identifikatsiya tizimlariga autentifikatsiya tizimlariga simmetrik kriptotizimlarga Correct1 [Question] Ochiq kalitlar infratuzilmasi nimalarni ta'minlaydi? ochiq kalitni identifikatsiyalash va uni taqsimlashni maxfiy kalitni identifikatsiyalash va uni taqsimlashni ochiq kalitni identifikatsiyalash va uni saqlash maxfiy kalitni identifikatsiyalash va uni saqlash Correct1 [Question] Elektron raqamli imzo bo'yicha birinchi standart? DSS RSA DES AES Correct1 [Question] Qanday kriptotizimlarda ochiq kalit kafolati talabi qo'yiladi? ochiq kalitli kriptotizimlarda bunday kriptotizim mavjud emas simmetrik kriptotizimlarda maxfiy kalitli kriptotizimlarda Correct1 [Question] Malumotni shifrlash va deshifrlashda turli kalitlardan foydalanuvchi algoritmni ko'rsating? RSA AES DES RC4 Correct1 [Question] Ochiq kalitli kriptotizimlarda kalitlarni boshqarishda qanday talab qo'yiladi? shaxsiy kalit maxfiyligini saqlash hamda ochiq kalit kafolati shaxsiy kalitni generatsiyalash hamda uni maxfiyligini saqlash ochiq kalitni generatsiyalash hamda uni maxfiyligini saqlash ochiq kalit maxfiyligini saqlash hamda maxfiy kalit kafolati Correct1 [Question] Elliptik egri chiziqda nuqtalarni qo'shish qaysi algoritm bajariladi? ECDSA EL-Gamal DSA RSA Correct1 [Question] El-Gamal asosidagi ERI algoritmda qaysi kalit orqali elektron hujjatga imzo qo'yiladi? maxfiy kalit orqali kalit ishlatilmaydi imzo qo'lda qo'yiladi ochiq kalit orqali Correct1 [Question] El-Gamal asosidagi ERI algoritmda qaysi kalit orqali elektron hujjatga qo'yilgan imzo tekshiriladi? ochiq kalit orqali maxfiy kalit orqali kalit ishlatilmaydi imzo qo'lda qo'yiladi Correct1 [Question] RSA asosidagi ERI algoritmda qaysi kalit orqali elektron hujjatga qo'yilgan imzo tekshiriladi? ochiq kalit orqali maxfiy kalit orqali imzo qo'lda qo'yiladi kalit ishlatilmaydi Correct1 [Question] RSA asosidagi ERI algoritmda qaysi kalit orqali elektron hujjatga imzo qo'yiladi? maxfiy kalit orqali ochiq kalit orqali kalit ishlatilmaydi imzo qo'lda qo'yiladi Correct1 [Question] El-Gamal shifrlash algoritmda qaysi parametrlar ochiq holda e'lon qilinadi? p tub son hamda p modul bo'yicha birlamchi ildiz g p va g



tub sonlarni( $p > g$ )  $p$  va  $g$  toq sonlarni( $p > g$ )  $p$  va  $g$  juft sonlarni( $p > g$ ) Correct1 [Question] Diffie-Hellman algoritmidagi qaysi parametrlar ochiq holda e'lon qilinadi?  $p$  va  $g$  tub sonlarni( $p > g$ )  $p$  tub sonni  $p$  va  $g$  toq sonlarni( $p > g$ )  $p$  va  $g$  juft sonlarni( $p > g$ ) Correct1 [Question] Evklidning kengaytirilgan algoritmdan RSA shifrlash algoritmining qaysi parametrini hisoblashda foydalaniladi? maxfiy kalitni ochiq kalitni tub sonlarni modul qiymatini Correct1 [Question] Elliptik egri chiziqda diskret logarifmlash muammosiga asoslangan algoritmi ko'rsat ing? ECDSA El-Gamal DSA RSA Correct1 [Question] Faktorlash muammosiga asoslangan algoritmi ko'rsating? RSA El-Gamal DSA ECDSA Correct1 [Question] RSA algoritmidagi maxfiy kalitni hisoblashda qaysi algoritmdan foydalanish mumkin? Evklidning kengaytirilgan algoritmdan qoldiqlar haqidagi Xitoy teoremasidan parameter bo'yicha darajaga oshirishdan Pohlig-Hellman algoritmdan Correct1 [Question] Diskret logarifm murakkabligini bartaraf etishda Pohlig-Hellman algoritmidagi yana qanday qo'shimcha usuldan foydalaniladi? qoldiqlar haqidagi Xitoy teoremasidan Evklid algoritmdan kengaytirilgan Evklid algoritmdan parameter bo'yicha darajaga oshirishdan Correct1 [Question] Qoldiqlar haqidagi Xitoy teoremasidan qaysi algoritmda foydalaniladi? Pohlig-Hellman algoritmidagi Pollard algoritmda RSA algoritmda El-Gamal algoritmda Correct1 [Question] El-Gamal algoritmidagi matematik murakkablikni qanday usul orqali bartaraf qilish mumkin? Pohlig-Hellman usuli Pollard usuli Xitoy teoremasi El-Gamal usuli Correct1 [Question] Pohlig-Hellman usuli qanday turdagi matematik murakkablikni yechishda foydalaniladi? diskret logarifmlash murakkabligini faktorlash murakkabligini elliptik egri chiziqda faktorlash murakkabligini daraja parameter murakkabligini Correct1 [Question] Diskret logarifmlash muammosini bartaraf etuvchi usul keltirilgan qatorni ko'rsating? Pohlig-Hellman usuli Pollard usuli Xitoy teoremasi RSA usuli Correct1 [Question] RSA algoritmidagi matematik murakkablikni qanday usul orqali bartaraf qilish mumkin? Pollard usuli Xitoy teoremasi Pohlig-Hellman usuli RSA usuli Correct1 [Question] Pollard usuli qanday turdagi matematik murakkablikni yechishda foydalaniladi? faktorlash murakkabligini diskret logarifmlash murakkabligini elliptik egri chiziqda diskret logarifmlash murakkabligini elliptik egri chiziqda faktorlash murakkabligini Correct1 [Question] Faktorlash muammosini bartaraf etuvchi usul keltirilgan qatorni ko'rsating? Pollard usuli Xitoy teoremasi Pohlig-Hellman usuli RSA usuli Correct1 [Question] Elliptik egri chiziqqa asoslangan Diffie-Hellman algoritmi qanday matematik murakkablikka asoslangan? Elliptik egri chiziqda diskret logarifmlash murakkabligiga asoslangan Diskret logarifmlash murakkabligiga asoslangan Elliptik egri chiziqda nuqtalarni ikkilantirish murakkabligiga asoslangan Elliptik egri chiziqda nuqtalarni qo'shish murakkabligiga asoslangan Correct1 [Question] O'zDSt ERI standartida,  $R$  - parametr e'lon qilinishi qanday bo'ladi? maxfiy xolatda e'lon qilinadi ochiq holatda e'lon qilinadi har bir tomon o'ziga alohida hisoblaydi  $R$  parametrdan foydalanmaydi Correct1 [Question] 7 soni bilan o'zaro tub bo'lgan sonlarni ko'rsating? 2,3,6 14,2,5 1,7,5 6,21,2 Correct1 [Question] RSA algoritmidagi  $p=3$ ,  $q=11$ ,  $e=3$  bo'lganda maxfiy kalitni qiymati topilsin:  $e \cdot d \equiv 1 \pmod{(N)}$ ? 7 6 8 5 Correct1 [Question] Faktorlash muammosini yechishning Pollard algoritmda dastlabki tub ko'paytuvchi topilgandan keyin qanday shart bajarilsa hisoblash tugatiladi?  $N/d$  hisoblanadi, agar natija tub bo'lsa hisoblash tugatiladi  $N/d$  hisoblanadi, agar natija tub bo'lmasa hisoblash tugatiladi  $d$  hisoblanadi, agar natija tub bo'lsa hisoblash tugatiladi  $d$  hisoblanadi, agar natija tub bo'lmasa hisoblash tugatiladi Correct1 [Question] O'zDSt 1092:2009 ERI standarti nechta algoritmdan iborat? 2 ta 3 ta 4 ta 1 ta asosiy Correct1 [Question] "A" va "B" foydalanuvchilar o'rtasida ma'lumot almashinishida qanday buzilishlar bo'lishi mumkin? rad etish, modifikatsiyalash, soxtalashtirish, takrorlash modifikatsiyalash, soxtalashtirish, maxfiylashtirish, takrorlash rad etish, modifikatsiyalash, soxtalashtirish, maxfiylashtirish rad etish, modifikatsiyalash, soxtalashtirish, maxfiylashtirish,

Correct1 [Question] "A" va "B" foydalanuvchilar o'rtasida elektron ma'lumot almashinishida "rad etish" qoida buzilishi qanday amalga oshiriladi? "A" foydalanuvchi yuborgan ma'lumotini yuborganligini rad etishi "A" foylanuvchi ma'lumotini qabul qilganligini rad etishi "A" foydalanuvchini o'rtada turgan odam tomonidan o'zgartirilganl "A" foydalanuvchi yuborgan ma'lumotini yubormaganligini rad etish Correct1 [Question] ERI qaysi xususiyatni taminlamaydi? Konfidensiallikni Rad etishni oldini olishni Yaxlitlikni Ma'lumot egasi shaxsini ko'rsatishni Correct1 [Question] Ochiq kalitli kriptotizimlarga asoslangan ERI algoritmda xesh funksiyaning roli qanday? ma'lumotni yaxlitligini tekshirishda foydalaniladi ma'lumotni maxfiyligini ta'minlashda foydalaniladi ma'lumotni deshifrlashda foydalaniladi ma'lumotni kim tomonidan yuborilganini tekshirishda foydalaniladi Correct1 [Question] "A" va "B" foydalanuvchilar ma'lumot almashmoqchi, "B" foydalanuvchi elektron hujja tga imzo qo'yish uchun qaysi kalitdan foydalanadi? "B" foydalanuvchini o'zining maxfiy kalitidan "A" foydalanuvchining maxfiy kalitidan "B" foydalanuvchi o'zining ochiq kalitidan "A" foydalanuvchining ochiq kalitidan Correct1 [Question] "A" va "B" foydalanuvchilar ma'lumot almashmoqchi, "A" foydalanuvchi elektron hujja tga imzo qo'yish uchun qaysi kalitdan foydalanadi? "A" foydalanuvchini o'zining maxfiy kalitidan "B" foydalanuvchining maxfiy kalitidan "A" foydalanuvchi o'zining ochiq kalitidan "B" foydalanuvchining ochiq kalitidan Correct1 [Question] "A" va "B" foydalanuvchilar ma'lumot almashmoqchi, "B" foydalanuvchi qabul qilgan ma'lumotni imzosini tekshirishda qaysi kalitdan foydalanadi? "A" foydalanuvchining ochiq kalitidan "A" foydalanuvchining maxfiy kalitidan "B" foydalanuvchi o'zining ochiq kalitidan "B" foydalanuvchini o'zining maxfiy kalitidan Correct1 [Question] "A" va "B" foydalanuvchilar ma'lumot almashmoqchi, "A" foydalanuvchi "B" tomondan qabul qilgan ma'lumotni imzosini tekshirishda qaysi kalitdan foydalanadi? "B" foydalanuvchining ochiq kalitidan "B" foydalanuvchining maxfiy kalitidan "A" foydalanuvchi o'zining ochiq kalitidan "A" foydalanuvchini o'zining maxfiy kalitidan Correct1 [Question] Ochiq kalitli kriptotizimlarga asoslangan kalitlarni taqsimlash Diffie-Hellman algo ritmi ishlash prinsipi qanday? umumiy maxfiy kalitni hosil qilishga asoslangan ochiq va yopiq kalitlar juftini hosil qilishga asoslangan maxfiy kalitni uzatishni talab etmaydigan prinsipga asoslangan ochiq kalitlarni hosil qilishga asoslangan Correct1 [Question] Ochiq kalitli El-Gamal shifrlash algoritmda ochiq kalit qanday hisoblanadi?  $y = g^a \pmod{p}$ , bu yerda g-birlamchi ildiz, a-maxfiy kalit, p-tub  $y = g^a \pmod{p}$ , bu yerda g-soni (p-1) dan kichik butun son, a-maxf  $y = g^a \pmod{p}$ , bu yerda g-soni p dan kichik butun son, amaxfiy k  $y = g^a \pmod{p}$ , bu yerda g-soni (p-1) bilan o'zaro tub bo'lgan but Correct1 Qanday funksiyalar asosiy akslantirishlar deyiladi Aralashtirish va tarqatish xususiyatlariga ega bo'lgan funksiyalar Shifrlash ... :Kalitdan foydalangan holda almashtirish uchun amalga oshiriladigan qayta almashtirishlar majmui ochiq ma'lumotni shifrlash va deshifrlash jarayonini tashkil etuvchi amallar majmui bo'lib, alifbo belgilarini almashtirish ketma ketligidan iborat :Kriptografik tizim ... shifrlash kaliti noma'lum bo'lgan holda shifrlangan ma'lumotni deshifrlashning qiyinlik darajasini belgilaydi :Kriptobardoshlilik Kriptotizimlar qanday turlarga bo'linadi? :Simmetrik va asimmetrik kriptotizim Axborotni aslidan o'zgartirilgan holatga akslantirish uslublarini topish va takomillashtirish bilan shug'ullanadigan fan nima deb ataladi? :Kriptografiya DES algoritmda dastlabki raund kaliti necha bitga teng? :48 bit DES da dastlabki kalit uzunligi necha bitga teng? :56 bit DES da blok har birining uzunligi necha bitga teng? :32 bit DES da raundlar soni nechta? 6:40 DES da S blok kanday funksiya bajaradi? #6 bitli blokni 4 bitga almashtiradi DES da blok E kengaytirilishidan so'ng kanday amal bajariladi? kalit bilan XOR amali bilan qo'shiladi DES qaysi tarmog' asosida ishlaydi #Feystel tarmog'i asosida DES da IP jadval qanday ish bajaradi? #Berilgan jadval bo'yicha bitlarning o'rnini aralashtiradi DES da shifrlangan matn bloki necha bitdan iborat buladi? :64 bit DES da S bloklar

soni nechta? 14:40 Kriptotizim – bu :shifrlash jarayonini tashkil etuvchi barcha amallar majmui : DES shifrlash algoritmi nechanchi yilda yaratilgan :1976 yilda Shifrlash kaliti noma'lum bo'lganda shifrlangan ma'lumotni deshifrlash qiyinlik darajasini nima belgilaydi :kriptobardoshlik Klassik shifrlash algoritmlari necha turga bo'linadi 19:40 O'rniga qo'yish shifrlash algoritmi nechta turga bo'linadi 20:40 Ochiq matndagi bitta belgi o'rniga shifr matndagi bitta belgi mos qo'yilsa, bunday o'rniga qo'yish algoritmi nima deyiladi :bir qiymatli Shifrlashda ishlatiladigan kalitlar qanday bo'ladi :simmetrik va asimmetrik Kriptotahlil bilan shug'ullanuvchi insonlar kimlar? :kriptoanalitiklar Agar A alfavit m ta elementdan iborat bo'lsa, u holda A to'plamdagi barcha o'rniga qo'yishlar soni nimaga teng bo'ladi? :m! Shifrlash algoritmlarida samarali tarqatish akslantirishi uchun, odatda, qanday akslantirishdan foydalaniladi :S blok Kriptotizim – bu :shifrlash jarayonini tashkil etuvchi barcha amallar majmui O'rniga qo'yish –almashtirish tarmoqlariga asoslangan shifrlash algoritmi qanday ataladi :SP– tarmoq AES shifrlash standartining mualliflari kimlar :Ridjmen va Deimen Barcha simmetrik shifrlash algoritmlari qanday shifrlash usullariga bo'linadi :blokli va oqimli DES shifrlash algoritmda kalit uzunligi va blok uzunligi mos holda qancha bo'lishi kerak :56 bit, 64 bit DES shifrlash algoritmi nechta rejimda ishlashi belgilab qo'yilgan :4 ta Shifrlanuvchi bloklar bir biriga bog'liq bo'lmagan holda alohida shifrlash algoritmi orqali qayta ishlanadigan DES shifrlash algoritmining rejimi qaysi :ECB DES shifrlash algoritmi qaysi tarmoqqa asoslangan :Feystel tarmog'i DES shifrlash algoritmda kalitlar fazosi necha bitdan iborat 110:40:00 DES shifrlash algoritmda shifrlanadigan malumotlar bloki necha bit? 102:40:00 DES shifrlash algoritmda shifrlash jarayoni nimalardan iborat? :kiruvchi blok, boshlang'ich almashtirish,16 raundli shifrlash va yakuniy almashtirish DES shifrlash algoritmda i raundi necha bitli kalitdan foydalaniladi? 118:40:00 XOR amali qanday amal? :2 modul bo'yicha qo'shish DES shifrlash algoritmda kengaytirish funksiyasi qanday vazifani bajaradi? :32 bitli blokni 48 bitli blokka kengaytiradi DES shifrlash algoritmi nechta rejimda ishlaydi? 18:40 DES shifrlash algoritmi kalitlarni kodlashda qaysi rejimdan foydalanadi? :ECB rejimi DES shifrlash algoritmda S bloklar nima uchun ishlatiladi? :48 bitli blokni 32 bitli blokka aylantirish uchun DES shifrlash algoritmda nechta S blok bor? 14:40 Sesar shifrlash usulini ko'rsating. : $(m + k) \bmod 26$  m harf tartib raqami, k kalit DES shifrlash algoritmda ochiq matn necha bitdan bloklarga ajratiladi? 102:40:00 DES shifrlash algoritmda shifrlash funksiyasini hosil qilishda nimalardan foydalaniladi? :E kengaytirish funksiyasi, kalit, S bloklardan, P almashtirishdan Xavfsizlik siyosati quyidagilar asosida yaratiladi :tashkilot ma'lumot tizimlarining umumiy tavsiflari asosida Shifrlashtirish so'zining ma'nosi nima? :Shifrlashtirish – almashtirish jarayoni bo'lib, berilgan matn shifrlangan matn bilan almashtiriladi. Deshifrlashtirish so'zining ma'nosi nima? :Deshifrlashtirish – shifrlashtirishga teskari jarayon. Kalit asosida shifrlangan matn o'z holatiga uzgartiriladi. Alfavit – bu :axborotni kodlashtirish uchun ishlatiladigan chekli belgilar to'plami. Kalit – bu? :kalit – matnlarni shifrlash va deshifrlash uchun kerak bo'lgan axborot Simmetrik kriptotizimlarda shifrlash va deshifrlashda qanday kalit ishlatiladi? :Bir xil kalit Ochiq kalitli tizimda shifrlash va deshifrlash uchun qanday kalit ishlatiladi? :ochiq va yopiq Kriptomustahkamlik – bu :Shifrning deshifrlashga nisbatan mustahkamligini xarakterlaydi Axborotni himoyalash maqsadida shifrlashning effektivligi quyidagilarga bog'liq? :Shifrni kriptomustahkamligi va kalitning sirini saqlashga Shifrlangan ma'lumot o'qilishi mumkin faqat :Kaliti berilgan bo'lsa Shifrlangan xabarning ma'lum qismi va unga mos keluvchi ochiq matn bo'yicha ishlatilgan shifrlash kalitining kerakli jarayonlar sonini aniqlash quyidagilardan iborat :Mumkin bo'lgan kalitlarning umumiy sonidan kam bo'lmagan Kalitlarni sezilarsiz o'zgartirish quyidagilarga olib kelishi mumkin :bitta va bir xil kalitdan foydalanganda ham shifrlangan xabarlar sezilarli darajada o'zgarishga :ga bo'ladi Quyidagilar bo'lmasligi kerak :shifrlash jarayonida

muntazam qo'llanadigan kalitlar orasida sodda va osongina aniqlash mumkin bo'lgan bog'liqlik

Mumkin bo'lgan to'plamlardan olingan har qanday kalitlar ... ni ta'minlaydi :axborotni ishonchli himoyalash

Simmetrik kriptotizim uchun qanday usullar qo'llaniladi? :o'rin almashtirish, gammalash, blokli shifrlash

Sezar almashtirishning mazmuni qanday izohlanadi? :Sezar almashtirish monoalfavitli guruhiga qarashli

Axborotni kodlash uchun foydalaniladigan chekli sondagi belgilar to'plami ... deb ataladi :Alifbo Alifboning elementlaridan (belgilaridan) tashkil topgan tartiblangan tuzilma ... deb ataladi :Matn

Dastlabki ma'lumotni bevosita shifrlash va deshifrlash uchun zarur manba ... deb ataladi :Kalit

Ochiq matn deb ataluvchi dastlabki ma'lumotni shifrlangan ma'lumot (kriptogramm holatiga o'tkazish jarayoni ... deb ataladi :Shifrlash

Shifrlashga teskari bo'lgan jarayon, ya'ni kalit yordamida shifrlangan ma'lumotni dastlabki holatga o'tkazish ... deb ataladi :Deshifrlash ...

ochiq ma'lumotni shifrlash va deshifrlash jarayonini tashkil etuvchi amallar majmui bo'lib, alifbo belgilarini almashtirish ketma ketligidan iborat. :Kriptografik tizim ...

shifrlash kaliti noma'lum bo'lgan holda shifrlangan ma'lumotni deshifrlashning qiyinlik darajasini belgilaydi. :Kriptobardoshlilik

Quyidagilardan qaysi biri matn jo'natilgan shaxsga qabul qilingan elektron matnning va matnni raqamli imzolovchining haqiqiy yoki nohaqiqiylikni aniqlash imkonini beradi? :Elektron raqamli imzo

Qaysi kriptotizimda shifrlash uchun ham va deshifrlash uchun ham bir xil kalitdan foydalaniladi? :Simmetrik kriptotizim ...

kriptobardoshli kalitlarni ishlab chiqish (yoki yaratish), ularni saqlash, hamda kalitlarni foydalanuvchilar orasida muhofazalangan holda taqsimlash jarayonlarini o'z ichiga oladi. :Kalitlarni taqsimlash va boshqarish

Ochiq kalitli kriptotizimlarda qanday kalitlar foydalaniladi? :ochiq va yopiq kalitlar

Kriptologiya maqsadlari o'zaro qarama qarshi bo'lgan ikkita yo'nalishiga ega. Bular qaysilar? :Kriptografiya va kriptotahlil

Kriptotizimlar ikki qismga bo'linadi. Bular qaysilar? :Simmetrik va asimmetrik kriptotizim

Axborotni aslidan o'zgartirilgan holatga akslantirish uslublarini topish va takomillashtirish bilan shug'ullanadigan fan qaysi? :Kriptografiya

Axborotni muxofaza qilish masalalari bilan shug'ullanadigan fan bo'lib

Cryptos maxfiy, logos ilm degan ma'noni anglatadigan fan qaysi? :Kriptologiya

Kriptotahlilchilarni maxfiyligi ta'minlangan ma'lumotlarga ega bo'lish, ularni deshifrlash chora tadbirlarini amalga oshirishga bo'lgan hatti harakatlar (hujumlar)i qaysi turlarga bo'linadi? :faol (aktiv) va faol bo'lmagan (passiv) hujumlar

Teskarisi mavjud bo'lmagan akslantirishlar qanday akslantirishlar deyiladi. :Bir tomonlama

Ma'lumotlarni himoyalash deganda nima tushiniladi? :Ma'lumotlarga ruxsat etilmagan kirishlardan himoyalash

Ma'lumotni qonuniy manbadan olingaligini kafolatlovchi va oluvchining haqiqiylikni tasdiqlovchi xizmat qanday nomlanadi? :autentifikatsiya

Zamonaviy kriptografiya qanday bo'limlardan iborat? :Simmetrik kriptotizimlar; ochiq kalitli kriptotizimlar; Elektron raqamli imzo; kalitlarni boshqarish

Kriptografik usullardan foydalanishning asosiy yo'nalishlari nimalardan iborat? :Aloqa kanali orqali maxfiy axborotlarni uzatish (masalan, elektron pochta orqali), uzatiliyotgan xabarlarni haqiqiylikni aniqlash, Shifr nima? :Shifrlash va deshifrlashda foydalaniladigan matematik funktsiyadan iborat bo'lgan kriptografik algoritmlar

$12 \cdot 11 \bmod 16$  ?  $15:40 \cdot 13 \cdot 4 \bmod 26$  ?  $5:40$

DES algoritmgacha muqobil bo'lgan algoritmlarni ko'rsating. :Uch karra DES, IDEA, Rijndael

DES algoritmining asosiy muammosi nimada? :kalit uzunligi 56 bit. Bugungi kunda ushbu uzunlik algoritmnining kriptobardoshlilik uchun yetarli emas

Xabarning autentifikatori sifatida ishlatilishi uchun xesh funktsiya qanday talablarga mos kelishi kerak? :Keltirilganlarning barchasiga mos kelishi kerak

MD5 qanday xossalarga ega? :Xesh kodning har bir biti kirishdagi har bir bitning funktsiyasidir. 128 bitli xesh kod uchun MD5 nisbatan kuchli xesh funktsiya hisoblanadi

SHA 1 algoritmining bajarilishi qanday mantiqdan iborat? :Algoritm kirishda maksimal uzunligi 264 bit bo'lgan xabarni qabul qilib, chiqishda uzunligi 160 bit bo'lgan xabarning dayjesteini yaratadi

MD5 xesh funktsiya qanaqa

xarakteristikaga ega? :daydjesti uzunligi 128 bit; Blok uzunligi 512 bit; Iteratsiya soni – 64 (har birida 16 iteratsiya bo'lgan 4 ta tsikl); Elementar mantiqiy funktsiyalar soni – 4; Qo'shimcha konstantalar sonu – 64. SHA 1 xesh funktsiya qanaqa xarakteristikaga ega? :Daydjesti uzunligi 160 bit; Blok uzunligi 512 bit; Iteratsiya soni – 80; Elementar mantiqiy funktsiyalar soni – 3; Qo'shimcha konstantalar sonu – 4. 4 31 mod 32 ? 19:40 21 20mod32? 13:40 SHA 256 xesh funktsiya qanaqa xarakteristikaga ega? :Xabar uzunligi 264 bit; Blok uzunligi 512 bit; So'z uzunligi 32 bit; Xabar daydjesti uzunligi 256 bit SHA 512 xesh funktsiya qanaqa xarakteristikaga ega? :Xabar uzunligi 2128 bit; Blok uzunligi 1024 bit; So'z uzunligi 64 bit; Xabar daydjesti uzunligi 512 bit Nisbatan mashhur bo'lgan xesh funktsiyalarni ko'rsating. :MD2, MD4, MD5, SHA Davlat yoki xalqaro standart sifatida ishlatilayotgan blokli shifrlash algoritmlarini ko'rsating. :DES, GOST28147, CAST, AES S box lar nima uchun yaratilgan? :Ochiq matn va shifrmtn orasidagi bog'liqlikni yuqotish uchun 12 22 mod 32 ? 20:40 ... shifrida shifrlanayotgan matn belgilari boshqa alifbo belgilariga almashadi :o'rniga qo'yish ... shifrida shifrlanayotgan matn belgilari qandaydir qoidaga asosan shifrlanayotgan matnning boshqa belgilariga almashadi :o'rin almashtirish ... shifrida shifrlanayotgan matn belgilari shifrnig gammasi deb ataluvchi qandaydir tasodifiy ketma ketlikning belgilari bilan qo'shiladi :gammalashtirish ... shifrida shifrlanayotgan matn belgilari analitik qoida (formul ga asosan almashadi. :analitik almashtirishga asoslangan Simmetrik algoritmlarni xavfsizligini ta'minlovchi omillarni ko'rsating. :uzatilayotgan shifrlangan xabarni kalitsiz ochish mumkin bo'lmasligi uchun algoritm yetarli darajada bardoshli bo'lishi lozim, uzatilayotgan xabarni xavfsizligi algoritmni maxfiyligiga emas Kriptotizim quyidagi komponentlardan iborat: :ochiq matnlar fazosi M, Kalitlar fazosi K, Shifrmtnlar fazosi C, Ek : M<sup>®</sup> C (shifrlash uchun) va Dk: C<sup>®</sup>M (deshifrlash uchun) funktsiyalar 2 5 mod32 ? 15:40 Serpent, Square, Twofish, RC6 algoritmlari qaysi turiga mansub? :simmetrik blokli algoritmlar Rijndael algoritmi S box uzunligi necha bit? 38:40:00 Simmetrik shifrlash algoritmlari blokli deyiladi, agar ... :shifrlashda ochiq matn fiksirlangan uzunlikdagi bloklarga bo'linsa To'g'ri mulohazani tanlang. :Rijndael algoritmi Feystel tarmog'iga asoslanmagan Xesh funktsiyani natijasi ... :fiksirlangan uzunlikdagi xabar AES algoritmi bloki uzunligi ... bitdan kam bo'lmasligi kerak. 38:40:00 Zamonaviy kriptografiya qanday bo'limlardan iborat? :Simmetrik kriptotizimlar; ochiq kalitli kriptotizimlar; Elektron raqamli imzo; kalitlarni boshqarish Kriptografik usullardan foydalanishning asosiy yo'nalishlari nimalardan iborat? :Aloqa kanali orqali maxfiy axborotlarni uzatish (masalan, elektron pochta orqali), uzatiliyotgan xabarlarini haqiqiyligini aniqlash, tashuvchilarda axborotlarni shifrlangan ko'rinish Shifr nima? :Shifrlash va deshifrlashda foydalaniladigan matematik funktsiyadan iborat bo'lgan krptografik algoritm Himoyalangan yoki xavfsizlikni ta'minlovchi protokol qanday protokol? :Hech bo'lmaganda bitta xavfsizlik funksiyasini qo'llab quvvatlashni ta'minlovchi protokol Protokol xavfsizligi nimalarda o'z ifodasini topadi? :Xavfsizlikni xarakterlovchi xossalr (maxfiylik, butunlik...) kafolati ta'minlanishida Kriptografik protokol bu :Bajarilish jarayonida ishtirokchilar tomonidan kriptografik algoritmlardan foydalanadigan protokol Tashqaridan kuzatib, xabarlarini bilib olishga va protokol bajarilishini buzishga urinuvchi qanday ataladi :Raqib tomon Kriptografik protokollarni qanday guruhlash mimkin :Ishtirokchilar soniga va uzatilayotgan xabar soniga ko'ra Ishtirokchilar soniga ko'ra kriptografik protokollar qanday turlarga bo'linadi? : Ikki tomonlama; Uchtomonlama; Ko'ptomonlama. S box lar nima uchun yaratilgan? :ochiq matn va shifrmtn orasidagi bog'liqlikni yuqotish uchun Oqimli shifrlashning mohiyati nimada? :Oqimli shifrlash birinchi navbatda axborotni bloklarga bo'lishning imkoni bo'lmagan hollarda zarur, Qandaydir ma'lumotlar oqimini har bir belgisini shifrlab, boshqa belgilarini kutmasdan kerakli joyga jo'natish uchun o Almashtirishlar turiga ko'ra shifrlarni qanday

guruhlarga ajratish mumkin? :o'rniga qo'yish shifri, o'rin almashtirish shifri, gammalashtirish shifri, analitik almashtirishga asoslangan shifr ... shifrida shifrlanayotgan matn belgilari boshqa alifbo belgilariga almashadi :o'rniga qo'yish ... shifrida shifrlanayotgan matn belgilari shifrnin gammasi deb ataluvchi qandaydir tasodifiy ketma ketlikning belgilari bilan qo'shiladi :gammalashtirish ... shifrida shifrlanayotgan matn belgilari analitik qoida (formul ga asosan almashadi :analitik almashtirishga asoslangan Simmetrik algoritmlarni xavfsizligini ta'minlovchi omillarni ko'rsating. :uzatilayotgan shifrlangan xabarni kalitsiz ochish mumkin bo'lmasligi uchun algoritm yetarli darajada bardoshli bo'lishi lozim, uzatilayotgan xabarni xavfsizligi algoritmni maxfiyligiga emas Kriptotizim quyidagi komponentlardan iborat: :ochiq matnlar fazosi M, Kalitlar fazosi K, Shifrmatnlar fazosi C, Ek :  $M \oplus C$  (shifrlash uchun) va Dk:  $C \oplus M$  (deshifrlash uchun) funktsiyalar 4 31 mod 32 ? 19:40 DES algoritimga muqobil bo'lgan algoritmni ko'rsating. :Uch karrali DES, IDEA, Rijndael DES algoritmining asosiy muammosi nimada? :kalit uzunligi 56 bit. Bugungu kunda ushbu uzunlik algoritmnin kriptobardoshlilik uchun yetarli emas Simmetrik blokli shifrlash rejimlarini ko'rsating. :ECB Electronic Codebook, CBC Cipher Block Chaining, CFB Cipher Feedback, OFB Output Feedback Asimmetrik kriptotizimlar qanday maqsadlarda ishlatiladi? :shifrlash, deshifrlash, ERI yaratish va tekshirish, kalitlar almashish uchun Diffi Xellman algoritminin maqsadi nimada? :algoritmnin maqsadi keyinchalik qandaydir simmetrik shifrlash algoritmda foydalanish uchun 2 ta foydalanuvchilar tomonidan kalitlarni xavfsiz almashishida 12 22 mod 32 ? 20:40 Rijndael algoritmi S box uzunligi necha bit? 38:40:00 : Simmetrik shifrlash algoritmlari blokli deyiladi, agar ... :shifrlashda ochiq matn fiksirlangan uzunlikdagi bloklarga bo'linsa To'g'ri mulohazani tanlang. :Rijndael algoritmi Feystel tarmog'iga asoslanmagan Xesh funktsiyani natijasi ... :fiksirlangan uzunlikdagi xabar AES algoritmi bloki uzunligi ... bitdan kam bo'lmasligi kerak. 38:40:00 2 5 mod32 ? 15:40 MD5 qanday xossalarga ega? :Xesh kodning har bir biti kirishdagi har bir bitning funktsiyasidir. 128 bitli xesh kod uchun MD5 nisbatan kuchli xesh funktsiya hisoblanadi SHA 1 algoritminin bajarilishi qanday mantiqdan iborat? :Algoritm kirishda maksimal uzunligi 264 bit bo'lgan xabarni qabul qilib, chiqishda uzunligi 160 bit bo'lgan xabarning daydjestini yaratadi MD5 xesh funktsiya qanaqa xarakteristikaga ega? :daydjesti uzunligi 128 bit; Blok uzunligi 512 bit; Iteratsiya soni – 64 (har birida 16 iteratsiya bo'lgan 4 ta tsikl); Elementar mantiqiy funktsiyalar soni – 4; Qo'shimcha konstantalar sonu – 64. 12 11 mod 16 ? 15:40 RIJNDAEL algoritmi qancha uzunligdagi kalitlarni qo'llab quvvatlaydi. :128 bitli, 192 bitli, 256 bitli Identifikasiyalash va autentifikasiyalash bu? :Foydalanuvchilarni ro'yxatdan o'tkazish tartibi va ro'yxatdan o'tish ma'lumotlarini tekshirish tartibi Blowfish shifrlash algoritmi bloki o'lchami qanday? :64 bit Blowfish algoritmi kaliti uzunligi qanday? :O'zgaruvchan Blowfish algoritmi raund akslantirishlari soni qancha? :16 marta Blowfish algoritmi qanday tur kriptotizimga kiradi? :Simmetrik Qanday manbaa asosida raund kalitlari yaratiladi? :Krish bloki uzunligiga bog'liq holda. Berilgan algoritmnin kriptobardoshlilik nimaga asoslangan? :Kalit uzunligiga. SHifrlash qanday amallar orqali amalga oshiriladi? :CHekli maydonda qo'shish mod 232 va mod 2 bo'yicha DES, GOST 28147 89 algoritmlari shifrlash bloki uzunligi qancha? :32 bit; E kengaytirish funksiyasining mohiyati qanday? :32 bitli Ri 1 blokni 48 bitli E(Ri 1) blokka akslantiradi; DES algoritmi Si – bloki vazifasi nimadan iborat? :48 bitli blokni 32 bitli blokka siqishdan iborat; DES algoritmi dastlabki o'rin almashtirish jadvalining o'lchami qanday? :8 x 8; 97 tub sonmi? :Tub Ikkilik sanoq tizimida berilgan 10111 sonini o'nlik sanoq tizimiga o'tkazing. 23:40 Quyidagi modulli ifodani qiymatini toping.  $(125 \cdot 45) \bmod 10$ . 17:40 Quyidagi modulli ifodani qiymatini toping.  $(148 \cdot 14432) \bmod 256$ . 77:20:00 Quyidagi ifodani qiymatini toping.  $17 \bmod 11$  17:40 Sonning teskarisini toppish amali qanday algoritm yordamida amalga oshiriladi? :Kengaytirilgan Yevklid Multiplikativ teskarilash deb nimaga

aytiladi? :Modul ustida ko'paytirish bo'yicha teskarilash Sonning o'zi va uning modul multiplikativ teskarisining ko'paytmasi nechaga teng 21:40 : DES algoritmi shifrlash blokining chap va o'ng qism bloklarining o'lchami qancha? :CHap qism blok 32 bit, o'ng qism blok 32 bit; SHifrlash bloki uzunligi qancha? :32 bit; DES algoritmi kalit uzunligi qancha? :56 bit; : DES algoritmi akslantirish raundlari soni qancha? :16 ta; DES algoritmida E kengaytirish akslantirishining mohiyati qanday? :32 bitli kirish blokini 48 bitli raund kalitiga mod2 maydonda qo'shish uchun 32 bitli blok 48 bitga kengaytiriladi ; Si – bloklarning vazifasi nimadan iborat? :48 bitli blokni 32 bitli blokka siqishdan iborat; DES algortimida Bitlar o'rinlarini almashtirishini aniqlovchi boshlang'ich jadval o'lchami qanday? :8 x 8; SHifrlash algoritmi chap va o'ng bloklarining o'lchami qanday? :CHap blok 32 bit, o'ng blok 32 bit; Raund kalitlari bitlarini siljitish qanday amalga oshiriladi? :Raund kalitlari bitlarini siljitish berilgan jadval bo'yicha hamma raundlar uchun bir xil amalga oshiriladi. DES algoritmi kaliti uzunligi qancha. :64 bit; DES algoritmi akslantirishlari raundlari soni qancha? :16; : Blowfish shifrlash algoritmi bloki o'lchami qancha? :64 bit : Blowfish algoritmi kaliti uzunligi qancha? :O'zgaruvchan Simmetrik shifrlash algoritmi bardoshligi nimaga asoslangan? :Kalit uzunligiga; Qanday amallar asosida blokli shifrlash akslantirishlari yaratiladi? : mod 2 bo'yicha qo'shish asosida; Bloklab shifrlashning asosiy yutuqlari nimalarda namoyon bo'ladi? :SHifrlangan ma'lumotga ochiq ma'lumotning chastotaviy xususiyatlari o'tmaydi O'rniga qo'yish va o'rin almashtirish shifrlarining mohiyatan farqi qanday? :SHifrlangan ma'lumot alfavitida Oddiy o'rniga qo'yish shifrlari badoshligi qanday aniqlanadi? :SHifirma'lumot alfavit belgilarining barcha mumkin bo'lgan holatlari soni bilan Uzliksiz shifrlashning qanday kriptografik qulaylik va samaradorlik tomonlari bor? :Tezligi yuqori va akslantirishlari apparat qurilmalarda qulay amalga oshirish imkoniyatiga ega Uzliksiz shifrlashning qanday kriptografik kamchiliklari bor? :Sinxronlash buzilganda shifrlanish xatolari tarqaladi Uzliksiz shifrlash algoritmlarida siljitish registrlarining qo'llanishini mohiyati nimada? :Tezligi yuqori va akslantirishlarini apparat qurilmalarini amalga oshirish samarali Xesh funksiya qanday kriptografik masalalarni echishga qo'llaniladi? :To'lalik (butunlik) masalasini echishga Blokli simmetrik kalitli shifrlash algoritmlarining bardoshligi qanday parametr bilan aniqlanadi? :Algoritm kaliti uzunligi bilan Agar  $a=19$  bo'lsa, u holda unga teskari bo'lgan sonni xarakteristikasi 26 bo'lgan maydonda hisoblang. 11:40 Kriptografiya va kriptotahlil yo'nalishlari mohiyatan qanday farqlarga ega? :Kriptografiya yo'nalishi ochiq ma'lumot asl holatini yashirish bilan, kriptotahlil yo'nalishi esa shifr ma'lumotga mos keluvchi ochiq ma'lumotni kalit noma'lum bo'lganda topish masala MD5 xesh algoritmi xesh qiymat uzunligi nechchiga teng? :128 bit MD5 xesh algoritmining raundlar soni nechchiga teng? 18:40 AES shifrlash standartining mualliflari kimlar :Ridjmen va Deimen XOR amali qanday amal? :2 modul bo'yicha qo'shish Kalit – bu? :kalit – matnlarni shifrlash va deshifrlash uchun kerak bo'lgan axborot Sonning moduli qaysi matematik ifoda orqali aniqlanadi Qoldiqli bo'lish O'zaro teskari sonlar ko'paytmasi nimaga teng. 0 OpenSSL nima? Secure Sockets Layer (SSL) va kriptografiya vositalarini amalga oshiruvchi asosiy dasturdir RC4 qanday algoritm Simmetrik oqimli shifrlash algoritmi A5/1 qanday algoritm Simmetrik oqimli shifrlash algoritmi MD5 algoritmida hesh qiymat uzunligi necha bitga teng 128 Kriptologiya qanday yo'nalishlarga bo'linadi? #kriptografiya va kriptotahlil kriptografiya va kriptotizim kripto va kriptotahlil kriptoanaliz va kriptotizim ++++ Kriptologiya nima bilan shug'ullanadi? #maxfiy kodlarni yaratish va buzish ilmi bilan maxfiy kodlarni buzish bilan maxfiy kodlarni yaratish bilan maxfiy kodlar orqali ma'lumotlarni yashirish bilan ++++ Kriptografiya nima bilan shug'ullanadi? #maxfiy kodlarni yaratish bilan maxfiy kodlarni buzish bilan maxfiy kodlar orqali ma'lumotlarni yashirish bilan shifrlash uslublarini bilmagan holda shifrlangan ma'lumotni asl holatini topish bilan ++++ Kriptotahlil nima bilan shug'ullanadi? #maxfiy kodlarni buzish bilan

maxfiy kodlarni yaratish bilan maxfiy kodlar orqali ma'lumotlarni yashirish bilan shifrlash uslublarini bilmagan holda shifrlangan ma'lumotni asl holatini topish bilan ++++ Shifrlash orqali ma'lumotning qaysi xususiyati ta'minlanadi? #maxfiyligi Butunliligi Ishonchliligi foydalanuvchanligi ++++ Ochiq kalitli kriptotizimlar kim tomonidan kashf qilingan? #U.Diffie va M.Hellman Rivest va Adlman Shamir va Rivest U.Diffie va Rivest ++++ Kriptologiya necha yo'nalishga bo'linadi? #2 14 16 18 ++++ Kriptologiya so'zining ma'nosi? #cryptos – maxfiy, logos – ilm cryptos – kodlash, logos – ilm cryptos – kripto, logos – yashiraman cryptos – maxfiy, logos – kalit ++++ Ochiq kalitli kriptotizimlar ma'lumotni qanday xususiyatini taminlaydi? #maxfiyligini Butunligini Foydalanuvchanligini ma'lumotni autentifikatsiyasini ++++ Kriptotizimlar kalitlar soni bo'yicha necha turga bo'linadi? #2 4 6 8 ++++ Kriptotizimlar kalitlar soni bo'yicha qanday turga bo'linadi? #simmetrik va assimetrik turlarga simmetrik va bir kalitli turlarga 3 kalitli turlarga assimetrik va 2 kalitli turlarga ++++ Simmetrik kriptotizimlardagi qanday muammoni ochiq kalitli kriptotizimlar bartaraf etdi? #maxfiy kalitni uzatish muammosini kalitni generatsiyalash muammosini ochiq kalitni uzatish muammosini kalitlar juftini hosil qilish muammosini ++++ Ochiq kalitli kriptotizimlarda qanday turdagi kalitlardan foydalanadi? #ochiq va maxfiy kalitlardan maxfiy kalitlar juftidan maxfiy kalitni uzatishni talab etmaydi ochiq kalitni talab etmaydi ++++ Assimetrik kriptotizimlarda necha kalitdan foydalaniladi? #2 ta 3 ta 4 ta kalit ishlatilmaydi ++++ Kerkxofs printsipi nimadan iborat? #kriptografik tizim faqat kalit noma'lum bo'lgan taqdirdagina maxfiylik ta'minlanadi kriptografik tizim faqat yopiq bo'lgan taqdirdagina maxfiylik ta'minlanadi kriptografik tizim faqat ikkita kalit ma'lum bo'lgan taqdirdagina maxfiylik ta'minlanadi ++++ Kalit bardoshliligi bu -? #eng yaxshi ma'lum algoritm bilan kalitni topish murakkabligidir eng yaxshi ma'lum algoritm yordamida yolg'on axborotni ro'kach qilishdir nazariy bardoshlilik amaliy bardoshlilik ++++ Ochiq kalitni kriptotizimlarda nechta kalitdan foydalanadi? #ikkita Bitta Uchta kalitdan foydalanilmaydi ++++ Ochiq kalitli kriptotizimlarda qaysi kalit orqali ma'lumot shifrlanadi? #ochiq kalit orqali maxfiy kalit orqali ma'lumot shifrlanmaydi ushbu tizimda kalitdan foydalanilmaydi ++++ Ochiq kalitli kriptotizimda, qaysi kalit orqali ma'lumot rasshifrovkalanadi? #maxfiy kalit orqali ochiq kalit orqali ma'lumot shifrlanmaydi ushbu tizimda kalitdan foydalanilmaydi ++++ Ochiq kalitli kriptotizimlarda asosan qanday turdagi sonlar bilan ishlaydi? #tub sonlar bilan kasr sonlar bilan chekli maydonda kasr sonlar faqat manfiy sonlar ++++ Qanday sonlar tub sonlar hisoblanadi? #1 va o'ziga bo'linadigan sonlarlar barcha toq sonlar juft bo'lmagan sonlar 2 ga bo'linmaydigan sonlar ++++ Sonlarni tublikka tekshirish algoritmlari nechta sinfga bo'linadi? #ikkita sinfga uchta sinfga bitta sinfga sinflarga bo'linmaydi ++++ Kriptotahlil nima bilan shug'ullanadi? #kalit yoki algoritmni bilmagan holda shifrlangan ma'lumotga mos keluvchi ochiq ma'lumotni topish bilan ochiq ma'lumotlarni shifrlash masalalarining matematik usliblari bilan maxfiy kodlarni yaratish bilan maxfiy kodlar orqali ma'lumotlarni yashirish bilan ++++ RSA algoritmining mualliflarini ko'rsating #R. Rayvest, A. Shamir, L. Adleman Diffi va M. Xellman R. Rayvest, K. Xellman, L. Adleman L. Adleman, El Gamal, K. Shnorr ++++ Ochiq kalitli shifrlash algoritmi keltirilgan qatorni toping? #RSA AES DES RC4 ++++ Ochiq kalitli shifrlash algoritmi keltirilgan qatorni toping? #El-Gamal AES DES RC4 ++++ Shifrlash orqali ma'lumotning qaysi xususiyati ta'minlanadi? #Maxfiyligi Butunliligi Ishonchliligi Foydalanuvchanliligi ++++ Kriptografiya bu -? #axborotni o'zgartirish vositalari va usullarini o'rganadigan fan axborot mazmunidan beruxsat erkin foydalanishdan muhofazalash axborotni buzishning oldini olish axborot almashtirish vosita va usullari bilan shug'ullanadigan fan sohasi ++++ Faqat simmetrik algoritm keltirilgan qatorni ko'rsating? #AES RSA El-Gamal Barcha javoblar to'g'ri ++++ Kriptotizimlar kalitlar soni bo'yicha nechta turga bo'linadi? #2 3 4 ++++



Kriptotizimlar kalitlar soni bo'yicha qanday turga bo'linadi? #simmetrik va assimetrik simmetrik va bitta kalitli 3 kalitli kriptotizimlar assimetrik va 2 ta kalitli ++++ Ferma testi qanday turdagi tublikka testlovchi algoritm hisoblanadi? #ehtimollik testlar tarkibiga kiruvchi algoritm aniqlashtirilgan testlar tarkibiga kiruvchi algoritm taqribiy testlar tarkibiga kiruvchi algoritm tublikka teslovchi algoritm hisoblanmaydi ++++ Solovey Shtrassen testi qanday turdagi tublikka testlovchi algoritm hisoblanadi? #ehtimollik testlar tarkibiga kiruvchi algoritm aniqlashtirilgan testlar tarkibiga kiruvchi algoritm taqribiy testlar tarkibiga kiruvchi algoritm tublikka teslovchi algoritm hisoblanmaydi ++++ Rabbi-Milner testi qanday turdagi tublikka testlovchi algoritm hisoblanadi? #ehtimollik testlar tarkibiga kiruvchi algoritm aniqlashtirilgan testlar tarkibiga kiruvchi algoritm taqribiy testlar tarkibiga kiruvchi algoritm tublikka teslovchi algoritm hisoblanmaydi ++++ Sonlarni tublikka tekshiruvchi algoritmlar necha sinfga bo'linadi? #2 3 4 5 ++++ Sonlarni tublikka tekshiruvchi algoritm qanday sinfga bo'linadi? #aniqlashtirilgan va ehtimolli testlar aniqlashtirilgan va taqribiy testlar taqribiy va ehtimolli testlar aniqlashtirilgan, ehtimolli va taqribiy testlar ++++ Sonlarni tublikka tekshiruvchi ehtimollikka asoslangan algoritmlar keltirilgan qatorni ko'rsating? #Ferma, Solovey Shtrassen, Rabbi-Milner Ferma, Solovey Shtrassen, Eyler Eyler, Solovey Shtrassen, Rabbi-Milner Ferma, Eyler, Rabbi-Milner ++++ Elliptik egriz chiqizlarda nuqtalar usitda qanday ammalar bajariladi? #nuqtalarni qo'shish va nuqtalarni ikkilantirish nuqtalarni qo'shish va nuqtalarni ko'paytirish nuqtalarni qo'shish va nuqtalarni bo'lish nuqtalarni ayirish va nuqtalarni ko'paytirish ++++ 1 ga va o'ziga bo'linadigan sonlar qanday sonlar hisoblanadi? #tub sonlar murakkab sonlar toq sonlar juft sonlar Elektron hujjat manbaini haqiqiyligini qaysi amal orqali amalga oshiriladi? #ERI orqali amalga oshiriladi shifrlash algoritmi orqali amalga oshiriladi kodlash orqali amalga oshiriladi autentifikatsiya orqali amalga oshiriladi ++++ Elektron hujjat yaxlitligini (o'zgarmasligini) tekshirish qaysi amal orqali amalga oshiriladi? #ERI orqali amalga oshiriladi kodlash orqali amalga oshiriladi shifrlash algoritmi orqali amalga oshiriladi autentifikatsiya orqali amalga oshiriladi ++++ Elektron hujjatni mualliflikdan bosh tortmasligini qaysi amal orqali amalga oshiriladi? #ERI orqali amalga oshiriladi kodlash orqali amalga oshiriladi autentifikatsiya orqali amalga oshiriladi shifrlash algoritmi orqali amalga oshiriladi ++++ Raqamli imzoni shakllantirish muolajasi qaysi algoritmga tegishli? #ERI algoritmiga kodlash algoritmiga shifrlash algoritmiga steganografiya algoritmiga ++++ ECDSA-2000 qaysi davlat standarti hisoblanadi? #AQSH Rossiya O'zbekiston Kanada ++++ O'zDSt 1092:2009 standarti qaysi davlat standarti hisoblanadi? #O'zbekiston AQSH Rossiya Kanada ++++ GOCT P 34.10-94 standarti qaysi davlat standarti hisoblanadi? #Rossiya O'zbekiston AQSH Kanada ++++ Seans kalitli hamda seans kalitsiz rejimlarda ishlidigan standartni ko'rsating? #O'zDSt 1092:2009 ECDSA-2000 GOCT P 34.10-94 DSA ++++ DSA qanday standart hisoblanadi? #ERI standarti shifrlash standarti kodlash standarti steganografik standart ++++ Ochiq kalitli kriptotizimlar qanday turdagi matematik murakkablikka asoslangan algoritmarga bo'linadi? #faktorizatsiyalash va diskret logarifmlash algoritmilariga modulyar arifmetika murakkabligiga asoslangan algoritmarga diskret logarifmlash murakkabligiga asoslangan algoritmarga faktorizatsiyalash murakkabligiga asoslangan algoritmarga ++++ Ochiq kalitli kriptotizimlarning bardoshligini ta'minlashda qanday murakkab muammo turiga asoslanadi? #faktorlash, diskret logarifmlash, elliptik egri chiziqda diskret logarifmlash faktorlash, diskret logarifmlash faktorlash, diskret logarifmlash, elliptik egri chiziqda faktorizatsiyalash faktorlash, diskret logarifmlash, modulyar arifmetikaga ++++ Ehtimolli testlar sonlarni tublikka tekshirishda qanday natijani beradi? #tekshirilayotgan son tub yoki tubmasligi haqida ehtimollik bilan javob beradi tekshirilayotgan son tub yoki tubmasligi haqida kafolatlangan aniq javob beradi tekshirilayotgan son tub yoki tubmasligi haqida tasodifiy ravishda javob beradi tekshirilayotgan

son tub yoki tubmasligini 0 va 1 qiymatlarga qarab javob beradi ++++ Sonlarni tublikka tekshirishning ehtimolli algoritmlariga quyidagilarning qaysilari kiradi? #Ferma, Rabbi-Milner, Poklington testlari Rabbi-Milner, Solovey-Shtrassen, Pollard testlari Ferma, Solovey-Shtrassen, Pollard testlari Rabbi Milner, Poklington, Pollard testlari ++++ Ochiq kalitli RSA shifrlash algoritmi bardoshlilik qanday matematik muammo turiga asoslangan? #faktorlash murakkabligiga diskret logarifmlash murakkabligiga elliptik egri chiziqlarda faktorizatsiyalash murakkabligiga elliptik egri chiziqlarda faktorizatsiyalash murakkabligiga ++++ Ochiq kalitli El-Gamal shifrlash algoritmi qanday matematik murakkablikka asoslanadi? #diskret logarifmlash murakkabligiga faktorlash murakkabligiga elliptik egri chiziqlarda diskret logarifmlash murakkabligiga elliptik egri chiziqlarda faktorlash murakkabligiga ++++ Diffie-Hellman algoritmi qanday matematik murakkablikka asoslanadi? #diskret logarifmlash murakkabligiga faktorlash murakkabligiga elliptik egri chiziqlarda diskret logarifmlash murakkabligiga elliptik egri chiziqlarda faktorlash murakkabligiga ++++ Diffie-Hellman qanday algoritm hisoblanadi? #kalitlarni ochiq taqsimlash algoritmi ochiq kalitli shifrlash algoritmi diskret logarifmlash murakkabligiga asoslangan shifrlash algoritmi faktorlash murakkabligiga asoslangan kalitlarni ochiq taqsimlash algoritmi ++++ ERI algoritmlari qanday muolajalardan iborat? #imzoni shakllantirish, imzoni tekshirish imzoni shakllantirish, imzo qo'yish va imzoni tekshirish imzoni shakllantirish va imzo qo'yish imzo qo'yish ++++ Ochiq kalitli kriptotizimlarda elektron hujjatlarga imzo qo'yish qaysi kalit orqali amalga oshiriladi? #shaxsiy kalit orqali ochiq kalit orqali imzo qo'yilishi kalitga bog'liq emas imzo qo'lda qo'yiladi ++++ Ochiq kalitli kriptotizimlarda elektron hujjatlarga qo'yilgan imzoni tekshirish qaysi kalit orqali amalga oshiriladi? #ochiq kalit orqali maxfiy kalit orqali imzo qo'yilishi kalitga bog'liq emas imzo qo'lda qo'yiladi ++++ Diskret logarifmlash murakkabligiga asoslangan algoritm keltirilgan qatorni ko'rsating? #Diffie-Hellman, EL-Gamal algoritmi RSA algoritmi EL-Gamal algoritmi Diffie-Hellman algoritmi ++++ Faktorlash murakkabligiga asoslangan algoritm keltirilgan qatorni ko'rsating? #RSA El-Gamal Diffie-Hellman DSA ++++ Karlmaykl sonlari qaysi tublikka tekshiruvchi algoritmlarda doim bajariladi? #Ferma testida Solovey-Shtrassen testida Eyler testida Rabbin testida ++++ Ochiq kalitli RSA shifrlash algoritmda maxfiy kalit qanday topiladi?  $e \cdot d \equiv 1 \pmod{p \cdot q}$  taqqoslamadan  $e \cdot d \equiv 1 \pmod{N}$   $e \cdot d \equiv 1 \pmod{p-1}$   $e \cdot d \equiv 1 \pmod{(p-1)(q-1)}$  ++++ Ochiq kalitli RSA shifrlash algoritmda qaysi parametrlar ochiq holda e'lon qilinadi? #N, e e N, d d ++++ Ochiq kalitli RSA shifrlash algoritmda "e" ochiq kalit, "d" shaxsiy kalit bo'lsa deshifrlash formulasi to'g'ri ko'rsatilgan qatorni belgilang?  $M = C^d \pmod{N}$   $M = C^d \pmod{N}$   $M = C^e \pmod{N}$   $M = C^e \pmod{N}$  ++++ Ochiq kalitli RSA shifrlash algoritmda "d" shaxsiy kalit, "e" ochiq kalit bo'lsa shifrlash formulasi to'g'ri ko'rsatilgan qatorni belgilang?  $C = M^e \pmod{N}$   $C = M^e \pmod{N}$   $C = M^d \pmod{N}$   $C = M^d \pmod{N}$  ++++ Ochiq kalitli El-Gamal shifrlash algoritmda "p" tub son bo'lsa maxfiy kalit qanday tanlanadi? #(p-1) bilan o'zaro tub bo'lgan (1,p-1) intervaldagi butun son p bilan o'zaro tub bo'lgan (1,p-1) intervaldagi butun son (1,p-1) intervaldagi tub son (p-1) bilan o'zaro tub bo'lgan (1,p) intervaldagi butun son ++++ Ochiq kalitli El-Gamal shifrlash algoritmda ochiq kalit qanday hisoblanadi?  $y = g^a \pmod{p}$ , bu yerda g-birlamchi ildiz, a-maxfiy kalit, p-tub son  $y = g^a \pmod{p}$ , bu yerda g-soni (p-1) dan kichik butun son, a-maxfiy kalit, p-tub son  $y = g^a \pmod{p}$ , bu yerda g-soni p dan kichik butun son, a-maxfiy kalit, p-tub son  $y = g^a \pmod{p}$ , bu yerda g-soni (p-1) bilan o'zaro tub bo'lgan butun son, a-maxfiy kalit, p-tub son ++++ Ochiq kalitli kriptotizimlarga asoslangan kalitlarni taqsimlash Diffie-Hellman algoritmi ishlash prinsipi qanday? #umumiy maxfiy kalitni hosil qilishga asoslangan ochiq va yopiq kalitlar juftini hosil qilishga asoslangan maxfiy kalitni uzatishni talab etmaydigan prinsipga asoslangan ochiq kalitlarni hosil qilishga asoslangan ++++ "A" va "B" foydalanuvchilar ma'lumot almashmoqchi, "A" foydalanuvchi "B" tomondan qabul qilgan ma'lumotni imzosini

tekshirishda qaysi kalitdan foydalanadi? # "B" foydalanuvchining ochiq kalitidan "B" foydalanuvchining maxfiy kalitidan "A" foydalanuvchi o'zining ochiq kalitidan "A" foydalanuvchini o'zining maxfiy kalitidan ++++ RSA algoritmda  $p=3$ ,  $q=11$ ,  $e=3$  bo'lganda maxfiy kalitni qiymati topilsin:  $e \cdot d \equiv 1 \pmod{(N)}$ ? # 7 6 8 5 ++++ Faktorlash muammosini bartaraf etuvchi usul keltirilgan qatorni ko'rsating? # Pollard usuli Xitoy teoremasi Pohlig-Hellman usulu RSA usuli ++++ Pollard usuli qanday turdagi matematik murakkablikni yechishda foydalaniladi? # faktorlash murakkabligini diskret logarifmlash murakkabligini elliptik egrzi chiziqda diskret logarifmlash murakkabligini elliptik egrzi chiziqda faktorlash murakkabligini ++++ RSA algoritmidagi matematik murakkablikni qanday usul orqali bartaraf qilish mumkin? # Pollard usuli Xitoy teoremasi Pohlig-Hellman usuli RSA usuli ++++ Diskret logarifmlash muammosini bartaraf etuvchi usul keltirilgan qatorni ko'rsating? # Pohlig-Hellman usuli Pollard usuli Xitoy teoremasi RSA usuli ++++ Pohlig-Hellman usuli qanday turdagi matematik murakkablikni yechishda foydalaniladi? # diskret logarifmlash murakkabligini faktorlash murakkabligini elliptik egrzi chiziqda faktorlash murakkabligini daraja parameter murakkabligini ++++ Evklidning kengaytirilgan algoritmidan RSA shifrlash algoritmining qaysi parametrini hisoblashda foydalaniladi? # maxfiy kalitni ochiq kalitni tub sonlarni modul qiymatini ++++ Diffie-Hellman algoritmda qaysi parametrlar ochiq holda e'lon qilinadi? #  $p$  va  $g$  tub sonlarni ( $p > g$ )  $p$  tub sonni  $p$  va  $g$  toq sonlarni ( $p > g$ )  $p$  va  $g$  juft sonlarni ( $p > g$ ) ++++ Axborot xavfsizligining pasayishi nimani anglatadi? # axborot xavfsizligi ma'lumotlarning tartibsizligi ma'lumotlarning mas'uliyatsizligi ichki xavfsizlik +++++ Tashkilotning iqtisodiy xavfsizligini ta'minlash muammosining eng muhim tarkibiy qismlaridan biri bu # Axborot texnologiyalari (IT) va tizimlar (IS) xavfsizligi Axborot texnologiyalari (IT) xavfsizligi Axborot tizimlarining xavfsizligi (IS) Texnik tizimlarning xavfsizligi (TS) +++++ Axborot tizimlari va texnologiyalarini rivojlantirish, joriy qilish va ulardan foydalanishning ajralmas qismi hisoblanadi # Axborot xavfsizligi kriptografiya steganografiya autentifikatsiya +++++ Zamonaviy dasturlash texnologiyasi sizni mutlaqo xatosiz va xavfsiz dasturlarni yaratishga imkon beradimi? # emas Ha noma'lum savol noto'g'ri +++++ Huquqiy hujjatlar talablariga yoki ma'lumot egalari tomonidan o'rnatilgan talablarga muvofiq mulkka tegishli va himoya qilinishi kerak bo'lgan ma'lumotlar # himoyalangan ma'lumotlar maxfiy ma'lumotlar keraksiz ma'lumotlar foydali ma'lumotlar ++++ Axborot egalari bo'lishi mumkin: # davlat, yuridik shaxs, shaxslar guruhi, yakka shaxs. davlat xizmatchisi, yuridik shaxs, shaxslar guruhi, jismoniy shaxs. davlat, yuridik shaxs, shaxslar guruhi, alohida aktsiyadorlik jamiyati. davlat, yuridik shaxs, shaxslar guruhi, alohida kompaniya. +++++ Axborotni qayta ishlashning avtomatlashtirilgan tizimlari nima uchun kerak? # ma'lumotlarni saqlash, qayta ishlash va uzatish uchun ma'lumotlarni saqlash, yangilash va yashirish uchun ma'lumotlarni saqlash, qayta ishlash va shifrlash uchun ma'lumotlarni saqlash, qayta ishlash va tahlil qilish uchun +++++ Axborot xavfsizligini buzishning potentsial yoki real xavfini keltirib chiqaradigan shartlar va omillar to'plami # Tahdid (axborot xavfsizligi) Maxfiylikni buzish Hodisa Hujum +++++ Axborot xavfsizligiga tahdidning bevosita sababi bo'lgan sub'ekt (shaxs, moddiy ob'ekt yoki jismoniy hodisa) # Axborot xavfsizligiga tahdid manbai Texnik xavfsizlik manbai Virus hujumining manbasi Xodimlarning manbasi +++++ Axborot tizimining xususiyati, unda ishlov beriladigan axborotga tahdidlarni amalga oshirishga imkon beradi # Zaiflik (axborot tizimi) Xaker hujumi Hodisa Qayta rasmiylashtirish +++++ Yashirin yoki mahfiy axborotni amalga oshirish natijasida shaxs, shaxslar guruhi yoki u mo'ljallanmagan har qanday tashkilot uchun foydalanish mumkin bo'lgan tahdid # Maxfiylikka tahdid (oshkor qilish tahdidi) Butunlik uchun tahdid Texnik tahdid Xaker hujumi +++++ Amalga oshirilishi natijasida ma'lumotlar o'zgartirilishi yoki yo'q qilinishi mumkin bo'lgan tahdid # Butunlik uchun tahdid Virusli hujum xavfi Tarmoq tahdidi Texnik

tahdid +++++ Tashkilotni o'z faoliyatida yo'naltiradigan hujjatlashtirilgan qoidalar, protseduralar, amaliyotlar yoki axborot xavfsizligi sohasidagi ko'rsatmalar to'plami #Xavfsizlik siyosati Davlat siyosati Korporativ etika Ko'rsatmalar +++++ Amalga oshirilishi avtomatlashtirilgan tizim mijozlariga xizmat ko'rsatishni rad etishga, tajovuzkorlarning o'z xohishlariga ko'ra manbalardan ruxsatsiz foydalanishiga olib keladigan tahdid hisoblanadi. #Xizmat tahdidini rad etish (mavjud tahdid) Texnik muammo Tizimning favqulodda to'xtashi Hujum +++++ Uning maxfiyligi, ochiqqligi va yaxlitligi ta'minlanadigan axborot xavfsizligi holati #Axborot xavfsizligi Ma'lumot xavfsizligi Operatsion tizim xavfsizligi Shaxsiy ma'lumotlar xavfsizligi +++++ Axborotni himoya qilish usuli #axborotni himoya qilishning muayyan printsiplari va vositalarini qo'llash tartibi va qoidalari. axborotni texnik himoya qilishning muayyan printsiplari va vositalarini qo'llash tartibi va qoidalari. ma'lum bir algoritmlar va axborot xavfsizligi vositalarini qo'llash tartibi va qoidalari. axborotni himoya qilishning ayrim algoritmlarini qo'llash tartibi va qoidalari. +++++ Apparat, dasturiy ta'minot, dasturiy ta'minot va apparat, axborotni himoya qilish uchun mo'ljallangan yoki ishlatiladigan materiallar va (yoki) materiallar #Axborot xavfsizligi vositasi Axborotni nusxalash vositasi Axborot uzatish vositasi Shaxsiy ma'lumotlarni uzatish vositasi +++++ Axborotni kriptografik o'zgartirish orqali himoya qilish #kriptografik ma'lumotlarni himoya qilish antivirus ma'lumotlarini himoya qilish ma'lumotlarni steganografik himoya qilish axborotni texnik himoya qilish +++++ Ruxsat berilgan shaxslarning kirib borishi yoki kirishiga to'sqinlik qiladigan vositalar to'plami va tashkiliy choralar yordamida axborotni himoya qilish himoya qilinadigan obyekt hisoblanadi. #axborotni jismoniy himoya qilish axborotni dasturiy himoyasi antivirus ma'lumotlarini himoya qilish oddiy ma'lumotlarni himoya qilish +++++ Muayyan tarmoq tugunini o'chirishga qaratilgan hujum turi (Xizmatni rad etish - DoS) #xizmatdan bosh tortish "ma'lumotlarga kirishni rad etish" "ma'lumotlarga kirishni rad etish" "parolga kirish taqiqlandi" +++++ Kriptovalyutatsiya atamasini birinchi bo'lib kiritgan olimni ko'rsating #F. Fridman Aristotel Shannon Aliqushchi +++++ IV asrda "antiscital" dekifrlash qurilmasini kim yaratgan. Mil. Avv. #Aristotel Sokrat Ptolemey Spital +++++ Qaysi olimning kitobida chastota kriptovalyutasi to'g'risida birinchi ma'lum eslatma mavjud? #Al-Kindi Aristotel Umar Xayyom Mirzo Ulug'bek +++++ Qur'on matni asosida arab tilidagi harflarning chastota jadvalini birinchi bo'lib kim aniqlagan? #Shihab al-Kalkasandi Umar Xayyom Mirzo Ulug'bek Imom Buxoriy +++++ Axborotni shifrlash va shifrlash usullarini qaysi fan rivojlantirmoqda? #Kriptologiya Informatika Matematika Fizika +++++ DES shifrlash algoritmi qaysi tarmoqqa asoslangan holda ishlaydi? #Feystel tarmog'iga asoslangan holda SPN tarmog'iga asoslangan holda hech qanday tarmoqqa asoslanmaydi Lai-Massey tarmog'iga asoslangan holda +++++ Quyida keltirilgan xususiyatlarning qaysilari xesh funksiyaga mos? #chiqishda fiksirlangan uzunlikdagi qiymatni beradi chiqishda bir xil qiymatni beradi kolliziyaga ega chiqishdagi qiymat bilan kiruvchi qiymatlar bir xil bo'ladi +++++ Quyida keltirilgan xususiyatlarning qaysilari xesh funksiyaga mos? #ixtiyoriy olingan har xil matn uchun xesh qiymatlar bir xil bo'lmaydi ixtiyoriy olingan bir xil matn uchun qiymatlar bir xil bo'lmaydi ixtiyoriy olingan har xil matn uchun xesh qiymatlar bir xil bo'ladi ixtiyoriy olingan har xil xesh qiymat uchun dastlabki ma'lumotlar bir xil bo'ladi +++++ DES shifrlash algoritmda har bir raunda necha bitli raund kalitlaridan foydalaniladi? #48 56 64 32 +++++ Qaysi hujum turida barcha bo'lishi mumkin bo'lgan variantlar ko'rib chiqiladi? #qo'pol kuch hujumi sotsial injineriya analitik hujum chastotalar tahlili +++++ Ma'lumotlarni autentifikatsiyalash kodlari deb qanday xesh funksiyalarga aytiladi? #kalitli xesh funksiyalarga kalitsiz xesh funksiyalarga kriptografik bo'lmagan xesh funksiyalarga kriptografik xesh funksiyalarga +++++ AES algoritmda raundlar soni nimaga bo'g'liq? #kalit uzunligiga kiruvchi blok uzunligiga foydalanilgan vaqtiga kiruvchi blok uzunligi va matn qiymatiga

+++++ A5/1 oqimli shifrlash algoritmda registrarning surilishi qanday kattalikka bog'liq? #maj funksiyasi qiymatiga kalit qiymatiga registr uzunligi qiymatiga hech qanday kattalikka bog'liq emas  
+++++ 16 raund davom etadigan blokli shifrlash algoritmi ko'rsating? #DES AES RC4 A5/1 +++++ 10 raund davom etadigan blokli shifrlash algoritmi ko'rsating? #AES DES RC4 A5/1 +++++ Xesh qiymatlarni yana qanday atash mumkin? #dayjest funksiya imzo raqamli imzo +++++ Ximoyalanuvchi ma'lumot boshqa bir ma'lumotni ichiga yashirish orqali maxfiyligini ta'minlaydigan usul qaysi? #steganografiya kodlash shifrlash autentifikatsiya +++++ Baytlar kesimida shifrlashni amalga oshiradigan algoritm keltirilgan qatorni ko'rsating? #RC4 A5/1 MD5 SHA1 +++++ Kolliziya deb nima nisbatan aytiladi? #ikkita har xil matn uchun bir xil xesh qiymat mos kelishi ikkita bir xil matn uchun bir xil xesh qiymat mos kelishi ikkita har xil matn uchun har xil xesh qiymat mos kelishi ikkita bir xil matn uchun bir xil xesh qiymat mos kelmasligiga +++++ Konfidensiallikni ta'minlash bu -? #ruxsat etilmagan "o'qishdan" himoyalash ruxsat etilmagan "yozishdan" himoyalash ruxsat etilmagan "bajarishdan" himoyalash ruxsat berilgan "amallarni" bajarish +++++ Sezar shifrlash algoritmi qaysi turdagi akslantirishga asoslangan? #o'rniga qo'yish o'rin almashtirish aralash kompozitsion +++++ CRC-3 tizimida CRC qiymatini hisoblash jarayonida ma'lumotga nechta nol biriktiriladi? #3 6 12 9 +++++ ... kriptotizimni shifrlash va rasshifrovkalash uchun sozlashda foydalaniladi. #kalit ochiq matn algoritm alifbo +++++ CRC-5 tizimida CRC qiymati hisoblash jarayonida ma'lumotga nechta nol biriktiriladi? #5 10 15 20 +++++ Rasshifrovkalash jarayonida kalit va ..... kerak bo'ladi #shifrmtn ochiq matn kodlash alifbo +++++ Kriptologiya qanday yo'nalishlarga bo'linadi? #kriptografiya va kriptotahlil kripto va kriptotahlil kriptografiya va kriptotizim kriptoanaliz va kriptotizim +++++ Kriptotizimlar kalitlar soni bo'yicha necha turga bo'linadi? #2 6 4 8 +++++ Kriptografiya nima bilan shug'ullanadi? #maxfiy kodlarni yaratish bilan maxfiy kodlar orqali ma'lumotlarni yashirish bilan maxfiy kodlarni buzish bilan shifrlash uslublarini bilmagan holda shifrlangan ma'lumotni asl holatini topish bilan +++++ Kerkxofs printsipi nimadan iborat? #kriptografik tizim faqat kalit noma'lum bo'lgan taqdirdagina maxfiylik ta'minlanadi kriptografik tizim faqat yopiq bo'lgan taqdirdagina maxfiylik ta'minlanadi kriptografik tizim faqat ikkita kalit ma'lum bo'lgan taqdirdagina maxfiylik ta'minlanadi kriptografik tizim faqat kalit ochiq bo'lgan taqdirdagina maxfiylik ta'minlanadi +++++ Shifrlash orqali ma'lumotning qaysi xususiyati ta'minlanadi? #maxfiyligi ishonchliligi butunliligi foydalanuvchanligi +++++ O'rniga qo'yish shifrlash sinfiga qanday algoritmlar kiradi? #shifrlash jarayonida ochiq ma'lumot alfavit belgilari shifr ma'lumot belgilariga almashtiriladigan algoritmlar shifrlash jarayonida ochiq ma'lumot alfaviti belgilarining o'rinlar almashtiriladigan algoritmlar shifrlash jarayonida kalitlarning o'zni almashtiriladigan algoritmlarga shifrlash jarayonida o'rniga qo'yish va o'rin almashtirish akslantirishlarning kombinatsiyalaridan birgalikda foydalaniladigan algoritmlar +++++ Kriptologiya necha yo'nalishga bo'linadi? #2 4 8 6 +++++ Kriptologiya so'zining ma'nosi? #cryptos – maxfiy, logos – ilm cryptos – maxfiy, logos – kalit cryptos – kripto, logos – yashiraman cryptos – kodlash, logos – ilm +++++ O'rniga qo'yish shifrlash algoritmlari necha sinfga bo'linadi? #2 6 4 8 +++++ O'rniga qo'yish shifrlash algoritmlari qanday sinfga bo'linadi? #bir qiymatli va ko'p qiymatli shifrlash bir qiymatli shifrlash ko'p qiymatli shifrlash uzluksiz qiymatli shifrlash +++++ Kriptologiya nima bilan shug'ullanadi? #maxfiy kodlarni yaratish va buzish ilmi bilan maxfiy kodlarni yaratish bilan maxfiy kodlarni buzish bilan maxfiy kodlar orqali ma'lumotlarni yashirish bilan +++++ Ma'lumotlarni kodlash va dekodlashda necha kalitdan foydalanadi? #kalit ishlatilmaydi 3 ta 2 ta 4 ta +++++ Simmetrik kriptotizimlarda necha kalitdan foydalaniladi? #1 ta 3 ta kalit ishlatilmaydi 4 ta +++++ Kriptotahlil nima bilan shug'ullanadi? #maxfiy kodlarni buzish bilan shifrlash uslublarini bilmagan holda shifrlangan ma'lumotni asl holatini topish bilan maxfiy kodlar orqali ma'lumotlarni

yashirish bilan maxfiy kodlarni yaratish bilan shifrlash uslublarini bilmagan holda shifrlangan ma'lumotni asl holatini topish bilan +++++ A5/1 oqimli shifrlash algoritmda dastlabki kalit uzunligi nechi bitga teng? #64 192 512 256 +++++ Steganografiya ma'lumotni qanday maxfiylashtiradi? #maxfiy xabarni soxta xabar ichiga berkitish orqali maxfiy xabarni kriptografik kalit yordamida shifrlash orqali maxfiy xabarni kodlash orqali maxfiy xabarni shifrlash orqali +++++ Shifrlash algoritmlari akslantirish turlariga qarab qanday turlarga bo'linad? #o'rniga qo'yish, o'rin almashtirish va kompozitsion akslantirishlarga o'rniga qo'yish, o'rin almashtirish va surish akslantirishlariga o'rniga qo'yish va o'rin almashtirish akslantirishlariga o'rniga qo'yish, sirush va kompozitsion shifrlash akslantirishlariga +++++ Blokli shifrlash algoritmlari arxitekturasini jihatidan qanday tarmoqlarga bo'linadi? #Feystel va SP Feystel va Petri SP va Petri Kvadrat va iyerarxik +++++ Zamonaviy kriptografiya qaysi bo'limlarni o'z ichiga oladi? #simmetrik kriptotizimlar, ochiq kalitli kriptotizimlar, elektron raqamli imzo kriptotizimlari, kriptobardoshli kalitlarni ishlab chiqish va boshqarish simmetrik kriptotizimlar, ochiq kalit algoritmgacha asoslangan kriptotizimlar, elektron raqamli imzo kriptotizimlari, foydalanuvchilarni ro'yxatga olish simmetrik kriptotizimlar, ochiq kalit algoritmgacha asoslangan kriptotizimlar, elektron raqamli imzo kriptotizimlari, foydalanuvchilarni identifikatsiya qilish simmetrik kriptotizimlar, ochiq kalit algoritmgacha asoslangan kriptotizimlar, elektron raqamli imzo kriptotizimlari, foydalanuvchilarni autentifikatsiyalash +++++ ARX amaliy nimalardan iborat? #add, rotate, xor add, rotate, mod add, mod, xor mod, rotate, xor +++++ Tasodifiy ketma-ketliklarni generatsiyalashga asoslangan shifrlash turi bu? #oqimli shifrlar blokli shifrlar ochiq kalitli shifrlar assimetrik shifrlar +++++ Qanday algoritmlarda chiqishda doim fiksirlangan uzunlikdagi qiymat chiqadi? #xesh algoritmlarda kodlash algoritmlarida shifrlash algoritmlarida steganografik algoritmlarda +++++ Ma'lumotni shifrlash va deshifrlash uchun bir xil kalitdan foydalanuvchi tizim bu? #simmetrik kriptotizim ochiq kalitli kriptotizim assimetrik kriptotizim xesh funksiyalar +++++ Ikki kalitli deyilganda qaysi kriptotizim nazarda tutiladi? #ochiq kalitli kriptotizim simmetrik kriptotizim xesh funksiyalar MAC tizimlari +++++ Simmetrik shifrlash algoritmlarida qanday muammo mavjud? #kalitni uzatish kalit generatsiyalash kalitni yo'q qilish muammo yo'q +++++ Sezar shifrlash usuli qaysi akslantirishga asoslangan? #o'rniga qo'yish o'rin almashtirish ochiq kalitli shifrlarga kombinatsion akslantirishga +++++ Ma'lumotni uzatishda kriptografik himoya ..... #konfidentsiallik va yaxlitlikni ta'minlaydi konfidentsiallik va foydalanuvchanlikni ta'minlaydi konfidentsiallikni ta'minlaydi foydalanuvchanlik ta'minlaydi va butunlikni +++++ Butunlikni ta'minlash bu - ? #ruxsat etilmagan "yozishdan" himoyalash ruxsat etilmagan "bajarishdan" himoyalash ruxsat etilmagan "o'qishdan" himoyalash ruxsat berilgan "amallarni" bajarish +++++ Shifrlash va deshifrlashda alohida kalitlardan foydalanuvchi kriptotizimlar bu? #ochiq kalitli kriptotizimlar simmetrik kriptotizimlar bir kalitli kriptotizimlar xesh funksiyalar +++++ Agar ochiq ma'lumot shifrlansa, natijasi .... bo'ladi. #shifrmavn ochiq mavn noma'lum kod +++++ Ochiq kalitli shifrlar axborotni qaysi xususiyatlarini ta'minlashda foydalaniladi? #konfidentsiallik va yaxlitlik konfidentsiallik va foydalanuvchanlik foydalanuvchanlik va yaxlitlik foydalanuvchanlik +++++ MD5 xesh funksiyasida kiruvchi ma'lumot uzunligi qanday bitli bloklarga bo'linadi? #512 1024 2048 4096 +++++ add amalining ma'nosi nima? #modul asosida qo'shish XOR amaliy surish (siklik surish, mantiqiy surish) akslantirish +++++ SHA1 xesh funksiyasida initsializatsiya bosqichida 5 ta necha bitli registrlardan foydalanadi? #32 64 128 256 +++++ O'zbekistonda kriptografiya sohasida faoliyat yurituvchi tashkilot nomini ko'rsating? #“UNICON.UZ” DUK “O'zstandart” agentligi Kadastr agentligi Davlat Soliq Qo'mitasi +++++ Faqat simmetrik shifrlash algoritmlari nomi keltirilgan qatorni ko'rsating? #AES, A5/1 SHA1, DES MD5, AES HMAC, RC4 +++++ HMAC tizimida kalit qiymati blok uzunligiga teng bo'lganda ma'lumotga

qanday biriktiriladi? #kalit qiymati o'zgartirilmagan holda ma'lumotga biriktiriladi kalit qiymati blok uzunligiga teng bo'lguncha nol qiymat bilan to'ldirilib hosil bo'lgan qiymat ma'lumotga biriktiriladi kalitni xesh qiymati hisoblanib, unga blok uzunligiga teng bo'lguncha nol qiymat qo'shiladi va yangi hosil bo'lgan qiymat ma'lumotga biriktiriladi xesh funksiyalarda kalit qiymatida foydalanilmaydi +++++ DES shifrlash algoritmda rasshifrovkalashda birinchi raunda qaysi kalitdan foydalaniladi? #16-raund kalitidan 1-raund kalitidan 1-raunda kalitdan foydalanilmaydi dastlabki kalitdan +++++ SHA1 xesh funksiyasida kiruvchi ma'lumot uzunligi qanday bitli bloklarga bo'linadi? #512 1024 2048 4096 +++++ AES shifrlash algoritmda blok uzunligi 128, kalit uzunligi 192 bit bo'lsa raundlar soni nechta bo'ladi? #12 10 14 6 +++++ AES shifrlash algoritmda nechta akslantirishdan foydalanadi? #4 3 2 akslantirishdan foydalanilmaydi +++++ GSM tarmog'ida foydalaniluvchi shifrlash algoritmi nomini ko'rsating? #A5/1 dastlabki kalitdan AES DES +++++ WEP protokolida (Wi-Fi tarmog'ida) foydalaniluvchi shifrlash algoritmi nomini ko'rsating? #RC4 DES SHA1 A5/1 +++++ rotate amalining ma'nosi nima? #surish (siklik surish, mantiqiy surish) modul asosida qo'shish XOR amali Akslantirish +++++ SHA1 xesh funksiyasida to'ldirish bitlarini qo'shishda ma'lumot uzunligi 512 modul bo'yicha qanday son bilan taqqoslanadigan qilib to'ldiriladi? #448 1002 988 772 +++++ HMAC tizimida kalit qiymati blok uzunligidan kichik bo'lganda ma'lumotga qanday biriktiriladi? #kalit qiymati blok uzunligiga teng bo'lguncha nol qiymat bilan to'ldirilib hosil bo'lgan qiymat ma'lumotga biriktiriladi kalitni xesh qiymati hisoblanib, unga blok uzunligiga teng bo'lguncha nol qiymat qo'shiladi va yangi hosil bo'lgan qiymat ma'lumotga biriktiriladi kalit qiymati o'zgartirilmagan holda ma'lumotga biriktiriladi xesh funksiyalarda kalit qiymatida foydalanilmaydi +++++ Kolliziya hodisasi qaysi turdagi algoritmlarga xos? #xesh funksiyalar ochiq kalitli shifrlash algoritmlari kalitlarni boshqarish tizimlari simmetrik shifrlash algoritmlari +++++ AES shifrlash algoritmda shifrlash jarayonida qanday akslantirishdan foydalaniladi? #SubBytes, ShiftRows, MixColumns va AddRoundKey SubBytes, ShiftRows va AddRoundKey SubBytes, MixColumns va AddRoundKey MixColumns, ShiftRows, SubBytes +++++ Faqat blokli simmetrik shifrlash algoritmlari nomi keltirilgan qatorni ko'rsating? #AES, DES A5/1, RC4 A5/1, MD5 SHA1, RC4 +++++ Vernam shifrlash algoritmda shifr matn C=101 ga, kalit K=111 ga teng bo'lsa shifr matn qiymati qanday bo'ladi? #010 101 111 110 +++++ Quyidagi ifoda nechta yechimga ega?  $3 \cdot x = 2 \pmod{7}$ . #bitta yechimga ega ikkita yechimga ega yechimga ega emas uchta yechimga ega +++++  $143 \pmod{17}$  nechiga teng? #7 6 5 8 +++++ Blokli shifrlash rejimlari qaysi algoritmlarda qo'llaniladi? #AES, DES Sezar, Affin MD5, SHA1 A5/1, RC4 +++++ MD5 xesh algoritmda nechta 32 bitli statik qiymatdan foydalanadi? #4 8 12 16 +++++ Sezar shifrlash algoritmda ochiq matn M=3 ga, kalit K=7 ga teng hamda p=26 ga teng bo'sa shifr matn qiymati neciga teng bo'ladi? #10 16 18 22 +++++ Qaysi xesh algoritmda 64 raund amal bajariladi? #MD5 MAC CRC SHA1 +++++ DES shifrlash standarti qaysi davlat standarti? #AQSH Rossiya Buyuk Britaniya Germaniya +++++ Qaysi blokli shifrlash algoritmda raund kalit uzunligi qiymatiga bo'g'liq? #AES IDEA DES RSA +++++ A5/1 oqimli shifrlash algoritmda  $x_{18}=1$ ,  $y_{21}=0$ ,  $z_{22}=1$  ga teng bo'lsa kalitni qiymatini toping #0 1 2 3 +++++ Kolliziya hodisasi deb nimaga aytiladi? #ikki xil matn uchun bir xil xesh qiymat chiqishi ikki xil matn uchun ikki xil xesh qiymat chiqishi bir xil matn uchun bir xil xesh qiymat chiqishi bir xil matn uchun bir xil xesh qiymat chiqishi +++++ 3 sonini 5 chekli maydonda teskarisini toping? #2 3 4 5 +++++ Bir qiymatli shifrlash qanday amalga oshiriladi? #ochiq ma'lumot alfaviti belgilarining har biriga shifr ma'lumot alfavitining bitta belgisi mos qo'yiladi ochiq ma'lumot alfaviti belgilarining har biriga shifr ma'lumot alfavitining ikkita yoki undan ortiq chekli sondagi belgilari mos qo'yiladi ochiq ma'lumot alfaviti belgilarining har ikkitasiga shifr ma'lumot alfavitining ikkita yoki undan ortiq

chekli sondagi belgilari mos qo'yiladi ochiq ma'lumot alfaviti belgilarining har juftiga shifr ma'lumot alfavitining bitta belgisi mos qo'yiladi +++++ DES shifrlash algoritmda raundlar soni nechta? #16 64 32 128 +++++ DES shifrlash algoritmda kalit uzunligi necha bitga teng? #56 256 192 512 +++++ RC4 oqimli shifrlash algoritmi asosan qayerda qo'llaniladi? #simsiz aloqa vositalaridagi mavjud WEP protokolida radioaloqa tarmoqlarda inernet trafiklarini shifrlashda mobil aloqa standarti GSM protokolida +++++ Xesh funsiyalarga qanday turlarga bo'linadi? #kalitli va kalitsiz xesh funsiyalarga kalitli va kriptografik bo'lmagan xesh funsiyalarga kalitsiz va kriptografik bo'lmagan xesh funsiyalarga kriptografik va kriptografik bo'lmagan xesh funsiyalarga +++++ AES shifrlash algoritmda raundlar soni nechaga teng bo'ladi? #10, 12, 14 14, 16, 18 18, 20, 22 22, 24, 26 +++++ A5/1 oqimli shifrlash algoritmda har bir qadamda kalit oqimining qanday qiymatini hosil qiladi? #bir biti bir bayti 64 biti 8 bayti +++++ CRC-4 tizimida CRC qiymatini hisoblash jarayonida ma'lumotga nechta nol biriktiriladi? #4 8 16 12 +++++ Blokli simmetrik shifrlash algoritmlari raund funksiyalarida qanday amallar bajariladi? #ARX PRX XOR RPT +++++ CRC-6 tizimida CRC qiymati hisoblash jarayonida ma'lumotga nechta nol biriktiriladi? #6 12 18 24 +++++ Qaysi maxfiylikni ta'minlash usulida kalitdan foydalanilmaydi? #kodlash shifrlash autentifikatsiya steganografiya +++++ Vernam shifrlash algoritm asosi qaysi mantiqiy hisoblashga asoslangan #XOR ARX ROX XRA +++++ Chastotalar tahlili kriptotahlil usuli samarali ishlidigan algorimtlar keltirilgan qatorni belgilang? #Sezar, Affin Vernam Vijiner RC4 +++++ Bitlar kesimida shifrlashni amalga oshiradigan algoritm keltirilgan qatorni ko'rsating? #A5/1 SHA1 RC4 MD5 +++++ Ma'lumotni konfidensialligini ta'minlash uchun ..... zarur. #shifrlash kodlash rasshifrovkalash deshifrlash +++++ Foydalanuvchanlikni ta'minlash bu-? #ruxsat etilmagan "bajarishdan" himoyalash ruxsat etilmagan "yozishdan" himoyalash ruxsat etilmagan "o'qishdan" himoyalash ruxsat berilgan "amallarni" bajarish +++++ Vijiner shifrlash algoritmi qaysi turdagi akslantirishga asoslanadi? #o'rniga qo'yish o'rin almashtirish kompozitsion aralash +++++ Kompyuter davriga tegishli shifrlarni aniqlang? #DES, AES shifri kodlar kitobi Sezar Enigma shifri +++++ .... shifrlar blokli va oqimli turlarga ajratiladi #simmetrik ochiq kalitli klassik assimetrik +++++ DES shifrlash algoritmi bu? #blokli shifrlash algoritmi oqimli shifrlash algoritmi ochiq kalitli shifrlash algoritmi asimetrik shifrlash algoritmi +++++ Ma'lumotga elektron raqamli imzo qo'yish hamda uni tekshirish qanday amalga oshiriladi? #Ma'lumotga raqamli imzo qo'yish maxfiy kalit orqali, imzoni tekshirish ochiq kalit orqali amalga oshiriladi Ma'lumotga raqamli imzo qo'yish ochiq kalit orqali, imzoni tekshirish maxfiy kalit orqali amalga oshiriladi Ma'lumotga raqamli imzo qo'yish maxfiy kalit orqali, imzoni tekshirish yopiq kalit orqali amalga oshiriladi Ma'lumotga raqamli imzo qo'yish hamda uni tekshirish maxfiy kalit orqali amalga oshiriladi +++++ A5/1 oqimli shifrlash algoritmda Z registr uzunligi nechi bitga teng? #23 18 19 20 +++++ Kerkxofs printsipi bo'yicha qanday taxminlar ilgari suriladi? #Kalitdan boshqa barcha ma'lumotlar barchaga ma'lum Faqat kalit barchaga ma'lum Barcha parametrlar barchaga ma'lum Shifrlash kaliti barchaga ma'lum +++++ Qaysi algoritm har bir qadamda bir bayt qiymatni shifrlaydi? #RC4 A5/1 RSA AES +++++ A5/1 oqimli shifrlash algoritmda maxfiy kalit necha registrga bo'linadi? #3 6 5 4 +++++ AES algoritmi qaysi tarmoq asosida qurilgan? #SP Feystel Petri va SP Petri +++++ Elektron raqamli imzo bo'yicha birinchi O'z DSt 1092 qaysi korxona tomonidan ishlab chiqilgan? #UNICON.UZ INFOCOM UZTELECOM O'zR axborot texnologiyalari va kommunikatsiyalarini rivojlantirish vazirligi +++++ AES shifrlash algoritmi nomini kengaytmasini ko'rsating? #Advanced Encryption Standard Advanced Encoding Standard Advanced Encryption Stadium Always Encryption Standard +++++ A5/1 shifrlash algoritmi bu? #oqimli shifrlash algoritmi blokli shifrlash algoritmi assimetrik shifrlash algoritmi ochiq kalitli shifrlash algoritmi +++++ RC4 shifrlash algoritmi qaysi turga mansub? #oqimli



shifrlar blokli shifrlar ochiq kalitli shifrlar assimetrik shifrlar +++++ Xeshlash algoritmlarini ko'rsating? #SHA1, MD5, O'z DST 1106 RSA, DSA, El-gamal DES, AES, Blowfish O'z DST 1105, ГОСТ 28147-89, FEAL +++++ AES shifrlash algoritmi bu? #blokli shifrlash algoritmi oqimli shifrlash algoritmi ochiq kalitli shifrlash algoritmi asimetrik shifrlash algoritmi +++++ ARX amali qaysi shifrlash algoritmlarida foydalaniladi? #Blokli shifrlashda Ikki kalitli shifrlashda Assimetrik shifrlashda Ochiq kalitli shifrlashda +++++ Kriptotizimlar kalitlar soni bo'yicha nechta turga bo'linadi? #2 3 4 5 +++++ A5/1 oqimli shifrlash algoritmda major qiymati hisoblash jarayonida, uchinchi (Z) registrning qaysi qiymati olinadi? #z10 z11 z12 z13 +++++ A5/1 oqimli shifrlash algoritmda X registr uzunligi nechki bitga teng? #19 16 17 15 +++++ Qaysi algoritmda har bir qadamda bir bit qiymatni shifrlaydi? #A5/1 RC4 RSA AES +++++ Mantiqiy XOR amalining asosi qanday hisoblashga asoslangan? #mod2 bo'yicha qo'shishga mod2 bo'yicha ko'paytirishga mod2 bo'yicha darajaga ko'tarishga mod2 bo'yicha bo'lishga +++++ Qaysi xesh algoritmda xesh qiymat 128 bitga teng bo'ladi? #MD5 SHA1 CRC MAC +++++ Qaysi xesh algoritmda xesh qiymat 160 bitga teng bo'ladi? #SHA1 MD5 CRC MAC +++++ Faqat AQSH davlatiga tegishli kriptografik standartlar nomini ko'rsating? #AES, DES AES, ГОСТ 28147-89 DES, O'z DST 1105-2009 SHA1, ГОСТ 3412-94 +++++ RC4 shifrlash algoritmi simmetrik turga mansub bo'lsa, unda nechta kalitdan foydalaniladi? #1 2 3 4 +++++ A5/1 oqimli shifrlash algoritmda major qiymati hisoblash jarayonida, birinchi (X) registrning qaysi qiymati olinadi? #x8 x9 x10 x11 +++++ DES shifrlash algoritmda S-bloklarga kiruvchi qiymatlar uzunligi necha bitga teng bo'ladi? #6 12 24 18 +++++ MD5 xesh funksiyasida initsializatsiya bosqichida 4 ta necha bitli registrlardan foydalanadi? #32 64 128 256 +++++ Imitatsiya turidagi hujumlarda ma'lumotlar qanday o'zgaradi? #ma'lumot qalbakilashtiriladi ma'lumot yo'q qilinadi ma'lumot ko'chirib olinadi ma'lumot dublikat qilinadi +++++ Sesar shifrlash algoritmda rasshifrovkalash formulasi qanday? # $M=(C-K) \bmod p$   $M=(C+K) \bmod p$   $M=(C*K) \bmod p$   $M=(C/K) \bmod p$  +++++ Faqat xesh funksiyalar nomi keltirilgan qatorni ko'rsating? #SHA1, MD5 SHA1, DES MD5, AES HMAC, A5/1 +++++ MD5 xesh funksiyasida chiquvchi qiymat uzunligi nechaga teng? #128 Ixtiyoriy 510 65 +++++ AES shifrlash algoritmi simmetrik turga mansub bo'lsa, unda nechta kalitdan foydalaniladi? #1 2 3 4 +++++ SHA1 xesh funksiyasida initsializatsiya bosqichida nechta registrdan foydalanadi? #5 10 15 20 +++++ MD5 xesh funksiyasida amallar necha raund davomida bajariladi? #64 128 512 256 +++++ DES shifrlash algoritmda S-bloklardan chiqqan qiymatlar uzunligi necha bitga teng bo'ladi? #4 8 12 16 +++++ MD5 xesh funksiyasida initsializatsiya bosqichida nechta 32 bitli registrdan foydalanadi? #4 8 12 16 +++++ Faqat oqimli simmetrik shifrlash algoritmlari nomi keltirilgan qatorni ko'rsating? #A5/1, RC4 AES, DES SHA1, RC4 A5/1, MD5 +++++ SHA1 xesh funksiyasida chiquvchi qiymat uzunligi nechaga teng? #160 Ixtiyoriy 512 256 +++++ O'zgartirish turidagi hujumlarda ma'lumotlar qanday o'zgaradi? #modifikatsiya qilinadi ma'lumot yo'q qilinadi ma'lumot dublikat qilinadi ma'lumot ko'chirib olinadi +++++ AES standarti qaysi algoritm asoslangan? #Rijndael RC6 Twofish Serpent +++++ SHA1 xesh funksiyasida amallar nechki raund davomida bajariladi? #80 128 256 512 +++++ 2 lik sanoq tizimida 0101 soniga 1111 sonini 2 modul bo'yicha qo'shing? #1010 0101 1001 1111 +++++ AES shifrlash standarti qaysi davlat standarti? #AQSH Rossiya Buyuk Britaniya Germaniya +++++ Qaysi algoritmda maj kattaligi ishlatiladi? #A5/1 RC4 SHA1 MD5 +++++ Qalbakilashtirish hujumi qaysi turdagi hujum turiga kiradi? #Imitatsiya o'zgartirish Fabrication modification +++++ SHA1 xesh funksiyasi qaysi davlat standarti? #AQSH Rossiya Germaniya Buyuk Britaniya +++++ Qayday akslantirishdan foydalanilsa chastotalar tahlili kriptotahlil usuliga bardoshli bo'ladi #bigram akslantirishidan o'rniga qo'yish akslantirishidan o'rin almashtirish akslantirishidan xech qanday akslantirishdan foydalanish shart emas +++++ SHA1 xesh algoritmda nechta 32 bitli statik

qiymatdan foydalanadi? #5 10 15 20 +++++ A5/1 oqimli shifrlash algoritmda maj(1,0,1) ga teng bo'lsa maj kattalik qiymatini toping? #1 0 2 3 +++++ SHA1 xesh funksiyada 102 bitli ma'lumot berilganda to'ldirish bitlari qanday to'ldiriladi? #bir bit 1, 345 ta 0, ma'lumot uzunligi qiymatining 64 bitli qiymati bilan bir bit 1, 345 ta 0, ma'lumot uzunligining dastlabki 64 bitli qiymati bilan bir bit 1, 409 ta 0, ma'lumot uzunligi qiymatining 64 bitli qiymati bilan bir bit 1, 409 ta 0, ma'lumot uzunligining dastlabki 64 bitli qiymati bilan +++++ Qaysi blokli shifrlash algoritmda 8 ta statik S-box lardan foydalaniladi? #DES RSA RC4 A5/1 +++++ Kriptotizimlar kalitlar soni bo'yicha qanday turga bo'linadi? #simmetrik va assimetrik turlarga assimetrik va 2 kalitli turlarga 3 kalitli turlarga simmetrik va bir kalitli turlarga +++++ Ko'p qiymatli shifrlash qanday amalga oshiriladi? #ochiq ma'lumot alfaviti belgilarining har biriga shifr ma'lumot alfavitining ikkita yoki undan ortiq chekli sondagi belgilari mos qo'yiladi ochiq ma'lumot alfaviti belgilarining har ikkitasiga shifr ma'lumot alfavitining ikkita yoki undan ortiq chekli sondagi belgilari mos qo'yiladi ochiq ma'lumot alfaviti belgilarining har biriga shifr ma'lumot alfavitining bitta belgisi mos qo'yiladi ochiq ma'lumot alfaviti belgilarining har juftiga shifr ma'lumot alfavitining bitta belgisi mos qo'yiladi +++++ A5/1 oqimli shifrlash algoritmi asosan qayerda qo'llaniladi? #mobil aloqa standarti GSM protokolida simsiz aloqa vositalaridagi mavjud WEP protokolida internet trafiklarini shifrlashda radioaloqa tarmoqlarida +++++ Assimetrik kriptotizimlarda necha kalitdan foydalaniladi? #2 ta 3 ta 4 ta kalit ishlatilmaydi +++++ AES algoritmda shifrlash kalitining uzunligi necha bitga teng? #128, 192, 256 bit 128, 156, 256 bit 256, 512 bit 128, 192 bit +++++ Kalit bardoshliligi bu -? #eng yaxshi ma'lum algoritmi bilan kalitni topish murakkabligidir eng yaxshi ma'lum algoritmi yordamida yolg'on axborotni ro'kach qilishdir amaliy bardoshlilik nazariy bardoshlilik +++++ RC4 oqimli shifrlash algoritmda har bir qadamda kalit oqimining qanday qiymatini hosil qiladi? #bir baytini bir bitini 64 bitini 8 baytini +++++ AES algoritmda nechta akslantirishlardan foydalaniladi? #4 2 5 6 +++++ Qanday funksiyalarga xesh funksiya deyiladi? #ixtiyoriy uzunlikdagi ma'lumotni biror fiksirlangan uzunlikga o'tkazuvchi funksiyaga aytiladi ma'lumot baytlarini boshqa qiymatlarga almashtiruvchi funksiyaga aytiladi ma'lumot bitlarini boshqa qiymatlarga almashtiruvchi funksiyaga aytiladi ixhtiyoriy uzunlikdagi ma'lumotni bit yoki baytlarini zichlashtirib beruvchi funksiyaga aytiladi +++++ Xesh funksiyalar qanday maqsadlarda ishlatiladi? #ma'lumotni to'liqligini nazoratlash va ma'lumot manbaini autentifikatsiyalashda ma'lumot manbaini autentifikatsiyalashda ma'lumotni butunligini nazoratlashda ma'lumotni maxfiyligini nazoratlash va ma'lumot manbaini haqiqiyligini tekshirishda +++++ Ma'lumotni sakkizlik sanoq tizimidan o'n oltilik sanoq tizimiga o'tkazish bu? #kodlash rasshifrovkalash yashirish shifrlash +++++ A5/1 shifri qaysi turga mansub? #oqimli shifrlar blokli shifrlar ochiq kalitli shifrlar assimetrik shifrlar +++++ Qaysi algoritmlar simmetrik blokli shifrlarga tegishli? #AES, DES A5/1, AES Vijiner, DES Sezar, AES +++++ Ma'lumotni mavjudligini yashirishni maqsad qilgan bilim sohasi bu? #steganografiya kriptografiya kodlash kriptotahlil +++++ Faqat simmetrik blokli shifrlarga xos bo'lgan atamani aniqlang? #blok uzunligi kalit uzunligi ochiq kalit kodlash jadvali +++++ Quyidagi ta'rif qaysi atamaga tegishli: "maxfiy kodlarni"ni buzish bilan shug'ullanadigan soha-bu? #kriptotahlil kripto kriptologiya kriptografiya +++++ Qadimiy davr klassik shifriga quyidagilarning qaysi biri tegishli? #Sezar kodlar kitobi Enigma shifri DES, AES shifri +++++ Quyidagi ta'rif qaysi kriptotizimga tegishli: ochiq matnni shifrlashda hamda rasshifrovkalashda mos holda ochiq va maxfiy kalitdan foydalanadi? #ochiq kalitli kriptotizimlar maxfiy kalitli kriptotizimlar simmetrik kriptotizimlar elektron raqamli imzo tizimlari +++++ Simmetrik shifrlar axborotni qaysi xususiyatlarini ta'minlashda foydalaniladi? #konfidensiallik va yaxlitlilik konfidensiallik va foydalanuvchanlik foydalanuvchanlik va yaxlitlilik foydalanuvchanlik +++++ Qanday algoritmlar qaytmas xususiyatiga ega hisoblanadi? #xesh

funksiyalar elektron raqamli imzo algoritmlari simmetrik kriptotizimlar ochiq kalitli kriptotizimlar  
+++++ Ochiq matn qismlarini takror shifrlashga asoslangan usul bu? #blokli shifrlar oqimli shifrlar  
assimetrik shifrlar ochiq kalitli shifrlar +++++ Ochiq kalitli shifrlashda deshifrlash qaysi kalit asosida  
amalga oshiriladi? #shaxsiy kalit ochiq kalit kalitdan foydalanilmaydi umumiy kalit +++++ Quyidagi  
ta'rif qaysi atamaga tegishli: "maxfiy kodlarni"ni yaratish bilan shug'ullanadigan soha-bu?  
#kriptografiya kriptologiya kriptotahlil kripto +++++ Simmetrik kriptotizimlarning asosiy kamchiligi  
bu? #kalitni taqsimlash zaruriyati kalitlarni esda saqlash murakkabligi shifrlash jarayonining ko'p  
vaqt olishi algoritmlarning xavfsiz emasligi +++++ Kriptotizimni boshqaradigan vosita? #kalit  
algoritm stegokalit kriptotizim boshqarilmaydi +++++ Quyidagi ta'rif qaysi kriptotizimga  
tegishli:ochiq matnni shifrlashda hamda rasshifrovkalashda bitta maxfiy kalitdan foydalaniladi?  
#simmetrik kriptotizimlar nosimmetrik kriptotizimlar ochiq kalitli kriptotizimlar assimetrik  
kriptotizimlar +++++ Kerxgofs prinsipiga ko'ra kriptotizimning to'liq xavfsiz bo'lishi faqat qaysi  
kattalik nomalum bo'lishiga asoslanishi kerak? #kalit protokol shifrmatn Algoritm +++++ Xesh  
funksiyalar nima maqsadda foydalaniladi? #ma'lumotlar yaxlitligini ta'minlashda ma'lumot egasini  
autentifikatsiyalashda ma'lumot maxfiyligini ta'minlashda ma'lumot manbaini  
autentifikatsiyalashda +++++ Chastotalar tahlili hujumi qanday amalga oshiriladi? #shifr matnda  
qatnashgan harflar sonini aniqlash orqali shifr matnda eng kam qatnashgan harflarni aniqlash  
orqali ochiq matnda qatnashgan harflar sonini aniqlash orqali ochiq matnda eng kam qatnashgan  
harflarni aniqlash orqali +++++ Xesh funksiyaga tegishli bo'lgan talabni aniqlang? #bir tomonlama  
funksiya bo'lishi chiqishda ixtiyoriy uzunlikda bo'lishi turli kirishlar bir xil chiqishlarni akslantirishi  
kolliziyaga bardoshli bo'lmasligi +++++ RC4 shifrlash algoritmi bu? #oqimli shifrlash algoritmi ochiq  
kalitli shifrlash algoritmi blokli shifrlash algoritmi asimetrik shifrlash algoritmi +++++ A5/1 shifrlash  
algoritmi simmetrik turga mansub bo'lsa, unda nechta kalitdan foydalaniladi? #1 2 3 4 +++++ Qaysi  
algoritmida, algoritmning necha round bajarilishi ochiq matn uzunligiga bog'liq? #A5/1 MD5 HMAC  
SHA1 +++++ Simmetrik va ochiq kalitli kriptotizimlar asosan nimasi bilan bir biridan farq qiladi?  
#kalitlar soni bilan matematik murakkabligi bilan farq qilmaydi biri maxfiylikni ta'minlasa, biri  
butunlikni ta'minlaydi +++++ A5/1 oqimli shifrlash algoritmida major qiymati hisoblash jarayonida,  
ikkinchi (Y) registrning qaysi qiymati olinadi? #y10 y11 y12 y13 +++++ Kalitli xesh funksiyalar  
qanday turdagi hujumlardan himoyalaydi? #imitatsiya va o'zgartirish turidagi hujumlardan  
ma'lumotni oshkor qilish turidagi hujumlardan DDOS hujumlaridan foydalanishni buzishga  
qaratilgan hujumlardan +++++ Sezar shifrlash algoritmida shifrlash formulasi qanday? # $C=(M+K) \bmod p$   
 $C=(M-K) \bmod p$   $C=(M*K) \bmod p$   $C=(M/K) \bmod p$  +++++ A5/1 oqimli shifrlash algoritmida Y  
registr uzunligi nechki bitga teng? #22 20 19 21 +++++ Kalitli xesh funksiyalardan foydalanish  
nimani kafolatlaydi? #fabrikatsiyani va modifikatsiyani oldini oladi ma'lumot yo'q qilinadi  
ma'lumot dublikat qilinadi ma'lumot ko'chirib olinadi +++++ DES shifrlash algoritmi simmetrik  
turga mansub bo'lsa, unda nechta kalitdan foydalaniladi? #1 2 3 4 +++++ AES tanlovi g'olibi  
bo'lgan algoritm nomini ko'rsating? Rijndael IDEA Blowfish Twofish +++++ AES shifrlash  
algoritmida 128 bitli ma'lumot bloki qanday o'lchamdagi jadvalga solinadi? #4x4 4x6 6x4 6x6  
+++++ A5/1 oqimli shifrlash algoritmida maj(1,0,1) ga teng bo'lsa qaysi registrlar suriladi? #birinchi  
va uchunchi registrlar suriladi faqat ikkinchi registr suriladi birinchi va ikkinchi registrlar suriladi  
faqat birinchi resgistr suriladi +++++ GSM tarmog'ida foydalaniluvchi shifrlash algoritmi nomini  
ko'rsating? #A5/1 DES RC4 AES +++++ HMAC tizimida kalit qiymati blok uzunligidan katta  
bo'lganda ma'lumotga qanday biriktiriladi? #kalitni xesh qiymati hisoblanib, unga blok uzunligiga  
teng bo'lguncha nol qiymat qo'shiladi va yangi hosil bo'lgan qiymat ma'lumotga biriktiriladi kalit  
qiymati blok uzunligiga teng bo'lguncha nol qiymat bilan to'ldirilib hosil bo'lgan qiymat

ma'lumotga biriktiriladi kalit qiymati o'zgartirilmagan holda ma'lumotga biriktiriladi xesh funksiyalarda kalit qiymatidan foydalanilmaydi +++++ Qaysi xesh algoritmda 80 raund amal bajariladi? #SHA1 CRC MD5 MAC +++++ Affin shifrlash algoritmda  $a=2$ ,  $b=3$ ,  $p=26$  hamda ochiq matn  $x=4$  ga teng bo'lsa, shifr matn qiymatini toping? #11 27 41 31 +++++ MD5 xesh funksiyada 48 bitli ma'lumot berilganda to'ldirish bitlari qanday to'ldiriladi? #bir bit 1, 399 ta 0, ma'lumot uzunligi qiymatining 64 bitli qiymati bilan bir bit 1, 399 ta 0, ma'lumot uzunligining dastlabki 64 bitli qiymati bilan bir bit 1, 463 ta 0, ma'lumot uzunligi qiymatining 64 bitli qiymati bilan bir bit 1, 463 ta 0, ma'lumot uzunligining dastlabki 64 bitli qiymati bilan +++++ AES shifrlash algoritmda ochiq matn bilan dastlab qanday amal bajariladi? #ochiq matn dastlabki kalit bilan XOR amali bajariladi ochiq matn birinchi raund kalit bilan XOR amali bajariladi ochiq matn ustida dastlab SubBytes akslantirishi amali bajariladi ochiq matn ustida dastlab ShiftRows akslantirishi amali bajariladi +++++ Vernam shifrlash algoritmda ochiq matn  $M=101$  ga, kalit  $K=111$  ga teng bo'lsa shifr matn qiymati qanday bo'ladi? #010 101 111 110 ?Konfidensiallikni ta minlash bu - ? +ruxsatsiz o qishdan himoyalash. -ruxsatsiz yozishdan himoyalash. -ruxsatsiz bajarishdan himoyalash. -ruxsat etilgan amallarni bajarish. ?Foydalanuvchanlikni ta minlash bu - ? +ruxsatsiz bajarishdan himoyalash. -ruxsatsiz yozishdan himoyalash. -ruxsatsiz o qishdan himoyalash. -ruxsat etilgan amallarni bajarish. ?Yaxlitlikni ta minlash bu - ? +ruxsatsiz yozishdan himoyalash. -ruxsatsiz o qishdan himoyalash. -ruxsatsiz bajarishdan himoyalash. -ruxsat etilgan amallarni bajarish. ?Jumlani to ldiring. Hujumchi kabi fikrlash ... kerak. +bo lishi mumkin bo lgan xavfni oldini olish uchun -kafolatlangan amallarni ta minlash uchun -ma lumot, axborot va tizimdan foydalanish uchun -ma lumotni aniq va ishonchli ekanligini bilish uchun ?Jumlani to ldiring. Tizimli fikrlash ... uchun kerak. +kafolatlangan amallarni ta minlash -bo lishi mumkin bo lgan xavfni oldini olish -ma lumot, axborot va tizimdan foydalanish -ma lumotni aniq va ishonchli ekanligini bilish ?Axborot xavfsizligida risk bu? +Manbaga zarar keltiradigan ichki yoki tashqi zaiflik ta sirida tahdid qilish ehtimoli. -U yoki bu faoliyat jarayonida nimaga erishishni xoxlashimiz. -Tashkilot uchun qadrli bo lgan ixtiyoriy narsa. -Tizim yoki tashkilotga zarar yetkazishi mumkin bo lgan istalmagan hodisa. ?Axborot xavfsizligida tahdid bu? +Aktivga zarar yetkazishi mumkin bo lgan istalmagan hodisa. -Noaniqlikning maqsadlarga ta siri. -U yoki bu faoliyat jarayonida nimaga erishishni xohlashimiz. -Tashkilot uchun qadrli bo lgan ixtiyoriy narsa. ?Axborot xavfsizligida aktiv bu? +Tashkilot yoki foydalanuvchi uchun qadrli bo lgan ixtiyoriy narsa. -Tizim yoki tashkilotga zarar yetkazishi mumkin bo lgan istalmagan hodisa. -Noaniqlikning maqsadlarga ta siri. -U yoki bu faoliyat jarayonida nimaga erishishni xohlashimiz. ?Axborot xavfsizligida zaiflik bu? +Tahdidga sabab bo luvchi tashkilot aktivi yoki boshqaruv tizimidagi nuqson. -Tashkilot uchun qadrli bo lgan ixtiyoriy narsa. -Tizim yoki tashkilotga zarar yetkazishi mumkin bo lgan istalmagan hodisa. -Noaniqlikning maqsadlarga ta siri. ?Axborot xavfsizligida boshqarish vositasi bu? +Natijasi zaiflik yoki tahdidga ta sir qiluvchi riskni o zgartiradigan harakatlar. -Bir yoki bir nechta tahdidga sabab bo luvchi tashkilot aktivi yoki boshqaruv tizimidagi kamchilik. -Tashkilot uchun qadrli bo lgan ixtiyoriy narsa. -Tizim yoki tashkilotga zarar yetkazishi mumkin bo lgan istalmagan hodisa. ?Har qanday vaziyatda biror bir hodisani yuzaga kelish ehtimoli qo shilsa .... +risk paydo bo ladi. -hujum paydo bo ladi. -tahdid paydo bo ladi. -aktiv paydo bo ladi. ?Jumlani to ldiring. Denial of service (DOS) hujumi axborotni .... xususiyatini buzushga qaratilgan. +foydalanuvchanlik -butunlik -konfidensiallik -ishonchlilik ?Jumlani to ldiring. ... sohasi tashkil etuvchilar xavfsizligi, aloqa xavfsizligi va dasturiy ta minotlar xavfsizligidan iborat. +Tizim xavfsizligi -Ma lumotlar xavfsizligi -Inson xavfsizligi -Tashkilot xavfsizligi ?Kriptologiya so ziga berilgan to g ri tavsifni toping? +Maxfiy shifrlarni yaratish va buzish fani va sanati. -Maxfiy shifrlarni yaratish fani va sanati. -Maxfiy shifrlarni buzish fani va sanati. -Axborotni

himoyalash fani va sanati. ?.... kriptotizimni shifrlash va deshifrlash uchun sozlashda foydalaniladi. +Kriptografik kalit -Ochiq matn -Alifbo -Algoritm ?Kriptografiya so ziga berilgan to g ri tavsifni toping? +Maxfiy shifrlarni yaratish fani va sanati. -Maxfiy shifrlarni yaratish va buzish fani va sanati. -Maxfiy shifrlarni buzish fani va sanati. -Axborotni himoyalash fani va sanati. ?Kriptotahlil so ziga berilgan to g ri tavsifni toping? +Maxfiy shifrlarni buzish fani va sanati. -Maxfiy shifrlarni yaratish fani va sanati. -Maxfiy shifrlarni yaratish va buzish fani va sanati. -Axborotni himoyalash fani va sanati. ?..... axborotni ifodalash uchun foydalaniladigan chekli sondagi belgilar to plami. +Alifbo -Ochiq matn -Shifrmtn -Kodlash ?Ma lumot shifrlansa, natijasi .... bo ladi. +shifrmtn -ochiq matn -nomalum -kod ?Deshifrlash uchun kalit va ..... kerak bo ladi. +shifrmtn -ochiq matn -kodlash -alifbo ?Ma lumotni shifrlash va deshifrlashda yagona kalitdan foydalanuvchi tizim bu - +simmetrik kriptotizim. -ochiq kalitli kriptotizim. -asimetrik kriptotizim. -xesh funksiyalar. ?Ikki kalitli kriptotizim bu - +ochiq kalitli kriptotizim. -simmetrik kriptotizim. -xesh funksiyalar. -MAC tizimlari. ?Axborotni mavjudligini yashirish bilan shug ullanuvchi fan sohasi bu - +steganografiya. -kriptografiya. -kodlash. -kriptotahlil. ?Axborotni foydalanuvchiga qulay tarzda taqdim etish uchun ..... amalga oshiriladi. +kodlash -shifrlash -yashirish -deshifrlash ?Jumlani to ldiring. Ma lumotni konfidensialligini ta minlash uchun ..... zarur. +shifrlash -kodlash -dekodlash -deshifrlash ?Ma lumotni mavjudligini yashirishda ..... +steganografik algoritmdan foydalaniladi. -kriptografik algoritmdan foydalaniladi. -kodlash algoritmidan foydalaniladi. -kriptotahlil algoritmidan foydalaniladi. ?Xesh funksiyalar - .... funksiya. +kalitsiz kriptografik -bir kalitli kriptografik -ikki kalitli kriptografik -ko p kalitli kriptografik ?Jumlani to ldiring. Ma lumotni uzatishda kriptografik himoya ..... +konfidensiallik va butunlikni ta minlaydi. -konfidensiallik va foydalanuvchanlikni ta minlaydi. -foydalanuvchanlik va butunlikni ta minlaydi. -konfidensiallik ta minlaydi. ?Jumlani to ldiring. ... kompyuter davriga tegishli shifrlarga misol bo la oladi. +DES, AES shifri -Sesar shifri -Kodlar kitobi -Enigma shifri ?.... kriptografik shifrlash algoritmlari blokli va oqimli turlarga ajratiladi. +Simmetrik -Ochiq kalitli -Asimmetrik -Klassik davr ?Jumlani to ldiring. .... shifrlar tasodifiy ketma-ketliklarni generatsiyalashga asoslanadi. +Oqimli -Blokli -Ochiq kalitli -Asimetrik ?Ochiq matn qismlarini takroriy shifrlovchi algoritmlar bu - +blokli shifrlar -oqimli shifrlash -ochiq kalitli shifrlar -asimmetrik shifrlar ?A5/1 shifri bu - +oqimli shifr. -blokli shifr. -ochiq kalitli shifr. -asimmetrik shifr ?Quyidagi muammolardan qaysi biri simmetrik kriptotizimlarga xos. +Kalitni taqsimlash zaruriyati. -Shifrlash jarayonining ko p vaqt olishi. -Kalitlarni esda saqlash murakkabligi. -Foydalanuvchilar tomonidan maqbul ko rilmasligi. ?Quyidagi atamalardan qaysi biri faqat simmetrik blokli shifrlarga xos? +Blok uzunligi. -Kalit uzunligi. -Ochiq kalit. -Kodlash jadvali. ?Jumlani to ldiring. Sesar shifri .... akslantirishga asoslangan. +o rniga qo yish -o rin almashtirish -ochiq kalitli -kombinatsion ?Kriptotizimning to liq xavfsiz bo lishi Kerxgofs prinsipiga ko ra qaysi kattalikning nomalum bo lishiga asoslanadi? +Kalit. -Algoritm. -Shifrmtn. -Protokol. ?Shifrlash va deshifrlashda turli kalitlardan foydalanuvchi shifrlar bu - +ochiq kalitli shifrlar. -simmetrik shifrlar. -bir kalitli shifrlar -xesh funksiyalar. ?Agar simmetrik kalitning uzunligi 64 bit bo lsa, jami bo lishi mumkin bo lgan kalitlar soni nechta? +264 -64! -642 -263 ?Axborotni qaysi xususiyatlari simmetrik shifrlar yordamida ta minlanadi. +Konfidensiallik va butunlik. -Konfidensiallik. -Butunlik va foydalanuvchanlik. -Foydalanuvchanlik va konfidensiallik. ?Axborotni qaysi xususiyatlari ochiq kalitli shifrlar yordamida ta minlanadi. +Konfidensiallik. -Konfidensiallik, butunlik va foydalanuvchanlik. -Butunlik va foydalanuvchanlik. -Foydalanuvchanlik va konfidensiallik. ?Elektron raqamli imzo tizimi. +MAC tizimlari. -Simmetrik shifrlash tizimlari. -Xesh funksiyalar. -Butunlik va foydalanuvchanlik. ?Qaysi ochiq kalitli algoritm katta sonni faktorlash muammosiga asoslanadi? +RSA algoritmi. -El-Gamal algoritmi. -DES. -TEA. ?Rad etishdan himoyalashda ochiq

kalitli kriptotizimlarning qaysi xususiyati muhim hisoblanadi. +Ikkita kalitdan foydalanilgani. - Matematik muammoga asoslanilgani. -Ochiq kalitni saqlash zaruriyati mavjud emasligi. -Shaxsiy kalitni saqlash zarurligi. ?Quyidagi talablardan qaysi biri xesh funksiyaga tegishli emas. +Bir tomonlama funksiya bo'lmayligi kerak. -Amalga oshirishdagi yuqori tezkorlik. -Turli kirishlar turli chiqishlarni akslantirishi. -Kolliziyaga bardoshli bo'lishi. ?Quyidagi xususiyatlardan qaysi biri elektron raqamli imzo tomonidan ta'minlanadi? +Axborot butunligini va rad etishdan himoyalash. -Axborot konfidensialligini va rad etishdan himoyalash. -Axborot konfidensialligi. -Axborot butunligi. ?Faqat ma'lumotni butunligini ta'minlovchi kriptotizimlarni ko'rsating. +MAC (Xabarlarini autentifikatsiya kodlari) tizimlari. -Elektron raqamli imzo tizimlari. -Ochiq kalitli kriptografik tizimlar. -Barcha javoblar to'g'ri. ?Foydalanuvchini tizimga tanitish jarayoni bu? +Identifikatsiya. - Autentifikatsiya. -Avtorizatsiya. -Ro'yxatga olish. ?Foydalanuvchini haqiqiylikni tekshirish jarayoni bu? +Autentifikatsiya. -Identifikatsiya. -Avtorizatsiya. -Ro'yxatga olish. ?Tizim tomonidan foydalanuvchilarga imtiyozlar berish jarayoni bu? +Avtorizatsiya. -Autentifikatsiya. -Identifikatsiya. -Ro'yxatga olish. ?Parolga asoslangan autentifikatsiya usulining asosiy kamchiligini ko'rsating? +Esda saqlash zaruriyati. -Birga olib yurish zaruriyati. -Almashtirib bo'lmaylik. -Qalbakilashtirish mumkinligi. ?Biror narsani bilishga asoslangan autentifikatsiya deyilganda quyidagilardan qaysilar tushuniladi. +PIN, Parol. -Token, mashinaning kaliti. -Yuz tasviri, barmoq izi. -Biometrik parametrlar. ?Tokenga asoslangan autentifikatsiya usulining asosiy kamchiligini ayting? +Doimo xavfsiz saqlab olib yurish zaruriyati. -Doimo esda saqlash zaruriyati. -Qalbakilashtirish muammosi mavjudligi. -Almashtirib bo'lmaylik. ?Esda saqlashni va olib yurishni talab etmaydigan autentifikatsiya usuli bu - +biometrik autentifikatsiya. -parolga asoslangan autentifikatsiya. - tokenga asoslangan autentifikatsiya. -ko'p faktorli autentifikatsiya. ?Qaysi biometrik parametr eng yuqori universallik xususiyatiga ega? +Yuz tasviri. -Ko'z qorachig'i. -Barmoq izi. -Qo'l shakli. ?Qaysi biometrik parametr eng yuqori takrorlanmaslik xususiyatiga ega? +Ko'z qorachig'i. -Yuz tasviri. - Barmoq izi. -Qo'l shakli. ?Quyidagilardan qaysi biri har ikkala tomonning haqiqiylikni tekshirish jarayonini ifodalaydi? +Ikki tomonlama autentifikatsiya. -Ikki faktorli autentifikatsiya. -Ko'p faktorli autentifikatsiya. -Biometrik autentifikatsiya. ?Parolga asoslangan autentifikatsiya usuliga qaratilgan hujumlarni ko'rsating? +Parollar lug'atidan foydalanish asosida hujum, yelka orqali qarash hujumi, zararli dasturlardan foydalanish asosida hujum. -Fizik o'g'irlash hujumi, yelka orqali qarash hujumi, zararli dasturlardan foydalanish asosida hujum. -Parollar lug'atidan foydalanish asosida hujum, yelka orqali qarash hujumi, qalbakilashtirish hujumi. -Parollar lug'atidan foydalanish asosida hujum, bazadagi parametrlarni almashtirish hujumi, zararli dasturlardan foydalanish asosida hujum. ?Tokenga asoslangan autentifikatsiya usuliga qaratilgan hujumlarni ko'rsating? +Fizik o'g'irlash, mobil qurilmalarda zararli dasturlardan foydalanishga asoslangan hujumlar -Parollar lug'atidan foydalanish asosida hujum, yelka orqali qarash hujumi, zararli dasturlardan foydalanish asosida hujum -Fizik o'g'irlash, yelka orqali qarash hujumi, zararli dasturlardan foydalanishga asoslangan hujumlar -Parollar lug'atidan foydalanish asosida hujum, bazadagi parametrlarni almashtirish hujumi, zararli dasturlardan foydalanish asosida hujum ?Foydalanuvchi parollari bazada qanday ko'rinishda saqlanadi? +Xeshlangan ko'rinishda. - Shifrlangan ko'rinishda. -Ochiq holatda. -Bazada saqlanmaydi. ?Agar parolning uzunligi 8 ta belgi va har bir o'rinda 128 ta turlicha belgidan foydalanish mumkin bo'lsa, bo'lishi mumkin bo'lgan jami parollar sonini toping. +1288 -8128 -128! -2128 ?Parolni "salt" (tuz) kattaligidan foydalanib xeshlashdan (h(password, salt)) asosiy maqsad nima? +Buzg'unchiga ortiqcha hisoblashni talab etuvchi murakkablikni yaratish. -Buzg'unchi topa olmasligi uchun yangi nomalum kiritish. -Xesh qiymatni tasodifiylik darajasini oshirish. -Xesh qiymatni qaytmaslik talabini oshirish.

?Quyidagilardan qaysi biri tabiiy tahdidga misol bo'ladi? +Yong in, suv toshishi, harorat ortishi. - Yong in, o'g'irlik, qisqa tutashuvlar. -Suv toshishi, namlikni ortib ketishi, bosqinchilik. -Bosqinchilik, terrorizm, o'g'irlik. ?Qaysi nazorat usuli axborotni fizik himoyalashda inson faktorini mujassamlashtirgan? +Mamuriy nazoratlash. -Fizik nazoratlash. -Texnik nazoratlash. -Apparat nazoratlash. ?Faqat ob'ektning egasi tomonidan foydalanishga mos bo'lgan mantiqiy foydalanish usulini ko'rsating? +Diskretsiya foydalanishni boshqarish. -Mandatli foydalanishni boshqarish. -Rolga asoslangan foydalanishni boshqarish. -Attributga asoslangan foydalanishni boshqarish. ?Qaysi usul ob'ektlar va sub'ektlarni klassifikatsiyalashga asoslangan? +Mandatli foydalanishni boshqarish. -Diskretsiya foydalanishni boshqarish. -Rolga asoslangan foydalanishni boshqarish. -Attributga asoslangan foydalanishni boshqarish. ?Biror faoliyat turi bilan bog'liq harakatlar va majburiyatlar to'plami bu? +Rol. -Imtiyoz. -Daraja. -Imkoniyat. ?Qoida, siyosat, qoida va siyosatni mujassamlashtirgan algoritmlar, majburiyatlar va maslahatlar kabi tushunchalar qaysi foydalanishni boshqarish usuliga aloqador. +Attributga asoslangan foydalanishni boshqarish. -Rolga asoslangan foydalanishni boshqarish. -Mandatli foydalanishni boshqarish. -Diskretsiya foydalanishni boshqarish. ?Bell-Lapadula modeli axborotni qaysi xususiyatini ta'minlashni maqsad qiladi? +Konfidentsiallik. -Butunlik. -Foydalanuvchanlik. -Ishonchlilik. ?Biba modeli axborotni qaysi xususiyatini ta'minlashni maqsad qiladi? +Butunlik. -Konfidentsiallik. -Foydalanuvchanlik. -Maxfiylik. ?Qaysi turdagi shifrlash vositasida barcha kriptografik parametrlar kompyuterning ishtirokisiz generatsiya qilinadi? +Apparat. -Dasturiy. -Simmetrik. -Ochiq kalitli. ?Qaysi turdagi shifrlash vositasida shifrlash jarayonida boshqa dasturlar kabi kompyuter resursidan foydalanadi? +Dasturiy. -Apparat. -Simmetrik. -Ochiq kalitli. ?Yaratishda biror matematik muammoga asoslanuvchi shifrlash algoritmini ko'rsating? +Ochiq kalitli shifrlar. -Simmetrik shifrlar. -Blokli shifrlar. -Oqimli shifrlar. ?Xesh funksiyalarda kolliziya hodisasi bu? +Ikki turli matnlarning xesh qiymatlarini bir xil bo'lishi. -Cheksiz uzunlikdagi axborotni xeshlay olishi. -Tezkorlikda xeshlash imkoniyati. -Turli matnlar uchun turli xesh qiymatlarni hosil bo'lishi. ?64 ta belgidan iborat Sesar shifrlash usulida kalitni bilmasdan turib nechta urinishda ochiq matnni aniqlash mumkin? +63 -63! -32 -322 ?Elektron raqamli imzo muolajalarini ko'rsating? +Imzoni shakllantirish va imkoni tekshirish. -Shifrlash va deshifrlash. -Imzoni xeshlash va xesh matnni deshifrlash. -Imzoni shakllantirish va xeshlash. ?"Yelka orqali qarash" hujumi qaysi turdagi autentifikatsiya usuliga qaratilgan. +Parolga asoslangan autentifikatsiya. -Tokenga asoslangan autentifikatsiya. -Biometrik autentifikatsiya. -Ko'z qorachig'iga asoslangan autentifikatsiya. ?Sotsial injineriyaga asoslangan hujumlar qaysi turdagi autentifikatsiya usuliga qaratilgan. +Parolga asoslangan autentifikatsiya. -Tokenga asoslangan autentifikatsiya. -Biometrik autentifikatsiya. -Ko'z qorachig'iga asoslangan autentifikatsiya. ?Yo'qolgan holatda almashtirish qaysi turdagi autentifikatsiya usuli uchun eng arzon. +Parolga asoslangan autentifikatsiya. -Tokenga asoslangan autentifikatsiya. -Biometrik autentifikatsiya. -Ko'z qorachig'iga asoslangan autentifikatsiya. ?Qalbakilashtirish hujumi qaysi turdagi autentifikatsiya usuliga qaratilgan. +Biometrik autentifikatsiya. -Biror narsani bilishga asoslangan autentifikatsiya. -Biror narsaga egalik qilishga asoslangan autentifikatsiya. -Tokenga asoslangan autentifikatsiya ?Axborotni butunligini ta'minlash usullarini ko'rsating. +Xesh funksiyalar, MAC. -Shifrlash usullari. -Assimetrik shifrlash usullari, CRC tizimlari. -Shifrlash usullari, CRC tizimlari. ?Quyidagilardan qaysi biri to'liq kompyuter topologiyalarini ifodalaymaydi. +LAN, GAN, OSI. -Yulduz, WAN, TCP/IP. -Daraxt, IP, OSI. -Shina, UDP, FTP. ?OSI tarmoq modeli nechta sathdan iborat? +7 -4 -6 -5 ?TCP/IP tarmoq modeli nechta sathdan iborat? +4 -7 -6 -5 ?Hajmi bo'yicha eng kichik hisoblangan tarmoq turi bu - +PAN -LAN -CAN -MAN ?IPv6 protokolida IP manzilni ifodalashda necha bit ajratiladi. +128 -32 -64 -4 ?IP manzilni domen nomlariga yoki aksincha

almashtirishni amalga oshiruvchi xizmat bu- +DNS -TCP/IP -OSI -UDP ?Natijasi tashkilotning amallariga va funksional harakatlariga zarar keltiruvchi hodisalarning potensial paydo bo'lishi bu? +Tahdid. -Zaiflik. -Hujum. -Aktiv. ?Zaiflik orqali AT tizimi xavfsizligini buzish tomon amalga oshirilgan harakat bu? +Hujum. -Zaiflik. -Tahdid. -Zararli harakat. ?Quyidagilardan qaysi biri tarmoq xavfsizligi muammolariga sabab bo'lmaydi? +Routerlardan foydalanmaslik. -Qurilma yoki dasturiy vositani noto'g'ri sozlanish. -Tarmoqni xavfsiz bo'lmagan tarzda va zaif loyihalash. -Tugma texnologiya zaifligi. ?Tarmoq xavfsizligini buzilishi biznes faoliyatga qanday ta'sir qiladi? +Biznes faoliyatning buzilishi, huquqiy javobgarlikka sababchi bo'ladi. -Axborotni o'g'irlanishi, tarmoq qurilmalarini fizik buzilishiga olib keladi. -Maxfiylikni yo'q qilishi, tarmoq qurilmalarini fizik buzilishiga olib keladi. -Huquqiy javobgarlik, tarmoq qurilmalarini fizik buzilishiga olib keladi. ?Razvedka hujumlari bu? +Asosiy hujumlarni oson amalga oshirish uchun tashkilot va tarmoq haqidagi axborotni to'plashni maqsad qiladi. -Turli texnologiyalardan foydalangan holda tarmoqqa kirishga harakat qiladi. -Foydalanuvchilarga va tashkilotlarda mavjud bo'lgan biror xizmatni cheklashga urinadi. -Tizimni fizik buzishni maqsad qiladi. ?Kirish hujumlari bu? +Turli texnologiyalardan foydalangan holda tarmoqqa kirishga harakat qiladi. -Asosiy hujumlarni oson amalga oshirish uchun tashkilot va tarmoq haqidagi axborotni to'plashni maqsad qiladi. -Foydalanuvchilarga va tashkilotlarda mavjud bo'lgan biror xizmatni cheklashga urinadi. -Tarmoq haqida axborotni to'plash hujumchilarga mavjud bo'lgan potensial zaiflikni aniqlashga harakat qiladi. ?Xizmatdan voz kechishga qaratilgan hujumlar bu? +Foydalanuvchilarga va tashkilotlarda mavjud bo'lgan biror xizmatni cheklashga urinadi. -Turli texnologiyalardan foydalangan holda tarmoqqa kirishga harakat qiladi. -Asosiy hujumlarni oson amalga oshirish uchun tashkilot va tarmoq haqidagi axborotni to'plashni maqsad qiladi. -Tarmoq haqida axborotni to'plash hujumchilarga mavjud bo'lgan potensial zaiflikni aniqlashga harakat qiladi. ?Paketlarni snifferlash, portlarni skanerlash va Ping buyrug'ini yuborish hujumlari qaysi hujumlar toifasiga kiradi? +Razvedka hujumlari. -Kirish hujumlari. -DOS hujumlari. -Zararli dasturlar yordamida amalga oshiriladigan hujumlar. ?O'zini yaxshi va foydali dasturiy vosita sifatida ko'rsatuvchi zararli dastur turi bu? +Trojan otlari. -Adware. -Spyware. -Backdoors. ?Marketing maqsadida yoki reklamani namoyish qilish uchun foydalanuvchini ko'rish rejimini kuzutib boruvchi zararli dastur turi bu? +Adware. -Trojan otlari. -Spyware. -Backdoors. ?Himoya mexanizmini aylanib o'tib tizimga ruxsatsiz kirish imkonini beruvchi zararli dastur turi bu? +Backdoors. -Adware. -Trojan otlari. -Spyware. ?Paket filterlari turidagi tarmoqlararo ekran vositasi OSI modelining qaysi sathida ishlaydi? +Tarmoq sathida. -Transport sathida. -Ilova sathida. -Kanal sathida. ?Tashqi tarmoqdagi foydalanuvchilardan ichki tarmoq resurslarini himoyalash qaysi himoya vositasining vazifasi hisoblanadi. +Tarmoqlararo ekran. -Antivirus. -Virtual himoyalangan tarmoq. -Router. ?Ichki tarmoq foydalanuvchilarini tashqi tarmoqqa bo'lgan murojaatlarini chegaralash qaysi himoya vositasining vazifasi hisoblanadi. +Tarmoqlararo ekran. -Antivirus. -Virtual himoyalangan tarmoq. -Router. ?2 lik sanoq tizimida 11011 soniga 11010 sonini 2 modul bo'yicha qo'shing? +00001 - 10000 -01100 -11111 ?2 lik sanoq tizimida 11011 soniga 00100 sonini 2 modul bo'yicha qo'shing? +11111 -10101 -11100 -01001 ?2 lik sanoq tizimida 11011 soniga 11010 sonini 2 modul bo'yicha qo'shing? +00001 -10000 -01100 -11111 ?Axborot saqlagich vositalaridan qayta foydalanish xususiyatini saqlab qolgan holda axborotni yo'q qilish usuli qaysi? +Bir necha marta takroran yozish va maxsus dasturlar yordamida saqlagichni tozalash -Magnitsizlantirish -Formatlash -Axborotni saqlagichdan o'chirish ?Elektron ma'lumotlarni yo'q qilishda maxsus qurilma ichida joylashtirilgan saqlagichning xususiyatlari o'zgartiriladigan usul bu ... +magnitsizlantirish. -shredirlash. -yanchish. -formatlash. ?Yo'q qilish usullari orasidan ekologik jihatdan ma



qullanmaydigan va maxsus joy talab qiladigan usul qaysi? +Yoqish -Maydalash -Ko mish -Kimyoviy ishlov berish ?Kiberjinoatchilik bu - ? +Kompyuter yoki boshqa qurilmalarga qarshi qilingan yoki kompyuter va boshqa qurilmalar orqali qilingan jinoiy faoliyat. -Kompyuterlar bilan bog liq falsafiy soha bo lib, foydalanuvchilarning xatti-harakatlari, kompyuterlar nimaga dasturlashtirilganligi va umuman insonlarga va jamiyatga qanday ta sir ko rsatishini o rganadi. -Hisoblashga asoslangan bilim sohasi bo lib, buzg unchilar mavjud bo lgan sharoitda amallarni kafolatlash uchun o zida texnologiya, inson, axborot va jarayonni mujassamlashtirgan. -Tizimlarni, tarmoqlarni va dasturlarni raqamli hujumlardan himoyalash amaliyoti. ?Kiberetika bu - ? +Kompyuterlar bilan bog liq falsafiy soha bo lib, foydalanuvchilarning xatti-harakatlari, kompyuterlar nimaga dasturlashtirilganligi va umuman insonlarga va jamiyatga qanday ta sir ko rsatishini o rganadi. - Kompyuter yoki boshqa qurilmalarga qarshi qilingan yoki kompyuter va boshqa qurilmalar orqali qilingan jinoiy faoliyat. -Hisoblashga asoslangan bilim sohasi bo lib, buzg unchilar mavjud bo lgan sharoitda amallarni kafolatlash uchun o zida texnologiya, inson, axborot va jarayonni mujassamlashtirgan. -Tizimlarni, tarmoqlarni va dasturlarni raqamli hujumlardan himoyalash amaliyoti. ?Shaxsiy simsiz tarmoqlar qo llanish sohasini belgilang +Tashqi qurilmalar kabellarining o rnida -Binolar va korxonalar va internet orasida belgilangan simsiz bog lanish -Butun dunyo bo yicha internetdan foydalanishda -Simli tarmoqlarni mobil kengaytirish ?VPNning texnik yechim arxitekturasiga ko ra turlari keltirilgan qatorni aniqlang? +Korporativ tarmoq ichidagi VPN; masofadan foydalaniluvchi VPN; korporativ tarmoqlararo VPN -Kanal sathidagi VPN; tarmoq sathidagi VPN; seans sathidagi VPN -Marshuritizator ko rinishidagi VPN; tramoqlararo ekran ko rinishidagi VPN -Dasturiy ko rinishdagi VPN; maxsus shifrlash protsessoriga ega apparat vosita ko rinishidagi VPN ?Axborotning konfidensialligi va butunligini ta minlash uchun ikki uz el orasida himoyalangan tunelni quruvchi himoya vositasi bu? +Virtual Private Network -Firewall -Antivirus -IDS ?Qanday tahdidlar passiv hisoblanadi? +Amalga oshishida axborot strukturasi va mazmunida hech narsani o zgartirmaydigan tahdidlar -Hech qachon amalga oshirilmaydigan tahdidlar - Axborot xavfsizligini buzmaydigan tahdidlar -Texnik vositalar bilan bog liq bo lgan tahdidlar ?Quyidagi qaysi hujum turi razvedka hujumlari turiga kirmaydi? +Ddos -Paketlarni snifferlash -Portlarni skanerlash -Ping buyrug ini yuborish ?Trafik orqali axborotni to plashga harakat qilish razvedka hujumlarining qaysi turida amalga oshiriladi? +Passiv -DNS izi -Lug atga asoslangan -Aktiv ?Portlarni va operatsion tizimni skanerlash razvedka hujumlarining qaysi turida amalga oshiriladi? +Aktiv -Passiv -DNS izi -Lug atga asoslangan ?Paketlarni snifferlash, portlarni skanerlash, ping buyrug ini yuborish qanday hujum turiga misol bo ladi? +Razvedka hujumlari -Xizmatdan voz kechishga undash hujumlari -Zararli hujumlar -Kirish hujumlari ?DNS serverlari tarmoqda qanday vazifani amalga oshiradi? +Xost nomlari va internet nomlarini IP manzillarga o zgartirish va teskarisini amalga oshiradi -Ichki tarmoqqa ulanishga harakat qiluvchi boshqa tarmoq uchun kiruvchi nuqta vazifasini bajaradi -Tashqi tarmoqqa ulanishga harakat qiluvchi ichki tarmoq uchun chiqish nuqtasi vazifasini bajaradi -Internet orqali ma lumotlarni almashinuvchi turli ilovalar uchun tarmoq ulanishlarini sozlash funksiyasini amalga oshiradi ?Markaziy xab yoki tugun orqali tarmoqni markazlashgan holda boshqarish qaysi tarmoq topologiyasida amalga oshiriladi? +Yulduz -Shina -Xalqa -Mesh ?Quyidagilardan qaysilari ananaviy tarmoq turi hisoblanadi? +WAN, MAN, LAN -OSI, TCP/IP -UDP, TCP/IP, FTP -Halqa, yulduz, shina, daraxt ?Quyidagilardan qaysilari tarmoq topologiyalari hisoblanadi? +Halqa, yulduz, shina, daraxt -UDP, TCP/IP, FTP -OSI, TCP/IP -SMTP, HTTP, UDP ?Yong inga qarshi tizimlarni aktiv chora turiga quyidagilardan qaysilari kiradi? +Yong inni aniqlash va bartaraf etish tizimi -Minimal darajada yonuvchan materiallardan foydalanish - Yetarlicha miqdorda qo shimcha chiqish yo llarini mavjudligi -Yong inga aloqador tizimlarni to g ri

madadlanganligi ?Yong inga qarshi kurashishning aktiv usuli to g ri ko rsatilgan javobni toping? +Tutunni aniqlovchilar, alangani aniqlovchilar va issiqlikni aniqlovchilar -Binoga istiqomat qiluvchilarni yong in sodir bo lganda qilinishi zarur bo lgan ishlar bilan tanishtirish -Minimal darajada yonuvchan materiallardan foydalanish, qo shimcha etaj va xonalar qurish -Yetarli sondagi qo shimcha chiqish yo llarining mavjudligi ?Yong inga qarshi kurashishning passiv usuliga kiruvchi choralarni to g ri ko rsatilgan javobni toping? +Minimal darajada yonuvchan materiallardan foydalanish, qo shimcha etaj va xonalar qurish -Tutun va alangani aniqlovchilar -O t o chirgich, suv purkash tizimlari -Tutun va alangani aniqlovchilar va suv purkash tizimlari ?Fizik himoyani buzilishiga olib keluvchi tahdidlar yuzaga kelish shakliga ko ra qanday guruhlarga bo linadi? +Tabiiy va sun iy -Ichki va tashqi -Aktiv va passiv -Bir faktorlik va ko p faktorli ?Quyidagilarnig qaysi biri tabiiy tahdidlarga misol bo la oladi? +Toshqinlar, yong in, zilzila -Bosqinchilik, terrorizm, o g irlik -O g irlik, toshqinlar, zilzila -Terorizim, toshqinlar, zilzila ?Quyidagilarnig qaysi biri sun iy tahdidlarga misol bo la oladi? +Bosqinchilik, terrorizm, o g irlik -Toshqinlar, zilzila, toshqinlar -O g irlik, toshqinlar, zilzila -Terorizim, toshqinlar, zilzila ?Kolliziya hodisasi deb nimaga aytiladi? +Ikki xil matn uchun bir xil xesh qiymat chiqishi -ikki xil matn uchun ikki xil xesh qiymat chiqishi -bir xil matn uchun bir xil xesh qiymat chiqishi -bir xil matn uchun ikki xil xesh qiymat chiqishi ?GSM tarmog ida foydalaniluvchi shifrlash algoritmi nomini ko rsating? +A5/1 -DES -AES -RC4 ?O zbekistonda kriptografiya sohasida faoliyat yurituvchi tashkilot nomini ko rsating? +"UNICON.UZ" DUK -"O zstandart" agentligi -Davlat Soliq Qo mitasi -Kadastr agentligi ?RC4 shifrlash algoritmi simmetrik turga mansub bo lsa, unda nechta kalitdan foydalaniladi? +1 -2 -3 -4 ?A5/1 shifrlash algoritmi simmetrik turga mansub bo lsa, unda nechta kalitdan foydalaniladi? +1 -2 -3 -4 ?AES shifrlash algoritmi simmetrik turga mansub bo lsa, unda nechta kalitdan foydalaniladi? +1 -2 -3 -4 ?DES shifrlash algoritmi simmetrik turga mansub bo lsa, unda nechta kalitdan foydalaniladi? +1 -2 -3 -4 ?A5/1 oqimli shifrlash algoritmda maxfiy kalit necha registrga bo linadi? +3 -4 -5 -6 ?Faqat simmetrik blokli shifrlarga xos bo lgan atamani aniqlang? +blok uzunligi -kalit uzunligi -ochiq kalit -kodlash jadvali ?A5/1 shifri qaysi turga mansub? +oqimli shifrlar -blokli shifrlar -ochiq kalitli shifrlar -assimetrik shifrlar ?.... shifrlar blokli va oqimli turlarga ajratiladi +simmetrik -ochiq kalitli -assimetrik -klassik ?Quyida keltirilgan xususiyatlarning qaysilari xesh funksiyaga mos? +ixtiyoriy olingan har xil matn uchun xesh qiymatlar bir xil bo lmaydi -ixtiyoriy olingan bir xil matn uchun qiymatlar bir xil bo lmaydi -ixtiyoriy olingan har xil matn uchun xesh qiymatlar bir xil bo ladi -ixtiyoriy olingan har xil xesh qiymat uchun dastlabki ma lumotlar bir xil bo ladi ?Quyida keltirilgan xususiyatlarning qaysilari xesh funksiyaga mos? +chiqishda fiksirlangan uzunlikdagi qiymatni beradi -chiqishda bir xil qiymatni beradi -chiqishdagi qiymat bilan kiruvchi qiymatlar bir xil bo ladi -kolliziyaga ega ?Xesh qiymatlarni yana qanday atash mumkin? +dayjest -funksiya -imzo -raqamli imzo ?A5/1 oqimli shifrlash algoritmda dastlabki kalit uzunligi nechki bitga teng? +64 -512 -192 -256 ?A5/1 oqimli shifrlash algoritmi asosan qayerda qo llaniladi? +mobil aloqa standarti GSM protokolida -simsiz aloqa vositalaridagi mavjud WEP protokolida -internet trafiklarini shifrlashda -radioaloqa tarmoqlarida ?Assimetrik kriptotizimlarda necha kalitdan foydalaniladi? +2 ta -3 ta -4 ta -kalit ishlatilmaydi ?Simmetrik kriptotizimlarda necha kalitdan foydalaniladi? +1 ta -3 ta -4 ta -kalit ishlatilmaydi ?Kriptotizimlar kalitlar soni bo yicha qanday turga bo linadi? +simmetrik va assimetrik turlarga -simmetrik va bir kalitli turlarga -3 kalitli turlarga -assimetrik va 2 kalitli turlarga ?Kriptologiya qanday yo nalishlarga bo linadi? +kriptografiya va kriptotahlil -kriptografiya va kriptotizim -kripto va kriptotahlil -kriptoanaliz va kriptotizim ?Qaysi chora tadbirlar virusdan zararlanish holatini kamaytiradi? +Barcha javoblar to g ri -Faqat litsenziyali dasturiy ta minotdan foydalanish. -Kompyuterni zamonaviy antivirus dasturiy vositasi bilan ta minlash va uni doimiy

yangilab borish. -Boshqa kompyuterda yozib olingan ma'lumotlarni o'qishdan oldin har bir saqlagichni antivirus tekshiruvidan o'tkazish. ?Antivirus dasturiy vositalari zararli dasturlarga qarshi to'liq himoyani ta'minlay olmasligining asosiy sababini ko'rsating? +Paydo bo'layotgan zararli dasturiy vositalar sonining ko'pligi. -Viruslar asosan antivirus ishlab chiqaruvchilar tomonidan yaratilishi. -Antivirus vositalarining samarali emasligi. -Aksariyat antivirus vositalarining pullik ekanligi. ?...umumiy tarmoqni ichki va tashqi qismlarga ajratib himoyalash imkonini beradi. +Tarmoqlararo ekran -Virtual himoyalangan tarmoq -Global tarmoq -Korxona tarmog'i ?RSA algoritmidan  $p=5$ ,  $q=13$ ,  $e=7$  ga teng bo'lsa, shaxsiy kalitni hisoblang? +7 -13 -65 -35 ?..... hujumida hujumchi o'rnatilgan aloqaga suqilib kiradi va aloqani bo'ladi. Nuqtalar o'rniga mos javobni qo'ying. +O'rnatilgan odam. -Qo'pol kuch. -Parolga qaratilgan. -DNS izi. ?Agar ob'ektning xavfsizlik darajasi sub'ektning xavfsizlik darajasidan kichik yoki teng bo'lsa, u holda O'qish uchun ruxsat beriladi. Ushbu qoida qaysi foydalanishni boshqarish usuliga tegishli. +MAC -DAC -RMAC -ABAC ?GSM tarmog'ida ovozli so'zlashuvlarni shifrlash algoritmi bu? +A5/1 -DES -GOST -RSA ?RSA algoritmidan ochiq kalit  $e=7$ ,  $N=35$  ga teng bo'lsa,  $M=2$  ga teng ochiq matnni shifrlash natijasini ko'rsating? +23 -35 -5 -7 ?RSA algoritmidan ochiq kalit  $e=7$ ,  $N=143$  ga teng bo'lsa,  $M=2$  ga teng ochiq matnni shifrlash natijasini ko'rsating? +128 -49 -11 -7 ?Jumlani to'ldiring. Agar axborotning o'g'irlanishi moddiy va ma'naviy boyliklarning yo'qotilishiga olib kelsa. -jinoyat sifatida baholanadi. -rag'bat hisoblanadi. -buzg'unchilik hisoblanadi. -guruhlar kurashi hisoblanadi. ?Jumlani to'ldiring. Simli va simsiz tarmoqlar orasidagi asosiy farq ... +tarmoq chetki nuqtalari orasidagi mutlaqo nazoratlamaydigan xudud mavjudligi. -tarmoq chetki nuqtalari orasidagi xududning kengligi. -himoya vositalarining chegaralanganligi. -himoyani amalga oshirish imkoniyati yo'qligi. ?Jumlani to'ldiring. Simmetrik shifrlash algoritmlari ochiq ma'lumotdan foydalanish tartibiga ko'ra ... +blokli va oqimli turlarga bo'linadi. -bir kalitli va ikki kalitli turlarga bo'linadi. -Feistel tarmog'iga asoslangan va SP tarmog'iga asoslangan turlarga bo'linadi. -murakkablikka va tizimni nazariy yondoshuvga asoslangan turlarga bo'linadi. ?Jumlani to'ldiring. Tarmoqlararo ekranning vazifasi ... +ishonchli va ishonchsiz tarmoqlar orasida ma'lumotlarga kirishni boshqarish. -tarmoq hujumlarini aniqlash. -trafikni taqiqlash. -tarmoqdagi xabarlar oqimini uzish va ulash. ?Faktorlash muammosi asosida yaratilgan assimetrik shifrlash usuli? +RSA -El-Gamal -Elliptik egri chiziqqa asoslangan shifrlash -Diffie-Hellman ?Eng zaif simsiz tarmoq protokolini ko'rsating? +WEP -WPA -WPA2 -WPA3 ?Axborotni shifrlashdan maqsadi nima? +Maxfiy xabar mazmunini yashirish. -Ma'lumotlarni zichlashtirish, siqish. -Ma'lumotlarni yig'ish va sotish. -Ma'lumotlarni uzatish. ?9 soni bilan o'zaro tub bo'lgan sonlarni ko'rsating? +10, 8 -6, 10 -18, 6 -9 dan tashqari barcha sonlar ?12 soni bilan o'zaro tub bo'lgan sonlarni ko'rsating? +11, 13 -14, 26 -144, 4 -12 dan tashqari barcha sonlar ?13 soni bilan o'zaro tub bo'lgan sonlarni ko'rsating? +5, 7 -12, 26 -14, 39 -13 dan tashqari barcha sonlar ?Jumlani to'ldiring. Autentifikatsiya tizimlari asoslanishiga ko'ra ... turga bo'linadi. +3 -2 -4 -5 ?...umumiy tarmoqni ichki va tashqi qismlarga ajratib himoyalash imkonini beradi. +Tarmoqlararo ekran -Virtual himoyalangan tarmoq -Global tarmoq -Korxona tarmog'i ?Antivirus dasturiy vositalari zararli dasturlarga qarshi to'liq himoyani ta'minlay olmasligining asosiy sababini ko'rsating? +Paydo bo'layotgan zararli dasturiy vositalar sonining ko'pligi. -Viruslar asosan antivirus ishlab chiqaruvchilar tomonidan yaratilishi. -Antivirus vositalarining samarali emasligi. -Aksariyat antivirus vositalarining pullik ekanligi. ?Qaysi chora tadbirlar virusdan zararlanish holatini kamaytiradi? +Barcha javoblar to'g'ri -Faqat litsenziyali dasturiy ta'minotdan foydalanish. -Kompyuterni zamonaviy antivirus dasturiy vositasi bilan ta'minlash va uni doimiy yangilab borish. -Boshqa kompyuterda yozib olingan ma'lumotlarni o'qishdan oldin har bir saqlagichni antivirus tekshiruvidan o'tkazish. ?Virus aniq bo'lganda va xususiyatlari aniq ajratilgan holatda eng katta

samaradorlikka ega zararli dasturni aniqlash usulini ko rsating? +Signaturaga asoslangan usul -O zgarishga asoslangan usul -Anomaliyaga asoslangan usul -Barcha javoblar to g ri ?Signatura (antiviruslarga aloqador bo lgan) bu-? +Fayldan topilgan bitlar qatori. -Fayldagi yoki katalogdagi o zgarish. -Normal holatdan tashqari holat. -Zararli dastur turi. ?Zararli dasturiy vositalarga qarshi foydalaniluvchi dasturiy vosita bu? +Antivirus -VPN -Tarmoqlararo ekran -Brandmauer ?Kompyuter viruslarini tarqalish usullarini ko rsating? +Ma lumot saqlovchilari, Internetdan yuklab olish va elektron pochta orqali. -Ma lumot saqlovchilari, Internetdan yuklab olish va skaner qurilmalari orqali. -Printer qurilmasi, Internetdan yuklab olish va elektron pochta orqali. -Barcha javoblar to g ri. ?Qurbon kompyuteridagi ma lumotni shifrlab, uni deshifrlash uchun to lovni amalga oshirishni talab qiluvchi zararli dastur bu-? +Ransomware. -Mantiqiy bombalar. -Rootkits. -Spyware. ?Internet tarmog idagi obro sizlantirilgan kompyuterlar bu-? +Botnet. -Backdoors. -Adware. -Virus. ?Biror mantiqiy shartni tekshiruvchi trigger va foydali yuklamadan iborat zararli dastur turi bu-? +Mantiqiy bombalar. -Backdoors. -Adware. -Virus. ?Buzg unchiga xavfsizlik tizimini aylanib o tib tizimga kirish imkonini beruvchi zararli dastur turi bu-? +Backdoors. -Adware. -Virus. -Trojan otlari. ?Ma lumotni to liq qayta tiklash qachon samarali amalga oshiriladi? +Saqlagichda ma lumot qayta yozilmagan bo lsa. -Ma lumotni o chirish Delete buyrug i bilan amalga oshirilgan bo lsa. -Ma lumotni o chirish Shifr+Delete buyrug i bilan amalga oshirilgan bo lsa. -Formatlash asosida ma lumot o chirilgan bo lsa. ?Ma lumotni zaxira nusxalash nima uchun potensial tahdidlarni paydo bo lish ehtimolini oshiradi. +Tahdidchi uchun nishon ko payadi. -Saqlanuvchi ma lumot hajmi ortadi. -Ma lumotni butunligi ta minlanadi. -Ma lumot yo qolgan taqdirda ham tiklash imkoniyati mavjud bo ladi. ?Qaysi xususiyatlar RAID texnologiyasiga xos emas? +Shaxsiy kompyuterda foydalanish mumkin. -Serverlarda foydalanish mumkin. -Xatoliklarni nazoratlash mumkin. -Disklarni "qaynoq almashtirish" mumkin. ?Qaysi zaxira nusxalash vositasi oddiy kompyuterlarda foydalanish uchun qo shimcha apparat va dasturiy vositani talab qiladi? +Lentali disklar. -Ko chma qattiq disklar. -USB disklar. -CD/DVD disklar. ?Ma lumotlarni zaxira nusxalash strategiyasi nimadan boshlanadi? +Zarur axborotni tanlashdan. -Mos zaxira nusxalash vositasini tanlashdan. -Mos zaxira nusxalash usulini tanlashdan. -Mos RAID sathini tanlashdan. ?Jumlani to ldiring. .... - muhim bo lgan axborot nusxalash yoki saqlash jarayoni bo lib, bu ma lumot yo qolgan vaqtda qayta tiklash imkoniyatini beradi. +Ma lumotlarni zaxira nusxalash -Kriptografik himoya -VPN -Tarmoqlararo ekran ?Paket filteri turidagi tarmoqlararo ekran vositasi nima asosida tekshirishni amalga oshiradi? +Tarmoq sathi parametrlari asosida. -Kanal sathi parametrlari asosida. -Ilova sathi parametrlari asosida. -Taqqimot sathi parametrlari asosida. ?Jumlani to ldiring. ... texnologiyasi lokal simsiz tarmoqlarga tegishli. +WI-FI -WI-MAX -GSM -Bluetooth ?Jumlani to ldiring. Kriptografik himoya axborotning ... xususiyatini ta minlamaydi. +Foydalanuvchanlik -Butunlik -Maxfiylik -Autentifikatsiya ?Jumlani to ldiring. Parol kalitdan .... farq qiladi. +tasodifiylik darajasi bilan -uzunligi bilan -belgilari bilan -samaradorligi bilan ?Parolga "tuz"ni qo shib xeshlashdan maqsad? +Tahdidchi ishini oshirish. -Murakkab parol hosil qilish. -Murakkab xesh qiymat hosil qilish. -Ya na bir maxfiy parametr kiritish. ?Axborotni foydalanuvchanligini buzishga qaratilgan tahdidlar bu? +DDOS tahdidlar. -Nusxalash tahdidlari. -Modifikatsiyalash tahdidlari. -O rtaga turgan odam tahdidi. ?Tasodifiy tahdidlarni ko rsating? +Texnik vositalarning buzilishi va ishlamasligi. -Axborotdan ruxsatsiz foydalanish. -Zararkunanda dasturlar. -An anaviy josuslik va diversiya. ?Xodimlarga faqat ruxsat etilgan saytlardan foydalanishga imkon beruvchi himoya vositasi bu? +Tarmoqlararo ekran. -Virtual Private Network. -Antivirus. -Router. ?Qaysi himoya vositasi yetkazilgan axborotning butunligini tekshiradi? +Virtual Private Network. -Tarmoqlararo ekran. -Antivirus. -Router. ?Qaysi himoya vositasi tomonlarni

autentifikatsiyalash imkoniyatini beradi? +Virtual Private Network. -Tarmoqlararo ekran. -Antivirus. -Router. ?Foydalanuvchi tomonidan kiritilgan taqiqlangan so'rovni qaysi himoya vositasi yordamida nazoratlash mumkin. +Tarmoqlararo ekran. -Virtual Private Network. -Antivirus. -Router. ?Qaysi himoya vositasi mavjud IP - paketni to'liq shifrlab, unga yangi IP sarlavha beradi? +Virtual Private Network. -Tarmoqlararo ekran. -Antivirus. -Router. ?Ochiq tarmoq yordamida himoyalangan tarmoqni qurish imkoniyatiga ega himoya vositasi bu? +Virtual Private Network. -Tarmoqlararo ekran. -Antivirus. -Router. ?Qaysi himoya vositasida mavjud paket shifrlangan holda yangi hosil qilingan mantiqiy paket ichiga kiritiladi? +Virtual Private Network. -Tarmoqlararo ekran. -Antivirus. -Router. ?Qaysi himoya vositasi tarmoqda uzatilayotgan axborotni butunligi, maxfiyligi va tomonlar autentifikatsiyasini ta'minlaydi? +Virtual Private Network. -Tarmoqlararo ekran. -Antivirus. -Router. ?Qaysi tarmoq himoya vositasi tarmoq manzili, identifikatorlar, interfeys manzili, port nomeri va boshqa parametrlar yordamida filtrlashni amalga oshiradi. +Tarmoqlararo ekran. -Antivirus. -Virtual himoyalangan tarmoq. -Router. ?Web-sahifa bu... +Yagona adresga ega bo'lgan, brauzer yordamida ochish va ko'rish imkoniyatiga ega bo'lgan hujjatdir -Tarmoqqa ulangan kompyuterda, klientga belgilangan umumiy vazifalarni bajarish uchun foydalaniluvchi sahifadir -Klient-server arxitekturasida asosidagi, keng tarqalgan Internetning axborot xizmati -HTML kodlari to'plami ?Web-sayt nima? +Aniq maqsad asosida mantiqiy bog'langan web-sahifalar birlashmasi -Klient-server texnologiyasiga asoslangan, keng tarqalgan Internetning axborot xizmatidir -A va B -Yagona adresga ega bo'lgan hujjat hisoblanib, uni ochish (brauzer yordamida) va o'qish imkoniyati mavjud ?WWW nechta komponentdan tashkil topgan? +4 -5 -3 -2 ?WWWning komponentlari qaysi javobda to'g'ri berilgan? +Dasturiy/texnik vositalar, HTML, HTTP, URI -HTML, FTP, WWW -HTML, CSS, PHP -HTML, JavaScript, JQuery, PHP ?Hozirgi kunda WWWning nechta versiyasi mavjud? +4 -3 -5 -2 ?Web 1.0 ning rivojlanish davrini toping? +1990-2000 yy. -2000-2005 yy. -1980-1990 yy. -2010-2015 yy. ?Web 2.0 ning rivojlanish davrini toping? +2000-2010 yy. -2010-2020 yy. -2020-2030 yy. -1990-2000 yy. ?Web 3.0 ning rivojlanish davrini toping? +2010-2020 yy. -2000-2010 yy. -2020-2030 yy. -1990-2000 yy. ?Web 4.0 ning rivojlanish davrini toping? +2020-2030 yy. -2000-2010 yy. -2010-2020 yy. -1990-2000 yy. ?HTML teglar necha xil bo'ladi? +Juft, toq, maxsus teglar -Toq teglari -Juft teglari -Ko'rinishi ko'p ?Qaysi teg HTML hujjatning tanasini ifodalaydi? +body -html -head -title ?Qaysi teg hujjatning stilini ifodalash uchun ishlatiladi? +style -head -isindex -body ?Qaysi teg HTML hujjatni ifodalaydi? +html -body -meta -isindex ?Qaysi teg HTML hujjat sarlavhasini ifodalaydi? +head -meta -title -body ?Havola to'g'ri ko'rsatilgan qatorni toping. +havola - havola - havola -Ekranni tozalash ?

\_\_\_\_\_ tegi nimani ifodalaydi? +Gorizontal chiziq chizish -Yangi satrga o'tish -qo'shtirnoq -Ekranni tozalash ?Jadval hosil qilish uchun qaysi tegdan foydalaniladi? + ?Jadval ustunlarini birlashtirish atributi qaysi javobda keltirilgan? ?Jadval satrlarini birlashtirish atributi qaysi javobda keltirilgan? ?HTML da shrift o'lchamini o'zgartirish uchun qaysi tegdan foydalaniladi? - - - ? tegi nimani ifodalaydi? +Yangi satrga o'tish -"uzilish" -qo'shtirnoq -Ekranni tozalash ? tegi nima uchun qo'llaniladi? +matnni paragraflarga ajratish uchun -Sarlavhani ifodalash uchun -Obyektni ko'rsatilgan joyga o'rnatish va shu nuqtadan bosh satrga matnni davom ettirish uchun qo'llaniladi -Tartibsiz ro'yxat hosil qilish uchun ?Rasmlar bilan ishlash teglarini qaysi javobda berilgan? +img, map, area, picture -Image, map, a, picture -Image, form, area, photo -img, iframe, areas, picture ? tegining vazifasi nima? +Matnni ajratilgan shaklda aniqlash -Matnni o'chirilgan shaklda belgilash -Matnni tagiga chizilgan shaklda belgilash -Matnni qiya shaklda belgilash ? tegining vazifasi nima? +Matnni tagiga chizilgan shaklda belgilash -Matnni o'chirilgan shaklda belgilash -Matnni ajratilgan shaklda aniqlash -Matnni qiya shaklda belgilash ?

+Matnni o'chirilgan shaklda belgilash -Matnni tagiga chizilgan shaklda belgilash -Matnni ajratilgan shaklda aniqlash -Matnni qir shaklda belgilash ? tegi nimani ifodalaydi? +Tartiblanmagan ro'yxat -Tartiblangan ro'yxat -Jadval yacheykasi -Yangi qatorga o'tish ? matni nimani ifodalaydi? +Teg kvadrat shaklidagi ro'yxat hosil qiladi -Teg aylana shaklidagi ro'yxat hosil qiladi -Teg alifbo ko'rinishdagi ro'yxatni hosil qiladi -Teg raqamli ko'rinishdagi ro'yxatni hosil qiladi ? matni nimani ifodalaydi? +Teg I., II., III., IV. va h.k ko'rinishdagi ro'yxatni hosil qiladi -Teg raqamli ko'rinishdagi ro'yxatni hosil qiladi -Teg kvadrat shaklidagi ro'yxat hosil qiladi -Teg 1., 2., 3., 4. va h.k ko'rinishdagi ro'yxatni hosil qiladi ? tegining majburiy atributini toping +src -title -href -type ?Qaysi teg forma ichida qayerga ma'lumot kiritilishini ifodalaydi? + - - - ?HTMLda forma elementlariga kiritilgan qiymatlarni tozalash uchun qaysi elementdan foydalaniladi? +reset -text -hidden -submit Kriptologiya qanday yo'nalishlarga bo'linadi? #kriptografiya va kriptotahlil kriptografiya va kriptotizim kripto va kriptotahlil kriptoanaliz va kriptotizim +++++ Kriptologiya nima bilan shug'ullanadi? #maxfiy kodlarni yaratish va buzish ilmi bilan maxfiy kodlarni buzish bilan maxfiy kodlarni yaratish bilan maxfiy kodlar orqali ma'lumotlarni yashirish bilan +++++ Kriptografiya nima bilan shug'ullanadi? #maxfiy kodlarni yaratish bilan maxfiy kodlarni buzish bilan maxfiy kodlar orqali ma'lumotlarni yashirish bilan shifrlash uslublarini bilmagan holda shifrlangan ma'lumotni asl holatini topish bilan +++++ Kriptotahlil nima bilan shug'ullanadi? #maxfiy kodlarni buzish bilan maxfiy kodlarni yaratish bilan maxfiy kodlar orqali ma'lumotlarni yashirish bilan shifrlash uslublarini bilmagan holda shifrlangan ma'lumotni asl holatini topish bilan +++++ Shifrlash orqali ma'lumotning qaysi xususiyati ta'minlanadi? #maxfiyligi Butunligi Ishonchliligi foydalanuvchanligi +++++ Ochiq kalitli kriptotizimlar kim tomonidan kashf qilingan? #U.Diffie va M.Hellman Rivest va Adlman Shamir va Rivest U.Diffie va Rivest +++++ Kriptologiya necha yo'nalishga bo'linadi? #2 14 16 18 +++++ Kriptologiya so'zining ma'nosi? #cryptos – maxfiy, logos – ilm cryptos – kodlash, logos – ilm cryptos – kripto, logos – yashiraman cryptos – maxfiy, logos – kalit +++++ Ochiq kalitli kriptotizimlar ma'lumotni qanday xususiyatini taminlaydi? #maxfiyligini Butunligini Foydalanuvchanligini ma'lumotni autentifikatsiyasini +++++ Kriptotizimlar kalitlar soni bo'yicha necha turga bo'linadi? #2 4 6 8 +++++ Kriptotizimlar kalitlar soni bo'yicha qanday turga bo'linadi? #simmetrik va assimetrik turlarga simmetrik va bir kalitli turlarga 3 kalitli turlarga assimetrik va 2 kalitli turlarga +++++ Simmetrik kriptotizimlardagi qanday muammoni ochiq kalitli kriptotizimlar bartaraf etdi? #maxfiy kalitni uzatish muammosini kalitni generatsiyalash muammosini ochiq kalitni uzatish muammosini kalitlar juftini hosil qilish muammosini +++++ Ochiq kalitli kriptotizimlarda qanday turdagi kalitlardan foydalanadi? #ochiq va maxfiy kalitlardan maxfiy kalitlar juftidan maxfiy kalitni uzatishni talab etmaydi ochiq kalitni talab etmaydi +++++ Assimetrik kriptotizimlarda necha kalitdan foydalaniladi? #2 ta 3 ta 4 ta kalit ishlatilmaydi +++++ Kerkxofs printsipi nimadan iborat? #kriptografik tizim faqat kalit noma'lum bo'lgan taqdirdagina maxfiylik ta'minlanadi kriptografik tizim faqat yopiq bo'lgan taqdirdagina maxfiylik ta'minlanadi kriptografik tizim faqat kalit ochiq bo'lgan taqdirdagina maxfiylik ta'minlanadi kriptografik tizim faqat ikkita kalit ma'lum bo'lgan taqdirdagina maxfiylik ta'minlanadi +++++ Kalit bardoshliligi bu -? #eng yaxshi ma'lum algoritim bilan kalitni topish murakkabligidir eng yaxshi ma'lum algoritim yordamida yolg'on axborotni ro'kach qilishdir nazariy bardoshlilik amaliy bardoshlilik +++++ Ochiq kalitni kriptotizimlarda nechta kalitdan foydalanadi? #Ikkita Bitta Uchta kalitdan foydalanilmaydi +++++ Ochiq kalitli kriptotizimlarda qaysi kalit orqali ma'lumot shifrlanadi? #ochiq kalit orqali maxfiy kalit orqali ma'lumot shifrlanmaydi ushbu tizimda kalitdan foydalanilmaydi +++++ Ochiq kalitli kriptotizimda, qaysi kalit orqali ma'lumot rasshifrovkalanadi? #maxfiy kalit orqali ochiq kalit orqali ma'lumot shifrlanmaydi ushbu tizimda kalitdan foydalanilmaydi +++++ Ochiq kalitli kriptotizimlarda

asosan qanday turdagi sonlar bilan ishlaydi? #tub sonlar bilan kasr sonlar bilan chekli maydonda kasr sonlar faqat manfiy sonlar ++++ Qanday sonlar tub sonlar hisoblanadi? #1 va o'ziga bo'linadigan sonlarlar barcha toq sonlar juft bo'lmagan sonlar 2 ga bo'linmaydigan sonlar ++++ Sonlarni tublikka tekshirish algoritmlari nechta sinfga bo'linadi? #ikkita sinfga uchta sinfga bitta sinfga sinflarga bo'linmaydi ++++ Kriptotahlil nima bilan shug'ullanadi? #kalit yoki algoritmi bilmagan holda shifrlangan ma'lumotga mos keluvchi ochiq ma'lumotni topish bilan ochiq ma'lumotlarni shifrlash masalalarining matematik uslublari bilan maxfiy kodlarni yaratish bilan maxfiy kodlar orqali ma'lumotlarni yashirish bilan ++++ RSA algoritmining mualliflarini ko'rsating #R. Rayvest, A. Shamir, L. Adleman Diffi va M. Xellman R. Rayvest, K. Xellman, L. Adleman L. Adleman, El Gamal, K. Shnorrr ++++ Ochiq kalitli shifrlash algoritmi keltirilgan qatorni toping? #RSA AES DES RC4 ++++ Ochiq kalitli shifrlash algoritmi keltirilgan qatorni toping? #El-Gamal AES DES RC4 ++++ Shifrlash orqali ma'lumotning qaysi xususiyati ta'minlanadi? #Maxfiyligi Butunliligi Ishonchliligi Foydalanuvchanliligi ++++ Kriptografiya bu -? #axborotni o'zgartirish vositalari va usullarini o'rganadigan fan axborot mazmunidan beruxsat erkin foydalanishdan muhofazalash axborotni buzishning oldini olish axborot almashtirish vosita va usullari bilan shug'ullanadigan fan sohasi ++++ Faqat simmetrik algoritmi keltirilgan qatorni ko'rsating? #AES RSA El-Gamal Barcha javoblar to'g'ri ++++ Kriptotizimlar kalitlar soni bo'yicha nechta turga bo'linadi? #2 3 4 ++++ Kriptotizimlar kalitlar soni bo'yicha qanday turga bo'linadi? #simmetrik va assimetrik simmetrik va bitta kalitli 3 kalitli kriptotizimlar assimetrik va 2 ta kalitli ++++ Ferma testi qanday turdagi tublikka testlovchi algoritmi hisoblanadi? #ehtimollik testlar tarkibiga kiruvchi algoritmi aniqlashtirilgan testlar tarkibiga kiruvchi algoritmi taqribiy testlar tarkibiga kiruvchi algoritmi tublikka teslovchi algoritmi hisoblanmaydi ++++ Solovey Shtrassen testi qanday turdagi tublikka testlovchi algoritmi hisoblanadi? #ehtimollik testlar tarkibiga kiruvchi algoritmi aniqlashtirilgan testlar tarkibiga kiruvchi algoritmi taqribiy testlar tarkibiga kiruvchi algoritmi tublikka teslovchi algoritmi hisoblanmaydi ++++ Rabbi-Milner testi qanday turdagi tublikka testlovchi algoritmi hisoblanadi? #ehtimollik testlar tarkibiga kiruvchi algoritmi aniqlashtirilgan testlar tarkibiga kiruvchi algoritmi taqribiy testlar tarkibiga kiruvchi algoritmi tublikka teslovchi algoritmi hisoblanmaydi ++++ Sonlarni tublikka tekshiruvchi algoritmlar nechta sinfga bo'linadi? #2 3 4 5 ++++ Sonlarni tublikka tekshiruvchi algoritmlar qanday sinfga bo'linadi? #aniqlashtirilgan va ehtimolli testlar aniqlashtirilgan va taqribiy testlar taqribiy va ehtimolli testlar aniqlashtirilgan, ehtimolli va taqribiy testlar ++++ Sonlarni tublikka tekshiruvchi ehtimollikka asoslangan algoritmlar keltirilgan qatorni ko'rsating? #Ferma, Solovey Shtrassen, Rabbi-Milner Ferma, Solovey Shtrassen, Eyler Eyler, Solovey Shtrassen, Rabbi-Milner Ferma, Eyler, Rabbi-Milner ++++ Elliptik egriz chiqizlarda nuqtalar usitda qanday ammalar bajariladi? #nuqtalarni qo'shish va nuqtalarni ikkilantirish nuqtalarni qo'shish va nuqtalarni ko'paytirish nuqtalarni qo'shish va nuqtalarni bo'lish nuqtalarni ayirish va nuqtalarni ko'paytirish ++++ 1 ga va o'ziga bo'linadigan sonlar qanday sonlar hisoblanadi? #tub sonlar murakkab sonlar toq sonlar juft sonlar Elektron hujjat manbaini haqiqiyligini qaysi amal orqali amalga oshiriladi? #ERI orqali amalga oshiriladi shifrlash algoritmi orqali amalga oshiriladi kodlash orqali amalga oshiriladi autentifikatsiya orqali amalga oshiriladi ++++ Elektron hujjat yaxlitligini (o'zgarmasligini) tekshirish qaysi amal orqali amalga oshiriladi? #ERI orqali amalga oshiriladi kodlash orqali amalga oshiriladi shifrlash algoritmi orqali amalga oshiriladi autentifikatsiya orqali amalga oshiriladi ++++ Elektron hujjatni mualliflikdan bosh tortmasligini qaysi amal orqali amalga oshiriladi? #ERI orqali amalga oshiriladi kodlash orqali amalga oshiriladi autentifikatsiya orqali amalga oshiriladi shifrlash algoritmi orqali amalga oshiriladi ++++ Raqamli imzoni shakllantirish muolajasi qaysi algoritimga tegishli? #ERI algoritimga kodlash algoritimga

shifrlash algoritmiga steganografiya algoritmiga ++++ ECDSA-2000 qaysi davlat standarti hisoblanadi? #AQSH Rossiya O'zbekiston Kanada ++++ O'zDSt 1092:2009 standarti qaysi davlat standarti hisoblanadi? #O'zbekiston AQSH Rossiya Kanada ++++ ГOCT P 34.10-94 standarti qaysi davlat standarti hisoblanadi? #Rossiya O'zbekiston AQSH Kanada ++++ Seans kalitli hamda seans kalitsiz rejimlarda ishlidigan standartni ko'rsating? #O'zDSt 1092:2009 ECDSA-2000 ГOCT P 34.10-94 DSA ++++ DSA qanday standart hisoblanadi? #ERI standarti shifrlash standarti kodlash standarti steganografik standart ++++ Ochiq kalitli kriptotizimlar qanday turdagi matematik murakkablikka asoslangan algoritmlarga bo'linadi? #faktorizatsiyalash va diskret logarifmlash algoritmlariga modulyar arifmetika murakkabligiga asoslangan algoritmlarga diskret logarifmlash murakkabligiga asoslangan algorimtlarga faktorizatsiyalash murakkabligiga asoslangan algorimtlarga ++++ Ochiq kalitli kriptotizimlarning bardoshligini ta'minlashda qanday murakkab muammo turiga asoslanadi? #faktorlash, diskret logarifmlash, elliptik egri chiziqda diskret logarifmlash faktorlash, diskret logarifmlash faktorlash, diskret logarifmlash, elliptik egri chiziqda faktorizatsiyalash faktorlash, diskret logarifmlash, modulyar arifmetikaga ++++ Ehtimolli testlar sonlarni tublikka tekshirishda qanday natijani beradi? #tekshirilayotgan son tub yoki tubmasligi haqida ehtimollik bilan javob beradi tekshirilayotgan son tub yoki tubmasligi haqida kafolatlangan aniq javob beradi tekshirilayotgan son tub yoki tubmasligi haqida tasodifiy ravishda javob beradi tekshirilayotgan son tub yoki tubmasligini 0 va 1 qiymatlarga qarab javob beradi ++++ Sonlarni tublikka tekshirishning ehtimolli algoritmlariga quyidagilarning qaysilari kiradi? #Ferma, Rabbi-Milner, Poklingtong testlari Rabbi-Milner, Solovey-Shtrassen, Pollard testlari Ferma, Solovey-Shtrassen, Pollard testlari Rabbi Milner, Poklington, Pollard testlari ++++ Ochiq kalitli RSA shifrlash algoritmi bardoshliligi qanday matematik muammo turiga asoslangan? #faktorlash murakkabligiga diskret logarifmlash murakkabligiga elliptik egri chiziqlarda faktorizatsiyalash murakkabligiga elliptik egri chiziqlarda faktorizatsiyalash murakkabligiga ++++ Ochiq kalitli El-Gamal shifrlash algoritmi qanday matematik murakkablikka asoslanadi? #diskret logarifmlash murakkabligiga faktorlash murakkabligiga elliptik egri chiziqda diskret logarifmlash murakkabligiga elliptik egri chiziqda faktorlash murakkabligiga ++++ Diffie-Helman algoritmi qanday matematik murakkablikka asoslanadi? #diskret logarifmlash murakkabligiga faktorlash murakkabligiga elliptik egri chiziqda diskret logarifmlash murakkabligiga elliptik egri chiziqda faktorlash murakkabligiga ++++ Diffie-Hellman qanday algoritm hisoblanadi? #kalitlarni ochiq taqsimlash algoritmi ochiq kalitli shifrlash algoritmi diskret logarifmlash murakkabligiga asoslangan shifrlash algoritmi faktorlash murakkabligiga asoslangan kalitlarni ochiq taqsimlash algoritmi ++++ ERI algoritmlari qanday muolajalalardan iborat? #imzoni shakllantirish, imzoni tekshirish imzoni shakllantirish, imzo qo'yish va imzoni tekshirish imzoni shakllantirish va imzo qo'yish imzo qo'yish ++++ Ochiq kalitli kriptotizimlarda elektron hujjatlarga imzo qo'yish qaysi kalit orqali amalga oshiriladi? #shaxsiy kalit orqali ochiq kalit orqali imzo qo'yilishi kalitga bog'liq emas imzo qo'lda qo'yiladi ++++ Ochiq kalitli kriptotizimlarda elektron hujjatlarga qo'yilgan imzoni tekshirish qaysi kalit orqali amalga oshiriladi? #ochiq kalit orqali maxfiy kalit orqali imzo qo'yilishi kalitga bog'liq emas imzo qo'lda qo'yiladi ++++ Diskret logarifmlash murakkabligiga asoslangan algoritm keltirilgan qatorni ko'rsating? #Diffie-Hellman, EL-Gamal algoritmi RSA algoritmi EL-Gamal algoritmi Diffie-Hellman algoritmi ++++ Faktorlash murakkabligiga asoslangan algoritm keltirilgan qatorni ko'rsating? #RSA El-Gamal Diffie-Hellman DSA ++++ Karlmaykl sonlari qaysi tublikka tekshiruvchi algoritmlarda doim bajariladi? #Ferma testida Solovey-Shtrassen testida Eyler testida Rabbin testida ++++ Ochiq kalitli RSA shifrlash algoritmida maxfiy kalit qanday topiladi?  $e*d=1 \pmod{(p*q)}$  taqqoslamadan  $e*d=1 \pmod{N}$   $e*d=1 \pmod{(p-1)}$   $e*d=1 \pmod{((p-1)(q-1))}$  ++++ Ochiq kalitli RSA shifrlash algoritmida qaysi



parametrlar ochiq holda e'lon qilinadi? #N,e N,d d ++++ Ochiq kalitli RSA shifrlash algoritmidagi "e" ochiq kalit, "d" shaxsiy kalit bo'lsa deshifrlash formulasi to'g'ri ko'rsatilgan qatorni belgilang? # $M=C^d \pmod N$   $M=C^d \pmod N$   $M=C^e \pmod N$   $M=C^e \pmod N$  ++++ Ochiq kalitli RSA shifrlash algoritmidagi "d" shaxsiy kalit, "e" ochiq kalit bo'lsa shifrlash formulasi to'g'ri ko'rsatilgan qatorni belgilang? # $C=M^e \pmod N$   $C=M^e \pmod N$   $C=M^d \pmod N$   $C=M^d \pmod N$  ++++ Ochiq kalitli El-Gamal shifrlash algoritmidagi "p" tub son bo'lsa maxfiy kalit qanday tanlanadi? #(p-1) bilan o'zaro tub bo'lgan (1,p-1) intervaldagi butun son p bilan o'zaro tub bo'lgan (1,p) intervaldagi butun son (1,p-1) intervaldagi tub son (p-1) bilan o'zaro tub bo'lgan (1,p) intervaldagi butun son ++++ Ochiq kalitli El-Gamal shifrlash algoritmidagi ochiq kalit qanday hisoblanadi? # $y=g^a \pmod p$ , bu yerda g-birlamchi ildiz, a-maxfiy kalit, p-tub son  $y=g^a \pmod p$ , bu yerda g-soni (p-1) dan kichik butun son, a-maxfiy kalit, p-tub son  $y=g^a \pmod p$ , bu yerda g-soni p dan kichik butun son, a-maxfiy kalit, p-tub son  $y=g^a \pmod p$ , bu yerda g-soni (p-1) bilan o'zaro tub bo'lgan butun son, a-maxfiy kalit, p-tub son ++++ Ochiq kalitli kriptotizimlarga asoslangan kalitlarni taqsimlash Diffie-Hellman algoritmi ishlash prinsipi qanday? #umumiy maxfiy kalitni hosil qilishga asoslangan ochiq va yopiq kalitlar juftini hosil qilishga asoslangan maxfiy kalitni uzatishni talab etmaydigan prinsipga asoslangan ochiq kalitlarni hosil qilishga asoslangan ++++ "A" va "B" foydalanuvchilar ma'lumot almashmoqchi, "A" foydalanuvchi "B" tomondan qabul qilgan ma'lumotni imzosini tekshirishda qaysi kalitdan foydalanadi? # "B" foydalanuvchining ochiq kalitidan "B" foydalanuvchining maxfiy kalitidan "A" foydalanuvchi o'zining ochiq kalitidan "A" foydalanuvchini o'zining maxfiy kalitidan ++++ RSA algoritmidagi p=3, q=11, e=3 bo'lganda maxfiy kalitni qiymati topilsin:  $e \cdot d \equiv 1 \pmod N$ ? #7 6 8 5 ++++ Faktorlash muammosini bartaraf etuvchi usul keltirilgan qatorni ko'rsating? #Pollard usuli Xitoy teoremasi Pohlig-Hellman usuli RSA usuli ++++ Pollard usuli qanday turdagi matematik murakkablikni yechishda foydalaniladi? #faktorlash murakkabligini diskret logarifmlash murakkabligini elliptik egrzi chiziqda diskret logarifmlash murakkabligini elliptik egrzi chiziqda faktorlash murakkabligini ++++ RSA algoritmidagi matematik murakkablikni qanday usul orqali bartaraf qilish mumkin? #Pollard usuli Xitoy teoremasi Pohlig-Hellman usuli RSA usuli ++++ Diskret logarifmlash muammosini bartaraf etuvchi usul keltirilgan qatorni ko'rsating? #Pohlig-Hellman usuli Pollard usuli Xitoy teoremasi RSA usuli ++++ Pohlig-Hellman usuli qanday turdagi matematik murakkablikni yechishda foydalaniladi? #diskret logarifmlash murakkabligini faktorlash murakkabligini elliptik egrzi chiziqda faktorlash murakkabligini daraja parameter murakkabligini ++++ Evklidning kengaytirilgan algoritmidan RSA shifrlash algoritmining qaysi parametrini hisoblashda foydalaniladi? #maxfiy kalitni ochiq kalitni tub sonlarni modul qiymatini ++++ Diffie-Hellman algoritmidagi qaysi parametrlar ochiq holda e'lon qilinadi? #p va g tub sonlarni (p>g) p tub sonni p va g toq sonlarni (p>g) p va g juft sonlarni (p>g) ++++ Axborot xavfsizligining pasayishi nimani anglatadi? #axborot xavfsizligi ma'lumotlarning tartibsizligi ma'lumotlarning mas'uliyatsizligi ichki xavfsizlik +++++ Tashkilotning iqtisodiy xavfsizligini ta'minlash muammosining eng muhim tarkibiy qismlaridan biri bu #Axborot texnologiyalari (IT) va tizimlar (IS) xavfsizligi Axborot texnologiyalari (IT) xavfsizligi Axborot tizimlarining xavfsizligi (IS) Texnik tizimlarning xavfsizligi (TS) +++++ Axborot tizimlari va texnologiyalarini rivojlantirish, joriy qilish va ulardan foydalanishning ajralmas qismi hisoblanadi #Axborot xavfsizligi kriptografiya steganografiya autentifikatsiya +++++ Zamonaviy dasturlash texnologiyasi sizni mutlaqo xatosiz va xavfsiz dasturlarni yaratishga imkon beradimi? #emas Ha noma'lum savol noto'g'ri +++++ Huquqiy hujjatlar talablariga yoki ma'lumot egalari tomonidan o'rnatilgan talablarga muvofiq mulkka tegishli va himoya qilinishi kerak bo'lgan ma'lumotlar #himoyalangan ma'lumotlar maxfiy ma'lumotlar keraksiz ma'lumotlar foydali ma'lumotlar ++++

Axborot egalari bo'lishi mumkin: #davlat, yuridik shaxs, shaxslar guruhi, yakka shaxs. davlat xizmatchisi, yuridik shaxs, shaxslar guruhi, jismoniy shaxs. davlat, yuridik shaxs, shaxslar guruhi, alohida aktsiyadorlik jamiyati. davlat, yuridik shaxs, shaxslar guruhi, alohida kompaniya. +++++ Axborotni qayta ishlashning avtomatlashtirilgan tizimlari nima uchun kerak? #ma'lumotlarni saqlash, qayta ishlash va uzatish uchun ma'lumotlarni saqlash, yangilash va yashirish uchun ma'lumotlarni saqlash, qayta ishlash va shifrlash uchun ma'lumotlarni saqlash, qayta ishlash va tahlil qilish uchun +++++ Axborot xavfsizligini buzishning potentsial yoki real xavfini keltirib chiqaradigan shartlar va omillar to'plami #Tahdid (axborot xavfsizligi) Maxfiylikni buzish Hodisa Hujum +++++ Axborot xavfsizligiga tahdidning bevosita sababi bo'lgan sub'ekt (shaxs, moddiy ob'ekt yoki jismoniy hodisa) #Axborot xavfsizligiga tahdid manbai Texnik xavfsizlik manbai Virus hujumining manbasi Xodimlarning manbasi +++++ Axborot tizimining xususiyati, unda ishlov beriladigan axborotga tahdidlarni amalga oshirishga imkon beradi #Zaiflik (axborot tizimi) Xaker hujumi Hodisa Qayta rasmiylashtirish +++++ Yashirin yoki mahfiy axborotni amalga oshirish natijasida shaxs, shaxslar guruhi yoki u mo'ljallanmagan har qanday tashkilot uchun foydalanish mumkin bo'lgan tahdid #Maxfiylikka tahdid (oshkor qilish tahdidi) Butunlik uchun tahdid Texnik tahdid Xaker hujumi +++++ Amalga oshirilishi natijasida ma'lumotlar o'zgartirilishi yoki yo'q qilinishi mumkin bo'lgan tahdid #Butunlik uchun tahdid Virusli hujum xavfi Tarmoq tahdidi Texnik tahdid +++++ Tashkilotni o'z faoliyatida yo'naltiradigan hujjatlashtirilgan qoidalar, protseduralar, amaliyotlar yoki axborot xavfsizligi sohasidagi ko'rsatmalar to'plami #Xavfsizlik siyosati Davlat siyosati Korporativ etika Ko'rsatmalar +++++ Amalga oshirilishi avtomatlashtirilgan tizim mijozlariga xizmat ko'rsatishni rad etishga, tajovuzkorlarning o'z xohishlariga ko'ra manbalardan ruxsatsiz foydalanishiga olib keladigan tahdid hisoblanadi. #Xizmat tahdidini rad etish (mavjud tahdid) Texnik muammo Tizimning favqulodda to'xtashi Hujum +++++ Uning maxfiyligi, ochiqqligi va yaxlitligi ta'minlanadigan axborot xavfsizligi holati #Axborot xavfsizligi Ma'lumot xavfsizligi Operatsion tizim xavfsizligi Shaxsiy ma'lumotlar xavfsizligi +++++ Axborotni himoya qilish usuli #axborotni himoya qilishning muayyan printsiplari va vositalarini qo'llash tartibi va qoidalari. axborotni texnik himoya qilishning muayyan printsiplari va vositalarini qo'llash tartibi va qoidalari. ma'lum bir algoritmlar va axborot xavfsizligi vositalarini qo'llash tartibi va qoidalari. axborotni himoya qilishning ayrim algoritmlarini qo'llash tartibi va qoidalari. +++++ Apparat, dasturiy ta'minot, dasturiy ta'minot va apparat, axborotni himoya qilish uchun mo'ljallangan yoki ishlatiladigan materiallar va (yoki) materiallar #Axborot xavfsizligi vositasi Axborotni nusxalash vositasi Axborot uzatish vositasi Shaxsiy ma'lumotlarni uzatish vositasi +++++ Axborotni kriptografik o'zgartirish orqali himoya qilish #kriptografik ma'lumotlarni himoya qilish antivirus ma'lumotlarini himoya qilish ma'lumotlarni steganografik himoya qilish axborotni texnik himoya qilish +++++ Ruxsat berilgan shaxslarning kirib borishi yoki kirishiga to'sqinlik qiladigan vositalar to'plami va tashkiliy choralar yordamida axborotni himoya qilish himoya qilinadigan obyekt hisoblanadi. #axborotni jismoniy himoya qilish axborotni dasturiy himoyasi antivirus ma'lumotlarini himoya qilish oddiy ma'lumotlarni himoya qilish +++++ Muayyan tarmoq tugunini o'chirishga qaratilgan hujum turi (Xizmatni rad etish - DoS) #xizmatdan bosh tortish "ma'lumotlarga kirishni rad etish" "ma'lumotlarga kirishni rad etish" "parolga kirish taqiqlandi" +++++ Kriptoalyutatsiya atamasini birinchi bo'lib kiritgan olimni ko'rsating #F. Fridman Aristotel Shannon Aliqushchi +++++ IV asrda "antiscital" dekifrlash qurilmasini kim yaratgan. Mil. Avv. #Aristotel Sokrat Ptolemey Spital +++++ Qaysi olimning kitobida chastota kriptoalyutasi to'g'risida birinchi ma'lum eslatma mavjud? #Al-Kindi Aristotel Umar Xayyom Mirzo Ulug'bek +++++ Qur'on matni asosida arab tilidagi harflarning chastota jadvalini birinchi bo'lib kim aniqlagan? #Shihab al-

Kalkasandi Umar Xayyom Mirzo Ulug'bek Imom Buxoriy +++++ Axborotni shifrlash va shifrlash usullarini qaysi fan rivojlantirmoqda? #Kriptologiya Informatika Matematika Fizika +++++ DES shifrlash algoritmi qaysi tarmoqqa asoslangan holda ishlaydi? #Feystel tarmog'iga asoslangan holda SPN tarmog'iga asoslangan holda hech qanday tarmoqqa asoslanmaydi Lai-Massey tarmog'iga asoslangan holda +++++ Quyida keltirilgan xususiyatlarning qaysilari xesh funksiyaga mos? #chiqishda fiksirlangan uzunlikdagi qiymatni beradi chiqishda bir xil qiymatni beradi kolliziyaga ega chiqishdagi qiymat bilan kiruvchi qiymatlar bir xil bo'ladi +++++ Quyida keltirilgan xususiyatlarning qaysilari xesh funksiyaga mos? #ixtiyoriy olingan har xil matn uchun xesh qiymatlar bir xil bo'lmaydi ixtiyoriy olingan bir xil matn uchun qiymatlar bir xil bo'lmaydi ixtiyoriy olingan har xil matn uchun xesh qiymatlar bir xil bo'ladi ixtiyoriy olingan har xil xesh qiymat uchun dastlabki ma'lumotlar bir xil bo'ladi +++++ DES shifrlash algoritmda har bir raunda necha bitli raund kalitlaridan foydalaniladi? #48 56 64 32 +++++ Qaysi hujum turida barcha bo'lishi mumkin bo'lgan variantlar ko'rib chiqiladi? #qo'pol kuch hujumi sotsial injineriya analitik hujum chastotalar tahlili +++++ Ma'lumotlarni autentifikatsiyalash kodlari deb qanday xesh funksiyalarga aytiladi? #kalitli xesh funksiyalarga kalitsiz xesh funksiyalarga kriptografik bo'lmagan xesh funksiyalarga kriptografik xesh funksiyalarga +++++ AES algoritmda raundlar soni nimaga bo'g'liq? #kalit uzunligiga kiruvchi blok uzunligiga foydalanilgan vaqtiga kiruvchi blok uzunligi va matn qiymatiga +++++ A5/1 oqimli shifrlash algoritmda registrning surilishi qanday kattalikka bog'liq? #maj funksiyasi qiymatiga kalit qiymatiga registr uzunligi qiymatiga hech qanday kattalikka bog'liq emas +++++ 16 raund davom etadigan blokli shifrlash algoritmi ko'rsating? #DES AES RC4 A5/1 +++++ 10 raund davom etadigan blokli shifrlash algoritmi ko'rsating? #AES DES RC4 A5/1 +++++ Xesh qiymatlarni yana qanday atash mumkin? #dayjest funksiya imzo raqamli imzo +++++ Ximoyalanuvchi ma'lumot boshqa bir ma'lumotni ichiga yashirish orqali maxfiyligini ta'minlaydigan usul qaysi? #steganografiya kodlash shifrlash autentifikatsiya +++++ Baytlar kesimida shifrlashni amalga oshiradigan algoritm keltirilgan qatorni ko'rsating? #RC4 A5/1 MD5 SHA1 +++++ Kolliziya deb nima nisbatan aytiladi? #ikkita har xil matn uchun bir xil xesh qiymat mos kelishi ikkita bir xil matn uchun bir xil xesh qiymat mos kelishi ikkita har xil matn uchun har xil xesh qiymat mos kelishi ikkita bir xil matn uchun bir xil xesh qiymat mos kelmasligiga +++++ Konfidensiallikni ta'minlash bu -? #ruxsat etilmagan "o'qishdan" himoyalash ruxsat etilmagan "yozishdan" himoyalash ruxsat etilmagan "bajarishdan" himoyalash ruxsat berilgan "amallarni" bajarish +++++ Sezar shifrlash algoritmi qaysi turdagi akslantirishga asoslangan? #o'rniga qo'yish o'rin almashtirish aralash kompozitsion +++++ CRC-3 tizimida CRC qiymatini hisoblash jarayonida ma'lumotga nechta nol biriktiriladi? #3 6 12 9 +++++ .... kriptotizimni shifrlash va rasshifrovkalash uchun sozlashda foydalaniladi. #kalit ochiq matn algoritm alifbo +++++ CRC-5 tizimida CRC qiymati hisoblash jarayonida ma'lumotga nechta nol biriktiriladi? #5 10 15 20 +++++ Rasshifrovkalash jarayonida kalit va ..... kerak bo'ladi #shifrmtn ochiq matn kodlash alifbo +++++ Kriptologiya qanday yo'nalishlarga bo'linadi? #kriptografiya va kriptotahlil kripto va kriptotahlil kriptografiya va kriptotizim kriptoanaliz va kriptotizim +++++ Kriptotizimlar kalitlar soni bo'yicha nechta turga bo'linadi? #2 6 4 8 +++++ Kriptografiya nima bilan shug'ullanadi? #maxfiy kodlarni yaratish bilan maxfiy kodlar orqali ma'lumotlarni yashirish bilan maxfiy kodlarni buzish bilan shifrlash uslublarini bilmagan holda shifrlangan ma'lumotni asl holatini topish bilan +++++ Kerkxofs printsipi nimadan iborat? #kriptografik tizim faqat kalit noma'lum bo'lgan taqdirdagina maxfiylik ta'minlanadi kriptografik tizim faqat yopiq bo'lgan taqdirdagina maxfiylik ta'minlanadi kriptografik tizim faqat ikkita kalit ma'lum bo'lgan taqdirdagina maxfiylik ta'minlanadi kriptografik tizim faqat kalit ochiq bo'lgan taqdirdagina maxfiylik ta'minlanadi +++++ Shifrlash orqali ma'lumotning qaysi xususiyati

ta'minlanadi? #maxfiyligi ishonchliligi butunliligi foydalanuvchanligi +++++ O'rniga qo'yish shifrlash sinfiga qanday algoritmlar kiradi? #shifrlash jarayonida ochiq ma'lumot alfaviti belgilari shifr ma'lumot belgilariga almashtiriladigan algoritmlar shifrlash jarayonida ochiq ma'lumot alfaviti belgilarining o'rinlar almashtiriladigan algoritmlar shifrlash jarayonida kalitlarning o'ri almashtiriladigan algoritmlarga shifrlash jarayonida o'rniga qo'yish va o'rin almashtirish akslantirishlarning kombinatsiyalaridan birgalikda foydalaniladigan algoritmlar +++++ Kriptologiya necha yo'nalishga bo'linadi? #2 4 8 6 +++++ Kriptologiya so'zining ma'nosi? #cryptos – maxfiy, logos – ilm cryptos – maxfiy, logos – kalit cryptos – kripto, logos – yashiraman cryptos – kodlash, logos – ilm +++++ O'rniga qo'yish shifrlash algoritmlari necha sinfga bo'linadi? #2 6 4 8 +++++ O'rniga qo'yish shifrlash algoritmlari qanday sinfga bo'linadi? #bir qiymatli va ko'p qiymatli shifrlash bir qiymatli shifrlash ko'p qiymatli shifrlash uzluksiz qiymatli shifrlash +++++ Kriptologiya nima bilan shug'ullanadi? #maxfiy kodlarni yaratish va buzish ilmi bilan maxfiy kodlarni yaratish bilan maxfiy kodlarni buzish bilan maxfiy kodlar orqali ma'lumotlarni yashirish bilan +++++ Ma'lumotlarni kodlash va dekodlashda necha kalitdan foydalanadi? #kalit ishlatilmaydi 3 ta 2 ta 4 ta +++++ Simmetrik kriptotizimlarda necha kalitdan foydalaniladi? #1 ta 3 ta kalit ishlatilmaydi 4 ta +++++ Kriptotahlil nima bilan shug'ullanadi? #maxfiy kodlarni buzish bilan shifrlash uslublarini bilmagan holda shifrlangan ma'lumotni asl holatini topish bilan maxfiy kodlar orqali ma'lumotlarni yashirish bilan maxfiy kodlarni yaratish bilan shifrlash uslublarini bilmagan holda shifrlangan ma'lumotni asl holatini topish bilan +++++ A5/1 oqimli shifrlash algoritmida dastlabki kalit uzunligi nechi bitga teng? #64 192 512 256 +++++ Steganografiya ma'lumotni qanday maxfiylashtiradi? #maxfiy xabarni soxta xabar ichiga berkitish orqali maxfiy xabarni kriptografik kalit yordamida shifrlash orqali maxfiy xabarni kodlash orqali maxfiy xabarni shifrlash orqali +++++ Shifrlash algoritmlari akslantirish turlariga qarab qanday turlarga bo'linad? #o'rniga qo'yish, o'rin almashtirish va kompozitsion akslantirishlarga o'rniga qo'yish, o'rin almashtirish va surish akslantirishlariga o'rniga qo'yish va o'rin almashtirish akslantirishlariga o'rniga qo'yish, sirush va kompozitsion shifrlash akslantirishlariga +++++ Blokli shifrlash algoritmlari arxitekturasini jihatidan qanday tarmoqlarga bo'linadi? #Feystel va SP Feystel va Petri SP va Petri Kvadrat va iyerarxik +++++ Zamonaviy kriptografiya qaysi bo'limlarni o'z ichiga oladi? #simmetrik kriptotizimlar, ochiq kalitli kriptotizimlar, elektron raqamli imzo kriptotizimlari, kriptobardoshli kalitlarni ishlab chiqish va boshqarish simmetrik kriptotizimlar, ochiq kalit algoritmiga asoslangan kriptotizimlar, elektron raqamli imzo kriptotizimlari, foydalanuvchilarni ro'yxatga olish simmetrik kriptotizimlar, ochiq kalit algoritmiga asoslangan kriptotizimlar, elektron raqamli imzo kriptotizimlari, foydalanuvchilarni identifikatsiya qilish simmetrik kriptotizimlar, ochiq kalit algoritmiga asoslangan kriptotizimlar, elektron raqamli imzo kriptotizimlari, foydalanuvchilarni autentifikatsiyalash +++++ ARX amali nimalardan iborat? #add, rotate, xor add, rotate, mod add, mod, xor mod, rotate, xor +++++ Tasodifiy ketma-ketliklarni generatsiyalashga asoslangan shifrlash turi bu? #oqimli shifrlar blokli shifrlar ochiq kalitli shifrlar assimetrik shifrlar +++++ Qanday algoritmlarda chiqishda doim fiksirlangan uzunlikdagi qiymat chiqadi? #xesh algoritmlarda kodlash algoritmlarida shifrlash algoritmlarida steganografik algoritmlarda +++++ Ma'lumotni shifrlash va deshifrlash uchun bir xil kalitdan foydalanuvchi tizim bu? #simmetrik kriptotizim ochiq kalitli kriptotizim assimetrik kriptotizim xesh funksiyalar +++++ Ikki kalitli deyilganda qaysi kriptotizim nazarda tutiladi? #ochiq kalitli kriptotizim simmetrik kriptotizim xesh funksiyalar MAC tizimlari +++++ Simmetrik shifrlash algoritmlarida qanday muammo mavjud? #kalitni uzatish kalit generatsiyalash kalitni yo'q qilish muammo yo'q +++++ Sezar shifrlash usuli qaysi akslantirishga asoslangan? #o'rniga qo'yish o'rin almashtirish ochiq kalitli shifrlarga kombinatsion akslantirishga +++++ Ma'lumotni uzatishda

kriptografik himoya ..... #konfidensiallik va yaxlitlikni ta'minlaydi konfidensiallik va foydalanuvchanlikni ta'minlaydi konfidensiallikni ta'minlaydi foydalanuvchanlik ta'minlaydi va butunlikni +++++ Butunlikni ta'minlash bu - ? #ruxsat etilmagan "yozishdan" himoyalash ruxsat etilmagan "bajarishdan" himoyalash ruxsat etilmagan "o'qishdan" himoyalash ruxsat berilgan "amallarni" bajarish +++++ Shifrlash va deshifrlashda alohida kalitlardan foydalanuvchi kriptotizimlar bu? #ochiq kalitli kriptotizimlar simmetrik kriptotizimlar bir kalitli kriptotizimlar xesh funksiyalar +++++ Agar ochiq ma'lumot shifrlansa, natijasi .... bo'ladi. #shifrmtn ochiq matn noma'lum kod +++++ Ochiq kalitli shifrlar axborotni qaysi xususiyatlarini ta'minlashda foydalaniladi? #konfidensiallik va yaxlitlik konfidensiallik va foydalanuvchanlik foydalanuvchanlik va yaxlitlik foydalanuvchanlik +++++ MD5 xesh funksiyasida kiruvchi ma'lumot uzunligi qanday bitli bloklarga bo'linadi? #512 1024 2048 4096 +++++ add amalining ma'nosi nima? #modul asosida qo'shish XOR amali surish (siklik surish, mantiqiy surish) akslantirish +++++ SHA1 xesh funksiyasida initsializatsiya bosqichida 5 ta necha bitli registrlardan foydalanadi? #32 64 128 256 +++++ O'zbekistonda kriptografiya sohasida faoliyat yurituvchi tashkilot nomini ko'rsating? #“UNICON.UZ” DUK “O'zstandart” agentligi Kadastr agentligi Davlat Soliq Qo'mitasi +++++ Faqat simmetrik shifrlash algoritmlari nomi keltirilgan qatorni ko'rsating? #AES, A5/1 SHA1, DES MD5, AES HMAC, RC4 +++++ HMAC tizimida kalit qiymati blok uzunligiga teng bo'lganda ma'lumotga qanday biriktiriladi? #kalit qiymati o'zgartirilmagan holda ma'lumotga biriktiriladi kalit qiymati blok uzunligiga teng bo'lguncha nol qiymat bilan to'ldirilib hosil bo'lgan qiymat ma'lumotga biriktiriladi kalitni xesh qiymati hisoblanib, unga blok uzunligiga teng bo'lguncha nol qiymat qo'shiladi va yangi hosil bo'lgan qiymat ma'lumotga biriktiriladi xesh funksiyalarda kalit qiymatida foydalanilmaydi +++++ DES shifrlash algoritmda rasshifrovkalashda birinchi raunda qaysi kalitdan foydalaniladi? #16-raund kalitidan 1-raund kalitidan 1-raunda kalitdan foydalanilmaydi dastlabki kalitdan +++++ SHA1 xesh funksiyasida kiruvchi ma'lumot uzunligi qanday bitli bloklarga bo'linadi? #512 1024 2048 4096 +++++ AES shifrlash algoritmda blok uzunligi 128, kalit uzunligi 192 bit bo'lsa raundlar soni nechta bo'ladi? #12 10 14 6 +++++ AES shifrlash algoritmda nechta akslantirishdan foydalanadi? #4 3 2 akslantirishdan foydalanilmaydi +++++ GSM tarmog'ida foydalaniluvchi shifrlash algoritmi nomini ko'rsating? #A5/1 dastlabki kalitdan AES DES +++++ WEP protokolida (Wi-Fi tarmog'ida) foydalaniluvchi shifrlash algoritmi nomini ko'rsating? #RC4 DES SHA1 A5/1 +++++ rotate amalining ma'nosi nima? #surish (siklik surish, mantiqiy surish) modul asosida qo'shish XOR amali Akslantirish +++++ SHA1 xesh funksiyasida to'ldirish bitlarini qo'shishda ma'lumot uzunligi 512 modul bo'yicha qanday son bilan taqqoslanadigan qilib to'ldiriladi? #448 1002 988 772 +++++ HMAC tizimida kalit qiymati blok uzunligidan kichik bo'lganda ma'lumotga qanday biriktiriladi? #kalit qiymati blok uzunligiga teng bo'lguncha nol qiymat bilan to'ldirilib hosil bo'lgan qiymat ma'lumotga biriktiriladi kalitni xesh qiymati hisoblanib, unga blok uzunligiga teng bo'lguncha nol qiymat qo'shiladi va yangi hosil bo'lgan qiymat ma'lumotga biriktiriladi kalit qiymati o'zgartirilmagan holda ma'lumotga biriktiriladi xesh funksiyalarda kalit qiymatida foydalanilmaydi +++++ Kolliziya hodisasi qaysi turdagi algoritmlarga xos? #xesh funksiyalar ochiq kalitli shifrlash algoritmlari kalitlarni boshqarish tizimlari simmetrik shifrlash algoritmlari +++++ AES shifrlash algoritmda shifrlash jarayonida qanday akslantirishdan foydalaniladi? #SubBytes, ShiftRows, MixColumns va AddRoundKey SubBytes, ShiftRows va AddRoundKey SubBytes, MixColumns va AddRoundKey MixColumns, ShiftRows, SubBytes +++++ Faqat blokli simmetrik shifrlash algoritmlari nomi keltirilgan qatorni ko'rsating? #AES, DES A5/1, RC4 A5/1, MD5 SHA1, RC4 +++++ Vernam shifrlash algoritmda shifr matn C=101 ga, kalit K=111 ga teng bo'lsa shifr matn qiymati qanday bo'ladi? #010 101 111 110

+++++ Quyidagi ifoda nechta yechimga ega?  $3^x \equiv 2 \pmod{7}$ . #bitta yechimga ega ikkita yechimga ega yechimga ega emas uchta yechimga ega +++++  $143 \pmod{17}$  nechiga teng? #7 6 5 8 +++++ Blokli shifrlash rejimlari qaysi algoritmlarda qo'llaniladi? #AES, DES Sezar, Affin MD5, SHA1 A5/1, RC4 +++++ MD5 xesh algoritmda nechta 32 bitli statik qiymatdan foydalanadi? #4 8 12 16 +++++ Sezar shifrlash algoritmda ochiq matn M=3 ga, kalit K=7 ga teng hamda p=26 ga teng bo'sa shifr matn qiymati neciga teng bo'ladi? #10 16 18 22 +++++ Qaysi xesh algoritmda 64 raund amal bajariladi? #MD5 MAC CRC SHA1 +++++ DES shifrlash standarti qaysi davlat standarti? #AQSH Rossiya Buyuk Britaniya Germaniya +++++ Qaysi blokli shifrlash algoritmda raund kalit uzunligi qiymatiga bo'g'liq? #AES IDEA DES RSA +++++ A5/1 oqimli shifrlash algoritmda  $x_{18}=1$ ,  $y_{21}=0$ ,  $z_{22}=1$  ga teng bo'lsa kalitni qiymatini toping #0 1 2 3 +++++ Kolliziya hodisasi deb nimaga aytiladi? #ikki xil matn uchun bir xil xesh qiymat chiqishi ikki xil matn uchun ikki xil xesh qiymat chiqishi bir xil matn uchun ikki xil xesh qiymat chiqishi bir xil matn uchun bir xil xesh qiymat chiqishi bir xil matn uchun bir xil xesh qiymat chiqishi +++++ 3 sonini 5 chekli maydonda teskarisini toping? #2 3 4 5 +++++ Bir qiymatli shifrlash qanday amalga oshiriladi? #ochiq ma'lumot alfaviti belgilarining har biriga shifr ma'lumot alfavitining bitta belgisi mos qo'yiladi ochiq ma'lumot alfaviti belgilarining har biriga shifr ma'lumot alfavitining ikkita yoki undan ortiq chekli sondagi belgilari mos qo'yiladi ochiq ma'lumot alfaviti belgilarining har ikkitasiga shifr ma'lumot alfavitining ikkita yoki undan ortiq chekli sondagi belgilari mos qo'yiladi ochiq ma'lumot alfaviti belgilarining har juftiga shifr ma'lumot alfavitining bitta belgisi mos qo'yiladi +++++ DES shifrlash algoritmda raundlar soni nechta? #16 64 32 128 +++++ DES shifrlash algoritmda kalit uzunligi necha bitga teng? #56 256 192 512 +++++ RC4 oqimli shifrlash algoritmi asosan qayerda qo'llaniladi? #simsiz aloqa vositalaridagi mavjud WEP protokolida radioaloqa tarmoqlarda inernet trafiklarini shifrlashda mobil aloqa standarti GSM protokolida +++++ Xesh funksiyalarga qanday turlarga bo'linadi? #kalitli va kalitsiz xesh funksiyalarga kalitli va kriptografik bo'lmagan xesh funksiyalarga kalitsiz va kriptografik bo'lmagan xesh funksiyalarga kriptografik va kriptografik bo'lmagan xesh funksiyalarga +++++ AES shifrlash algoritmda raundlar soni nechaga teng bo'ladi? #10, 12, 14 14, 16, 18 18, 20, 22 22, 24, 26 +++++ A5/1 oqimli shifrlash algoritmda har bir qadamda kalit oqimining qanday qiymatini hosil qiladi? #bir biti bir bayti 64 biti 8 bayti +++++ CRC-4 tizimida CRC qiymatini hisoblash jarayonida ma'lumotga nechta nol biriktiriladi? #4 8 16 12 +++++ Blokli simmetrik shifrlash algoritmlari raund funksiyalarida qanday amallar bajariladi? #ARX PRX XOR RPT +++++ CRC-6 tizimida CRC qiymati hisoblash jarayonida ma'lumotga nechta nol biriktiriladi? #6 12 18 24 +++++ Qaysi maxfiylikni ta'minlash usulida kalitdan foydalanilmaydi? #kodlash shifrlash autentifikatsiya steganografiya +++++ Vernam shifrlash algoritm asosi qaysi mantiqiy hisoblashga asoslangan #XOR ARX ROX XRA +++++ Chastotalar tahlili kriptotahlil usuli samarali ishlidigan algorimtlar keltirilgan qatorni belgilang? #Sezar, Affin Vernam Vijiner RC4 +++++ Bitlar kesimida shifrlashni amalga oshiradigan algoritm keltirilgan qatorni ko'rsating? #A5/1 SHA1 RC4 MD5 +++++ Ma'lumotni konfidensialligini ta'minlash uchun ..... zarur. #shifrlash kodlash rasshifrovkalash deshifrlash +++++ Foydalanuvchanlikni ta'minlash bu-? #ruxsat etilmagan "bajarishdan" himoyalash ruxsat etilmagan "yozishdan" himoyalash ruxsat etilmagan "o'qishdan" himoyalash ruxsat berilgan "amallarni" bajarish +++++ Vijiner shifrlash algoritmi qaysi turdagi akslantirishga asoslanadi? #o'rniga qo'yish o'rin almashtirish kompozitsion aralash +++++ Kompyuter davriga tegishli shifrlarni aniqlang? #DES, AES shifri kodlar kitobi Sezar Enigma shifri +++++ .... shifrlar blokli va oqimli turlarga ajratiladi #simmetrik ochiq kalitli klassik assimetrik +++++ DES shifrlash algoritmi bu? #blokli shifrlash algoritmi oqimli shifrlash algoritmi ochiq kalitli shifrlash algoritmi asimetrik shifrlash algoritmi +++++ Ma'lumotga elektron raqamli imzo qo'yish hamda uni

tekshirish qanday amalga oshiriladi? #Ma'umotga raqamli imzo qo'yish maxfiy kalit orqali, imzoni tekshirish ochiq kalit orqali amalga oshiriladi Ma'lumotga raqamli imzo qo'yish ochiq kalit orqali, imzoni tekshirish maxfiy kalit orqali amalga oshiriladi Ma'lumotga raqamli imzo qo'yish maxfiy kalit orqali, imzoni tekshirish yopiq kalit orqali amalga oshiriladi Ma'lumotga raqamli imzo qo'yish hamda uni tekshirish maxfiy kalit orqali amalga oshiriladi +++++ A5/1 oqimli shifrlash algoritmda Z registr uzunligi nechki bitga teng? #23 18 19 20 +++++ Kerkxofs printsipi bo'yicha qanday taxminlar ilgari suriladi? #Kalitdan boshqa barcha ma'lumotlar barchaga ma'lum Faqat kalit barchaga ma'lum Barcha parametrlar barchaga ma'lum Shifrlash kaliti barchaga ma'lum +++++ Qaysi algoritm har bir qadamda bir bayt qiymatni shifrlaydi? #RC4 A5/1 RSA AES +++++ A5/1 oqimli shifrlash algoritmda maxfiy kalit necha registrga bo'linadi? #3 6 5 4 +++++ AES algoritmi qaysi tarmoq asosida qurilgan? #SP Feystel Petri va SP Petri +++++ Elektron raqamli imzo bo'yicha birinchi O'z DSt 1092 qaysi korxona tomonidan ishlab chiqilgan? #UNICON.UZ INFOCOM UZTELECOM O'zR axborot texnologiyalari va kommunikatsiyalarini rivojlantirish vazirligi +++++ AES shifrlash algoritmi nomini kengaytmasini ko'rsating? #Advanced Encryption Standard Advanced Encoding Standard Advanced Encryption Stadium Always Encryption Standard +++++ A5/1 shifrlash algoritmi bu? #oqimli shifrlash algoritmi blokli shifrlash algoritmi assimetrik shifrlash algoritmi ochiq kalitli shifrlash algoritmi +++++ RC4 shifrlash algoritmi qaysi turga mansub? #oqimli shifrlar blokli shifrlar ochiq kalitli shifrlar assimetrik shifrlar +++++ Xeshlash algoritmlarini ko'rsating? #SHA1, MD5, O'z DSt 1106 RSA, DSA, El-gamal DES, AES, Blovfish O'z DSt 1105, FOCT 28147-89, FEAL +++++ AES shifrlash algoritmi bu? #blokli shifrlash algoritmi oqimli shifrlash algoritmi ochiq kalitli shifrlash algoritmi asimmetrik shifrlash algoritmi +++++ ARX amali qaysi shifrlash algoritmlarida foydalaniladi? #Blokli shifrlashda Ikki kalitli shifrlashda Assimetrik shifrlashda Ochiq kalitli shifrlashda +++++ Kriptotizimlar kalitlar soni bo'yicha nechta turga bo'linadi? #2 3 4 5 +++++ A5/1 oqimli shifrlash algoritmda major qiymati hisoblash jarayonida, uchinchi (Z) registrning qaysi qiymati olinadi? #z10 z11 z12 z13 +++++ A5/1 oqimli shifrlash algoritmda X registr uzunligi nechki bitga teng? #19 16 17 15 +++++ Qaysi algorimtda har bir qadamda bir bit qiymatni shifrlaydi? #A5/1 RC4 RSA AES +++++ Mantiqiy XOR amalining asosi qanday hisoblashga asoslangan? #mod2 bo'yicha qo'shishga mod2 bo'yicha ko'paytirishga mod2 bo'yicha darajaga ko'tarishga mod2 bo'yicha bo'lishga +++++ Qaysi xesh algoritmda xesh qiymat 128 bitga teng bo'ladi? #MD5 SHA1 CRC MAC +++++ Qaysi xesh algoritmda xesh qiymat 160 bitga teng bo'ladi? #SHA1 MD5 CRC MAC +++++ Faqat AQSH davlatiga tegishli kriptografik standartlar nomini ko'rsating? #AES, DES AES, FOCT 28147-89 DES, O'z DST 1105-2009 SHA1, FOCT 3412-94 +++++ RC4 shifrlash algoritmi simmetrik turga mansub bo'lsa, unda nechta kalitdan foydalaniladi? #1 2 3 4 +++++ A5/1 oqimli shifrlash algoritmda major qiymati hisoblash jarayonida, birinchi (X) registrning qaysi qiymati olinadi? #x8 x9 x10 x11 +++++ DES shifrlash algoritmda S-bloklarga kiruvchi qiymatlar uzunligi nechki bitga teng bo'ladi? #6 12 24 18 +++++ MD5 xesh funksiyasida initsializatsiya bosqichida 4 ta nechki bitli registrlardan foydalaniladi? #32 64 128 256 +++++ Imitatsiya turidagi hujumlarda ma'lumotlar qanday o'zgaradi? #ma'lumot qalbakilashtiriladi ma'lumot yo'q qilinadi ma'lumot ko'chirib olinadi ma'lumot dublikat qilinadi +++++ Sesar shifrlash algoritmda rasshifrovkalash formulasi qanday?  $M=(C-K) \bmod p$   $M=(C+K) \bmod p$   $M=(C*K) \bmod p$   $M=(C/K) \bmod p$  +++++ Faqat xesh funksiyalar nomi keltirilgan qatorni ko'rsating? #SHA1, MD5 SHA1, DES MD5, AES HMAC, A5/1 +++++ MD5 xesh funksiyasida chiquvchi qiymat uzunligi nechki bitga teng? #128 Ixtiyoriy 510 65 +++++ AES shifrlash algoritmi simmetrik turga mansub bo'lsa, unda nechta kalitdan foydalaniladi? #1 2 3 4 +++++ SHA1 xesh funksiyasida initsializatsiya bosqichida nechki bitga teng? #5 10 15 20 +++++ MD5 xesh funksiyasida amallar

necha raund davomida bajariladi? #64 128 512 256 +++++ DES shifrlash algoritmda S-bloklardan chiqqan qiymatlar uzunligi necha bitga teng bo'ladi? #4 8 12 16 +++++ MD5 xesh funksiyasida initsializatsiya bosqichida nechta 32 bitli registrdan foydalanadi? #4 8 12 16 +++++ Faqat oqimli simmetrik shifrlash algoritmlari nomi keltirilgan qatorni ko'rsating? #A5/1, RC4 AES, DES SHA1, RC4 A5/1, MD5 +++++ SHA1 xesh funksiyasida chiquvchi qiymat uzunligi nechaga teng? #160 Ixtiyoriy 512 256 +++++ O'zgartirish turidagi hujumlarda ma'lumotlar qanday o'zgaradi? #modifikatsiya qilinadi ma'lumot yo'q qilinadi ma'lumot dublikat qilinadi ma'lumot ko'chirib olinadi +++++ AES standarti qaysi algoritm asoslangan? #Rijndael RC6 Twofish Serpent +++++ SHA1 xesh funksiyasida amallar nechi raund davomida bajariladi? #80 128 256 512 +++++ 2 lik sanoq tizimida 0101 soniga 1111 sonini 2 modul bo'yicha qo'shing? #1010 0101 1001 1111 +++++ AES shifrlash standarti qaysi davlat standarti? #AQSH Rossiya Buyuk Britaniya Germaniya +++++ Qaysi algoritmda maj kattaligi ishlatiladi? #A5/1 RC4 SHA1 MD5 +++++ Qalbakilashtirish hujumi qaysi turdagi hujum turiga kiradi? #Immitatsiya o'zgartirish Fabrication modification +++++ SHA1 xesh funksiyasi qaysi davlat standarti? #AQSH Rossiya Germaniya Buyuk Britaniya +++++ Qayday akslantirishdan foydalanilsa chastotalar tahlili kriptotahlil usuliga bardoshli bo'ladi #bigram akslantirishidan o'rniga qo'yish akslantirishidan o'rin almashtirish akslantirishidan xech qanday akslantirishdan foydalanish shart emas +++++ SHA1 xesh algoritmda nechta 32 bitli statik qiymatdan foydalanadi? #5 10 15 20 +++++ A5/1 oqimli shifrlash algoritmda maj(1,0,1) ga teng bo'lsa maj kattalik qiymatini toping? #1 0 2 3 +++++ SHA1 xesh funksiyada 102 bitli ma'lumot berilganda to'ldirish bitlari qanday to'ldiriladi? #bir bit 1, 345 ta 0, ma'lumot uzunligi qiymatining 64 bitli qiymati bilan bir bit 1, 345 ta 0, ma'lumot uzunligining dastlabki 64 bitli qiymati bilan bir bit 1, 409 ta 0, ma'lumot uzunligi qiymatining 64 bitli qiymati bilan bir bit 1, 409 ta 0, ma'lumot uzunligining dastlabki 64 bitli qiymati bilan +++++ Qaysi blokli shifrlash algoritmda 8 ta statik S-box lardan foydalaniladi? #DES RSA RC4 A5/1 +++++ Kriptotizimlar kalitlar soni bo'yicha qanday turga bo'linadi? #simmetrik va assimetrik turlarga assimetrik va 2 kalitli turlarga 3 kalitli turlarga simmetrik va bir kalitli turlarga +++++ Ko'p qiymatli shifrlash qanday amalga oshiriladi? #ochiq ma'lumot alfaviti belgilarining har biriga shifr ma'lumot alfavitining ikkita yoki undan ortiq chekli sondagi belgilari mos qo'yiladi ochiq ma'lumot alfaviti belgilarining har ikkitasiga shifr ma'lumot alfavitining ikkita yoki undan ortiq chekli sondagi belgilari mos qo'yiladi ochiq ma'lumot alfaviti belgilarining har biriga shifr ma'lumot alfavitining bitta belgisi mos qo'yiladi ochiq ma'lumot alfaviti belgilarining har juftiga shifr ma'lumot alfavitining bitta belgisi mos qo'yiladi +++++ A5/1 oqimli shifrlash algoritmi asosan qayerda qo'llaniladi? #mobil aloqa standarti GSM protokolida simsiz aloqa vositalaridagi mavjud WEP protokolida internet trafiklarini shifrlashda radioaloqa tarmoqlarida +++++ Assimetrik kriptotizimlarda necha kalitdan foydalaniladi? #2 ta 3 ta 4 ta kalit ishlatilmaydi +++++ AES algoritmda shifrlash kalitining uzunligi necha bitga teng? #128, 192, 256 bit 128, 156, 256 bit 256, 512 bit 128, 192 bit +++++ Kalit bardoshliligi bu -? #eng yaxshi ma'lum algoritmi bilan kalitni topish murakkabligidir eng yaxshi ma'lum algoritmi yordamida yolg'on axborotni ro'kach qilishdir amaliy bardoshlilik nazariy bardoshlilik +++++ RC4 oqimli shifrlash algoritmda har bir qadamda kalit oqimining qanday qiymatini hosil qiladi? #bir baytini bir bitini 64 bitini 8 baytini +++++ AES algoritmda nechta akslantirishlardan foydalaniladi? #4 2 5 6 +++++ Qanday funksiyalarga xesh funksiya deyiladi? #ixtiyoriy uzunlikdagi ma'lumotni biror fiksirlangan uzunlikga o'tkazuvchi funksiyaga aytiladi ma'lumot baytlarini boshqa qiymatlarga almashtiruvchi funksiyaga aytiladi ma'lumot bitlarini boshqa qiymatlarga almashtiruvchi funksiyaga aytiladi ixtiyoriy uzunlikdagi ma'lumotni bit yoki baytlarini zichlashtirib beruvchi funksiyaga aytiladi +++++ Xesh funksiyalar qanday maqsadlarda ishlatiladi? #ma'lumotni to'liqligini nazoratlash va ma'lumot



manbaini autentifikatsiyalashda ma'lumot manbaini autentifikatsiyalashda ma'lumotni butunligini nazoratlashda ma'lumotni maxfiyligini nazoratlash va ma'lumot manbaini haqiqiyligini tekshirishda +++++ Ma'lumotni sakkizlik sanoq tizimidan o'n oltilik sanoq tizimiga o'tkazish bu? #kodlash rasshifrovkalash yashirish shifrlash +++++ A5/1 shifri qaysi turga mansub? #oqimli shifrlar blokli shifrlar ochiq kalitli shifrlar assimetrik shifrlar +++++ Qaysi algoritmlar simmetrik blokli shifrlarga tegishli? #AES, DES A5/1, AES Vijiner, DES Sezar, AES +++++ Ma'lumotni mavjudligini yashirishni maqsad qilgan bilim sohasi bu? #steganografiya kriptografiya kodlash kriptotahlil +++++ Faqat simmetrik blokli shifrlarga xos bo'lgan atamani aniqlang? #blok uzunligi kalit uzunligi ochiq kalit kodlash jadvali +++++ Quyidagi ta'rif qaysi atamaga tegishli: "maxfiy kodlarni"ni buzish bilan shug'ullanadigan soha-bu? #kriptotahlil kripto kriptologiya kriptografiya +++++ Qadimiy davr klassik shifriga quyidagilarning qaysi biri tegishli? #Sezar kodlar kitobi Enigma shifri DES, AES shifri +++++ Quyidagi ta'rif qaysi kriptotizimga tegishli: ochiq matnni shifrlashda hamda rasshifrovkalashda mos holda ochiq va maxfiy kalitdan foydalanadi? #ochiq kalitli kriptotizimlar maxfiy kalitli kriptotizimlar simmetrik kriptotizimlar elektron raqamli imzo tizimlari +++++ Simmetrik shifrlar axborotni qaysi xususiyatlarini ta'minlashda foydalaniladi? #konfidensiallik va yaxlitlik konfidensiallik va foydalanuvchanlik foydalanuvchanlik va yaxlitlik foydalanuvchanlik +++++ Qanday algoritmlar qaytmas xususiyatiga ega hisoblanadi? #xesh funksiyalar elektron raqamli imzo algoritmlari simmetrik kriptotizimlar ochiq kalitli kriptotizimlar +++++ Ochiq matn qismlarini takror shifrlashga asoslangan usul bu? #blokli shifrlar oqimli shifrlar assimetrik shifrlar ochiq kalitli shifrlar +++++ Ochiq kalitli shifrlashda deshifrlash qaysi kalit asosida amalga oshiriladi? #shaxsiy kalit ochiq kalit kalitdan foydalanilmaydi umumiy kalit +++++ Quyidagi ta'rif qaysi atamaga tegishli: "maxfiy kodlarni"ni yaratish bilan shug'ullanadigan soha-bu? #kriptografiya kriptologiya kriptotahlil kripto +++++ Simmetrik kriptotizimlarning asosiy kamchiligi bu? #kalitni taqsimlash zaruriyati kalitlarni esda saqlash murakkabligi shifrlash jarayonining ko'p vaqt olishi algoritmlarning xavfsiz emasligi +++++ Kriptotizimni boshqaradigan vosita? #kalit algoritm stegokalit kriptotizim boshqarilmaydi +++++ Quyidagi ta'rif qaysi kriptotizimga tegishli:ochiq matnni shifrlashda hamda rasshifrovkalashda bitta maxfiy kalitdan foydalaniladi? #simmetrik kriptotizimlar nosimmetrik kriptotizimlar ochiq kalitli kriptotizimlar assimetrik kriptotizimlar +++++ Kerxgofs prinsipiga ko'ra kriptotizimning to'liq xavfsiz bo'lishi faqat qaysi kattalik nomalum bo'lishiga asoslanishi kerak? #kalit protokol shifrmtn Algoritm +++++ Xesh funksiyalar nima maqsadda foydalaniladi? #ma'lumotlar yaxlitligini ta'minlashda ma'lumot egasini autentifikatsiyalashda ma'lumot maxfiyligini ta'minlashda ma'lumot manbaini autentifikatsiyalashda +++++ Chastotalar tahlili hujumi qanday amalga oshiriladi? #shifr matnda qatnashgan harflar sonini aniqlash orqali shifr matnda eng kam qatnashgan harflarni aniqlash orqali ochiq matnda qatnashgan harflar sonini aniqlash orqali ochiq matnda eng kam qatnashgan harflarni aniqlash orqali +++++ Xesh funksiyaga tegishli bo'lgan talabni aniqlang? #bir tomonlama funksiya bo'lishi chiqishda ixtiyoriy uzunlikda bo'lishi turli kirishlar bir xil chiqishlarni akslantirishi kolliziyaga bardoshli bo'lmasligi +++++ RC4 shifrlash algoritmi bu? #oqimli shifrlash algoritmi ochiq kalitli shifrlash algoritmi blokli shifrlash algoritmi asimetrik shifrlash algoritmi +++++ A5/1 shifrlash algoritmi simmetrik turga mansub bo'lsa, unda nechta kalitdan foydalaniladi? #1 2 3 4 +++++ Qaysi algoritmda, algoritmnining necha round bajarilishi ochiq matn uzunligiga bog'liq? #A5/1 MD5 HMAC SHA1 +++++ Simmetrik va ochiq kalitli kriptotizimlar asosan nimasi bilan bir biridan farq qiladi? #kalitlar soni bilan matematik murakkabligi bilan farq qilmaydi biri maxfiylikni ta'minlasa, biri butunlikni ta'minlaydi +++++ A5/1 oqimli shifrlash algoritmda major qiymati hisoblash jarayonida, ikkinchi (Y) registrning qaysi qiymati olinadi? #y10 y11 y12 y13 +++++ Kalitli xesh funksiyalar

qanday turdagi hujumlardan himoyalaydi? #imitatsiya va o'zgartirish turidagi hujumlardan ma'lumotni oshkor qilish turidagi hujumlardan DDOS hujumlaridan foydalanishni buzishga qaratilgan hujumlardan +++++ Sezar shifrlash algoritmda shifrlash formulasi qanday? # $C=(M+K) \bmod p$   $C=(M-K) \bmod p$   $C=(M*K) \bmod p$   $C=(M/K) \bmod p$  +++++ A5/1 oqimli shifrlash algoritmda Y registr uzunligi nechki bitga teng? #22 20 19 21 +++++ Kalitli xesh funksiyalardan foydalanish nimani kafolatlaydi? #fabrikatsiyani va modifikatsiyani oldini oladi ma'lumot yo'q qilinadi ma'lumot dublikat qilinadi ma'lumot ko'chirib olinadi +++++ DES shifrlash algoritmi simmetrik turga mansub bo'lsa, unda nechta kalitdan foydalaniladi? #1 2 3 4 +++++ AES tanlovi g'olibi bo'lgan algoritm nomini ko'rsating? Rijndael IDEA Blowfish Twofish +++++ AES shifrlash algoritmda 128 bitli ma'lumot bloki qanday o'lchamdagi jadvalga solinadi? #4x4 4x6 6x4 6x6 +++++ A5/1 oqimli shifrlash algoritmda maj(1,0,1) ga teng bo'lsa qaysi registrlar suriladi? #birinchi va uchinchi registrlar suriladi faqat ikkinchi registr suriladi birinchi va ikkinchi registrlar suriladi faqat birinchi resgistr suriladi +++++ GSM tarmog'ida foydalaniluvchi shifrlash algoritmi nomini ko'rsating? #A5/1 DES RC4 AES +++++ HMAC tizimida kalit qiymati blok uzunligidan katta bo'lganda ma'lumotga qanday biriktiriladi? #kalitni xesh qiymati hisoblanib, unga blok uzunligiga teng bo'lguncha nol qiymat qo'shiladi va yangi hosil bo'lgan qiymat ma'lumotga biriktiriladi kalit qiymati blok uzunligiga teng bo'lguncha nol qiymat bilan to'ldirilib hosil bo'lgan qiymat ma'lumotga biriktiriladi kalit qiymati o'zgartirilmagan holda ma'lumotga biriktiriladi xesh funksiyalarda kalit qiymatidan foydalanilmaydi +++++ Qaysi xesh algoritmda 80 raund amal bajariladi? #SHA1 CRC MD5 MAC +++++ Affin shifrlash algoritmda  $a=2$ ,  $b=3$ ,  $p=26$  hamda ochiq matn  $x=4$  ga teng bo'lsa, shifr matn qiymatini toping? #11 27 41 31 +++++ MD5 xesh funksiyada 48 bitli ma'lumot berilganda to'ldirish bitlari qanday to'ldiriladi? #bir bit 1, 399 ta 0, ma'lumot uzunligi qiymatining 64 bitli qiymati bilan bir bit 1, 399 ta 0, ma'lumot uzunligining dastlabki 64 bitli qiymati bilan bir bit 1, 463 ta 0, ma'lumot uzunligi qiymatining 64 bitli qiymati bilan bir bit 1, 463 ta 0, ma'lumot uzunligining dastlabki 64 bitli qiymati bilan +++++ AES shifrlash algoritmda ochiq matn bilan dastlab qanday amal bajariladi? #ochiq matn dastlabki kalit bilan XOR amali bajariladi ochiq matn birinchi raund kalit bilan XOR amali bajariladi ochiq matn ustida dastlab SubBytes akslantirishi amali bajariladi ochiq matn ustida dastlab ShiftRows akslantirishi amali bajariladi +++++ Vernam shifrlash algoritmda ochiq matn  $M=101$  ga, kalit  $K=111$  ga teng bo'lsa shifr matn qiymati qanday bo'ladi? #010 101 111 110 ?Konfidensiallikni ta minlash bu - ? +ruxsatsiz o qishdan himoyalash. -ruxsatsiz yozishdan himoyalash. -ruxsatsiz bajarishdan himoyalash. -ruxsat etilgan amallarni bajarish. ?Foydalanuvchanlikni ta minlash bu - ? +ruxsatsiz bajarishdan himoyalash. -ruxsatsiz yozishdan himoyalash. -ruxsatsiz o qishdan himoyalash. -ruxsat etilgan amallarni bajarish. ?Yaxlitlikni ta minlash bu - ? +ruxsatsiz yozishdan himoyalash. -ruxsatsiz o qishdan himoyalash. -ruxsatsiz bajarishdan himoyalash. -ruxsat etilgan amallarni bajarish. ?Jumlani to ldiring. Hujumchi kabi fikrlash ... kerak. +bo lishi mumkin bo lgan xavfni oldini olish uchun -kafolatlangan amallarni ta minlash uchun -ma lumot, axborot va tizimdan foydalanish uchun -ma lumotni aniq va ishonchli ekanligini bilish uchun ?Jumlani to ldiring. Tizimli fikrlash ... uchun kerak. +kafolatlangan amallarni ta minlash -bo lishi mumkin bo lgan xavfni oldini olish -ma lumot, axborot va tizimdan foydalanish -ma lumotni aniq va ishonchli ekanligini bilish ?Axborot xavfsizligida risk bu? +Manbaga zarar keltiradigan ichki yoki tashqi zaiflik ta sirida tahdid qilish ehtimoli. -U yoki bu faoliyat jarayonida nimaga erishishni xoxlashimiz. -Tashkilot uchun qadrli bo lgan ixtiyoriy narsa. -Tizim yoki tashkilotga zarar yetkazishi mumkin bo lgan istalmagan hodisa. ?Axborot xavfsizligida tahdid bu? +Aktivga zarar yetkazishi mumkin bo lgan istalmagan hodisa. -Noaniqlikning maqsadlarga ta siri. -U yoki bu faoliyat jarayonida nimaga erishishni xohlashimiz. -

Tashkilot uchun qadrlı bo'lgan ixtiyoriy narsa. ?Axborot xavfsizligida aktiv bu? +Tashkilot yoki foydalanuvchi uchun qadrlı bo'lgan ixtiyoriy narsa. -Tizim yoki tashkilotga zarar yetkazishi mumkin bo'lgan istalmagan hodisa. -Noaniqlikning maqsadlarga ta'siri. -U yoki bu faoliyat jarayonida nimaga erishishni xohlashimiz. ?Axborot xavfsizligida zaiflik bu? +Tahdidga sabab bo'luvchi tashkilot aktivi yoki boshqaruv tizimidagi nuqson. -Tashkilot uchun qadrlı bo'lgan ixtiyoriy narsa. -Tizim yoki tashkilotga zarar yetkazishi mumkin bo'lgan istalmagan hodisa. -Noaniqlikning maqsadlarga ta'siri. ?Axborot xavfsizligida boshqarish vositasi bu? +Natijasi zaiflik yoki tahdidga ta'sir qiluvchi riskni o'zgartiradigan harakatlar. -Bir yoki bir nechta tahdidga sabab bo'luvchi tashkilot aktivi yoki boshqaruv tizimidagi kamchilik. -Tashkilot uchun qadrlı bo'lgan ixtiyoriy narsa. -Tizim yoki tashkilotga zarar yetkazishi mumkin bo'lgan istalmagan hodisa. ?Har qanday vaziyatda biror bir hodisani yuzaga kelish ehtimoli qo'shilsa .... +risk paydo bo'ladi. -hujum paydo bo'ladi. -tahdid paydo bo'ladi. -aktiv paydo bo'ladi. ?Jumlani to'ldiring. Denial of service (DOS) hujumi axborotni .... xususiyatini buzushga qaratilgan. +foydalanuvchanlik -butunlik -konfidensiallik -ishonchlik ?Jumlani to'ldiring. ... sohasi tashkil etuvchilar xavfsizligi, aloqa xavfsizligi va dasturiy ta'minotlar xavfsizligidan iborat. +Tizim xavfsizligi -Ma'lumotlar xavfsizligi -Inson xavfsizligi -Tashkilot xavfsizligi ?Kriptologiya so'ziga berilgan to'g'ri tavsifni toping? +Maxfiy shifrlarni yaratish va buzish fani va sanati. -Maxfiy shifrlarni yaratish fani va sanati. -Maxfiy shifrlarni buzish fani va sanati. -Axborotni himoyalash fani va sanati. ?.... kriptotizimni shifrlash va deshifrlash uchun sozlashda foydalaniladi. +Kriptografik kalit -Ochiq matn -Alifbo -Algoritm ?Kriptografiya so'ziga berilgan to'g'ri tavsifni toping? +Maxfiy shifrlarni yaratish fani va sanati. -Maxfiy shifrlarni yaratish va buzish fani va sanati. -Maxfiy shifrlarni buzish fani va sanati. -Axborotni himoyalash fani va sanati. ?Kriptotahlil so'ziga berilgan to'g'ri tavsifni toping? +Maxfiy shifrlarni buzish fani va sanati. -Maxfiy shifrlarni yaratish fani va sanati. -Maxfiy shifrlarni yaratish va buzish fani va sanati. -Axborotni himoyalash fani va sanati. ?..... axborotni ifodalash uchun foydalaniladigan chekli sondagi belgilar to'plami. +Alifbo -Ochiq matn -Shifmatn -Kodlash ?Ma'lumot shifrlansa, natijasi .... bo'ladi. +shifmatn -ochiq matn -nomalum -kod ?Deshifrlash uchun kalit va ..... kerak bo'ladi. +shifmatn -ochiq matn -kodlash -alifbo ?Ma'lumotni shifrlash va deshifrlashda yagona kalitdan foydalanuvchi tizim bu - +simmetrik kriptotizim. -ochiq kalitli kriptotizim. -asimmetrik kriptotizim. -xesh funksiyalar. ?Ikki kalitli kriptotizim bu - +ochiq kalitli kriptotizim. -simmetrik kriptotizim. -xesh funksiyalar. -MAC tizimlari. ?Axborotni mavjudligini yashirish bilan shug'ullanuvchi fan sohasi bu - +steganografiya. -kriptografiya. -kodlash. -kriptotahlil. ?Axborotni foydalanuvchiga qulay tarzda taqdim etish uchun ..... amalga oshiriladi. +kodlash -shifrlash -yashirish -deshifrlash ?Jumlani to'ldiring. Ma'lumotni konfidensialligini ta'minlash uchun ..... zarur. +shifrlash -kodlash -dekodlash -deshifrlash ?Ma'lumotni mavjudligini yashirishda ..... +steganografik algoritmdan foydalaniladi. -kriptografik algoritmdan foydalaniladi. -kodlash algoritmidan foydalaniladi. -kriptotahlil algoritmidan foydalaniladi. ?Xesh funksiyalar - .... funksiya. +kalitsiz kriptografik -bir kalitli kriptografik -ikki kalitli kriptografik -ko'p kalitli kriptografik ?Jumlani to'ldiring. Ma'lumotni uzatishda kriptografik himoya ..... +konfidensiallik va butunlikni ta'minlaydi. -konfidensiallik va foydalanuvchanlikni ta'minlaydi. -foydalanuvchanlik va butunlikni ta'minlaydi. -konfidensiallik ta'minlaydi. ?Jumlani to'ldiring. ... kompyuter davriga tegishli shifrlarga misol bo'la oladi. +DES, AES shifri -Sezar shifri -Kodlar kitobi -Enigma shifri ?.... kriptografik shifrlash algoritmlari blokli va oqimli turlarga ajratiladi. +Simmetrik -Ochiq kalitli -Asimmetrik -Klassik davr ?Jumlani to'ldiring. .... shifrlar tasodifiy ketma-ketliklarni generatsiyalashga asoslanadi. +Oqimli -Blokli -Ochiq kalitli -Asimmetrik ?Ochiq matn qismlarini takroriy shifrlovchi algoritmlar bu - +blokli shifrlar -oqimli shifrlash -ochiq kalitli shifrlar -asimmetrik shifrlar ?A5/1 shifri bu - +oqimli shifr. -blokli shifr. -ochiq kalitli shifr. -

asimmetrik shifr ?Quyidagi muammolardan qaysi biri simmetrik kriptotizimlarga xos. +Kalitni taqsimlash zaruriyati. -Shifrlash jarayonining ko p vaqt olishi. -Kalitlarni esda saqlash murakkabligi. -Foydalanuvchilar tomonidan maqbul ko rilmaligi. ?Quyidagi atamalardan qaysi biri faqat simmetrik blokli shifrlarga xos? +Blok uzunligi. -Kalit uzunligi. -Ochiq kalit. -Kodlash jadvali. ?Jumlani to ldiring. Sesar shifri .... akslantirishga asoslangan. +o rniga qo yish -o rin almashtirish -ochiq kalitli -kombinatsion ?Kriptotizimning to liq xavfsiz bo lishi Kerxgo fs prinsipiga ko ra qaysi kattalikning nomalum bo lishiga asoslanadi? +Kalit. -Algoritm. -Shifrmtn. -Protokol. ?Shifrlash va deshifrlashda turli kalitlardan foydalanuvchi shifrlar bu - +ochiq kalitli shifrlar. -simmetrik shifrlar. -bir kalitli shifrlar -xesh funksiyalar. ?Agar simmetrik kalitning uzunligi 64 bit bo lsa, jami bo lishi mumkin bo lgan kalitlar soni nechta? +264 -64! -642 -263 ?Axborotni qaysi xususiyatlari simmetrik shifrlar yordamida ta minlanadi. +Konfidensiallik va butunlik. -Konfidensiallik. -Butunlik va foydalanuvchanlik. -Foydalanuvchanlik va konfidensiallik. ?Axborotni qaysi xususiyatlari ochiq kalitli shifrlar yordamida ta minlanadi. +Konfidensiallik. -Konfidensiallik, butunlik va foydalanuvchanlik. -Butunlik va foydalanuvchanlik. -Foydalanuvchanlik va konfidensiallik. ?Elektron raqamli imzo tizimi. +MAC tizimlari. -Simmetrik shifrlash tizimlari. -Xesh funksiyalar. -Butunlik va foydalanuvchanlik. ?Qaysi ochiq kalitli algoritm katta sonni faktorlash muammosiga asoslanadi? +RSA algoritmi. -El-Gamal algoritmi. -DES. -TEA. ?Rad etishdan himoyalashda ochiq kalitli kriptotizimlarning qaysi xususiyati muhim hisoblanadi. +Ikkita kalitdan foydalanilgani. -Matematik muammoga asoslanilgani. -Ochiq kalitni saqlash zaruriyati mavjud emasligi. -Shaxsiy kalitni saqlash zarurligi. ?Quyidagi talablardan qaysi biri xesh funksiyaga tegishli emas. +Bir tomonlama funksiya bo lmasligi kerak. -Amalga oshirishdagi yuqori tezkorlik. -Turli kirishlar turli chiqishlarni akslantirishi. -Kolliziyaga bardoshli bo lishi. ?Quyidagi xususiyatlardan qaysi biri elektron raqamli imzo tomonidan ta minlanadi? +Axborot butunligini va rad etishdan himoyalash. -Axborot konfidensialligini va rad etishdan himoyalash. -Axborot konfidensialligi. -Axborot butunligi. ?Faqat ma lumotni butunligini ta minlovchi kriptotizimlarni ko rsating. +MAC (Xabarlarini autentifikatsiya kodlari) tizimlari. -Elektron raqamli imzo tizimlari. -Ochiq kalitli kriptografik tizimlar. -Barcha javoblar to g ri. ?Foydalanuvchini tizimga tanitish jarayoni bu? +Identifikatsiya. -Autentifikatsiya. -Avtorizatsiya. -Ro yxatga olish. ?Foydalanuvchini haqiqiyligini tekshirish jarayoni bu? +Autentifikatsiya. -Identifikatsiya. -Avtorizatsiya. -Ro yxatga olish. ?Tizim tomonidan foydalanuvchilarga imtiyozlar berish jarayoni bu? +Avtorizatsiya. -Autentifikatsiya. -Identifikatsiya. -Ro yxatga olish. ?Parolga asoslangan autentifikatsiya usulining asosiy kamchiligini ko rsating? +Esda saqlash zaruriyati. -Birga olib yurish zaruriyati. -Almashtirib bo lmaslik. -Qalbakilashtirish mumkinligi. ?Biror narsani bilishga asoslangan autentifikatsiya deyilganda quyidagilardan qaysilar tushuniladi. +PIN, Parol. -Token, mashinaning kaliti. -Yuz tasviri, barmoq izi. -Biometrik parametrlar. ?Tokenga asoslangan autentifikatsiya usulining asosiy kamchiligini ayting? +Doimo xavfsiz saqlab olib yurish zaruriyati. -Doimo esda saqlash zaruriyati. -Qalbakilashtirish muammosi mavjudligi. -Almashtirib bo lmaslik. ?Esda saqlashni va olib yurishni talab etmaydigan autentifikatsiya usuli bu - +biometrik autentifikatsiya. -parolga asoslangan autentifikatsiya. -tokenga asoslangan autentifikatsiya. -ko p faktorli autentifikatsiya. ?Qaysi biometrik parametr eng yuqori universallik xususiyatiga ega? +Yuz tasviri. -Ko z qorachig i. -Barmoq izi. -Qo l shakli. ?Qaysi biometrik parametr eng yuqori takrorlanmaslik xususiyatiga ega? +Ko z qorachig i. -Yuz tasviri. -Barmoq izi. -Qo l shakli. ?Quyidagilardan qaysi biri har ikkala tomonning haqiqiyligini tekshirish jarayonini ifodalaydi? +Ikki tomonlama autentifikatsiya. -Ikki faktorli autentifikatsiya. -Ko p faktorli autentifikatsiya. -Biometrik autentifikatsiya. ?Parolga asoslangan autentifikatsiya usuliga qaratilgan hujumlarni ko rsating? +Parollar lug atidan foydalanish asosida hujum, yelka orqali

qarash hujumi, zararli dasturlardan foydanish asosida hujum. -Fizik o g irlash hujumi, yelka orqali qarash hujumi, zararli dasturlardan foydanish asosida hujum. -Parollar lug atidan foydalanish asosida hujum, yelka orqali qarash hujumi, qalbakilashtirish hujumi. -Parollar lug atidan foydalanish asosida hujum, bazadagi parametрни almashtirish hujumi, zararli dasturlardan foydanish asosida hujum. ?Tokenga asoslangan autentifikatsiya usuliga qaratilgan hujumlarni ko rsating? +Fizik o g irlash, mobil qurilmalarda zararli dasturlardan foydalanishga asoslangan hujumlar -Parollar lug atidan foydalanish asosida hujum, yelka orqali qarash hujumi, zararli dasturlardan foydanish asosida hujum -Fizik o g irlash, yelka orqali qarash hujumi, zararli dasturlardan foydalanishga asoslangan hujumlar -Parollar lug atidan foydalanish asosida hujum, bazadagi parametрни almashtirish hujumi, zararli dasturlardan foydalanish asosida hujum ?Foydalanuvchi parollari bazada qanday ko rinishda saqlanadi? +Xeshlangan ko rinishda. - Shifrlangan ko rinishda. -Ochiq holatda. -Bazada saqlanmaydi. ?Agar parolning uzunligi 8 ta belgi va har bir o rinda 128 ta turlicha belgidan foydalanish mumkin bo lsa, bo lishi mumkin bo lgan jami parollar sonini toping. +1288 -8128 -128! -2128 ?Parolni "salt" (tuz) kattaligidan foydalanib xeshlashdan (h(password, salt)) asosiy maqsad nima? +Buzg unchiga ortiqcha hisoblashni talab etuvchi murakkablikni yaratish. -Buzg unchi topa olmasligi uchun yangi nomalum kiritish. -Xesh qiymatni tasodifiylik darajasini oshirish. -Xesh qiymatni qaytmaslik talabini oshirish. ?Quyidagilardan qaysi biri tabiiy tahdidga misol bo ladi? +Yong in, suv toshishi, harorat ortishi. - Yong in, o g irlik, qisqa tutashuvlar. -Suv toshishi, namlikni ortib ketishi, bosqinchilik. -Bosqinchilik, terrorizm, o g irlik. ?Qaysi nazorat usuli axborotni fizik himoyalashda inson faktorini mujassamlashtirgan? +Ma muriy nazoratlash. -Fizik nazoratlash. -Texnik nazoratlash. -Apparat nazoratlash. ?Faqat ob ektning egasi tomonidan foydalanishga mos bo lgan mantiqiy foydalanish usulini ko rsating? +Diskretsion foydalanishni boshqarish. -Mandatli foydalanishni boshqarish. - Rolga asoslangan foydalanishni boshqarish. -Attributga asoslangan foydalanishni boshqarish. ?Qaysi usul ob ektlar va sub ektlarni klassifikatsiyalashga asoslangan? +Mandatli foydalanishni boshqarish. -Diskretsion foydalanishni boshqarish. -Rolga asoslangan foydalanishni boshqarish. - Attributga asoslangan foydalanishni boshqarish. ?Biror faoliyat turi bilan bog liq harakatlar va majburiyatlar to plami bu? +Rol. -Imtiyoz. -Daraja. -Imkoniyat. ?Qoida, siyosat, qoida va siyosatni mujassamlashtirgan algoritmlar, majburiyatlar va maslahatlar kabi tushunchalar qaysi foydalanishni boshqarish usuliga aloqador. +Attributga asoslangan foydalanishni boshqarish. - Rolga asoslangan foydalanishni boshqarish. -Mandatli foydalanishni boshqarish. -Diskretsion foydalanishni boshqarish. ?Bell-Lapadula modeli axborotni qaysi xususiyatini ta minlashni maqsad qiladi? +Konfidensiallik. -Butunlik. -Foydalanuvchanlik. -Ishonchlilik. ?Biba modeli axborotni qaysi xususiyatini ta minlashni maqsad qiladi? +Butunlik. -Konfidensiallik. -Foydalanuvchanlik. - Maxfiylik. ?Qaysi turdagi shifrlash vositasida barcha kriptografik parametrlar kompyuterning ishtirokisiz generatsiya qilinadi? +Apparat. -Dasturiy. -Simmetrik. -Ochiq kalitli. ?Qaysi turdagi shifrlash vositasida shifrlash jarayonida boshqa dasturlar kabi kompyuter resursidan foydalanadi? +Dasturiy. -Apparat. -Simmetrik. -Ochiq kalitli. ?Yaratishda biror matematik muammoga asoslanuvchi shifrlash algoritmini ko rsating? +Ochiq kalitli shifrlar. -Simmetrik shifrlar. -Blokli shifrlar. -Oqimli shifrlar. ?Xesh funksiyalarda kolliziya hodisasi bu? +Ikki turli matnlarning xesh qiymatlarini bir xil bo lishi. -Cheksiz uzunlikdagi axborotni xeshlay olishi. -Tezkorlikda xeshlash imkoniyati. -Turli matnlar uchun turli xesh qiymatlarni hosil bo lishi. ?64 ta belgidan iborat Sesar shifrlash usulida kalitni bilmasdan turib nechta urinishda ochiq matnni aniqlash mumkin? +63 -63! - 32 -322 ?Elektron raqamli imzo muolajalarini ko rsating? +Imzoni shakllantirish va imkoni tekshirish. -Shifrlash va deshifrlash. -Imzoni xeshlash va xesh matnni deshifrlash. -Imzoni

shakllartirish va xeshlash. ?"Yelka orqali qarash" hujumi qaysi turdagi autentifikatsiya usuliga qaratilgan. +Parolga asoslangan autentifikatsiya. -Tokenga asoslangan autentifikatsiya. -Biometrik autentifikatsiya. -Ko z qorachig iga asoslangan autentifikatsiya. ?Sotsial injineriyaga asoslangan hujumlar qaysi turdagi autentifikatsiya usuliga qaratilgan. +Parolga asoslangan autentifikatsiya. -Tokenga asoslangan autentifikatsiya. -Biometrik autentifikatsiya. -Ko z qorachig iga asoslangan autentifikatsiya. ?Yo qolgan holatda almashtirish qaysi turdagi autentifikatsiya usuli uchun eng arzon. +Parolga asoslangan autentifikatsiya. -Tokenga asoslangan autentifikatsiya. -Biometrik autentifikatsiya. -Ko z qorachig iga asoslangan autentifikatsiya. ?Qalbakilashtirish hujumi qaysi turdagi autentifikatsiya usuliga qaratilgan. +Biometrik autentifikatsiya. -Biror narsani bilishga asoslangan autentifikatsiya. -Biror narsaga egalik qilishga asoslangan autentifikatsiya. -Tokenga asoslangan autentifikatsiya ?Axborotni butunligini ta minlash usullarini ko rsating. +Xesh funksiyalar, MAC. -Shifrlash usullari. -Assimetrik shifrlash usullari, CRC tizimlari. -Shifrlash usullari, CRC tizimlari. ?Quyidagilardan qaysi biri to liq kompyuter topologiyalarini ifodalamaydi. +LAN, GAN, OSI. -Yulduz, WAN, TCP/IP. -Daraxt, IP, OSI. -Shina, UDP, FTP. ?OSI tarmoq modeli nechta sathdan iborat? +7 -4 -6 -5 ?TCP/IP tarmoq modeli nechta sathdan iborat? +4 -7 -6 -5 ?Hajmi bo yicha eng kichik hisoblangan tarmoq turi bu - +PAN -LAN -CAN -MAN ?IPv6 protokolida IP manzilni ifodalashda necha bit ajratiladi. +128 -32 -64 -4 ?IP manzilni domen nomlariga yoki aksincha almashtirishni amalga oshiruvchi xizmat bu- +DNS -TCP/IP -OSI -UDP ?Natijasi tashkilotning amallariga va funksional harakatlariga zarar keltiruvchi hodisalarning potensial paydo bo lishi bu? +Tahdid. -Zaiflik. -Hujum. -Aktiv. ?Zaiflik orqali AT tizimi xavfsizligini buzish tomon amalga oshirilgan harakat bu? +Hujum. -Zaiflik. -Tahdid. -Zararli harakat. ?Quyidagilardan qaysi biri tarmoq xavfsizligi muammolariga sabab bo lmaydi? +Routerlardan foydalanmaslik. -Qurilma yoki dasturiy vositani noto g ri sozlanish. -Tarmoqni xavfsiz bo lmagani tarzda va zaif loyihalash. -Tug ma texnologiya zaifligi. ?Tarmoq xavfsizligini buzilishi biznes faoliyatga qanday ta sir qiladi? +Biznes faoliyatning buzilishi, huquqiy javobgarlikka sababchi bo ladi. -Axborotni o g irlanishi, tarmoq qurilmalarini fizik buzilishiga olib keladi. -Maxfiylikni yo qolishi, tarmoq qurilmalarini fizik buzilishiga olib keladi. -Huquqiy javobgarlik, tarmoq qurilmalarini fizik buzilishiga olib keladi. ?Razvedka hujumlari bu? +Asosiy hujumlarni oson amalga oshirish uchun tashkilot va tarmoq haqidagi axborotni to plashni maqsad qiladi. -Turli texnologiyalardan foydalangan holda tarmoqqa kirishga harakat qiladi. -Foydalanuvchilarga va tashkilotlarda mavjud bo lgan biror xizmatni cheklashga urinadi. -Tizimni fizik buzishni maqsad qiladi. ?Kirish hujumlari bu? +Turli texnologiyalardan foydalangan holda tarmoqqa kirishga harakat qiladi. -Asosiy hujumlarni oson amalga oshirish uchun tashkilot va tarmoq haqidagi axborotni to plashni maqsad qiladi. -Foydalanuvchilarga va tashkilotlarda mavjud bo lgan biror xizmatni cheklashga urinadi. -Tarmoq haqida axborotni to plash hujumchilarga mavjud bo lgan potensial zaiflikni aniqlashga harakat qiladi. ?Xizmatdan vos kechishga qaratilgan hujumlar bu? +Foydalanuvchilarga va tashkilotlarda mavjud bo lgan biror xizmatni cheklashga urinadi. -Turli texnologiyalardan foydalangan holda tarmoqqa kirishga harakat qiladi. -Asosiy hujumlarni oson amalga oshirish uchun tashkilot va tarmoq haqidagi axborotni to plashni maqsad qiladi. -Tarmoq haqida axborotni to plash hujumchilarga mavjud bo lgan potensial zaiflikni aniqlashga harakat qiladi. ?Paketlarni snifferlash, portlarni skanerlash va Ping buyrug ini yuborish hujumlari qaysi hujumlar toifasiga kiradi? +Razvedka hujumlari. -Kirish hujumlari. -DOS hujumlari. -Zararli dasturlar yordamida amalga oshiriladigan hujumlar. ?O zini yaxshi va foydali dasturiy vosita sifatida ko rsatuvchi zararli dastur turi bu? +Trojan otlari. -Adware. -Spyware. -Backdoors. ?Marketing maqsadida yoki reklamani namoyish qilish uchun foydalanuvchini ko rish rejimini kuzutib boruvchi zararli dastur turi bu?

+Adware. -Trojan otlari. -Spyware. -Backdoors. ?Himoya mexanizmini aylanib o tib tizimga ruxsatsiz kirish imkonini beruvchi zararli dastur turi bu? +Backdoors. -Adware. -Trojan otlari. -Spyware. ?Paket filterlari turidagi tarmoqlararo ekran vositasi OSI modelining qaysi sathida ishlaydi? +Tarmoq sathida. -Transport sathida. -Ilova sathida. -Kanal sathida. ?Tashqi tarmoqdagi foydalanuvchilardan ichki tarmoq resurslarini himoyalash qaysi himoya vositasining vazifasi hisoblanadi. +Tarmoqlararo ekran. -Antivirus. -Virtual himoyalangan tarmoq. -Router. ?Ichki tarmoq foydalanuvchilarini tashqi tarmoqqa bo lgan murojaatlarini chegaralash qaysi himoya vositasining vazifasi hisoblanadi. +Tarmoqlararo ekran. -Antivirus. -Virtual himoyalangan tarmoq. -Router. ?2 lik sanoq tizimida 11011 soniga 11010 sonini 2 modul bo yicha qo shing? +00001 - 10000 -01100 -11111 ?2 lik sanoq tizimida 11011 soniga 00100 sonini 2 modul bo yicha qo shing? +11111 -10101 -11100 -01001 ?2 lik sanoq tizimida 11011 soniga 11010 sonini 2 modul bo yicha qo shing? +00001 -10000 -01100 -11111 ?Axborot saqlagich vositalaridan qayta foydalanish xususiyatini saqlab qolgan holda axborotni yo q qilish usuli qaysi? +Bir necha marta takroran yozish va maxsus dasturlar yordamida saqlagichni tozalash -Magnitsizlantirish -Formatlash -Axborotni saqlagichdan o chirish ?Elektron ma lumotlarni yo q qilishda maxsus qurilma ichida joylashtirilgan saqlagichning xususiyatlari o zgartiriladigan usul bu ... +magnitsizlantirish. -shredirlash. -yanchish. -formatlash. ?Yo q qilish usullari orasidan ekologik jihatdan ma qullanmaydigan va maxsus joy talab qiladigan usul qaysi? +Yoqish -Maydalash -Ko mish -Kimyoviy ishlov berish ?Kiberjinoyatchilik bu - ? +Kompyuter yoki boshqa qurilmalarga qarshi qilingan yoki kompyuter va boshqa qurilmalar orqali qilingan jinoiy faoliyat. -Kompyuterlar bilan bog liq falsafiy soha bo lib, foydalanuvchilarning xatti-harakatlari, kompyuterlar nimaga dasturlashtirilganligi va umuman insonlarga va jamiyatga qanday ta sir ko rsatishini o rganadi. -Hisoblashga asoslangan bilim sohasi bo lib, buzg unchilar mavjud bo lgan sharoitda amallarni kafolatlash uchun o zida texnologiya, inson, axborot va jarayonni mujassamlashtirgan. -Tizimlarni, tarmoqlarni va dasturlarni raqamli hujumlardan himoyalash amaliyoti. ?Kiberetika bu - ? +Kompyuterlar bilan bog liq falsafiy soha bo lib, foydalanuvchilarning xatti-harakatlari, kompyuterlar nimaga dasturlashtirilganligi va umuman insonlarga va jamiyatga qanday ta sir ko rsatishini o rganadi. -Kompyuter yoki boshqa qurilmalarga qarshi qilingan yoki kompyuter va boshqa qurilmalar orqali qilingan jinoiy faoliyat. -Hisoblashga asoslangan bilim sohasi bo lib, buzg unchilar mavjud bo lgan sharoitda amallarni kafolatlash uchun o zida texnologiya, inson, axborot va jarayonni mujassamlashtirgan. -Tizimlarni, tarmoqlarni va dasturlarni raqamli hujumlardan himoyalash amaliyoti. ?Shaxsiy simsiz tarmoqlar qo llanish sohasini belgilang +Tashqi qurilmalar kabellarining o rnida -Binolar va korxonalar va internet orasida belgilangan simsiz bog lanish -Butun dunyo bo yicha internetdan foydalanishda -Simli tarmoqlarni mobil kengaytirish ?VPNning texnik yechim arxitekturasiga ko ra turlari keltirilgan qatorni aniqlang? +Korporativ tarmoq ichidagi VPN; masofadan foydalaniluvchi VPN; korporativ tarmoqlararo VPN -Kanal sathidagi VPN; tarmoq sathidagi VPN; seans sathidagi VPN -Marshuritizator ko rinishidagi VPN; tramoqlararo ekran ko rinishidagi VPN -Dasturiy ko rinishdagi VPN; maxsus shifrlash protsessoriga ega apparat vosita ko rinishidagi VPN ?Axborotning konfidensialligi va butunligini ta minlash uchun ikki uzal orasida himoyalangan tunelni quruvchi himoya vositasi bu? +Virtual Private Network -Firewall -Antivirus -IDS ?Qanday tahdidlar passiv hisoblanadi? +Amalga oshishida axborot strukturasi va mazmunida hech narsani o zgartirmaydigan tahdidlar -Hech qachon amalga oshirilmaydigan tahdidlar -Axborot xavfsizligini buzmaydigan tahdidlar -Texnik vositalar bilan bog liq bo lgan tahdidlar ?Quyidagi qaysi hujum turi razvedka hujumlari turiga kirmaydi? +Ddos -Paketlarni snifferlash -Portlarni skanerlash -Ping buyrug ini yuborish ?Trafik orqali axborotni to plashga harakat qilish

razvedka hujumlarining qaysi turida amalga oshiriladi? +Passiv -DNS izi -Lug atga asoslangan -Aktiv  
?Portlarni va operatsion tizimni skanerlash razvedka hujumlarining qaysi turida amalga oshiriladi?  
+Aktiv -Passiv -DNS izi -Lug atga asoslangan ?Paketlarni snifferlash, portlarni skanerlash, ping  
buyrug ini yuborish qanday hujum turiga misol bo ladi? +Razvedka hujumlari -Xizmatdan voz  
kechishga undash hujumlari -Zararli hujumlar -Kirish hujumlari ?DNS serverlari tarmoqda qanday  
vazifani amalga oshiradi? +Xost nomlari va internet nomlarini IP manzillarga o zgartirish va  
teskarisini amalga oshiradi -Ichki tarmoqqa ulanishga harakat qiluvchi boshqa tarmoq uchun  
kiruvchi nuqta vazifasini bajaradi -Tashqi tarmoqqa ulanishga harakat qiluvchi ichki tarmoq uchun  
chiqish nuqtasi vazifasini bajaradi -Internet orqali ma lumotlarni almashinuvchi turli ilovalar uchun  
tarmoq ulanishlarini sozlash funksiyasini amalga oshiradi ?Markaziy xab yoki tugun orqali  
tarmoqni markazlashgan holda boshqarish qaysi tarmoq topologiyasida amalga oshiriladi? +Yulduz  
-Shina -Xalqa -Mesh ?Quyidagilardan qaysilari ananaviy tarmoq turi hisoblanadi? +WAN, MAN,  
LAN -OSI, TCP/IP -UDP, TCP/IP, FTP -Halqa, yulduz, shina, daraxt ?Quyidagilardan qaysilari tarmoq  
topologiyalari hisoblanadi? +Halqa, yulduz, shina, daraxt -UDP, TCP/IP, FTP -OSI, TCP/IP -SMTP,  
HTTP, UDP ?Yong inga qarshi tizimlarni aktiv chora turiga quyidagilardan qaysilari kiradi? +Yong  
inni aniqlash va bartaraf etish tizimi -Minimal darajada yonuvchan materiallardan foydalanish -  
Yetarlicha miqdorda qo shimcha chiqish yo llarini mavjudligi -Yong inga aloqador tizimlarni to g ri  
madadlanganligi ?Yong inga qarshi kurashishning aktiv usuli to g ri ko rsatilgan javobni toping?  
+Tutunni aniqlovchilar, alangani aniqlovchilar va issiqlikni aniqlovchilar -Binoga istiqomat  
qiluvchilarni yong in sodir bo lganda qilinishi zarur bo lgan ishlar bilan tanishtirish -Minimal  
darajada yonuvchan materiallardan foydalanish, qo shimcha etaj va xonalar qurish -Yetarli sondagi  
qo shimcha chiqish yo llarining mavjudligi ?Yong inga qarshi kurashishning passiv usuliga kiruvchi  
choralarni to g ri ko rsatilgan javobni toping? +Minimal darajada yonuvchan materiallardan  
foydalanish, qo shimcha etaj va xonalar qurish -Tutun va alangani aniqlovchilar -O t o chirgich, suv  
purchash tizimlari -Tutun va alangani aniqlovchilar va suv purchash tizimlari ?Fizik himoyani  
buzilishiga olib keluvchi tahdidlar yuzaga kelish shakliga ko ra qanday guruhlarga bo linadi? +Tabiiy  
va sun iy -Ichki va tashqi -Aktiv va passiv -Bir faktorlik va ko p faktorli ?Quyidagilarnnig qaysi biri  
tabiiy tahdidlarga misol bo la oladi? +Toshqinlar, yong in, zilzila -Bosqinchilik, terrorizm, o g irlik -O  
g irlik, toshqinlar, zilzila -Terorizim, toshqinlar, zilzila ?Quyidagilarnnig qaysi biri sun iy tahdidlarga  
misol bo la oladi? +Bosqinchilik, terrorizm, o g irlik -Toshqinlar, zilzila, toshqinlar -O g irlik,  
toshqinlar, zilzila -Terorizim, toshqinlar, zilzila ?Kolliziya hodisasi deb nimaga aytiladi? +Ikki xil  
matn uchun bir xil xesh qiymat chiqishi -ikki xil matn uchun ikki xil xesh qiymat chiqishi -bir xil  
matn uchun bir xil xesh qiymat chiqishi -bir xil matn uchun ikki xil xesh qiymat chiqishi ?GSM  
tarmog ida foydanalaniluvchi shifrlash algoritmi nomini ko rsating? +A5/1 -DES -AES -RC4 ?O  
zbekistonda kriptografiya sohasida faoliyat yurituvchi tashkilot nomini ko rsating? +"UNICON.UZ"  
DUK -"O zstandart" agentligi -Davlat Soliq Qo mitasi -Kadastr agentligi ?RC4 shifrlash algoritmi  
simmetrik turga mansub bo lsa, unda nechta kalitdan foydalaniladi? +1 -2 -3 -4 ?A5/1 shifrlash  
algoritmi simmetrik turga mansub bo lsa, unda nechta kalitdan foydalaniladi? +1 -2 -3 -4 ?AES  
shifrlash algoritmi simmetrik turga mansub bo lsa, unda nechta kalitdan foydalaniladi? +1 -2 -3 -4  
?DES shifrlash algoritmi simmetrik turga mansub bo lsa, unda nechta kalitdan foydalaniladi? +1 -2  
-3 -4 ?A5/1 oqimli shifrlash algoritmidan maxfiy kalit necha registrga bo linadi? +3 -4 -5 -6 ?Faqat  
simmetrik blokli shifrlarga xos bo lgan atamani aniqlang? +blok uzunligi -kalit uzunligi -ochiq kalit -  
kodlash jadvali ?A5/1 shifri qaysi turga mansub? +oqimli shifrlar -blokli shifrlar -ochiq kalitli shifrlar  
-assimetrik shifrlar ?.... shifrlar blokli va oqimli turlarga ajratiladi +simmetrik -ochiq kalitli -  
assimetrik -klassik ?Quyida keltirilgan xususiyatlarning qaysilari xesh funksiyaga mos? +ixtiyoriy



olingan har xil matn uchun xesh qiymatlar bir xil bo'lmaydi -ixtiyoriy olingan bir xil matn uchun qiymatlar bir xil bo'lmaydi -ixtiyoriy olingan har xil matn uchun xesh qiymatlar bir xil bo'ladi -ixtiyoriy olingan har xil xesh qiymat uchun dastlabki ma'lumotlar bir xil bo'ladi? Quyida keltirilgan xususiyatlarning qaysilari xesh funksiyaga mos? +chiqishda fiksirlangan uzunlikdagi qiymatni beradi -chiqishda bir xil qiymatni beradi -chiqishdagi qiymat bilan kiruvchi qiymatlar bir xil bo'ladi -kolliziyaga ega? Xesh qiymatlarni yana qanday atash mumkin? +dayjest -funksiya -imzo -raqamli imzo? A5/1 oqimli shifrlash algoritmda dastlabki kalit uzunligi nechki bitga teng? +64 -512 -192 -256? A5/1 oqimli shifrlash algoritmi asosan qayerda qo'llaniladi? +mobil aloqa standarti GSM protokolida -simsiz aloqa vositalaridagi mavjud WEP protokolida -internet trafiklarini shifrlashda -radioaloqa tarmoqlarida? Assimetrik kriptotizimlarda nechki kalitdan foydalaniladi? +2 ta -3 ta -4 ta -kalit ishlatilmaydi? Simmetrik kriptotizimlarda nechki kalitdan foydalaniladi? +1 ta -3 ta -4 ta -kalit ishlatilmaydi? Kriptotizimlar kalitlar soni bo'yicha qanday turga bo'linadi? +simmetrik va assimetrik turlarga -simmetrik va bir kalitli turlarga -3 kalitli turlarga -assimetrik va 2 kalitli turlarga? Kriptologiya qanday yo'nalishlarga bo'linadi? +kriptografiya va kriptotahlil -kriptografiya va kriptotizim -kripto va kriptotahlil -kriptoanaliz va kriptotizim? Qaysi chora tadbirlar virusdan zararlanish holatini kamaytiradi? +Barcha javoblar to'g'ri -Faqat litsenziyalik dasturiy ta'minotdan foydalanish. -Kompyuterni zamonaviy antivirus dasturiy vositasi bilan ta'minlash va uni doimiy yangilab borish. -Boshqa kompyuterda yozib olingan ma'lumotlarni o'qishdan oldin har bir saqlagichni antivirus tekshiruvidan o'tkazish. ?Antivirus dasturiy vositalari zararli dasturlarga qarshi to'liq himoyani ta'minlay olmasligining asosiy sababini ko'rsating? +Paydo bo'layotgan zararli dasturiy vositalar sonining ko'pligi. -Viruslar asosan antivirus ishlab chiqaruvchilar tomonidan yaratilishi. -Antivirus vositalarining samarali emasligi. -Aksariyat antivirus vositalarining pullik ekanligi. ?...umumiy tarmoqni ichki va tashqi qismlarga ajratib himoyalash imkonini beradi. +Tarmoqlararo ekran -Virtual himoyalangan tarmoq -Global tarmoq -Korxona tarmog'i? RSA algoritmda  $p=5$ ,  $q=13$ ,  $e=7$  ga teng bo'lsa, shaxsiy kalitni hisoblang? +7 -13 -65 -35 ?..... hujumida hujumchi o'rnatilgan aloqaga suqilib kiradi va aloqani bo'ladi. Nuqtalar o'rniga mos javobni qo'ying. +O'rnatilgan odam. -Qo'pol kuch. -Parolga qaratilgan. -DNS izi. ?Agar ob'ektning xavfsizlik darajasi sub'ektning xavfsizlik darajasidan kichik yoki teng bo'lsa, u holda O'qish uchun ruxsat beriladi. Ushbu qoida qaysi foydalanishni boshqarish usuliga tegishli. +MAC -DAC -RMAC -ABAC? GSM tarmog'ida ovozli so'zlashuvlarni shifrlash algoritmi bu? +A5/1 -DES -GOST -RSA? RSA algoritmda ochiq kalit  $e=7$ ,  $N=35$  ga teng bo'lsa,  $M=2$  ga teng ochiq matnni shifrlash natijasini ko'rsating? +23 -35 -5 -7? RSA algoritmda ochiq kalit  $e=7$ ,  $N=143$  ga teng bo'lsa,  $M=2$  ga teng ochiq matnni shifrlash natijasini ko'rsating? +128 -49 -11 -7? Jumlani to'ldiring. Agar axborotning o'g'irlanishi moddiy va ma'naviy boyliklarning yo'qotilishiga olib kelsa. +jinoyat sifatida baholanadi. -rag'bat hisoblanadi. -buzg'unchilik hisoblanadi. -guruhlar kurashi hisoblanadi. ?Jumlani to'ldiring. Simli va simsiz tarmoqlar orasidagi asosiy farq ... +tarmoq chetki nuqtalari orasidagi mutlaqo nazoratlamaydigan xudud mavjudligi. -tarmoq chetki nuqtalari orasidagi xududning kengligi. -himoya vositalarining chegaralanganligi. -himoyani amalga oshirish imkoniyati yo'qligi. ?Jumlani to'ldiring. Simmetrik shifrlash algoritmlari ochiq ma'lumotdan foydalanish tartibiga ko'ra ... +blokli va oqimli turlarga bo'linadi. -bir kalitli va ikki kalitli turlarga bo'linadi. -Feystel tarmog'iga asoslangan va SP tarmog'iga asoslangan turlarga bo'linadi. -murakkablikka va tizimni nazariy yondoshuvga asoslangan turlarga bo'linadi. ?Jumlani to'ldiring. Tarmoqlararo ekranning vazifasi ... +ishonchli va ishonchsiz tarmoqlar orasida ma'lumotlarga kirishni boshqarish. -tarmoq hujumlarini aniqlash. -trafikni taqiqlash. -tarmoqdagi xabarlar oqimini uzish va ulash. ?Faktirlash muammosi asosida yaratilgan assimetrik shifrlash usuli? +RSA -El-Gamal -Elliptik egri chiziqqa asoslangan shifrlash -

Diffi-Xelman ?Eng zaif simsiz tarmoq protokolini ko rsating? +WEP -WPA -WPA2 -WPA3  
 ?Axborotni shifrlashdan maqsadi nima? +Maxfiy xabar mazmunini yashirish. -Ma lumotlarni zichlashtirish, siqish. -Malumotlarni yig ish va sotish. -Ma lumotlarni uzatish. ?9 soni bilan o zaro tub bo lgan sonlarni ko rsating? +10, 8 -6, 10 -18, 6 -9 dan tashqari barcha sonlar ?12 soni bilan o zaro tub bo lgan sonlarni ko rsating? +11, 13 -14, 26 -144, 4 -12 dan tashqari barcha sonlar ?13 soni bilan o zaro tub bo lgan sonlarni ko rsating? +5, 7 -12, 26 -14, 39 -13 dan tashqari barcha sonlar ?Jumlani to ldiring. Autentifikatsiya tizimlari asoslanishiga ko ra ... turga bo linadi. +3 -2 -4 -5 ?...umumiy tarmoqni ichki va tashqi qismlarga ajratib himoyalash imkonini beradi.

+Tarmoqlararo ekran -Virtual himoyalangan tarmoq -Global tarmoq -Korxona tarmog i ?Antivirus dasturiy vositalari zararli dasturlarga qarshi to liq himoyani ta minlay olmasligining asosiy sababini ko rsating? +Paydo bo layotgan zararli dasturiy vositalar sonining ko pligi. -Viruslar asosan antivirus ishlab chiqaruvchilar tomonidan yaratilishi. -Antivirus vositalarining samarali emasligi. -Aksariyat antivirus vositalarining pullik ekanligi. ?Qaysi chora tadbirlar virusdan zararlanish holatini kamaytiradi? +Barcha javoblar to g ri -Faqat litsenziyali dasturiy ta minotdan foydalanish. -Kompyuterni zamonaviy antivirus dasturiy vositasi bilan ta minlash va uni doimiy yangilab borish. -Boshqa kompyuterda yozib olingan ma lumotlarni o qishdan oldin har bir saqlagichni antivirus tekshiruvidan o tkazish. ?Virus aniq bo lganda va xususiyatlari aniq ajratilgan holatda eng katta samaradorlikka ega zararli dasturni aniqlash usulini ko rsating? +Signaturaga asoslangan usul -O zgarishga asoslangan usul -Anomaliyaga asoslangan usul -Barcha javoblar to g ri ?Signatura (antiviruslarga aloqador bo lgan) bu-? +Fayldan topilgan bitlar qatori. -Fayldagi yoki katalogdagi o zgarish. -Normal holatdan tashqari holat. -Zararli dastur turi. ?Zararli dasturiy vositalarga qarshi foydalaniluvchi dasturiy vosita bu? +Antivirus -VPN -Tarmoqlararo ekran -Brandmauer

?Kompyuter viruslarini tarqalish usullarini ko rsating? +Ma lumot saqlovchilari, Internetdan yuklab olish va elektron pochta orqali. -Ma lumot saqlovchilari, Internetdan yuklab olish va skaner qurilmalari orqali. -Printer qurilmasi, Internetdan yuklab olish va elektron pochta orqali. -Barcha javoblar to g ri. ?Qurbon kompyuteridagi ma lumotni shifrlab, uni deshifrlash uchun to lovni amalga oshirishni talab qiluvchi zararli dastur bu-? +Ransomware. -Mantiqiy bombalar. -Rootkits. -Spyware. ?Internet tarmog idagi obro sizlantirilgan kompyuterlar bu-? +Botnet. -Backdoors. -Adware. -Virus. ?Biror mantiqiy shartni tekshiruvchi trigger va foydali yuklamadan iborat zararli dastur turi bu-? +Mantiqiy bombalar. -Backdoors. -Adware. -Virus. ?Buzg unchiga xavfsizlik tizimini aylanib o tib tizimga kirish imkonini beruvchi zararli dastur turi bu-? +Backdoors. -Adware. -Virus. -Trojan otlari. ?Ma lumotni to liq qayta tiklash qachon samarali amalga oshiriladi? +Saqlagichda ma lumot qayta yozilmagan bo lsa. -Ma lumotni o chirish Delete buyrug i bilan amalga oshirilgan bo lsa. -Ma lumotni o chirish Shifr+Delete buyrug i bilan amalga oshirilgan bo lsa. -Formatlash asosida ma lumot o chirilgan bo lsa. ?Ma lumotni zaxira nusxalash nima uchun potensial tahdidlarni paydo bo lish ehtimolini oshiradi. +Tahdidchi uchun nishon ko payadi. -Saqlanuvchi ma lumot hajmi ortadi. -Ma lumotni butunligi ta minlanadi. -Ma lumot yo qolgan taqdirda ham tiklash imkoniyati mavjud bo ladi. ?Qaysi xususiyatlar RAID texnologiyasiga xos emas? +Shaxsiy kompyuterda foydalanish mumkin. -Serverlarda foydalanish mumkin. -Xatoliklarni nazoratlash mumkin. -Disklarni "qaynoq almashtirish" mumkin. ?Qaysi zaxira nusxalash vositasi oddiy kompyuterlarda foydalanish uchun qo shimcha apparat va dasturiy vositani talab qiladi? +Lentali disklar. -Ko chma qattiq disklar. -USB disklar. -CD/DVD disklar. ?Ma lumotlarni zaxira nusxalash strategiyasi nimadan boshlanadi? +Zarur axborotni tanlashdan. -Mos zaxira nusxalash vositasini tanlashdan. -Mos zaxira nusxalash usulini tanlashdan. -Mos RAID sathini tanlashdan. ?Jumlani to ldiring. .... - muhim bo lgan axborot nusxalash yoki saqlash jarayoni bo lib, bu ma lumot yo qolgan

vaqtda qayta tiklash imkoniyatini beradi. +Ma lumotlarni zaxira nusxalash -Kriptografik himoya - VPN -Tarmoqlararo ekran ?Paket filteri turidagi tarmoqlararo ekran vositasi nima asosida tekshirishni amalga oshiradi? +Tarmoq sathi parametrlari asosida. -Kanal sathi parametrlari asosida. -Ilova sathi parametrlari asosida. -Taqqimot sathi parametrlari asosida. ?Jumlani to ldiring. ... texnologiyasi lokal simsiz tarmoqlarga tegishli. +WI-FI -WI-MAX -GSM -Bluetooth ?Jumlani to ldiring. Kriptografik himoya axborotning ... xususiyatini ta minlamaydi.

+Foydalanuvchanlik -Butunlik -Maxfiylik -Autentifikatsiya ?Jumlani to ldiring. Parol kalitdan .... farq qiladi. +tasodifiylik darajasi bilan -uzunligi bilan -belgilari bilan -samaradorligi bilan ?Parolga "tuz"ni qo shib xeshlashdan maqsad? +Tahdidchi ishini oshirish. -Murakkab parol hosil qilish. -Murakkab xesh qiymat hosil qilish. -Ya na bir maxfiy parametr kiritish. ?Axborotni foydalanuvchanligini buzishga qaratilgan tahdidlar bu? +DDOS tahdidlar. -Nusxalash tahdidlari. -Modifikatsiyalash tahdidlari. -O rtaga turgan odam tahdidi. ?Tasodifiy tahdidlarni ko rsating?

+Texnik vositalarning buzilishi va ishlamasligi. -Axborotdan ruxsatsiz foydalanish. -Zararkunanda dasturlar. -An anaviy josuslik va diversiya. ?Xodimlarga faqat ruxsat etilgan saytlardan foydalanishga imkon beruvchi himoya vositasi bu? +Tarmoqlararo ekran. -Virtual Private Network. -Antivirus. -Router. ?Qaysi himoya vositasi yetkazilgan axborotning butunligini tekshiradi? +Virtual Private Network. -Tarmoqlararo ekran. -Antivirus. -Router. ?Qaysi himoya vositasi tomonlarni autentifikatsiyalash imkoniyatini beradi? +Virtual Private Network. -Tarmoqlararo ekran. -Antivirus. -Router. ?Foydalanuvchi tomonidan kiritilgan taqiqlangan so rovni qaysi himoya vositasi yordamida nazoratlash mumkin. +Tarmoqlararo ekran. -Virtual Private Network. -Antivirus. -Router. ?Qaysi himoya vositasi mavjud IP - paketni to liq shifrlab, unga yangi IP sarlavha beradi?

+Virtual Private Network. -Tarmoqlararo ekran. -Antivirus. -Router. ?Ochiq tarmoq yordamida himoyalangan tarmoqni qurish imkoniyatiga ega himoya vositasi bu? +Virtual Private Network. -Tapmoklapapo ekran. -Antivirus. -Router. ?Qaysi himoya vositasida mavjud paket shifrlangan holda yangi hosil qilingan mantiqiy paket ichiga kiritiladi? +Virtual Private Network. -Tarmoqlararo ekran. -Antivirus. -Router. ?Qaysi himoya vositasi tarmoqda uzatilayotgan axborotni butunligi, maxfiyligi va tomonlar autentifikatsiyasini ta minlaydi? +Virtual Private Network. -Tarmoqlararo ekran. -Antivirus. -Router. ?Qaysi tarmoq himoya vositasi tarmoq manzili, identifikatorlar, interfeys manzili, port nomeri va boshqa parametrlar yordamida filtrlashni amalga oshiradi.

+Tarmoqlararo ekran. -Antivirus. -Virtual himoyalangan tarmoq. -Router. ?Web-sahifa bu... +Yagona adresga ega bo lgan, brauzer yordamida ochish va ko rish imkoniyatiga ega bo lgan hujjatdir -Tarmoqqa ulangan kompyuterda, klientga belgilangan umumiy vazifalarni bajarish uchun foydalaniluvchi sahifadir -Klient-server arxitekturasida asosidagi, keng tarqalgan Internetning axborot xizmati -HTML kodlari to plami ?Web-sayt nima? +Aniq maqsad asosida mantiqiy bog langan web-sahifalar birlashmasi -Klient-server texnologiyasiga asoslangan, keng tarqalgan internetning axborot xizmatidir -A va B -Yagona adresga ega bo lgan hujjat hisoblanib, uni ochish (brauzer yordamida) va o qish imkoniyati mavjud ?WWW nechta komponentdan tashkil topgan?

+4 -5 -3 -2 ?WWWning komponentlari qaysi javobda to g ri berilgan? +Dasturiy/texnik vositalar, HTML, HTTP, URI -HTML, FTP, WWW -HTML, CSS, PHP -HTML, JavaScript, JQuery, PHP ?Hozirgi kunda WWWning nechta versiyasi mavjud? +4 -3 -5 -2 ?Web 1.0 ning rivojlanish davrini toping? +1990-2000 yy. -2000-2005 yy. -1980-1990 yy. -2010-2015 yy. ?Web 2.0 ning rivojlanish davrini toping? +2000-2010 yy. -2010-2020 yy. -2020-2030 yy. -1990-2000 yy. ?Web 3.0 ning rivojlanish davrini toping? +2010-2020 yy. -2000-2010 yy. -2020-2030 yy. -1990-2000 yy. ?Web 4.0 ning rivojlanish davrini toping? +2020-2030 yy. -2000-2010 yy. -2010-2020 yy. -1990-2000 yy. ?HTML teglar necha xil bo ladi? +Juft, toq, maxsus teglar -Toq teglari -Juft teglari -Ko rinishi ko p ?Qaysi

teg HTML hujjatning tanasini ifodalaydi? +body -html -head -title ?Qaysi teg hujjatning stilini ifodalash uchun ishlatiladi? +style -head -isindex -body ?Qaysi teg HTML hujjatni ifodalaydi? +html -body -meta -isindex ?Qaysi teg HTML hujjat sarlavhasini ifodalaydi? +head -meta -title -body ?Havola to g ri ko rsatilgan qatorni toping. +havola - havola - havola -Ekranni tozalash ?

\_\_\_\_\_ tegi nimani ifodalaydi? +Gorizontal chiziq chizish -Yangi satrga o tish -qo shtirnoq -Ekranni tozalash ?Jadval hosil qilish uchun qaysi tegdan foydalaniladi? + ?Jadval ustunlarini birlashtirish atributi qaysi javobda keltirilgan? ?Jadval satrlarini birlashtirish atributi qaysi javobda keltirilgan? ?HTML da shrift o lchamini o zgartirish uchun qaysi tegdan foydalaniladi? - - - ? tegi nimani ifodalaydi? +Yangi satrga o tish -"uzilish" -qo shtirnoq - Ekranni tozalash ? tegi nima uchun qo llaniladi? +matnni paragraflarga ajratish uchun -Sarlavhani ifodalash uchun -Obyektni ko rsatilgan joyga o rnatish va shu nuqtadan bo sh satrga matnni davom ettirish uchun qo llaniladi -Tartibsiz ro yxat hosil qilish uchun ?Rasmlar bilan ishlash teglarini qaysi javobda berilgan? +img, map, area, picture -Image, map, a, picture -Image, form, area, photo -img, iframe, areas, picture ? tegining vazifasi nima? +Matnni ajratilgan shaklda aniqlash -Matnni o chirilgan shaklda belgilash -Matnni tagiga chizilgan shaklda belgilash -Matnni qiya shaklda belgilash ? tegining vazifasi nima? +Matnni tagiga chizilgan shaklda belgilash -Matnni o chirilgan shaklda belgilash -Matnni ajratilgan shaklda aniqlash -Matnni qia shaklda belgilash ? +Matnni o chirilgan shaklda belgilash -Matnni tagiga chizilgan shaklda belgilash -Matnni ajratilgan shaklda aniqlash -Matnni qia shaklda belgilash ? tegi nimani ifodalaydi? +Tartiblanmagan ro yxat - Tartiblangan ro yxat -Jadval yacheykasi -Yangi qatorga o tish ? matni nimani ifodalaydi? +Teg kvadrat shaklidagi ro yxat hosil qiladi -Teg aylana shaklidagi ro yxat hosil qiladi -Teg alifbo ko rinishdagi ro yxatni hosil qiladi -Teg raqamli ko rinishdagi ro yxatni hosil qiladi ? matni nimani ifodalaydi? +Teg I., II., III., IV. va h.k ko rinishdagi ro yxatni hosil qiladi -Teg raqamli ko rinishdagi ro yxatni hosil qiladi -Teg kvadrat shaklidagi ro yxat hosil qiladi -Teg 1., 2., 3., 4. va h.k ko rinishdagi ro yxatni hosil qiladi ? tegining majburiy atributini toping +src -title -href -type ?Qaysi teg forma ichida qayerga ma lumot kiritilishini ifodalaydi? + - - - ?HTMLda forma elementlariga kiritilgan qiymatlarni tozalash uchun qaysi elementdan foydalaniladi? +reset -text -hidden -submit Yuliy Sezar ma'lumotlarni shifrlashda alfavit xarflarni nechtaga surib shifrlagan? ===== 4 taga===== 2 taga===== 5 taga===== #3 taga +++++ WiMAX qanday simsiz tarmoq turiga kiradi? ===== Lokal ===== Global===== Shaxsiy ===== #Regional +++++ Wi-Fi necha Gs chastotali to'lqinda ishlaydi? ===== #2.4-5 Gs===== 2.4-2.485 Gs===== 1.5-11 Gs===== 2.3-13.6 Gs +++++ Quyidagi parollarning qaysi biri "bardoshli parol"ga kiradi? ===== #Onx458&hdsh) ===== 12456578===== salomDunyo===== Mashina777 +++++ Ma'lumotlarni tasodifiy sabablar tufayli yo'qolish sababini belgilang===== #Quvvat o'chishi, dasturiy ta'minot to'satdan o'zgarishi yoki qurilmani to'satdan zararlanishi===== Tashkilotdagi muhim ma'lumotlarni modifikatsiyalanishi yoki o'g'irlanishi===== Ma'lumotlarni saqlash vositasini to'g'ri joylashtirilmagani yoki ma'lumotlar bazasini xatolik bilan boshqarilganligi. ===== Zilzila, yong'in, suv toshqini va hak. +++++ Sub'ektga ma'lum vakolat va resurslarni berish muolajasi-bu: ===== #Avtorizatsiya===== Haqiqiylikni tasdiqlash===== Autentifikatsiya===== Identifikatsiya +++++ Token, Smartkartalarda xavfsizlik tomonidan kamchiligi nimada? ===== Foydalanish davrida maxfiylik kamayib boradi===== Qurilmalarni ishlab chiqarish murakkab jarayon===== #Qurilmani yo'qotilishi katta xavf olib kelishi mumkin===== Qurilmani qalbakilashtirish oson +++++ Ma'lumotlarni yo'qolish sabab bo'luvchi tabiiy tahdidlarni ko'rsating===== Quvvat o'chishi, dasturiy ta'minot to'satdan o'zgarishi yoki qurilmani to'satdan zararlanishi===== #Zilzila, yong'in, suv toshqini va hak. ===== Tashkilotdagi muhim ma'lumotlarni modifikatsiyalanishi yoki o'g'irlanishi===== Qasddan yoki tasodifiy ma'lumotni o'chirib yuborilishi, ma'lumotlarni saqlash

vositasini to'g'ri joylashtirilmagani +++++ Foydalanish huquqini cheklovchi matritsa modeli bu...  
==== #Bella La-Padulla modeli==== Denning modeli==== Landver modeli==== Huquqlarni  
cheklovchi model +++++ Parollash siyosatiga ko'ra parol tanlash shartlari qanday? ==== Kamida 8  
belgi; katta va kichik xavflar, sonlar qo'llanishi kerak. ==== #Kamida 8 belgi; katta va kichik xavflar,  
sonlar , kamida bitta maxsus simvol qo'llanishi kerak. ==== Kamida 6 belgi; katta xavflar, sonlar ,  
kamida bitta maxsus simvol qo'llanishi kerak. ==== Kamida 6 belgi; katta va kichik xavflar, kamida  
bitta maxsus simvol qo'llanishi kerak. +++++ MD5, SHA1, SHA256, O'z DSt 1106:2009- qanday  
algoritmlar deb ataladi? ==== Kodlash==== #Xeshlash==== Shifrlash==== Stenografiya +++++  
Global simsiz tarmoqda qaysi standartlar ishlaydi? ==== Wi-Fi, 3G==== WIMAX, 2G==== Wi-Fi,  
IRDA==== #CDPD, 4G +++++ RSA algoritmi qaysi yilda ishlab chiqilgan? ==== #1977 yil==== 1966  
yil==== 1988 yil==== 1956 yil +++++ Qaysi texnologiyada ma'lumotni bir vaqtda bir necha diskarga  
navbatlab yoziladi? ==== RAID 1==== #RAID 0==== RAID 5==== RAID 3 +++++ Windows OT lokal  
xavfsizlik siyosatini sozlash oynasiga o'tish uchun buyruqlar satrida qaysi buyruq yoziladi? ====  
#secpol.msc==== regedit==== chkdsk==== diskcopy +++++ Zimmermann telegrami, Enigma shifri,  
SIGABA kriptografiyaning qaysi davriga to'g'ri keladi? ==== O'rta asr davrida==== 15 asr  
davrida==== #1-2 jahon urushu davri==== 21 asr davrida +++++ Bell-LaPadula (BLP) modeli -bu..  
==== Axborlarni nazoratlovchi model==== #Bu hukumat va harbiy dasturlarda kirishni  
boshqarishni kuchaytirish uchun ishlatiladigan avtomatlashgan modeli==== Foydalanuvchilarni  
ro'yxatga olish , nazoratlash va tahlil qiluvchi model==== Tarmoq boshqarish va tahlil qiluvchi  
model +++++ Internetning dastlabki nomini to'g'ri belgilang. ==== #ARPANET==== INTRANET====  
INTERNET==== NETWORK +++++ Axborot xavfsizligining asosiy maqsadlaridan biribu...====  
Ob'ektga bevosita ta'sir qilish==== #Axborotlarni o'g'irlanishini, yo'qolishini, soxtalashtirilishini  
oldini olish==== Axborotlarni shifrlash, saqlash, yetkazib berish==== Tarmoqdagi  
foydalanuvchilarni xavfsizligini ta'minlab berish +++++ Konfidentsiallikga to'g'ri ta'rif keltiring.====  
#axborot inshonchliligi, tarqatilishi mumkin emasligi, maxfiyligi kafolati; ==== axborot  
konfidentsialligi, tarqatilishi mumkinligi, maxfiyligi kafolati; ==== axborot inshonchliligi, tarqatilishi  
mumkin emasligi, parollanganligi kafolati; ==== axborot inshonchliligi, axborotlashganligi,  
maxfiyligi kafolati; +++++ Yaxlitlikni buzilishi bu - ...==== #Soxtalashtirish va o'zgartirish====  
Ishonchsizlik va soxtalashtirish==== Soxtalashtirish==== Butunmaslik va yaxlitlanmaganlik +++++  
Kriptografiyaning asosiy maqsadi nima? ==== ishonchlilik, butunlikni ta'minlash====  
autentifikatsiya, identifikatsiya==== #maxfiylik, yaxlitlikni ta'minlash==== ma'lumotlarni shaklini  
o'zgartirish +++++ Kriptografiyada kalitning vazifasi nima? ==== Bir qancha kalitlar yig'indisi====  
#Matnni shifrlash va shifrini ochish uchun kerakli axborot==== Axborotli kalitlar to'plami====  
Belgini va raqamlarni shifrlash va shifrini ochish uchun kerakli axborot +++++ Qo'yish, o'rin  
almashtirish, gammalash kriptografiyaning qaysi turiga bog'liq? ==== assimetrik kriptotizimlar====  
ochiq kalitli kriptotizimlar==== #simmetrik kriptotizimlar==== autentifikatsiyalash +++++  
Autentifikatsiya nima? ==== Tizim me'yoriy va g'ayritabiiy hollarda rejalashtirilgandek o'zini  
tutishligi holati==== #Ma'lum qilingan foydalanuvchi, jarayon yoki qurilmaning haqiqiy ekanligini  
tekshirish muolajasi==== Istalgan vaqtda dastur majmuasining mumkinligini kafolati==== Tizim  
noodatiy va tabiiy hollarda qurilmaning haqiqiy ekanligini tekshirish muolajasi +++++  
Identifikatsiya bu- ...==== #Foydalanuvchini uning identifikatori (nomi) bo'yicha aniqlash  
jarayoni==== Ishonchliligini tarqalishi mumkin emasligi kafolati==== Axborot boshlang'ich  
ko'rinishda ekanligi uni saqlash, uzatishda ruxsat etilmagan o'zgarishlar==== Axborotni butunligini  
saqlab qolgan holda uni elementlarini o'zgartirishga yo'l qo'ymaslik +++++ Kriptologiya –qanday  
fan? ==== axborotni qayta akslantirishning matematik usullarini izlaydi va tadqiq qiladi==== kalitni

bilmasdan shifrlangan matnni ochish imkoniyatlarini o'rganadi==== kalitlarni bilmasdan shifrn  
ochishga bardoshlilikni aniqlovchi shifrlash tavsifi==== #axborotni qayta akslantirib himoyalash  
muammosi bilan shug'ullanadi +++++ Kriptobardoshlilik deb nimaga aytiladi? ==== #kalitlarni  
bilmasdan shifrn ochishga bardoshlilikni aniqlovchi shifrlash tavsifi==== axborotni qayta  
akslantirib himoyalash muammosi bilan shug'ullanadi==== kalitni bilmasdan shifrlangan matnni  
ochish imkoniyatlarini o'rganadi==== axborotni qayta akslantirishning matematik usullarini izlaydi  
va tadqiq qiladi +++++ Kriptografiya matn –bu.. ==== matnni shifrlash va shifrn ochish uchun  
kerakli axborot==== axborot belgilarini kodlash uchun foydalaniladigan chekli to'plam==== #alifbo  
elementlarining tartiblangan to'plami==== kalit axborotni shifrlovchi kalitlar +++++ Kriptotizimga  
qo'yiladigan umumiy talablardan biri nima? ==== shifrlash algoritmining tarkibiy elementlarini  
o'zgartirish imkoniyati bo'lishi lozim==== ketma-ket qo'llaniladigan kalitlar o'rtasida oddiy va oson  
bog'liqlik bo'lishi kerak==== #shifr matn uzunligi ochiq matn uzunligiga teng bo'lishi kerak====  
maxfiylik o'ta yuqori darajada bo'lmoqligi lozim +++++ Axborot qanday sifatlarga ega bo'lishi  
kerak? ==== uzluksiz va uzlukli==== ishonchli, qimmatli va uzlukli==== #ishonchli, qimmatli va  
to'liq==== ishonchli, qimmatli va uzluksiz +++++ Tekstni boshqa tekst ichida ma'nosini yashirib  
keltirish nima deb ataladi?==== sirli yozuv==== #steganografiya==== skrembler==== shifr  
mashinalar +++++ Berilgan ta'riflardan qaysi biri asimmetrik tizimlarga xos? ==== Asimmetrik  
tizimlarda  $k_1=k_2$  bo'ladi, ya'ni  $k$  – kalit bilan axborot ham shifrlanadi, ham deshifrlanadi====  
#Asimmetrik kriptotizimlarda  $k_1 \neq k_2$  bo'lib,  $k_1$  ochiq kalit,  $k_2$  yopiq kalit deb yuritiladi,  $k_1$  bilan  
axborot shifrlanadi,  $k_2$  bilan esa deshifrlanadi==== Asimmetrik kriptotizimlarda yopiq kalit axborot  
almashinuvining barcha ishtirokchilariga ma'lum bo'ladi, ochiq kalitni esa faqat qabul qiluvchi  
biladi==== Asimmetrik kriptotizimlarda  $k_1 \neq k_2$  bo'lib, kalitlar hammaga oshkor etiladi +++++  
Shaxsning, axborot kommunikatsiya tizimidan foydalanish huquqiga ega bo'lish uchun  
foydalaniluvchining maxfiy bo'lmagan qayd yozuvi – bu...==== parol==== #login====  
identifikatsiya==== token +++++ Uning egasi haqiqiyligini aniqlash jarayonida tekshiruv axboroti  
sifatida ishlatiladigan belgilar ketma-ketligi (maxfiy so'z) – nima? ==== login==== #parol====  
identifikatsiya==== maxfiy maydon +++++ Kodlash nima? ==== Ma'lumot boshqa formatga  
o'zgartiriladi, biroq uni faqat maxsus shaxslar qayta o'zgartirishi mumkin bo'ladi==== Ma'lumot  
boshqa formatga o'zgartiriladi, barcha shaxslar kalit yordamida qayta o'zgartirishi mumkin  
bo'ladi==== Maxfiy xabarni soxta xabar ichiga berkitish orqali aloqani yashirish hisoblanadi====  
#Ma'lumotni osongina qaytarish uchun hammaga ochiq bo'lgan sxema yordamida ma'lumotlarni  
boshqa formatga o'zgartirishdir +++++ Ro'yxatdan o'tish-bu...==== #foydalanuvchilarni ro'yxatga  
olish va ularga dasturlar va ma'lumotlarni ishlatishga huquq berish jarayoni==== axborot tizimlari  
ob'yekt va subhektlariga uni tanish uchun nomlar (identifikator) berish va berilgan nom bo'yicha  
solishtirib uni aniqlash jarayoni==== ob'ekt yoki subhektning unga berilgan identifikatorga mosligini  
tekshirish va belgilar ketma-ketligidan iborat maxfiy kodini tekshirish orqali aslligini aniqlash====  
foydalanuvchining resursdan foydalanish huquqlari va ruxsatlarini tekshirish jarayoni +++++  
Shifrtakstni ochiq tekstga akslantirish jarayoni nima deb ataladi? ==== Xabar==== Shifrlangan  
xabar==== Shifrlash==== #Deshifrlash +++++ .....–hisoblashga asoslangan bilim sohasi bo'lib,  
buzg'unchilar mavjud bo'lgan sharoitda amallarni kafolatlash uchun o'zida texnologiya, inson,  
axborot va jarayonni mujassamlashtirgan. ==== Axborot xavfsizligi==== Kiberjtnoyatchilik====  
#Kiberxavfsizlik==== Risklar +++++ Risk nima? ==== Potensial kuchlanish yoki zarar==== Tasodifiy  
tahdid==== #Potensial foyda yoki zarar==== Katta yo'qotish +++++ Tahdid nima? Tashkilot uchun  
qadrli bo'lgan ixtiyoriy narsa==== Bu riskni o'zgartiradigan harakatlar==== #Tashkilotga zarar  
yetkazishi mumkin bo'lgan istalmagan hodisa==== Bu noaniqlikning maqsadlarga ta'siri +++++

Axborotni shifrnı ochish (deshifrlash) bilan qaysi fan shug'ullanadi? ===== Kartografiya=====  
 #Kriptoanaliz===== Kriptologiya===== Adamar usuli +++++ Qaysi juftlik RSA algoritmining ochiq va  
 yopiq kalitlarini ifodalaydi? ===== {d, e} – ochiq, {e, n} – yopiq; ===== #{d, n} – yopiq, {e, n} – ochiq;  
 ===== {e, n} – yopiq, {d, n} – ochiq; ===== {e, n} – ochiq, {d, n} – yopiq; +++++ Zamonaviy  
 kriptografiya qanday bo'limlardan iborat? ===== Elektron raqamli imzo; kalitlarni boshqarish;=====  
 Simmetrik kriptotizimlar; ochiq kalitli kriptotizimlar; ===== #Simmetrik kriptotizimlar; ochiq kalitli  
 kriptotizimlar; Elektron raqamli imzo; kalitlarni boshqarish ===== Simmetrik kriptotizimlar; ochiq  
 kalitli kriptotizimlar; kalitlarni boshqarish +++++ Shifr nima?===== #Shifrlash va deshifrlashda  
 foydalaniladigan matematik funktsiyadan iborat bo'lgan kriptografik algoritm ===== Kalitlarni  
 taqsimlash usuli===== Kalitlarni boshqarish usuli ===== Kalitlarni generatsiya qilish usuli +++++ Ko'z  
 pardasi, yuz tuzilishi, ovoz tembri, -bular autentifikatsiyaning qaysi faktoriga mos belgilar? =====  
 #Biometrik autentifikatsiya===== Biron nimaga egalik asosida===== Biron nimani bilish asosida=====  
 Parolga asoslangan +++++ Ochiq kalitli kriptotizimlarning mohiyati nimadan iborat? ===== Ochiq  
 kalitli kriptotizimlarda shifrlash va deshifrlashda 1 ta –kalitdan foydalaniladi===== #Ochiq kalitli  
 kriptotizimlarda bir-biri bilan matematik bog'langan 2 ta – ochiq va yopiq kalitlardan  
 foydalaniladi===== Ochiq kalitli kriptotizimlarda ma'lumotlarni faqat shifrlash mumkin===== Ochiq  
 kalitli kriptotizimlarda ma'lumotlarni faqat deshifrlash mumkin +++++ Assimmetrik kriptotizimlar  
 qanday maqsadlarda ishlatiladi? ===== #Shifrlash, deshifrlash, ERI yaratish va tekshirish, kalitlar  
 almashish uchun===== ERI yaratish va tekshirish, kalitlar almashish uchun===== Shifrlash,  
 deshifrlash, kalitlar almashish uchun===== Heshlash uchun +++++ Ma'lumotlar butunligi qanday  
 algoritmlar orqali amalga oshiriladi? ===== Simmetrik algoritmlar===== Assimmetrik algoritmlar=====  
 #Xesh funksiyalar===== Kodlash +++++ To'rtta bir-biri bilan bog'langan bog'lamlar strukturasi  
 (kvadrat shaklida) qaysi topologiya turiga mansub? ===== Yulduz===== To'liq bog'lanishli=====  
 #Xalqa===== Yacheykali +++++ Lokal tarmoqlarda keng tarqalgan topologiya turi qaysi? =====  
 Xalqa===== To'liqbog'langan===== Umumiy shina===== #Yulduz +++++ Ethernet kontsentratori  
 qanday vazifani bajaradi?===== #kompyuterdan kelayotgan axborotni qolgan barcha kompyuterga  
 yo'naltirib beradi===== kompyuterdan kelayotgan axborotni boshqa bir kompyuterga yo'naltirib  
 beradi===== kompyuterdan kelayotgan axborotni xalqa bo'ylab joylashgan keyingi  
 kompyuterga===== tarmoqning ikki segmentini bir biriga ulaydi +++++ OSI modelida nechta sath  
 mavjud? ===== 4 ta===== 5 ta===== #7 ta===== 3 ta +++++ Identifikatsiya, autentifikatsiya  
 jarayonlaridan o'tgan foydalanuvchi uchun tizimda bajarishi mumkin bo'lgan amallarga ruxsat  
 berish jarayoni bu... ===== Shifrlash===== Identifikatsiya===== Autentifikatsiya===== #Avtorizatsiya  
 +++++ Ma'lumotlarni inson xatosi tufayli yo'qolish sababini belgilang. ===== Tashkilotdagi muhim  
 ma'lumotlarni modifikatsiyalanishi yoki o'g'irlanishi. ===== #Ma'lumotlarni saqlash vositasini to'g'ri  
 joylashtirilmagani yoki ma'lumotlar bazasini xatolik bilan boshqarilganligi. ===== Quvvat o'chishi,  
 dasturiy ta'minot to'satdan o'zgarishi yoki qurilmani to'satdan zararlanishi===== Zilzila, yong'in, suv  
 toshqini va hak. +++++ "Parol", "PIN" kodlarni xavfsizlik tomonidan kamchiligi nimadan iborat?  
 ===== Parolni esda saqlash kerak bo'ladi. ===== Parolni almashtirish jarayoni murakkabligi===== Parol  
 uzunligi soni cheklangan===== #Foydalanish davrida maxfiylik kamayib boradi +++++ Qaysi tarmoq  
 kabelining axborot uzatish tezligi yuqori hisoblanadi? ===== #Optik tolali===== O'rama juft=====  
 Koaksial ===== Telefon kabeli +++++ Nima uchun autentifikatsiyalashda parol ko'p qo'llaniladi?  
 ===== #Sarf xarajati kam, almashtirish oson===== Parolni foydalanuvchi ishlab chiqadi===== Parolni  
 o'g'rishlash qiyin===== Serverda parollar saqlanmaydi +++++ Elektron xujjatlarni yo'q qilish usullari  
 qaysilar? ===== Yoqish, ko'mish, yanchish===== #Shredirlash, magnitsizlantirish, yanchish=====  
 Shredirlash, yoqish, ko'mish===== Kimyoviy usul, yoqish. +++++ Ruxsatlarni nazoratlash, "Qopqon",

Yong'inga qarshi tizimlar, Yoritish tizimlari, Ogohlantirish tizimlari , Quvvat manbalari, Video kuzatuv tizimlari, Qurollarni aniqlash, Muhitni nazoratlash amalga oshirish qanday nazorat turiga kiradi? ===== Fizik nazorat===== #Texnik nazorat===== Ma'muriy nazorat===== Tashkiliy nazorat +++++ Avtorizatsiya tushunchasi odatda qaysi tushuncha bilan sinonim sifatida ham foydalanadi? ===== Foydalanish===== Tarmoqni loyixalash===== Identifikatsiya===== #Foydalanishni boshqarish +++++ Foydalanishni boshqarish –bu... ===== Sub'ektni Sub'ektga ishlash qobilyatini aniqlashdir. ===== #Sub'ektni Ob'ektga ishlash qobilyatini aniqlashdir. ===== Ob'ektni Ob'ektga ishlash qobilyatini aniqlashdir===== Autentifikatsiyalash jarayonidir +++++ Foydalanishni boshqarishda inson, dastur, jarayon va hokazolar nima vazifani bajaradi? ===== #Sub'ekt===== Ob'ekt===== Tizim===== Jarayon +++++ Foydalanishna boshqarishda ma'lumot , resurs, jarayon nima vazifani bajaradi ? ===== #Ob'ekt===== Sub'ekt===== Tizim===== Jarayon +++++ MAC usuli bilan foydalanishni boshqarishda xavfsizlik markazlashgan holatda kim tomonidan amalga oshiriladi? ===== Foydalaguvchining o'zi===== #Xavfsizlik siyosati ma'muri===== Dastur tomonidan===== Boshqarish amaalga oshirilmaydi +++++ Agar Sub'ektning xavfsizlik darajasida Ob'ektning xavfsizlik darajasi mavjud bo'lsa, u holda uchun qanday amalga ruxsat beriladi? ===== Yozish ===== O'zgartirish===== #O'qish===== Yashirish +++++ Agar Sub'ektning xavfsizlik darajasi Ob'ektning xavfsizlik darajasida bo'lsa, u holda qanday amalga ruxsat beriladi? ===== #Yozish ===== O'qish===== O'zgartirish===== Yashirish +++++ Rol tushunchasiga ta'rif bering. ===== Foydalanishni boshqarish===== #Muayyan faoliyat turi bilan bog'liq harakatlar va majburiyatlar to'plami sifatida belgilanishi mumkin===== Muayyan faoliyat turi bilan bog'liq imkoniyatlar to'plami sifatida belgilanishi mumkin===== Vakolitlarni taqsimlash +++++ Wi-Fi tarmoqlarida quyida keltirilgan qaysi shifrlash protokollaridan foydalaniladi.===== WEB, SSL, WPA2===== WPA, TLS===== WPA, FTP===== #WEP, WPA, WPA2 +++++ Foydalanishni boshqarishning qaysi usuli – Ob'ektlar va Sub'ektlarning atributlari, ular bilan mumkin bo'lgan amallar va so'rovlarga mos keladigan muhit uchun qoidalarni tahlil qilish asosida foydalanishlarni boshqaradi. ===== MAC===== #ABAC===== DAC===== RBAC +++++ Qanday tarmoq qisqa masofalarda qurilmalar o'rtasida ma'lumot almashinish imkoniyatini taqdim etadi? ===== #Shaxsiy tarmoq===== Lokal===== Mintaqaviy ===== CAMPUS +++++ Quyidagilardan lokal tarmoqqa berilgan ta'rifni belgilang. ===== Odatda ijaraga olingan telekommunikatsiya liniyalaridan foydalanadigan tarmoqlardagi tugunlarni bir-biriga bog'laydi. ===== Bu tarmoq shahar yoki shaharcha bo'ylab tarmoqlarning o'zaro bog'lanishini nazarda tutadi===== Qisqa masofalarda qurilmalar o'rtasida ma'lumot almashinish imkoniyatini taqdim etadi===== #Kompyuterlar va ularni bog'lab turgan qurilmalardan iborat bo'lib, ular odatda bitta tarmoqda bo'ladi. +++++ Quyidagilardan mintaqaviy tarmoqqa berilgan ta'rifni belgilang. ===== Kompyuterlar va ularni bog'lab turgan qurilmalardan iborat bo'lib, ular odatda bitta tarmoqda bo'ladi. ===== Bu tarmoq shahar yoki shaharcha bo'ylab tarmoqlarning o'zaro bog'lanishini nazarda tutadi===== #Odatda ijaraga olingan telekommunikatsiya liniyalaridan foydalanadigan tarmoqlardagi tugunlarni bir-biriga bog'laydi. ===== Qisqa masofalarda qurilmalar o'rtasida ma'lumot almashinish imkoniyatini taqdim etadi +++++ Router nima? ===== Tarmoq qurilmasi bo'lib, ko'plab tarmoqlarni ulash uchun yoki LAN segmentlarini bog'lash uchun xizmat qiladi Hisoblash qurilmasining ajralmas qismi bo'lib, qurilmani tarmoqqa ulash imkoniyatini taqdim etadi===== Ko'plab tarmoqlarni ulash uchun yoki LAN segmentlarini bog'lash uchun xizmat qiladi. ===== Qabul qilingan signalni barcha chiquvchi portlarga emas balki paketda manzili keltirilgan portga uzatadi===== #Qabul qilingan ma'lumotlarni tarmoq sathiga tegishli manzillarga ko'ra (IP manzil) uzatadi. +++++ Fire Wall ning vazifasi... ===== #Tarmoqlar orasida aloqa o'rnatish jarayonida tashkilot va Internet tarmog'i orasida xavfsizlikni ta'minlaydi===== Kompyuterlar tizimi xavfsizligini ta'minlaydi===== Ikkita kompyuter o'rtasida aloqa



o'rnatish jarayonida Internet tarmog'i orasida xavfsizlikni ta'minlaydi==== Uy tarmog'i orasida aloqa o'rnatish jarayonida tashkilot va Internet tarmog'i orasida xavfsizlikni ta'minlaydi +++++ Stenografiya ma'nosi qanday? ==== sirli xat==== #sirli yozuv==== maxfiy axborot==== maxfiy belgi +++++ Shifrlash kaliti noma'lum bo'lganda shifrlangan ma'lumotni deshifrlash qiyinlik darajasini nima belgilaydi? ==== Shifr matn uzunligi==== #Kriptobardoshlik==== Shifrlash algoritmi==== Texnika va texnologiyalar +++++ Ma'lumotlarni yo'q qilish odatda necha xil usulidan foydalaniladi? ==== #4 xil==== 8 xil==== 7 xil==== 5 xil +++++ Kiberjinoyatchilik bu -. . . ==== #Kompyuter yoki boshqa qurilmalarga qarshi qilingan yoki kompyuter va boshqa qurilmalar orqali qilingan jinoiy faoliyat. ==== Kompyuter o'yinlari==== Faqat banklardan pul o'g'irlanishi==== Autentifikatsiya jarayonini buzish +++++ Axborot xavfsizligiga bo'ladigan tahdidlarning qaysi biri maqsadli (atayin) tahdidlar deb hisoblanadi? ==== Tabiiy ofat va avariya==== Texnik vositalarning buzilishi va ishlamasligi==== #Strukturalarni ruxsatsiz modifikatsiyalash==== Foydalanuvchilar va xizmat ko'rsatuvchi hodimlarning hatoliklari +++++ Axborot xavfsizligiga bo'ladigan tahdidlarning qaysi biri tasodifiy tahdidlar deb hisoblanadi? ==== Axborotdan ruxsatsiz foydalanish==== Zararkunanda dasturlar==== An'anaviy josuslik va diversiya haqidagi ma'lumotlar tahlili==== #Texnik vositalarning buzilishi va ishlamasligi +++++ Axborotni uzatish va saqlash jarayonida o'z strukturasi va yoki mazmunini saqlash xususiyati nima deb ataladi? ==== Axborotning konfidentsialligi==== Foydalanuvchanligi==== #Ma'lumotlar butunligi==== Ixchamligi +++++ Biometrik autentifikatsiyalashning avfzalliklari-bu: ==== Bir marta ishlatilishi==== #Biometrik parametrlarning noyobligi==== Biometrik parametrlarni o'zgartirish imkoniyati==== Autentifikatsiyalash jarayonining soddaligi +++++ Simli va simsiz tarmoqlar orasidagi asosiy farq nimadan iborat? ==== #Tarmoq chetki nuqtalari orasidagi mutlaqo nazoratlamaydigan hudud==== Tarmoq chetki nuqtalari orasidagi xududning kengligi asosida qurilmalar holati==== Himoya vositalarining chegaralanganligi==== Himoyani amalga oshirish imkoniyati yo'qligi va ma'lum protokollarning ishlatilishi +++++ Simmetrik shifrlashning noqulayligi – bu: ==== #Maxfiy kalitlar bilan ayirboshlash zaruriyatidir==== Kalitlar maxfiyligi==== Kalitlar uzunligi==== Shifrlashga ko'p vaqt sarflanishi va ko'p yuklanishi +++++ Autentifikatsiya faktorlari nechta? ==== 4 ta==== #3 ta==== 5 ta==== 6 ta +++++ Kompyuter tizimida ro'yxatga olish protsedurasini loyihalashtirish, qaysi standart bo'yicha to'g'ri keltirilgan. ===== #O'z DSt ISO/IEC 27002:2008==== O'z DSt ISO/IEC 27002:2005===== O'z DSt ISO/IEC 27002:2009===== O'z DSt ISO/IEC 27002:2000===== +++++ Parollar bilan ishlashdagi tavsiyalar qaysi qatorda to'g'ri ko'rsatilgan?==== #Tizimga kirishdagi qayta urinishlar sonini parolning minimal uzunligiga va muhofaza qilinayotgan tizimning qiymatiga muvofiq belgilash;===== Ro'yxatga olish protsedurasi uchun ruxsat berilgan vaqtni olib tashlash. Agar u ko'paytirilgan bo'lsa, tizimning ro'yxatga olishini davom ettirish;===== Oxirgi muvaffaqiyatli ro'yxatga olishdan boshlab, boshqa urinishlar so'ramaslik;===== Kiritilayotgan parolni ko'rsatmaslik yoki variant sifatida bir xil parol tanlash.===== +++++ O'zbekiston Respublikasining "Axborotlashtirish to'g'risida"gi qonunining nechinchi moddasida "Axborot resurslari va axborot tizimlarini muhofaza qilishni maqsadlari" keltiriladi ? ==== 19 - modda==== 18 - modda==== 20 - modda==== 21- modda +++++ O'zbekiston Respublikasining "Axborotlashtirish to'g'risida"gi qonunining nechinchi moddasida "Axborot resurslari va axborot tizimlari muhofaza qilinishini tashkil etish " ko'rsatilgan? ==== 20 - modda==== 21 - modda==== 22 - modda==== 19 - modda +++++ ISO/IEC 27000 seriyali standart sohaning quyidagi 10 ta yo'nalishi bo'yicha boshqarish tamoyillari va amaliy tavsiyalari qachon ishlab chiqilgan? ====2005 yilda ====2000 yilda ====2002 yilda ====2004 yilda +++++ ISO/IEC 27000 seriyali standartda sohaning nechta yo'nalishi bo'yicha boshqarish tamoyillari va amaliy

tavsiyalari ishlab chiqilgan? ==== 10 ta==== 5 ta==== 8 ta==== 12 ta +++++ “Axborot texnologiyasi. Xavfsizlikni ta’minlash metodlari. Axborot xavfsizligini boshqarishning amaliy qoidalari ISO/IEC standartining qaysi seriyasida kiritilgan? ==== ISO/IEC 27002:2005==== ISO/IEC 27000:2000==== ISO/IEC 27001:2005==== ISO/IEC 27003:2007 +++++ Fransiyaning ma’lumotlar xavfsizligi to’g’risidagi direktivasi nechinchi yilda kuchga kirdi? ==== 2004 yildan==== 2000 yildan==== 2001 yildan==== 2005 yildan +++++ Italiyaning ma’lumotlar xavfsizligi kodeksi qachon qabul qilingan? ==== 2003 yilda==== 2007 yilda==== 2008 yilda==== 2010 yilda +++++ Avtorizatsiya qilingan foydalanuvchilarning foydalanishini cheklash uchun operatsion tizim darajasida axborot xavfsizligi qanday vositalarini ishlatishi kerak ? ==== Avtorizatsiya qilingan foydalanuvchilar foydalanishini boshqarishning belgilangan siyosatiga muvofiq autentifikatsiya qilinadi; ==== Avtorizatsiya qilingan foydalanuvchilarni foydalanishini boshqarish ixtiyoriy ravishda autentifikatsiya qilinadi; ==== Tizimdan foydalanishga muvaffaqiyatli urinishni bir marta yo’lga qo’yadi va boshqa urinishlarda talab etilmaydi; ==== Zarur bo’lgan holda foydalanuvchilarning ulanishga ruxsat beradi. +++++ Kompyuter tizimida ro’yxatga olish protsedurasini loyihalashtirish, qaysi standart bo’yicha to’g’ri keltirilgan. ==== O’z DSt ISO/IEC 27002:2008 ==== O’z DSt ISO/IEC 27002:2005==== O’z DSt ISO/IEC 27002:2009==== O’z DSt ISO/IEC 27002:2000 +++++ To’g’ri rejalashtirilgan ro’yxatga olish protsedurasi xususiyatlarga ega bo’lishi qaysi qatorda to’g’ri ko’rsatilgan. ==== Ro’yxatga olish jarayoni muvaffaqiyatli tugatilmagunicha tizimlar yoki ilovalar nomlarini aks ettirmaslik; ==== Kompyuterdan avtorizatsiya qilinmagan foydalanuvchilar ham foydalanishi mumkinligi to’g’risida ogohlantiruvchi umumiy xabarnomani aks ettirish; ==== Ro’yxatga olish protsedurasi davomida avtorizatsiya qilinmagan foydalanuvchilarga yordam berishi mumkin bo’lgan xabarlar - yo’l-yo’riqlarni taklif etishlik; ==== Ro’yxatga olish axborotini faqat birinchi kirish ma’lumotlari kiritilganidan so’ng tasdiqlash. Xato kiritilgan holatda ma’lumotlarning qaysi qismi to’g’ri yoki noto’g’riligi to’g’risida axborot berish. +++++ Kompyuter tizimida ro’yxatga olish protsedurasini loyihalashtirish, qaysi qatorda to’g’ri keltirilgan. ==== Parolga kirishga qayta urinishlar sonini parolning minimal uzunligiga va muhofaza qilinayotgan tizimning qiymatiga muvofiq belgilash; ==== Ro’yxatga olishning keyingi urinishlari o’rtasidagi vaqtinchalik kechikishni ulash yoki istalgan maxsus avtorizatsiyasiz ro’yxatga olishning keyingi urinishlariga imkon berish; ==== Ma’lumotlarni uzatishda aloqa seansini uzmasdan davom etishlik; ==== Agar tizimga kirishga urinishlarning maksimal soniga erishilgan bo’lsa, ushbu holat bo’yicha foydalanuvchiga axborot berish. +++++ Parollar bilan ishlashdagi tavsiyalar qaysi qatorda to’g’ri ko’rsatilgan? ==== Tizimga kirishdagi qayta urinishlar sonini parolning minimal uzunligiga va muhofaza qilinayotgan tizimning qiymatiga muvofiq belgilash; ==== Ro’yxatga olish protsedurasi uchun ruxsat berilgan vaqtni olib tashlash. Agar u ko’paytirilgan bo’lsa, tizimning ro’yxatga olishini davom ettirish; ==== Oxirgi muvaffaqiyatli ro’yxatga olishdan boshlab, boshqa urinishlar so’ramaslik; ==== Kiritilayotgan parolni ko’rsatmaslik yoki variant sifatida bir xil parol tanlash. +++++ Agar parollar tizimga kirish seansi jarayonida tarmoq orqali oddiy matnda uzatilsa, ular tarmoqda qaysi dasturlar orqali tutib olinishi mumkin? ==== SNIFFER==== ADOBE FLASH PLAYER 32.0.0.171==== SOFT4BOOST TOOLBAR CLEANER 5.8.9.965==== COMODO DRAGON 70.0.3538.110 +++++ Foydalanishni cheklash bo’yicha qanday tadbirlarning qo’llanishini ko’rib chiqish zarur?==== Tizimning amaliy funksiyalaridan foydalanishni boshqarish uchun menyuni saqlash; ==== Foydalanuvchilarning o’qishi, yozib olishi, yo’q qilishi, bajarishi kerak bo’lgan holatlarga istisno tariqasida ruxsat berish; ==== Boshqa ilovalarning foydalanish huquqlariga ruxsat berish; ==== Konfidensial axborotga ishlov beradigan biznesilovalardan chiqariladigan ma’lumotlar va faqat avtorizatsiya qilingan terminallarning adresiga va tayinlangan joyga yuborilishiga ishonch hosil qilish. ortiqcha axborotni

yo'q qilish uchun chiqarish jarayonini da ++++ O'zbekiston Respublikasining "Davlat sirlarini saqlash to'g'risida" qonuni qachon ishlab chiqilgan. ===== 1993 yil 7 may===== 1995 yil 7 aprel===== 2017 yil 7 fevral===== 1992 yil 10 dekabr ++++ Davlat sirlarini saqlashning huquqiy asosi qaysi qatorda to'g'ri ko'rsatilgan. ===== O'zbekiston Respublikasi Konstitutsiyasi===== ISO/IEC 27002:2005, IDT standarti===== O'z DSt ISO IEC 27002-2016 (uz) ===== O'zbekiston Respublikasi "Jinoyat kodeksi" ++++ Kasbiy maxfiylik to'g'risida ma'lumot qaysi qatorda to'g'ri ko'rsatilgan? ===== Shaxsning huquqlari va qonuniy manfaatlariga ziyon yetkazishi mumkin bo'lgan o'z kasbiy majburiyatlari bajarilganligi sababli, ishonchli shaxsga ma'lum bo'lgan sir===== Bu boshqa shaxsning huquqlari va qonuniy manfaatlariga ziyon yetkazishi mumkin bo'lgan davlat xizmati bilan bog'liq bo'lgan ishonchli shaxsga ma'lum bo'lgan sir===== Ishonchli shaxsning huquqlari va qonuniy manfaatlariga ziyon yetkazishi mumkin bo'lmagan davlat bilan bog'liq bo'lgan, ishonchli yoki shaxsga (egalikka) ma'lum bo'lgan sir===== Kirish cheklangan professional faoliyat bilan bog'liq bo'lmagan ma'lumotlar ++++ Kasbiy (professional) sirlarga oid sirlar qaysi qatorda to'g'ri ko'rsatilgan? ===== Tibbiy maxfiylik, aloqa sirlari, notarial sir, advokatning maxfiyligi, qabul qilish sirlari (farzand asrab olish to'g'risida qaror qabul qilgan sudyalardan tashqari), sug'urtalovchining sirlari, e'tirozning siri (saylovlardagi yopik ovoz berish) ===== Tibbiy maxfiylik, tijorat sirlari, advokatning maxfiyligi, sug'urtalovchining sirlari, e'tirozning siri (saylovlardagi yopik ovoz berish) ===== Tijorat sirlari, tibbiy maxfiylik, harbiy sirlar, advokatning maxfiyligi, sug'urtalovchining sirlari, e'tirozning siri (saylovlardagi yopik ovoz berish) ===== Davlat sirlari, tijorat sirlari, tibbiy maxfiylik, harbiy sirlar, advokatning maxfiyligi, sug'urtalovchining sirlari ++++ Shaxs siri turlari. ===== Biografik va identifikatsiya ma'lumotlari, shaxsiy xarakteristikalar (jumladan, shaxsiy odatlar va nayranglar), oilaviy ahvol haqida ma'lumot (oilaviy munosabatlar). ===== Tibbiy maxfiylik, aloqa sirlari, notarial sir, advokatning maxfiyligi, qabul qilish sirlari (farzand asrab olish to'g'risida qaror qabul qilgan sudyalardan tashqari), sug'urtalovchining sirlari, Tibbiy maxfiylik, aloqa sirlari, notarial sir, advokatning maxfiyligi, qabul qili Advokatning maxfiyligi, qabul qilish sirlari (farzand asrab olish to'g'risida qaror qabul qilgan sudyalardan tashqari), sug'urtalovchining sirlari===== Davlat sirlari, tijorat sirlari, tibbiy maxfiylik, harbiy sirlar, advokatning maxfiyligi, sug'urtalovchining sirlari. ++++ Qachondan Yevropa Ittifoqining barcha mamlakatlarida, jumladan, telekommunikatsiya sohasida yagona shaxsiy ma'lumot himoya qilish tizimi yaratildi? ===== 1998 yilda===== 1996 yilda===== 1999 yilda===== 2003 yilda ++++ Davlat sirlari- bu? ===== Davlat tomonidan qo'riqlanadigan va maxsus ro'yxatlar bilan chegaralab qo'yiladigan alohida ahamiyatli, mutlaqo maxfiy va maxfiy harbiy, siyosiy, iqtisodiy, ilmiytexnikaviy va o'zga xil ma'lumotlar===== Birovga bevosita zarar etkazilishiga yo'l qo'ymaslik xavfi mavjud bo'lmagan shartdir. ===== Shaxs, jamiyat va davlatning hayotiy manfaatlariga putur yetkazadigan shart-sharoit va omillar majmui. ===== Insonning, jamiyatning va davlatning ilg'or rivojlanishining mavjudligi va imkoniyatlarini ishonchli ta'minlaydigan ehtiyojlar majmui. ++++ Xavfsizlikka tahdid - bu ..? ===== Shaxs, jamiyat va davlat hayotiy manfaatlariga putur etkazadigan shart-sharoit va omillarning kombinatsiyasi. ===== Bu hech kimga mumkin bo'lmagan zararni keltirib chiqarishga yo'l qo'ymaslik xavfi mavjud bo'lmagan shartdir. ===== Birovga bevosita zarar etkazilishiga yo'l qo'ymaslik xavfi mavjud bo'lmagan shartdir. ===== Davlatning harbiy, tashqi siyosat, iqtisodiy, razvedka, kontr-razvedka va operativ-qidiruv faoliyati sohasidagi davlat tomonidan muhofaza qilinadigan ma'lumotlar ++++ Xavfsizlik – bu ? ===== Bu hech kimga mumkin bo'lmagan zararni keltirib chiqarishga yo'l qo'ymaslik xavfi mavjud bo'lmagan shartdir===== Shaxs, jamiyat va davlat hayotiy manfaatlariga putur etkazadigan shart-sharoit va omillarning kombinatsiyasi===== Davlatning harbiy, tashqi siyosat, iqtisodiy, razvedka, kontr-razvedka va operativ-qidiruv faoliyati sohasidagi davlat tomonidan muhofaza qilinadigan ma'lumotlar=====

Birovga bevosita zarar etkazilishiga yo'l qo'ymaslik xavfi mavjud bo'lmagan shartdir ++++

Hayotning turli sohalarida davlat xavfsizligiga qancha tahdid mavjud? ===== 5===== 4===== 2===== 3

++++ ... - bu egasining mavjud yoki mumkin bo'lgan sharoitlarda daromadlarini ko'paytirishga imkon beruvchi ma'lumotlarning maxfiyligi, keraksiz xarajatlardan qochish, tovarlar, ishlar, xizmatlar uchun bozorda pozitsiyani saqlab qolish yoki boshqa tijorat manfaa tijorat sirlari===== davlat sirlari===== kasbiy sirlar===== Xizmat sirlari ++++ ...- bu uning kontseptsiyasini va huquqiy rejimini belgilash nuqtai nazaridan eng katta qiyinchilikni anglatadi, chunki turli vaqtlarda bunday turdagi maxfiylik kiritilgan va hozirda turli xil tarkibga ega. ===== Xizmat sirlari===== Davlat sirlari===== kasbiy sirlar===== Tijorat sirlari ++++ ...- bu kirish huquqi cheklangan (tibbiy, notarius, advokat sirlari, yozishmalar sirlari, telefon so'zlashuvlari, pochta, telegraf va boshqa xabarlar va h.k.) bilan bog'liq bo'lgan axborot. ===== Kasbiy sirlar===== Xizmat sirlari===== Davlat sirlari===== Tijorat sirlari ++++ ...- bu yozishmalar, telefon so'zlashuvlari, pochta, telegraf va boshqa kommunikatsiyalar sirlari===== Aloqa sirlari===== Natarial sirlar===== Advokatlik sirlari===== Sug'urta sirlari ++++ ... - bu yuridik yordam ko'rsatish bilan bog'liq holda advokatga bildirilgan ma'lumotlar===== Advokatlik sirlari===== Aloqa sirlari===== Natarial sirlar===== Sug'urta sirlari ++++

Shubhali, firmaning qaltislik va xavfsizlikka oid qoidalarni buzish ehtimoli jihatidan qaysi kategoriya eng ko'p uchraydi? ===== Xodimlar===== xakerlar===== hujumchilar===== qarshi tomonlar (shartnoma bo'yicha ishlaydigan shaxslar) ++++ Ma'lumotlarning tasnifi va himoyalanganligini ta'minlash uchun kim javobgar? ===== rahbarlar===== foydalanuvchilar===== Administratorlar ===== Ma'lumot egalari ++++ Sir qanday toifalarga bo'linadi? ===== ob'ektiv, sub'ektiv===== shaxsiy, umumiy===== xalqaro, davlat===== tijorat, bank ++++ Davlat sirlari egasi kim? ===== davlat===== jamiyat===== xukumat===== xarbiy bo'linmalar ++++ Axborotni himoyalash darajasi nima bilan belgilanadi? ===== Maxfiylik grifi bilan===== Axborotni konfidensialligi bilan===== Axborotni qimmatligi bilan===== Axborotni ruxsat etilganligi bilan ++++ Axborot xavfsizligini boshqarishning asosiy vazifalarini sanab o'ting===== ob'ekt va sub'ektlarning konfiguratsiyani boshqarishgaruxsati,hisob yozuvlarini boshqarish va faol tarmoq qurilmalariga ruxsatga ega bo'lish huquqlari, dasturiy vositalarni yangilanishini boshqarish bilan===== ob'ekt va sub'ektlarning konfiguratsiyasini boshqarishga ruxsati, hisob yozuvlarini boshqarish va faol tarmoq qurilmalariga ruxsatga ega bo'lish huquqlari, ===== ob'ektning konfiguratsiyani boshqarishgaruxsati,hisob yozuvlarini boshqarish va faol tarmoq qurilmalariga ruxsatga ega bo'lish huquqlari, dasturiy vositalarni yangilanishini boshqarish bilan===== ob'ektning konfiguratsiyani boshqarishga ruxsati,hisob yozuvlarini boshqarish va faol tarmoq qurilmalariga ruxsatga ega bo'lish huquqlari, apparat vositalarni yangilanishini boshqarish bilan ++++ Ranjirlash bu ? ===== Axborotni himoyalash usuli, birinchidan, himoyalangan axborotni maxfiylik darajasi bo'yicha bo'lish, ikkinchidan,himoyalangan axborotga ruxsatni cheklashni reglamentlash===== Axborotni himoyalash usuli ,asosiy tashkiliy choralarni qamrab oladi – maxfiy xujjatlarga ruxsatni maksimal chegaralash===== Axborotni himoyalash usuli,yolg'on ma'lumotlarni tarqatish orqali himoyalash===== Axborotni himoyalash usuli,yolg'on ma'lumotlarni tarqatish orqali himoyalash axborotni himoyalash usulibo'lib endi tan olinmoqda ++++

Dezinformatsiya bu ? ===== Axborotni himoyalash usuli, davlatning tashkilotning faoliyatiga tegishli bo'lgan yolg'on ma'lumotlarni tarqatish===== Axborotni himoyalash usuli asosiy tashkiliy choralarni qamrab oladi – maxfiy xujjatlarga ruxsatni maksimal chegaralash===== Axborotni himoyalash usuli birinchidan, himoyalangan axborotni maxfiylik darajasi bo'yicha bo'lish, ikkinchidan,himoyalangan axborotga ruxsatni cheklashni reglamentlash===== Axborotni himoyalash usulibo'lib endi tan olinmoqda ++++ Kodlash bu ? ===== Axborotni himoyalash usuli,asosiy maqsadi raqibdan himoyalangan axborotni asosiy mazmunini kodlash orqali

o'zgartirish va aloqa kanallari orqali jo'natish===== Axborotnihimoyalash usuli, himoyalanadigan ma'lumotni istalgan vaqtda olish imkoniyatini ta'minlash, axborot tashuvchilarni soni va joyi bo'yicha axborot, ushbu axborot foydalanuvchilari to'g'risidagi ma'lumot. ===== Axborotni himoyalash usuli, sirniqulflar emas odamlar qo'riqlaydi degan ma'noni bildiradi===== Axborotni himoyalash usuli, ma'lumotlarni apparat vositalar yordamida uzatish ++++ Shifrlash bu ? ===== Har xil radio uskunalari orqali xabarlarini uzatishda, yozma xabarlar jo'natishda va boshqa holatlarda raqib tomonidan ushbu xabarlarini ushlab qolish xavfi mavjud bo'lgan hollarda tez-tez ishlatiladigan axborotni himoya qilish usuli===== himoya qilinadigan axborotning har qanday tashuvchisi to'g'risida, yashirin ma'lumotlarning barcha tashuvchilarning soniva joylashgan o'rni, shuningdek, ushbu axborotning barcha foydalanuvchilari to'g'risidagi ma'lumotlarni olish imkonini beruvchi axborotni axborotni muhofaza qilishda "sirlarni qulfemas, balki odamlar saqlaydi" deb tarjima qilingan umumiy iboraasosida juda muhim rol o'ynaydi===== axborotni himoya qilish usuli, bu raqibdan muhofaza qilinadigan ma'lumotlarning mazmunini yashirishni maqsad qilib oladi va aloqa kanallari orqali ma'lumotlarni uzatishda shartli ravishda ochiq matn kodlarini ishlatib, raqobatchining qo'lga tushib qolish xav ++++ Axborot xavfsizligining asosiy yo'nalishlari ... ===== axborotni huquqiy, tashkiliy va texnik jihatdan himoya qilish===== faqat axborotlarni muhandislik yuli bilan himoya qilish===== faqat tashkiliy yunalishda axborotni xavfsizligi taminlash===== axborotni faqat dasturiy ta'minotdan himoya qilish ++++ Axborotni xavfsizligi ... ===== axborot xavfsizligini ta'minlashga qaratilgan choratadbirlar majmuasi===== foydalanuvchi talablariga muvofiq ma'lumotlar bazasi tuzilishini ishlab chiqish jarayoni===== muayyan vazifani bajarish uchun kichik dastur. ===== axborotni faqat dasturiy ta'minotdan himoya qilish ++++ Axborotni himoya qilish vositalari bular? ===== jismoniy apparat, apparat, dasturiy ta'minot va kriptografik usullar===== apparat ta'minoti===== dasturiy ta'minot===== apparat va kriptografik usullar ++++ Axborot xavfsizligi tushunchasi ... ===== axborotni muhofaza qilishning mazmuni, maqsadlari, tamoyillari va tashkil etilishi bo'yicha nuqtai nazar===== ichki va tashqi tahdidlardan axborot xavfsizligi holati===== axborot xavfsizligi kuchlari va vositalari===== axborot xavfsizligini ta'minlash ++++ Axborot xavfsizligining asosiy komponentlari: ===== konfidentsiallik, mavjudlik va yaxlitlik===== mavjudligi va yaxlitligi===== Xavfsizlik===== yaxlitlik ++++ Tahdid ... ===== axloqiy yoki moddiy zararga olib keladigan potentsial yoki faktik ta'sir===== ma'lumotlarni to'plash va almashish uchun mo'ljallangan dastur, til, tashkiliy va texnik vositalar tizimi===== aniqlash jarayoni ushbu bosqich talablarining rivojlanish holatiga javob beradi===== aniqlash jarayoni ushbu bosqich talablarining rivojlanish holatiga javob beradi ++++ Axborot xavfsizligi tizimi...? ===== korxona axborot xavfsizligini ta'minlashga qaratilgan tashkiliy-texnik chora-tadbirlar majmui===== axborot resurslarini muhofaza qilish holati===== shaxsiy ma'lumotlardan foydalanishni himoyalash===== axborotni taqdim etish va tarqatish bilan bog'liq axborotni saqlash, qidirish va qayta ishlash tizimi va tegishli tashkilot resurslari ++++ Xavfsizlik siyosatining asoslari===== foydalanishni boshqarish usuli===== risklarni boshqarish===== dasturiy ta'minot===== aloqa kanallarini tanlash ++++ Axborotning yaxlitligi ===== axborotning dolzarbligi va muvofiqligi, uni yo'qqilishdan va ruxsat etilmagan o'zgarishlardan himoya qilish===== axborotdan ruxsatsiz foydalanishdan himoya qilish===== kerakli axborot xizmatini oqilona vaqt ichida olish imkoniyati===== axborotga ruxsat etilishi ++++ "To'qsariqkitob"ga muvofiq tuzilmaviy himoya qanday sinfda qo'llaniladi? ===== B2===== B1===== C1===== C2 ++++ Axborot xavfsizligining necha asosiy komponenti mavjud? ===== 3===== 2===== 4===== 5 ++++ Ma'lumotlarni taqdim etish va ularni himoya qilish darajasini belgilash maqomi quyidagilardir: Axborotning maxfiyligi Axborotning yaxlitligi mavjudligi Kompaktlik ++++ Qonuniy foydalanuvchilar uchun himoyalangan ma'lumotlarga to'siqsiz kirishni ta'minlaydigan

mulk: mavjudligi axborotning maxfiyligi axborotning yaxlitligi Kompaktlik ++++ Maxfiy axborotning yo'qolishi va siqib ketishining oldini olish bo'yicha chora-tadbirlar va himoyalangan ommaviy axborotning yo'qotilishi quyidagilar hisoblanadi: axborot xavfsizligi Axborot himoyasi axborot urushi axborotning zaiflashuvi ++++ Ba'zi mamlakatlar rahbarlari hozirda qaysi dasturlarni ishlab chiqmoqda? Cyber dasturlari Windows dasturlari ishonchli dasturlar Yangi dasturlar ++++ Tashkilot ichidagi tartibni biladiganlardan qaysi biri katta zarar etkazishi mumkin? Xafa qilingan xodimlar boshqaruvchilar Hackerlar barcha xodimlar ++++ Maxfiylik, maxfiylik yoki maxfiylikni yo'qotishga olib kelishi mumkin bo'lgan potentsial hodisa, jarayonlar yoki hodisalar quyidagilardan iborat: tahdid Xavfsizlik kamomadi hujum qilish yaxlitlik ++++ Axborotni himoya qilish tartibi ma'lumotlar .....ga nisbatan belgilanmaydi. jamoat arboblarning faoliyati; davlat sirini; maxfiy axborot; shaxsiy ma'lumotlar ++++ OAV ni ro'yxatdan o'tkazish rad etilishi mumkin emas ... maqsadga muvofiq kelmasa; ariza noo'rin shaxs tomonidan topshirilgan bo'lsa; agar arizadagi ma'lumotlar haqiqatga to'g'ri kelmasa; agar ro'yxatdan o'tkazuvchi organ xuddi shu nom va tarqatish shakli bo'lgan boshqa ommaviy axborot vositasini ro'yxatdan o'tkazgan bo'lsa. ++++ Qaysi ma'lumotlar mahfiylashtiriladi? fuqarolik mudofaasi kuchlari va vositalari haqidagi ma'lumotlar demografik holat; jinoyat holati; inson va fuqarolik huquqlari va erkinliklarini buzish; ++++ Hujjatning raqamli imzosini kim tekshira oladi? hujjatning elektron namunasini, jo'natuvchining ochiq kalitini va raqamli imzoning haqiqiy qiymatini aylantiradigan har qanday manfaatdor shaxs; faqat elektron nusxa hujjati va yuboruvchining ochiq kalitini konvertatsiya qilish bo'yicha mutaxassis elektron hujjatning hujjat almashinuvidan foydalangan holda, jo'natuvchining ochiq kalitini va haqiqiy raqamli imzo qiymatini ishlatuvchi mutaxassis; faqat elektron hujjatning jo'natuvchisi. ++++ Hujjatlangan axborot rejimi bu? elektron raqamli imzoga ega elektron hujjat; tanlangan ma'lumotni ma'lum maqsadlar uchun; har qanday belgi shaklida tanlangan ma'lumotlar; aniqlash uchun elektron axborot. ++++ Shaxsiy ma'lumotlarni qayta ishlashga subyekt roziligi so'raladi qachonki hujjatlar .... uchun qayta ishlanayotgan bo'lsa operatorning professional faoliyati uchun; jurnalistning professional faoliyati uchun; pochta jo'natmalari uchun; agar uning roziligini olish imkoni bo'lmasa, shaxsiy ma'lumotlarning hayotiy manfaatlarini himoya qilish. ++++ Davlat mulkini boshqarish tartibi nimalar uchun o'rnatiladi? tabiatda noyob va o'zgarmas bo'lgan ma'lumotlar uchun har qanday ochiq axborot; har qanday jamoat tashkilot; davlat organlari uchun. ++++ Axborot huquqi nuqtai nazaridan ma'lumot bu taqdim etish shakllaridan qat'iy nazar barcha ma'lumotlar qonunchilik, huquqiy hodisalar, huquqni muhofaza qilish organlari to'g'risidagi ma'lumotlar muayyan yuridik fanni rivojlantirish va uning amaliy qo'llanilishi haqidagi ma'lumotlar; ob'ektiv bilimlarni ifodalash shakli. ++++ Axborotning huquqiy munosabatlari obyektlari bo'lolmaydi? axborot egalari; nolegal axborot; axborot tizimining elementlari; axborot tizimlari; ++++ Axborot sohasida umumiy boshqaruvni amalga oshirish huquqiga ega emas ... Maslahatchi ekspertlar Axborot texnologiyalari vazirligi; Fan va innovatsiyalar agentligi; Xizmat ko'rsatuvchilar ++++ Arxiv fondidagi axborotning ochiqligi qanday ta'minlanadi? axborotdan foydalanishning turli usullari va ma'lumotlarning bir toifasidan boshqasiga ma'lumot uzatilishi orqali axborotdan foydalanishning turli usullari orqali arxiv fondining huquqiy maqomi orqali ma'lumotlarning bir toifasidan boshqasiga ma'lumot uzatilishi orqali ++++ Tijorat siri bilan bog'liq bo'lmagan sifatni ko'rsating savdo sirlarini o'z ichiga olgan ma'lumotlar ta'sis hujjatlarida belgilanadi; ma'lumot haqiqiy yoki potentsial tijorat qiymatiga ega; axborotdan erkin foydalanish mumkin emas; axborot egasi maxfiyligini himoya qilish uchun choralar ko'radi. ++++ Axborot xavfsizligining asosiy ob'ektlari? yopiq muzokaralarni o'tkazish uchun mo'ljallangan binolar va davlat sirlari va maxfiy axborot bilan bog'liq axborotni o'z ichiga

olgan axborot resurslari axborot mahsulotlari; axborot texnologiyalari sohasida malakali xodimlar. Ixtiyoriy turdagi yopiq axborotlar ++++ Qonunchilikni rivojlantirishning hozirgi bosqichida axborot huquqining sub'ekti bu? axborot sohasida jamoatchilik bilan aloqalar axborotni ishlab chiqarish, yig'ish, qaytaishlash, to'plash, saqlash, qidirish, uzatish, tarqatish va iste'mol qilish jarayoniday uzaga keladigan axborot munosabatlari axborot tarmoqlari, axborot resurslari, axborot texnologiyalari, kommunikatsiya tarmoqlari orqali axborot vositalari va vositalari texnologiyalari bo'yicha mehnat natijalarining jamiyati axborot va ular bilan bog'liq faoliyatdan olingan mahsulotlar ++++ Quyidagilardan qaysi biri xizmat siriga aloqador emas? Mehnat shikastlanishi munosabati bilan xodimning sog'lig'iga olib keladigan zarar Davlat siri Kasbiy sir; tegishli organ faoliyatining sirlari; ++++ Quyidagi variantlardan qaysi biri hujjatlashtirilgan axborotning huquqiy rejimiga kiradi? elektron raqamli imzo Bank sirlari Shaxsiy malumotlar Davlat sirlari ++++ Tahririyat majburiyatiga kiradi? intellektual faoliyat natijalari bo'lgan mualliflik huquqlariga rioya qilish fuqarolarning xatlariga javob berish va ularning vakolatiga kiradigan organlarga xat yuborish; har qanday holatda, uning nomini oshkor qilmaslik sharti bilan axborot manbasini sir tutish fuqaroning sha'ni, qadr-qimmatini yoki biznes obro'siga ta'sir etsa, uni rad etish yoki fuqaroga o'qish huquqini berish; ++++ Qaysi ma'lumotlar davlat tomonidan himoyalangan bilan davlat siriga kirmaydi? siyosatchilarning shaxsiy hayoti haqidagi ma'lumotlar tarqalishi davlatga zarar etkazishi mumkin ma'lumotlar Iqtisodiy sohadagi malumotlar Tezkor qidiruv haqidagi ma'lumotlar ++++ Tadbirkorlik faoliyati bilan shug'ullanuvchi shaxslar qaysi axborotga nisbatan tijorat siri rejimini o'rnatishi mumkin? moliyaviy-iqtisodiy axborotni tashkil etuvchi va ortiqcha xarajatlardan qochish imkonini beradigan axborotlarga nisbatan oziq-ovqat xavfsizligini taminlovchi axborotlarga nisbatan ishlab chiqarish jarohatlari, kasbiy ko'rsatkichlari haqidagi axborotlarga nisbatan to'lov tizimi va mehnat sharoitlari to'g'risidagi axborotlarga nisbatan CCC ++++ Himoyalangan ma'lumotlarga tegishli bo'lmagan sifatni ko'rsatib himoyalangan ma'lumotlarga kirish axborot resurslari egasi bilan cheklangan faqat hujjatlashtirilgan ma'lumotlar muhofaza qilinadi himoyalangan ma'lumotlarga kirish faqat qonun bilan cheklangan ma'lumotlarini himoya qilish qonun bilan belgilanadi ++++ Quyidagilarning qaysi biri axborot huquqi tamoyili emas sanoatda nanotexnologiyalarni qo'llashning afzalliklari printsipi aylanish printsipi tarqatish printsipi tillarning tengligi printsipi ++++ Antivirusli himoyaning asosiy vositasi? qimmatli ma'lumotlarni zaxiralash qattiq disklarni muntazam ravishda skanerlash axborot xavfsizligi sohasida malakali kadrlar tayyorlash Ma'lumotlarni klassifikatsiyalash ++++ Veb - server bu masofaviy erkin foydalanishni ta'minlaydigan kompyuter yoki dasturiy ta'minot tizimi kompyuter uchun o'yin konsoli modemning bir turi Hizmat taqdim etadigan ulkan kompyuter ++++ Har kim ega bo'lgan huquq to'g'ri ko'rsatilgan javobni tanlang. har qanday qonuniy yo'l bilan ma'lumot olish izlash, qabul qilish, uzatish, ishlab chiqarish va tarqatish har qanday tarzda ma'lumot izlash, qabul qilish, uzatish, ishlab chiqarish va tarqatish axborotni har qanday tarzda qidirish va tarqatish Ixtiyoriy fuqaro ega bo'lgan huquq bu yerda ko'rsatilmagan ++++ Qanday taqdim etilishidan qat'i nazar jismoniy shaxslar, ob'ektlar, faktlar, hodisalar, hodisalar va hodisalar haqida ma'lumotlar , bu ? axborot Axborot tizimi Ma'lumotlar Axborot resurslari ++++ Fuqarolarning hayoti faktlari, voqealari va holatlari va uning kimligini aniqlashga imkon beradigan ma'lumotlar nima deyiladi? Shaxsiy ma'lumotlar Shaxs sirlari axborot Axborot resursi ++++ Kirish huquqi cheklangan hujjatlashtirilgan axborot deb nimaga aytiladi? Konfidensial axborot Daxshatli sir Oddiy sir axborot ++++ Mulkchilik vakolatlarini to'liq amalga oshiruvchi, foydalanuvchi va axborotni boshqaruvchi sub'ekt kim? axborot egasi. hacker Mulkdor shaxs Begona shaxs ++++ Axborot resurslariga nisbatan egalik huquqi borasidagi munosabatlarni tartibga soluvchi organ qaysi? Axborot va

fuqarolik qonunchiligi fuqarolik qonunchiligi jinoyat qonunchiligi Soliq qonunchiligi ++++ Davlat sirlariga aloqador ma'lumotlarni o'z ichiga olgan axborot resurslari egasi, uni qanday tasarruf etish huquqiga ega? faqat tegishli davlat hokimiyat organlari ruxsati bilan O'zi hohlaganicha MFY ruhsati bilan Militsiya ruhsati bilan istaganicha ++++ Axborot resurslari O'zbekiston Respublikasining qonun hujjatlari nazarda tutilgan mustasno hollardan tashqari, tovar bo'lishi mumkin har doim tovar bo'lishi mumkin; tovar bo'lishi mumkin emas; Faqatgina sotilganda tovarga aylanadi ++++ Himoya nazariyasining tarkibiy qismlari qaysi qatorda to'g'ri ko'rsatilgan? himoya muammosining kelib chiqishi, mohiyati va mazmuni haqida to'liq va tizimli ma'lumotlar har qanday tanlangan strategik o'rnatish doirasida himoya vazifalarini har qanday to'plamini hal qilishning zarur usullari va vositalarini o'z ichiga olgan metodologik va instrumental bazalar axborotni muhofaza qilish ishlarini tashkil etish va ta'minlash bo'yicha ilmiy asoslangan takliflar axborotni muhofaza qilish nazariyasi va amaliyotini rivojlantirishning istiqbolli yo'nalishlarining ilmiy asoslangan prognozi ++++ Umumiy nazariy xarakterning asosiy tamoyillari qaysilar? O'rganilayotgan tizimlar va jarayonlarning etarli modellarini yaratish, bunda maqsadlar shunday qo'yilishi kerakki, ixtiyoriy etapda ularning yutuqlarini moddiy baholash imkoni bo'lsin Ishlab chiqilgan yechimlarni birlashtirish O'rganilayotgan tizimlar va ishlab chiqilgan yechimlarning maksimal tuzilishi Ishlab chiqilgan tushunchalarni amalga oshirishda radikal evolyutsiya ++++ Axborotni himoya qilish jarayonlariga nima eng ko'p ta'sir ko'rsatadi? tasodifiy omillarning kuchli ta'siri texnik tizimlarning ishlashini tashkil etish va ta'minlash stoxastiklik modellashtirish jarayonlari ++++ Noaniq to'plamlar nazariyasi usullari qanday tizimlarni tavsiflash uchun ishlatiladi? elementlari faqat ma'lum bir ehtimollik bilan bir yoki boshqa to'plamlarga tegishli bo'lganda Himoya jarayonlari tavsifini rasmiylashtirish uchun Katta tizimlarni himoya qilish jarayonlarini tavsiflash Katta tizimlarni himoya qilish muammolarini tavsiflash ++++ Lingvistik o'zgaruvchilar nazariyasi usullaridan nima uchun foydalaniladi? ekspert-tahlilchilarning norasmiy hukmlari va xulosalariga asoslangan katta tizimlar modellarini yaratish Himoya jarayonlari tavsifini rasmiylashtirish uchun Katta tizimlarni himoya qilish jarayonlarini tavsiflash Katta tizimlarni himoya qilish muammolarini tavsiflash ++++ Eng mashhur norasmiy baholash usullari qaysilar? ekspert baholash usullari jamoaviy baholash usullari shaxsiy baholash usullari prognozlash usullari ++++ Ko'p faktorli statistik usullarning asoslari nima? korrelyatsiya-regression tahlil qilish tartib-taomillaridan foydalanish stokastik tahlil usullaridan foydalanish dinamik tahlil usullaridan foydalanish korrelyatsion tahlil usullaridan foydalanish ++++ Axborot xavfsizligi masalalariga bag'ishlangan O'zbekiston Respublikasining asosiy qonuni qaysi? O'zbekiston Respublikasining "Axborotlashtirish to'g'risida"gi qonuni. O'zbekiston Respublikasining "axborot erkinligi prinsiplari va kafolatlari to'g'risida" gi qonuni» "Elektron raqamli imzo to'g'risida". O'zbekiston Respublikasining "elektron hisoblash mashinalari va ma'lumotlar bazalari uchun dasturlarni huquqiy muhofaza qilish to'g'risida" gi qonuni» ++++ O'zbekiston Respublikasining "Elektron hisoblash mashinalari va ma'lumotlar bazalari uchun dasturlarni huquqiy muhofaza qilish to'g'risida" gi Qonunini qanday munosabatlarni tartibga soladi? kompyuterlar va ma'lumotlar bazalari uchun dasturlarni yaratish, huquqiy himoya qilish va ulardan foydalanish bilan bog'liq munosabatlar kompyuterlar va ma'lumotlar bazalari uchun dasturlarni yaratish, huquqiy himoya qilish va ulardan foydalanish tartibi kompyuterlar va ma'lumotlar bazalari uchun dasturlarni o'zgartirish, huquqiy himoya qilish va ulardan foydalanish tartibi. kompyuter va ma'lumotlar bazalari uchun dasturlarni tarqatish, huquqiy himoya qilish va ulardan foydalanish tartibi. ++++ O'zbekiston Respublikasining 1993 yil 7 maydagi "Davlat sirlarini himoya qilish to'g'risida" gi Qonuni qaysi munosabatlarni tartibga soladi? davlat sirlari, davlat, harbiy va rasmiy sirlarning toifalarini belgilaydi. Rejimli ob'ektlar. Axborotni



davlat sirlariga kiritish davlat yoki harbiy sirni biladigan fuqarolarning huquqlari Davlat sirlarini himoya qilish bo'yicha O'zbekiston Respublikasi davlat xavfsizlik xizmati huquqlari. Davlat sirlarini sertifikatlashtirish tartibi ++++ Axborot xavfsizligi standartlarining asosiy vazifasi? axborot texnologiyalari mahsulotlarining malakasi bo'yicha ishlab chiqaruvchilar, iste'molchilar va mutaxassislar o'rtasida o'zaro hamkorlik qilish uchun asos yaratish. Axborot texnologiyalari mahsulotlarining malakasi bo'yicha ishlab chiqaruvchilar, iste'molchilar va ekspertlar o'rtasidagi huquqlarni oqlash Axborot texnologiyalari mahsulotlarining malakasi bo'yicha ishlab chiqaruvchilar, iste'molchilar va mutaxassislar o'rtasidagi huquqlarni ajratib turadi Axborot texnologiyalari mahsulotlarini qabul qilish tartibini nazorat qilish ++++ O'zbekiston Respublikasi milliy sertifikatlashtirish organi? O'zbekiston davlat standartlashtirish markazi O'zbekiston Respublikasi Vazirlar Mahkamasi huzuridagi-O'zstandart DXXning vakolatli organi (sertifikatlashtirish markazi) Yo'nalishlar bo'yicha ekspert komissiyalari Yo'nalishlar bo'yicha ekspert komissiyalari ++++ AX soxasi mahsulotlarini sertifikatlash va axborotlashtirish obyektlarini axborot xavfsizli talablariga muvofiqligini attestatsiyalovchi akkreditlangan organ qaysi? DXXning vakolatli organi (sertifikatlashtirish markazi) O'zbekiston davlat standartlashtirish markazi O'zbekiston Respublikasi Vazirlar Mahkamasi huzuridagi-O'zstandart Yo'nalishlar bo'yicha ekspert komissiyalari Vazirlik va idoralarning rejim-maxfiy organlari ++++ AQSh Milliy xavfsizlik agentligining (NSA) maqsadi? Texnik vositalar yordamida AQSh milliy xavfsizligini ta'minlash AQSh milliy xavfsizligini dasturiy vositalar yordamida ta'minlash tashkiliy tadbirlar orqali AQShning milliy xavfsizligini ta'minlash taktik operatsiyalar orqali AQSh milliy xavfsizligini ta'minlash ++++ Mualliflik huquqi, nom berish huquqi va muallifning obro'sini himoya qilish huquqi qanchagacha saqlanib qoladi? Muddatsiz Hayot davomida Hayot davomida va o'limdan keyin 50 yil Hayot davomida va o'limdan keyin 25 yil ++++ Dasturga taqdim etilgan himoya nimalar uchun qo'llanilmaydi? kompyuter dasturining asosiy g'oyalari va tamoyillariga amal qilmaydi kompyuter dasturining manba kodiga taalluqli emas kompyuter dasturining ob'ekt kodiga taalluqli emas kompilyatsiya qilingan kompyuter dasturi kodini qamrab olmaydi ++++ 848-sonli O'zbekiston Respublikasining "Davlat sirlarini saqlash to'g'risida"gi qonuniqachon qabul qilingan? 1993-yil 7-may 2000-yil 23-mart 1998-yil 4-may 1992-yil 12-dekabr ++++ Davlat sirlari tushunchasi O'zbekiston Respublikasining "Davlat sirlarini saqlash to'g'risida" qonunining nechanchi moddasida keltirilgan? 1 - modda 4 - modda 8 - modda 5 - modda ++++ Davlat sirlarini saqlashning huquqiy asosi O'zbekiston Respublikasi Konstitutsiyasi, ushbu Qonun va unga muvofiq ravishda chiqariladigan. O'zbekiston Respublikasining boshqa qonun hujjatlaridan iborat. Ushbu so'zlar O'zbekiston Respublikasining "Davlat sirlarini saqlash to'g'risida" qonunining 2 - modda 4 - modda 8 - modda 5 - modda ++++ O'zbekiston Respublikasining davlat sirlariga nimalar kiradi? davlat sirlari, harbiy sirlar, xizmat sirlari davlat sirlari, harbiy sirlar, maxfiy sirlar davlat sirlari, maxfiy sirlar, konfidensial ma'lumotlar harbiy sirlar, konfidensial ma'lumotlar, xizmat sirlari ++++ Mulk egasiga mavjud yoki ehtimoliy sharoitlarda daromadlarni ko'paytirishga, ortiqcha xarajatlarni qoplamaslikka, tovarlar, ishlar, xizmatlar uchun bozorda pozitsiyani saqlab qolish yoki boshqa tijorat manfaatlariga ega bo'lish imkonini beradigan ma'lumotlar Tijorat siri Xarbiy sir Xizmat siri Davlat siri ++++ ... - bu boshqa shaxsning (ishonchli shaxsning) huquqlari va qonuniy manfaatlariga ziyon etkazishi mumkin bo'lgan davlat yoki kommunal xizmat bilan bog'liq bo'lmagan, o'z kasbiy majburiyatlari bajarilganligi sababli, ishonchli yoki shaxsga (egalikka) ma'lu Kasbiy maxfiylik Xizmat siri Tijorat siri Shaxsiy sir ++++ Shaxsiy ma'lumotlardagi ma'lumotni o'zlarining sha'ni, qadr-qimmati, ishbilarmonlik obro'siga, yaxshi nomga, boshqa noyob imtiyozlarga va mulkiy manfaatlariga zarar etkazishi mumkin bo'lgan axborot nima deyiladi? Shaxs siri Davlat siri Maxfiy axborot Kasb siri ++++ Inson huquqlari

umumjahon deklaratsiyasi nechanchi moddasi quyidagi so'zlar bilan boshlanadi: "Barcha odamlar erkin va teng huquqqa egadirlar va huquqlari bilan tengdirlar". Maxfiylik huquqi konstitutsiyaviy inson huquqlaridan biridir? 1 - modda 4 - modda 8 - modda 5 - modda ++++ Nechanchi yildan beri Evropa Ittifoqining barcha mamlakatlarida, jumladan, telekommunikatsiya sohasida yagona shaxsiy ma'lumot himoya qilish tizimi yaratildi? 1998-yil 1993-yil 1992-yil 1996-yil ++++ Ob'ektlarni o'zaro aloqasini, tuzilishini, qiymatini, kerakli xossalarini va sabablarini o'rganishdagi farazlar qanday ataladi? Buzg'unchining gipotetik modeli Sarguzashtqidiruvchi modeli Bella va La-Padula modeli Denning modeli ++++ Sabablar, maqsadlar va usullarga bog'liq holda axborot xavfsizligini buzuvchilarni nechta kategoriyaga ajratish mumkin? 4 ta 2 ta 3 ta 8 ta ++++ Odatda, yosh, ko'pincha talaba yoki yuqori sinf o'quvchisi va unda o'ylab qilingan xujum rejası kamdankam bo'ladi. U nishonini tasodifan tanlaydi, qiyinchiliklarga duch kelsa chekinadi. Bunday sarguzasht qidiruvchi muvaffaqiyatlarini fakat yaqin do'stlari—k Sarguzasht qidiruvchilar Ishonchsiz xodimlar G'oyaviy xakerlar Xakerlar-professionallar ++++ U o'zining e'tiqodi asosida muayyan nishonlarni (xostlar va resurslarni) tanlaydi. Uning yaxshi ko'rgan xujum turi Web-serverning axborotini o'zgartirishi yoki, juda kam hollarda, xujumlanuvchi resurslar ishini blokirovka qilish. Bular kimlar? G'oyaviy xakerlar Sarguzasht qidiruvchilar Ishonchsiz xodimlar Xakerlar-professionallar ++++ U harakatlarning aniq rejasiga ega va ma'lum resurslarni mo'ljallaydi. Uning xujumlari yaxshi o'ylangan va odatda bir necha bosqichda amalga oshiriladi. Avval u dastlabki axborotni yig'adi (operatsion tizim turi, taqdim etiladigan servislari va qo'llaniladigan h Xakerlar-professionallar G'oyaviy xakerlar Sarguzasht qidiruvchilar Ishonchsiz xodimlar ++++ O'zining harakatlari bilan sanoat josusi etkazadigan muammoga teng muammoni tug'diradi. Buning ustiga uning borligini aniqlash murakkabroq. Undan tashqari unga tarmoqning tashqi himoyasini emas, balki faqat, odatda unchalik kat'iy bo'lmagan tarmo Ishonchsiz xodimlar Xakerlar-professionallar Sarguzasht qidiruvchilar Ishonchsiz xodimlar ++++ Foydalanish xuquqini cheklash vositalarini qurish maqsadida aktiv sub'ektlar S' va passiv ob'ektlar Q tushunchalari kiritilgan bo'lib sub'ektlarning passiv ob'ektlardan foydalanish xuquqlari turlicha bo'ladigan model qaysi? Bella va La-Padula modeli Sarguzasht qidiruvchi modeli Denning modeli Buzg'unchining gipotetik modeli ++++ Ushbu model maxfiylikning turli satxiga ega bo'lgan xujjatlar bilan ishlashdagi ximoya vositalarining ierarxik (shajara) modelidir. Bu qaysi model? Denning modeli Bella va La-Padula modeli Sarguzasht qidiruvchimodeli Buzg'unchining gipotetik modeli ++++ Qaysi model «foydalanishxuquqinicheklovchi matritsa modeli» debyuritiladi? Bella va La-Padula modeli Sarguzasht qidiruvchi modeli Denning modeli Buzg'unchining gipotetik modeli ++++ "O'zbekiston Respublikasi Axborot texnologiyalari va kommunikatsiyalarini rivojlantirish vazirligini tashkil etish to'g'risida"gi farmon qachon qabul qilingan? 2015-yil 4-fevral 2014-yil 8-dekabr 2016-yil 20-noyabr 2013-yil 3-mart ++++ Tahdidlarningta'riflamosravishda, nechta variantdakamaytirishmumkin? 3ta 8ta 4ta 1ta ++++ Tahdid axborotga salbiy ta'sir ko'rsatishi mumkin bo'lgan hodisa, voqea va tasodiflar (yoki ularning paydo bo'lishi ehtimoli) sifatida talqin etiladi. Ushbu parametr har qanday hodisa, voqea va tasodiflar yuzaga kelib qolsa, tahdidni ularning tabiatidan kelib c Ikkinchi Birinchi Uchinchi To'rtinchi ++++ Tahdid axborot xavfsizligini buzish ehtimoli mavjud bo'lgan vaziyat (ehtimol, xavf) sifatida qaraladi. Bu variant, garchi tavsiflovchi lug'atlarda mavjud bo'lgan tahdidlarning umumiy xavfi sifatida tavsiflansa-da, bu tahdid mutlaqo, xavf, vaziyat va imkoniyat sifa Birinchi Ikkinchi Uchinchi To'rtinchi ++++ Tahdid axborotning bir yoki boshqa shaklining zaifligiga olib keladigan haqiqiy yoki potensial mumkin bo'lgan harakatlar yoki shartlar sifatida tavsiflanadi. Ba'zi xatti-harakatlar yoki tahdidlarni faqat shartlar bilan identifikatsiya qilish bu tanlovning mohiyatini t Uchinchi Ikkinchi Birinchi To'rtinchi

++++ Qonunchilikka muvofiq unga ruxsat cheklangan hujjatlashgan axborot qanday axborot? Konfidensial axborot Xarbiy axborot Kasbiy axborot Maxfiy axborot +++++ Axborot xavfsizligini boshqarishning amaliy qoidalari ISO/IEC standartining qaysi seriyasida kiritilgan? ISO/IEC 27002:2005 ISO/IEC 27000:2000 ISO/IEC 27001:2005 ISO/IEC 27003:2007 +++++ Kompyuter tizimida ro'yxatga olish protsedurasini shunday loyihalashtirish kerakki, ruxsatsiz foydalanish imkoniyati minimumga ISO/IEC standartining seriyasi buyicha keltirilsin va avtorizatsiya qilinmagan foydalanuvchiga yordam berilmasin. Ushbu seriya O'zDSt ISO/IEC 27002:2008 O'zDSt ISO/IEC 27000:2000 O'zDSt ISO/IEC 27003:2007 O'zDSt ISO/IEC 27002:2005 +++++ Agar parollar tizimga kirish seansi jarayonida tarmoq orqali oddiy matnda uzatilsa, ular tarmoqda qanday dastur orqali tutib olinishi mumkin? Sniffer Antispufing Spuffer Antispam +++++ "Davlat sirlarini saqlashning xuquqiy asosi" O'zbekiston Respublikasining "Davlat sirlari saqlash to'g'risida"gi qonunning nechanchi moddasida keltirilgan? 2-modda 1-modda 4-modda 8-modda +++++ O'zbekiston Respublikasi davlat sirlari nechiga bo'linadi? 3 2 4 5 +++++ Mulk egasiga mavjud yoki ehtimoliy sharoitlarda daromadlarni ko'paytirishga, ortiqcha xarajatlarni qoplamaslikka, tovarlar, ishlar, xizmatlar uchun bozorda pozitsiyani saqlab qolish yoki boshqa tijorat manfaatlariga ega bo'lish imkonini beradigan ma'lumotla Tijorat siri Kasbiy maxfiylik Davlat sirlari Xizmat sirlari +++++ "Barcha odamlar erkin va teng xuquqqa egadirlar va xuquqlari bilan tengdirlar".Maxfiylik xuquqi konstitutsiyaviy inson xuquqlaridan biridir. Ushbu ta'rif "Inson xuquqlari umumjahon deklaratsiyasi" ning nechanchi moddasida keltirilgan? 1 2 4 5 Manba: +++++ Biografik va identifikatsiya ma'lumotlari ( tug'ilish, asrab olish, ajralish), qanday axborot turiga kiradi? Shaxsiy sirlar Aloqa sirlari Davlat sirlar Kasbiy maxfiylik +++++ Obyektlarni o'zaro aloqasini, tuzilishini, qiymatini, kerakli xossalarni va sabablarini o'rganishdagi farazlar qanday model hisoblanadi? Buzg'unchining gipotetik modeli Axborot xavfsizligini buzuvchining modellari Xavfsizlik modellarini tashkil etish modeli T.J.Y modeli +++++ Sabablar, maqsadlar va usullarga bog'liq holda axborot xavfsizligini buzuvchilaridan nechta kategoriyaga ajratiladi? 4 ta 3 ta 5 ta 6 ta +++++ Qanday hakerlar odatda yosh ko'pincha talaba yoki yuqori sinf o'quvchisi bo'ladi va unda o'ylab qilingan xujum rejasi kamdan-kam bo'ladi. U nishonni tasodifan tanlaydi, qiyinchiliklarga duch kelsa chekinadi? Sarguzasht qidiruvchi G'oyali hakerlar Ishonchsiz xodimlar Xakerlar-professionallar +++++ Qanday hakerlar o'zining etiqodi asosida muayyan nishonlarni (xostlar va resurslarni) tanlaydi. Uning yahshi ko'rgan xujumturi Web serverning axborotni o'zgartirishi va xujumlanuvchi resurslarini blokirovka qilish bo'ladi? G'oyali hakerlar Ishonchsiz xodimlar Xakerlar-professionallar Sarguzasht qidiruvchi +++++ Ximoyalangan axborot maqomini buzulishi axborotning nechta shaklini qo'llash orqali ifodalanadi? 6ta 4ta 7ta 5ta +++++ Ximoyalangan axborotga taxdidlarning mavjud bo'lishlik ko'rinishlari nech xil bo'ladi? 3 2 4 5 +++++ Axborotni uzatilishida beqarorlikni keltirib chiqaruvchi ta'sirlar omillarining tuzilishi necha xil? 4 3 5 6 +++++ "Konfedensial axborot ximoyasini tashkillashtirish tartibi konfedensial axborotni elementlar bilan ximoyalashni tashkil etish" to'g'risidagi nizom nechanchi sonli ro'yxat raqami bilan belgilanadi? 2081 2080 1980 2082 +++++ Konfedensiallikni saqlash va oshkor etmaslik to'g'risida kontraktlarga qo'yilgan talablarni belgilashda quyidagi qaysi jihatlarga amal qilish kerak? Aktivlarni boshqarish, xodimlarning xavfsizligi Konfedensial axborotdan foydalanishga ruxsat berishda kontrkatni imzolayotgan shaxsning majburiyatlari va xuquqlari Tashkilot uzluksiz ishining ta'minlanishini boshqarish Axborot tizimlarini sotib olish, ishlab chiqish va ularga xizmat ko'rsatish +++++ Shartnomaning amal qilish muddati to'xtatilgan xollarda qanday choralar ko'rish zarur? Kontrakt muddati tugagan xollarda axborot yo'qqilinishi yoki qaytarilishi kerak bo'lgan muddatlarni belgilash Xodimlarning xavfsizligini ta'minlash Foydalanishni boshqarish Axborot xavfsiligi

identifikatorlarini boshqarish ++++ Konfedensiallikka rioya qilish va oshkor etmaslik to'g'risidagi shartnomalar nima uchun mo'ljallangan? Tashkilot axborot aktivlarini muhofaza qilish Axborot xavfsizligini ta'minlash Jismoniy xavfsizlik va atrof-muhit xavfsizligini ta'minlash Xodimlarning xavfsizligini ta'minlash ++++ Avtorizatsiya qilingan foydalanuvchilarning foydalanishini cheklash uchun operatsion tizim darajasida axborot xavfsizligi vositalarini necha turga bo'lish kerak? 6 5 4 3 ++++ Tizimga xavfsiz kirish tartibi nechiga bo'linadi? 2 4 5 3 ++++ Axborot servislaridan foydalanish tizimiga xavfsiz kirish prodsedurasidan foydalanish yordamida ta'minlangan bo'lishi bu? Tizimga xavfsiz kirish tartibi Avtorizatsiya qilingan foydalanuvchi Parollarni boshqarish tizimi Axborotdan foydalanishni cheklash ++++ Qanday xakerlar harakatning aniq rejasiga ega va ma'lum resurslarni mo'ljallaydi. Uning hujumlari yaxshi o'ylangan va odatda birnecha bosqichda amalga oshiriladi? Xakerlar-professionallar Sarguzasht qidiruvchi G'oyali hakerlar Ishonchsiz xodimlar ++++ Huquqiy boshqarish haqida ma'lumot nimani anglatadi Har qanday axborot, muallifning, asarni yoki asardan foydalanish shartlari to'g'risidagi ma'lumotni har qanday raqamlar yoki kodlarni aniqlaydi har qanday axborot, muallifni aniqlaydi asardan foydalanish shartlari to'g'risidagi ma'lumotlar har qanday raqam yoki kodlar ++++ Mualliflik huquqini himoya qilish belgisi Bir doira ichida lotin harfidan "C" istisno mulk egasining nomi (nomlanishi) mulkiy huquqlar , asarning birinchi nashr qilingan yili har qanday axborot, muallifni aniqlaydi asardan foydalanish shartlari to'g'risidagi ma'lumotlar har qanday raqam yoki kodlar ++++ Mualliflik huquqi boshqa davlatda tan olinadimi? xalqaro shartnomaga muvofiq ushbu huquq tan olinadi. xalqaro shartnoma mavjud bo'lmasa, bu huquq tan olinmaydi Hududiy xarakter tabiatiga bogliq Milliy xarakter tabiatiga bogliq ++++ Mualliflik huquqi quyidagilarga bo'linadi. shaxsiy mulk va mulkiy huquqlar shaxsiy mulk va jamoatchilik huquqlari axloqiy huquqlar shaxsiy mulk huquqi ++++ Rasmiy topshiriqlarni bajarish tartibida yaratilgan mulk huquqlariga kim egalik qiladi? agar u va uning muallifi o'rtasida tuzilgan shartnomada nazarda tutilgan bo'lsa, ish beruvchiga tegishlidir Muallif o'rtasidagi shartnoma aks etilmagan holda muallifning o'ziga tegishlidir ijarachiga tegishli Muallifga tegishli ++++ Mualliflikhuquqito'g'risidagibutunjahonkonvensiyasiqach onqabulqilingan ? 1952 yil 6 sentyabr 1954 yil 6 sentyabr 1972 yil16 oktyabr 1996 yil 26 dekabr ++++ Respublika mualliflik huquqini himoya qilish agentligining rasmiy sayti <http://ima.uz> <http://lcweb.loc.gov> <http://lcweb.loc.gov> <http://lcweb.ru> ++++ Axborot resurslarini muhofaza qilishning tizimli yondashuviga nima talab qilinadi? xavfsizlik masalalarini ta'minoti va hal qilish uchun muhim ahamiyatga ega bo'lgan barcha bir-biriga bog'liq, o'zaro ta'sirlashadigan va vaqtincha o'zgaruvchan elementlar, shartlar va omillarni ko'rib chiqish. tizimning o'zaro va davriy o'zgaruvchan elementlarini hisobga olish vaqt bo'yicha o'zgaruvchan elementlarni hisobga olish O'zaro hamkorlikva vaqt bo'yicha o'zgaruvchan elementlar va omillarni hisobga olish ++++ Axborot xavfsizligining asosiy tamoyillari. Tizimli, kompleksli, himoya qilishning uzluksizligi, oqilona etarlilik, boshqarish va qo'llanilish moslashuvchanligi , algoritmlarning ochiqqligi va himoya mexanizmlari , himoya choralari va vositalarini qo'llashning soddaligi Tizimli, kompleksli, himoya qilishning davomiyligi himoya choralari va vositalardan foydalanish qulayligi algoritmlarning ochiqqligi va muhofaza mexanizmlari ++++ Himoyani buzishga erisha olmaydigan tizimini yaratish mumkinmi? mumkin emas. deyarli mumkin himoyani tizimliligini inobatga olinsa Agar himoya choralari va vositalarini qo'llash qulayligi hisobga olinsa Algoritmlarning ochiqqligi printsipini va himoya mexanizmlarini hisobga olsak , asosan mumkin ++++ Himoya vositalarining himoya darajasini o'zgartirishi uchun nima bo'lishi kerak? tayinli moslashuvchan bo'lishi kerak Ommaviy bo'lishi kerak ma'lum bir xossalarga ega bo'lishi kerak ba'zi bir o'lchamlarga ega bo'lishi kerak ++++ Algoritmlarning ochiqqligi tamoyili va himoya mexanizmlarining mohiyati faqatgina tizimli tashkilotlarning sir tutilishi va uning quyi

tizimlarining ishlash algoritmlari sababli himoya qilish mumkin emas muhofazani faqat maxfiylik bilan ta'minlash mumkin emas strukturaviy tuzilma va algoritmlar tomonidan muhofaza qilinmasligi kerak murakkablik tufayli himoya qilish mumkin emas ++++ Baxtsiz hodisalar va tabiiy ofatlardan ko'riladigan zararni minimallashtirish nimalarga bogliq ob'ektning joylashishini to'g'ri tanlash; tabiiy ofatlar va baxtsiz hodisalar bilan shug'ullanish bo'yicha mutaxassislarni tayyorlash, ularning oqibatlarini bartaraf etish tizimning rivojlanishi va faoliyatida yuzaga kelishi mumkin bo'lgan baxtsiz hodisalar va tabiiy ofatlarni hisobga olgan holda yuzaga kelishi mumkin bo'lgan tabiiy ofatlarni bartaraf etish himoya usullarini to'g'ri tanlash ++++ Qaysi usul axborotning yaxlitligini ta'minlashning eng samarali usullaridan biridir Ma'lumotlarning takrorlanishi kodlash shifrlash Zichlashtirish ++++ Ma'lumotni tiklash vaqtida takrorlash usullari qanday farqlanishi mumkin? Tezkor va Tezkor bo'lmagan Strategik, taktik chaqqon uzoq muddatli ++++ o'paytirish usullari quyidagi usullarga bo'linadi. markazlashtirilgan takrorlash; tarqatilgan takrorlash Masofali takrorlash Mahalliy takrorlash Markazlashtirilgan takrorlash ++++ Axborot tizimlarining bardoshliligi Axborot tizimining ushbu funktsiyasi alohida jihozlar, bloklar, davrlarning ishlamay qolgan holatlarida ishlashni ta'minlaydi. bu axborot tizimining ishonchliligi bu axborot tizimining to'g'riligi bu axborot tizimining kengayishi ++++ Bardoshli tizimlarni qurishning asosiy yondashuvlari qaysilar? axborotni kodlashni bardoshli qilish; adaptiv tizimlarni yaratish zahiralash axborotni kodlash Shovqinga bardosh kodlash ++++ Standartlarni ishlatishga nima yordam beradi? axborot xavfsizligi ta'minotini maqsadi qat'iy belgilanadi Axborot xavfsizligini boshqarishning samarali tizimi mavjud emas Mavjud dasturiy vositalardan (dasturiy ta'minotdan) foydalanish shartlari yaratilmagan. axborot xavfsizligi va uning hozirgi holatini baholash ++++ Standartlashtirish ob'ektlarining turlari tizim (axborot, texnik, tashkiliy-texnologik, apparat, kriptografik va xokazo) AT mahsulotlari, AT texnologiyalar (shu jumladan jarayonlarni, muolajani) Axborot tizimi AT mahsulotlari AT texnologiyasi ++++ Muayyan hodisa yoki harakatlarning borligini isbotlash qobiliyati va ularni qo'llab quvvatlaydigan mantiqiy ob'ektlarni aniqlash ... rad etolmaslik butunlik muvofiqlik Audit ++++ Tashkilotning yuqori darajali boshqaruvi tomonidan rasmiy ravishda ifodalangan maqsad va vazifalari - bu ... siyosat strategiya reja Xatarlarni boshqarish ++++ Tizim holatining identifikasion korsatkichida xavfsizlik siyosatining buzilganligi aniqlangan xolati bu .... Axborot xavfsizligidagi holat axborot xavfsizligi intsidenti axborot xavfsizligiga tahdidi axborot xavfsizligi xavfi ++++ Xavf quyidagi elementlar bilan ifodalanishi mumkin (ortiqchasini olib tashlang): hodisa aktiv tahdid zaiflik ++++ AQSH mudofaa vazirligi kompyuter tizimlarini xavfsizligi mezonlariga qanday xavfsizlik toifalari taklif etiladi? xavfsizlik siyosati audit va to'g'ri boshqarish siyosati auditorlik va ishonchni ta'minlash bo'yicha ishonch siyosati auditorlik va to'g'riligini ta'minlash bo'yicha siyosat, audit va moslashuvchanlik ++++ Kompyuter himoyasi uchun antiotladkaning nechta usuli mavjud 5 ta 4 ta 3 ta 6 ta ++++ Otladchikning borligini tekshiruvchi o'rnatilgan funksiyalar qanday xususiyatga ega Antiotladkaning oddiy texnikasi o'ziga IsDebuggerPresent funksiyasini chaqirish xususiyatiga ega Antiotladkaning oddiy texnikasi o'ziga DebuggerPresent funksiyasini chaqirish xususiyatiga ega Antiotladkaning oddiy texnikasi o'ziga IsDebugger funksiyasini chaqirish xususiyatiga ega Antiotladkaning oddiy texnikasi o'ziga IsPresent funksiyasini chaqirish xususiyatiga ega ++++ Kompyuter himoyasi uchun antiotladkaning qaysi usulida ThreadHideDebugger nomli yangi flagga ega bo'ladi Otladchikning borligini tekshiruvchi o'rnatilgan funksiyalar usuli Potoklarni yashirish usuli Flaglarni tekshirish usuli To'xtash nuqtalarini aniqlash usuli ++++ Trassirovka mexanizmini ishga tushirishdagi Tracerning nechta rejimi mavjud? 3 ta 2 ta 4 ta 5 ta ++++ Trassirovka mexanizmini ishga tushirishdagi Tracerning oddiy(normal) rejimi bu ....? Standart rejim, barcha foydalanuvchi dasturlari uchun trassirovka rejimini yoqadi

O'chirish ishlovchilaridan tashqari butun dastur uchun trassirovka rejimini yoqadi Chiqarish operatorlari uchun iz rejimini yoqadi Chiqarish operatorlari uchun sozlash rejimini yoqadi ++++ Trassirovka mexanizmini ishga tushirishdagi Tracerning asosiy dastur trassirovkasi (Trace Main) rejimi bu ....? O'chirish ishlovchilaridan tashqari butun dastur uchun trassirovka rejimini yoqadi Chiqarish operatorlari uchun iz rejimini yoqadi Chiqarish operatorlari uchun sozlash rejimini yoqadi Standart rejim, barcha foydalanuvchi dasturlari uchun trassirovka rejimini yoqadi ++++ Trassirovka mexanizmini ishga tushirishdagi Tracerning uzluksiz ishlovlar trassirovkasi (Trace INT) rejimi bu ....? Chiqarish operatorlari uchun iz rejimini yoqadi. Standart rejim, barcha foydalanuvchi dasturlari uchun trassirovka rejimini yoqadi. O'chirish ishlovchilaridan tashqari butun dastur uchun trassirovka rejimini yoqadi Chiqarish operatorlari uchun sozlash rejimini yoqadi ++++ Windows operatsion tizimidagi driverlarning saqlanish joyi? Windowsda qurilma Driverlari C: WINDOWS\SYSTEM32 katalogida saqlanadi. Windowsda qurilma Driverlari C: WINDOWS\ADMIN katalogida saqlanadi Windowsda qurilma Driverlari C: WINDOWS\FILE katalogida saqlanadi. Windowsda qurilma Driverlari C: WINDOWS\ROOT katalogida saqlanadi. ++++ Driver so'zining ma'nosi? Haydovchi. Sozlovchi Boshqaruvchi Ma'mur ++++ Kirishni cheklash tizimi nechta funksional blokdan iborat? 4 ta 5 ta 3 ta 2 ta ++++ Kirishni cheklash tizimining birinchi funksional bloki bu ? subyektlarga ruxsat berish bloki===== ruxsatni boshqarish dispetcheri apparat-dasturiy mexanizmlardan foydalangan holda yaratilgan bo'lib yetarli darajadagi subyektlarni obyektlarga ruxsatini cheklash bloki. ===== dasturni saqlash va uzatishda kriptografik qayta ishlash bloki. ===== xotirani tozalash bloki. ++++ Kirishni cheklash tizimining ikkinchi funksional bloki bu? ===== ruxsatni boshqarish dispetcheri apparat-dasturiy mexanizmlardan foydalangan holda yaratilgan bo'lib yetarli darajadagi subyektlarni obyektlarga ruxsatini cheklash bloki===== subyektlarga ruxsat berish bloki. ===== dasturni saqlash va uzatishda kriptografik qayta ishlash bloki===== xotirani tozalash bloki. ++++ Kirishni cheklash tizimining uchinchi funksional bloki bu? ===== dasturni saqlash va uzatishda kriptografik qayta ishlash bloki. ===== xotirani tozalash bloki. ===== subyektlarga ruxsat berish bloki===== ruxsatni boshqarish dispetcheri apparat-dasturiy mexanizmlardan foydalangan holda yaratilgan bo'lib yetarli darajadagi subyektlarni obyektlarga ruxsatini cheklash bloki ++++ Kirishni cheklash tizimining to'rtinchi funksional bloki bu? ===== xotirani tozalash bloki. ===== ruxsatni boshqarish dispetcheri apparat-dasturiy mexanizmlardan foydalangan holda yaratilgan bo'lib yetarli darajadagi subyektlarni obyektlarga ruxsatini cheklash bloki===== subyektlarga ruxsat berish bloki===== dasturni saqlash va uzatishda kriptografik qayta ishlash bloki. ++++ Shadow Defender bu - ? ===== Operatsion tizimni soya rejimida ishga tushiruvchi vazifasini bajaradigan va barcha bajarilgan amallar keyin windows OT qayta ishga tushurilgunga qadar qattiq diskda saqlab turish imkonini beradigan dastur===== Operatsion tizimni soya rejimida ishga tushiruvchi vazifasini bajaradigan va barcha bajarilgan amallar keyin windows OT qayta ishga tushurilgunga qadar o'chirib turish imkonini beradigan dastur===== Operatsion tizimni ish rejimini monitoring qilish imkonini beradigan dastur===== Operatsion tizimni faqat admin rejimida ishga tushirish imkonini beradigan dastur ++++ Shadow defender ..... himoyalovchi rejim ham deb ataladi===== "Soya rejimi" ===== "Mehmon rejimi" ===== "Admin rejimi" ===== "Kuzatuvchi rejimi" ++++ Ochiq kodli dasturiy taminot bu? ===== dasturiy ta'minotni ishlab chiqarishning shunday usuliki, unda dasturlarning yaratilayotgan dastlabki kodi ochiq ya'ni barcha ko'rib chiqishi va o'zgartirish kiritishi uchun ochiq bo'ladi. ===== dasturiy ta'minotni ishlab chiqarishning shunday usuliki, unda dasturlarning yaratilayotgan dastlabki kodi yopiq bo'ladi===== o'zgartirish imkoni bo'lmagan dasturiy ta'minot===== Litsensiyaga ega bo'lgan o'zgartirish imkoni bo'lmagan dasturiy ta'minot ++++ Yopiq kodli dasturiy ta'minot bu ? ===== o'z nomi bilan asos kodi yopiq bolgan dasturiy

ta'minot==== dasturiy ta'minotni ishlab chiqarishning shunday usuliki, unda dasturlarning yaratilayotgan dastlabki kodi ochiq bo'ladi==== o'zgartirish imkoni faqat litsenziya asosidagi dasturiy ta'minot==== Litsenziyaga ega va o'zgartirish imkoni bo'lgan dasturiy ta'minot ++++ Universal grafika bu ? ==== Windows dasturlarning qurilmalarga va dastur ta'minotiga bog'liqsizligini ta'minlaydi==== Operatsion tizimdagi dasturlar interfeysi==== Windows dasturlarni internet orqali yangilash vazifasini bajarish grafikasi. ==== Umumiy qoidalar to'plami ++++ Yagona interfeys bu? ==== Windowsda foydalanuvchining muloqoti yagona, ya'ni turli dasturlar bilan ishlash qoidalari umumiy bo'lgan interfeysdir==== Windows dasturlarni internet orqali yangilash vazifasini bajarish grafikasi==== Umumiy qoidalar to'plami==== Operatsion tizimdagi dasturlar interfeysi ++++ Operatsion tizimning ko'p masalaliligi bu ? ==== Operatsion tizimning dasturlararo ma'lumot almashish imkoniga ega ekanligidir. ==== Operatsion tizimning faqat internet orqali ma'lumot almashish imkoniga ega ekanligidir==== Operatsion tizimning qo'shimcha imkoniyat qo'shish imkoniga ega ekanligidir. ==== Operatsion tizimning ochiq kodli dasturlarni qo'llab - quvvatlash imkoniga ega ekanligidir ++++ DDE nima ? ==== Dinamic Data Exchange - ma'lumotlarning dinamik almashinuvi. ==== Dinamic Datetime Exchange - ma'lumotlarning dinamik almashinuvi==== Dinamic Diagram Exchange - diagrammalarni dinamik almashinuvi ==== Dinamic Delete Exchange – o'chirishlarni dinamik almashinuvi ++++ Axborot jamiyati bu ?==== bu axborot iqtisodiyoti paradigmasi doirasida faoliyat yuritadigan jamiyat==== bu axborot siyosati paradigmasi doirasida faoliyat yuritadigan jamiyat==== bu axborotlashgan jamiyat==== paradigma doirasida faoliyat yuritadigan internetsiz jamiyat ++++ Komyuter etikasi bu ? fanlararo tadqiqotlar sohasi bo'lib, texnik, axloqiy, huquqiy, ijtimoiy, siyosiy va falsafiy masalalarni ko'rib chiqishni o'z ichiga oladi fanlararo tadqiqotlar sohasi bo'lib, texnik, axloqiy, huquqiy, ijtimoiy, siyosiy va falsafiy masalalarni ko'rib chiqishni o'z ichiga oladi==== siyosiy masalalarni ko'rib chiqishni o'z ichiga oladi==== falsafiy masalalarni ko'rib chiqishni o'z ichiga oladi ++++ IFIP nima ? ==== International Federation for Information Processing ya'ni Xalqaro axborotni qayta ishlash federatsiyasi==== International Federation for Information Press ya'ni Xalqaro axborotni nashr etish federatsiyasi==== International Federation for Information Protect ya'ni Xalqaro axborotni himoyalash federatsiyasi==== International Federation for Information Private ya'ni Xalqaro axborotni maxfiylash federatsiyasi I: S:Axborot xavfsizligining asosiy maqsadlaridan biribu... +:Axborotlarni o'g'irlanishini, yo'qolishini, soxtalashtirishini oldini olish -:Ob'ektga bevosita ta'sir qilish -:Axborotlarni shifrlash, saqlash, yetkazib berish -:Tarmoqdagi foydalanuvchilarni xavfsizligini ta'minlab berish I: S:Konfidentsiallikga to'g'ri ta'rif keltirg. +:axborot inshonchiligi, tarqatilishi mumkin emasligi, maxfiyligi kafolati; -:axborot konfidentsialligi, tarqatilishi mumkinligi, maxfiyligi kafolati; -:axborot inshonchliligi, tarqatilishi mumkin emasligi, parollanganligi kafolati; -:axborot inshonchililigi, axborotlashganligi, maxfiyligi kafolati; I: S:Yaxlitlikni buzilishi bu - ... +:Soxtalashtirish va o'zgartirish -:Ishonchsizlik va soxtalashtirish -:Soxtalashtirish -:Butunmaslik va yaxlitlanmaganlik I: S:Kompyuter virusi nima? +:Maxsus yozilgan va zararli dastur -: .exe fayl -:Boshqariluvchi dastur -:Kengaytmaga ega bo'lgan fayl I: S:Axborotni himoyalash uchun qanday usullar qo'llaniladi? +:Kodlashtirish, kriptografiya, stegonografiya -:Kodlashtirish va kriptografiya, maxsus yozilgan kod -:Stegonografiya, kriptografiya, orfografiya -:Kriptografiya, kodlashtirish, sintaksis I: S:Kriptografiyaning asosiy maqsadi... +:maxfiylik, yaxlitlikni ta'minlash -:ishonchlilik, butunlikni ta'minlash -:autentifikatsiya, identifikatsiya -:ishonchlilik, butunlikni ta'minlash, autentifikatsiya, identifikatsiya I: S:SMTP - Simple Mail Transfer protokol nima? +:elektron pochta protokoli -:transport protokoli -:internet protokoli -:Internetda ommaviy tus olgan dastur I: S:Kompyuter tarmog'ining asosiy komponentlariga nisbatan xavf-xatarlar... +:uzilish, tutib qolish, o'zgartirish,

soxtalashtirish -:o'zgartirish, soxtalashtirish -:tutib qolish, o'zgarish, uzilish -:soxtalashtirish, uzilish, o'zgartirish I: S:...ma'lumotlar oqimini passiv hujumlardan himoya qilishga xizmat qiladi.

+:konfidentsiallik -:identifikatsiya -:autentifikatsiya -:maxfiylik I: S:Foydalanish huquqini cheklovchi matritsa modeli bu... +:Bella La-Padulla modeli -:Dening modeli -:Landver modeli -:Huquqlarni cheklovchi model I: S:Kalit – bu ... +:Matnni shifrlash va shifrini ochish uchun kerakli axborot -:Bir qancha kalitlar yig'indisi -:Axborotli kalitlar to'plami -:Belgini va raqamlarni shifrlash va shifrini ochish uchun kerakli axborot I: S:Qo'yish, o'rin almashtirish, gammalash kriptografiyaning qaysi turiga bog'liq? +:simmetrik kriptotizimlar -:assimetrik kriptotizimlar -:ochiq kalitli kriptotizimlar -:autentifikatsiyalash I: S:Autentifikatsiya nima? +:Ma'lum qilingan foydalanuvchi, jarayon yoki qurilmaning haqiqiy ekanligini tekshirish muolajasi -:Tizim me'yoriy va g'ayritabiiy hollarda rejalashtirilgandek o'zini tutishligi holati -:Istalgan vaqtda dastur majmuasining mumkinligini kafolati -:Tizim noodatiy va tabiiy hollarda qurilmaning haqiqiy ekanligini tekshirish muolajasi I: S:Identifikatsiya bu- ... +:Foydalanuvchini uning identifikatori (nomi) bo'yicha aniqlash jarayoni -:Ishonchliligini tarqalishi mumkin emasligi kafolati -:Axborot boshlang'ich ko'rinishda ekanligi uni saqlash, uzatishda ruxsat etilmagan o'zgarishlar -:Axborotni butunligini saqlab qolgan holda uni elementlarini o'zgartirishga yo'l qo'ymaslik I: S:O'rin almashtirish shifri bu - ... +:Murakkab bo'lmagan kriptografik akslantirish -:Kalit asosida generatsiya qilish -:Ketma-ket ochiq matnni ustiga qo'yish -:Belgilangan biror uzunliklarga bo'lib chiqib shifrlash I: S:Simmetrik kalitli shifrlash tizimi necha turga bo'linadi. +:2 turga -:3 turga -:4 turga -:5 turga S:Kriptografiyada matn –bu.. +:alifbo elementlarining tartiblangan to'plami -:matnni shifrlash va shifrini ochish uchun kerakli axborot -:axborot belgilarini kodlash uchun foydalaniladigan chekli to'plam -:kalit axborotni shifrlash uchun kalitlar I: S:Kriptoanaliz –bu.. +:kalitlarni bilmasdan shifrnı ochishga bardoshlilikni aniqlash uchun shifrlash tavsifi -:axborotni qayta akslantirishning matematik usullarini izlaydi va tadqiq qiladi -:axborotni qayta akslantirib himoyalash muammosi bilan shug'ullanadi -:kalitni bilmasdan shifrlangan matnnı ochish imkoniyatlarini o'rganadi I: S:Shifrlash atamasini belgilang. +:akslantirish jarayoni ochiq matn deb nomlanadigan matn shifrmatnga almashtiriladi -:kalit asosida shifrmatn ochiq matnga akslantiriladi -:shifrlashga teskari jarayon -:Almashtirish jarayoni bo'lib: ochiq matn deb nomlanadigan matn o'girilgan holatga almashtiriladi I: S:Blokli shifrlash tushunchasi nima? +:shifrlanadigan matn blokiga qo'llaniladigan asosiy akslantirish -:murakkab bo'lmagan kriptografik akslantirish -:axborot simvollarini boshqa alfavit simvolları bilan almashtirish -:ochiq matnning har bir harfi yoki simvoli alohida shifrlanishi I: S:Simmetrik kriptotizimning uzluksiz tizimida ... +:ochiq matnning har bir harfi va simvoli alohida shifrlanadi -:belgilangan biror uzunliklarga teng bo'linib chiqib shifrlanadi -:murakkab bo'lmagan kriptografik akslantirish orqali shifrlanadi -:ketma-ket ochiq matnlarnı o'rniga qo'yish orqali shifrlanadi I: S:Kriptotizimga qo'yiladigan umumiy talablardan biri nima? +:shifr matn uzunligi ochiq matn uzunligiga teng bo'lishi kerak -:shifrlash algoritmining tarkibiy elementlarini o'zgartirish imkoniyati bo'lishi lozim -:ketma-ket qo'llaniladigan kalitlar o'rtasida oddiy va oson bog'liqlik bo'lishi kerak -:maxfiylik o'ta yuqori darajada bo'lmoqligi lozim I: S:Berilgan ta'riflardan qaysi biri asimmetrik tizimlarga xos? +:Asimmetrik kriptotizimlarda  $k_1 \neq k_2$  bo'lib,  $k_1$  ochiq kalit,  $k_2$  yopiq kalit deb yuritiladi,  $k_1$  bilan axborot shifrlanadi,  $k_2$  bilan esa deshifrlanadi -:Asimmetrik tizimlarda  $k_1 = k_2$  bo'ladi, ya'ni  $k$  – kalit bilan axborot ham shifrlanadi, ham deshifrlanadi -:Asimmetrik kriptotizimlarda yopiq kalit axborot almashinuvining barcha ishtirokchilariga ma'lum bo'ladi, ochiq kalitni esa faqat qabul qiluvchi biladi -:Asimmetrik kriptotizimlarda  $k_1 \neq k_2$  bo'lib, kalitlar hammaga oshkor etiladi I: S:Yetarlicha kriptoturg'unlikka ega, dastlabki matn simvollarini almashtirish uchun bir necha alfavitdan foydalanishga asoslangan almashtirish usulini belgilang. +:Vijener matritsasi, Sesar usuli -



:Monoalfavitli almashtirish -:Polialfavitli almashtirish -:O'rin almashtirish I: S:Simmetrik guruh deb nimaga aytiladi? +:O'rin almashtirish va joylashtirish -:O'rin almashtirish va solishtirish - :Joylashtirish va solishtirish -:O'rin almashtirish va transportizatsiyalash I: S:Qo'yish, o'rin almashtirish, gammalash kriptografiyaning qaysi turiga bog'liq? +:simmetrik kriptosistemalar -:assimetrik kriptosistemalar -:ochiq kalitli kriptosistemalar -:autentifikatsiyalash I: S:Xavfli viruslar bu - ... +:kompyuter ishlashida jiddiy nuqsonlarga sabab bo'luvchi viruslar -:tizimda mavjudligi turli taassurot (ovoz, video) bilan bog'liq viruslar, bo'sh xotirani -kamaytirsada, dastur va ma'lumotlarga ziyon yetkazmaydi -:o'z-o'zidan tarqalish mexanizmi amalga oshiriluvchi viruslar -:dastur va ma'lumotlarni buzilishiga hamda kompyuter ishlashiga zarur axborotni o'chirilishiga bevosita olib keluvchi, muolajalari oldindan ishlash algoritmlariga joylangan viruslar I: S:Elektron raqamli imzo tizimi qanday muolajalarni amalga oshiradi? +:raqamli imzoni shakllantirish va tekshirish muolajasi -:raqamli imzoni hisoblash muolajasi -:raqamli imzoni hisoblash va tekshirish muolajasi -:raqamli imzoni shakllantirish muolajasi I: S:Shifrlashning kombinatsiyalangan usulida qanday kriptotizimlarning kriptografik kalitlaridan foydalaniladi? +:Simmetrik va assimetrik -:Simmetrik -:Assimetrik, chiziqli -:Gammalashgan, simmetrik, assimetrik I: S:Axborot himoyasi nuqtai nazaridan kompyuter tarmoqlarini nechta turga ajratish mumkin? +:Korporativ va umumfoydalanuvchi -:Regional, korporativ -:Lokal, global -:Shaharlararo, lokal, global I: S:Shaxsning, o'zini axborot kommunikatsiya tizimiga tanishtirish jarayonida qo'llaniladigan belgilar ketmaketligi bo'lib, axborot kommunikatsiya tizimidan foydalanish huquqiga ega bo'lish uchun foydalaniluvchining maxfiy bo'lmagan qayd yozuvi – bu... +:login parol -:identifikatsiya -:maxfiy maydon -:token I: S:Uning egasi haqiqiylikni aniqlash jarayonida tekshiruv axboroti sifatida ishlatiladigan belgilar ketma-ketligi (maxfiy so'z) – nima? +:parol -:login -:identifikatsiya -:maxfiy maydon foydalanuvchilarni ro'yxatga olish va ularga dasturlar va ma'lumotlarni ishlatishga huquq berish jarayoni I: S:Identifikatsiya jarayoni qanday jarayon? +:axborot tizimlari obyekt va subhektlariga uni tanish uchun nomlar (identifikator) berish va berilgan nom bo'yicha solishtirib uni aniqlash jarayoni -:ob'ekt yoki subhektni unga berilgan identifikatorga mosligini tekshirish va belgilar ketmaketligidan iborat maxfiy kodini tekshirish orqali aslligini aniqlash -:foydalanuvchining resursdan foydalanish huquqlari va ruxsatlarini tekshirish jarayoni -:foydalanuvchilarni ro'yxatga olish va ularga dasturlar va ma'lumotlarni ishlatishga huquq berish jarayoni I: S:Autentifikatsiya jarayoni qanday jarayon? +:ob'ekt yoki subhektni unga berilgan identifikatorga mosligini tekshirish va belgilar ketmaketligidan iborat maxfiy kodini tekshirish orqali aslligini aniqlash -:axborot tizimlari obyekt va subhektlariga uni tanish uchun nomlar (identifikator) berish va berilgan nom bo'yicha solishtirib uni aniqlash jarayoni -:foydalanuvchining resursdan foydalanish huquqlari va ruxsatlarini tekshirish jarayoni -:foydalanuvchilarni ro'yxatga olish va ularga dasturlar va ma'lumotlarni ishlatishga huquq berish jarayoni I: S:Ro'yxatdan o'tish-bu... +:foydalanuvchilarni ro'yxatga olish va ularga dasturlar va ma'lumotlarni ishlatishga huquq berish jarayoni -:axborot tizimlari ob'yekt va subhektlariga uni tanish uchun nomlar (identifikator) berish va berilgan nom bo'yicha solishtirib uni aniqlash jarayoni -:ob'ekt yoki subhektni unga berilgan identifikatorga mosligini tekshirish va belgilar ketma-ketligidan iborat maxfiy kodini tekshirish orqali aslligini aniqlash -:foydalanuvchining resursdan foydalanish huquqlari va ruxsatlarini tekshirish jarayoni I: S:Axborot qanday sifatlarga ega bo'lishi kerak? +:ishonchli, qimmatli va to'liq -:uzluksiz va uzlukli -:ishonchli, qimmatli va uzlukli -:ishonchli, qimmatli va uzluksiz I: S:Axborotning eng kichik o'lchov birligi nima? +:bit -:kilobayt -:bayt -:bitta simvol I: S:Axborotlarni saqlovchi va tashuvchi vositalar qaysilar? +:USB fleshka, CD va DVD disklar -:Qattiq disklar va CDRom -:CD va DVD, kesh xotira -:Qattiq disklar va DVDROM I: S:Avtorizatsiya jarayoni qanday jarayon? +:foydalanuvchining

resursdan foydalanish huquqlari va ruxsatlarini tekshirish jarayoni -:axborot tizimlari obyekt va subhektlariga uni tanish uchun nomlar (identifikator) berish va -berilgan nom bo'yicha solishtirib uni aniqlash jarayoni -:ob'ekt yoki subhektning unga berilgan identifikatorga mosligini tekshirish va belgilar ketma-ketligidan iborat maxfiy kodini tekshirish orqali aslligini aniqlash. -:parollash jarayoni I: S:Imzo bu nima? +:hujjatning haqiqiylikini va yuborgan fizik shaxsga tegishli ekanligini tasdiqlaydigan insonning fiziologik xususiyati. -:elektron hujjatlarning haqiqiylik va butunligini nazorat qilishni ta'minlovchi bo'lgan qo'yilgan imzoning analogi -:hujjatning haqiqiylikini va biror bir yuridik shaxsga tegishli ekanligini tasdiqlovchi isbotdir. -:hujjatda elektron raqamli imzoni yaratish uchun mo'ljallangan belgilar ketma-ketligi; I: S:Sezarning shifrlash sistemasining kamchiligi nimada? +:Harflarning so'zlarda kelish chastotasini yashirmaydi -:Alfavit tartibining o'zgarmasligi -:Kalitlar sonining kamchiligi -:Shifrttekstni ochish osonligi I: S:Axborot xavfsizligi va xavfsizlik san'ati haqidagi fan .... deyiladi. +:Kriptografiya -:Kriptotahlil -:Kriptologiya -:Kriptoanalitik I: S:Tekstni boshqa tekst ichida ma'nosini yashirib keltirish bu - ... +:steganografiya -:sirli yozuv -:skrembler -:rotor mashinalar I: S:Shifrttekstni ochiq tekstga akslantirish jarayoni nima deb ataladi? +:Deshifrlash -:Xabar -:Shifrlangan xabar -:Shifrlash I: S:.....-hisoblashga asoslangan bilim sohasi bo'lib, buzg'unchilar mavjud bo'lgan sharoitda amallarni kafolatlash uchun o'zida texnologiya, inson, axborot va jarayonni mujassamlashtirgan. +:Kiberxavfsizlik -:Axborot xavfsizligi -:Kiberjtnoyatchilik -:Risklar I: S:Risk nima? +:Potensial foyda yoki zarar -:Potensial kuchlanish yoki zarar -:Tasodifiy taxdid -:Katta yo'qotish I: S:Tahdid nima? +:Tashkilotga zarar yetkazishi mumkin bo'lgan istalmagan hodisa -:Tashkilot uchun qadrlil bo'lgan ixtiyoriy narsa -:Bu riskni o'zgartiradigan harakatlar bo'lib -:Bu noaniqlikning maqsadlarga ta'siri I: S:Kodlash nima? +:Ma'lumotni osongina qaytarish uchun hammaga ochiq bo'lgan sxema yordamida ma'lumotlarni boshqa formatga o'zgartirishdir -:Ma'lumot boshqa formatga o'zgartiriladi, biroq uni faqat maxsus shaxslar qayta o'zgartirishi mumkin bo'ladi -:Ma'lumot boshqa formatga o'zgartiriladi, barcha shaxslar kalit yordamida qayta o'zgartirishi mumkin bo'ladi -:Maxfiy xabarni soxta xabar ichiga berkitish orqali aloqani yashirish hisoblanadi I: S:Shifrlash nima? +:Ma'lumot boshqa formatga o'zgartiriladi, biroq uni faqat maxsus shaxslar qayta o'zgartirishi mumkin bo'ladi -:Ma'lumotni osongina qaytarish uchun hammaga ochiq bo'lgan sxema yordamida ma'lumotlarni boshqa formatga o'zgartirishdir -:Ma'lumot boshqa formatga o'zgartiriladi, barcha shaxslar kalit yordamida qayta o'zgartirishi mumkin bo'ladi -:Maxfiy xabarni soxta xabar ichiga berkitish orqali aloqani yashirish hisoblanadi I: S:Axborotni shifrni ochish (deshifrlash) bilan qaysi fan shug'ullanadi? +:Kriptoanaliz -:Kartografiya -:Kriptologiya -:Adamar usuli I: S:Qaysi juftlik RSA algoritmining ochiq va yopiq kalitlarini ifodalaydi? +:{d, n} – yopiq, {e, n} – ochiq; -: {d, e} – ochiq, {e, n} – yopiq; -: {e, n} – yopiq, {d, n} – ochiq; -: {e, n} – ochiq, {d, n} – yopiq; I: S:Zamonaviy kriptografiya qanday bo'limlardan iborat? -:Elektron raqamli imzo; kalitlarni boshqarish -:Simmetrik kriptotizimlar; ochiq kalitli kriptotizimlar; +:Simmetrik kriptotizimlar; ochiq kalitli kriptotizimlar; Elektron raqamli imzo; kalitlarni boshqarish -:Simmetrik kriptotizimlar; ochiq kalitli kriptotizimlar; kalitlarni boshqarish I: S:Kompyuterning tashqi interfeysi deganda nima tushuniladi? +:kompyuter bilan tashqi qurilmani bog'lovchi simlar va ular orqali axborot almashinish qoidalari to'plamlari -:tashqi qurilmani kompyuterga bog'lashda ishlatiladigan ulovchi simlar -:kompyuterning tashqi portlari. -:tashqi qurilma bilan kompyuter o'rtasida axborot almashinish qoidalari to'plami I: S:Lokal tarmoqlarda keng tarqalgan topologiya turi qaysi? +:Yulduz -:Xalqa -:To'liqbog'langan -:Umumiy shina I: S:Ethernet kontsentratori qanday vazifani bajaradi? +:kompyuterdan kelayotgan axborotni qolgan barcha kompyuterga yo'naltirib beradi -:kompyuterdan kelayotgan axborotni boshqa bir kompyuterga yo'naltirib beradi -:kompyuterdan

kelayotgan axborotni xalqa bo'ylab joylashgan keyingi kompyuterga -:tarmoqning ikki segmentini bir biriga ulaydi I: S:OSI modelida nechta sath mavjud? +:7 ta -:4 ta -:5 ta -:3 ta I: S:Identifikatsiya, autentifikatsiya jarayonlaridan o'tgan foydalanuvchi uchun tizimda bajarishi mumkin bo'lgan amallarga ruxsat berish jarayoni bu... +:Avtorizatsiya -:Shifrlash -:Identifikatsiya -:Autentifikatsiya I: S:Autentifikatsiya faktorlari nechta? +:3 ta -:4 ta -:5 ta -:6 ta I: S:Ko'z pardasi, yuz tuzilishi, ovoz tembri-bular autentifikatsiyaning qaysi faktoriga mos belgilar? +:Biometrik autentifikatsiya -:Biron nimaga egalik asosida -:Biron nimani bilish asosida -:Parolga asoslangan I: S:Fizik xavfsizlikda Yong'inga qarshi tizimlar necha turga bo'linadi? +:2 taga -:4 taga -:3 taga -:5 taga I: S:Avtorizatsiya tushunchasi odatda qaysi tushuncha bilan sinonim sifatida ham foydalanadi? +:Foydalanishni boshqarish -:Foydalanish -:Tarmoqni loyixalash -:Identifikatsiya I: S:Foydalanishni boshqarish – bu... +:Sub'ektni Ob'ektga ishlash qobilyatini aniqlashdir. -:Sub'ektni Sub'ektga ishlash qobilyatini aniqlashdir. -:Ob'ektni Ob'ektga ishlash qobilyatini aniqlashdir -:Autentifikatsiyalash jarayonidir I: S:Foydalanishni boshqarishda inson, dastur, jarayon va hokazolar nima vazifani bajaradi? +:Sub'ekt -:Ob'ekt -:Tizim -:Jarayon I: S:Foydalanishna boshqarishda ma'lumot , resurs, jarayon nima vazifani bajaradi ? +:Ob'ekt -:Sub'ekt -:Tizim -:Jarayon I: S:MAC usuli bilan foydalanishni boshqarishda xavfsizlik markazlashgan holatda kim tomonidan amalga oshiriladi? +:Xavfsizlik siyosati ma'muri -:Foydalaguvchining o'zi -:Dastur tomonidan -:Boshqarish amaalgaga oshirilmaydi I: S:Agar Sub'ektning xavfsizlik darajasida Ob'ektning xavfsizlik darajasi mavjud bo'lsa, u holda uchun qanday amalga ruxsat beriladi? +:O'qish -:Yozish -:O'zgartirish -:Yashirish I: S:Agar Sub'ektning xavfsizlik darajasi Ob'ektning xavfsizlik darajasida bo'lsa, u holda qanday amalga ruxsat beriladi? +:Yozish -:O'qish -:O'zgartirish -:Yashirish I: S:Rol tushunchasiga ta'rif bering. +:Muayyan faoliyat turi bilan bog'liq harakatlar va majburiyatlar to'plami sifatida belgilanishi mumkin -:Foydalanishni boshqarish -:Muayyan faoliyat turi bilan bog'liq imkoniyatlar to'plami sifatida belgilanishi mumkin -:Vakolitlarni taqsimlash I: S:Foydalanishni boshqarishning qaysi usuli – Ob'ektlar va Sub'ektlarning atributlari, ular bilan mumkin bo'lgan amallar va so'rovlarga mos keladigan muhit uchun qoidalarni tahlil qilish asosida foydalanishlarni boshqaradi. +:ABAC -:MAC -:DAC -:RBAC I: S:Qanday tarmoq qisqa masofalarda qurilmalar o'rtasida ma'lumot almashinish imkoniyatini taqdim etadi? +:Shaxsiy tarmoq -:Lokal -:Mintaqaviy -:CAMPUS I: S:Tarmoq kartasi bu... +:Hisoblash qurilmasining ajralmas qismi bo'lib, qurilmani tarmoqqa ulash imkoniyatini taqdim etadi. -:Tarmoq repetiri odatda signalni tiklash yoki qaytarish uchun foydalaniladi. -:Ko'plab tarmoqlarni ulash uchun yoki LAN segmentlarini bog'lash uchun xizmat qiladi. -:Qabul qilingan signalni barcha chiquvchi portlarga emas balki paketda manzili keltirilgan portga uzatadi. I: S:Server xotirasidagi joyni bepul yoki pulli ijagara berish xizmati qanday ataladi? +:Qabul qilingan signalni barcha chiquvchi portlarga emas balki paketda manzili keltirilgan portga uzatadi. -:Hisoblash qurilmasining ajralmas qismi bo'lib, qurilmani tarmoqqa ulash imkoniyatini taqdim etadi. -:Signalni tiklash yoki qaytarish uchun foydalaniladi. -:Ko'plab tarmoqlarni ulash uchun yoki LAN segmentlarini bog'lash uchun xizmat qiladi. S:Imzoni haqiqiyligini tekshirish qaysi kalit yordamida amalga oshiriladi? +:Imzo muallifining ochiq kaliti yordamida -:Ma'lumotni qabul qilgan foydalanuvchining ochiq kaliti yordamida -:Ma'lumotni qabul qilgan foydalanuvchining maxfiy kaliti yordamida -:Imzo muallifining maxfiy kaliti yordamida I: S:Quyidagilardan lokal tarmoqqa berilgan ta'rifni belgilang. +:Kompyuterlar va ularni bog'lab turgan qurilmalardan iborat bo'lib, ular odatda bitta tarmoqda bo'ladi. -:Odatda ijaraga olingan telekommunikatsiya liniyalaridan foydalanadigan tarmoqlardagi tugunlarni bir-biriga bog'laydi. -:Bu tarmoq shahar yoki shaharcha bo'ylab tarmoqlarning o'zaro bog'lanishini nazarda tutadi -:Qisqa masofalarda qurilmalar o'rtasida ma'lumot almashinish imkoniyatini taqdim etadi I: S:Quyidagilardan mintaqaviy tarmoqqa

berilgan ta'rifni belgilang. +:Odatda ijaraga olingan telekommunikatsiya liniyalaridan foydalanadigan tarmoqlardagi tugunlarni birbiriga bog'laydi. -:Kompyuterlar va ularni bog'lab turgan qurilmalardan iborat bo'lib, ular odatda bitta tarmoqda bo'ladi. -:Bu tarmoq shahar yoki shaharcha bo'ylab tarmoqlarning o'zaro bog'lanishini nazarda tutadi -:Qisqa masofalarda qurilmalar o'rtasida ma'lumot almashinish imkoniyatini taqdim etadi. I: S:Repetir nima? +:Odatda signalni tiklash yoki qaytarish uchun foydalaniladi -:Tarmoq qurilmasi bo'lib, ko'plab tarmoqlarni ulash uchun yoki LAN segmentlarini bog'lash uchun xizmat qiladi -:Hisoblash qurilmasining ajralmas qismi bo'lib, qurilmani tarmoqqa ulash imkoniyatini taqdim etadi -:Ko'plab tarmoqlarni ulash uchun yoki LAN segmentlarini bog'lash uchun xizmat qiladi. Qabul qilingan signalni barcha chiquvchi portlarga emas balki paketda manzili keltirilgan portga uzatadi I: S:Hub nima? +:Tarmoq qurilmasi bo'lib, ko'plab tarmoqlarni ulash uchun yoki LAN segmentlarini bog'lash uchun xizmat qiladi -:Hisoblash qurilmasining ajralmas qismi bo'lib, qurilmani tarmoqqa ulash imkoniyatini taqdim etadi, Odatda signalni tiklash yoki qaytarish uchun foydalaniladi -:Ko'plab tarmoqlarni ulash uchun yoki LAN segmentlarini bog'lash uchun xizmat qiladi. -:Qabul qilingan signalni barcha chiquvchi portlarga emas balki paketda manzili keltirilgan portga uzatadi I: S:Router nima? +:Qabul qilingan ma'lumotlarni tarmoq sathiga tegishli manzillarga ko'ra (IP manzil) uzatadi. -:Tarmoq qurilmasi bo'lib, ko'plab tarmoqlarni ulash uchun yoki LAN segmentlarini bog'lash uchun xizmat qiladi Hisoblash qurilmasining ajralmas qismi bo'lib, qurilmani tarmoqqa ulash imkoniyatini taqdim etadi -:Ko'plab tarmoqlarni ulash uchun yoki LAN segmentlarini bog'lash uchun xizmat qiladi. -:Qabul qilingan signalni barcha chiquvchi portlarga emas balki paketda manzili keltirilgan portga uzatadi I: S:Asosan tarmoq, tizim va tashkilot haqidagi axborot olish maqsadda amalga oshiriladigan tarmoq hujumi qaysi +:Razvedka hujumlari -:Kirish hujumlari -:DOS hujumi -:Zararli hujumlar I: S:Razvedka hujumiga berilgan ta'rifni aniqlang +:Asosiy hujumlarni oson amalga oshirish uchun tashkilot va tarmoq haqidagi axborotni to'plashni maqsad qiladi; -:Hujumchi turli texnologiyalardan foydalangan holda tarmoqqa kirishga harakat qiladi hujumchi -:Mijozlarga, foydalanuvchilarga va tashkilotlarda mavjud bo'lgan biror xizmatni cheklashga urinadi; -:Zararli hujumlar tizim yoki tarmoqqa bevosita va bilvosita ta'sir qiladi; I: S:Antivirus dasturlarini ko'rsating? +:Drweb, Nod32, Kaspersky -:arj, rar, pkzip, pkunzip -:winrar, winzip, winarj -:pak, lha I: S:Wi-Fi tarmoqlarida quyida keltirilgan qaysi shifrlash protokollaridan foydalaniladi +:wep, wpa, wpa2 -:web, wpa, wpa2 -:wpa, wpa2 -:wpa, wpa2, wap I: S:Axborot himoyalangan qanday sifatlarga ega bo'lishi kerak? +:ishonchli, qimmatli va to'liq -:uzluksiz va uzlukli -:ishonchli, qimmatli va uzlukli -:ishonchli, qimmatli va uzluksiz I: S:Virtual xususiy tarmoqni qisqartmasini belgilang. +:VPN -:APN -:ATM -:Ad-hoc I: S:Fire Wall ning vazifasi... +:Tarmoqlar orasida aloqa o'rnatish jarayonida tashkilot va Internet tarmog'i orasida xavfsizlikni ta'minlaydi -:Kompyuterlar tizimi xavfsizligini ta'minlaydi -:Ikkita kompyuter o'rtasida aloqa o'rnatish jarayonida Internet tarmog'i orasida xavfsizlikni ta'minlaydi -:Uy tarmog'i orasida aloqa o'rnatish jarayonida tashkilot va Internet tarmog'i orasida xavfsizlikni ta'minlaydi I: S:Kompyuter virusi nima? +:maxsus yozilgan va zararli dastur -:exe fayl -:boshqariluvchi dastur -:Kengaytmaga ega bo'lgan fayl I: S:Kompyuterning viruslar bilan zararlanish yo'llarini ko'rsating +:disk, maxsus tashuvchi qurilma va kompyuter tarmoqlari orqali -:faqat maxsus tashuvchi qurilma orqali -:faqat kompyuter tarmoqlari orqali -:zararlanish yo'llari juda ko'p I: S:Troyan dasturlari bu... +:virus dasturlar -:antivirus dasturlar -:o'yin dasturlari -:yangilovchi dasturlar I: S:Stenografiya ma'nosi qanday? +:sirli yozuv -:sirli xat -:maxfiy axborot -:maxfiy belgi I: S:Kriptologiya yo'nalishlari nechta? +:2 -:3 -:4 -:5 I: S:Kriptografiyaning asosiy maqsadi nima? +:maxfiylik, yaxlitlilikni ta'minlash -:ishonchlilik, butunlilikni ta'minlash -:autentifikatsiya, identifikatsiya -:ishonchlilik, butunlilikni ta'minlash,

autentifikatsiya, identifikatsiya I: S:Shifrlash kaliti noma'lum bo'lganda shifrlangan ma'lumotni deshifrlash qiyinlik darajasini nima belgilaydi? +:Kriptobardoshlik -:Shifr matn uzunligi -:Shifrlash algoritmi -:Texnika va texnologiyalar I: S:Barcha simmetrik shifrlash algoritmlari qanday shifrlash usullariga bo'linadi? +:Blokli va oqimli -:DES va oqimli -:Feystel va Verman -:SP- tarmoq va IP I: S:Diskni shifrlash nima uchun amalga oshiriladi? +:Ma'lumotni saqlash vositalarida saqlangan ma'lumot konfidensialligini ta'minlash uchun amalga oshiriladi -:Xabarni yashirish uchun amalga oshiriladi -:Ma'lumotni saqlash vositalarida saqlangan ma'lumot butunligini ta'minlash uchun amalga oshiriladi -:Ma'lumotni saqlash vositalarida saqlangan ma'lumot foydalanuvchanligini ta'minlash uchun amalga oshiriladi I: S:Ma'lumotlarni yo'q qilish odatda necha xil usulidan foydalaniladi? +:4 xil -:8 xil -:7 xil -:5 xil I: S:Kiberjinoyatchilik bu -. . . +:Kompyuter yoki boshqa qurilmalarga qarshi qilingan yoki kompyuter va boshqa qurilmalar orqali qilingan jinoiy faoliyat. -:Kompyuter o'yinlari -:Faqat banklardan pul o'g'irlanishi -:Autentifikatsiya jarayonini buzish I: S:Fishing nima? +:Internetdagi firibgarlikning bir turi bo'lib, uning maqsadi foydalanuvchining maxfiy ma'lumotlaridan, login/parol, foydalanish imkoniyatiga ega bo'lishdir. -:Ma'lumotlar bazalarini xatoligi -:Mualliflik huquqini buzilishi -:Lug'at orqali xujum qilish. I: S:Nuqson nima? +:Dasturni amalga oshirishdagi va loyixalashdagi zaifliklarning barchasi nuqsondir -:Dasturiy ta'minotni amalga oshirish bosqichiga tegishli bo'lgan muammo -:Dasturlardagi ortiqcha reklamalar -:Autentifikatsiya jarayonini buzish I: S:Risklarni boshqarishda risklarni aniqlash jarayoni bu-.. +:Tashkilot xavfsizligiga ta'sir qiluvchi tashqi va ichki risklarning manbasi, sababi, oqibati va haklarni aniqlash. -:Risklarni baholash bosqichi tashkilotning risk darajasini baholaydi va risk ta'siri va ehtimolini o'lchashni ta'minlaydi. -:Risklarni davolash bu – aniqlangan risklar uchun mos nazoratni tanlash va amalga oshirish jarayoni. -:Risk monitoringi yangi risklarni paydo bo'lish imkoniyatini aniqlash. I: S:Tizim ishlamay turganda yoki foydalanuvchilar ma'lumot bilan ishlamay turganda zahiralash amalga oshirilsa .... deb ataladi. +:"Sovuq saxiralash" -:"Issiq zaxiralash" -:"Iliq saxiralash" -:"To'liq zaxiralash" I: S:Asimmetrik kriptotizimlarda axborotni shifrlashda va rasshifrovka qilish uchun nechta kalit ishlatiladi? +:Ikkita kalit -:Bitta kalit -:Elektron raqamli imzo -:Foydalanuvchi identifikatori I: S:Axborot xavfsizligiga bo'ladigan tahdidlarning qaysi biri maqsadli (atayin) tahdidlar deb hisoblanadi? +:Strukturalarni ruxsatsiz modifikatsiyalash -:Tabiiy ofat va avariya -:Texnik vositalarning buzilishi va ishlamasligi -:Foydalanuvchilar va xizmat ko'rsatuvchi hodimlarning hatoliklari} I: S:Axborot xavfsizligiga bo'ladigan tahdidlarning qaysi biri tasodifiy tahdidlar deb hisoblanadi? +:Texnik vositalarning buzilishi va ishlamasligi -:Axborotdan ruxsatsiz foydalanish -:Zararkunanda dasturlar -:An'anaviy josuslik va diversiya haqidagi ma'lumotlar tahlili} I: S:Axborotni uzatish va saqlash jarayonida o'z strukturasi va yoki mazmunini saqlash xususiyati nima deb ataladi? +:Ma'lumotlar butunligi -:Axborotning konfedentsialligi -:Foydalanuvchanligi -:Ixchamligi I: S:Axborotning buzilishi yoki yo'qotilishi xavfiga olib keluvchi himoyalannuvchi ob'ektga qarshi qilingan xarakatlar qanday nomlanadi? +:Tahdid -:Zaiflik -:Hujum -:Butunlik} I: S:Biometrik autentifikatsiyalashning avfzalliklari-bu: +:Biometrik parametrlarning noyobligi -:Bir marta ishlatilishi -:Biometrik parametrlarni o'zgartirish imkoniyati -:Autentifikatsiyalash jarayonining soddaligi I: S:Foydalanish huquqlariga (mualliflikka) ega barcha foydalanuvchilar axborotdan foydalana olishliklari-bu: +:Foydalanuvchanligi -:Ma'lumotlar butunligi -:Axborotning konfedensialligi -:Ixchamligi S:Simsiz tarmoqlarni kategoriyalarini to'g'ri ko'rsating? +:Simsiz shaxsiy tarmoq (PAN), simsiz lokal tarmoq (LAN), simsiz regional tarmoq (MAN) va Simsiz global tarmoq (WAN) -:Simsiz internet tarmoq (IAN )va Simsiz telefon tarmoq (WLAN), Simsiz shaxsiy tarmoq (PAN) va Simsiz global tarmoq (WIMAX) -:Simsiz internet tarmoq (IAN) va uy simsiz tarmog'i -:Simsiz chegaralanmagan tarmoq (LAN), simsiz kirish nuqtalari I: S:Sub'ektga ma'lum

vakolat va resurslarni berish muolajasi-bu: +:Avtorizatsiya -:Haqiqiylikni tasdiqlash -  
:Autentifikatsiya -:Identifikatsiya I: S:Tarmoq operatsion tizimining to'g'ri konfiguratsiyasini  
madadlash masalasini odatda kim hal etadi? +:Tizim ma'muri -:Tizim foydalanuvchisi -:Korxona  
raxbari -:Operator I: S:Tarmoqlararo ekran texnologiyasi-bu: +:Ichki va tashqi tarmoq o'rtasida filtr  
va himoya vazifasini bajaradi -:Ichki va tashqi tarmoq o'rtasida axborotni o'zgartirish vazifasini  
bajaradi -:Qonuniy foydalanuvchilarni himoyalash -:Ishonchsiz tarmoqdan kirishni boshqarish} I:  
S:Xizmat qilishdan voz kechishga undaydigan taqsimlangan hujum turini ko'rsating? +:DDoS  
(Distributed Denial of Service) hujum -:Tarmoq hujumlari -:Dastur hujumlari asosidagi (Denial of  
Service) hujum -:Virus hujumlari} I: S:Uyishtirilmagan tahdid, ya'ni tizim yoki dasturdagi  
qurilmaning jismoniy xatoligi – bu... +:Tasodifiy tahdid -:Uyishtirilgan tahdid -:Faol tahdid -:Passiv  
tahdid I: S:Axborot xavfsizligi qanday asosiy xarakteristikalariga ega? +:Butunlik, konfidentsiallik,  
foydalana olishlik -:Butunlik, himoya, ishonchlilikni urganib chiqishlilik -:Konfidentsiallik, foydalana  
olishlik -:Himoyalanganlik, ishonchlilik, butunlik I: S:Virtualashtirishga qaratilgan dasturiy  
vositalarni belgilang. +:VMware, VirtualBox -:HandyBakcup -:Eset32 -:Cryptool I: S:Cloud  
Computing texnologiyasi nechta katta turga ajratiladi? +:3 turga -:2 turga -:4 turga -:5 turga I:  
S:O'rnatilgan tizimlar-bu... +:Bu ko'pincha real vaqt hisoblash cheklovlariga ega bo'lgan kattaroq  
mexanik yoki elektr tizimidagi maxsus funksiyaga ega, boshqaruvchidir -:Korxona ichki tarmog'iga  
ulangan korporativ tarmog'idan bo'ladigan hujumlardan himoyalash -:Korxona ichki tarmog'ini  
Internet global tarmog'idan ajratib qo'yish -:Bu ko'pincha global tizimda hisoblash cheklovlariga  
ega bo'lgan mexanik yoki elektr tizimidagi maxsus funksiyaga ega qurilmadir I: S:Axborotdan  
oqilona foydalanish kodeksi qaysi tashkilot tomonidan ishlab chiqilgan? +:AQSH sog'liqni saqlash  
va insonlarga xizmat ko'rsatish vazirligi -:AQSH Mudofaa vazirligi -:O'zbekiston Axborot  
texnologiyalari va kommunikatsiyalarni rivojlantirish vazirligi -:Rossiya kiberjinoyatlarga qarshu  
kurashish davlat qo'mitasi I: S:Xizmat qilishdan voz kechishga undaydigan taqsimlangan hujum  
turini ko'rsating? +:Tarmoq hujumlari -:Dastur hujumlari asosidagi (Denial of Service) hujum -  
:Virus hujumlari -:Passiv hujum I: S:Token, Smartkartalarda xavfsizlik tomonidan kamchiligi nimada  
+:Qurilmani yo'qotilishi katta xavf olib kelishi mumkin -:Foydalanish davrida maxfiylik kamayib  
boradi -:Qurilmalarni ishlab chiqarish murakkab jarayon -:Qurilmani qalbakilashtirish oson I:  
S:Tarmoqlararo ekranlarning asosiy turlarini ko'rsating? +:Tatbiqiy sath shlyuzi, seans sathi shlyuzi,  
ekranlovchi marshrutizator -:Tatbiqiy sath shlyuzi, seans sathi shlyuzi, fizik sath shlyuzi -:Tatbiqiy  
sath shlyuzi, fizik sath shlyuzi, ekranlovchi marshrutizator -:Fizik sath shlyuzi, ekranlovchi  
marshrutizator, tahlillovchi marshrutizator I: S:Spam bilan kurashishning dasturiy uslubida nimalar  
ko'zda tutiladi? +:Elektron pochta qutisiga kelib tushadigan ma'lumotlar dasturlar asosida filtrlanib  
cheklanadi -:Elektron pochta qutisiga kelib tushadigan spamlar me'yoriy xujjatlar asosida  
cheklanadi va bloklanadi -:Elektron pochta qutisiga kelib tushadigan spamlar ommaviy ravishda  
cheklanadi -:Elektron pochta qutisiga kelib spamlar mintaqaviy hududlarda cheklanadi I:  
S:Ma'lumotlarni yo'qolish sabab bo'luvchi tabiiy tahdidlarni ko'rsating +:Zilzila, yong'in, suv  
toshqini va hak. -:Quvvat o'chishi, dasturiy ta'minot to'satdan o'zgarishi yoki qurilmani to'satdan  
zararlanishi -:Tashkilotdagi muhim ma'lumotlarni modifikatsiyalanishi yoki o'g'irlanishi -:Qasddan  
yoki tasodifiy ma'lumotni o'chirib yuborilishi, ma'lumotlarni saqlash vositasini to'g'ri  
joylashtirilmagani I: S:Ma'lumotlarni tasodifiy sabablar tufayli yo'qolish sababini belgilang  
+:Quvvat o'chishi, dasturiy ta'minot to'satdan o'zgarishi yoki qurilmani to'satdan zararlanishi -  
:Tashkilotdagi muhim ma'lumotlarni modifikatsiyalanishi yoki o'g'irlanishi -:Ma'lumotlarni saqlash  
vositasini to'g'ri joylashtirilmagani yoki ma'lumotlar bazasini xatolik bilan boshqarilganligi. -:Zilzila,  
yong'in, suv toshqini va hak I: S:Ma'lumotlarni inson xatosi tufayli yo'qolish sababini belgilang.

+:Ma'lumotlarni saqlash vositasini to'g'ri joylashtirilmagani yoki ma'lumotlar bazasini xatolik bilan boshqarilganligi. -:Tashkilotdagi muhim ma'lumotlarni modifikatsiyalanishi yoki o'g'irlanishi - :Quvvat o'chishi, dasturiy ta'minot to'satdan o'zgarishi yoki qurilmani to'satdan zararlanishi - :Zilzila, yong'in, suv toshqini va hak I: S:Ma'lumotlarni g'arazli hatti harakatlar yo'qolish sababini ko'rsating. +:Tashkilotdagi muhim ma'lumotlarni modifikatsiyalanishi yoki o'g'irlanishi -:Quvvat o'chishi, dasturiy ta'minot to'satdan o'zgarishi yoki qurilmani to'satdan zararlanishi - :Ma'lumotlarni saqlash vositasini to'g'ri joylashtirilmagani yoki ma'lumotlar bazasini xatolik bilan boshqarilganligi. -:Zilzila, yong'in, suv toshqini va hak I: S:Internet orqali masofada joylashgan kompyuterga yoki tarmoq resurslariga DoS hujumlari uyushtirilishi natijasida.. +:Foydalanuvchilar kerakli axborot resurlariga murojaat qilish imkoniyatidan mahrum qilinadilar - :Foydalanuvchilarning maxfiy axborotlari kuzatilib, masofadan buzg'unchilarga etkaziladi -:Axborot tizimidagi ma'lumotlar bazalari o'g'irlanib ko'lga kiritilgach, ular yo'q qilinadilar -:Foydalanuvchilar axborotlariga ruxsatsiz o'zgartirishlar kiritilib, ularning yaxlitligi buziladi I: S:"Parol", "PIN" kodlarni xavfsizlik tomonidan kamchiligi nimadan iborat? +:Foydalanish davrida maxfiylik kamayib boradi - :Parolni esda saqlash kerak bo'ladi -:Parolni almashtirish jarayoni murakkabligi -:Parol uzunligi soni cheklangan I: S:Yaxlitlikni buzilishi bu - ... +:Soxtalashtirish va o'zgartirish -:Ishonchsizlik va soxtalashtirish -:Soxtalashtirish -:Butunmaslik va yaxlitlanmaganlik I: S:Tarmoqda joylashgan fayllar va boshqa resurslardan foydalanishni taqdim etuvchi tarmoqdagi kompyuter nima? +:Server -:Bulutli tizim -:Superkompyuter -:Tarmoq I: S:Tahdid nima? +:Tizim yoki tashkilotga zarar yetkazishi mumkin bo'lgan istalmagan hodisa. -:Tashkilot uchun qadrli bo'lgan ixtiyoriy narsa -:Bu riskni o'zgartiradigan harakatlar bo'lib -:Bu noaniqlikning maqsadlarga ta'siri S:Fizik to'siqlarni o'rnatish , Xavfsizlik qo'riqchilarini ishga olish, Fizik qulflar qo'yishni amalga oshirish qanday nazorat turiga kiradi? +:Fizik nazorat -:Texnik nazorat -:Ma'muriy nazorat -:Tashkiliy nazorat I: S:Ruxsatlarni nazoratlash, "Qopqon", Yong'inga qarshi tizimlar, Yoritish tizimlari, Ogohlantirish tizimlari , Quvvat manbalari, Video kuzatuv tizimlari, Qurollarni aniqlash, Muhitni nazoratlash amalga oshirish qanday nazorat turiga kiradi? -:Fizik nazorat +:Texnik nazorat -:Ma'muriy nazorat -:Tashkiliy nazorat I: S:Qoida va muolajalarni yaratish, Joylashuv arxitekturasini loyihalash, Xavfsizlik belgilari va ogohlantirish signallari, Ishchi joy xavfsizligini ta'minlash, Shaxs xavfsizligini ta'minlash amalga oshirish qanday nazorat turiga kiradi? -:Fizik nazorat -:Texnik nazorat +:Ma'muriy nazorat -:Tashkiliy nazorat I: S:Ikkilik sanoq tizimida qanday raqamlardan foydalanamiz? +:Faqat 0 va 1 -:Faqat 1 -:Faqat 0 -:Barcha raqamlardan I: S:Yuliy Sezar ma'lumotlarni shifrlashda alfavit xarflarni nechtaga surib shifrlagan? +:3 taga -:4 taga -:2 taga -:5 taga I: S:WiMAX qanday simsiz tarmoq turiga kiradi? +:Regional -:Lokal -:Global -:Shaxsiy I: S:Wi-Fi necha Gs chastotali to'liqida ishlaydi? +:2.4-5 Gs -:2.4-2.485 Gs -:1.5-11 Gs -:2.3-13.6 Gs I: S:Quyidagi parollarning qaysi biri "bardoshli parol"ga kiradi? +:Onx458&hdsh) -:12456578 - :salomDunyo -:Mashina777 I: S:Parollash siyosatiga ko'ra parol tanlash shartlari qanday? +:Kamida 8 belgi; katta va kichik xavflar, sonlar , kamida bitta maxsus simvol qo'llanishi kerak. -:Kamida 8 belgi; katta va kichik xavflar, sonlar qo'llanishi kerak. -:Kamida 6 belgi; katta xarflar, sonlar , kamida bitta maxsus simvol qo'llanishi kerak. -:Kamida 6 belgi; katta va kichik xarflar, kamida bitta maxsus simvol qo'llanishi kerak. I: S:MD5, SHA1, SHA256, O'z DSt 1106:2009- qanday algoritmlar deb ataladi? +:Xeshlash -:Kodlash -:Shifrlash -:Stenografiya I: S:LTE Advances standarti global simsiz tarmoqning nechanshi avlodiga mansub? +:4G -:3G -:2G -:1G I: S:Bluetooth necha Gs chastotali to'liqida ishlaydi? +:2.4-2.485 Gs -:2.4-5 Gs -:1.5-11 Gs -:2.3-13.6 Gs I: S:Axborot o'lchovini o'sish tartibini to'g'ri tanlang +:Bit,bayt,kilobayt,megabayt -:Bit,bayt,megabayt,kilobayt -:Gigabayt,megabayt,pikobayt -:Gigabayt,pikobayat,terobayt I: S:Axborot o'lchovini kamayish

tartibini to'g'ri tanlang +:Gigabayt,megabayt,kilobayt -:Bit,bayt,kilobayt,megabayt -  
:Gigabayt,megabayt,pikobayt -:Gigabayt,pikobayat,terobayt I: S:"Parol", "PIN" kodlarni xavfsizlik  
tomonidan kamchiligi nimadan iborat? +:Foydalanish davrida maxfiylik kamayib boradi -:Parolni  
esda saqlash kerak bo'ladi -:Parolni almashtirish jarayoni murakkabligi -:Parol uzunligi soni  
cheklangan I: S:Axborot xavfsizligin ta'minlashda qo'llaniladigan me'yoriy hujjatlarning birinchi  
darajadagi hujjati-bu.. +:Qonun -:Qaror -:Standart -:Farmon I: S: Elektron raqamli imzo kalitlari  
ro'yxatga olish qaysi tashkilot tomonidan bajariladi? +:Sertifikatlari ro'yxatga olish markazlari -  
:Tegishli Vazirliklar -:Davlat Hokimiyati -:Axborot xavfsizligi markazlari I: S: Elektron raqamli imzo  
to'g'risidagi Qonun qachon qabul qilingan? +:2003 yil 11 dekabr -:2005 yil 2 mart -:2010 yil 1  
sentyabr -:2015 yil 5 yanvar I: S:Global simsiz tarmoqda qaysi standartlar ishlaydi? +:CDPD, 4G -  
:Wi-Fi, 3G -:WIMAX, 2G -:Wi-Fi, IRDA I: S:Kompyuter IPv4 manzilni to'g'ri kiritilishini ko'rsating.  
+:192.168.100.001 -:12:AC:14:1C:3B:13 -:1254-1255-3645 -:01001:00011:0111 I: S:Kompyuter  
yoki boshqa qurilmalarga qarshi qilingan yoki kompyuter va boshqa qurilmalar orqali qilingan  
jinoiat-... +:Kiberjinoiat -:Kibersport -:Kiberterror -:Hakerlar uyushmasi I: S:Masofadan ERI olish  
uchun qaysi internet manzilga murojaat qilinadi? +:e-imzo.uz -:elektron-imzo.uz -:imzo.uz -:eri.uz  
I: S:Konfidentsial axborotdan foydalanish tushunchasi... +:Muayyan shaxsga tarkibida konfidensial  
xarakterli ma'lumot bo'lgan axborot bilan tanishishga vakolatli mansabdor shaxsning ruxsati. -  
:Korxona o'z faoliyatini buzilishsiz va to'xtalishsiz yurgiza oladigan vaqt bo'yicha barqaror  
bashoratlanuvchi atrof-muhit holati. -:Ma'lumotlarning ma'lumotlar bazasiga tegishli darajasini  
aniqlash va belgilash. -:Olingan ma'lumotlar jo'natuvchisining so'ralganiga mosligini tasdiqlash.  
Yuliy Sezar ma'lumotlarni shifrlashda alfavit xarflarni nechtaga surib shifrlagan? ==== 4 taga==== 2  
taga==== 5 taga==== #3 taga +++++ WiMAX qanday simsiz tarmoq turiga kiradi? ==== Lokal ====  
Global==== Shaxsiy ==== #Regional +++++ Wi-Fi necha Gs chastotali to'lqinda ishlaydi? ==== #2.4-  
5 Gs==== 2.4-2.485 Gs==== 1.5-11 Gs==== 2.3-13.6 Gs +++++ Quyidagi parollarning qaysi biri  
"bardoshli parol"ga kiradi? ==== #Onx458&hdsh) ==== 12456578==== salomDunyo====  
Mashina777 +++++ Ma'lumotlarni tasodifiy sabablar tufayli yo'qolish sababini belgilang====  
#Quvvat o'chishi, dasturiy ta'minot to'satdan o'zgarishi yoki qurilmani to'satdan zararlanishi====  
Tashkilotdagi muhim ma'lumotlarni modifikatsiyalanishi yoki o'g'irlanishi==== Ma'lumotlarni  
saqlash vositasini to'g'ri joylashtirilmagani yoki ma'lumotlar bazasini xatolik bilan boshqarilganligi.  
==== Zilzila, yong'in, suv toshqini va hak. +++++ Sub'ektga ma'lum vakolat va resurslarni berish  
muolajasi-bu: ==== #Avtorizatsiya==== Haqiqiylikni tasdiqlash==== Autentifikatsiya====  
Identifikatsiya +++++ Token, Smartkartalarda xavfsizlik tomonidan kamchiligi nimada? ====  
Foydalanish davrida maxfiylik kamayib boradi==== Qurilmalarni ishlab chiqarish murakkab  
jarayon==== #Qurilmani yo'qotilishi katta xavf olib kelishi mumkin==== Qurilmani qalbakilashtirish  
oson +++++ Ma'lumotlarni yo'qolish sabab bo'luvchi tabiiy tahdidlarni ko'rsating==== Quvvat  
o'chishi, dasturiy ta'minot to'satdan o'zgarishi yoki qurilmani to'satdan zararlanishi==== #Zilzila,  
yong'in, suv toshqini va hak. ==== Tashkilotdagi muhim ma'lumotlarni modifikatsiyalanishi yoki  
o'g'irlanishi==== Qasddan yoki tasodifiy ma'lumotni o'chirib yuborilishi, ma'lumotlarni saqlash  
vositasini to'g'ri joylashtirilmagani +++++ Foydalanish huquqini cheklovchi matritsa modeli bu...  
==== #Bella La-Padulla modeli==== Dening modeli==== Landver modeli==== Huquqlarni  
cheklovchi model +++++ Parollash siyosatiga ko'ra parol tanlash shartlari qanday? ==== Kamida 8  
belgi; katta va kichik xavflar, sonlar qo'llanishi kerak. ==== #Kamida 8 belgi; katta va kichik xavflar,  
sonlar , kamida bitta maxsus simvol qo'llanishi kerak. ==== Kamida 6 belgi; katta xavflar, sonlar ,  
kamida bitta maxsus simvol qo'llanishi kerak. ==== Kamida 6 belgi; katta va kichik xavflar, kamida  
bitta maxsus simvol qo'llanishi kerak. +++++ MD5, SHA1, SHA256, O'z DSt 1106:2009- qanday



algoritmlar deb ataladi? ===== Kodlash===== #Xeshlash===== Shifrlash===== Stenografiya +++++  
Global simsiz tarmoqda qaysi standartlar ishlaydi? ===== Wi-Fi, 3G===== WIMAX, 2G===== Wi-Fi,  
IRDA===== #CDPD, 4G +++++ RSA algoritmi qaysi yilda ishlab chiqilgan? ===== #1977 yil===== 1966  
yil===== 1988 yil===== 1956 yil +++++ Qaysi texnologiyada ma'lumotni bir vaqtda bir necha disklarga  
navbatlab yoziladi? ===== RAID 1===== #RAID 0===== RAID 5===== RAID 3 +++++ Windows OT lokal  
xavfsizlik siyosatini sozlash oynasiga o'tish uchun buyruqlar satrida qaysi buyruq yoziladi? =====  
#secpol.msc===== regedit===== chkdsk===== diskcopy +++++ Zimmermann telegrami, Enigma shifri,  
SIGABA kriptografiyaning qaysi davriga to'g'ri keladi? ===== O'rta asr davrida===== 15 asr  
davrida===== #1-2 jahon urushu davri===== 21 asr davrida +++++ Bell-LaPadula (BLP) modeli -bu..  
===== Axborlarni nazoratlovchi model===== #Bu hukumat va harbiy dasturlarda kirishni  
boshqarishni kuchaytirish uchun ishlatiladigan avtomatlashgan modeli===== Foydalanuvchilarni  
ro'yxatga olish , nazoratlash va tahlil qiluvchi model===== Tarmoq boshqarish va tahlil qiluvchi  
model +++++ Internetning dastlabki nomini to'g'ri belgilang. ===== #ARPANET===== INTRANET=====  
INTERNET===== NETWORK +++++ Axborot xavfsizligining asosiy maqsadlaridan biribu...=====  
Ob'ektga bevosita ta'sir qilish===== #Axborotlarni o'g'irlanishini, yo'qolishini, soxtalashtirilishini  
oldini olish===== Axborotlarni shifrlash, saqlash, yetkazib berish===== Tarmoqdagi  
foydalanuvchilarni xavfsizligini ta'minlab berish +++++ Konfidentsiallikga to'g'ri ta'rif keltiring.=====  
#axborot inshonchliligi, tarqatilishi mumkin emasligi, maxfiyligi kafolati; ===== axborot  
konfidentsialligi, tarqatilishi mumkinligi, maxfiyligi kafolati; ===== axborot inshonchliligi, tarqatilishi  
mumkin emasligi, parollanganligi kafolati; ===== axborot inshonchliligi, axborotlashganligi,  
maxfiyligi kafolati; +++++ Yaxlitlikni buzilishi bu - ...===== #Soxtalashtirish va o'zgartirish=====  
Ishonchsizlik va soxtalashtirish===== Soxtalashtirish===== Butunmaslik va yaxlitlanmaganlik +++++  
Kriptografiyaning asosiy maqsadi nima? ===== ishonchlilik, butunlikni ta'minlash=====  
autentifikatsiya, identifikatsiya===== #maxfiylik, yaxlitlikni ta'minlash===== ma'lumotlarni shaklini  
o'zgartirish +++++ Kriptografiyada kalitning vazifasi nima? ===== Bir qancha kalitlar yig'indisi=====  
#Matnni shifrlash va shifrini ochish uchun kerakli axborot===== Axborotli kalitlar to'plami=====  
Belgini va raqamlarni shifrlash va shifrini ochish uchun kerakli axborot +++++ Qo'yish, o'rin  
almashtirish, gammalash kriptografiyaning qaysi turiga bog'liq? ===== assimetrik kriptotizimlar=====  
ochiq kalitli kriptotizimlar===== #simmetrik kriptotizimlar===== autentifikatsiyalash +++++  
Autentifikatsiya nima? ===== Tizim me'yoriy va g'ayritabiiy hollarda rejalashtirilgandek o'zini  
tutishligi holati===== #Ma'lum qilingan foydalanuvchi, jarayon yoki qurilmaning haqiqiy ekanligini  
tekshirish muolajasi===== Istalgan vaqtda dastur majmuasining mumkinligini kafolati===== Tizim  
noodatiy va tabiiy hollarda qurilmaning haqiqiy ekanligini tekshirish muolajasi +++++  
Identifikatsiya bu- ...===== #Foydalanuvchini uning identifikatori (nomi) bo'yicha aniqlash  
jarayoni===== Ishonchliligini tarqalishi mumkin emasligi kafolati===== Axborot boshlang'ich  
ko'rinishda ekanligi uni saqlash, uzatishda ruxsat etilmagan o'zgarishlar===== Axborotni butunligini  
saqlab qolgan holda uni elementlarini o'zgartirishga yo'l qo'ymaslik +++++ Kriptologiya –qanday  
fan? ===== axborotni qayta akslantirishning matematik usullarini izlaydi va tadqiq qiladi===== kalitni  
bilmasdan shifrlangan matnni ochish imkoniyatlarini o'rganadi===== kalitlarni bilmasdan shifrn  
ochishga bardoshlilikni aniqlovchi shifrlash tavsifi===== #axborotni qayta akslantirib himoyalash  
muammosi bilan shug'ullanadi +++++ Kriptobardoshlilik deb nimaga aytiladi? ===== #kalitlarni  
bilmasdan shifrn ochishga bardoshlilikni aniqlovchi shifrlash tavsifi===== axborotni qayta  
akslantirib himoyalash muammosi bilan shug'ullanadi===== kalitni bilmasdan shifrlangan matnni  
ochish imkoniyatlarini o'rganadi===== axborotni qayta akslantirishning matematik usullarini izlaydi  
va tadqiq qiladi +++++ Kriptografiyada matn –bu.. ===== matnni shifrlash va shifrini ochish uchun

kerakli axborot==== axborot belgilarini kodlash uchun foydalaniladigan chekli to'plam==== #alifbo elementlarining tartiblangan to'plami==== kalit axborotni shifrllovchi kalitlar +++++ Kriptotizimga qo'yiladigan umumiy talablardan biri nima? ==== shifrlash algoritmining tarkibiy elementlarini o'zgartirish imkoniyati bo'lishi lozim==== ketma-ket qo'llaniladigan kalitlar o'rtasida oddiy va oson bog'liqlik bo'lishi kerak==== #shifr matn uzunligi ochiq matn uzunligiga teng bo'lishi kerak==== maxfiylik o'ta yuqori darajada bo'lmoqligi lozim +++++ Axborot qanday sifatlarga ega bo'lishi kerak? ==== uzluksiz va uzlukli==== ishonchli, qimmatli va uzlukli==== #ishonchli, qimmatli va to'liq==== ishonchli, qimmatli va uzluksiz +++++ Tekstni boshqa tekst ichida ma'nosini yashirib keltirish nima deb ataladi?==== sirli yozuv==== #steganografiya==== skrembler==== shifr mashinalar +++++ Berilgan ta'riflardan qaysi biri asimmetrik tizimlarga xos? ==== Asimmetrik tizimlarda  $k_1=k_2$  bo'ladi, ya'ni  $k$  – kalit bilan axborot ham shifrlanadi, ham deshifrlanadi==== #Asimmetrik kriptotizimlarda  $k_1 \neq k_2$  bo'lib,  $k_1$  ochiq kalit,  $k_2$  yopiq kalit deb yuritiladi,  $k_1$  bilan axborot shifrlanadi,  $k_2$  bilan esa deshifrlanadi==== Asimmetrik kriptotizimlarda yopiq kalit axborot almashinuvining barcha ishtirokchilariga ma'lum bo'ladi, ochiq kalitni esa faqat qabul qiluvchi biladi==== Asimmetrik kriptotizimlarda  $k_1 \neq k_2$  bo'lib, kalitlar hammaga oshkor etiladi +++++ Shaxsning, axborot kommunikatsiya tizimidan foydalanish huquqiga ega bo'lish uchun foydalaniluvchining maxfiy bo'lmagan qayd yozuvi – bu...==== parol==== #login==== identifikatsiya==== token +++++ Uning egasi haqiqiylikni aniqlash jarayonida tekshiruv axboroti sifatida ishlatiladigan belgilar ketma-ketligi (maxfiy so'z) – nima? ==== login==== #parol==== identifikatsiya==== maxfiy maydon +++++ Kodlash nima? ==== Ma'lumot boshqa formatga o'zgartiriladi, biroq uni faqat maxsus shaxslar qayta o'zgartirishi mumkin bo'ladi==== Ma'lumot boshqa formatga o'zgartiriladi, barcha shaxslar kalit yordamida qayta o'zgartirishi mumkin bo'ladi==== Maxfiy xabarni soxta xabar ichiga berkitish orqali aloqani yashirish hisoblanadi==== #Ma'lumotni osongina qaytarish uchun hammaga ochiq bo'lgan sxema yordamida ma'lumotlarni boshqa formatga o'zgartirishdir +++++ Ro'yxatdan o'tish-bu...==== #foydalanuvchilarni ro'yxatga olish va ularga dasturlar va ma'lumotlarni ishlatishga huquq berish jarayoni==== axborot tizimlari ob'yekt va subhektlariga uni tanish uchun nomlar (identifikator) berish va berilgan nom bo'yicha solishtirib uni aniqlash jarayoni==== ob'ekt yoki subhektning unga berilgan identifikatorga mosligini tekshirish va belgilar ketma-ketligidan iborat maxfiy kodini tekshirish orqali aslligini aniqlash==== foydalanuvchining resursdan foydalanish huquqlari va ruxsatlarini tekshirish jarayoni +++++ Shifrtakstni ochiq tekstga akslantirish jarayoni nima deb ataladi? ==== Xabar==== Shifrlangan xabar==== Shifrlash==== #Deshifrlash +++++ .....–hisoblashga asoslangan bilim sohasi bo'lib, buzg'unchilar mavjud bo'lgan sharoitda amallarni kafolatlash uchun o'zida texnologiya, inson, axborot va jarayonni mujassamlashtirgan. ==== Axborot xavfsizligi==== Kiberjtnoyatchilik==== #Kiberxavfsizlik==== Risklar +++++ Risk nima? ==== Potensial kuchlanish yoki zarar==== Tasodifiy tahdid==== #Potensial foyda yoki zarar==== Katta yo'qotish +++++ Tahdid nima? Tashkilot uchun qadrlil bo'lgan ixtiyoriy narsa==== Bu riskni o'zgartiradigan harakatlar==== #Tashkilotga zarar yetkazishi mumkin bo'lgan istalmagan hodisa==== Bu noaniqlikning maqsadlarga ta'siri +++++ Axborotni shifrnı ochish (deshifrlash) bilan qaysi fan shug'ullanadi? ==== Kartografiya==== #Kriptoanaliz==== Kriptologiya==== Adamar usuli +++++ Qaysi juftlik RSA algoritmining ochiq va yopiq kalitlarini ifodalaydi? ====  $\{d, e\}$  – ochiq,  $\{e, n\}$  – yopiq; ====  $\{d, n\}$  – yopiq,  $\{e, n\}$  – ochiq; ====  $\{e, n\}$  – yopiq,  $\{d, n\}$  – ochiq; ====  $\{e, n\}$  – ochiq,  $\{d, n\}$  – yopiq; +++++ Zamonaviy kriptografiya qanday bo'limlardan iborat? ==== Elektron raqamli imzo; kalitlarni boshqarish;==== Simmetrik kriptotizimlar; ochiq kalitli kriptotizimlar; ==== #Simmetrik kriptotizimlar; ochiq kalitli kriptotizimlar; Elektron raqamli imzo; kalitlarni boshqarish ==== Simmetrik kriptotizimlar; ochiq

kalitli kriptotizimlar; kalitlarni boshqarish +++++ Shifr nima?==== #Shifrlash va deshifrlashda foydalaniladigan matematik funktsiyadan iborat bo'lgan kriptografik algoritm ==== Kalitlarni taqsimlash usuli==== Kalitlarni boshqarish usuli ==== Kalitlarni generatsiya qilish usuli +++++ Ko'z pardasi, yuz tuzilishi, ovoz tembri, -bular autentifikatsiyaning qaysi faktoriga mos belgilar? ==== #Biometrik autentifikatsiya==== Biron nimaga egalik asosida==== Biron nimani bilish asosida==== Parolga asoslangan +++++ Ochiq kalitli kriptotizimlarning mohiyati nimadan iborat? ==== Ochiq kalitli kriptotizimlarda shifrlash va deshifrlashda 1 ta –kalitdan foydalaniladi==== #Ochiq kalitli kriptotizimlarda bir-biri bilan matematik bog'langan 2 ta – ochiq va yopiq kalitlardan foydalaniladi==== Ochiq kalitli kriptotizimlarda ma'lumotlarni faqat shifrlash mumkin==== Ochiq kalitli kriptotizimlarda ma'lumotlarni faqat deshifrlash mumkin +++++ Assimetrik kriptotizimlar qanday maqsadlarda ishlatiladi? ==== #Shifrlash, deshifrlash, ERI yaratish va tekshirish, kalitlar almashish uchun==== ERI yaratish va tekshirish, kalitlar almashish uchun==== Shifrlash, deshifrlash, kalitlar almashish uchun==== Heshlash uchun +++++ Ma'lumotlar butunligi qanday algritmlar orqali amalga oshiriladi? ==== Simmetrik aloritmlar==== Assimetrik aloritmlar==== #Xesh funksiyalar==== Kodlash +++++ To'rtta bir-biri bilan bog'langan bog'lamlar strukturasi (kvadrat shaklida) qaysi topologiya turiga mansub? ==== Yulduz==== To'liq bog'lanishli==== #Xalqa==== Yacheykali +++++ Lokal tarmoqlarda keng tarqalgan topologiya turi qaysi? ==== Xalqa==== To'liqbog'langan==== Umumiy shina==== #Yulduz +++++ Ethernet kontsentratori qanday vazifani bajaradi?==== #kompyuterdan kelayotgan axborotni qolgan barcha kompyuterga yo'naltirib beradi==== kompyuterdan kelayotgan axborotni boshqa bir kompyuterga yo'naltirib beradi==== kompyuterdan kelayotgan axborotni xalqa bo'ylab joylashgan keyingi kompyuterga==== tarmoqning ikki segmentini bir biriga ulaydi +++++ OSI modelida nechta sath mavjud? ==== 4 ta==== 5 ta==== #7 ta==== 3 ta +++++ Identifikatsiya, autentifikatsiya jarayonlaridan o'tgan foydalanuvchi uchun tizimda bajarishi mumkin bo'lgan amallarga ruxsat berish jarayoni bu... ==== Shifrlash==== Identifikatsiya==== Autentifikatsiya==== #Avtorizatsiya +++++ Ma'lumotlarni inson xatosi tufayli yo'qolish sababini belgilang. ==== Tashkilotdagi muhim ma'lumotlarni modifikatsiyalanishi yoki o'g'irlanishi. ==== #Ma'lumotlarni saqlash vositasini to'g'ri joylashtirilmagani yoki ma'lumotlar bazasini xatolik bilan boshqarilganligi. ==== Quvvat o'chishi, dasturiy ta'minot to'satdan o'zgarishi yoki qurilmani to'satdan zararlanishi==== Zilzila, yong'in, suv toshqini va hak. +++++ "Parol", "PIN" kodlarni xavfsizlik tomonidan kamchiligi nimadan iborat? ==== Parolni esda saqlash kerak bo'ladi. ==== Parolni almashtirish jarayoni murakkabligi==== Parol uzunligi soni cheklangan==== #Foydalanish davrida maxfiylik kamayib boradi +++++ Qaysi tarmoq kabelining axborot uzatish tezligi yuqori hisoblanadi? ==== #Optik tolali==== O'rama juft==== Koaksial ==== Telefon kabeli +++++ Nima uchun autentifikatsiyalashda parol ko'p qo'llaniladi? ==== #Sarf xarajati kam, almashtirish oson==== Parolni foydalanubchi ishlab chiqadi==== Parolni o'g'rishlash qiyin==== Serverda parollar saqlanmaydi +++++ Elektron xujjatlarni yo'q qilish usullari qaysilar? ==== Yoqish, ko'mish, yanchish==== #Shredirlash, magnitsizlantirish, yanchish==== Shredirlash, yoqish, ko'mish==== Kimyoviy usul, yoqish. +++++ Ruxsatlarni nazoratlash, "Qopqon", Yong'inga qarshi tizimlar, Yoritish tizimlari, Ogohlantirish tizimlari , Quvvat manbalari, Video kuzatuv tizimlari, Qurollarni aniqlash, Muhitni nazoratlash amalga oshirish qanday nazorat turiga kiradi? ==== Fizik nazorat==== #Texnik nazorat==== Ma'muriy nazorat==== Tashkiliy nazorat +++++ Avtorizatsiya tushunchasi odatda qaysi tushuncha bilan sinonim sifatida ham foydalanadi? ==== Foydalanish==== Tarmoqni loyixalash==== Identifikatsiya==== #Foydalanishni boshqarish +++++ Foydalanishni boshqarish –bu... ==== Sub'ektni Sub'ektga ishlash qobilyatini aniqlashdir. ==== #Sub'ektni Ob'ektga ishlash qobilyatini aniqlashdir. ==== Ob'ektni Ob'ektga ishlash

qobilyatini aniqlashdir==== Autentifikatsiyalash jarayonidir +++++ Foydalanishni boshqarishda inson, dastur, jarayon va hokazolar nima vazifani bajaradi? ==== #Sub'ekt==== Ob'ekt==== Tizim==== Jarayon +++++ Foydalanishna boshqarishda ma'lumot , resurs, jarayon nima vazifani bajaradi ? ==== #Ob'ekt==== Sub'ekt==== Tizim==== Jarayon +++++ MAC usuli bilan foydalanishni boshqarishda xavfsizlik markazlashgan holatda kim tomonidan amalga oshiriladi? ==== Foydalaguvchining o'zi==== #Xavfsizlik siyosati ma'muri==== Dastur tomonidan==== Boshqarish amalg'a oshirilmaydi +++++ Agar Sub'ektning xavfsizlik darajasida Ob'ektning xavfsizlik darajasi mavjud bo'lsa, u holda uchun qanday amalga ruxsat beriladi? ==== Yozish ==== O'zgartirish==== #O'qish==== Yashirish +++++ Agar Sub'ektning xavfsizlik darajasi Ob'ektning xavfsizlik darajasida bo'lsa, u holda qanday amalga ruxsat beriladi? ==== #Yozish ==== O'qish==== O'zgartirish==== Yashirish +++++ Rol tushunchasiga ta'rif bering. ==== Foydalanishni boshqarish==== #Muayyan faoliyat turi bilan bog'liq harakatlar va majburiyatlar to'plami sifatida belgilanishi mumkin==== Muayyan faoliyat turi bilan bog'liq imkoniyatlar to'plami sifatida belgilanishi mumkin==== Vakolitlarni taqsimlash +++++ Wi-Fi tarmoqlarida quyida keltirilgan qaysi shifrlash protokollaridan foydalaniladi.==== WEB, SSL, WPA2==== WPA, TLS==== WPA, FTP==== #WEP, WPA, WPA2 +++++ Foydalanishni boshqarishning qaysi usuli – Ob'ektlar va Sub'ektlarning atributlari, ular bilan mumkin bo'lgan amallar va so'rovlarga mos keladigan muhit uchun qoidalarni tahlil qilish asosida foydalanishlarni boshqaradi. ==== MAC==== #ABAC==== DAC==== RBAC +++++ Qanday tarmoq qisqa masofalarda qurilmalar o'rtasida ma'lumot almashinish imkoniyatini taqdim etadi? ==== #Shaxsiy tarmoq==== Lokal==== Mintaqaviy ==== CAMPUS +++++ Quyidagilardan lokal tarmoqqa berilgan ta'rifni belgilang. ==== Odatda ijaraga olingan telekommunikatsiya liniyalaridan foydalanadigan tarmoqlardagi tugunlarni bir-biriga bog'laydi. ==== Bu tarmoq shahar yoki shaharcha bo'ylab tarmoqlarning o'zaro bog'lanishini nazarda tutadi==== Qisqa masofalarda qurilmalar o'rtasida ma'lumot almashinish imkoniyatini taqdim etadi==== #Kompyuterlar va ularni bog'lab turgan qurilmalardan iborat bo'lib, ular odatda bitta tarmoqda bo'ladi. +++++ Quyidagilardan mintaqaviy tarmoqqa berilgan ta'rifni belgilang. ==== Kompyuterlar va ularni bog'lab turgan qurilmalardan iborat bo'lib, ular odatda bitta tarmoqda bo'ladi. ==== Bu tarmoq shahar yoki shaharcha bo'ylab tarmoqlarning o'zaro bog'lanishini nazarda tutadi==== #Odatda ijaraga olingan telekommunikatsiya liniyalaridan foydalanadigan tarmoqlardagi tugunlarni bir-biriga bog'laydi. ==== Qisqa masofalarda qurilmalar o'rtasida ma'lumot almashinish imkoniyatini taqdim etadi +++++ Router nima? ==== Tarmoq qurilmasi bo'lib, ko'plab tarmoqlarni ulash uchun yoki LAN segmentlarini bog'lash uchun xizmat qiladi Hisoblash qurilmasining ajralmas qismi bo'lib, qurilmani tarmoqqa ulash imkoniyatini taqdim etadi==== Ko'plab tarmoqlarni ulash uchun yoki LAN segmentlarini bog'lash uchun xizmat qiladi. ==== Qabul qilingan signalni barcha chiquvchi portlarga emas balki paketda manzili keltirilgan portga uzatadi==== #Qabul qilingan ma'lumotlarni tarmoq sathiga tegishli manzillarga ko'ra (IP manzil) uzatadi. +++++ Fire Wall ning vazifasi... ==== #Tarmoqlar orasida aloqa o'rnatish jarayonida tashkilot va Internet tarmog'i orasida xavfsizlikni ta'minlaydi==== Kompyuterlar tizimi xavfsizligini ta'minlaydi==== Ikkita kompyuter o'rtasida aloqa o'rnatish jarayonida Internet tarmog'i orasida xavfsizlikni ta'minlaydi==== Uy tarmog'i orasida aloqa o'rnatish jarayonida tashkilot va Internet tarmog'i orasida xavfsizlikni ta'minlaydi +++++ Stenografiya ma'nosi qanday? ==== sirli xat==== #sirli yozuv==== maxfiy axborot==== maxfiy belgi +++++ Shifrlash kaliti noma'lum bo'lganda shifrlangan ma'lumotni deshifrlash qiyinlik darajasini nima belgilaydi? ==== Shifr matn uzunligi==== #Kriptobardoshlik==== Shifrlash algoritmi==== Texnika va texnologiyalar +++++ Ma'lumotlarni yo'q qilish odatda necha xil usulidan foydalaniladi? ==== #4 xil==== 8 xil==== 7 xil==== 5 xil +++++ Kiberjinoyatchilik bu -. . . ==== #Kompyuter yoki

boshqa qurilmalarga qarshi qilingan yoki kompyuter va boshqa qurilmalar orqali qilingan jinoiy faoliyat. ===== Kompyuter o'yinlari===== Faqat banklardan pul o'g'irlanishi===== Autentifikatsiya jarayonini buzish +++++ Axborot xavfsizligiga bo'ladigan tahdidlarning qaysi biri maqsadli (atayin) tahdidlar deb hisoblanadi? ===== Tabiiy ofat va avariya===== Texnik vositalarning buzilishi va ishlamasligi===== #Strukturalarni ruxsatsiz modifikatsiyalash===== Foydalanuvchilar va xizmat ko'rsatuvchi hodimlarning hatoliklari +++++ Axborot xavfsizligiga bo'ladigan tahdidlarning qaysi biri tasodifiy tahdidlar deb hisoblanadi? ===== Axborotdan ruxsatsiz foydalanish===== Zararkunanda dasturlar===== An'anaviy josuslik va diversiya haqidagi ma'lumotlar tahlili===== #Texnik vositalarning buzilishi va ishlamasligi +++++ Axborotni uzatish va saqlash jarayonida o'z strukturasi va yoki mazmunini saqlash xususiyati nima deb ataladi? ===== Axborotning konfidentsialligi===== Foydalanuvchanligi===== #Ma'lumotlar butunligi===== Ixchamligi +++++ Biometrik autentifikatsiyalashning avfzalliklari-bu: ===== Bir marta ishlatilishi===== #Biometrik parametrlarning noyobligi===== Biometrik parametrlarni o'zgartirish imkoniyati===== Autentifikatsiyalash jarayonining soddaligi +++++ Simli va simsiz tarmoqlar orasidagi asosiy farq nimadan iborat? ===== #Tarmoq chetki nuqtalari orasidagi mutlaqo nazoratlamaydigan hudud===== Tarmoq chetki nuqtalari orasidagi xududning kengligi asosida qurilmalar holati===== Himoya vositalarining chegaralanganligi===== Himoyani amalga oshirish imkoniyati yo'qligi va ma'lum protokollarning ishlatilishi +++++ Simmetrik shifrlashning noqulayligi – bu: ===== #Maxfiy kalitlar bilan ayirboshlash zaruriyatidir===== Kalitlar maxfiyligi===== Kalitlar uzunligi===== Shifrlashga ko'p vaqt sarflanishi va ko'p yuklanishi +++++ Autentifikatsiya faktorlari nechta? ===== 4 ta===== #3 ta===== 5 ta===== 6 ta +++++ Kompyuter tizimida ro'yxatga olish protsedurasini loyihalashtirish, qaysi standart bo'yicha to'g'ri keltirilgan. ===== #O'z DSt ISO/IEC 27002:2008===== O'z DSt ISO/IEC 27002:2005===== O'z DSt ISO/IEC 27002:2009===== O'z DSt ISO/IEC 27002:2000===== +++++ Parollar bilan ishlashdagi tavsiyalar qaysi qatorda to'g'ri ko'rsatilgan?===== #Tizimga kirishdagi qayta urinishlar sonini parolning minimal uzunligiga va muhofaza qilinayotgan tizimning qiymatiga muvofiq belgilash;===== Ro'yxatga olish protsedurasini uchun ruxsat berilgan vaqtni olib tashlash. Agar u ko'paytirilgan bo'lsa, tizimning ro'yxatga olishini davom ettirish;===== Oxirgi muvaffaqiyatli ro'yxatga olishdan boshlab, boshqa urinishlar so'ramaslik;===== Kiritilayotgan parolni ko'rsatmaslik yoki variant sifatida bir xil parol tanlash.===== OSI modelida nechta tarmoq satxi bor ? J: 7 OSI modelining birinchi satxi qanday nomlanadi J: Fizik satx OSI modelining ikkinchi satxi qanday nomlanadi J: Kanal satxi OSI modelining uchinchi satxi qanday nomlanadi J: Tarmoq satxi OSI modelining oltinchi satxi qanday nomlanadi J: Taqdimlash satxi OSI modelining yettinchi satxi qanday nomlanadi J: Amaliy satx OSI modelining qaysi satxlari tarmoqqa bog'liq satxlar hisoblanadi J: fizik, kanal va tarmoq satxlari OSI modelining tarmoq satxi vazifalari keltirilgan qurilmalarning qaysi birida bajariladi J: Marshrutizator OSI modelining fizik satxi qanday funktsiyalarni bajaradi J: Elektr signallarini uzatish va qabul qilish Foydalanishna boshqarishda ma'lumot , resurs, jarayon nima vazifani bajaradi ? J: Obyekt Foydalanishni boshqarishda inson, dastur, jarayon va xokazolar nima vazifani bajaradi? J: Subyekt Simmetrik kriptotizimlarda ... jumlanini davom ettiring J: shifrlash va shifrni ochish uchun bitta va aynan shu kalitdan foydalaniladi Simmetrik kalitli shifrlash tizimi necha turga bo'linadi. J: 2 turga Axborotning eng kichik o'lchov birligi nima? J: bit Ko'z pardasi, yuz tuzilishi, ovoz tembrini: bular autentifikatsiyaning qaysi faktoriga mos belgilar? J: Biometrik autentifikatsiya Kriptografiyaning asosiy maqsadi... J: maxfiylik, yaxlitlikni ta'minlash Ro'yxatdan o'tish bu? foydalanuvchilarni ro'yxatga olish va ularga dasturlar va ma'lumotlarni ishlatishga huquq berish jarayoni Qanday xujumda zararli hujumlar tizim yoki tarmoqqa bevosita va bilvosita ta'sir qiladi? J:

Zararli hujumlar Qanday xujumda hujumchi turli texnologiyalardan foydalangan holda tarmoqqa kirishga harakat qiladi? J: Kirish hujumlari Keltirilgan protokollarning qaysilari kanal satxi protokollariga mansub J: Ethernet, FDDI Xesh-:funktsiyani natijasi ... J: fiksirlangan uzunlikdagi xabar Ethernet kontsentratori qanday vazifani bajaradi J: kompyuterdan kelayotgan axborotni qolgan barcha kompyuterga yo'naltirib beradi Axborotlarni saqllovchi va tashuvchi vositalar qaysilar? J: fleshka, CD va DVD disklar Faol hujum turi deb... J: Maxfiy uzatish jarayonini uzib qo'yish, modifikatsiyalash, qalbaki shifr ma'lumotlar tayyorlash harakatlaridan iborat jarayon Foydalanishni boshqarishning qaysi usulida foydalanishlar Subyektlar va Obyektlarni klassifikatsiyalashga asosan boshqariladi. J: MAC Foydalanishni boshqarishning qaysi usulida tizimdagi shaxsiy Obyektlarni himoyalash uchun qo'llaniladi J: DAC Foydalanishni boshqarishning qaysi modelida Obyekt egasining o'zi undan foydalanish huquqini va kirish turini o'zi belgilaydi J: DACfInternetda elektron pochta bilan ishlash uchun TCP/IPga asoslangan qaysi protokoldan foydalaniladi? Foydalanishni boshqarishning qaysi usuli -: Obyektlar va Subyektlarning atributlari, ular bilan mumkin bo'lgan amallar va so'rovlarga mos keladigan muhit uchun qoidalarini tahlil qilish asosida foydalanishlarni boshqaradi. J: ABAC Foydalanishni boshqarishning qaysi modelida har bir Obyekt uchun har bir foydalanuvchini foydalanish ruxsatini belgilash o'rniga, rol uchun Obyektlardan foydalanish ruxsati ko'rsatiladi? J: RBAC To'rtta bir-:biri bilan bog'langan bog'lamlar strukturasi (kvadrat shaklida) qaysi topologiya turiga mansub J: Xalqa Yulduz To'liq bog'lanishli Yacheykali Qanday xujum asosiy hujumlarni oson amalga oshirish uchun tashkilot va tarmoq haqidagi axborotni to'plashni maqsad qiladi? J: DNS tizimlari, Razvedka hujumlari ..... – hisoblashga asoslangan bilim sohasi bo'lib, buzg'unchilar mavjud bo'lgan sharoitda amallarni kafolatlash uchun o'zida texnologiya, inson, axborot va jarayonni mujassamlashtirgan. J: Kiberxavfsizlik Elektron raqamli imzo tizimi qanday muolajalarni amalga oshiradi? J: raqamli imzoni shakllantirish va tekshirish muolajasi Kriptologiya -: J: axborotni qayta akslantirib himoyalash muammosi bilan shug'ullanadi Shifrtexstni ochiq tekstga akslantirish jarayoni nima deb ataladi? J: Deshifrlash Xavfsizlikning asosiy yo'nalishlarini sanab o'ting. J: Axborot xavfsizligi, Iqtisodiy xavfsizlik, Mudofaa xavfsizligi, Ijtimoiy xavfsizlik, Ekologik xavfsizlik Autentifikatsiya faktorlari nechta J: 3 Kriptografiyada matn – J: alifbo elementlarining tartiblangan to'plami Konfidentsiallikga to'g'ri ta'rif keltiring. J: axborot inshonchiligi, tarqatilishi mumkin emasligi, maxfiyligi kafolati; Shaxsning, o'zini axborot kommunikatsiya tizimiga tanishtirish jarayonida qo'llaniladigan belgilar ketma- :ketligi bo'lib, axborot kommunikatsiya tizimidan foydalanish huquqiga ega bo'lish uchun foydalaniluvchining maxfiy bo'lmagan qayd yozuvi – bu? J: login Kriptoanaliz – J: kalitlarni bilmasdan shifrnı ochishga bardoshlilikni aniqlovchi shifrlash tavsifi sifatarga ega bo'lishi kerak? J: ishonchli, qimmatli va to'liq Shifrlash – J: akslantirish jarayoni: ochiq matn deb nomlanadigan matn shifrmatnga almashtiriladi Qo'yish, o'rin almashtirish, gammalash kriptografiyaning qaysi turiga bog'liq? J: simmetrik kriptosistemalar Foydalanishni boshqarish –bu... J: Subyektnı Obyektga ishlash qobilyatini aniqlashdir. Kompyuterning tashqi interfeysi deganda nima tushuniladi? J: kompyuter bilan tashqi qurilmani bog'lovchi simlar va ular orqali axborot almashinish qoidalari to'plamlari Kodlash nima? J: Ma'lumotni osongina qaytarish uchun hammaga Tarmoq kartasi bu... J: Hisoblash qurilmasining ajralmas qismi bo'lib, qurilmani tarmoqqa ulash imkoniyatini taqdim etadi. Elektron raqamli imzo deb – J: xabar muallifi va tarkibini aniqlash maqsadida shifrmatnga qo'shilgan qo'shimcha Hab bu... J: ko'plab tarmoqlarni ulash uchun yoki LAN segmentlarini bog'lash uchun xizmat qiladi. Switch bu... J: Qabul qilingan signalni barcha chiquvchi portlarga emas balki paketda manzili keltirilgan portga uzatadi. Axborot xavfsizligining asosiy maqsadlaridan biri-: bu... J: Axborotlarni o'g'irlanishini, yo'qolishini,

soxtalashtirilishini oldini olish Uning egasi haqiqiylikni aniqlash jarayonida tekshiruv axboroti sifatida ishlatiladigan belgilar ketma-ketligi (maxfiy soʻz) – bu? J: parol Internetda elektron pochta bilan ishlash uchun TCP/IPga asoslangan qaysi protokoldan foydalaniladi? J: SMTP, POP yoki IMAR Kalit taqsimlashda koʻproq nimalarga eʼtibor beriladi? J: Tez, aniq va maxfiyligiga Agar Subyektning xavfsizlik darajasi Obyektning xavfsizlik darajasida boʻlsa, u holda qanday amalga ruxsat beriladi. J: Yozish Qanday xujumda hujumchi mijozlarga, foydalanuvchilarga va tashkilotlarda mavjud boʻlgan biror xizmatni cheklashga urinadi? J: Xizmatdan voz kechishga undash (Denial of service, DOS) hujumlari Kalit – bu ... J: Matnni shifrlash va shifrini ochish uchun kerakli axborot Elektr signallarini qabul qilish va uzatish vazifalarini OSI modelining qaysi satxi bajaradi J: Fizik satx Blokli shifrlash-: J: shifrlanadigan matn blokiga qoʻllaniladigan asosiy akslantirish Kriptobardoshlilik deb ... J: kalitlarni bilmasdan shifrnı ochishga bardoshlilikni aniqlovchi shifrlash tavsifi Maʼlumotlar butunligi qanday algritmlar orqali amalga oshiriladi J: Xesh funksiyalar Kriptografiya – J: axborotni qayta akslantirishning matematik usullarini izlaydi va tadqiq qiladi Keltirilgan protokollarning qaysilari transport satxi protokollariga mansub J: TCP,UDP Tekstni boshqa tekst ichida maʼnosini yashirib keltirish bu -: J: steganografiya Yaxlitlikni buzilishi bu -: ... J: Soxtalashtirish va oʻzgartirish Biometrik autentifikatsiyalash usullari anʼanaviy usullarga nisbatan avfzalliklari qaysi javobda toʻgʻri koʻrsatilgan? J: barchasi Keltirilgan protokollarning qaysilari kanal satxi protokollariga mansub J: Ethernet, FDDI Avtorizatsiya tushunchasi odatda qaysi tushuncha bilan sinonim sifatida ham foydalanadi? J: Foydalanishni boshqarish Tarmoq repiteri bu... J: Signalni tiklash yoki qaytarish uchun foydalaniladi. Ochiq kalitli kriptotizimlarning mohiyati nimadan iborat? J: Ochiq kalitli kriptotizimlarda bir-biri bilan matematik bogʻlangan 2 ta – ochiq va yopiq kalitlardan foydalaniladi Agar Subyektning xavfsizlik darajasida Obyektning xavfsizlik darajasi mavjud boʻlsa, u holda uchun qanday amalga ruxsat beriladi J: Oʻqish MAC usuli bilan foydalanishni boshqarishda xavfsizlik markazlashgan holatda kim tomonidan amalga oshiriladi J: xavfsizlik siyosati maʼmuri Berilgan taʼriflardan qaysi biri asimmetrik tizimlarga xos? J: Asimmetrik kriptotizimlarda  $k_1 \neq k_2$  boʻlib,  $k_1$  ochiq kalit,  $k_2$  yopiq kalit deb yuritiladi,  $k_1$  bilan axborot shifrlanadi,  $k_2$  bilan esa deshifrlanadi Maʼlumotlarni uzatishning optimal marshrutlarini aniqlash vazifalarini OSI modelining qaysi satxi bajaradi J: Tarmoq satxi Foydalanishni boshqarishning mandatli modelida Obyektning xavfsizlik darajasi nimaga bogʻliq.. J: Tashkilotda Obyektning muhimlik darajasi bilan yoki yoʻqolgan taqdirda keltiradigan zarar miqdori bilan xarakterlanadi Qaysi juftlik RSA algoritmining ochiq va yopiq kalitlarini ifodalaydi J:  $\{d, n\}$  – yopiq,  $\{e, n\}$  – ochiq; Diskni shifrlash nima uchun amalga oshiriladi? J: Maʼlumotni saqlash vositalarida saqlangan maʼlumot konfidensialligini taʼminlash uchun amalga oshiriladi Tahdid nima? J: Tashkilotga zarar yetkazishi mumkin boʻlgan istalmagan hodisa. Risk J: Potensial foyda yoki zarar barcha kabel va tarmoq tizimlari; tizim va kabellarni fizik nazoratlash; tizim va kabel uchun quvvat manbai; tizimni madadlash muhiti. Bular tarmoqning qaysi satxiga kiradi? J: Fizik satx Identifikatsiya, autentifikatsiya jarayonlaridan oʻtgan foydalanuvchi uchun tizimda bajarishi mumkin boʻlgan amallarga ruxsat berish jarayoni bu... J: Avtorizatsiya Xavfsizlikning asosiy yoʻnalishlarini sanab oʻting. J: Axborot xavfsizligi, Iqtisodiy xavfsizlik, Mudofaa xavfsizligi, Ijtimoiy xavfsizlik, Ekologik xavfsizlik Kompyuter tarmoqlari bu – J: Bir biriga osonlik bilan maʼlumot va resurslarni taqsimlash uchun ulangan Elektron raqamli imzo tizimi qanday muolajalarni amalga oshiradi? J: raqamli imzoni shakllantirish va tekshirish muolajasi Kriptografiyada matn – J: alifbo elementlarining tartiblangan toʻplami Autentifikatsiya jarayoni qanday jarayon? J: obyekt yoki subhektning unga berilgan identifikatorga mosligini tekshirish va belgilar ketmaketligidan iborat maxfiy kodini tekshirish orqali aslligini aniqlash Rol tushunchasiga taʼrif bering. J: Muayyan faoliyat turi bilan

bog'liq harakatlar va majburiyatlar to'plami sifatida belgilanishi mumkin Avtorizatsiya jarayoni qanday jarayon? J: foydalanuvchining resursdan foydalanish huquqlari va ruxsatlarini tekshirish jarayoni Faqat foydalanuvchiga ma'lum va biror tizimda autentifikatsiya jarayonidan o'tishni ta'minlovchi biror axborot nima J: Parol Elektron raqamli imzo deb – J: xabar muallifi va tarkibini aniqlash maqsadida shifratma qo'shilgan qo'shimcha TCP/IP modelida nechta satx mavjud J: 4 Kriptoanaliz – J: kalitlarni bilmasdan shifrni ochishga bardoshlilikni aniqlovchi shifrlash tavsifi Shifrlashning kombinatsiyalangan usulida qanday kriptotizimlarning kriptografik kalitlaridan foydalaniladi? J: Simmetrik va assimetrik Shifrlash nima? J: Ma'lumot boshqa formatga o'zgartiriladi, barcha shaxslar kalit yordamida qayta o'zgartirishi mumkin bo'ladi Kriptografiyada alifbo – J: axborot belgilarini kodlash uchun foydalaniladigan chekli to'plam Kripto tizimga qo'yiladigan umumiy talablardan biri J: shifr matn uzunligi ochiq matn uzunligiga teng bo'lishi kerak Simmetrik kriptotizimning uzluksiz tizimida ... J: ochiq matnning har bir harfi va simvoli alohida shifrlanadi Axborot resursi – bu? J: axborot tizimi tarkibidagi elektron shakldagi axborot, ma'lumotlar banki, ma'lumotlar bazasi Stenografiya ma'nosi... J: sirli yozuv Identifikatsiya jarayoni qanday jarayon? J: axborot tizimlari obyekt va subhektlariga uni tanish uchun nomlar (identifikator) berish va berilgan nom bo'yicha solishtirib uni aniqlash jarayoni Ma'lumotlarni inson xatosi tufayli yo'qolish sababini belgilang. J: Ma'lumotlarni saqlash vositasini to'g'ri joylashtirilmagani yoki ma'lumotlar bazasini xatolik bilan boshqarilganligi. 2. Qo'yish, o'rin almashtirish, gammalash kriptografiyaning qaysi turiga bog'liq? J: simmetrik kriptotizimlar 3. Quyidagilardan lokal tarmoqqa berilgan ta'rifni belgilang. J: Kompyuterlar va ularni bog'lab turgan qurilmalardan iborat bo'lib, ular odatda bitta tarmoqda bo'ladi. 4. Uning egasi haqiqiyligini aniqlash jarayonida tekshiruv axboroti sifatida ishlatiladigan belgilar ketma-ketligi (maxfiy so'z) – nima? J: parol 5. Rol tushunchasiga ta'rif bering. Muayyan faoliyat turi bilan bog'liq harakatlar va majburiyatlar to'plami sifatida belgilanishi mumkin 6. Foydalanish huquqini cheklovchi matritsa modeli bu... J: Bella La-Padulla modeli 8. Shifrtakstni ochiq tekstga akslantirish jarayoni nima deb ataladi? J: Deshifrlash 9. Axborot xavfsizligiga bo'ladigan tahdidlarning qaysi biri maqsadli (atayin) tahdidlar deb hisoblanadi? J: Strukturalarni ruxsatsiz modifikatsiyalash 10. Shifrlash kaliti noma'lum bo'lganda shifrlangan ma'lumotni deshifrlash qiyinlik darajasini nima belgilaydi? J: Kriptobardoshlik 11. Foydalanishni boshqarish – bu... J: Sub'ektni Ob'ektga ishlash qobiliyatini aniqlashdir. 12. Lokal tarmoqlarda keng tarqalgan topologiya turi qaysi? J: Yulduz 13. RSA algoritmi qaysi yilda ishlab chiqilgan? J: 1977 yil 14. Elektron xujjatlarni yo'q qilish usullari qaysilar? J: Shredirlash, magnitsizlantirish, yanchish 15. Kriptografiyada kalitning vazifasi nima? J: Matnni shifrlash va shifrni ochish uchun kerakli axborot 16. WiMAX qanday simsiz tarmoq turiga kiradi? J: Regional 17. Shaxsning, axborot kommunikatsiya tizimidan foydalanish huquqiga ega bo'lish uchun foydalaniluvchining maxfiy bo'lmagan qayd yozuvi – bu... J: login 18. Stenografiya ma'nosi qanday? J: sirli yozuv 19. Fire Wall ning vazifasi... J: Tarmoqlar orasida aloqa o'rnatish jarayonida tashkilot va Internet tarmog'i orasida xavfsizlikni ta'minlaydi 20. Yaxlitlikni buzilishi bu - ... J: Soxtalashtirish va o'zgartirish 2. Rezident virus... tezkor xotirada saqlanadi 3. Tashkilot va uning AKT doirasida aktivlarni shu jumladan, kritik axborotni boshqarish, himoyalash va taqsimlashni belgilovchi qoidalar, ko'rsatmalar, amaliyoti fanda qanday nomladi? AKT xavfsizlik siyosati 4. O'chirilgan yoki formatlangan ma'lumotlarni tikovchi dasturni belgilang. Recuva, R.saver 5. Zaiflik – bu... tizimda mavjud bo'lgan xavfsizlik muammoasi bo'lib, ular asosan tizimning yaxshi shakllantirilmaganligi yoki sozlanmaganligi sababli kelib chiqadi. 6. Axborot xavfsizligi timsollarini ko'rsating. Alisa, Bob, Eva 7. Kiberetika tushunchasi: Kompyuter va kompyuter tarmoqlarida odamlarning etikasi 8. "Axborot olish va kafolatlari va erkinligi to'g'risda"gi Qonuni qachon kuchga



kirgan? 1997 yil 24 aprel 9. DIR viruslari nimani zararlaydi? FAT tarkibini zararlaydi 10. Virusning signaturasi (virusga taalluqli baytlar ketmaketligi) bo'yicha operativ xotira va fayllarni ko'rish natijasida ma'lum viruslarni topuvchi va xabar beruvchi dasturiy ta'minot nomi nima deb ataladi? Detektorlar 11. Agar foydalanuvchi tizimda ma'lumot bilan ishlash vaqtida ham zahiralash amalga oshirilishi .... deb ataladi? "Issiq xaxiralash" 12. Aksariyat tijorat tashkilotlari uchun ichki tarmoq xavfsizligini taminlashning zaruriy sharti-bu... Tamoqlararo ekranlarning o'rnatilishi 13. Axborot xavfsizligida axborotning bahosi qanday aniqlanadi? Axborot xavfsizligi buzilgan taqdirda ko'rilishi mumkin bo'lgan zarar miqdori bilan 14. Kompyuter yoki boshqa qurilmalarga qarshi qilingan yoki kompyuter va boshqa qurilmalar orqali qilingan jinoyat-... Kiberjinoyat deb ataladi 15. Antiviruslarni, qo'llanish usuliga ko'ra... turlari mavjud? detektorlar, faglar, vaktinalar, privivkalar, revizorlar, monitorlar 16. Qaysi siyosatga ko'ra faqat ma'lum xavfli xizmatlar/hujumlar yoki harakatlar bloklanadi? Ruxsat berishga asoslangan siyosat 17. DIR viruslari nimani zararlaydi? FAT tarkibini zararlaydi 18. Makroviruslar nimalarni zararlaydi? Ma'lum dasturlash tilida yozilgan va turli ofis ilovalari – MS Word hujjati, MS Excel elektron jadvali, Corel Draw tasviri, fayllarida joylashgan “makroslar” yoki “skriptlar”ni zararlaydi. 19. Ma'lumotlarni zahira nusxasini saqllovchi va tikovchi dasturni belgilang. HandyBackup 20. Tizim ishlamay turganda yoki foydalanuvchilar ma'lumot bilan ishlamay turganda zahiralash amalga oshirilsa .... deb ataladi. "Sovuq saxiralash" 21. “Elektron hujjat” tushunchasi haqida to'g'ri ta'rif berilgan qatorni ko'rsating. Elektron shaklda qayd etilgan, elektron raqamli imzo bilan tasdiqlangan va elektron hujjatning uni identifikatsiya qilish imkoniyatini beradigan boshqa rekvizitlariga ega bo'lgan axborot elektron hujjatdir 22. Polimorf viruslar tushunchasi to'g'ri ko'rsating. Viruslar turli ko'rinishdagi shifrlangan viruslar bo'lib, o'zining ikkilik shaklini nusxadan-nusxaga o'zgartirib boradi 23. Fishing (ing. Phishing – baliq ovlash) bu... Internetdagi firibgarlikning bir turi bo'lib, uning maqsadi foydalanuvchining maxfiy ma'lumotlaridan, login/parol, foydalanish imkoniyatiga ega bo'lishdir. Xavfsizlikning asosiy yo'nalishlarini sanab o'ting. Axborot xavfsizligi, Iqtisodiy xavfsizlik, Mudofaa xavfsizligi, Ijtimoiy xavfsizlik, Ekologik xavfsizlik Axborot xavfsizligining asosiy maqsadlaridan biri- bu... Axborotlarni o'g'irlanishini, yo'qolishini, soxtalashtirilishini oldini olish Konfidentsiallikga to'g'ri ta'rif keltiring. axborot inshonchliligi, tarqatilishi mumkin emasligi, maxfiyligi kafolati; Yaxlitlikni buzilishi bu - ... Soxtalashtirish va o'zgartirish ... axborotni himoyalash tizimi deyiladi. Axborotning zaif tomonlarini kamaytiruvchi axborotga ruxsat etilmagan kirishga, uning chiqib ketishiga va yo'qotilishiga to'sqinlik qiluvchi tashkiliy, texnik, dasturiy, texnologik va boshqa vosita, usul va choralarning ko Kompyuter virusi nima? maxsus yozilgan va zararli dastur Axborotni himoyalash uchun ... usullari qo'llaniladi. kodlashtirish, kriptografiya, stegonografiya Stenografiya mahnosi... sirli yozuv Kriptologiya yo'nalishlari nechta? 2 Kriptografiyaning asosiy maqsadi... maxfiylik, yaxlitlikni ta'minlash SMTP - Simple Mail Transfer protokol nima? elektron pochta protokoli SKIP protokoli... Internet protokollari uchun kriptokalitlarning oddiy boshqaruvi Kompyuter tarmog'ining asosiy komponentlariga nisbatan xavf-xatarlar... uzilish, tutib qolish, o'zgartirish, soxtalashtirish ...ma'lumotlar oqimini passiv hujumlardan himoya qilishga xizmat qiladi. konfidentsiallik Foydalanish huquqini cheklovchi matritsa modeli bu... Bella La-Padulla modeli Kommunikatsion qism tizimlarida xavfsizlikni ta'minlanishida necha xil shifrlash ishlatiladi? 2 Kompyuter tarmoqlarida tarmoqning uzoqlashtirilgan elementlari o'rtasidagi aloqa qaysi standartlar yordamida amalga oshiriladi? TCP/IP, X.25 protokollar Himoya tizimi kompleksligiga nimalar orqali erishiladi? Xuquqiy tashkiliy, muhandis, texnik va dasturiy matematik elementlarning mavjudligi orqali Kalit – bu ... Matnni shifrlash va shifrini ochish uchun kerakli axborot Qo'yish, o'rin almashtirish, gammalash kriptografiyaning qaysi turiga bog'liq? simmetrik kriptotizimlar

Autentifikatsiya nima? Ma'lum qilingan foydalanuvchi, jarayon yoki qurilmaning haqiqiy ekanligini tekshirish muolajasi Identifikatsiya bu- ... Foydalanuvchini uning identifikatori (nomi) bo'yicha aniqlash jarayoni O'rin almashtirish shifri bu - ... Murakkab bo'lmagan kriptografik akslantirish Simmetrik kalitli shifrlash tizimi necha turga bo'linadi. 2 turga Kalitlar boshqaruvi 3 ta elementga ega bo'lgan axborot almashinish jarayonidir bular ... hosil qilish, yig'ish, taqsimlash Kriptologiya - axborotni qayta akslantirib himoyalash muammosi bilan shug'ullanadi Kriptografiyada alifbo - axborot belgilarini kodlash uchun foydalaniladigan chekli to'plam Simmetrik kriptotizimlarda ... jumlani davom ettiring shifrlash va shifrnı ochish uchun bitta va aynan shu kalitdan foydalaniladi Kriptobardoshlilik deb ... kalitlarni bilmasdan shifrnı ochishga bardoshlilikni aniqlovchi shifrlash tavsifi Elektron raqamli imzo deb - xabar muallifi va tarkibini aniqlash maqsadida shifrmatnga qo'shilgan qo'shimcha Kriptografiya - axborotni qayta akslantirishning matematik usullarini izlaydi va tadqiq qiladi Kriptografiyada matn - alifbo elementlarining tartiblangan to'plami Kriptoanaliz - kalitlarni bilmasdan shifrnı ochishga bardoshlilikni aniqlovchi shifrlash tavsifi Shifrlash - akslantirish jarayoni: ochiq matn deb nomlanadigan matn shifrmatnga almashtiriladi Kalit taqsimlashda ko'proq nimalarga e'tibor beriladi? Tez, aniq va maxfiyligiga Faol hujum turi deb... Maxfiy uzatish jarayonini uzib qo'yish, modifikatsiyalash, qalbaki shifr ma'lumotlar tayyorlash harakatlaridan iborat jarayon Blokli shifrlash- shifrlanadigan matn blokiga qo'llaniladigan asosiy akslantirish Simmetrik kriptotizmning uzluksiz tizimida ... ochiq matnning har bir harfi va simvoli alohida shifrlanadi Kripto tizimga qo'yiladigan umumiy talablardan biri shifr matn uzunligi ochiq matn uzunligiga teng bo'lishi kerak Quyidagi tengliklardan qaysilari shifrlash va deshifrlashni ifodalaydi?  $E_k(T)=T$ ,  $D_k(T)=T$  Berilgan ta'riflardan qaysi biri assimetrik tizimlarga xos? Assimetrik kriptotizimlarda  $k_1 \neq k_2$  bo'lib,  $k_1$  ochiq kalit,  $k_2$  yopiq kalit deb yuritiladi,  $k_1$  bilan axborot shifrlanadi,  $k_2$  bilan esa deshifrlanadi Yetarlicha kriptoturg'unlikka ega, dastlabki matn simvollarini almashtirish uchun bir necha alfavitdan foydalanishga asoslangan almashtirish usulini belgilang Vijnier matritsasi, Sesar usuli Akslantirish tushunchasi deb nimaga aytiladi? 1- to'plamli elementlariga 2-to'plam elementalriga mos bo'lishiga Simmetrik guruh deb nimaga aytiladi? O'rin almashtirish va joylashtirish Qo'yish, o'rin almashtirish, gammalash kriptografiyaning qaysi turiga bog'liq? simmetrik kriptositemalar Xavfli viruslar bu - ... kompyuter ishlashida jiddiy nuqsonlarga sabab bo'luvchi viruslar Mantiqiy bomba - bu ... Ma'lum sharoitlarda zarar keltiruvchi harakatlarni bajaruvchi dastur yoki uning alohida modullari Elektron raqamli imzo tizimi qanday muolajani amalga oshiradi? raqamli imzoni shakllantirish va tekshirish muolajasi Shifrlashning kombinatsiyalangan usulida qanday kriptotizimlarning kriptografik kalitlaridan foydalaniladi? Simmetrik va assimetrik Axborot himoyasi nuqtai nazaridan kompyuter tarmoqlarini nechta turga ajratish mumkin? Korporativ va umumfoydalanuvchi Elektromagnit nurlanish va ta'sirlanishlardan himoyalash usullari nechta turga bo'linadi? Sust va faol Internetda elektron pochta bilan ishlash uchun TCP/IPga asoslangan qaysi protokoldan foydalaniladi? SMTP, POP yoki IMAR Axborot resursi - bu? axborot tizimi tarkibidagi elektron shakldagi axborot, ma'lumotlar banki, ma'lumotlar bazasi Shaxsning, o'zini axborot kommunikatsiya tizimiga tanishtirish jarayonida qo'llaniladigan belgilar ketmaketligi bo'lib, axborot kommunikatsiya tizimidan foydalanish huquqiga ega bo'lish uchun foydalaniluvchining maxfiy bo'lmagan qayd yozuvi - bu? login Uning egasi haqiqiyligini aniqlash jarayonida tekshiruv axboroti sifatida ishlatiladigan belgilar ketmaketligi (maxfiy so'z) - bu? parol Identifikatsiya jarayoni qanday jarayon? axborot tizimlari ob'yekt va subhektlariga uni tanish uchun nomlar (identifikator) berish va berilgan nom bo'yicha solishtirib uni aniqlash jarayoni Autentifikatsiya jarayoni qanday jarayon? ob'yekt yoki subhektning unga berilgan identifikatorga mosligini tekshirish va belgilar ketmaketligidan iborat maxfiy kodini

tekshirish orqali aslligini aniqlash Avtorizatsiya jarayoni qanday jarayon? foydalanuvchining resursdan foydalanish huquqlari va ruxsatlarini tekshirish jarayoni Ro'yxatdan o'tish bu? foydalanuvchilarni ro'yxatga olish va ularga dasturlar va ma'lumotlarni ishlatishga huquq berish jarayoni Axborot qanday sifatlarga ega bo'lishi kerak? ishonchli, qimmatli va to'liq Axborotning eng kichik o'lchov birligi nima? bit Elektronhujjatning rekvizitlari nechta qismdan iborat? 4 Axborotlarni saqlovchi va tashuvchi vositalar qaysilar? fleshka, CD va DVD disklar Imzo bu nima? hujjatning haqiqiylikini va yuborgan fizik shaxsga tegishli ekanligini tasdiqlaydigan insonning fiziologik xususiyati. Muhr bu nima? hujjatning haqi-qiylikini va biror bir yuridik shaxsga tegishli ekanligi-ni tasdiqlovchi isbotdir. DSA – nima Raqamli imzo algoritmi El Gamal algoritmi qanday algoritm Shifrlash algoritmi va raqamli imzo algoritmi Sezarning shifrlash sistemasining kamchiligi Harflarning so'zlarda kelish chastotasini yashirmaydi Axborot xavfsizligi va xavfsizlik san'ati haqidagi fan .... deyiladi? Kriptografiya Tekstni boshqa tekst ichida ma'nosini yashirib keltirish bu - steganografiya Shifrttekstni ochiq tekstga akslantirish jarayoni nima deb ataladi? Deshifrlash ..... – hisoblashga asoslangan bilim sohasi bo'lib, buzg'unchilar mavjud bo'lgan jaroitda amallarni kafolatlash uchun o'zida texnologiya, inson, axborot va jarayonni mujassamlashtirgan. Kiberxavfsizlik Risk Potensial foyda yoki zarar Kiberxavfsizlik nechta bilim sohasini o'z ichiga oladi. 8 “Ma'lumotlar xavfsizligi” bilim sohasi..... ma'lumotlarni saqlashda, qayta ishlashda va uzatishda himoyani ta'minlashni maqsad qiladi. “Dasturiy ta'minotlar xavfsizligi” bilim sohasi..... foydalanilayotgan tizim yoki axborot xavfsizligini ta'minlovchi dasturiy ta'minotlarni ishlab chiqish va foydalanish jarayoniga e'tibor qaratadi. “Tashkil etuvchilar xavfsizligi” ..... katta tizimlarda integrallashgan tashkil etuvchilarni loyihalash, sotib olish, testlash, analiz qilish va texnik xizmat ko'rsatishga e'tibor qaratadi. “Aloqa xavfsizligi” bilim sohasi..... tashkil etuvchilar o'rtasidagi aloqani himoyalashga etibor qaratib, o'zida fizik va mantiqiy ulanishni birlashtiradi. “Tizim xavfsizligi” bilim sohasi..... tashkil etuvchilar, ulanishlar va dasturiy ta'minotdan iborat bo'lgan tizim xavfsizligining aspektlariga e'tibor qaratadi. “Inson xavfsizligi” bilim sohasi.... kiberxavfsizlik bilan bog'liq inson hatti harakatlarini o'rganishdan tashqari, tashkilotlar (masalan, xodim) va shaxsiy hayot sharoitida shaxsiy ma'lumotlarni va shaxsiy hayotni himoya qilishga e'tibor qaratadi. “Tashkilot xavfsizligi” bilim sohasi .... tashkilotni kiberxavfsizlik tahdidlaridan himoyalash va tashkilot vazifasini muvaffaqiyatli bajarishini “Jamoat xavfsizligi” bilim sohasi ..... u yoki bu darajada jamiyatda ta'sir ko'rsatuvchi kiberxavfsizlik omillariga e'tibor qaratadi. Tahdid nima? tizim yoki Tashkilotga zarar yetkazishi mumkin bo'lgan istalmagan hodisa. Kodlash nima? Ma'lumotni osongina qaytarish uchun hammaga ochiq bo'lgan sxema yordamida ma'lumotlarni boshqa formatga o'zgartirishdir Shifrlash nima? Ma'lumot boshqa formatga o'zgartiriladi, biroq uni faqat maxsus shaxslar qayta o'zgartirishi mumkin bo'ladi Bir martalik bloknotda Qanday kalitlardan foydalaniladi? Ochiq kalitdan Ikkilik sanoq tizimida berilgan 10111 sonini o'nlik sanoq tizimiga o'tkazing. 23 Agar RSA algotirmida n ochiq kalitni, d maxfiy kalitni ifodalasa, qaysi formula deshifrlashni ifodalaydi.  $M = C^d \bmod n$ ; O'nlik sanoq tizimida berilgan quyidagi sonlarni ikkil sanoq tizi miga o'tkazing. 65 100001 Quyidagi modulli ifodani qiymatini toping.  $(125 \cdot 45) \bmod 10$ . 5 Quyidagi modulli ifodani qiymatini toping  $(148 + 14432) \bmod 256$ . 244 Agar RSA algotirmida e ochiq kalitni, d maxfiy kalitni ifodalasa, qaysi formula deshifrlashni ifodalaydi.  $C = M^e \bmod n$ ; - tog'ri javob Axborotni shifrnı ochish (deshifrlash) bilan qaysi fan shug'ullanadi Kriptologiya. Qaysi juftlik RSA algoritmining ochiq va yopiq kalitlarini ifodalaydi {d, n} – yopiq, {e, n} – ochiq; Zamonaviy kriptografiya qanday bo'limlardan iborat? Simmetrik kriptotizimlar; ochiq kalitli kriptotizimlar; Elektron raqamli imzo; kalitlarni boshqarish 1. Kriptografik usullardan foydalanishning asosiy yo'nalishlari nimalardan iborat? Aloqa kanali orqali maxfiy axborotlarni

uzatish (masalan, elektron pochta orqali), uzatiliyotgan xabarlarini haqiqiylikni aniqlash, tashuvchilarda axborotlarni shifrlangan ko Shifr nima? Shifrlash va deshifrlashda foydalaniladigan matematik funktsiyadan iborat bo'lgan kriptografik algoritm Ochiq kalitli kriptotizimlarning mohiyati nimadan iborat? Ochiq kalitli kriptotizimlarda bir-biri bilan matematik bog'langan 2 ta – ochiq va yopiq kalitlardan foydalaniladi Oqimli shifrlashning mohiyati nimada? Oqimli shifrlash birinchi navbatda axborotni bloklarga bo'lishning imkoni bo'lmagan hollarda zarur, Qandaydir ma'lumotlar oqimini har bir belgisini shifrlab, boshqa belgilarini kutmasdan kerakli joyga jo'natish uchun o Simmetrik algoritmlarni xavfsizligini ta'minlovchi omillarni ko'rsating. uzatilayotgan shifrlangan xabarni kalitsiz ochish mumkin bo'lmashligi uchun algoritm yetarli darajada bardoshli bo'lishi lozim, uzatilayotgan xabarni xavfsizligi algoritmni maxfiyligiga emas Kriptotizim quyidagi komponentlardan iborat: ochiq matnlar fazosi M, Kalitlar fazosi K, Shifrmtnlar fazosi C, Ek :  $M \oplus C$  (shifrlash uchun) va Dk:  $C \oplus M$  (deshifrlash uchun) funktsiyalar Serpent, Square, Twofish, RC6 , AES algoritmlari qaysi turiga mansub? simmetrik blokli algoritmlar DES algoritmgiga muqobil bo'lgan algoritmni ko'rsating. Uch karrali DES, IDEA, Rijndael DES algoritmining asosiy muammosi nimada? kalit uzunligi 56 bit. Bugungu kunda ushbu uzunlik algoritmning kriptobardoshliligi uchun yetarli emas Asimmetrik kriptotizimlar qanday maqsadlarda ishlatiladi? shifrlash, deshifrlash, ERI yaratish va tekshirish, kalitlar almashish uchun  $12+22 \bmod 32$  ?  $2 \cdot 2+5 \bmod 32$  ?  $7$  Kriptografik elektron raqamli imzolarda qaysi kalitlar ma'lumotni yaxlitligini ta'minlashda ishlatiladi. ochiq kalitlar  $12+11 \bmod 16$  ?  $7$  RIJNDAEL algoritmi qancha uzunligdagi kalitlarni qo'llab quvvatlaydi. 128 bitli, 192 bitli, 256 bitli Xesh-funktsiyani natijasi ... uzunlikdagi xabar RSA algoritmi qanday jarayonlardan tashkil topgan Kalitni generatsiyalash; Shifrlash; Deshifrlash. RSA algoritmidan amalda foydalanish uchun tanlanuvchi tub sonlar uzunligi kamida necha bit bo'lishi talab etiladi. 2048 Ma'lumotlar butunligi qanday algritmlar orqali amalga oshiriladi Xesh funktsiyalar To'rtta bir-biri bilan bog'langan bog'lamlar strukturasi (kvadrat shaklida) qaysi topologiya turiga mansub Xalqa Qaysi topologiya birgalikda foydalanilmaydigan muhitni qo'llamasligi mumkin to'liq bog'lanishli Kompyuterning tashqi interfeysi deganda nima tushuniladi kompyuter bilan tashqi qurilmani bog'lovchi simlar va ular orqali axborot almashinish qoidalari to'plamlari Lokal tarmoqlarda keng tarqalgan topologiya turi qaysi Yulduz Ethernet kontsentratori qanday vazifani bajaradi kompyuterdan kelayotgan axborotni qolgan barcha kompyuterga yo'naltirib beradi OSI modelida nechta sath mavjud 7 OSI modelining to'rtinchi sathi qanday nomlanadi Transport sathi OSI modelining beshinchi sathi qanday nomlanadi Seanslar sathi OSI modelining birinchi sathi qanday nomlanadi Fizik sath OSI modelining ikkinchi sathi qanday nomlanadi Kanal sathi OSI modelining uchinchi sathi qanday nomlanadi Tarmoq sathi OSI modelining oltinchi sathi qanday nomlanadi Taqdimlash sathi OSI modelining ettinchi sathi qanday nomlanadi Amaliy sath OSI modelining qaysi sathlari tarmoqqa bog'liq sathlar hisoblanadi fizik, kanal va tarmoq sathlari OSI modelining tarmoq sathi vazifalari keltirilgan qurilmalarning qaysi birida bajariladi Marshrutizator Elektr signallarini qabul qilish va uzatish vazifalarini OSI modelining qaysi sathi bajaradi Fizik sath Ma'lumotlarni uzatishning optimal marshrutlarini aniqlash vazifalarini OSI modelining qaysi sathi bajaradi Tarmoq sathi Keltirilgan protokollarning qaysilari tarmoq sathi protokollariga mansub IP, IPX Keltirilgan protokollarning qaysilari transport sathi protokollariga mansub TCP,UDP OSI modelining fizik sathi qanday funktsiyalarni bajaradi Elektr signallarini uzatish va qabul qilish OSI modeliningamaliy sathi qanday funktsiyalarni bajaradi Klient dasturlari bilan o'zaro muloqotda bo'lish Keltirilgan protokollarning qaysilari kanal sathi protokollariga mansub Ethernet, FDDI Keltirilgan protokollarning qaysilari taqdimlash sathi protokollariga mansub SNMP, Telnet Identifikatsiya, autentifikatsiya jarayonlaridan o'tgan foydalanuvchi uchun tizimda bajarishi mumkin bo'lgan

amallarga ruxsat berish jarayoni bu... Avtorizatsiya Autentifikatsiya faktorlari nechta 3 Faqat foydalanuvchiga ma'lum va biror tizimda autentifikatsiya jarayonidan o'tishni ta'minlovchi biror axborot nima Parol Ko'z pardasi, yuz tuzilishi, ovoz temбри. Biometrik autentifikatsiya barcha kabel va tarmoq tizimlari; tizim va kabellarni fizik nazoratlash; tizim va kabel uchun quvvat manbai; tizimni madadlash muhiti. Bular tarmoqning qaysi satxiga kiradi. Fizik satx Fizik xavfsizlikda Yong'inga qarshi tizimlar necha turga bo'linadi 2 Avtorizatsiya tushunchasi odatda qaysi tushuncha bilan sinonim sifatida ham foydalanadi. Foydalanishni boshqarish Foydalanishni boshqarish –bu... sub'ektni sub'ektga ishlash qobiliyatini aniqlashdir. Foydalanishna boshqarishda inson, dastur, jarayon va xokazolar nima vazifani bajaradi, Sub'ekt Foydalanishna boshqarishda ma'lumot , resurs, jarayon nima vazifani bajaradi ? Ob'ekt Foydalanishna boshqarishning nechta usuli mavjud? 4 Foydalanishni boshqarishning qaysi usulida tizimdagi shaxsiy ob'ektlarni himoyalash uchun qo'llaniladi DAC Foydalanishni boshqarishning qaysi modelida ob'ekt egasining o'zi undan foydalanish huquqini va kirish turini o'zi belgilaydi DAC Foydalanishni boshqarishning qaysi usulida foydalanishlar sub'ektlar va ob'ektlarni klassifikatsiyalashga asosan boshqariladi. MAC Foydalanishni boshqarishning mandatli modelida Ob'ektning xavfsizlik darajasi nimaga bog'liq.. Tashkilotda ob'ektning muhimlik darajasi bilan yoki yo'qolgan taqdirda keltiradigan zarar miqdori bilan xarakterlanadi MAC usuli bilan foydalanishni boshqarishda xavfsizlik markazlashgan holatda kim tomonidan amalga oshiriladi xavfsizlik siyosati ma'muri Agar sub'ektning xavfsizlik darajasida ob'ektning xavfsizlik darajasi mavjud bo'lsa, u holda uchun qanday amalga ruxsat beriladi O'qish Agar sub'ektning xavfsizlik darajasi ob'ektning xavfsizlik darajasida bo'lsa, u holda qanday amalga ruxsat beriladi. Yozish Foydalanishni boshqarishning qaysi modelida har bir ob'ekt uchun har bir foydalanuvchini foydalanish ruxsatini belgilash o'rniga, rol uchun ob'ektlardan foydalanish ruxsati ko'rsatiladi? RBAC Rol tushunchasiga ta'rif bering. Muayyan faoliyat turi bilan bog'liq harakatlar va majburiyatlar to'plami sifatida belgilanishi mumkin Foydalanishni boshqarishning qaysi usuli - ob'ektlar va sub'ektlarning atributlari, ular bilan mumkin bo'lgan amallar va so'rovlarga mos keladigan muhit uchun qoidalarni tahlil qilish asosida foydalanishlarni boshqaradi. ABAC XACML foydalanishni boshqarishni qaysi usulining standarti? ABAC Biometrik autentifikatsiyalash usullari an'anaviy usullarga nisbatan avfzalliklari qaysi javobda to'g'ri ko'rsatilgan? barchasi Axborotning kriptografik himoya vositalari necha turda? 3 Dasturiy shifrlash vositalari necha turga bo'linadi 4 Diskni shifrlash nima uchun amalga oshiriladi? Ma'lumotni saqlash vositalarida saqlangan ma'lumot konfidensialligini ta'minlash uchun amalga oshiriladi Ma'lumotlarni yo'q qilish odatda necha hil usulidan foydalaniladi? 4 Kompyuter tarmoqlari bu – Bir biriga osonlik bilan ma'lumot va resurslarni taqsimlash uchun ulangan kompyuterlar guruhi Tarmoq modeli –bu.. ikki Hisoblash tizimlariorasidagi aloqani ularning ichki tuzilmaviy vatexnologik asosidan qat'iy nazar muvaffaqiyatli o'rnatilishini asosidir to'plami OSI modelida nechta tarmoq sathi bor 7 OSI modeli 7 stahi bu llova OSI modeli 1 stahi bu Fizik OSI modeli 2 stahi bu Kanal TCP/IP modelida nechta satx mavjud 4 Qanday tarmoq qisqa masofalarda qurilmalar o'rtasid a ma'lumot almashinish imkoniyatini taqdim etadi. Shaxsiy tarmoq Tarmoq kartasi bu... Hisoblash qurilmasining ajralmas qismi bo'lib, qurilmani tarmoqqa ulash imkoniyatini taqdim etadi. Switch bu... Qabul qilingan signalni barcha chiquvchi portlarga emas balki paketda manzili keltirilgan portga uzatadi Hab bu... ko'plab tarmoqlarni ulash uchun yoki LAN segmentlarini bog'lash uchun xizmat qiladi. Tarmoq repiteri bu... Signalni tiklash yoki qaytarish uchun foydalaniladi. Qanday tizim host nomlari va internet nomlarini IP manzillarga o'zgartirish yoki teskarisini amalga oshiradi. DNS tizimlari ..... protokoli ulanishga asoslangan protokol bo'lib, internet orqali ma'lumotlarni almashinuvchi turli ilovalar uchun tarmoq ulanishlarini sozlashga yordam beradi. TCP .... protokolidan odatda o'yin va

video ilovalar tomonidan keng foydalaniladi. UDP Qaysi protokol ma'lumotni yuborishdan oldin aloqa o'rnatish uchun zarur bo'lgan manzil ma'lumotlari bilan ta'minlaydi. IP Tarmoq taxdidlari necha turga bo'linadi 4 Qanday xujum asosiy hujumlarni oson amalga oshirish uchun tashkilot va tarmoq haqidagi axborotni to'plashni maqsad qiladi; Razvedka hujumlari Qanday xujum hujumchi turli texnologiyalardan foydalangan holda tarmoqqa kirishga harakat qiladi Kirish hujumlari Qanday xujum da hujumchi mijozlarga, foydalanuvchilarga va tashkilotlarda mavjud bo'lgan biror xizmatni cheklashga urinadi; Xizmatdan voz kechishga undash (Denial of service, DOS) hujumlari Qanday xujumdp zararli hujumlar tizim yoki tarmoqqa bevosita va bilvosita ta'sir qiladi; Zararli hujumlar Elektron raqamli imzo algoritmi qanday bosqichlardan iborat bo'ladi? Imzo qo'yish va imzoni tekshirishdan Imzoni haqiqiyiligini tekshirish qaysi kalit yordamida amalga oshiriladi? Imzo muallifining ochiq kaliti yordamida Tarmoq modeli-bu... Ikki hisoblash tizimlari orasidagi aloqani ularning ichki tuzilmaviy va texnologik asosidan qat'iy nazar muvaffaqiyatli o'rnatilishini asosidir OSI modeli nechta sathga ajraladi? 7 Fizik sathning vazifasi nimadan iborat Qurilma, signal va binar o'zgartirishlar Ilova sathning vazifasi nimadan iborat Ilovalarni tarmoqqa ulanish jarayoni Kanal sathning vazifasi nimadan iborat Fizik manzillash Tarmoq sathning vazifasi nimadan iborat Yo'lni aniqlash va mantiqiy manzillash TCP/IP modeli nechta sathdan iborat 4 Quyidagilarninf qaysi biri Kanal sathi protokollari Ethernet, Token Ring, FDDI, X.25, Frame Relay, RS-232, v.35. Quyidagilarninf qaysi biri tarmoq sathi protokollari . IP, ICMP, ARP, RARP Quyidagilarninf qaysi biri transport sathi protokollari TCP, UDP, RTP Quyidagilarninf qaysi biri ilova sathi protokollari HTTP, Telnet, FTP, TFTP, SNMP, DNS, SMTP va hak TCP/IP modelining kanal sathiga OSI modelining qaysi sathlari mos keladi Kanal, Fizik TCP/IP modelining tarmoq sathiga OSI modelining qaysi sathlari mos keladi Tarmoq TCP/IP modelining transport sathiga OSI modelining qaysi sathlari mos keladi Transport TCP/IP modelining ilova sathiga OSI modelining qaysi sathlari mos keladi Ilova, taqdimot, seans Quyidagilardan lokal tarmoqqa berilgan ta'rifni belgilang. Kompyuterlar va ularni bog'lab turgan qurilmalardan iborat bo'lib, ular odatda bitta tarmoqda bo'ladi. Quyidagilardan mintaqaviy tarmoqqa berilgan ta'rifni belgilang. . Odatda ijaraga olingan telekommunikatsiya liniyalaridan foydalanadigan tarmoqlardagi tugunlarni birbiriga bog'laydi. Quyidagilardan MAN tarmoqqa berilgan ta'rifni belgilang. Bu tarmoq shahar yoki shaharcha bo'ylab tarmoqlarning o'zaro bog'lanishini nazarda tutadi Quyidagilardan shaxsiy tarmoqqa berilgan ta'rifni belgilang. Qisqa masofalarda qurilmalar o'rtasida ma'lumot almashinish imkoniyatini taqdim etadi Quyidagilardan qaysi biri tarmoqning yulduz topologiyasiga berilgan Tarmoqda har bir kompyuter yoki tugun markaziy tugunga individual bog'langan bo'ladi Quyidagilardan qaysi biri tarmoqning shina topologiyasiga berilgan Tarmoqda yagona kabel barcha kompyuterlarni o'zida birlashtiradi Quyidagilardan qaysi biri tarmoqning halqa topologiyasiga berilgan Yuboriluvchi va qabul qilinuvchi ma'lumot TOKYeN yordamida manziliga yetkaziladi Quyidagilardan qaysi biri tarmoqning mesh topologiyasiga berilgan Tarmoqdagi barcha kompyuter va tugunlar bir-biri bilan o'zaro bog'langan bo'ladi Tarmoq kartasi nima? Hisoblash qurilmasining ajralmas qismi bo'lib, qurilmani tarmoqqa ulash imkoniyatini taqdim etadi Repetir nima? Odatda signalni tiklash yoki qaytarish uchun foydalaniladi Hub nima? Tarmoq qurilmasi bo'lib, ko'plab tarmoqlarni ulash uchun yoki LAN segmentlarini bog'lash uchun xizmat qiladi Switch nima? Ko'plab tarmoqlarni ulash uchun yoki LAN segmentlarini bog'lash uchun xizmat qiladi. Qabul qilingan signalni barcha chiquvchi portlarga emas balki paketda manzili keltirilgan portga uzatadi Router nima? Qabul qilingan ma'lumotlarni tarmoq sathiga tegishli manzillarga ko'ra (IP manzil) uzatadi DNS tizimlari. Host nomlari va internet nomlarini IP manzillarga o'zgartirish yoki teskarisini amalga oshiradi TCP bu- ... Transmission Control Protocol UDP bu-... User datagram protocol Tarmoq xavfsizligiga

tahdidlar tavsiflangan bandni belgilang Ichki, tashqi Tarmoq xavfsizligining buzilishi natijasida biznes faoliyatining buzilishi qanday oqibatlarga olib keladi Biznes jarayonlarni to'xtab qolishiga olib keladi Tarmoq xavfsizligining buzilishi natijasida ishlab chiqarishning yo'qolishi qanday oqibatlarga olib keladi Hujum natijasida ishlab chiqarishi yo'qolgan hollarda uni qayta tiklash ko'p vaqt talab qiladi va bu vaqtda ishlab chiqarish to'xtab qoladi Tarmoq xavfsizligining buzilishi natijasida maxfiylikni yo'qolishi qanday oqibatlarga olib keladi Konfidensial axborotni chiqib ketishi natijasida, tashkilot shaxsiy ma'lumotlarini yo'qolishi mumkin Tarmoq xavfsizligining buzilishi natijasida axborotning o'g'irlanishi qanday oqibatlarga olib keladi Tashkilot xodimlarining shaxsiy va ishga oid ma'lumotlarini kutilmaganda oshkor bo'lishi ushbu xodimlarga bevosita ta'sir qiladi Quyidagi ta'riflardan qaysi biri tarmoqning texnologik zaifligini ifodalaydi Tarmoq qurilmalari, switch yoki routerlardagi autentifikatsiya usullarining yetarlicha bardoshli bo'lmashligi Quyidagi ta'riflardan qaysi biri tarmoqning sozlanishdagi zaifligini ifodalaydi tizim xizmatlarini xavfsiz bo'lmagan tarzda sozlanishi, joriy sozlanish holatida qoldirish, parollarni noto'g'ri boshqarilishi Quyidagi ta'riflardan qaysi biri tarmoqning xavfsizlik siyosatidagi zaifligini ifodalaydi. Xavfsizlik siyosatidagi zaiflikni yuzaga kelishiga tashkilotning xavfsizlik siyosatida qoidalar va qarshi choralarni noto'g'ri ishlab chiqilgani sabab bo'ladi. Asosan tarmoq, tizim va tashkilot haqidagi axborot olish maqsadida amalga oshiriladigan tarmoq hujumi qaysi Razvedka hujumlari Ma'lumotlarni zaxira nusxalash bu – ... Muhim bo'lgan axborot nusxalash yoki saqlash jarayoni bo'lib, bu ma'lumot yo'qolgan vaqtda qayta tiklash imkoniyatini beradi Zarar yetkazilgandan keyin tizimni normal ish holatiga qaytarish va tizimda saqlanuvchi muhim ma'lumotni yo'qolishidan so'ng uni qayta tiklash uchun qanday amaldan foydalanamiz Zaxira nusxalash Ma'lumotlarni inson xatosi tufayli yo'qolish sababiga ta'rif bering Qasddan yoki tasodifiy ma'lumotni o'chirib yuborilishi, ma'lumotlarni saqlash vositasini to'g'ri joylashtirilmagani yoki ma'lumotlar bazasini xatolik bilan boshqarilganligi. Zahira nusxalash strategiyasi nechta bosqichni o'z ichiga oladi? 5 Zaxiralash uchun zarur axborotni aniqlash nechta bosqichda amalga oshiriladi. 4 Zaxira nusxalovchi vositalar tanlashdagi narx xususiyatiga berilgan ta'rifni aniqlash Har bir tashkilot o'zining budjetiga mos bo'lgan zaxira nusxalash vositasiga ega bo'lishi shart. RAID texnologiyasining transkripsiyasi qanday. Random Array of Independent Disks RAID texnologiyasida nechta satx mavjud 6 OSI modelining birinchi sathi qanday nomlanadi Fizik sath OSI modelining ikkinchi sathi qanday nomlanadi Kanal sathi OSI modelining uchinchi sathi qanday nomlanadi Tarmoq sathi OSI modelining oltinchi sathi qanday nomlanadi Taqdimlash sathi OSI modelining ettinchi sathi qanday nomlanadi Amaliy sath Elektr signallarini qabul qilish va uzatish vazifalarini OSI modelining qaysi sathi bajaradi Fizik sath Keltirilgan protokollarning qaysilari transport sathi protokollariga mansub TCP,UDP OSI modelining fizik sathi qanday funktsiyalarni bajaradi Elektr signallarini uzatish va qabul qilish OSI modelining amaliy sathi qanday funktsiyalarni bajaradi Klient dasturlari bilan o'zaro muloqotda bo'lish 12 gacha bo'lgan va 12 bilan o'zaro tub bo'lgan sonlar soni nechta? 8 ta Yevklid algoritmi qanday natijani beradi? Sonning eng katta umumiy bo'luvchisini topish Qanday sonlar tub sonlar deb yuritiladi? Faqatgina 1 ga va o'ziga bo'linadigan sonlar tub sonlar deyiladi. To'liq zaxiralash To'liq va o'sib boruvchi usullarning mujassamlashgan ko'rinishi bo'lib, oxirgi zaxiralangan nusxadan boshlab bo'lgan o'zgarishlarni zaxira nusxalab boradi. • Amalga oshirish to'liq zaxiralashga qaraganda tez amalga oshiriladi. • Qayta tikla O'sib boruvchi zaxiralash Zaxiralangan ma'lumotga nisbatan o'zgarish yuz berganda zaxirilash amalga oshiriladi. • Oxirgi zaxira nusxalash sifatida ixtiyoriy zaxiralash usuli bo'lishi mumkin (to'liq saxiralashdan). • Saqlash uchun kam hajm va amalga oshiris Differensial zaxiralash Ushbu zaxiralashda tarmoqqa bog'lanishamalga oshiriladi. • Iliq zaxiralashda, tizim yangilanishi

davomiy yangilanishni qabul qilish uchun ulanadi Ushbu jarayon ma'lumot qanday yo'qolgani, ma'lumotni qayta tiklash dasturiy vositasi va ma'lumotni tiklash manzilini qayergaligiga bog'liq bo'ladi. Qaysi jarayon Ma'lumotlarni qayta tiklash Antivirus dasturlarini ko'rsating? Drweb, Nod32, Kaspersky Wi-Fi tarmoqlarida quyida keltirilgan qaysi shifrlash protokollaridan foydalaniladi wep, wpa, wpa2 Axborot himoyalangan qanday sifatlarga ega bo'lishi kerak? ishonchli, qimmatli va to'liq Axborotning eng kichik o'lchov birligi nima? bit Virtual xususiy tarmoq – bu? VPN Xavfli viruslar bu - ... kompyuter ishlashida jiddiy nuqsonlarga sabab bo'luvchi viruslar Mantiqiy bomba – bu ... Ma'lum sharoitlarda zarar keltiruvchi harakatlarni bajaruvchi dastur yoki uning alohida modullari Rezident virus... tezkor xotirada saqlanadi DIR viruslari nimani zararlaydi? FAT tarkibini zararlaydi .... kompyuter tarmoqlari bo'yicha tarqalib, komlg'yuterlarning tarmoqdagi manzilini aniqlaydi va u yerda o'zining nusxasini qoldiradi «Chuvalchang» va replikatorli virus Mutant virus... shifrlash va deshifrlash algoritmlaridan iborat- to'g'ri javob Fire Wall ning vazifasi... tarmoqlar orasida aloqa o'rnatish jarayonida tashkilot va Internet tarmog'i orasida xavfsizlikni ta'minlaydi Kompyuter virusi nima? maxsus yozilgan va zararli dastur Kompyuterning viruslar bilan zararlanish yo'llarini ko'rsating disk, maxsus tashuvchi qurilma va kompyuter tarmoqlari orqali Trojan dasturlari bu... virus dasturlar Kompyuter viruslari xarakterlariga nisbatan necha turga ajraladi? 5 Antiviruslarni, qo'llanish usuliga ko'ra... turlari mavjud detektorlar, faglar, vaktsinalar, privivkalar, revizorlar, monitorlar Axborotni himoyalash uchun ... usullari qo'llaniladi. kodlashtirish, kriptografiya, stegonografiya Stenografiya mahnosi... sirli yozuv ...sirli yozuvning umumiy nazariyasini yaratdiki, u fan sifatida stenografiyaning bazasi hisoblanadi K.Shennon Kriptologiya yo'nalishlari nechta? 2 Kriptografiyaning asosiy maqsadi... maxfiylik, yaxlitlikni ta'minlash Zararli dasturiy vositalarni aniqlash turlari nechta 3 Signaiurana asoslangan ...bu fayldan topilgan bitlar qatori bo'lib, maxsus belgilarni o'z ichiga oladi. Bu o'rinda ularning xesh qiymatlari ham signatura sifatida xizmat qilishi mumkin. O'zgarishni aniqlashga asoslangan Zararli dasturlar biror joyda joylashishi sababli, agar tizimdagi biror joyga o'zgarishni aniqlansa, u holda u zararlanishni ko'rsatishi mumkin Anomaliyaga asoslangan Noodatiy yoki virusga o'xshash yoki potensial zararli harakatlari yoki xususiyatlarni topishni maqsad qiladi Antiairuslar qanday usulda viruslarni aniqlaydi Signaturaga asoslangan Viruslar - o'zini o'zi ko'paytiradigan programma bo'lib, o'zini boshqa programma ichiga, kompyuterning yuklanuvchi sektoriga yoki hujjat ichiga biriktiradi Rootkitlar- ushbu zararli dasturiy vosita operatsion tizim tomonidan aniqlanmasligi uchun ma'lum harakatlarini yashiradi Backdoorlar - zararli dasturiy kodlar bo'lib, hujumchiga autentifikatsiyani amalga oshirmasdan aylanib o'tib tizimga kirish imkonini beradi, maslan, administrator parolisiz imtiyozga ega bo'lish Trojan otlari- bir qarashda yaxshi va foydali kabi ko'rinuvchi dasturiy vosita sifatida ko'rsada, yashiringan zararli koddan iborat bo'ladi Ransomware- mazkur zararli dasturiy ta'minot qurbon kompyuterida mavjud qimmatli fayllarni shifrlaydi yoki qulflab qo'yib, to'lov amalga oshirilishini talab qiladi Resurslardan foydalanish usuliga ko'ra viruslar qanday turlarga bo'linadi Virus parazit, Virus cherv Zararlagan obyektlar turiga ko'ra Dasturiy, yuklanuvchi, Makroviruslar, multiplatformali viruslar Faollashish prinsipiga ko'ra Resident, Norezident Dastur kodini tashkil qilish yondashuviga ko'ra Shifrlangan, shifrlanmagan, Polimorf Shifrlanmagan viruslar o'zini oddiy dasturlar kabi ko'rsatadi va bunda dastur kodida hech qanday qo'shimcha ishlashlar mavjud bo'lmaydi.  $P=31$ ,  $q=29$  eyler funksiyasida  $f(p,q)$  ni hisoblang  $840\ 256 \bmod 25=?$  6 bu yaxlit «butun»ni tashkil etuvchi bog'liq yoki o'zaro bog'langan tashkil etuvchilar guruhi nima deyiladi. Tizim Tashkilotni himoyalash maqsadida amalga oshirilgan xavfsizlik nazoratini tavsiflovchi yuqori sathli hujjat yoki hujjatlar to'plami nima duvidadi Xavfsizlik siyosati RSA shifrlash algoritmidan foydalaniladigan sonlarning spektri o'lchami qanday?  $p$  va  $q$  –sonlarning



ko'paytmasini ifodalovchi sonning spektoriga teng; DES algoritmi akslantirishlari raundlari soni qancha? 16; DES algoritmi shifrlash blokining chap va o'ng qism bloklarining o'lchami qancha? CHap qism blok 32 bit, o'ng qism blok 32 bit; Simmetrik va asimmetrik shifrlash algoritmlarining qanday mohiyatan farqli tomonlari bor? SHifrlash va deshifrlash jarayonlari uchun kalitlarni generatsiya qilish qoidalariga ko'ra farqlanadi 19 gacha bo'lgan va 19 bilan o'zaro tub bo'lgan sonlar soni nechta? 18 ta 10 gacha bo'lgan va 10 bilan o'zaro tub bo'lgan sonlar soni nechta? 4 ta Eyler funsiyasida (1) qiymati nimaga teng? 0 Eyler funsiyasida 60 sonining qiymatini toping. 59 Eyler funsiyasi yordamida 1811 sonining qiymatini toping. 1810 97 tub sonmi? Tub Quyidagi modulli ifodani qiymatini toping  $(148 + 14432) \bmod 256$ . 244 Quyidagi sonlarning eng katta umumiy bo'luvchilarini toping. 88 i 220 44 Quyidagi ifodani qiymatini toping.  $-17 \bmod 11$  5 2 soniga 10 modul bo'yicha teskari sonni toping. Ø Tashkilotning maqsadlari va vazifalari hamda xavfsizlikni ta'minlash sohasidagi tadbirlar tavsiflanadigan yuqori darajadagi reja nima? Kiberxavfsizlik siyosati Kiberxavfsizlik siyosati tashkilotda nimani ta'minlaydi? tashkilot masalalarini yechish himoyasini yoki ish jarayoni himoyasini ta'minlaydi Kiberxavfsizlikni ta'minlash masalalari bo'yicha xavfsizlik siyosati shablonlarini ishlab chiqadigan yetakchi tashkilotni aniqlang SANS (System Administration Networking and Security) Korxonaning davomli muvaffaqiyat bilan faoliyat yuritishini ta'minlashga mo'ljallangan strukturalangan va o'zaro bog'langan harakatlar to'plami- ... Strategiya Tahdidlarning muvaffaqiyatli amalga oshirilishiga imkon beruvchi har qanday omil – bu ... Zaiflik ISO/IEC 27002:2005 – .... Axborot texnologiyasi. Xavfsizlikni ta'minlash metodlari. Axborot xavfsizligini boshqarishning amaliy qoidalari O'zDStISO/IEC 27005:2013 – .... Axborot texnologiyasi. Xavfsizlikni ta'minlash usullari. Axborot xavfsizligi risklarini boshqarish Axborot xavfsizligi arxitekturasining nechta satxi bor? 3 Rahbariy hujjat. Ma'lumotlar uzatish tarmog'ida axborot xavfsizligini ta'minlash to'g'risida Nizom - Xujjat raqamini toping RH 45-215:2009 Davlat hokimiyati va boshqaruv organlarining axborot xavfsizligini ta'minlash dasturini ishlab chiqish tartibi - Xujjat raqamini toping RH 45-185:2011 Davlat organlari saytlarini joylashtirish uchun provayderlar serverlari va texnik maydonlarning axborot xavfsizligini ta'minlash darajasini aniqlash tartibi - Xujjat raqamini toping RH 45-193:2007 Aloqa va axborotlashtirish sohasida axborot xavfsizligi. Atamalar va ta'riflar - Xujjat raqamini toping TSt 45- 010:2010 Quyidagilardan qaysi standart aloqa va axborotlashtirish sohasida axborot xavfsizligidagi asosiy atama va ta'riflarni belgilaydi? TSt 45-010:2010 Sub'ekt identifikatorini tizimga yoki talab qilgan sub'ektga taqdim qilish jarayoni nima? Identifikatsiya Foydalanuvchini (yoki biror tomonni) tizimdan foydalanish uchun ruxsati mavjudligini aniqlash jarayoni nima? Autentifikatsiya Identifikatsiya va autentifikatsiyadan o'tgan foydalanuvchilarga tizimda bajarishi mumkin bo'lgan amallarga ruxsat berish jarayoni – nima deyiladi? Avtorizatsiya Identifikatsiya nima? Sub'ekt identifikatorini tizimga yoki talab qilgan sub'ektga taqdim qilish jarayoni Autentifikatsiya nima? Foydalanuvchini (yoki biror tomonni) tizimdan foydalanish uchun ruxsati mavjudligini aniqlash jarayoni Avtorizatsiya nima? Identifikatsiya va autentifikatsiyadan o'tgan foydalanuvchilarga tizimda bajarishi mumkin bo'lgan amallarga ruxsat berish jarayoni ... - Faqat foydalanuvchiga ma'lum va biror tizimda autentifikatsiya jarayonidan o'tishni ta'minlovchi biror axborot Parol Smart karta o'lchamidagi, kichik xajmdagi xotira va xisoblash imkoniyatiga ega bo'lgan, o'zida parol yoki kalitni saqlovchi qurilma nima deb ataladi? Token, Smartkarta Smarkarta nima asosida autentifikatsiyalaydi? Something you have Faqat bir marta foydalaniluvchi, xar bir sessiya uchun o'zgarib turadigan parol nima deyiladi? One-time password (OTP) Foydalanuvchining tarmoqdagi harakatini, shu jumladan, uning resurslardan foydalanishga urinishini qayd etish nima deb ataladi? Ma'murlash Amaldagi qonunchilikka mos ravishda texnik, dasturiy va dasturiy-texnik vositalar yordamida axborot

xavfsizligining nokriptografik usullari bilan ta'minlashni inobatga oluvchi axborot himoyasi nima? Axborotning texnik himoyasi Nazorat hududi – bu ... Qo'riqlanuvchi soha bo'lib, uning ichida kommunikatsiya qurilmalari hamda axborot tarmog'ining lokal tarkibiy qurilmalarini birlashtiruvchi barcha nuqtalar joylashadi Texnik himoya vositalari – bu ... Texnik qurilmalar, komplekslar yoki tizimlar yordamida ob'ektni himoyalashdir Bu axborotni tutib olish qurilmasi bo'lib, ularda uzatuvchi qurilma sifatida kontaktli mikrofonlardan foydalaniladi Stetoskoplar Xesh funktsiya to'g'ri ko'rsatilgan javobni aniqlang. MD5 MD5, SHA1, Tiger xesh funktsiyalari uchun blok uzunligi necha baytga teng? 64 bayt Sub'ektni ob'ektga ishlash qobiliyatini aniqlash – nima? Foydalanishni boshqarish Foydalanishni boshqarishda sub'ekt bu - .... Inson, dastur, jarayon Foydalanishni boshqarishning qaysi usuli tizimdagi shaxsiy ob'ektlarni himoyalash uchun qo'llaniladi? Discretionary access control DAC Foydalanishni boshqarishning qaysi usulidan asosan operatsion tizimlarda qo'llaniladi? Discretionary access control DAC Foydalanishni boshqarishning qaysi usulida foydalanishlar sub'ektlar va ob'ektlarni klassifikatsiyalashga asosan boshqariladi? Mandatory access control MAC Foydalanishni boshqarishning qaysi usulida xavfsizlik markazlashgan tarzda xavfsizlik siyosati m'muri tomonidan amalga oshiriladi? Mandatory access control MAC Foydalanishni boshqarishning qaysi usulida har bir foydalanuvchini foydalanish ruxsatini belgilash o'rniga rol uchun ob'ektlardan foydalanish ruxsatini ko'rsatish yetarli bo'ladi? Role-based access control RBAC Foydalanishni boshqarishning qaysi usulida sub'ekt va ob'ektlarga tegishli xuquqlarni ma'murlash oson kechadi? Role-based access control RBAC Firibgarlikni oldini olish uchun bir shaxs tomonidan ko'plab vazifalarni bajarishga ruxsat bermaslik zarur. Bu muammo foydalanishni boshqarishni qaysi usulida bartaraf etiladi? Role-based access control RBAC Ob'ekt va sub'ektlarning attributlari, ular bilan mumkin bo'lgan amallar va so'rovlarga mos keladigan muxit uchun qoidalarni taxlil qilish asosida foydalanishni boshqarish - .... Attribute based access control ABAC Attribute based access control ABAC usuli attributlari qaysilar? Foydalanuvchi attributlari, Resurs attributlari, Ob'ekt va muxit attributlari Foydalanishni boshqarishning qaysi usulida ruxsatlar va xarakteristikani kim bajarayotganligi to'g'risidagi xolatlar “agar, u xolda” buyrug'idan tashkil topgan qoidalarga asoslanadi? Attribute based access control ABAC XASML standarti foydalanishni boshqarishning qaysi usulida qo'llaniladi? Attribute based access control ABAC XASML standartida qoida nima? Maqsad, ta'sir, shart, majburiyat va maslahatlar XASML standartida maqsad nima? Sub'ekt ob'ekt ustida nima xarakteristik qilishi Lampsonning foydalanishni boshqarish matritsasi nimalardan tashkil topgan? Imtiyozlar ro'yxati Access control list va Capability list bu nimaning asosiy elementi xisoblanadi? Lampson matritsasining Lampson matritsasining satrlarida nima ifodalanadi? Sub'ektlar Foydalanishni boshqarishning mantiqiy vositalari infratuzilma va uning ichidagi tizimlarda ... uchun foydalaniladi. Mandat, Tasdiqlash, Avtorizatsiya SHaxsiy simsiz tarmoq standartini aniqlang. Bluetooth, IEEE 802.15, IRDA Lokal simsiz tarmoq standartini aniqlang. IEEE 802.11, Wi-Fi, HiperLAN Regional simsiz tarmoq standartini aniqlang. IEEE 802.16, WiMAX Global simsiz tarmoq standartini aniqlang. CDPD, 2G, 2.5G, 3G, 4G, 5G Bluetooth, IEEE 802.15, IRDA standartida ishlovchi simsiz tarmoq turini aniqlang. SHaxsiy simsiz tarmoq IEEE 802.11, Wi-Fi, HiperLAN standartida ishlovchi simsiz tarmoq turini aniqlang. Lokal simsiz tarmoq IEEE 802.16, WiMAX standartida ishlovchi simsiz tarmoq turini aniqlang. Regional simsiz tarmoq CDPD, 2G, 2.5G, 3G, 4G, 5G standartida ishlovchi simsiz tarmoq turini aniqlang. Global simsiz tarmoq Bluetooth qanday chastota oralig'ida ishlaydi? 2.4-2.485 Ggts Wi-Fi qanday chastota oralig'ida ishlaydi? 2.4-5 Ggts WiMax tarmog'ining tezligi qancha? 1 Gbit/sekund Quyidagilardan qaysi biri MITM xujumiga tegishli xattixarakat xisoblanadi? Aloqa seansini konfidentsialligini va yaxlitligini buzish WiMAX tarmoq arxitekturasini nechta tashkil etuvchidan

iborat? 5 WiMAX tarmoq arxitekturasida qaysi tashkil etuvchidan iborat? Base station, Subscriber station, Mobile station, Relay station, Operator network GSM raqamli mobil telefonlarining nechanchi avlodi uchun ishlab chiqilgan protokol? Ikkinchi avlodi GSM standarti qaysi tashkilot tomonidan ishlab chiqilgan? European telecommunications standards institute .... – o'zida IMSI raqamini, autentifikatsiyalash kaliti, foydalanuvchi ma'lumoti va xavfsizlik algoritmlarini saqlaydi. Sim karta Rutoken S qurilmasining og'irligi qancha? 6.3 gramm True Crypt dasturi qaysi algoritmlardan foydalanib shifrlaydi? AES, Serpent, Twofish Ma'lumotni saqlash vositalarida saqlangan ma'lumot konfidentsialligini aniqlash qaysi dasturiy shifrlash vositalarining vazifasi? Disc encryption software BestCrypt dasturi qaysi algoritmlardan foydalanib shifrlaydi? AES, Serpent, Twofish AxCrypt dasturi qaysi algoritmlardan foydalanib shifrlaydi? AES-256 Qog'oz ko'rinishidagi axborotlarni yo'q qilish qurilmasining nomini kiriting. Shredder Ma'lumotlarni bloklarga bo'lib, bir qancha (kamida ikkita) qattiq diskda rezerv nusxasini yozish qaysi texnologiya? RAID 0 Qaysi texnologiyada ma'lumotni ko'plab nusxalari bir vaqtda bir necha disklarga yoziladi? RAID 1 Qaysi texnologiyada ma'lumotlarni bir necha disklarda bayt satxida ajratilgan xolda yoziladi? RAID 3 Qaysi texnologiyada ma'lumotlarni bir necha disklarda bayt satxida ajratilgan xolda yoziladi va nazorat bitlari ham ular ichida taqsimlanadi? RAID 5 Disk zararlanganda "qaynoq almashtirish" yordamida uni almashtirish mumkin. Bu xususiyat qaysi texnologiyaga tegishli? RAID 50 Zaxiralashning qanday turlari mavjud? To'liq, o'sib boruvchi, differentsial IOS, Android, USB xotiralardan ma'lumotlarni tiklash uchun qaysi dasturdan foydalaniladi? EASEUS Data recovery wizard Foydalanuvchi ma'lumotlarini qo'lga kirituvchi va uni xujumchiga yuboruvchi dasturiy kod nima? Spyware Operatsion tizim tomonidan aniqlanmasligi uchun ma'lum xarakatlarni yashirish nima deyiladi? Rootkits Qurbon kompyuterda mavjud qimmatli fayllarni shifrlaydi yoki qulflab qo'yib to'lov amalga oshirishni talab qiladi. Bu qaysi zararli dastur? Ransomware Quyidagilardan o'zidan ko'payishi yo'q bo'lganlarini belgilang. Mantiqiy bomba, Trojan oti, Backdoors Viruslar resurslardan foydalanish usuliga ko'ra qanday turlarga bo'linadi? Virus parazitlar, virus chervlar Viruslar zararlangan ob'ektlar turiga ko'ra qanday turlarga bo'linadi? Dasturiy, yuklanuvchi, makroviruslar, ko'p platformali Viruslar faollashish printsipiga ko'ra qanday turlarga bo'linadi? Rezident, norezident Viruslar dastur kodini tashkil qilish yondoshuviga ko'ra qanday turlarga bo'linadi? SHifrlangan, shifrlanmagan, polimorf Dastlabki virus nechanchi yilda yaratilgan? 1988 ILOVEYOU virusi keltirgan zarar qancha? 10 mlrd. Dollar CodeRed virusi keltirgan zarar qancha? 2 mlrd. Dollar Melissa virusi keltirgan zarar qancha? 80 million dollar NetSky virusi keltirgan zarar qancha? 18 mlrd. Dollar MyDoom virusi keltirgan zarar qancha? 38 mlrd. Dollar Risk monitoring ..... ni paydo bo'lish imkoniyatini aniqlaydi. Yangi risklar ..... riskni tutuvchi mos nazorat usuli amalga oshirilganligini kafolatlaydi. Risk monitoring Axborot xavfsizligi siyoatining necha hil turi bor? 3 Internetdan foydalanish siyosatining nechta turi mavjud? 4 Nomuntazam siyosat (Promiscuous Policy) nima? Tizim resurslaridan foydalanishda hech qanday cheklovlar qo'ymaydi Paranoid siyosati (Paranoid Policy) – bu .... Hamma narsa ta'qiqlanadi Ruxsat berishga asoslangan siyosat (Permissive Policy) – bu ... Faqat ma'lum hizmatlar/hujumlar/harakatlar bloklanadi Ehtiyotkorlik siyosati (Prudent Policy) – bu .... Barcha hizmatlar blokirovka qilingandan so'ng bog'lanadi Tizim resurslaridan foydalanishda hech qanday cheklovlar qo'ymaydi. Bu qaysi xavfsizlik siyosatiga hos? Nomuntazam siyosat (Promiscuous Policy) Barcha hizmatlar blokirovka qilingandan so'ng bog'lanadi. Bu qaysi xavfsizlik siyosatiga hos? Ehtiyotkorlik siyosati (Prudent Policy) Faqat ma'lum hizmatlar/hujumlar/harakatlar bloklanadi. Bu qaysi xavfsizlik siyosatiga hos? Ruxsat berishga asoslangan siyosat (Permissive Policy) Hamma narsa ta'qiqlanadi. Bu qaysi xavfsizlik siyosatiga hos? Paranoid siyosati (Paranoid Policy) Tizim arxitekturasining turlari nechta?

5 Internet, havo hujumidan mudofaa, transport tizimlari qaysi tizim arxitekturasiga xos? Hamkorlik tizimlari arxitekturasi Cloud computing texnologiyasining nechta asosiy turi mavjud? 3 Raqamli soatlar qaysi texnologiyaga tegishli? O'rnatilgan tizimlar (Embedde systems) Xavfsizlikning asosiy yo'nalishlarini sanab o'ting. \*Axborot xavfsizligi, Iqtisodiy xavfsizlik, Mudofaa xavfsizligi, Ijtimoiy xavfsizlik, Ekologik xavfsizlik Axborot xavfsizligining asosiy maqsadlaridan biri- bu... \*Axborotlarni o'g'irlanishini, yo'qolishini, soxtalashtirilishini oldini olish Konfidentsiallikga to'g'ri ta'rif keltiring. \*axborot inshonchliligi, tarqatilishi mumkin emasligi, maxfiyligi kafolati; Yaxlitlikni buzilishi bu - ... \*Soxtalashtirish va o'zgartirish ... axborotni himoyalash tizimi deyiladi. \*Axborotning zaif tomonlarini kamaytiruvchi axborotga ruxsat etilmagan kirishga, uning chiqib ketishiga va yo'qotilishiga to'sqinlik qiluvchi tashkiliy, texnik, dasturiy, texnologik va boshqa vosita, usul va choralarning Kompyuter virusi nima? \*maxsus yozilgan va zararli dastur Axborotni himoyalash uchun ... usullari qo'llaniladi. \*kodlashtirish, kriptografiya, stegonografiya Stenografiya ma'nosi... \*sirli yozuv Kriptografiyaning asosiy maqsadi... \*maxfiylik, yaxlitlikni ta'minlash SMTP - Simple Mail Transfer protokol nima? \*elektron pochta protokoli SKIP protokoli... \*Internet protokollari uchun kriptokalitlarning oddiy boshqaruvi Kompyuter tarmog'ining asosiy komponentlariga nisbatan xavf-xatarlar... \*uzilish, tutib qolish, o'zgartirish, soxtalashtirish ...ma'lumotlar oqimini passiv hujumlardan himoya qilishga xizmat qiladi. \*konfidentsiallik Foydalanish huquqini cheklovchi matritsa modeli bu... \*Bella La-Padulla modeli Kompyuter tarmoqlarida tarmoqning uzoqlashtirilgan elementlari o'rtasidagi aloqa qaysi standartlar yordamida amalga oshiriladi? \*TCP/IP, X.25 protokollar Himoya tizimi kompleksligiga nimalar orqali erishiladi? \*Xuquqiy tashkiliy, muhandis, texnik va dasturiy matematik elementlarning mavjudligi orqali Kalit – bu ... \*Matnni shifrlash va shifrini ochish uchun kerakli axborot Qo'yish, o'rin almashtirish, gammalash kriptografiyaning qaysi turiga bog'liq? \*simmetrik kriptotizimlar Autentifikatsiya nima? \*Ma'lum qilingan foydalanuvchi, jarayon yoki qurilmaning haqiqiy ekanligini tekshirish muolajasi Identifikatsiya bu- ... \*Foydalanuvchini uning identifikatori (nomi) bo'yicha aniqlash jarayoni O'rin almashtirish shifri bu - ... \*Murakkab bo'lmagan kriptografik akslantirish Simmetrik kalitli shifrlash tizimi necha turga bo'linadi. \*2 turga Kalitlar boshqaruvi 3 ta elementga ega bo'lgan axborot almashinish jarayonidir bular ... \*hosil qilish, yig'ish, taqsimlash Kriptologiya - \*axborotni qayta akslantirib himoyalash muammosi bilan shug'ullanadi Kriptografiyada alifbo – \*axborot belgilarini kodlash uchun foydalaniladigan chekli to'plam Simmetrik kriptotizimlarda ... jumlaning davom ettiring \*shifrlash va shifrni ochish uchun bitta va aynan shu kalitdan foydalaniladi Kriptobardoshlilik deb ... \*kalitlarni bilmasdan shifrni ochishga bardoshlilikni aniqlovchi shifrlash tavsifi Elektron raqamli imzo deb – \*xabar muallifi va tarkibini aniqlash maqsadida shifrmata qo'shilgan qo'shimcha Kriptografiya – \*axborotni qayta akslantirishning matematik usullarini izlaydi va tadqiq qiladi Kriptografiyada matn – \*alifbo elementlarining tartiblangan to'plami Kriptoanaliz – \*kalitlarni bilmasdan shifrni ochishga bardoshlilikni aniqlovchi shifrlash tavsifi Shifrlash – \*akslantirish jarayoni: ochiq matn deb nomlanadigan matn shifrmata almashtiriladi Kalit taqsimlashda ko'proq nimalarga e'tibor beriladi? \*Tez, aniq va maxfiyligiga Faol hujum turi deb... \*Maxfiy uzatish jarayonini uzib qo'yish, modifikatsiyalash, qalbaki shifr ma'lumotlar tayyorlash harakatlaridan iborat jarayon Blokli shifrlash- \*shifrlanadigan matn blokiga qo'llaniladigan asosiy akslantirish Simmetrik kriptotizimning uzluksiz tizimida ... \*ochiq matnning har bir harfi va simvoli alohida shifrlanadi Kripto tizimga qo'yiladigan umumiy talablardan biri \*shifr matn uzunligi ochiq matn uzunligiga teng bo'lishi kerak Berilgan ta'riflardan qaysi biri asimmetrik tizimlarga xos? \*Asimmetrik kriptotizimlarda  $k_1 \neq k_2$  bo'lib,  $k_1$  ochiq kalit,  $k_2$  yopiq kalit deb yuritiladi,  $k_1$  bilan axborot shifrlanadi,  $k_2$  bilan esa deshifrlanadi Yetarlicha kriptoturg'unlikka

ega, dastlabki matn simvollarini almashtirish uchun bir necha alfavitdan foydalanishga asoslangan almashtirish usulini belgilang \*Vijener matritsasi, Sesar usuli Akslantirish tushunchasi deb nimaga aytiladi? \*1- to'plamli elementlariga 2-to'plam elementalriga mos bo'lishiga Simmetrik guruh deb nimaga aytiladi? \*O'rin almashtirish va joylashtirish Qo'yish, o'rin almashtirish, gammalash kriptografiyaning qaysi turiga bog'liq? \*simmetrik kriptosistemalar Xavfli viruslar bu - ...

\*kompyuter ishlashida jiddiy nuqsonlarga sabab bo'luvchi viruslar Mantiqiy bomba – bu ...

\*Ma'lum sharoitlarda zarar keltiruvchi harakatlarni bajaruvchi dastur yoki uning alohida modullari Elektron raqamli imzo tizimi qanday muolajalarni amalga oshiradi? \*raqamli imzoni shakllantirish va tekshirish muolajasi Shifrlashning kombinatsiyalangan usulida qanday kriptotizimlarning kriptografik kalitlaridan foydalaniladi? \*Simmetrik va assimetrik Axborot himoyasi nuqtai nazaridan kompyuter tarmoqlarini nechta turga ajratish mumkin? \*Korporativ va umumfoydalanuvchi Elektromagnit nurlanish va ta'sirlanishlardan himoyalash usullari nechta turga bo'linadi? \*Sust va faol Internetda elektron pochta bilan ishlash uchun TCP/IPga asoslangan qaysi protokoldan foydalaniladi? \*SMTP, POP yoki IMAR Axborot resursi – bu? \*axborot tizimi tarkibidagi elektron shakldagi axborot, ma'lumotlar banki, ma'lumotlar bazasi Shaxsning, o'zini axborot kommunikatsiya tizimiga tanishtirish jarayonida qo'llaniladigan belgilar ketmaketligi bo'lib, axborot kommunikatsiya tizimidan foydalanish huquqiga ega bo'lish uchun foydalaniluvchining maxfiy bo'lmagan qayd yozuvi – bu? \*login Uning egasi haqiqiylikni aniqlash jarayonida tekshiruv axboroti sifatida ishlatiladigan belgilar ketma-ketligi (maxfiy so'z) – bu?

\*parol Identifikatsiya jarayoni qanday jarayon? \* axborot tizimlari obyekt va subhektlariga uni tanish uchun nomlar (identifikator) berish va berilgan nom bo'yicha solishtirib uni aniqlash jarayoni Autentifikatsiya jarayoni qanday jarayon? \*obyekt yoki subhektning unga berilgan identifikatorga mosligini tekshirish va belgilar ketmaketligidan iborat maxfiy kodini tekshirish orqali aslligini aniqlash Avtorizatsiya jarayoni qanday jarayon? \*foydalanuvchining resursdan foydalanish huquqlari va ruxsatlarini tekshirish jarayoni Ro'yxatdan o'tish bu? \*foydalanuvchilarni ro'yxatga olish va ularga dasturlar va ma'lumotlarni ishlatishga huquq berish jarayoni Axborot qanday sifatlarga ega bo'lishi kerak? \*ishonchli, qimmatli va to'liq Axborotning eng kichik o'lchov birligi nima? \*bit Elektron hujjatning rekvizitlari nechta qismdan iborat? \*4 Axborotlarni saqllovchi va tashuvchi vositalar qaysilar? \*fleshka, CD va DVD disklar Imzo bu nima ? \*hujjatning haqiqiylikni va yuborgan fizik shaxsga tegishli ekanligini tasdiqlaydigan insonning fiziologik xususiyati. Muhr bu nima? \*hujjatning haqiqiylikni va biror bir yuridik shaxsga tegishli ekanligini tasdiqlovchi isbotdir DSA – nima \*Raqamli imzo algoritmi El Gamal algoritmi qanday algoritm

\*Shifrlash algoritmi va raqamli imzo algoritmi Sezarning shifrlash sistemasining kamchiligi

\*Harflarning so'zlarda kelish chastotasini yashirmaydi Axborot xavfsizligi va xavfsizlik san'ati haqidagi fan .... deyiladi? \*Kriptografiya Tekstni boshqa tekst ichida ma'nosini yashirib keltirish bu - \*steganografiya Shifrttekstni ochiq tekstga akslantirish jarayoni nima deb ataladi? \*Deshifrlash ..... – hisoblashga asoslangan bilim sohasi bo'lib, buzg'unchilar mavjud bo'lgan sharoitda amallarni kafolatlash uchun o'zida texnologiya, inson, axborot va jarayonni mujassamlashtirgan.

\*Kiberxavfsizlik Risk \*Potensial foyda yoki zarar Tahdid nima? \*Tashkilotga zarar yetkazishi mumkin bo'lgan istalmagan hodisa. Kodlash nima? \*Ma'lumotni osongina qaytarish uchun hammaga ochiq bo'lgan sxema yordamida ma'lumotlarni boshqa formatga o'zgartirishdir Shifrlash nima? Ma'lumotni osongina qaytarish uchun hammaga ochiq bo'lgan sxema yordamida ma'lumotlarni boshqa formatga o'zgartirishdir Axborotni shifrnı ochish (deshifrlash) bilan qaysi fan shug'ullanadi Kriptoanaliz Qaysi juftlik RSA algoritmining ochiq va yopiq kalitlarini ifodalaydi {d, e} – ochiq, {e, n} – yopiq; Zamonaviy kriptografiya qanday bo'limlardan iborat? Electron

raqamli imzo; kalitlarni boshqarish Kriptografik usullardan foydalanishning asosiy yo'nalishlari nimalardan iborat? uzatilyotgan xabarlarini haqiqiyligini aniqlash Shifr nima? \* Shifrlash va deshifrlashda foydalaniladigan matematik funktsiyadan iborat bo'lgan krptografik algoritm Ochiq kalitli kriptotizimlarning mohiyati nimadan iborat? \*Ochiq kalitli kriptotizimlarda bir-biri bilan matematik bog'langan 2 ta – ochiq va yopiq kalitlardan foydalaniladi Oqimli shifrlashning mohiyati nimada? Oqimli shifrlash birinchi navbatda axborotni bloklarga bo'lishning imkoni bo'lmagan hollarda zarur, Qandaydir ma'lumotlar oqimini har bir belgisini shifrlab, boshqa belgilarini kutmasdan kerakli joyga jo'natish uchun oqimli shifrlash zarur, Oqimli shifrlash algoritmlari ma'lumotlarni bitlar yoki belgilar bo'yicha shifrlaydi Simmetrik algoritmlarni xavfsizligini ta'minlovchi omillarni ko'rsating. \*uzatilayotgan shifrlangan xabarni kalitsiz ochish mumkin bo'lmashligi uchun algoritm yetarli darajada bardoshli bo'lishi lozim, uzatilayotgan xabarni xavfsizligi algoritmni maxfiyligiga emas Kriptotizim qaysi komponentlardan iborat? \*ochiq matnlar fazosi M, Kalitlar fazosi K, Shifrmtnlar fazosi C, Ek : M C (shifrlash uchun) va Dk: C M (deshifrlash uchun) funktsiyalar Asimmetrik kriptotizimlar qanday maqsadlarda ishlatiladi? \*shifrlash, deshifrlash, ERI yaratish va tekshirish, kalitlar almashish uchun Kriptografik elektron raqamli imzolarda qaysi kalitlar ma'lumotni yaxlitligini ta'minlashda ishlatiladi. \*ochiq kalitlar Xesh-funktsiyani natijasi ... Kiruvchi xabar uzunligidan uzun xabar RSA algoritmi qanday jarayonlardan tashkil topgan \*Kalitni generatsiyalash; Shifrlash; Deshifrlash. Ma'lumotlar butunligi qanday algritmlar orqali amalga oshiriladi \*Xesh funktsiyalar To'rtta bir-biri bilan bog'langan bog'lamlar strukturasi (kvadrat shaklida) qaysi topologiya turiga mansub \*Xalqa Qaysi topologiya birgalikda foydalanilmaydigan muhitni qo'llamasligi mumkin? \*to'liq bog'lanishli Kompyuterning tashqi interfeysi deganda nima tushuniladi? \*kompyuter bilan tashqi qurilmani bog'lovchi simlar va ular orqali axborot almashinish qoidalari to'plamlari Lokal tarmoqlarda keng tarqalgan topologiya turi qaysi? \*Yulduz Ethernet kontsentratori qanday vazifani bajaradi \*kompyuterdan kelayotgan axborotni qolgan barcha kompyuterga yo'naltirib beradi OSI modelida nechta satx mavjud \*7 OSI modelining to'rtinchi satxi qanday nomlanadi \*Transport satxi OSI modelining beshinchi satxi qanday nomlanadi \*Seanslar satxi OSI modelining birinchi satxi qanday nomlanadi \*Fizik satx OSI modelining ikkinchi satxi qanday nomlanadi \*Kanal satxi OSI modelining uchinchi satxi qanday nomlanadi \*Tarmoq satxi OSI modelining oltinchi satxi qanday nomlanadi \*Taqdimlash satxi OSI modelining yettinchi satxi qanday nomlanadi \*Amaliy satx OSI modelining qaysi satxlari tarmoqqa bog'liq satxlar hisoblanadi \*fizik, kanal va tarmoq satxlari OSI modelining tarmoq satxi vazifalari keltirilgan qurilmalarning qaysi birida bajariladi \*Marshrutizator Elektr signallarini qabul qilish va uzatish vazifalarini OSI modelining qaysi satxi bajaradi \*Fizik satx Ma'lumotlarni uzatishning optimal marshrutlarini aniqlash vazifalarini OSI modelining qaysi satxi bajaradi \*Tarmoq satxi Keltirilgan protokollarning qaysilari tarmoq satxi protokollariga mansub \*IP, IPX Keltirilgan protokollarning qaysilari transport satxi protokollariga mansub \*TCP,UDP OSI modelining fizik satxi qanday funktsiyalarni bajaradi \*Elektr signallarini uzatish va qabul qilish OSI modelining amaliy satxi qanday funktsiyalarni bajaradi \*Klient dasturlari bilan o'zaro muloqotda bo'lish Keltirilgan protokollarning qaysilari kanal satxi protokollariga mansub \*Ethernet, FDDI Keltirilgan protokollarning qaysilari taqdimlash satxi protokollariga mansub \*SNMP, Telnet Identifikatsiya, autentifikatsiya jarayonlaridan o'tgan foydalanuvchi uchun tizimda bajarishi mumkin bo'lgan amallarga ruxsat berish jarayoni bu... \*Avtorizatsiya Autentifikatsiya faktorlari nechta 4 Faqat foydalanuvchiga ma'lum va biror tizimda autentifikatsiya jarayonidan o'tishni ta'minlovchi biror axborot nima Login Ko'z pardasi, yuz tuzilishi, ovoz tembri- bular autentifikatsiyaning qaysi faktoriga mos belgilar? Biron nimaga egalik asosida barcha kabel va tarmoq tizimlari; tizim va

kabellarni fizik nazoratlash; tizim va kabel uchun quvvat manbai; tizimni madadlash muhiti. Bular tarmoqning qaysi satxiga kiradi? \*Fizik satx Fizik xavfsizlikda Yong'inga qarshi tizimlar necha turga bo'linadi \*2 Avtorizatsiya tushunchasi odatda qaysi tushuncha bilan sinonim sifatida ham foydalanadi? \*Foydalanishni boshqarish Foydalanishni boshqarish –bu... Subyektni Subyektga ishlash qobiliyatini aniqlashdir. Foydalanishni boshqarishda inson, dastur, jarayon va xokazolar nima vazifani bajaradi? Obyekt Foydalanishna boshqarishda ma'lumot , resurs, jarayon nima vazifani bajaradi ? \*Obyekt Foydalanishna boshqarishning nechta usuli mavjud? \*4 Foydalanishni boshqarishning qaysi usulida tizimdagi shaxsiy Obyektlarni himoyalash uchun qo'llaniladi ABAC Foydalanishni boshqarishning qaysi modelida Obyekt egasining o'zi undan foydalanish huquqini va kirish turini o'zi belgilaydi ABAC Foydalanishni boshqarishning qaysi usulida foydalanishlar Subyektlar va Obyektlarni klassifikatsiyalashga asosan boshqariladi. ABAC Foydalanishni boshqarishning mandatli modelida Obyektning xavfsizlik darajasi nimaga bog'liq.. Tashkilotda Obyektning muhimlik darajasi bilan yoki yuzaga keladigan foyda miqdori bilan bilan xarakterlanadi MAC usuli bilan foydalanishni boshqarishda xavfsizlik markazlashgan holatda kim tomonidan amalga oshiriladi \*xavfsizlik siyosati ma'muri Agar Subyektning xavfsizlik darajasida Obyektning xavfsizlik darajasi mavjud bo'lsa, u holda uchun qanday amalga ruxsat beriladi Yozish Agar Subyektning xavfsizlik darajasi Obyektning xavfsizlik darajasida bo'lsa, u holda qanday amalga ruxsat beriladi. \*Yozish Foydalanishni boshqarishning qaysi modelida har bir Obyekt uchun har bir foydalanuvchini foydalanish ruxsatini belgilash o'rniga, rol uchun Obyektlardan foydalanish ruxsati ko'rsatiladi? ABAC Rol tushunchasiga ta'rif bering. \*Muayyan faoliyat turi bilan bog'liq harakatlar va majburiyatlar to'plami sifatida belgilanishi mumkin Foydalanishni boshqarishning qaysi usuli - Obyektlar va Subyektlarning atributlari, ular bilan mumkin bo'lgan amallar va so'rovlarga mos keladigan muhit uchun qoidalarni tahlil qilish asosida foydalanishlarni boshqaradi. \*ABAC XACML foydalanishni boshqarishni qaysi usulining standarti? \*ABAC Biometrik autentifikatsiyalash usullari an'anaviy usullarga nisbatan avfzalliklari qaysi javobda to'g'ri ko'rsatilgan? \*barchasi Axborotning kriptografik himoya vositalari necha turda? 4 Dasturiy shifrlash vositalari necha turga bo'linadi \*4 Diskni shifrlash nima uchun amalga oshiriladi? \*Ma'lumotni saqlash vositalarida saqlangan ma'lumot konfidensialligini ta'minlash uchun amalga oshiriladi Ma'lumotlarni yo'q qilish odatda necha hil usulidan foydalaniladi? 8 Kompyuter tarmoqlari bu – \*Bir biriga osonlik bilan ma'lumot va resurslarni taqsimlash uchun ulangan kompyuterlar guruhi Tarmoq modeli –bu.. ikki Matematik modellar to'plami OSI modelida nechta tarmoq satxi bor \*7 OSI modeli 7 satxi bu \*Ilova OSI modeli 1 satxi bu Ilova OSI modeli 2 satxi bu Ilova TCP/IP modelida nechta satx mavjud \*4 Qanday tarmoq qisqa masofalarda qurilmalar o'rtasid a ma'lumot almashinish imkoniyatini taqdim etadi? Lokal Tarmoq kartasi bu... \*Hisoblash qurilmasining ajralmas qismi bo'lib, qurilmani tarmoqqa ulash imkoniyatini taqdim etadi. Switch bu... Hisoblash qurilmasining ajralmas qismi bo'lib, qurilmani tarmoqqa ulash imkoniyatini taqdim etadi. Hab bu... Hisoblash qurilmasining ajralmas qismi bo'lib, qurilmani tarmoqqa ulash imkoniyatini taqdim etadi. Tarmoq repiteri bu... Hisoblash qurilmasining ajralmas qismi bo'lib, qurilmani tarmoqqa ulash imkoniyatini taqdim etadi. Qanday tizim host nomlari va internet nomlarini IP manzillarga o'zgartirish yoki teskarisini amalga oshiradi. \*DNS tizimlari ..... protokoli ulanishga asoslangan protokol bo'lib, internet orqali ma'lumotlarni almashinuvchi turli ilovalar uchun tarmoq ulanishlarini sozlashga yordam beradi. \*TCP .... protokolidan odatda o'yin va video ilovalar tomonidan keng foydalaniladi. \*UDP Qaysi protokol ma'lumotni yuborishdan oldin aloqa o'rnatish uchun zarur bo'lgan manzil ma'lumotlari bilan ta'minlaydi. TCP Tarmoq taxdidlari necha turga bo'linadi 2 Qanday xujum asosiy hujumlarni oson amalga oshirish uchun tashkilot va tarmoq haqidagi axborotni to'plashni maqsad qiladi; \*Razvedka

hujumlari Qanday xujum hujumchi turli texnologiyalardan foydalangan holda tarmoqqa kirishga harakat qiladi Razvedka hujumlari Qanday xujum da hujumchi mijozlarga, foydalanuvchilaga va tashkilotlarda mavjud bo'lgan biror xizmatni cheklashga urinadi; Razvedka hujumlari Qanday xujumdp zararli hujumlar tizim yoki tarmoqqa bevosita va bilvosita ta'sir qiladi; Razvedka hujumlari RSA elektron raqamli imzo algoritmidagi ochiq kalit e qanday shartni qanoatlantirishi shart? \*e soni Eyler funksiyasi - bilan o'zaro tub RSA elektron raqamli imzo algoritmidagi yopiq kalit d qanday hisoblanadi? Bu yerda p va q tub sonlar,  $n=pq$ , - Eyler funksiyasi, e-ochiq kalit \* Elektron raqamli imzo algoritmi qanday bosqichlardan iborat bo'ladi? \*Imzo qo'yish va imzoni tekshirishdan Imzoni haqiqiyligini tekshirish qaysi kalit yordamida amalga oshiriladi? \*Imzo muallifining ochiq kaliti yordamida Tarmoq modeli-bu... \*Ikki hisoblash tizimlari orasidagi aloqani ularning ichki tuzilmaviy va texnologik asosidan qat'iy nazar muvaffaqiyatli o'rnatilishini asosidir OSI modeli nechta satxga ajraladi? 2 Fizik satxning vazifasi nimadan iborat \*Qurilma, signal va binar o'zgartirishlar Ilova satxning vazifasi nimadan iborat Qurilma, signal va binar o'zgartirishlar Kanal satxning vazifasi nimadan iborat Qurilma, signal va binar o'zgartirishlar Tarmoq satxning vazifasi nimadan iborat Qurilma, signal va binar o'zgartirishlar TCP/IP modeli nechta satxdan iborat \*4 Quyidagilarninf qaysi biri Kanal satxi protokollari \*Ethernet, Token Ring, FDDI, X.25, Frame Relay, RS-232, v.35. Quyidagilarninf qaysi biri tarmoq satxi protokollari Ethernet, Token Ring, FDDI, X.25, Frame Relay, RS-232, v.35. Quyidagilarninf qaysi biri transport satxi protokollari Ethernet, Token Ring, FDDI, X.25, Frame Relay, RS-232, v.35. Quyidagilarninf qaysi biri ilova satxi protokollari Ethernet, Token Ring, FDDI, X.25, Frame Relay, RS-232, v.35. TCP/IP modelining kanal satxiga OSI modelining qaysi satxlari mos keladi \*Kanal, Fizik TCP/IP modelining tarmoq satxiga OSI modelining qaysi satxlari mos keladi Kanal, Fizik TCP/IP modelining transport satxiga OSI modelining qaysi satxlari mos keladi Kanal, Fizik TCP/IP modelining ilova satxiga OSI modelining qaysi satxlari mos keladi Kanal, Fizik Quyidagilardan lokal tarmoqqa berilgan ta'rifni belgilang. \*Kompyuterlar va ularni bog'lab turgan qurilmalardan iborat bo'lib, ular odatda bitta tarmoqda bo'ladi. Quyidagilardan mintaqaviy tarmoqqa berilgan ta'rifni belgilang. Kompyuterlar va ularni bog'lab turgan qurilmalardan iborat bo'lib, ular odatda bitta tarmoqda bo'ladi. Quyidagilardan MAN tarmoqqa berilgan ta'rifni belgilang. Kompyuterlar va ularni bog'lab turgan qurilmalardan iborat bo'lib, ular odatda bitta tarmoqda bo'ladi. Quyidagilardan shaxsiy tarmoqqa berilgan ta'rifni belgilang. Kompyuterlar va ularni bog'lab turgan qurilmalardan iborat bo'lib, ular odatda bitta tarmoqda bo'ladi. Quyidagilardan qaysi biri tarmoqning yulduz topologiyasiga berilgan \*Tarmoqda har bir kompyuter yoki tugun Markaziy tugunga individual bog'langan bo'ladi Quyidagilardan qaysi biri tarmoqning shina topologiyasiga berilgan Tarmoqda har bir kompyuter yoki tugun markaziy tugunga individual bog'langan bo'ladi Quyidagilardan qaysi biri tarmoqning halqa topologiyasiga berilgan Tarmoqda har bir kompyuter yoki tugun markaziy tugunga individual bog'langan bo'ladi Quyidagilardan qaysi biri tarmoqning mesh topologiyasiga berilgan Tarmoqda har bir kompyuter yoki tugun markaziy tugunga individual bog'langan bo'ladi Tarmoq kartasi nima? \*Hisoblash qurilmasining ajralmas qismi bo'lib, qurilmani tarmoqqa ulash imkoniyatini taqdim etadi Repetir nima? Hisoblash qurilmasining ajralmas qismi bo'lib, qurilmani tarmoqqa ulash imkoniyatini taqdim etadi Hub nima? Hisoblash qurilmasining ajralmas qismi bo'lib, qurilmani tarmoqqa ulash imkoniyatini taqdim etadi Switch nima? Hisoblash qurilmasining ajralmas qismi bo'lib, qurilmani tarmoqqa ulash imkoniyatini taqdim etadi Router nima? Hisoblash qurilmasining ajralmas qismi bo'lib, qurilmani tarmoqqa ulash imkoniyatini taqdim etadi DNS tizimlari. \*Host nomlari va internet nomlarini IP manzillarga o'zgartirish yoki teskarisini amalga oshiradi TCP bu- ... \*Transmission Control Protocol UDP bu-... User domain protocol IP protokolining necha xil



versiyasi mavjud? 1 Tarmoq xavfsizligiga tahdidlar tavsiflangan bandni belgilang \*Ichki, tashqi Tarmoq xavfsizligining buzilishi natijasida biznes faoliyatining buzilishi qanday oqibatlarga olib keladi \*Biznes jarayonlarni to'xtab qolishiga olib keladi Tarmoq xavfsizligining buzilishi natijasida ishlab chiqarishning yo'qolishi qanday oqibatlarga olib keladi Biznesda ixtiyoriy hujum biznes jarayonlarni to'xtab qolishiga olib keladi Tarmoq xavfsizligining buzilishi natijasida maxfiylikni yo'qolishi qanday oqibatlarga olib keladi Biznesda ixtiyoriy hujum biznes jarayonlarni to'xtab qolishiga olib keladi Tarmoq xavfsizligining buzilishi natijasida axborotning o'g'irlanishi qanday oqibatlarga olib keladi Biznesda ixtiyoriy hujum biznes jarayonlarni to'xtab qolishiga olib keladi Quyidagi ta'riflardan qaysi biri tarmoqning texnologik zaifligini ifodalaydi \*Tarmoq qurilmalari, switch yoki routerlardagi autentifikatsiya usullarining yetarlicha bardoshli bo'lmashligi Quyidagi ta'riflardan qaysi biri tarmoqning sozlanishdagi zaifligini ifodalaydi Tarmoq qurilmalari, switch yoki routerlardagi autentifikatsiya usullarining yetarlicha bardoshli bo'lmashligi Quyidagi ta'riflardan qaysi biri tarmoqning xavfsizlik siyosatidagi zaifligini ifodalaydi. Tarmoq qurilmalari, switch yoki routerlardagi autentifikatsiya usullarining yetarlicha bardoshli bo'lmashligi Asosan tarmoq, tizim va tashkilot haqidagi axborot olish maqsadda amalga oshiriladigan tarmoq hujumi qaysi \*Razvedka hujumlari Razvedka hujumiga berilgan ta'rifni aniqlang \*Asosiy hujumlarni oson amalga oshirish uchun tashkilot va tarmoq haqidagi axborotni to'plashni maqsad qiladi; Kirish hujumiga berilgan ta'rifni aniqlang asosiy hujumlarni oson amalga oshirish uchun tashkilot va tarmoq haqidagi axborotni to'plashni maqsad qiladi; DOS hujumiga berilgan ta'rifni aniqlang asosiy hujumlarni oson amalga oshirish uchun tashkilot va tarmoq haqidagi axborotni to'plashni maqsad qiladi; Zararli hujumga berilgan ta'rifni aniqlang asosiy hujumlarni oson amalga oshirish uchun tashkilot va tarmoq haqidagi axborotni to'plashni maqsad qiladi; Razvedka hujumari necha turga bo'linadi 1 Qaysi hujum jarayoni TCP/IP tarmog'ida paketlarni tutib olish, dekodlash, tekshirish va tarjima qilishni o'z ichiga oladi \*Paketlarni snifferlash Tarmoqlaro ekranni OSI modeli bo'yicha qanday turlarga bo'lindi? \*• paket filterlari tarmoq satxida ishlaydi; ekspert paketi filterlari – transport sahida ishlaydi; ilova proksilari – ilova satxida Tarmoqlaro ekranni foydalanilgan texnologiyasi bo'yicha qanday turlarga bo'lindi? paket filterlari tarmoq satxida ishlaydi; ekspert paketi filterlari – transport sahida ishlaydi; ilova proksilari – ilova satxida Tarmoqlaro ekranni bajarilishiga ko'ra qanday turlarga bo'lindi? paket filterlari tarmoq satxida ishlaydi; ekspert paketi filterlari – transport sahida ishlaydi; ilova proksilari – ilova satxida Tarmoqlaro ekranni ulanish sxemasi bo'yicha qanday turlarga bo'lindi? paket filterlari tarmoq satxida ishlaydi; ekspert paketi filterlari – transport sahida ishlaydi; ilova proksilari – ilova satxida Paket filtrlari tarmoqlararo ekrani vazifasi nima? \*Tarmoq satxida paketlarni tahlillashga asoslan; Ilova proksilari tarmoqlararo ekrani vazifasi nima? Tarmoq satxida paketlarni tahlillashga asoslan; Ekspert paket filtrlari tarmoqlararo ekrani vazifasi nima? Tarmoq satxida paketlarni tahlillashga asoslan; Quyidagilardan qaysi biri paket filtrlari tarmoqlararo ekrani kamchiligini ifodalaydi. \*Bu turdagi tarmoqlararo ekran TCP aloqani tekshirmaydi. Ilova satxi ma'lumotlarni, zararli dasturlarni va hak. tekshirmaydi. Quyidagilardan qaysi biri ekspert paket filtrlari tarmoqlararo ekrani kamchiligini ifodalaydi. Bu turdagi tarmoqlararo ekran TCP aloqani tekshirmaydi. Ilova satxi ma'lumotlarni, zararli dasturlarni va hak. tekshirmaydi. Simsiz tarmoqlarning nechta turi mavjud 5 Bluetooth qanday simsiz tarmoq turiga kiradi. Global Wifi qanday simsiz tarmoq turiga kiradi. Global LTE, CDMA, HSDPA qanday simsiz tarmoq turiga kiradi. \*Global WiMAX qanday simsiz tarmoq turiga kiradi. Global Bluetooth texnologiyasida autentifikatsiya bu... Ikki autentifikatsiyalangan tarmoqda ma'ulmotni almashinish jarayonida tinglashdan va uchunchi tomondan bo'ladigan hujumlardan himoyalash uchun shifrlash amalga oshirish. Bluetooth texnologiyasida konfidensiallik bu... \*Ikki autentifikatsiyalangan

tarmoqda ma'ulmotni almashinish jarayonida tinglashdan va uchunchi tomondan bo'ladigan hujumlardan himoyalash uchun shifrlash amalga oshirish. Bluetooth texnologiyasida avtorizatsiya bu... Ikki autentifikatsiyalangan tarmoqda ma'ulmotni almashinish jarayonida tinglashdan va uchunchi tomondan bo'ladigan hujumlardan himoyalash uchun shifrlash amalga oshirish. GSM bu ...

\*Global System for Mobile Communications Simsiz tarmoq Bluetooth ishlash rejimlari nechta? 2

Kompyuterda hodisalar haqidagi ma'lumot qayerda saqlanadi? \*hodisalar jurnaliga Windows operatsion tizimida xatolik hodisasiga berilgan ta'rifni belgilang. \*Ma'lumotni yo'qotish yoki funktsionallikni yo'qotish kabi muhim muammoni ko'rsatadigan voqea. Masalan, agar xizmat ishga tushirish paytida yuklana olmasa, xatolik hodisasi qayd Windows operatsion tizimida ogohlantirish hodisasiga berilgan ta'rifni belgilang. Ma'lumotni yo'qotish yoki funktsionallikni yo'qotish kabi muhim muammoni ko'rsatadigan voqea. Masalan, agar xizmat ishga tushirish paytida yuklana olmasa, xatolik hodisasi Windows operatsion tizimida axborot hodisasiga berilgan ta'rifni belgilang. Ma'lumotni yo'qotish yoki funktsionallikni yo'qotish kabi muhim muammoni ko'rsatadigan voqea. Masalan, agar xizmat ishga tushirish paytida yuklana olmasa, xatolik hodisasi qayd Windows operatsion tizimida muvaffaqiyatli audit hodisasiga berilgan ta'rifni belgilang. Ma'lumotni yo'qotish yoki funktsionallikni yo'qotish kabi muhim muammoni ko'rsatadigan voqea. Masalan, agar xizmat ishga tushirish paytida yuklana olmasa, xatolik ho Windows operatsion tizimida muvaffaqiyatsiz audit hodisasiga berilgan ta'rifni belgilang. Ma'lumotni yo'qotish yoki funktsionallikni yo'qotish kabi muhim muammoni ko'rsatadigan voqea. Masalan, agar xizmat ishga tushirish paytida yuklana olmasa, xatolik Ma'lumotlarni zaxira nusxalash bu – ...

\*Muhim bo'lgan axborot nusxalash yoki saqlash jarayoni bo'lib, bu ma'lumot yo'qolgan vaqtda qayta tiklash imkoniyatini beradi Zarar yetkazilgandan keyin tizimni normal ish holatiga qaytarish va tizimda saqlanuvchi muhim ma'lumotni yo'qolishidan so'ng uni qayta tiklash uchun qanday amaldan foydalanamiz

\*Zaxira nusxalash Ma'lumotlarni inson xatosi tufayli yo'qolish sababiga ta'rif bering

\*Qasddan yoki tasodifiy ma'lumotni o'chirib yuborilishi, ma'lumotlarni saqlash vositasini to'g'ri joylashtirilmagani yoki ma'lumotlar bazasini xatolik bilan boshqarilganligi. Ma'lumotlarni g'arazli hatti harakatlar yo'qolish sababiga ta'rif bering

Qasddan yoki tasodifiy ma'lumotni o'chirib yuborilishi, ma'lumotlarni saqlash vositasini to'g'ri joylashtirilmagani yoki ma'lumotlar bazasini xatolik bilan boshqarilganligi. Ma'lumotlarni tasodifiy sabablar tufayli yo'qolish sababiga ta'rif bering

Qasddan yoki tasodifiy ma'lumotni o'chirib yuborilishi, ma'lumotlarni saqlash vositasini to'g'ri joylashtirilmagani yoki ma'lumotlar bazasini xatolik bilan boshqarilganligi. Ma'lumotlarni tabiiy ofatlar tufayli yo'qolish sababiga ta'rif bering

Qasddan yoki tasodifiy ma'lumotni o'chirib yuborilishi, ma'lumotlarni saqlash vositasini to'g'ri joylashtirilmagani yoki ma'lumotlar bazasini xatolik bilan boshqarilganligi. Zahira nusxalash strategiyasi nechta bosqichni o'z ichiga oladi? 7

Zaxiralash uchun zarur axborotni aniqlash nechta bosqichda amalga oshiriladi. \*4

Zaxira nusxalovchi vositalar tanlashdagi narx xususiyatiga berilgan ta'rifni nelgilash

\*Har bir tashkilot o'zining budjetiga mos bo'lgan zaxira nusxalash vositasiga ega bo'lishi shart. Zaxira nusxalovchi vositalar tanlashdagi ishonchlilik xususiyatiga berilgan ta'rifni nelgilash

Har bir tashkilot o'zining budjetiga mos bo'lgan zaxira nusxalash vositasiga ega bo'lishi shart. Zaxira nusxalovchi vositalar tanlashdagi tezlik xususiyatiga berilgan ta'rifni nelgilash

Har bir tashkilot o'zining budjetiga mos bo'lgan zaxira nusxalash vositasiga ega bo'lishi shart. Zaxira nusxalovchi vositalar tanlashdagi foydalanuvchanlik xususiyatiga berilgan ta'rifni nelgilash

Har bir tashkilot o'zining budjetiga mos bo'lgan zaxira nusxalash vositasiga ega bo'lishi shart. Zaxira nusxalovchi vositalar tanlashdagi qulaylik xususiyatiga berilgan ta'rifni nelgilash

Har bir tashkilot o'zining budjetiga mos bo'lgan zaxira nusxalash vositasiga ega bo'lishi shart. RAID texnologiyasining transkripsiyasi qanday.

Redundant Array of Independent Disks RAID texnologiyasida nechta satx mavjud 3 RAID 0: diskni navbatlanishi bu-.. \*Ma'lumotni bloklarga bo'lib, bir qancha qattiq diskda ularni yozadi, U IO unumdorligini yuklamani ko'plab kanal va disk drayverlariga bo'lish orqali yaxshilaydi. Agar disk buzilsa, ma'lumotni tiklab bo'lmaydi. • Kamida ikkita RAID 1: diskni navbatlanishi bu-.. Ma'lumotni bloklarga bo'lib, bir qancha qattiq diskda ularni yozadi, U IO unumdorligini yuklamani ko'plab kanal va disk drayverlariga bo'lish orqali yaxshilaydi. Agar disk buzilsa, ma'lumotni tiklab bo'lmaydi. • Kamida ikkita disk talab qilinadi RAID 3: diskni navbatlanishi bu-.. Ma'lumotni bloklarga bo'lib, bir qancha qattiq diskda ularni yozadi, U IO unumdorligini yuklamani ko'plab kanal va disk drayverlariga bo'lish orqali yaxshilaydi. Agar disk buzilsa, ma'lumotni tiklab bo'lmaydi. • Kamida ikkita disk talab qilinadi RAID 5: diskni navbatlanishi bu-.. Ma'lumotni bloklarga bo'lib, bir qancha qattiq diskda ularni yozadi, U IO unumdorligini yuklamani ko'plab kanal va disk drayverlariga bo'lish orqali yaxshilaydi. Agar disk buzilsa, ma'lumotni tiklab bo'lmaydi. • Kamida ikkita disk talab qilinadi RAID 10: diskni navbatlanishi bu-.. \*Gibrid satx bo'lib, RAID 1 va RAID 0 satxlaridan iborat va kamida 4 ta diskni talab etadi RAID 50: diskni navbatlanishi bu-.. Gibrid satx bo'lib, RAID 1 va RAID 0 satxlaridan iborat va kamida 4 ta diskni talab etadi Ma'lumotlarni nusxalash usullari necha xil usulda amalga oshiriladi? \*3 Issiq zaxiralash usuliga berilgan ta'rifni belgilang. \*Ushbu usulda foydalanuvchi tizimni boshqarayotgan vaqtda ham zaxira nusxalash jarayoni davom ettiriladi. Mazkur zaxiralash usulini amalga oshirish tizimni harakatsiz vaqtini kamaytiradi. Iliq zaxiralash usuliga berilgan ta'rifni belgilang. Ushbu usulda foydalanuvchi tizimni boshqarayotgan vaqtda ham zaxira nusxalash jarayoni davom ettiriladi. Mazkur zaxiralash usulini amalga oshirish tizimni harakatsiz vaqtini kamaytiradi. Sovuq zaxiralash usuliga berilgan ta'rifni belgilang. Ushbu usulda foydalanuvchi tizimni boshqarayotgan vaqtda ham zaxira nusxalash jarayoni davom ettiriladi. Mazkur zaxiralash usulini amalga oshirish tizimni harakatsiz vaqtini kamaytiradi. Ichki zahiralash qanday amalga oshiriladi Ichki zahiralashda mahalliy yoki global serverlardan foydalaniladi OSI modelining birinchi satxi qanday nomlanadi \*Fizik satx OSI modelining ikkinchi satxi qanday nomlanadi \*Kanal satxi OSI modelining uchinchi satxi qanday nomlanadi \*Tarmoq satxi OSI modelining oltinchi satxi qanday nomlanadi \*Taqdimlash satxi OSI modelining ettinchi satxi qanday nomlanadi \*Amaliy satx Elektr signallarini qabul qilish va uzatish vazifalarini OSI modelining qaysi satxi bajaradi \*Fizik satx Keltirilgan protokollarning qaysilari transport satxi protokollariga mansub \*TCP,UDP OSI modelining fizik satxi qanday funktsiyalarni bajaradi \*Elektr signallarini uzatish va qabul qilish OSI modelining amaliy satxi qanday funktsiyalarni bajaradi \*Klient dasturlari bilan o'zaro muloqotda bo'lish 12 gacha bo'lgan va 12 bilan o'zaro tub bo'lgan sonlar soni nechta? 6 ta Yevklid algoritmi qanday natijani beradi? \*Sonning eng katta umumiy bo'luvchisini topish Qanday sonlar tub sonlar deb yuritiladi? \*Faqatgina 1 ga va o'ziga bo'linadigan sonlar tub sonlar deyiladi. To'liq zaxiralash Tiklashning tezligi yuqori. axira nusxalash jarayonining sekin va ma'lumotni saqlash uchun ko'p hajm talab etadi O'sib boruvchi zaxiralash Tiklashning tezligi yuqori. Zaxira nusxalash jarayonining sekin va ma'lumotni saqlash uchun ko'p hajm talab etadi Differensial zaxiralash Tiklashning tezligi yuqori. Zaxira nusxalash jarayonining sekin va ma'lumotni saqlash uchun ko'p hajm talab etadi Ushbu jarayon ma'lumot qanday yo'qolgani, ma'lumotni qayta tiklash dasturiy vositasi va ma'lumotni tiklash anzilini qayergaligiga bog'liq bo'ladi. Qaysi jarayon Ma'lumotlarni qayta tiklash Antivirus dasturlarini ko'rsating? \*Drweb, Nod32, Kaspersky Wi-Fi tarmoqlarida quyida keltirilgan qaysi shifrlash protokollaridan foydalaniladi \*wep, wpa, wpa2 Axborot himoyalangan qanday sifatlariga ega bo'lishi kerak? \*ishonchli, qimmatli va to'liq Axborotning eng kichik o'lchov birligi nima? \*bit Virtual xususiy tarmoq – bu? \*VPN Xavfli viruslar bu - ... \*kompyuter ishlashida jiddiy nuqsonlarga

sabab bo'luvchi viruslar Mantiqiy bomba – bu ... \*Ma'lum sharoitlarda zarar keltiruvchi harakatlarni bajaruvchi dastur yoki uning alohida modullari Rezident virus... \*tezkor xotirada saqlanadi DIR viruslari nimani zararlaydi? \*FAT tarkibini zararlaydi .... kompyuter tarmoqlari bo'yicha tarqalib, kompyuterning tarmoqdagi manzilini aniqlaydi va u yerda o'zining nusxasini qoldiradi \*«Chuvalchang» va replikatorli virus Mutant virus... \*shifrlash va deshifrlash algoritmlaridan iborat Fire Wall ning vazifasi... \*tarmoqlar orasida aloqa o'rnatish jarayonida tashkilot va Internet tarmog'i orasida xavfsizlikni ta'minlaydi Kompyuter virusi nima? \*maxsus yozilgan va zararli dastur Kompyuterning viruslar bilan zararlanish yo'llarini ko'rsating \*disk, maxsus tashuvchi qurilma va kompyuter tarmoqlari orqali Trojan dasturlari bu... \*virus dasturlar Kompyuter viruslari xarakterlariga nisbatan necha turga ajraladi? \*5 Antiviruslarni, qo'llanish usuliga ko'ra... turlari mavjud \*detektorlar, faglar, vaksinalar, privivkalar, revizorlar, monitorlar Axborotni himoyalash uchun ... usullari qo'llaniladi. \*kodlashtirish, kriptografiya, stegonografiya Stenografiya mahnosi... \*sirli yozuv ...sirli yozuvning umumiy nazariyasini yaratdiki, u fan sifatida stenografiyaning bazasi hisoblanadi \*K.Shennon Kriptologiya yo'nalishlari nechta? \*2 Kriptografiyaning asosiy maqsadi... \*maxfiylik, yaxlitlikni ta'minlash Zararli dasturiy vositalarni aniqlash turlari nechta \*3 Signaiurana asoslangan \*....bu fayldan topilgan bitlar qatori bo'lib, maxsus belgilarni o'z ichiga oladi. Bu o'rinda ularning xesh qiymatlari ham signatura sifatida xizmat qilishi mumkin. O'zgarishni aniqlashga asoslangan ....bu fayldan topilgan bitlar qatori bo'lib, maxsus belgilarni o'z ichiga oladi. Bu o'rinda ularning xesh qiymatlari ham signatura sifatida xizmat qilishi mumkin. Anomaliyaga asoslangan ....bu fayldan topilgan bitlar qatori bo'lib, maxsus belgilarni o'z ichiga oladi. Bu o'rinda ularning xesh qiymatlari ham signatura sifatida xizmat qilishi mumkin. Antiairuslar qanday usulda viruslarni aniqlaydi Anomaliyaga asoslangan Viruslar - bir qarashda yaxshi va foydali kabi ko'rinuvchi dasturiy vosita sifatida ko'rinsada, yashiringan zararli koddan iborat bo'ladi Rootkitlar- bir qarashda yaxshi va foydali kabi ko'rinuvchi dasturiy vosita sifatida ko'rinsada, yashiringan zararli koddan iborat bo'ladi Backdoorlar - bir qarashda yaxshi va foydali kabi ko'rinuvchi dasturiy vositasifatida ko'rinsada, yashiringan zararli koddan iborat bo'ladi Trojan otlari- \*bir qarashda yaxshi va foydali kabi ko'rinuvchi dasturiy vosita sifatida ko'rinsada, yashiringan zararli koddan iborat bo'ladi Ransomware- bir qarashda yaxshi va foydali kabi ko'rinuvchi dasturiy vosita sifatida ko'rinsada, yashiringan zararli koddan iborat bo'ladi Resurslardan foydalanish usuliga ko'ra viruslar qanday turlarga bo'linadi \*Virus parazit, Virus cherv Zararlagan obyektlar turiga ko'ra Virus parazit, Virus cherv Faollashish prinsipiga ko'ra Virus parazit, Virus cherv Dastur kodini tashkil qilish yondashuviga ko'ra Virus parazit, Virus cherv Shifrlanmagan viruslar \*o'zini oddiy dasturlar kabi ko'rsatadi va bunda dastur kodida hech qanday qo'shimcha ishlashlar mavjud bo'lmaydi. Shifrlangan viruslar o'zini oddiy dasturlar kabi ko'rsatadi va bunda dastur kodida hech qanday qo'shimcha ishlashlar mavjud bo'lmaydi. Polimorf viruslar o'zini oddiy dasturlar kabi ko'rsatadi va bunda dastur kodida hech qanday qo'shimcha ishlashlar mavjud bo'lmaydi. Dasturiy viruslar-... bir vaqtning o'zida turli xildagi Obyektlarni zararlaydi. Masalan, OneHalf.3544 virusi ham MS-DOS dasturlari ham qattiq diskning yuklanuvchi sektorlarini zararlasa, Anarchy oilasiga tegishli viruslar MS-DOS va Windows dasturlaridan tashqari, MS Word hujjatlarini ham zararlay oladi. Ko'p platformali viruslar \*bir vaqtning o'zida turli xildagi Obyektlarni zararlaydi. Masalan, OneHalf.3544 virusi ham MS-DOS dasturlari ham qattiq diskning yuklanuvchi sektorlarini zararlasa, Anarchy oilasiga tegishli viruslar MS-DOS va Windows dasturlaridan tashqari, MS Word hujjatlarini ham zararlay oladi. Yuklanuvchi viruslar bir vaqtning o'zida turli xildagi Obyektlarni zararlaydi. Masalan, OneHalf.3544 virusi ham MS-DOS dasturlari ham qattiq diskning yuklanuvchi sektorlarini zararlasa, Anarchy oilasiga tegishli viruslar MS-DOS va

Windows dasturlaridan tashqari, MS Word hujjatlarini ham zararlaysin. Makroviruslar... bir vaqtning o'zida turli xildagi Obyektlarni zararlaysin. Masalan, OneHalf.3544 virusi ham MS-DOS dasturlari ham qattiq diskning yuklanuvchi sektorlarini zararlaysin, Anarchy oilasiga tegishli viruslar MS-DOS va Windows dasturlaridan tashqari, MS Word hujjatlarini ham zararlaysin. Birinchi kompyuter virusi nima deb nomlangan Cherv P= 31, q=29 Eyer funksiyasida  $f(p,q)$  ni hisoblang  $*840 \ 256 \bmod 25 = ?$  5 bu yaxlit «butun»ni tashkil etuvchi bog'liq yoki o'zaro bog'langan tashkil etuvchilar guruhi nima deyiladi. \*Tizim Tashkilotni himoyalash maqsadida amalga oshirilgan xavfsizlik nazoratini tavsiflovchi yuqori satxli hujjat yoki hujjatlar to'plami nima deyiladi Standart RSA shifrlash algoritmidan foydalaniladigan sonlarning spektri o'lchami qanday? 65535; DES algoritmi akslantirishlari raundlari soni qancha? \*16; DES algoritmi shifrlash blokining chap va o'ng qism bloklarining o'lchami qancha? CHap qism blok 32 bit, o'ng qism blok 48 bit; Simmetrik va asimmetrik shifrlash algoritmlarining qanday mohiyatan farqli tomonlari bor? SHifrlash va deshifrlash jarayonlarida kalitlardan foydalanish qoidalariga ko'ra farqlanadi 19 gacha bo'lgan va 19 bilan o'zaro tub bo'lgan sonlar soni nechta? 19 ta 10 gacha bo'lgan va 10 bilan o'zaro tub bo'lgan sonlar soni nechta? \*4 ta Qaysi formula qoldiqli bo'lish qonunini ifodalaydi Eyer funksiyasida (1) qiymati nimaga teng? \*0 Eyer funksiyasida 60 sonining qiymatini toping. 59 Eyer funksiyasi yordamida 1811 sonining qiymatini toping. \*1810 97 tub sonmi? \*Tub Quyidagi modulli ifodani qiymatini toping  $(148 + 14432) \bmod 256$ . \*244 Quyidagi sonlarning eng katta umumiy bo'luvchilarini toping. 88 i 220 21 Quyidagi ifodani qiymatini toping.  $-17 \bmod 11$  6 2 soniga 10 modul bo'yicha teskari sonni toping. 3 I: S: Xavfsizlikning asosiy yo'nalishlarini sanab o'ting. +: Axborot xavfsizligi, Iqtisodiy xavfsizlik, Mudofaa xavfsizligi, Ijtimoiy xavfsizlik, Ekologik xavfsizlik -: Axborot va Iqtisodiy xavfsizlik, Signallar havfsizligi, Mobil aloqa xavfsizligi, Dasturiy ta'minot xavfsizligi -: Mudofaa xavfsizligi, Ijtimoiy xavfsizlik, Signallar havfsizligi, Mobil aloqa xavfsizligi, Ekologik xavfsizlik -: Axborot xavfsizligi, Iqtisodiy xavfsizlik, Mudofaa xavfsizligi, Ijtimoiy xavfsizlik, Dasturiy ta'minot xavfsizligi, Ekologik xavfsizlik I: S: Axborot xavfsizligining asosiy maqsadlaridan biribu... +: Axborotlarni o'g'irlanishini, yo'qolishini, soxtalashtirishini oldini olish -:Ob'yektga bevosita ta'sir qilish -: Axborotlarni shifrlash, saqlash, yetkazib berish -: Tarmoqdagi foydalanuvchilarni xavfsizligini ta'minlab berish I: S: Konfidentsiallikga to'g'ri ta'rif keltiring. +: axborot inshonchliligi, tarqatilishi mumkin emasligi, maxfiyligi kafolati; -:axborot konfidentsialligi, tarqatilishi mumkinligi, maxfiyligi kafolati; -:axborot inshonchliligi, tarqatilishi mumkin emasligi, parollanganligi kafolati; -:axborot inshonchliligi, axborotlashganligi, maxfiyligi kafolati; I: S: Yaxlitlikni buzilishi bu - ... +: Soxtalashtirish va o'zgartirish -: Ishonchsizlik va soxtalashtirish -: Soxtalashtirish -: Butunmaslik va yaxlitlanmaganlik I: S:... axborotni himoyalash tizimi deyiladi. +: Axborotning zaif tomonlarini kamaytiruvchi axborotga ruxsat etilmagan kirishga, uning chiqib ketishiga va yo'qotilishiga to'sqinlik qiluvchi tashkiliy, texnik, dasturiy, texnologik va boshqa vosita, usul va choralarning kompleksi -: Axborot egalari hamda vakolatli davlat organlari shaxsan axborotning qimmatliligi, uning yo'qotilishidan keladigan zarar va himoyalash mexanizmining narxidan kelib chiqqan holda axborotni himoyalashning zaruriy darajasi -: Axborot egalari hamda vakolatli davlat organlari shaxsan axborotning qimmatliligi, uning yo'qotilishidan keladigan zarar va himoyalash mexanizmining zaruriy darajasi hamda tizimning turini, himoyalash usullar va vositalari -: Axborotning zaif tomonlarini kamaytiruvchi axborotga ruxsat etilmagan kirishga, uning chiqib ketishiga va yo'qotilishiga to'sqinlik qiluvchi tashkiliy, texnik, dasturiy, texnologik va boshqa vosita, usul I: S: Kompyuter virusi nima? +: maxsus yozilgan va zararli dastur -: .exe fayl -: boshqariluvchi dastur -: Kengaytmaga ega bo'lgan fayl I: S: Kriptografiyaning asosiy maqsadi... +: maxfiylik, yaxlitlikni ta'minlash -:ishonchlilik, butunlikni ta'minlash -:autentifikatsiya,

identifikatsiya -:ishonchlilik, butunlilikni ta'minlash, autentifikatsiya, identifikatsiya I: S: SMTP - Simple Mail Transfer protokol nima? +: elektron pochta protokoli -:transport protokoli -:internet protokoli -:Internetda ommaviy tus olgan dastur I: S: SKIP protokoli... +: Internet protokollari uchun kriptokalitlarning oddiy boshqaruvi -:Protokollar boshqaruvi -:E-mail protokoli -:Lokal tarmoq protokollari uchun kriptokalitlarning oddiy boshqaruvi I: S: Kompyuter tarmog'ining asosiy komponentlariga nisbatan xavf-xatarlar... +: uzilish, tutib qolish, o'zgartirish, soxtalashtirish -:o'zgartirish, soxtalashtirish -:tutib qolish, o'zgarish, uzilish -:soxtalashtirish, uzilish, o'zgartirish I: S: ...ma'lumotlar oqimini passiv hujumlardan himoya qilishga xizmat qiladi. +: konfidentsiallik -:identifikatsiya -:autentifikatsiya -: maxfiylik I: S: Foydalanish huquqini cheklovchi matritsa modeli bu... +: Bella La-Padulla modeli -:Dening modeli -:Landver modeli -:Huquqlarni cheklovchi model I: S: Kompyuter tarmoqlarida tarmoqning uzoqlashtirilgan elemenlari o'rtasidagi aloqa qaysi standartlar yordamida amalga oshiriladi? +: TCP/IP, X.25 protokollar -:X.25 protokollar -:TCP/IP -:SMTP I: S: Autentifikatsiya nima? +: Ma'lum qilingan foydalanuvchi, jarayon yoki qurilmaning haqiqiy ekanligini tekshirish muolajasi -: Tizim meyoriy va g'ayritabiiy hollarda rejalashtirilgandek o'zini tutishligi holati -: Istalgan vaqtda dastur majmuasining mumkinligini kafolati -:Tizim noodatiy va tabiiy hollarda qurilmaning haqiqiy ekanligini tekshirish muolajasi I: S:Identifikatsiya bu- ... +: Foydalanuvchini uning identifikatori (nomi) bo'yicha aniqlash jarayoni -:Ishonchliligini tarqalishi mumkin emasligi kafolati -:Axborot boshlang'ich ko'rinishda ekanligi uni saqlash, uzatishda ruxsat etilmagan o'zgarishlar -:Axborotni butunligini saqlab qolgan holda uni elementlarini o'zgartirishga yo'l qo'ymaslik I: S:O'rin almashtirish shifri bu - ... +: Murakkab bo'lmagan kriptografik akslantirish -:Kalit asosida generatsiya qilish -:Ketma-ket ochiq matnni ustiga qo'yish -:Belgilangan biror uzunliklarga bo'lib chiqib shifrlash I: S:Simmetrik kalitli shifrlash tizimi necha turga bo'linadi. +: 2 turga -:3 turga -:4 turga -: 5 turga I: S: Kalitlar boshqaruvi 3 ta elementga ega bo'lgan axborot almashinish jarayonidir bular ... +: hosil qilish, yig'ish, taqsimlash -:ishonchliligi, maxfiyligi, aniqligi -:xavfsizlik, tez ishlashi, to'g'ri taqsimlanishi -:abonentlar soni, xavfsizligi, maxfiyligi I: S: Kriptologiya - +: axborotni qayta akslantirib himoyalash muammosi bilan shug'ullanadi -:axborotni qayta akslantirishning matematik usullarini izlaydi va tadqiq qiladi -:kalitni bilmasdan shifrlangan matnni ochish imkoniyatlarini o'rganadi -:kalitlarni bilmasdan shifrnı ochishga bardoshlilikni aniqlovchi shifrlash tavsifi I: S: Kriptografiyada alifbo – +: axborot belgilarini kodlash uchun foydalaniladigan chekli to'plam -:matnni shifrlash va shifrnı ochish uchun kerakli axborot -:xabar muallifi va tarkibini aniqlash maqsadida shifrmatnga qo'shilgan qo'shimcha -:kalit axborotni shifrllovchi kalitlar I: S: Simmetrik kriptotizimlarda ... jumlanı davom ettiring +: shifrlash va shifrnı ochish uchun bitta va aynan shu kalitdan foydalaniladi -:bir-biriga matematik usullar bilan bog'langan ochiq va yopiq kalitlardan foydalaniladi -:axborot ochiq kalit yordamida shifrlanadi, shifrnı ochish esa faqat yopiq kalit yordamida amalga oshiriladi -:kalitlardan biri ochiq boshqasi esa yopiq hisoblanadi I: S: Kriptobardoshlilik deb ... +: kalitlarnı bilmasdan shifrnı ochishga bardoshlilikni aniqlovchi shifrlash tavsifi -:axborotni qayta akslantirib himoyalash muammosi bilan shug'ullanadi -:kalitni bilmasdan shifrlangan matnnı ochish imkoniyatlarini o'rganadi -:axborotni qayta akslantirishning matematik usullarini izlaydi va tadqiq qiladi I: S: Elektron raqamli imzo deb – +: xabar muallifi va tarkibini aniqlash maqsadida shifrmatnga qo'shilgan qo'shimcha -:matnnı shifrlash va shifrnı ochish uchun kerakli axborot -:axborot belgilarini kodlash uchun foydalaniladigan chekli to'plam -:kalit axborotni shifrllovchi kalitlar I: S: Kriptografiya – +: axborotni qayta akslantirishning matematik usullarini izlaydi va tadqiq qiladi -:axborotni qayta akslantirib himoyalash muammosi bilan shug'ullanadi -:kalitni bilmasdan shifrlangan matnnı ochish imkoniyatlarini o'rganadi -:kalitlarnı bilmasdan shifrnı ochishga bardoshlilikni aniqlovchi shifrlash

tavsifi I: S: Kriptografiyada matn – +: alifbo elementlarining tartiblangan to'plami -:matnni shifrlash va shifrini ochish uchun kerakli axborot -:axborot belgilarini kodlash uchun foydalaniladigan chekli to'plam -:kalit axborotni shifrllovchi kalitlar I: S: Kriptoanaliz – +: kalitlarni bilmasdan shifrn ochishga bardoshlilikni aniqlovchi shifrlash tavsifi -:axborotni qayta akslantirishning matematik usullarini izlaydi va tadqiq qiladi -:axborotni qayta akslantirib himoyalash muammosi bilan shug'ullanadi -:kalitni bilmasdan shifrlangan matnni ochish imkoniyatlarini o'rganadi I: S: Shifrlash – +: akslantirish jarayoni ochiq matn deb nomlanadigan matn shifrmatnga almashtiriladi -:kalit asosida shifrmatn ochiq matnga akslantiriladi -:shifrlashga teskari jarayon -:Almashtirish jarayoni bo'lib: ochiq matn deb nomlanadigan matn o'girilgan holatga almashtiriladi I: S: Faol hujum turi deb... +: Maxfiy uzatish jarayonini uzib qo'yish, modifikatsiyalash, qalbaki shifr ma'lumotlar tayyorlash harakatlaridan iborat jarayon -:Maxfiy ma'lumotni aloqa tarmog'ida uzatilayotganda eshitish, tahrir qilish, yozib olish harakatlaridan iborat uzatilayotgan ma'lumotni qabul qiluvchiga o'zgartirishsiz yetkazish jarayoni -:Ma'lumotga o'zgartirish kiritmay uni kuzatish jarayoni -:Sust hujumdan farq qilmaydigan jarayon I: S: Blokli shifrlash- +: shifrlanadigan matn blokiga qo'llaniladigan asosiy akslantirish -:murakkab bo'lmagan kriptografik akslantirish -:axborot simvollarini boshqa alfavit simvollar bilan almashtirish -:ochiq matnning har bir harfi yoki simvoli alohida shifrlanishi I: S: Simmetrik kriptotizimning uzluksiz tizimida ... +: ochiq matnning har bir harfi va simvoli alohida shifrlanadi -:belgilangan biror uzunliklarga teng bo'linib chiqib shifrlanadi -:murakkab bo'lmagan kriptografik akslantirish orqali shifrlanadi -:ketma-ket ochiq matnlarni o'rniga qo'yish orqali shifrlanadi I: S: Kriptotizimga qo'yiladigan umumiy talablardan biri +: shifr matn uzunligi ochiq matn uzunligiga teng bo'lishi kerak -:shifrlash algoritmining tarkibiy elementlarini o'zgartirish imkoniyati bo'lishi lozim -:ketma-ket qo'llaniladigan kalitlar o'rtasida oddiy va oson bog'liqlik bo'lishi kerak -:maxfiylik o'ta yuqori darajada bo'lmoqligi lozim I: S: Berilgan ta'riflardan qaysi biri asimmetrik tizimlarga xos? +: Asimmetrik kriptotizimlarda  $k_1 \neq k_2$  bo'lib,  $k_1$  ochiq kalit,  $k_2$  yopiq kalit deb yuritiladi,  $k_1$  bilan axborot shifrlanadi,  $k_2$  bilan esa deshifrlanadi -:Asimmetrik tizimlarda  $k_1 = k_2$  bo'ladi, ya'ni  $k$  – kalit bilan axborot ham shifrlanadi, ham deshifrlanadi -:Asimmetrik kriptotizimlarda yopiq kalit axborot almashinuvining barcha ishtirokchilariga ma'lum bo'ladi, ochiq kalitni esa faqat qabul qiluvchi biladi -:Asimmetrik kriptotizimlarda  $k_1 \neq k_2$  bo'lib, kalitlar hammaga oshkor etiladi I: S: Yetarlicha kriptoturg'unlikka ega, dastlabki matn simvollarini almashtirish uchun bir necha alfavitdan foydalanishga asoslangan almashtirish usulini belgilang +: Vijener matritsasi, Sesar usuli -:monoalfavitli almashtirish -:polialfavitli almashtirish -:o'rin almashtirish I: S: Akslantirish tushunchasi deb nimaga aytiladi? +: 1-to'plamli elementlariga 2-to'plam elementalriga mos bo'lishiga -:1-to'plamli elementlariga 2-to'plam elementalrini qarama-qarshiligiga -:har bir elementni o'ziga ko'payimasiga -:agar birinchi va ikkinchi to'plam bir qiymatga ega bulmasa I: S: Simmetrik guruh deb nimaga aytiladi? +: O'rin almashtirish va joylashtirish -:O'rin almashtirish va solishtirish -:Joylashtirish va solishtirish -:O'rin almashtirish va transportizatsiyalash I: S: Qo'yish, o'rin almashtirish, gammalash kriptografiyaning qaysi turiga bog'liq? +: simmetrik kriptosistemalar -:assimmetrik kriptosistemalar -:ochiq kalitli kriptosistemalar -:autentifikatsiyalash I: S: Internetda elektron pochta bilan ishlash uchun TCP/IPga asoslangan qaysi protokoldan foydalaniladi? +: SMTP, POP yoki IMAP -:SKIP, ATM, FDDI -:X.25 va IMAR -:SMTP, TCP/IP I: S: Axborot resursi – bu? +: axborot tizimi tarkibidagi elektron shakldagi axborot, ma'lumotlar banki, ma'lumotlar bazasi -:cheklanmagan doiradagi shaxslar uchun mo'ljallangan hujjatlashtirilgan axborot, bosma, audio, audiovizual hamda boshqa xabarlar va materiallar -:identifikatsiya qilish imkonini beruvchi rekvizitlari qo'yilgan holda moddiy jismda qayd etilgan axborot -:manbalari va taqdim etilish shaklidan qathi nazar shaxslar, predmetlar,

faktlar, voqealar, hodisalar va jarayonlar to'g'risidagi ma'lumotlar I: S: Shaxsning, o'zini axborot kommunikatsiya tizimiga tanishtirish jarayonida qo'llaniladigan belgilar ketmaketligi bo'lib, axborot kommunikatsiya tizimidan foydalanish huquqiga ega bo'lish uchun foydalaniluvchining maxfiy bo'lmagan qayd yozuvi – bu? +: login parol -:identifikatsiya -:maxfiy maydon -: token I: S: Uning egasi haqiqiyligini aniqlash jarayonida tekshiruv axboroti sifatida ishlatiladigan belgilar ketma-ketligi (maxfiy so'z) – bu? +: parol -:login -:identifikatsiya -:maxfiy maydon foydalanuvchilarni ro'yxatga olish va ularga dasturlar va ma'lumotlarni ishlatishga huquq berish jarayoni I: S: Identifikatsiya jarayoni qanday jarayon? +: axborot tizimlari obyekt va subhektlariga uni tanish uchun nomlar (identifikator) berish va berilgan nom bo'yicha solishtirib uni aniqlash jarayoni -:obyekt yoki subhektni unga berilgan identifikatorga mosligini tekshirish va belgilar ketmaketligidan iborat maxfiy kodini tekshirish orqali aslligini aniqlash -:foydalanuvchining resursdan foydalanish huquqlari va ruxsatlarini tekshirish jarayoni -:foydalanuvchilarni ro'yxatga olish va ularga dasturlar va ma'lumotlarni ishlatishga huquq berish jarayoni I: S: Autentifikatsiya jarayoni qanday jarayon? +: obyekt yoki subhektni unga berilgan identifikatorga mosligini tekshirish va belgilar ketmaketligidan iborat maxfiy kodini tekshirish orqali aslligini aniqlash -:axborot tizimlari obyekt va subhektlariga uni tanish uchun nomlar (identifikator) berish va berilgan nom bo'yicha solishtirib uni aniqlash jarayoni -:foydalanuvchining resursdan foydalanish huquqlari va ruxsatlarini tekshirish jarayoni -:foydalanuvchilarni ro'yxatga olish va ularga dasturlar va ma'lumotlarni ishlatishga huquq berish jarayoni I: S: Ro'yxatdan o'tish bu? +: foydalanuvchilarni ro'yxatga olish va ularga dasturlar va ma'lumotlarni ishlatishga huquq berish jarayoni -:axborot tizimlari ob'yekt va subhektlariga uni tanish uchun nomlar (identifikator) berish va berilgan nom bo'yicha solishtirib uni aniqlash jarayoni -:ob'yekt yoki subhektni unga berilgan identifikatorga mosligini tekshirish va belgilar ketmaketligidan iborat maxfiy kodini tekshirish orqali aslligini aniqlash -:foydalanuvchining resursdan foydalanish huquqlari va ruxsatlarini tekshirish jarayoni I: S: Axborot qanday sifatlarga ega bo'lishi kerak? +: ishonchli, qimmatli va to'liq -:uzluksiz va uzlukli -:ishonchli, qimmatli va uzlukli -:ishonchli, qimmatli va uzluksiz I: S: Axborotning eng kichik o'lchov birligi nima? +: bit -:kilobayt -:bayt -:bitta simvol I: S: Elektron hujjatning rekvizitlari nechta qismdan iborat? +: 4 -:5 -:6 -:7 I: S: Axborotlarni saqlovchi va tashuvchi vositalar qaysilar? +: fleshka, CD va DVD disklar -:Qattiq disklar va CDROM -:CD va DVD, DVDROM -:Qattiq disklar va DVDROM I: S: Avtorizatsiya jarayoni qanday jarayon? +: foydalanuvchining resursdan foydalanish huquqlari va ruxsatlarini tekshirish jarayoni -:axborot tizimlari obyekt va subhektlariga uni tanish uchun nomlar (identifikator) berish va -berilgan nom bo'yicha solishtirib uni aniqlash jarayoni -:obyekt yoki subhektni unga berilgan identifikatorga mosligini tekshirish va belgilar ketmaketligidan iborat maxfiy kodini tekshirish orqali aslligini aniqlash. -: parollash jarayoni I: S: Kodlash nima? +: Ma'lumotni osongina qaytarish uchun hammaga ochiq bo'lgan sxema yordamida ma'lumotlarni boshqa formatga o'zgartirishdir -:Ma'lumot boshqa formatga o'zgartiriladi, biroq uni faqat maxsus shaxslar qayta o'zgartirishi mumkin bo'ladi -:Ma'lumot boshqa formatga o'zgartiriladi, barcha shaxslar kalit yordamida qayta o'zgartirishi mumkin bo'ladi -:Maxfiy xabarni soxta xabar ichiga berkitish orqali aloqani yashirish hisoblanadi I: S: Shifrlash nima? +: Ma'lumot boshqa formatga o'zgartiriladi, biroq uni faqat maxsus shaxslar qayta o'zgartirishi mumkin bo'ladi -:Ma'lumotni osongina qaytarish uchun hammaga ochiq bo'lgan sxema yordamida ma'lumotlarni boshqa formatga o'zgartirishdir -: Ma'lumot boshqa formatga o'zgartiriladi, barcha shaxslar kalit yordamida qayta o'zgartirishi mumkin bo'ladi -:Maxfiy xabarni soxta xabar ichiga berkitish orqali aloqani yashirish hisoblanadi I: S: Axborotni shifrnı ochish (deshifrlash) bilan qaysi fan shug'ullanadi +:Kriptoanaliz -:Kartografiya -:Kriptologiya -:Adamar usuli I: S: Qaysi juftlik RSA



algoritmining ochiq va yopiq kalitlarini ifodalaydi +: {d, n} – yopiq, {e, n} – ochiq; -: {d, e} – ochiq, {e, n} – yopiq; -: {e, n} – yopiq, {d, n} – ochiq; -: {e, n} – ochiq, {d, n} – yopiq; I: S: Zamonaviy kriptografiya qanday bo'limlardan iborat? -: Elektron raqamli imzo; kalitlarni boshqarish -: Simmetrik kriptotizimlar; ochiq kalitli kriptotizimlar; +: Simmetrik kriptotizimlar; ochiq kalitli kriptotizimlar; Elektron raqamli imzo; kalitlarni boshqarish -: Simmetrik kriptotizimlar; ochiq kalitli kriptotizimlar; kalitlarni boshqarish I: S: Shifr nima? +: Shifrlash va deshifrlashda foydalaniladigan matematik funktsiyadan iborat bo'lgan kriptografik algoritmlar -: Kalitlarni taqsimlash usuli -: Kalitlarni boshqarish usuli -: Kalitlarni generatsiya qilish usuli I: S: Ochik kalitli kriptotizimlarning mohiyati nimadan iborat? +: Ochik kalitli kriptotizimlarda bir-biri bilan matematik bog'langan 2 ta – ochik va yopiq kalitlardan foydalaniladi -: Ochik kalitli kriptotizimlarda shifrlash va deshifrlashda 1 ta – kalitdan foydalaniladi -: Ochik kalitli kriptotizimlarda ma'lumotlarni faqat shifrlash mumkin -: Ochik kalitli kriptotizimlarda ma'lumotlarni faqat deshifrlash mumkin I: S: Oqimli shifrlashning mohiyati nimada? +: Oqimli shifrlash birinchi navbatda axborotni bloklarga bo'lishning imkoni bo'lmagan hollarda zarur, -: Qandaydir ma'lumotlar oqimini har bir belgisini shifrlab, boshqa belgilarini kutmasdan kerakli joyga jo'natish uchun oqimli shifrlash zarur, -: Oqimli shifrlash algoritmlari ma'lumotlarni bitlar yoki belgilar bo'yicha shifrlaydi -: Oqimli shifrlash birinchi navbatda axborotni bloklarga bo'lishning imkoni bo'lmagan hollarda zarur, I: S: Simmetrik algoritmlarni xavfsizligini ta'minlovchi omillarni ko'rsating. +: uzatilayotgan shifrlangan xabarni kalitsiz ochish mumkin bo'lmashligi uchun algoritmlar yetarli darajada bardoshli bo'lishi lozim, uzatilayotgan xabarni xavfsizligi algoritmlarni maxfiyligiga emas, balki kalitni maxfiyligiga bog'liq bo'lishi lozim, -: uzatilayotgan xabarni xavfsizligi kalitni maxfiyligiga emas, balki algoritmlarni maxfiyligiga bog'liq bo'lishi lozim -: uzatilayotgan xabarni xavfsizligi shifrlanayotgan xabarni uzunligiga bog'liq bo'lishi lozim -: uzatilayotgan xabarni xavfsizligi shifrlanayotgan xabarni uzunligiga emas, balki shifrlashda foydalaniladigan arifmetik amallar soniga bog'liq bo'lishi lozim I: S: Asimmetrik kriptotizimlar qanday maqsadlarda ishlatiladi? +: shifrlash, deshifrlash, ERI yaratish va tekshirish, kalitlar almashish uchun -: ERI yaratish va tekshirish, kalitlar almashish uchun -: shifrlash, deshifrlash, kalitlar almashish uchun -: Heshlash uchun I: S: Kriptografik elektron raqamli imzolarda qaysi kalitlar ma'lumotni yaxlitligini ta'minlashda ishlatiladi. +: ochik kalitlar -: yopiq kalitlar -: seans kalitlari -: Barcha tildagi kalitlar I: S: Kompyuterning tashqi interfeysi deganda nima tushuniladi? +: kompyuter bilan tashqi qurilmani bog'lovchi simlar va ular orqali axborot almashinish qoidalarini to'plamlari -: tashqi qurilmani kompyuterga bog'lashda ishlatiladigan ulovchi simlar -: kompyuterning tashqi portlari. -: tashqi qurilma bilan kompyuter o'rtasida axborot almashinish qoidalarini to'plami I: S: Lokal tarmoqlarda keng tarqalgan topologiya turi qaysi? +: Yulduz -: Xalqa -: To'liqbog'langan -: Umumiy shina I: S: Ethernet kontsentratori qanday vazifani bajaradi +: kompyuterdan kelayotgan axborotni qolgan barcha kompyuterga yo'naltirib beradi -: kompyuterdan kelayotgan axborotni boshqa bir kompyuterga yo'naltirib beradi -: kompyuterdan kelayotgan axborotni xalqa bo'ylab joylashgan keyingi kompyuterga -: tarmoqning ikki segmentini bir biriga ulaydi I: S: OSI modelida nechta satx mavjud +: 7 -: 4 -: 5 -: 3 I: S: OSI modelining to'rtinchi satxi qanday nomlanadi +: Transport satxi -: Amaliy satxi -: Seanslar satxi -: Taqdimlash satxi I: S: OSI modelining beshinchi satxi qanday nomlanadi +: Seanslar satxi -: Tarmoq satxi -: Fizik satxi -: Amaliy satxi I: S: OSI modelining birinchi satxi qanday nomlanadi +: Fizik satxi -: Seanslar satxi -: Transport satxi -: Taqdimlash satxi I: S: OSI modelining ikkinchi satxi qanday nomlanadi +: Kanal satxi -: Amaliy satxi -: Fizik satxi -: Seanslar satxi I: S: OSI modelining uchinchi satxi qanday nomlanadi +: Tarmoq satxi -: Amaliy satxi -: Kanal satxi -: Taqdimlash satxi I: S: OSI modelining oltinchi satxi qanday nomlanadi +: Taqdimlash satxi -: Amaliy satxi -: Seanslar satxi -: Kanal satxi I: S: OSI modelining

yettinchi satxi qanday nomlanadi +: Amaliy satx -:Seanslar satxi -:Transport satxi -:Taqdimlash satxi  
 I: S: OSI modelining qaysi satxlari tarmoqqa bog'liq satxlar hisoblanadi +: fizik, kanal va tarmoq  
 satxlari -:seans va amaliy satxlar -:amaliy va taqdimlash satxlari -:transport va seans satxlari I: S:  
 OSI modelining tarmoq satxi vazifalari keltirilgan qurilmalarning qaysi birida bajariladi +:  
 Marshrutizator -:Ko'priq -:Tarmoq adapter -:Kontsentrator I: S: Elektr signallarini qabul qilish va  
 uzatish vazifalarini OSI modelining qaysi satxi bajaradi +: Fizik satx -:Kanal satxi -:Tarmoq satxi -  
 -:Transport satxi I: S: Ma'lumotlarni uzatishning optimal marshrutlarini aniqlash vazifalarini OSI  
 modelining qaysi satxi bajaradi +: Tarmoq satxi -:Kanal satxi -:Amaliy satx -:Transport satxi I: S:  
 Keltirilgan protokollarning qaysilari tarmoq satxi protokollariga mansub +: IP, IPX -:NFS, FTP -  
 -:Ethernet, FDDI -:TCP,UDP I: S: Keltirilgan protokollarning qaysilari transport satxi protokollariga  
 mansub +: TCP,UDP -:NFS, FTP -:IP, IPX -:Ethernet, FDDI I: S: OSI modelining fizik satxi qanday  
 funktsiyalarni bajaradi +: Elektr signallarini uzatish va qabul qilish -:Aloqa kanalini va  
 ma'lumotlarni uzatish muxitiga murojaat qilishni boshqarish -:Bog'lanish seansini yaratish,  
 kuzatish, oxirigacha ta'minlash -:Klient dasturlari bilan o'zaro muloqotda bo'lish I: S:  
 Identifikatsiya, autentifikatsiya jarayonlaridan o'tgan foydalanuvchi uchun tizimda bajarishi  
 mumkin bo'lgan amallarga ruxsat berish jarayoni bu... +: Avtorizatsiya -:Shifrlash -:Identifikatsiya -  
 -:Autentifikatsiya I: S: Autentifikatsiya faktorlari nechta +: 3 -:4 -:5 -: 6 I: S: Ko'z pardasi, yuz  
 tuzilishi, ovoz tembri- bular autentifikatsiyaning qaysi faktoriga mos belgilar? +: Biometrik  
 autentifikatsiya -:Biron nimaga egalik asosida -:Biron nimani bilish asosida -:Parolga asoslangan I:  
 S: Barcha kabel va tarmoq tizimlari; tizim va kabellarni fizik nazoratlash; tizim va kabel uchun  
 quvvat manbai; tizimni madadlash muhiti. Bular tarmoqning qaysi satxiga kiradi? +: Fizik satx -  
 -:Tarmoq satxi -:Amaliy satx -:Tadbiqiy sath I: S: Fizik xavfsizlikda Yong'inga qarshi tizimlar necha  
 turga bo'linadi +: 2 -:4 -:3 -:5 I: S: Foydalanishni boshqarishda inson, dastur, jarayon va xokazolar  
 nima vazifani bajaradi? +: Subyekt -:Obyekt -:Tizim -:Jarayon I: S: MAC usuli bilan foydalanishni  
 boshqarishda xavfsizlik markazlashgan holatda kim tomonidan amalga oshiriladi +: xavfsizlik  
 siyosati ma'muri -:Foydalaguvchining o'zi -:Dastur tomonidan -:Boshqarish amaalgga oshirilmaydi I:  
 S: Agar Subyektning xavfsizlik darajasida Obyektning xavfsizlik darajasi mavjud bo'lsa, u holda  
 uchun qanday amalga ruxsat beriladi +: O'qish -:Yozish -:O'zgartirish -:Yashirish I: S: Agar  
 Subyektning xavfsizlik darajasi Obyektning xavfsizlik darajasida bo'lsa, u holda qanday amalga  
 ruxsat beriladi. +: Yozish -:O'qish -:O'zgartirish -:Yashirish I: S: Rol tushunchasiga ta'rif bering. +:  
 Muayyan faoliyat turi bilan bog'liq harakatlar va majburiyatlar to'plami sifatida belgilanishi  
 mumkin -:Foydalanishni boshqarish -:Muayyan faoliyat turi bilan bog'liq imkoniyatlar to'plami  
 sifatida belgilanishi mumkin -:Vakolitlarni taqsimlash I: S: Foydalanishni boshqarishning qaysi usuli  
 - Obyektlar va Subyektlarning atributlari, ular bilan mumkin bo'lgan amallar va so'rovlarga mos  
 keladigan muhit uchun qoidalarni tahlil qilish asosida foydalanishlarni boshqaradi. +: ABAC -:MAC -  
 -:DAC -:RBAC I: S: Biometrik autentifikatsiyalash usullari an'anaviy usullarga nisbatan avfzalliklari  
 qaysi javobda to'g'ri ko'rsatilgan? +: barchasi -:biometrik alomatlarining ishga layoqatli shaxsdan  
 ajratib bo'lmazligi -:biometrik alomatlarini soxtalashtirishning qiyinligi -:biometrik alomatlarini  
 noyobligi tufayli autentifikatsiyalashning ishonchlilik darajasi yuqoriligi I: S: OSI modeli 7 satxi bu +:  
 Ilova -:Seans -:Fizik -:Kanal I: S: OSI modeli 1 satxi bu +: Fizik -:Ilova -:Seans -:Kanal I: S: OSI modeli  
 2 satxi bu +:Kanal -: Fizik -:Ilova -:Seans I: S: TCP/IP modelida nechta satx mavjud +: 4 -:3 -:2 -:8 I: S:  
 Qanday tarmoq qisqa masofalarda qurilmalar o'rtasid a ma'lumot almashinish imkoniyatini  
 taqdim etadi? +: Shaxsiy tarmoq -:Lokal -:Mintaqaviy -:CAMPUS I: S: Tarmoq kartasi bu... +:  
 Hisoblash qurilmasining ajralmas qismi bo'lib, qurilmani tarmoqqa ulash imkoniyatini taqdim  
 etadi. -:Tarmoq repetiri odatda signalni tiklash yoki qaytarish uchun foydalaniladi. -:ko'plab

tarmoqlarni ulash uchun yoki LAN segmentlarini bog'lash uchun xizmat qiladi. -:qabul qilingan signalni barcha chiquvchi portlarga emas balki paketda manzili keltirilgan portga uzatadi. I: S: Server xotirasidagi joyni bepul yoki pulli ijagara berish xizmati qanday ataladi? +: Qabul qilingan signalni barcha chiquvchi portlarga emas balki paketda manzili keltirilgan portga uzatadi. -:Hisoblash qurilmasining ajralmas qismi bo'lib, qurilmani tarmoqqa ulash imkoniyatini taqdim etadi. -:Signalni tiklash yoki qaytarish uchun foydalaniladi. -:Ko'plab tarmoqlarni ulash uchun yoki LAN segmentlarini bog'lash uchun xizmat qiladi. I: S: Hab bu... +: ko'plab tarmoqlarni ulash uchun yoki LAN segmentlarini bog'lash uchun xizmat qiladi. -:Hisoblash qurilmasining ajralmas qismi bo'lib, qurilmani tarmoqqa ulash imkoniyatini taqdim etadi. -:Tarmoq repetiri odatda signalni tiklash yoki qaytarish uchun foydalaniladi. -:qabul qilingan signalni barchachiquvchi portlarga emas balki paketda manzili keltirilgan portga uzatadi. I: S: Tarmoq repiteri bu... +: Signalni tiklash yoki qaytarish uchun foydalaniladi. -:Hisoblash qurilmasining ajralmas qismi bo'lib, qurilmani tarmoqqa ulash imkoniyatini taqdim etadi. -:ko'plab tarmoqlarni ulash uchun yoki LAN segmentlarini bog'lash uchun xizmat qiladi. -:qabul qilingan signalni barcha chiquvchi portlarga emas balki paketda manzili keltirilgan portga uzatadi. I: S: Qanday tizim host nomlari va internet nomlarini IP manzillarga o'zgartirish yoki teskarisini amalga oshiradi. +: DNS tizimlari -:TCP/IP -:Ethernet -:Token ring I: S: ..... protokoli ulanishga asoslangan protokol bo'lib, internet orqali ma'lumotlarni almashinuvchi turli ilovalar uchun tarmoq ulanishlarini sozlashga yordam beradi. +: TCP -:IP -:HTTP -:FTP I: S: .... protokolidan odatda o'yin va video ilovalar tomonidan keng foydalaniladi. +: UDP -:HTTP -:TCP -:FTP I: S: Qaysi protokol ma'lumotni yuborishdan oldin aloqa o'rnatish uchun zarur bo'lgan manzil ma'lumotlari bilan ta'minlaydi. +: IP -:TCP -:HTTP -:FTP I: S: Tarmoq taxdidlari necha turga bo'linadi +: 4 -:2 -:3 -:5 I: S: Qanday xujum asosiy hujumlarni oson amalga oshirish uchun tashkilot va tarmoq haqidagi axborotni to'plashni maqsad qiladi; +: Razvedka hujumlari -:Kirish hujumlari -:Xizmatdan voz kechishga undash (Denial of service, DOS) hujumlari -:Zararli hujumlar I: S: Qanday xujum hujumchi turli texnologiyalardan foydalangan holda tarmoqqa kirishga harakat qiladi +: Kirish hujumlari -:Razvedka hujumlari -:Xizmatdan voz kechishga undash (Denial of service, DOS) hujumlari -:Zararli hujumlar I: S: Qanday xujum da hujumchi mijozlarga, foydalanuvchilarga va tashkilotlarda mavjud bo'lgan biror xizmatni cheklashga urinadi; +: Xizmatdan voz kechishga undash (Denial of service, DOS) hujumlari -:Razvedka hujumlari -:Kirish hujumlari -:Zararli hujumlar I: S: Qanday xujumdp zararli hujumlar tizim yoki tarmoqqa bevosita va bilvosita ta'sir qiladi; +: Zararli hujumlar -:Razvedka hujumlari -:Kirish hujumlari -:Xizmatdan voz kechishga undash (Denial of service, DOS) hujumlari I: S: RSA elektron raqamli imzo algoritmidagi ochiq kalit e qanday shartni qanoatlantirishi shart? +: e soni Eyler funksiyasi -  $\phi(n)$  bilan o'zaro tub -:e ning qiymati  $[1,n]$  kesmaga tegishli ixtiyoriy son -:e soni ixtiyoriy tub son -:e soni ixtiyoriy butun musbat son I: S: RSA elektron raqamli imzo algoritmidagi yopiq kalit d qanday hisoblanadi? Bu yerda p va q tub sonlar,  $n=pq$ ,  $\phi(n)$ - Eyler funksiyasi,e-ochiq kalit +:  $d=e^{(-1)} \bmod \phi(n)$  -:  $d=e^{(-1)} \bmod q$  -: $d=e^{(-1)} \bmod q$  -: $d=e^{(-1)} \bmod p$  I: S: Elektron raqamli imzo algoritmi qanday bosqichlardan iborat bo'ladi? +: Imzo qo'yish va imzoni tekshirishdan -:Faqat imzo qo'yishdan -:Faqat imzoni tekshirishdan -:Barcha javoblar to'g'ri I: S: Imzoni haqiqiyligini tekshirish qaysi kalit yordamida amalga oshiriladi? +: Imzo muallifining ochiq kaliti yordamida -:Ma'lumotni qabul qilgan foydalanuvchining ochiq kaliti yordamida -:Ma'lumotni qabul qilgan foydalanuvchining maxfiy kaliti yordamida -:Imzo muallifining maxfiy kaliti yordamida I: S: Tarmoq modeli-bu... +: Ikki hisoblash tizimlari orasidagi aloqani ularning ichki tuzilmaviy va texnologik asosidan qat'iy nazar muvaffaqiyatli o'rnatilishini asosidir -:Global tarmoq qurish usullari -:Lokal tarmoq qurish usullari -:To'g'ri javob yo'q. I: S: OSI modeli nechta satxga ajraladi? +:

7 -2 -4 -3 I: S: TCP/IP modelining kanal satxiga OSI modelining qaysi satxlari mos keladi +: Kanal, Fizik -:Tarmoq -:Transport -:Ilova, taqdimot, seans. I: S: TCP/IP modelining tarmoq satxiga OSI modelining qaysi satxlari mos keladi +: Tarmoq -:Kanal, Fizik -:Transport -:Ilova, taqdimot, seans. I: S: TCP/IP modelining transport satxiga OSI modelining qaysi satxlari mos keladi +: Transport -:Kanal, Fizik -:Tarmoq -:Ilova, taqdimot, seans. I: S: TCP/IP modelining ilova satxiga OSI modelining qaysi satxlari mos keladi +: Ilova, taqdimot, seans -:Kanal, Fizik -:Tarmoq -:Transport I: S: Quyidagilardan lokal tarmoqqa berilgan ta'rifni belgilang. +: Kompyuterlar va ularni bog'lab turgan qurilmalardan iborat bo'lib, ular odatda bitta tarmoqda bo'ladi. -:Odatda ijaraga olingan telekommunikatsiya liniyalaridan foydalanadigan tarmoqlardagi tugunlarni bir-biriga bog'laydi. -:Bu tarmoq shahar yoki shaharcha bo'ylab tarmoqlarning o'zaro bog'lanishini nazarda tutadi -:Qisqa masofalarda qurilmalar o'rtasida ma'lumot almashinish imkoniyatini taqdim etadi I: S: Quyidagilardan mintaqaviy tarmoqqa berilgan ta'rifni belgilang. +: Odatda ijaraga olingan telekommunikatsiya liniyalaridan foydalanadigan tarmoqlardagi tugunlarni birbiriga bog'laydi. -:Kompyuterlar va ularni bog'lab turgan qurilmalardan iborat bo'lib, ular odatda bitta tarmoqda bo'ladi. -:Bu tarmoq shahar yoki shaharcha bo'ylab tarmoqlarning o'zaro bog'lanishini nazarda tutadi -:Qisqa masofalarda qurilmalar o'rtasida ma'lumot almashinish imkoniyatini taqdim etadi. I: S: Repetir nima? +: Odatda signalni tiklash yoki qaytarish uchun foydalaniladi -:Tarmoq qurilmasi bo'lib, ko'plab tarmoqlarni ulash uchun yoki LAN segmentlarini bog'lash uchun xizmat qiladi -:Hisoblash qurilmasining ajralmas qismi bo'lib, qurilmani tarmoqqa ulash imkoniyatini taqdim etadi -:Ko'plab tarmoqlarni ulash uchun yoki LAN segmentlarini bog'lash uchun xizmat qiladi. Qabul qilingan signalni barcha chiquvchi portlarga emas balki paketda manzili keltirilgan portga uzatadi I: S: Hub nima? +: Tarmoq qurilmasi bo'lib, ko'plab tarmoqlarni ulash uchun yoki LAN segmentlarini bog'lash uchun xizmat qiladi -:Hisoblash qurilmasining ajralmas qismi bo'lib, qurilmani tarmoqqa ulash imkoniyatini taqdim etadi, Odatda signalni tiklash yoki qaytarish uchun foydalaniladi -:Ko'plab tarmoqlarni ulash uchun yoki LAN segmentlarini bog'lash uchun xizmat qiladi. -:Qabul qilingan signalni barcha chiquvchi portlarga emas balki paketda manzili keltirilgan portga uzatadi I: S: Router nima? +: Qabul qilingan ma'lumotlarni tarmoq satxiga tegishli manzillarga ko'ra (IP manzil) uzatadi. -:Tarmoq qurilmasi bo'lib, ko'plab tarmoqlarni ulash uchun yoki LAN segmentlarini bog'lash uchun xizmat qiladi Hisoblash qurilmasining ajralmas qismi bo'lib, qurilmani tarmoqqa ulash imkoniyatini taqdim etadi -:Ko'plab tarmoqlarni ulash uchun yoki LAN segmentlarini bog'lash uchun xizmat qiladi. -:Qabul qilingan signalni barcha chiquvchi portlarga emas balki paketda manzili keltirilgan portga uzatadi I: S: Asosan tarmoq, tizim va tashkilot haqidagi axborot olish maqsadda amalga oshiriladigan tarmoq hujumi qaysi +: Razvedka hujumlari -:Kirish hujumlari -:DOS hujumi -:Zararli hujumlar I: S: Razvedka hujumiga berilgan ta'rifni aniqlang +: Asosiy hujumlarni oson amalga oshirish uchun tashkilot va tarmoq haqidagi axborotni to'plashni maqsad qiladi; -:hujumchi turli texnologiyalardan foydalangan holda tarmoqqa kirishga harakat qiladi hujumchi -:mijozlarga, foydalanuvchilarga va tashkilotlarda mavjud bo'lgan biror xizmatni cheklashga urinadi; -:zararli hujumlar tizim yoki tarmoqqa bevosita va bilvosita ta'sir qiladi; I: S: OSI modelining birinchi satxi qanday nomlanadi +: Fizik satx -:Seanslar satxi -:Transport satxi -:Taqdimlash satxi I: S: OSI modelining ikkinchi satxi qanday nomlanadi +: Kanal satxi -:Amaliy satxi -:Fizik satx -:Seanslar satxi I: S: OSI modelining uchinchi satxi qanday nomlanadi +: Tarmoq satxi -:Amaliy satx -:Kanal satxi -:Taqdimlash satxi I: S: OSI modelining oltinchi satxi qanday nomlanadi +: Taqdimlash satxi -:Amaliy satx -:Seanslar satxi -:Kanal satxi I: S: OSI modelining ettinchi satxi qanday nomlanadi +: Amaliy satx -:Seanslar satxi -:Transport satxi -:Taqdimlash satxi I: S: Elektr signallarini qabul qilish va uzatish vazifalarini OSI modelining qaysi

satxi bajaradi +: Fizik satx -:Kanal satxi -:Tarmoq satxi -:Transport satxi I: S: Keltirilgan protokollarning qaysilari transport satxi protokollariga mansub +: TCP,UDP -:NFS, FTP -:IP, IPX -:Ethernet, FDDI I: S: OSI modelining fizik satxi qanday funksiyalarni bajaradi +: Elektr signallarini uzatish va qabul qilish -:Aloqa kanalini va ma'lumotlarni uzatish muxitiga murojat qilishni boshqarish -:Bog'lanish seansini yaratish, kuzatish, oxirigacha ta'minlash -:Klient dasturlari bilan o'zaro muloqotda bo'lish I: S: OSI modelining amaliy satxi qanday funksiyalarni bajaradi +: Klient dasturlari bilan o'zaro muloqotda bo'lish -:Aloqa kanalini va ma'lumotlarni uzatish muxitiga murojat qilishni boshqarish -:Bog'lanish seansini yaratish, kuzatish, oxirigacha ta'minlash -:Elektr signallariniuzatish va qabul qilish I: S: Yevklid algoritmi qanday natijani beradi? +: Sonning eng katta umumiy bo'luvchisini toppish -:Sonning turli bo'luvchilarini toppish -:Sonning eng kichik umumiy karralisini toppish -:Sonning eng katta umumiy bo'linuvchisini topish I: S: Qanday sonlar tub sonlar deb yuritiladi? +: Faqatgina 1 ga va o'ziga bo'linadigan sonlar tub sonlar deyiladi. -:O'zidan boshqa bo'luvchilari mavjud bo'lgan sonlar tub sonlar deyiladi. -:Agar sonning 1 dan boshqa bo'luvchilari bo'lsa. -:Faqatgina 1 ga o'ziga bo'linmaydigan sonlar tub sonlar deyiladi. I: S: OSI modelining birinchi satxi qanday nomlanadi +: Fizik satx -:Seanslar satxi -:Transport satxi -:Taqqimlash satxi I: S: OSI modelining ikkinchi satxi qanday nomlanadi +: Kanal satxi -:Amaliy satxi -:Fizik satx -:Seanslar satxi I: S: OSI modelining uchinchi satxi qanday nomlanadi +: Tarmoq satxi -:Amaliy satx -:Kanal satxi -:Taqqimlash satxi I: S: OSI modelining oltinchi satxi qanday nomlanadi +: Taqqimlash satxi -:Amaliy satx -:Seanslar satxi -:Kanal satxi I: S: OSI modelining ettinchi satxi qanday nomlanadi +: Amaliy satx -:Seanslar satxi -:Transport satxi -:Taqqimlash satxi I: S: Elektr signallarini qabul qilish va uzatish vazifalarini OSI modelining qaysi satxi bajaradi +: Fizik satx -:Kanal satxi -:Tarmoq satxi -:Transport satxi I: S: Keltirilgan protokollarning qaysilari transport satxi protokollariga mansub +: TCP,UDP -:NFS, FTP -:IP, IPX -:Ethernet, FDDI I: S: OSI modelining fizik satxi qanday funksiyalarni bajaradi +: Elektr signallarini uzatish va qabul qilish -:Aloqa kanalini va ma'lumotlarni uzatish muxitiga murojat qilishni boshqarish -:Bog'lanish seansini yaratish, kuzatish, oxirigacha ta'minlash -:Klient dasturlari bilan o'zaro muloqotda bo'lish I: S: OSI modeliningamaliy satxi qanday funksiyalarni bajaradi +: Klient dasturlari bilan o'zaro muloqotda bo'lish -:Aloqa kanalini va ma'lumotlarni uzatish muxitiga murojat qilishni boshqarish -:Bog'lanish seansini yaratish, kuzatish, oxirigacha ta'minlash -:Elektr signallariniuzatish va qabul qilish I: S: Yevklid algoritmi qanday natijani beradi? +: Sonning eng katta umumiy bo'luvchisini toppish -:Sonning turli bo'luvchilarini toppish -:Sonning eng kichik umumiy karralisini toppish -:Sonning eng katta umumiy bo'linuvchisini topish I: S: Qanday sonlar tub sonlar deb yuritiladi? +: Faqatgina 1 ga va o'ziga bo'linadigan sonlar tub sonlar deyiladi. -:O'zidan boshqa bo'luvchilari mavjud bo'lgan sonlar tub sonlar deyiladi. -:Agar sonning 1 dan boshqa bo'luvchilari bo'lsa. -:Faqatgina 1 ga o'ziga bo'linmaydigan sonlar tub sonlar deyiladi. I: S: Antivirus dasturlarini ko'rsating? +: Drweb, Nod32, Kaspersky -:arj, rar, pkzip, pkunzip -:winrar, winzip, winarj -:pak, lha I: S: Wi-Fi tarmoqlarida quyida keltirilgan qaysi shifrlash protokollaridan foydalaniladi +: wep, wpa, wpa2 -:web, wpa, wpa2 -:wpa, wpa2 -:wpa, wpa2, wap I: S: Axborot himoyalangan qanday sifatarga ega bo'lishi kerak? +: ishonchli, qimmatli va to'liq -:uzluksiz va uzlukli -:ishonchli, qimmatli va uzlukli -:ishonchli, qimmatli va uzluksiz I: S: Axborotning eng kichik o'lchov birligi nima? +: bit -:kilobayt -:bayt -:bitta simvol I: S: Virtual xususiy tarmoq – bu? +: VPN -:APN -:ATM -:Ad-hoc I: S: Xavfli viruslar bu - ... +: kompyuter ishlashida jiddiy nuqsonlarga sabab bo'luvchi viruslar -:tizimda mavjudligi turli taassurot (ovoz, video) bilan bog'liq viruslar, bo'sh xotirani kamaytirsada, dastur va ma'lumotlarga ziyon yetkazmaydi -:o'z-o'zidan tarqalish mexanizmi amalga oshiriluvchi viruslar -:dastur va ma'lumotlarni buzilishiga hamda kompyuter ishlashiga zarur axborotni o'chirilishiga bevosita olib

keluvchi, muolajalari oldindan ishlash algoritmlariga joylangan viruslar I: S: Mantiqiy bomba – bu ...  
 +: Ma`lum sharoitlarda zarar keltiruvchi harakatlarni bajaruvchi dastur yoki uning alohida modullari -:Viruslar va zarar keltiruvchi dasturlarni tarqatish kanallari -:Viruslar kodiga boshqarishni uzatish -:Qidirishning passiv mexanizmlarini amalga oshiruvchi, yahni dasturiy fayllarga tuzoq qo'yuvchi viruslar I: S: Rezident virus... +: tezkor xotirada saqlanadi -:to'liqligicha bajarilayotgan faylda joylashadi -:ixtiyoriy sektorlarda joylashgan bo'ladi -:alohida joyda joylashadi I: S: DIR viruslari nimani zararlaydi? +: FAT tarkibini zararlaydi -:com, exe kabi turli fayllarni zararlaydi -:yuklovchi dasturlarni zararlaydi -:Operatsion tizimdagi sonfig.sys faylni zararlaydi I: S:.... kompyuter tarmoqlari bo'yicha tarqalib, komlg'yuterlarning tarmoqdagi manzilini aniqlaydi va u yerda o'zining nusxasini qoldiradi +: «Chuvalchang» va replikatorli virus -:Kvazivirus va troyan virus -:Troyan dasturi -:Mantiqiy bomba I: S: Fire Wall ning vazifasi... +: tarmoqlar orasida aloqa o'rnatish jarayonida tashkilot va Internet tarmog'i orasida xavfsizlikni ta'minlaydi -:kompyuterlar tizimi xavfsizligini ta'minlaydi -:Ikkita kompyuter o'rtasida aloqa o'rnatish jarayonida Internet tarmog'i orasida xavfsizlikni ta'minlaydi -:uy tarmog'i orasida aloqa o'rnatish jarayonida tashkilot va Internet tarmog'i orasida xavfsizlikni ta'minlaydi I: S: Kompyuter virusi nima? +: maxsus yozilgan va zararli dastur -:exe fayl -:boshqariluvchi dastur -:Kengaytmaga ega bo'lgan fayl I: S: Kompyuterning viruslar bilan zararlanish yo'llarini ko'rsating +: disk, maxsus tashuvchi qurilma va kompyuter tarmoqlari orqali -: faqat maxsus tashuvchi qurilma orqali -: faqat kompyuter tarmoqlari orqali -:zararlanish yo'llari juda ko'p I: S: Troyan dasturlari bu... +: virus dasturlar -:antivirus dasturlar -:o'yin dasturlari -:yangilovchi dasturlar I: S: Kompyuter viruslari xarakterlariga nisbatan necha turga ajraladi? +: 5 -:4 -:2 -:3 I: S: Antiviruslarni, qo'llanish usuliga ko'ra... turlari mavjud +: detektorlar, faglar, vaktsinalar, privivkalar, revizorlar, monitorlar -:detektorlar, falglar, revizorlar, monitorlar, revizatsiyalar -:vaktsinalar, privivkalar, revizorlar, tekshiruvchilar -:privivkalar, revizorlar, monitorlar, programma, revizorlar, monitorlar I: S: Stenografiya mahnosi... +: sirli yozuv -:sirli xat -:maxfiy axborot -:maxfiy belgi I: S: ...sirli yozuvning umumiy nazariyasini yaratdiki, u fan sifatida stenografiyaning bazasi hisoblanadi +: K.Shennon -:Sezar -:U.Xill -:Fon Neyman I: S: Kriptologiya yo'nalishlari nechta? +: 2 -:3 -:4 -:5 I: S: Kriptografiyaning asosiy maqsadi... +: maxfiylik, yaxlitlilikni ta'minlash -:ishonchlilik, butunlilikni ta'minlash -:autentifikatsiya, identifikatsiya -:ishonchlilik, butunlilikni ta'minlash, autentifikatsiya, identifikatsiya I: S: DES algoritmi akslantirishlari raundlari soni qancha? +: 16; -:14; -:12; -:32; I: S: DES algoritmi shifrlash blokining chap va o'ng qism bloklarining o'lchami qancha? +: CHap qism blok 32 bit, o'ng qism blok 32 bit; -:CHap qism blok 32 bit, o'ng qism blok 48 bit; -:CHap qism blok 64 bit, o'ng qism blok 64 bit; -:CHap qism blok 16 bit, o'ng qism blok 16 bit; I: S: 19 gacha bo'lgan va 19 bilan o'zaro tub bo'lgan sonlar soni nechta? +: 18 ta; -:19 ta -:11 ta -:9 ta I: S: 10 gacha bo'lgan va 10 bilan o'zaro tub bo'lgan sonlar soni nechta? +: 3 ta -:7 ta -:8 ta; -:9 ta I: S: Qaysi formula qoldiqli bo'lish qonunini ifodalaydi +:  $a = bq + r, 0 \leq r < b$ , -: $a = p_1^{a_1} p_2^{a_2} p_3^{a_3} \dots p_k^{a_k}$  -: $M = r1^k2$ ; -: $M = v(k1+k2)$  I: S: Eyler funksiyasida  $p=11$  va  $q=13$  sonining qiymatini toping. +: 16 -:59 -:30 -:21 I: S: Eyler funksiyasi yordamida 1811 sonining qiymatini toping. +: 1810 -:2111 -:16 -:524 I: S: 97 tub sonmi? +: Tub -:murakkab -:Natural -:To'g'ri javob yo'q I: S: Quyidagi modulli ifodani qiymatini toping  $(148 + 14432) \bmod 256$ . +: 244 -:200 -:156 -:154 I: S: Quyidagi sonlarning eng katta umumiy bo'luvchilarini toping. 88 i 220 +: 44 -:21 -:42 -:20 I: S: Quyidagi ifodani qiymatini toping.  $-16 \bmod 11$  +: 6 -:5 -:7 -:11 I: S: 2 soniga 10 modul bo'yicha teskari sonni toping. +:  $\emptyset$  -:3 -:10 -:25 I: S: 2 soniga 10 modul bo'yicha teskari sonni toping. +:  $\emptyset$  -:3 -:10 -:25 I: S: DES da dastlabki kalit uzunligi necha bitga teng? +:56 bit -:128 bit -:64 bit -:32 bit I: S: DES da bloklar har birining uzunligi necha bitga teng? +:32 bit -:56 bit -:48 bit -:64 bit I: S: DES da

raundlar soni nechta? +:16 -:32 -:8 -:48 I: S: Shifrlash kaliti noma'lum bo'lganda shifrlangan ma'lumotni deshifrlash qiyinlik darajasini nima belgilaydi +:kriptobardoshlik -:Shifr matn uzunligi -:Shifrlash algoritmi -:Texnika va texnologiyalar I: S: Barcha simmetrik shifrlash algoritmlari qanday shifrlash usullariga bo'linadi +:blokli va oqimli -:DES va oqimli -:Feystel va Verman -:SP- tarmoq va IP I: S: DES shifrlash algoritmda shifrlanadigan malumotlar bloki necha bit? +:64 -:32 -:48 -:56 I: S: XOR amali qanday amal? +:2 modul bo'yicha qo'shish -:264 modul bo'yicha qo'shish -:232 modul bo'yicha qo'shish -:248 modul bo'yicha qo'shish I: S:  $4+31 \bmod 32$  ? +:3 -:4 -:31 -:32 I: S:  $21+20 \bmod 32$  ? +:9 -:12 -:16 -:41 I: S:  $12+22 \bmod 32$  ? +:2 -:12 -:22 -:32 I: S: AES algoritmi bloki uzunligi ... bitdan kam bo'lmasligi kerak. +:128 -:512 -:256 -:192 I: S: Xesh-:funktsiyani natijasi ... +:fiksirlangan uzunlikdagi xabar -:Kiruvchi xabar uzunligidagi xabar -:Kiruvchi xabar uzunligidan uzun xabar -:fiksirlanmagan uzunlikdagi xabar I: S:  $2+5 \bmod 32$  ? +:7 -:32 -:2 -:5 I: S: 97 tub sonmi? +:Tub -:murakkab -:Natural -:To'g'ri javob yo'q I: S: Ikkilik sanoq tizimida berilgan 10111 sonini o'nlik sanoq tizimiga o'tkazing. +:23 -:20 -:21 -:19 I: S: Quyidagi ifodani qiymatini toping.  $-17 \bmod 11$  +:5 -:6 -:7 -:11 I: S: Diskni shifrlash nima uchun amalga oshiriladi? +: Ma'lumotni saqlash vositalarida saqlangan ma'lumot konfidensialligini ta'minlash uchun amalga oshiriladi -:Xabarni yashirish uchun amalga oshiriladi -:Ma'lumotni saqlash vositalarida saqlangan ma'lumot butunligini ta'minlash uchun amalga oshiriladi -:Ma'lumotni saqlash vositalarida saqlangan ma'lumot foydalanuvchanligini ta'minlash uchun amalga oshiriladi I: S: Ma'lumotlarni yo'q qilish odatda necha hil usulidan foydalaniladi? +: 4 -:8 -:7 -:5 I: S: OSI modelida nechta tarmoq satxi bor +: 7 -:6 -:5 -:4 I: S: Diskni shifrlash nima uchun amalga oshiriladi? +: Ma'lumotni saqlash vositalarida saqlangan ma'lumot konfidensialligini ta'minlash uchun amalga oshiriladi -:Xabarni yashirish uchun amalga oshiriladi -:Ma'lumotni saqlash vositalarida saqlangan ma'lumot butunligini ta'minlash uchun amalga oshiriladi -:Ma'lumotni saqlash vositalarida saqlangan ma'lumot foydalanuvchanligini ta'minlash uchun amalga oshiriladi I: S: Ma'lumotlarni yo'q qilish odatda necha hil usulidan foydalaniladi? +: 4 -:8 -:7 -:5 I: S: OSI modelida nechta tarmoq satxi bor +: 7 -:6 -:5 -:4 I: S: "Axborot erkinligi prinsiplari va kafolatlari to'g'risida"gi qonun moddadan iborat +:16 -:18 -:11 -:14 I: S: Kompyuter etikasi instituti notijoriy tashkilot tomonidan texnologiyani axloqiy nuqta nazardan targ'ib qilish bo'yicha nechta etika qoidalari keltirilgan +:10 -:18 -:11 -:14 I: S: Kiberjinoyatchilik bu -. . . +: Kompyuter yoki boshqa qurilmalarga qarshi qilingan yoki kompyuter va boshqa qurilmalar orqali qilingan jinoiy faoliyat. -: Kompyuter o'yinlari -: Faqat banklardan pul o'g'irlanishi -: autentifikatsiya jarayonini buzish I: S: Fishing nima? +: Internetdagi firibgarlikning bir turi bo'lib, uning maqsadi foydalanuvchining maxfiy ma'lumotlaridan, login/parol, foydalanish imkoniyatiga ega bo'lishdir. -: Ma'lumotlar bazalarini xatoligi -: Mualliflik huquqini buzilishi -: Lug'at orqali xujum qilish. I: S: Bag nima? +: Dasturiy ta'minotni amalga oshirish bosqichiga tegishli bo'lgan muammo -: Mualliflik huquqini buzilishi -: Dasturlardagi ortiqcha reklamalar -: Autentifikatsiya jarayonini buzish I: S: Nuqson nima? +: Dasturni amalga oshirishdagi va loyixalashdagi zaifliklarning barchasi nuqsondir -: Dasturiy ta'minotni amalga oshirish bosqichiga tegishli bo'lgan muammo -: Dasturlardagi ortiqcha reklamalar -: Autentifikatsiya jarayonini buzish I: S: Quyidagilardan qaysi birida xavfsiz dasturlash tillari keltirilgan. +: C#, Scala, Java -: C, C#, java -: C++, Scala, Java -: Misra-C, Java, c++ I: S: Quyidagilardan qaysi biri dasturiy maxsulotlarga qo'yiladigan xavfsizlik talablari hisoblanidi. +: Vazifaviy, novazifaviy, qolgan talablar -: Qolgan talablar, anaviy taablar, etika talablari -: Vazifaviy, novazifaviy, etika talablari. -: Vazifaviy, etika talablari, foydalanuvchanlik talablari. I: S: Dasturiy ta'minotda kirish va chiqishga aloqador bo'lgan talablar qanday talablar sirasiga kiradi? +:Vazifaviy -: Novazifaviy -: Etika talablari -: Qolgan talablar I: S: Dasturda tizim amalga oshirishi kerak bo'lgan

vazifalar bu.. +:Vazifaviy -: Novazifaviy -: Etika talablari -: Qolgan talablar I: S: Risklarni boshqarishda risklarni aniqlash jarayoni bu.. +: Tashkilot xavfsizligiga ta'sir qiluvchi tashqi va ichki risklarning manbasi, sababi, oqibati va haklarni aniqlash. -: Risklarni baholash bosqichi tashkilotning risk darajasini baholaydi va risk ta'siri va ehtimolini o'lchashni ta'minlaydi. -: Risklarni davolash bu – aniqlangan risklar uchun mos nazoratni tanlash va amalga oshirish jarayoni. -: Risk monitoringi yangi risklarni paydo bo'lish imkoniyatini aniqlash. I: S: Tizim ishlamay turganda yoki foydalanuvchilar ma'lumot bilan ishlamay turganda zahiralash amalga oshirilsa .... deb ataladi.

+: "Sovuq saxiralash" -: "Issiq zaxiralash" -: "Iliq saxiralash" -: "To'liq zaxiralash" I: S: Agar axborotning o'g'irlanishi moddiy va ma'naviy boyliklarning yo'qotilishi bilan bog'liq bo'lsa bu nima deb yuritiladi? +: Jinoyat sifatida baholanadi -: Rag'bat hisoblanadi -: Buzgunchilik hisoblanadi -: Guruhlar kurashi hisoblanadi I: S: Asimmetrik kriptotizimlarda axborotni shifrlashda va rasshifrovka qilish uchun qanday kalit ishlatiladi? +: Ikki kalit -: Bitta kalit -: Elektron raqamli imzo -: Foydalanuvchi identifikatori I: S: Axborot xavfsizligida axborotning bahosi qanday aniqlanadi? +: Axborot xavfsizligi buzulgan taqdirda ko'rilishi mumkin bo'lgan zarar miqdori bilan -: Axborot xavfsizligi buzulgan taqdirda axborotni foydalanuvchi uchun muhurligi bilan -: Axborotni noqonuniy foydalanishlardan o'zgartirishlardan va yo'q qilishlardan himoyalanganligi bilan -: Axborotni saqlovchi, ishlovchi va uzatuvchi apparat va dasturiy vositalarning qiymati bilan} I: S: Axborot xavfsizligiga bo'ladigan tahdidlarning qaysi biri maqsadli (atayin) tahdidlar deb hisoblanadi? +: Strukturalarni ruxsatsiz modifikatsiyalash -: Tabiiy ofat va avariya -: Texnik vositalarning buzilishi va ishlamasligi -: Foydalanuvchilar va xizmat ko'rsatuvchi hodimlarning hatoliklari} I: S: Axborot xavfsizligiga bo'ladigan tahdidlarning qaysi biri tasodifiy tahdidlar deb hisoblanadi? +: Texnik vositalarning buzilishi va ishlamasligi -: Axborotdan ruxsatsiz foydalanish -: Zararkunanda dasturlar -: An'anaviy josuslik va diversiya haqidagi ma'lumotlar tahlili} I: S: Axborot xavfsizligini ta'minlovchi choralarni ko'rsating? +: 1-huquqiy, 2-tashkiliy-ma'muriy, 3-injener-texnik -: 1-axloqiy, 2-tashkiliy-ma'muriy, 3-fizikaviy-kimyoviy -: 1-dasturiy, 2-tashkiliy-ma'muriy, 3-huquqiy -: 1-aparat, 2-texnikaviy, 3-huquqiy} I: S: Axborot xavfsizligining huquqiy ta'minoti qaysi me'yorlarni o'z ichiga oladi +: Xalqaro va milliy huquqiy me'yorlarni -: Tashkiliy va xalqaro me'yorlarni -: Ananaviy va korporativ me'yorlarni -: Davlat va nodavlat tashkilotlarime'yorlarni} I: S: Axborotni uzatish va saqlash jarayonida o'z strukturasi va yoki mazmunini saqlash xususiyati nima deb ataladi? +: Ma'lumotlar butunligi -: Axborotning konfidentsialligi -: Foydalanuvchanligi -: Ixchamligi} I: S: Axborotning buzilishi yoki yo'qotilishi xavfiga olib keluvchi himoyalovchi ob'ektga qarshi qilingan xarakatlar qanday nomlanadi? +: Tahdid -: Zaiflik -: Hujum -: Butunlik} I: S: Biometrik autentifikatsiyalashning avfzalliklari-bu: +: Biometrik alomatlarining noyobligi -: Bir marta ishlatilishi -: Biometrik alomatlarini o'zgartirish imkoniyati -: Autentifikatsiyalash jarayonining soddaligi I: S: Foydalanish huquqlariga (mualliflikka) ega barcha foydalanuvchilar axborotdan foydalana olishliklari-bu: +: Foydalanuvchanligi -: Ma'lumotlar butunligi -: Axborotning konfidentsialligi -: Ixchamligi I: S: Global simsiz tarmoqning ta'sir doirasi qanday? +: Butun dunyo bo'yicha -: Binolar va korpuslar -: O'rtacha kattalikdagishahar -: Foydalanuvchi yaqinidagi tarmoq I: S: Foydalanuvchini identifikatsiyalashda qanday ma'lumotdan foydalaniladi? +: Identifikatori -: Telefon raqami -: Parol -: Avtorizatsiyasi I: S: Foydalanuvchining tarmoqdagi harakatlarini va resurslardan foydalanishga urinishini qayd etish-bu: +: Ma'murlash -: Autentifikatsiya -: Identifikatsiya -: Sertifikatsiyalash I: S: Kompyuter tizimini ruxsatsiz foydalanishdan himoyalashni, muhim kompyuter tizimlarni rezervlash, o'g'irlash va diversiyadan himoyalashni ta'minlash rezerv elektr manbai, xavfsizlikning maxsus dasturiy va apparat vositalarini ishlab chiqish va amalga +: Injener-texnik -: Molyaviy -: Tashkiliy-ma'muriy -: Huquqiy I: S: Ma'lum qilingan foydalanuvchi, jarayon yoki qurilmaning haqiqiy ekanligini



tekshirish muolajasi-bu: +:Autentifikatsiya -:Identifikatsiya -:Ma`murlash (accounting) -  
:Avtorizatsiya I: S: O`zini tarqatishda kompyuter tarmoqlari va elektron pochta protokollari va komandalaridan foydalanadi—bu: +:Tarmoq viruslari -:Pochta viruslari -:Fayl viruslari -:Protokol viruslari I: S: Qanday viruslar xavfli hisoblanadi? +:kompyuter ishlashida jiddiy nuqsonlarga olib keluvchi -:Jiddiy nuqsonlarga olib kelmaydigan ammo foydalanuvchini chalg`itadigan. -:Katta viruslar va odatda zararli dasturlar -:Passiv viruslar I: S: Rezident bo`lmagan viruslar qachon xotirani zararlaydi? +:Faqat faollashgan vaqtida -:Faqat o`chirilganda -:Kompyuter yoqilganda -  
:Tarmoq orqali ma`lumot almashishda I: S: Simli va simsiz tarmoqlar orasidagi asosiy farq nimadan iborat? +:Tarmoq chetki nuqtalari orasidagi mutlaqo nazoratlamaydigan xudud -:Tarmoq chetki nuqtalari orasidagi xududning kengligi asosida qurilmalarholati -:Himoya vositalarining chegaralanganligi -:Himoyani amalga oshirish imkoniyati yo`qligi va ma'lum protokollarning ishlatilishi I: S: Simmetrik shifrlashning noqulayligi – bu: +:Maxfiy kalitlar bilan ayirboshlash zaruriyatidir -:Kalitlar maxfiyligi -:Kalitlar uzunligi -:SHifrlashga ko`p vaqt sarflanishi va ko`p yuklanishi I: S: Simsiz tarmoqlarni kategoriyalarini to`g`ri ko`rsating? +:Simsiz shaxsiy tarmoq (PAN), simsiz lokal tarmoq (LAN), simsiz regional tarmoq (MAN) va Simsiz global tarmoq (WAN) -:Simsiz internet tarmoq (IAN )va Simsiz telefon tarmoq (WLAN), Simsiz shaxsiy tarmoq (PAN) va Simsiz global tarmoq (WIMAX) -:Simsiz internet tarmoq (IAN) va uy simsiz tarmog`i -:Simsiz chegaralanmagan tarmoq (LAN), simsiz kirish nuqtalari I: S: Sub`ektga ma`lum vakolat va resurslarni berish muolajasi-bu: +:Avtorizatsiya -:Haqiqiylikni tasdiqlash -:Autentifikatsiya -:Identifikatsiya I: S: Tarmoq operatsion tizimining to`g`ri konfiguratsiyasini madadlash masalasini odatda kim hal etadi? +:Tizim ma`muri -:Tizim foydalanuvchisi -:Korxona raxbari -:Operator I: S: Tarmoqlararo ekran texnologiyasi-bu: +:Ichki va tashqi tarmoq o`rtasida filtr va himoya vazifasini bajaradi -:Ichki va tashqi tarmoq o`rtasida axborotni o`zgartirish vazifasini bajaradi -:Qonuniy foydalanuvchilarni himoyalash -:Ishonchsiz tarmoqdan kirishni boshqarish} I: S: Xizmat qilishdan voz kechishga undaydigan taqsimlangan hujum turini ko`rsating? +:DDoS (Distributed Denial of Service) hujum -:Tarmoq hujumlari -:Dastur hujumlari asosidagi (Denial of Service) hujum -:Virus hujumlari} I: S: Uyishtirilmagan tahdid, ya`ni tizim yoki dasturdagi qurilmaning jismoniy xatoligi – bu... +:Tasodifiy tahdid -:Uyishtirilgan tahdid -:Faol tahdid -:Passiv tahdid I: S: Axborot xavfsizligi qanday asosiy xarakteristikalariga ega? +:Butunlik, konfidentsiallik, foydalana olishlik -:Butunlik, himoya, ishonchlilikni urganib chiqishlilik -:Konfidentsiallik, foydalana olishlik -:Himoyalanganlik, ishonchlilik, butunlik } I: S: Tizim ishlamay turganda yoki foydalanuvchilar ma'lumot bilan ishlamay turganda zahiralash amalga oshirilsa .... deb ataladi. +:"Sovuq saxiralash" -:"Issiq zaxiralash" -:"Iliq saxiralash" -:"To'liq zaxiralash" I: S: Agar foydalanuvchi tizimda ma'lumot bilan ishlash vaqtida ham zahiralash amalga oshirilishi .... deb ataladi? +:"Issiq zaxiralash" -:"Sovuq saxiralash" -:"Iliq saxiralash" -:"To'liq zaxiralash" I: S: Ma'lumotlarni zahira nusxasini saqlovchi va tikovchi dasturni belgilang +:HandyBakcup -:Recuva, R.saver -:Cryptool -:Eset32 I: S: O'chirilgan, formatlangan ma'lumotlarni tikovchi dasturni belgilang. +:Recuva, R.saver -:HandyBakcup -:Cryptool -:Eset32 I: S: Virtuallashtirishga qaratilgan dasturiy vositalarni belgilang. +:VMware, VirtualBox -  
:HandyBakcup -:Eset32 -:Cryptool I: S: Cloud Computing texnologiyasi nechta katta turga ajratiladi? +:3 turga -:2 turga -:4 turga -:5 turga I: S: O'rnatilgan tizimlar-bu... +:Bu ko'pincha real vaqt hisoblash cheklovlariga ega bo'lgan kattaroq mexanik yoki elektr tizimidagi maxsus funksiyaga ega, boshqaruvchidir -:Korxona ichki tarmog`iga ulangan korporativ tarmog`idan bo'ladigan hujumlardan himoyalash -:Korxona ichki tarmog`ini Internet global tarmog`idan ajratib qo'yish -:Bu ko'pincha global tizimda hisoblash cheklovlariga ega bo'lgan mexanik yoki elektr tizimidagi maxsus funksiyaga ega qurilmadir I: S: Axborotdan oqilona foydalanish kodeksi qaysi

tashkilot tomonidan ishlab chiqilgan? +:AQSH sog'liqni saqlash va insonlarga xizmat ko'rsatish vazirligi -:AQSH Mudofaa vazirligi -:O'zbekiston Axborot texnologiyalari va kommunikatsiyalarni rivojlantirish vazirligi -:Rossiya kiberjinoatlarga qarshu kurashish davlat qo'mitasi I: S: Axborotdan oqilona foydalanish kodeksi nechanchi yil ishlab chiqilgan? +:1973 yil -:1980 yil -:1991 yil -:2002 yil I: S: Kompyuter bilan bog'liq falsafiy soha bo'lib, foydalanuvchilarning xatti-harakatlari, kompyuterlar nimaga dasturlashtirilganligi va umuman insonlarga va jamiyatga qanday ta'sir ko'rsatishini o'rgatadigan soha nima deb ataladi? +:Kiberetika -:Kiberhuquq -:Kiberqoida -:Kiberxavfsizlik I: S: Kompyuter yoki boshqa qurilmalarga qarshi qilingan yoki kompyuter va boshqa qurilmalar orqali qilingan jinoyat-... +:Kiberjinoyat -:Kibersport -:Kiberterror -:Hakerlar uyushmasi I: S: Tarmoqlararo ekran paket filtrlari qaysi sathda ishlaydi? +:Tarmoq sathida -:Ilova sathida -:Kanal sathida -:Fizik sathida I: S: Tarmoqlararo ekran ekspert paketi filtrlari qaysi sathda ishlaydi? +:Transport sathida -:Ilova sathida -:Kanal sathida -:Fizik sathida I: S: Spam bilan kurashishning dasturiy uslubida nimalar ko'zda tutiladi? +:Elektron pochta qutisiga kelib tushadigan ma'lumotlar dasturlar asosida filtrlanib cheklanadi -:Elektron pochta qutisiga kelib tushadigan spamlar me'yoriy xujjatlar asosida cheklanadi va bloklanadi -:Elektron pochta qutisiga kelib tushadigan spamlar ommaviy ravishda cheklanadi -:Elektron pochta qutisiga kelib spamlar mintaqaviy hududlarda cheklanadi I: S: Ma'lumotlarni yo'qolish sabab bo'luvchi tabiiy tahdidlarni ko'rsating +:Zilzila, yong'in, suv toshqini va hak -:Quvvat o'chishi, dasturiy ta'minot to'satdan o'zgarishi yoki qurilmani to'satdan zararlanishi -:Tashkilotdagi muhim ma'lumotlarni modifikatsiyalanishi yoki o'g'irlanishi -:Qasddan yoki tasodifiy ma'lumotni o'chirib yuborilishi, ma'lumotlarni saqlash vositasini to'g'ri joylashtirilmagani I: S: Ma'lumotlarni tasodifiy sabablar tufayli yo'qolish sababini belgilang +:Quvvat o'chishi, dasturiy ta'minot to'satdan o'zgarishi yoki qurilmani to'satdan zararlanishi -:Tashkilotdagi muhim ma'lumotlarni modifikatsiyalanishi yoki o'g'irlanishi -:Ma'lumotlarni saqlash vositasini to'g'ri joylashtirilmagani yoki ma'lumotlar bazasini xatolik bilan boshqarilganligi. -:Zilzila, yong'in, suv toshqini va hak I: S: Ma'lumotlarni inson xatosi tufayli yo'qolish sababini belgilang. +:Ma'lumotlarni saqlash vositasini to'g'ri joylashtirilmagani yoki ma'lumotlar bazasini xatolik bilan boshqarilganligi. -:Tashkilotdagi muhim ma'lumotlarni modifikatsiyalanishi yoki o'g'irlanishi -:Quvvat o'chishi, dasturiy ta'minot to'satdan o'zgarishi yoki qurilmani to'satdan zararlanishi -:Zilzila, yong'in, suv toshqini va hak I: S: Ma'lumotlarni g'arazli hatti harakatlar yo'qolish sababini ko'rsating. +:Tashkilotdagi muhim ma'lumotlarni modifikatsiyalanishi yoki o'g'irlanishi -:Quvvat o'chishi, dasturiy ta'minot to'satdan o'zgarishi yoki qurilmani to'satdan zararlanishi -:Ma'lumotlarni saqlash vositasini to'g'ri joylashtirilmagani yoki ma'lumotlar bazasini xatolik bilan boshqarilganligi. -:Zilzila, yong'in, suv toshqini va hak I: S: Kompyuterda hodisalar haqidagi ma'lumot qayerda saqlanadi? +:Hodisalar jurnaliga -:Operativ xotiraga -:Kesh xotiraga -:Vaqtinchalik faylga I: S: Internet orqali masofada joylashgan kompyuterga yoki tarmoq resurslariga DoS hujumlari uyushtirilishi natijasida.. +:Foydalanuvchilar kerakli axborot resurlariga murojaat qilish imkoniyatidan mahrum qilinadilar -:Foydalanuvchilarning maxfiy axborotlari kuzatilib, masofadan buzg'unchilarga etkaziladi -:Axborot tizimidagi ma'lumotlar bazalari o'g'irlanib ko'lga kiritilgach, ular yo'q qilinadilar -:Foydalanuvchilar axborotlariga ruxsatsiz o'zgartirishlar kiritilib, ularning yaxlitligi buziladi I: S: Dasturlarni buzish va undagi mualliflik huquqini buzush uchun yo'naltirilgan buzg'unchi bu - ... +:Krakker -:Hakker -:Virus bot -:Ishonchsiz dasturchi I: S: Antivirus dasturiy vositalari viruslarni tahlil qilishiga ko'ra necha turga bo'linadi? +:2 turga: fayl Signaturaga va evristikaga asoslangan -:2 turga: faol va passiv -:2 turga: pulli va pulsiz -:2 turga: litsenziyali va ochiq I: S: "Parol", "PIN" kodlarni xavfsizlik tomonidan kamchiligi nimadan iborat? +:Foydalanish davrida maxfiylik kamayib boradi -:Parolni

esda saqlash kerak bo'ladi -:Parolni almashtirish jarayoni murakkabligi -:Parol uzunligi soni cheklangan I: S: Yaxlitlikni buzilishi bu - ... +:Soxtalashtirish va o'zgartirish -:Ishonchsizlik va soxtalashtirish -:Soxtalashtirish -:Butunmaslik va yaxlitlanmaganlik I: S: Tarmoqda joylashgan fayllar va boshqa resurslardan foydalanishni taqdim etuvchi tarmoqdagi kompyuter nima? +:Server -:Bulutli tizim -:Superkompyuter -:Tarmoq I: S: Tahdid nima? +:Tizim yoki tashkilotga zarar yetkazishi mumkin bo'lgan istalmagan hodisa. -:Tashkilot uchun qadrli bo'lgan ixtiyoriy narsa -:Bu riskni o'zgartiradigan harakatlar bo'lib -:Bu noaniqlikning maqsadlarga ta'siri I: S: Risk nima? +:Potensial kuchlanish yoki zarar -:Potensial foyda yoki zarar -:Tasodifiy taxdid -:Katta yo'qotish I: S: Qaysi tarmoq kabelining axborot uzatish tezligi yuqori hisoblanadi? +:Optik tolali -:O'rama juft -:Koaksial -:Telefon kabeli I: S: Nima uchun autentifikatsiyalashda parol ko'p qo'llaniladi? +:Sarflar xarajati kam, almashtirish oson -:Parolni eslab qolish oson -:Parolni o'g'rishlash qiyin -:Serverda parollarni saqlash oson I: S: Elektron xujjatlarni yo'q qilish usullari qaysilar? +:Shredirlash, magnitsizlantirish, yanchish -:Yoqish, ko'mish, yanchish -:Shredirlash, yoqish, ko'mish -:Kimyoviy usul, yoqish. I: S: Elektron raqamli imzo algoritmi qanday bosqichlardan iborat bo'ladi? +:Imzo qo'yish va imzoni tekshirishdan -:Faqat imzo qo'yishdan -:Faqat imzoni tekshirishdan -:Kalitlarni taqsimlashdan I: S: Elektron pochtaga kirishda foydalanuvchi qanday autentifikatsiyalashdan o'tadi? +:Parol asosida -:Smart karta asosida -:Biometrik asosida -:Ikki tomonlama I: S: Qaysi javobda xavfsizlik siyosatini amalga oshirishdagi Jazolar bosqichiga to'g'ri ta'rif berilgan. -: tashkilot o'z siyosatini ishlab chiqishdan oldin o'z aktivlari uchun risklarni baholashi shart -: tashkilot o'z xavfsizlik siyosatini ishlab chiqishdan oldin umumiy qoidalarini o'rnatilish shart -: yangi xavfsizlik siyosatini ishlab chiqish yoki mavjudiga qo'shimcha kiritish jarayonida boshqaruvchi bo'lishi shart +: ma'lum tashkilotlarda tashkilotlarda qat'iy siyosatlarni mavjud. Agar xodimlar ushbu siyosatlarga amal qilmasa, ularga qarshi bir qancha choralar qo'llaniladi. I: S: Qaysi javobda xavfsizlik siyosatini amalga oshirishdagi Xodimlarni o'rgatish bosqichiga to'g'ri ta'rif berilgan. -: tashkilot o'z siyosatini ishlab chiqishdan oldin o'z aktivlari uchun risklarni baholashi shart -: tashkilot o'z xavfsizlik siyosatini ishlab chiqishdan oldin umumiy qoidalarini o'rnatilish shart -: yangi xavfsizlik siyosatini ishlab chiqish yoki mavjudiga qo'shimcha kiritish jarayonida boshqaruvchi bo'lishi shart +: xodimlarga tashkilot xavfsizlik siyosati davomli ravishda o'rgatilishi shart I: S: Galstuk babochka usuli nima? +: Risklarni baholash usuli -: Risklarni qabul qilish usuli -: shifrlash algoritmi -: Risklarni hosil qilish usuli. I: S: Lotin alifbosida DADA so'zini 3 kalit bilan shifrlagandan so'ng qaysi so'z hosil bo'ladi. A=0, B=1....Z=25. +:GDGD -: NANA -: GPGP -: FDFD I: S: Lotin alifbosida NON so'zini 3 kalit bilan shifrlagandan so'ng qaysi so'z hosil bo'ladi. A=0, B=1....Z=25. -:GDGD -: NANA +: QRQ -: FDFD I: S: Fizik to'siqlarni o'rnatish, Xavfsizlik qo'riqchilarini ishga olish, Fizik qulflar qo'yishni amalga oshirish qanday nazorat turiga kiradi? +:Fizik nazorat -: Texnik nazorat -: Ma'muriy nazorat -: Tashkiliy nazorat I: S: Ruxsatlarni nazoratlash, "Qopqon", Yong'inga qarshi tizimlar, Yoritish tizimlari, Ogohlantirish tizimlari, Quvvat manbalari, Video kuzatuv tizimlari, Qurollarni aniqlash, Muhitni nazoratlash amalga oshirish qanday nazorat turiga kiradi? -: Fizik nazorat +:Texnik nazorat -: Ma'muriy nazorat -: Tashkiliy nazorat I: S: Qoida va muolajalarni yaratish, Joylashuv arxitekturasini loyihalash, Xavfsizlik belgilari va ogohlantirish signallari, Ishchi joy xavfsizligini ta'minlash, Shaxs xavfsizligini ta'minlash amalga oshirish qanday nazorat turiga kiradi? -: Fizik nazorat -: Texnik nazorat +: Ma'muriy nazorat -: Tashkiliy nazorat I: S: Ikkilik sanoq tizimida qanday raqamlardan foydalanamiz? +: Faqat 0 va 1 -: Faqat 1 -: Faqat 0 -: Barcha raqamlardan I: S: AES shifrlash algoritmi necha rounddan iborat +: 10, 12, 14 -: 10,14,16 -: 12,14,16 -: 16 I: S: Hodisalar daraxti usuli nima? +: Risklarni baholash usuli -: Risklarni qabul qilish usuli -: shifrlash algoritmi -: Risklarni hosil qilish usuli I: S: Yuliy Sezar ma'lumotlarni shifrlashda

alfavit xarflarni nechtaga surib shifrlagan? +:3 taga -:4 taga -:2 taga -:5 taga I: S: WiMAX qanday simsiz tarmoq turiga kiradi. +: Regional -: Lokal -: Global -: Shaxsiy I: S: Wi-Fi necha Gs chastotali to'liqida ishlaydi? +: 2.4-5 Gs -: 2.4-2.485 Gs -: 1.5-11 Gs -: 2.3-13.6 Gs I: S: Quyidagi parollarning qaysi biri "bardoshli parol"ga kiradi? +: Onx458&hdsh) +: 12456578 +: salomDunyo +: Mashina777 I: S: Parollash siyosatiga ko'ra parol tanlash shartlari qanday? +: Kamida 8 belgi: katta va kichik xavflar, sonlar , kamida bitta maxsus simvol qo'llanishi kerak. -: Kamida 8 belgi: katta va kichik xavflar, sonlar qo'llanishi kerak. -: Kamida 6 belgi: katta xavflar, sonlar , kamida bitta maxsus simvol qo'llanishi kerak. -: Kamida 6 belgi: katta va kichik xavflar, kamida bitta maxsus simvol qo'llanishi kerak. 1. Avtorizatsiya tushunchasi odatda qaysi tushuncha bilan sinonim sifatida ham foydalanadi? Foydalanishni boshqarish 2. To'rtta bir-biri bilan bog'langan bog'lamlar strukturasi (kvadrat shaklida) qaysi topologiya turiga mansub? Xalqa 3. Ko'z pardasi, yuz tuzilishi, ovoz tembri, -bular autentifikatsiyaning qaysi faktoriga mos belgilar? Biometrik autentifikatsiya 5. Ruxsatlarni nazoratlash, "Qopqon", Yong'inga qarshi tizimlar, Yoritish tizimlari, Ogohlantirish tizimlari , Quvvat manbalari, Video kuzatuv tizimlari, Qurollarni aniqlash, Muhitni nazoratlash amalga oshirish qanday nazorat turiga kiradi? Texnik nazorat 6. Ma'lumotlarni yo'qolish sabab bo'luvchi tabiiy tahdidlarni ko'rsating Zilzila, yong'in, suv toshqini va hak. 7. Token, Smartkartalarda xavfsizlik tomonidan kamchiligi nimada? Qurilmalarni ishlab chiqarish murakkab jarayon 8. Foydalanishni boshqarish –bu... Sub'ektni Sub'ektga ishlash qobiliyatini aniqlashdir. 9. Ro'yxatdan o'tish-bu... foydalanuvchilarni ro'yxatga olish va ularga dasturlar va ma'lumotlarni ishlatishga huquq berish jarayoni 10. MAC usuli bilan foydalanishni boshqarishda xavfsizlik markazlashgan holatda kim tomonidan amalga oshiriladi? Xavfsizlik siyosati ma'muri 11. MD5, SHA1, SHA256, O'z DSt 1106:2009- qanday algoritmlar deb ataladi? Shifrlash 12. Shifr nima? Shifrlash va deshifrlashda foydalaniladigan matematik funktsiyadan iborat bo'lgan krptografik algoritm 13. Ethernet kontsentratori qanday vazifani bajaradi? kompyuterdan kelayotgan axborotni qolgan barcha kompyuterga yo'naltirib beradi 14. Tekstni boshqa tekst ichida ma'nosini yashirib keltirish nima deb ataladi? steganografiya 15. Qaysi juftlik RSA algoritmining ochiq va yopiq kalitlarini ifodalaydi? {d, n} – yopiq, {e, n} – ochiq; 16. Zimmermann telegrami, Enigma shifri, SIGABA kriptografiyaning qaysi davriga to'g'ri keladi? 1-2 jahon urushu davri 17. Ochiq kalitli kriptotizimlarning mohiyati nimadan iborat? Ochiq kalitli kriptotizimlarda bir-biri bilan matematik bog'langan 2 ta – ochiq va yopiq kalitlardan foydalaniladi 18. ....–hisoblashga asoslangan bilim sohasi bo'lib, buzg'unchilar mavjud bo'lgan sharoitda amallarni kafolatlash uchun o'zida texnologiya, inson, axborot va jarayonni mujassamlashtirgan. Kiberxavfsizlik 19. Kriptografiyaning asosiy maqsadi nima? maxfiylik, yaxlitlilikni ta'minlash 20. Foydalanishni boshqarishning qaysi usuli – Ob'ektlar va Sub'ektlarning atributlari, ular bilan mumkin bo'lgan amallar va so'rovlarga mos keladigan muhit uchun qoidalarni tahlil qilish asosida foydalanishlarni boshqaradi. ABAC 1. Avtorizatsiya tushunchasi odatda qaysi tushuncha bilan sinonim sifatida ham foydalanadi? Foydalanishni boshqarish 2. To'rtta bir-biri bilan bog'langan bog'lamlar strukturasi (kvadrat shaklida) qaysi topologiya turiga mansub? Xalqa 3. Ko'z pardasi, yuz tuzilishi, ovoz tembri, -bular autentifikatsiyaning qaysi faktoriga mos belgilar? Biometrik autentifikatsiya 5. Ruxsatlarni nazoratlash, "Qopqon", Yong'inga qarshi tizimlar, Yoritish tizimlari, Ogohlantirish tizimlari , Quvvat manbalari, Video kuzatuv tizimlari, Qurollarni aniqlash, Muhitni nazoratlash amalga oshirish qanday nazorat turiga kiradi? Texnik nazorat 6. Ma'lumotlarni yo'qolish sabab bo'luvchi tabiiy tahdidlarni ko'rsating Zilzila, yong'in, suv toshqini va hak. 9. Ro'yxatdan o'tish-bu... foydalanuvchilarni ro'yxatga olish va ularga dasturlar va ma'lumotlarni ishlatishga huquq berish jarayoni 10. MAC usuli bilan foydalanishni boshqarishda xavfsizlik markazlashgan holatda kim

tomonidan amalga oshiriladi? Xavfsizlik siyosati ma'muri 12. Shifr nima? Shifrlash va deshifrlashda foydalaniladigan matematik funktsiyadan iborat bo'lgan krptografik algoritm 13. Ethernet kontsentratori qanday vazifani bajaradi? kompyuterdan kelayotgan axborotni qolgan barcha kompyuterga yo'naltirib beradi 14. Tekstni boshqa tekst ichida ma'nosini yashirib keltirish nima deb ataladi? steganografiya 15. Qaysi juftlik RSA algoritmining ochiq va yopiq kalitlarini ifodalaydi?  $\{d, n\}$  – yopiq,  $\{e, n\}$  – ochiq; 16. Zimmermann telegrami, Enigma shifri, SIGABA kriptografiyaning qaysi davriga to'g'ri keladi? 1-2 jahon urushu davri 17. Ochiq kalitli kriptotizimlarning mohiyati nimadan iborat? Ochiq kalitli kriptotizimlarda bir-biri bilan matematik bog'langan 2 ta – ochiq va yopiq kalitlardan foydalaniladi 18. ....–hisoblashga asoslangan bilim sohasi bo'lib, buzg'unchilar mavjud bo'lgan sharoitda amallarni kafolatlash uchun o'zida texnologiya, inson, axborot va jarayonni mujassamlashtirgan. Kiberxavfsizlik 19. Kriptografiyaning asosiy maqsadi nima? maxfiylik, yaxlitlikni ta'minlash 1. Ma'lumotlarni zahira nusxasini saqlovchi va tikovchi dasturni belgilang. HandyBackup 2. Makroviruslar nimalarni zararlaydi? Ma'lum dasturlash tilida yozilgan va turli ofis ilovalari – MS Word hujjati, MS Excel elektron jadvali, Corel Draw tasviri, fayllarida joylashgan "makroslar" yoki "skriptlar"ni zararlaydi. 3. Ehtiyotkorlik siyosati (Prudent Policy) – bu .... Barcha xizmatlar blokirovka qilingandan so'ng bog'lanadi 4. Qaysi siyosatga ko'ra faqat ma'lum xavfli xizmatlar/hujumlar yoki harakatlar bloklanadi? Ruxsat berishga asoslangan siyosat 5. Nuqson atamasiga berilgan ma'noni ko'rsating. Dasturni amalga oshirishdagi va loyixalashdagi zaifliklarning barchasi 6. Hamma narsa ta'qiqlanadi. Bu qaysi xavfsizlik siyosatiga hos? Paranoid siyosati (Paranoid Policy) 7. "Axborot olish va kafolatlari va erkinligi to'g'risda"gi Qonuni qachon kuchga kirgan? 1997 yil 24 aprel 8. Adware-zararli dastur vazifasi nimadan iborat? marketing maqsadida yoki reklamani namoyish qilish uchun foydalanuvchini ko'rish rejimini kuzutib boruvchi dasturiy ta'minot. 9. Axborot xavfsizligiga bo'ladigan tahdidlarning qaysi biri maqsadli (atayin) tahdidlar deb hisoblanadi? Strukturalarni ruxsatsiz modifikatsiyalash 10. Axborot xavfsizligi boshqaruv tizimida "Aktiv" so'zi nimani anglatadi? Axborot xavfsizligida tashkilot uchun qimmatbaho bo'lgan va himoyalaniishi lozim bo'lgan narsalar 11. Fishing (ing. Fishing – baliq ovlash) bu... Internetdagi firibgarlikning bir turi bo'lib, uning maqsadi foydalanuvchining maxfiy ma'lumotlaridan, login/parol, foydalanish imkoniyatiga ega bo'lishdir. 12. Ma'lumotlarni zaxira nusxalash bu – ... Muhim bo'lgan axborot nusxalash yoki saqlash jarayoni. 13. .... riskni tutuvchi mos nazorat usuli amalga oshirilganligini kafolatlaydi. Risk monitoring 14. O'chirilgan yoki formatlangan ma'lumotlarni tikovchi dasturni belgilang. Recuva, R.saver 15. "Avtorizatsiya" atamasi qaysi tushuncha bilan sinonim sifatida ham foydalanadi? Foydalanishni boshqarish 16. Kiberetika tushunchasi: Kompyuter va kompyuter tarmoqlarida odamlarning etikasi 17. Rootkits-qanday zararli dastur? ushbu zararli dasturiy vosita operatsion tizim tomonidan aniqlanmasligi uchun ma'lum harakatlarini yashiradi. 18. "Fishing" tushunchasi: Tashkilot va odamlarning maxsus va shaxsiy ma'lumotlarini olishga qaratilgan internet-hujumi 19. Enterprise Information Security Policies, EISP-bu... Tashkilot axborot xavfsizligi siyosati 20. Asosan tarmoq, tizim va tashkilot haqidagi axborot olish maqsadida amalga oshiriladigan tarmoq hujumi qaysi? Razvedka hujumlari 1. Hamma narsa ta'qiqlanadi. Bu qaysi xavfsizlik siyosatiga hos? Paranoid siyosati (Paranoid Policy) 2. Spam bilan kurashishning dasturiy uslubida nimalar ko'zda tutiladi? Elektron pochta qutisiga kelib tushadigan ma'lumotlar dasturlar asosida filtrlanib cheklanadi. 3. Axborot xavfsizligida axborotning bahosi qanday aniqlanadi? Axborot xavfsizligi buzulgan taqdirda ko'rilishi mumkin bo'lgan zarar miqdori bilan 4. Antiviruslarni, qo'llanish usuliga ko'ra... turlari mavjud? detektorlar, faglar, vaktsinalar, privivkalar, revizorlar, monitorlar 5. "Axborotlashtirish to'g'risida"gi Qonunning maqsadi nimadan iborat? Axborotlashtirish, axborot resurslari va axborot tizimlaridan foydalanish

sohasidagi munosabatlarni tartibga solish. 6. Ma'lumotlarni bloklarga bo'lib, bir qancha (kamida ikkita) qattiq diskda rezerv nusxasini yozish qaysi texnologiya? RAID 0 7. "Avtorizatsiya" atamasi qaysi tushuncha bilan sinonim sifatida ham foydalanadi? Foydalanishni boshqarish 8. "Elektron hujjat" tushunchasi haqida to'g'ri ta'rif berilgan qatorni ko'rsating. Elektron shaklda qayd etilgan, elektron raqamli imzo bilan tasdiqlangan va elektron hujjatning uni identifikatsiya qilish imkoniyatini beradigan boshqa rekvizitlariga ega bo'lgan axborot elektron hujjatdir 9. Doktorlar, detektorlarga xos bo'lgan ishni bajargan holda zararlangan fayldan viruslarni chiqarib tashlaydigan va faylni oldingi holatiga qaytaradigan dasturiy ta'minot nomini belgilang. Faglar 10. Dastlabki virus nechanchi yilda yaratilgan? 1986 11. Rezident virus... tezkor xotirada saqlanadi 12. Zaiflik – bu... tizimda mavjud bo'lgan xavfsizlik muammoasi bo'lib, ular asosan tizimning yaxshi shakllantirilmaganligi yoki sozlanmaganligi sababli kelib chiqadi. 13. Asosan tarmoq, tizim va tashkilot haqidagi axborot olish maqsadda amalga oshiriladigan tarmoq hujumi qaysi? Razvedka hujumlari 14. Virusning signaturasi (virusga taalluqli baytlar ketmaketligi) bo'yicha operativ xotira va fayllarni ko'rish natijasida ma'lum viruslarni topuvchi va xabar beruvchi dasturiy ta'minot nomi nima deb ataladi? Detektorlar 15. Makroviruslar nimalarni zararlaydi? Ma'lum dasturlash tilida yozilgan va turli ofis ilovalari – MS Word hujjati, MS Excel elektron jadvali, Corel Draw tasviri, fayllarida joylashgan "makrosalar" yoki "skriptlar"ni zararlaydi. 16. Texnik himoya vositalari – bu ... Texnik qurilmalar, komplekslar yoki tizimlar yordamida ob'ektni himoyalashdir 17. Kompyuter yoki boshqa qurilmalarga qarshi qilingan yoki kompyuter va boshqa qurilmalar orqali qilingan jinoyat... Kiberjinoyat deb ataladi 19. Issue-Specific Security Policies, ISSP-bu... Muammofa qaratilgan xavfsizlik siyosati 20. Axborot xavfsizligin ta'minlashda birinchi darajadagi me'yoriy hujjat nomini belgilang. qonunlar 1. Foydalanishni boshqarishning qaysi usuli – Ob'ektlar va Sub'ektlarning atributlari, ular bilan mumkin bo'lgan amallar va so'rovlarga mos keladigan muhit uchun qoidalarni tahlil qilish asosida foydalanishlarni boshqaradi. ABAC 2. MAC usuli bilan foydalanishni boshqarishda xavfsizlik markazlashgan holatda kim tomonidan amalga oshiriladi? Xavfsizlik siyosati ma'muri 3. Kriptografiyaning asosiy maqsadi nima? maxfiylik, yaxlitlikni ta'minlash 4. Uning egasi haqiqiyligini aniqlash jarayonida tekshiruv axboroti sifatida ishlatiladigan belgilar ketma-ketligi (maxfiy so'z) – nima? parol 5. Global simsiz tarmoqda qaysi standartlar ishlaydi? CDPD, 4G 6. Autentifikatsiya faktorlari nechta? 3 ta 8. Kriptografiyada matn –bu.. alifbo elementlarining tartiblangan to'plami 9. Stenografiya ma'nosi qanday? sirli yozuv 11. Axborot xavfsizligiga bo'ladigan tahdidlarning qaysi biri tasodifiy tahdidlar deb hisoblanadi? Texnik vositalarning buzilishi va ishlamasligi 12. Ochiq kalitli kriptotizimlarning mohiyati nimadan iborat? Ochiq kalitli kriptotizimlarda bir-biri bilan matematik bog'langan 2 ta – ochiq va yopiq kalitlardan foydalaniladi 13. Ma'lumotlar butunligi qanday algritmlar orqali amalga oshiriladi? Xesh funksiyalar 14. WiMAX qanday simsiz tarmoq turiga kiradi? Regional 15. Simmetrik shifrlashning noqulayligi – bu: Maxfiy kalitlar bilan ayirboshlash zaruriyatidir 16. Ma'lumotlarni yo'qolish sabab bo'luvchi tabiiy tahdidlarni ko'rsating Zilzila, yong'in, suv toshqini va hak. 17. Ma'lumotlarni tasodifiy sabablar tufayli yo'qolish sababini belgilang Quvvat o'chishi, dasturiy ta'minot to'satdan o'zgarishi yoki qurilmani to'satdan zararlanishi 18. Ko'z pardasi, yuz tuzilishi, ovoz tembri, -bular autentifikatsiyaning qaysi faktoriga mos belgilar? Biometrik autentifikatsiya 1. Yuliy Sezar ma'lumotlarni shifrlashda alfavit xarflarni nechtaga surib shifrlagan? 3 taga 2. Kriptotizimga qo'yiladigan umumiy talablardan biri nima? shifr matn uzunligi ochiq matn uzunligiga teng bo'lishi kerak 3. Autentifikatsiya faktorlari nechta? 3 ta 4. Axborot xavfsizligining asosiy maqsadlaridan biri-bu... Axborotlarni o'g'irlanishini, yo'qolishini, soxtalashtirilishini oldini olish 5. Ma'lumotlarni inson xatosi tufayli yo'qolish sababini belgilang. Ma'lumotlarni saqlash vositasini to'g'ri

joylashtirilmagani yoki ma'lumotlar bazasini xatolik bilan boshqarilganligi. 6. Qaysi tarmoq kabelining axborot uzatish tezligi yuqori hisoblanadi? Optik tolali 7. Ma'lumotlar butunligi qanday alqitmlar orqali amalga oshiriladi? Xesh funksiyalar 8. Zimmermann telegrami, Enigma shifri, SIGABA kriptografiyaning qaysi davriga to'g'ri keladi? 1-2 jahon urushu davri 9. Foydalanishni boshqarishning qaysi usuli – Ob'ektlar va Sub'ektlarning atributlari, ular bilan mumkin bo'lgan amallar va so'rovlarga mos keladigan muhit uchun qoidalarni tahlil qilish asosida foydalanishlarni boshqaradi. ABAC 10. Ochiq kalitli kriptotizimlarning mohiyati nimadan iborat? Ochiq kalitli kriptotizimlarda bir-biri bilan matematik bog'langan 2 ta – ochiq va yopiq kalitlardan foydalaniladi 11. Sub'ektga ma'lum vakolat va resurslarni berish muolajasi-bu: Avtorizatsiya 12. Kriptografiyaning asosiy maqsadi nima? maxfiylik, yaxlitlikni ta'minlash 13. Identifikatsiya bu- ... Foydalanuvchini uning identifikatori (nomi) bo'yicha aniqlash jarayoni 14. Fire Wall ning vazifasi... Tarmoqlar orasida aloqa o'rnatish jarayonida tashkilot va Internet tarmog'i orasida xavfsizlikni ta'minlaydi 15. Kiberjinoatchilik bu – . . . Kompyuter yoki boshqa qurilmalarga qarshi qilingan yoki kompyuter va boshqa qurilmalar orqali qilingan jinoiy faoliyat. 16. Berilgan ta'riflardan qaysi biri asimmetrik tizimlarga xos? Asimmetrik kriptotizimlarda  $k_1 \neq k_2$  bo'lib,  $k_1$  ochiq kalit,  $k_2$  yopiq kalit deb yuritiladi,  $k_1$  bilan axborot shifrlanadi,  $k_2$  bilan esa deshifrlanadi 17. Biometrik autentifikatsiyalashning avfzalliklari-bu: Biometrik parametrlarning noyoblighi 18. "Parol", "PIN" kodlarni xavfsizlik tomonidan kamchilighi nimadan iborat? Foydalanish davrida maxfiylik kamayib boradi 19. Kriptografiyada kalitning vazifasi nima? 1. Spyware-qanday zararli dastur? Foydalanuvchi ma'lumotlarini qo'lga kirituvchi va uni hujumchiga yuboruvchi dasturiy kod. 2. Axborot xavfsizligin ta'minlashda birinchi darajadagi me'yoriy hujjat nomini belgilang. Qonunlar 3. Adware-zararli dastur vazifasi nimadan iborat? marketing maqsadida yoki reklamani namoyish qilish uchun foydalanuvchini ko'rish rejimini kuzutib boruvchi dasturiy ta'minot. 4. Ma'lumotlarni zahira nusxasini saqlovchi va tikovchi dasturni belgilang. HandyBackup 5. Qaysi texnologiyada ma'lumotlarni bir necha disklarda bayt satxida ajratilgan xolda yoziladi va nazorat bitlari ham ular ichida taqsimlanadi? RAID 5 6. Axborot xavfsizligi boshqaruv tizimida "Aktiv" so'zi nimani anglatadi? Axborot xavfsizligida tashkilot uchun qimmatbaho bo'lgan va himoyalaniishi lozim bo'lgan narsalar 7. Dasturlarni buzish va undagi mualliflik huquqini buzush uchun yo'naltirilgan buzg'unchi bu - ... . Krakker 8. Qaysi siyosatga ko'ra hamma narsa ta'qiqlanadi? Paranoid siyosat 9. .... riskni tutuvchi mos nazorat usuli amalga oshirilganligini kafolatlaydi. Risk monitoring 10. Ehtiyotkorlik siyosati (Prudent Policy) – bu .... Barcha hizmatlar blokirovka qilingandan so'ng bog'lanadi 11. Xizmat qilishdan voz kechishga undaydigan taqsimlangan hujum turini ko'rsating? DDoS (Distributed Denial of Service) hujum 12. Kiberetika tushunchasi: Kompyuter va kompyuter tarmoqlarida odamlarning etikasi 13. "Elektron hujjat" tushunchasi haqida to'g'ri ta'rif berilgan qatorni ko'rsating. Elektron shaklda qayd etilgan, elektron raqamli imzo bilan tasdiqlangan va elektron hujjatning uni identifikatsiya qilish imkoniyatini beradigan boshqa rekvizitlariga ega bo'lgan axborot elektron hujjatdir 14. "Avtorizatsiya" atamasi qaysi tushuncha bilan sinonim sifatida ham foydalanadi? Foydalanishni boshqarish 15. Polimorf viruslar tushunchasi to'g'ri ko'rsating. Viruslar turli ko'rinishdagi shifrlangan viruslar bo'lib, o'zining ikkilik shaklini nusxadan-nusxaga o'zgartirib boradi 16. Rezident virus... tezkor xotirada saqlanadi 17. Hamma narsa ta'qiqlanadi. Bu qaysi xavfsizlik siyosatiga hos? Paranoid siyosati (Paranoid Policy) 1. Kiberetika tushunchasi: Kompyuter va kompyuter tarmoqlarida odamlarning etikasi 2. "Avtorizatsiya" atamasi qaysi tushuncha bilan sinonim sifatida ham foydalanadi? Foydalanishni boshqarish 3. Doktorlar, detektorlarga xos bo'lgan ishni bajargan holda zararlangan fayldan viruslarni chiqarib tashlaydigan va faylni oldingi holatiga qaytaradigan dasturiy ta'minot nomini belgilang. Faglar 4.

Zararli dasturlar qanday turlarga bo'linadi? Dasturdagi zaifliklar(atayin qilingan) va zararli dasturlar(atayin qilingan) 5. Aksariyat tijorat tashkilotlari uchun ichki tarmoq xavfsizligini taminlashning zaruriy sharti-bu... Tamoqlararo ekranlarning o'rnatilishi 6. Bag atamasini nima ma'noni beradi? Dasturiy ta'minotni amalga oshirish bosqichiga tegishli bo'lgan muammo 7. Tashkilotni himoyalash maqsadida amalga oshirilgan xavfsizlik nazoratini tavsiflovchi yuqori sathli hujjat yoki hujjatlar to'plami nima deyiladi? Xavfsizlik siyosat 8. Ma'lumotlarni zahira nusxasini saqlovchi va tikovchi dasturni belgilang. HandyBakcup 9. DIR viruslari nimani zararlaydi? FAT tarkibini zararlaydi 10. .... riskni tutuvchi mos nazorat usuli amalga oshirilganligini kafolatlaydi. Risk monitoring 11. Nuqson atamasiga berilgan ma'noni ko'rsating. Dasturni amalga oshirishdagi va loyixalashdagi zaifliklarning barchasi 12. "Axborot olish kafolatlari va erkinligi to'g'risida"gi Qonunning 10-moddasi mazmuni qanday? Axborot manbaini oshkor etmaslik 13. Qaysi siyosat turli hisoblash resurslaridan to'g'ri foydalanishni belgilaydi? Maqbul foydalanish siyosati 14. Axborot xavfsizligi boshqaruv tizimida "Aktiv" so'zi nimani anglatadi? Axborot xavfsizligida tashkilot uchun qimmatbaho bo'lgan va himoyalaniishi lozim bo'lgan narsalar 15. O'chirilgan yoki formatlangan ma'lumotlarni tikovchi dasturni belgilang. Recuva, R.saver 16. Qaysi texnologiyada ma'lumotlarni bir necha disklarda bayt satxida ajratilgan xolda yoziladi? RAID 3 17. Xavfsizlikni ta'minlashning bir yoki bir necha tizimi hamda loyihalashni nazoratlash va ulardan foydalanish xususida to'liq tasavvurga ega shaxs kim deb ataladi? Xavfsizlik ma'muri (admin) 19. Ma'lumotlarni blokarga bo'lib, bir qancha (kamida ikkita) qattiq diskda rezerv nusxasini yozish qaysi texnologiya? RAID 0 20. Qaysi siyosatda Administrator xavfsiz va zarur xizmatlarga individual ravishda ruxsat beradi? Extiyotkorlik siyosati 1. Ma'lumotlarni yo'qolish sabab bo'luvchi tabiiy tahdidlarni ko'rsating Zilzila, yong'in, suv toshqini va hak. 2. Shaxsning, axborot kommunikatsiya tizimidan foydalanish huquqiga ega bo'lish uchun foydalaniluvchining maxfiy bo'lmagan qayd yozuvi – bu... login 3. Berilgan ta'riflardan qaysi biri asimmetrik tizimlarga xos? Asimmetrik kriptotizimlarda  $k_1 \neq k_2$  bo'lib,  $k_1$  ochiq kalit,  $k_2$  yopiq kalit deb yuritiladi,  $k_1$  bilan axborot shifrlanadi,  $k_2$  bilan esa deshifrlanadi 6. Zimmermann telegrami, Enigma shifri, SIGABA kriptografiyaning qaysi davriga to'g'ri keladi? 1-2 jahon urushu davri 7. Wi-Fi necha Gs chastotali to'liqida ishlaydi? 2.4-5 Gs 8. Wi-Fi tarmoqlarida quyida keltirilgan qaysi shifrlash protokollaridan foydalaniladi. WEP, WPA, WPA2 11. Konfidentsiallikga to'g'ri ta'rif keltiring. axborot inshonchliligi, tarqatilishi mumkin emasligi, maxfiyligi kafolati; 12. Autentifikatsiya nima? Ma'lum qilingan foydalanuvchi, jarayon yoki qurilmaning haqiqiy ekanligini tekshirish muolajasi 13. Axborotni uzatish va saqlash jarayonida o'z strukturasi va yoki mazmunini saqlash xususiyati nima deb ataladi? Ma'lumotlar butunligi 14. ....–hisoblashga asoslangan bilim sohasi bo'lib, buzg'unchilar mavjud bo'lgan sharoitda amallarni kafolatlash uchun o'zida texnologiya, inson, axborot va jarayonni mujassamlashtirgan. Kiberxavfsizlik 15. Qaysi juftlik RSA algoritmining ochiq va yopiq kalitlarini ifodalaydi?  $\{d, n\}$  – yopiq,  $\{e, n\}$  – ochiq; 16. Kodlash nima? Ma'lumotni osongina qaytarish uchun hammaga ochiq bo'lgan sxema yordamida ma'lumotlarni boshqa formatga o'zgartirishdir 17. Qo'yish, o'rin almashtirish, gammalash kriptografiyaning qaysi turiga bog'liq? simmetrik kriptotizimlar 18. Kriptografiyada kalitning vazifasi nima? Matnni shifrlash va shifrini ochish uchun kerakli axborot 19. To'rtta bir-biri bilan bog'langan bog'lamlar strukturasi (kvadrat shaklida) qaysi topologiya turiga mansub? Xalqa 20. Axborot xavfsizligiga bo'ladigan tahdidlarning qaysi biri tasodifiy tahdidlar deb hisoblanadi? Texnik vositalarning buzilishi va ishlamasligi 1. Konfidentsiallikga to'g'ri ta'rif keltiring. axborot inshonchliligi, tarqatilishi mumkin emasligi, maxfiyligi kafolati; 2. Foydalanishni boshqarish –bu... Sub'ektni Ob'ektga ishlash qobiliyatini aniqlashdir. 3. Uning egasi haqiqiyiligini aniqlash jarayonida tekshiruv axboroti sifatida



ishlatiladigan belgilar ketma-ketligi (maxfiy so'z) – nima? parol 4. To'rtta bir-biri bilan bog'langan bog'lamlar strukturasi (kvadrat shaklida) qaysi topologiya turiga mansub? Xalqa 5. Kodlash nima? Ma'lumotni osongina qaytarish uchun hamma ochiq bo'lgan sxema yordamida ma'lumotlarni boshqa formatga o'zgartirishdir 6. Lokal tarmoqlarda keng tarqalgan topologiya turi qaysi? Yulduz 7. Axborotni uzatish va saqlash jarayonida o'z strukturasi va yoki mazmunini saqlash xususiyati nima deb ataladi? Ma'lumotlar butunligi 8. Wi-Fi necha Gs chastotali to'lqinda ishlaydi? 2.4-5 Gs 9. Yaxlitlikni buzilishi bu - ... Soxtalashtirish va o'zgartirish 10. Zimmermann telegrami, Enigma shifri, SIGABA kriptografiyaning qaysi davriga to'g'ri keladi? 1-2 jahon urushu davri 11. Axborot xavfsizligiga bo'ladigan tahdidlarning qaysi biri maqsadli (atayin) tahdidlar deb hisoblanadi? Strukturalarni ruxsatsiz modifikatsiyalash 12. Kriptotizimga qo'yiladigan umumiy talablardan biri nima? shifr matn uzunligi ochiq matn uzunligiga teng bo'lishi kerak 13. Risk nima? Potensial foyda yoki zarar 14. Assimetrik kriptotizimlar qanday maqsadlarda ishlatiladi? Shifrlash, deshifrlash, ERI yaratish va tekshirish, kalitlar almashish uchun 15. Ma'lumotlarni yo'q qilish odatda necha xil usulidan foydalaniladi? 4 xil 16. MAC usuli bilan foydalanishni boshqarishda xavfsizlik markazlashgan holatda kim tomonidan amalga oshiriladi? Xavfsizlik siyosati ma'muri 17. Quyidagilardan mintaqaviy tarmoqqa berilgan ta'rifni belgilang. Odatda ijaraga olingan telekommunikatsiya liniyalaridan foydalanadigan tarmoqlardagi tugunlarni bir-biriga bog'laydi. 3. Ehtiyotkorlik siyosati (Prudent Policy) – bu .... Barcha hizmatlar blokirovka qilingandan so'ng bog'lanadi 4. Axborot xavfsizligin ta'minlashda birinchi darajadagi me'yoriy hujjat nomini belgilang. Qonunlar 5. Rootkits-qanday zararli dastur? ushbu zararli dasturiy vosita operatsion tizim tomonidan aniqlanmasligi uchun ma'lum harakatlarini yashiradi. 6. Qaysi texnologiyada ma'lumotni ko'plab nusxalari bir vaqtda bir necha disklarga yoziladi? RAID 1 7. "Axborotlashtirish to'g'risida"gi Qonunning maqsadi nimadan iborat? Axborotlashtirish, axborot resurslari va axborot tizimlaridan foydalanish sohasidagi munosabatlarni tartibga solish. 8. Hamma narsa ta'qiqlanadi. Bu qaysi xavfsizlik siyosatiga hos? Paranoid siyosati (Paranoid Policy) 10. Qaysi siyosatga ko'ra hamma narsa ta'qiqlanadi? Paranoid siyosat 11. Tizim ishlamay turganda yoki foydalanuvchilar ma'lumot bilan ishlamay turganda zahiralash amalga oshirilsa .... deb ataladi. "Sovuq saxiralash" 12. Virusning signaturasi (virusga taalluqli baytlar ketmaketligi) bo'yicha operativ xotira va fayllarni ko'rish natijasida ma'lum viruslarni topuvchi va xabar beruvchi dasturiy ta'minot nomi nima deb ataladi? Detektorlar 13. Dasturlarni buzish va undagi mualliflik huquqini buzush uchun yo'naltirilgan buzg'unchi bu - ... . Krakker 14. "Fishing" tushunchasi: Tashkilot va odamlarning maxsus va shaxsiy ma'lumotlarini olishga qaratilgan internet-hujumi 15. O'zbekiston Respublikasi hududida turli ijtimoiy tarmoqlar platformalari cheklanishiga "Shaxsga doir ma'lumotlar to'g'risida"gi Qonunning qaysi moddasi sabab qilib olingan? 27(1)-modda. O'zbekiston Respublikasi fuqarolarining shaxsga doir ma'lumotlariga ishlov berishning alohida shartlari 16. Ma'lumotlarni zaxira nusxalash bu – ... Muhim bo'lgan axborot nusxalash yoki saqlash jarayoni. 17. Fishing (ing. Fishing – baliq ovlash) bu... Internetdagi firibgarlikning bir turi bo'lib, uning maqsadi foydalanuvchining maxfiy ma'lumotlaridan, login/parol, foydalanish imkoniyatiga ega bo'lishdir. 18. Dastlabki virus nechanchi yilda yaratilgan? 1986 19. "Backdoors"-qanday zararli dastur? zararli dasturiy kodlar bo'lib, hujumchiga autentifikatsiyani amalga oshirmasdan aylanib o'tib tizimga kirish imkonini beradi, maslan, administrator parolisiz imtiyozga ega bo'lish 20. Kiberetika tushunchasi: Kompyuter va kompyuter tarmoqlarida odamlarning etikasi 3. Ma'lumotlarni yo'q qilish odatda necha xil usulidan foydalaniladi? 4 xil 4. Ko'z pardasi, yuz tuzilishi, ovoz tembri, -bular autentifikatsiyaning qaysi faktoriga mos belgilar? Biometrik autentifikatsiya 5. Rol tushunchasiga ta'rif bering. Muayyan faoliyat turi bilan bog'liq harakatlar va majburiyatlar to'plami sifatida

belgilanishi mumkin 6. Identifikatsiya bu- ... Foydalanuvchini uning identifikatori (nomi) bo'yicha aniqlash jarayoni 7. Shifr nima? Shifrlash va deshifrlashda foydalaniladigan matematik funktsiyadan iborat bo'lgan kriptografik algoritm 8. Ma'lumotlarni inson xatosi tufayli yo'qolish sababini belgilang. Ma'lumotlarni saqlash vositasini to'g'ri joylashtirilmagani yoki ma'lumotlar bazasini xatolik bilan boshqarilganligi. 10. Stenografiya ma'nosi qanday? sirli yozuv 11. OSI modelida nechta sath mavjud? 7 ta 12. Kriptografiyada kalitning vazifasi nima? Matnni shifrlash va shifrini ochish uchun kerakli axborot 13. Qanday tarmoq qisqa masofalarda qurilmalar o'rtasida ma'lumot almashinish imkoniyatini taqdim etadi? Shaxsiy tarmoq 15. Risk nima? Potensial foyda yoki zarar 16. Kodlash nima? Ma'lumotni osongina qaytarish uchun hammaga ochiq bo'lgan sxema yordamida ma'lumotlarni boshqa formatga o'zgartirishdir 17. Foydalanishni boshqarishning qaysi usuli – Ob'ektlar va Sub'ektlarning atributlari, ular bilan mumkin bo'lgan amallar va so'rovlarga mos keladigan muhit uchun qoidalarni tahlil qilish asosida foydalanishlarni boshqaradi. ABAC 18. Shaxsning, axborot kommunikatsiya tizimidan foydalanish huquqiga ega bo'lish uchun foydalaniluvchining maxfiy bo'lmagan qayd yozuvi – bu... login 19. Zamonaviy kriptografiya qanday bo'limlardan iborat? Simmetrik kriptotizimlar; ochiq kalitli kriptotizimlar; Elektron raqamli imzo; kalitlarni boshqarish 1. Spam bilan kurashishning dasturiy uslubida nimalar ko'zda tutiladi? Elektron pochta qutisiga kelib tushadigan ma'lumotlar dasturlar asosida filtrlanib cheklanadi. 2. Ma'lumotlarni bloklarga bo'lib, bir qancha (kamida ikkita) qattiq diskda rezerv nusxasini yozish qaysi texnologiya? RAID 0 3. Tizim ishlamay turganda yoki foydalanuvchilar ma'lumot bilan ishlamay turganda zahiralash amalga oshirilsa .... deb ataladi. "Sovuq saxiralash" 4. Xavfsizlikni ta'minlashning bir yoki bir necha tizimi hamda loyihalashni nazoratlash va ulardan foydalanish xususida to'liq tasavvurga ega shaxs kim deb ataladi? Xavfsizlik ma'muri (admin) 5. Qaysi texnologiyada ma'lumotlarni bir necha disklarda bayt satxida ajratilgan xolda yoziladi va nazorat bitlari ham ular ichida taqsimlanadi? RAID 5 6. Tashkilotni himoyalash maqsadida amalga oshirilgan xavfsizlik nazoratini tavsiflovchi yuqori sathli hujjat yoki hujjatlar to'plami nima deyiladi? Xavfsizlik siyosat 7. Fishing (ing. Fishing – baliq ovlash) bu... Internetdagi firibgarlikning bir turi bo'lib, uning maqsadi foydalanuvchining maxfiy ma'lumotlaridan, login/parol, foydalanish imkoniyatiga ega bo'lishdir. 8. Bag atamasini nima ma'noni beradi? Dasturiy ta'minotni amalga oshirish bosqichiga tegishli bo'lgan muammo 9. "Backdoors"-qanday zararli dastur? zararli dasturiy kodlar bo'lib, hujumchiga autentifikatsiyani amalga oshirmasdan aylanib o'tib tizimga kirish imkonini beradi, maslan, administrator parolisiz imtiyozga ega bo'lish 10. Dastlabki virus nechanchi yilda yaratilgan? 1986 11. Virusning signaturasi (virusga taalluqli baytlar ketmaketligi) bo'yicha operativ xotira va fayllarni ko'rish natijasida ma'lum viruslarni topuvchi va xabar beruvchi dasturiy ta'minot nomi nima deb ataladi? Detektorlar 12. Risk monitoringi ..... ni paydo bo'lish imkoniyatini aniqlaydi. Yangi risklar 13. Ransomware qanday zarar keltiradi? mazkur zararli dasturiy ta'minot qurbon kompyuterida mavjud qimmatli fayllarni shifrlaydi yoki qulflab qo'yib, to'lov amalga oshirilishini talab qiladi. 14. O'zbekiston Respublikasi hududida turli ijtimoiy tarmoqlar platformalari cheklanishiga "Shaxsga doir ma'lumotlar to'g'risida"gi Qonunning qaysi moddasi sabab qilib olingan? 27(1)-modda. O'zbekiston Respublikasi fuqarolarining shaxsga doir ma'lumotlariga ishlov berishning alohida shartlari 15. Texnik himoya vositalari – bu ... Texnik qurilmalar, komplekslar yoki tizimlar yordamida ob'ektni himoyalashdir 17. Enterprise Information Security Policies, EISP-bu... Tashkilot axborot xavfsizligi siyosati 18. Qaysi siyosatga ko'ra hamma narsa ta'qiqlanadi? Paranoid siyosat 19. "Fishing" tushunchasi: Tashkilot va odamlarning maxsus va shaxsiy ma'lumotlarini olishga qaratilgan internet-hujumi 20. Axborot xavfsizligining huquqiy ta'minoti qaysi me'yorlarni o'z ichiga oladi? Xalqaro va milliy huquqiy me'yorlarni 1. "Fishing"

tushunchasi: Tashkilot va odamlarning maxsus va shaxsiy ma'lumotlarini olishga qaratilgan internet-hujumi 2. Dasturlarni buzish va undagi mualliflik huquqini buzush uchun yo'naltirilgan buzg'unchi bu - ... . Krakker 3. Agar foydalanuvchi tizimda ma'lumot bilan ishlash vaqtida ham zahiralash amalga oshirilishi .... deb ataladi? "Issiq zaxiralash" 4. Xizmat qilishdan voz kechishga undaydigan taqsimlangan hujum turini ko'rsating? DDoS (Distributed Denial of Service) hujum 5. Nuqson atamasiga berilgan ma'noni ko'rsating. Dasturni amalga oshirishdagi va loyixalashdagi zaifliklarning barchasi 6. Risklarni identifikatsiya qilishdan maqsad nima? Potensial zarar yetkazadigan ehtimoliy insidentlarni prognozlash va bu zarar qay tarzda olinishi mumkinligi to'g'risida tasavvurga ega bo'lish 7. Dastlabki virus nechanchi yilda yaratilgan? 1986 8. Rootkits-qanday zararli dastur? ushbu zararli dasturiy vosita operatsion tizim tomonidan aniqlanmasligi uchun ma'lum harakatlarini yashiradi. 9. Qaysi siyosatga ko'ra hamma narsa ta'qiqlanadi? Paranoid siyosat 10. Ko'p platformali viruslar bu... Bir vaqtning o'zida turli xildagi ob'ektlarni zararlaydi. Masalan, OneHalf.3544 virusi ham MS-DOS dasturlari ham qattiq diskning yuklanuvchi sektorlarini zararlaydi 11. "Axborot olish kafolatlari va erkinligi to'g'risida"gi Qonunning 10-moddasi mazmuni qanday? Axborot manbaini oshkor etmaslik 12. Risk monitoringi ..... ni paydo bo'lish imkoniyatini aniqlaydi. Yangi risklar 13. "Elektron hujjat" tushunchasi haqida to'g'ri ta'rif berilgan qatorni ko'rsating. Elektron shaklda qayd etilgan, elektron raqamli imzo bilan tasdiqlangan va elektron hujjatning uni identifikatsiya qilish imkoniyatini beradigan boshqa rekvizitlariga ega bo'lgan axborot elektron hujjatdir 15. O'zbekiston Respublikasi hududida turli ijtimoiy tarmoqlar platformalari cheklanishiga "Shaxsga doir ma'lumotlar to'g'risida"gi Qonunning qaysi moddasi sabab qilib olingan? 27(1)-modda. O'zbekiston Respublikasi fuqarolarining shaxsga doir ma'lumotlariga ishlov berishning alohida shartlari 16. Qaysi texnologiyada ma'lumotlarni bir necha disklarda bayt satxida ajratilgan xolda yoziladi va nazorat bitlari ham ular ichida taqsimlanadi? RAID 5 17. Axborot xavfsizligiga bo'ladigan tahdidlarning qaysi biri maqsadli (atayin) tahdidlar deb hisoblanadi? Strukturalarni ruxsatsiz modifikatsiyalash 18. "Backdoors"-qanday zararli dastur? zararli dasturiy kodlar bo'lib, hujumchiga autentifikatsiyani amalga oshirmasdan aylanib o'tib tizimga kirish imkonini beradi, maslan, administrator parolisiz imtiyozga ega bo'lish 19. Botnet-nima? internet tarmog'idagi obro'sizlantirilgan kompyuterlar bo'lib, taqsimlangan hujumlarni amalga oshirish uchun hujumchi tomonidan foydalaniladi. 20. Axborot xavfsizligida axborotning bahosi qanday aniqlanadi? Axborot xavfsizligi buzulgan taqdirda ko'rilishi mumkin bo'lgan zarar miqdori bilan Windows OT lokal xavfsizlik siyosatini sozlash oynasiga o'tish uchun "Buyruqlar satri"ga quyidagi so'rovlardan qaysi biri kiritiladi? J:secpol.msc

[https://drive.google.com/file/d/1C4h9EIJk4gYj5fHSj1Jb7uEAl4mpc6aj/view?usp=drive\\_link](https://drive.google.com/file/d/1C4h9EIJk4gYj5fHSj1Jb7uEAl4mpc6aj/view?usp=drive_link)

[https://drive.google.com/file/d/1K4VMDuTrKXvj7nBjF8oUWHn7Va7FN7kr/view?usp=drive\\_link](https://drive.google.com/file/d/1K4VMDuTrKXvj7nBjF8oUWHn7Va7FN7kr/view?usp=drive_link)

[Question]

ГОСТ Р 34.10-94 qanday standart hisoblanadi?

ERI standarti

kodlash standarti

steganografik standart

shifrlash standarti

Correct1

[Question]

O'zDSt 1092:2009 qanday standart hisoblanadi?

ERI standarti

shifrlash standarti

kodlash standarti

steganografik standart

Correct1

[Question]

DSA qanday standart hisoblanadi?

ERI standarti

shifrlash standarti

kodlash standarti

steganografik standart

Correct1

[Question]

Seans kalitli hamda seans kalitsiz rejimlarda ishlidigan  
standartni ko'rsating?

O'zDSt 1092:2009

ECDSA-2000

ГОСТ Р 34.10-94

DSA

Correct1

[Question]

ГОСТ Р 34.10-94 standarti qaysi davlat standarti  
hisoblanadi?

Rossiya

O'zbekiston

AQSH

Kanada

Correct1

[Question]

O'zDSt 1092:2009 standarti qaysi davlat standarti hisoblanadi?

O'zbekiston

AQSH

Rossiya

Kanada

Correct1

[Question]

ECDSA-2000 qaysi davlat standarti hisoblanadi?

AQSH

Rossiya

O'zbekiston

Kanada

Correct1

[Question]

Raqamli imzoni shakllantirish muolajasi qaysi algoritmgaga tegishli?

ERI algoritmgaga

kodlash algoritmgaga

shifrlash algoritmgaga

steganografiya algoritmgaga

Correct1

[Question]

Elektron hujjatni mualliflikdan bosh tortmasligini qaysi amal orqali amalga oshiriladi?

ERI orqali amalga oshiriladi

kodlash orqali amalga oshiriladi

autentifikatsiya orqali amalga oshiriladi

shifrlash algoritmi orqali amalga oshiriladi

Correct1

[Question]

Elektron hujjat yaxlitligini (o'zgarmasligini) tekshirish qaysi amal orqali amalga

oshiriladi?

ERI orqali amalga oshiriladi

kodlash orqali amalga oshiriladi

shifrlash algoritmi orqali amalga oshiriladi

autentifikatsiya orqali amalga oshiriladi

Correct1

[Question]

Elektron hujjat manbaini haqiqiyligini qaysi amal orqali amalga oshiriladi?

ERI orqali amalga oshiriladi

shifrlash algoritmi orqali amalga oshiriladi

kodlash orqali amalga oshiriladi

autentifikatsiya orqali amalga oshiriladi

Correct1

[Question]

1 ga va o'ziga bo'linadigan sonlar qanday sonlar hisoblanadi?

tub sonlar

murakkab sonlar

toq sonlar

juft sonlar

Correct1

[Question]

Elliptik egriz chiqizlarda nuqtalar usitda qanday ammalar bajariladi?

nuqtalarni qo'shish va nuqtalarni ikkilantirish

nuqtalarni qo'shish va nuqtalarni ko'paytirish

nuqtalarni qo'shish va nuqtalarni bo'lish

nuqtalarni ayirish va nuqtalarni ko'paytirish

Correct1

[Question]

Sonlarni tublikka tekshiruvchi ehtimollikka asoslangan algoritmlar keltirilgan qatordan qaysi ko'rsatib berilgan?

Ferma, Solovey Shtrassen, Rabbi-Milner

Ferma, Solovey Shtrassen, Eyler

Eyler, Solovey Shtrassen, Rabbi-Milner

Ferma, Eyler, Rabbi-Milner

Correct1

[Question]

Sonlarni tublikka tekshiruvchi algorimtlar qanday sinfga bo'linadi?

aniqlashtirilgan va ehtimolli testlar

aniqlashtirilgan va taqribiy testlar

taqribiy va ehtimolli testlar

aniqlashtirilgan, ehtimolli va taqribiy testlar

Correct1

[Question]

Sonlarni tublikka tekshiruvchi algoritmlar necha sinfga bo'linadi?

2

3

4

5

Correct1

[Question]

Rabbi-Milner testi qanday turdagi tublikka testlovchi algoritm hisoblanadi?

ehtimollik testlar tarkibiga kiruvchi algoritm

aniqlashtirilgan testlar tarkibiga kiruvchi algoritm

taqribiy testlar tarkibiga kiruvchi algoritm

tublikka teslovchi algoritm hisoblanmaydi

Correct1

[Question]

Solovey Shtrassen testi qanday turdagi tublikka testlovchi algoritm hisoblanadi?

ehtimollik testlar tarkibiga kiruvchi algoritm

aniqlashtirilgan testlar tarkibiga kiruvchi algoritm

taqribiy testlar tarkibiga kiruvchi algoritm

tublikka teslovchi algoritm hisoblanmaydi

Correct1

[Question]

Ferma testi qanday turdagi tublikka testlovchi algoritm

hisoblanadi?

ehtimollik testlar tarkibiga kiruvchi algoritm

aniqlashtirilgan testlar tarkibiga kiruvchi algoritm

taqribiy testlar tarkibiga kiruvchi algoritm

tublikka teslovchi algoritm hisoblanmaydi

Correct1

[Question]

Kriptotizimlar kalitlar soni bo'yicha qanday turga

bo'linadi?

simmetrik va assimetrik

simmetrik va bitta kalitli

3 kalitli kriptotizimlar

assimetrik va 2 ta kalitli

Correct1

[Question]

Kriptotizimlar kalitlar soni bo'yicha nechta turga

bo'linadi?

2

3

4

5

Correct1

[Question]

Faqat simmetrik algoritm keltirilgan qatorni ko'rsating?

AES

RSA

El-Gamal

Barcha javoblar to'g'ri

Correct1

[Question]

Kriptografiya bu -?

axborotni o'zgartirish vositalari va usullarini

o'rganadigan fan

axborot mazmunidan beruxsat erkin foydalanishdan

muhofazalash



axborotni buzishning oldini olish

axborot almashtirish vosita va usullari bilan

shug'ullanadigan fa

Correct1

[Question]

Shifrlash orqali ma'lumotning qaysi xususiyati

ta'minlanadi?

maxfiyligi

butunliligi

ishonchliligi

foydalanuvchanliligi

Correct1

[Question]

Ochiq kalitli shifrlash algoritmi keltirilgan qatorni toping?

El-Gamal

AES

DES

RC4

Correct1

[Question]

Ochiq kalitli shifrlash algoritmi keltirilgan qatorni toping?

RSA

AES

DES

RC4

Correct1

[Question]

RSA algoritmining mualliflarini ko'rsating

R. Rayvest, A. Shamir, L. Adleman

Diffi va M. Xellman

R. Rayvest, K. Xellman, L. Adleman

L. Adleman, El Gamal, K. Shnorr

Correct1

[Question]

Kriptotahlil nima bilan shug'ullanadi?

kalit yoki algoritmi bilmagan holda shifrlangan

ma'lumotga mos k

ochiq ma'lumotlarni shifrlash masalalarining matematik

uslublari

maxfiy kodlarni yaratish bilan

maxfiy kodlar orqali ma'lumotlarni yashirish bilan

Correct1

[Question]

Sonlarni tublikka tekshirish algoritmlari nechta sinfga

bo'linadi?

ikkita sinfga

uchta sinfga

bitta sinfga

sinflarga bo'linmaydi

Correct1

[Question]

Qanday sonlar tub sonlar hisoblanadi?

1 va o'ziga bo'linadigan sonlarlar

barcha toq sonlar

juft bo'lmagan sonlar

2 ga bo'linmaydigan sonlar

Correct1

[Question]

Ochiq kalitli kriptotizimlarda asosan qanday turdagi

sonlar bilan ishlaydi?

tub sonlar bilan

kasr sonlar bilan

chekli maydonda kasr sonlar

faqat manfiy sonlar

Correct1

[Question]

Ochiq kalitli kriptotizimda, qaysi kalit orqali ma'lumot

rasshifrovkalanadi?

maxfiy kalit orqali

ochiq kalit orqali

ma'lumot shifrlanmaydi

ushbu tizimda kalitdan foydalanilmaydi

Correct1

[Question]

Ochiq kalitli kriptotizimlarda qaysi kalit orqali ma'lumot shifrlanadi?

ochiq kalit orqali

maxfiy kalit orqali

ushbu tizimda kalitdan foydalanilmaydi

ma'lumot shifrlanmaydi

Correct1

[Question]

Ochiq kalitni kriptotizimlarda nechta kalitdan foydalanadi?

ikkita

bitta

uchta

kalitdan foydalanilmaydi

Correct1

[Question]

Kalit bardoshliligi bu -?

eng yaxshi ma'lum algoritm bilan kalitni topish

murakkabligidir

eng yaxshi ma'lum algoritm yordamida yolg'on axborotni

ro'kach qi

nazariy bardoshlilik

amaliy bardoshlilik

Correct1

[Question]

Kerkxofs printsipi nimadan iborat?

kriptografik tizim faqat kalit noma'lum bo'lgan

taqdirdagina maxf

kriptografik tizim faqat yopiq bo'lgan taqdirdagina

maxfiylik ta'

kriptografik tizim faqat kalit ochiq bo'lgan taqdirdagina

maxfiyl

kriptografik tizim faqat ikkita kalit ma'lum bo'lgan

taqdirdagina

Correct1

[Question]

Assimetrik kriptotizimlarda necha kalitdan foydalaniladi?

2 ta

3 ta

4 ta

kalit ishlatilmaydi

Correct1

[Question]

Ochiq kalitli kriptotizimlarda qanday turdagi kalitlardan foydalanadi?

ochiq va maxfiy kalitlardan

maxfiy kalitlar juftidan

maxfiy kalitni uzatishni talab etmaydi

ochiq kalitni talab etmaydi

Correct1

[Question]

Simmetrik kriptotizimlardagi qanday muammoni ochiq kalitli kriptotizimlar bartaraf etdi?

maxfiy kalitni uzatish muammosini

kalitni generatsiyalash muammosini

ochiq kalitni uzatish muammosini

kalitlar juftini hosil qilish muammosini

Correct1

[Question]

Kriptotizimlar kalitlar soni bo'yicha qanday turga bo'linadi?

simmetrik va assimetrik turlarga

simmetrik va bir kalitli turlarga

3 kalitli turlarga

assimetrik va 2 kalitli turlarga

Correct1

[Question]

Kriptotizimlar kalitlar soni bo'yicha necha turga bo'linadi?

2

4

6

8

Correct1

[Question]

Ochiq kalitli kriptotizimlar ma'lumotni qanday xususiyatini taminlaydi?

maxfiyligini

butunligini

foydalanuvchanligini

ma'lumotni autentifikatsiyasini

Correct1

[Question]

Kriptologiya so'zining ma'nosi?

cryptos – maxfiy, logos – ilm

cryptos – kodlash, logos – ilm

cryptos – kriptο, logos – yashiraman

cryptos – maxfiy, logos – kalit

Correct1

[Question]

Kriptologiya necha yo'nalishga bo'linadi?

2

14

16

18

Correct1

[Question]

Ochiq kalitli kriptotizimlar kim tomonidan kashf qilingan?

U.Diffie va M.Hellman

Rivest va Adlman

Shamir va Rivest

U.Diffie va Rivest

Correct1

[Question]

Shifrlash orqali ma'lumotning qaysi xususiyati

ta'minlanadi?

maxfiyligi

butunliligi

ishonchliligi

foydalanuvchanligi

Correct1

[Question]

Kriptotahlil nima bilan shug'ullanadi?

maxfiy kodlarni buzish bilan

maxfiy kodlarni yaratish bilan

shifrlash uslublarini bilmagan holda shifrlangan

ma'lumotni asl h

maxfiy kodlar orqali ma'lumotlarni yashirish bilan

Correct1

[Question]

Kriptografiya nima bilan shug'ullanadi?

maxfiy kodlarni yaratish bilan

maxfiy kodlarni buzish bilan

maxfiy kodlar orqali ma'lumotlarni yashirish bilan

shifrlash uslublarini bilmagan holda shifrlangan

ma'lumotni asl h

Correct1

[Question]

Kriptologiya nima bilan shug'ullanadi?

maxfiy kodlarni yaratish va buzish ilmi bilan

maxfiy kodlarni buzish bilan

maxfiy kodlarni yaratish bilan

maxfiy kodlar orqali ma'lumotlarni yashirish bilan

Correct1

[Question]

Kriptologiya qanday yo'nalishlarga bo'linadi?

kriptografiya va kriptotahlil

kriptografiya va kriptotizim

kripto va kriptotahlil

kriptoanaliz va kriptotizim

Correct1

[Question]

Ochiq kalitli El-Gamal shifrlash algoritmda "p" tub son bo'lsa maxfiy kalit qanday tanlanadi?

(p-1) bilan o'zaro tub bo'lgan (1,p-1) intervaldagi butun son

p bilan o'zaro tub bo'lgan (1,p-1) intervaldagi butun son  
(1,p-1) intervaldagi tub son

(p-1) bilan o'zaro tub bo'lgan (1,p) intervaldagi butun son

Correct1

[Question]

Ochiq kalitli RSA shifrlash algoritmda "p=7" tub son bo'lsa Eyler funskiyasi  $\varphi(p)$  qanday qiymat qaytaradi?

6

7

$\varphi(7)$

$\varphi(6)$

Correct1

[Question]

Ochiq kalitli RSA shifrlash algoritmda "p" tub son bo'lsa Eyler funskiyasi  $\varphi(p)$  qanday qiymat qaytaradi?

p-1

p

$\varphi(p)$

$\varphi(p-1)$

Correct1

[Question]

Ochiq kalitli RSA shifrlash algoritmda "d" shaxsiy kalit, "e" ochiq kalit bo'lsa shifrlash formulasi to'g'ri ko'rsatilgan qatorni belgilang?

$C = M^e \pmod{N}$

$C = M^e \pmod{\varphi(N)}$

$C = M^d \pmod{\varphi(N)}$

$$C = M^d \pmod{N}$$

Correct1

[Question]

Ochiq kalitli RSA shifrlash algoritmidagi "e" ochiq kalit,

"d" shaxsiy kalit bo'lsa d

eshifrlash formulasi to'g'ri ko'rsatilgan qatorni belgilang?

$$M = C^d \pmod{N}$$

$$M = C^d \pmod{\varphi(N)}$$

$$M = C^e \pmod{N}$$

$$M = C^e \pmod{\varphi(N)}$$

Correct1

[Question]

Ochiq kalitli RSA shifrlash algoritmidagi qaysi parametrlar

ochiq holda e'lon qilinadi

i?

N, e

e

N, d

d

Correct1

[Question]

Ochiq kalitli RSA shifrlash algoritmidagi maxfiy kalit

qanday topiladi?

$$e \cdot d = 1 \pmod{\varphi(p \cdot q)} \text{ taqqoslamadan}$$

$$e \cdot d = 1 \pmod{N}$$

$$e \cdot d = 1 \pmod{p-1}$$

$$e \cdot d = 1 \pmod{(p-1)(q-1)}$$

Correct1

[Question]

Ochiq kalitli RSA shifrlash algoritmidagi ochiq kalit "e"

qanday topiladi?

$\varphi(N)$  bilan o'zaro tub va undan kichik bo'lgan son

tanlanadi

$\varphi(N)$  dan kichik tub son tanlanadi

$\varphi(N)$  dan katta tub son tanlanadi

$\varphi(N)$  ning tub ko'paytuvchilaridan biri tanlanadi



Correct1

[Question]

Faktorlash muammosini yechishning Pollard usulida

funksiya argumenti boshlangich qi

ymati nechiga teng bo'ladi?

2

1

3

0

Correct1

[Question]

Faktorlash muammosini yechishning Pollard usulida eng

kichik polinom qanday tanlana

di?

$x^2+1$

$x+1$

$x$

$x^2$

Correct1

[Question]

Faktorlash muammosini yechishning Pollard usulida

tanlanadigan funksiya qanday ko'r

inishda bo'ladi?

kvadratik polinom

chiziqli polinom

kubik polinom

funksiya argumentiga bog'liq emas

Correct1

[Question]

Agar sonlarni tublikka tekshirishning Rabbin-Miller

testida beshta tublikka guvohi

mavjud bo'lsa tekshirilayotgan sonni tub bo'lishi ehtimoli

nechiga teng?

$1-2^{-5}$

$1-(1/2)$

$1-2^5$

$$1-5^{(-2)}$$

Correct1

[Question]

Agar sonlarni tublikka tekshirishning Ferma testida uchta tublikka guvohi mavjud bo

'lsa tekshirilayotgan sonni tub bo'lishi ehtimoli nechiga teng?

$$1-2^{(-3)}$$

$$1-(1/2)$$

$$1-2^3$$

$$1-3^{(-2)}$$

Correct1

[Question]

Agar sonlarni tublikka tekshirishning Solavey-Shtrassen testida ikkita tublikka guv

ohi mavjud bo'lsa tekshirilayotgan sonni tub bo'lishi ehtimoli nechiga teng?

$$1-2^{(-2)}$$

$$1-(1/2)$$

$$1-2^2$$

$$1-(1/(2^{(-2)}))$$

Correct1

[Question]

“murakkabligiga guvoh” termini qaysi algoritmlarda ishlatiladi

sonlarni tublikka tekshirish algoritmlarida

shifrlash algoritmlarida

kodlash algoritmlarida

steganografik algoritmlarda

Correct1

[Question]

“soxta tublikka guvoh” termini qaysi algoritmlarda ishlatiladi

sonlarni tublikka tekshirish algoritmlarida

shifrlash algoritmlarida

steganografik algoritmlarda

kodlash algoritmlarida

Correct1

[Question]

“Psevdotub” termini qaysi algoritmlarda ishlatiladi

sonlarni tublikka tekshirish algoritmlarida

shifrlash algoritmlarida

steganografik algoritmlarda

kodlash algoritmlarida

Correct1

[Question]

Qanday sonlar murakkab sonlar deyiladi?

ko'paytuvchilarga ajraladigan sonlar murakkab sonlar  
deyiladi

ko'paytuvchilarga ajralmaydigan sonlar murakkab sonlar  
deyiladi

ko'paytuvchilarga ajralmaydigan toq sonlar sonlar  
murakkab sonlar

ko'paytuvchilarga ajraladigan juft sonlar murakkab sonlar  
deyilad

Correct1

[Question]

RSA algoritmi qaysi tizimga mansub?

Ochiq kalitli tizimlar

Maxfiy kalitli tizimlar

Xesh-funksiyalar

Tasodifiy sonlar generatori

Correct1

[Question]

Sonlarni tublikka tekshirishda qaysi algoritm Karlmaykl  
sonlarida ham to'g'ri ishlay  
di?

Ferma algoritmida

Solovey Shtrassen algoritmida

Rabin-Milner algoritmida

Eyler algoritmida

Correct1

[Question]

Sonlarni tublikka tekshirishda qaysi algoritm samarali hisoblanadi?

Rabin Milner

Solovey Shtrassen

Ferma

Eyler

Correct1

[Question]

Qaysi algoritm o'rtada turgan odam hujumiga bardoshsiz hisoblanadi?

Diffie-Hellman

RSA

ElGamal

DSA

Correct1

[Question]

Diffie-Hellman algoritmi qanday hujumga bardoshsiz hisoblanadi?

o'rtada turgan odam hujumiga

chastotalar tahlili hujumiga

yon kanal tahlili hujumiga

to'liq tanlash hujumiga

Correct1

[Question]

RSA shifrlash algoritmida qaysi parametrlar ochiq holda e'lon qilinadi?

ochiq kalit –  $e$ , hamda modul qiymati -  $N$

maxfiy kalit –  $d$ , hamda modul qiymati -  $N$

ochiq kalit –  $e$ , hamda tub sonlar –  $p, q$

maxfiy kalit –  $d$ , hamda tub sonlar –  $p, q$

Correct1

[Question]

Qaysi kalit orqali ERI qo'yiladi?

shaxsiy kalit orqali

ochiq kalit orqali

kalit ishtirok etmaydi

ikkala kalit birgalikda ishtirok etadi

Correct1

[Question]

O'zbekistonning qanday ERI standarti mavjud?

O'zDSt 1092:2009

DSA

ECDSA-2000

ГОСТ Р 34.10-94

Correct1

[Question]

O'zbekistonning nechta ERI standarti mavjud?

1 ta

2 ta

3 ta

mavjud emas

Correct1

[Question]

Amerikaning qanday ERI standarti mavjud?

DSA va ECDSA-2000

DSA va ГОСТ Р 34.10-94

ECDSA-2000 va ГОСТ Р 34.10-94

ГОСТ Р 34.10-94 va O'zDSt 1092:2009

Correct1

[Question]

Amerikaning nechta ERI standarti mavjud?

2 ta

1 ta

3 ta

mavjud emas

Correct1

[Question]

RSA algoritmidagi  $p$ ,  $q$  tub sonlar bo'lsa, modul qiymati  $N$  qanday topiladi?

$N=p*q$

$N=p/q$

$N=q/p$

$N=p-q$

Correct1

[Question]

Karlmaykl sonlari qaysi tublikka tekshiruvchi

algoritmida doim bajariladi?

Ferma testida

Solovey-Shtrassen testida

Eyler testida

Rabbin testida

Correct1

[Question]

Faktorlash murakkabligiga asoslangan algoritm keltirilgan

qatorni ko'rsating?

RSA

El-Gamal

Diffie-Hellman

DSA

Correct1

[Question]

Diskret logarifmlash murakkabligiga asoslangan algoritm

keltirilgan qatorni ko'rsat

ing?

Diffie-Hellman, EL-Gamal algoritmi

RSA algoritmi

EL-Gamal algoritmi

Diffie-Hellman algoritmi

Correct1

[Question]

RSA shifrlash algoritmida tanlangan p va q sonlarga

qanday talab qo'yiladi?

tub bo'lishi

o'zaro tub bo'lishi

butun son bo'lishi

toq son bo'lishi

Correct1

[Question]

O'zDSt 1092:2009 ERI standarti birinchi algoritmi

qanday rejimlarda ishlaydi?

kalitli va kalitsiz

ochiq kalitli va maxfiy kalitli

ochiq va maxfiy

1 ta asosiy rejimi mavjud

Correct1

[Question]

Ochiq kalitli kriptotizimlarda elektron hujjatlarga

qo'yilgan imzoni tekshirish qay

si kalit orqali amalga oshiriladi?

ochiq kalit orqali

maxfiy kalit orqali

imzo qo'yilishi kalitga bog'liq emas

imzo qo'lda qo'yiladi

Correct1

[Question]

Ochiq kalitli kriptotizimlarda elektron hujjatlarga imzo

qo'yish qaysi kalit orqali

amalga oshiriladi?

shaxsiy kalit orqali

ochiq kalit orqali

imzo qo'yilishi kalitga bog'liq emas

imzo qo'lda qo'yiladi

Correct1

[Question]

ERI algoritmlari qanday muolajalardan iborat?

imzoni shakllantirish, imzoni tekshirish

imzoni shakllantirish, imzo qo'yish va imzoni tekshirish

imzoni shakllantirish va imzo qo'yish

imzo qo'yish

Correct1

[Question]

ERI algoritmlari nechta muolajadan iborat?

ikkita

bitta asosiy

uchta

to'rtta

Correct1

[Question]

Faqat tub son keltirilgan qatorni toping?

2, 5

5, 25

16, 3

3, 21

Correct1

[Question]

Diffie-Hellman qanday algoritm hisoblanadi?

kalitlarni ochiq taqsimlash algoritmi

ochiq kalitli shifrlash algoritmi

diskret logarifmlash murakkabligiga asoslangan shifrlash

algoritm

faktordash murakkabligiga asoslangan kalitlarni ochiq

taqsimlash

Correct1

[Question]

Diffie-Helman algoritmi qanday matematik

murakkablikka asoslanadi?

diskret logarifmlash murakkabligiga

faktordash murakkabligiga

elliptik egri chiziqda diskret logarifmlash murakkabligiga

elliptik egri chiziqda faktordash murakkabligiga

Correct1

[Question]

Ochiq kalitli El-Gamal shifrlash algoritmi qanday

matematik murakkablikka asoslanad

i?

diskret logarifmlash murakkabligiga

faktordash murakkabligiga

elliptik egri chiziqda diskret logarifmlash murakkabligiga

elliptik egri chiziqda faktordash murakkabligiga



Correct1

[Question]

Ochiq kalitli RSA shifrlash algoritmi bardoshliligi qanday matematik muammo turiga

asoslangan?

faktorklash murakkabligiga

diskret logarifmlash murakkabligiga

elliptik egri chiqizlarda faktORIZatsiyalash murakkabligiga

elliptik egri chiziqlarda faktORIZatsiyalash murakkabligiga

Correct1

[Question]

Sonlarni tublikka tekshirishning ehtimolli algoritmlariga

quyidagilarning qaysilari

kiradi?

Ferma, Rabbi-Milner, Poklingtong testlari

Rabbi-Milner, Solovey-Shtrassen, Pollard testlari

Ferma, Solovey-Shtrassen, Pollard testlari

Rabbi Milner, Poklington, Pollard testlari

Correct1

[Question]

Ehtimolli testlar sonlarni tublikka tekshirishda qanday

natijani beradi?

tekshirilayotgan son tub yoki tubmasligi haqida ehtimollik

bilan

tekshirilayotgan son tub yoki tubmasligi haqida

kafolatlangan ani

tekshirilayotgan son tub yoki tubmasligi haqida tasodifiy

ravishd

tekshirilayotgan son tub yoki tubmasligini 0 va 1

qiymatlarga qar

Correct1

[Question]

Faqat tub son keltirilgan qatorni toping?

3, 5

5, 15

16, 2

3, 18

Correct1

[Question]

Ochiq kalitli kriptotizimlarning bardoshligini ta'minlashda

qanday murakkab muammo

turiga asoslanadi?

faktoriallash, diskret logarifmlash, elliptik egri chiziqlarda

diskret

faktoriallash, diskret logarifmlash

faktoriallash, diskret logarifmlash, elliptik egri chiziqlarda

faktorial

faktoriallash, diskret logarifmlash, modulyar arifmetikaga

Correct1

[Question]

Ochiq kalitli kriptotizimlarning matematik asosi nimaga

asoslangan?

oson hisoblanadigan bir tomonlama funksiyalarga

modulyar arifmetikaga

faktorializatsiyalashga

diskret logarifmlashga

Correct1

[Question]

Ochiq kalitli kriptotizimlar qanday turdagi matematik

murakkablikka asoslangan algo

ritmlarga bo'linadi?

faktorializatsiyalash va diskret logarifmlash algoritmlariga

modulyar arifmetika murakkabligiga asoslangan

algoritmlarga

diskret logarifmlash murakkabligiga asoslangan

algoritmlarga

faktorializatsiyalash murakkabligiga asoslangan

algoritmlarga

Correct1

[Question]

ГОСТ Р 34.10-94 qanday standart hisoblanadi?

ERI standarti

kodlash standarti

steganografik standart

shifrlash standarti

Correct1

[Question]

O'zDSt 1092:2009 qanday standart hisoblanadi?

ERI standarti

shifrlash standarti

kodlash standarti

steganografik standart

Correct1

[Question]

DSA qanday standart hisoblanadi?

ERI standarti

shifrlash standarti

kodlash standarti

steganografik standart

Correct1

[Question]

Seans kalitli hamda seans kalitsiz rejimlarda ishlidigan  
standartni ko'rsating?

O'zDSt 1092:2009

ECDSA-2000

ГОСТ Р 34.10-94

DSA

Correct1

[Question]

ГОСТ Р 34.10-94 standarti qaysi davlat standarti  
hisoblanadi?

Rossiya

O'zbekiston

AQSH

Kanada

Correct1

[Question]

O'zDSt 1092:2009 standarti qaysi davlat standarti

hisoblanadi?

O'zbekiston

AQSH

Rossiya

Kanada

Correct1

[Question]

ECDSA-2000 qaysi davlat standarti hisoblanadi?

AQSH

Rossiya

O'zbekiston

Kanada

Correct1

[Question]

Raqamli imzoni shakllantirish muolajasi qaysi algoritmgaga tegishli?

ERI algoritmgaga

kodlash algoritmgaga

shifrlash algoritmgaga

steganografiya algoritmgaga

Correct1

[Question]

Elektron hujjatni mualliflikdan bosh tortmasligini qaysi amal orqali amalga oshiriladi?

ERI orqali amalga oshiriladi

kodlash orqali amalga oshiriladi

autentifikatsiya orqali amalga oshiriladi

shifrlash algoritmi orqali amalga oshiriladi

Correct1

[Question]

Elektron hujjat yaxlitligini (o'zgarmasligini) tekshirish qaysi amal orqali amalga oshiriladi?

ERI orqali amalga oshiriladi

kodlash orqali amalga oshiriladi

shifrlash algoritmi orqali amalga oshiriladi

autentifikatsiya orqali amalga oshiriladi

Correct1

[Question]

Elektron hujjat manbaini haqiqiyligini qaysi amal orqali amalga oshiriladi?

ERI orqali amalga oshiriladi

shifrlash algoritmi orqali amalga oshiriladi

kodlash orqali amalga oshiriladi

autentifikatsiya orqali amalga oshiriladi

Correct1

[Question]

1 ga va o'ziga bo'linadigan sonlar qanday sonlar hisoblanadi?

tub sonlar

murakkab sonlar

toq sonlar

juft sonlar

Correct1

[Question]

Elliptik egriz chiqizlarda nuqtalar usitda qanday ammalar bajariladi?

nuqtalarni qo'shish va nuqtalarni ikkilantirish

nuqtalarni qo'shish va nuqtalarni ko'paytirish

nuqtalarni qo'shish va nuqtalarni bo'lish

nuqtalarni ayirish va nuqtalarni ko'paytirish

Correct1

[Question]

Sonlarni tublikka tekshiruvchi ehtimollikka asoslangan algoritmlar keltirilgan qato rni ko'rsating?

Ferma, Solovey Shtrassen, Rabbi-Milner

Ferma, Solovey Shtrassen, Eyler

Eyler, Solovey Shtrassen, Rabbi-Milner

Ferma, Eyler, Rabbi-Milner

Correct1

[Question]

Sonlarni tublikka tekshiruvchi algorimtlar qanday sinfga bo'linadi?

aniqlashtirilgan va ehtimolli testlar

aniqlashtirilgan va taqribiy testlar

taqribiy va ehtimolli testlar

aniqlashtirilgan, ehtimolli va taqribiy testlar

Correct1

[Question]

Sonlarni tublikka tekshiruvchi algoritmlar necha sinfga bo'linadi?

2

3

4

5

Correct1

[Question]

Rabbi-Milner testi qanday turdagi tublikka testlovchi algoritm hisoblanadi?

ehtimollik testlar tarkibiga kiruvchi algoritm

aniqlashtirilgan testlar tarkibiga kiruvchi algoritm

taqribiy testlar tarkibiga kiruvchi algoritm

tublikka teslovchi algoritm hisoblanmaydi

Correct1

[Question]

Solovey Shtrassen testi qanday turdagi tublikka testlovchi algoritm hisoblanadi?

ehtimollik testlar tarkibiga kiruvchi algoritm

aniqlashtirilgan testlar tarkibiga kiruvchi algoritm

taqribiy testlar tarkibiga kiruvchi algoritm

tublikka teslovchi algoritm hisoblanmaydi

Correct1

[Question]

Ferma testi qanday turdagi tublikka testlovchi algoritm hisoblanadi?

ehtimollik testlar tarkibiga kiruvchi algoritm

aniqlashtirilgan testlar tarkibiga kiruvchi algoritm

taqribiy testlar tarkibiga kiruvchi algoritm

tublikka teslovchi algoritm hisoblanmaydi

Correct1

[Question]

Kriptotizimlar kalitlar soni bo'yicha qanday turga

bo'linadi?

simmetrik va assimetrik

simmetrik va bitta kalitli

3 kalitli kriptotizimlar

assimetrik va 2 ta kalitli

Correct1

[Question]

Kriptotizimlar kalitlar soni bo'yicha nechta turga

bo'linadi?

2

3

4

5

Correct1

[Question]

Faqat simmetrik algoritm keltirilgan qatorni ko'rsating?

AES

RSA

El-Gamal

Barcha javoblar to'g'ri

Correct1

[Question]

Kriptografiya bu -?

axborotni o'zgartirish vositalari va usullarini

o'rganadigan fan

axborot mazmunidan beruxsat erkin foydalanishdan

muhofazalash

axborotni buzishning oldini olish

axborot almashtirish vosita va usullari bilan

shug'ullanadigan fa

Correct1

[Question]

Shifrlash orqali ma'lumotning qaysi xususiyati ta'minlanadi?

maxfiyligi

butunliligi

ishonchliligi

foydalanuvchanliligi

Correct1

[Question]

Ochiq kalitli shifrlash algoritmi keltirilgan qatorni toping?

El-Gamal

AES

DES

RC4

Correct1

[Question]

Ochiq kalitli shifrlash algoritmi keltirilgan qatorni toping?

RSA

AES

DES

RC4

Correct1

[Question]

RSA algoritmining mualliflarini ko'rsating

R. Rayvest, A. Shamir, L. Adleman

Diffi va M. Xellman

R. Rayvest, K. Xellman, L. Adleman

L. Adleman, El Gamal, K. Shnorr

Correct1

[Question]

Kriptotahlil nima bilan shug'ullanadi?

kalit yoki algoritmni bilmagan holda shifrlangan

ma'lumotga mos k

ochiq ma'lumotlarni shifrlash masalalarining matematik

uslublari



maxfiy kodlarni yaratish bilan

maxfiy kodlar orqali ma'lumotlarni yashirish bilan

Correct1

[Question]

Sonlarni tublikka tekshirish algoritmlari nechta sinfga bo'linadi?

ikkita sinfga

uchta sinfga

bitta sinfga

sinflarga bo'linmaydi

Correct1

[Question]

Qanday sonlar tub sonlar hisoblanadi?

1 va o'ziga bo'linadigan sonlarlar

barcha toq sonlar

juft bo'lmagan sonlar

2 ga bo'linmaydigan sonlar

Correct1

[Question]

Ochiq kalitli kriptotizimlarda asosan qanday turdagi sonlar bilan ishlaydi?

tub sonlar bilan

kasr sonlar bilan

chekli maydonda kasr sonlar

faqat manfiy sonlar

Correct1

[Question]

Ochiq kalitli kriptotizimda, qaysi kalit orqali ma'lumot rasshifrovkalanadi?

maxfiy kalit orqali

ochiq kalit orqali

ma'lumot shifrlanmaydi

ushbu tizimda kalitdan foydalanilmaydi

Correct1

[Question]

Ochiq kalitli kriptotizimlarda qaysi kalit orqali ma'lumot

shifrlanadi?

ochiq kalit orqali

maxfiy kalit orqali

ushbu tizimda kalitdan foydalanilmaydi

ma'lumot shifrlanmaydi

Correct1

[Question]

Ochiq kalitni kriptotizimlarda nechta kalitdan

foydalanadi?

ikkita

bitta

uchta

kalitdan foydalanilmaydi

Correct1

[Question]

Kalit bardoshliligi bu -?

eng yaxshi ma'lum algoritm bilan kalitni topish

murakkabligidir

eng yaxshi ma'lum algoritm yordamida yolg'on axborotni

ro'kach qi

nazariy bardoshlilik

amaliy bardoshlilik

Correct1

[Question]

Kerkxofs printsipi nimadan iborat?

kriptografik tizim faqat kalit noma'lum bo'lgan

taqdirdagina maxf

kriptografik tizim faqat yopiq bo'lgan taqdirdagina

maxfiylik ta'

kriptografik tizim faqat kalit ochiq bo'lgan taqdirdagina

maxfiyl

kriptografik tizim faqat ikkita kalit ma'lum bo'lgan

taqdirdagina

Correct1

[Question]

Assimetrik kriptotizimlarda necha kalitdan foydalaniladi?

2 ta

3 ta

4 ta

kalit ishlatilmaydi

Correct1

[Question]

Ochiq kalitli kriptotizimlarda qanday turdagi kalitlardan foydalanadi?

ochiq va maxfiy kalitlardan

maxfiy kalitlar juftidan

maxfiy kalitni uzatishni talab etmaydi

ochiq kalitni talab etmaydi

Correct1

[Question]

Simmetrik kriptotizimlardagi qanday muammoni ochiq kalitli kriptotizimlar bartaraf etdi?

maxfiy kalitni uzatish muammosini

kalitni generatsiyalash muammosini

ochiq kalitni uzatish muammosini

kalitlar juftini hosil qilish muammosini

Correct1

[Question]

Kriptotizimlar kalitlar soni bo'yicha qanday turga bo'linadi?

simmetrik va assimetrik turlarga

simmetrik va bir kalitli turlarga

3 kalitli turlarga

assimetrik va 2 kalitli turlarga

Correct1

[Question]

Kriptotizimlar kalitlar soni bo'yicha necha turga bo'linadi?

2

4

6

8

Correct1

[Question]

Ochiq kalitli kriptotizimlar ma'lumotni qanday xususiyatini taminlaydi?

maxfiyligini

butunligini

foydalanuvchanligini

ma'lumotni autentifikatsiyasini

Correct1

[Question]

Kriptologiya so'zining ma'nosi?

cryptos – maxfiy, logos – ilm

cryptos – kodlash, logos – ilm

cryptos – kriptο, logos – yashiraman

cryptos – maxfiy, logos – kalit

Correct1

[Question]

Kriptologiya necha yo'nalishga bo'linadi?

2

14

16

18

Correct1

[Question]

Ochiq kalitli kriptotizimlar kim tomonidan kashf qilingan?

U.Diffie va M.Hellman

Rivest va Adlman

Shamir va Rivest

U.Dlffie va Rivest

Correct1

[Question]

Shifrlash orqali ma'lumotning qaysi xususiyati ta'minlanadi?

maxfiyligi

butunliligi

ishonchliligi

foydalanuvchanligi

Correct1

[Question]

Kriptotahlil nima bilan shug'ullanadi?

maxfiy kodlarni buzish bilan

maxfiy kodlarni yaratish bilan

shifrlash uslublarini bilmagan holda shifrlangan

ma'lumotni asl h

maxfiy kodlar orqali ma'lumotlarni yashirish bilan

Correct1

[Question]

Kriptografiya nima bilan shug'ullanadi?

maxfiy kodlarni yaratish bilan

maxfiy kodlarni buzish bilan

maxfiy kodlar orqali ma'lumotlarni yashirish bilan

shifrlash uslublarini bilmagan holda shifrlangan

ma'lumotni asl h

Correct1

[Question]

Kriptologiya nima bilan shug'ullanadi?

maxfiy kodlarni yaratish va buzish ilmi bilan

maxfiy kodlarni buzish bilan

maxfiy kodlarni yaratish bilan

maxfiy kodlar orqali ma'lumotlarni yashirish bilan

Correct1

[Question]

Kriptologiya qanday yo'nalishlarga bo'linadi?

kriptografiya va kriptotahlil

kriptografiya va kriptotizim

kripto va kriptotahlil

kriptoanaliz va kriptotizim

Correct1

[Question]

Ochiq kalitli El-Gamal shifrlash algoritmidagi "p" tub son

bo'lsa maxfiy kalit qanday

tanlanadi?

(p-1) bilan o'zaro tub bo'lgan (1,p-1) intervaldagi butun son

p bilan o'zaro tub bo'lgan (1,p-1) intervaldagi butun son  
(1,p-1) intervaldagi tub son

(p-1) bilan o'zaro tub bo'lgan (1,p) intervaldagi butun son

Correct1

[Question]

Ochiq kalitli RSA shifrlash algoritmda "p=7" tub son

bo'lsa Eyler funskiyasi  $\varphi(p)$

qanday qiymat qaytaradi?

6

7

$\varphi(7)$

$\varphi(6)$

Correct1

[Question]

Ochiq kalitli RSA shifrlash algoritmda "p" tub son bo'lsa

Eyler funskiyasi  $\varphi(p)$  qa

nday qiymat qaytaradi?

p-1

p

$\varphi(p)$

$\varphi(p-1)$

Correct1

[Question]

Ochiq kalitli RSA shifrlash algoritmda "d" shaxsiy kalit,

"e" ochiq kalit bo'lsa s

hifrlash formulasi to'g'ri ko'rsatilgan qatorni belgilang?

$C=M^e \pmod N$

$C=M^e \pmod \varphi(N)$

$C=M^d \pmod \varphi(N)$

$C=M^d \pmod N$

Correct1

[Question]

Ochiq kalitli RSA shifrlash algoritmda "e" ochiq kalit,

"d" shaxsiy kalit bo'lsa d

eshifrlash formulasi to'g'ri ko'rsatilgan qatorni belgilang?

$$M=C^d \pmod{N}$$

$$M=C^d \pmod{\varphi(N)}$$

$$M=C^e \pmod{N}$$

$$M=C^e \pmod{\varphi(N)}$$

Correct1

[Question]

Ochiq kalitli RSA shifrlash algoritmda qaysi parametrlar

ochiq holda e'lon qilinad

i?

N,e

e

N,d

d

Correct1

[Question]

Ochiq kalitli RSA shifrlash algoritmda maxfiy kalit

qanday topiladi?

$$e*d=1 \pmod{\varphi(p*q)} \text{ taqqoslamadan}$$

$$e*d=1 \pmod{N}$$

$$e*d=1 \pmod{p-1}$$

$$e*d=1 \pmod{(p-1)(q-1)}$$

Correct1

[Question]

Ochiq kalitli RSA shifrlash algoritmda ochiq kalit "e"

qanday topiladi?

$\varphi(N)$  bilan o'zaro tub va undan kichik bo'lgan son

tanlanadi

$\varphi(N)$  dan kichik tub son tanlanadi

$\varphi(N)$  dan katta tub son tanlanadi

$\varphi(N)$  ning tub ko'paytuvchilaridan biri tanlanadi

Correct1

[Question]

Faktirlash muammosini yechishning Pollard usulida

funksiya argumenti boshlangich qi

ymati nechiga teng bo'ladi?

2

1

3

0

Correct1

[Question]

Faktorlash muammosini yechishning Pollard usulida eng

kichik polinom qanday tanlana

di?

$x^2+1$

$x+1$

$x$

$x^2$

Correct1

[Question]

Faktorlash muammosini yechishning Pollard usulida

tanlanadigan funksiya qanday ko'r

inishda bo'ladi?

kvadratik polinom

chiziqli polinom

kubik polinom

funksiya argumentiga bog'liq emas

Correct1

[Question]

Agar sonlarni tublikka tekshirishning Rabin-Miller

testida beshta tublikka guvohi

mavjud bo'lsa tekshirilayotgan sonni tub bo'lishi ehtimoli

nechiga teng?

$1-2^{-5}$

$1-(1/2)$

$1-2^5$

$1-5^{-2}$

Correct1

[Question]



Agar sonlarni tublikka tekshirishning Ferma testida uchta

tublikka guvohi mavjud bo

'lsa tekshirilayotgan sonni tub bo'lishi ehtimoli nechiga

teng?

$$1-2^{(-3)}$$

$$1-(1/2)$$

$$1-2^3$$

$$1-3^{(-2)}$$

Correct1

[Question]

Agar sonlarni tublikka tekshirishning Solavey-Shtrassen

testida ikkita tublikka guv

ohi mavjud bo'lsa tekshirilayotgan sonni tub bo'lishi

ehtimoli nechiga teng?

$$1-2^{(-2)}$$

$$1-(1/2)$$

$$1-2^2$$

$$1-(1/(2^{(-2)}))$$

Correct1

[Question]

“murakkabligiga guvoh” termini qaysi algoritmlarda

ishlatiladi

sonlarni tublikka tekshirish algoritmlarida

shifrlash algoritmlarida

kodlash algoritmlarida

steganografik algoritmlarda

Correct1

[Question]

“soxta tublikka guvoh” termini qaysi algoritmlarda

ishlatiladi

sonlarni tublikka tekshirish algoritmlarida

shifrlash algoritmlarida

steganografik algoritmlarda

kodlash algoritmlarida

Correct1

[Question]

“Psevdotub” termini qaysi algoritmlarda ishlatiladi

sonlarni tublikka tekshirish algoritmlarida

shifrlash algoritmlarida

steganografik algoritmlarda

kodlash algoritmlarida

Correct1

[Question]

Qanday sonlar murakkab sonlar deyiladi?

ko'paytuvchilarga ajraladigan sonlar murakkab sonlar  
deyiladi

ko'paytuvchilarga ajralmaydigan sonlar murakkab sonlar  
deyiladi

ko'paytuvchilarga ajralmaydigan toq sonlar sonlar  
murakkab sonlar

ko'paytuvchilarga ajraladigan juft sonlar murakkab sonlar  
deyilad

Correct1

[Question]

RSA algoritmi qaysi tizimga mansub?

Ochiq kalitli tizimlar

Maxfiy kalitli tizimlar

Xesh-funksiyalar

Tasodifiy sonlar generatori

Correct1

[Question]

Sonlarni tublikka tekshirishda qaysi algoritm Karlmaykl  
sonlarida ham to'g'ri ishlay  
di?

Ferma algoritmida

Solovey Shtrassen algoritmida

Rabin-Milner algoritmida

Eyler algoritmida

Correct1

[Question]

Sonlarni tublikka tekshirishda qaysi algoritm samarali  
hisoblanadi?

Rabin Milner

Solovey Shtrassen

Ferma

Eyler

Correct1

[Question]

Qaysi algoritm o'rtada turgan odam hujumiga bardoshsiz hisoblanadi?

Diffie-Hellman

RSA

ElGamal

DSA

Correct1

[Question]

Diffie-Hellman algoritmi qanday hujumga bardoshsiz hisoblanadi?

o'rtada turgan odam hujumiga

chastotalar tahlili hujumiga

yon kanal tahlili hujumiga

to'liq tanlash hujumiga

Correct1

[Question]

RSA shifrlash algoritmidan qaysi parametrlar ochiq holda e'lon qilinadi?

ochiq kalit –  $e$ , hamda modul qiymati -  $N$

maxfiy kalit –  $d$ , hamda modul qiymati -  $N$

ochiq kalit –  $e$ , hamda tub sonlar –  $p, q$

maxfiy kalit –  $d$ , hamda tub sonlar –  $p, q$

Correct1

[Question]

Qaysi kalit orqali ERI qo'yiladi?

shaxsiy kalit orqali

ochiq kalit orqali

kalit ishtirok etmaydi

ikkala kalit birgalikda ishtirok etadi

Correct1

[Question]

O'zbekistonning qanday ERI standarti mavjud?

O'zDSt 1092:2009

DSA

ECDSA-2000

ГОСТ Р 34.10-94

Correct1

[Question]

O'zbekistonning nechta ERI standarti mavjud?

1 ta

2 ta

3 ta

mavjud emas

Correct1

[Question]

Amerikaning qanday ERI standarti mavjud?

DSA va ECDSA-2000

DSA va ГОСТ Р 34.10-94

ECDSA-2000 va ГОСТ Р 34.10-94

ГОСТ Р 34.10-94 va O'zDSt 1092:2009

Correct1

[Question]

Amerikaning nechta ERI standarti mavjud?

2 ta

1 ta

3 ta

mavjud emas

Correct1

[Question]

RSA algoritmidagi  $p$ ,  $q$  tub sonlar bo'lsa, modul qiymati  $N$  qanday topiladi?

$N=p*q$

$N=p/q$

$N=q/p$

$N=p-q$

Correct1

[Question]

Karlmaykl sonlari qaysi tublikka tekshiruvchi  
algoritmarda doim bajariladi?

Ferma testida

Solovey-Shtrassen testida

Eyler testida

Rabbin testida

Correct1

[Question]

Faktorlash murakkabligiga asoslangan algoritm keltirilgan  
qatorni ko'rsating?

RSA

El-Gamal

Diffie-Hellman

DSA

Correct1

[Question]

Diskret logarifmlash murakkabligiga asoslangan algoritm  
keltirilgan qatorni ko'rsat  
ing?

Diffie-Hellman, EL-Gamal algoritmi

RSA algoritmi

EL-Gamal algoritmi

Diffie-Hellman algoritmi

Correct1

[Question]

RSA shifrlash algoritmida tanlangan  $p$  va  $q$  sonlarga  
qanday talab qo'yiladi?

tub bo'lishi

o'zaro tub bo'lishi

butun son bo'lishi

toq son bo'lishi

Correct1

[Question]

O'zDSt 1092:2009 ERI standarti birinchi algoritmi  
qanday rejimlarda ishlaydi?

kalitli va kalitsiz

ochiq kalitli va maxfiy kalitli

ochiq va maxfiy

1 ta asosiy rejimi mavjud

Correct1

[Question]

Ochiq kalitli kriptotizimlarda elektron hujjatlarga

qo'yilgan imzoni tekshirish qay

si kalit orqali amalga oshiriladi?

ochiq kalit orqali

maxfiy kalit orqali

imzo qo'yilishi kalitga bog'liq emas

imzo qo'lda qo'yiladi

Correct1

[Question]

Ochiq kalitli kriptotizimlarda elektron hujjatlarga imzo

qo'yish qaysi kalit orqali

amalga oshiriladi?

shaxsiy kalit orqali

ochiq kalit orqali

imzo qo'yilishi kalitga bog'liq emas

imzo qo'lda qo'yiladi

Correct1

[Question]

ERI algoritmlari qanday muolajalardan iborat?

imzoni shakllantirish, imzoni tekshirish

imzoni shakllantirish, imzo qo'yish va imzoni tekshirish

imzoni shakllantirish va imzo qo'yish

imzo qo'yish

Correct1

[Question]

ERI algoritmlari nechta muolajadan iborat?

ikkita

bitta asosiy

uchta

to'rtta

Correct1

[Question]

Faqat tub son keltirilgan qatorni toping?

2, 5

5, 25

16, 3

3, 21

Correct1

[Question]

Diffie-Hellman qanday algoritm hisoblanadi?

kalitlarni ochiq taqsimlash algoritmi

ochiq kalitli shifrlash algoritmi

diskret logarifmlash murakkabligiga asoslangan shifrlash  
algoritm

faktorlash murakkabligiga asoslangan kalitlarni ochiq  
taqsimlash

Correct1

[Question]

Diffie-Helman algoritmi qanday matematik

murakkablikka asoslanadi?

diskret logarifmlash murakkabligiga

faktorlash murakkabligiga

elliptik egri chiziqda diskret logarifmlash murakkabligiga

elliptik egri chiziqda faktorlash murakkabligiga

Correct1

[Question]

Ochiq kalitli El-Gamal shifrlash algoritmi qanday

matematik murakkablikka asoslanad

i?

diskret logarifmlash murakkabligiga

faktorlash murakkabligiga

elliptik egri chiziqda diskret logarifmlash murakkabligiga

elliptik egri chiziqda faktorlash murakkabligiga

Correct1

[Question]

Ochiq kalitli RSA shifrlash algoritmi bardoshliligi qanday

matematik muammo turiga

asoslangan?

faktordash murakkabligiga

diskret logarifmlash murakkabligiga

elliptik egri chiqizlarda faktORIZatsiyalash murakkabligiga

elliptik egri chiziqlarda faktORIZatsiyalash murakkabligiga

Correct1

[Question]

Sonlarni tublikka tekshirishning ehtimolli algoritmlariga

quyidagilarning qaysilari

kiradi?

Ferma, Rabbi-Milner, Poklingtong testlari

Rabbi-Milner, Solovey-Shtrassen, Pollard testlari

Ferma, Solovey-Shtrassen, Pollard testlari

Rabbi Milner, Poklington, Pollard testlari

Correct1

[Question]

Ehtimolli testlar sonlarni tublikka tekshirishda qanday

natijani beradi?

tekshirilayotgan son tub yoki tubmasligi haqida ehtimollik

bilan

tekshirilayotgan son tub yoki tubmasligi haqida

kafolatlangan ani

tekshirilayotgan son tub yoki tubmasligi haqida tasodifiy

ravishd

tekshirilayotgan son tub yoki tubmasligini 0 va 1

qiymatlarga qar

Correct1

[Question]

Faqat tub son keltirilgan qatorni toping?

3, 5

5, 15

16, 2

3, 18

Correct1

[Question]



Ochiq kalitli kriptotizimlarning bardoshligini ta'minlashda

qanday murakkab muammo

turiga asoslanadi?

faktorlash, diskret logarifmlash, elliptik egri chiziqda

diskret

faktorlash, diskret logarifmlash

faktorlash, diskret logarifmlash, elliptik egri chiziqda

faktoriz

faktorlash, diskret logarifmlash, modulyar arifmetikaga

Correct1

[Question]

Ochiq kalitli kriptotizimlarning matematik asosi nimaga

asoslangan?

oson hisoblanadigan bir tomonlama funksiyalarga

modulyar arifmetikaga

faktorizatsiyalashga

diskret logarifmlashga

Correct1

[Question]

Ochiq kalitli kriptotizimlar qanday turdagi matematik

murakkablikka asoslangan algo

ritmlarga bo'linadi?

faktorizatsiyalash va diskret logarifmlash algoritmlariga

modulyar arifmetika murakkabligiga asoslangan

algoritmlarga

diskret logarifmlash murakkabligiga asoslangan

algorimtlarga

faktorizatsiyalash murakkabligiga asoslangan

algorimtlarga

Correct1

[Question]

RSA algoritmidan qanday maqsadda foydalaniladi?

Shifrlash va elektron raqamli imzo

Autentifikatsiya va xeshlash

Shifrlash

Elektron raqamli imzo

Correct1

[Question]

El Gamal algoritmidan qanday maqsadda foydalaniladi?

Shifrlash va elektron raqamli imzo

Autentifikatsiya va xeshlash

Shifrlash

Elektron raqamli imzo

Correct1

[Question]

DSSda qaysi algoritmdan foydalanilgan?

Toxir El Gamal algoritmi

K. Shnorr

RSA

ESIGN

Correct1

[Question]

DSA algoritmidan qanday maqsadda foydalaniladi?

Elektron raqamli imzo

Autentifikatsiya

Shifrlash

Xeshlash

Correct1

[Question]

EC DSA elektron raqamli imzo algoritmi qanday

matematik murakkablik asosida yaratil

gan?

Elliptik egri chiziqli diskret logarifm

Diskret logarifmlashni hisoblash

Tub ko'paytuvchilarga ajratish

Chiziqli algebraik tenglamalar sistemasini yechish

Correct1

[Question]

Elektron raqamli imzo algoritmlari bardoshligini yanada

oshirishda qanday funksiyal

ardan foydalaniladi?

Xesh-funksiya

Matematik funksiya

Bir tomonlama funksiya

Logarifmik funksiya

Correct1

[Question]

ГОСТ Р 34. 10-2001 elektron raqamli imzo algoritmda

qaysi xesh-funksiyadan foyda

laniladi?

ГОСТ Р 34.11-94

O'z DSt 1106

A5

SHA-256

Correct1

[Question]

Sonlarni tublikka tekshirishning Solavey-Shtrassen testida

Lejandr simvoli qiymati

qanday aniqlanadi?

(a/p)

(p/a)

(p-1)/2

(a-1)/2

Correct1

[Question]

Sonlarni tublikka tekshirishning Solavey-Shtrassen testida

qanday simvoldan foydala

nadi?

Lejandr simvolidan

Karlmaykl simvolidan

Eyler simvolidan

Lukas simvolidan

Correct1

[Question]

Elektron raqamli imzo bo'yicha birinchi O'z DSt 1092

qaysi korxona tomonidan ishlab

chiqilgan?

UNICON.UZ

INFOCOM

UZTELECOM

O'zR axborot texnologiyalari va kommunikatsiyalarini  
rivojlanti

Correct1

[Question]

O'z DSt 1092 standarti qanday matematik murakkablik  
asosida yaratilgan?

Parametrli algebra

Elliptik egri chiziqli diskret logarifm

Diskret logarifmlashni hisoblash

Tub ko'paytuvchilarga ajratish

Correct1

[Question]

O'z DSt 1092 standartida qanday amallardan  
foydalanilgan?

Parametr bilan ko'paytirish, parametr bilan darajaga  
ko'tarish,

Ko'paytirish, darajaga ko'tarish, teskarilash

Qo'shish ayirish ko'paytirish, bo'lish

Qo'shish, bo'lish, ayirish, darajaga ko'tarish

Correct1

[Question]

Umumiy bo'luvchi bu -

Berilgan a va v sonlarni bo'luvchi butun son

Berilgan a va v sonlarga karrali son

Tub son

O'zaro tub son

Correct1

[Question]

Eng katta umumiy bo'luvchi qanday belgilanadi?

EKUB(a, b)

EKUD

EKUK

EKUK(a,b)

Correct1

[Question]

Faktorlash – bu

Berilgan sonning tub ko'paytuvchilarini topish

Sonlar nazariyasining eng dastlabki masalalaridan biri

Berilgan sonni biror amal yoki xususiyatga ko'ra uning  
tashkil et

Berilgan to'plamni uning tashkil etuvchilari orqali  
ifodalanishi

Correct1

[Question]

Xeshlash algoritmlaridan qaysi xususiyatni ta'minlashda  
foydalaniladi?

Butunlik

Maxfiylik

Foydalanuvchanlik

Autentifikatsiya

Correct1

[Question]

AQSH ning elektron raqamli imzo standartini ko'rsating

DSS

DSA

RSA

ESIGN

Correct1

[Question]

DES shifrlash algoritmi...

Simmetrik blokli shifr.

Ochiq kalitli shifr.

Assimetrik shifr.

Ikki kalitli shifr.

Correct1

[Question]

Faktorlash muammosi ifodalangan qatorni ko'rsating?

$N=p*q;$

$Y=(g^a) \bmod p;$

$N=\text{SQRT}(P);$

$Y=g^a;$

Correct1

[Question]

17 soni bilan o'zaro tub bo'lgan sonlarni ko'rsating?

16, 18

12, 34

14, 51

17 dan tashqari barcha sonlar

Correct1

[Question]

Qaysi algoritm Karlmaykl sonlarini murakkab son sifatida aniqlaydi?

Solovey-Shtrassen algoritmi

Ferma algoritmi

Rabbin Miller algoritmi

RSA algoritmi

Correct1

[Question]

Eyler kriteriyasidan qaysi algoritmda foydalanadi?

Solovey-Shtrassen algortmida

Ferma algoritmida

Rabbin Miller algoritmida

RSA algoritmida

Correct1

[Question]

Ellipti egri chiziqlarda funksiya koeffitsentlari  $a, b$  qiymati qanday shartni qanoatlantirishi kerak?

$4a^3+27b^2 \neq 0$

$4a^2+27b^2 \neq 0$

$4a^3+27b^3 \neq 0$

$4a^2+27b^3 \neq 0$

Correct1

[Question]

13 soni bilan o'zaro tub bo'lgan sonlarni ko'rsating?

5, 7

12, 26

14, 39

13 dan tashqari barcha sonlar

Correct1

[Question]

Agar RSA algoritmi uchun  $p=3$  va  $q=7$  bo'lsa,  $n$  va  $\varphi(n)$

ni hisoblang?

21, 12

21, 21

12, 21

12, 12

Correct1

[Question]

Ochiq kalitli RSA shifrlash algoritmidagi " $p=11$ " tub son

bo'lsa Eyler funksiyasi  $\varphi(p)$

qanday qiymat qaytaradi?

10

8

6

4

Correct1

[Question]

$-19 \bmod 11$  nechiga teng?

3

5

4

2

Correct1

[Question]

$143 \bmod 17$  nechiga teng?

7

6

5

8

Correct1

[Question]

2 lik sanoq tizimida 0101 soniga 1111 sonini 2 modul

bo'yicha qo'shing?

1010

101

1111

1001

Correct1

[Question]

Sonlarni tublikka tekshirishning Solovey-Shtrassen testida

Lejandr simvoli qanday q

iymatlarni qabul qilishi mumkin?

0,-1,1

0,1

0,-1

1, -1

Correct1

[Question]

Sonlarni tublikka tekshirishning Solovey-Shtrassen testida

qanday simvoldan foydala

nadi?

Lejandr simvalidan

Karlmaykl simvalidan

Eyler simvalidan

Lukas simvalidan

Correct1

[Question]

Sonlarni tublikka tekshirishning Solovey-Shtrassen testida

qanday taqqoslamadan foy

dalanadi?

$a^{((p-1)/2)} \equiv (a/p) \pmod p$

$a^{((p-1)/2)} \equiv 1 \pmod p$

$a^{((p-1)/2)} \not\equiv (a/p) \pmod p$

$a^{((p-1)/2)} \not\equiv 1 \pmod p$

Correct1

[Question]

Sonlarni tublikka tekshirishning Ferma testida qanday



taqqoslama bajarilganda teksh

irilayotgan son murakkab bo'ladi?

$$a^{(n-1)} \equiv 1 \pmod{n}$$

$$a^{(n-1)} = 1 \pmod{n}$$

$$a^{(\varphi(n)-1)} \equiv 1 \pmod{n}$$

$$a^{(\varphi(n)-1)} = 1 \pmod{n}$$

Correct1

[Question]

Sonlarni tublikka tekshirishning Ferma testida qanday

taqqoslamadan foydalaniladi?

$$a^{(n-1)} = 1 \pmod{n}$$

$$a^{(\varphi(n)-1)} = 1 \pmod{n}$$

$$a^{(\varphi(n))} = 1 \pmod{n}$$

$$a^{(n-1)} \equiv 1 \pmod{n}$$

Correct1

[Question]

Sonlarni tublikka tekshirishning Solovey-Shtrassen testida

qanday kriteriyadan foyd

alanadi?

Eyler kriteriyasidan

Karlmaykl sonlari kriteriyasidan

Murakkab sonlar kriteriyasidan

Tub sonlar kriteriyasidan

Correct1

[Question]

O'zDSt 1092:2009 ERI standarti ikkinchi algoritmi

qanday murakkablikka asoslanadi?

elliptik egri chiziqlarda diskret logarifmlash

murakkabligiga

diskret logarifmlash murakkabligiga

faktORIZatsiyalash murakkabligiga

elliptik egri chiziqlarda faktORIZatsiyalash murakkabligiga

Correct1

[Question]

O'zDSt 1092:2009 ERI standarti birinchi algoritmi

qanday murakkablikka asoslanadi?

daraja parametr muammosiga

diskret logarifmlash muammosiga

faktORIZatsiyalash muammosiga

elliptik egri chiziqlarda faktORIZatsiyalash murakkabligiga

Correct1

[Question]

DSA ERI standarti qanday murakkablikka asoslanadi?

diskret logarifmlash masalasini murakkabligiga

faktORIZatsiyalash masalasi murakkabligiga

elliptik egri chiziqlarga asoslangan diskret logarifmlash

masalas

elliptik egri chiziqlarga asoslangan faktORIZatsiyalash

masalasi

Correct1

[Question]

O'zDSt 1092:2009 standarti bu?

ERI standarti

Shifrlash standarti

Xesh funksiya standarti

Kalitni generatsiyalash standarti

Correct1

[Question]

Ochiq kalitli kriptotizimlarga asoslangan ERI

algoritmlarida kalitlar juftini qaysi

tomon hosil qiladi?

kalitlar juftini ma'lumot yuboruvchi tomon hosil qiladi

kalitlar juftini ma'lumot qabul qiluvchi tomon hosil qiladi

kalitlar juftini har bir foydalanuvchining o'zi hosil qiladi

uchinchi ishonchli tomon hosil qiladi

Correct1

[Question]

ERI algoritmlari qanday turdagi masalalarni yechishga

imkon beradi?

ma'lumot yaxlitligini tekshirish, ma'lumot manbani

autentifikatsi

ma'lumot yaxlitligini tekshirish, ma'lumot manbani

autentifikatsi

ma'lumot manbani autentifikatsiyalash hamda rad

etishdan himoyala

ma'lumot yaxlitligini tekshirish, rad etishdan himoyalash

Correct1

[Question]

Qanday algoritm yordamida diskret logarifmlash

muammosini bartaraf etiladi?

Polig-Hellman algoritmi

Diffie-Hellman algoritmi

Pollard algoritmi

Eyler-Ferma algoritmi

Correct1

[Question]

Ochiq kalitli kriptotizimlarga asoslangan kalitlarni

taqsimlovchi Diffie-Hellman al

goritmi vazifasi nima?

umumiy maxfiy kalitni hosil qilish

ochiq va yopiq kalitlar juftini hosil qilish

maxfiy kalitni uzatishni talab etmaydi

ochiq kalitlarni hosil qilish

Correct1

[Question]

Ochiq kalitli RSA shifrlash algoritmida "e" ochiq kalit

bo'lsa shifrlash formulasi

to'g'ri ko'rsatilgan qatorni belgilang?

$C = M^e \pmod{N}$

$C = M^e \pmod{\varphi(N)}$

$C = M^d \pmod{\varphi(N)}$

$C = M^d \pmod{N}$

Correct1

[Question]

Ochiq kalitli RSA shifrlash algoritmida "d" maxfiy kalit

bo'lsa rasshifrovkalash fo

rmulasi to'g'ri ko'rsatilgan qatorni belgilang?

$M = C^d \pmod{N}$

$$M = C^d \pmod{?(N)}$$

$$M = C^e \pmod{N}$$

$$M = C^e \pmod{?(N)}$$

Correct1

[Question]

Nosimmetrik kriptografiya asosida birinchi bo'lib

elektron raqamli imzo bo'yicha mi

lily standart yaratgan davlat?

AQSh

Germaniya

Rossiya

Koreya

Correct1

[Question]

Aniqlashtirilgan testlar sonlarni tublikka tekshirishda

qanday natijani beradi?

tekshirilayotgan son tub yoki tubmasligi haqida

kafolatlangan ani

tekshirilayotgan son tub yoki tubmasligi haqida tasodifiy

ravishd

tekshirilayotgan son tub yoki tubmasligi haqida ehtimollik

bilan

tekshirilayotgan son tub yoki tubmasligini 0 va 1

oraliqdagi qiym

Correct1

[Question]

Malumotni shifrlash va deshifrlashda turli kalitlardan

foydalanuvchi algoritmni ko'

rsating?

El-Gamal

AES

DES

RC4

Correct1

[Question]

"A" va "B" foydalanuvchilar maxfiy tarzda ma'lumot

almashmoqchi, "A" foydalanuvchi

qabul qilgan ma'lumotni rasshifrovkalash uchun qaysi kalitdan foydalanadi?

o'zining maxfiy kalitidan foydalanadi

o'zining ochiq kalitidan foydalanadi

"B" foydalanuvchining maxfiy kalitidan foydalanadi

"B" foydalanuvchining ochiq kalitidan foydalanadi

Correct1

[Question]

"A" va "B" foydalanuvchilar maxfiy tarzda ma'lumot almashmoqchi, "A" foydalanuvchi ma'lumotni shifrlab yuborish uchun qaysi kalitdan foydalanadi?

"B" foydalanuvchining ochiq kalitidan foydalanadi

o'zining ochiq kalitidan foydalanadi

"B" foydalanuvchining maxfiy kalitidan foydalanadi

o'zining maxfiy kalitidan foydalanadi

Correct1

[Question]

Quyida keltirilgan qaysi standart ochiq kalitli infratuzilmalar uchun mo'ljallangan?

X.509 standarti

DSA standarti

ECDSA standarti

RSA standarti

Correct1

[Question]

X.509 standarti nima uchun mo'ljallangan?

ochiq kalitli infratuzilmalar uchun

raqamli imzo uchun

maxfiy kalit uchun

ochiq kalit uchun

Correct1

[Question]

Tashkilot imzosi nimada aks etishi kerak?

raqamli sertifikatda

shifrlashda

kodlashda

raqamli imzoda

Correct1

[Question]

Foydalanuchi ochiq kaliti nimada aks etishi kerak?

raqamli sertifikatda

raqamli imzoda

shifrlashda

kodlashda

Correct1

[Question]

Foydalanuvchi nomi haqidagi ma'lumotlar nimada aks etishi kerak?

raqamli sertifikatda

raqamli imzoda

shifrlashda

kodlashda

Correct1

[Question]

Raqamli sertifikat qanday parametrlarni o'z ichiga oladi?

foydalanuvchi nomini, uning ochiq kalitini va tashkilot imzosini

foydalanuvchi nomini, uning maxfiy kalitini va tashkilot imzosini

foydalanuvchi maxfiy hamda ochiq kalitini va tashkilot imzosini

foydalanuvchi maxfiy hamda ochiq kalitini

Correct1

[Question]

Ochiq kalit kafolati deganda nima tushiniladi?

ochiq kalit domenda bo'lishi va hammaga ko'rinishi tushiniladi

maxfiy kalit domenda bo'lishi va hammaga ko'rinishi tushiniladi

ochiq kalit domenda bo'lishi va hammadan sir saqlanishi

tushinila

maxfiy kalit domenda bo'lishi va hammadan sir

saqlanishi tushinil

Correct1

[Question]

Shaxsiy kalitni maxfiylikini saqlash deganda nima

tushiniladi?

kalitni boshqarish davomida tomonlardan maxfiy tarzda

saqlanishi

kalitni to'g'riligiga kafolat berilishi

kalitlarni butunligini ta'minlanishi

kalitni raqamli sertifikat bilan maxfiylikini ta'minlanishi

Correct1

[Question]

Ochiq kalitni taqsimlash jarayoni qaysi tizimga tegishli

ochiq kalitlar infratuzilmasiga

autentifikatsiya tizimlariga

simmetrik kriptotizimlarga

identifikatsiya tizimlariga

Correct1

[Question]

Ochiq kalitni identifikatsiyalash jarayoni qaysi tizimga

tegishli

ochiq kalitlar infratuzilmasiga

identifikatsiya tizimlariga

autentifikatsiya tizimlariga

simmetrik kriptotizimlarga

Correct1

[Question]

Ochiq kalitlar infratuzilmasi nimalarni ta'minlaydi?

ochiq kalitni identifikatsiyalash va uni taqsimlashni

maxfiy kalitni identifikatsiyalash va uni taqsimlashni

ochiq kalitni identifikatsiyalash va uni saqlash

maxfiy kalitni identifikatsiyalash va uni saqlash

Correct1

[Question]

Elektron raqamli imzo bo'yicha birinchi standart?

DSS

RSA

DES

AES

Correct1

[Question]

Qanday kriptotizimlarda ochiq kalit kafolati talabi  
qo'yiladi?

ochiq kalitli kriptotizimlarda

bunday kriptotizim mavjud emas

simmetrik kriptotizimlarda

maxfiy kalitli kriptotizimlarda

Correct1

[Question]

Malumotni shifrlash va deshifrlashda turli kalitlardan  
foydalanuvchi algoritmi ko'  
rsating?

RSA

AES

DES

RC4

Correct1

[Question]

Ochiq kalitli kriptotizimlarda kalitlarni boshqarishda  
qanday talab qo'yiladi?

shaxsiy kalit maxfiyligini saqlash hamda ochiq kalit  
kafolati

shaxsiy kalitni generatsiyalash hamda uni maxfiyligini  
saqlash

ochiq kalitni generatsiyalash hamda uni maxfiyligini  
saqlash

ochiq kalit maxfiyligini saqlash hamda maxfiy kalit  
kafolati

Correct1



[Question]

Elliptik egri chiziqda nuqtalarni qo'shish qaysi algoritim bajariladi?

ECDSA

EL-Gamal

DSA

RSA

Correct1

[Question]

El-Gamal asosidagi ERI algoritmida qaysi kalit orqali elektron hujjatga imzo qo'yiladi?

maxfiy kalit orqali

kalit ishlatilmaydi

imzo qo'lda qo'yiladi

ochiq kalit orqali

Correct1

[Question]

El-Gamal asosidagi ERI algoritmida qaysi kalit orqali elektron hujjatga qo'yilgan imzo tekshiriladi?

ochiq kalit orqali

maxfiy kalit orqali

kalit ishlatilmaydi

imzo qo'lda qo'yiladi

Correct1

[Question]

RSA asosidagi ERI algoritmida qaysi kalit orqali elektron hujjatga qo'yilgan imzo tekshiriladi?

ochiq kalit orqali

maxfiy kalit orqali

imzo qo'lda qo'yiladi

kalit ishlatilmaydi

Correct1

[Question]

RSA asosidagi ERI algoritmda qaysi kalit orqali elektron

hujjatga imzo qo'yiladi?

maxfiy kalit orqali

ochiq kalit orqali

kalit ishlatilmaydi

imzo qo'lda qo'yiladi

Correct1

[Question]

El-Gamal shifrlash algoritmda qaysi parametrlar ochiq

holda e'lon qilinadi?

p tub son hamda p modul bo'yicha birlamchi ildiz g

p va g tub sonlarni( $p > g$ )

p va g toq sonlarni( $p > g$ )

p va g juft sonlarni( $p > g$ )

Correct1

[Question]

Diffie-Hellman algoritmda qaysi parametrlar ochiq holda

e'lon qilinadi?

p va g tub sonlarni( $p > g$ )

p tub sonni

p va g toq sonlarni( $p > g$ )

p va g juft sonlarni( $p > g$ )

Correct1

[Question]

Evklidning kengaytirilgan algoritmidan RSA shifrlash

algoritmining qaysi parametrlar

i hisoblashda foydalaniladi?

maxfiy kalitni

ochiq kalitni

tub sonlarni

modul qiymatini

Correct1

[Question]

Elliptik egri chiziqda diskret logarifmlash muammosiga

asoslangan algoritmni ko'rsat

ing?

ECDSA

El-Gamal

DSA

RSA

Correct1

[Question]

Faktorlash muammosiga asoslangan algoritmni

ko'rsating?

RSA

El-Gamal

DSA

ECDSA

Correct1

[Question]

RSA algoritmda maxfiy kalitni hisoblashda qaysi

algoritmdan foydalanish mumkin?

Evklidning kengaytirilgan algoritmidan

qoldiqlar haqidagi Xitoy teoremasidan

parameter bo'yicha darajaga oshirishdan

Pohlig-Hellman algoritmidan

Correct1

[Question]

Diskret logarifm murakkabligini bartaraf etishda PohligHellman algoritmda yana qa

nday qo'shimcha usuldan foydalanadi?

qoldiqlar haqidagi Xitoy teoremasidan

Evklid algoritmidan

kengaytirilgan Evklid algoritmidan

parameter bo'yicha darajaga oshirishdan

Correct1

[Question]

Qoldiqlar haqidagi Xitoy teoremasidan qaysi algoritmda

foydalaniladi?

Pohlig-Hellman algoritmda

Pollard algoritmda

RSA algoritmda

El-Gamal algoritmda

Correct1

[Question]

El-Gamal algoritmidagi matematik murakkablikni qanday  
usul orqali bartaraf qilish m  
umkin?

Pohlig-Hellman usulu

Pollard usuli

Xitoy teoremasi

El-Gamal usuli

Correct1

[Question]

Pohlig-Hellman usuli qanday turdagi matematik  
murakkablikni yechishda foydalaniladi

?

diskret logarifmlash murakkabligini

faktorgirash murakkabligini

elliptik egrzi chiziqda faktorgirash murakkabligini

daraja parameter murakkabligini

Correct1

[Question]

Diskret logarifmlash muammosini bartaraf etuvchi usul  
keltirilgan qatorni ko'rsatin

g?

Pohlig-Hellman usuli

Pollard usuli

Xitoy teoremasi

RSA usuli

Correct1

[Question]

RSA algoritmidagi matematik murakkablikni qanday usul  
orqali bartaraf qilish mumkin

?

Pollard usuli

Xitoy teoremasi

Pohlig-Hellman usuli

RSA usuli

Correct1

[Question]

Pollard usuli qanday turdagi matematik murakkablikni yechishda foydalaniladi?

faktorlash murakkabligini

diskret logarifmlash murakkabligini

elliptik egrzi chiziqda diskret logarifmlash murakkabligini

elliptik egrzi chiziqda faktorlash murakkabligini

Correct1

[Question]

Faktorlash muammosini bartaraf etuvchi usul keltirilgan qatorni ko'rsating?

Pollard usuli

Xitoy teoremasi

Pohlig-Hellman usulu

RSA usuli

Correct1

[Question]

Elliptik egri chiziqqa asoslangan Diffie Hellman algoritmi qanda matematik murakkab

likka asoslanagan?

Elliptik egri chiziqda diskret logarifmlash murakkabligiga asosla

Diskret logarifmlash murakkabligiga asoslangan

Elliptik egri chiziqda nuqtlarni ikkilantirish

murakkabligiga aso

Elliptik egri chiziqda nuqtalarni qo'shish murakkabligiga asoslan

Correct1

[Question]

O'zDSt ERI standartida,  $R$  - parametr e'lon qilinishi

qanday bo'ladi?

maxfiy xolatda e'lon qilinadi

ochiq holatda e'lon qilinadi

har bir tomon o'ziga alohida hisoblaydi

$R$  parametrdan foydalanmaydi

Correct1

[Question]

7 soni bilan o'zaro tub bo'lgan sonlarni ko'rsating?

2,3,6

14,2,5

1,7,5

6,21,2

Correct1

[Question]

RSA algoritmidagi  $p=3$ ,  $q=11$ ,  $e=3$  bo'lganda maxfiy kalitni qiymati topilsin:  $e \cdot d \equiv 1 \pmod{\varphi(N)}$

7

6

8

5

Correct1

[Question]

Faktorlash muammosini yechishning Pollard algoritmidagi dastlabki tub ko'paytuvchi to

pilgandan keyin qanday shart bajarilsa hisoblash

tugatiladi?

$N/d$  hisoblanadi, agar natija tub bo'lsa hisoblash tugatiladi

$N/d$  hisoblanadi, agar natija tub bo'lmasa hisoblash

tugatiladi

$d$  hisoblanadi, agar natija tub bo'lsa hisoblash tugatiladi

$d$  hisoblanadi, agar natija tub bo'lmasa hisoblash

tugatiladi

Correct1

[Question]

O'zDSt 1092:2009 ERI standarti nechta algoritmdan iborat?

2 ta

3 ta

4 ta

1 ta asosiy

Correct1

[Question]

"A" va "B" foydalanuvchilar o'rtasida ma'lumot almashinishida qanday buzilishlar bo'lishi mumkin?

rad etish, modifikatsiyalash, soxtalashtirish, takrorlash  
modifikatsiyalash, soxtalashtirish, maxfiylashtirish, takrorlash

rad etish, modifikatsiyalash, soxtalashtirish, maxfiylashtirish

rad etish, modifikatsiyalash, soxtalashtirish, maxfiylashtirish,

Correct1

[Question]

"A" va "B" foydalanuvchilar o'rtasida elektron ma'lumot almashinishida "rad etish"

qoida buzilishi qanday amalga oshiriladi?

"A" foydalanuvchi yuborgan ma'lumotini yuborganligini rad etishi

"A" foydalanuvchi ma'lumotini qabul qilganligini rad etishi

"A" foydalanuvchini o'rtada turgan odam tomonidan o'zgartirilganl

"A" foydalanuvchi yuborgan ma'lumotini yubormaganligini rad etish

Correct1

[Question]

ERI qaysi xususiyatni taminlamaydi?

Konfidensiallikni

Rad etishni oldini olishni

Yaxlitlikni

Ma'lumot egasi shaxsini ko'rsatishni

Correct1

[Question]

Ochiq kalitli kriptotizimlarga asoslangan ERI algoritmidaxesh funksiyaning roli qanday?

ma'lumotni yaxlitligini tekshirishda foydalaniladi

ma'lumotni maxfiyligini ta'minlashda foydalaniladi

ma'lumotni deshifrlashda foydalaniladi

ma'lumotni kim tomonidan yuborilganini tekshirishda  
foydalaniladi

Correct1

[Question]

"A" va "B" foydalanuvchilar ma'lumot almashmoqchi,

"B" foydalanuvchi elektron hujja

tga imzo qo'yish uchun qaysi kalitdan foydalanadi?

"B" foydalanuvchini o'zining maxfiy kalitidan

"A" foydalanuvchining maxfiy kalitidan

"B" foydalanuvchi o'zining ochiq kalitidan

"A" foydalanuvchining ochiq kalitidan

Correct1

[Question]

"A" va "B" foydalanuvchilar ma'lumot almashmoqchi,

"A" foydalanuvchi elektron hujja

tga imzo qo'yish uchun qaysi kalitdan foydalanadi?

"A" foydalanuvchini o'zining maxfiy kalitidan

"B" foydalanuvchining maxfiy kalitidan

"A" foydalanuvchi o'zining ochiq kalitidan

"B" foydalanuvchining ochiq kalitidan

Correct1

[Question]

"A" va "B" foydalanuvchilar ma'lumot almashmoqchi,

"B" foydalanuvchi qabul qilgan m

a'lumotni imzosini tekshirishda qaysi kalitdan

foydalanadi?

"A" foydalanuvchining ochiq kalitidan

"A" foydalanuvchining maxfiy kalitidan

"B" foydalanuvchi o'zining ochiq kalitidan

"B" foydalanuvchini o'zining maxfiy kalitidan

Correct1

[Question]

"A" va "B" foydalanuvchilar ma'lumot almashmoqchi,



"A" foydalanuvchi "B" tomondan qabul qilgan ma'lumotni imzosini tekshirishda qaysi kalitdan foydalanadi?

"B" foydalanuvchining ochiq kalitidan

"B" foydalanuvchining maxfiy kalitidan

"A" foydalanuvchi o'zining ochiq kalitidan

"A" foydalanuvchini o'zining maxfiy kalitidan

Correct1

[Question]

Ochiq kalitli kriptotizimlarga asoslangan kalitlarni

taqsimlash Diffie-Hellman algo

ritmi ishlash prinsipi qanday?

umumiy maxfiy kalitni hosil qilishga asoslangan

ochiq va yopiq kalitlar juftini hosil qilishga asoslangan

maxfiy kalitni uzatishni talab etmaydigan prinsipga

asoslangan

ochiq kalitlarni hosil qilishga asoslangan

Correct1

[Question]

Ochiq kalitli El-Gamal shifrlash algoritmida ochiq kalit

qanday hisoblanadi?

$y = g^a \pmod{p}$ , bu yerda  $g$ -birlamchi ildiz,  $a$ -maxfiy kalit,  $p$ -tub

$y = g^a \pmod{p}$ , bu yerda  $g$ -soni  $(p-1)$  dan kichik butun son,  $a$ -maxfiy

$y = g^a \pmod{p}$ , bu yerda  $g$ -soni  $p$  dan kichik butun son,  $a$ -maxfiy

$y = g^a \pmod{p}$ , bu yerda  $g$ -soni  $(p-1)$  bilan o'zaro tub bo'lgan butun

Correct1

Qanday funksiyalar asosiy akslantirishlar deyiladi

Aralashtirish va tarqatish xususiyatlariga ega bo'lgan

funksiyalar

Shifr ... :Kalitdan foydalangan holda almashtirish uchun

amalga oshiriladigan qayta almashtirishlar majmui

ochiq ma'lumotni shifrlash va deshifrlash jarayonini

tashkil etuvchi amallar majmui bo'lib, alifbo belgilarini

almashtirish ketma ketligidan iborat :Kriptografik tizim

:... shifrlash kaliti noma'lum bo'lgan holda shifrlangan  
ma'lumotni deshifrlashning qiyinlik darajasini belgilaydi  
:Kriptobardoshlilik

Kriptotizimlar qanday turlarga bo'linadi? :Simmetrik va  
asimmetrik kriptotizim

Axborotni aslidan o'zgartirilgan holatga akslantirish  
uslublarini topish va takomillashtirish bilan

shug'ullanadigan fan nima deb ataladi? :Kriptografiya  
DES algoritmidagi dastlabki raund kaliti necha bitga teng?  
:48 bit

DES da dastlabki kalit uzunligi necha bitga teng? :56 bit  
DES da bloklar har birining uzunligi necha bitga teng?  
:32 bit

DES da raundlar soni nechta? 6:40

DES da S blok kanday funktsiya bajaradi? #6 bitli blokni 4  
bitga almashtiradi

DES da blok E kengaytirilishidan so'ng kanday amal  
bajariladi? kalit bilan XOR amali bilan qo'shiladi

DES qaysi tarmog' asosida ishlaydi #Feistel tarmog'i  
asosida

DES da IP jadval qanday ish bajaradi? #Berilgan jadval  
bo'yicha bitlarning o'rnini aralashtiradi

DES da shifrlangan matn bloki necha bitdan iborat  
buladi? :64 bit

DES da S bloklar soni nechta? 14:40

Kriptotizim – bu :shifrlash jarayonini tashkil etuvchi  
barcha amallar majmui

: DES shifrlash algoritmi nechanchi yilda yaratilgan :1976  
yilda

Shifrlash kaliti noma'lum bo'lganda shifrlangan  
ma'lumotni deshifrlash qiyinlik darajasini nima belgilaydi  
:kriptobardoshlilik

Klassik shifrlash algoritmlari necha turga bo'linadi 19:40  
O'rniga qo'yish shifrlash algoritmi nechta turga bo'linadi  
20:40

Ochiq matndagi bitta belgi o'rniga shifr mantdagi bitta belgi mos qo'yilsa, bunday o'rniga qo'yish algoritmi nima deyiladi :bir qiymatli

Shifrlashda ishlatiladigan kalitlar qanday bo'ladi

:simmetrik va asimmetrik

Kriptotahlil bilan shug'ullanuvchi insonlar kimlar?

:kriptoanalitiklar

Agar A alfavit m ta elementdan iborat bo'lsa, u holda A to'plamdagi barcha o'rniga qo'yishlar soni nimaga teng bo'ladi? :m!

Shifrlash algoritmlarida samarali tarqatish akslantirishi uchun, odatda, qanday akslantirishdan foydalaniladi :S blok

Kriptotizim – bu :shifrlash jarayonini tashkil etuvchi barcha amallar majmui

O'rniga qo'yish –almashtirish tarmoqlariga asoslangan shifrlash algoritmi qanday ataladi :SP– tarmoq

AES shifrlash standartining mualliflari kimlar :Ridjmen va Deimen

Barcha simmetrik shifrlash algoritmlari qanday shifrlash usullariga bo'linadi :blokli va oqimli

DES shifrlash algoritmda kalit uzunligi va blok uzunligi mos holda qancha bo'lishi kerak :56 bit, 64 bit

DES shifrlash algoritmi nechta rejimda ishlashi belgilab qo'yilgan :4 ta

Shifrlanuvchi bloklar bir biriga bog'liq bo'lmagan holda alohida shifrlash algoritmi orqali qayta ishlanadigan DES shifrlash algoritmining rejimi qaysi :ECB

DES shifrlash algoritmi qaysi tarmoqqa asoslangan :Feystel tarmog'i

DES shifrlash algoritmda kalitlar fazosi necha bitdan iborat 110:40:00

DES shifrlash algoritmda shifrlanadigan malumotlar bloki necha bit? 102:40:00

DES shifrlash algoritmda shifrlash jarayoni nimalardan iborat? :kiruvchi blok, boshlang'ich almashtirish,16

raundli shifrlash va yakuniy almashtirish

DES shifrlash algoritmda i raundi necha bitli kalitdan

foydalaniladi? 118:40:00

XOR amali qanday amal? :2 modul bo'yicha qo'shish

DES shifrlash algoritmda kengaytirish funksiyasi qanday

vazifani bajaradi? :32 bitli blokni 48 bitli blokka

kengaytiradi

DES shifrlash algoritmi necha rejimda ishlaydi? 18:40

DES shifrlash algoritmi kalitlarni kodlashda qaysi

rejimdan foydalanadi? :ECB rejimi

DES shifrlash algoritmda S bloklar nima uchun

ishlatiladi? :48 bitli blokni 32 bitli blokka aylantirish

uchun

DES shifrlash algoritmda nechta S blok bor? 14:40

Sezar shifrlash usulini ko'rsating. : $(m \cdot k) \bmod 26$  m harf

tartib raqami, k kalit

DES shifrlash algoritmda ochiq matn necha bitdan

bloklarga ajratiladi? 102:40:00

DES shifrlash algoritmda shifrlash funksiyasini hosil

qilishda nimalardan foydalaniladi? :E kengaytirish

funksiyasi, kalit, S bloklardan, P almashtirishdan

Xavfsizlik siyosati quyidagilar asosida yaratiladi

:tashkilot ma'lumot tizimlarining umumiy tavsiflari

asosida

Shiflashtirish so'zining ma'nosi nima? :Shiflashtirish –

almashtirish jarayoni bo'lib, berilgan matn shifrlangan

matn bilan almashtiriladi.

Deshiflashtirish so'zining ma'nosi nima?

:Deshiflashtirish – shiflashtirishga teskari jarayon. Kalit

asosida shifrlangan matn o'z holatiga uzgartiriladi.

Alfavit – bu :axborotni kodlashtirish uchun ishlatiladigan

chekli belgilar to'plami.

Kalit – bu? :kalit – matnlarni shifrlash va deshifrlash

uchun kerak bo'lgan axborot

Simmetrik kriptotizimlarda shifrlash va deshifrlashda

qanday kalit ishlatiladi? :Bir xil kalit

Ochiq kalitli tizimda shifrlash va deshifrlash uchun

qanday kalit ishlatiladi? :ochiq va yopiq

Kriptomustahkamlik – bu :Shifrning deshifrlashga

nisbatan mustahkamligini xarakterlaydi

Axborotni himoyalash maqsadida shifrlashning

effektivligi quydagilarga bog'liq? :Shifrn

kriptomustahkamligi va kalitning sirini saqlashga

Shifrlangan ma'lumot o'qilishi mumkin faqat :Kaliti

berilgan bo'lsa

Shifrlangan xabarning ma'lum qismi va unga mos

keluvchi ochiq matn bo'yicha ishlatilgan shifrlash

kalitining kerakli jarayonlar sonini aniqlash

quyidagilardan iborat :Mumkin bo'lgan kalitlarning

umumiy sonidan kam bo'lmagan

Kalitlarni sezgarsiz o'zgartirish quydagilarga olib kelishi

mumkin :bitta va bir xil kalitdan foydalanganda ham

shifrlangan xabarlar sezilarli darajada o'zgarishga :ga

bo'ladi

Quyidagilar bo'lmasligi kerak :shifrlash jarayonida

muntazam qo'llanadigan kalitlar orasida sodda va

osongina aniqlash mumkin bo'lgan bog'liqlik

Mumkin bo'lgan to'plamlardan olingan har qanday

kalitlar ... ni ta'minlaydi :axborotni ishonchli himoyalash

Simmetrik kriptotizim uchun qanday usullar qo'llaniladi?

:o'rin almashtirish, gammalash, blokli shifrlash

Sezar almashtirishning mazmuni qanday izohlanadi?

:Sezar almashtirish monoalfavitli guruhiga qarashli

Axborotni kodlash uchun foydalaniladigan chekli sondagi

belgilar to'plami ... deb ataladi :Alifbo

Alifboning elementlaridan (belgilaridan) tashkil topgan

tartiblangan tuzilma ... deb ataladi :Matn

Dastlabki ma'lumotni bevosita shifrlash va deshifrlash

uchun zarur manba ... deb ataladi :Kalit

Ochiq matn deb ataluvchi dastlabki ma'lumotni

shifrlangan ma'lumot (kriptogramm holatiga o'tkazish

jarayoni ... deb ataladi :Shifrlash

Shifrlashga teskari bo'lgan jarayon, ya'ni kalit yordamida shifrlangan ma'lumotni dastlabki holatga o'tkazish ... deb ataladi :Deshifrlash

... ochiq ma'lumotni shifrlash va deshimrlash jarayonini tashkil etuvchi amallar majmui bo'lib, alifbo belgilarini almashtirish ketma ketligidan iborat. :Kriptografik tizim ... shifrlash kaliti noma'lum bo'lgan holda shifrlangan ma'lumotni deshimrlashning qiyinlik darajasini belgilaydi. :Kriptobardoshlilik

Quyidagilardan qaysi biri matn jo'natilgan shaxsga qabul qilingan elektron matnning va matnni raqamli imzolovchining haqiqiy yoki nohaqiqiyiligini aniqlash imkonini beradi? :Elektron raqamli imzo

Qaysi kriptotizimda shifrlash uchun ham va deshimrlash uchun ham bir xil kalitdan foydalaniladi? :Simmetrik kriptotizim

... kriptobardoshli kalitlarni ishlab chiqish (yoki yaratish), ularni saqlash, hamda kalitlarni foydalanuvchilar orasida muhofazalangan holda taqsimlash jarayonlarini o'z ichiga oladi. :Kalitlarni taqsimlash va boshqarish

Ochiq kalitli kriptotizimlarda qanday kalitlar foydalaniladi? :ochiq va yopiq kalitlar

Kriptologiya maqsadlari o'zaro qarama qarshi bo'lgan ikkita yo'nalishiga ega. Bular qaysilar? :Kriptografiya va kriptotahlil

Kriptotizimlar ikki qismga bo'linadi. Bular qaysilar? :Simmetrik va asimmetrik kriptotizim

Axborotni aslidan o'zgartirilgan holatga akslantirish uslublarini topish va takomillashtirish bilan shug'ullanadigan fan qaysi? :Kriptografiya

Axborotni muxofaza qilish masalalari bilan shug'ullanadigan fan bo'lib Cryptos maxfiy, logos ilm degan ma'noni anglatadigan fan qaysi? :Kriptologiya Kriptotahlilchilarni maxfiyligi ta'minlangan ma'lumotlarga ega bo'lish, ularni deshimrlash chora tadbirlarini amalga oshirishga bo'lgan hatti harakatlar

(hujumlar)i qaysi turlarga bo'linadi? :faol (aktiv) va faol

bo'lmagan (passiv) hujumlar

Teskarisi mavjud bo'lmagan akslantirishlar qanday

akslantirishlar deyiladi. :Bir tomonlama

Ma'lumotlarni himoyalash deganda nima tushiniladi?

:Ma'lumotlarga ruxsat etilmagan kirishlardan himoyalash

Ma'lumotni qonuniy manbadan olingaligini kafolatlovchi

va oluvchining haqiqiylikini tasdiqlovchi xizmat qanday

nomlanadi? :autentifikatsiya

Zamonaviy kriptografiya qanday bo'limlardan iborat?

:Simmetrik kriptotizimlar; ochiq kalitli kriptotizimlar;

Elektron raqamli imzo; kalitlarni boshqarish

Kriptografik usullardan foydalanishning asosiy

yo'nalishlari nimalardan iborat? :Aloqa kanali orqali

maxfiy axborotlarni uzatish (masalan, elektron pochta

orqali), uzatilyotgan xabarlarni haqiqiylikini aniqlash,

Shifr nima? :Shifrlash va deshifrlashda foydalaniladigan

matematik funktsiyadan iborat bo'lgan kriptografik

algoritm

$12 \cdot 11 \bmod 16 = 15:40$

$13 \cdot 4 \bmod 26 = 5:40$

DES algoritmgaga muqobil bo'lgan algoritmni ko'rsating.

:Uch karrali DES, IDEA, Rijndael

DES algoritmining asosiy muammosi nimada? :kalit

uzunligi 56 bit. Bugungu kunda ushbu uzunlik

algoritmning kriptobardoshlilik uchun yetarli emas

Xabarning autentifikatori sifatida ishlatilishi uchun xesh

funktsiya qanday talablarga mos kelishi kerak?

:Keltirilganlarning barchasiga mos kelishi kerak

MD5 qanday xossalarga ega? :Xesh kodning har bir biti

kirishdagi har bir bitning funktsiyasidir. 128 bitli xesh

kod uchun MD5 nisbatan kuchli xesh funktsiya

hisoblanadi

SHA 1 algoritmining bajarilishi qanday mantiqdan iborat?

:Algoritm kirishda maksimal uzunligi 264 bit bo'lgan

xabarni qabul qilib, chiqishda uzunligi 160 bit bo'lgan

xabarning daydjestini yaratadi

MD5 xesh funktsiya qanaqa xarakteristikaga ega?

:daydjesti uzunligi 128 bit; Blok uzunligi 512 bit;

Iteratsiya soni – 64 (har birida 16 iteratsiya bo'lgan 4 ta

tsikl); Elementar mantiqiy funktsiyalar soni – 4;

Qo'shimcha konstantalar sonu – 64.

SHA 1 xesh funktsiya qanaqa xarakteristikaga ega?

:Daydjesti uzunligi 160 bit; Blok uzunligi 512 bit;

Iteratsiya soni – 80; Elementar mantiqiy funktsiyalar soni

– 3; Qo'shimcha konstantalar sonu – 4.

4 31 mod 32 ? 19:40

21 20mod32? 13:40

SHA 256 xesh funktsiya qanaqa xarakteristikaga ega?

:Xabar uzunligi 264 bit; Blok uzunligi 512 bit; So'z

uzunligi 32 bit; Xabar daydjesti uzunligi 256 bit

SHA 512 xesh funktsiya qanaqa xarakteristikaga ega?

:Xabar uzunligi 2128 bit; Blok uzunligi 1024 bit; So'z

uzunligi 64 bit; Xabar daydjesti uzunligi 512 bit

Nisbatan mashhur bo'lgan xesh funktsiyalarni ko'rsating.

:MD2, MD4, MD5, SHA

Davlat yoki xalqaro standart sifatida ishlatilayotgan blokli

shifrlash algoritmlarini ko'rsating. :DES, GOST28147,

CAST, AES

S box lar nima uchun yaratilgan? :Ochiq matn va

shifrmtn orasidagi bog'liqlikni yuqotish uchun

12 22 mod 32 ? 20:40

... shifrida shifrlanayotgan matn belgilari boshqa alifbo

belgilariga almashadi :o'rniga qo'yish

... shifrida shifrlanayotgan matn belgilari qandaydir

qoidaga asosan shifrlanayotgan matnning boshqa

belgilariga almashadi :o'rin almashtirish

... shifrida shifrlanayotgan matn belgilari shifrnig

gammasi deb ataluvchi qandaydir tasodifiy ketma

ketlikning belgilari bilan qo'shiladi :gammalashtirish

... shifrd shifrlanayotgan matn belgilari analitik qoida

(formul ga asosan almashadi. :analitik almashtirishga



asoslangan

Simmetrik algoritmlarni xavfsizligini ta'minlovchi

omillarni ko'rsating. :uzatilayotgan shifrlangan xabarni

kalitsiz ochish mumkin bo'lmashligi uchun algoritm yetarli

darajada bardoshli bo'lishi lozim, uzatilayotgan xabarni

xavfsizligi algoritmnini maxfiyligiga emas

Kriptotizim quyidagi komponentlardan iborat: :ochiq

matnlar fazosi M, Kalitlar fazosi K, Shifrmatnlar fazosi C,

$E_k : M \rightarrow C$  (shifrlash uchun) va  $D_k : C \rightarrow M$  (deshifrlash

uchun) funktsiyalar

2 5 mod 32 ? 15:40

Serpent, Square, Twofish, RC6 algoritmlari qaysi turiga

mansub? :simmetrik blokli algoritmlar

Rijndael algoritmi S box uzunligi necha bit? 38:40:00

Simmetrik shifrlash algoritmlari blokli deyiladi, agar ...

:shifrlashda ochiq matn fiksirlangan uzunlikdagi

bloklarga bo'linsa

To'g'ri mulohazani tanlang. :Rijndael algoritmi Feistel

tarmog'iga asoslanmagan

Xesh funktsiyani natijasi ... :fiksirlangan uzunlikdagi

xabar

AES algoritmi bloki uzunligi ... bitdan kam bo'lmashligi

kerak. 38:40:00

Zamonaviy kriptografiya qanday bo'limlardan iborat?

:Simmetrik kriptotizimlar; ochiq kalitli kriptotizimlar;

Elektron raqamli imzo; kalitlarni boshqarish

Kriptografik usullardan foydalanishning asosiy

yo'nalishlari nimalardan iborat? :Aloqa kanali orqali

maxfiy axborotlarni uzatish (masalan, elektron pochta

orqali), uzatilyotgan xabarlarni haqiqiylikni aniqlash,

tashuvchilarda axborotlarni shifrlangan ko'rinish

Shifr nima? :Shifrlash va deshifrlashda foydalaniladigan

matematik funktsiyadan iborat bo'lgan kriptografik

algoritm

Himoyalangan yoki xavfsizlikni ta'minlovchi protokol

qanday protokol? :Hech bo'lmaganda bitta xavfsizlik

funksiyasini qo'llab quvvatlashni ta'minlovchi protokol

Protokol xavfsizligi nimalarda o'z ifodasini topadi?

:Xavfsizlikni xarakterlovchi xossalari (maxfiylik, butunlik...) kafolati ta'minlanishida

Kriptografik protokol bu :Bajarilish jarayonida

ishtirokchilar tomonidan kriptografik algoritmlardan foydalanadigan protokol

Tashqaridan kuzatib, xabarlarini bilib olishga va protokol bajarilishini buzishga urinuvchi qanday ataladi :Raqib tomon

Kriptografik protokollarni qanday guruhlash mumkin

:Ishtirokchilar soniga va uzatilayotgan xabar soniga ko'ra

Ishtirokchilar soniga ko'ra kriptografik protokollar

qanday turlarga bo'linadi? : Ikki tomonlama;

Uchtomonlama; Ko'ptomonlama.

S box lar nima uchun yaratilgan? :ochiq matn va

shifmatn orasidagi bog'liqlikni yuqotish uchun

Oqimli shifrlashning mohiyati nimada? :Oqimli shifrlash

birinchi navbatda axborotni bloklarga bo'lishning imkonini

bo'lmagan hollarda zarur, Qandaydir ma'lumotlar oqimini

har bir belgisini shifrlab, boshqa belgilarini kutmasdan

kerakli joyga jo'natish uchun o

Almashtirishlar turiga ko'ra shifrlarni qanday guruhlarga

ajratish mumkin? :o'rniga qo'yish shifri, o'rin

almashtirish shifri, gammalashtirish shifri, analitik

almashtirishga asoslangan shifr

... shifrida shifrlanayotgan matn belgilari boshqa alifbo

belgilariga almashadi :o'rniga qo'yish

... shifrida shifrlanayotgan matn belgilari shifrnin

gammasi deb ataluvchi qandaydir tasodifiy ketma

ketlikning belgilari bilan qo'shiladi :gammalashtirish

... shifrida shifrlanayotgan matn belgilari analitik qoida

(formulaga asosan almashadi :analitik almashtirishga

asoslangan

Simmetrik algoritmlarni xavfsizligini ta'minlovchi

omillarni ko'rsatib. :uzatilayotgan shifrlangan xabarni

kalitsiz ochish mumkin bo'lganligi uchun algoritm yetarli  
darajada bardoshli bo'lishi lozim, uzatilayotgan xabarni  
xavfsizligi algoritmni maxfiyligiga emas

Kriptotizim quyidagi komponentlardan iborat: :ochiq  
matnlar fazosi  $M$ , Kalitlar fazosi  $K$ , Shifmatnlar fazosi  $C$ ,  
 $E_k : M \rightarrow C$  (shifrlash uchun) va  $D_k : C \rightarrow M$  (deshifrlash  
uchun) funktsiyalar

4 31 mod 32 ? 19:40

DES algoritmiga muqobil bo'lgan algoritmni ko'rsating.

:Uch karrali DES, IDEA, Rijndael

DES algoritmining asosiy muammosi nimada? :kalit  
uzunligi 56 bit. Bugungu kunda ushbu uzunlik  
algoritmning kriptobardoshliligi uchun yetarli emas

Simmetrik blokli shifrlash rejimlarini ko'rsating. :ECB  
Electronic Codebook, CBC Cipher Block Chaining, CFB  
Cipher Feedback, OFB Output Feedback

Asimmetrik kriptotizimlar qanday maqsadlarda  
ishlatiladi? :shifrlash, deshifrlash, ERI yaratish va  
tekshirish, kalitlar almashish uchun

Diffi Xellman algoritmining maqsadi nimada?

:algoritmining maqsadi keyinchalik qandaydir simmetrik  
shifrlash algoritmida foydalanish uchun 2 ta  
foydalanuvchilar tomonidan kalitlarni xavfsiz  
almashishida

12 22 mod 32 ? 20:40

Rijndael algoritmi S box uzunligi necha bit? 38:40:00

: Simmetrik shifrlash algoritmlari blokli deyiladi, agar ...

:shifrlashda ochiq matn fiksirlangan uzunlikdagi

bloklarga bo'linsa

To'g'ri mulohazani tanlang. :Rijndael algoritmi Feystel  
tarmog'iga asoslanmagan

Xesh funktsiyani natijasi ... :fiksirlangan uzunlikdagi  
xabar

AES algoritmi bloki uzunligi ... bitdan kam bo'lganligi  
kerak. 38:40:00

2 5 mod32 ? 15:40

MD5 qanday xossalarga ega? :Xesh kodning har bir biti  
kirishdagi har bir bitning funktsiyasidir. 128 bitli xesh  
kod uchun MD5 nisbatan kuchli xesh funktsiya  
hisoblanadi

SHA 1 algoritmining bajarilishi qanday mantiqdan iborat?

:Algoritm kirishda maksimal uzunligi 264 bit bo'lgan  
xabarni qabul qilib, chiqishda uzunligi 160 bit bo'lgan  
xabarning daydjestini yaratadi

MD5 xesh funktsiya qanaqa xarakteristikaga ega?

:daydjesti uzunligi 128 bit; Blok uzunligi 512 bit;  
Iteratsiya soni – 64 (har birida 16 iteratsiya bo'lgan 4 ta  
tsikl); Elementar mantiqiy funktsiyalar soni – 4;  
Qo'shimcha konstantalar sonu – 64.

12 11 mod 16 ? 15:40

RIJNDAEL algoritmi qancha uzunligdagi kalitlarni

qo'llab quvvatlaydi. :128 bitli, 192 bitli, 256 bitli

Identifikasiyalash va autentifikasiyalash bu?

:Foydalanuvchilarni ro'yxatdan o'tkazish tartibi va  
ro'yxatdan o'tish ma'lumotlarini tekshirish tartibi

Blowfish shifrlash algoritmi bloki o'lchami qanday? :64  
bit

Blowfish algoritmi kaliti uzunligi qanday? :O'zgaruvchan

Blowfish algoritmi raund akslantirishlari soni qancha? :16  
marta

Blowfish algoritmi qanday tur kriptotizimga kiradi?

:Simmetrik

Qanday manbaa asosida raund kalitlari yaratiladi? :Krish  
bloki uzunligiga bog'liq holda.

Berilgan algoritmning kriptobardoshliligi nimaga  
asoslangan? :Kalit uzunligiga.

Shifrlash qanday amallar orqali amalga oshiriladi?

:CHEkli maydonda qo'shish mod 232 va mod 2 bo'yicha

DES, GOST 28147 89 algoritmlari shifrlash bloki  
uzunligi qancha? :32 bit;

E kengaytirish funksiyasining mohiyati qanday? :32 bitli

Ri 1 blokni 48 bitli E(Ri 1) blokka akslantiradi;

DES algoritmi Si – bloki vazifasi nimadan iborat? :48

bitli blokni 32 bitli blokka siqishdan iborat;

DES algoritmi dastlabki o'rin almashtirish jadvalining

o'lchami qanday? :8 x 8;

97 tub sonmi? :Tub

Ikkilik sanoq tizimida berilgan 10111 sonini o'nlik sanoq

tizimiga o'tkazing. 23:40

Quyidagi modulli ifodani qiymatini toping.

$(125 \cdot 45) \bmod 10$ . 17:40

Quyidagi modulli ifodani qiymatini toping. (148 14432)

$\bmod 256$ . 77:20:00

Quyidagi ifodani qiymatini toping.  $17 \bmod 11$  17:40

Sonning teskarisini toppish amali qanday algoritm

yordamida amalga oshiriladi? :Kengaytirilgan Yevklid

Multiplikativ teskarilash deb nimaga aytiladi? :Modul

ustida ko'paytirish bo'yicha teskarilash

Sonning o'zi va uning modul multiplikativ teskarisining

ko'paytmasi nechaga teng 21:40

: DES algoritmi shifrlash blokining chap va o'ng qism

bloklarining o'lchami qancha? :CHap qism blok 32 bit,

o'ng qism blok 32 bit;

SHifrlash bloki uzunligi qancha ? :32 bit;

DES algoritmi kalit uzunligi qancha? :56 bit;

: DES algoritmi akslantirish raundlari soni qancha? :16 ta;

DES algoritmida E kengaytirish akslantirishining

mohiyati qanday? :32 bitli kirish blokini 48 bitli raund

kalitiga mod2 maydonda qo'shish uchun 32 bitli blok 48

bitga kengaytiriladi ;

Si – bloklarning vazifasi nimadan iborat? :48 bitli blokni

32 bitli blokka siqishdan iborat;

DES algortimida Bitlar o'rinlarini almashtirilishini

aniqlovchi boshlang'ich jadval o'lchami qanday? :8 x 8;

SHifrlash algoritmi chap va o'ng bloklarining o'lchami

qanday? :CHap blok 32 bit, o'ng blok 32 bit;

Raund kalitlari bitlarini siljitish qanday amalga oshiriladi?

:Raund kalitlari bitlarini siljitish berilgan jadval bo'yicha

hamma raundlar uchun bir xil amalga oshiriladi.

DES algoritmi kaliti uzunligi qancha. :64 bit;

DES algoritmi akslantirishlari raundlari soni qancha? :16;

: Blowfish shifrlash algoritmi bloki o'lchami qancha? :64 bit

: Blowfish algoritmi kaliti uzunligi qancha?

:O'zgaruvchan

Simmetrik shifrlash algoritmi bardoshligi nimaga asoslangan? :Kalit uzunligiga;

Qanday amallar asosida blokli shifrlash akslantirishlari yaratiladi? : mod 2 bo'yicha qo'shish asosida;

Blokli shifrlashning asosiy yutuqlari nimalarda namoyon bo'ladi? :SHifrlangan ma'lumotga ochiq ma'lumotning chastotaviy xususiyatlari o'tmaydi  
O'rniga qo'yish va o'rin almashtirish shifrlarining mohiyatan farqi qanday? :SHifrlangan ma'lumot alfavitida

Oddiy o'rniga qo'yish shifrlari bardoshligi qanday aniqlanadi? :SHifrlangan ma'lumot alfavit belgilarining barcha mumkin bo'lgan holatlari soni bilan

Uzliksiz shifrlashning qanday kriptografik qulaylik va samaradorlik tomonlari bor? :Tezligi yuqori va akslantirishlari apparat qurilmalarda qulay amalga oshirish imkoniyatiga ega

Uzliksiz shifrlashning qanday kriptografik kamchiliklari bor? :Sinxronlash buzilganda shifrlanish xatolari tarqaladi

Uzliksiz shifrlash algoritmlarida siljitish registrlarining qo'llanishini mohiyati nimada? :Tezligi yuqori va akslantirishlarini apparat qurilmalarini amalga oshirish samarali

Xesh funksiya qanday kriptografik masalalarni echishga qo'llaniladi? :To'lalilik (butunlik) masalasini echishga  
Blokli simmetrik kalitli shifrlash algoritmlarining bardoshligi qanday parametr bilan aniqlanadi? :Algoritm kaliti uzunligi bilan

Agar  $a=19$  bo'lsa, u holda unga teskari bo'lgan sonni  
xarakteristikasi 26 bo'lgan maydonda hisoblang. 11:40  
Kriptografiya va kriptotahlil yo'nalishlari mohiyatan  
qanday farqlarga ega? :Kriptografiya yo'nalishi ochiq  
ma'lumot asl holatini yashirish bilan, kriptotahlil  
yo'nalishi esa shifr ma'lumotga mos keluvchi ochiq  
ma'lumotni kalit noma'lum bo'lganda topish masala  
MD5 xesh algoritmi xesh qiymat uzunligi nechchiga  
teng? :128 bit

MD5 xesh algoritmining raundlar soni nechchiga teng?  
18:40

AES shifrlash standartining mualliflari kimlar :Ridjmen  
va Deimen

XOR amali qanday amal? :2 modul bo'yicha qo'shish  
Kalit – bu? :kalit – matnlarni shifrlash va deshifrlash  
uchun kerak bo'lgan axborot

Sonning moduli qaysi matematik ifoda orqali aniqlanadi  
Qoldiqli bo'lish

O'zaro teskari sonlar ko'paytmasi nimaga teng. 0

OpenSSL nima? Secure Sockets Layer (SSL) va  
kriptografiya vositalarini amalga oshiruvchi asosiy  
dasturdir

RC4 qanday algoritm Simmetrik oqimli shifrlash  
algoritmi

A5/1 qanday algoritm Simmetrik oqimli shifrlash  
algoritmi

MD5 algoritmidagi hesh qiymat uzunligi necha bitga teng  
128

Kriptologiya qanday yo'nalishlarga bo'linadi?

#kriptografiya va kriptotahlil

kriptografiya va kriptotizim

kripto va kriptotahlil

kriptoanaliz va kriptotizim

++++

Kriptologiya nima bilan shug'ullanadi?

#maxfiy kodlarni yaratish va buzish ilmi bilan

maxfiy kodlarni buzish bilan

maxfiy kodlarni yaratish bilan

maxfiy kodlar orqali ma'lumotlarni yashirish bilan

++++

Kriptografiya nima bilan shug'ullanadi?

#maxfiy kodlarni yaratish bilan

maxfiy kodlarni buzish bilan

maxfiy kodlar orqali ma'lumotlarni yashirish bilan

shifrlash uslublarini bilmagan holda shifrlangan

ma'lumotni asl holatini topish bilan

++++

Kriptotahlil nima bilan shug'ullanadi?

#maxfiy kodlarni buzish bilan

maxfiy kodlarni yaratish bilan

maxfiy kodlar orqali ma'lumotlarni yashirish bilan

shifrlash uslublarini bilmagan holda shifrlangan

ma'lumotni asl holatini topish bilan

++++

Shifrlash orqali ma'lumotning qaysi xususiyati

ta'minlanadi?

#maxfiyligi

Butunliligi

Ishonchliligi

foydalanuvchanligi

++++

Ochiq kalitli kriptotizimlar kim tomonidan kashf

qilingan?

#U.Diffie va M.Hellman

Rivest va Adlman

Shamir va Rivest

U.Diffie va Rivest

++++

Kriptologiya necha yo'nalishga bo'linadi?

#2

14

16



++++

Kriptologiya so'zining ma'nosi?

#cryptos – maxfiy, logos – ilm

cryptos – kodlash, logos – ilm

cryptos – kript, logos – yashiraman

cryptos – maxfiy, logos – kalit

++++

Ochiq kalitli kriptotizimlar ma'lumotni qanday

xususiyatini taminlaydi?

#maxfiyligini

Butunligini

Foydalanuvchanligini

ma'lumotni autentifikatsiyasini

++++

Kriptotizimlar kalitlar soni bo'yicha necha turga

bo'linadi?

#2

4

6

8

++++

Kriptotizimlar kalitlar soni bo'yicha qanday turga

bo'linadi?

#simmetrik va assimetrik turlarga

simmetrik va bir kalitli turlarga

3 kalitli turlarga

assimetrik va 2 kalitli turlarga

++++

Simmetrik kriptotizimlardagi qanday muammoni ochiq

kalitli kriptotizimlar bartaraf etdi?

#maxfiy kalitni uzatish muammosini

kalitni generatsiyalash muammosini

ochiq kalitni uzatish muammosini

kalitlar juftini hosil qilish muammosini

++++

Ochiq kalitli kriptotizimlarda qanday turdagi kalitlardan

foydalanadi?

#ochiq va maxfiy kalitlardan

maxfiy kalitlar juftidan

maxfiy kalitni uzatishni talab etmaydi

ochiq kalitni talab etmaydi

++++

Assimetrik kriptotizimlarda necha kalitdan foydalaniladi?

#2 ta

3 ta

4 ta

kalit ishlatilmaydi

++++

Kerkxofs printsipli nimadan iborat?

#kriptografik tizim faqat kalit noma'lum bo'lgan

taqdirdagina maxfiylik ta'minlanadi

kriptografik tizim faqat yopiq bo'lgan taqdirdagina

maxfiylik ta'minlanadi

kriptografik tizim faqat kalit ochiq bo'lgan taqdirdagina

maxfiylik ta'minlanadi

kriptografik tizim faqat ikkita kalit ma'lum bo'lgan

taqdirdagina maxfiylik ta'minlanadi

++++

Kalit bardoshliligi bu -?

#eng yaxshi ma'lum algoritm bilan kalitni topish

murakkabligidir

eng yaxshi ma'lum algoritm yordamida yolg'on axborotni

ro'kach qilishdir

nazariy bardoshlilik

amaliy bardoshlilik

++++

Ochiq kalitli kriptotizimlarda nechta kalitdan

foydalanadi?

#Ikkita

Bitta

Uchta

kalitdan foydalanilmaydi

++++

Ochiq kalitli kriptotizimlarda qaysi kalit orqali ma'lumot shifrlanadi?

#ochiq kalit orqali

maxfiy kalit orqali

ma'lumot shifrlanmaydi

ushbu tizimda kalitdan foydalanilmaydi

++++

Ochiq kalitli kriptotizimda, qaysi kalit orqali ma'lumot rasshifrovkalanadi?

#maxfiy kalit orqali

ochiq kalit orqali

ma'lumot shifrlanmaydi

ushbu tizimda kalitdan foydalanilmaydi

++++

Ochiq kalitli kriptotizimlarda asosan qanday turdagi sonlar bilan ishlaydi?

#tub sonlar bilan

kasr sonlar bilan

chekli maydonda kasr sonlar

faqat manfiy sonlar

++++

Qanday sonlar tub sonlar hisoblanadi?

#1 va o'ziga bo'linadigan sonlarlar

barcha toq sonlar

juft bo'lmagan sonlar

2 ga bo'linmaydigan sonlar

++++

Sonlarni tublikka tekshirish algoritmlari nechta sinfga bo'linadi?

#ikkita sinfga

uchta sinfga

bitta sinfga

sinflarga bo'linmaydi

++++

Kriptotahlil nima bilan shug'ullanadi?

#kalit yoki algoritmni bilmagan holda shifrlangan

ma'lumotga mos keluvchi ochiq ma'lumotni topish bilan

ochiq ma'lumotlarni shifrlash masalalarining matematik

uslublari bilan

maxfiy kodlarni yaratish bilan

maxfiy kodlar orqali ma'lumotlarni yashirish bilan

++++

RSA algoritmining mualliflarini ko'rsating

#R. Rayvest, A. Shamir, L. Adleman

Diffi va M. Xellman

R. Rayvest, K. Xellman, L. Adleman

L. Adleman, El Gamal, K. Shnorr

++++

Ochiq kalitli shifrlash algoritmi keltirilgan qatorni toping?

#RSA

AES

DES

RC4

++++

Ochiq kalitli shifrlash algoritmi keltirilgan qatorni toping?

#El-Gamal

AES

DES

RC4

++++

Shifrlash orqali ma'lumotning qaysi xususiyati

ta'minlanadi?

#Maxfiyligi

Butunliligi

Ishonchliligi

Foydalanuvchanliligi

++++

Kriptografiya bu -?

#axborotni o'zgartirish vositalari va usullarini

o'rganadigan fan

axborot mazmunidan beruxsat erkin foydalanishdan

muhofazalash

axborotni buzishning oldini olish

axborot almashtirish vosita va usullari bilan

shug'ullanadigan fan sohasi

++++

Faqat simmetrik algoritm keltirilgan qatorni ko'rsating?

#AES

RSA

El-Gamal

Barcha javoblar to'g'ri

++++

Kriptotizimlar kalitlar soni bo'yicha nechta turga

bo'linadi?

#2

3

4

++++

Kriptotizimlar kalitlar soni bo'yicha qanday turga

bo'linadi?

#simmetrik va assimetrik

simmetrik va bitta kalitli

3 kalitli kriptotizimlar

assimetrik va 2 ta kalitli

++++

Ferma testi qanday turdagi tublikka testlovchi algoritm

hisoblanadi?

#ehtimollik testlar tarkibiga kiruvchi algoritm

aniqlashtirilgan testlar tarkibiga kiruvchi algoritm

taqribiy testlar tarkibiga kiruvchi algoritm

tublikka teslovchi algoritm hisoblanmaydi

++++

Solovey Shtrassen testi qanday turdagi tublikka testlovchi

algoritm hisoblanadi?

#ehtimollik testlar tarkibiga kiruvchi algoritm

aniqlashtirilgan testlar tarkibiga kiruvchi algoritm

taqribiy testlar tarkibiga kiruvchi algoritm

tublikka teslovchi algoritm hisoblanmaydi

++++

Rabbi-Milner testi qanday turdagi tublikka testlovchi

algoritm hisoblanadi?

#ehtimollik testlar tarkibiga kiruvchi algoritm

aniqlashtirilgan testlar tarkibiga kiruvchi algoritm

taqribiy testlar tarkibiga kiruvchi algoritm

tublikka teslovchi algoritm hisoblanmaydi

++++

Sonlarni tublikka tekshiruvchi algoritmlar necha sinfga

bo'linadi?

#2

3

4

5

++++

Sonlarni tublikka tekshiruvchi algoritmlar qanday sinfga

bo'linadi?

#aniqlashtirilgan va ehtimolli testlar

aniqlashtirilgan va taqribiy testlar

taqribiy va ehtimolli testlar

aniqlashtirilgan, ehtimolli va taqribiy testlar

++++

Sonlarni tublikka tekshiruvchi ehtimollikka asoslangan

algoritmlar keltirilgan qatorni ko'rsating?

#Ferma, Solovey Shtrassen, Rabbi-Milner

Ferma, Solovey Shtrassen, Eyler

Eyler, Solovey Shtrassen, Rabbi-Milner

Ferma, Eyler, Rabbi-Milner

++++

Elliptik egriz chiqizlarda nuqtalar usitda qanday ammalar

bajariladi?

#nuqtalarni qo'shish va nuqtalarni ikkilantirish

nuqtalarni qo'shish va nuqtalarni ko'paytirish

nuqtalarni qo'shish va nuqtalarni bo'lish

nuqtalarni ayirish va nuqtalarni ko'paytirish

++++

1 ga va o'ziga bo'linadigan sonlar qanday sonlar

hisoblanadi?

#tub sonlar

murakkab sonlar

toq sonlar

juft sonlar

Elektron hujjat manbaini haqiqiyligini qaysi amal orqali

amalga oshiriladi?

#ERI orqali amalga oshiriladi

shifrlash algoritmi orqali amalga oshiriladi

kodlash orqali amalga oshiriladi

autentifikatsiya orqali amalga oshiriladi

++++

Elektron hujjat yaxlitligini (o'zgarmasligini) tekshirish

qaysi amal orqali amalga oshiriladi?

#ERI orqali amalga oshiriladi

kodlash orqali amalga oshiriladi

shifrlash algoritmi orqali amalga oshiriladi

autentifikatsiya orqali amalga oshiriladi

++++

Elektron hujjatni mualliflikdan bosh tortmasligini qaysi

amal orqali amalga oshiriladi?

#ERI orqali amalga oshiriladi

kodlash orqali amalga oshiriladi

autentifikatsiya orqali amalga oshiriladi

shifrlash algoritmi orqali amalga oshiriladi

++++

Raqamli imzoni shakllantirish muolajasi qaysi algoritmga

tegishli?

#ERI algoritmiga

kodlash algoritmiga

shifrlash algoritmiga

steganografiya algoritmiga

++++

ECDSA-2000 qaysi davlat standarti hisoblanadi?

#AQSH

Rossiya

O'zbekiston

Kanada

++++

O'zDSt 1092:2009 standarti qaysi davlat standarti  
hisoblanadi?

#O'zbekiston

AQSH

Rossiya

Kanada

++++

ГОСТ Р 34.10-94 standarti qaysi davlat standarti  
hisoblanadi?

#Rossiya

O'zbekiston

AQSH

Kanada

++++

Seans kalitli hamda seans kalitsiz rejimlarda ishlidigan  
standartni ko'rsating?

#O'zDSt 1092:2009

ECDSA-2000

ГОСТ Р 34.10-94

DSA

++++

DSA qanday standart hisoblanadi?

#ERI standarti

shifrlash standarti

kodlash standarti

steganografik standart

++++

Ochiq kalitli kriptotizimlar qanday turdagi matematik  
murakkablikka asoslangan algoritmlarga bo'linadi?

#faktorizatsiyalash va diskret logarifmlash algoritmlariga



modulyar arifmetika murakkabligiga asoslangan

algoritmlarga

diskret logarifmlash murakkabligiga asoslangan

algorimtlarga

faktORIZatsiyalash murakkabligiga asoslangan

algorimtlarga

++++

Ochiq kalitli kriptotizimlarning bardoshligini ta'minlashda

qanday murakkab muammo turiga asoslanadi?

#faktorlash, diskret logarifmlash, elliptik egri chiziqda

diskret logarifmlash

faktorlash, diskret logarifmlash

faktorlash, diskret logarifmlash, elliptik egri chiziqda

faktORIZatsiyalash

faktorlash, diskret logarifmlash, modulyar arifmetikaga

++++

Ehtimolli testlar sonlarni tublikka tekshirishda qanday

natijani beradi?

#tekshirilayotgan son tub yoki tubmasligi haqida

ehtimollik bilan javob beradi

tekshirilayotgan son tub yoki tubmasligi haqida

kafolatlangan aniq javob beradi

tekshirilayotgan son tub yoki tubmasligi haqida tasodifiy

ravishda javob beradi

tekshirilayotgan son tub yoki tubmasligini 0 va 1

qiymatlarga qarab javob beradi

++++

Sonlarni tublikka tekshirishning ehtimolli algoritmlariga

quyidagilarning qaysilari kiradi?

#Ferma, Rabbi-Milner, Poklingtong testlari

Rabbi-Milner, Solovey-Shtrassen, Pollard testlari

Ferma, Solovey-Shtrassen, Pollard testlari

Rabbi Milner, Poklington, Pollard testlari

++++

Ochiq kalitli RSA shifrlash algoritmi bardoshliligi qanday

matematik muammo turiga asoslangan?

#faktorlash murakkabligiga

diskret logarifmlash murakkabligiga

elliptik egri chiqizlarda faktorizatsiyalash murakkabligiga

elliptik egri chiziqlarda faktorizatsiyalash murakkabligiga

++++

Ochiq kalitli El-Gamal shifrlash algoritmi qanday

matematik murakkablikka asoslanadi?

#diskret logarifmlash murakkabligiga

faktorlash murakkabligiga

elliptik egri chiziqda diskret logarifmlash murakkabligiga

elliptik egri chiziqda faktorlash murakkabligiga

++++

Diffie-Helman algoritmi qanday matematik

murakkablikka asoslanadi?

#diskret logarifmlash murakkabligiga

faktorlash murakkabligiga

elliptik egri chiziqda diskret logarifmlash murakkabligiga

elliptik egri chiziqda faktorlash murakkabligiga

++++

Diffie-Hellman qanday algoritm hisoblanadi?

#kalitlarni ochiq taqsimlash algoritmi

ochiq kalitli shifrlash algoritmi

diskret logarifmlash murakkabligiga asoslangan shifrlash  
algoritmi

faktorlash murakkabligiga asoslangan kalitlarni ochiq

taqsimlash algoritmi

++++

ERI algoritmlari qanday muolajalardan iborat?

#imzoni shakllantirish, imzoni tekshirish

imzoni shakllantirish, imzo qo'yish va imzoni tekshirish

imzoni shakllantirish va imzo qo'yish

imzo qo'yish

++++

Ochiq kalitli kriptotizimlarda elektron hujjatlarga imzo

qo'yish qaysi kalit orqali amalga oshiriladi?

#shaxsiy kalit orqali

ochiq kalit orqali

imzo qo'yilishi kalitga bog'liq emas

imzo qo'lda qo'yiladi

++++

Ochiq kalitli kriptotizimlarda elektron hujjatlarga

qo'yilgan imzoni tekshirish qaysi kalit orqali amalga

oshiriladi?

#ochiq kalit orqali

maxfiy kalit orqali

imzo qo'yilishi kalitga bog'liq emas

imzo qo'lda qo'yiladi

++++

Diskret logarifmlash murakkabligiga asoslangan algoritm

keltirilgan qatorni ko'rsating?

#Diffie-Hellman, EL-Gamal algoritmi

RSA algoritmi

EL-Gamal algoritmi

Diffie-Hellman algoritmi

++++

Faktorlash murakkabligiga asoslangan algoritm keltirilgan

qatorni ko'rsating?

#RSA

El-Gamal

Diffie-Hellman

DSA

++++

Karlmaykl sonlari qaysi tublikka tekshiruvchi

algoritmida doim bajariladi?

#Ferma testida

Solovey-Shtrassen testida

Eyler testida

Rabbin testida

++++

Ochiq kalitli RSA shifrlash algoritmida maxfiy kalit

qanday topiladi?

# $e \cdot d \equiv 1 \pmod{p \cdot q}$  taqqoslamadan

$$e \cdot d \equiv 1 \pmod{N}$$

$$e \cdot d \equiv 1 \pmod{(p-1)}$$

$$e \cdot d \equiv 1 \pmod{(p-1)(q-1)}$$

++++

Ochiq kalitli RSA shifrlash algoritmidagi qaysi parametrlar

ochiq holda e'lon qilinadi?

#N,e

e

N,d

d

++++

Ochiq kalitli RSA shifrlash algoritmidagi "e" ochiq kalit,

"d" shaxsiy kalit bo'lsa deshifrlash formulasi to'g'ri

ko'rsatilgan qatorni belgilang?

$$M = C^d \pmod{N}$$

$$M = C^d \pmod{(N)}$$

$$M = C^e \pmod{N}$$

$$M = C^e \pmod{(N)}$$

++++

Ochiq kalitli RSA shifrlash algoritmidagi "d" shaxsiy kalit,

"e" ochiq kalit bo'lsa shifrlash formulasi to'g'ri

ko'rsatilgan qatorni belgilang?

$$C = M^e \pmod{N}$$

$$C = M^e \pmod{(N)}$$

$$C = M^d \pmod{(N)}$$

$$C = M^d \pmod{N}$$

++++

Ochiq kalitli El-Gamal shifrlash algoritmidagi "p" tub son

bo'lsa maxfiy kalit qanday tanlanadi?

#(p-1) bilan o'zaro tub bo'lgan (1,p-1) intervaldagi butun son

p bilan o'zaro tub bo'lgan (1,p-1) intervaldagi butun son

(1,p-1) intervaldagi tub son

(p-1) bilan o'zaro tub bo'lgan (1,p) intervaldagi butun son

++++

Ochiq kalitli El-Gamal shifrlash algoritmidagi ochiq kalit

qanday hisoblanadi?

$y = g^a \pmod{p}$ , bu yerda  $g$ -birlamchi ildiz,  $a$ -maxfiy

kalit,  $p$ -tub son

$y = g^a \pmod{p}$ , bu yerda  $g$ -soni  $(p-1)$  dan kichik butun

son,  $a$ -maxfiy kalit,  $p$ -tub son

$y = g^a \pmod{p}$ , bu yerda  $g$ -soni  $p$  dan kichik butun son,  $a$ -maxfiy kalit,  $p$ -tub son

$y = g^a \pmod{p}$ , bu yerda  $g$ -soni  $(p-1)$  bilan o'zaro tub

bo'lgan butun son,  $a$ -maxfiy kalit,  $p$ -tub son

++++

Ochiq kalitli kriptotizimlarga asoslangan kalitlarni

taqsimlash Diffie-Hellman algoritmi ishlash prinsipi

qanday?

#umumiy maxfiy kalitni hosil qilishga asoslangan

ochiq va yopiq kalitlar juftini hosil qilishga asoslangan

maxfiy kalitni uzatishni talab etmaydigan prinsipga

asoslangan

ochiq kalitlarni hosil qilishga asoslangan

++++

"A" va "B" foydalanuvchilar ma'lumot almashmoqchi,

"A" foydalanuvchi "B" tomondan qabul qilgan

ma'lumotni imzosini tekshirishda qaysi kalitdan

foydalanadi?

#"B" foydalanuvchining ochiq kalitidan

"B" foydalanuvchining maxfiy kalitidan

"A" foydalanuvchi o'zining ochiq kalitidan

"A" foydalanuvchini o'zining maxfiy kalitidan

++++

RSA algoritmda  $p=3$ ,  $q=11$ ,  $e=3$  bo'lganda maxfiy kalitni

qiymati topilsin:  $e \cdot d \equiv 1 \pmod{N}$ ?

#7

6

8

5

++++

Faktorlash muammosini bartaraf etuvchi usul keltirilgan

qatorni ko'rsating?

#Pollard usuli

Xitoy teoremasi

Pohlig-Hellman usulu

RSA usuli

++++

Pollard usuli qanday turdagi matematik murakkablikni

yechishda foydalaniladi?

#faktorlash murakkabligini

diskret logarifmlash murakkabligini

elliptik egrzi chiziqda diskret logarifmlash murakkabligini

elliptik egrzi chiziqda faktorlash murakkabligini

++++

RSA algoritmidagi matematik murakkablikni qanday usul

orqali bartaraf qilish mumkin?

#Pollard usuli

Xitoy teoremasi

Pohlig-Hellman usuli

RSA usuli

++++

Diskret logarifmlash muammosini bartaraf etuvchi usul

keltirilgan qatorni ko'rsating?

#Pohlig-Hellman usuli

Pollard usuli

Xitoy teoremasi

RSA usuli

++++

Pohlig-Hellman usuli qanday turdagi matematik

murakkablikni yechishda foydalaniladi?

#diskret logarifmlash murakkabligini

faktorlash murakkabligini

elliptik egrzi chiziqda faktorlash murakkabligini

daraja parameter murakkabligini

++++

Evklidning kengaytirilgan algoritmidan RSA shifrlash

algoritmining qaysi parametrini hisoblashda

foydalaniladi?

#maxfiy kalitni

ochiq kalitni

tub sonlarni

modul qiymatini

++++

Diffie-Hellman algoritmda qaysi parametrlar ochiq holda

e'lon qilinadi?

#p va g tub sonlarni( $p > g$ )

p tub sonni

p va g toq sonlarni( $p > g$ )

p va g juft sonlarni( $p > g$ )

++++

Axborot xavfsizligining pasayishi nimani anglatadi?

#axborot xavfsizligi

ma'lumotlarning tartibsizligi

ma'lumotlarning mas'uliyatsizligi

ichki xavfsizlik

+++++

Tashkilotning iqtisodiy xavfsizligini ta'minlash

muammosining eng muhim tarkibiy qismlaridan biri bu

#Axborot texnologiyalari (IT) va tizimlar (IS) xavfsizligi

Axborot texnologiyalari (IT) xavfsizligi

Axborot tizimlarining xavfsizligi (IS)

Texnik tizimlarning xavfsizligi (TS)

+++++

Axborot tizimlari va texnologiyalarini rivojlantirish, joriy

qilish va ulardan foydalanishning ajralmas qismi

hisoblanadi

#Axborot xavfsizligi

kriptografiya

steganografiya

autentifikatsiya

+++++

Zamonaviy dasturlash texnologiyasi sizni mutlaqo xatosiz

va xavfsiz dasturlarni yaratishga imkon beradimi?

#emas

Ha

noma'lum

savol noto'g'ri

+++++

Huquqiy hujjatlar talablariga yoki ma'lumot egalari

tomonidan o'rnatilgan talablarga muvofiq mulkka tegishli

va himoya qilinishi kerak bo'lgan ma'lumotlar

#himoyalangan ma'lumotlar

maxfiy ma'lumotlar

keraksiz ma'lumotlar

foydali ma'lumotlar

+++++

Axborot egalari bo'lishi mumkin:

#davlat, yuridik shaxs, shaxslar guruhi, yakka shaxs.

davlat xizmatchisi, yuridik shaxs, shaxslar guruhi,

jismoniy shaxs.

davlat, yuridik shaxs, shaxslar guruhi, alohida

aktsiyadorlik jamiyati.

davlat, yuridik shaxs, shaxslar guruhi, alohida kompaniya.

+++++

Axborotni qayta ishlashning avtomatlashtirilgan tizimlari

nima uchun kerak?

#ma'lumotlarni saqlash, qayta ishlash va uzatish uchun

ma'lumotlarni saqlash, yangilash va yashirish uchun

ma'lumotlarni saqlash, qayta ishlash va shifrlash uchun

ma'lumotlarni saqlash, qayta ishlash va tahlil qilish uchun

+++++

Axborot xavfsizligini buzishning potentsial yoki real

xavfini keltirib chiqaradigan shartlar va omillar to'plami

#Tahdid (axborot xavfsizligi)

Maxfiylikni buzish

Hodisa

Hujum

+++++

Axborot xavfsizligiga tahdidning bevosita sababi bo'lgan

sub'ekt (shaxs, moddiy ob'ekt yoki jismoniy hodisa)



#Axborot xavfsizligiga tahdid manbai

Texnik xavfsizlik manbai

Virus hujumining manbasi

Xodimlarning manbasi

+++++

Axborot tizimining xususiyati, unda ishlov beriladigan

axborotga tahdidlarni amalga oshirishga imkon beradi

#Zaiflik (axborot tizimi)

Xaker hujumi

Hodisa

Qayta rasmiylashtirish

+++++

Yashirin yoki mahfiy axborotni amalga oshirish natijasida

shaxs, shaxslar guruhi yoki u mo'ljallanmagan har qanday

tashkilot uchun foydalanish mumkin bo'lgan tahdid

#Maxfiylikka tahdid (oshkor qilish tahdidi)

Butunlik uchun tahdid

Texnik tahdid

Xaker hujumi

+++++

Amalga oshirilishi natijasida ma'lumotlar o'zgartirilishi

yoki yo'q qilinishi mumkin bo'lgan tahdid

#Butunlik uchun tahdid

Virusli hujum xavfi

Tarmoq tahdidi

Texnik tahdid

+++++

Tashkilotni o'z faoliyatida yo'naltiradigan

hujjatlashtirilgan qoidalar, protseduralar, amaliyotlar yoki

axborot xavfsizligi sohasidagi ko'rsatmalar to'plami

#Xavfsizlik siyosati

Davlat siyosati

Korporativ etika

Ko'rsatmalar

+++++

Amalga oshirilishi avtomatlashtirilgan tizim mijozlariga

xizmat ko'rsatishni rad etishga, tajovuzkorlarning o'z  
xohishlariga ko'ra manbalardan ruxsatsiz foydalanishiga  
olib keladigan tahdid hisoblanadi.

#Xizmat tahdidini rad etish (mavjud tahdid)

Texnik muammo

Tizimning favqulodda to'xtashi

Hujum

+++++

Uning maxfiyligi, ochiqqligi va yaxlitligi ta'minlanadigan  
axborot xavfsizligi holati

#Axborot xavfsizligi

Ma'lumot xavfsizligi

Operatsion tizim xavfsizligi

Shaxsiy ma'lumotlar xavfsizligi

+++++

Axborotni himoya qilish usuli

#axborotni himoya qilishning muayyan printsiplari va  
vositalarini qo'llash tartibi va qoidalari.

axborotni texnik himoya qilishning muayyan printsiplari  
va vositalarini qo'llash tartibi va qoidalari.

ma'lum bir algoritmlar va axborot xavfsizligi vositalarini  
qo'llash tartibi va qoidalari.

axborotni himoya qilishning ayrim algoritmlarini qo'llash  
tartibi va qoidalari.

+++++

Apparat, dasturiy ta'minot, dasturiy ta'minot va apparat,  
axborotni himoya qilish uchun mo'ljallangan yoki  
ishlatiladigan materiallar va (yoki) materiallar

#Axborot xavfsizligi vositasi

Axborotni nusxalash vositasi

Axborot uzatish vositasi

Shaxsiy ma'lumotlarni uzatish vositasi

+++++

Axborotni kriptografik o'zgartirish orqali himoya qilish

#kriptografik ma'lumotlarni himoya qilish

antivirus ma'lumotlarini himoya qilish

ma'lumotlarni steganografik himoya qilish

axborotni texnik himoya qilish

+++++

Ruxsat berilgan shaxslarning kirib borishi yoki kirishiga  
to'sqinlik qiladigan vositalar to'plami va tashkiliy choralar  
yordamida axborotni himoya qilish himoya qilinadigan  
obyekt hisoblanadi.

#axborotni jismoniy himoya qilish

axborotni dasturiy himoyasi

antivirus ma'lumotlarini himoya qilish

oddiy ma'lumotlarni himoya qilish

+++++

Muayyan tarmoq tugunini o'chirishga qaratilgan hujum  
turi (Xizmatni rad etish - DoS)

#xizmatdan bosh tortish

"ma'lumotlarga kirishni rad etish"

"ma'lumotlarga kirishni rad etish"

"parolga kirish taqiqlandi"

+++++

Kriptovalyutatsiya atamasini birinchi bo'lib kiritgan  
olimni ko'rsating

#F. Fridman

Aristotel

Shannon

Aliqushchi

+++++

IV asrda "antiscital" dekifrlash qurilmasini kim yaratgan.

Mil. Avv.

#Aristotel

Sokrat

Ptolemey

Spital

+++++

Qaysi olimning kitobida chastota kriptovalyutasi  
to'g'risida birinchi ma'lum eslatma mavjud?

#Al-Kindi

Aristotel

Umar Xayyom

Mirzo Ulug'bek

+++++

Qur'on matni asosida arab tilidagi harflarning chastota  
jadvalini birinchi bo'lib kim aniqlagan?

#Shihab al-Kalkasandi

Umar Xayyom

Mirzo Ulug'bek

Imom Buxoriy

+++++

Axborotni shifrlash va shifrlash usullarini qaysi fan  
rivojlantirmoqda?

#Kriptologiya

Informatika

Matematika

Fizika

+++++

DES shifrlash algoritmi qaysi tarmoqqa asoslangan holda  
ishlaydi?

#Feystel tarmog'iga asoslangan holda

SPN tarmog'iga asoslangan holda

hech qanday tarmoqqa asoslanmaydi

Lai-Massey tarmog'iga asoslangan holda

+++++

Quyida keltirilgan xususiyatlarning qaysilari xesh  
funktsiyaga mos?

#chiqishda fiksirlangan uzunlikdagi qiymatni beradi

chiqishda bir xil qiymatni beradi

kolliziyaga ega

chiqishdagi qiymat bilan kiruvchi qiymatlar bir xil bo'ladi

+++++

Quyida keltirilgan xususiyatlarning qaysilari xesh  
funktsiyaga mos?

#ixtiyoriy olingan har xil matn uchun xesh qiymatlar bir  
xil bo'lmaydi

ixtiyoriy olingan bir xil matn uchun qiymatlar bir xil

bo'lmaydi

ixtiyoriy olingan har xil matn uchun xesh qiymatlar bir xil

bo'ladi

ixtiyoriy olingan har xil xesh qiymat uchun dastlabki

ma'lumotlar bir xil bo'ladi

+++++

DES shifrlash algoritmda har bir raunda necha bitli raund

kalitlaridan foydalaniladi?

#48

56

64

32

+++++

Qaysi hujum turida barcha bo'lishi mumkin bo'lgan

variantlar ko'rib chiqiladi?

#qo'pol kuch hujumi

sotsial injineriya

analitik hujum

chastotalar tahlili

+++++

Ma'lumotlarni autentifikatsiyalash kodlari deb qanday

xesh funksiyalarga aytiladi?

#kalitli xesh funksiyalarga

kalitsiz xesh funksiyalarga

kriptografik bo'lmagan xesh funksiyalarga

kriptografik xesh funksiyalarga

+++++

AES algoritmda raundlar soni nimaga bo'g'liq?

#kalit uzunligiga

kiruvchi blok uzunligiga

foydalanilgan vaqtiga

kiruvchi blok uzunligi va matn qiymatiga

+++++

A5/1 oqimli shifrlash algoritmda registrnlarning surilishi

qanday kattalikka bog'liq?

#maj funksiyasi qiymatiga

kalit qiymatiga

registr uzunligi qiymatiga

hech qanday kattalikka bog'liq emas

+++++

16 raund davom etadigan blokli shifrlash algoritmi

ko'rsating?

#DES

AES

RC4

A5/1

+++++

10 raund davom etadigan blokli shifrlash algoritmi

ko'rsating?

#AES

DES

RC4

A5/1

+++++

Xesh qiymatlarni yana qanday atash mumkin?

#dayjest

funksiya

imzo

raqamli imzo

+++++

Ximoyalanuvchi ma'lumot boshqa bir ma'lumotni ichiga

yashirish orqali maxfiyligini ta'minlaydigan usul qaysi?

#steganografiya

kodlash

shifrlash

autentifikatsiya

+++++

Baytlar kesimida shifrlashni amalga oshiradigan algoritm

keltirilgan qatorni ko'rsating?

#RC4

A5/1

MD5

SHA1

+++++

Kolliziya deb nima nisbatan aytiladi?

#ikkita har xil matn uchun bir xil xesh qiymat mos kelishi

ikkita bir xil matn uchun bir xil xesh qiymat mos kelishi

ikkita har xil matn uchun har xil xesh qiymat mos kelishi

ikkita bir xil matn uchun bir xil xesh qiymat mos

kelmasligiga

+++++

Konfidensiallikni ta'minlash bu -?

#ruxsat etilmagan "o'qishdan" himoyalash

ruxsat etilmagan "yozishdan" himoyalash

ruxsat etilmagan "bajarishdan" himoyalash

ruxsat berilgan "amallarni" bajarish

+++++

Sezar shifrlash algoritmi qaysi turdagi akslantirishga

asoslangan?

#o'rniga qo'yish

o'rin almashtirish

aralash

kompozitsion

+++++

CRC-3 tizimida CRC qiymatini hisoblash jarayonida

ma'lumotga nechta nol biriktiriladi?

#3

6

12

9

+++++

.... kriptotizimni shifrlash va rasshifrovkalash uchun

sozlashda foydalaniladi.

#kalit

ochiq matn

algoritm

alifbo

+++++

CRC-5 tizimida CRC qiymati hisoblash jarayonida  
ma'lumotga nechta nol biriktiriladi?

#5

10

15

20

+++++

Rasshifrovkalash jarayonida kalit va ..... kerak bo'ladi

#shifrmtn

ochiq matn

kodlash

alifbo

+++++

Kriptologiya qanday yo'nalishlarga bo'linadi?

#kriptografiya va kriptotahlil

kripto va kriptotahlil

kriptografiya va kriptotizim

kriptoanaliz va kriptotizim

+++++

Kriptotizimlar kalitlar soni bo'yicha necha turga  
bo'linadi?

#2

6

4

8

+++++

Kriptografiya nima bilan shug'ullanadi?

#maxfiy kodlarni yaratish bilan

maxfiy kodlar orqali ma'lumotlarni yashirish

bilan maxfiy kodlarni buzish bilan

shifrlash uslublarini bilmagan holda shifrlangan

ma'lumotni asl holatini topish bilan

+++++

Kerkxofs printsipi nimadan iborat?

#kriptografik tizim faqat kalit noma'lum bo'lgan



taqdirdagina maxfiylik ta'minlanadi

kriptografik tizim faqat yopiq bo'lgan taqdirdagina

maxfiylik ta'minlanadi

kriptografik tizim faqat ikkita kalit ma'lum bo'lgan

taqdirdagina maxfiylik ta'minlanadi

kriptografik tizim faqat kalit ochiq bo'lgan taqdirdagina

maxfiylik ta'minlanadi

+++++

Shifrlash orqali ma'lumotning qaysi xususiyati

ta'minlanadi?

#maxfiyligi

ishonchliligi

butunliligi

foydalanuvchanligi

+++++

O'rniga qo'yish shifrlash sinfiga qanday algoritmlar

kiradi?

#shifrlash jarayonida ochiq ma'lumot alfavit belgilari

shifr ma'lumot belgilariga almashtiriladigan algoritmlar

shifrlash jarayonida ochiq ma'lumot alfaviti belgilarining

o'rinlar almashtiriladigan algoritmalar

shifrlash jarayonida kalitlarning o'ri almashtiriladigan

algoritmlarga

shifrlash jarayonida o'rniga qo'yish va o'rin almashtirish

akslantirishlarning kombinatsiyalaridan birgalikda

foydalaniladigan algoritmlar

+++++

Kriptologiya necha yo'nalishga bo'linadi?

#2

4

8

6

+++++

Kriptologiya so'zining ma'nosi?

#cryptos – maxfiy, logos – ilm

cryptos – maxfiy, logos – kalit

cryptos – kriptο, logos – yashiraman

cryptos – kodlash, logos – ilm

+++++

O'rniga qo'yish shifrlash algoritmlari necha sinfga  
bo'linadi?

#2

6

4

8

+++++

O'rniga qo'yish shifrlash algoritmlari qanday sinfga  
bo'linadi?

#bir qiymatli va ko'p qiymatli shifrlash

bir qiymatli shifrlash

ko'p qiymatli shifrlash

uzluksiz qiymatli shifrlash

+++++

Kriptologiya nima bilan shug'ullanadi?

#maxfiy kodlarni yaratish va buzish ilmi bilan

maxfiy kodlarni yaratish bilan

maxfiy kodlarni buzish bilan

maxfiy kodlar orqali ma'lumotlarni yashirish bilan

+++++

Ma'lumotlarni kodlash va dekodlashda necha kalitdan  
foydalanadi?

#kalit ishlatilmaydi

3 ta

2 ta

4 ta

+++++

Simmetrik kriptotizimlarda necha kalitdan foydalaniladi?

#1 ta

3 ta

kalit ishlatilmaydi

4 ta

+++++

Kriptotahlil nima bilan shug'ullanadi?

#maxfiy kodlarni buzish bilan

shifrlash uslublarini bilmagan holda shifrlangan

ma'lumotni asl holatini

topish bilan

maxfiy kodlar orqali ma'lumotlarni yashirish bilan

maxfiy kodlarni yaratish bilan shifrlash uslublarini

bilmagan holda shifrlangan ma'lumotni asl holatini topish

bilan

+++++

A5/1 oqimli shifrlash algoritmda dastlabki kalit uzunligi

nechi bitga teng?

#64

192

512

256

+++++

Steganografiya ma'lumotni qanday maxfiylashtiradi?

#maxfiy xabarni soxta xabar ichiga berkitish orqali

maxfiy xabarni kriptografik kalit yordamida shifrlash

orqali

maxfiy xabarni kodlash orqali

maxfiy xabarni shifrlash orqali

+++++

Shifrlash algoritmlari akslantirish turlariga qarab qanday

turlarga bo'linad?

#o'rniga qo'yish, o'rin almashtirish va kompozitsion

akslantirishlarga

o'rniga qo'yish, o'rin almashtirish va surish

akslantirishlariga

o'rniga qo'yish va o'rin almashtirish akslantirishlariga

o'rniga qo'yish, sirush va kompozitsion shifrlash

akslantirishlariga

+++++

Blokli shifrlash algoritmlari arxitekturasini jihatidan qanday

tarmoqlarga bo'linadi?

#Feystel va SP

Feystel va Petri

SP va Petri

Kvadrat va iyerarxik

+++++

Zamonaviy kriptografiya qaysi bo'limlarni o'z ichiga  
oladi?

#simmetrik kriptotizimlar, ochiq kalitli kriptotizimlar,  
elektron raqamli imzo kriptotizimlari, kriptobardoshli  
kalitlarni ishlab chiqish va boshqarish

simmetrik kriptotizimlar, ochiq kalit algoritmiga

asoslangan kriptotizimlar, elektron raqamli imzo

kriptotizimlari, foydalanuvchilarni ro'yxatga olish

simmetrik kriptotizimlar, ochiq kalit algoritmiga

asoslangan kriptotizimlar, elektron raqamli imzo

kriptotizimlari, foydalanuvchilarni identifikatsiya qilish

simmetrik kriptotizimlar, ochiq kalit algoritmiga

asoslangan kriptotizimlar, elektron raqamli imzo

kriptotizimlari, foydalanuvchilarni autentifikatsiyalash

+++++

ARX amali nimalardan iborat?

#add, rotate, xor

add, rotate, mod

add, mod, xor

mod, rotate, xor

+++++

Tasodifiy ketma-ketliklarni generatsiyalashga asoslangan  
shifrlash turi bu?

#oqimli shifrlar

blokli shifrlar

ochiq kalitli shifrlar

assimetrik shifrlar

+++++

Qanday algoritmlarda chiqishda doim fiksirlangan  
uzunlikdagi qiymat chiqadi?

#xesh algoritmlarda

kodlash algoritmlarida

shifrlash algoritmlarida

steganografik algoritmlarda

+++++

Ma'lumotni shifrlash va deshifrlash uchun bir xil kalitdan

foydalanuvchi tizim bu?

#simmetrik kriptotizim

ochiq kalitli kriptotizim

assimetrik kriptotizim

xesh funksiyalar

+++++

Ikki kalitli deyilganda qaysi kriptotizim nazarda tutiladi?

#ochiq kalitli kriptotizim

simmetrik kriptotizim

xesh funksiyalar

MAC tizimlari

+++++

Simmetrik shifrlash algoritmlarida qanday muammo

mavjud?

#kalitni uzatish

kalit generatsiyalash

kalitni yo'q qilish

muammo yo'q

+++++

Sezar shifrlash usuli qaysi akslantirishga asoslangan?

#o'rniga qo'yish

o'rin almashtirish

ochiq kalitli shifrlarga

kombinatsion akslantirishga

+++++

Ma'lumotni uzatishda kriptografik himoya .....

#konfidensiallik va yaxlitlikni ta'minlaydi

konfidensiallik va foydalanuvchanlikni ta'minlaydi

konfidensiallikni ta'minlaydi

foydalanuvchanlik ta'minlaydi va butunlikni

+++++

Butunlikni ta'minlash bu - ?

#ruxsat etilmagan "yozishdan" himoyalash

ruxsat etilmagan "bajarishdan" himoyalash

ruxsat etilmagan "o'qishdan" himoyalash

ruxsat berilgan "amallarni" bajarish

+++++

Shifrlash va deshifrlashda alohida kalitlardan

foydalanuvchi kriptotizimlar bu?

#ochiq kalitli kriptotizimlar

simmetrik kriptotizimlar

bir kalitli kriptotizimlar

xesh funksiyalar

+++++

Agar ochiq ma'lumot shifrlansa, natijasi .... bo'ladi.

#shifrmtn

ochiq matn

noma'lum

kod

+++++

Ochiq kalitli shifrlar axborotni qaysi xususiyatlarini

ta'minlashda foydalaniladi?

#konfidensiallik va yaxlitlik

konfidensiallik va foydalanuvchanlik

foydalanuvchanlik va yaxlitlik

foydalanuvchanlik

+++++

MD5 xesh funksiyasida kiruvchi ma'lumot uzunligi

qanday bitli bloklarga bo'linadi?

#512

1024

2048

4096

+++++

add amalining ma'nosi nima?

#modul asosida qo'shish

XOR amali

surish (siklik surish, mantiqiy surish)

akslantirish

+++++

SHA1 xesh funksiyasida initsializatsiya bosqichida 5 ta  
necha bitli registrlardan foydalanadi?

#32

64

128

256

+++++

O'zbekistonda kriptografiya sohasida faoliyat yurituvchi  
tashkilot nomini ko'rsating?

#"UNICON.UZ" DUK

"O'zstandart" agentligi

Kadastr agentligi

Davlat Soliq Qo'mitasi

+++++

Faqat simmetrik shifrlash algoritmlari nomi keltirilgan  
qatorni ko'rsating?

#AES, A5/1

SHA1, DES

MD5, AES

HMAC, RC4

+++++

HMAC tizimida kalit qiymati blok uzunligiga teng

bo'lganda ma'lumotga qanday biriktiriladi?

#kalit qiymati o'zgartirilmagan holda ma'lumotga

biriktiriladi

kalit qiymati blok uzunligiga teng bo'lguncha nol qiymat

bilan to'ldirilib hosil bo'lgan qiymat ma'lumotga

biriktiriladi

kalitni xesh qiymati hisoblanib, unga blok uzunligiga teng

bo'lguncha nol qiymat qo'shiladi va yangi hosil bo'lgan

qiymat ma'lumotga biriktiriladi

xesh funksiyalarda kalit qiymatida foydalanilmaydi

+++++

DES shifrlash algoritmda rasshifrovkalashda birinchi

raunda qaysi kalitdan foydalaniladi?

#16-raund kalitidan

1-raund kalitidan

1-raunda kalitdan foydalanilmaydi

dastlabki kalitdan

+++++

SHA1 xesh funksiyasida kiruvchi ma'lumot uzunligi

qanday bitli bloklarga bo'linadi?

#512

1024

2048

4096

+++++

AES shifrlash algoritmda blok uzunligi 128, kalit

uzunligi 192 bit bo'lsa raundlar soni nechta bo'ladi?

#12

10

14

6

+++++

AES shifrlash algoritmda nechta akslantirishdan

foydalanadi?

#4

3

2

akslantirishdan foydalanilmaydi

+++++

GSM tarmog'ida foydalaniluvchi shifrlash algoritmi

nomini ko'rsating?

#A5/1

dastlabki kalitdan

AES

DES

+++++

WEP protokolida (Wi-Fi tarmog'ida) foydalaniluvchi



shifrlash algoritmi nomini ko'rsating?

#RC4

DES

SHA1

A5/1

+++++

rotate amalining ma'nosi nima?

#surish (siklik surish, mantiqiy surish)

modul asosida qo'shish

XOR amali

Akslantirish

+++++

SHA1 xesh funksiyasida to'ldirish bitlarini qo'shishda

ma'lumot uzunligi 512 modul bo'yicha qanday son bilan

taqqoslanadigan qilib to'ldiriladi?

#448

1002

988

772

+++++

HMAC tizimida kalit qiymati blok uzunligidan kichik

bo'lganda ma'lumotga qanday biriktiriladi?

#kalit qiymati blok uzunligiga teng bo'lguncha nol qiymat

bilan to'ldirilib hosil bo'lgan qiymat ma'lumotga

biriktiriladi

kalitni xesh qiymati hisoblanib, unga blok uzunligiga teng

bo'lguncha nol qiymat qo'shiladi va yangi hosil bo'lgan

qiymat ma'lumotga biriktiriladi

kalit qiymati o'zgartirilmagan holda ma'lumotga

biriktiriladi

xesh funksiyalarda kalit qiymatida foydalanilmaydi

+++++

Kolliziya hodisasi qaysi turdagi algoritmlarga xos?

#xesh funksiyalar

ochiq kalitli shifrlash algoritmlari

kalitlarni boshqarish tizimlari

simmetrik shifrlash algoritmlari

+++++

AES shifrlash algoritmda shifrlash jarayonida qanday akslantirishdan foydalaniladi?

#SubBytes, ShiftRows, MixColumns va AddRoundKey

SubBytes, ShiftRows va AddRoundKey

SubBytes, MixColumns va AddRoundKey

MixColumns, ShiftRows, SubBytes

+++++

Faqat blokli simmetrik shifrlash algoritmlari nomi keltirilgan qatorni ko'rsating?

#AES, DES

A5/1, RC4

A5/1, MD5

SHA1, RC4

+++++

Vernam shifrlash algoritmda shifr matn  $C=101$  ga, kalit  $K=111$  ga teng bo'lsa shifr matn qiymati qanday bo'ladi?

#010

101

111

110

+++++

Quyidagi ifoda nechta yechimga ega?  $3 \cdot x = 2 \pmod{7}$ .

#bitta yechimga ega

ikkita yechimga ega

yechimga ega emas

uchta yechimga ega

+++++

$143 \pmod{17}$  nechiga teng?

#7

6

5

8

+++++

Blokli shifrlash rejimlari qaysi algoritmlarda qo'llaniladi?

#AES, DES

Sezar, Affin

MD5, SHA1

A5/1, RC4

+++++

MD5 xesh algoritmda nechta 32 bitli statik qiymatdan foydalanadi?

#4

8

12

16

+++++

Sezar shifrlash algoritmda ochiq matn  $M=3$  ga, kalit  $K=7$  ga teng hamda  $p=26$  ga teng bo'sa shifr matn qiymati neciga teng bo'ladi?

#10

16

18

22

+++++

Qaysi xesh algoritmda 64 raund amal bajariladi?

#MD5

MAC

CRC

SHA1

+++++

DES shifrlash standarti qaysi davlat standarti?

#AQSH

Rossiya

Buyuk Britaniya

Germaniya

+++++

Qaysi blokli shifrlash algoritmda raund kalit uzunligi qiymatiga bo'g'liq?

#AES

IDEA

DES

RSA

+++++

A5/1 oqimli shifrlash algoritmda  $x_{18}=1$ ,  $y_{21}=0$ ,  $z_{22}=1$

ga teng bo'lsa kalitni qiymatini toping

#0

1

2

3

+++++

Kolliziya hodisasi deb nimaga aytiladi?

#ikki xil matn uchun bir xil xesh qiymat chiqishi

ikki xil matn uchun ikki xil xesh qiymat chiqishi

bir xil matn uchun ikki xil xesh qiymat chiqishi

bir xil matn uchun bir xil xesh qiymat chiqishi bir xil

matn uchun bir xil xesh qiymat chiqishi

+++++

3 sonini 5 chekli maydonda teskarisini toping?

#2

3

4

5

+++++

Bir qiymatli shifrlash qanday amalga oshiriladi?

#ochiq ma'lumot alfaviti belgilarining har biriga shifr

ma'lumot alfavitining bitta belgisi mos qo'yiladi

ochiq ma'lumot alfaviti belgilarining har biriga shifr

ma'lumot alfavitining ikkita yoki undan ortiq chekli

sondagi belgilari mos qo'yiladi

ochiq ma'lumot alfaviti belgilarining har ikkitasiga shifr

ma'lumot alfavitining ikkita yoki undan ortiq chekli

sondagi belgilari mos qo'yiladi

ochiq ma'lumot alfaviti belgilarining har juftiga shifr

ma'lumot alfavitining bitta belgisi mos qo'yiladi

+++++

DES shifrlash algoritmda raundlar soni nechta?

#16

64

32

128

+++++

DES shifrlash algoritmda kalit uzunligi necha bitga teng?

#56

256

192

512

+++++

RC4 oqimli shifrlash algoritmi asosan qayerda

qo'llaniladi?

#simsiz aloqa vositalaridagi mavjud WEP protokolida

radioaloqa tarmoqlarda

internet trafiklarini shifrlashda

mobil aloqa standarti GSM protokolida

+++++

Xesh funksiyalarga qanday turlarga bo'linadi?

#kalitli va kalitsiz xesh funksiyalarga

kalitli va kriptografik bo'lmagan xesh funksiyalarga

kalitsiz va kriptografik bo'lmagan xesh funksiyalarga

kriptografik va kriptografik bo'lmagan xesh funksiyalarga

+++++

AES shifrlash algoritmda raundlar soni nechaga teng

bo'ladi?

#10, 12, 14

14, 16, 18

18, 20, 22

22, 24, 26

+++++

A5/1 oqimli shifrlash algoritmda har bir qadamda kalit

oqimining qanday qiymatini hosil qiladi?

#bir biti

bir bayti

64 biti

8 bayti

+++++

CRC-4 tizimida CRC qiymatini hisoblash jarayonida  
ma'lumotga nechta nol biriktiriladi?

#4

8

16

12

+++++

Blokli simmetrik shifrlash algoritmlari raund  
funktsiyalarida qanday amallar bajariladi?

#ARX

PRX

XOR

RPT

+++++

CRC-6 tizimida CRC qiymati hisoblash jarayonida  
ma'lumotga nechta nol biriktiriladi?

#6

12

18

24

+++++

Qaysi maxfiylikni ta'minlash usulida kalitdan  
foydalanilmaydi?

#kodlash

shifrlash

autentifikatsiya

steganografiya

+++++

Vernam shifrlash algoritm asosi qaysi mantiqiy  
hisoblashga asoslangan

#XOR

ARX

ROX

XRA

+++++

Chastotalar tahlili kriptotahlil usuli samarali ishlidigan  
algorimtlar keltirilgan qatorni belgilang?

#Sezar, Affin

Vernam

Vijiner

RC4

+++++

Bitlar kesimida shifrlashni amalga oshiradigan algoritm  
keltirilgan qatorni ko'rsating?

#A5/1

SHA1

RC4

MD5

+++++

Ma'lumotni konfidensialligini ta'minlash uchun ..... zarur.

#shifrlash

kodlash

rasshifrovkalash

deshifrlash

+++++

Foydanaluvchanlikni ta'minlash bu-?

#ruxsat etilmagan "bajarishdan" himoyalash

ruxsat etilmagan "yozishdan" himoyalash

ruxsat etilmagan "o'qishdan" himoyalash

ruxsat berilgan "amallarni" bajarish

+++++

Vijiner shifrlash algoritmi qaysi turdagi akslantirishga  
asoslanadi?

#o'rniga qo'yish

o'rin almashtirish

kompozitsion

aralash

+++++

Kompyuter davriga tegishli shifrlarni aniqlang?

#DES, AES shifri

kodlar kitobi

Sezar

Enigma shifri

+++++

.... shifrlar blokli va oqimli turlarga ajratiladi

#simmetrik

ochiq kalitli

klassik

assimetrik

+++++

DES shifrlash algoritmi bu?

#blokli shifrlash algoritmi

oqimli shifrlash algoritmi

ochiq kalitli shifrlash algoritmi

asimetrik shifrlash algoritmi

+++++

Ma'lumotga elektron raqamli imzo qo'yish hamda uni  
tekshirish qanday amalga oshiriladi?

#Ma'umotga raqamli imzo qo'yish maxfiy kalit orqali,  
imzoni tekshirish ochiq kalit orqali amalga oshiriladi

Ma'lumotga raqamli imzo qo'yish ochiq kalit orqali,  
imzoni tekshirish maxfiy kalit orqali amalga oshiriladi

Ma'lumotga raqamli imzo qo'yish maxfiy kalit orqali,  
imzoni tekshirish yopiq kalit orqali amalga oshiriladi

Ma'lumotga raqamli imzo qo'yish hamda uni tekshirish  
maxfiy kalit orqali amalga oshiriladi

+++++

A5/1 oqimli shifrlash algoritmda Z registr uzunligi nechi  
bitga teng?

#23

18

19

20

+++++

Kerkxofs printsipi bo'yicha qanday taxminlar ilgari  
suriladi?



#Kalitdan boshqa barcha ma'lumotlar barchaga ma'lum

Faqat kalit barchaga ma'lum

Barcha parametrlar barchaga ma'lum

Shifrlash kaliti barchaga ma'lum

+++++

Qaysi algoritim har bir qadamda bir bayt qiymatni

shifrlaydi?

#RC4

A5/1

RSA

AES

+++++

A5/1 oqimli shifrlash algoritmida maxfiy kalit necha

registriga bo'linadi?

#3

6

5

4

+++++

AES algoritmi qaysi tarmoq asosida qurilgan?

#SP

Feistel

Petri va SP

Petri

+++++

Elektron raqamli imzo bo'yicha birinchi O'z DSt 1092

qaysi korxona tomonidan ishlab chiqilgan?

#UNICON.UZ

INFOCOM

UZTELECOM

O'zR axborot texnologiyalari va kommunikatsiyalarini

rivojlantirish vazirligi

+++++

AES shifrlash algoritmi nomini kengaytmasini

ko'rsating?

#Advanced Encryption Standard

Advanced Encoding Standard

Advanced Encryption Stadium

Always Encryption Standard

+++++

A5/1 shifrlash algoritmi bu?

#oqimli shifrlash algoritmi

blokli shifrlash algoritmi

assimetrik shifrlash algoritmi

ochiq kalitli shifrlash algoritmi

+++++

RC4 shifrlash algoritmi qaysi turga mansub?

#oqimli shifrlar

blokli shifrlar

ochiq kalitli shifrlar

assimetrik shifrlar

+++++

Xeshlash algoritmlarini ko'rsating?

#SHA1, MD5, O'z DSt 1106

RSA, DSA, El-gamal

DES, AES, Blomfish

O'z DSt 1105, ГОСТ 28147-89, FEAL

+++++

AES shifrlash algoritmi bu?

#blokli shifrlash algoritmi

oqimli shifrlash algoritmi

ochiq kalitli shifrlash algoritmi

asimetrik shifrlash algoritmi

+++++

ARX amali qaysi shifrlash algoritmlarida foydalaniladi?

#Blokli shifrlashda

Ikki kalitli shifrlashda

Assimetrik shifrlashda

Ochiq kalitli shifrlashda

+++++

Kriptotizimlar kalitlar soni bo'yicha nechta turga

bo'linadi?

#2

3

4

5

+++++

A5/1 oqimli shifrlash algoritmda major qiymati hisoblash  
jarayonida, uchinchi (Z) registrning qaysi qiymati  
olinadi?

#z10

z11

z12

z13

+++++

A5/1 oqimli shifrlash algoritmda X registr uzunligi nechi  
bitga teng?

#19

16

17

15

+++++

Qaysi algorimtda har bir qadamda bir bit qiymatni  
shifrlaydi?

#A5/1

RC4

RSA

AES

+++++

Mantiqiy XOR amalining asosi qanday hisoblashga  
asoslangan?

#mod2 bo'yicha qo'shishga

mod2 bo'yicha ko'paytirishga

mod2 bo'yicha darajaga ko'tarishga

mod2 bo'yicha bo'lishga

+++++

Qaysi xesh algoritmda xesh qiymat 128 bitga teng  
bo'ladi?

#MD5

SHA1

CRC

MAC

+++++

Qaysi xesh algoritmda xesh qiymat 160 bitga teng

bo'ladi?

#SHA1

MD5

CRC

MAC

+++++

Faqat AQSH davlatiga tegishli kriptografik standartlar

nomini ko'rsating?

#AES, DES

AES, GOST 28147-89

DES, O'z DST 1105-2009

SHA1, GOST 3412-94

+++++

RC4 shifrlash algoritmi simmetrik turga mansub bo'lsa,

unda nechta kalitdan foydalaniladi?

#1

2

3

4

+++++

A5/1 oqimli shifrlash algoritmda major qiymati hisoblash

jarayonida, birinchi (X) registrning qaysi qiymati olinadi?

#x8

x9

x10

x11

+++++

DES shifrlash algoritmda S-bloklarga kiruvchi qiymatlar

uzunligi necha bitga teng bo'ladi?

#6

12

24

18

+++++

MD5 xesh funksiyasida initsializatsiya bosqichida 4 ta  
necha bitli registrlardan foydalanadi?

#32

64

128

256

+++++

Imitatsiya turidagi hujumlarda ma'lumotlar qanday  
o'zgaradi?

#ma'lumot qalbakilashtiriladi

ma'lumot yo'q qilinadi

ma'lumot ko'chirib olinadi

ma'lumot dublikat qilinadi

+++++

Sezar shifrlash algoritmidan rasshifrovkalash formulasi  
qanday?

# $M = (C - K) \bmod p$

$M = (C + K) \bmod p$

$M = (C * K) \bmod p$

$M = (C / K) \bmod p$

+++++

Faqat xesh funksiyalar nomi keltirilgan qatorni  
ko'rsating?

#SHA1, MD5

SHA1, DES

MD5, AES

HMAC, A5/1

+++++

MD5 xesh funksiyasida chiquvchi qiymat uzunligi  
nechaga teng?

#128

Ixtiyoriy

510

65

+++++

AES shifrlash algoritmi simmetrik turga mansub bo'lsa,  
unda nechta kalitdan foydalaniladi?

#1

2

3

4

+++++

SHA1 xesh funksiyasida initsializatsiya bosqichida nechta  
registrdan foydalanadi?

#5

10

15

20

+++++

MD5 xesh funksiyasida amallar necha raund davomida  
bajariladi?

#64

128

512

256

+++++

DES shifrlash algoritmda S-bloklardan chiqqan qiymatlar  
uzunligi necha bitga teng bo'ladi?

#4

8

12

16

+++++

MD5 xesh funksiyasida initsializatsiya bosqichida nechta  
32 bitli registrdan foydalanadi?

#4

8

12

16

+++++

Faqat oqimli simmetrik shifrlash algoritmlari nomi  
keltirilgan qatorni ko'rsating?

#A5/1, RC4

AES, DES

SHA1, RC4

A5/1, MD5

+++++

SHA1 xesh funksiyasida chiquvchi qiymat uzunligi  
nechaga teng?

#160

Ixtiyoriy

512

256

+++++

O'zgartirish turidagi hujumlarda ma'lumotlar qanday  
o'zgaradi?

#modifikatsiya qilinadi

ma'lumot yo'q qilinadi

ma'lumot dublikat qilinadi

ma'lumot ko'chirib olinadi

+++++

AES standarti qaysi algoritm asoslangan?

#Rijndael

RC6

Twofish

Serpent

+++++

SHA1 xesh funksiyasida amallar nechchi raund davomida  
bajariladi?

#80

128

256

512

+++++

2 lik sanoq tizimida 0101 soniga 1111 sonini 2 modul

bo'yicha qo'shing?

#1010

0101

1001

1111

+++++

AES shifrlash standarti qaysi davlat standarti?

#AQSH

Rossiya

Buyuk Britaniya

Germaniya

+++++

Qaysi algoritmda maj kattaligi ishlatiladi?

#A5/1

RC4

SHA1

MD5

+++++

Qalbakilashtirish hujumi qaysi turdagi hujum turiga

kiradi?

#Immitatsiya

o'zgartirish

Fabrication

modification

+++++

SHA1 xesh funksiyasi qaysi davlat standarti?

#AQSH

Rossiya

Germaniya

Buyuk Britaniya

+++++

Qayday akslantirishdan foydalanilsa chastotalar tahlili

kriptotahlil usuliga bardoshli bo'ladi

#bigram akslantirishidan

o'rniga qo'yish akslantirishidan



o'rin almashtirish akslantirishidan

xech qanday akslantirishdan foydalanish shart emas

+++++

SHA1 xesh algoritmda nechta 32 bitli statik qiymatdan  
foydalanadi?

#5

10

15

20

+++++

A5/1 oqimli shifrlash algoritmda maj(1,0,1) ga teng  
bo'lsa maj kattalik qiymatini toping?

#1

0

2

3

+++++

SHA1 xesh funksiyada 102 bitli ma'lumot berilganda  
to'ldirish bitlari qanday to'ldiriladi?

#bir bit 1, 345 ta 0, ma'lumot uzunligi qiymatining 64  
bitli qiymati bilan

bir bit 1, 345 ta 0, ma'lumot uzunligining dastlabki 64  
bitli qiymati bilan

bir bit 1, 409 ta 0, ma'lumot uzunligi qiymatining 64 bitli  
qiymati bilan

bir bit 1, 409 ta 0, ma'lumot uzunligining dastlabki 64  
bitli qiymati bilan

+++++

Qaysi blokli shifrlash algoritmda 8 ta statik S-box lardan  
foydalaniladi?

#DES

RSA

RC4

A5/1

+++++

Kriptotizimlar kalitlar soni bo'yicha qanday turga

bo'linadi?

#simmetrik va assimetrik turlarga

assimetrik va 2 kalitli turlarga

3 kalitli turlarga

simmetrik va bir kalitli turlarga

+++++

Ko'p qiymatli shifrlash qanday amalga oshiriladi?

#ochiq ma'lumot alfaviti belgilarining har biriga shifr

ma'lumot alfavitining ikkita yoki undan ortiq chekli

sondagi belgilari mos qo'yiladi

ochiq ma'lumot alfaviti belgilarining har ikkitasiga shifr

ma'lumot alfavitining ikkita yoki undan ortiq chekli

sondagi belgilari mos qo'yiladi

ochiq ma'lumot alfaviti belgilarining har biriga shifr

ma'lumot alfavitining bitta belgisi mos qo'yiladi

ochiq ma'lumot alfaviti belgilarining har juftiga shifr

ma'lumot alfavitining bitta belgisi mos qo'yiladi

+++++

A5/1 oqimli shifrlash algoritmi asosan qayerda

qo'llaniladi?

#mobil aloqa standart GSM protokolida

simsiz aloqa vositalaridagi mavjud WEP protokolida

internet trafiklarini shifrlashda

radioaloqa tarmoqlarida

+++++

Assimetrik kriptotizimlarda necha kalitdan foydalaniladi?

#2 ta

3 ta

4 ta

kalit ishlatilmaydi

+++++

AES algoritmidagi shifrlash kalitining uzunligi necha bitga

teng?

#128, 192, 256 bit

128, 156, 256 bit

256, 512 bit

128, 192 bit

+++++

Kalit bardoshliligi bu -?

#eng yaxshi ma'lum algoritm bilan kalitni topish

murakkabligidir

eng yaxshi ma'lum algoritm yordamida yolg'on axborotni

ro'kach qilishdir

amaliy bardoshlilik

nazariy bardoshlilik

+++++

RC4 oqimli shifrlash algoritmida har bir qadamda kalit

oqimining qanday qiymatini hosil qiladi?

#bir baytini

bir bitini

64 bitini

8 baytini

+++++

AES algoritmida nechta akslantirishlardan foydalaniladi?

#4

2

5

6

+++++

Qanday funksiyalarga xesh funksiya deyiladi?

#ixtiyoriy uzunlikdagi ma'lumotni biror fiksirlangan

uzunlikga o'tkazuvchi funksiyaga aytiladi

ma'lumot baytlarini boshqa qiymatlarga almashtiruvchi

funksiyaga aytiladi

ma'lumot bitlarini boshqa qiymatlarga almashtiruvchi

funksiyaga aytiladi

ixtiyoriy uzunlikdagi ma'lumotni bit yoki baytlarini

zichlashtirib beruvchi funksiyaga aytiladi

+++++

Xesh funksiyalar qanday maqsadlarda ishlatiladi?

#ma'lumotni to'liqligini nazoratlash va ma'lumot

manbaini autentifikatsiyalashda

ma'lumot manbaini autentifikatsiyalashda

ma'lumotni butunligini nazoratlashda

ma'lumotni maxfiyligini nazoratlash va ma'lumot

manbaini haqiqiylikini tekshirishda

+++++

Ma'lumotni sakkizlik sanoq tizimidan o'n oltilik sanoq

tizimiga o'tkazish bu?

#kodlash

rasshifrovkalash

yashirish

shifrlash

+++++

A5/1 shifri qaysi turga mansub?

#oqimli shifrlar

blokli shifrlar

ochiq kalitli shifrlar

assimetrik shifrlar

+++++

Qaysi algoritmlar simmetrik blokli shifrlarga tegishli?

#AES, DES

A5/1, AES

Vijiner, DES

Sezar, AES

+++++

Ma'lumotni mavjudligini yashirishni maqsad qilgan bilim

sohasi bu?

#steganografiya

kriptografiya

kodlash

kriptotahlil

+++++

Faqat simmetrik blokli shifrlarga xos bo'lgan atamani

aniqlang?

#blok uzunligi

kalit uzunligi

ochiq kalit

kodlash jadvali

+++++

Quyidagi ta'rif qaysi atamaga tegishli: "maxfiy kodlarni"ni buzish bilan shug'ullanadigan soha-bu?

#kriptotahlil

kripto

kriptologiya

kriptografiya

+++++

Qadimiy davr klassik shifriga quyidagilarning qaysi biri tegishli?

#Sezar

kodlar kitobi

Enigma shifri

DES, AES shifri

+++++

Quyidagi ta'rif qaysi kriptotizimga tegishli: ochiq matnni shifrlashda hamda rasshifrovkalashda mos holda ochiq va maxfiy kalitdan foydalanadi?

#ochiq kalitli kriptotizimlar

maxfiy kalitli kriptotizimlar

simmetrik kriptotizimlar

elektron raqamli imzo tizimlari

+++++

Simmetrik shifrlar axborotni qaysi xususiyatlarini ta'minlashda foydalaniladi?

#konfidensiallik va yaxlitlik

konfidensiallik va foydalanuvchanlik

foydalanuvchanlik va yaxlitlik

foydalanuvchanlik

+++++

Qanday algorimtlar qaytmas xususiyatiga ega hisoblanadi?

#xesh funksiyalar

elektron raqamli imzo algoritmlari

simmetrik kriptotizimlar

ochiq kalitli kriptotizimlar

+++++

Ochiq matn qismlarini takror shifrlashga asoslangan usul

bu?

#blokli shifrlar

oqimli shifrlar

assimetrik shifrlar

ochiq kalitli shifrlar

+++++

Ochiq kalitli shifrlashda deshifrlash qaysi kalit asosida

amalga oshiriladi?

#shaxsiy kalit

ochiq kalit

kalitdan foydalanilmaydi

umumiy kalit

+++++

Quyidagi ta'rif qaysi atamaga tegishli: "maxfiy

kodlarni"ni yaratish bilan shug'ullanadigan soha-bu?

#kriptografiya

kriptologiya

kriptotahlil

kripto

+++++

Simmetrik kriptotizimlarning asosiy kamchiligi bu?

#kalitni taqsimlash zaruriyati

kalitlarni esda saqlash murakkabligi

shifrlash jarayonining ko'p vaqt olishi

algoritmning xavfsiz emasligi

+++++

Kriptotizimni boshqaradigan vosita?

#kalit

algoritm

stegokalit

kriptotizim boshqarilmaydi

+++++

Quyidagi ta'rif qaysi kriptotizimga tegishli:ochiq matnni

shifrlashda hamda rasshifrovkalashda bitta maxfiy

kalitdan foydalaniladi?

#simmetrik kriptotizimlar

nosimmetrik kriptotizimlar

ochiq kalitli kriptotizimlar

assimetrik kriptotizimlar

+++++

Kerxgofs prinsipiga ko'ra kriptotizimning to'liq xavfsiz

bo'lishi faqat qaysi kattalik nomalum bo'lishiga

asoslanishi kerak?

#kalit

protokol

shifrmavn

Algoritm

+++++

Xesh funksiyalar nima maqsadda foydalaniladi?

#ma'lumotlar yaxlitligini ta'minlashda

ma'lumot egasini autentifikatsiyalashda

ma'lumot maxfiyligini ta'minlashda

ma'lumot manbaini autentifikatsiyalashda

+++++

Chastotalar tahlili hujumi qanday amalga oshiriladi?

#shifr matnda qatnashgan harflar sonini aniqlash orqali

shifr matnda eng kam qatnashgan harflarni aniqlash orqali

ochiq matnda qatnashgan harflar sonini aniqlash orqali

ochiq matnda eng kam qatnashgan harflarni aniqlash

orqali

+++++

Xesh funksiyaga tegishli bo'lgan talabni aniqlang?

#bir tomonlama funksiya bo'lishi

chiqishda ixtiyoriy uzunlikda bo'lishi

turli kirishlar bir xil chiqishlarni akslantirishi

kolliziyaga bardoshli bo'lmasligi

+++++

RC4 shifrlash algoritmi bu?

#oqimli shifrlash algoritmi

ochiq kalitli shifrlash algoritmi

blokli shifrlash algoritmi

asimetrik shifrlash algoritmi

+++++

A5/1 shifrlash algoritmi simmetrik turga mansub bo'lsa,  
unda nechta kalitdan foydalaniladi?

#1

2

3

4

+++++

Qaysi algoritmda, algoritmning necha round bajarilishi  
ochiq matn uzunligiga bog'liq?

#A5/1

MD5

HMAC

SHA1

+++++

Simmetrik va ochiq kalitli kriptotizimlar asosan nimasi  
bilan bir biridan farq qiladi?

#kalitlar soni bilan

matematik murakkabligi bilan

farq qilmaydi

biri maxfiylikni ta'minlasa, biri butunlikni ta'minlaydi

+++++

A5/1 oqimli shifrlash algoritmda major qiymati hisoblash  
jarayonida, ikkinchi (Y) registrning qaysi qiymati olinadi?

#y10

y11

y12

y13

+++++

Kalitli xesh funksiyalar qanday turdagi hujumlardan  
himoyalaydi?

#imitatsiya va o'zgartirish turidagi hujumlardan

ma'lumotni oshkor qilish turidagi hujumlardan



DDOS hujumlaridan

foydalanishni buzishga qaratilgan hujumlardan

+++++

Sezar shifrlash algoritmida shifrlash formulasi qanday?

# $C=(M+K) \bmod p$

$C=(M-K) \bmod p$

$C=(M*K) \bmod p$

$C=(M/K) \bmod p$

+++++

A5/1 oqimli shifrlash algoritmida Y registr uzunligi nechi

bitga teng?

#22

20

19

21

+++++

Kalitli xesh funksiyalardan foydalanish nimani

kafolatlaydi?

#fabrikatsiyani va modifikatsiyani oldini oladi

ma'lumot yo'q qilinadi

ma'lumot dublikat qilinadi

ma'lumot ko'chirib olinadi

+++++

DES shifrlash algoritmi simmetrik turga mansub bo'lsa,

unda nechta kalitdan foydalaniladi?

#1

2

3

4

+++++

AES tanlovi g'olibi bo'lgan algoritm nomini ko'rsating?

Rijndael

IDEA

Blowfish

Twofish

+++++

AES shifrlash algoritmda 128 bitli ma'lumot bloki

qanday o'lchamdagi jadvalga solinadi?

#4x4

4x6

6x4

6x6

+++++

A5/1 oqimli shifrlash algoritmda maj(1,0,1) ga teng

bo'lsa qaysi registrlar suriladi?

#birinchi va uchunchi registrlar suriladi

faqat ikkinchi registr suriladi

birinchi va ikkinchi registrlar suriladi

faqat birinchi resgistr suriladi

+++++

GSM tarmog'ida foydalaniluvchi shifrlash algoritmi

nomini ko'rsating?

#A5/1

DES

RC4

AES

+++++

HMAC tizimida kalit qiymati blok uzunligidan katta

bo'lganda ma'lumotga qanday biriktiriladi?

#kalitni xesh qiymati hisoblanib, unga blok uzunligiga

teng bo'lguncha nol qiymat qo'shiladi va yangi hosil

bo'lgan qiymat ma'lumotga biriktiriladi

kalit qiymati blok uzunligiga teng bo'lguncha nol qiymat

bilan to'ldirilib hosil bo'lgan qiymat ma'lumotga

biriktiriladi

kalit qiymati o'zgartirilmagan holda ma'lumotga

biriktiriladi

xesh funksiyalarda kalit qiymatidan foydalanilmaydi

+++++

Qaysi xesh algoritmda 80 raund amal bajariladi?

#SHA1

CRC

MD5

MAC

+++++

Affin shifrlash algoritmda  $a=2$ ,  $b=3$ ,  $p=26$  hamda ochiq matn  $x=4$  ga teng bo'lsa, shifr matn qiymatini toping?

#11

27

41

31

+++++

MD5 xesh funksiyada 48 bitli ma'lumot berilganda to'ldirish bitlari qanday to'ldiriladi?

#bir bit 1, 399 ta 0, ma'lumot uzunligi qiymatining 64

bitli qiymati bilan

bir bit 1, 399 ta 0, ma'lumot uzunligining dastlabki 64

bitli qiymati bilan

bir bit 1, 463 ta 0, ma'lumot uzunligi qiymatining 64 bitli

qiymati bilan

bir bit 1, 463 ta 0, ma'lumot uzunligining dastlabki 64

bitli qiymati bilan

+++++

AES shifrlash algoritmda ochiq matn bilan dastlab qanday amal bajariladi?

#ochiq matn dastlabki kalit bilan XOR amali bajariladi

ochiq matn birinchi raund kalit bilan XOR amali

bajariladi

ochiq matn ustida dastlab SubBytes akslantirishi amali

bajariladi

ochiq matn ustida dastlab ShiftRows akslantirishi amali

bajariladi

+++++

Vernam shifrlash algoritmda ochiq matn  $M=101$  ga, kalit  $K=111$  ga teng bo'lsa shifr matn qiymati qanday bo'ladi?

#010

101

111

?Konfidensiallikni ta minlash bu - ?

+ruxsatsiz o qishdan himoyalash.

-ruxsatsiz yozishdan himoyalash.

-ruxsatsiz bajarishdan himoyalash.

-ruxsat etilgan amallarni bajarish.

?Foydalanuvchanlikni ta minlash bu - ?

+ruxsatsiz bajarishdan himoyalash.

-ruxsatsiz yozishdan himoyalash.

-ruxsatsiz o qishdan himoyalash.

-ruxsat etilgan amallarni bajarish.

?Yaxlitlikni ta minlash bu - ?

+ruxsatsiz yozishdan himoyalash.

-ruxsatsiz o qishdan himoyalash.

-ruxsatsiz bajarishdan himoyalash.

-ruxsat etilgan amallarni bajarish.

?Jumlani to ldiring. Hujumchi kabi fikrlash ... kerak.

+bo lishi mumkin bo lgan xavfni oldini olish uchun

-kafolatlangan amallarni ta minlash uchun

-ma lumot, axborot va tizimdan foydalanish uchun

-ma lumotni aniq va ishonchli ekanligini bilish uchun

?Jumlani to ldiring. Tizimli fikrlash ... uchun kerak.

+kafolatlangan amallarni ta minlash

-bo lishi mumkin bo lgan xavfni oldini olish

-ma lumot, axborot va tizimdan foydalanish

-ma lumotni aniq va ishonchli ekanligini bilish

?Axborot xavfsizligida risk bu?

+Manbaga zarar keltiradigan ichki yoki tashqi zaiflik ta  
sirida tahdid qilish ehtimoli.

-U yoki bu faoliyat jarayonida nimaga erishishni  
xoxlashimiz.

-Tashkilot uchun qadrli bo lgan ixtiyoriy narsa.

-Tizim yoki tashkilotga zarar yetkazishi mumkin bo lgan  
istalmagan hodisa.

?Axborot xavfsizligida tahdid bu?

+Aktivga zarar yetkazishi mumkin bo lgan istalmagan

hodisa.

-Noaniqlikning maqsadlarga ta siri.

-U yoki bu faoliyat jarayonida nimaga erishishni xohlashimiz.

-Tashkilot uchun qadrli bo lgan ixtiyoriy narsa.

?Axborot xavfsizligida aktiv bu?

+Tashkilot yoki foydalanuvchi uchun qadrli bo lgan ixtiyoriy narsa.

-Tizim yoki tashkilotga zarar yetkazishi mumkin bo lgan istalmagan hodisa.

-Noaniqlikning maqsadlarga ta siri.

-U yoki bu faoliyat jarayonida nimaga erishishni xohlashimiz.

?Axborot xavfsizligida zaiflik bu?

+Tahdidga sabab bo luvchi tashkilot aktivi yoki boshqaruv tizimidagi nuqson.

-Tashkilot uchun qadrli bo lgan ixtiyoriy narsa.

-Tizim yoki tashkilotga zarar yetkazishi mumkin bo lgan istalmagan hodisa.

-Noaniqlikning maqsadlarga ta siri.

?Axborot xavfsizligida boshqarish vositasi bu?

+Natijasi zaiflik yoki tahdidga ta sir qiluvchi riskni o zgartiradigan harakatlar.

-Bir yoki bir nechta tahdidga sabab bo luvchi tashkilot aktivi yoki boshqaruv tizimidagi kamchilik.

-Tashkilot uchun qadrli bo lgan ixtiyoriy narsa.

-Tizim yoki tashkilotga zarar yetkazishi mumkin bo lgan istalmagan hodisa.

?Har qanday vaziyatda biror bir hodisani yuzaga kelish ehtimoli qo shilsa ....

+risk paydo bo ladi.

-hujum paydo bo ladi.

-tahdid paydo bo ladi.

-aktiv paydo bo ladi.

?Jumlani to ldiring. Denial of service (DOS) hujumi axborotni .... xususiyatini buzushga qaratilgan.

+foydalanuvchanlik

-butunlik

-konfidensiallik

-ishonchlilik

?Jumlani to'ldiring. ... sohasi tashkil etuvchilar

xavfsizligi, aloqa xavfsizligi va dasturiy ta'minotlar

xavfsizligidan iborat.

+Tizim xavfsizligi

-Ma'lumotlar xavfsizligi

-Inson xavfsizligi

-Tashkilot xavfsizligi

?Kriptologiya so'ziga berilgan to'g'ri tavsifni toping?

+Maxfiy shifrlarni yaratish va buzish fani va sanati.

-Maxfiy shifrlarni yaratish fani va sanati.

-Maxfiy shifrlarni buzish fani va sanati.

-Axborotni himoyalash fani va sanati.

?.... kriptotizimni shifrlash va deshifrlash uchun sozlashda  
foydalaniladi.

+Kriptografik kalit

-Ochiq matn

-Alifbo

-Algoritm

?Kriptografiya so'ziga berilgan to'g'ri tavsifni toping?

+Maxfiy shifrlarni yaratish fani va sanati.

-Maxfiy shifrlarni yaratish va buzish fani va sanati.

-Maxfiy shifrlarni buzish fani va sanati.

-Axborotni himoyalash fani va sanati.

?Kriptotahlil so'ziga berilgan to'g'ri tavsifni toping?

+Maxfiy shifrlarni buzish fani va sanati.

-Maxfiy shifrlarni yaratish fani va sanati.

-Maxfiy shifrlarni yaratish va buzish fani va sanati.

-Axborotni himoyalash fani va sanati.

?..... axborotni ifodalash uchun foydalaniladigan chekli  
sondagi belgilar to'plami.

+Alifbo

-Ochiq matn

-Shifrmavn

-Kodlash

?Ma lumot shifrlansa, natijasi .... bo ladi.

+shifrmavn

-ochiq matn

-nomalum

-kod

?Deshifrlash uchun kalit va ..... kerak bo ladi.

+shifrmavn

-ochiq matn

-kodlash

-alfbo

?Ma lumotni shifrlash va deshimrlashda yagona kalitdan

foydalanuvchi tizim bu -

+simmetrik kriptotizim.

-ochiq kalitli kriptotizim.

-asimetrik kriptotizim.

-xesh funksiyalar.

?Ikki kalitli kriptotizim bu -

+ochiq kalitli kriptotizim.

-simmetrik kriptotizim.

-xesh funksiyalar.

-MAC tizimlari.

?Axborotni mavjudligini yashirish bilan shug ullanuvchi

fan sohasi bu -

+steganografiya.

-kriptografiya.

-kodlash.

-kriptotahlil.

?Axborotni foydalanuvchiga qulay tarzda taqdim etish

uchun ..... amalga oshiriladi.

+kodlash

-shifrlash

-yashirish

-deshifrlash

?Jumlani to ldiring. Ma lumotni konfidensialligini ta

minlash uchun ..... zarur.

+shifrlash

-kodlash

-dekodlash

-deshifrlash

?Ma lumotni mavjudligini yashirishda .....

+steganografik algoritmdan foydalaniladi.

-kriptografik algoritmdan foydalaniladi.

-kodlash algoritmidan foydalaniladi.

-kriptotahlil algoritmidan foydalaniladi.

?Xesh funksiyalar - .... funksiya.

+kalitsiz kriptografik

-bir kalitli kriptografik

-ikki kalitli kriptografik

-ko p kalitli kriptografik

?Jumlani to ldiring. Ma lumotni uzatishda kriptografik

himoya .....

+konfidensiallik va butunlikni ta minlaydi.

-konfidensiallik va foydalanuvchanlikni ta minlaydi.

-foydalanuvchanlik va butunlikni ta minlaydi.

-konfidensiallik ta minlaydi.

?Jumlani to ldiring. ... kompyuter davriga tegishli

shifrlarga misol bo la oladi.

+DES, AES shifri

-Sesar shifri

-Kodlar kitobi

-Enigma shifri

?.... kriptografik shifrlash algoritmlari blokli va oqimli

turlarga ajratiladi.

+Simmetrik

-Ochiq kalitli

-Asimmetrik

-Klassik davr

?Jumlani to ldiring. .... shifrlar tasodifiy ketma-ketliklarni

generatsiyalashga asoslanadi.

+Oqimli



-Blokli

-Ochiq kalitli

-Asimetrik

?Ochiq matn qismlarini takroriy shifrlovchi algoritmlar bu

-

+blokli shifrlar

-oqimli shifrlash

-ochiq kalitli shifrlar

-asimmetrik shifrlar

?A5/1 shifri bu -

+oqimli shifr.

-blokli shifr.

-ochiq kalitli shifr.

-asimmetrik shifr

?Quyidagi muammolardan qaysi biri simmetrik

kriptotizimlarga xos.

+Kalitni taqsimlash zaruriyati.

-Shifrlash jarayonining ko p vaqt olishi.

-Kalitlarni esda saqlash murakkabligi.

-Foydalanuvchilar tomonidan maqbul ko rilmasligi.

?Quyidagi atamalardan qaysi biri faqat simmetrik blokli

shifrlarga xos?

+Blok uzunligi.

-Kalit uzunligi.

-Ochiq kalit.

-Kodlash jadvali.

?Jumlani to ldiring. Sezar shifri .... akslantirishga

asoslangan.

+o rniga qo yish

-o rin almashtirish

-ochiq kalitli

-kombinatsion

?Kriptotizimning to liq xavfsiz bo lishi Kerxgofts

prinsipiga ko ra qaysi kattalikning nomalum bo lishiga

asoslanadi?

+Kalit.

-Algoritm.

-Shifratn.

-Protokol.

?Shifrlash va deshifrlashda turli kalitlardan foydalanuvchi

shifrlar bu -

+ochiq kalitli shifrlar.

-simmetrik shifrlar.

-bir kalitli shifrlar

-xesh funksiyalar.

?Agar simmetrik kalitning uzunligi 64 bit bo'lsa, jami bo

lishi mumkin bo'lgan kalitlar soni nechta?

+264

-64!

-642

-263

?Axborotni qaysi xususiyatlari simmetrik shifrlar

yordamida ta'minlanadi.

+Konfidentsiallik va butunlik.

-Konfidentsiallik.

-Butunlik va foydalanuvchanlik.

-Foydalanuvchanlik va konfidentsiallik.

?Axborotni qaysi xususiyatlari ochiq kalitli shifrlar

yordamida ta'minlanadi.

+Konfidentsiallik.

-Konfidentsiallik, butunlik va foydalanuvchanlik.

-Butunlik va foydalanuvchanlik.

-Foydalanuvchanlik va konfidentsiallik.

?Elektron raqamli imzo tizimi.

+MAC tizimlari.

-Simmetrik shifrlash tizimlari.

-Xesh funksiyalar.

-Butunlik va foydalanuvchanlik.

?Qaysi ochiq kalitli algoritm katta sonni faktorlash

muammosiga asoslanadi?

+RSA algoritmi.

-El-Gamal algoritmi.

-DES.

-TEA.

?Rad etishdan himoyalashda ochiq kalitli

kriptotizimlarning qaysi xususiyati muhim hisoblanadi.

+Ikkita kalitdan foydalanilgani.

-Matematik muammoga asoslanilgani.

-Ochiq kalitni saqlash zaruriyati mavjud emasligi.

-Shaxsiy kalitni saqlash zarurligi.

?Quyidagi talablardan qaysi biri xesh funksiyaga tegishli  
emas.

+Bir tomonlama funksiya bo'lmash kerak.

-Amalga oshirishdagi yuqori tezkorlik.

-Turli kirishlar turli chiqishlarni akslantirishi.

-Kolliziyaga bardoshli bo'lishi.

?Quyidagi xususiyatlardan qaysi biri elektron raqamli  
imzo tomonidan ta'minlanadi?

+Axborot butunligini va rad etishdan himoyalash.

-Axborot konfidensialligini va rad etishdan himoyalash.

-Axborot konfidensialligi.

-Axborot butunligi.

?Faqat ma'lumotni butunligini ta'minlovchi  
kriptotizimlarni ko'rsating.

+MAC (Xabarlarni autentifikatsiya kodlari) tizimlari.

-Elektron raqamli imzo tizimlari.

-Ochiq kalitli kriptografik tizimlar.

-Barcha javoblar to'g'ri.

?Foydalanuvchini tizimga tanitish jarayoni bu?

+Identifikatsiya.

-Autentifikatsiya.

-Avtorizatsiya.

-Ro'yxatga olish.

?Foydalanuvchini haqiqiylikini tekshirish jarayoni bu?

+Autentifikatsiya.

-Identifikatsiya.

-Avtorizatsiya.

-Ro'yxatga olish.

?Tizim tomonidan foydalanuvchilarga imtiyozlar berish

jarayoni bu?

+Avtorizatsiya.

-Autentifikatsiya.

-Identifikatsiya.

-Ro'yxatga olish.

?Parolga asoslangan autentifikatsiya usulining asosiy

kamchiligini ko'rsating?

+Esda saqlash zaruriyati.

-Birga olib yurish zaruriyati.

-Almashtirib bo'lmazlik.

-Qalbakilashtirish mumkinligi.

?Biror narsani bilishga asoslangan autentifikatsiya

deyilganda quyidagilardan qaysilar tushuniladi.

+PIN, Parol.

-Token, mashinaning kaliti.

-Yuz tasviri, barmoq izi.

-Biometrik parametrlar.

?Tokenga asoslangan autentifikatsiya usulining asosiy

kamchiligini ayting?

+Doimo xavfsiz saqlab olib yurish zaruriyati.

-Doimo esda saqlash zaruriyati.

-Qalbakilashtirish muammosi mavjudligi.

-Almashtirib bo'lmazlik.

?Esda saqlashni va olib yurishni talab etmaydigan

autentifikatsiya usuli bu -

+biometrik autentifikatsiya.

-parolga asoslangan autentifikatsiya.

-tokenga asoslangan autentifikatsiya.

-ko'p faktorli autentifikatsiya.

?Qaysi biometrik parametr eng yuqori universallik

xususiyatiga ega?

+Yuz tasviri.

-Ko'z qorachig'i.

-Barmoq izi.

-Qo'l shakli.

?Qaysi biometrik parametr eng yuqori takrorlanmaslik

xususiyatiga ega?

+Ko'z qorachig'i.

-Yuz tasviri.

-Barmoq izi.

-Qo'l shakli.

?Quyidagilardan qaysi biri har ikkala tomonning

haqiqiylikni tekshirish jarayonini ifodalaydi?

+Ikki tomonlama autentifikatsiya.

-Ikki faktorli autentifikatsiya.

-Ko'p faktorli autentifikatsiya.

-Biometrik autentifikatsiya.

?Parolga asoslangan autentifikatsiya usuliga qaratilgan

hujumlarni ko'rsatgani?

+Parollar lug'atidan foydalanish asosida hujum, yelka

orqali qarash hujumi, zararli dasturlardan foydalanish

asosida hujum.

-Fizik o'g'irlash hujumi, yelka orqali qarash hujumi,

zararli dasturlardan foydalanish asosida hujum.

-Parollar lug'atidan foydalanish asosida hujum, yelka

orqali qarash hujumi, qalbakilashtirish hujumi.

-Parollar lug'atidan foydalanish asosida hujum, bazadagi

parametrni almashtirish hujumi, zararli dasturlardan

foydalanish asosida hujum.

?Tokenga asoslangan autentifikatsiya usuliga qaratilgan

hujumlarni ko'rsatgani?

+Fizik o'g'irlash, mobil qurilmalarda zararli dasturlardan

foydalanishga asoslangan hujumlar

-Parollar lug'atidan foydalanish asosida hujum, yelka

orqali qarash hujumi, zararli dasturlardan foydalanish

asosida hujum

-Fizik o'g'irlash, yelka orqali qarash hujumi, zararli

dasturlardan foydalanishga asoslangan hujumlar

-Parollar lug'atidan foydalanish asosida hujum, bazadagi

parametrni almashtirish hujumi, zararli dasturlardan

foydalanish asosida hujum

?Foydalanuvchi parollari bazada qanday ko rinishda

saqlanadi?

+Xeshlangan ko rinishda.

-Shifrlangan ko rinishda.

-Ochiq holatda.

-Bazada saqlanmaydi.

?Agar parolning uzunligi 8 ta belgi va har bir o rinda 128

ta turlicha belgidan foydalanish mumkin bo lsa, bo lishi

mumkin bo lgan jami parollar sonini toping.

+1288

-8128

-128!

-2128

?Parolni "salt" (tuz) kattaligidan foydalanib xeshlashdan

(h(password, salt)) asosiy maqsad nima?

+Buzg unchiga ortiqcha hisoblashni talab etuvchi

murakkablikni yaratish.

-Buzg unchi topa olmasligi uchun yangi nomalum kiritish.

-Xesh qiymatni tasodifiylik darajasini oshirish.

-Xesh qiymatni qaytmaslik talabini oshirish.

?Quyidagilardan qaysi biri tabiy tahdidga misol bo ladi?

+Yong in, suv toshishi, harorat ortishi.

-Yong in, o g irlik, qisqa tutashuvlar.

-Suv toshishi, namlikni ortib ketishi, bosqinchilik.

-Bosqinchilik, terrorizm, o g irlik.

?Qaysi nazorat usuli axborotni fizik himoyalashda inson

faktorini mujassamlashtirgan?

+Ma muriy nazoratlash.

-Fizik nazoratlash.

-Texnik nazoratlash.

-Apparat nazoratlash.

?Faqat ob ektning egasi tomonidan foydalanishga mos bo

lgan mantiqiy foydalanish usulini ko rsating?

+Diskretsion foydalanishni boshqarish.

-Mandatli foydalanishni boshqarish.

-Rolga asoslangan foydalanishni boshqarish.

-Attributga asoslangan foydalanishni boshqarish.

?Qaysi usul ob ektlar va sub ektlarni klassifikatsiyalashga asoslangan?

+Mandatli foydalanishni boshqarish.

-Diskretsiyon foydalanishni boshqarish.

-Rolga asoslangan foydalanishni boshqarish.

-Attributga asoslangan foydalanishni boshqarish.

?Biror faoliyat turi bilan bog liq harakatlar va majburiyatlar to plami bu?

+Rol.

-Imtiyoz.

-Daraja.

-Imkoniyat.

?Qoida, siyosat, qoida va siyosatni mujassamlashtirgan algoritmlar, majburiyatlar va maslahatlar kabi tushunchalar qaysi foydalanishni boshqarish usuliga aloqador.

+Attributga asoslangan foydalanishni boshqarish.

-Rolga asoslangan foydalanishni boshqarish.

-Mandatli foydalanishni boshqarish.

-Diskretsiyon foydalanishni boshqarish.

?Bell-Lapadula modeli axborotni qaysi xususiyatini ta minlashni maqsad qiladi?

+Konfidensiallik.

-Butunlik.

-Foydalanuvchanlik.

-Ishonchlilik.

?Biba modeli axborotni qaysi xususiyatini ta minlashni maqsad qiladi?

+Butunlik.

-Konfidensiallik.

-Foydalanuvchanlik.

-Maxfiylik.

?Qaysi turdagi shifrlash vositasida barcha kriptografik parametrlar kompyuterning ishtirokisiz generatsiya qilinadi?

+Apparat.

-Dasturiy.

-Simmetrik.

-Ochiq kalitli.

?Qaysi turdagi shifrlash vositasida shifrlash jarayonida

boshqa dasturlar kabi kompyuter resursidan foydalanadi?

+Dasturiy.

-Apparat.

-Simmetrik.

-Ochiq kalitli.

?Yaratishda biror matematik muammoga asoslanuvchi

shifrlash algoritmini ko'rsating?

+Ochiq kalitli shifrlar.

-Simmetrik shifrlar.

-Blokli shifrlar.

-Oqimli shifrlar.

?Xesh funksiyalarda kolliziya hodisasi bu?

+Ikki turli matnlarning xesh qiymatlarini bir xil bo'lishi.

-Cheksiz uzunlikdagi axborotni xeshlay olishi.

-Tezkorlikda xeshlash imkoniyati.

-Turli matnlar uchun turli xesh qiymatlarni hosil bo'lishi.

?64 ta belgidan iborat Sezar shifrlash usulida kalitni

bilmasdan turib nechta urinishda ochiq matnni aniqlash

mumkin?

+63

-63!

-32

-322

?Elektron raqamli imzo muolajalarini ko'rsating?

+Imzoni shakllantirish va imkonini tekshirish.

-Shifrlash va deshifrlash.

-Imzoni xeshlash va xesh matnni deshifrlash.

-Imzoni shakllantirish va xeshlash.

? "Yelka orqali qarash" hujumi qaysi turdagi

autentifikatsiya usuliga qaratilgan.

+Parolga asoslangan autentifikatsiya.



-Tokenga asoslangan autentifikatsiya.

-Biometrik autentifikatsiya.

-Ko z qorachig iga asoslangan autentifikatsiya.

?Sotsial injineriyaga asoslangan hujumlar qaysi turdagi autentifikatsiya usuliga qaratilgan.

+Parolga asoslangan autentifikatsiya.

-Tokenga asoslangan autentifikatsiya.

-Biometrik autentifikatsiya.

-Ko z qorachig iga asoslangan autentifikatsiya.

?Yo qolgan holatda almashtirish qaysi turdagi autentifikatsiya usuli uchun eng arzon.

+Parolga asoslangan autentifikatsiya.

-Tokenga asoslangan autentifikatsiya.

-Biometrik autentifikatsiya.

-Ko z qorachig iga asoslangan autentifikatsiya.

?Qalbakilashtirish hujumi qaysi turdagi autentifikatsiya usuliga qaratilgan.

+Biometrik autentifikatsiya.

-Biror narsani bilishga asoslangan autentifikatsiya.

-Biror narsaga egalik qilishga asoslangan autentifikatsiya.

-Tokenga asoslangan autentifikatsiya

?Axborotni butunligini ta minlash usullarini ko rsating.

+Xesh funksiyalar, MAC.

-Shifrlash usullari.

-Assimetrik shifrlash usullari, CRC tizimlari.

-Shifrlash usullari, CRC tizimlari.

?Quyidagilardan qaysi biri to liq kompyuter topologiyalarini ifodalamaydi.

+LAN, GAN, OSI.

-Yulduz, WAN, TCP/IP.

-Daraxt, IP, OSI.

-Shina, UDP, FTP.

?OSI tarmoq modeli nechta sathdan iborat?

+7

-4

-6

-5

?TCP/IP tarmoq modeli nechta sathdan iborat?

+4

-7

-6

-5

?Hajmi bo'yicha eng kichik hisoblangan tarmoq turi bu -

+PAN

-LAN

-CAN

-MAN

?IPv6 protokolida IP manzilni ifodalashda necha bit

ajratiladi.

+128

-32

-64

-4

?IP manzilni domen nomlariga yoki aksincha

almashtirishni amalga oshiruvchi xizmat bu-

+DNS

-TCP/IP

-OSI

-UDP

?Natijasi tashkilotning amallariga va funksional

harakatlariga zarar keltiruvchi hodisalarning potensial

paydo bo'lishi bu?

+Tahdid.

-Zaiflik.

-Hujum.

-Aktiv.

?Zaiflik orqali AT tizimi xavfsizligini buzish tomon

amalga oshirilgan harakat bu?

+Hujum.

-Zaiflik.

-Tahdid.

-Zararli harakat.

?Quyidagilardan qaysi biri tarmoq xavfsizligi

muammolariga sabab bo'lmaydi?

+Routerlardan foydalanmaslik.

-Qurilma yoki dasturiy vositani noto'g'ri sozlanish.

-Tarmoqni xavfsiz bo'lmagan tarzda va zaif loyihalash.

-Tug'na texnologiya zaifligi.

?Tarmoq xavfsizligini buzulishi biznes faoliyatga qanday ta'sir qiladi?

+Biznes faoliyatning buzilishi, huquqiy javobgarlikka sababchi bo'ladi.

-Axborotni o'g'irlanishi, tarmoq qurilmalarini fizik buzilishiga olib keladi.

-Maxfiylikni yo'q qilishi, tarmoq qurilmalarini fizik buzilishiga olib keladi.

-Huquqiy javobgarlik, tarmoq qurilmalarini fizik buzilishiga olib keladi.

?Razvedka hujumlari bu?

+Asosiy hujumlarni oson amalga oshirish uchun tashkilot va tarmoq haqidagi axborotni to'plashni maqsad qiladi.

-Turli texnologiyalardan foydalangan holda tarmoqqa kirishga harakat qiladi.

-Foydalanuvchilarga va tashkilotlarda mavjud bo'lgan biror xizmatni cheklashga urinadi.

-Tizimni fizik buzishni maqsad qiladi.

?Kirish hujumlari bu?

+Turli texnologiyalardan foydalangan holda tarmoqqa kirishga harakat qiladi.

-Asosiy hujumlarni oson amalga oshirish uchun tashkilot va tarmoq haqidagi axborotni to'plashni maqsad qiladi.

-Foydalanuvchilarga va tashkilotlarda mavjud bo'lgan biror xizmatni cheklashga urinadi.

-Tarmoq haqida axborotni to'plash hujumchilarga mavjud bo'lgan potensial zaiflikni aniqlashga harakat qiladi.

?Xizmatdan voz kechishga qaratilgan hujumlar bu?

+Foydalanuvchilarga va tashkilotlarda mavjud bo'lgan biror xizmatni cheklashga urinadi.

-Turli texnologiyalardan foydalangan holda tarmoqqa

kirishga harakat qiladi.

-Asosiy hujumlarni oson amalga oshirish uchun tashkilot

va tarmoq haqidagi axborotni to'plashni maqsad qiladi.

-Tarmoq haqida axborotni to'plash hujumchilarga mavjud

bo'lgan potensial zaiflikni aniqlashga harakat qiladi.

?Paketlarni snifferlash, portlarni skanerlash va Ping

buyrug'ini yuborish hujumlari qaysi hujumlar toifasiga

kiradi?

+Razvedka hujumlari.

-Kirish hujumlari.

-DOS hujumlari.

-Zararli dasturlar yordamida amalga oshiriladigan

hujumlar.

?O'zini yaxshi va foydali dasturiy vosita sifatida ko'

rsatuvchi zararli dastur turi bu?

+Troyan otlari.

-Adware.

-Spyware.

-Backdoors.

?Marketing maqsadida yoki reklamani namoyish qilish

uchun foydalanuvchini ko'rish rejimini kuzutib boruvchi

zararli dastur turi bu?

+Adware.

-Troyan otlari.

-Spyware.

-Backdoors.

?Himoya mexanizmini aylanib o'tib tizimga ruxsatsiz

kirish imkonini beruvchi zararli dastur turi bu?

+Backdoors.

-Adware.

-Troyan otlari.

-Spyware.

?Paket filterlari turidagi tarmoqlararo ekran vositasi OSI

modelining qaysi sathida ishlaydi?

+Tarmoq sathida.

-Transport sathida.

-Ilova sathida.

-Kanal sathida.

?Tashqi tarmoqdagi foydalanuvchilardan ichki tarmoq

resurslarini himoyalash qaysi himoya vositasining

vazifasi hisoblanadi.

+Tarmoqlararo ekran.

-Antivirus.

-Virtual himoyalangan tarmoq.

-Router.

?Ichki tarmoq foydalanuvchilarini tashqi tarmoqqa bo

lgan murojaatlarini chegaralash qaysi himoya vositasining

vazifasi hisoblanadi.

+Tarmoqlararo ekran.

-Antivirus.

-Virtual himoyalangan tarmoq.

-Router.

?2 lik sanoq tizimida 11011 soniga 11010 sonini 2 modul

bo yicha qo shing?

+00001

-10000

-01100

-11111

?2 lik sanoq tizimida 11011 soniga 00100 sonini 2 modul

bo yicha qo shing?

+11111

-10101

-11100

-01001

?2 lik sanoq tizimida 11011 soniga 11010 sonini 2 modul

bo yicha qo shing?

+00001

-10000

-01100

-11111

?Axborot saqlagich vositalaridan qayta foydalanish

xususiyatini saqlab qolgan holda axborotni yo q qilish

usuli qaysi?

+Bir necha marta takroran yozish va maxsus dasturlar yordamida saqlagichni tozalash

-Magnitsizlantirish

-Formatlash

-Axborotni saqlagichdan o chirish

?Elektron ma lumotlarni yo q qilishda maxsus qurilma

ichida joylashtirilgan saqlagichning xususiyatlari o

zgartiriladigan usul bu ...

+magnitsizlantirish.

-shredirlash.

-yanchish.

-formatlash.

?Yo q qilish usullari orasidan ekologik jihatdan ma

qullanmaydigan va maxsus joy talab qiladigan usul qaysi?

+Yoqish

-Maydalash

-Ko mish

-Kimyoviy ishlov berish

?Kiberjinoatchilik bu - ?

+Kompyuter yoki boshqa qurilmalarga qarshi qilingan

yoki kompyuter va boshqa qurilmalar orqali qilingan

jinoiy faoliyat.

-Kompyuterlar bilan bog liq falsafiy soha bo lib,

foydalanuvchilarning xatti-harakatlari, kompyuterlar

nimaga dasturlashtirilganligi va umuman insonlarga va

jamiyatga qanday ta sir ko rsatishini o rganadi.

-Hisoblashga asoslangan bilim sohasi bo lib, buzg

unchilar mavjud bo lgan sharoitda amallarni kafolatlash

uchun o zida texnologiya, inson, axborot va jarayonni

mujassamlashtirgan.

-Tizimlarni, tarmoqlarni va dasturlarni raqamli

hujumlardan himoyalash amaliyoti.

?Kiberetika bu - ?

+Kompyuterlar bilan bog liq falsafiy soha bo lib,

foydalanuvchilarning xatti-harakatlari, kompyuterlar  
nimaga dasturlashtirilganligi va umuman insonlarga va  
jamiyatga qanday ta'sir ko'rsatishini o'rganadi.

-Kompyuter yoki boshqa qurilmalarga qarshi qilingan  
yoki kompyuter va boshqa qurilmalar orqali qilingan  
jinoiy faoliyat.

-Hisoblashga asoslangan bilim sohasi bo'lib, buzg  
unchilar mavjud bo'lgan sharoitda amallarni kafolatlash  
uchun o'zida texnologiya, inson, axborot va jarayonni  
mujassamlashtirgan.

-Tizimlarni, tarmoqlarni va dasturlarni raqamli  
hujumlardan himoyalash amaliyoti.

?Shaxsiy simsiz tarmoqlar qo'llanish sohasini belgilang

+Tashqi qurilmalar kabellarining o'rnida

-Binolar va korxonalar va internet orasida belgilangan  
simsiz bog'lanish

-Butun dunyo bo'yicha internetdan foydalanishda

-Simli tarmoqlarni mobil kengaytirish

?VPNning texnik yechim arxitekturasiga ko'ra turlari  
keltirilgan qatorni aniqlang?

+Korporativ tarmoq ichidagi VPN; masofadan  
foydalaniluvchi VPN; korporativ tarmoqlararo VPN

-Kanal sathidagi VPN; tarmoq sathidagi VPN; seans  
sathidagi VPN

-Marshurizator ko'rinishidagi VPN; tarmoqlararo ekran  
ko'rinishidagi VPN

-Dasturiy ko'rinishdagi VPN; maxsus shifrlash  
prosessoriga ega apparat vosita ko'rinishidagi VPN

?Axborotning konfidensialligi va butunligini ta'minlash  
uchun ikki uzal orasida himoyalangan tunelni quruvchi  
himoya vositasi bu?

+Virtual Private Network

-Firewall

-Antivirus

-IDS

?Qanday tahdidlar passiv hisoblanadi?

+Amalga oshishida axborot strukturasi va mazmunida

hech narsani o zgartirmaydigan tahdidlar

-Hech qachon amalga oshirilmaydigan tahdidlar

-Axborot xavfsizligini buzmaydigan tahdidlar

-Texnik vositalar bilan bog liq bo lgan tahdidlar

?Quyidagi qaysi hujum turi razvedka hujumlari turiga

kirmaydi?

+Ddos

-Pakatlarni snifferlash

-Portlarni skanerlash

-Ping buyrug ini yuborish

?Trafik orqali axborotni to plashga harakat qilish

razvedka hujumlarining qaysi turida amalga oshiriladi?

+Passiv

-DNS izi

-Lug atga asoslangan

-Aktiv

?Portlarni va operatsion tizimni skanerlash razvedka

hujumlarining qaysi turida amalga oshiriladi?

+Aktiv

-Passiv

-DNS izi

-Lug atga asoslangan

?Pakatlarni snifferlash, portlarni skanerlash, ping buyrug

ini yuborish qanday hujum turiga misol bo ladi?

+Razvedka hujumlari

-Xizmatdan voz kechishga undash hujumlari

-Zararli hujumlar

-Kirish hujumlari

?DNS serverlari tarmoqda qanday vazifani amalga

oshiradi?

+Xost nomlari va internet nomlarini IP manzillarga o

zgartirish va teskarisini amalga oshiradi

-Ichki tarmoqqa ulanishga harakat qiluvchi boshqa tarmoq

uchun kiruvchi nuqta vazifasini bajaradi

-Tashqi tarmoqqa ulanishga harakat qiluvchi ichki tarmoq



uchun chiqish nuqtasi vazifasini bajaradi

-Internet orqali ma'lumotlarni almashinuvchi turli ilovalar  
uchun tarmoq ulanishlarini sozlash funksiyasini amalga  
oshiradi

?Markaziy xab yoki tugun orqali tarmoqni markazlashgan  
holda boshqarish qaysi tarmoq topologiyasida amalga  
oshiriladi?

+Yulduz

-Shina

-Xalqa

-Mesh

?Quyidagilardan qaysilari ananaviy tarmoq turi  
hisoblanadi?

+WAN, MAN, LAN

-OSI, TCP/IP

-UDP, TCP/IP, FTP

-Halqa, yulduz, shina, daraxt

?Quyidagilardan qaysilari tarmoq topologiyalari  
hisoblanadi?

+Halqa, yulduz, shina, daraxt

-UDP, TCP/IP, FTP

-OSI, TCP/IP

-SMTP, HTTP, UDP

?Yong in qarshi tizimlarni aktiv chora turiga  
quyidagilardan qaysilari kiradi?

+Yong inni aniqlash va bartaraf etish tizimi

-Minimal darajada yonuvchan materiallardan foydalanish

-Yetarlicha miqdorda qo'shimcha chiqish yo'llarini  
mavjudligi

-Yong in qarshi tizimlarni to'g'ri madadlanganligi

?Yong in qarshi kurashishning aktiv usuli to'g'ri ko'rsatilgan javobni toping?

+Tutunni aniqlovchilar, alangani aniqlovchilar va  
issiqlikni aniqlovchilar

-Binoga istiqomat qiluvchilarni yong in sodir bo'lganda  
qilinishi zarur bo'lgan ishlar bilan tanishtirish

-Minimal darajada yonuvchan materiallardan foydalanish,

qo shimcha etaj va xonalar qurish

-Yetarli sondagi qo shimcha chiqish yo'llarining mavjudligi

?Yong'inga qarshi kurashishning passiv usuliga kiruvchi

choralarni to'g'ri ko'rsatilgan javobni toping?

+Minimal darajada yonuvchan materiallardan foydalanish, qo shimcha etaj va xonalar qurish

-Tutun va alangani aniqlovchilar

-O't o'chirgich, suv purkash tizimlari

-Tutun va alangani aniqlovchilar va suv purkash tizimlari

?Fizik himoyani buzilishiga olib keluvchi tahdidlar

yuzaga kelish shakliga ko'ra qanday guruhlariga bo'linadi?

+Tabiiy va sun'iy

-Ichki va tashqi

-Aktiv va passiv

-Bir faktorlik va ko'p faktorli

?Quyidagilarni qaysi biri tabiiy tahdidlariga misol bo'la oladi?

+Toshqinlar, yong'in, zilzila

-Bosqinchilik, terrorizm, o'g'irlik

-O'g'irlik, toshqinlar, zilzila

-Terorizm, toshqinlar, zilzila

?Quyidagilarni qaysi biri sun'iy tahdidlariga misol bo'la oladi?

+Bosqinchilik, terrorizm, o'g'irlik

-Toshqinlar, zilzila, toshqinlar

-O'g'irlik, toshqinlar, zilzila

-Terorizm, toshqinlar, zilzila

?Kolliziya hodisasi deb nimaga aytiladi?

+Ikki xil matn uchun bir xil xesh qiymat chiqishi

-ikki xil matn uchun ikki xil xesh qiymat chiqishi

-bir xil matn uchun bir xil xesh qiymat chiqishi

-bir xil matn uchun ikki xil xesh qiymat chiqishi

?GSM tarmog'ida foydalaniluvchi shifrlash algoritmi nomini ko'rsating?

+A5/1

-DES

-AES

-RC4

?O zbekistonda kriptografiya sohasida faoliyat yurituvchi  
tashkilot nomini ko'rsating?

+"UNICON.UZ" DUK

-"O zstandart" agentligi

-Davlat Soliq Qo'mitasi

-Kadastr agentligi

?RC4 shifrlash algoritmi simmetrik turga mansub bo'lsa,  
unda nechta kalitdan foydalaniladi?

+1

-2

-3

-4

?A5/1 shifrlash algoritmi simmetrik turga mansub bo'lsa,  
unda nechta kalitdan foydalaniladi?

+1

-2

-3

-4

?AES shifrlash algoritmi simmetrik turga mansub bo'lsa,  
unda nechta kalitdan foydalaniladi?

+1

-2

-3

-4

?DES shifrlash algoritmi simmetrik turga mansub bo'lsa,  
unda nechta kalitdan foydalaniladi?

+1

-2

-3

-4

?A5/1 oqimli shifrlash algoritmida maxfiy kalit necha  
registrga bo'linadi?

+3

-4

-5

-6

?Faqat simmetrik blokli shifrlarga xos bo'lgan atamani  
aniqlang?

+blok uzunligi

-kalit uzunligi

-ochiq kalit

-kodlash jadvali

?A5/1 shifri qaysi turga mansub?

+oqimli shifrlar

-blokli shifrlar

-ochiq kalitli shifrlar

-assimetrik shifrlar

?... shifrlar blokli va oqimli turlarga ajratiladi

+simmetrik

-ochiq kalitli

-assimetrik

-klassik

?Quyida keltirilgan xususiyatlarning qaysilari xesh  
funktsiyaga mos?

+ixtiyoriy olingan har xil matn uchun xesh qiymatlar bir  
xil bo'lmaydi

-ixtiyoriy olingan bir xil matn uchun qiymatlar bir xil bo'  
lmaydi

-ixtiyoriy olingan har xil matn uchun xesh qiymatlar bir  
xil bo'ladi

-ixtiyoriy olingan har xil xesh qiymat uchun dastlabki ma'  
lumotlar bir xil bo'ladi

?Quyida keltirilgan xususiyatlarning qaysilari xesh  
funktsiyaga mos?

+chiqishda fiksirlangan uzunlikdagi qiymatni beradi

-chiqishda bir xil qiymatni beradi

-chiqishdagi qiymat bilan kiruvchi qiymatlar bir xil bo'  
ladi

-kolliziyaga ega

?Xesh qiymatlarni yana qanday atash mumkin?

+dayjest

-funksiya

-imzo

-raqamli imzo

?A5/1 oqimli shifrlash algoritmida dastlabki kalit uzunligi

nechi bitga teng?

+64

-512

-192

-256

?A5/1 oqimli shifrlash algoritmi asosan qayerda qo

llaniladi?

+mobil aloqa standarti GSM protokolida

-simsiz aloqa vositalaridagi mavjud WEP protokolida

-internet trafiklarini shifrlashda

-radioaloqa tarmoqlarida

?Assimetrik kriptotizimlarda necha kalitdan

foydalaniladi?

+2 ta

-3 ta

-4 ta

-kalit ishlatilmaydi

?Simmetrik kriptotizimlarda necha kalitdan foydalaniladi?

+1 ta

-3 ta

-4 ta

-kalit ishlatilmaydi

?Kriptotizimlar kalitlar soni bo yicha qanday turga bo

linadi?

+simmetrik va assimetrik turlarga

-simmetrik va bir kalitli turlarga

-3 kalitli turlarga

-assimetrik va 2 kalitli turlarga

?Kriptologiya qanday yo nalishlarga bo linadi?

+kriptografiya va kriptotahlil

-kriptografiya va kriptotizim

-kripto va kriptotahlil

-kriptoanaliz va kriptotizim

?Qaysi chora tadbirlar virusdan zararlanish holatini

kamaytiradi?

+Barcha javoblar to'g'ri

-Faqat litsenziyalı dasturiy ta'minotdan foydalanish.

-Kompyuterni zamonaviy antivirus dasturiy vositasi bilan ta'minlash va uni doimiy yangilab borish.

-Boshqa kompyuterda yozib olingan ma'lumotlarni o'qishdan oldin har bir saqlagichni antivirus tekshiruvidan o'tkazish.

?Antivirus dasturiy vositalari zararli dasturlarga qarshi to'liq himoyani ta'minlay olmasligining asosiy sababini ko'rsating?

+Paydo bo'layotgan zararli dasturiy vositalar sonining ko'pligi.

-Viruslar asosan antivirus ishlab chiqaruvchilar tomonidan yaratilishi.

-Antivirus vositalarining samarali emasligi.

-Aksariyat antivirus vositalarining pullik ekanligi.

?...umumiy tarmoqni ichki va tashqi qismlarga ajratib himoyalash imkonini beradi.

+Tarmoqlararo ekran

-Virtual himoyalangan tarmoq

-Global tarmoq

-Korxona tarmog'i

?RSA algoritmidan  $p=5$ ,  $q=13$ ,  $e=7$  ga teng bo'lsa, shaxsiy kalitni hisoblang?

+7

-13

-65

-35

?..... hujumida hujumchi o'rnatilgan aloqaga suqilib kiradi va aloqani bo'ladi. Nuqtalar o'rniga mos javobni qo'ying.

+O'rta turgan odam.

-Qo'pol kuch.

-Parolga qaratilgan.

-DNS izi.

?Agar ob'ektning xavfsizlik darajasi sub'ektning xavfsizlik darajasidan kichik yoki teng bo'lsa, u holda O'qish uchun ruxsat beriladi. Ushbu qoida qaysi foydalanishni boshqarish usuliga tegishli.

+MAC

-DAC

-RMAC

-ABAC

?GSM tarmog'ida ovozli sozlashuvlarni shifrlash algoritmi bu?

+A5/1

-DES

-FCOCT

-RSA

?RSA algoritmidagi ochiq kalit  $e=7$ ,  $N=35$  ga teng bo'lsa,  $M=2$  ga teng ochiq matnni shifrlash natijasini ko'rsating?

+23

-35

-5

-7

?RSA algoritmidagi ochiq kalit  $e=7$ ,  $N=143$  ga teng bo'lsa,  $M=2$  ga teng ochiq matnni shifrlash natijasini ko'rsating?

+128

-49

-11

-7

?Jumlani to'ldiring. Agar axborotning o'zirlanishi moddiy va ma'naviy boyliklarning yo'qotilishiga olib kelsa.

+jinoyat sifatida baholanadi.

-rag'bat hisoblanadi.

-buzg'unchilik hisoblanadi.

-guruhlar kurashi hisoblanadi.

?Jumlani to'ldiring. Simli va simsiz tarmoqlar orasidagi asosiy farq ...

+tarmoq chetki nuqtalari orasidagi mutlaqo

nazoratlamaydigan xudud mavjudligi.

-tarmoq chetki nuqtalari orasidagi xududning kengligi.

-himoya vositalarining chegaralanganligi.

-himoyani amalga oshirish imkoniyati yo'qligi.

?Jumlani to'ldiring. Simmetrik shifrlash algoritmlari

ochiq ma'lumotdan foydalanish tartibiga ko'ra ...

+blokli va oqimli turlarga bo'linadi.

-bir kalitli va ikki kalitli turlarga bo'linadi.

-Feistel tarmog'iga asoslangan va SP tarmog'iga

asoslangan turlarga bo'linadi.

-murakkablikka va tizimni nazariy yondoshuvga

asoslangan turlarga bo'linadi.

?Jumlani to'ldiring. Tarmoqlararo ekranning vazifasi ...

+ishonchli va ishonchsiz tarmoqlar orasida ma'lumotlarga kirishni boshqarish.

-tarmoq hujumlarini aniqlash.

-trafikni taqiqlash.

-tarmoqdagi xabarlar oqimini uzish va ulash.

?Faktirlash muammosi asosida yaratilgan assimetrik shifrlash usuli?

+RSA

-El-Gamal

-Elliptik egri chiziqqa asoslangan shifrlash

-Diffie-Hellman

?Eng zaif simsiz tarmoq protokolini ko'rsating?

+WEP

-WPA

-WPA2

-WPA3

?Axborotni shifrlashdan maqsadi nima?

+Maxfiy xabar mazmunini yashirish.

-Ma'lumotlarni zichlashtirish, siqish.



-Malumotlarni yig'ish va sotish.

-Malumotlarni uzatish.

?9 soni bilan o'zaro tub bo'lgan sonlarni ko'rsating?

+10, 8

-6, 10

-18, 6

-9 dan tashqari barcha sonlar

?12 soni bilan o'zaro tub bo'lgan sonlarni ko'rsating?

+11, 13

-14, 26

-144, 4

-12 dan tashqari barcha sonlar

?13 soni bilan o'zaro tub bo'lgan sonlarni ko'rsating?

+5, 7

-12, 26

-14, 39

-13 dan tashqari barcha sonlar

?Jumlani to'ldiring. Autentifikatsiya tizimlari

asoslanishiga ko'ra ... turga bo'linadi.

+3

-2

-4

-5

?...umumiy tarmoqni ichki va tashqi qismlarga ajratib

himoyalash imkonini beradi.

+Tarmoqlararo ekran

-Virtual himoyalangan tarmoq

-Global tarmoq

-Korxona tarmog'i

?Antivirus dasturiy vositalari zararli dasturlarga qarshi to

liq himoyani ta'minlay olmasligining asosiy sababini ko

rsating?

+Paydo bo'layotgan zararli dasturiy vositalar sonining ko

pligi.

-Viruslar asosan antivirus ishlab chiqaruvchilar

tomonidan yaratilishi.

-Antivirus vositalarining samarali emasligi.

-Aksariyat antivirus vositalarining pullik ekanligi.

?Qaysi chora tadbirlar virusdan zararlanish holatini kamaytiradi?

+Barcha javoblar to'g'ri

-Faqat litsenziyalı dasturiy ta'minotdan foydalanish.

-Kompyuterni zamonaviy antivirus dasturiy vositasi bilan ta'minlash va uni doimiy yangilab borish.

-Boshqa kompyuterda yozib olingan ma'lumotlarni o'qishdan oldin har bir saqlagichni antivirus tekshiruvidan o'tkazish.

?Virus aniq bo'lganda va xususiyatlari aniq ajratilgan holatda eng katta samaradorlikka ega zararli dasturni aniqlash usulini ko'rsating?

+Signaturaga asoslangan usul

-O'zgarishga asoslangan usul

-Anomaliyaga asoslangan usul

-Barcha javoblar to'g'ri

?Signatura (antiviruslarga aloqador bo'lgan) bu-?

+Fayldan topilgan bitlar qatori.

-Fayldagi yoki katalogdagi o'zgarish.

-Normal holatdan tashqari holat.

-Zararli dastur turi.

?Zararli dasturiy vositalarga qarshi foydalaniluvchi dasturiy vosita bu?

+Antivirus

-VPN

-Tarmoqlararo ekran

-Brandmauer

?Kompyuter viruslarini tarqalish usullarini ko'rsating?

+Ma'lumot saqlovchilari, Internetdan yuklab olish va elektron pochta orqali.

-Ma'lumot saqlovchilari, Internetdan yuklab olish va skaner qurilmalari orqali.

-Printer qurilmasi, Internetdan yuklab olish va elektron pochta orqali.

-Barcha javoblar to'g'ri.

?Qurbon kompyuteridagi ma'lumotni shifrlab, uni  
deshifrlash uchun to'lovni amalga oshirishni talab  
qiluvchi zararli dastur bu-?

+Ransomware.

-Mantiqiy bombalar.

-Rootkits.

-Spyware.

?Internet tarmog'idagi obrolar sizlantirilgan kompyuterlar  
bu-?

+Botnet.

-Backdoors.

-Adware.

-Virus.

?Biror mantiqiy shartni tekshiruvchi trigger va foydali  
yuklamadan iborat zararli dastur turi bu-?

+Mantiqiy bombalar.

-Backdoors.

-Adware.

-Virus.

?Buzgunchi xavfsizlik tizimini aylanib o'tib tizimga  
kirish imkonini beruvchi zararli dastur turi bu-?

+Backdoors.

-Adware.

-Virus.

-Trojan otlari.

?Ma'lumotni to'liq qayta tiklash qachon samarali amalga  
oshiriladi?

+Saqlagichda ma'lumot qayta yozilmagan bo'lsa.

-Ma'lumotni o'chirish Delete buyrug'i bilan amalga  
oshirilgan bo'lsa.

-Ma'lumotni o'chirish Shifr+Delete buyrug'i bilan amalga  
oshirilgan bo'lsa.

-Formatlash asosida ma'lumot o'chirilgan bo'lsa.

?Ma'lumotni zaxira nusxalash nima uchun potensial  
tahdidlarni paydo bo'lish ehtimolini oshiradi.

+Tahdidchi uchun nishon ko payadi.

-Saqlanuvchi ma lumot hajmi ortadi.

-Ma lumotni butunligi ta minlanadi.

-Ma lumot yo qolgan taqdirda ham tiklash imkoniyati mavjud bo ladi.

?Qaysi xususiyatlar RAID texnologiyasiga xos emas?

+Shaxsiy kompyuterda foydalanish mumkin.

-Serverlarda foydalanish mumkin.

-Xatoliklarni nazoratlash mumkin.

-Disklarni "qaynoq almashtirish" mumkin.

?Qaysi zaxira nusxalash vositasi oddiy kompyuterlarda foydalanish uchun qo shimcha apparat va dasturiy vositani talab qiladi?

+Lentali disklar.

-Ko chma qattiq disklar.

-USB disklar.

-CD/DVD disklar.

?Ma lumotlarni zaxira nusxalash strategiyasi nimadan boshlanadi?

+Zarur axborotni tanlashdan.

-Mos zaxira nusxalash vositasini tanlashdan.

-Mos zaxira nusxalash usulini tanlashdan.

-Mos RAID sathini tanlashdan.

?Jumlani to ldiring. .... - muhim bo lgan axborot nusxalash yoki saqlash jarayoni bo lib, bu ma lumot yo qolgan vaqtda qayta tiklash imkoniyatini beradi.

+Ma lumotlarni zaxira nusxalash

-Kriptografik himoya

-VPN

-Tarmoqlararo ekran

?Paket filteri turidagi tarmoqlararo ekran vositasi nima asosida tekshirishni amalga oshiradi?

+Tarmoq sathi parametrlari asosida.

-Kanal sathi parametrlari asosida.

-Ilova sathi parametrlari asosida.

-Taqqimot sathi parametrlari asosida.

?Jumlani to ldiring. ... texnologiyasi lokal simsiz

tarmoqlarga tegishli.

+WI-FI

-WI-MAX

-GSM

-Bluetooth

?Jumlani to ldiring. Kriptografik himoya axborotning ...

xususiyatini ta minlamaydi.

+Foydalanuvchanlik

-Butunlik

-Maxfiylik

-Autentifikatsiya

?Jumlani to ldiring. Parol kalitdan .... farq qiladi.

+tasodifiylik darajasi bilan

-uzunligi bilan

-belgilari bilan

-samaradorligi bilan

?Parolga "tuz"ni qo shib xeshlashdan maqsad?

+Tahdidchi ishini oshirish.

-Murakkab parol hosil qilish.

-Murakkab xesh qiymat hosil qilish.

-Ya na bir maxfiy parametr kiritish.

?Axborotni foydalanuvchanligini buzishga qaratilgan

tahdidlar bu?

+DDOS tahdidlar.

-Nusxalash tahdidlari.

-Modifikatsiyalash tahdidlari.

-O rtaga turgan odam tahdidi.

?Tasodifiy tahdidlarni ko rsating?

+Texnik vositalarning buzilishi va ishlamasligi.

-Axborotdan ruxsatsiz foydalanish.

-Zararkunanda dasturlar.

-An anaviy josuslik va diversiya.

?Xodimlarga faqat ruxsat etilgan saytlardan foydalanishga

imkon beruvchi himoya vositasi bu?

+Tarmoqlararo ekran.

-Virtual Private Network.

-Antivirus.

-Router.

?Qaysi himoya vositasi yetkazilgan axborotning

butunligini tekshiradi?

+Virtual Private Network.

-Tarmoqlararo ekran.

-Antivirus.

-Router.

?Qaysi himoya vositasi tomonlarni autentifikatsiyalash

imkoniyatini beradi?

+Virtual Private Network.

-Tarmoqlararo ekran.

-Antivirus.

-Router.

?Foydalanuvchi tomonidan kiritilgan taqiqlangan so'rovni

qaysi himoya vositasi yordamida nazoratlash mumkin.

+Tarmoqlararo ekran.

-Virtual Private Network.

-Antivirus.

-Router.

?Qaysi himoya vositasi mavjud IP - paketni to'liq shifrlab,

unga yangi IP sarlavha beradi?

+Virtual Private Network.

-Tarmoqlararo ekran.

-Antivirus.

-Router.

?Ochiq tarmoq yordamida himoyalangan tarmoqni qurish

imkoniyatiga ega himoya vositasi bu?

+Virtual Private Network.

-Tarmoqlararo ekran.

-Antivirus.

-Router.

?Qaysi himoya vositasida mavjud paket shifrlangan holda

yangi hosil qilingan mantiqiy paket ichiga kiritiladi?

+Virtual Private Network.

-Tarmoqlararo ekran.

-Antivirus.

-Router.

?Qaysi himoya vositasi tarmoqda uzatilayotgan axborotni butunligi, maxfiyligi va tomonlar autentifikatsiyasini ta'minlaydi?

+Virtual Private Network.

-Tarmoqlararo ekran.

-Antivirus.

-Router.

?Qaysi tarmoq himoya vositasi tarmoq manzili, identifikatorlar, interfeys manzili, port nomeri va boshqa parametrlar yordamida filtrlashni amalga oshiradi.

+Tarmoqlararo ekran.

-Antivirus.

-Virtual himoyalangan tarmoq.

-Router.

?Web-sahifa bu...

+Yagona adresga ega bo'lgan, brauzer yordamida ochish va ko'rish imkoniyatiga ega bo'lgan hujjatdir

-Tarmoqqa ulangan kompyuterda, klientga belgilangan umumiy vazifalarni bajarish uchun foydalaniluvchi sahifadir

-Klient-server arxitekturasi asosidagi, keng tarqalgan Internetning axborot xizmati

-HTML kodlari to'plami

?Web-sayt nima?

+Aniq maqsad asosida mantiqiy bog'langan web-sahifalar birlashmasi

-Klient-server texnologiyasiga asoslangan, keng tarqalgan internetning axborot xizmatidir

-A va B

-Yagona adresga ega bo'lgan hujjat hisoblanib, uni ochish (brauzer yordamida) va o'qish imkoniyati mavjud

?WWW nechta komponentdan tashkil topgan?

+4

-5

-3

-2

?WWWning komponentlari qaysi javobda to'g'ri berilgan?

+Dasturiy/texnik vositalar, HTML, HTTP, URI

-HTML, FTP, WWW

-HTML, CSS, PHP

-HTML, JavaScript, JQuery, PHP

?Hozirgi kunda WWWning nechta versiyasi mavjud?

+4

-3

-5

-2

?Web 1.0 ning rivojlanish davrini toping?

+1990-2000 yy.

-2000-2005 yy.

-1980-1990 yy.

-2010-2015 yy.

?Web 2.0 ning rivojlanish davrini toping?

+2000-2010 yy.

-2010-2020 yy.

-2020-2030 yy.

-1990-2000 yy.

?Web 3.0 ning rivojlanish davrini toping?

+2010-2020 yy.

-2000-2010 yy.

-2020-2030 yy.

-1990-2000 yy.

?Web 4.0 ning rivojlanish davrini toping?

+2020-2030 yy.

-2000-2010 yy.

-2010-2020 yy.

-1990-2000 yy.

?HTML teglar necha xil bo'ladi?

+Juft, toq, maxsus teglar



-Toq teglari

-Juft teglari

-Ko rinishi ko p

?Qaysi teg HTML hujjatning tanasini ifodalaydi?

+body

-html

-head

-title

?Qaysi teg hujjatning stilini ifodalash uchun ishlatiladi?

+style

-head

-isindex

-body

?Qaysi teg HTML hujjatni ifodalaydi?

+html

-body

-meta

-isindex

?Qaysi teg HTML hujjat sarlavhasini ifodalaydi?

+head

-meta

-title

-body

?Havola to g ri ko rsatilgan qatorni toping.

+havola

- havola

- havola

-Ekranni tozalash

?

---

tegi nimani ifodalaydi?

+Gorizontal chiziq chizish

-Yangi satrga o tish

-qo shtirnoq

-Ekranni tozalash

?Jadval hosil qilish uchun qaysi tegdan foydalaniladi?

+

?Jadval ustunlarini birlashtirish atributi qaysi javobda keltirilgan?

?Jadval satrlarini birlashtirish atributi qaysi javobda keltirilgan?

?HTML da shrift o lchamini o zgartirish uchun qaysi tegdan foydalaniladi?

-

-

-

?

tegi nimani ifodalaydi?

+Yangi satrga o tish

-"uzilish"

-qo shtirnoq

-Ekranni tozalash

?

tegi nima uchun qo llaniladi?

+matnni paragraflarga ajratish uchun

-Sarlavhani ifodalash uchun

-Obyektni ko rsatilgan joyga o rnatish va shu nuqtadan bo sh satrga matnni davom ettirish uchun qo llaniladi

-Tartibsiz ro yxat hosil qilish uchun

?Rasmlar bilan ishlash teglarini qaysi javobda berilgan?

+Img, map, area, picture

-Image, map, a, picture

-Image, form, area, photo

-Img, iframe, areas, picture

? tegining vazifasi nima?

+Matnni ajratilgan shaklda aniqlash

-Matnni o chirilgan shaklda belgilash

-Matnni tagiga chizilgan shaklda belgilash

-Matnni qiya shaklda belgilash

? tegining vazifasi nima?

+Matnni tagiga chizilgan shaklda belgilash

-Matnni o chirilgan shaklda belgilash

-Matnni ajratilgan shaklda aniqlash

-Matnni qia shaklda belgilash

?

+Matnni o chirilgan shaklda belgilash

-Matnni tagiga chizilgan shaklda belgilash

-Matnni ajratilgan shaklda aniqlash

-Matnni qia shaklda belgilash

?

tegi nimani ifodalaydi?

+Tartiblanmagan ro yxat

-Tartiblangan ro yxat

-Jadval yacheykasi

-Yangi qatorga o tish

?

matni nimani ifodalaydi?

+Teg kvadrat shaklidagi ro yxat hosil qiladi

-Teg aylana shaklidagi ro yxat hosil qiladi

-Teg alifbo ko rinishdagi ro yxatni hosil qiladi

-Teg raqamli ko rinishdagi ro yxatni hosil qiladi

?

matni nimani ifodalaydi?

+Teg I., II., III., IV. va h.k ko rinishdagi ro yxatni hosil qiladi

-Teg raqamli ko rinishdagi ro yxatni hosil qiladi

-Teg kvadrat shaklidagi ro yxat hosil qiladi

-Teg 1., 2., 3., 4. va h.k ko rinishdagi ro yxatni hosil qiladi

? tegining majburiy atributini toping

+src

-title

-href

-type

?Qaysi teg forma ichida qayerga ma lumot kiritilishini ifodalaydi?

+

-

-

-

?HTMLda forma elementlariga kiritilgan qiymatlarni tozalash uchun qaysi elementdan foydalaniladi?

+reset

-text

-hidden

-submit

Kriptologiya qanday yo'nalishlarga bo'linadi?

#kriptografiya va kriptotahlil

kriptografiya va kriptotizim

kripto va kriptotahlil

kriptoanaliz va kriptotizim

++++

Kriptologiya nima bilan shug'ullanadi?

#maxfiy kodlarni yaratish va buzish ilmi bilan

maxfiy kodlarni buzish bilan

maxfiy kodlarni yaratish bilan

maxfiy kodlar orqali ma'lumotlarni yashirish bilan

++++

Kriptografiya nima bilan shug'ullanadi?

#maxfiy kodlarni yaratish bilan

maxfiy kodlarni buzish bilan

maxfiy kodlar orqali ma'lumotlarni yashirish bilan

shifrlash uslublarini bilmagan holda shifrlangan

ma'lumotni asl holatini topish bilan

++++

Kriptotahlil nima bilan shug'ullanadi?

#maxfiy kodlarni buzish bilan

maxfiy kodlarni yaratish bilan

maxfiy kodlar orqali ma'lumotlarni yashirish bilan

shifrlash uslublarini bilmagan holda shifrlangan

ma'lumotni asl holatini topish bilan

++++

Shifrlash orqali ma'lumotning qaysi xususiyati ta'minlanadi?

#maxfiyligi

Butunligi

Ishonchliligi

foydalanuvchanligi

++++

Ochiq kalitli kriptotizimlar kim tomonidan kashf  
qilingan?

#U.Diffie va M.Hellman

Rivest va Adlman

Shamir va Rivest

U.Diffie va Rivest

++++

Kriptologiya necha yo'nalishga bo'linadi?

#2

14

16

18

++++

Kriptologiya so'zining ma'nosi?

#cryptos – maxfiy, logos – ilm

cryptos – kodlash, logos – ilm

cryptos – kriptologiya, logos – yashiraman

cryptos – maxfiy, logos – kalit

++++

Ochiq kalitli kriptotizimlar ma'lumotni qanday  
xususiyatini taminlaydi?

#maxfiyligini

Butunligini

Foydalanuvchanligini

ma'lumotni autentifikatsiyasini

++++

Kriptotizimlar kalitlar soni bo'yicha necha turga  
bo'linadi?

#2

4

6

8

++++

Kriptotizimlar kalitlar soni bo'yicha qanday turga  
bo'linadi?

#simmetrik va assimetrik turlarga

simmetrik va bir kalitli turlarga

3 kalitli turlarga

assimetrik va 2 kalitli turlarga

++++

Simmetrik kriptotizimlardagi qanday muammoni ochiq  
kalitli kriptotizimlar bartaraf etdi?

#maxfiy kalitni uzatish muammosini

kalitni generatsiyalash muammosini

ochiq kalitni uzatish muammosini

kalitlar juftini hosil qilish muammosini

++++

Ochiq kalitli kriptotizimlarda qanday turdagi kalitlardan  
foydalanadi?

#ochiq va maxfiy kalitlardan

maxfiy kalitlar juftidan

maxfiy kalitni uzatishni talab etmaydi

ochiq kalitni talab etmaydi

++++

Assimetrik kriptotizimlarda necha kalitdan foydalaniladi?

#2 ta

3 ta

4 ta

kalit ishlatilmaydi

++++

Kerkxofs printsipli nimadan iborat?

#kriptografik tizim faqat kalit noma'lum bo'lgan

taqdirdagina maxfiylik ta'minlanadi

kriptografik tizim faqat yopiq bo'lgan taqdirdagina

maxfiylik ta'minlanadi

kriptografik tizim faqat kalit ochiq bo'lgan taqdirdagina

maxfiylik ta'minlanadi

kriptografik tizim faqat ikkita kalit ma'lum bo'lgan

taqdirdagina maxfiylik ta'minlanadi

++++

Kalit bardoshliligi bu -?

#eng yaxshi ma'lum algoritm bilan kalitni topish

murakkabligidir

eng yaxshi ma'lum algoritm yordamida yolg'on axborotni

ro'kach qilishdir

nazariy bardoshlilik

amaliy bardoshlilik

++++

Ochiq kalitni kriptotizimlarda nechta kalitdan

foydalanadi?

#Ikkita

Bitta

Uchta

kalitdan foydalanilmaydi

++++

Ochiq kalitli kriptotizimlarda qaysi kalit orqali ma'lumot

shifrlanadi?

#ochiq kalit orqali

maxfiy kalit orqali

ma'lumot shifrlanmaydi

ushbu tizimda kalitdan foydalanilmaydi

++++

Ochiq kalitli kriptotizimda, qaysi kalit orqali ma'lumot

rasshifrovkalanadi?

#maxfiy kalit orqali

ochiq kalit orqali

ma'lumot shifrlanmaydi

ushbu tizimda kalitdan foydalanilmaydi

++++

Ochiq kalitli kriptotizimlarda asosan qanday turdagi

sonlar bilan ishlaydi?

#tub sonlar bilan

kasr sonlar bilan

chekli maydonda kasr sonlar

faqat manfiy sonlar

++++

Qanday sonlar tub sonlar hisoblanadi?

#1 va o'ziga bo'linadigan sonlarlar

barcha toq sonlar

juft bo'lmagan sonlar

2 ga bo'linmaydigan sonlar

++++

Sonlarni tublikka tekshirish algoritmlari nechta sinfga

bo'linadi?

#ikkita sinfga

uchta sinfga

bitta sinfga

sinflarga bo'linmaydi

++++

Kriptotahlil nima bilan shug'ullanadi?

#kalit yoki algoritmi bilmagan holda shifrlangan

ma'lumotga mos keluvchi ochiq ma'lumotni topish bilan

ochiq ma'lumotlarni shifrlash masalalarining matematik

uslublari bilan

maxfiy kodlarni yaratish bilan

maxfiy kodlar orqali ma'lumotlarni yashirish bilan

++++

RSA algoritmining mualliflarini ko'rsating

#R. Rayvest, A. Shamir, L. Adleman

Diffi va M. Hellman

R. Rayvest, K. Hellman, L. Adleman

L. Adleman, El Gamal, K. Shnorr

++++

Ochiq kalitli shifrlash algoritmi keltirilgan qatorni toping?

#RSA

AES

DES

RC4

++++



Ochiq kalitli shifrlash algoritmi keltirilgan qatorni toping?

#El-Gamal

AES

DES

RC4

++++

Shifrlash orqali ma'lumotning qaysi xususiyati

ta'minlanadi?

#Maxfiyligi

Butunliligi

Ishonchliligi

Foydalanuvchanliligi

++++

Kriptografiya bu -?

#axborotni o'zgartirish vositalari va usullarini

o'rganadigan fan

axborot mazmunidan beruxsat erkin foydalanishdan

muhofazalash

axborotni buzishning oldini olish

axborot almashtirish vosita va usullari bilan

shug'ullanadigan fan sohasi

++++

Faqat simmetrik algoritm keltirilgan qatorni ko'rsating?

#AES

RSA

El-Gamal

Barcha javoblar to'g'ri

++++

Kriptotizimlar kalitlar soni bo'yicha nechta turga

bo'linadi?

#2

3

4

++++

Kriptotizimlar kalitlar soni bo'yicha qanday turga

bo'linadi?

#simmetrik va assimetrik

simmetrik va bitta kalitli

3 kalitli kriptotizimlar

assimetrik va 2 ta kalitli

++++

Ferma testi qanday turdagi tublikka testlovchi algoritm

hisoblanadi?

#ehtimollik testlar tarkibiga kiruvchi algoritm

aniqlashtirilgan testlar tarkibiga kiruvchi algoritm

taqribiy testlar tarkibiga kiruvchi algoritm

tublikka teslovchi algoritm hisoblanmaydi

++++

Solovey Shtrassen testi qanday turdagi tublikka testlovchi

algoritm hisoblanadi?

#ehtimollik testlar tarkibiga kiruvchi algoritm

aniqlashtirilgan testlar tarkibiga kiruvchi algoritm

taqribiy testlar tarkibiga kiruvchi algoritm

tublikka teslovchi algoritm hisoblanmaydi

++++

Rabbi-Milner testi qanday turdagi tublikka testlovchi

algoritm hisoblanadi?

#ehtimollik testlar tarkibiga kiruvchi algoritm

aniqlashtirilgan testlar tarkibiga kiruvchi algoritm

taqribiy testlar tarkibiga kiruvchi algoritm

tublikka teslovchi algoritm hisoblanmaydi

++++

Sonlarni tublikka tekshiruvchi algoritmlar necha sinfga

bo'linadi?

#2

3

4

5

++++

Sonlarni tublikka tekshiruvchi algoritmlar qanday sinfga

bo'linadi?

#aniqlashtirilgan va ehtimolli testlar

aniqlashtirilgan va taqribiy testlar

taqribiy va ehtimolli testlar

aniqlashtirilgan, ehtimolli va taqribiy testlar

++++

Sonlarni tublikka tekshiruvchi ehtimollikka asoslangan

algoritmlar keltirilgan qatorni ko'rsating?

#Ferma, Solovey Shtrassen, Rabbi-Milner

Ferma, Solovey Shtrassen, Eyler

Eyler, Solovey Shtrassen, Rabbi-Milner

Ferma, Eyler, Rabbi-Milner

++++

Elliptik egriz chiqizlarda nuqtalar usitda qanday ammalar

bajariladi?

#nuqtalarni qo'shish va nuqtalarni ikkilantirish

nuqtalarni qo'shish va nuqtalarni ko'paytirish

nuqtalarni qo'shish va nuqtalarni bo'lish

nuqtalarni ayirish va nuqtalarni ko'paytirish

++++

1 ga va o'ziga bo'linadigan sonlar qanday sonlar

hisoblanadi?

#tub sonlar

murakkab sonlar

toq sonlar

juft sonlar

Elektron hujjat manbaini haqiqiyligini qaysi amal orqali

amalga oshiriladi?

#ERI orqali amalga oshiriladi

shifrlash algoritmi orqali amalga oshiriladi

kodlash orqali amalga oshiriladi

autentifikatsiya orqali amalga oshiriladi

++++

Elektron hujjat yaxlitligini (o'zgarmasligini) tekshirish

qaysi amal orqali amalga oshiriladi?

#ERI orqali amalga oshiriladi

kodlash orqali amalga oshiriladi

shifrlash algoritmi orqali amalga oshiriladi

autentifikatsiya orqali amalga oshiriladi

++++

Elektron hujjatni mualliflikdan bosh tortmasligini qaysi  
amal orqali amalga oshiriladi?

#ERI orqali amalga oshiriladi

kodlash orqali amalga oshiriladi

autentifikatsiya orqali amalga oshiriladi

shifrlash algoritmi orqali amalga oshiriladi

++++

Raqamli imzoni shakllantirish muolajasi qaysi algoritmgaga  
tegishli?

#ERI algoritmgaga

kodlash algoritmgaga

shifrlash algoritmgaga

steganografiya algoritmgaga

++++

ECDSA-2000 qaysi davlat standarti hisoblanadi?

#AQSH

Rossiya

O'zbekiston

Kanada

++++

O'zDSt 1092:2009 standarti qaysi davlat standarti  
hisoblanadi?

#O'zbekiston

AQSH

Rossiya

Kanada

++++

ГОСТ Р 34.10-94 standarti qaysi davlat standarti  
hisoblanadi?

#Rossiya

O'zbekiston

AQSH

Kanada

++++

Seans kalitli hamda seans kalitsiz rejimlarda ishlidigan

standartni ko'rsating?

#O'zDSt 1092:2009

ECDSA-2000

ГОСТ Р 34.10-94

DSA

++++

DSA qanday standart hisoblanadi?

#ERI standarti

shifrlash standarti

kodlash standarti

steganografik standart

++++

Ochiq kalitli kriptotizimlar qanday turdagi matematik

murakkablikka asoslangan algoritmlarga bo'linadi?

#faktorizatsiyalash va diskret logarifmlash algoritmlariga

modulyar arifmetika murakkabligiga asoslangan

algoritmlarga

diskret logarifmlash murakkabligiga asoslangan

algorimtlarga

faktorizatsiyalash murakkabligiga asoslangan

algorimtlarga

++++

Ochiq kalitli kriptotizimlarning bardoshligini ta'minlashda

qanday murakkab muammo turiga asoslanadi?

#faktorlash, diskret logarifmlash, elliptik egri chiziqda

diskret logarifmlash

faktorlash, diskret logarifmlash

faktorlash, diskret logarifmlash, elliptik egri chiziqda

faktorizatsiyalash

faktorlash, diskret logarifmlash, modulyar arifmetikaga

++++

Ehtimolli testlar sonlarni tublikka tekshirishda qanday

natijani beradi?

#tekshirilayotgan son tub yoki tubmasligi haqida

ehtimollik bilan javob beradi

tekshirilayotgan son tub yoki tubmasligi haqida

kafolatlangan aniq javob beradi

tekshirilayotgan son tub yoki tubmasligi haqida tasodifiy

ravishda javob beradi

tekshirilayotgan son tub yoki tubmasligini 0 va 1

qiymatlarga qarab javob beradi

++++

Sonlarni tublikka tekshirishning ehtimolli algoritmlariga

quyidagilarning qaysilari kiradi?

#Ferma, Rabbi-Milner, Poklingtong testlari

Rabbi-Milner, Solovey-Shtrassen, Pollard testlari

Ferma, Solovey-Shtrassen, Pollard testlari

Rabbi Milner, Poklington, Pollard testlari

++++

Ochiq kalitli RSA shifrlash algoritmi bardoshlilik qanday

matematik muammo turiga asoslangan?

#faktorlash murakkabligiga

diskret logarifmlash murakkabligiga

elliptik egri chiqizlarda faktorizatsiyalash murakkabligiga

elliptik egri chiziqlarda faktorizatsiyalash murakkabligiga

++++

Ochiq kalitli El-Gamal shifrlash algoritmi qanday

matematik murakkablikka asoslanadi?

#diskret logarifmlash murakkabligiga

faktorlash murakkabligiga

elliptik egri chiziqda diskret logarifmlash murakkabligiga

elliptik egri chiziqda faktorlash murakkabligiga

++++

Diffie-Helman algoritmi qanday matematik

murakkablikka asoslanadi?

#diskret logarifmlash murakkabligiga

faktorlash murakkabligiga

elliptik egri chiziqda diskret logarifmlash murakkabligiga

elliptik egri chiziqda faktorlash murakkabligiga

++++

Diffie-Hellman qanday algoritm hisoblanadi?

#kalitlarni ochiq taqsimlash algoritmi

ochiq kalitli shifrlash algoritmi

diskret logarifmlash murakkabligiga asoslangan shifrlash  
algoritmi

faktorlash murakkabligiga asoslangan kalitlarni ochiq  
taqsimlash algoritmi

++++

ERI algoritmlari qanday muolajalardan iborat?

#imzoni shakllantirish, imzoni tekshirish

imzoni shakllantirish, imzo qo'yish va imzoni tekshirish

imzoni shakllantirish va imzo qo'yish

imzo qo'yish

++++

Ochiq kalitli kriptotizimlarda elektron hujjatlarga imzo  
qo'yish qaysi kalit orqali amalga oshiriladi?

#shaxsiy kalit orqali

ochiq kalit orqali

imzo qo'yilishi kalitga bog'liq emas

imzo qo'lda qo'yiladi

++++

Ochiq kalitli kriptotizimlarda elektron hujjatlarga  
qo'yilgan imzoni tekshirish qaysi kalit orqali amalga  
oshiriladi?

#ochiq kalit orqali

maxfiy kalit orqali

imzo qo'yilishi kalitga bog'liq emas

imzo qo'lda qo'yiladi

++++

Diskret logarifmlash murakkabligiga asoslangan algoritm  
keltirilgan qatorni ko'rsating?

#Diffie-Hellman, EL-Gamal algoritmi

RSA algoritmi

EL-Gamal algoritmi

Diffie-Hellman algoritmi

++++

Faktorlash murakkabligiga asoslangan algoritm keltirilgan

qatorni ko'rsating?

#RSA

El-Gamal

Diffie-Hellman

DSA

++++

Karlmaykl sonlari qaysi tublikka tekshiruvchi

algoritmida doim bajariladi?

#Ferma testida

Solovey-Shtrassen testida

Eyler testida

Rabbin testida

++++

Ochiq kalitli RSA shifrlash algoritmda maxfiy kalit

qanday topiladi?

# $e*d \equiv 1 \pmod{p*q}$  taqqoslamadan

$e*d \equiv 1 \pmod{N}$

$e*d \equiv 1 \pmod{p-1}$

$e*d \equiv 1 \pmod{(p-1)(q-1)}$

++++

Ochiq kalitli RSA shifrlash algoritmda qaysi parametrlar

ochiq holda e'lon qilinadi?

#N,e

e

N,d

d

++++

Ochiq kalitli RSA shifrlash algoritmda "e" ochiq kalit,

"d" shaxsiy kalit bo'lsa deshifrlash formulasi to'g'ri

ko'rsatilgan qatorni belgilang?

# $M = C^d \pmod{N}$

$M = C^d \pmod{N}$

$M = C^e \pmod{N}$

$M = C^e \pmod{N}$

++++

Ochiq kalitli RSA shifrlash algoritmda "d" shaxsiy kalit,



“e” ochiq kalit bo'lsa shifrlash formulasi to'g'ri

ko'rsatilgan qatorni belgilang?

$$C = M^e \pmod{N}$$

$$C = M^e \pmod{N}$$

$$C = M^d \pmod{N}$$

$$C = M^d \pmod{N}$$

++++

Ochiq kalitli El-Gamal shifrlash algoritmda "p" tub son

bo'lsa maxfiy kalit qanday tanlanadi?

#(p-1) bilan o'zaro tub bo'lgan (1,p-1) intervaldagi butun son

p bilan o'zaro tub bo'lgan (1,p-1) intervaldagi butun son

(1,p-1) intervaldagi tub son

(p-1) bilan o'zaro tub bo'lgan (1,p) intervaldagi butun son

++++

Ochiq kalitli El-Gamal shifrlash algoritmda ochiq kalit

qanday hisoblanadi?

# $y = g^a \pmod{p}$ , bu yerda g-birlamchi ildiz, a-maxfiy kalit, p-tub son

$y = g^a \pmod{p}$ , bu yerda g-soni (p-1) dan kichik butun son, a-maxfiy kalit, p-tub son

$y = g^a \pmod{p}$ , bu yerda g-soni p dan kichik butun son, a-maxfiy kalit, p-tub son

$y = g^a \pmod{p}$ , bu yerda g-soni (p-1) bilan o'zaro tub bo'lgan butun son, a-maxfiy kalit, p-tub son

++++

Ochiq kalitli kriptotizimlarga asoslangan kalitlarni

taqsimlash Diffie-Hellman algoritmi ishlash prinsipi

qanday?

#umumiy maxfiy kalitni hosil qilishga asoslangan

ochiq va yopiq kalitlar juftini hosil qilishga asoslangan

maxfiy kalitni uzatishni talab etmaydigan prinsipga

asoslangan

ochiq kalitlarni hosil qilishga asoslangan

++++

"A" va "B" foydalanuvchilar ma'lumot almashmoqchi,

"A" foydalanuvchi "B" tomondan qabul qilgan

ma'lumotni imzosini tekshirishda qaysi kalitdan

foydalanadi?

#"B" foydalanuvchining ochiq kalitidan

"B" foydalanuvchining maxfiy kalitidan

"A" foydalanuvchi o'zining ochiq kalitidan

"A" foydalanuvchini o'zining maxfiy kalitidan

++++

RSA algoritmda  $p=3$ ,  $q=11$ ,  $e=3$  bo'lganda maxfiy kalitni

qiymati topilsin:  $e \cdot d \equiv 1 \pmod{N}$ ?

#7

6

8

5

++++

Faktorlash muammosini bartaraf etuvchi usul keltirilgan

qatorni ko'rsating?

#Pollard usuli

Xitoy teoremasi

Pohlig-Hellman usulu

RSA usuli

++++

Pollard usuli qanday turdagi matematik murakkablikni

yechishda foydalaniladi?

#faktorlash murakkabligini

diskret logarifmlash murakkabligini

elliptik egrzi chiziqda diskret logarifmlash murakkabligini

elliptik egrzi chiziqda faktorlash murakkabligini

++++

RSA algoritmidagi matematik murakkablikni qanday usul

orqali bartaraf qilish mumkin?

#Pollard usuli

Xitoy teoremasi

Pohlig-Hellman usuli

RSA usuli

++++

Diskret logarifmlash muammosini bartaraf etuvchi usul

keltirilgan qatorni ko'rsating?

#Pohlig-Hellman usuli

Pollard usuli

Xitoy teoremasi

RSA usuli

++++

Pohlig-Hellman usuli qanday turdagi matematik

murakkablikni yechishda foydalaniladi?

#diskret logarifmlash murakkabligini

faktorklash murakkabligini

elliptik egrzi chiziqda faktorklash murakkabligini

daraja parameter murakkabligini

++++

Evklidning kengaytirilgan algoritmidan RSA shifrlash

algoritmining qaysi parametrini hisoblashda

foydalaniladi?

#maxfiy kalitni

ochiq kalitni

tub sonlarni

modul qiymatini

++++

Diffie-Hellman algoritmda qaysi parametrlar ochiq holda

e'lon qilinadi?

#p va g tub sonlarni( $p > g$ )

p tub sonni

p va g toq sonlarni( $p > g$ )

p va g juft sonlarni( $p > g$ )

++++

Axborot xavfsizligining pasayishi nimani anglatadi?

#axborot xavfsizligi

ma'lumotlarning tartibsizligi

ma'lumotlarning mas'uliyatsizligi

ichki xavfsizlik

+++++

Tashkilotning iqtisodiy xavfsizligini ta'minlash

muammosining eng muhim tarkibiy qismlaridan biri bu

#Axborot texnologiyalari (IT) va tizimlar (IS) xavfsizligi

Axborot texnologiyalari (IT) xavfsizligi

Axborot tizimlarining xavfsizligi (IS)

Texnik tizimlarning xavfsizligi (TS)

+++++

Axborot tizimlari va texnologiyalarini rivojlantirish, joriy

qilish va ulardan foydalanishning ajralmas qismi

hisoblanadi

#Axborot xavfsizligi

kriptografiya

steganografiya

autentifikatsiya

+++++

Zamonaviy dasturlash texnologiyasi sizni mutlaqo xatosiz

va xavfsiz dasturlarni yaratishga imkon beradimi?

#emas

Ha

noma'lum

savol noto'g'ri

+++++

Huquqiy hujjatlar talablariga yoki ma'lumot egalari

to'monidan o'rnatilgan talablarga muvofiq mulkka tegishli

va himoya qilinishi kerak bo'lgan ma'lumotlar

#himoyalangan ma'lumotlar

maxfiy ma'lumotlar

keraksiz ma'lumotlar

foydali ma'lumotlar

+++++

Axborot egalari bo'lishi mumkin:

#davlat, yuridik shaxs, shaxslar guruhi, yakka shaxs.

davlat xizmatchisi, yuridik shaxs, shaxslar guruhi,

jismoniy shaxs.

davlat, yuridik shaxs, shaxslar guruhi, alohida

aktsiyadorlik jamiyati.

davlat, yuridik shaxs, shaxslar guruhi, alohida kompaniya.

+++++

Axborotni qayta ishlashning avtomatlashtirilgan tizimlari

nima uchun kerak?

#ma'lumotlarni saqlash, qayta ishlash va uzatish uchun

ma'lumotlarni saqlash, yangilash va yashirish uchun

ma'lumotlarni saqlash, qayta ishlash va shifrlash uchun

ma'lumotlarni saqlash, qayta ishlash va tahlil qilish uchun

+++++

Axborot xavfsizligini buzishning potentsial yoki real

xavfini keltirib chiqaradigan shartlar va omillar to'plami

#Tahdid (axborot xavfsizligi)

Maxfiylikni buzish

Hodisa

Hujum

+++++

Axborot xavfsizligiga tahdidning bevosita sababi bo'lgan

sub'ekt (shaxs, moddiy ob'ekt yoki jismoniy hodisa)

#Axborot xavfsizligiga tahdid manbai

Texnik xavfsizlik manbai

Virus hujumining manbasi

Xodimlarning manbasi

+++++

Axborot tizimining xususiyati, unda ishlov beriladigan

axborotga tahdidlarni amalga oshirishga imkon beradi

#Zaiflik (axborot tizimi)

Xaker hujumi

Hodisa

Qayta rasmiylashtirish

+++++

Yashirin yoki mahfiy axborotni amalga oshirish natijasida

shaxs, shaxslar guruhi yoki u mo'ljallanmagan har qanday

tashkilot uchun foydalanish mumkin bo'lgan tahdid

#Maxfiylikka tahdid (oshkor qilish tahdidi)

Butunlik uchun tahdid

Texnik tahdid

Xaker hujumi

+++++

Amalga oshirilishi natijasida ma'lumotlar o'zgartirilishi

yoki yo'q qilinishi mumkin bo'lgan tahdid

#Butunlik uchun tahdid

Virusli hujum xavfi

Tarmoq tahdidi

Texnik tahdid

+++++

Tashkilotni o'z faoliyatida yo'naltiradigan

hujjatlashtirilgan qoidalar, protseduralar, amaliyotlar yoki

axborot xavfsizligi sohasidagi ko'rsatmalar to'plami

#Xavfsizlik siyosati

Davlat siyosati

Korporativ etika

Ko'rsatmalar

+++++

Amalga oshirilishi avtomatlashtirilgan tizim mijozlariga

xizmat ko'rsatishni rad etishga, tajovuzkorlarning o'z

xohishlariga ko'ra manbalardan ruxsatsiz foydalanishiga

olib keladigan tahdid hisoblanadi.

#Xizmat tahdidini rad etish (mavjud tahdid)

Texnik muammo

Tizimning favqulodda to'xtashi

Hujum

+++++

Uning maxfiyligi, ochiqligi va yaxlitligi ta'minlanadigan

axborot xavfsizligi holati

#Axborot xavfsizligi

Ma'lumot xavfsizligi

Operatsion tizim xavfsizligi

Shaxsiy ma'lumotlar xavfsizligi

+++++

Axborotni himoya qilish usuli

#axborotni himoya qilishning muayyan printsiplari va

vositalarini qo'llash tartibi va qoidalari.

axborotni texnik himoya qilishning muayyan printsiplari

va vositalarini qo'llash tartibi va qoidalari.

ma'lum bir algoritmlar va axborot xavfsizligi vositalarini  
qo'llash tartibi va qoidalari.

axborotni himoya qilishning ayrim algoritmlarini qo'llash  
tartibi va qoidalari.

+++++

Apparat, dasturiy ta'minot, dasturiy ta'minot va apparat,  
axborotni himoya qilish uchun mo'ljallangan yoki  
ishlatiladigan materiallar va (yoki) materiallar

#Axborot xavfsizligi vositasi

Axborotni nusxalash vositasi

Axborot uzatish vositasi

Shaxsiy ma'lumotlarni uzatish vositasi

+++++

Axborotni kriptografik o'zgartirish orqali himoya qilish

#kriptografik ma'lumotlarni himoya qilish

antivirus ma'lumotlarini himoya qilish

ma'lumotlarni steganografik himoya qilish

axborotni texnik himoya qilish

+++++

Ruxsat berilgan shaxslarning kirib borishi yoki kirishiga  
to'sqinlik qiladigan vositalar to'plami va tashkiliy choralar  
yordamida axborotni himoya qilish himoya qilinadigan  
obyekt hisoblanadi.

#axborotni jismoniy himoya qilish

axborotni dasturiy himoyasi

antivirus ma'lumotlarini himoya qilish

oddiy ma'lumotlarni himoya qilish

+++++

Muayyan tarmoq tugunini o'chirishga qaratilgan hujum  
turi (Xizmatni rad etish - DoS)

#xizmatdan bosh tortish

"ma'lumotlarga kirishni rad etish"

"ma'lumotlarga kirishni rad etish"

"parolga kirish taqiqlandi"

+++++

Kriptovalyutatsiya atamasini birinchi bo'lib kiritgan

olimni ko'rsating

#F. Fridman

Aristotel

Shannon

Aliqushchi

+++++

IV asrda "antiscital" dekifrlash qurilmasini kim yaratgan.

Mil. Avv.

#Aristotel

Sokrat

Ptolemey

Spital

+++++

Qaysi olimning kitobida chastota kriptovalyutasi

to'g'risida birinchi ma'lum eslatma mavjud?

#Al-Kindi

Aristotel

Umar Xayyom

Mirzo Ulug'bek

+++++

Qur'on matni asosida arab tilidagi harflarning chastota

jadvalini birinchi bo'lib kim aniqlagan?

#Shihab al-Kalkasandi

Umar Xayyom

Mirzo Ulug'bek

Imom Buxoriy

+++++

Axborotni shifrlash va shifrlash usullarini qaysi fan

rivojlantirmoqda?

#Kriptologiya

Informatika

Matematika

Fizika

+++++

DES shifrlash algoritmi qaysi tarmoqqa asoslangan holda

ishlaydi?



#Feystel tarmog'iga asoslangan holda

SPN tarmog'iga asoslangan holda

hech qanday tarmoqqa asoslanmaydi

Lai-Massey tarmog'iga asoslangan holda

+++++

Quyida keltirilgan xususiyatlarning qaysilari xesh

funksiyaga mos?

#chiqishda fiksirlangan uzunlikdagi qiymatni beradi

chiqishda bir xil qiymatni beradi

kolliziyaga ega

chiqishdagi qiymat bilan kiruvchi qiymatlar bir xil bo'ladi

+++++

Quyida keltirilgan xususiyatlarning qaysilari xesh

funksiyaga mos?

#ixtiyoriy olingan har xil matn uchun xesh qiymatlar bir

xil bo'lmaydi

ixtiyoriy olingan bir xil matn uchun qiymatlar bir xil

bo'lmaydi

ixtiyoriy olingan har xil matn uchun xesh qiymatlar bir xil

bo'ladi

ixtiyoriy olingan har xil xesh qiymat uchun dastlabki

ma'lumotlar bir xil bo'ladi

+++++

DES shifrlash algoritmda har bir raunda necha bitli raund

kalitlaridan foydalaniladi?

#48

56

64

32

+++++

Qaysi hujum turida barcha bo'lishi mumkin bo'lgan

variantlar ko'rib chiqiladi?

#qo'pol kuch hujumi

sotsial injineriya

analitik hujum

chastotalar tahlili

+++++

Ma'lumotlarni autentifikatsiyalash kodlari deb qanday  
xesh funksiyalarga aytiladi?

#kalitli xesh funksiyalarga

kalitsiz xesh funksiyalarga

kriptografik bo'lmagan xesh funksiyalarga

kriptografik xesh funksiyalarga

+++++

AES algoritmidan raundlar soni nimaga bo'g'liq?

#kalit uzunligiga

kiruvchi blok uzunligiga

foydalanilgan vaqtiga

kiruvchi blok uzunligi va matn qiymatiga

+++++

A5/1 oqimli shifrlash algoritmidan registrning surilishi

qanday kattalikka bog'liq?

#maj funksiyasi qiymatiga

kalit qiymatiga

registr uzunligi qiymatiga

hech qanday kattalikka bog'liq emas

+++++

16 raund davom etadigan blokli shifrlash algoritmi

ko'rsating?

#DES

AES

RC4

A5/1

+++++

10 raund davom etadigan blokli shifrlash algoritmi

ko'rsating?

#AES

DES

RC4

A5/1

+++++

Xesh qiymatlarni yana qanday atash mumkin?

#dayjest

funksiya

imzo

raqamli imzo

+++++

Ximoyalanuvchi ma'lumot boshqa bir ma'lumotni ichiga

yashirish orqali maxfiyligini ta'minlaydigan usul qaysi?

#steganografiya

kodlash

shifrlash

autentifikatsiya

+++++

Baytlar kesimida shifrlashni amalga oshiradigan algoritim

keltirilgan qatorni ko'rsating?

#RC4

A5/1

MD5

SHA1

+++++

Kolliziya deb nima nisbatan aytiladi?

#ikkita har xil matn uchun bir xil xesh qiymat mos kelishi

ikkita bir xil matn uchun bir xil xesh qiymat mos kelishi

ikkita har xil matn uchun har xil xesh qiymat mos kelishi

ikkita bir xil matn uchun bir xil xesh qiymat mos

kelmasligiga

+++++

Konfidensiallikni ta'minlash bu -?

#ruxsat etilmagan "o'qishdan" himoyalash

ruxsat etilmagan "yozishdan" himoyalash

ruxsat etilmagan "bajarishdan" himoyalash

ruxsat berilgan "amallarni" bajarish

+++++

Sezar shifrlash algoritmi qaysi turdagi akslantirishga

asoslangan?

#o'rniga qo'yish

o'rin almashtirish

aralash

kompozitsion

+++++

CRC-3 tizimida CRC qiymatini hisoblash jarayonida

ma'lumotga nechta nol biriktiriladi?

#3

6

12

9

+++++

.... kriptotizimni shifrlash va rasshifrovkalash uchun  
sozlashda foydalaniladi.

#kalit

ochiq matn

algoritm

alifbo

+++++

CRC-5 tizimida CRC qiymati hisoblash jarayonida

ma'lumotga nechta nol biriktiriladi?

#5

10

15

20

+++++

Rasshifrovkalash jarayonida kalit va ..... kerak bo'ladi

#shifrmtn

ochiq matn

kodlash

alifbo

+++++

Kriptologiya qanday yo'nalishlarga bo'linadi?

#kriptografiya va kriptotahlil

kripto va kriptotahlil

kriptografiya va kriptotizim

kriptoanaliz va kriptotizim

+++++

Kriptotizimlar kalitlar soni bo'yicha necha turga

bo'linadi?

#2

6

4

8

+++++

Kriptografiya nima bilan shug'ullanadi?

#maxfiy kodlarni yaratish bilan

maxfiy kodlar orqali ma'lumotlarni yashirish

bilan maxfiy kodlarni buzish bilan

shifrlash uslublarini bilmagan holda shifrlangan

ma'lumotni asl holatini topish bilan

+++++

Kerkxofs printsipi nimadan iborat?

#kriptografik tizim faqat kalit noma'lum bo'lgan

taqdirdagina maxfiylik ta'minlanadi

kriptografik tizim faqat yopiq bo'lgan taqdirdagina

maxfiylik ta'minlanadi

kriptografik tizim faqat ikkita kalit ma'lum bo'lgan

taqdirdagina maxfiylik ta'minlanadi

kriptografik tizim faqat kalit ochiq bo'lgan taqdirdagina

maxfiylik ta'minlanadi

+++++

Shifrlash orqali ma'lumotning qaysi xususiyati

ta'minlanadi?

#maxfiyligi

ishonchliligi

butunliligi

foydalanuvchanligi

+++++

O'rniga qo'yish shifrlash sinfiga qanday algoritmlar

kiradi?

#shifrlash jarayonida ochiq ma'lumot alfavit belgilari

shifr ma'lumot belgilariga almashtiriladigan algoritmlar

shifrlash jarayonida ochiq ma'lumot alfaviti belgilarining

o'rinlar almashtiriladigan algoritmalar

shifrlash jarayonida kalitlarning o'rnini almashtiriladigan  
algoritmarga

shifrlash jarayonida o'rniga qo'yish va o'rin almashtirish  
akslantirishlarning kombinatsiyalaridan birgalikda  
foydalaniladigan algoritmalar

+++++

Kriptologiya necha yo'nalishga bo'linadi?

#2

4

8

6

+++++

Kriptologiya so'zining ma'nosi?

#cryptos – maxfiy, logos – ilm

cryptos – maxfiy, logos – kalit

cryptos – kriptologiya, logos – yashiraman

cryptos – kodlash, logos – ilm

+++++

O'rniga qo'yish shifrlash algoritmalarini necha sinfga  
bo'linadi?

#2

6

4

8

+++++

O'rniga qo'yish shifrlash algoritmalarini qanday sinfga  
bo'linadi?

#bir qiymatli va ko'p qiymatli shifrlash

bir qiymatli shifrlash

ko'p qiymatli shifrlash

uzluksiz qiymatli shifrlash

+++++

Kriptologiya nima bilan shug'ullanadi?

#maxfiy kodlarni yaratish va buzish ilmi bilan

maxfiy kodlarni yaratish bilan

maxfiy kodlarni buzish bilan

maxfiy kodlar orqali ma'lumotlarni yashirish bilan

+++++

Ma'lumotlarni kodlash va dekodlashda necha kalitdan

foydalanadi?

#kalit ishlatilmaydi

3 ta

2 ta

4 ta

+++++

Simmetrik kriptotizimlarda necha kalitdan foydalaniladi?

#1 ta

3 ta

kalit ishlatilmaydi

4 ta

+++++

Kriptotahlil nima bilan shug'ullanadi?

#maxfiy kodlarni buzish bilan

shifrlash uslublarini bilmagan holda shifrlangan

ma'lumotni asl holatini

topish bilan

maxfiy kodlar orqali ma'lumotlarni yashirish bilan

maxfiy kodlarni yaratish bilan shifrlash uslublarini

bilmagan holda shifrlangan ma'lumotni asl holatini topish

bilan

+++++

A5/1 oqimli shifrlash algoritmda dastlabki kalit uzunligi

nechi bitga teng?

#64

192

512

256

+++++

Steganografiya ma'lumotni qanday maxfiylashtiradi?

#maxfiy xabarni soxta xabar ichiga berkitish orqali

maxfiy xabarni kriptografik kalit yordamida shifrlash

orqali

maxfiy xabarni kodlash orqali

maxfiy xabarni shifrlash orqali

+++++

Shifrlash algoritmlari akslantirish turlariga qarab qanday turlarga bo'linad?

#o'rniga qo'yish, o'rin almashtirish va kompozitsion akslantirishlarga

o'rniga qo'yish, o'rin almashtirish va surish akslantirishlariga

o'rniga qo'yish va o'rin almashtirish akslantirishlariga

o'rniga qo'yish, sirush va kompozitsion shifrlash akslantirishlariga

+++++

Blokli shifrlash algoritmlari arxitekturasini jihatidan qanday tarmoqlarga bo'linadi?

#Feystel va SP

Feystel va Petri

SP va Petri

Kvadrat va iyerarxik

+++++

Zamonaviy kriptografiya qaysi bo'limlarni o'z ichiga oladi?

#simmetrik kriptotizimlar, ochiq kalitli kriptotizimlar, elektron raqamli imzo kriptotizimlari, kriptobardoshli kalitlarni ishlab chiqish va boshqarish

simmetrik kriptotizimlar, ochiq kalit algoritmiga

asoslangan kriptotizimlar, elektron raqamli imzo

kriptotizimlari, foydalanuvchilarni ro'yxatga olish

simmetrik kriptotizimlar, ochiq kalit algoritmiga

asoslangan kriptotizimlar, elektron raqamli imzo

kriptotizimlari, foydalanuvchilarni identifikatsiya qilish

simmetrik kriptotizimlar, ochiq kalit algoritmiga

asoslangan kriptotizimlar, elektron raqamli imzo

kriptotizimlari, foydalanuvchilarni autentifikatsiyalash

+++++



ARX amali nimalardan iborat?

#add, rotate, xor

add, rotate, mod

add, mod, xor

mod, rotate, xor

+++++

Tasodifiy ketma-ketliklarni generatsiyalashga asoslangan

shifrlash turi bu?

#oqimli shifrlar

blokli shifrlar

ochiq kalitli shifrlar

assimetrik shifrlar

+++++

Qanday algoritmlarda chiqishda doim fiksirlangan

uzunlikdagi qiymat chiqadi?

#xesh algoritmlarda

kodlash algoritmlarida

shifrlash algoritmlarida

steganografik algoritmlarda

+++++

Ma'lumotni shifrlash va deshifrlash uchun bir xil kalitdan

foydalanuvchi tizim bu?

#simmetrik kriptotizim

ochiq kalitli kriptotizim

assimetrik kriptotizim

xesh funksiyalar

+++++

Ikki kalitli deyilganda qaysi kriptotizim nazarda tutiladi?

#ochiq kalitli kriptotizim

simmetrik kriptotizim

xesh funksiyalar

MAC tizimlari

+++++

Simmetrik shifrlash algoritmlarida qanday muammo

mavjud?

#kalitni uzatish

kalit generatsiyalash

kalitni yo'q qilish

muammo yo'q

+++++

Sezar shifrlash usuli qaysi akslantirishga asoslangan?

#o'rniga qo'yish

o'rin almashtirish

ochiq kalitli shifrlarga

kombinatsion akslantirishga

+++++

Ma'lumotni uzatishda kriptografik himoya .....

#konfidensiallik va yaxlitlikni ta'minlaydi

konfidensiallik va foydalanuvchanlikni ta'minlaydi

konfidensiallikni ta'minlaydi

foydalanuvchanlik ta'minlaydi va butunlikni

+++++

Butunlikni ta'minlash bu - ?

#ruxsat etilmagan "yozishdan" himoyalash

ruxsat etilmagan "bajarishdan" himoyalash

ruxsat etilmagan "o'qishdan" himoyalash

ruxsat berilgan "amallarni" bajarish

+++++

Shifrlash va deshifrlashda alohida kalitlardan

foydalanuvchi kriptotizimlar bu?

#ochiq kalitli kriptotizimlar

simmetrik kriptotizimlar

bir kalitli kriptotizimlar

xesh funksiyalar

+++++

Agar ochiq ma'lumot shifrlansa, natijasi .... bo'ladi.

#shifrmtn

ochiq matn

noma'lum

kod

+++++

Ochiq kalitli shifrlar axborotni qaysi xususiyatlarini

ta'minlashda foydalaniladi?

#konfidensiallik va yaxlitlik

konfidensiallik va foydalanuvchanlik

foydalanuvchanlik va yaxlitlik

foydalanuvchanlik

+++++

MD5 xesh funksiyasida kiruvchi ma'lumot uzunligi

qanday bitli bloklarga bo'linadi?

#512

1024

2048

4096

+++++

add amalining ma'nosi nima?

#modul asosida qo'shish

XOR amali

surish (siklik surish, mantiqiy surish)

akslantirish

+++++

SHA1 xesh funksiyasida initsializatsiya bosqichida 5 ta

necha bitli registrlardan foydalanadi?

#32

64

128

256

+++++

O'zbekistonda kriptografiya sohasida faoliyat yurituvchi

tashkilot nomini ko'rsating?

#"UNICON.UZ" DUK

"O'zstandart" agentligi

Kadastr agentligi

Davlat Soliq Qo'mitasi

+++++

Faqat simmetrik shifrlash algoritmlari nomi keltirilgan

qatorni ko'rsating?

#AES, A5/1

SHA1, DES

MD5, AES

HMAC, RC4

+++++

HMAC tizimida kalit qiymati blok uzunligiga teng

bo'lganda ma'lumotga qanday biriktiriladi?

#kalit qiymati o'zgartirilmagan holda ma'lumotga

biriktiriladi

kalit qiymati blok uzunligiga teng bo'lguncha nol qiymat

bilan to'ldirilib hosil bo'lgan qiymat ma'lumotga

biriktiriladi

kalitni xesh qiymati hisoblanib, unga blok uzunligiga teng

bo'lguncha nol qiymat qo'shiladi va yangi hosil bo'lgan

qiymat ma'lumotga biriktiriladi

xesh funksiyalarda kalit qiymatida foydalanilmaydi

+++++

DES shifrlash algoritmda rasshifrovkalashda birinchi

raunda qaysi kalitdan foydalaniladi?

#16-raund kalitidan

1-raund kalitidan

1-raunda kalitdan foydalanilmaydi

dastlabki kalitdan

+++++

SHA1 xesh funksiyasida kiruvchi ma'lumot uzunligi

qanday bitli bloklarga bo'linadi?

#512

1024

2048

4096

+++++

AES shifrlash algoritmda blok uzunligi 128, kalit

uzunligi 192 bit bo'lsa raundlar soni nechta bo'ladi?

#12

10

14

6

+++++

AES shifrlash algoritmda nechta akslantirishdan  
foydalanadi?

#4

3

2

akslantirishdan foydalanilmaydi

+++++

GSM tarmog'ida foydalaniluvchi shifrlash algoritmi  
nomini ko'rsating?

#A5/1

dastlabki kalitdan

AES

DES

+++++

WEP protokolida (Wi-Fi tarmog'ida) foydalaniluvchi  
shifrlash algoritmi nomini ko'rsating?

#RC4

DES

SHA1

A5/1

+++++

rotate amalining ma'nosi nima?

#surish (siklik surish, mantiqiy surish)

modul asosida qo'shish

XOR amali

Akslantirish

+++++

SHA1 xesh funksiyasida to'ldirish bitlarini qo'shishda  
ma'lumot uzunligi 512 modul bo'yicha qanday son bilan  
taqqoslanadigan qilib to'ldiriladi?

#448

1002

988

772

+++++

HMAC tizimida kalit qiymati blok uzunligidan kichik

bo'lganda ma'lumotga qanday biriktiriladi?

#kalit qiymati blok uzunligiga teng bo'lguncha nol qiymat bilan to'ldirilib hosil bo'lgan qiymat ma'lumotga biriktiriladi

kalitni xesh qiymati hisoblanib, unga blok uzunligiga teng bo'lguncha nol qiymat qo'shiladi va yangi hosil bo'lgan qiymat ma'lumotga biriktiriladi

kalit qiymati o'zgartirilmagan holda ma'lumotga biriktiriladi

xesh funksiyalarda kalit qiymatida foydalanilmaydi

+++++

Kolliziya hodisasi qaysi turdagi algoritmlarga xos?

#xesh funksiyalar

ochiq kalitli shifrlash algoritmlari

kalitlarni boshqarish tizimlari

simmetrik shifrlash algoritmlari

+++++

AES shifrlash algoritmida shifrlash jarayonida qanday akslantirishdan foydalaniladi?

#SubBytes, ShiftRows, MixColumns va AddRoundKey

SubBytes, ShiftRows va AddRoundKey

SubBytes, MixColumns va AddRoundKey

MixColumns, ShiftRows, SubBytes

+++++

Faqat blokli simmetrik shifrlash algoritmlari nomi keltirilgan qatorni ko'rsating?

#AES, DES

A5/1, RC4

A5/1, MD5

SHA1, RC4

+++++

Vernam shifrlash algoritmida shifr matn  $C=101$  ga, kalit  $K=111$  ga teng bo'lsa shifr matn qiymati qanday bo'ladi?

#010

101

111

110

+++++

Quyidagi ifoda nechta yechimga ega?  $3 \cdot x = 2 \pmod{7}$ .

#bitta yechimga ega

ikkita yechimga ega

yechimga ega emas

uchta yechimga ega

+++++

$143 \pmod{17}$  nechiga teng?

#7

6

5

8

+++++

Blokli shifrlash rejimlari qaysi algoritmlarda qo'llaniladi?

#AES, DES

Sezar, Affin

MD5, SHA1

A5/1, RC4

+++++

MD5 xesh algoritmidan nechta 32 bitli statik qiymatdan foydalanadi?

#4

8

12

16

+++++

Sezar shifrlash algoritmidan ochiq matn  $M=3$  ga, kalit  $K=7$  ga teng hamda  $p=26$  ga teng bo'sa shifr matn qiymati neciga teng bo'ladi?

#10

16

18

22

+++++

Qaysi xesh algoritmda 64 raund amal bajariladi?

#MD5

MAC

CRC

SHA1

+++++

DES shifrlash standarti qaysi davlat standarti?

#AQSH

Rossiya

Buyuk Britaniya

Germaniya

+++++

Qaysi blokli shifrlash algoritmda raund kalit uzunligi

qiymatiga bo'g'liq?

#AES

IDEA

DES

RSA

+++++

A5/1 oqimli shifrlash algoritmda  $x_{18}=1$ ,  $y_{21}=0$ ,  $z_{22}=1$

ga teng bo'lsa kalitni qiymatini toping

#0

1

2

3

+++++

Kolliziya hodisasi deb nimaga aytiladi?

#ikki xil matn uchun bir xil xesh qiymat chiqishi

ikki xil matn uchun ikki xil xesh qiymat chiqishi

bir xil matn uchun ikki xil xesh qiymat chiqishi

bir xil matn uchun bir xil xesh qiymat chiqishi bir xil

matn uchun bir xil xesh qiymat chiqishi

+++++

3 sonini 5 chekli maydonda teskarisini toping?

#2

3



4

5

+++++

Bir qiymatli shifrlash qanday amalga oshiriladi?

#ochiq ma'lumot alfaviti belgilarining har biriga shifr

ma'lumot alfavitining bitta belgisi mos qo'yiladi

ochiq ma'lumot alfaviti belgilarining har biriga shifr

ma'lumot alfavitining ikkita yoki undan ortiq chekli

sondagi belgilari mos qo'yiladi

ochiq ma'lumot alfaviti belgilarining har ikkitasiga shifr

ma'lumot alfavitining ikkita yoki undan ortiq chekli

sondagi belgilari mos qo'yiladi

ochiq ma'lumot alfaviti belgilarining har juftiga shifr

ma'lumot alfavitining bitta belgisi mos qo'yiladi

+++++

DES shifrlash algoritmda raundlar soni nechta?

#16

64

32

128

+++++

DES shifrlash algoritmda kalit uzunligi necha bitga teng?

#56

256

192

512

+++++

RC4 oqimli shifrlash algoritmi asosan qayerda

qo'llaniladi?

#simsiz aloqa vositalaridagi mavjud WEP protokolida

radioaloqa tarmoqlarda

internet trafiklarini shifrlashda

mobil aloqa standarti GSM protokolida

+++++

Xesh funsiyalarga qanday turlarga bo'linadi?

#kalitli va kalitsiz xesh funsiyalarga

kalitli va kriptografik bo'lmagan xesh funksiyalarga

kalitsiz va kriptografik bo'lmagan xesh funksiyalarga

kriptografik va kriptografik bo'lmagan xesh funksiyalarga

+++++

AES shifrlash algoritmda raundlar soni nechaga teng

bo'ladi?

#10, 12, 14

14, 16, 18

18, 20, 22

22, 24, 26

+++++

A5/1 oqimli shifrlash algoritmda har bir qadamda kalit

oqimining qanday qiymatini hosil qiladi?

#bir biti

bir bayti

64 biti

8 bayti

+++++

CRC-4 tizimida CRC qiymatini hisoblash jarayonida

ma'lumotga nechta nol biriktiriladi?

#4

8

16

12

+++++

Blokli simmetrik shifrlash algoritmlari raund

funksiyalarida qanday amallar bajariladi?

#ARX

PRX

XOR

RPT

+++++

CRC-6 tizimida CRC qiymati hisoblash jarayonida

ma'lumotga nechta nol biriktiriladi?

#6

12

18

24

+++++

Qaysi maxfiylikni ta'minlash usulida kalitdan

foydalanilmaydi?

#kodlash

shifrlash

autentifikatsiya

steganografiya

+++++

Vernam shifrlash algoritm asosi qaysi mantiqiy

hisoblashga asoslangan

#XOR

ARX

ROX

XRA

+++++

Chastotalar tahlili kriptotahlil usuli samarali ishlidigan

algorimtlar keltirilgan qatorni belgilang?

#Sezar, Affin

Vernam

Vijiner

RC4

+++++

Bitlar kesimida shifrlashni amalga oshiradigan algoritm

keltirilgan qatorni ko'rsating?

#A5/1

SHA1

RC4

MD5

+++++

Ma'lumotni konfidensialligini ta'minlash uchun ..... zarur.

#shifrlash

kodlash

rasshifrovkalash

deshifrlash

+++++

Foydanaluvchanlikni ta'minlash bu-?

#ruxsat etilmagan "bajarishdan" himoyalash

ruxsat etilmagan "yozishdan" himoyalash

ruxsat etilmagan "o'qishdan" himoyalash

ruxsat berilgan "amallarni" bajarish

+++++

Vijiner shifrlash algoritmi qaysi turdagi akslantirishga  
asoslanadi?

#o'rniga qo'yish

o'rin almashtirish

kompozitsion

aralash

+++++

Kompyuter davriga tegishli shifrlarni aniqlang?

#DES, AES shifri

kodlar kitobi

Sezar

Enigma shifri

+++++

.... shifrlar blokli va oqimli turlarga ajratiladi

#simmetrik

ochiq kalitli

klassik

assimetrik

+++++

DES shifrlash algoritmi bu?

#blokli shifrlash algoritmi

oqimli shifrlash algoritmi

ochiq kalitli shifrlash algoritmi

asimetrik shifrlash algoritmi

+++++

Ma'lumotga elektron raqamli imzo qo'yish hamda uni  
tekshirish qanday amalga oshiriladi?

#Ma'umotga raqamli imzo qo'yish maxfiy kalit orqali,  
imzoni tekshirish ochiq kalit orqali amalga oshiriladi

Ma'lumotga raqamli imzo qo'yish ochiq kalit orqali,  
imzoni tekshirish maxfiy kalit orqali amalga oshiriladi

Ma'lumotga raqamli imzo qo'yish maxfiy kalit orqali,  
imzoni tekshirish yopiq kalit orqali amalga oshiriladi

Ma'lumotga raqamli imzo qo'yish hamda uni tekshirish  
maxfiy kalit orqali amalga oshiriladi

+++++

A5/1 oqimli shifrlash algoritmda Z registr uzunligi nechi  
bitga teng?

#23

18

19

20

+++++

Kerkxofs printsipi bo'yicha qanday taxminlar ilgari  
suriladi?

#Kalitdan boshqa barcha ma'lumotlar barchaga ma'lum

Faqat kalit barchaga ma'lum

Barcha parametrlar barchaga ma'lum

Shifrlash kaliti barchaga ma'lum

+++++

Qaysi algoritm har bir qadamda bir bayt qiymatni  
shifrlaydi?

#RC4

A5/1

RSA

AES

+++++

A5/1 oqimli shifrlash algoritmda maxfiy kalit necha  
registrga bo'linadi?

#3

6

5

4

+++++

AES algoritmi qaysi tarmoq asosida qurilgan?

#SP

Feystel

Petri va SP

Petri

+++++

Elektron raqamli imzo bo'yicha birinchi O'z DSt 1092

qaysi korxona tomonidan ishlab chiqilgan?

#UNICON.UZ

INFOCOM

UZTELECOM

O'zR axborot texnologiyalari va kommunikatsiyalarini

rivojlantirish vazirligi

+++++

AES shifrlash algoritmi nomini kengaytmasini

ko'rsating?

#Advanced Encryption Standard

Advanced Encoding Standard

Advanced Encryption Stadium

Always Encryption Standard

+++++

A5/1 shifrlash algoritmi bu?

#oqimli shifrlash algoritmi

blokli shifrlash algoritmi

assimetrik shifrlash algoritmi

ochiq kalitli shifrlash algoritmi

+++++

RC4 shifrlash algoritmi qaysi turga mansub?

#oqimli shifrlar

blokli shifrlar

ochiq kalitli shifrlar

assimetrik shifrlar

+++++

Xeshlash algoritmlarini ko'rsating?

#SHA1, MD5, O'z DSt 1106

RSA, DSA, El-gamal

DES, AES, Blomfish

O'z DSt 1105, FOCT 28147-89, FEAL

+++++

AES shifrlash algoritmi bu?

#blokli shifrlash algoritmi

oqimli shifrlash algoritmi

ochiq kalitli shifrlash algoritmi

asimetrik shifrlash algoritmi

+++++

ARX amali qaysi shifrlash algoritmlarida foydalaniladi?

#Blokli shifrlashda

Ikki kalitli shifrlashda

Assimetrik shifrlashda

Ochiq kalitli shifrlashda

+++++

Kriptotizimlar kalitlar soni bo'yicha nechta turga

bo'linadi?

#2

3

4

5

+++++

A5/1 oqimli shifrlash algoritmida major qiymati hisoblash

jarayonida, uchinchi (Z) registrning qaysi qiymati

olinadi?

#z10

z11

z12

z13

+++++

A5/1 oqimli shifrlash algoritmida X registr uzunligi nech

bitga teng?

#19

16

17

15

+++++

Qaysi algoritmda har bir qadamda bir bit qiymatni

shifrlaydi?

#A5/1

RC4

RSA

AES

+++++

Mantiqiy XOR amalining asosi qanday hisoblashga

asoslangan?

#mod2 bo'yicha qo'shishga

mod2 bo'yicha ko'paytirishga

mod2 bo'yicha darajaga ko'tarishga

mod2 bo'yicha bo'lishga

+++++

Qaysi xesh algoritmda xesh qiymat 128 bitga teng

bo'ladi?

#MD5

SHA1

CRC

MAC

+++++

Qaysi xesh algoritmda xesh qiymat 160 bitga teng

bo'ladi?

#SHA1

MD5

CRC

MAC

+++++

Faqat AQSH davlatiga tegishli kriptografik standartlar

nomini ko'rsating?

#AES, DES

AES, GOST 28147-89

DES, O'z DST 1105-2009

SHA1, GOST 3412-94

+++++

RC4 shifrlash algoritmi simmetrik turga mansub bo'lsa,



unda nechta kalitdan foydalaniladi?

#1

2

3

4

+++++

A5/1 oqimli shifrlash algoritmda major qiymati hisoblash jarayonida, birinchi (X) registrning qaysi qiymati olinadi?

#x8

x9

x10

x11

+++++

DES shifrlash algoritmda S-bloklarga kiruvchi qiymatlar uzunligi necha bitga teng bo'ladi?

#6

12

24

18

+++++

MD5 xesh funksiyasida initsializatsiya bosqichida 4 ta necha bitli registrlardan foydalanadi?

#32

64

128

256

+++++

Imitatsiya turidagi hujumlarda ma'lumotlar qanday o'zgaradi?

#ma'lumot qalbakilashtiriladi

ma'lumot yo'q qilinadi

ma'lumot ko'chirib olinadi

ma'lumot dublikat qilinadi

+++++

Sezar shifrlash algoritmda rasshifrovkalash formulasi qanday?

# $M=(C-K) \bmod p$

$M=(C+K) \bmod p$

$M=(C*K) \bmod p$

$M=(C/K) \bmod p$

+++++

Faqat xesh funksiyalar nomi keltirilgan qatorni

ko'rsating?

#SHA1, MD5

SHA1, DES

MD5, AES

HMAC, A5/1

+++++

MD5 xesh funksiyasida chiquvchi qiymat uzunligi

nechaga teng?

#128

Ixtiyoriy

510

65

+++++

AES shifrlash algoritmi simmetrik turga mansub bo'lsa,

unda nechta kalitdan foydalaniladi?

#1

2

3

4

+++++

SHA1 xesh funksiyasida initsializatsiya bosqichida nechta

registrdan foydalanadi?

#5

10

15

20

+++++

MD5 xesh funksiyasida amallar nechta raund davomida

bajariladi?

#64

128

512

256

+++++

DES shifrlash algoritmda S-bloklardan chiqqan qiymatlar  
uzunligi necha bitga teng bo'ladi?

#4

8

12

16

+++++

MD5 xesh funksiyasida initsializatsiya bosqichida nechta  
32 bitli registrdan foydalanadi?

#4

8

12

16

+++++

Faqat oqimli simmetrik shifrlash algoritmlari nomi  
keltirilgan qatorni ko'rsating?

#A5/1, RC4

AES, DES

SHA1, RC4

A5/1, MD5

+++++

SHA1 xesh funksiyasida chiquvchi qiymat uzunligi  
nechaga teng?

#160

Ixtiyoriy

512

256

+++++

O'zgartirish turidagi hujumlarda ma'lumotlar qanday  
o'zgaradi?

#modifikatsiya qilinadi

ma'lumot yo'q qilinadi

ma'lumot dublikat qilinadi

ma'lumot ko'chirib olinadi

+++++

AES standarti qaysi algoritm asoslangan?

#Rijndael

RC6

Twofish

Serpent

+++++

SHA1 xesh funksiyasida amallar nechi raund davomida

bajariladi?

#80

128

256

512

+++++

2 lik sanoq tizimida 0101 soniga 1111 sonini 2 modul

bo'yicha qo'shing?

#1010

0101

1001

1111

+++++

AES shifrlash standarti qaysi davlat standarti?

#AQSH

Rossiya

Buyuk Britaniya

Germaniya

+++++

Qaysi algoritmda maj kattaligi ishlatiladi?

#A5/1

RC4

SHA1

MD5

+++++

Qalbakilashtirish hujumi qaysi turdagi hujum turiga

kiradi?

#Immitatsiya

o'zgartirish

Fabrication

modification

+++++

SHA1 xesh funksiyasi qaysi davlat standarti?

#AQSH

Rossiya

Germaniya

Buyuk Britaniya

+++++

Qayday akslantirishdan foydalanilsa chastotalar tahlili

kriptotahlil usuliga bardoshli bo'ladi

#bigram akslantirishidan

o'rniga qo'yish akslantirishidan

o'rin almashtirish akslantirishidan

xech qanday akslantirishdan foydalanish shart emas

+++++

SHA1 xesh algoritmda nechta 32 bitli statik qiymatdan

foydalanadi?

#5

10

15

20

+++++

A5/1 oqimli shifrlash algoritmda maj(1,0,1) ga teng

bo'lsa maj kattalik qiymatini toping?

#1

0

2

3

+++++

SHA1 xesh funksiyada 102 bitli ma'lumot berilganda

to'ldirish bitlari qanday to'ldiriladi?

#bir bit 1, 345 ta 0, ma'lumot uzunligi qiymatining 64

bitli qiymati bilan

bir bit 1, 345 ta 0, ma'lumot uzunligining dastlabki 64

bitli qiymati bilan

bir bit 1, 409 ta 0, ma'lumot uzunligi qiymatining 64 bitli

qiymati bilan

bir bit 1, 409 ta 0, ma'lumot uzunligining dastlabki 64

bitli qiymati bilan

+++++

Qaysi blokli shifrlash algoritmda 8 ta statik S-box lardan  
foydalaniladi?

#DES

RSA

RC4

A5/1

+++++

Kriptotizimlar kalitlar soni bo'yicha qanday turga  
bo'linadi?

#simmetrik va assimetrik turlarga

assimetrik va 2 kalitli turlarga

3 kalitli turlarga

simmetrik va bir kalitli turlarga

+++++

Ko'p qiymatli shifrlash qanday amalga oshiriladi?

#ochiq ma'lumot alfaviti belgilarining har biriga shifr

ma'lumot alfavitining ikkita yoki undan ortiq chekli

sondagi belgilari mos qo'yiladi

ochiq ma'lumot alfaviti belgilarining har ikkitasiga shifr

ma'lumot alfavitining ikkita yoki undan ortiq chekli

sondagi belgilari mos qo'yiladi

ochiq ma'lumot alfaviti belgilarining har biriga shifr

ma'lumot alfavitining bitta belgisi mos qo'yiladi

ochiq ma'lumot alfaviti belgilarining har juftiga shifr

ma'lumot alfavitining bitta belgisi mos qo'yiladi

+++++

A5/1 oqimli shifrlash algoritmi asosan qayerda  
qo'llaniladi?

#mobil aloqa standarti GSM protokolida

simsiz aloqa vositalaridagi mavjud WEP protokolida

internet trafiklarini shifrlashda

radioaloqa tarmoqlarida

+++++

Assimetrik kriptotizimlarda necha kalitdan foydalaniladi?

#2 ta

3 ta

4 ta

kalit ishlatilmaydi

+++++

AES algoritmda shifrlash kalitining uzunligi necha bitga  
teng?

#128, 192, 256 bit

128, 156, 256 bit

256, 512 bit

128, 192 bit

+++++

Kalit bardoshliligi bu -?

#eng yaxshi ma'lum algoritm bilan kalitni topish

murakkabligidir

eng yaxshi ma'lum algoritm yordamida yolg'on axborotni  
ro'kach qilishdir

amaliy bardoshlilik

nazariy bardoshlilik

+++++

RC4 oqimli shifrlash algoritmda har bir qadamda kalit  
oqimining qanday qiymatini hosil qiladi?

#bir baytini

bir bitini

64 bitini

8 baytini

+++++

AES algoritmda nechta akslantirishlardan foydalaniladi?

#4

2

5

6

+++++

Qanday funksiyalarga xesh funksiya deyiladi?

#ixtiyoriy uzunlikdagi ma'lumotni biror fiksirlangan

uzunlikga o'tkazuvchi funksiyaga aytiladi

ma'lumot baytlarini boshqa qiymatlarga almashtiruvchi

funksiyaga aytiladi

ma'lumot bitlarini boshqa qiymatlarga almashtiruvchi

funksiyaga aytiladi

ixtiyoriy uzunlikdagi ma'lumotni bit yoki baytlarini

zichlashtirib beruvchi funksiyaga aytiladi

+++++

Xesh funksiyalar qanday maqsadlarda ishlatiladi?

#ma'lumotni to'liqligini nazoratlash va ma'lumot

manbaini autentifikatsiyalashda

ma'lumot manbaini autentifikatsiyalashda

ma'lumotni butunligini nazoratlashda

ma'lumotni maxfiyligini nazoratlash va ma'lumot

manbaini haqiqiylikini tekshirishda

+++++

Ma'lumotni sakkizlik sanoq tizimidan o'n oltilik sanoq

tizimiga o'tkazish bu?

#kodlash

rasshifrovkalash

yashirish

shifrlash

+++++

A5/1 shifri qaysi turga mansub?

#oqimli shifrlar

blokli shifrlar

ochiq kalitli shifrlar

assimetrik shifrlar

+++++

Qaysi algoritmlar simmetrik blokli shifrlarga tegishli?

#AES, DES



A5/1, AES

Vijiner, DES

Sezar, AES

+++++

Ma'lumotni mavjudligini yashirishni maqsad qilgan bilim  
sohasi bu?

#steganografiya

kriptografiya

kodlash

kriptotahlil

+++++

Faqat simmetrik blokli shifrlarga xos bo'lgan atamani  
aniqlang?

#blok uzunligi

kalit uzunligi

ochiq kalit

kodlash jadvali

+++++

Quyidagi ta'rif qaysi atamaga tegishli: "maxfiy  
kodlarni"ni buzish bilan shug'ullanadigan soha-bu?

#kriptotahlil

kripto

kriptologiya

kriptografiya

+++++

Qadimiy davr klassik shifriga quyidagilarning qaysi biri  
tegishli?

#Sezar

kodlar kitobi

Enigma shifri

DES, AES shifri

+++++

Quyidagi ta'rif qaysi kriptotizimga tegishli: ochiq matnni  
shifrlashda hamda rasshifrovkalashda mos holda ochiq va  
maxfiy kalitdan foydalanadi?

#ochiq kalitli kriptotizimlar

maxfiy kalitli kriptotizimlar

simmetrik kriptotizimlar

elektron raqamli imzo tizimlari

+++++

Simmetrik shifrlar axborotni qaysi xususiyatlarini

ta'minlashda foydalaniladi?

#konfidensiallik va yaxlitlik

konfidensiallik va foydalanuvchanlik

foydalanuvchanlik va yaxlitlik

foydalanuvchanlik

+++++

Qanday algorimtlar qaytmas xususiyatiga ega

hisoblanadi?

#xesh funksiyalar

elektron raqamli imzo algoritmlari

simmetrik kriptotizimlar

ochiq kalitli kriptotizimlar

+++++

Ochiq matn qismlarini takror shifrlashga asoslangan usul

bu?

#blokli shifrlar

oqimli shifrlar

assimetrik shifrlar

ochiq kalitli shifrlar

+++++

Ochiq kalitli shifrlashda deshifrlash qaysi kalit asosida

amalga oshiriladi?

#shaxsiy kalit

ochiq kalit

kalitdan foydalanilmaydi

umumiy kalit

+++++

Quyidagi ta'rif qaysi atamaga tegishli: "maxfiy

kodlarni"ni yaratish bilan shug'ullanadigan soha-bu?

#kriptografiya

kriptologiya

kriptotahlil

kripto

+++++

Simmetrik kriptotizimlarning asosiy kamchiligi bu?

#kalitni taqsimlash zaruriyati

kalitlarni esda saqlash murakkabligi

shifrlash jarayonining ko'p vaqt olishi

algoritmlarning xavfsiz emasligi

+++++

Kriptotizimni boshqaradigan vosita?

#kalit

algoritm

stegokalit

kriptotizim boshqarilmaydi

+++++

Quyidagi ta'rif qaysi kriptotizimga tegishli:ochiq matnni

shifrlashda hamda rasshifrovkalashda bitta maxfiy

kalitdan foydalaniladi?

#simmetrik kriptotizimlar

nosimmetrik kriptotizimlar

ochiq kalitli kriptotizimlar

assimetrik kriptotizimlar

+++++

Kerxgofs prinsipiga ko'ra kriptotizimning to'liq xavfsiz

bo'lishi faqat qaysi kattalik nomalum bo'lishiga

asoslanishi kerak?

#kalit

protokol

shifrmavn

Algoritm

+++++

Xesh funksiyalar nima maqsadda foydalaniladi?

#ma'lumotlar yaxlitligini ta'minlashda

ma'lumot egasini autentifikatsiyalashda

ma'lumot maxfiyligini ta'minlashda

ma'lumot manbaini autentifikatsiyalashda

+++++

Chastotalar tahlili hujumi qanday amalga oshiriladi?

#shifr matnda qatnashgan harflar sonini aniqlash orqali

shifr matnda eng kam qatnashgan harflarni aniqlash orqali

ochiq matnda qatnashgan harflar sonini aniqlash orqali

ochiq matnda eng kam qatnashgan harflarni aniqlash

orqali

+++++

Xesh funksiyaga tegishli bo'lgan talabni aniqlang?

#bir tomonlama funksiya bo'lishi

chiqishda ixtiyoriy uzunlikda bo'lishi

turli kirishlar bir xil chiqishlarni akslantirishi

kolliziyaga bardoshli bo'lmasligi

+++++

RC4 shifrlash algoritmi bu?

#oqimli shifrlash algoritmi

ochiq kalitli shifrlash algoritmi

blokli shifrlash algoritmi

asimetrik shifrlash algoritmi

+++++

A5/1 shifrlash algoritmi simmetrik turga mansub bo'lsa,

unda nechta kalitdan foydalaniladi?

#1

2

3

4

+++++

Qaysi algoritmda, algoritmning necha round bajarilishi

ochiq matn uzunligiga bog'liq?

#A5/1

MD5

HMAC

SHA1

+++++

Simmetrik va ochiq kalitli kriptotizimlar asosan nimasi

bilan bir biridan farq qiladi?

#kalitlar soni bilan

matematik murakkabligi bilan

farq qilmaydi

biri maxfiylikni ta'minlasa, biri butunlikni ta'minlaydi

+++++

A5/1 oqimli shifrlash algoritmda major qiymati hisoblash

jarayonida, ikkinchi (Y) registrning qaysi qiymati olinadi?

#y10

y11

y12

y13

+++++

Kalitli xesh funksiyalar qanday turdagi hujumlardan

himoyalaydi?

#imitatsiya va o'zgartirish turidagi hujumlardan

ma'lumotni oshkor qilish turidagi hujumlardan

DDOS hujumlaridan

foydalanishni buzishga qaratilgan hujumlardan

+++++

Sezar shifrlash algoritmda shifrlash formulasi qanday?

# $C=(M+K) \bmod p$

$C=(M-K) \bmod p$

$C=(M*K) \bmod p$

$C=(M/K) \bmod p$

+++++

A5/1 oqimli shifrlash algoritmda Y registr uzunligi nech

bitga teng?

#22

20

19

21

+++++

Kalitli xesh funksiyalardan foydalanish nimani

kafolatlaydi?

#fabrikatsiyani va modifikatsiyani oldini oladi

ma'lumot yo'q qilinadi

ma'lumot dublikat qilinadi

ma'lumot ko'chirib olinadi

+++++

DES shifrlash algoritmi simmetrik turga mansub bo'lsa,

unda nechta kalitdan foydalaniladi?

#1

2

3

4

+++++

AES tanlovi g'olibi bo'lgan algoritm nomini ko'rsating?

Rijndael

IDEA

Blowfish

Twofish

+++++

AES shifrlash algoritmida 128 bitli ma'lumot bloki

qanday o'lchamdagi jadvalga solinadi?

#4x4

4x6

6x4

6x6

+++++

A5/1 oqimli shifrlash algoritmida maj(1,0,1) ga teng

bo'lsa qaysi registrlar suriladi?

#birinchi va uchunchi registrlar suriladi

faqat ikkinchi registr suriladi

birinchi va ikkinchi registrlar suriladi

faqat birinchi resgistr suriladi

+++++

GSM tarmog'ida foydalaniluvchi shifrlash algoritmi

nomini ko'rsating?

#A5/1

DES

RC4

AES

+++++

HMAC tizimida kalit qiymati blok uzunligidan katta

bo'lganda ma'lumotga qanday biriktiriladi?

#kalitni xesh qiymati hisoblanib, unga blok uzunligiga

teng bo'lguncha nol qiymat qo'shiladi va yangi hosil

bo'lgan qiymat ma'lumotga biriktiriladi

kalit qiymati blok uzunligiga teng bo'lguncha nol qiymat

bilan to'ldirilib hosil bo'lgan qiymat ma'lumotga

biriktiriladi

kalit qiymati o'zgartirilmagan holda ma'lumotga

biriktiriladi

xesh funksiyalarda kalit qiymatidan foydalanilmaydi

+++++

Qaysi xesh algoritmda 80 raund amal bajariladi?

#SHA1

CRC

MD5

MAC

+++++

Affin shifrlash algoritmda  $a=2$ ,  $b=3$ ,  $p=26$  hamda ochiq

matn  $x=4$  ga teng bo'lsa, shifr matn qiymatini toping?

#11

27

41

31

+++++

MD5 xesh funksiyada 48 bitli ma'lumot berilganda

to'ldirish bitlari qanday to'ldiriladi?

#bir bit 1, 399 ta 0, ma'lumot uzunligi qiymatining 64

bitli qiymati bilan

bir bit 1, 399 ta 0, ma'lumot uzunligining dastlabki 64

bitli qiymati bilan

bir bit 1, 463 ta 0, ma'lumot uzunligi qiymatining 64 bitli

qiymati bilan

bir bit 1, 463 ta 0, ma'lumot uzunligining dastlabki 64

bitli qiymati bilan

+++++

AES shifrlash algoritmda ochiq matn bilan dastlab

qanday amal bajariladi?

#ochiq matn dastlabki kalit bilan XOR amali bajariladi

ochiq matn birinchi raund kalit bilan XOR amali

bajariladi

ochiq matn ustida dastlab SubBytes akslantirishi amali

bajariladi

ochiq matn ustida dastlab ShiftRows akslantirishi amali

bajariladi

+++++

Vernam shifrlash algoritmda ochiq matn  $M=101$  ga, kalit

$K=111$  ga teng bo'lsa shifr matn qiymati qanday bo'ladi?

#010

101

111

110

?Konfidensiallikni ta'minlash bu - ?

+ruxsatsiz o'qishdan himoyalash.

-ruxsatsiz yozishdan himoyalash.

-ruxsatsiz bajarishdan himoyalash.

-ruxsat etilgan amallarni bajarish.

?Foydalanuvchanlikni ta'minlash bu - ?

+ruxsatsiz bajarishdan himoyalash.

-ruxsatsiz yozishdan himoyalash.

-ruxsatsiz o'qishdan himoyalash.

-ruxsat etilgan amallarni bajarish.

?Yaxlitlikni ta'minlash bu - ?

+ruxsatsiz yozishdan himoyalash.

-ruxsatsiz o'qishdan himoyalash.

-ruxsatsiz bajarishdan himoyalash.

-ruxsat etilgan amallarni bajarish.

?Jumlani to'ldiring. Hujumchi kabi fikrlash ... kerak.

+bo'lishi mumkin bo'lgan xavfni oldini olish uchun

-kafolatlangan amallarni ta'minlash uchun

-ma'lumot, axborot va tizimdan foydalanish uchun



-ma lumotni aniq va ishonchli ekanligini bilish uchun

?Jumlani to'ldiring. Tizimli fikrlash ... uchun kerak.

+kafolatlangan amallarni ta'minlash

-bo'lishi mumkin bo'lgan xavfni oldini olish

-ma lumot, axborot va tizimdan foydalanish

-ma lumotni aniq va ishonchli ekanligini bilish

?Axborot xavfsizligida risk bu?

+Manbaga zarar keltiradigan ichki yoki tashqi zaiflik ta'sirida tahdid qilish ehtimoli.

-U yoki bu faoliyat jarayonida nimaga erishishni xohlashimiz.

-Tashkilot uchun qadrlil bo'lgan ixtiyoriy narsa.

-Tizim yoki tashkilotga zarar yetkazishi mumkin bo'lgan istalmagan hodisa.

?Axborot xavfsizligida tahdid bu?

+Aktivga zarar yetkazishi mumkin bo'lgan istalmagan hodisa.

-Noaniqlikning maqsadlarga ta'siri.

-U yoki bu faoliyat jarayonida nimaga erishishni xohlashimiz.

-Tashkilot uchun qadrlil bo'lgan ixtiyoriy narsa.

?Axborot xavfsizligida aktiv bu?

+Tashkilot yoki foydalanuvchi uchun qadrlil bo'lgan ixtiyoriy narsa.

-Tizim yoki tashkilotga zarar yetkazishi mumkin bo'lgan istalmagan hodisa.

-Noaniqlikning maqsadlarga ta'siri.

-U yoki bu faoliyat jarayonida nimaga erishishni xohlashimiz.

?Axborot xavfsizligida zaiflik bu?

+Tahdidga sabab bo'luvchi tashkilot aktivi yoki boshqaruv tizimidagi nuqson.

-Tashkilot uchun qadrlil bo'lgan ixtiyoriy narsa.

-Tizim yoki tashkilotga zarar yetkazishi mumkin bo'lgan istalmagan hodisa.

-Noaniqlikning maqsadlarga ta'siri.

?Axborot xavfsizligida boshqarish vositasi bu?

+Natijasi zaiflik yoki tahdidga ta'sir qiluvchi riskni o'zgartiradigan harakatlar.

-Bir yoki bir nechta tahdidga sabab bo'luvchi tashkilot aktivi yoki boshqaruv tizimidagi kamchilik.

-Tashkilot uchun qadrlil bo'lgan ixtiyoriy narsa.

-Tizim yoki tashkilotga zarar yetkazishi mumkin bo'lgan istalmagan hodisa.

?Har qanday vaziyatda biror bir hodisani yuzaga kelish ehtimoli qo'shilsa ....

+risk paydo bo'ladi.

-hujum paydo bo'ladi.

-tahdid paydo bo'ladi.

-aktiv paydo bo'ladi.

?Jumlani to'ldiring. Denial of service (DOS) hujumi axborotni .... xususiyatini buzushga qaratilgan.

+foydalanuvchanlik

-butunlik

-konfidensiallik

-ishonchlilik

?Jumlani to'ldiring. ... sohasi tashkilot etuvchilar xavfsizligi, aloqa xavfsizligi va dasturiy ta'minotlar xavfsizligidan iborat.

+Tizim xavfsizligi

-Ma'lumotlar xavfsizligi

-Inson xavfsizligi

-Tashkilot xavfsizligi

?Kriptologiya so'ziga berilgan to'g'ri tavsifni toping?

+Maxfiy shifrlarni yaratish va buzish fani va sanati.

-Maxfiy shifrlarni yaratish fani va sanati.

-Maxfiy shifrlarni buzish fani va sanati.

-Axborotni himoyalash fani va sanati.

?.... kriptotizimni shifrlash va deshifrlash uchun sozlashda foydalaniladi.

+Kriptografik kalit

-Ochiq matn

-Alifbo

-Algoritm

?Kriptografiya so'ziga berilgan to'g'ri tavsifni toping?

+Maxfiy shifrlarni yaratish fani va sanati.

-Maxfiy shifrlarni yaratish va buzish fani va sanati.

-Maxfiy shifrlarni buzish fani va sanati.

-Axborotni himoyalash fani va sanati.

?Kriptotahlil so'ziga berilgan to'g'ri tavsifni toping?

+Maxfiy shifrlarni buzish fani va sanati.

-Maxfiy shifrlarni yaratish fani va sanati.

-Maxfiy shifrlarni yaratish va buzish fani va sanati.

-Axborotni himoyalash fani va sanati.

?..... axborotni ifodalash uchun foydalaniladigan chekli

sondagi belgilar to'plami.

+Alifbo

-Ochiq matn

-Shifrmtn

-Kodlash

?Ma'lumot shifrlansa, natijasi .... bo'ladi.

+shifrmtn

-ochiq matn

-nomalum

-kod

?Deshifrlash uchun kalit va ..... kerak bo'ladi.

+shifrmtn

-ochiq matn

-kodlash

-alifbo

?Ma'lumotni shifrlash va deshifrlashda yagona kalitdan

foydalanuvchi tizim bu -

+simmetrik kriptotizim.

-ochiq kalitli kriptotizim.

-asimetrik kriptotizim.

-xesh funksiyalar.

?Ikki kalitli kriptotizim bu -

+ochiq kalitli kriptotizim.

-simmetrik kriptotizim.

-xesh funksiyalar.

-MAC tizimlari.

?Axborotni mavjudligini yashirish bilan shug ullanuvchi

fan sohasi bu -

+steganografiya.

-kriptografiya.

-kodlash.

-kriptotahlil.

?Axborotni foydalanuvchiga qulay tarzda taqdim etish

uchun ..... amalga oshiriladi.

+kodlash

-shifrlash

-yashirish

-deshifrlash

?Jumlani to ldiring. Ma lumotni konfidensialligini ta

minlash uchun ..... zarur.

+shifrlash

-kodlash

-dekodlash

-deshifrlash

?Ma lumotni mavjudligini yashirishda .....

+steganografik algoritmdan foydalaniladi.

-kriptografik algoritmdan foydalaniladi.

-kodlash algoritmidan foydalaniladi.

-kriptotahlil algoritmidan foydalaniladi.

?Xesh funksiyalar - .... funksiya.

+kalitsiz kriptografik

-bir kalitli kriptografik

-ikki kalitli kriptografik

-ko p kalitli kriptografik

?Jumlani to ldiring. Ma lumotni uzatishda kriptografik

himoya .....

+konfidensiallik va butunlikni ta minlaydi.

-konfidensiallik va foydalanuvchanlikni ta minlaydi.

-foydalanuvchanlik va butunlikni ta minlaydi.

-konfidensiallik ta minlaydi.

?Jumlani to lding. ... kompyuter davriga tegishli

shifrlarga misol bo la oladi.

+DES, AES shifri

-Sezar shifri

-Kodlar kitobi

-Enigma shifri

?... kriptografik shifrlash algoritmlari blokli va oqimli

turlarga ajratiladi.

+Simmetrik

-Ochiq kalitli

-Asimmetrik

-Klassik davr

?Jumlani to lding. .... shifrlar tasodifiy ketma-ketliklarni

generatsiyalashga asoslanadi.

+Oqimli

-Blokli

-Ochiq kalitli

-Asimetrik

?Ochiq matn qismlarini takroriy shifrovchi algoritmlar bu

-

+blokli shifrlar

-oqimli shifrlash

-ochiq kalitli shifrlar

-asimmetrik shifrlar

?A5/1 shifri bu -

+oqimli shifr.

-blokli shifr.

-ochiq kalitli shifr.

-asimmetrik shifr

?Quyidagi muammolardan qaysi biri simmetrik

kriptotizimlarga xos.

+Kalitni taqsimlash zaruriyati.

-Shifrlash jarayonining ko p vaqt olishi.

-Kalitlarni esda saqlash murakkabligi.

-Foydalanuvchilar tomonidan maqbul ko rilmasligi.

?Quyidagi atamalardan qaysi biri faqat simmetrik blokli

shifrlarga xos?

+Blok uzunligi.

-Kalit uzunligi.

-Ochiq kalit.

-Kodlash jadvali.

?Jumlani to'ldiring. Sezar shifri .... akslantirishga

asoslangan.

+o'rniga qo'yish

-o'rnini almashtirish

-ochiq kalitli

-kombinatsion

?Kriptotizimning to'liq xavfsiz bo'lishi Kerxgofs

prinsipiga ko'ra qaysi kattalikning nomalumi bo'lishiga

asoslanadi?

+Kalit.

-Algoritm.

-Shifratma.

-Protokol.

?Shifrlash va deshifrlashda turli kalitlardan foydalanuvchi

shifrlar bu -

+ochiq kalitli shifrlar.

-simmetrik shifrlar.

-bir kalitli shifrlar

-xesh funksiyalar.

?Agar simmetrik kalitning uzunligi 64 bit bo'lsa, jami bo

lishi mumkin bo'lgan kalitlar soni nechta?

+264

-64!

-642

-263

?Axborotni qaysi xususiyatlari simmetrik shifrlar

yordamida ta'minlanadi.

+Konfidentsiallik va butunlik.

-Konfidentsiallik.

-Butunlik va foydalanuvchanlik.

-Foydalanuvchanlik va konfidensiallik.

?Axborotni qaysi xususiyatlari ochiq kalitli shifrlar yordamida ta'minlanadi.

+Konfidensiallik.

-Konfidensiallik, butunlik va foydalanuvchanlik.

-Butunlik va foydalanuvchanlik.

-Foydalanuvchanlik va konfidensiallik.

?Elektron raqamli imzo tizimi.

+MAC tizimlari.

-Simmetrik shifrlash tizimlari.

-Xesh funksiyalar.

-Butunlik va foydalanuvchanlik.

?Qaysi ochiq kalitli algoritm katta sonni faktorlash muammosiga asoslanadi?

+RSA algoritmi.

-El-Gamal algoritmi.

-DES.

-TEA.

?Rad etishdan himoyalashda ochiq kalitli kriptotizimlarning qaysi xususiyati muhim hisoblanadi.

+Ikkita kalitdan foydalanilgani.

-Matematik muammoga asoslanilgani.

-Ochiq kalitni saqlash zaruriyati mavjud emasligi.

-Shaxsiy kalitni saqlash zarurligi.

?Quyidagi talablardan qaysi biri xesh funksiyaga tegishli emas.

+Bir tomonlama funksiya bo'lmayligi kerak.

-Amalga oshirishdagi yuqori tezkorlik.

-Turli kirishlar turli chiqishlarni akslantirishi.

-Kolliziyaga bardoshli bo'lishi.

?Quyidagi xususiyatlardan qaysi biri elektron raqamli imzo tomonidan ta'minlanadi?

+Axborot butunligini va rad etishdan himoyalash.

-Axborot konfidensialligini va rad etishdan himoyalash.

-Axborot konfidensialligi.

-Axborot butunligi.

?Faqat ma lumotni butunligini ta minlovchi

kriptotizimlarni ko rsating.

+MAC (Xabarlarni autentifikatsiya kodlari) tizimlari.

-Elektron raqamli imzo tizimlari.

-Ochiq kalitli kriptografik tizimlar.

-Barcha javoblar to g ri.

?Foydalanuvchini tizimga tanitish jarayoni bu?

+Identifikatsiya.

-Autentifikatsiya.

-Avtorizatsiya.

-Ro yxatga olish.

?Foydalanuvchini haqiqiylikini tekshirish jarayoni bu?

+Autentifikatsiya.

-Identifikatsiya.

-Avtorizatsiya.

-Ro yxatga olish.

?Tizim tomonidan foydalanuvchilarga imtiyozlar berish jarayoni bu?

+Avtorizatsiya.

-Autentifikatsiya.

-Identifikatsiya.

-Ro yxatga olish.

?Parolga asoslangan autentifikatsiya usulining asosiy kamchiligini ko rsating?

+Esda saqlash zaruriyati.

-Birga olib yurish zaruriyati.

-Almashtirib bo lmaslik.

-Qalbakilashtirish mumkinligi.

?Biror narsani bilishga asoslangan autentifikatsiya deyilganda quyidagilardan qaysilar tushuniladi.

+PIN, Parol.

-Token, mashinaning kaliti.

-Yuz tasviri, barmoq izi.

-Biometrik parametrlar.

?Tokenga asoslangan autentifikatsiya usulining asosiy kamchiligini ayting?



+Doimo xavfsiz saqlab olib yurish zaruriyati.

-Doimo esada saqlash zaruriyati.

-Qalbakilashtirish muammosi mavjudligi.

-Almashtirib bo'lmazlik.

?Esda saqlashni va olib yurishni talab etmaydigan

autentifikatsiya usuli bu -

+biometrik autentifikatsiya.

-parolga asoslangan autentifikatsiya.

-tokenga asoslangan autentifikatsiya.

-ko p faktorli autentifikatsiya.

?Qaysi biometrik parametr eng yuqori universallik

xususiyatiga ega?

+Yuz tasviri.

-Ko z qorachig'i.

-Barmoq izi.

-Qo'l shakli.

?Qaysi biometrik parametr eng yuqori takrorlanmaslik

xususiyatiga ega?

+Ko z qorachig'i.

-Yuz tasviri.

-Barmoq izi.

-Qo'l shakli.

?Quyidagilardan qaysi biri har ikkala tomonning

haqiqiylikni tekshirish jarayonini ifodalaydi?

+Ikki tomonlama autentifikatsiya.

-Ikki faktorli autentifikatsiya.

-Ko p faktorli autentifikatsiya.

-Biometrik autentifikatsiya.

?Parolga asoslangan autentifikatsiya usuliga qaratilgan

hujumlarni ko'rsatadi?

+Parollar lug'atidan foydalanish asosida hujum, yelka

orqali qarash hujumi, zararli dasturlardan foydalanish

asosida hujum.

-Fizik o'g'irlash hujumi, yelka orqali qarash hujumi,

zararli dasturlardan foydalanish asosida hujum.

-Parollar lug'atidan foydalanish asosida hujum, yelka

orqali qarash hujumi, qalbakilashtirish hujumi.

-Parollar lug atidan foydalanish asosida hujum, bazadagi parametrni almashtirish hujumi, zararli dasturlardan foydanish asosida hujum.

?Tokenga asoslangan autentifikatsiya usuliga qaratilgan hujumlarni ko rsating?

+Fizik o g irlash, mobil qurilmalarda zararli dasturlardan foydalanishga asoslangan hujumlar

-Parollar lug atidan foydalanish asosida hujum, yelka orqali qarash hujumi, zararli dasturlardan foydanish asosida hujum

-Fizik o g irlash, yelka orqali qarash hujumi, zararli dasturlardan foydalanishga asoslangan hujumlar

-Parollar lug atidan foydalanish asosida hujum, bazadagi parametrni almashtirish hujumi, zararli dasturlardan foydalanish asosida hujum

?Foydalanuvchi parollari bazada qanday ko rinishda saqlanadi?

+Xeshlangan ko rinishda.

-Shifrlangan ko rinishda.

-Ochiq holatda.

-Bazada saqlanmaydi.

?Agar parolning uzunligi 8 ta belgi va har bir o rinda 128 ta turlicha belgidan foydalanish mumkin bo lsa, bo lishi mumkin bo lgan jami parollar sonini toping.

+1288

-8128

-128!

-2128

?Parolni "salt" (tuz) kattaligidan foydalanib xeshlashdan (h(password, salt)) asosiy maqsad nima?

+Buzg unchiga ortiqcha hisoblashni talab etuvchi murakkablikni yaratish.

-Buzg unchi topa olmasligi uchun yangi nomalum kiritish.

-Xesh qiymatni tasodifiylik darajasini oshirish.

-Xesh qiymatni qaytmaslik talabini oshirish.

?Quyidagilardan qaysi biri tabiiy tahdidga misol bo'ladi?

+Yong'in, suv toshishi, harorat ortishi.

-Yong'in, o'g'irlik, qisqa tutashuvlar.

-Suv toshishi, namlikni ortib ketishi, bosqinchilik.

-Bosqinchilik, terrorizm, o'g'irlik.

?Qaysi nazorat usuli axborotni fizik himoyalashda inson faktorini mujassamlashtirgan?

+Mamuriy nazoratlash.

-Fizik nazoratlash.

-Texnik nazoratlash.

-Apparat nazoratlash.

?Faqat ob'ektning egasi tomonidan foydalanishga mos bo'lgan mantiqiy foydalanish usulini ko'rsating?

+Diskretion foydalanishni boshqarish.

-Mandatli foydalanishni boshqarish.

-Rolga asoslangan foydalanishni boshqarish.

-Attributga asoslangan foydalanishni boshqarish.

?Qaysi usul ob'ektlar va sub'ektlarni klassifikatsiyalashga asoslangan?

+Mandatli foydalanishni boshqarish.

-Diskretion foydalanishni boshqarish.

-Rolga asoslangan foydalanishni boshqarish.

-Attributga asoslangan foydalanishni boshqarish.

?Biror faoliyat turi bilan bog'liq harakatlar va majburiyatlar to'plami bu?

+Rol.

-Imtiyoz.

-Daraja.

-Imkoniyat.

?Qoida, siyosat, qoida va siyosatni mujassamlashtirgan algoritmlar, majburiyatlar va maslahatlar kabi tushunchalar qaysi foydalanishni boshqarish usuliga aloqador.

+Attributga asoslangan foydalanishni boshqarish.

-Rolga asoslangan foydalanishni boshqarish.

-Mandatli foydalanishni boshqarish.

-Diskretion foydalanishni boshqarish.

?Bell-Lapadula modeli axborotni qaysi xususiyatini ta minlashni maqsad qiladi?

+Konfidensiallik.

-Butunlik.

-Foydalanuvchanlik.

-Ishonchlilik.

?Biba modeli axborotni qaysi xususiyatini ta minlashni maqsad qiladi?

+Butunlik.

-Konfidensiallik.

-Foydalanuvchanlik.

-Maxfiylik.

?Qaysi turdagi shifrlash vositasida barcha kriptografik parametrlar kompyuterning ishtirokisiz generatsiya qilinadi?

+Apparat.

-Dasturiy.

-Simmetrik.

-Ochiq kalitli.

?Qaysi turdagi shifrlash vositasida shifrlash jarayonida boshqa dasturlar kabi kompyuter resursidan foydalanadi?

+Dasturiy.

-Apparat.

-Simmetrik.

-Ochiq kalitli.

?Yaratishda biror matematik muammoga asoslanuvchi shifrlash algoritmini ko rsating?

+Ochiq kalitli shifrlar.

-Simmetrik shifrlar.

-Blokli shifrlar.

-Oqimli shifrlar.

?Xesh funksiyalarda kolliziya hodisasi bu?

+Ikki turli matnlarning xesh qiymatlarini bir xil bo lishi.

-Cheksiz uzunlikdagi axborotni xeshlay olishi.

-Tezkorlikda xeshlash imkoniyati.

-Turli matnlar uchun turli xesh qiymatlarni hosil bo'lishi.

?64 ta belgidan iborat Sezar shifrlash usulida kalitni bilmasdan turib nechta urinishda ochiq matnni aniqlash mumkin?

+63

-63!

-32

-322

?Elektron raqamli imzo muolajalarini ko'rsating?

+Imzoni shakllantirish va imkoni tekshirish.

-Shifrlash va deshifrlash.

-Imzoni xeshlash va xesh matnni deshifrlash.

-Imzoni shakllantirish va xeshlash.

? "Yelka orqali qarash" hujumi qaysi turdagi autentifikatsiya usuliga qaratilgan.

+Parolga asoslangan autentifikatsiya.

-Tokenga asoslangan autentifikatsiya.

-Biometrik autentifikatsiya.

-Ko'z qorachig'iga asoslangan autentifikatsiya.

?Sotsial injineriyaga asoslangan hujumlar qaysi turdagi autentifikatsiya usuliga qaratilgan.

+Parolga asoslangan autentifikatsiya.

-Tokenga asoslangan autentifikatsiya.

-Biometrik autentifikatsiya.

-Ko'z qorachig'iga asoslangan autentifikatsiya.

?Yo'qolgan holatda almashtirish qaysi turdagi autentifikatsiya usuli uchun eng arzon.

+Parolga asoslangan autentifikatsiya.

-Tokenga asoslangan autentifikatsiya.

-Biometrik autentifikatsiya.

-Ko'z qorachig'iga asoslangan autentifikatsiya.

?Qalbakilashtirish hujumi qaysi turdagi autentifikatsiya usuliga qaratilgan.

+Biometrik autentifikatsiya.

-Biror narsani bilishga asoslangan autentifikatsiya.

-Biror narsaga egalik qilishga asoslangan autentifikatsiya.

-Tokenga asoslangan autentifikatsiya

?Axborotni butunligini ta minlash usullarini ko rsating.

+Xesh funksiyalar, MAC.

-Shifrlash usullari.

-Assimetrik shifrlash usullari, CRC tizimlari.

-Shifrlash usullari, CRC tizimlari.

?Quyidagilardan qaysi biri to liq kompyuter

topologiyalarini ifodalamaydi.

+LAN, GAN, OSI.

-Yulduz, WAN, TCP/IP.

-Daraxt, IP, OSI.

-Shina, UDP, FTP.

?OSI tarmoq modeli nechta sathdan iborat?

+7

-4

-6

-5

?TCP/IP tarmoq modeli nechta sathdan iborat?

+4

-7

-6

-5

?Hajmi bo yicha eng kichik hisoblangan tarmoq turi bu -

+PAN

-LAN

-CAN

-MAN

?IPv6 protokolida IP manzilni ifodalashda necha bit

ajratiladi.

+128

-32

-64

-4

?IP manzilni domen nomlariga yoki aksincha

almashtirishni amalga oshiruvchi xizmat bu-

+DNS

-TCP/IP

-OSI

-UDP

?Natijasi tashkilotning amallariga va funksional

harakatlariga zarar keltiruvchi hodisalarning potensial

paydo bo'lishi bu?

+Tahdid.

-Zaiflik.

-Hujum.

-Aktiv.

?Zaiflik orqali AT tizimi xavfsizligini buzish tomon

amalga oshirilgan harakat bu?

+Hujum.

-Zaiflik.

-Tahdid.

-Zararli harakat.

?Quyidagilardan qaysi biri tarmoq xavfsizligi

muammolariga sabab bo'lmaydi?

+Routerlardan foydalanmaslik.

-Qurilma yoki dasturiy vositani noto'g'ri sozlanish.

-Tarmoqni xavfsiz bo'lmagan tarzda va zaif loyihalash.

-Tug'na texnologiya zaifligi.

?Tarmoq xavfsizligini buzulishi biznes faoliyatga qanday

ta'sir qiladi?

+Biznes faoliyatning buzilishi, huquqiy javobgarlikka

sababchi bo'ladi.

-Axborotni o'g'irlanishi, tarmoq qurilmalarini fizik

buzilishiga olib keladi.

-Maxfiylikni yo'q qilishi, tarmoq qurilmalarini fizik

buzilishiga olib keladi.

-Huquqiy javobgarlik, tarmoq qurilmalarini fizik

buzilishiga olib keladi.

?Razvedka hujumlari bu?

+Asosiy hujumlarni oson amalga oshirish uchun tashkilot

va tarmoq haqidagi axborotni to'plashni maqsad qiladi.

-Turli texnologiyalardan foydalangan holda tarmoqqa

kirishga harakat qiladi.

-Foydalanuvchilarga va tashkilotlarda mavjud bo'lgan  
biror xizmatni cheklashga urinadi.

-Tizimni fizik buzishni maqsad qiladi.

?Kirish hujumlari bu?

+Turli texnologiyalardan foydalangan holda tarmoqqa  
kirishga harakat qiladi.

-Asosiy hujumlarni oson amalga oshirish uchun tashkilot  
va tarmoq haqidagi axborotni to'plashni maqsad qiladi.

-Foydalanuvchilarga va tashkilotlarda mavjud bo'lgan  
biror xizmatni cheklashga urinadi.

-Tarmoq haqida axborotni to'plash hujumchilarga mavjud  
bo'lgan potensial zaiflikni aniqlashga harakat qiladi.

?Xizmatdan voz kechishga qaratilgan hujumlar bu?

+Foydalanuvchilarga va tashkilotlarda mavjud bo'lgan  
biror xizmatni cheklashga urinadi.

-Turli texnologiyalardan foydalangan holda tarmoqqa  
kirishga harakat qiladi.

-Asosiy hujumlarni oson amalga oshirish uchun tashkilot  
va tarmoq haqidagi axborotni to'plashni maqsad qiladi.

-Tarmoq haqida axborotni to'plash hujumchilarga mavjud  
bo'lgan potensial zaiflikni aniqlashga harakat qiladi.

?Paketlarni snifferlash, portlarni skanerlash va Ping  
buyrug'ini yuborish hujumlari qaysi hujumlar toifasiga  
kiradi?

+Razvedka hujumlari.

-Kirish hujumlari.

-DOS hujumlari.

-Zararli dasturlar yordamida amalga oshiriladigan  
hujumlar.

?O'zini yaxshi va foydali dasturiy vosita sifatida ko'rsatuvchi  
zararli dastur turi bu?

+Troyan otlari.

-Adware.

-Spyware.

-Backdoors.



?Marketing maqsadida yoki reklamani namoyish qilish uchun foydalanuvchini ko'rish rejimini kuzutib boruvchi zararli dastur turi bu?

+Adware.

-Trojan otlari.

-Spyware.

-Backdoors.

?Himoya mexanizmini aylanib o'tib tizimga ruxsatsiz kirish imkonini beruvchi zararli dastur turi bu?

+Backdoors.

-Adware.

-Trojan otlari.

-Spyware.

?Paket filterlari turidagi tarmoqlararo ekran vositasi OSI modelining qaysi sathida ishlaydi?

+Tarmoq sathida.

-Transport sathida.

-Ilova sathida.

-Kanal sathida.

?Tashqi tarmoqdagi foydalanuvchilardan ichki tarmoq resurslarini himoyalash qaysi himoya vositasining vazifasi hisoblanadi.

+Tarmoqlararo ekran.

-Antivirus.

-Virtual himoyalangan tarmoq.

-Router.

?Ichki tarmoq foydalanuvchilarini tashqi tarmoqqa bog'langan murojaatlarini chegaralash qaysi himoya vositasining vazifasi hisoblanadi.

+Tarmoqlararo ekran.

-Antivirus.

-Virtual himoyalangan tarmoq.

-Router.

?2 lik sanoq tizimida 11011 soniga 11010 sonini 2 modul bo'yicha qo'shing?

+00001

-10000

-01100

-11111

?2 lik sanoq tizimida 11011 soniga 00100 sonini 2 modul

bo yicha qo shing?

+11111

-10101

-11100

-01001

?2 lik sanoq tizimida 11011 soniga 11010 sonini 2 modul

bo yicha qo shing?

+00001

-10000

-01100

-11111

?Axborot saqlagich vositalaridan qayta foydalanish

xususiyatini saqlab qolgan holda axborotni yo q qilish

usuli qaysi?

+Bir necha marta takroran yozish va maxsus dasturlar

yordamida saqlagichni tozalash

-Magnitsizlantirish

-Formatlash

-Axborotni saqlagichdan o chirish

?Elektron ma lumotlarni yo q qilishda maxsus qurilma

ichida joylashtirilgan saqlagichning xususiyatlari o

zgartiriladigan usul bu ...

+magnitsizlantirish.

-shredirlash.

-yanchish.

-formatlash.

?Yo q qilish usullari orasidan ekologik jihatdan ma

qullanmaydigan va maxsus joy talab qiladigan usul qaysi?

+Yoqish

-Maydalash

-Ko mish

-Kimyoviy ishlov berish

?Kiberjinoatchilik bu - ?

+Kompyuter yoki boshqa qurilmalarga qarshi qilingan yoki kompyuter va boshqa qurilmalar orqali qilingan jinoiy faoliyat.

-Kompyuterlar bilan bog liq falsafiy soha bo lib, foydalanuvchilarning xatti-harakatlari, kompyuterlar nimaga dasturlashtirilganligi va umuman insonlarga va jamiyatga qanday ta sir ko rsatishini o rganadi.

-Hisoblashga asoslangan bilim sohasi bo lib, buzg unchilar mavjud bo lgan sharoitda amallarni kafolatlash uchun o zida texnologiya, inson, axborot va jarayonni mujassamlashtirgan.

-Tizimlarni, tarmoqlarni va dasturlarni raqamli hujumlardan himoyalash amaliyoti.

?Kiberetika bu - ?

+Kompyuterlar bilan bog liq falsafiy soha bo lib, foydalanuvchilarning xatti-harakatlari, kompyuterlar nimaga dasturlashtirilganligi va umuman insonlarga va jamiyatga qanday ta sir ko rsatishini o rganadi.

-Kompyuter yoki boshqa qurilmalarga qarshi qilingan yoki kompyuter va boshqa qurilmalar orqali qilingan jinoiy faoliyat.

-Hisoblashga asoslangan bilim sohasi bo lib, buzg unchilar mavjud bo lgan sharoitda amallarni kafolatlash uchun o zida texnologiya, inson, axborot va jarayonni mujassamlashtirgan.

-Tizimlarni, tarmoqlarni va dasturlarni raqamli hujumlardan himoyalash amaliyoti.

?Shaxsiy simsiz tarmoqlar qo llanish sohasini belgilang

+Tashqi qurilmalar kabellarining o rnida

-Binolar va korxonalar va internet orasida belgilangan simsiz bog lanish

-Butun dunyo bo yicha internetdan foydalanishda

-Simli tarmoqlarni mobil kengaytirish

?VPNning texnik yechim arxitekturasiga ko ra turlari keltirilgan qatorni aniqlang?

+Korporativ tarmoq ichidagi VPN; masofadan

foydalaniluvchi VPN; korporativ tarmoqlararo VPN

-Kanal sathidagi VPN; tarmoq sathidagi VPN; seans  
sathidagi VPN

-Marshurizator ko rinishidagi VPN; tramoqlararo ekran  
ko rinishidagi VPN

-Dasturiy ko rinishdagi VPN; maxsus shifrlash  
protssessoriga ega apparat vosita ko rinishidagi VPN

?Axborotning konfidensialligi va butunligini ta minlash  
uchun ikki uzal orasida himoyalangan tunelni quruvchi  
himoya vositasi bu?

+Virtual Private Network

-Firewall

-Antivirus

-IDS

?Qanday tahdidlar passiv hisoblanadi?

+Amalga oshishida axborot strukturasi va mazmunida  
hech narsani o zgartirmaydigan tahdidlar

-Hech qachon amalga oshirilmaydigan tahdidlar

-Axborot xavfsizligini buzmaydigan tahdidlar

-Texnik vositalar bilan bog liq bo lgan tahdidlar

?Quyidagi qaysi hujum turi razvedka hujumlari turiga  
kirmaydi?

+Ddos

-Paketlarni snifferlash

-Portlarni skanerlash

-Ping buyrug ini yuborish

?Trafik orqali axborotni to plashga harakat qilish  
razvedka hujumlarining qaysi turida amalga oshiriladi?

+Passiv

-DNS izi

-Lug atga asoslangan

-Aktiv

?Portlarni va operatsion tizimni skanerlash razvedka  
hujumlarining qaysi turida amalga oshiriladi?

+Aktiv

-Passiv

-DNS izi

-Lug atga asoslangan

?Paketlarni snifferlash, portlarni skanerlash, ping buyrug

ini yuborish qanday hujum turiga misol bo ladi?

+Razvedka hujumlari

-Xizmatdan voz kechishga undash hujumlari

-Zararli hujumlar

-Kirish hujumlari

?DNS serverlari tarmoqda qanday vazifani amalga

oshiradi?

+Xost nomlari va internet nomlarini IP manzillarga o

zgartirish va teskarisini amalga oshiradi

-Ichki tarmoqqa ulanishga harakat qiluvchi boshqa tarmoq

uchun kiruvchi nuqta vazifasini bajaradi

-Tashqi tarmoqqa ulanishga harakat qiluvchi ichki tarmoq

uchun chiqish nuqtasi vazifasini bajaradi

-Internet orqali ma lumotlarni almashinuvchi turli ilovalar

uchun tarmoq ulanishlarini sozlash funksiyasini amalga

oshiradi

?Markaziy xab yoki tugun orqali tarmoqni markazlashgan

holda boshqarish qaysi tarmoq topologiyasida amalga

oshiriladi?

+Yulduz

-Shina

-Xalqa

-Mesh

?Quyidagilardan qaysilari ananaviy tarmoq turi

hisoblanadi?

+WAN, MAN, LAN

-OSI, TCP/IP

-UDP, TCP/IP, FTP

-Halqa, yulduz, shina, daraxt

?Quyidagilardan qaysilari tarmoq topologiyalari

hisoblanadi?

+Halqa, yulduz, shina, daraxt

-UDP, TCP/IP, FTP

-OSI, TCP/IP

-SMTP, HTTP, UDP

?Yong inga qarshi tizimlarni aktiv chora turiga

quyidagilardan qaysilari kiradi?

+Yong inni aniqlash va bartaraf etish tizimi

-Minimal darajada yonuvchan materiallardan foydalanish

-Yetarlicha miqdorda qo shimcha chiqish yo llarini  
mavjudligi

-Yong inga aloqador tizimlarni to g ri madadlanganligi

?Yong inga qarshi kurashishning aktiv usuli to g ri ko  
rsatilgan javobni toping?

+Tutunni aniqlovchilar, alangani aniqlovchilar va  
issiqlikni aniqlovchilar

-Binoga istiqomat qiluvchilarni yong in sodir bo lganda  
qilinishi zarur bo lgan ishlar bilan tanishtirish

-Minimal darajada yonuvchan materiallardan foydalanish,  
qo shimcha etaj va xonalar qurish

-Yetarli sondagi qo shimcha chiqish yo llarining  
mavjudligi

?Yong inga qarshi kurashishning passiv usuliga kiruvchi  
choralarni to g ri ko rsatilgan javobni toping?

+Minimal darajada yonuvchan materiallardan  
foydalanish, qo shimcha etaj va xonalar qurish

-Tutun va alangani aniqlovchilar

-O t o chirgich, suv purkash tizimlari

-Tutun va alangani aniqlovchilar va suv purkash tizimlari

?Fizik himoyani buzilishiga olib keluvchi tahdidlar  
yuzaga kelish shakliga ko ra qanday guruhlarga bo linadi?

+Tabiiy va sun iy

-Ichki va tashqi

-Aktiv va passiv

-Bir faktorlik va ko p faktorli

?Quyidagilarnig qaysi biri tabiiy tahdidlarga misol bo la  
oladi?

+Toshqinlar, yong in, zilzila

-Bosqinchilik, terrorizm, o g irlik

-O g irlik, toshqinlar, zilzila

-Terorizm, toshqinlar, zilzila

?Quyidagilarnig qaysi biri sun iy tahdidlarga misol bo la  
oladi?

+Bosqinchilik, terrorizm, o g irlik

-Toshqinlar, zilzila, toshqinlar

-O g irlik, toshqinlar, zilzila

-Terorizm, toshqinlar, zilzila

?Kolliziya hodisasi deb nimaga aytiladi?

+Ikki xil matn uchun bir xil xesh qiymat chiqishi

-ikki xil matn uchun ikki xil xesh qiymat chiqishi

-bir xil matn uchun bir xil xesh qiymat chiqishi

-bir xil matn uchun ikki xil xesh qiymat chiqishi

?GSM tarmog ida foydalaniluvchi shifrlash algoritmi  
nomini ko rsating?

+A5/1

-DES

-AES

-RC4

?O zbekistonda kriptografiya sohasida faoliyat yurituvchi  
tashkilot nomini ko rsating?

+ "UNICON.UZ" DUK

- "O zstandart" agentligi

- Davlat Soliq Qo mitasi

- Kadastr agentligi

?RC4 shifrlash algoritmi simmetrik turga mansub bo lsa,  
unda nechta kalitdan foydalaniladi?

+1

-2

-3

-4

?A5/1 shifrlash algoritmi simmetrik turga mansub bo lsa,  
unda nechta kalitdan foydalaniladi?

+1

-2

-3

-4

?AES shifrlash algoritmi simmetrik turga mansub bo'lsa,  
unda nechta kalitdan foydalaniladi?

+1

-2

-3

-4

?DES shifrlash algoritmi simmetrik turga mansub bo'lsa,  
unda nechta kalitdan foydalaniladi?

+1

-2

-3

-4

?AES/1 oqimli shifrlash algoritmida maxfiy kalit necha  
registrga bo'linadi?

+3

-4

-5

-6

?Faqat simmetrik blokli shifrlarga xos bo'lgan atamani  
aniqlang?

+blok uzunligi

-kalit uzunligi

-ochiq kalit

-kodlash jadvali

?AES/1 shifri qaysi turga mansub?

+oqimli shifrlar

-blokli shifrlar

-ochiq kalitli shifrlar

-assimetrik shifrlar

?... shifrlar blokli va oqimli turlarga ajratiladi

+simmetrik

-ochiq kalitli

-assimetrik

-klassik



?Quyida keltirilgan xususiyatlarning qaysilari xesh

funksiyaga mos?

+ixtiyoriy olingan har xil matn uchun xesh qiymatlar bir xil bo lmaydi

-ixtiyoriy olingan bir xil matn uchun qiymatlar bir xil bo lmaydi

-ixtiyoriy olingan har xil matn uchun xesh qiymatlar bir xil bo ladi

-ixtiyoriy olingan har xil xesh qiymat uchun dastlabki ma lumotlar bir xil bo ladi

?Quyida keltirilgan xususiyatlarning qaysilari xesh

funksiyaga mos?

+chiqishda fiksirlangan uzunlikdagi qiymatni beradi

-chiqishda bir xil qiymatni beradi

-chiqishdagi qiymat bilan kiruvchi qiymatlar bir xil bo ladi

-kolliziyaga ega

?Xesh qiymatlarni yana qanday atash mumkin?

+dayjest

-funksiya

-imzo

-raqamli imzo

?A5/1 oqimli shifrlash algoritmida dastlabki kalit uzunligi nechi bitga teng?

+64

-512

-192

-256

?A5/1 oqimli shifrlash algoritmi asosan qayerda qo llaniladi?

+mobil aloqa standart GSM protokolida

-simsiz aloqa vositalaridagi mavjud WEP protokolida

-internet trafiklarini shifrlashda

-radioaloqa tarmoqlarida

?Assimetrik kriptotizimlarda necha kalitdan

foydalaniladi?

+2 ta

-3 ta

-4 ta

-kalit ishlatilmaydi

?Simmetrik kriptotizimlarda necha kalitdan foydalaniladi?

+1 ta

-3 ta

-4 ta

-kalit ishlatilmaydi

?Kriptotizimlar kalitlar soni bo'yicha qanday turga bo'linadi?

+simmetrik va assimetrik turlarga

-simmetrik va bir kalitli turlarga

-3 kalitli turlarga

-assimetrik va 2 kalitli turlarga

?Kriptologiya qanday yo'nalishlarga bo'linadi?

+kriptografiya va kriptotahlil

-kriptografiya va kriptotizim

-kripto va kriptotahlil

-kriptoanaliz va kriptotizim

?Qaysi chora tadbirlar virusdan zararlanish holatini kamaytiradi?

+Barcha javoblar to'g'ri

-Faqat litsenziyalı dasturiy ta'minotdan foydalanish.

-Kompyuterni zamonaviy antivirus dasturiy vositasi bilan ta'minlash va uni doimiy yangilab borish.

-Boshqa kompyuterda yozib olingan ma'lumotlarni o'qishdan oldin har bir saqlagichni antivirus tekshiruvidan o'tkazish.

?Antivirus dasturiy vositalari zararli dasturlarga qarshi to'liq himoyani ta'minlay olmasligining asosiy sababini ko'rsating?

+Paydo bo'layotgan zararli dasturiy vositalar sonining ko'payishi.

-Viruslar asosan antivirus ishlab chiqaruvchilar tomonidan yaratilishi.

-Antivirus vositalarining samarali emasligi.

-Aksariyat antivirus vositalarining pullik ekanligi.

?...umumiy tarmoqni ichki va tashqi qismlarga ajratib  
himoyalash imkonini beradi.

+Tarmoqlararo ekran

-Virtual himoyalangan tarmoq

-Global tarmoq

-Korxona tarmog i

?RSA algoritmidan  $p=5$ ,  $q=13$ ,  $e=7$  ga teng bo lsa, shaxsiy  
kalitni hisoblang?

+7

-13

-65

-35

?..... hujumida hujumchi o rnatilgan aloqaga suqilib kiradi  
va aloqani bo ladi. Nuqtalar o rniga mos javobni qo ying.

+O rtada turgan odam.

-Qo pol kuch.

-Parolga qaratilgan.

-DNS izi.

?Agar ob ektning xavfsizlik darajasi sub ektning  
xavfsizlik darajasidan kichik yoki teng bo lsa, u holda O  
qish uchun ruxsat beriladi. Ushbu qoida qaysi  
foydalanishni boshqarish usuliga tegishli.

+MAC

-DAC

-RMAC

-ABAC

?GSM tarmog ida ovozli so zlashuvlarni shifrlash  
algoritmi bu?

+A5/1

-DES

-ГOCT

-RSA

?RSA algoritmidan ochiq kalit  $e=7$ ,  $N=35$  ga teng bo lsa,  
 $M=2$  ga teng ochiq matnni shifrlash natijasini ko rsating?

+23

-35

-5

-7

?RSA algoritmidagi ochiq kalit  $e=7$ ,  $N=143$  ga teng bo'lsa,  
 $M=2$  ga teng ochiq matnning shifrlash natijasini ko'rsating?

+128

-49

-11

-7

?Jumlani to'ldiring. Agar axborotning o'zirlanishi  
moddiy va ma'naviy boyliklarning yo'qotilishiga olib  
kelsa.

+jinoyat sifatida baholanadi.

-rag'bat hisoblanadi.

-buzg'unchilik hisoblanadi.

-guruhlar kurashi hisoblanadi.

?Jumlani to'ldiring. Simli va simsiz tarmoqlar orasidagi  
asosiy farq ...

+tarmoq chetki nuqtalari orasidagi mutlaqo  
nazoratlamaydigan xudud mavjudligi.

-tarmoq chetki nuqtalari orasidagi xududning kengligi.

-himoya vositalarining chegaralanganligi.

-himoyani amalga oshirish imkoniyati yo'qligi.

?Jumlani to'ldiring. Simmetrik shifrlash algoritmlari  
ochiq ma'lumotdan foydalanish tartibiga ko'ra ...

+blokli va oqimli turlarga bo'linadi.

-bir kalitli va ikki kalitli turlarga bo'linadi.

-Feistel tarmog'iga asoslangan va SP tarmog'iga  
asoslangan turlarga bo'linadi.

-murakkablikka va tizimni nazariy yondoshuvga  
asoslangan turlarga bo'linadi.

?Jumlani to'ldiring. Tarmoqlararo ekranning vazifasi ...

+ishonchli va ishonchsiz tarmoqlar orasida ma'lumotlarga  
kirishni boshqarish.

-tarmoq hujumlarini aniqlash.

-trafikni taqiqlash.

-tarmoqdagi xabarlar oqimini uzish va ulash.

?Faktorlash muammosi asosida yaratilgan assimetrik shifrlash usuli?

+RSA

-El-Gamal

-Elliptik egri chiziqqa asoslangan shifrlash

-Diffi-Xelman

?Eng zaif simsiz tarmoq protokolini ko'rsating?

+WEP

-WPA

-WPA2

-WPA3

?Axborotni shifrlashdan maqsadi nima?

+Maxfiy xabar mazmunini yashirish.

-Ma'lumotlarni zichlashtirish, siqish.

-Ma'lumotlarni yig'ish va sotish.

-Ma'lumotlarni uzatish.

?9 soni bilan o'zaro tub bo'lgan sonlarni ko'rsating?

+10, 8

-6, 10

-18, 6

-9 dan tashqari barcha sonlar

?12 soni bilan o'zaro tub bo'lgan sonlarni ko'rsating?

+11, 13

-14, 26

-144, 4

-12 dan tashqari barcha sonlar

?13 soni bilan o'zaro tub bo'lgan sonlarni ko'rsating?

+5, 7

-12, 26

-14, 39

-13 dan tashqari barcha sonlar

?Jumlani to'ldiring. Autentifikatsiya tizimlari

asoslanishiga ko'ra ... turga bo'linadi.

+3

-2

-4

-5

?...umumiy tarmoqni ichki va tashqi qismlarga ajratib

himoyalash imkonini beradi.

+Tarmoqlararo ekran

-Virtual himoyalangan tarmoq

-Global tarmoq

-Korxona tarmog i

?Antivirus dasturiy vositalari zararli dasturlarga qarshi to

liq himoyani ta minlay olmasligining asosiy sababini ko

rsating?

+Paydo bo layotgan zararli dasturiy vositalar sonining ko

pligi.

-Viruslar asosan antivirus ishlab chiqaruvchilar

tomonidan yaratilishi.

-Antivirus vositalarining samarali emasligi.

-Aksariyat antivirus vositalarining pullik ekanligi.

?Qaysi chora tadbirlar virusdan zararlanish holatini

kamaytiradi?

+Barcha javoblar to g ri

-Faqat litsenziyalı dasturiy ta minotdan foydalanish.

-Kompyuterni zamonaviy antivirus dasturiy vositasi bilan

ta minlash va uni doimiy yangilab borish.

-Boshqa kompyuterda yozib olingan ma lumotlarni o

qishdan oldin har bir saqlagichni antivirus tekshiruvidan o

tkazish.

?Virus aniq bo lganda va xususiyatlari aniq ajratilgan

holatda eng katta samaradorlikka ega zararli dasturni

aniqlash usulini ko rsating?

+Signaturaga asoslangan usul

-O zgarishga asoslangan usul

-Anomaliyaga asoslangan usul

-Barcha javoblar to g ri

?Signatura (antiviruslarga aloqador bo lgan) bu-?

+Fayldan topilgan bitlar qatori.

-Fayldagi yoki katalogdagi o'zgarish.

-Normal holatdan tashqari holat.

-Zararli dastur turi.

?Zararli dasturiy vositalarga qarshi foydalaniluvchi

dasturiy vosita bu?

+Antivirus

-VPN

-Tarmoqlararo ekran

-Brandmauer

?Kompyuter viruslarini tarqalish usullarini ko'rsating?

+Malumot saqlovchilari, Internetdan yuklab olish va elektron pochta orqali.

-Malumot saqlovchilari, Internetdan yuklab olish va skaner qurilmalari orqali.

-Printer qurilmasi, Internetdan yuklab olish va elektron pochta orqali.

-Barcha javoblar to'g'ri.

?Qurbon kompyuteridagi malumotni shifrlab, uni deshifrlash uchun to'lovni amalga oshirishni talab qiluvchi zararli dastur bu-?

+Ransomware.

-Mantiqiy bombalar.

-Rootkits.

-Spyware.

?Internet tarmog'idagi obro'sizlantirilgan kompyuterlar bu-?

+Botnet.

-Backdoors.

-Adware.

-Virus.

?Bironi mantiqiy shartni tekshiruvchi trigger va foydali yuklamadan iborat zararli dastur turi bu-?

+Mantiqiy bombalar.

-Backdoors.

-Adware.

-Virus.

?Buzg unchiga xavfsizlik tizimini aylanib o tib tizimga

kirish imkonini beruvchi zararli dastur turi bu-?

+Backdoors.

-Adware.

-Virus.

-Trojan otlari.

?Ma lumotni to liq qayta tiklash qachon samarali amalga oshiriladi?

+Saqlagichda ma lumot qayta yozilmagan bo lsa.

-Ma lumotni o chirish Delete buyrug i bilan amalga oshirilgan bo lsa.

-Ma lumotni o chirish Shifr+Delete buyrug i bilan amalga oshirilgan bo lsa.

-Formatlash asosida ma lumot o chirilgan bo lsa.

?Ma lumotni zaxira nusxalash nima uchun potensial tahdidlarni paydo bo lish ehtimolini oshiradi.

+Tahdidchi uchun nishon ko payadi.

-Saqlanuvchi ma lumot hajmi ortadi.

-Ma lumotni butunligi ta minlanadi.

-Ma lumot yo qolgan taqdirda ham tiklash imkoniyati mavjud bo ladi.

?Qaysi xususiyatlar RAID texnologiyasiga xos emas?

+Shaxsiy kompyuterda foydalanish mumkin.

-Serverlarda foydalanish mumkin.

-Xatoliklarni nazoratlash mumkin.

-Disklarni "qaynoq almashtirish" mumkin.

?Qaysi zaxira nusxalash vositasi oddiy kompyuterlarda foydalanish uchun qo shimcha apparat va dasturiy vositani talab qiladi?

+Lentali disklar.

-Ko chma qattiq disklar.

-USB disklar.

-CD/DVD disklar.

?Ma lumotlarni zaxira nusxalash strategiyasi nimadan boshlanadi?

+Zarur axborotni tanlashdan.



-Mos zaxira nusxalash vositasini tanlashdan.

-Mos zaxira nusxalash usulini tanlashdan.

-Mos RAID sathini tanlashdan.

?Jumlani to'ldiring. .... - muhim bo'lgan axborot

nusxalash yoki saqlash jarayoni bo'lib, bu ma'lumot yo

qolgan vaqtda qayta tiklash imkoniyatini beradi.

+Ma'lumotlarni zaxira nusxalash

-Kriptografik himoya

-VPN

-Tarmoqlararo ekran

?Paket filteri turidagi tarmoqlararo ekran vositasi nima

asosida tekshirishni amalga oshiradi?

+Tarmoq sathi parametrlari asosida.

-Kanal sathi parametrlari asosida.

-Ilova sathi parametrlari asosida.

-Taqdimot sathi parametrlari asosida.

?Jumlani to'ldiring. ... texnologiyasi lokal simsiz

tarmoqlarga tegishli.

+WI-FI

-WI-MAX

-GSM

-Bluetooth

?Jumlani to'ldiring. Kriptografik himoya axborotning ...

xususiyatini ta'minlamaydi.

+Foydalanuvchanlik

-Butunlik

-Maxfiylik

-Autentifikatsiya

?Jumlani to'ldiring. Parol kalitidan .... farq qiladi.

+tasodifiylik darajasi bilan

-uzunligi bilan

-belgilari bilan

-samaradorligi bilan

?Parolga "tuz"ni qo'shib xeshlashdan maqsad?

+Tahdidchi ishini oshirish.

-Murakkab parol hosil qilish.

-Murakkab xesh qiymat hosil qilish.

-Ya na bir maxfiy parametr kiritish.

?Axborotni foydalanuvchanligini buzishga qaratilgan tahdidlar bu?

+DDOS tahdidlar.

-Nusxalash tahdidlari.

-Modifikatsiyalash tahdidlari.

-O rtaga turgan odam tahdidi.

?Tasodifiy tahdidlarni ko rsating?

+Texnik vositalarning buzilishi va ishlamasligi.

-Axborotdan ruxsatsiz foydalanish.

-Zararkunanda dasturlar.

-An anaviy josuslik va diversiya.

?Xodimlarga faqat ruxsat etilgan saytlardan foydalanishga imkon beruvchi himoya vositasi bu?

+Tarmoqlararo ekran.

-Virtual Private Network.

-Antivirus.

-Router.

?Qaysi himoya vositasi yetkazilgan axborotning butunligini tekshiradi?

+Virtual Private Network.

-Tarmoqlararo ekran.

-Antivirus.

-Router.

?Qaysi himoya vositasi tomonlarni autentifikatsiyalash imkoniyatini beradi?

+Virtual Private Network.

-Tarmoqlararo ekran.

-Antivirus.

-Router.

?Foydalanuvchi tomonidan kiritilgan taqiqlangan so rovni qaysi himoya vositasi yordamida nazoratlash mumkin.

+Tarmoqlararo ekran.

-Virtual Private Network.

-Antivirus.

-Router.

?Qaysi himoya vositasi mavjud IP - paketni to liq shifrlab, unga yangi IP sarlavha beradi?

+Virtual Private Network.

-Tarmoqlararo ekran.

-Antivirus.

-Router.

?Ochiq tarmoq yordamida himoyalangan tarmoqni qurish imkoniyatiga ega himoya vositasi bu?

+Virtual Private Network.

-Tarmoklapapo ekran.

-Antivirus.

-Router.

?Qaysi himoya vositasida mavjud paket shifrlangan holda yangi hosil qilingan mantiqiy paket ichiga kiritiladi?

+Virtual Private Network.

-Tarmoqlararo ekran.

-Antivirus.

-Router.

?Qaysi himoya vositasi tarmoqda uzatilayotgan axborotni butunligi, maxfiyligi va tomonlar autentifikatsiyasini ta minlaydi?

+Virtual Private Network.

-Tarmoqlararo ekran.

-Antivirus.

-Router.

?Qaysi tarmoq himoya vositasi tarmoq manzili, identifikatorlar, interfeys manzili, port nomeri va boshqa parametrlar yordamida filtrlashni amalga oshiradi.

+Tarmoqlararo ekran.

-Antivirus.

-Virtual himoyalangan tarmoq.

-Router.

?Web-sahifa bu...

+Yagona adresga ega bo lgan, brauzer yordamida ochish va ko rish imkoniyatiga ega bo lgan hujjatdir

-Tarmoqqa ulangan kompyuterda, klientga belgilangan

umumiy vazifalarni bajarish uchun foydalaniluvchi

sahifadir

-Klient-server arxitekturasida asosidagi, keng tarqalgan

Internetning axborot xizmati

-HTML kodlari to'plami

?Web-sayt nima?

+Aniq maqsad asosida mantiqiy bog'langan web-sahifalar

birlashmasi

-Klient-server texnologiyasiga asoslangan, keng tarqalgan

internetning axborot xizmatidir

-A va B

-Yagona adresga ega bo'lgan hujjat hisoblanib, uni ochish

(brauzer yordamida) va o'qish imkoniyati mavjud

?WWW nechta komponentdan tashkil topgan?

+4

-5

-3

-2

?WWWning komponentlari qaysi javobda to'g'ri

berilgan?

+Dasturiy/texnik vositalar, HTML, HTTP, URI

-HTML, FTP, WWW

-HTML, CSS, PHP

-HTML, JavaScript, JQuery, PHP

?Hozirgi kunda WWWning nechta versiyasi mavjud?

+4

-3

-5

-2

?Web 1.0 ning rivojlanish davrini toping?

+1990-2000 yy.

-2000-2005 yy.

-1980-1990 yy.

-2010-2015 yy.

?Web 2.0 ning rivojlanish davrini toping?

+2000-2010 yy.

-2010-2020 yy.

-2020-2030 yy.

-1990-2000 yy.

?Web 3.0 ning rivojlanish davrini toping?

+2010-2020 yy.

-2000-2010 yy.

-2020-2030 yy.

-1990-2000 yy.

?Web 4.0 ning rivojlanish davrini toping?

+2020-2030 yy.

-2000-2010 yy.

-2010-2020 yy.

-1990-2000 yy.

?HTML teglar necha xil bo ladi?

+Juft, toq, maxsus teglar

-Toq teglari

-Juft teglari

-Ko rinishi ko p

?Qaysi teg HTML hujjatning tanasini ifodalaydi?

+body

-html

-head

-title

?Qaysi teg hujjatning stilini ifodalash uchun ishlatiladi?

+style

-head

-isindex

-body

?Qaysi teg HTML hujjatni ifodalaydi?

+html

-body

-meta

-isindex

?Qaysi teg HTML hujjat sarlavhasini ifodalaydi?

+head

-meta

-title

-body

?Havola to g ri ko rsatilgan qatorni toping.

+havola

- havola

- havola

-Ekranni tozalash

?

---

tegi nimani ifodalaydi?

+Gorizontal chiziq chizish

-Yangi satrga o tish

-qo shtirnoq

-Ekranni tozalash

?Jadval hosil qilish uchun qaysi tegdan foydalaniladi?

+

?Jadval ustunlarini birlashtirish atributi qaysi javobda keltirilgan?

?Jadval satrlarini birlashtirish atributi qaysi javobda keltirilgan?

?HTML da shrift o lchamini o zgartirish uchun qaysi tegdan foydalaniladi?

-

-

-

?

tegi nimani ifodalaydi?

+Yangi satrga o tish

-"uzilish"

-qo shtirnoq

-Ekranni tozalash

?

tegi nima uchun qo llaniladi?

+matnni paragraflarga ajratish uchun

-Sarlavhani ifodalash uchun

-Obyektni ko'rsatilgan joyga o'rnatish va shu nuqtadan bo

sh satrga matnni davom ettirish uchun qo'llaniladi

-Tartibsiz ro'yxat hosil qilish uchun

? Rasmlar bilan ishlash teglarini qaysi javobda berilgan?

+img, map, area, picture

-Image, map, a, picture

-Image, form, area, photo

-img, iframe, areas, picture

? tegining vazifasi nima?

+Matnni ajratilgan shaklda aniqlash

-Matnni o'chirilgan shaklda belgilash

-Matnni tagiga chizilgan shaklda belgilash

-Matnni qiyâ shaklda belgilash

? tegining vazifasi nima?

+Matnni tagiga chizilgan shaklda belgilash

-Matnni o'chirilgan shaklda belgilash

-Matnni ajratilgan shaklda aniqlash

-Matnni qiyâ shaklda belgilash

?

+Matnni o'chirilgan shaklda belgilash

-Matnni tagiga chizilgan shaklda belgilash

-Matnni ajratilgan shaklda aniqlash

-Matnni qiyâ shaklda belgilash

?

tegi nimani ifodalaydi?

+Tartiblanmagan ro'yxat

-Tartiblangan ro'yxat

-Jadval yacheykasi

-Yangi qatorga o'tish

?

matni nimani ifodalaydi?

+Teg kvadrat shaklidagi ro'yxat hosil qiladi

-Teg aylana shaklidagi ro'yxat hosil qiladi

-Teg alifbo ko'rinishdagi ro'yxatni hosil qiladi

-Teg raqamli ko'rinishdagi ro'yxatni hosil qiladi

?

matni nimani ifodalaydi?

+Teg I., II., III., IV. va h.k ko rinishidagi ro yxatni hosil qiladi

-Teg raqamli ko rinishdagi ro yxatni hosil qiladi

-Teg kvadrat shaklidagi ro yxat hosil qiladi

-Teg 1., 2., 3., 4. va h.k ko rinishidagi ro yxatni hosil qiladi

? tegining majburiy atributini toping

+src

-title

-href

-type

?Qaysi teg forma ichida qayerga ma lumot kiritilishini ifodalaydi?

+

-

-

-

?HTMLda forma elementlariga kiritilgan qiymatlarni tozalash uchun qaysi elementdan foydalaniladi?

+reset

-text

-hidden

-submit

Yuliy Sezar ma'lumotlarni shifrlashda alfavit xarflarni

nechtaga surib shifrlagan? =====

4 taga=====

2 taga=====

5 taga=====

#3 taga

+++++

WiMAX qanday simsiz tarmoq turiga kiradi? =====

Lokal =====

Global=====

Shaxsiy =====

#Regional



+++++

Wi-Fi necha Gs chastotali to'lqinda ishlaydi? =====

#2.4-5 Gs=====

2.4-2.485 Gs=====

1.5-11 Gs=====

2.3-13.6 Gs

+++++

Quyidagi parollarning qaysi biri "bardoshli parol"ga

kiradi? =====

#Onx458&hdsh) =====

12456578=====

salomDunyo=====

Mashina777

+++++

Ma'lumotlarni tasodifiy sabablar tufayli yo'qolish

sababini belgilang=====

#Quvvat o'chishi, dasturiy ta'minot to'satdan o'zgarishi

yoki qurilmani to'satdan zararlanishi=====

Tashkilotdagi muhim ma'lumotlarni modifikatsiyalanishi

yoki o'g'irlanishi=====

Ma'lumotlarni saqlash vositasini to'g'ri

joylashtirilmagani yoki ma'lumotlar bazasini xatolik bilan

boshqarilganligi. =====

Zilzila, yong'in, suv toshqini va hak.

+++++

Sub'ektga ma'lum vakolat va resurslarni berish

muolajasi-bu: =====

#Avtorizatsiya=====

Haqiqiylikni tasdiqlash=====

Autentifikatsiya=====

Identifikatsiya

+++++

Token, Smartkartalarda xavfsizlik tomonidan kamchiligi

nimada? =====

Foydalanish davrida maxfiylik kamayib boradi=====

Qurilmalarni ishlab chiqarish murakkab jarayon=====

#Qurilmani yo'qotilishi katta xavf olib kelishi

mumkin=====

Qurilmani qalbakilashtirish oson

+++++

Ma'lumotlarni yo'qolish sabab bo'luvchi tabiiy

tahdidlarni ko'rsating=====

Quvvat o'chishi, dasturiy ta'minot to'satdan o'zgarishi

yoki qurilmani to'satdan zararlanishi=====

#Zilzila, yong'in, suv toshqini va hak. =====

Tashkilotdagi muhim ma'lumotlarni modifikatsiyalanishi

yoki o'g'irlanishi=====

Qasddan yoki tasodifiy ma'lumotni o'chirib yuborilishi,

ma'lumotlarni saqlash vositasini to'g'ri joylashtirilmagani

+++++

Foydalanish huquqini cheklovchi matritsa modeli bu...

=====

#Bella La-Padulla modeli=====

Dening modeli=====

Landver modeli=====

Huquqlarni cheklovchi model

+++++

Parollash siyosatiga ko'ra parol tanlash shartlari qanday?

=====

Kamida 8 belgi; katta va kichik xavflar, sonlar qo'llanishi

kerak. =====

#Kamida 8 belgi; katta va kichik xavflar, sonlar , kamida

bitta maxsus simvol qo'llanishi kerak. =====

Kamida 6 belgi; katta xarflar, sonlar , kamida bitta

maxsus simvol qo'llanishi kerak. =====

Kamida 6 belgi; katta va kichik xarflar, kamida bitta

maxsus simvol qo'llanishi kerak.

+++++

MD5, SHA1, SHA256, O'z DSt 1106:2009- qanday

algoritmlar deb ataladi? =====

Kodlash=====

#Xeshlash=====

Shifrlash=====

Stenografiya

+++++

Global simsiz tarmoqda qaysi standartlar ishlaydi? =====

Wi-Fi, 3G=====

WIMAX, 2G=====

Wi-Fi, IRDA=====

#CDPD, 4G

+++++

RSA algoritmi qaysi yilda ishlab chiqilgan? =====

#1977 yil=====

1966 yil=====

1988 yil=====

1956 yil

+++++

Qaysi texnologiyada ma'lumotni bir vaqtda bir necha

disklarga navbatlab yoziladi? =====

RAID 1=====

#RAID 0=====

RAID 5=====

RAID 3

+++++

Windows OT lokal xavfsizlik siyosatini sozlash oynasiga

o'tish uchun buyruqlar satrida qaysi buyruq yoziladi?

=====

#secpol.msc=====

regedit=====

chkdsk=====

diskcopy

+++++

Zimmermann telegrami, Enigma shifri, SIGABA

kriptografiyaning qaysi davriga to'g'ri keladi? =====

O'rta asr davrida=====

15 asr davrida=====

#1-2 jahon urushu davri=====

21 asr davrida

+++++

Bell-LaPadula (BLP) modeli -bu.. ====

Axborlarni nazoratlovchi model=====

#Bu hukumat va harbiy dasturlarda kirishni boshqarishni

kuchaytirish uchun ishlatiladigan avtomatlashgan

modeli=====

Foydalanuvchilarni ro'yxatga olish , nazoratlash va tahlil

qiluvchi model=====

Tarmoq boshqarish va tahlil qiluvchi model

+++++

Internetning dastlabki nomini to'g'ri belgilang. =====

#ARPANET=====

INTRANET=====

INTERNET=====

NETWORK

+++++

Axborot xavfsizligining asosiy maqsadlaridan biribu...=====

Ob'ektga bevosita ta'sir qilish=====

#Axborotlarni o'g'irlanishini, yo'qolishini,

soxtalashtirilishini oldini olish=====

Axborotlarni shifrlash, saqlash, yetkazib berish=====

Tarmoqdagi foydalanuvchilarni xavfsizligini ta'minlab

berish

+++++

Konfidentsiallikga to'g'ri ta'rif keltiring.=====

#axborot inshonchliligi, tarqatilishi mumkin emasligi,

maxfiyligi kafolati; =====

axborot konfidensialligi, tarqatilishi mumkinligi,

maxfiyligi kafolati; =====

axborot inshonchliligi, tarqatilishi mumkin emasligi,

parollanganligi kafolati; =====

axborot inshonchliligi, axborotlashganligi, maxfiyligi

kafolati;

+++++

Yaxlitlikni buzilishi bu - ...=====

#Soxtalashtirish va o'zgartirish=====

Ishonchsizlik va soxtalashtirish=====

Soxtalashtirish=====

Butunmaslik va yaxlitlanmaganlik

+++++

Kriptografiyaning asosiy maqsadi nima? =====

ishonchlilik, butunlilikni ta'minlash=====

autentifikatsiya, identifikatsiya=====

#maxfiylik, yaxlitlilikni ta'minlash=====

ma'lumotlarni shaklini o'zgartish

+++++

Kriptografiyada kalitning vazifasi nima? =====

Bir qancha kalitlar yig'indisi=====

#Matnni shifrlash va shifrini ochish uchun kerakli

axborot=====

Axborotli kalitlar to'plami=====

Belgini va raqamlarni shifrlash va shifrini ochish uchun

kerakli axborot

+++++

Qo'yish, o'rin almashtirish, gammalash kriptografiyaning

qaysi turiga bog'liq? =====

assimetrik kriptotizimlar=====

ochiq kalitli kriptotizimlar=====

#simmetrik kriptotizimlar=====

autentifikatsiyalash

+++++

Autentifikatsiya nima? =====

Tizim me'yoriy va g'ayritabiiy hollarda

rejalashtirilgandek o'zini tutishligi holati=====

#Ma'lum qilingan foydalanuvchi, jarayon yoki

qurilmaning haqiqiy ekanligini tekshirish muolajasi=====

Istalgan vaqtda dastur majmuasining mumkinligini

kafolati=====

Tizim noodatiy va tabiiy hollarda qurilmaning haqiqiy

ekanligini tekshirish muolajasi

+++++

Identifikatsiya bu- ...=====

#Foydalanuvchini uning identifikatori (nomi) bo'yicha

aniqlash jarayoni====

Ishonchliligini tarqalishi mumkin emasligi kafolati====

Axborot boshlang'ich ko'rinishda ekanligi uni saqlash,

uzatishda ruxsat etilmagan o'zgarishlar=====

Axborotni butunligini saqlab qolgan holda uni

elementlarini o'zgartirishga yo'l qo'ymaslik

+++++

Kriptologiya –qanday fan? =====

axborotni qayta akslantirishning matematik usullarini

izlaydi va tadqiq qiladi=====

kalitni bilmasdan shifrlangan matnni ochish

imkoniyatlarini o'rganadi=====

kalitlarni bilmasdan shifrni ochishga bardoshlilikni

aniqlovchi shifrlash tavsifi=====

#axborotni qayta akslantirib himoyalash muammosi bilan

shug'ullanadi

+++++

Kriptobardoshlilik deb nimaga aytiladi? =====

#kalitlarni bilmasdan shifrni ochishga bardoshlilikni

aniqlovchi shifrlash tavsifi=====

axborotni qayta akslantirib himoyalash muammosi bilan

shug'ullanadi=====

kalitni bilmasdan shifrlangan matnni ochish

imkoniyatlarini o'rganadi=====

axborotni qayta akslantirishning matematik usullarini

izlaydi va tadqiq qiladi

+++++

Kriptografiyada matn –bu.. =====

matnni shifrlash va shifrini ochish uchun kerakli

axborot=====

axborot belgilarini kodlash uchun foydalaniladigan chekli

to'plam=====

#alifbo elementlarining tartiblangan to'plami=====

kalit axborotni shifrlovchi kalitlar

+++++

Kriptotizimga qo'yiladigan umumiy talablardan biri

nima? =====

shifrlash algoritmining tarkibiy elementlarini o'zgartirish

imkoniyati bo'lishi lozim=====

ketma-ket qo'llaniladigan kalitlar o'rtasida oddiy va oson

bog'liqlik bo'lishi kerak=====

#shifr matn uzunligi ochiq matn uzunligiga teng bo'lishi

kerak=====

maxfiylik o'ta yuqori darajada bo'lmoqligi lozim

+++++

Axborot qanday sifatlarga ega bo'lishi kerak? =====

uzluksiz va uzlukli=====

ishonchli, qimmatli va uzlukli=====

#ishonchli, qimmatli va to'liq=====

ishonchli, qimmatli va uzluksiz

+++++

Tekstni boshqa tekst ichida ma'nosini yashirib keltirish

nima deb ataladi?=====

sirli yozuv=====

#steganografiya=====

skrembler=====

shifr mashinalar

+++++

Berilgan ta'riflardan qaysi biri asimmetrik tizimlarga xos?

=====

Asimmetrik tizimlarda  $k_1=k_2$  bo'ladi, ya'ni  $k$  – kalit bilan

axborot ham shifrlanadi, ham deshifrlanadi=====

#Asimmetrik kriptotizimlarda  $k_1 \neq k_2$  bo'lib,  $k_1$  ochiq

kalit,  $k_2$  yopiq kalit deb yuritiladi,  $k_1$  bilan axborot

shifrlanadi,  $k_2$  bilan esa deshifrlanadi=====

Asimmetrik kriptotizimlarda yopiq kalit axborot

almashinuvining barcha ishtirokchilariga ma'lum bo'ladi,

ochiq kalitni esa faqat qabul qiluvchi biladi=====

Asimmetrik kriptotizimlarda  $k_1 \neq k_2$  bo'lib, kalitlar

hammaga oshkor etiladi

+++++

Shaxsning, axborot kommunikatsiya tizimidan

foydalanish huquqiga ega bo'lish uchun

foydalaniluvchining maxfiy bo'lmagan qayd yozuvi –

bu...=====

parol=====

#login=====

identifikatsiya=====

token

+++++

Uning egasi haqiqiyligini aniqlash jarayonida tekshiruv

axboroti sifatida ishlatiladigan belgilar ketma-ketligi

(maxfiy so'z) – nima? =====

login=====

#parol=====

identifikatsiya=====

maxfiy maydon

+++++

Kodlash nima? =====

Ma'lumot boshqa formatga o'zgartiriladi, biroq uni faqat

maxsus shaxslar qayta o'zgartirishi

mumkin bo'ladi=====

Ma'lumot boshqa formatga o'zgartiriladi, barcha shaxslar

kalit yordamida qayta o'zgartirishi

mumkin bo'ladi=====

Maxfiy xabarni soxta xabar ichiga berkitish orqali aloqani

yashirish hisoblanadi=====

#Ma'lumotni osongina qaytarish uchun hammaga ochiq

bo'lgan sxema yordamida ma'lumotlarni boshqa formatga

o'zgartirishdir

+++++

Ro'yxatdan o'tish-bu...=====

#foydalanuvchilarni ro'yxatga olish va ularga dasturlar va

ma'lumotlarni ishlatishga huquq berish jarayoni=====

axborot tizimlari ob'yekt va subhektlariga uni tanish

uchun nomlar (identifikator) berish va berilgan nom

bo'yicha solishtirib uni aniqlash jarayoni=====



ob'ekt yoki subhektni unga berilgan identifikatorga  
mosligini tekshirish va belgilar ketma-ketligidan iborat  
maxfiy kodini tekshirish orqali aslligini aniqlash====  
foydalanuvchining resursdan foydalanish huquqlari va  
ruxsatlarini tekshirish jarayoni

+++++

Shifrttekstni ochiq tekstga akslantirish jarayoni nima deb  
ataladi? =====

Xabar=====

Shifrlangan xabar=====

Shifrlash=====

#Deshifrlash

+++++

.....—hisoblashga asoslangan bilim sohasi bo'lib,  
buzg'unchilar mavjud bo'lgan sharoitda amallarni  
kafolatlash uchun o'zida texnologiya, inson, axborot va  
jarayonni mujassamlashtirgan. =====

Axborot xavfsizligi=====

Kiberjtnoyatchilik=====

#Kiberxavfsizlik=====

Risklar

+++++

Risk nima? =====

Potensial kuchlanish yoki zarar=====

Tasodifiy tahdid=====

#Potensial foyda yoki zarar=====

Katta yo'qotish

+++++

Tahdid nima?

Tashkilot uchun qadrli bo'lgan ixtiyoriy narsa=====

Bu riskni o'zgartiradigan harakatlar=====

#Tashkilotga zarar yetkazishi mumkin bo'lgan istalmagan  
hodisa=====

Bu noaniqlikning maqsadlarga ta'siri

+++++

Axborotni shifrnı ochish (deshifrlash) bilan qaysi fan

shug'ullanadi? =====

Kartografiya=====

#Kriptoanaliz=====

Kriptologiya=====

Adamar usuli

+++++

Qaysi juftlik RSA algoritmining ochiq va yopiq kalitlarini

ifodalaydi? =====

$\{d, e\}$  – ochiq,  $\{e, n\}$  – yopiq; =====

$\#\{d, n\}$  – yopiq,  $\{e, n\}$  – ochiq; =====

$\{e, n\}$  – yopiq,  $\{d, n\}$  – ochiq; =====

$\{e, n\}$  – ochiq,  $\{d, n\}$  – yopiq;

+++++

Zamonaviy kriptografiya qanday bo'limlardan iborat?

=====

Elektron raqamli imzo; kalitlarni boshqarish;=====

Simmetrik kriptotizimlar; ochiq kalitli kriptotizimlar;

=====

#Simmetrik kriptotizimlar; ochiq kalitli kriptotizimlar;

Elektron raqamli imzo; kalitlarni boshqarish =====

Simmetrik kriptotizimlar; ochiq kalitli kriptotizimlar;

kalitlarni boshqarish

+++++

Shifr nima?=====

#Shifrlash va deshifrlashda foydalaniladigan matematik

funktsiyadan iborat bo'lgan kriptografik algoritim =====

Kalitlarni taqsimlash usuli=====

Kalitlarni boshqarish usuli =====

Kalitlarni generatsiya qilish usuli

+++++

Ko'z pardasi, yuz tuzilishi, ovoz tembri, -bular

autentifikatsiyaning qaysi faktoriga mos belgilar? =====

#Biometrik autentifikatsiya=====

Biron nimaga egalik asosida=====

Biron nimani bilish asosida=====

Parolga asoslangan

+++++

Ochiq kalitli kriptotizimlarning mohiyati nimadan iborat?

=====

Ochiq kalitli kriptotizimlarda shifrlash va deshifrlashda 1

ta –kalitdan foydalaniladi=====

#Ochiq kalitli kriptotizimlarda bir-biri bilan matematik

bog'langan 2 ta – ochiq va yopiq kalitlardan

foydalaniladi=====

Ochiq kalitli kriptotizimlarda ma'lumotlarni faqat

shifrlash mumkin=====

Ochiq kalitli kriptotizimlarda ma'lumotlarni faqat

deshifrlash mumkin

+++++

Assimmetrik kriptotizimlar qanday maqsadlarda

ishlatiladi? =====

#Shifrlash, deshifrlash, ERI yaratish va tekshirish, kalitlar

almashish uchun=====

ERI yaratish va tekshirish, kalitlar almashish uchun=====

Shifrlash, deshifrlash, kalitlar almashish uchun=====

Heshlash uchun

+++++

Ma'lumotlar butunligi qanday algritmlar orqali amalga

oshiriladi? =====

Simmetrik algoritmlar=====

Assimmetrik algoritmlar=====

#Xesh funksiyalar=====

Kodlash

+++++

To'rtta bir-biri bilan bog'langan bog'lamlar strukturasi

(kvadrat shaklida) qaysi topologiya turiga mansub? =====

Yulduz=====

To'liq bog'lanishli=====

#Xalqa=====

Yacheykali

+++++

Lokal tarmoqlarda keng tarqalgan topologiya turi qaysi?

=====

Xalqa=====

To'liqbog'langan=====

Umumiy shina=====

#Yulduz

+++++

Ethernet kontsentratori qanday vazifani bajaradi?=====

#kompyuterdan kelayotgan axborotni qolgan barcha

kompyuterga yo'naltirib beradi=====

kompyuterdan kelayotgan axborotni boshqa bir

kompyuterga yo'naltirib beradi=====

kompyuterdan kelayotgan axborotni xalqa bo'ylab

joylashgan keyingi kompyuterga=====

tarmoqning ikki segmentini bir biriga ulaydi

+++++

OSI modelida nechta sath mavjud? =====

4 ta=====

5 ta=====

#7 ta=====

3 ta

+++++

Identifikatsiya, autentifikatsiya jarayonlaridan o'tgan

foydalanuvchi uchun tizimda bajarishi mumkin bo'lgan

amallarga ruxsat berish jarayoni bu... =====

Shifrlash=====

Identifikatsiya=====

Autentifikatsiya=====

#Avtorizatsiya

+++++

Ma'lumotlarni inson xatosi tufayli yo'qolish sababini

belgilang. =====

Tashkilotdagi muhim ma'lumotlarni modifikatsiyalanishi

yoki o'g'irlanishi. =====

#Ma'lumotlarni saqlash vositasini to'g'ri

joylashtirilmagani yoki ma'lumotlar bazasini xatolik bilan

boshqarilganligi. =====

Quvvat o'chishi, dasturiy ta'minot to'satdan o'zgarishi

yoki qurilmani to'satdan zararlanishi=====

Zilzila, yong'in, suv toshqini va hak.

+++++

"Parol", "PIN" kodlarni xavfsizlik tomonidan kamchiligi

nimadan iborat? =====

Parolni esda saqlash kerak bo'ladi. =====

Parolni almashtirish jarayoni murakkabligi=====

Parol uzunligi soni cheklangan=====

#Foydalanish davrida maxfiylik kamayib boradi

+++++

Qaysi tarmoq kabelining axborot uzatish tezligi yuqori

hisoblanadi? =====

#Optik tolali=====

O'rama juft=====

Koaksial =====

Telefon kabeli

+++++

Nima uchun autentifikatsiyalashda parol ko'p

qo'llaniladi? =====

#Sarf xarajati kam, almashtirish oson=====

Parolni foydalanubchi ishlab chiqadi=====

Parolni o'g'rishlash qiyin=====

Serverda parollar saqlanmaydi

+++++

Elektron xujjatlarni yo'q qilish usullari qaysilar? =====

Yoqish, ko'mish, yanchish=====

#Shredirlash, magnitsizlantirish, yanchish=====

Shredirlash, yoqish, ko'mish=====

Kimyoviy usul, yoqish.

+++++

Ruxsatlarni nazoratlash, "Qopqon", Yong'inga qarshi

tizimlar, Yoritish tizimlari, Ogohlantirish tizimlari ,

Quvvat manbalari, Video kuzatuv tizimlari, Qurollarni

aniqlash, Muhitni nazoratlash amalga oshirish qanday

nazorat turiga kiradi? =====

Fizik nazorat=====

#Texnik nazorat=====

Ma'muriy nazorat=====

Tashkiliy nazorat

+++++

Avtorizatsiya tushunchasi odatda qaysi tushuncha bilan

sinonim sifatida ham foydalanadi? =====

Foydalanish=====

Tarmoqni loyixalash=====

Identifikatsiya=====

#Foydalanishni boshqarish

+++++

Foydalanishni boshqarish –bu... =====

Sub'ektni Sub'ektga ishlash qobiliyatini aniqlashdir. =====

#Sub'ektni Ob'ektga ishlash qobiliyatini aniqlashdir.

=====

Ob'ektni Ob'ektga ishlash qobiliyatini aniqlashdir=====

Autentifikatsiyalash jarayonidir

+++++

Foydalanishni boshqarishda inson, dastur, jarayon va

hokazolar nima vazifani bajaradi? =====

#Sub'ekt=====

Ob'ekt=====

Tizim=====

Jarayon

+++++

Foydalanishna boshqarishda ma'lumot , resurs, jarayon

nima vazifani bajaradi ? =====

#Ob'ekt=====

Sub'ekt=====

Tizim=====

Jarayon

+++++

MAC usuli bilan foydalanishni boshqarishda xavfsizlik

markazlashgan holatda kim tomonidan amalga oshiriladi?

=====

Foydalaguvchining o'zi=====

#Xavfsizlik siyosati ma'muri=====

Dastur tomonidan=====

Boshqarish amalg oshirilmaydi

+++++

Agar Sub'ektning xavfsizlik darajasida Ob'ektning

xavfsizlik darajasi mavjud bo'lsa, u holda uchun qanday

amalg ruxsat beriladi? =====

Yozish =====

O'zgartirish=====

#O'qish=====

Yashirish

+++++

Agar Sub'ektning xavfsizlik darajasi Ob'ektning

xavfsizlik darajasida bo'lsa, u holda qanday amalg ruxsat

beriladi? =====

#Yozish =====

O'qish=====

O'zgartirish=====

Yashirish

+++++

Rol tushunchasiga ta'rif bering. =====

Foydalanishni boshqarish=====

#Muayyan faoliyat turi bilan bog'liq harakatlar va

majburiyatlar to'plami sifatida belgilanishi mumkin=====

Muayyan faoliyat turi bilan bog'liq imkoniyatlar to'plami

sifatida belgilanishi mumkin=====

Vakolitlarni taqsimlash

+++++

Wi-Fi tarmoqlarida quyida keltirilgan qaysi shifrlash

protokollaridan foydalaniladi.=====

WEB, SSL, WPA2=====

WPA, TLS=====

WPA, FTP=====

#WEP, WPA, WPA2

+++++

Foydalanishni boshqarishning qaysi usuli – Ob’ektlar va Sub’ektlarning atributlari, ular bilan mumkin bo’lgan amallar va so’rovlarga mos keladigan muhit uchun qoidalarni tahlil qilish asosida foydalanishlarni boshqaradi. ====

MAC=====

#ABAC=====

DAC=====

RBAC

+++++

Qanday tarmoq qisqa masofalarda qurilmalar o’rtasida ma’lumot almashinish imkoniyatini taqdim etadi? =====

#Shaxsiy tarmoq=====

Lokal=====

Mintaqaviy =====

CAMPUS

+++++

Quyidagilardan lokal tarmoqqa berilgan ta’rifni belgilang.

=====

Odatda ijaraga olingan telekommunikatsiya liniyalaridan foydalanadigan tarmoqlardagi tugunlarni bir-biriga bog’laydi. =====

Bu tarmoq shahar yoki shaharcha bo’ylab tarmoqlarning o’zaro bog’lanishini nazarda tutadi=====

Qisqa masofalarda qurilmalar o’rtasida ma’lumot almashinish imkoniyatini taqdim etadi=====

#Kompyuterlar va ularni bog’lab turgan qurilmalardan iborat bo’lib, ular odatda bitta tarmoqda bo’ladi.

+++++

Quyidagilardan mintaqaviy tarmoqqa berilgan ta’rifni belgilang. =====

Kompyuterlar va ularni bog’lab turgan qurilmalardan iborat bo’lib, ular odatda bitta tarmoqda bo’ladi. =====

Bu tarmoq shahar yoki shaharcha bo’ylab tarmoqlarning o’zaro bog’lanishini nazarda tutadi=====

#Odatda ijaraga olingan telekommunikatsiya liniyalaridan



foydalanadigan tarmoqlardagi tugunlarni bir-biriga

bog'laydi. ====

Qisqa masofalarda qurilmalar o'rtasida ma'lumot

almashinish imkoniyatini taqdim etadi

+++++

Router nima? ====

Tarmoq qurilmasi bo'lib, ko'plab tarmoqlarni ulash uchun

yoki LAN segmentlarini bog'lash uchun xizmat qiladi

Hisoblash qurilmasining ajralmas qismi bo'lib, qurilmani

tarmoqqa ulash imkoniyatini taqdim etadi====

Ko'plab tarmoqlarni ulash uchun yoki LAN segmentlarini

bog'lash uchun xizmat qiladi. ====

Qabul qilingan signalni barcha chiquvchi portlarga emas

balki paketda manzili keltirilgan portga uzatadi====

#Qabul qilingan ma'lumotlarni tarmoq sathiga tegishli

manzillarga ko'ra (IP manzil) uzatadi.

+++++

Fire Wall ning vazifasi... ====

#Tarmoqlar orasida aloqa o'rnatish jarayonida tashkilot

va Internet tarmog'i orasida xavfsizlikni ta'minlaydi====

Kompyuterlar tizimi xavfsizligini ta'minlaydi====

Ikkita kompyuter o'rtasida aloqa o'rnatish jarayonida

Internet tarmog'i orasida xavfsizlikni ta'minlaydi====

Uy tarmog'i orasida aloqa o'rnatish jarayonida tashkilot

va Internet tarmog'i orasida xavfsizlikni ta'minlaydi

+++++

Stenografiya ma'nosi qanday? ====

sirli xat====

#sirli yozuv====

maxfiy axborot====

maxfiy belgi

+++++

Shifrlash kaliti noma'lum bo'lganda shifrlangan

ma'lumotni deshifrlash qiyinlik darajasini nima

belgilaydi? ====

Shifr matn uzunligi====

#Kriptobardoshlik=====

Shifrlash algoritmi=====

Texnika va texnologiyalar

+++++

Ma'lumotlarni yo'q qilish odatda necha xil usulidan

foydalaniladi? =====

#4 xil=====

8 xil=====

7 xil=====

5 xil

+++++

Kiberjinoyatchilik bu -. . . =====

#Kompyuter yoki boshqa qurilmalarga qarshi qilingan

yoki kompyuter va boshqa qurilmalar orqali qilingan

jinoiy faoliyat. =====

Kompyuter o'yinlari=====

Faqat banklardan pul o'g'irlanishi=====

Autentifikatsiya jarayonini buzish

+++++

Axborot xavfsizligiga bo'ladigan tahdidlarning qaysi biri

maqsadli (atayin) tahdidlar deb hisoblanadi? =====

Tabiiy ofat va avariya=====

Texnik vositalarning buzilishi va ishlamasligi=====

#Strukturalarni ruxsatsiz modifikatsiyalash=====

Foydalanuvchilar va xizmat ko'rsatuvchi hodimlarning

hatoliklari

+++++

Axborot xavfsizligiga bo'ladigan tahdidlarning qaysi biri

tasodifiy tahdidlar deb hisoblanadi? =====

Axborotdan ruxsatsiz foydalanish=====

Zararkunanda dasturlar=====

An'anaviy josuslik va diversiya haqidagi ma'lumotlar

tahlili=====

#Texnik vositalarning buzilishi va ishlamasligi

+++++

Axborotni uzatish va saqlash jarayonida o'z strukturasi va

yoki mazmunini saqlash xususiyati nima deb ataladi?

=====

Axborotning konfidentsialligi=====

Foydalanuvchanligi=====

#Ma'lumotlar butunligi=====

Ixchamligi

+++++

Biometrik autentifikatsiyalashning avfzalliklari-bu: =====

Bir marta ishlatilishi=====

#Biometrik parametrlarning noyobligi=====

Biometrik parametrlarni o'zgartirish imkoniyati=====

Autentifikatsiyalash jarayonining soddaligi

+++++

Simli va simsiz tarmoqlar orasidagi asosiy farq nimadan  
iborat? =====

#Tarmoq chetki nuqtalari orasidagi mutlaqo

nazoratlamaydigan hudud=====

Tarmoq chetki nuqtalari orasidagi xududning kengligi  
asosida qurilmalar holati=====

Himoya vositalarining chegaralanganligi=====

Himoyani amalga oshirish imkoniyati yo'qligi va ma'lum  
protokollarning ishlatilishi

+++++

Simmetrik shifrlashning noqulayligi – bu: =====

#Maxfiy kalitlar bilan ayirboshlash zaruriyatidir=====

Kalitlar maxfiyligi=====

Kalitlar uzunligi=====

Shifrlashga ko'p vaqt sarflanishi va ko'p yuklanishi

+++++

Autentifikatsiya faktorlari nechta? =====

4 ta=====

#3 ta=====

5 ta=====

6 ta

+++++++

Kompyuter tizimida ro'yxatga olish protsedurasini

loyihalashtirish, qaysi standart bo'yicha to'g'ri keltirilgan.

=====

#O'z DSt ISO/IEC 27002:2008=====

O'z DSt ISO/IEC 27002:2005=====

O'z DSt ISO/IEC 27002:2009=====

O'z DSt ISO/IEC 27002:2000=====

+++++++

Parollar bilan ishlashdagi tavsiyalar qaysi qatorda to'g'ri ko'rsatilgan?=====

#Tizimga kirishdagi qayta urinishlar sonini parolning minimal uzunligiga va muhofaza qilinayotgan tizimning qiymatiga muvofiq belgilash;=====

Ro'yxatga olish protsedurasi uchun ruxsat berilgan vaqtni olib tashlash. Agar u ko'paytirilgan bo'lsa, tizimning ro'yxatga olishini davom ettirish;=====

Oxirgi muvaffaqiyatli ro'yxatga olishdan boshlab, boshqa urinishlar so'ramaslik;=====

Kiritilayotgan parolni ko'rsatmaslik yoki variant sifatida bir xil parol tanlash.=====

++++

O'zbekiston Respublikasining "Axborotlashtirish to'g'risida"gi qonunining nechinchi moddasida "Axborot resurslari va axborot tizimlarini muhofaza qilishni maqsadlari" keltiriladi ? =====

19 - modda=====

18 - modda=====

20 - modda=====

21- modda

++++

O'zbekiston Respublikasining "Axborotlashtirish to'g'risida"gi qonunining nechinchi moddasida "Axborot resurslari va axborot tizimlari muhofaza qilinishini tashkil etish " ko'rsatilgan? =====

20 - modda=====

21 - modda=====

22 - modda=====

19 - modda

++++

ISO/IEC 27000 seriyali standart sohaning quyidagi 10 ta  
yo'nalishi bo'yicha boshqarish tamoyillari va amaliy  
tavsiyalari qachon ishlab chiqilgan?

====2005 yilda

====2000 yilda

====2002 yilda

====2004 yilda

++++

ISO/IEC 27000 seriyali standartda sohaning nechta  
yo'nalishi bo'yicha boshqarish tamoyillari va amaliy  
tavsiyalari ishlab chiqilgan? ====

10 ta====

5 ta====

8 ta====

12 ta

++++

"Axborot texnologiyasi. Xavfsizlikni ta'minlash  
metodlari. Axborot xavfsizligini boshqarishning amaliy  
qoidalar ISO/IEC standartining qaysi seriyasida  
kiritilgan? ====

ISO/IEC 27002:2005====

ISO/IEC 27000:2000====

ISO/IEC 27001:2005====

ISO/IEC 27003:2007

++++

Fransiyaning ma'lumotlar xavfsizligi to'g'risidagi  
direktivasi nechinchi yilda kuchga kirdi? ====

2004 yildan====

2000 yildan====

2001 yildan====

2005 yildan

++++

Italiyaning ma'lumotlar xavfsizligi kodeksi qachon qabul  
qilingan? ====

2003 yilda=====

2007 yilda=====

2008 yilda=====

2010 yilda

++++

Avtorizatsiya qilingan foydalanuvchilarning  
foydalanishini cheklash uchun operatsion tizim darajasida  
axborot xavfsizligi qanday vositalarini ishlatishi kerak ?

=====

Avtorizatsiya qilingan foydalanuvchilar foydalanishini  
boshqarishning belgilangan siyosatiga muvofiq  
autentifikatsiya qilinadi; =====

Avtorizatsiya qilingan foydalanuvchilarni foydalanishini  
boshqarish ixtiyoriy ravishda autentifikatsiya qilinadi;

=====

Tizimdan foydalanishga muvaffaqiyatli urinishni bir  
marta yo'lga qo'yadi va boshqa urinishlarda talab  
etilmaydi; =====

Zarur bo'lgan holda foydalanuvchilarning ulanishga  
ruxsat beradi.

++++

Kompyuter tizimida ro'yxatga olish protsedurasini  
loyihalashtirish, qaysi standart bo'yicha to'g'ri keltirilgan.

=====

O'z DSt ISO/IEC 27002:2008 =====

O'z DSt ISO/IEC 27002:2005=====

O'z DSt ISO/IEC 27002:2009=====

O'z DSt ISO/IEC 27002:2000

++++

To'g'ri rejalashtirilgan ro'yxatga olish protsedurasi  
xususiyatlarga ega bo'lishi qaysi qatorda to'g'ri  
ko'rsatilgan. =====

Ro'yxatga olish jarayoni muvaffaqiyatli tugatilmagunicha  
tizimlar yoki ilovalar nomlarini aks ettirmaslik; =====

Kompyuterdan avtorizatsiya qilinmagan foydalanuvchilar  
ham foydalanishi mumkinligi to'g'risida ogohlantiruvchi

umumiy xabarnomani aks ettirish; =====

Ro'yxatga olish protsedurasi davomida avtorizatsiya  
qilinmagan foydalanuvchilarga yordam berishi mumkin  
bo'lgan xabarlar - yo'l-yo'riqlarni taklif etishlik; =====

Ro'yxatga olish axborotini faqat birinchi kirish  
ma'lumotlari kiritilganidan so'ng tasdiqlash. Xato  
kiritilgan holatda ma'lumotlarning qaysi qismi to'g'ri  
yoki noto'g'riligi to'g'risida axborot berish.

++++

Kompyuter tizimida ro'yxatga olish protsedurasini  
loyihalashtirish, qaysi qatorda to'g'ri keltirilgan. =====  
Parolga kirishga qayta urinishlar sonini parolning minimal  
uzunligiga va muhofaza qilinayotgan tizimning qiymatiga  
muvofig belgilash; =====

Ro'yxatga olishning keyingi urinishlari o'rtasidagi  
vaqtinchalik kechikishni ulash yoki istalgan maxsus  
avtorizatsiyasiz ro'yxatga olishning keyingi urinishlariga  
imkon berish; =====

Ma'lumotlarni uzatishda aloqa seansini uzmasdan davom  
etishlik; =====

Agar tizimga kirishga urinishlarning maksimal soniga  
erishilgan bo'lsa, ushbu holat bo'yicha foydalanuvchiga  
axborot berish.

++++

Parollar bilan ishlashdagi tavsiyalar qaysi qatorda to'g'ri  
ko'rsatilgan? =====

Tizimga kirishdagi qayta urinishlar sonini parolning  
minimal uzunligiga va muhofaza qilinayotgan tizimning  
qiymatiga muvofig belgilash; =====

Ro'yxatga olish protsedurasi uchun ruxsat berilgan vaqtni  
olib tashlash. Agar u ko'paytirilgan bo'lsa, tizimning  
ro'yxatga olishini davom ettirish; =====

Oxirgi muvaffaqiyatli ro'yxatga olishdan boshlab, boshqa  
urinishlar so'ramaslik; =====

Kiritilayotgan parolni ko'rsatmaslik yoki variant sifatida  
bir xil parol tanlash.

++++

Agar parollar tizimga kirish seansi jarayonida tarmoq orqali oddiy matnda uzatilsa, ular tarmoqda qaysi dasturlar orqali tutib olinishi mumkin? =====

SNIFFER=====

ADOBE FLASH PLAYER 32.0.0.171=====

SOFT4BOOST TOOLBAR CLEANER 5.8.9.965=====

COMODO DRAGON 70.0.3538.110

++++

Foydalanishni cheklash bo'yicha qanday tadbirlarning qo'llanishini ko'rib chiqish zarur?=====

Tizimning amaliy funksiyalaridan foydalanishni

boshqarish uchun menyuni saqlash; =====

Foydalanuvchilarning o'qishi, yozib olishi, yo'q qilishi, bajarishi kerak bo'lgan holatlarga istisno tariqasida ruxsat berish; =====

Boshqa ilovalarning foydalanish huquqlariga ruxsat berish; =====

Konfidensial axborotga ishlov beradigan biznesilovalardan chiqariladigan ma'lumotlar va faqat avtorizatsiya qilingan terminallarning adresiga va tayinlangan joyga yuborilishiga ishonch hosil qilish. ortiqcha axborotni yo'q qilish uchun chiqarish jarayonini da

++++

O'zbekiston Respublikasining "Davlat sirlarini saqlash to'g'risida" qonuni qachon ishlab chiqilgan. =====

1993 yil 7 may=====

1995 yil 7 aprel=====

2017 yil 7 fevral=====

1992 yil 10 dekabr

++++

Davlat sirlarini saqlashning huquqiy asosi qaysi qatorda to'g'ri ko'rsatilgan. =====

O'zbekiston Respublikasi Konstitutsiyasi=====

ISO/IEC 27002:2005, IDT standarti=====

O'z DSt ISO IEC 27002-2016 (uz) =====



O'zbekiston Respublikasi "Jinoyat kodeksi"

++++

Kasbiy maxfiylik to'g'risida ma'lumot qaysi qatorda  
to'g'ri ko'rsatilgan?

=====

Shaxsning huquqlari va qonuniy manfaatlariga ziyon  
yetkazishi mumkin bo'lgan o'z kasbiy majburiyatlari  
bajarilganligi sababli, ishonchli shaxsga ma'lum bo'lgan  
sir=====

Bu boshqa shaxsning huquqlari va qonuniy manfaatlariga  
ziyon yetkazishi mumkin bo'lgan davlat xizmati bilan  
bog'liq bo'lgan ishonchli shaxsga ma'lum bo'lgan  
sir=====

Ishonchli shaxsning huquqlari va qonuniy manfaatlariga  
ziyon yetkazishi mumkin bo'lmagan davlat bilan bog'liq  
bo'lgan, ishonchli yoki shaxsga (egalikka) ma'lum  
bo'lgan sir=====

Kirish cheklangan professional faoliyat bilan bog'liq  
bo'lmagan ma'lumotlar

++++

Kasbiy (professional) sirlarga oid sirlar qaysi qatorda  
to'g'ri ko'rsatilgan? =====

Tibbiy maxfiylik, aloqa sirlari, notarial sir, advokatning  
maxfiyligi, qabul qilish sirlari (farzand asrab olish  
to'g'risida qaror qabul qilgan sudyalardan tashqari),  
sug'urtalovchining sirlari, e'tirozning siri (saylovlardagi  
yopik ovoz berish) =====

Tibbiy maxfiylik, tijorat sirlari, advokatning maxfiyligi,  
sug'urtalovchining sirlari, e'tirozning siri (saylovlardagi  
yopik ovoz berish) =====

Tijorat sirlari, tibbiy maxfiylik, harbiy sirlar, advokatning  
maxfiyligi, sug'urtalovchining sirlari, e'tirozning siri  
(saylovlardagi yopik ovoz berish) =====

Davlat sirlari, tijorat sirlari, tibbiy maxfiylik, harbiy sirlar,  
advokatning maxfiyligi, sug'urtalovchining sirlari

++++

Shaxs siri turlari. ====

Biografik va identifikatsiya ma'lumotlari, shaxsiy xarakteristikalar (jumladan, shaxsiy odatlar va nayranglar), oilaviy ahvol haqida ma'lumot (oilaviy munosabatlar). ====

Tibbiy maxfiylik, aloqa sirlari, notarial sir, advokatning maxfiyligi, qabul qilish sirlari (farzand asrab olish to'g'risida qaror qabul qilgan sudyalardan tashqari), sug'urtalovchining sirlari, Tibbiy maxfiylik, aloqa sirlari, notarial sir, advokatning maxfiyligi, qabul qili Advokatning maxfiyligi, qabul qilish sirlari (farzand asrab olish to'g'risida qaror qabul qilgan sudyalardan tashqari), sug'urtalovchining sirlari=====

Davlat sirlari, tijorat sirlari, tibbiy maxfiylik, harbiy sirlar, advokatning maxfiyligi, sug'urtalovchining sirlari.

++++

Qachondan Yevropa Ittifoqining barcha mamlakatlarida, jumladan, telekommunikatsiya sohasida yagona shaxsiy ma'lumot himoya qilish tizimi yaratildi? =====

1998 yilda=====

1996 yilda=====

1999 yilda=====

2003 yilda

++++

Davlat sirlari- bu? =====

Davlat tomonidan qo'riqlanadigan va maxsus ro'yxatlar bilan chegaralab qo'yiladigan alohida ahamiyatli, mutlaqo maxfiy va maxfiy harbiy, siyosiy, iqtisodiy, ilmiytexnikaviy va o'zga xil ma'lumotlar=====

Birovga bevosita zarar etkazilishiga yo'l qo'ymaslik xavfi mavjud bo'lmagan shartdir. =====

Shaxs, jamiyat va davlatning hayotiy manfaatlariga putur yetkazadigan shart-sharoit va omillar majmui. =====

Insonning, jamiyatning va davlatning ilg'or rivojlanishining mavjudligi va imkoniyatlarini ishonchli ta'minlaydigan ehtiyojlar majmui.

++++

Xavfsizlikka tahdid - bu ..? =====

Shaxs, jamiyat va davlat hayotiy manfaatlariga putur  
etkazadigan shart-sharoit va omillarning kombinatsiyasi.

=====

Bu hech kimga mumkin bo'lmagan zararni keltirib  
chiqarishga yo'l qo'ymaslik xavfi mavjud bo'lmagan  
shartdir. =====

Birovga bevosita zarar etkazilishiga yo'l qo'ymaslik xavfi  
mavjud bo'lmagan shartdir. =====

Davlatning harbiy, tashqi siyosat, iqtisodiy, razvedka,  
kontr-razvedka va operativ-qidiruv faoliyati sohasidagi  
davlat tomonidan muhofaza qilinadigan ma'lumotlar

++++

Xavfsizlik – bu ? =====

Bu hech kimga mumkin bo'lmagan zararni keltirib  
chiqarishga yo'l qo'ymaslik xavfi mavjud bo'lmagan  
shartdir=====

Shaxs, jamiyat va davlat hayotiy manfaatlariga putur  
etkazadigan shart-sharoit va omillarning  
kombinatsiyasi=====

Davlatning harbiy, tashqi siyosat, iqtisodiy, razvedka,  
kontr-razvedka va operativ-qidiruv faoliyati sohasidagi  
davlat tomonidan muhofaza qilinadigan ma'lumotlar=====

Birovga bevosita zarar etkazilishiga yo'l qo'ymaslik xavfi  
mavjud bo'lmagan shartdir

++++

Hayotning turli sohalarida davlat xavfsizligiga qancha  
tahdid mavjud? =====

5=====

4=====

2=====

3

++++

... - bu egasining mavjud yoki mumkin bo'lgan  
sharoitlarda daromadlarini ko'paytirishga imkon beruvchi  
ma'lumotlarning maxfiyligi, keraksiz xarajatlardan

qochish, tovarlar, ishlar, xizmatlar uchun bozorda  
pozitsiyani saqlab qolish yoki boshqa tijorat manfaa

tijorat sirlari=====

davlat sirlari=====

kasbiy sirlar=====

Xizmat sirlari

++++

...- bu uning kontseptsiyasini va huquqiy rejimini  
belgilash nuqtai nazaridan eng katta qiyinchilikni  
anglatadi, chunki turli vaqtlarda bunday turdagi maxfiylik  
kiritilgan va hozirda turli xil tarkibga ega. =====

Xizmat sirlari=====

Davlat sirlari=====

kasbiy sirlar=====

Tijorat sirlari

++++

...- bu kirish huquqi cheklangan (tibbiy, notarius, advokat  
sirlari, yozishmalar sirlari, telefon so'zlashuvlari, pochta,  
telegraf va boshqa xabarlar va h.k.) bilan bog'liq bo'lgan  
axborot. =====

Kasbiy sirlar=====

Xizmat sirlari=====

Davlat sirlari=====

Tijorat sirlari

++++

...- bu yozishmalar, telefon so'zlashuvlari, pochta,  
telegraf va boshqa kommunikatsiyalar sirlari=====

Aloqa sirlari=====

Natariial sirlar=====

Advokatlik sirlari=====

Sug`urta sirlari

++++

... - bu yuridik yordam ko'rsatish bilan bog'liq holda  
advokatga bildirilgan ma'lumotlar=====

Advokatlik sirlari=====

Aloqa sirlari=====

Natarial sirlar=====

Sug`urta sirlari

++++

Shubhali, firmaning qaltislik va xavfsizlikka oid

qoidalarni buzish ehtimoli jihatidan qaysi kategoriya eng

ko`p uchraydi? =====

Xodimlar=====

xakerlar=====

hujumchilar=====

qarshi tomonlar (shartnoma bo'yicha ishlaydigan shaxslar)

++++

Ma'lumotlarning tasnifi va himoyalanganligini ta'minlash

uchun kim javobgar? =====

rahbarlar=====

foydalanuvchilar=====

Administratorlar =====

Ma'lumot egalari

++++

Sir qanday toifalarga bo`linadi? =====

ob`ektiv, sub`ektiv=====

shaxsiy, umumiy=====

xalqaro, davlat=====

tijorat, bank

++++

Davlat sirlari egasi kim? =====

davlat=====

jamiyat=====

xukumat=====

xarbiy bo`linmalar

++++

Axborotni himoyalash darajasi nima bilan belgilanadi?

=====

Maxfiylik grifi bilan=====

Axborotni konfidensialligi bilan=====

Axborotni qimmati bilan=====

Axborotni ruxsat etilganligi bilan

++++

Axborot xavfsizligini boshqarishning asosiy vazifalarini

sanab o'ting=====

ob'ekt va sub'ektlarning konfiguratsiyani

boshqarishgaruxsati,hisob yozuvlarini boshqarish va faol

tarmoq qurilmalariga ruxsatga ega bo'lish huquqlari,

dasturiy vositalarni yangilanishini boshqarish bilan=====

ob'ekt va sub'ektlarning konfiguratsiyasini boshqarishga

ruxsati, hisob yozuvlarini boshqarish va faol tarmoq

qurilmalariga ruxsatga ega bo'lish huquqlari, =====

ob'ektning konfiguratsiyani boshqarishgaruxsati,hisob

yo'zuvlarini boshqarish va faol tarmoq qurilmalariga

ruxsatga ega bo'lish huquqlari, dasturiy vositalarni

yangilanishini boshqarish bilan=====

ob'ektning konfiguratsiyani boshqarishga ruxsati,hisob

yo'zuvlarini boshqarish va faol tarmoq qurilmalariga

ruxsatga ega bo'lish huquqlari, apparat vositalarni

yangilanishini boshqarish bilan

++++

Ranjirlash bu ? =====

Axborotni himoyalash usuli, birinchidan,

himoyalananadigan axborotni maxfiylik darajasi bo'yicha

bo'lish, ikkinchidan,himoyalananadigan axborotga ruxsatni

cheklashni reglamentlash=====

Axborotni himoyalash usuli ,asosiy tashkiliy choralarni

qamrab oladi – maxfiy xujjatlarga ruxsatni maksimal

chegaralash=====

Axborotni himoyalash usuli,yolg'on ma'lumotlarni

tarqatish orqali himoyalash=====

Axborotni himoyalash usuli,yolg'on ma'lumotlarni

tarqatish orqali himoyalash axborotni himoyalash

usulibo'lib endi tan olinmoqda

++++

Dezinformatsiya bu ? =====

Axborotni himoyalash usuli, davlatning tashkilotning

faoliyatiga tegishli bo'lgan yolg'on ma'lumotlarni

tarqatish=====

Axborotni himoyalash usuli asosiy tashkiliy choralarni  
qamrab oladi – maxfiy xujjatlarga ruxsatni maksimal  
chegaralash=====

Axborotni himoyalash usuli birinchidan, himoyalananadigan  
axborotni maxfiylik darajasi bo'yicha bo'lish,  
ikkinchidan,himoyalananadigan axborotga ruxsatni  
cheklashni reglamentlash=====

Axborotni himoyalash usulibo'lib endi tan olinmoqda

++++

Kodlash bu ? =====

Axborotni himoyalash usuli,asosiy maqsadi raqibdan  
himoyalananadigan axborotni asosiy mazmunini kodlash  
orqali o'zgartirish va aloqa kanallari orqali jo'natish=====

Axborotnihimoyalash usuli, himoyalananadigan ma'lumotni  
istalgan vaqtda olish imkoniyatini ta'minlash, axborot  
tashuvchilarni soni va joyi bo'yicha axborot, ushbu  
axborot foydalanuvchilari to'g'risidagi ma'lumot. =====

Axborotni himoyalash usuli, sirniqulflar emas odamlar  
qo'riqlaydi degan ma'noni bildiradi=====

Axborotni himoyalash usuli, ma'lumotlarni apparat  
vositalar yordamida uzatish

++++

Shifrlash bu ? =====

Har xil radio uskunalari orqali xabarlarni uzatishda,  
yozma xabarlar jo'natishda va boshqa holatlarda raqib  
tomonidan ushbu xabarlarni ushlab qolish xavfi mavjud  
bo'lgan hollarda tez-tez ishlatiladigan axborotni himoya  
qilish usuli=====

himoya qilinadigan axborotning har qanday tashuvchisi  
to'g'risida, yashirin ma'lumotlarning barcha  
tashuvchilarning soniva joylashgan o'rni, shuningdek,  
ushbu axborotning barcha foydalanuvchilari to'g'risidagi  
ma'lumotlarni olish imkonini beruvchi axborotn  
axborotni muhofaza qilishda "sirlarni qulfemas, balki  
odamlar saqlaydi" deb tarjima qilingan umumiy

iboraasosida juda muhim rol o'ynaydi=====

axborotni himoya qilish usuli, bu raqibdan muhofaza  
qilinadigan ma'lumotlarning mazmunini yashirishni  
maqsad qilib oladi va aloqa kanallari orqali ma'lumotlarni  
uzatishda shartli ravishda ochiq matn kodlarini ishlatib,  
raqobatchining qo'lga tushib qolish xav

++++

Axborot xavfsizligining asosiy yo'nalishlari ... =====

axborotni huquqiy, tashkiliy va texnik jihatdan himoya  
qilish=====

faqat axborotlarni muhandislik yuli bilan

himoya qilish=====

faqat tashkiliy yunalishda axborotni xavfsizligi

taminlash=====

axborotni faqat dasturiy ta'minotdan himoya qilish

++++

Axborotni xavfsizligi ... =====

axborot xavfsizligini ta'minlashga qaratilgan choratadbirlar majmuasi=====

foydalanuvchi talablariga muvofiq ma'lumotlar bazasi

tuzilishini ishlab chiqish jarayoni=====

muayyan vazifani bajarish uchun kichik dastur. =====

axborotni faqat dasturiy ta'minotdan himoya qilish

++++

Axborotni himoya qilish vositalari bular? =====

jismoniy apparat, apparat, dasturiy ta'minot va

kriptografik usullar=====

apparat ta'minoti=====

dasturiy ta'minot=====

apparat va kriptografik usullar

++++

Axborot xavfsizligi tushunchasi ... =====

axborotni muhofaza qilishning mazmuni, maqsadlari,  
tamoyillari va tashkil etilishi bo'yicha nuqtai nazar=====

ichki va tashqi tahdidlardan axborot xavfsizligi

holati=====

axborot xavfsizligi kuchlari va vositalari=====



axborot xavfsizligini ta'minlash

++++

Axborot xavfsizligining asosiy komponentlari: =====

konfidentsiallik, mavjudlik va yaxlitlik=====

mavjudligi va yaxlitligi=====

Xavfsizlik=====

yaxlitlik

++++

Tahdid ... =====

axloqiy yoki moddiy zararga olib keladigan potentsial

yoki faktik ta'sir=====

ma'lumotlarni to'plash va almashish uchun mo'ljallangan

dastur, til, tashkiliy va texnik vositalar tizimi=====

aniqlash jarayoni ushbu bosqich talablarining rivojlanish

holatiga javob beradi=====

aniqlash jarayoni ushbu bosqich talablarining rivojlanish

holatiga javob beradi

++++

Axborot xavfsizligi tizimi...? =====

korxona axborot xavfsizligini ta'minlashga qaratilgan

tashkiliy-texnik chora-tadbirlar majmui=====

axborot resurslarini muhofaza qilish holati=====

shaxsiy ma'lumotlardan foydalanishni himoyalash=====

axborotni taqdim etish va tarqatish bilan bog'liq axborotni

saqlash, qidirish va qayta ishlash tizimi va tegishli

tashkilot resurslari

++++

Xavfsizlik siyosatining asoslari=====

foydalanishni boshqarish usuli=====

risklarni boshqarish=====

dasturiy ta'minot=====

aloqa kanallarini tanlash

++++

Axborotning yaxlitligi =====

axborotning dolzarbligi va muvofiqligi, uni yo'qqilishdan

va ruxsat etilmagan o'zgarishlardan himoya qilish=====

axborotdan ruxsatsiz foydalanishdan himoya qilish=====

kerakli axborot xizmatini oqilona vaqt ichida olish

imkoniyati=====

axborotga ruxsat etilishi

++++

"To'qsariqkitob"ga muvofiq tuzilmaviy himoya qanday

sinfda qo'llaniladi? =====

B2=====

B1=====

C1=====

C2

++++

Axborot xavfsizligining necha asosiy komponenti

mavjud? =====

3=====

2=====

4=====

5

++++

Ma'lumotlarni taqdim etish va ularni himoya qilish

darajasini belgilash maqomi quyidagilardir:

Axborotning maxfiyligi

Axborotning yaxlitligi

mavjudligi

Kompaktlik

++++

Qonuniy foydalanuvchilar uchun himoyalangan

ma'lumotlarga to'siqsiz kirishni ta'minlaydigan mulk:

mavjudligi

axborotning maxfiyligi

axborotning yaxlitligi

Kompaktlik

++++

Maxfiy axborotning yo'qolishi va siqib ketishining oldini

olish bo'yicha chora-tadbirlar va himoyalangan ommaviy

axborotning yo'qotilishi quyidagilar hisoblanadi:

axborot xavfsizligi

Axborot himoyasi

axborot urushi

axborotning zaiflashuvi

++++

Ba'zi mamlakatlar rahbarlari hozirda qaysi dasturlarni

ishlab chiqmoqda?

Cyber dasturlari

Windows dasturlari

ishonchli dasturlar

Yangi dasturlar

++++

Tashkilot ichidagi tartibni biladiganlardan qaysi biri katta

zarar etkazishi mumkin?

Xafa qilingan xodimlar

boshqaruvchilar

Hackerlar

barcha xodimlar

++++

Maxfiylik, maxfiylik yoki maxfiylikni yo'qotishga olib

kelishi mumkin bo'lgan potentsial hodisa, jarayonlar yoki

hodisalar quyidagilardan iborat:

tahdid

Xavfsizlik kamomadi

hujum qilish

yaxlitlik

++++

Axborotni himoya qilish tartibi ma'lumotlar .....ga

nisbatan belgilanmaydi.

jamoat arboblarning faoliyati;

davlat sirini;

maxfiy axborot;

shaxsiy ma'lumotlar

++++

OAV ni ro'yxatdan o'tkazish rad etilishi mumkin emas ...

maqsadga muvofiq kelmasa;

ariza noo'rin shaxs tomonidan topshirilgan bo'lsa;  
agar arizadagi ma'lumotlar haqiqatga to'g'ri kelmasa;  
agar ro'yxatdan o'tkazuvchi organ xuddi shu nom va  
tarqatish shakli bo'lgan boshqa ommaviy axborot  
vositasini ro'yxatdan o'tkazgan bo'lsa.

++++

Qaysi ma'lumotlar mahfiylashtiriladi?

fuqarolik mudofaasi kuchlari va vositalari haqidagi  
ma'lumotlar

demografik holat;

jinoyat holati;

inson va fuqarolik huquqlari va erkinliklarini buzish;

++++

Hujjatning raqamli imzosini kim tekshira oladi?

hujjatning elektron namunasini, jo'natuvchining ochiq

kalitini va raqamli imzoning haqiqiy qiymatini

aylantiradigan har qanday manfaatdor shaxs;

faqat elektron nusxa hujjati va yuboruvchining ochiq

kalitini konvertatsiya qilish bo'yicha mutaxassis

elektron hujjatning hujjat almashinuvidan foydalangan

holda, jo'natuvchining ochiq kalitini va haqiqiy raqamli

imzo qiymatini ishlatuvchi mutaxassis;

faqat elektron hujjatning jo'natuvchisi.

++++

Hujjatlangan axborot rejimi bu?

elektron raqamli imzoga ega elektron hujjat;

tanlangan ma'lumotni ma'lum maqsadlar uchun;

har qanday belgi shaklida tanlangan ma'lumotlar;

aniqlash uchun elektron axborot.

++++

Shaxsiy malumotlarni qayta ishlashga subyekt roziligi

so'raladi qachonki hujjatlar .... uchun qayta

ishlanayotgan bo'lsa

operatorning professional faoliyati uchun;

jurnalistning professional faoliyati uchun;

pochta jo'natmalari uchun;

agar uning roziligini olish imkoni bo'lmasa, shaxsiy ma'lumotlarning hayotiy manfaatlarini himoya qilish.

++++

Davlat mulkini boshqarish tartibi nimalar uchun o'rnatiladi?

tabiatda noyob va o'zgarmas bo'lgan ma'lumotlar uchun har qanday ochiq axborot;  
har qanday jamoat tashkilot;  
davlat organlari uchun.

++++

Axborot huquqi nuqtai nazaridan ma'lumot bu taqdim etish shakllaridan qat'iy nazar barcha ma'lumotlar qonunchilik, huquqiy hodisalar, huquqni muhofaza qilish organlari to'g'risidagi ma'lumotlar muayyan yuridik fanni rivojlantirish va uning amaliy qo'llanilishi haqidagi ma'lumotlar;  
ob'ektiv bilimlarni ifodalash shakli.

++++

Axborotning huquqiy munosabatlari obyektlari bo'lolmaydi?

axborot egalari;  
nolegal axborot;  
axborot tizimining elementlari;  
axborot tizimlari;

++++

Axborot sohasida umumiy boshqaruvni amalga oshirish huquqiga ega emas ...

Maslahatchi ekspertlar

Axborot texnologiyalari vazirligi;  
Fan va innovatsiyalar agentligi;  
Xizmat ko'rsatuvchilar

++++

Arxiv fondidagi axborotning ochiqligi qanday ta'minlanadi?

axborotdan foydalanishning turli usullari va ma'lumotlarning bir toifasidan boshqasiga ma'lumot

uzatilishi orqali

axborotdan foydalanishning turli usullari orqali

arxiv fondining huquqiy maqomi orqali

ma'lumotlarning bir toifasidan boshqasiga ma'lumot

uzatilishi orqali

++++

Tijorat siri bilan bog'liq bo'lmagan sifatni ko'rsating

savdo sirlarini o'z ichiga olgan ma'lumotlar ta'sis

hujjatlarida belgilanadi;

ma'lumot haqiqiy yoki potentsial tijorat qiymatiga ega;

axborotdan erkin foydalanish mumkin emas;

axborot egasi maxfiyligini himoya qilish uchun choralar

ko'radi.

++++

Axborot xavfsizligining asosiy ob'ektlari?

yopiq muzokaralarni o'tkazish uchun mo'ljallangan

binolar va davlat sirlari va maxfiy axborot bilan bog'liq

axborotni o'z ichiga olgan axborot resurslari

axborot mahsulotlari;

axborot texnologiyalari sohasida malakali xodimlar.

Ixtiyoriy turdagi yopiq axborotlar

++++

Qonunchilikni rivojlantirishning hozirgi bosqichida

axborot huquqining sub'ekti bu?

axborot sohasida jamoatchilik bilan aloqalar

axborotni ishlab chiqarish, yig'ish, qaytaishlash, to'plash,

saqlash, qidirish, uzatish, tarqatish va iste'mol qilish

jarayonidagi uzaga keladigan axborot munosabatlari

axborot tarmoqlari, axborot resurslari, axborot

texnologiyalari, kommunikatsiya tarmoqlari orqali

axborot vositalari va vositalari texnologiyalari bo'yicha

mehnat natijalarining jamiyati

axborot va ular bilan bog'liq faoliyatdan olingan

mahsulotlar

++++

Quyidagilardan qaysi biri xizmat siriga aloqador emas?

Mehnat shikastlanishi munosabati bilan xodimning

sog'lig'iga olib keladigan zarar

Davlat siri

Kasbiy sir;

tegishli organ faoliyatining sirlari;

++++

Quyidagi variantlardan qaysi biri hujjatlashtirilgan

axborotning huquqiy rejimiga kiradi?

elektron raqamli imzo

Bank sirlari

Shaxsiy malumotlar

Davlat sirlari

++++

Tahririyat majburiyatiga kiradi?

intellektual faoliyat natijalari bo'lgan mualliflik

huquqlariga rioya qilish

fuqarolarning xatlariga javob berish va ularning

vakolatiga kiradigan organlarga xat yuborish;

har qanday holatda, uning nomini oshkor qilmaslik sharti

bilan axborot manbasini sir tutish

fuqaroning sha'ni, qadr-qimmatini yoki biznes obro'siga

ta'sir etsa, uni rad etish yoki fuqaroga o'qish huquqini

berish;

++++

Qaysi ma'lumotlar davlat tomonidan himoyalangani bilan

davlat siriga kirmaydi?

siyosatchilarning shaxsiy hayoti haqidagi ma'lumotlar

tarqalishi davlatga zarar etkazishi mumkin ma'lumotlar

Iqtisodiy sohadadi malumotlar

Tezkor qidiruv haqidagi ma'lumotlar

++++

Tadbirkorlik faoliyati bilan shug'ullanuvchi shaxslar qaysi

axborotga nisbatan tijorat siri rejimini o'rnatishi mumkin?

moliyaviy-iqtisodiy axborotni tashkil etuvchi va ortiqcha

xarajatlardan qochish imkonini beradigan axborotlarga

nisbatan

oziq-ovqat xavfsizligini taminlovchi axborotlarga

nisbatan

ishlab chiqarish jarohatlari, kasbiy ko'rsatkichlari

haqidagi axborotlarga nisbatan

to'lov tizimi va mehnat sharoitlari to'g'risidagi

axborotlarga nisbatan

++++

Himoyalangan ma'lumotlarga tegishli bo'lmagan sifatni

ko'rsating

himoyalangan ma'lumotlarga kirish axborot resurslari

egasi bilan cheklangan

faqat hujjatlashtirilgan ma'lumotlar muhofaza qilinadi

himoyalangan ma'lumotlarga kirish faqat qonun bilan

cheklangan

ma'lumotlarini himoya qilish qonun bilan belgilanadi

++++

Quyidagilarning qaysi biri axborot huquqi tamoyili emas

sanoatda nanotexnologiyalarni qo'llashning afzalliklari

printsipi

aylanish printsipi

tarqatish printsipi

tillarning tengligi printsipi

++++

Antivirusli himoyaning asosiy vositasi?

qimmatli ma'lumotlarni zaxiralash

qattiq disklarni muntazam ravishda skanerlash

axborot xavfsizligi sohasida malakali kadrlar tayyorlash

Ma'lumotlarni klassifikatsiyalash

++++

Veb - server bu

masofaviy erkin foydalanishni ta'minlaydigan kompyuter

yoki dasturiy ta'minot tizimi

kompyuter uchun o'yin konsoli

modemning bir turi

Hizmat taqdim etadigan ulkan kompyuter

++++



Har kim ega bo'lgan huquq to'g'ri ko'rsatilgan javobni

tanlang.

har qanday qonuniy yo'l bilan ma'lumot olish izlash, qabul

qilish, uzatish, ishlab chiqarish va tarqatish

har qanday tarzda ma'lumot izlash, qabul qilish, uzatish,

ishlab chiqarish va tarqatish

axborotni har qanday tarzda qidirish va tarqatish

Ixtiyoriy fuqaro ega bo'lgan huquq bu yerda

ko'rsatilmagan

++++

Qanday taqdim etilishidan qat'i nazar jismoniy shaxslar,

ob'ektlar, faktlar, hodisalar, hodisalar va hodisalar haqida

ma'lumotlar , bu ?

axborot

Axborot tizimi

Ma'lumotlar

Axborot resurslari

++++

Fuqarolarning hayoti faktlari, voqealari va holatlari va

uning kimligini aniqlashga imkon beradigan ma'lumotlar

nima deyiladi?

Shaxsiy ma'lumotlar

Shaxs sirlari

axborot

Axborot resursi

++++

Kirish huquqi cheklangan hujjatlashtirilgan axborot deb

nimaga aytiladi?

Konfidensial axborot

Daxshatli sir

Oddiy sir

axborot

++++

Mulkchilik vakolatlarini to'liq amalga oshiruvchi,

foydalanuvchi va axborotni boshqaruvchi sub'ekt kim?

axborot egasi.

hacker

Mulkdor shaxs

Begona shaxs

++++

Axborot resurslariga nisbatan egalik huquqi borasidagi  
munosabatlarni tartibga soluvchi organ qaysi?

Axborot va fuqarolik qonunchiligi

fuqarolik qonunchiligi

jinoyat qonunchiligi

Soliq qonunchiligi

++++

Davlat sirlariga aloqador ma'lumotlarni o'z ichiga olgan  
axborot resurslari egasi, uni qanday tasarruf etish  
huquqiga ega?

faqat tegishli davlat hokimiyat organlari ruxsati bilan

O'zi hohlaganicha

MFY ruhsati bilan

Militsiya ruhsati bilan istaganicha

++++

Axborot resurslari

O'zbekiston Respublikasining qonun hujjatlari nazarda  
tutilgan mustasno hollardan tashqari, tovar bo'lishi  
mumkin

har doim tovar bo'lishi mumkin;

tovar bo'lishi mumkin emas;

Faqatgina sotilganda tovarga aylanadi

++++

Himoya nazariyasining tarkibiy qismlari qaysi qatorda  
to'g'ri ko'rsatilgan?

himoya muammosining kelib chiqishi, mohiyati va  
mazmuni haqida to'liq va tizimli ma'lumotlar

har qanday tanlangan strategik o'rnatish doirasida himoya  
vazifalarini har qanday to'plamini hal qilishning zarur  
usullari va vositalarini o'z ichiga olgan metodologik va  
instrumental bazalar

axborotni muhofaza qilish ishlarini tashkil etish va

ta'minlash bo'yicha ilmiy asoslangan takliflar

axborotni muhofaza qilish nazariyasi va amaliyotini

rivojlantirishning istiqbolli yo'nalishlarining ilmiy

asoslangan prognozi

++++

Umumiy nazariy xarakterning asosiy tamoyillari qaysilar?

O'rganilayotgan tizimlar va jarayonlarning etarli

modellarini yaratish, bunda maqsadlar shunday qo'yilishi

kerakki, ixtiyoriy etapda ularning yutuqlarini moddiy

baholash imkoni bo'lsin

Ishlab chiqilgan yechimlarni birlashtirish

O'rganilayotgan tizimlar va ishlab chiqilgan

yechimlarning maksimal tuzilishi

Ishlab chiqilgan tushunchalarni amalga oshirishda radikal

evolyutsiya

++++

Axborotni himoya qilish jarayonlariga nima eng ko'p ta'sir

ko'rsatadi?

tasodifiy omillarning kuchli ta'siri

texnik tizimlarning ishlashini tashkil etish va ta'minlash

stoxastiklik

modellashtirish jarayonlari

++++

Noaniq to'plamlar nazariyasi usullari qanday tizimlarni

tavsiflash uchun ishlatiladi?

elementlari faqat ma'lum bir ehtimollik bilan bir yoki

boshqa to'plamlarga tegishli bo'lganda

Himoya jarayonlari tavsifini rasmiylashtirish uchun

Katta tizimlarni himoya qilish jarayonlarini tavsiflash

Katta tizimlarni himoya qilish muammolarini tavsiflash

++++

Lingvistik o'zgaruvchilar nazariyasi usullaridan nima

uchun foydalaniladi?

ekspert-tahlilchilarning norasmiy hukmlari va

xulosalariga asoslangan katta tizimlar modellarini yaratish

Himoya jarayonlari tavsifini rasmiylashtirish uchun

Katta tizimlarni himoya qilish jarayonlarini tavsiflash

Katta tizimlarni himoya qilish muammolarini tavsiflash

++++

Eng mashhur norasmiy baholash usullari qaysilar?

ekspert baholash usullari

jamoaviy baholash usullari

shaxsiy baholash usullari

prognozlash usullari

++++

Ko'p faktorli statistik usullarning asoslari nima?

korrelyatsiya-regression tahlil qilish tartib-taomillaridan

foydalanish

stokastik tahlil usullaridan foydalanish

dinamik tahlil usullaridan foydalanish

korrelyatsion tahlil usullaridan foydalanish

++++

Axborot xavfsizligi masalalariga bag'ishlangan

O'zbekiston Respublikasining asosiy qonuni qaysi?

O'zbekiston Respublikasining "Axborotlashtirish

to'g'risida"gi qonuni.

O'zbekiston Respublikasining "axborot erkinligi

prinsiplari va kafolatlari to'g'risida" gi qonuni»

"Elektron raqamli imzo to'g'risida".

O'zbekiston Respublikasining "elektron hisoblash

mashinalari va ma'lumotlar bazalari uchun dasturlarni

huquqiy muhofaza qilish to'g'risida" gi qonuni»

++++

O'zbekiston Respublikasining "Elektron hisoblash

mashinalari va ma'lumotlar bazalari uchun dasturlarni

huquqiy muhofaza qilish to'g'risida" gi Qonunini qanday

munosabatlarni tartibga soladi?

kompyuterlar va ma'lumotlar bazalari uchun dasturlarni

yaratish, huquqiy himoya qilish va ulardan foydalanish

bilan bog'liq munosabatlar

kompyuterlar va ma'lumotlar bazalari uchun dasturlarni

yaratish, huquqiy himoya qilish va ulardan foydalanish

tartibi

kompyuterlar va ma'lumotlar bazalari uchun dasturlarni o'zgartirish, huquqiy himoya qilish va ulardan foydalanish tartibi.

kompyuter va ma'lumotlar bazalari uchun dasturlarni tarqatish, huquqiy himoya qilish va ulardan foydalanish tartibi.

++++

O'zbekiston Respublikasining 1993 yil 7 maydagi "Davlat sirlarini himoya qilish to'g'risida" gi Qonuni qaysi munosabatlarni tartibga soladi?

davlat sirlari, davlat, harbiy va rasmiy sirlarning toifalarini belgilaydi. Rejimli ob'ektlar. Axborotni davlat sirlariga kiritish

davlat yoki harbiy sirni biladigan fuqarolarning huquqlari

Davlat sirlarini himoya qilish bo'yicha O'zbekiston

Respublikasi davlat xavfsizlik xizmati huquqlari.

Davlat sirlarini sertifikatlashtirish tartibi

++++

Axborot xavfsizligi standartlarining asosiy vazifasi?

axborot texnologiyalari mahsulotlarining malakasi

bo'yicha ishlab chiqaruvchilar, iste'molchilar va mutaxassislar o'rtasida o'zaro hamkorlik qilish uchun asos yaratish.

Axborot texnologiyalari mahsulotlarining malakasi

bo'yicha ishlab chiqaruvchilar, iste'molchilar va ekspertlar o'rtasidagi huquqlarni oqlash

Axborot texnologiyalari mahsulotlarining malakasi

bo'yicha ishlab chiqaruvchilar, iste'molchilar va mutaxassislar o'rtasidagi huquqlarni ajratib turadi

Axborot texnologiyalari mahsulotlarini qabul qilish tartibini nazorat qilish

++++

O'zbekiston Respublikasi milliy sertifikatlashtirish organi?

O'zbekiston davlat standartlashtirish markazi O'zbekiston

Respublikasi Vazirlar Mahkamasi huzuridagi-O'zstandart

DXXning vakolatli organi (sertifikatlashtirish markazi)

Yo'nalishlar bo'yicha ekspert komissiyalari

Yo'nalishlar bo'yicha ekspert komissiyalari

++++

AX soxasi mahsulotlarini sertifikatlash va

axborotlashtirish obyektlarini axborot xavfsizli talablariga

muvofigligini attestatsiyalovchi akkreditlangan organ

qaysi?

DXXning vakolatli organi (sertifikatlashtirish markazi)

O'zbekiston davlat standartlashtirish markazi O'zbekiston

Respublikasi Vazirlar Mahkamasi huzuridagi-O'zstandart

Yo'nalishlar bo'yicha ekspert komissiyalari

Vazirlik va idoralarning rejim-maxfiy organlari

++++

AQSh Milliy xavfsizlik agentligining (NSA) maqsadi?

Texnik vositalar yordamida AQSh milliy xavfsizligini

ta'minlash

AQSh milliy xavfsizligini dasturiy vositalar yordamida

ta'minlash

tashkiliy tadbirlar orqali AQShning milliy xavfsizligini

ta'minlash

taktik operatsiyalar orqali AQSh milliy xavfsizligini

ta'minlash

++++

Mualliflik huquqi, nom berish huquqi va muallifning

obro'sini himoya qilish huquqi qanchagacha saqlanib

qoladi?

Muddatsiz

Hayot davomida

Hayot davomida va o'limdan keyin 50 yil

Hayot davomida va o'limdan keyin 25 yil

++++

Dasturga taqdim etilgan himoya nimalar uchun

qo'llanilmaydi?

kompyuter dasturining asosiy g'oyalari va tamoyillariga

amal qilmaydi

kompyuter dasturining manba kodiga taalluqli emas

kompyuter dasturining ob'ekt kodiga taalluqli emas

kompilyatsiya qilingan kompyuter dasturi kodini qamrab

olmaydi

++++

848-sonli O'zbekiston Respublikasining "Davlat sirlarini

saqlash to'g'risida"gi qonuniqachon qabul qilingan?

1993-yil 7-may

2000-yil 23-mart

1998-yil 4-may

1992-yil 12-dekabr

++++

Davlat sirlari tushunchasi O'zbekiston Respublikasining

"Davlat sirlarini saqlash to'g'risida" qonunining

nechanchi moddasida keltirilgan?

1 - modda

4 - modda

8 - modda

5 - modda

++++

Davlat sirlarini saqlashning huquqiy asosi O'zbekiston

Respublikasi Konstitutsiyasi, ushbu Qonun va unga

muvofiq ravishda chiqariladigan. O'zbekiston

Respublikasining boshqa qonun hujjatlaridan iborat.

Ushbu so'zlar O'zbekiston Respublikasining "Davlat

2 - modda

4 - modda

8 - modda

5 - modda

++++

O'zbekiston Respublikasining davlat sirlariga nimalar

kiradi?

davlat sirlari, harbiy sirlar, xizmat sirlari

davlat sirlari, harbiy sirlar, maxfiy sirlar

davlat sirlari, maxfiy sirlar, konfidensial ma'lumotlar

harbiy sirlar, konfidensial ma'lumotlar, xizmat sirla

++++

Mulk egasiga mavjud yoki ehtimoliy sharoitlarda daromadlarni ko'paytirishga, ortiqcha xarajatlarni qoplamaslikka, tovarlar, ishlar, xizmatlar uchun bozorda pozitsiyani saqlab qolish yoki boshqa tijorat manfaatlariga ega bo'lish imkonini beradigan ma'lumotla

Tijorat siri

Xarbiy sir

Xizmat siri

Davlat siri

++++

... - bu boshqa shaxsning (ishonchli shaxsning) huquqlari va qonuniy manfaatlariga ziyon etkazishi mumkin bo'lgan davlat yoki kommunal xizmat bilan bog'liq bo'lmagan, o'z kasbiy majburiyatlari bajarilganligi sababli, ishonchli yoki shaxsga (egalikka) ma'lu

Kasbiy maxfiylik

Xizmat siri

Tijorat siri

Shaxsiy sir

++++

Shaxsiy ma'lumotlardagi ma'lumotni o'zlarining sha'ni, qadr-qimmati, ishbilarmonlik obro'siga, yaxshi nomga, boshqa noyob imtiyozlarga va mulkiy manfaatlariga zarar etkazishi mumkin bo'lgan axborot nima deyiladi?

Shaxs siri

Davlat siri

Maxfiy axborot

Kasb siri

++++

Inson huquqlari umumjahon deklaratsiyasi nechanchi moddasi quyidagi so'zlar bilan boshlanadi: "Barcha odamlar erkin va teng huquqqa egadirlar va huquqlari bilan tengdirlar". Maxfiylik huquqi konstitutsiyaviy inson huquqlaridan biridir?



1 - modda

4 - modda

8 - modda

5 - modda

++++

Nechanchi yildan beri Evropa Ittifoqining barcha mamlakatlarida, jumladan, telekommunikatsiya sohasida yagona shaxsiy ma'lumot himoya qilish tizimi yaratildi?

1998-yil

1993-yil

1992-yil

1996-yil

++++

Ob'ektlarni o'zaro aloqasini, tuzilishini, qiymatini, kerakli xossalarni va sabablarini o'rganishdagi farazlar qanday ataladi?

Buzg'unchining gipotetik modeli

Sarguzashtqidiruvchi modeli

Bella va La-Padula modeli

Denning modeli

++++

Sabablar, maqsadlar va usullarga bog'liq holda axborot xavfsizligini buzuvchilarni nechta kategoriyaga ajratish mumkin?

4 ta

2 ta

3 ta

8 ta

++++

Odatda, yosh, ko'pincha talaba yoki yuqori sinf o'quvchisi va unda o'ylab qilingan xujum rejasi kamdankam bo'ladi. U nishonini tasodifan tanlaydi, qiyinchiliklarga duch kelsa chekinadi. Bunday sarguzasht qidiruvchi muvaffaqiyatlarini fakat yaqin do'stlari—k

Sarguzasht qidiruvchilar

Ishonchsiz xodimlar

G'oyaviy xakerlar

Xakerlar-professionallar

++++

U o'zining e'tiqodi asosida muayyan nishonlarni (xostlar va resurslarni) tanlaydi. Uning yaxshi ko'rgan xujum turi Web-serverning axborotini o'zgartirishi yoki, juda kam hollarda, xujumlanuvchi resurslar ishini blokirovka qilish.

Bular kimlar?

G'oyaviy xakerlar

Sarguzasht qidiruvchilar

Ishonchsiz xodimlar

Xakerlar-professionallar

++++

U harakatlarning aniq rejasiga ega va ma'lum resurslarni mo'ljallaydi. Uning xujumlari yaxshi o'ylangan va odatda bir necha bosqichda amalga oshiriladi. Avval u dastlabki axborotni yig'adi (operatsion tizim turi, taqdim etiladigan servislar va qo'llaniladigan h

Xakerlar-professionallar

G'oyaviy xakerlar

Sarguzasht qidiruvchilar

Ishonchsiz xodimlar

++++

O'zining harakatlari bilan sanoat josusi etkazadigan muammoga teng muammoni tug'diradi. Buning ustiga uning borligini aniqlash murakkabroq. Undan tashqari unga tarmoqning tashqi himoyasini emas, balki faqat, odatda unchalik kat'iy bo'lmagan tarmo

Ishonchsiz xodimlar

Xakerlar-professionallar

Sarguzasht qidiruvchilar

Ishonchsiz xodimlar

++++

Foydalanish xuquqini cheklash vositalarini qurish maqsadida aktiv sub'ektlar S' va passiv ob'ektlar Q tushunchalari kiritilgan bo'lib sub'ektlarning passiv ob'ektlardan foydalanish xuquqlari turlicha bo'ladigan

model qaysi?

Bella va La-Padula modeli

Sarguzasht qidiruvchi modeli

Denning modeli

Buzg'unchining gipotetik modeli

++++

Ushbu model maxfiylikning turli satxiga ega bo'lgan

xujjatlar bilan ishlashdagi ximoya vositalarining ierarxik

(shajara) modelidir. Bu qaysi model?

Denning modeli

Bella va La-Padula modeli

Sarguzasht qidiruvchimodeli

Buzg'unchining gipotetik modeli

++++

Qaysi model «foydalanishxuquqinicheklovchi matritsa  
modeli» debyuritoladi?

Bella va La-Padula modeli

Sarguzasht qidiruvchi modeli

Denning modeli

Buzg'unchining gipotetik modeli

++++

“O‘zbekiston Respublikasi Axborot texnologiyalari va  
kommunikatsiyalarini rivojlantirish vazirligini tashkil  
etish to‘g‘risida”gi farmon qachon qabul qilingan?

2015-yil 4-fevral

2014-yil 8-dekabr

2016-yil 20-noyabr

2013-yil 3-mart

++++

Tahdidlarningta'riflarga mos ravishda, nechta  
variantdakamaytirish mumkin?

3ta

8ta

4ta

1ta

++++

Tahdid axborotga salbiy ta'sir ko'rsatishi mumkin bo'lgan hodisa, voqea va tasodiflar (yoki ularning paydo bo'lishi ehtimoli) sifatida talqin etiladi. Ushbu parametr har qanday hodisa, voqea va tasodiflar yuzaga kelib qolsa, tahdidni ularning tabiatidan kelib c

Ikkinchi

Birinchi

Uchinchi

To'rtinchi

++++

Tahdid axborot xavfsizligini buzish ehtimoli mavjud bo'lgan vaziyat (ehtimol, xavf) sifatida qaraladi. Bu variant, garchi tavsiflovchi lug'atlarda mavjud bo'lgan tahdidlarning umumiy xavfi sifatida tavsiflansa-da, bu tahdid mutlaqo, xavf, vaziyat va imkoniyat sifa

Birinchi

Ikkinchi

Uchinchi

To'rtinchi

++++

Tahdid axborotning bir yoki boshqa shaklining zaifligiga olib keladigan haqiqiy yoki potensial mumkin bo'lgan harakatlar yoki shartlar sifatida tavsiflanadi. Ba'zi xatti-harakatlar yoki tahdidlarni faqat shartlar bilan identifikatsiya qilish bu tanlovning mohiyatini t

Uchinchi

Ikkinchi

Birinchi

To'rtinchi

++++

Qonunchilikka muvofiq unga ruxsat cheklangan hujjatlashgan axborot qanday axborot?

Konfidensial axborot

Xarbiy axborot

Kasbiy axborot

Maxfiy axborot

++++

Axborot xavfsizligini boshqarishning amaliy qoidalari

ISO/IEC standartining qaysi seriyasida kiritilgan?

ISO/IEC 27002:2005

ISO/IEC 27000:2000

ISO/IEC 27001:2005

ISO/IEC 27003:2007

++++

Kompyuter tizimida ro'yxatga olish protsedurasini

shunday loyihalashtirish kerakki, ruxsatsiz foydalanish

imkoniyati minimumga ISO/IEC standartining seriyasi

buyicha keltirilsin va avtorizatsiya qilinmagan

foydalanuvchiga yordam berilmasin. Ushbu seriya

O'zDSt ISO/IEC 27002:2008

O'zDSt ISO/IEC 27000:2000

O'zDSt ISO/IEC 27003:2007

O'zDSt ISO/IEC 27002:2005

++++

Agar parollar tizimga kirish seansi jarayonida tarmoq

orqali oddiy matnda uzatilsa, ular tarmoqda qanday dastur

orqali tutib olinishi mumkin?

Sniffer

Antispufing

Spuffer

Antispam

++++

"Davlat sirlarini saqlashning xuquqiy asosi" O'zbekiston

Respublikasining "Davlat sirlari saqlash to'g'risida"gi

qonunning nechanchi moddasida keltirilgan?

2-modda

1-modda

4-modda

8-modda

++++

O'zbekiston Respublikasi davlat sirlari nechiga bo'linadi?

3

2

4

5

++++

Mulk egasiga mavjud yoki ehtimoliy sharoitlarda daromadlarni ko'paytirishga, ortiqcha xarajatlarni qoplamaslikka, tovarlar, ishlar, xizmatlar uchun bozorda pozitsiyani saqlab qolish yoki boshqa tijorat manfaatlariga ega bo'lish imkonini beradigan ma'lumotla

Tijorat siri

Kasbiy maxfiylik

Davlat sirlari

Xizmat sirlari

++++

"Barcha odamlar erkin va teng xuquqqa egadirlar va xuquqlari bilan tengdirlar".Maxfiylik xuquqi konstitutsiyaviy inson xuquqlaridan biridir. Ushbu ta'rif "Inson xuquqlari umumjahon deklaratsiyasi" ning nechanchi moddasida keltirilgan?

1

2

4

5

Manba:

++++

Biografik va identifikatsiya ma'lumotlari ( tug'ilish, asrab olish, ajralish), qanday axborot turiga kiradi?

Shaxsiy sirlar

Aloqa sirlari

Davlat sirlar

Kasbiy maxfiylik

++++

Obyektlarni o'zaro aloqasini, tuzilishini, qiymatini, kerakli xossalarni va sabablarini o'rganishdagi farazlar qanday model hisoblanadi?

Buzg'unchining gipotetik modeli

Axborot xavfsizligini buzuvchining modellari

Xavfsizlik modellarini tashkil etish modeli

T.J.Y modeli

++++

Sabablar, maqsadlar va usullarga bog'liq holda axborot xavfsizligini buzuvchilaridan nechta kategoriyaga ajratiladi?

4 ta

3 ta

5 ta

6 ta

++++

Qanday hakerlar odatda yosh ko'pincha talaba yoki yuqori sinf o'quvchisi bo'ladi va unda o'ylab qilingan xujum rejasi kamdan-kam bo'ladi. U nishonni tasodifan tanlaydi, qiyinchiliklarga duch kelsa chekinadi?

Sarguzasht qidiruvchi

G'oyali hakerlar

Ishonchsiz xodimlar

Xakerlar-professionallar

++++

Qanday hakerlar o'zining etiqodi asosida muayyan nishonlarni (xostlar va resurslarni) tanlaydi. Uning yahshi ko'rgan xujumturi Web serverning axborotni o'zgartirishi va xujumlanuvchi resurslarini blokirovka qilish bo'ladi?

G'oyali hakerlar

Ishonchsiz xodimlar

Xakerlar-professionallar

Sarguzasht qidiruvchi

++++

Ximoyalangan axborot maqomini buzulishi axborotning nechta shaklini qo'llash orqali ifodalanadi?

6ta

4ta

7ta

5ta

++++

Ximoyalangn axborotga taxdidlarning mavjud bo'lishlik  
ko'rinishlari nech xil bo'ladi?

3

2

4

5

++++

Axborotni uzatilishida beqarorlikni keltirib chiqaruvchi  
ta'sirlar omillarining tuzilishi necha xil?

4

3

5

6

++++

"Konfederal axborot ximoyasini tashkillashtirish tartibi  
konfederal axborotni elementlar bilan ximoyalashni  
tashkil etish" to'g'risidagi nizom nechanchi sonli ro'yxat  
raqami bilan belgilanadi?

2081

2080

1980

2082

++++

Konfederallikni saqlash va oshkor etmaslik to'g'risida  
kontraktlarga qo'yilgan talablarni belgilashda quyidagi  
qaysi jihatlarga amal qilish kerak?

Aktivlarni boshqarish, xodimlarning xavfsizligi

Konfederal axborotdan foydalanishga ruxsat berishda  
kontraktni imzolayotgan shaxsning majburiyatlari va  
xuquqlari

Tashkilot uzluksiz ishining ta'minlanishini boshqarish

Axborot tizimlarini sotib olish, ishlab chiqish va ularga  
xizmat ko'rsatish

++++

Shartnomaning amal qilish muddati to'xtatilgan hollarda



qanday choralar ko'rish zarur?

Kontrakt muddati tugagan xollarda axborot yo'qqilinishi

yoki qaytarilishi kerak bo'lgan muddatlarni belgilash

Xodimlarning xavfsizligini ta'minlash

Foydalanishni boshqarish

Axborot xavfsiligi identifikatorlarini boshqarish

++++

Konfedensiallikka rioya qilish va oshkor etmaslik

to'g'risidagi shartnomalar nima uchun mo'ljallangan?

Tashkilot axborot aktivlarini muhofaza qilish

Axborot xavfsizligini ta'minlash

Jismoniy xavfsizlik va atrof-muhit xavfsiligini ta'minlash

Xodimlarning xavfsizligini ta'minlash

++++

Avtorizatsiya qilingan foydalanuvchilarning

foydalanishini cheklash uchun operatsion tizim darajasida

axborot xavfsizligi vositalarini necha turga bo'lish kerak?

6

5

4

3

++++

Tizimga xavfsiz kirish tartibi nechiga bo'linadi?

2

4

5

3

++++

Axborot servislaridan foydalanish tizimiga xavfsiz kirish

prodsedurasidan foydalanish yordamida ta'minlangan

bo'lishi bu?

Tizimga xavfsiz kirish tartibi

Avtorizatsiya qilingan foydalanuvchi

Parollarni boshqarish tizimi

Axborotdan foydalanishni cheklash

++++

Qanday xakkerlar harakatning aniq rejasiga ega va  
ma'lum resurslarni mo'ljallaydi. Uning hujumlari yaxshi  
o'ylangan va odatda birnecha bosqichda amalga  
oshiriladi?

Xakerlar-professionallar

Sarguzasht qidiruvchi

G'oyali hakerlar

Ishonchsiz xodimlar

++++

Huquqiy boshqarish haqida ma'lumot nimani anglatadi  
Har qanday axborot, muallifning, asarni yoki asardan  
foydalanish shartlari to'g'risidagi ma'lumotni har qanday  
raqamlar yoki kodlarni aniqlaydi  
har qanday axborot, muallifni aniqlaydi  
asardan foydalanish shartlari to'g'risidagi ma'lumotlar  
har qanday raqam yoki kodlar

++++

Mualliflik huquqini himoya qilish belgisi  
Bir doira ichida lotin harfidan "C" istisno mulk egasining  
nomi (nomlanishi) mulkiy huquqlar , asarning birinchi  
nashr qilingan yili  
har qanday axborot, muallifni aniqlaydi  
asardan foydalanish shartlari to'g'risidagi ma'lumotlar  
har qanday raqam yoki kodlar

++++

Mualliflik huquqi boshqa davlatda tan olinadimi?  
xalqaro shartnomaga muvofiq ushbu huquq tan olinadi.  
xalqaro shartnoma mavjud bo'lmasa, bu huquq tan  
olinmaydi

Hududiy xarakter tabiatiga bogliq

Milliy xarakter tabiatiga bogliq

++++

Mualliflik huquqi quyidagilarga bo'linadi.  
shaxsiy mulk va mulkiy huquqlar  
shaxsiy mulk va jamoatchilik huquqlari  
axloqiy huquqlar

shaxsiy mulk huquqi

++++

Rasmiy topshiriqlarni bajarish tartibida yaratilgan mulk huquqlariga kim egalik qiladi?

agar u va uning muallifi o'rtasida tuzilgan shartnomada nazarda tutilgan bo'lsa, ish beruvchiga tegishlidir

Muallif o'rtasidagi shartnoma aks etilmagan holda muallifning o'ziga tegishlidir

ijarachiga tegishli

Muallifga tegishli

++++

Mualliflik huquqito'g'risidagi butun jahon konvensiyasi qachon qabul qilingan ?

1952 yil 6 sentyabr

1954 yil 6 sentyabr

1972 yil 16 oktyabr

1996 yil 26 dekabr

++++

Respublika mualliflik huquqini himoya qilish

agentligining rasmiy sayti

<http://ima.uz>

<http://lcweb.loc.gov>

<http://lcweb.loc.uz>

<http://lcweb.ru>

++++

Axborot resurslarini muhofaza qilishning tizimli

yondashuviga nima talab qilinadi?

xavfsizlik masalalarini ta'minoti va hal qilish uchun

muhim ahamiyatga ega bo'lgan barcha bir-biriga bog'liq,

o'zaro ta'sirlashadigan va vaqtincha o'zgaruvchan

elementlar, shartlar va omillarni ko'rib chiqish.

tizimning o'zaro va davriy o'zgaruvchan elementlarini

hisobga olish

vaqt bo'yicha o'zgaruvchan elementlarni hisobga olish

O'zaro hamkorlik va vaqt bo'yicha o'zgaruvchan

elementlar va omillarni hisobga olish

++++

Axborot xavfsizligining asosiy tamoyillari.

Tizimli, kompleksli, himoya qilishning uzluksizligi,

oqilona etarlilik, boshqarish va qo'llanilish

moslashuvchanligi , algoritmlarning ochiqqligi va himoya

mexanizmlari , himoya choralari va vositalarini

qo'llashning soddaligi

Tizimli, kompleksli, himoya qilishning davomiyligi

himoya choralari va vositalardan foydalanish qulayligi

algoritmlarning ochiqqligi va muhofaza mexanizmlari

++++

Himoyani buzishga erisha olmaydigan tizimini yaratish

mumkinmi?

mumkin emas.

deyarli mumkin himoyani tizimlilikini inobatga olinsa

Agar himoya choralari va vositalarini qo'llash qulayligi

hisobga olinsa

Algoritmlarning ochiqqligi printsipini va himoya

mexanizmlarini hisobga olsak , asosan mumkin

++++

Himoya vositalarining himoya darajasini o'zgartirishi

uchun nima bo'lishi kerak?

tayinli moslashuvchan bo'lishi kerak

Ommaviy bo'lishi kerak

ma'lum bir xossalarga ega bo'lishi kerak

ba'zi bir o'lchamlarga ega bo'lishi kerak

++++

Algoritmlarning ochiqqligi tamoili va himoya

mexanizmlarining mohiyati

faqatgina tizimli tashkilotlarning sir tutilishi va uning

quyi tizimlarining ishlash algoritmlari sababli himoya

qilish mumkin emas

muhofazani faqat maxfiylik bilan ta'minlash mumkin

emas

strukturaviy tuzilma va algoritmlar tomonidan muhofaza

qilinmasligi kerak

murakkablik tufayli himoya qilish mumkin emas

++++

Baxtsiz hodisalar va tabiiy ofatlardan ko'riladigan zararni

minimallashtirish nimalarga bogliq

ob'ektning joylashishini to'g'ri tanlash;tabiiy ofatlar va

baxtsiz hodisalar bilan shug'ullanish bo'yicha

mutaxassislarni tayyorlash, ularning oqibatlarini bartaraf

etish

tizimning rivojlanishi va faoliyatida yuzaga kelishi

mumkin bo'lgan baxtsiz hodisalar va tabiiy ofatlarni

hisobga olgan holda

yuzaga kelishi mumkin bo'lgan tabiiy ofatlarni bartaraf

etish

himoya usullarini to'g'ri tanlash

++++

Qaysi usul axborotning yaxlitligini ta'minlashning eng

samarali usullaridan biridir

Ma'lumotlarning takrorlanishi

kodlash

shifrlash

Zichlashtirish

++++

Ma'lumotni tiklash vaqtida takrorlash usullari qanday

farqlanishi mumkin?

Tezkor va Tezkor bo'lmagan

Strategik, taktik

chaqqon

uzoq muddatli

++++

o'paytirish usullari quyidagi usullarga bo'linadi.

markazlashtirilgan takrorlash;tarqatilgan takrorlash

Masofali takrorlash

Mahalliy takrorlash

Markazlashtirilgan takrorlash

++++

Axborot tizimlarining bardoshliligi

Axborot tizimining ushbu funktsiyasi alohida jihozlar, bloklar, davrlarning ishlamay qolgan holatlarida ishlashni ta'minlaydi.

bu axborot tizimining ishonchliligi

bu axborot tizimining to'g'riligi

bu axborot tizimining kengayishi

++++

Bardoshli tizimlarni qurishning asosiy yondashuvlari

qaysilar?

axborotni kodlashni bardoshli qilish; adaptiv tizimlarni

yaratish

zahirialash

axborotni kodlash

Shovqinga bardosh kodlash

++++

Standartlarni ishlatishga nima yordam beradi?

axborot xavfsizligi ta'minotini maqsadi qat'iy belgilanadi

Axborot xavfsizligini boshqarishning samarali tizimi

mavjud emas

Mavjud dasturiy vositalardan (dasturiy

ta'minotdan)foydalanish shartlari yaratilmagan.

axborot xavfsizligi va uning hozirgi holatini baholash

++++

Standartlashtirish ob'yektlarining turlari

tizim (axborot, texnik, tashkiliy-texnologik, apparat,

kriptografik va xokazo)AT mahsulotlari, ATtexnologiyalar (shu jumladan jarayonlarni, muolajani)

Axborot tizimi

AT mahsulotlari

AT texnologiyasi

++++

Muayyan hodisa yoki harakatlarning borligini isbotlash

qobiliyati va ularni qo'llab quvvatlaydigan mantiqiy

ob'ektlarni aniqlash ...

rad etolmaslik

butunlik

muvofiqlik

Audit

++++

Tashkilotning yuqori darajali boshqaruvi tomonidan  
rasmiy ravishda ifodalangan maqsad va vazifalari - bu ...

siyosat

strategiya

reja

Xatarlarni boshqarish

++++

Tizim holatining identifikasion korsatkichida xavfsizlik  
siyosatining buzilganligi aniqlangan xolati bu ....

Axborot xavfsizligidagi holat

axborot xavfsizligi intsidenti

axborot xavfsizligiga tahdidi

axborot xavfsizligi xavfi

++++

Xavf quyidagi elementlar bilan ifodalanishi mumkin  
(ortiqchasini olib tashlang):

hodisa

aktiv

tahdid

zaiflik

++++

AQSH mudofaa vazirligi kompyuter tizimlarini

xavfsizligi mezonlariga qanday xavfsizlik toifalari taklif  
etiladi ?

xavfsizlik siyosati

audit va to'g'ri boshqarish siyosati

auditorlik va ishonchni ta'minlash bo'yicha ishonch  
siyosati

auditorlik va to'g'riligini ta'minlash bo'yicha siyosat, audit  
va moslashuvchanlik

++++

Komputer himoyasi uchun antiotladkaning nechta usuli

mavjud

5 ta

4 ta

3 ta

6 ta

++++

Otladchikning borligini tekshiruvchi o'rnatilgan

funksiyalar qanday xususiyatga ega

Antiotladkaning oddiy texnikasi o'ziga

IsDebuggerPresent funksiyasini chaqirish xususiyatiga  
ega

Antiotladkaning oddiy texnikasi o'ziga DebuggerPresent  
funksiyasini chaqirish xususiyatiga ega

Antiotladkaning oddiy texnikasi o'ziga IsDebugger  
funksiyasini chaqirish xususiyatiga ega

Antiotladkaning oddiy texnikasi o'ziga IsPresent  
funksiyasini chaqirish xususiyatiga ega

++++

Komputer himoyasi uchun antiotladkaning qaysi usulida

ThreadHideDebugger nomli yangi flagga ega bo'ladi

Otladchikning borligini tekshiruvchi o'rnatilgan  
funksiyalar usuli

Potoklarni yashirish usuli

Flaglarni tekshirish usuli

To'xtash nuqtalarini aniqlash usuli

++++

Trassirovka mexanizmini ishga tushirishdagi Tracerning  
nechta rejimi mavjud?

3 ta

2 ta

4 ta

5 ta

++++

Trassirovka mexanizmini ishga tushirishdagi Tracerning  
oddiy(normal) rejimi bu ....?

Standart rejim, barcha foydalanuvchi dasturlari uchun  
trassirovka rejimini yoqadi

O'chirish ishlovchilaridan tashqari butun dastur uchun



trassirovka rejimini yoqadi

Chiqarish operatorlari uchun iz rejimini yoqadi

Chiqarish operatorlari uchun sozlash rejimini yoqadi

++++

Trassirovka mexanizmini ishga tushirishdagi Tracerning

asosiy dastur trassirovkasi (Trace Main) rejimi bu ....?

O'chirish ishlovchilaridan tashqari butun dastur uchun

trassirovka rejimini yoqadi

Chiqarish operatorlari uchun iz rejimini yoqadi

Chiqarish operatorlari uchun sozlash rejimini yoqadi

Standart rejim, barcha foydalanuvchi dasturlari uchun

trassirovka rejimini yoqadi

++++

Trassirovka mexanizmini ishga tushirishdagi Tracerning

uzluksiz ishlovlar trassirovkasi (Trace INT) rejimi bu ....?

Chiqarish operatorlari uchun iz rejimini yoqadi.

Standart rejim, barcha foydalanuvchi dasturlari uchun

trassirovka rejimini yoqadi.

O'chirish ishlovchilaridan tashqari butun dastur uchun

trassirovka rejimini yoqadi

Chiqarish operatorlari uchun sozlash rejimini yoqadi

++++

Windows operatsion tizimidagi driverlarning saqlanish  
joyi?

Windowsda qurilma Driverlari C: WINDOWS\SYSTEM32  
katalogida saqlanadi.

Windowsda qurilma Driverlari C: WINDOWS\ADMIN  
katalogida saqlanadi

Windowsda qurilma Driverlari C: WINDOWS\FILE  
katalogida saqlanadi.

Windowsda qurilma Driverlari C: WINDOWS\ROOT  
katalogida saqlanadi.

++++

Driver so'zining ma'nosi?

Haydovchi.

Sozlovchi

Boshqaruvchi

Ma'mur

++++

Kirishni cheklash tizimi nechta funksional blokdan  
iborat?

4 ta

5 ta

3 ta

2 ta

++++

Kirishni cheklash tizimining birinchi funksional bloki bu  
?

subyektlarga ruxsat berish bloki=====

ruxsatni boshqarish dispetcheri apparat-dasturiy  
mexanizmlardan foydalangan holda yaratilgan bo'lib  
yetarli darajadagi subyektlarni obyektlarga ruxsatini  
cheklash bloki. =====

dasturni saqlash va uzatishda kriptografik qayta ishlash  
bloki. =====

xotirani tozalash bloki.

++++

Kirishni cheklash tizimining ikkinchi funksional bloki bu?

=====

ruxsatni boshqarish dispetcheri apparat-dasturiy  
mexanizmlardan foydalangan holda yaratilgan bo'lib  
yetarli darajadagi subyektlarni obyektlarga ruxsatini  
cheklash bloki=====

subyektlarga ruxsat berish bloki. =====

dasturni saqlash va uzatishda kriptografik qayta ishlash  
bloki=====

xotirani tozalash bloki.

++++

Kirishni cheklash tizimining uchinchi funksional bloki  
bu? =====

dasturni saqlash va uzatishda kriptografik qayta ishlash  
bloki. =====

xotirani tozalash bloki. ====

subyektlarga ruxsat berish bloki=====

ruxsatni boshqarish dispetcheri apparat-dasturiy  
mexanizmlardan foydalangan holda yaratilgan bo'lib  
yetarli darajadagi subyektlarni obyektlarga ruxsatini  
cheklash bloki

++++

Kirishni cheklash tizimining to'rtinchi funksional bloki  
bu? =====

xotirani tozalash bloki. =====

ruxsatni boshqarish dispetcheri apparat-dasturiy  
mexanizmlardan foydalangan holda yaratilgan bo'lib  
yetarli darajadagi subyektlarni obyektlarga ruxsatini  
cheklash bloki=====

subyektlarga ruxsat berish bloki=====

dasturni saqlash va uzatishda kriptografik qayta ishlash  
bloki.

++++

Shadow Defender bu - ? =====

Operatsion tizimni soya rejimida ishga tushiruvchi  
vazifasini bajaradigan va barcha bajarilgan amallar keyin  
windows OT qayta ishga tushurilgunga qadar qattiq  
diskda saqlab turish imkonini beradigan dastur=====

Operatsion tizimni soya rejimida ishga tushiruvchi  
vazifasini bajaradigan va barcha bajarilgan amallar keyin  
windows OT qayta ishga tushurilgunga qadar o'chirib  
turish imkonini beradigan dastur=====

Operatsion tizimni ish rejimini monitoring qilish imkonini  
beradigan dastur=====

Operatsion tizimni faqat admin rejimida ishga tushirish  
imkonini beradigan dastur

++++

Shadow defender ..... himoyalovchi rejim ham deb  
ataladi=====

"Soya rejimi" =====

"Mehmon rejimi" =====

“Admin rejimi” =====

“Kuzatuvchi rejimi”

++++

Ochiq kodli dasturiy taminot bu? =====

dasturiy ta’minotni ishlab chiqarishning shunday usuliki,  
unda dasturlarning yaratilayotgan dastlabki kodi ochiq  
ya’ni barcha ko’rib chiqishi va o’zgartirish kiritishi uchun  
ochiq bo’ladi. =====

dasturiy ta’minotni ishlab chiqarishning shunday usuliki,  
unda dasturlarning yaratilayotgan dastlabki kodi yopiq  
bo’ladi=====

o’zgartirish imkoni bo’lmagan dasturiy ta’minot=====

Litsenziyaga ega bo’lgan o’zgartirish imkoni bo’lmagan  
dasturiy ta’minot

++++

Yopiq kodli dasturiy ta’minot bu ? =====

o’z nomi bilan asos kodi yopiq bolgan dasturiy  
ta’minot=====

dasturiy ta’minotni ishlab chiqarishning shunday usuliki,  
unda dasturlarning yaratilayotgan dastlabki kodi ochiq  
bo’ladi=====

o’zgartirish imkoni faqat litenziya asosidagi dasturiy  
ta’minot=====

Litsenziyaga ega va o’zgartirish imkoni bo’lgan dasturiy  
ta’minot

++++

Universal grafika bu ? =====

Windows dasturlarning qurilmalarga va dastur ta'minotiga  
bog'liqsizligini ta'minlaydi=====

Operatsion tizimdagi dasturlar interfeysi=====

Windows dasturlarni internet orqali yangilash vazifasini  
bajarish grafikasi. =====

Umumiy qoidalar to’plami

++++

Yagona interfeys bu? =====

Windowsda foydalanuvchining muloqoti yagona, ya'ni

turli dasturlar bilan ishlash qoidalarini umumiy bo'lgan

interfeysdir====

Windows dasturlarini internet orqali yangilash vazifasini

bajarish grafikasi====

Umumiy qoidalar to'plami====

Operatsion tizimdagi dasturlar interfeysi

++++

Operatsion tizimning ko'p masalaliligi bu ? =====

Operatsion tizimning dasturlararo ma'lumot almashish

imkoniga ega ekanligidir. =====

Operatsion tizimning faqat internet orqali ma'lumot

almashish imkoniga ega ekanligidir=====

Operatsion tizimning qo'shimcha imkoniyat qo'shish

imkoniga ega ekanligidir. =====

Operatsion tizimning ochiq kodli dasturlarini qo'llab -

quvvatlash imkoniga ega ekanligidir

++++

DDE nima ? =====

Dinamic Data Exchange - ma'lumotlarning dinamik

almashinuvi. =====

Dinamic Datetime Exchange - ma'lumotlarning dinamik

almashinuvi=====

Dinamic Diagram Exchange - diagrammalarni dinamik

almashinuvi =====

Dinamic Delete Exchange – o'chirishlarni dinamik

almashinuvi

++++

Axborot jamiyati bu ?=====

bu axborot iqtisodiyoti paradigmasi doirasida faoliyat

yuritadigan jamiyat=====

bu axborot siyosati paradigmasi doirasida faoliyat

yuritadigan jamiyat=====

bu axborotlashgan jamiyat=====

paradigma doirasida faoliyat yuritadigan internetsiz

jamiyat

++++

Komyuter etikasi bu ?

fanlararo tadqiqotlar sohasi bo'lib, texnik, axloqiy, huquqiy, ijtimoiy, siyosiy va falsafiy masalalarni ko'rib chiqishni o'z ichiga oladi

fanlararo tadqiqotlar sohasi bo'lib, texnik, axloqiy, huquqiy, ijtimoiy, siyosiy va falsafiy masalalarni ko'rib chiqishni o'z ichiga oladi=====

siyosiy masalalarni ko'rib chiqishni o'z ichiga oladi=====

falsafiy masalalarni ko'rib chiqishni o'z ichiga oladi

++++

IFIP nima ? =====

International Federation for Information Processing ya'ni

Xalqaro axborotni qayta ishlash federatsiyasi=====

International Federation for Information Press ya'ni

Xalqaro axborotni nashr etish federatsiyasi=====

International Federation for Information Protect ya'ni

Xalqaro axborotni himoyalash federatsiyasi=====

International Federation for Information Private ya'ni

Xalqaro axborotni maxfiylash federatsiyasi

I:

S:Axborot xavfsizligining asosiy maqsadlaridan biribu...

+:Axborotlarni o'g'irlanishini, yo'qolishini, soxtalashtirilishini oldini olish

-:Ob'ektga bevosita ta'sir qilish

-:Axborotlarni shifrlash, saqlash, yetkazib berish

-:Tarmoqdagi foydalanuvchilarni xavfsizligini ta'minlab berish

I:

S:Konfidentsiallikga to'g'ri ta'rif keltiring.

+:axborot inshonchliligi, tarqatilishi mumkin emasligi, maxfiyligi kafolati;

-:axborot konfidensialligi, tarqatilishi mumkinligi, maxfiyligi kafolati;

-:axborot inshonchliligi, tarqatilishi mumkin emasligi, parollanganligi kafolati;

-:axborot inshonchliligi, axborotlashganligi, maxfiyligi

kafolati;

I:

S:Yaxlitlikni buzilishi bu - ...

+:Soxtalashtirish va o'zgartirish

-:Ishonchsizlik va soxtalashtirish

-:Soxtalashtirish

-:Butunmaslik va yaxlitlanmaganlik

I:

S:Kompyuter virusi nima?

+:Maxsus yozilgan va zararli dastur

-: .exe fayl

-:Boshqariluvchi dastur

-:Kengaytmaga ega bo'lgan fayl

I:

S:Axborotni himoyalash uchun qanday usullar  
qo'llaniladi?

+:Kodlashtirish, kriptografiya, stegonografiya

-:Kodlashtirish va kriptografiya, maxsus yozilgan kod

-:Stegonografiya, kriptografiya, orfografiya

-:Kriptografiya, kodlashtirish, sintaksis

I:

S:Kriptografiyaning asosiy maqsadi...

+:maxfiylik, yaxlitlilikni ta'minlash

-:ishonchlilik, butunlilikni ta'minlash

-:autentifikatsiya, identifikatsiya

-:ishonchlilik, butunlilikni ta'minlash, autentifikatsiya,  
identifikatsiya

I:

S:SMTP - Simple Mail Transfer protokol nima?

+:elektron pochta protokoli

-:transport protokoli

-:internet protokoli

-:Internetda ommaviy tus olgan dastur

I:

S:Kompyuter tarmog'ining asosiy komponentlariga  
nisbatan xavf-xatarlar...

+:uzilish, tutib qolish, o'zgartirish, soxtalashtirish

-:o'zgartirish, soxtalashtirish

-:tutib qolish, o'zgarish, uzilish

-:soxtalashtirish, uzilish, o'zgartirish

I:

S:...ma'lumotlar oqimini passiv hujumlardan himoya qilishga xizmat qiladi.

+:konfidentsiallik

-:identifikatsiya

-:autentifikatsiya

-:maxfiylik

I:

S:Foydalanish huquqini cheklovchi matritsa modeli bu...

+:Bella La-Padulla modeli

-:Dening modeli

-:Landver modeli

-:Huquqlarni cheklovchi model

I:

S:Kalit – bu ...

+:Matnni shifrlash va shifrini ochish uchun kerakli axborot

-:Bir qancha kalitlar yig'indisi

-:Axborotli kalitlar to'plami

-:Belgini va raqamlarni shifrlash va shifrini ochish uchun kerakli axborot

I:

S:Qo'yish, o'rin almashtirish, gammalash kriptografiyaning qaysi turiga bog'liq?

+:simmetrik kriptotizimlar

-:assimetrik kriptotizimlar

-:ochiq kalitli kriptotizimlar

-:autentifikatsiyalash

I:

S:Autentifikatsiya nima?

+:Ma'lum qilingan foydalanuvchi, jarayon yoki qurilmaning haqiqiy ekanligini tekshirish muolajasi



-:Tizim me'yoriy va g'ayritabiiy hollarda

rejalashtirilgandek o'zini tutishligi holati

-:Istalgan vaqtda dastur majmuasining mumkinligini  
kafolati

-:Tizim noodatiy va tabiiy hollarda qurilmaning haqiqiy  
ekanligini tekshirish muolajasi

I:

S:Identifikatsiya bu- ...

+:Foydalanuvchini uning identifikatori (nomi) bo'yicha  
aniqlash jarayoni

-:Ishonchliligini tarqalishi mumkin emasligi kafolati

-:Axborot boshlang'ich ko'rinishda ekanligi uni saqlash,  
uzatishda ruxsat etilmagan o'zgarishlar

-:Axborotni butunligini saqlab qolgan holda uni  
elementlarini o'zgartirishga yo'l qo'ymaslik

I:

S:O'rin almashtirish shifri bu - ...

+:Murakkab bo'lmagan kriptografik akslantirish

-:Kalit asosida generatsiya qilish

-:Ketma-ket ochiq matnni ustiga qo'yish

-:Belgilangan biror uzunliklarga bo'lib chiqib shifrlash

I:

S:Simmetrik kalitli shifrlash tizimi necha turga bo'linadi.

+:2 turga

-:3 turga

-:4 turga

-:5 turga

S:Kriptografiyada matn –bu..

+:alifbo elementlarining tartiblangan to'plami

-:matnni shifrlash va shifrini ochish uchun kerakli axborot

-:axborot belgilarini kodlash uchun foydalaniladigan  
chekli to'plam

-:kalit axborotni shifrlovchi kalitlar

I:

S:Kriptoanaliz –bu..

+:kalitlarni bilmasdan shifrnı ochishga bardoshlilikni

aniqllovchi shifrlash tavsifi

-:axborotni qayta akslantirishning matematik usullarini  
izlaydi va tadqiq qiladi

-:axborotni qayta akslantirib himoyalash muammosi bilan  
shug'ullanadi

-:kalitni bilmasdan shifrlangan matnni ochish  
imkoniyatlarini o'rganadi

I:

S:Shifrlash atamasini belgilang.

+:akslantirish jarayoni ochiq matn deb nomlanadigan  
matn shifrmtn ga almashtiriladi

-:kalit asosida shifrmtn ochiq matn ga akslantiriladi

-:shifrlashga teskari jarayon

-:Almashtirish jarayoni bo'lib: ochiq matn deb  
nomlanadigan matn o'girilgan holatga almashtiriladi

I:

S:Blokli shifrlash tushunchasi nima?

+:shifrlanadigan matn blokiga qo'llaniladigan asosiy  
akslantirish

-:murakkab bo'lmagan kriptografik akslantirish

-:axborot simvollarini boshqa alfavit simvollarini bilan  
almashtirish

-:ochiq matnning har bir harfi yoki simvoli alohida  
shifrlanishi

I:

S:Simmetrik kriptotizimning uzluksiz tizimida ...

+:ochiq matnning har bir harfi va simvoli alohida  
shifrlanadi

-:belgilangan biror uzunliklarga teng bo'linib chiqib  
shifrlanadi

-:murakkab bo'lmagan kriptografik akslantirish orqali  
shifrlanadi

-:ketma-ket ochiq matnlarni o'rniga qo'yish orqali  
shifrlanadi

I:

S:Kriptotizimga qo'yiladigan umumiy talablardan biri

nima?

+:shifr matn uzunligi ochiq matn uzunligiga teng bo'lishi  
kerak

-:shifrlash algoritmining tarkibiy elementlarini

o'zgartirish imkoniyati bo'lishi lozim

-:ketma-ket qo'llaniladigan kalitlar o'rtasida oddiy va  
oson bog'liqlik bo'lishi kerak

-:maxfiylik o'ta yuqori darajada bo'lmoqligi lozim

I:

S:Berilgan ta'riflardan qaysi biri asimmetrik tizimlarga  
xos?

+:Asimmetrik kriptotizimlarda  $k_1 \neq k_2$  bo'lib,  $k_1$  ochiq  
kalit,  $k_2$  yopiq kalit deb yuritiladi,  $k_1$  bilan axborot  
shifrlanadi,  $k_2$  bilan esa deshifrlanadi

-:Asimmetrik tizimlarda  $k_1 = k_2$  bo'ladi, yahni  $k$  – kalit  
bilan axborot ham shifrlanadi, ham deshifrlanadi

-:Asimmetrik kriptotizimlarda yopiq kalit axborot  
almashinuvining barcha ishtirokchilariga ma'lum bo'ladi,  
ochiq kalitni esa faqat qabul qiluvchi biladi

-:Asimmetrik kriptotizimlarda  $k_1 \neq k_2$  bo'lib, kalitlar  
hammaga oshkor etiladi

I:

S:Yetarlicha kriptoturg'unlikka ega, dastlabki matn  
simvollarini almashtirish uchun bir necha alfavitdan  
foydalanishga asoslangan almashtirish usulini belgilang.

+:Vijener matritsasi, Sezar usuli

-:Monoalfavitli almashtirish

-:Polialfavitli almashtirish

-:O'rin almashtirish

I:

S:Simmetrik guruh deb nimaga aytiladi?

+:O'rin almashtirish va joylashtirish

-:O'rin almashtirish va solishtirish

-:Joylashtirish va solishtirish

-:O'rin almashtirish va transportizatsiyalash

I:

S:Qo'yish, o'rin almashtirish, gammalash

kriptografiyaning qaysi turiga bog'liq?

+:simmetrik kriptosistemalar

-:assimetrik kriptosistemalar

-:ochiq kalitli kriptosistemalar

-:autentifikatsiyalash

I:

S:Xavfli viruslar bu - ...

+:kompyuter ishlashida jiddiy nuqsonlarga sabab

bo'luvchi viruslar

-:tizimda mavjudligi turli taassurot (ovoz, video) bilan

bog'liq viruslar, bo'sh xotirani -kamaytirsada, dastur va ma'lumotlarga ziyon yetkazmaydi

-:o'z-o'zidan tarqalish mexanizmi amalga oshiriluvchi viruslar

-:dastur va ma'lumotlarni buzilishiga hamda kompyuter ishlashiga zarur axborotni o'chirilishiga bevosita olib keluvchi, muolajalari oldindan ishlash algoritmlariga joylangan viruslar

I:

S:Elektron raqamli imzo tizimi qanday muolajalarni amalga oshiradi?

+:raqamli imzoni shakllantirish va tekshirish muolajasi

-:raqamli imzoni hisoblash muolajasi

-:raqamli imzoni hisoblash va tekshirish muolajasi

-:raqamli imzoni shakllantirish muolajasi

I:

S:Shifrlashning kombinatsiyalangan usulida qanday kriptotizimlarning kriptografik kalitlaridan foydalaniladi?

+:Simmetrik va assimetrik

-:Simmetrik

-:Assimetrik, chiziqli

-:Gammalashgan, simmetrik, assimetrik

I:

S:Axborot himoyasi nuqtai nazaridan kompyuter tarmoqlarini nechta turga ajratish mumkin?

+:Korporativ va umumfoydalanuvchi

-:Regional, korporativ

-:Lokal, global

-:Shaharlararo, lokal, global

I:

S:Shaxsning, o'zini axborot kommunikatsiya tizimiga

tanishtirish jarayonida qo'llaniladigan belgilar ketmaketligi bo'lib, axborot kommunikatsiya tizimidan

foydalanish huquqiga ega bo'lish uchun

foydalaniluvchining maxfiy bo'lmagan qayd yozuvi –

bu...

+:login parol

-:identifikatsiya

-:maxfiy maydon

-:token

I:

S:Uning egasi haqiqiyligini aniqlash jarayonida tekshiruv

axboroti sifatida ishlatiladigan belgilar ketma-ketligi

(maxfiy so'z) – nima?

+:parol

-:login

-:identifikatsiya

-:maxfiy maydon foydalanuvchilarni ro'yxatga olish va

ularga dasturlar va ma'lumotlarni ishlatishga huquq berish

jarayoni

I:

S:Identifikatsiya jarayoni qanday jarayon?

+:axborot tizimlari obyekt va subhektlariga uni tanish

uchun nomlar (identifikator) berish va berilgan nom

bo'yicha solishtirib uni aniqlash jarayoni

-:ob'ekt yoki subhektni unga berilgan identifikatorga

mosligini tekshirish va belgilar ketmaketligidan iborat

maxfiy kodini tekshirish orqali aslligini aniqlash

-:foydalanuvchining resursdan foydalanish huquqlari va

ruxsatlarini tekshirish jarayoni

-:foydalanuvchilarni ro'yxatga olish va ularga dasturlar va

ma'lumotlarni ishlatishga huquq berish jarayoni

I:

S: Autentifikatsiya jarayoni qanday jarayon?

+: ob'ekt yoki subhektni unga berilgan identifikatorga mosligini tekshirish va belgilar ketma-ketligidan iborat maxfiy kodini tekshirish orqali asliligini aniqlash

-: axborot tizimlari obyekt va subhektlariga uni tanish uchun nomlar (identifikator) berish va berilgan nom bo'yicha solishtirib uni aniqlash jarayoni

-: foydalanuvchining resursdan foydalanish huquqlari va ruxsatlarini tekshirish jarayoni

-: foydalanuvchilarni ro'yxatga olish va ularga dasturlar va ma'lumotlarni ishlatishga huquq berish jarayoni

I:

S: Ro'yxatdan o'tish-bu...

+: foydalanuvchilarni ro'yxatga olish va ularga dasturlar va ma'lumotlarni ishlatishga huquq berish jarayoni

-: axborot tizimlari ob'ekt va subhektlariga uni tanish uchun nomlar (identifikator) berish va berilgan nom bo'yicha solishtirib uni aniqlash jarayoni

-: ob'ekt yoki subhektni unga berilgan identifikatorga mosligini tekshirish va belgilar ketma-ketligidan iborat maxfiy kodini tekshirish orqali asliligini aniqlash

-: foydalanuvchining resursdan foydalanish huquqlari va ruxsatlarini tekshirish jarayoni

I:

S: Axborot qanday sifatlarga ega bo'lishi kerak?

+: ishonchli, qimmatli va to'liq

-: uzluksiz va uzlukli

-: ishonchli, qimmatli va uzlukli

-: ishonchli, qimmatli va uzluksiz

I:

S: Axborotning eng kichik o'lchov birligi nima?

+: bit

-: kilobayt

-: bayt

-: bitta simvol

I:

S:Axborotlarni saqllovchi va tashuvchi vositalar qaysilar?

+:USB fleshka, CD va DVD disklar

-:Qattiq disklar va CDRom

-:CD va DVD, kesh xotira

-:Qattiq disklar va DVDROM

I:

S:Avtorizatsiya jarayoni qanday jarayon?

+:foydalanuvchining resursdan foydalanish huquqlari va ruxsatlarini tekshirish jarayoni

-:axborot tizimlari obyekt va subhektlariga uni tanish uchun nomlar (identifikator) berish va -berilgan nom bo'yicha solishtirib uni aniqlash jarayoni

-:ob'ekt yoki subhektga unga berilgan identifikatorga mosligini tekshirish va belgilar ketma-ketligidan iborat maxfiy kodini tekshirish orqali aslligini aniqlash.

-:parollash jarayoni

I:

S:Imzo bu nima ?

+:hujjatning haqiqiylikini va yuborgan fizik shaxsga tegishli ekanligini tasdiqlaydigan insonning fiziologik xususiyati.

-:elektron hujjatlarning haqiqiylik va butunligi-ni nazorat qilishni ta'minlovchi bo'lgan qo'yilgan imzoning analogi

-:hujjatning haqiqiylikini va biror bir yuridik shaxsga tegishli ekanligini tasdiqlovchi isbotdir.

-:hujjatda elektron raqamli imzoni yaratish uchun mo'ljallangan belgilar ketma-ketligi;

I:

S:Sezarning shifrlash sistemasining kamchiligi nimada?

+:Harflarning so'zlarda kelish chastotasini yashirmaydi

-:Alfavit tartibining o'zgarmasligi

-:Kalitlar sonining kamchiligi

-:Shifrtakstni ochish osonligi

I:

S:Axborot xavfsizligi va xavfsizlik san'ati haqidagi fan

.... deyiladi.

+:Kriptografiya

-:Kriptotahlil

-:Kriptologiya

-:Kriptoanalitik

I:

S:Tekstni boshqa tekst ichida ma'nosini yashirib keltirish

bu - ...

+:steganografiya

-:sirli yozuv

-:skrembler

-:rotor mashinalar

I:

S:Shifrttekstni ochiq tekstga akslantirish jarayoni nima deb

ataladi?

+:Deshifrlash

-:Xabar

-:Shifrlangan xabar

-:Shifrlash

I:

S:.....—hisoblashga asoslangan bilim sohasi bo'lib,

buzg'unchilar mavjud bo'lgan sharoitda amallarni

kafolatlash uchun o'zida texnologiya, inson, axborot va

jarayonni mujassamlashtirgan.

+:Kiberxavfsizlik

-:Axborot xavfsizligi

-:Kiberjtnoyatchilik

-:Risklar

I:

S:Risk nima?

+:Potensial foyda yoki zarar

-:Potensial kuchlanish yoki zarar

-:Tasodifiy taxdid

-:Katta yo'qotish

I:

S:Tahdid nima?



+:Tashkilotga zarar yetkazishi mumkin bo'lgan

istalmagan hodisa

-:Tashkilot uchun qadrli bo'lgan ixtiyoriy narsa

-:Bu riskni o'zgartiradigan harakatlar bo'lib

-:Bu noaniqlikning maqsadlarga ta'siri

I:

S:Kodlash nima?

+:Ma'lumotni osongina qaytarish uchun hammaga ochiq bo'lgan sxema yordamida ma'lumotlarni boshqa formatga o'zgartirishdir

-:Ma'lumot boshqa formatga o'zgartiriladi, biroq uni faqat maxsus shaxslar qayta o'zgartirishi mumkin bo'ladi

-:Ma'lumot boshqa formatga o'zgartiriladi, barcha shaxslar kalit yordamida qayta o'zgartirishi mumkin bo'ladi

-:Maxfiy xabarni soxta xabar ichiga berkitish orqali aloqani yashirish hisoblanadi

I:

S:Shifrlash nima?

+:Ma'lumot boshqa formatga o'zgartiriladi, biroq uni faqat maxsus shaxslar qayta o'zgartirishi mumkin bo'ladi

-:Ma'lumotni osongina qaytarish uchun hammaga ochiq bo'lgan sxema yordamida ma'lumotlarni boshqa formatga o'zgartirishdir

-:Ma'lumot boshqa formatga o'zgartiriladi, barcha shaxslar kalit yordamida qayta o'zgartirishi mumkin bo'ladi

-:Maxfiy xabarni soxta xabar ichiga berkitish orqali aloqani yashirish hisoblanadi

I:

S:Axborotni shifrnı ochish (deshifrlash) bilan qaysi fan shug'ullanadi?

+:Kriptoanaliz

-:Kartografiya

-:Kriptologiya

-:Adamar usuli

I:

S:Qaysi juftlik RSA algoritmining ochiq va yopiq kalitlarini ifodalaydi?

+:{d, n} – yopiq, {e, n} – ochiq;

-:{d, e} – ochiq, {e, n} – yopiq;

-:{e, n} – yopiq, {d, n} – ochiq;

-:{e, n} – ochiq, {d, n} – yopiq;

I:

S:Zamonaviy kriptografiya qanday bo'limlardan iborat?

-:Elektron raqamli imzo; kalitlarni boshqarish

-:Simmetrik kriptotizimlar; ochiq kalitli kriptotizimlar;

+:Simmetrik kriptotizimlar; ochiq kalitli kriptotizimlar;

Elektron raqamli imzo; kalitlarni boshqarish

-:Simmetrik kriptotizimlar; ochiq kalitli kriptotizimlar;

kalitlarni boshqarish

I:

S:Kompyuterning tashqi interfeysi deganda nima tushuniladi?

+:kompyuter bilan tashqi qurilmani bog'lovchi simlar va ular orqali axborot almashinish qoidalarini to'plamlari

-:tashqi qurilmani kompyuterga bog'lashda ishlatiladigan ulovchi simlar

-:kompyuterning tashqi portlari.

-:tashqi qurilma bilan kompyuter o'rtasida axborot almashinish qoidalarini to'plami

I:

S:Lokal tarmoqlarda keng tarqalgan topologiya turi qaysi?

+:Yulduz

-:Xalqa

-:To'liqbog'langan

-:Umumiy shina

I:

S:Ethernet kontsentratori qanday vazifani bajaradi?

+:kompyuterdan kelayotgan axborotni qolgan barcha kompyuterga yo'naltirib beradi

-:kompyuterdan kelayotgan axborotni boshqa bir

kompyuterga yo'naltirib beradi

-:kompyuterdan kelayotgan axborotni xalqa bo'ylab

joylashgan keyingi kompyuterga

-:tarmoqning ikki segmentini bir biriga ulaydi

I:

S:OSI modelida nechta sath mavjud?

+:7 ta

-:4 ta

-:5 ta

-:3 ta

I:

S:Identifikatsiya, autentifikatsiya jarayonlaridan o'tgan

foydalanuvchi uchun tizimda bajarishi mumkin bo'lgan

amallarga ruxsat berish jarayoni bu...

+:Avtorizatsiya

-:Shifrlash

-:Identifikatsiya

-:Autentifikatsiya

I:

S:Autentifikatsiya faktorlari nechta?

+:3 ta

-:4 ta

-:5 ta

-:6 ta

I:

S:Ko'z pardasi, yuz tuzilishi, ovoz tembri-bular

autentifikatsiyaning qaysi faktoriga mos belgilar?

+:Biometrik autentifikatsiya

-:Biron nimaga egalik asosida

-:Biron nimani bilish asosida

-:Parolga asoslangan

I:

S:Fizik xavfsizlikda Yong'inga qarshi tizimlar necha

turga bo'linadi?

+:2 taga

-:4 taga

-:3 taga

-:5 taga

I:

S:Avtorizatsiya tushunchasi odatda qaysi tushuncha bilan sinonim sifatida ham foydalanadi?

+:Foydalanishni boshqarish

-:Foydalanish

-:Tarmoqni loyixalash

-:Identifikatsiya

I:

S:Foydalanishni boshqarish –bu...

+:Sub'ektni Ob'ektga ishlash qobilyatini aniqlashdir.

-:Sub'ektni Sub'ektga ishlash qobilyatini aniqlashdir.

-:Ob'ektni Ob'ektga ishlash qobilyatini aniqlashdir

-:Autentifikatsiyalash jarayonidir

I:

S:Foydalanishni boshqarishda inson, dastur, jarayon va hokazolar nima vazifani bajaradi?

+:Sub'ekt

-:Ob'ekt

-:Tizim

-:Jarayon

I:

S:Foydalanishna boshqarishda ma'lumot , resurs, jarayon nima vazifani bajaradi ?

+:Ob'ekt

-:Sub'ekt

-:Tizim

-:Jarayon

I:

S:MAC usuli bilan foydalanishni boshqarishda xavfsizlik markazlashgan holatda kim tomonidan amalga oshiriladi?

+:Xavfsizlik siyosati ma'muri

-:Foydalaguvchining o'zi

-:Dastur tomonidan

-:Boshqarish amalgaga oshirilmaydi

I:

S:Agar Sub'ektning xavfsizlik darajasida Ob'ektning xavfsizlik darajasi mavjud bo'lsa, u holda uchun qanday amalga ruxsat beriladi?

+:O'qish

-:Yozish

-:O'zgartirish

-:Yashirish

I:

S:Agar Sub'ektning xavfsizlik darajasi Ob'ektning xavfsizlik darajasida bo'lsa, u holda qanday amalga ruxsat beriladi?

+:Yozish

-:O'qish

-:O'zgartirish

-:Yashirish

I:

S:Rol tushunchasiga ta'rif bering.

+:Muayyan faoliyat turi bilan bog'liq harakatlar va majburiyatlar to'plami sifatida belgilanishi mumkin

-:Foydalanishni boshqarish

-:Muayyan faoliyat turi bilan bog'liq imkoniyatlar to'plami sifatida belgilanishi mumkin

-:Vakolatlarni taqsimlash

I:

S:Foydalanishni boshqarishning qaysi usuli – Ob'ektlar va Sub'ektlarning atributlari, ular bilan mumkin bo'lgan amallar va so'rovlarga mos keladigan muhit uchun qoidalarni tahlil qilish asosida foydalanishlarni boshqaradi.

+:ABAC

-:MAC

-:DAC

-:RBAC

I:

S:Qanday tarmoq qisqa masofalarda qurilmalar o'rtasida

ma'lumot almashinish imkoniyatini taqdim etadi?

+:Shaxsiy tarmoq

-:Lokal

-:Mintaqaviy

-:CAMPUS

I:

S:Tarmoq kartasi bu...

+:Hisoblash qurilmasining ajralmas qismi bo'lib,

qurilmani tarmoqqa ulash imkoniyatini taqdim etadi.

-:Tarmoq repetiri odatda signalni tiklash yoki qaytarish  
uchun foydalaniladi.

-:Ko'plab tarmoqlarni ulash uchun yoki LAN

segmentlarini bog'lash uchun xizmat qiladi.

-:Qabul qilingan signalni barcha chiquvchi portlarga emas  
balki paketda manzili keltirilgan portga uzatadi.

I:

S:Server xotirasidagi joyni bepul yoki pulli ijagara berish  
xizmati qanday ataladi?

+:Qabul qilingan signalni barcha chiquvchi portlarga  
emas balki paketda manzili keltirilgan portga uzatadi.

-:Hisoblash qurilmasining ajralmas qismi bo'lib,  
qurilmani tarmoqqa ulash imkoniyatini taqdim etadi.

-:Signalni tiklash yoki qaytarish uchun foydalaniladi.

-:Ko'plab tarmoqlarni ulash uchun yoki LAN

segmentlarini bog'lash uchun xizmat qiladi.

S:Imzoni haqiqiylikini tekshirish qaysi kalit yordamida  
amalga oshiriladi?

+:Imzo muallifining ochiq kaliti yordamida

-:Ma'lumotni qabul qilgan foydalanuvchining ochiq kaliti  
yordamida

-:Ma'lumotni qabul qilgan foydalanuvchining maxfiy  
kaliti yordamida

-:Imzo muallifining maxfiy kaliti yordamida

I:

S:Quyidagilardan lokal tarmoqqa berilgan ta'rifni

belgilang.

+:Kompyuterlar va ularni bog'lab turgan qurilmalardan iborat bo'lib, ular odatda bitta tarmoqda bo'ladi.

-:Odatda ijaraga olingan telekommunikatsiya liniyalaridan foydalanadigan tarmoqlardagi tugunlarni bir-biriga bog'laydi.

-:Bu tarmoq shahar yoki shaharcha bo'ylab tarmoqlarning o'zaro bog'lanishini nazarda tutadi

-:Qisqa masofalarda qurilmalar o'rtasida ma'lumot almashinish imkoniyatini taqdim etadi

I:

S:Quyidagilardan mintaqaviy tarmoqqa berilgan ta'rifni belgilang.

+:Odatda ijaraga olingan telekommunikatsiya liniyalaridan foydalanadigan tarmoqlardagi tugunlarni birbiriga bog'laydi.

-:Kompyuterlar va ularni bog'lab turgan qurilmalardan iborat bo'lib, ular odatda bitta tarmoqda bo'ladi.

-:Bu tarmoq shahar yoki shaharcha bo'ylab tarmoqlarning o'zaro bog'lanishini nazarda tutadi

-:Qisqa masofalarda qurilmalar o'rtasida ma'lumot almashinish imkoniyatini taqdim etadi.

I:

S:Repetir nima?

+:Odatda signalni tiklash yoki qaytarish uchun foydalaniladi

-:Tarmoq qurilmasi bo'lib, ko'plab tarmoqlarni ulash uchun yoki LAN segmentlarini bog'lash uchun xizmat qiladi

-:Hisoblash qurilmasining ajralmas qismi bo'lib, qurilmani tarmoqqa ulash imkoniyatini taqdim etadi

-:Ko'plab tarmoqlarni ulash uchun yoki LAN segmentlarini bog'lash uchun xizmat qiladi. Qabul qilingan signalni barcha chiquvchi portlarga emas balki paketda manzili keltirilgan portga uzatadi

I:

S:Hub nima?

+:Tarmoq qurilmasi bo'lib, ko'plab tarmoqlarni ulash uchun yoki LAN segmentlarini bog'lash uchun xizmat qiladi

-:Hisoblash qurilmasining ajralmas qismi bo'lib, qurilmani tarmoqqa ulash imkoniyatini taqdim etadi, Odatda signalni tiklash yoki qaytarish uchun foydalaniladi

-:Ko'plab tarmoqlarni ulash uchun yoki LAN segmentlarini bog'lash uchun xizmat qiladi.

-:Qabul qilingan signalni barcha chiquvchi portlarga emas balki paketda manzili keltirilgan portga uzatadi

I:

S:Router nima?

+:Qabul qilingan ma'lumotlarni tarmoq sathiga tegishli manzillarga ko'ra (IP manzil) uzatadi.

-:Tarmoq qurilmasi bo'lib, ko'plab tarmoqlarni ulash uchun yoki LAN segmentlarini bog'lash uchun xizmat qiladi Hisoblash qurilmasining ajralmas qismi bo'lib, qurilmani tarmoqqa ulash imkoniyatini taqdim etadi

-:Ko'plab tarmoqlarni ulash uchun yoki LAN segmentlarini bog'lash uchun xizmat qiladi.

-:Qabul qilingan signalni barcha chiquvchi portlarga emas balki paketda manzili keltirilgan portga uzatadi

I:

S:Asosan tarmoq, tizim va tashkilot haqidagi axborot olish maqsadda amalga oshiriladigan tarmoq hujumi qaysi

+:Razvedka hujumlari

-:Kirish hujumlari

-:DOS hujumi

-:Zararli hujumlar

I:

S:Razvedka hujumiga berilgan ta'rifni aniqlang

+:Asosiy hujumlarni oson amalga oshirish uchun tashkilot va tarmoq haqidagi axborotni to'plashni maqsad qiladi;

-:Hujumchi turli texnologiyalardan foydalangan holda tarmoqqa kirishga harakat qiladi hujumchi -:Mijozlarga,



foydalanuvchilarga va tashkilotlarda mavjud bo'lgan biror

xizmatni cheklashga urinadi;

-:Zararli hujumlar tizim yoki tarmoqqa bevosita va

bilvosita ta'sir qiladi;

I:

S:Antivirus dasturlarini ko'rsating?

+:Drweb, Nod32, Kaspersky

-:arj, rar, pkzip, pkunzip

-:winrar, winzip, winarj

-:pak, lha

I:

S:Wi-Fi tarmoqlarida quyida keltirilgan qaysi shifrlash

protokollaridan foydalaniladi

+:wep, wpa, wpa2

-:web, wpa, wpa2

-:wpa, wpa2

-:wpa, wpa2, wap

I:

S:Axborot himoyalangan qanday sifatlarga ega bo'lishi

kerak?

+:ishonchli, qimmatli va to'liq

-:uzluksiz va uzlukli

-:ishonchli, qimmatli va uzlukli

-:ishonchli, qimmatli va uzluksiz

I:

S:Virtual xususiy tarmoqni qisqartmasini belgilang.

+:VPN

-:APN

-:ATM

-:Ad-hoc

I:

S:Fire Wall ning vazifasi...

+:Tarmoqlar orasida aloqa o'rnatish jarayonida tashkilot  
va Internet tarmog'i orasida xavfsizlikni ta'minlaydi

-:Kompyuterlar tizimi xavfsizligini ta'minlaydi

-:Ikkita kompyuter o'rtasida aloqa o'rnatish jarayonida

Internet tarmog'i orasida xavfsizlikni ta'minlaydi

-:Uy tarmog'i orasida aloqa o'rnatish jarayonida tashkilot  
va Internet tarmog'i orasida xavfsizlikni ta'minlaydi

I:

S:Kompyuter virusi nima?

+:maxsus yozilgan va zararli dastur

-.exe fayl

-.boshqariluvchi dastur

-.Kengaytmaga ega bo'lgan fayl

I:

S:Kompyuterning viruslar bilan zararlanish yo'llarini  
ko'rsating

+:disk, maxsus tashuvchi qurilma va kompyuter  
tarmoqlari orqali

-.faqat maxsus tashuvchi qurilma orqali

-.faqat kompyuter tarmoqlari orqali

-.zararlanish yo'llari juda ko'p

I:

S:Troyan dasturlari bu...

+:virus dasturlar

-.antivirus dasturlar

-.o'yin dasturlari

-.yangilovchi dasturlar

I:

S:Stenografiya ma'nosi qanday?

+:sirli yozuv

-.sirli xat

-.maxfiy axborot

-.maxfiy belgi

I:

S:Kriptologiya yo'nalishlari nechta?

+:2

-.3

-.4

-.5

I:

S:Kriptografiyaning asosiy maqsadi nima?

+:maxfiylik, yaxlitlikni ta'minlash

-:ishonchlilik, butunlikni ta'minlash

-:autentifikatsiya, identifikatsiya

-:ishonchlilik, butunlikni ta'minlash, autentifikatsiya, identifikatsiya

I:

S:Shifrlash kaliti noma'lum bo'lganda shifrlangan ma'lumotni deshifrlash qiyinlik darajasini nima belgilaydi?

+:Kriptobardoshlik

-:Shifr matn uzunligi

-:Shifrlash algoritmi

-:Texnika va texnologiyalar

I:

S:Barcha simmetrik shifrlash algoritmlari qanday shifrlash usullariga bo'linadi?

+:Blokli va oqimli

-:DES va oqimli

-:Feystel va Verman

-:SP– tarmoq va IP

I:

S:Diskni shifrlash nima uchun amalga oshiriladi?

+:Ma'lumotni saqlash vositalarida saqlangan ma'lumot konfidensialligini ta'minlash uchun amalga oshiriladi

-:Xabarni yashirish uchun amalga oshiriladi

-:Ma'lumotni saqlash vositalarida saqlangan ma'lumot butunligini ta'minlash uchun amalga oshiriladi

-:Ma'lumotni saqlash vositalarida saqlangan ma'lumot foydalanuvchanligini ta'minlash uchun amalga oshiriladi

I:

S:Ma'lumotlarni yo'q qilish odatda necha xil usulidan foydalaniladi?

+:4 xil

-:8 xil

-:7 xil

-:5 xil

I:

S:Kiberjinoyatchilik bu –. . .

+:Kompyuter yoki boshqa qurilmalarga qarshi qilingan yoki kompyuter va boshqa qurilmalar orqali qilingan jinoiy faoliyat.

-:Kompyuter o'yinlari

-:Faqat banklardan pul o'g'irlanishi

-:Autentifikatsiya jarayonini buzish

I:

S:Fishing nima?

+:Internetdagi firibgarlikning bir turi bo'lib, uning maqsadi foydalanuvchining maxfiy ma'lumotlaridan, login/parol, foydalanish imkoniyatiga ega bo'lishdir.

-:Ma'lumotlar bazalarini xatoligi

-:Mualliflik huquqini buzilishi

-:Lug'at orqali xujum qilish.

I:

S:Nuqson nima?

+:Dasturni amalga oshirishdagi va loyixalashdagi zaifliklarning barchasi nuqsondir

-:Dasturiy ta'minotni amalga oshirish bosqichiga tegishli bo'lgan muammo

-:Dasturlardagi ortiqcha reklamalar

-:Autentifikatsiya jarayonini buzish

I:

S:Risklarni boshqarishda risklarni aniqlash jarayoni bu-..

+:Tashkilot xavfsizligiga ta'sir qiluvchi tashqi va ichki risklarning manbasi, sababi, oqibati va haklarni aniqlash.

-:Risklarni baholash bosqichi tashkilotning risk darajasini baholaydi va risk ta'siri va ehtimolini o'lchashni ta'minlaydi.

-:Risklarni davolash bu – aniqlangan risklar uchun mos nazoratni tanlash va amalga oshirish jarayoni.

-:Risk monitoringi yangi risklarni paydo bo'lish imkoniyatini aniqlash.

I:

S:Tizim ishlamay turganda yoki foydalanuvchilar ma'lumot bilan ishlamay turganda zahiralash amalga oshirilsa .... deb ataladi.

+: "Sovuq saxiralash"

-: "Issiq zaxiralash"

-: "Iliq saxiralash"

-: "To'liq zaxiralash"

I:

S: Asimmetrik kriptotizimlarda axborotni shifrlashda va rasshifrovka qilish uchun nechta kalit ishlatiladi?

+: Ikkita kalit

-: Bitta kalit

-: Elektron raqamli imzo

-: Foydalanuvchi identifikatori

I:

S: Axborot xavfsizligiga bo'ladigan tahdidlarning qaysi biri maqsadli (atayin) tahdidlar deb hisoblanadi?

+: Strukturalarni ruxsatsiz modifikatsiyalash

-: Tabiiy ofat va avariya

-: Texnik vositalarning buzilishi va ishlamasligi

-: Foydalanuvchilar va xizmat ko'rsatuvchi hodimlarning hatoliklari}

I:

S: Axborot xavfsizligiga bo'ladigan tahdidlarning qaysi biri tasodifiy tahdidlar deb hisoblanadi?

+: Texnik vositalarning buzilishi va ishlamasligi

-: Axborotdan ruxsatsiz foydalanish

-: Zararkunanda dasturlar

-: An'anaviy josuslik va diversiya haqidagi ma'lumotlar tahlili}

I:

S: Axborotni uzatish va saqlash jarayonida o'z strukturasi va yoki mazmunini saqlash xususiyati nima deb ataladi?

+: Ma'lumotlar butunligi

-: Axborotning konfidentsialligi

-:Foydalanuvchanligi

-:Ixchamligi

I:

S:Axborotning buzilishi yoki yo'qotilishi xavfiga olib  
keluvchi himoyalanuvchi ob'ektga qarshi qilingan  
xarakatlar qanday nomlanadi?

+:Tahdid

-:Zaiflik

-:Hujum

-:Butunlik}

I:

S:Biometrik autentifikatsiyalashning avfzalliklari-bu:

+:Biometrik parametrlarning noyoblighi

-:Bir marta ishlatilishi

-:Biometrik parametrlarni o'zgartirish imkoniyati

-:Autentifikatsiyalash jarayonining soddalighi

I:

S:Foydalanish huquqlariga (mualliflikka) ega barcha  
foydalanuvchilar axborotdan foydalana olishliklari-bu:

+:Foydalanuvchanligi

-:Ma'lumotlar butunligi

-:Axborotning konfidentsialligi

-:Ixchamlighi

S:Simsiz tarmoqlarni kategoriyalarini to'g'ri ko'rsating?

+:Simsiz shaxsiy tarmoq (PAN), simsiz lokal tarmoq  
(LAN), simsiz regional tarmoq (MAN) va Simsiz global  
tarmoq (WAN)

-:Simsiz internet tarmoq (IAN )va Simsiz telefon tarmoq  
(WLAN), Simsiz shaxsiy tarmoq (PAN) va Simsiz global  
tarmoq (WIMAX)

-:Simsiz internet tarmoq (IAN) va uy simsiz tarmog'i

-:Simsiz chegaralanmagan tarmoq (LAN), simsiz kirish  
nuqtalari

I:

S:Sub'ektga ma'lum vakolat va resurslarni berish  
muolajasi-bu:

+:Avtorizatsiya

-:Haqiqiylikni tasdiqlash

-:Autentifikatsiya

-:Identifikatsiya

I:

S:Tarmoq operatsion tizimining to'g'ri konfiguratsiyasini  
madadlash masalasini odatda kim hal etadi?

+:Tizim ma'muri

-:Tizim foydalanuvchisi

-:Korxona raxbari

-:Operator

I:

S:Tarmoqlararo ekran texnologiyasi-bu:

+:Ichki va tashqi tarmoq o'rtasida filtr va himoya  
vazifasini bajaradi

-:Ichki va tashqi tarmoq o'rtasida axborotni o'zgartirish  
vazifasini bajaradi

-:Qonuniy foydalanuvchilarni himoyalash

-:Ishonchsiz tarmoqdan kirishni boshqarish}

I:

S:Xizmat qilishdan voz kechishga undaydigan  
taqsimlangan hujum turini ko'rsating?

+:DDoS (Distributed Denial of Service) hujum

-:Tarmoq hujumlari

-:Dastur hujumlari asosidagi (Denial of Service) hujum

-:Virus hujumlari}

I:

S:Uyishtirilmagan tahdid, ya'ni tizim yoki dasturdagi  
qurilmaning jismoniy xatoligi – bu...

+:Tasodifiy tahdid

-:Uyishtirilgan tahdid

-:Faol tahdid

-:Passiv tahdid

I:

S:Axborot xavfsizligi qanday asosiy xarakteristikalariga  
ega?

+:Butunlik, konfidentsiallik, foydalana olishlik

-:Butunlik, himoya, ishonchlilikni urganib chiqishlilik

-:Konfidentsiallik, foydalana olishlik

-:Himoyalanganlik, ishonchlilik, butunlik

I:

S:Virtuallashtirishga qaratilgan dasturiy vositalarni

belgilang.

+:VMware, VirtualBox

-:HandyBakcup

-:Eset32

-:Cryptool

I:

S:Cloud Computing texnologiyasi nechta katta turga

ajratiladi?

+:3 turga

-:2 turga

-:4 turga

-:5 turga

I:

S:O'rnatilgan tizimlar-bu...

+:Bu ko'pincha real vaqt hisoblash cheklovlariga ega

bo'lgan kattaroq mexanik yoki elektr tizimidagi maxsus

funksiyaga ega, boshqaruvchidir

-:Korxona ichki tarmog'iga ulangan korporativ

tarmog'idan bo'ladigan hujumlardan himoyalash

-:Korxona ichki tarmog'ini Internet global tarmog'idan

ajratib qo'yish

-:Bu ko'pincha global tizimda hisoblash cheklovlariga ega

bo'lgan mexanik yoki elektr tizimidagi maxsus funksiyaga

ega qurilmadir

I:

S:Axborotdan oqilona foydalanish kodeksi qaysi tashkilot

toimonidan ishlab chiqilgan?

+:AQSH sog'liqni saqlash va insonlarga xizmat ko'rsatish

vazirligi

-:AQSH Mudofaa vazirligi



-:O'zbekiston Axborot texnologiyalari va

kommunikatsiyalarni rivojlantirish vazirligi

-:Rossiya kiberjinoyatlarga qarshu kurashish davlat  
qo'mitasi

I:

S:Xizmat qilishdan voz kechishga undaydigan

taqsimlangan hujum turini ko'rsating?

+:Tarmoq hujumlari

-:Dastur hujumlari asosidagi (Denial of Service) hujum

-:Virus hujumlari

-:Passiv hujum

I:

S:Token, Smartkartalarda xavfsizlik tomonidan

kamchiligi nimada

+:Qurilmani yo'qotilishi katta xavf olib kelishi mumkin

-:Foydalanish davrida maxfiylik kamayib boradi

-:Qurilmalarni ishlab chiqarish murakkab jarayon

-:Qurilmani qalbakilashtirish oson

I:

S:Tarmoqlararo ekranlarning asosiy turlarini ko'rsating?

+:Tatbiqiy sath shlyuzi, seans sathi shlyuzi, ekranlovchi  
marshrutizator

-:Tatbiqiy sath shlyuzi, seans sathi shlyuzi, fizik sath  
shlyuzi

-:Tatbiqiy sath shlyuzi, fizik sath shlyuzi, ekranlovchi  
marshrutizator

-:Fizik sath shlyuzi, ekranlovchi marshrutizator,  
tahlillovchi marshrutizator

I:

S:Spam bilan kurashishning dasturiy uslubida nimalar  
ko'zda tutiladi?

+:Elektron pochta qutisiga kelib tushadigan ma'lumotlar  
dasturlar asosida filtrlanib cheklanadi

-:Elektron pochta qutisiga kelib tushadigan spamlar  
me'yoriy xujjatlar asosida cheklanadi va bloklanadi

-:Elektron pochta qutisiga kelib tushadigan spamlar

ommaviy ravishda cheklanadi

-:Elektron pochta qutisiga kelib spamlar mintaqaviy hududlarda cheklanadi

I:

S:Ma'lumotlarni yo'qolish sabab bo'luvchi tabiiy tahdidlarni ko'rsating

+:Zilzila, yong'in, suv toshqini va hak.

-:Quvvat o'chishi, dasturiy ta'minot to'satdan o'zgarishi yoki qurilmani to'satdan zararlanishi

-:Tashkilotdagi muhim ma'lumotlarni modifikatsiyalanishi yoki o'g'irlanishi

-:Qasddan yoki tasodifiy ma'lumotni o'chirib yuborilishi, ma'lumotlarni saqlash vositasini to'g'ri joylashtirilmagani

I:

S:Ma'lumotlarni tasodifiy sabablar tufayli yo'qolish sababini belgilang

+:Quvvat o'chishi, dasturiy ta'minot to'satdan o'zgarishi yoki qurilmani to'satdan zararlanishi

-:Tashkilotdagi muhim ma'lumotlarni modifikatsiyalanishi yoki o'g'irlanishi

-:Ma'lumotlarni saqlash vositasini to'g'ri joylashtirilmagani yoki ma'lumotlar bazasini xatolik bilan boshqarilganligi.

-:Zilzila, yong'in, suv toshqini va hak

I:

S:Ma'lumotlarni inson xatosi tufayli yo'qolish sababini belgilang.

+:Ma'lumotlarni saqlash vositasini to'g'ri joylashtirilmagani yoki ma'lumotlar bazasini xatolik bilan boshqarilganligi.

-:Tashkilotdagi muhim ma'lumotlarni modifikatsiyalanishi yoki o'g'irlanishi

-:Quvvat o'chishi, dasturiy ta'minot to'satdan o'zgarishi yoki qurilmani to'satdan zararlanishi

-:Zilzila, yong'in, suv toshqini va hak

I:

S:Ma'lumotlarni g'arazli hatti harakatlar yo'qolish

sababini ko'rsating.

+:Tashkilotdagi muhim ma'lumotlarni

modifikatsiyalanishi yoki o'g'irlanishi

-:Quvvat o'chishi, dasturiy ta'minot to'satdan o'zgarishi

yoki qurilmani to'satdan zararlanishi

-:Ma'lumotlarni saqlash vositasini to'g'ri

joylashtirilmagani yoki ma'lumotlar bazasini xatolik bilan

boshqarilganligi.

-:Zilzila, yong'in, suv toshqini va hak

I:

S:Internet orqali masofada joylashgan kompyuterga yoki

tarmoq resurslariga DoS hujumlari uyushtirilishi

natijasida..

+:Foydalanuvchilar kerakli axborot resurlariga murojaat

qilish imkoniyatidan mahrum qilinadilar

-:Foydalanuvchilarning maxfiy axborotlari kuzatilib,

masofadan buzg'unchilarga etkaziladi

-:Axborot tizimidagi ma'lumotlar bazalari o'g'irlanib

ko'lga kiritilgach, ular yo'q qilinadilar

-:Foydalanuvchilar axborotlariga ruxsatsiz o'zgartirishlar

kiritilib, ularning yaxlitligi buziladi

I:

S:"Parol", "PIN" kodlarni xavfsizlik tomonidan

kamchiligi nimadan iborat?

+:Foydalanish davrida maxfiylik kamayib boradi

-:Parolni esda saqlash kerak bo'ladi

-:Parolni almashtirish jarayoni murakkabligi

-:Parol uzunligi soni cheklangan

I:

S:Yaxlitlikni buzilishi bu - ...

+:Soxtalashtirish va o'zgartirish

-:Ishonchsizlik va soxtalashtirish

-:Soxtalashtirish

-:Butunmaslik va yaxlitlanmaganlik

I:

S:Tarmoqda joylashgan fayllar va boshqa resurslardan foydalanishni taqdim etuvchi tarmoqdagi kompyuter nima?

+:Server

-:Bulutli tizim

-:Superkompyuter

-:Tarmoq

I:

S:Tahdid nima?

+:Tizim yoki tashkilotga zarar yetkazishi mumkin bo'lgan istalmagan hodisa.

-:Tashkilot uchun qadrli bo'lgan ixtiyoriy narsa

-:Bu riskni o'zgartiradigan harakatlar bo'lib

-:Bu noaniqlikning maqsadlarga ta'siri

S:Fizik to'siqlarni o'rnatish , Xavfsizlik qo'riqchilarini ishga olish, Fizik qulflar qo'yishni amalga oshirish qanday nazorat turiga kiradi?

+:Fizik nazorat

-:Texnik nazorat

-:Ma'muriy nazorat

-:Tashkiliy nazorat

I:

S:Ruxsatlarni nazoratlash, "Qopqon", Yong'inga qarshi tizimlar, Yoritish tizimlari, Ogohlantirish tizimlari , Quvvat manbalari, Video kuzatuv tizimlari, Qurollarni aniqlash, Muhitni nazoratlash amalga oshirish qanday nazorat turiga kiradi?

-:Fizik nazorat

+:Texnik nazorat

-:Ma'muriy nazorat

-:Tashkiliy nazorat

I:

S:Qoida va muolajalarni yaratish, Joylashuv arxitekturasini loyihalash, Xavfsizlik belgilari va ogohlantirish signallari, Ishchi joy xavfsizligini ta'minlash, Shaxs xavfsizligini ta'minlash amalga oshirish

qanday nazorat turiga kiradi?

-:Fizik nazorat

-:Texnik nazorat

+:Ma'muriy nazorat

-:Tashkiliy nazorat

I:

S:Ikkilik sanoq tizimida qanday raqamlardan

foydalanamiz?

+:Faqat 0 va 1

-:Faqat 1

-:Faqat 0

-:Barcha raqamlardan

I:

S:Yuliy Sezar ma'lumotlarni shifrlashda alfavit xarflarni

nechtaga surib shifrlagan?

+:3 taga

-:4 taga

-:2 taga

-:5 taga

I:

S:WiMAX qanday simsiz tarmoq turiga kiradi?

+:Regional

-:Lokal

-:Global

-:Shaxsiy

I:

S:Wi-Fi necha Gs chastotali to'liqida ishlaydi?

+:2.4-5 Gs

-:2.4-2.485 Gs

-:1.5-11 Gs

-:2.3-13.6 Gs

I:

S:Quyidagi parollarning qaysi biri "bardoshli parol" ga kiradi?

+:Onx458&hdsh)

-:12456578

-:salomDunyo

-:Mashina777

I:

S:Parollash siyosatiga ko'ra parol tanlash shartlari

qanday?

+:Kamida 8 belgi; katta va kichik xavflar, sonlar , kamida

bitta maxsus simvol qo'llanishi kerak. -:Kamida 8 belgi;

katta va kichik xavflar, sonlar qo'llanishi kerak.

-:Kamida 6 belgi; katta xarflar, sonlar , kamida bitta

maxsus simvol qo'llanishi kerak.

-:Kamida 6 belgi; katta va kichik xarflar, kamida bitta

maxsus simvol qo'llanishi kerak.

I:

S:MD5, SHA1, SHA256, O'z DSt 1106:2009- qanday

algoritmlar deb ataladi?

+:Xeshlash

-:Kodlash

-:Shifrlash

-:Stenografiya

I:

S:LTE Advances standarti global simsiz tarmoqning

nechanshi avlodiga mansub?

+:4G

-:3G

-:2G

-:1G

I:

S:Bluetooth necha Gs chastotali to'lqinda ishlaydi?

+:2.4-2.485 Gs

-:2.4-5 Gs

-:1.5-11 Gs

-:2.3-13.6 Gs

I:

S:Axborot o'lchovini o'sish tartibini to'g'ri tanlang

+:Bit,bayt,kilobayt,megabayt

-:Bit,bayt,megabayt,kilobayt

-:Gigabayt,megabayt,pikobayt

-:Gigabayt,pikobayat,terobayt

I:

S:Axborot o'lchovini kamayish tartibini to'g'ri tanlang

+:Gigabayt,megabayt,kilobayt

-:Bit,bayt,kilobayt,megabayt

-:Gigabayt,megabayt,pikobayt

-:Gigabayt,pikobayat,terobayt

I:

S:"Parol", "PIN" kodlarni xavfsizlik tomonidan

kamchiligi nimadan iborat?

+:Foydalanish davrida maxfiylik kamayib boradi

-:Parolni esda saqlash kerak bo'ladi

-:Parolni almashtirish jarayoni murakkabligi

-:Parol uzunligi soni cheklangan

I:

S:Axborot xavfsizligin ta'minlashda qo'llaniladigan

me'yoriy hujjatlarning birinchi darajadagi hujjati-bu..

+:Qonun

-:Qaror

-:Standart

-:Farmon

I:

S: Elektron raqamli imzo kalitlari ro'yxatga olish qaysi

tashkilot tomonidan bajariladi?

+:Sertifikatlari ro'yxatga olish markazlari

-:Tegishli Vazirliklar

-:Davlat Hokimiyati

-:Axborot xavfsizligi markazlari

I:

S: Elektron raqamli imzo to'g'risidagi Qonun qachon

qabul qilingan?

+:2003 yil 11 dekabr

-:2005 yil 2 mart

-:2010 yil 1 sentyabr

-:2015 yil 5 yanvar

I:

S:Global simsiz tarmoqda qaysi standartlar ishlaydi?

+:CDPD, 4G

-:Wi-Fi, 3G

-:WIMAX, 2G

-:Wi-Fi, IRDA

I:

S:Kompyuter IPv4 manzilni to'g'ri kiritilishini ko'rsating.

+:192.168.100.001

-:12:AC:14:1C:3B:13

-:1254-1255-3645

-:01001:00011:0111

I:

S:Kompyuter yoki boshqa qurilmalarga qarshi qilingan  
yoki kompyuter va boshqa qurilmalar orqali qilingan  
jinoyat-...

+:Kiberjinoyat

-:Kibersport

-:Kiberterror

-:Hakerlar uyushmasi

I:

S:Masofadan ERI olish uchun qaysi internet manzilga  
murojaat qilinadi?

+:e-imzo.uz

-:elektron-imzo.uz

-:imzo.uz

-:eri.uz

I:

S:Konfidentsial axborotdan foydalanish tushunchasi...

+:Muayyan shaxsga tarkibida konfidensial xarakterli  
ma'lumot bo'lgan axborot bilan tanishishga vakolatli  
mansabdor shaxsning ruxsati.

-:Korxona o'z faoliyatini buzilishsiz va to'xtalishsiz  
yurgiza oladigan vaqt bo'yicha barqaror bashoratlanuvchi  
atrof-muhit holati.

-:Ma'lumotlarning ma'lumotlar bazasiga tegishli



darajasini aniqlash va belgilash.

-:Olingan ma'lumotlar jo'natuvchisining so'ralganiga mosligini tasdiqlash.

Yuliy Sezar ma'lumotlarni shifrlashda alfavit xarflarni nechtaga surib shifrlagan? ====

4 taga=====

2 taga=====

5 taga=====

#3 taga

+++++

WiMAX qanday simsiz tarmoq turiga kiradi? ====

Lokal =====

Global=====

Shaxsiy =====

#Regional

+++++

Wi-Fi necha Gs chastotali to'lqinda ishlaydi? ====

#2.4-5 Gs=====

2.4-2.485 Gs=====

1.5-11 Gs=====

2.3-13.6 Gs

+++++

Quyidagi parollarning qaysi biri "bardoshli parol"ga kiradi? ====

#Onx458&hdsh) =====

12456578=====

salomDunyo=====

Mashina777

+++++

Ma'lumotlarni tasodifiy sabablar tufayli yo'qolish sababini belgilang=====

#Quvvat o'chishi, dasturiy ta'minot to'satdan o'zgarishi yoki qurilmani to'satdan zararlanishi=====

Tashkilotdagi muhim ma'lumotlarni modifikatsiyalanishi yoki o'g'irlanishi=====

Ma'lumotlarni saqlash vositasini to'g'ri

joylashtirilmagani yoki ma'lumotlar bazasini xatolik bilan

boshqarilganligi. ====

Zilzila, yong'in, suv toshqini va hak.

+++++

Sub'ektga ma'lum vakolat va resurslarni berish

muolajasi-bu: ====

#Avtorizatsiya=====

Haqiqiylikni tasdiqlash=====

Autentifikatsiya=====

Identifikatsiya

+++++

Token, Smartkartalarda xavfsizlik tomonidan kamchiligi

nimada? =====

Foydalanish davrida maxfiylik kamayib boradi=====

Qurilmalarni ishlab chiqarish murakkab jarayon=====

#Qurilmani yo'qotilishi katta xavf olib kelishi

mumkin=====

Qurilmani qalbakilashtirish oson

+++++

Ma'lumotlarni yo'qolish sabab bo'luvchi tabiiy

tahdidlarni ko'rsating=====

Quvvat o'chishi, dasturiy ta'minot to'satdan o'zgarishi

yoki qurilmani to'satdan zararlanishi=====

#Zilzila, yong'in, suv toshqini va hak. =====

Tashkilotdagi muhim ma'lumotlarni modifikatsiyalanishi

yoki o'g'irlanishi=====

Qasddan yoki tasodifiy ma'lumotni o'chirib yuborilishi,

ma'lumotlarni saqlash vositasini to'g'ri joylashtirilmagani

+++++

Foydalanish huquqini cheklovchi matritsa modeli bu...

=====

#Bella La-Padulla modeli=====

Dening modeli=====

Landver modeli=====

Huquqlarni cheklovchi model

+++++

Parollash siyosatiga ko'ra parol tanlash shartlari qanday?

=====

Kamida 8 belgi; katta va kichik xavflar, sonlar qo'llanishi  
kerak. =====

#Kamida 8 belgi; katta va kichik xavflar, sonlar , kamida  
bitta maxsus simvol qo'llanishi kerak. =====

Kamida 6 belgi; katta xarflar, sonlar , kamida bitta  
maxsus simvol qo'llanishi kerak. =====

Kamida 6 belgi; katta va kichik xarflar, kamida bitta  
maxsus simvol qo'llanishi kerak.

+++++

MD5, SHA1, SHA256, O'z DSt 1106:2009- qanday  
algoritmlar deb ataladi? =====

Kodlash=====

#Xeshlash=====

Shifrlash=====

Stenografiya

+++++

Global simsiz tarmoqda qaysi standartlar ishlaydi? =====

Wi-Fi, 3G=====

WIMAX, 2G=====

Wi-Fi, IRDA=====

#CDPD, 4G

+++++

RSA algoritmi qaysi yilda ishlab chiqilgan? =====

#1977 yil=====

1966 yil=====

1988 yil=====

1956 yil

+++++

Qaysi texnologiyada ma'lumotni bir vaqtda bir necha  
disklarga navbatlab yoziladi? =====

RAID 1=====

#RAID 0=====

RAID 5=====

RAID 3

+++++

Windows OT lokal xavfsizlik siyosatini sozlash oynasiga

o'tish uchun buyruqlar satrida qaysi buyruq yoziladi?

====

#secpol.msc=====

regedit=====

chkdsk=====

diskcopy

+++++

Zimmermann telegrami, Enigma shifri, SIGABA

kriptografiyaning qaysi davriga to'g'ri keladi? =====

O'rta asr davrida=====

15 asr davrida=====

#1-2 jahon urushu davri=====

21 asr davrida

+++++

Bell-LaPadula (BLP) modeli -bu.. =====

Axborlarni nazoratlovchi model=====

#Bu hukumat va harbiy dasturlarda kirishni boshqarishni

kuchaytirish uchun ishlatiladigan avtomatlashgan

modeli=====

Foydalanuvchilarni ro'yxatga olish , nazoratlash va tahlil

qiluvchi model=====

Tarmoq boshqarish va tahlil qiluvchi model

+++++

Internetning dastlabki nomini to'g'ri belgilang. =====

#ARPANET=====

INTRANET=====

INTERNET=====

NETWORK

+++++

Axborot xavfsizligining asosiy maqsadlaridan biribu...=====

Ob'ektga bevosita ta'sir qilish=====

#Axborotlarni o'g'irlanishini, yo'qolishini,

soxtalashtirilishini oldini olish=====

Axborotlarni shifrlash, saqlash, yetkazib berish=====

Tarmoqdagi foydalanuvchilarni xavfsizligini ta'minlab

berish

+++++

Konfidentsiallikga to'g'ri ta'rif keltiring.=====

#axborot inshonchliligi, tarqatilishi mumkin emasligi,

maxfiyligi kafolati; =====

axborot konfidentsialligi, tarqatilishi mumkinligi,

maxfiyligi kafolati; =====

axborot inshonchliligi, tarqatilishi mumkin emasligi,

parollanganligi kafolati; =====

axborot inshonchliligi, axborotlashganligi, maxfiyligi

kafolati;

+++++

Yaxlitlikni buzilishi bu - ...=====

#Soxtalashtirish va o'zgartirish=====

Ishonchsizlik va soxtalashtirish=====

Soxtalashtirish=====

Butunmaslik va yaxlitlanmaganlik

+++++

Kriptografiyaning asosiy maqsadi nima? =====

ishonchlilik, butunlilikni ta'minlash=====

autentifikatsiya, identifikatsiya=====

#maxfiylik, yaxlitlikni ta'minlash=====

ma'lumotlarni shaklini o'zgartirish

+++++

Kriptografiyada kalitning vazifasi nima? =====

Bir qancha kalitlar yig'indisi=====

#Matnni shifrlash va shifrini ochish uchun kerakli

axborot=====

Axborotli kalitlar to'plami=====

Belgini va raqamlarni shifrlash va shifrini ochish uchun

kerakli axborot

+++++

Qo'yish, o'rin almashtirish, gammalash kriptografiyaning

qaysi turiga bog'liq? =====

assimetrik kriptotizimlar=====

ochiq kalitli kriptotizimlar=====

#simmetrik kriptotizimlar=====

autentifikatsiyalash

+++++

Autentifikatsiya nima? =====

Tizim me'yoriy va g'ayritabiiy hollarda

rejalashtirilgandek o'zini tutishligi holati=====

#Ma'lum qilingan foydalanuvchi, jarayon yoki

qurilmaning haqiqiy ekanligini tekshirish muolajasi=====

Istalgan vaqtda dastur majmuasining mumkinligini

kafolati=====

Tizim noodatiy va tabiiy hollarda qurilmaning haqiqiy

ekanligini tekshirish muolajasi

+++++

Identifikatsiya bu- ...=====

#Foydalanuvchini uning identifikatori (nomi) bo'yicha

aniqlash jarayoni=====

Ishonchliligini tarqalishi mumkin emasligi kafolati=====

Axborot boshlang'ich ko'rinishda ekanligi uni saqlash,

uzatishda ruxsat etilmagan o'zgarishlar=====

Axborotni butunligini saqlab qolgan holda uni

elementlarini o'zgartirishga yo'l qo'ymaslik

+++++

Kriptologiya –qanday fan? =====

axborotni qayta akslantirishning matematik usullarini

izlaydi va tadqiq qiladi=====

kalitni bilmasdan shifrlangan matnni ochish

imkoniyatlarini o'rganadi=====

kalitlarni bilmasdan shifrni ochishga bardoshlilikni

aniqlovchi shifrlash tavsifi=====

#axborotni qayta akslantirib himoyalash muammosi bilan

shug'ullanadi

+++++

Kriptobardoshlilik deb nimaga aytiladi? =====

#kalitlarni bilmasdan shifrni ochishga bardoshlilikni

aniqlovchi shifrlash tavsifi=====

axborotni qayta akslantirib himoyalash muammosi bilan

shug'ullanadi=====

kalitni bilmasdan shifrlangan matnni ochish

imkoniyatlarini o'rganadi=====

axborotni qayta akslantirishning matematik usullarini

izlaydi va tadqiq qiladi

+++++

Kriptografiya matn –bu.. =====

matnni shifrlash va shifrini ochish uchun kerakli

axborot=====

axborot belgilarini kodlash uchun foydalaniladigan chekli

to'plam=====

#alifbo elementlarining tartiblangan to'plami=====

kalit axborotni shifrlovchi kalitlar

+++++

Kriptotizimga qo'yiladigan umumiy talablardan biri

nima? =====

shifrlash algoritmining tarkibiy elementlarini o'zgartirish

imkoniyati bo'lishi lozim=====

ketma-ket qo'llaniladigan kalitlar o'rtasida oddiy va oson

bog'liqlik bo'lishi kerak=====

#shifr matn uzunligi ochiq matn uzunligiga teng bo'lishi

kerak=====

maxfiylik o'ta yuqori darajada bo'lmoqligi lozim

+++++

Axborot qanday sifatlarga ega bo'lishi kerak? =====

uzluksiz va uzlukli=====

ishonchli, qimmatli va uzlukli=====

#ishonchli, qimmatli va to'liq=====

ishonchli, qimmatli va uzluksiz

+++++

Tekstni boshqa tekst ichida ma'nosini yashirib keltirish

nima deb ataladi?=====

sirli yozuv=====

#steganografiya=====

skrembler=====

shifr mashinalar

+++++

Berilgan ta'riflardan qaysi biri asimmetrik tizimlarga xos?

=====

Asimmetrik tizimlarda  $k_1=k_2$  bo'ladi, ya'ni  $k$  – kalit bilan

axborot ham shifrlanadi, ham deshifrlanadi=====

#Asimmetrik kriptotizimlarda  $k_1 \neq k_2$  bo'lib,  $k_1$  ochiq

kalit,  $k_2$  yopiq kalit deb yuritiladi,  $k_1$  bilan axborot

shifrlanadi,  $k_2$  bilan esa deshifrlanadi=====

Asimmetrik kriptotizimlarda yopiq kalit axborot

almashinuvining barcha ishtirokchilariga ma'lum bo'ladi,

ochiq kalitni esa faqat qabul qiluvchi biladi=====

Asimmetrik kriptotizimlarda  $k_1 \neq k_2$  bo'lib, kalitlar

hammaga oshkor etiladi

+++++

Shaxsning, axborot kommunikatsiya tizimidan

foydalanish huquqiga ega bo'lish uchun

foydalaniluvchining maxfiy bo'lmagan qayd yozuvi –

bu...=====

parol=====

#login=====

identifikatsiya=====

token

+++++

Uning egasi haqiqiylikni aniqlash jarayonida tekshiruv

axboroti sifatida ishlatiladigan belgilar ketma-ketligi

(maxfiy so'z) – nima? =====

login=====

#parol=====

identifikatsiya=====

maxfiy maydon

+++++

Kodlash nima? =====

Ma'lumot boshqa formatga o'zgartiriladi, biroq uni faqat

maxsus shaxslar qayta o'zgartirishi

mumkin bo'ladi=====



Ma'lumot boshqa formatga o'zgartiriladi, barcha shaxslar  
kalit yordamida qayta o'zgartirishi  
mumkin bo'ladi====

Maxfiy xabarni soxta xabar ichiga berkitish orqali aloqani  
yashirish hisoblanadi====

#Ma'lumotni osongina qaytarish uchun hammaga ochiq  
bo'lgan sxema yordamida ma'lumotlarni boshqa formatga  
o'zgartirishdir

+++++

Ro'yxatdan o'tish-bu...====

#foydalanuvchilarni ro'yxatga olish va ularga dasturlar va  
ma'lumotlarni ishlatishga huquq berish jarayoni====  
axborot tizimlari ob'yekt va subhektlariga uni tanish  
uchun nomlar (identifikator) berish va berilgan nom  
bo'yicha solishtirib uni aniqlash jarayoni====

ob'ekt yoki subhektni unga berilgan identifikatorga  
mosligini tekshirish va belgilar ketma-ketligidan iborat  
maxfiy kodini tekshirish orqali aslligini aniqlash====  
foydalanuvchining resursdan foydalanish huquqlari va  
ruxsatlarini tekshirish jarayoni

+++++

Shifrtexstni ochiq tekstga akslantirish jarayoni nima deb  
ataladi? ====

Xabar=====

Shifrlangan xabar=====

Shifrlash=====

#Deshifrlash

+++++

.....—hisoblashga asoslangan bilim sohasi bo'lib,  
buzg'unchilar mavjud bo'lgan sharoitda amallarni  
kafolatlash uchun o'zida texnologiya, inson, axborot va  
jarayonni mujassamlashtirgan. =====

Axborot xavfsizligi=====

Kiberjtnoyatchilik=====

#Kiberxavfsizlik=====

Risklar

+++++

Risk nima? =====

Potensial kuchlanish yoki zarar=====

Tasodifiy tahdid=====

#Potensial foyda yoki zarar=====

Katta yo'qotish

+++++

Tahdid nima?

Tashkilot uchun qadrli bo'lgan ixtiyoriy narsa=====

Bu riskni o'zgartiradigan harakatlar=====

#Tashkilotga zarar yetkazishi mumkin bo'lgan istalmagan  
hodisa=====

Bu noaniqlikning maqsadlarga ta'siri

+++++

Axborotni shifrnı ochish (deshifrlash) bilan qaysi fan  
shug'ullanadi? =====

Kartografiya=====

#Kriptoanaliz=====

Kriptologiya=====

Adamar usuli

+++++

Qaysi juftlik RSA algoritmining ochiq va yopiq kalitlarini  
ifodalaydi? =====

$\{d, e\}$  – ochiq,  $\{e, n\}$  – yopiq; =====

$\#\{d, n\}$  – yopiq,  $\{e, n\}$  – ochiq; =====

$\{e, n\}$  – yopiq,  $\{d, n\}$  – ochiq; =====

$\{e, n\}$  – ochiq,  $\{d, n\}$  – yopiq;

+++++

Zamonaviy kriptografiya qanday bo'limlardan iborat?  
=====

Elektron raqamli imzo; kalitlarnı boshqarish;=====

Simmetrik kriptotizimlar; ochiq kalitli kriptotizimlar;

=====

#Simmetrik kriptotizimlar; ochiq kalitli kriptotizimlar;

Elektron raqamli imzo; kalitlarnı boshqarish =====

Simmetrik kriptotizimlar; ochiq kalitli kriptotizimlar;

kalitlarni boshqarish

+++++

Shifr nima?====

#Shifrlash va deshifrlashda foydalaniladigan matematik

funktsiyadan iborat bo'lgan kriptografik algoritim ====

Kalitlarni taqsimlash usuli=====

Kalitlarni boshqarish usuli =====

Kalitlarni generatsiya qilish usuli

+++++

Ko'z pardasi, yuz tuzilishi, ovoz tembri, -bular

autentifikatsiyaning qaysi faktoriga mos belgilar? =====

#Biometrik autentifikatsiya=====

Biron nimaga egalik asosida=====

Biron nimani bilish asosida=====

Parolga asoslangan

+++++

Ochiq kalitli kriptotizimlarning mohiyati nimadan iborat?

=====

Ochiq kalitli kriptotizimlarda shifrlash va deshifrlashda 1

ta –kalitdan foydalaniladi=====

#Ochiq kalitli kriptotizimlarda bir-biri bilan matematik

bog'langan 2 ta – ochiq va yopiq kalitlardan

foydalaniladi=====

Ochiq kalitli kriptotizimlarda ma'lumotlarni faqat

shifrlash mumkin=====

Ochiq kalitli kriptotizimlarda ma'lumotlarni faqat

deshifrlash mumkin

+++++

Assimmetrik kriptotizimlar qanday maqsadlarda

ishlatiladi? =====

#Shifrlash, deshifrlash, ERI yaratish va tekshirish, kalitlar

almashish uchun=====

ERI yaratish va tekshirish, kalitlar almashish uchun=====

Shifrlash, deshifrlash, kalitlar almashish uchun=====

Heshlash uchun

+++++

Ma'lumotlar butunligi qanday algritmlar orqali amalga

oshiriladi? =====

Simmetrik algritmlar=====

Assimmetrik algritmlar=====

#Xesh funksiyalar=====

Kodlash

+++++

To'rtta bir-biri bilan bog'langan bog'lamlar strukturasi

(kvadrat shaklida) qaysi topologiya turiga mansub? =====

Yulduz=====

To'liq bog'lanishli=====

#Xalqa=====

Yacheykali

+++++

Lokal tarmoqlarda keng tarqalgan topologiya turi qaysi?

=====

Xalqa=====

To'liqbog'langan=====

Umumiy shina=====

#Yulduz

+++++

Ethernet kontsentratori qanday vazifani bajaradi?=====

#kompyuterdan kelayotgan axborotni qolgan barcha

kompyuterga yo'naltirib beradi=====

kompyuterdan kelayotgan axborotni boshqa bir

kompyuterga yo'naltirib beradi=====

kompyuterdan kelayotgan axborotni xalqa bo'ylab

joylashgan keyingi kompyuterga=====

tarmoqning ikki segmentini bir biriga ulaydi

+++++

OSI modelida nechta sath mavjud? =====

4 ta=====

5 ta=====

#7 ta=====

3 ta

+++++

Identifikatsiya, autentifikatsiya jarayonlaridan o'tgan  
foydalanuvchi uchun tizimda bajarishi mumkin bo'lgan  
amallarga ruxsat berish jarayoni bu... =====

Shifrlash=====

Identifikatsiya=====

Autentifikatsiya=====

#Avtorizatsiya

+++++

Ma'lumotlarni inson xatosi tufayli yo'qolish sababini  
belgilang. =====

Tashkilotdagi muhim ma'lumotlarni modifikatsiyalanishi  
yoki o'g'irlanishi. =====

#Ma'lumotlarni saqlash vositasini to'g'ri  
joylashtirilmagani yoki ma'lumotlar bazasini xatolik bilan  
boshqarilganligi. =====

Quvvat o'chishi, dasturiy ta'minot to'satdan o'zgarishi  
yoki qurilmani to'satdan zararlanishi=====

Zilzila, yong'in, suv toshqini va hak.

+++++

"Parol", "PIN" kodlarni xavfsizlik tomonidan kamchiligi  
nimadan iborat? =====

Parolni esda saqlash kerak bo'ladi. =====

Parolni almashtirish jarayoni murakkabligi=====

Parol uzunligi soni cheklangan=====

#Foydalanish davrida maxfiylik kamayib boradi

+++++

Qaysi tarmoq kabelining axborot uzatish tezligi yuqori  
hisoblanadi? =====

#Optik tolali=====

O'rama juft=====

Koaksial =====

Telefon kabeli

+++++

Nima uchun autentifikatsiyalashda parol ko'p  
qo'llaniladi? =====

#Sarf xarajati kam, almashtirish oson=====

Parolni foydalanubchi ishlab chiqadi=====

Parolni o'g'rishlash qiyin=====

Serverda parollar saqlanmaydi

+++++

Elektron xujjatlarni yo'q qilish usullari qaysilar? =====

Yoqish, ko'mish, yanchish=====

#Shredirlash, magnitsizlantirish, yanchish=====

Shredirlash, yoqish, ko'mish=====

Kimyoviy usul, yoqish.

+++++

Ruxsatlarni nazoratlash, "Qopqon", Yong'inga qarshi  
tizimlar, Yoritish tizimlari, Ogohlantirish tizimlari ,  
Quvvat manbalari, Video kuzatuv tizimlari, Qurollarni  
aniqlash, Muhitni nazoratlash amalga oshirish qanday  
nazorat turiga kiradi? =====

Fizik nazorat=====

#Texnik nazorat=====

Ma'muriy nazorat=====

Tashkiliy nazorat

+++++

Avtorizatsiya tushunchasi odatda qaysi tushuncha bilan  
sinonim sifatida ham foydalanadi? =====

Foydalanish=====

Tarmoqni loyixalash=====

Identifikatsiya=====

#Foydalanishni boshqarish

+++++

Foydalanishni boshqarish –bu... =====

Sub'ektni Sub'ektga ishlash qobiliyatini aniqlashdir. =====

#Sub'ektni Ob'ektga ishlash qobiliyatini aniqlashdir.

=====

Ob'ektni Ob'ektga ishlash qobiliyatini aniqlashdir=====

Autentifikatsiyalash jarayonidir

+++++

Foydalanishni boshqarishda inson, dastur, jarayon va  
hokazolar nima vazifani bajaradi? =====

#Sub'ekt=====

Ob'ekt=====

Tizim=====

Jarayon

+++++

Foydalanishna boshqarishda ma'lumot , resurs, jarayon

nima vazifani bajaradi ? =====

#Ob'ekt=====

Sub'ekt=====

Tizim=====

Jarayon

+++++

MAC usuli bilan foydalanishni boshqarishda xavfsizlik

markazlashgan holatda kim tomonidan amalga oshiriladi?

=====

Foydalaguvchining o'zi=====

#Xavfsizlik siyosati ma'muri=====

Dastur tomonidan=====

Boshqarish amaalga oshirilmaydi

+++++

Agar Sub'ektning xavfsizlik darajasida Ob'ektning

xavfsizlik darajasi mavjud bo'lsa, u holda uchun qanday

amalga ruxsat beriladi? =====

Yozish =====

O'zgartirish=====

#O'qish=====

Yashirish

+++++

Agar Sub'ektning xavfsizlik darajasi Ob'ektning

xavfsizlik darajasida bo'lsa, u holda qanday amalga ruxsat

beriladi? =====

#Yozish =====

O'qish=====

O'zgartirish=====

Yashirish

+++++

Rol tushunchasiga ta'rif bering. ====

Foydalanishni boshqarish=====

#Muayyan faoliyat turi bilan bog'liq harakatlar va  
majburiyatlar to'plami sifatida belgilanishi mumkin=====

Muayyan faoliyat turi bilan bog'liq imkoniyatlar to'plami  
sifatida belgilanishi mumkin=====

Vakolitlarni taqsimlash

+++++

Wi-Fi tarmoqlarida quyida keltirilgan qaysi shifrlash  
protokollaridan foydalaniladi.=====

WEB, SSL, WPA2=====

WPA, TLS=====

WPA, FTP=====

#WEP, WPA, WPA2

+++++

Foydalanishni boshqarishning qaysi usuli – Ob'ektlar va  
Sub'ektlarning atributlari, ular bilan mumkin bo'lgan  
amallar va so'rovlarga mos keladigan muhit uchun  
qoidalarni tahlil qilish asosida foydalanishlarni  
boshqaradi. =====

MAC=====

#ABAC=====

DAC=====

RBAC

+++++

Qanday tarmoq qisqa masofalarda qurilmalar o'rtasida  
ma'lumot almashinish imkoniyatini taqdim etadi? =====

#Shaxsiy tarmoq=====

Lokal=====

Mintaqaviy =====

CAMPUS

+++++

Quyidagilardan lokal tarmoqqa berilgan ta'rifni belgilang.  
=====

Odatda ijaraga olingan telekommunikatsiya liniyalaridan  
foydalanadigan tarmoqlardagi tugunlarni bir-biriga



bog'laydi. ====

Bu tarmoq shahar yoki shaharcha bo'ylab tarmoqlarning  
o'zaro bog'lanishini nazarda tutadi=====

Qisqa masofalarda qurilmalar o'rtasida ma'lumot  
almashinish imkoniyatini taqdim etadi=====

#Kompyuterlar va ularni bog'lab turgan qurilmalardan  
iborat bo'lib, ular odatda bitta tarmoqda bo'ladi.

+++++

Quyidagilardan mintaqaviy tarmoqqa berilgan ta'rifni  
belgilang. =====

Kompyuterlar va ularni bog'lab turgan qurilmalardan  
iborat bo'lib, ular odatda bitta tarmoqda bo'ladi. =====

Bu tarmoq shahar yoki shaharcha bo'ylab tarmoqlarning  
o'zaro bog'lanishini nazarda tutadi=====

#Odatda ijaraga olingan telekommunikatsiya liniyalaridan  
foydalanadigan tarmoqlardagi tugunlarni bir-biriga  
bog'laydi. =====

Qisqa masofalarda qurilmalar o'rtasida ma'lumot  
almashinish imkoniyatini taqdim etadi

+++++

Router nima? =====

Tarmoq qurilmasi bo'lib, ko'plab tarmoqlarni ulash uchun  
yoki LAN segmentlarini bog'lash uchun xizmat qiladi

Hisoblash qurilmasining ajralmas qismi bo'lib, qurilmani  
tarmoqqa ulash imkoniyatini taqdim etadi=====

Ko'plab tarmoqlarni ulash uchun yoki LAN segmentlarini  
bog'lash uchun xizmat qiladi. =====

Qabul qilingan signalni barcha chiquvchi portlarga emas  
balki paketda manzili keltirilgan portga uzatadi=====

#Qabul qilingan ma'lumotlarni tarmoq sathiga tegishli  
manzillarga ko'ra (IP manzil) uzatadi.

+++++

Fire Wall ning vazifasi... =====

#Tarmoqlar orasida aloqa o'rnatish jarayonida tashkilot  
va Internet tarmog'i orasida xavfsizlikni ta'minlaydi=====

Kompyuterlar tizimi xavfsizligini ta'minlaydi=====

Ikkita kompyuter o'rtasida aloqa o'rnatish jarayonida

Internet tarmog'i orasida xavfsizlikni ta'minlaydi=====

Uy tarmog'i orasida aloqa o'rnatish jarayonida tashkilot

va Internet tarmog'i orasida xavfsizlikni ta'minlaydi

+++++

Stenografiya ma'nosi qanday? =====

sirli xat=====

#sirli yozuv=====

maxfiy axborot=====

maxfiy belgi

+++++

Shifrlash kaliti noma'lum bo'lganda shifrlangan

ma'lumotni deshifrlash qiyinlik darajasini nima

belgilaydi? =====

Shifr matn uzunligi=====

#Kriptobardoshlik=====

Shifrlash algoritmi=====

Texnika va texnologiyalar

+++++

Ma'lumotlarni yo'q qilish odatda necha xil usulidan

foydalaniladi? =====

#4 xil=====

8 xil=====

7 xil=====

5 xil

+++++

Kiberjinoatchilik bu -. . . =====

#Kompyuter yoki boshqa qurilmalarga qarshi qilingan

yoki kompyuter va boshqa qurilmalar orqali qilingan

jinoiy faoliyat. =====

Kompyuter o'yinlari=====

Faqat banklardan pul o'g'irlanishi=====

Autentifikatsiya jarayonini buzish

+++++

Axborot xavfsizligiga bo'ladigan tahdidlarning qaysi biri

maqsadli (atayin) tahdidlar deb hisoblanadi? =====

Tabiy ofat va avariya=====

Texnik vositalarning buzilishi va ishlamasligi=====

#Strukturalarni ruxsatsiz modifikatsiyalash=====

Foydalanuvchilar va xizmat ko'rsatuvchi hodimlarning  
hatoliklari

+++++

Axborot xavfsizligiga bo'ladigan tahdidlarning qaysi biri  
tasodifiy tahdidlar deb hisoblanadi? =====

Axborotdan ruxsatsiz foydalanish=====

Zararkunanda dasturlar=====

An'anaviy josuslik va diversiya haqidagi ma'lumotlar  
tahlili=====

#Texnik vositalarning buzilishi va ishlamasligi

+++++

Axborotni uzatish va saqlash jarayonida o'z strukturasi va  
yoki mazmunini saqlash xususiyati nima deb ataladi?

=====

Axborotning konfidentsialligi=====

Foydalanuvchanligi=====

#Ma'lumotlar butunligi=====

Ixchamligi

+++++

Biometrik autentifikatsiyalashning avfzalliklari-bu: =====

Bir marta ishlatilishi=====

#Biometrik parametrlarning noyobligi=====

Biometrik parametrlarni o'zgartirish imkoniyati=====

Autentifikatsiyalash jarayonining soddaligi

+++++

Simli va simsiz tarmoqlar orasidagi asosiy farq nimadan  
iborat? =====

#Tarmoq chetki nuqtalari orasidagi mutlaqo

nazoratlamaydigan hudud=====

Tarmoq chetki nuqtalari orasidagi xududning kengligi  
asosida qurilmalar holati=====

Himoya vositalarining chegaralanganligi=====

Himoyani amalga oshirish imkoniyati yo'qligi va ma'lum

protokollarning ishlatilishi

+++++

Simmetrik shifrlashning noqulayligi – bu: ====

#Maxfiy kalitlar bilan ayirboshlash zaruriyatidir=====

Kalitlar maxfiyligi=====

Kalitlar uzunligi=====

Shifrlashga ko'p vaqt sarflanishi va ko'p yuklanishi

+++++

Autentifikatsiya faktorlari nechta? =====

4 ta=====

#3 ta=====

5 ta=====

6 ta

+++++++

Kompyuter tizimida ro'yxatga olish protsedurasini

loyihalashtirish, qaysi standart bo'yicha to'g'ri keltirilgan.

=====

#O'z DSt ISO/IEC 27002:2008=====

O'z DSt ISO/IEC 27002:2005=====

O'z DSt ISO/IEC 27002:2009=====

O'z DSt ISO/IEC 27002:2000=====

+++++++

Parollar bilan ishlashdagi tavsiyalar qaysi qatorda to'g'ri

ko'rsatilgan?=====

#Tizimga kirishdagi qayta urinishlar sonini parolning

minimal uzunligiga va muhofaza qilinayotgan tizimning

qiymatiga muvofiq belgilash;=====

Ro'yxatga olish protsedurasi uchun ruxsat berilgan vaqtni

olib tashlash. Agar u ko'paytirilgan bo'lsa, tizimning

ro'yxatga olishini davom ettirish;=====

Oxirgi muvaffaqiyatli ro'yxatga olishdan boshlab, boshqa

urinishlar so'ramaslik;=====

Kiritilayotgan parolni ko'rsatmaslik yoki variant sifatida

bir xil parol tanlash.=====

OSI modelida nechta tarmoq satxi bor ?

J: 7

OSI modelining birinchi satxi qanday nomlanadi

J: Fizik satx

OSI modelining ikkinchi satxi qanday nomlanadi

J: Kanal satxi

OSI modelining uchinchi satxi qanday nomlanadi

J: Tarmoq satxi

OSI modelining oltinchi satxi qanday nomlanadi

J: Taqdimlash satxi

OSI modelining yettinchi satxi qanday nomlanadi

J: Amaliy satx

OSI modelining qaysi satxlari tarmoqqa bog'liq satxlar hisoblanadi

J: fizik, kanal va tarmoq satxlari

OSI modelining tarmoq satxi vazifalari keltirilgan qurilmalarning qaysi birida bajariladi

J: Marshrutizator

OSI modelining fizik satxi qanday funktsiyalarni bajaradi

J: Elektr signallarini uzatish va qabul qilish

Foydalanishna boshqarishda ma'lumot , resurs, jarayon nima vazifani bajaradi ?

J: Obyekt

Foydalanishni boshqarishda inson, dastur, jarayon va xokazolar nima vazifani bajaradi?

J: Subyekt

Simmetrik kriptotizimlarda ... jumlaning davom ettiring

J: shifrlash va shifrni ochish uchun bitta va aynan shu kalitdan foydalaniladi

Simmetrik kalitli shifrlash tizimi necha turga bo'linadi.

J: 2 turga

Axborotning eng kichik o'lchov birligi nima?

J: bit

Ko'z pardasi, yuz tuzilishi, ovoz tembri:- bular autentifikatsiyaning qaysi faktoriga mos belgilar?

J: Biometrik autentifikatsiya

Kriptografiyaning asosiy maqsadi...

J: maxfiylik, yaxlitlilikni ta'minlash

Ro'yxatdan o'tish bu?

foydalanuvchilarni ro'yxatga olish va ularga dasturlar va ma'lumotlarni ishlatishga huquq berish jarayoni

Qanday xujumda zararli hujumlar tizim yoki tarmoqqa bevosita va bilvosita ta'sir qiladi?

J: Zararli hujumlar

Qanday xujumda hujumchi turli texnologiyalardan foydalangan holda tarmoqqa kirishga harakat qiladi?

J: Kirish hujumlari

Keltirilgan protokollarning qaysilari kanal satxi protokollariga mansub

J: Ethernet, FDDI

Xesh-:funktsiyani natijasi ...

J: fiksirlangan uzunlikdagi xabar

Ethernet kontsentratori qanday vazifani bajaradi

J: kompyuterdan kelayotgan axborotni qolgan barcha kompyuterga yo'naltirib beradi

Axborotlarni saqllovchi va tashuvchi vositalar qaysilar?

J: fleshka, CD va DVD disklar

Faol hujum turi deb...

J: Maxfiy uzatish jarayonini uzib qo'yish, modifikatsiyalash, qalbaki shifr ma'lumotlar tayyorlash harakatlaridan iborat jarayon

Foydalanishni boshqarishning qaysi usulida

foydalanishlar Subyektlar va Obyektlarni klassifikatsiyalashga asosan boshqariladi.

J: MAC

Foydalanishni boshqarishning qaysi usulida tizimdagi shaxsiy Obyektlarni himoyalash uchun qo'llaniladi

J: DAC

Foydalanishni boshqarishning qaysi modelida Obyekt egasining o'zi undan foydalanish huquqini va kirish turini o'zi belgilaydi

J: DACfInternetda elektron pochta bilan ishlash uchun

TCP/IPga asoslangan qaysi protokoldan foydalaniladi?

Foydalanishni boshqarishning qaysi usuli -: Obyektlar va

Subyektlarning atributlari, ular bilan mumkin bo'lgan amallar va so'rovlarga mos keladigan muhit uchun qoidalarni tahlil qilish asosida foydalanishlarni boshqaradi.

J: ABAC

Foydalanishni boshqarishning qaysi modelida har bir Obyekt uchun har bir foydalanuvchini foydalanish ruxsatini belgilash o'rniga, rol uchun Obyektlardan foydalanish ruxsati ko'rsatiladi?

J: RBAC

To'rtta bir-biri bilan bog'langan bog'lamlar strukturasi (kvadrat shaklida) qaysi topologiya turiga mansub

J: Xalqa Yulduz To'liq bog'lanishli Yacheykali

Qanday xujum asosiy hujumlarni oson amalga oshirish uchun tashkilot va tarmoq haqidagi axborotni to'plashni maqsad qiladi?

J: DNS tizimlari, Razvedka hujumlari

..... – hisoblashga asoslangan bilim sohasi bo'lib, buzg'unchilar mavjud bo'lgan sharoitda amallarni kafolatlash uchun o'zida texnologiya, inson, axborot va jarayonni mujassamlashtirgan.

J: Kiberxavfsizlik

Elektron raqamli imzo tizimi qanday muolajalarni amalga oshiradi?

J: raqamli imzoni shakllantirish va tekshirish muolajasi

Kriptologiya -:

J: axborotni qayta akslantirib himoyalash muammosi bilan shug'ullanadi

Shifrtexstni ochiq tekstga akslantirish jarayoni nima deb ataladi?

J: Deshifrlash

Xavfsizlikning asosiy yo'nalishlarini sanab o'ting.

J: Axborot xavfsizligi, Iqtisodiy xavfsizlik, Mudofaa xavfsizligi, Ijtimoiy xavfsizlik, Ekologik xavfsizlik  
Autentifikatsiya faktorlari nechta

J: 3

Kriptografiyada matn –

J: alifbo elementlarining tartiblangan to'plami

Konfidentsiallikga to'g'ri ta'rif keltiring.

J: axborot inshonchliligi, tarqatilishi mumkin emasligi, maxfiyligi kafolati;

Shaxsning, o'zini axborot kommunikatsiya tizimiga

tanishtirish jarayonida qo'llaniladigan belgilar ketma-

:ketligi bo'lib, axborot kommunikatsiya tizimidan

foydalanish huquqiga ega bo'lish uchun

foydalaniluvchining maxfiy bo'lmagan qayd yozuvi – bu?

J: login

Kriptoanaliz –

J: kalitlarni bilmasdan shifrnı ochishga bardoshlilikni

aniqlovchi shifrlash tavsifi

sifatlarga ega bo'lishi kerak?

J: ishonchli, qimmatli va to'liq

Shifrlash –

J: akslantirish jarayoni: ochiq matn deb nomlanadigan

matn shifrmatnga almashtiriladi

Qo'yish, o'rin almashtirish, gammalash kriptografiyaning qaysi turiga bog'liq?

J: simmetrik kriptosistemalar

Foydalanishni boshqarish –bu...

J: Subyektı Obyektga ishlash qobilyatini aniqlashdir.

Kompyuterning tashqi interfeysi deganda nima tushuniladi?

J: kompyuter bilan tashqi qurilmani bog'lovchi simlar va

ular orqali axborot almashinish qoidalari to'plamlari

Kodlash nima?

J: Ma'lumotni osongina qaytarish uchun hammaga

Tarmoq kartasi bu...

J: Hisoblash qurilmasining ajralmas qismi bo'lib,

qurilmani tarmoqqa ulash imkoniyatini taqdim etadi.

Elektron raqamli imzo deb –

J: xabar muallifi va tarkibini aniqlash maqsadida

shifrmatnga qo'shilgan qo'shimcha



Hab bu...

J: ko'plab tarmoqlarni ulash uchun yoki LAN segmentlarini bog'lash uchun xizmat qiladi.

Switch bu...

J: Qabul qilingan signalni barcha chiquvchi portlarga emas balki paketda manzili keltirilgan portga uzatadi.

Axborot xavfsizligining asosiy maqsadlaridan biri-: bu...

J: Axborotlarni o'g'irlanishini, yo'qolishini, soxtalashtirilishini oldini olish

Uning egasi haqiqiyligini aniqlash jarayonida tekshiruv axboroti sifatida ishlatiladigan belgilar ketma-ketligi (maxfiy so'z) – bu?

J: parol

Internetda elektron pochta bilan ishlash uchun TCP/IPga asoslangan qaysi protokoldan foydalaniladi?

J: SMTP, POP yoki IMAR

Kalit taqsimlashda ko'proq nimalarga e'tibor beriladi?

J: Tez, aniq va maxfiyligiga

Agar Subyektning xavfsizlik darajasi Obyektning xavfsizlik darajasida bo'lsa, u holda qanday amalga ruxsat beriladi.

J: Yozish

Qanday xujumda hujumchi mijozlarga, foydalanuvchilarga va tashkilotlarda mavjud bo'lgan biror xizmatni cheklashga urinadi?

J: Xizmatdan voz kechishga undash (Denial of service, DOS) hujumlari

Kalit – bu ...

J: Matnni shifrlash va shifrini ochish uchun kerakli axborot

Elektr signallarini qabul qilish va uzatish vazifalarini OSI modelining qaysi satxi bajaradi

J: Fizik satx

Blokli shifrlash-:

J: shifrlanadigan matn blokiga qo'llaniladigan asosiy akslantirish

Kriptobardoshlilik deb ...

J: kalitlarni bilmasdan shifrnı ochishga bardoshlilikni  
aniqllovchi shifrlash tavsifi

Ma'lumotlar butunligi qanday algritmlar orqali amalga  
oshiriladi

J: Xesh funksiyalar

Kriptografiya –

J: axborotni qayta akslantirishning matematik usullarini  
izlaydi va tadqiq qiladi

Keltirilgan protokollarning qaysilari transport satxi  
protokollariga mansub

J: TCP,UDP

Tekstni boshqa tekst ichida ma'nosini yashirib keltirish  
bu -:

J: steganografiya

Yaxlitlikni buzilishi bu -: ...

J: Soxtalashtirish va o'zgartirish

Biometrik autentifikatsiyalash usullari an'anaviy  
usullarga nisbatan avfzalliklari qaysi javobda to'g'ri  
ko'rsatilgan?

J: barchasi

Keltirilgan protokollarning qaysilari kanal satxi  
protokollariga mansub

J: Ethernet, FDDI

Avtorizatsiya tushunchasi odatda qaysi tushuncha bilan  
sinonim sifatida ham foydalanadi?

J: Foydalanishni boshqarish

Tarmoq repiteri bu...

J: Signalni tiklash yoki qaytarish uchun foydalaniladi.

Ochiq kalitli kriptotizimlarning mohiyati nimadan iborat?

J: Ochiq kalitli kriptotizimlarda bir-:biri bilan matematik  
bog'langan 2 ta – ochiq va yopiq kalitlardan foydalaniladi

Agar Subyektning xavfsizlik darajasida Obyektning  
xavfsizlik darajasi mavjud bo'lsa, u holda uchun qanday  
amalga ruxsat beriladi

J: O'qish

MAC usuli bilan foydalanishni boshqarishda xavfsizlik markazlashgan holatda kim tomonidan amalga oshiriladi

J: xavfsizlik siyosati ma'muri

Berilgan ta'riflardan qaysi biri asimmetrik tizimlarga xos?

J: Asimmetrik kriptotizimlarda  $k_1 \neq k_2$  bo'lib,  $k_1$  ochiq

kalit,  $k_2$  yopiq kalit deb yuritiladi,  $k_1$  bilan axborot

shifrlanadi,  $k_2$  bilan esa deshifrlanadi

Ma'lumotlarni uzatishning optimal marshrutlarini

aniqlash vazifalarini OSI modelining qaysi satxi bajaradi

J: Tarmoq satxi

Foydalanishni boshqarishning mandatli modelida

Obyektning xavfsizlik darajasi nimaga bog'liq..

J: Tashkilotda Obyektning muhimlik darajasi bilan yoki

yo'qolgan taqdirda keltiradigan zarar miqdori bilan

xarakterlanadi

Qaysi juftlik RSA algoritmining ochiq va yopiq kalitlarini

ifodalaydi

J:  $\{d, n\}$  – yopiq,  $\{e, n\}$  – ochiq;

Diskni shifrlash nima uchun amalga oshiriladi?

J: Ma'lumotni saqlash vositalarida saqlangan ma'lumot

konfidensialligini ta'minlash uchun amalga oshiriladi

Tahdid nima?

J: Tashkilotga zarar yetkazishi mumkin bo'lgan

istalmagan hodisa.

Risk

J: Potensial foyda yoki zarar

barcha kabel va tarmoq tizimlari; tizim va kabellarni fizik

nazoratlash; tizim va kabel uchun quvvat manbai; tizimni

madadlash muhiti. Bular tarmoqning qaysi satxiga kiradi?

J: Fizik satx

Identifikatsiya, autentifikatsiya jarayonlaridan o'tgan

foydalanuvchi uchun tizimda bajarishi mumkin bo'lgan

amallarga ruxsat berish jarayoni bu...

J: Avtorizatsiya

Xavfsizlikning asosiy yo'nalishlarini sanab o'ting.

J: Axborot xavfsizligi, Iqtisodiy xavfsizlik, Mudofaa

xavfsizligi, Ijtimoiy xavfsizlik, Ekologik xavfsizlik

Kompyuter tarmoqlari bu –

J: Bir biriga osonlik bilan ma'lumot va resurslarni

taqsimlash uchun ulangan

Elektron raqamli imzo tizimi qanday muolajalarni amalga oshiradi?

J: raqamli imzoni shakllantirish va tekshirish muolajasi

Kriptografiyada matn –

J: alifbo elementlarining tartiblangan to'plami

Autentifikatsiya jarayoni qanday jarayon?

J: obyekt yoki subhektni unga berilgan identifikatorga

mosligini tekshirish va belgilar ketmaketligidan iborat

maxfiy kodini tekshirish orqali aslligini aniqlash

Rol tushunchasiga ta'rif bering.

J: Muayyan faoliyat turi bilan bog'liq harakatlar va

majburiyatlar to'plami sifatida belgilanishi mumkin

Avtorizatsiya jarayoni qanday jarayon?

J: foydalanuvchining resursdan foydalanish huquqlari va

ruxsatlarini tekshirish jarayoni

Faqat foydalanuvchiga ma'lum va biror tizimda

autentifikatsiya jarayonidan o'tishni ta'minlovchi biror

axborot nima

J: Parol

Elektron raqamli imzo deb –

J: xabar muallifi va tarkibini aniqlash maqsadida

shifratmatga qo'shilgan qo'shimcha

TCP/IP modelida nechta satx mavjud

J: 4

Kriptoanaliz –

J: kalitlarni bilmasdan shifrnı ochishga bardoshlilikni

aniqlovchi shifrlash tavsifi

Shifrlashning kombinatsiyalangan usulida qanday

kriptotizimlarning kriptografik kalitlaridan foydalaniladi?

J: Simmetrik va assimetrik

Shifrlash nima?

J: Ma'lumot boshqa formatga o'zgartiriladi, barcha

shaxslar kalit yordamida qayta o'zgartirishi mumkin

bo'ladi

Kriptografiyada alifbo –

J: axborot belgilarini kodlash uchun foydalaniladigan

chekli to'plam

Kripto tizimga qo'yiladigan umumiy talablardan biri

J: shifr matn uzunligi ochiq matn uzunligiga teng bo'lishi

kerak

Simmetrik kriptotizimning uzluksiz tizimida ...

J: ochiq matnning har bir harfi va simvoli alohida

shifrlanadi

Axborot resursi – bu?

J: axborot tizimi tarkibidagi elektron shakldagi axborot,

ma'lumotlar banki, ma'lumotlar bazasi

Stenografiya ma'nosi...

J: sirli yozuv

Identifikatsiya jarayoni qanday jarayon?

J: axborot tizimlari obyekt va subhektlariga uni tanish

uchun nomlar (identifikator) berish va berilgan nom

bo'yicha solishtirib uni aniqlash jarayoni

Ma'lumotlarni inson xatosi tufayli yo'qolish sababini

belgilang.

J: Ma'lumotlarni saqlash vositasini to'g'ri

joylashtirilmagani yoki ma'lumotlar bazasini xatolik bilan

boshqarilganligi.

2. Qo'yish, o'rin almashtirish, gammalash

kriptografiyaning qaysi turiga bog'liq?

J: simmetrik kriptotizimlar

3. Quyidagilardan lokal tarmoqqa berilgan ta'rifni

belgilang.

J: Kompyuterlar va ularni bog'lab turgan qurilmalardan

iborat bo'lib, ular odatda bitta tarmoqda bo'ladi.

4. Uning egasi haqiqiyligini aniqlash jarayonida tekshiruv

axboroti sifatida ishlatiladigan belgilar ketma-ketligi

(maxfiy so'z) – nima?

J: parol

5. Rol tushunchasiga ta'rif bering.

Muayyan faoliyat turi bilan bog'liq harakatlar va majburiyatlar to'plami sifatida belgilanishi mumkin

6. Foydalanish huquqini cheklovchi matritsa modeli bu...

J: Bella La-Padulla modeli

8. Shifrtexstni ochiq tekstga akslantirish jarayoni nima deb ataladi?

J: Deshifrlash

9. Axborot xavfsizligiga bo'ladigan tahdidlarning qaysi biri maqsadli (atayin) tahdidlar deb hisoblanadi?

J: Strukturalarni ruxsatsiz modifikatsiyalash

10. Shifrlash kaliti noma'lum bo'lganda shifrlangan ma'lumotni deshifrlash qiyinlik darajasini nima

belgilaydi?

J: Kriptobardoshlik

11. Foydalanishni boshqarish –bu...

J: Sub'ektni Ob'ektga ishlash qobiliyatini aniqlashdir.

12. Lokal tarmoqlarda keng tarqalgan topologiya turi qaysi?

J: Yulduz

13. RSA algoritmi qaysi yilda ishlab chiqilgan?

J: 1977 yil

14. Elektron xujjatlarni yo'q qilish usullari qaysilar?

J: Shredirlash, magnitsizlantirish, yanchish

15. Kriptografiyada kalitning vazifasi nima?

J: Matnni shifrlash va shifrini ochish uchun kerakli axborot

16. WiMAX qanday simsiz tarmoq turiga kiradi?

J: Regional

17. Shaxsning, axborot kommunikatsiya tizimidan foydalanish huquqiga ega bo'lish uchun foydalaniluvchining maxfiy bo'lmagan qayd yozuvi – bu...

J: login

18. Stenografiya ma'nosi qanday?

J: sirli yozuv

19. Fire Wall ning vazifasi...

J: Tarmoqlar orasida aloqa o'rnatish jarayonida tashkilot va Internet tarmog'i orasida xavfsizlikni ta'minlaydi

20. Yaxlitlikni buzilishi bu - ...

J: Soxtalashtirish va o'zgartirish

2. Rezident virus...

tezkor xotirada saqlanadi

3. Tashkilot va uning AKT doirasida aktivlarni shu

jumladan, kritik axborotni boshqarish, himoyalash va taqsimlashni belgilovchi qoidalar, ko'rsatmalar, amaliyoti fanda qanday nomladi?

AKT xavfsizlik siyosati

4. O'chirilgan yoki formatlangan ma'lumotlarni tikovchi dasturni belgilang.

Recuva, R.saver

5. Zaiflik – bu...

tizimda mavjud bo'lgan xavfsizlik muammoasi bo'lib, ular asosan tizimning yaxshi shakllantirilmaganligi yoki sozlanmaganligi sababli kelib chiqadi.

6. Axborot xavfsizligi timsollarini ko'rsating.

Alisa, Bob, Eva

7. Kiberetika tushunchasi:

Kompyuter va kompyuter tarmoqlarida odamlarning etikasi

8. "Axborot olish va kafolatlari va erkinligi to'g'risda"gi

Qonuni qachon kuchga kirgan?

1997 yil 24 aprel

9. DIR viruslari nimani zararlaydi?

FAT tarkibini zararlaydi

10. Virusning signaturasi (virusga taalluqli baytlar ketmaketligi) bo'yicha operativ xotira va fayllarni ko'rish natijasida ma'lum viruslarni topuvchi va xabar beruvchi dasturiy ta'minot nomi nima deb ataladi?

Detektorlar

11. Agar foydalanuvchi tizimda ma'lumot bilan ishlash vaqtida ham zahiralash amalga oshirilishi .... deb ataladi?

"Issiq zaxiralash"

12. Aksariyat tijorat tashkilotlari uchun ichki tarmoq

xavfsizligini taminlashning zaruriy sharti-bu...

Tarmoqlararo ekranlarning o'rnatilishi

13. Axborot xavfsizligida axborotning bahosi qanday

aniqlanadi?

Axborot xavfsizligi buzulgan taqdirda ko'rilishi mumkin

bo'lgan zarar miqdori bilan

14. Kompyuter yoki boshqa qurilmalarga qarshi qilingan

yoki kompyuter va boshqa qurilmalar orqali qilingan

jinoyat-...

Kiberjinoyat deb ataladi

15. Antiviruslarni, qo'llanish usuliga ko'ra... turlari

mavjud?

detektorlar, faglar, vaksinalar, privivkalar, revizorlar,

monitorlar

16. Qaysi siyosatga ko'ra faqat ma'lum xavfli

xizmatlar/hujumlar yoki harakatlar bloklanadi?

Ruxsat berishga asoslangan siyosat

17. DIR viruslari nimani zararlaydi?

FAT tarkibini zararlaydi

18. Makroviruslar nimalarni zararlaydi?

Ma'lum dasturlash tilida yozilgan va turli ofis ilovalari –

MS Word hujjati, MS Excel elektron jadvali, Corel Draw

tasviri, fayllarida joylashgan "makroslar" yoki

"skriptlar"ni zararlaydi.

19. Ma'lumotlarni zahira nusxasini saqlovchi va tikovchi

dasturni belgilang.

HandyBakcup

20. Tizim ishlamay turganda yoki foydalanuvchilar

ma'lumot bilan ishlamay turganda zahiralash amalga

oshirilsa .... deb ataladi.

"Sovuq saxiralash"

21. "Elektron hujjat" tushunchasi haqida to'g'ri ta'rif

berilgan qatorni ko'rsating.

Elektron shaklda qayd etilgan, elektron raqamli imzo

bilan tasdiqlangan va elektron hujjatning uni



identifikatsiya qilish imkoniyatini beradigan boshqa

rekvizitlariga ega bo'lgan axborot elektron hujjatdir

22. Polimorf viruslar tushunchasi to'g'ri ko'rsating.

Viruslar turli ko'rinishdagi shifrlangan viruslar bo'lib, o'zining ikkilik shaklini nusxadan-nusxaga o'zgartirib boradi

23. Fishing (ing. Phishing – baliq ovlash) bu...

Internetdagi firibgarlikning bir turi bo'lib, uning maqsadi foydalanuvchining maxfiy ma'lumotlaridan, login/parol, foydalanish imkoniyatiga ega bo'lishdir.

Xavfsizlikning asosiy yo'nalishlarini sanab o'ting.

Axborot xavfsizligi, Iqtisodiy xavfsizlik, Mudofaa xavfsizligi, Ijtimoiy xavfsizlik, Ekologik xavfsizlik

Axborot xavfsizligining asosiy maqsadlaridan biri- bu...

Axborotlarni o'g'irlanishini, yo'qolishini, soxtalashtirilishini oldini olish

Konfidentsiallikga to'g'ri ta'rif keltiring. axborot inshonchiligi, tarqatilishi mumkin emasligi, maxfiyligi kafolati;

Yaxlitlikni buzilishi bu - ... Soxtalashtirish va o'zgartirish

... axborotni himoyalash tizimi deyiladi. Axborotning zaif tomonlarini kamaytiruvchi axborotga ruxsat etilmagan kirishga, uning chiqib ketishiga va yo'qotilishiga to'sqinlik qiluvchi tashkiliy, texnik, dasturiy, texnologik va boshqa vosita, usul va choralarning ko

Kompyuter virusi nima? maxsus yozilgan va zararli dastur

Axborotni himoyalash uchun ... usullari qo'llaniladi. kodlashtirish, kriptografiya, stegonografiya

Stenografiya mahnosi... sirli yozuv

Kriptologiya yo'nalishlari nechta? 2

Kriptografiyaning asosiy maqsadi... maxfiylik, yaxlitlikni ta'minlash

SMTP - Simple Mail Transfer protokol nima? elektron

pochta protokoli

SKIP protokoli... Internet protokollari uchun

kriptokalitlarning oddiy boshqaruvi

Kompyuter tarmog'ining asosiy komponentlariga

nisbatan xavf-xatarlar... uzilish, tutib qolish, o'zgartirish,  
soxtalashtirish

...ma'lumotlar oqimini passiv hujumlardan himoya

qilishga xizmat qiladi. konfidentsiallik

Foydalanish huquqini cheklovchi matritsa modeli bu...

Bella La-Padulla modeli

Kommunikatsion qism tizimlarida xavfsizlikni

ta'minlanishida necha xil shifrlash ishlatiladi? 2

Kompyuter tarmoqlarida tarmoqning uzoqlashtirilgan

elemenlari o'rtasidagi aloqa qaysi standartlar yordamida  
amalga oshiriladi? TCP/IP, X.25 protokollar

Himoya tizimi kompleksligiga nimalar orqali erishiladi?

Xuquqiy tashkiliy, muhandis, texnik va dasturiy

matematik elementlarning mavjudligi orqali

Kalit – bu ... Matnni shifrlash va shifrini ochish uchun

kerakli axborot

Qo'yish, o'rin almashtirish, gammalash

kriptografiyaning qaysi turiga bog'liq? simmetrik

kriptotizimlar

Autentifikatsiya nima? Ma'lum qilingan foydalanuvchi,

jarayon yoki qurilmaning haqiqiy ekanligini tekshirish

muolajasi

Identifikatsiya bu- ... Foydalanuvchini uning

identifikatori (nomi) bo'yicha aniqlash jarayoni

O'rin almashtirish shifri bu - ... Murakkab bo'lmagan

kriptografik akslantirish

Simmetrik kalitli shifrlash tizimi necha turga bo'linadi. 2

turga

Kalitlar boshqaruvi 3 ta elementga ega bo'lgan axborot

almashinish jarayonidir bular ... hosil qilish, yig'ish,

taqsimlash

Kriptologiya - axborotni qayta akslantirib himoyalash

muammosi bilan shug'ullanadi

Kriptografiya alifbo – axborot belgilarini kodlash  
uchun foydalaniladigan chekli to'plam

Simmetrik kriptotizimlarda ... jumlani davom ettiring  
shifrlash va shifrnı ochish uchun bitta va aynan shu  
kalitdan foydalaniladi

Kriptobardoshlilik deb ... kalitlarni bilmasdan shifrnı  
ochishga bardoshlilikni aniqlovchi shifrlash tavsifi

Elektron raqamli imzo deb – xabar muallifi va tarkibini  
aniqlash maqsadida shifratnga qo'shilgan qo'shimcha

Kriptografiya – axborotni qayta akslantirishning  
matematik usullarini izlaydi va tadqiq qiladi

Kriptografiya matn – alifbo elementlarining  
tartiblangan to'plami

Kriptoanaliz – kalitlarni bilmasdan shifrnı ochishga  
bardoshlilikni aniqlovchi shifrlash tavsifi

Shifrlash – akslantirish jarayoni: ochiq matn deb  
nomlanadigan matn shifratnga almashtiriladi

Kalit taqsimlashda ko'proq nimalarga e'tibor beriladi?

Tez, aniq va maxfiyligiga

Faol hujum turi deb... Maxfiy uzatish jarayonini uzib  
qo'yish, modifikatsiyalash, qalbaki shifrlar ma'lumotlar  
tayyorlash harakatlaridan iborat jarayon

Blokli shifrlash- shifrlanadigan matn blokiga  
qo'llaniladigan asosiy akslantirish

Simmetrik kriptotizimning uzluksiz tizimida ... ochiq  
matnning har bir harfi va simvoli alohida shifrlanadi

Kripto tizimga qo'yiladigan umumiy talablardan biri  
shifrlar matn uzunligi ochiq matn uzunligiga teng bo'lishi  
kerak

Quyidagi tengliklardan qaysilari shifrlash va  
deshifrlashni ifodalaydi?  $E_{k1}(T)=T$ ,  $D_{k2}(T1)=T$

Berilgan ta'riflardan qaysi biri assimmetrik tizimlarga  
xos? Assimmetrik kriptotizimlarda  $k1 \neq k2$  bo'lib,  $k1$  ochiq  
kalit,  $k2$  yopiq kalit deb yuritiladi,  $k1$  bilan axborot  
shifrlanadi,  $k2$  bilan esa deshimflanadi

Yetarlicha kriptoturg'unlikka ega, dastlabki matn  
simvollarini almashtirish uchun bir necha alfavitdan  
foydalanishga asoslangan almashtirish usulini belgilang  
Vijiner matritsasi, Sezar usuli

Akslantirish tushunchasi deb nimaga aytiladi? 1-  
to'plamli elementlariga 2-to'plam elementalriga mos  
bo'lishiga

Simmetrik guruh deb nimaga aytiladi? O'rin  
almashtirish va joylashtirish

Qo'yish, o'rin almashtirish, gammalash  
kriptografiyaning qaysi turiga bog'liq? simmetrik  
kriptositemalar

Xavfli viruslar bu - ... kompyuter ishlashida jiddiy  
nuqsonlarga sabab bo'luvchi viruslar

Mantiqiy bomba – bu ... Ma'lum sharoitlarda zarar  
keltiruvchi harakatlarni bajaruvchi dastur yoki uning  
alohida modullari

Elektron raqamli imzo tizimi qanday muolajani amalga  
oshiradi? raqamli imzoni shakllantirish va tekshirish  
muolajasi

Shifrlashning kombinatsiyalangan usulida qanday  
kriptotizimlarning kriptografik kalitlaridan foydalaniladi?  
Simmetrik va assimetrik

Axborot himoyasi nuqtai nazaridan kompyuter  
tarmoqlarini nechta turga ajratish mumkin? Korporativ va  
umumfoydalanuvchi

Elektromagnit nurlanish va ta'sirlanishlardan  
himoyalash usullari nechta turga bo'linadi? Sust va faol  
Internetda elektron pochta bilan ishlash uchun TCP/IPga  
asoslangan qaysi protokoldan foydalaniladi? SMTP, POP  
yoki IMAR

Axborot resursi – bu? axborot tizimi tarkibidagi elektron  
shakldagi axborot, ma'lumotlar banki, ma'lumotlar bazasi

Shaxsning, o'zini axborot kommunikatsiya tizimiga  
tanishtirish jarayonida qo'llaniladigan belgilar ketmaketligi bo'lib, axborot kommunikatsiya tizimidan  
foydalanish huquqiga ega bo'lish uchun

foydalaniluvchining maxfiy bo'lmagan qayd yozuvi – bu?

login

Uning egasi haqiqiylikni aniqlash jarayonida tekshiruv  
axboroti sifatida ishlatiladigan belgilar ketma-ketligi

(maxfiy so'z) – bu? parol

Identifikatsiya jarayoni qanday jarayon? axborot  
tizimlari ob'yekt va subhektlariga uni tanish uchun  
nomlar (identifikator) berish va berilgan nom bo'yicha  
solishtirib uni aniqlash jarayoni

Autentifikatsiya jarayoni qanday jarayon? ob'yekt yoki  
subhektga unga berilgan identifikatorga mosligini  
tekshirish va belgilar ketmaketligidan iborat maxfiy  
kodini tekshirish orqali aslligini aniqlash

Avtorizatsiya jarayoni qanday jarayon?  
foydalanuvchining resursdan foydalanish huquqlari va  
ruxsatlarini tekshirish jarayoni

Ro'yxatdan o'tish bu? foydalanuvchilarni ro'yxatga  
olish va ularga dasturlar va ma'lumotlarni ishlatishga  
huquq berish jarayoni

Axborot qanday sifatlarga ega bo'lishi kerak? ishonchli,  
qimmatli va to'liq

Axborotning eng kichik o'lchov birligi nima? bit

Elektronhujjatning rekvizitlari nechta qismdan iborat? 4

Axborotlarni saqlovchi va tashuvchi vositalar qaysilar?  
flashka, CD va DVD disklar

Imzo bu nima? hujjatning haqiqiylikni va yuborgan  
fizik shaxsga tegishli ekanligini tasdiqlaydigan insonning  
fiziologik xususiyati.

Muhr bu nima? hujjatning haqiqiylikni va biror bir  
yuridik shaxsga tegishli ekanligini tasdiqlovchi isbotdir.

DSA – nima Raqamli imzo algoritmi

El Gamal algoritmi qanday algoritm Shifrlash algoritmi  
va raqamli imzo algoritmi

Sezarining shifrlash sistemasining kamchiligi Harflarning  
so'zlarda kelish chastotasini yashirmaydi

Axborot xavfsizligi va xavfsizlik san'ati haqidagi fan ....

deyiladi? Kriptografiya

Tekstni boshqa tekst ichida ma'nosini yashirib keltirish

bu - steganografiya

Shifrttekstni ochiq tekstga akslantirish jarayoni nima deb

ataladi? Deshifrlash

..... – hisoblashga asoslangan bilim sohasi bo'lib,

buzg'unchilar mavjud bo'lgan jaroitda amallarni

kafolatlash uchun o'zida texnologiya, inson, axborot va

jarayonni mujassamlashtirgan. Kiberxavfsizlik

Risk Potensial foyda yoki zarar

Kiberxavfsizlik nechta bilim sohasini o'z ichiga oladi. 8

“Ma'lumotlar xavfsizligi” bilim sohasi..... ma'lumotlarni

saqlashda, qayta ishlashda va uzatishda himoyani

ta'minlashni maqsad qiladi.

“Dasturiy ta'minotlar xavfsizligi” bilim sohasi.....

foydalanilayotgan tizim yoki axborot xavfsizligini

ta'minlovchi dasturiy ta'minotlarni ishlab chiqish va

foydalanish jarayoniga e'tibor qaratadi.

“Tashkil etuvchilar xavfsizligi” ..... katta tizimlarda

integrallashgan tashkil etuvchilarni loyihalash, sotib olish,

testlash, analiz qilish va texnik xizmat ko'rsatishga e'tibor

qaratadi.

“Aloqa xavfsizligi” bilim sohasi..... tashkil etuvchilar

o'rtasidagi aloqani himoyalashga etibor qaratib, o'zida

fizik va mantiqiy ulanishni birlashtiradi.

“Tizim xavfsizligi” bilim sohasi..... tashkil etuvchilar,

ulanishlar va dasturiy ta'minotdan iborat bo'lgan tizim

xavfsizligining aspektlariga e'tibor qaratadi.

“Inson xavfsizligi” bilim sohasi.... kiberxavfsizlik bilan

bog'liq inson hatti harakatlarini o'rganishdan tashqari,

tashkilotlar (masalan, xodim) va shaxsiy hayot sharoitida

shaxsiy ma'lumotlarni va shaxsiy hayotni himoya qilishga

e'tibor qaratadi.

“Tashkilot xavfsizligi” bilim sohasi .... tashkilotni

kiberxavfsizlik tahdidlaridan himoyalash va tashkilot

vazifasini muvaffaqiyatli bajarishini

“Jamoat xavfsizligi” bilim sohasi ..... u yoki bu darajada jamiyatda ta’sir ko’rsatuvchi kiberxavfsizlik omillariga e’tibor qaratadi.

Tahdid nima? tizim yoki Tashkilotga zarar yetkazishi mumkin bo’lgan istalmagan hodisa.

Kodlash nima? Ma’lumotni osongina qaytarish uchun hammaga ochiq bo’lgan sxema yordamida ma’lumotlarni boshqa formatga o’zgartirishdir

Shifrlash nima? Ma’lumot boshqa formatga o’zgartiriladi, biroq uni faqat maxsus shaxslar qayta o’zgartirishi mumkin bo’ladi

Bir martalik bloknotda Qanday kalitlardan foydalaniladi?

Ochiq kalitdan

Ikkilik sanoq tizimida berilgan 10111 sonini o’nlik sanoq tizimiga o’tkazing. 23

Agar RSA algoritimida  $n$  ochiq kalitni,  $d$  maxfiy kalitni ifodalasa, qaysi formula deshifrlashni ifodalaydi.  $M = C_d \pmod n$ ;

O’nlik sanoq tizimida berilgan quyidagi sonlarni ikkil sanoq tizimiga o’tkazing. 65 100001

Quyidagi modulli ifodani qiymatini toping.

$(125 \cdot 45) \pmod{10}$ . 5

Quyidagi modulli ifodani qiymatini toping  $(148 + 14432) \pmod{256}$ . 244

Agar RSA algoritimida  $e$  ochiq kalitni,  $d$  maxfiy kalitni ifodalasa, qaysi formula deshifrlashni ifodalaydi.  $C = M_e \pmod n$ ; -tog’ri javob

Axborotni shifrnı ochish (deshifrlash) bilan qaysi fan shug’ullanadi Kriptologiya.

Qaysi juftlik RSA algoritmining ochiq va yopiq kalitlarini ifodalaydi  $\{d, n\}$  – yopiq,  $\{e, n\}$  – ochiq;

Zamonaviy kriptografiya qanday bo’limlardan iborat?

Simmetrik kriptotizimlar; ochiq kalitli kriptotizimlar;

Elektron raqamli imzo; kalitlarni boshqarish

1. Kriptografik usullardan foydalanishning asosiy yo’nalishlari nimalardan iborat? Aloqa kanali orqali

maxfiy axborotlarni uzatish (masalan, elektron pochta orqali), uzatilyotgan xabarlarni haqiqiylikini aniqlash, tashuvchilarda axborotlarni shifrlangan ko

Shifr nima? Shifrlash va deshifrlashda foydalaniladigan matematik funktsiyadan iborat bo'lgan kriptografik algoritmi

Ochiq kalitli kriptotizimlarning mohiyati nimadan iborat?

Ochiq kalitli kriptotizimlarda bir-biri bilan matematik bog'langan 2 ta – ochiq va yopiq kalitlardan foydalaniladi

Oqimli shifrlashning mohiyati nimada? Oqimli shifrlash birinchi navbatda axborotni bloklarga bo'lishning imkoni bo'lmagan hollarda zarur, Qandaydir ma'lumotlar oqimini har bir belgisini shifrlab, boshqa belgilarini kutmasdan kerakli joyga jo'natish uchun o

Simmetrik algoritmlarni xavfsizligini ta'minlovchi omillarni ko'rsating. uzatilayotgan shifrlangan xabarni kalitsiz ochish mumkin bo'lmashligi uchun algoritmi yetarli darajada bardoshli bo'lishi lozim, uzatilayotgan xabarni xavfsizligi algoritmi maxfiyligiga emas

Kriptotizim quyidagi komponentlardan iborat: ochiq matnlar fazosi  $M$ , Kalitlar fazosi  $K$ , Shifmatnlar fazosi  $C$ ,  $E_k : M \rightarrow C$  (shifrlash uchun) va  $D_k : C \rightarrow M$  (deshifrlash uchun) funktsiyalar

Serpent, Square, Twofish, RC6, AES algoritmlari qaysi turiga mansub? simmetrik blokli algoritmlar

DES algoritimga muqobil bo'lgan algoritmi ko'rsating.

Uch karrali DES, IDEA, Rijndael

DES algoritmining asosiy muammosi nimada? kalit uzunligi 56 bit. Bugungu kunda ushbu uzunlik algoritmi kriptobardoshliligi uchun yetarli emas

Asimmetrik kriptotizimlar qanday maqsadlarda ishlatiladi? shifrlash, deshifrlash, ERI yaratish va tekshirish, kalitlar almashish uchun

$12+22 \bmod 32 = 2$

$2+5 \bmod 32 = 7$

Kriptografik elektron raqamli imzolarda qaysi kalitlar



ma'lumotni yaxlitligini ta'minlashda ishlatiladi. ochiq

kalitlar

$12+11 \bmod 16 = 7$

RIJNDAEL algoritmi qancha uzunligdagi kalitlarni

qo'llab quvvatlaydi. 128 bitli, 192 bitli, 256 bitli

Xesh-funktsiyani natijasi ... uzunlikdagi xabar

RSA algoritmi qanday jarayonlardan tashkil topgan

Kalitni generatsiyalash; Shifrlash; Deshifrlash.

RSA algoritmidan amalda foydalanish uchun tanlanuvchi

tub sonlar uzunligi kamida necha bit bo'lishi talab etiladi.

2048

Ma'lumotlar butunligi qanday algritmlar orqali amalga

oshiriladi Xesh funksiyalar

To'rtta bir-biri bilan bog'langan bog'lamlar strukturasi

(kvadrat shaklida) qaysi topologiya turiga mansub Xalqa

Qaysi topologiya birgalikda foydalanilmaydigan muhitni

qo'llamasligi mumkin to'liq bog'lanishli

Kompyuterning tashqi interfeysi deganda nima

tushuniladi kompyuter bilan tashqi qurilmani bog'lovchi

simlar va ular orqali axborot almashinish qoidalari

to'plamlari

Lokal tarmoqlarda keng tarqalgan topologiya turi qaysi

Yulduz

Ethernet kontsentratori qanday vazifani bajaradi

kompyuterdan kelayotgan axborotni qolgan barcha

kompyuterga yo'naltirib beradi

OSI modelida nechta sath mavjud 7

OSI modelining to'rtinchi sathi qanday nomlanadi

Transport sathi

OSI modelining beshinchi sathi qanday nomlanadi

Seanslar sathi

OSI modelining birinchi sathi qanday nomlanadi Fizik

sath

OSI modelining ikkinchi sathi qanday nomlanadi Kanal

sathi

OSI modelining uchinchi sathi qanday nomlanadi Tarmoq

sathi

OSI modelining oltinchi sathi qanday nomlanadi

Taqdimlash sathi

OSI modelining ettinchi sathi qanday nomlanadi Amaliy  
sath

OSI modelining qaysi sathlari tarmoqqa bog'liq sathlar  
hisoblanadi fizik, kanal va tarmoq sathlari

OSI modelining tarmoq sathi vazifalari keltirilgan

qurilmalarning qaysi birida bajariladi Marshrutizator

Elektr signallarini qabul qilish va uzatish vazifalarini OSI  
modelining qaysi sathi bajaradi Fizik sath

Ma'lumotlarni uzatishning optimal marshrutlarini  
aniqlash vazifalarini OSI modelining qaysi sathi bajaradi

Tarmoq sathi

Keltirilgan protokollarning qaysilari tarmoq sathi  
protokollariga mansub IP, IPX

Keltirilgan protokollarning qaysilari transport sathi  
protokollariga mansub TCP,UDP

OSI modelining fizik sathi qanday funktsiyalarni bajaradi  
Elektr signallarini uzatish va qabul qilish

OSI modelining amaliy sathi qanday funktsiyalarni  
bajaradi Klient dasturlari bilan o'zaro muloqotda bo'lish

Keltirilgan protokollarning qaysilari kanal sathi  
protokollariga mansub Ethernet, FDDI

Keltirilgan protokollarning qaysilari taqdimlash sathi  
protokollariga mansub SNMP, Telnet

Identifikatsiya, autentifikatsiya jarayonlaridan o'tgan  
foydalanuvchi uchun tizimda bajarishi mumkin bo'lgan

amallarga ruxsat berish jarayoni bu... Avtorizatsiya

Autentifikatsiya faktorlari nechta 3

Faqat foydalanuvchiga ma'lum va biror tizimda  
autentifikatsiya jarayonidan o'tishni ta'minlovchi biror  
axborot nima Parol

Ko'z pardasi, yuz tuzilishi, ovoz tembri. Biometrik  
autentifikatsiya

barcha kabel va tarmoq tizimlari; tizim va kabellarni fizik

nazoratlash; tizim va kabel uchun quvvat manbai; tizimni madadlash muhiti. Bular tarmoqning qaysi satxiga kiradi.

Fizik satx

Fizik xavfsizlikda Yong'inga qarshi tizimlar necha turga bo'linadi 2

Avtorizatsiya tushunchasi odatda qaysi tushuncha bilan sinonim sifatida ham foydalanadi. Foydalanishni boshqarish

Foydalanishni boshqarish –bu... sub'ektni sub'ektga ishlash qobiliyatini aniqlashdir.

Foydalanishna boshqarishda inson, dastur, jarayon va xokazolar nima vazifani bajaradi, Sub'ekt

Foydalanishna boshqarishda ma'lumot , resurs, jarayon nima vazifani bajaradi ? Ob'ekt

Foydalanishna boshqarishning nechta usuli mavjud? 4

Foydalanishni boshqarishning qaysi usulida tizimdagi shaxsiy ob'ektlarni himoyalash uchun qo'llaniladi DAC

Foydalanishni boshqarishning qaysi modelida ob'ekt egasining o'zi undan foydalanish huquqini va kirish turini o'zi belgilaydi DAC

Foydalanishni boshqarishning qaysi usulida

foydalanishlar sub'ektlar va ob'ektlarni

klassifikatsiyalashga asosan boshqariladi. MAC

Foydalanishni boshqarishning mandatli modelida

Ob'ektning xavfsizlik darajasi nimaga bog'liq..

Tashkilotda ob'ektning muhimlik darajasi bilan yoki yo'qolgan taqdirda keltiradigan zarar miqdori bilan xarakterlanadi

MAC usuli bilan foydalanishni boshqarishda xavfsizlik markazlashgan holatda kim tomonidan amalga oshiriladi xavfsizlik siyosati ma'muri

Agar sub'ektning xavfsizlik darajasida ob'ektning xavfsizlik darajasi mavjud bo'lsa, u holda uchun qanday amalga ruxsat beriladi O'qish

Agar sub'ektning xavfsizlik darajasi ob'ektning xavfsizlik darajasida bo'lsa, u holda qanday amalga ruxsat beriladi.

Yozish

Foydalanishni boshqarishning qaysi modelida har bir ob'ekt uchun har bir foydalanuvchini foydalanish ruxsatini belgilash o'rniga, rol uchun ob'ektlardan foydalanish ruxsati ko'rsatiladi? RBAC

Rol tushunchasiga ta'rif bering. Muayyan faoliyat turi bilan bog'liq harakatlar va majburiyatlar to'plami sifatida belgilanishi mumkin

Foydalanishni boshqarishning qaysi usuli - ob'ektlar va sub'ektlarning atributlari, ular bilan mumkin bo'lgan amallar va so'rovlarga mos keladigan muhit uchun qoidalarni tahlil qilish asosida foydalanishlarni boshqaradi. ABAC

XACML foydalanishni boshqarishni qaysi usulining standarti? ABAC

Biometrik autentifikatsiyalash usullari an'anaviy usullarga nisbatan avfzalliklari qaysi javobda to'g'ri ko'rsatilgan? barchasi

Axborotning kriptografik himoya vositalari necha turda?

3

Dasturiy shifrlash vositalari necha turga bo'linadi 4

Diskni shifrlash nima uchun amalga oshiriladi?

Ma'lumotni saqlash vositalarida saqlangan ma'lumot konfidensialligini ta'minlash uchun amalga oshiriladi

Ma'lumotlarni yo'q qilish odatda necha hil usulidan foydalaniladi? 4

Kompyuter tarmoqlari bu – Bir biriga osonlik bilan ma'lumot va resurslarni taqsimlash uchun ulangan kompyuterlar guruhi

Tarmoq modeli –bu.. ikki Hisoblash tizimlariorasidagi aloqani ularning ichki tuzilmaviy vatexnologik asosidan qat'iy nazar muvaffaqiyatli o'rnatilishini asosidir to'plami

OSI modelida nechta tarmoq sathi bor 7

OSI modeli 7 stahi bu llova

OSI modeli 1 stahi bu Fizik

OSI modeli 2 stahi bu Kanal

TCP/IP modelida nechta satx mavjud 4

Qanday tarmoq qisqa masofalarda qurilmalar o'rtasid a  
ma'lumot almashinish imkoniyatini taqdim etadi. Shaxsiy  
tarmoq

Tarmoq kartasi bu... Hisoblash qurilmasining ajralmas  
qismi bo'lib, qurilmani tarmoqqa ulash imkoniyatini  
taqdim etadi.

Switch bu... Qabul qilingan signalni barcha chiquvchi  
portlarga emas balki paketda manzili keltirilgan portga  
uzatadi

Hab bu... ko'plab tarmoqlarni ulash uchun yoki LAN  
segmentlarini bog'lash uchun xizmat qiladi.

Tarmoq repiteri bu... Signalni tiklash yoki qaytarish  
uchun foydalaniladi.

Qanday tizim host nomlari va internet nomlarini IP  
manzillarga o'zgartirish yoki teskarisini amalga oshiradi.

DNS tizimlari

..... protokoli ulanishga asoslangan protokol bo'lib,  
internet orqali ma'lumotlarni almashinuvchi turli ilovalar  
uchun tarmoq ulanishlarini sozlashga yordam beradi. TCP  
.... protokolidan odatda o'yin va video ilovalar tomonidan  
keng foydalaniladi. UDP

Qaysi protokol ma'lumotni yuborishdan oldin aloqa  
o'rnatish uchun zarur bo'lgan manzil ma'lumotlari bilan  
ta'minlaydi. IP

Tarmoq taxdidlari necha turga bo'linadi 4

Qanday xujum asosiy hujumlarni oson amalga oshirish  
uchun tashkilot va tarmoq haqidagi axborotni to'plashni  
maqsad qiladi; Razvedka hujumlari

Qanday xujum hujumchi turli texnologiyalardan  
foydalangan holda tarmoqqa kirishga harakat qiladi Kirish  
hujumlari

Qanday xujum da hujumchi mijozlarga,  
foydalanuvchilaga va tashkilotlarda mavjud bo'lgan biror  
xizmatni cheklashga urinadi; Xizmatdan voz kechishga

undash (Denial of service, DOS) hujumlari

Qanday xujumdp zararli hujumlar tizim yoki tarmoqqa

bevosita va bilvosita ta'sir qiladi; Zararli hujumlar

Elektron raqamli imzo algoritmi qanday bosqichlardan

iborat bo'ladi? Imzo qo'yish va imzoni tekshirishdan

Imzoni haqiqiyligini tekshirish qaysi kalit yordamida

amalga oshiriladi? Imzo muallifining ochiq kaliti

yordamida

Tarmoq modeli-bu... Ikki hisoblash tizimlari orasidagi

aloqani ularning ichki tuzilmaviy va texnologik asosidan

qat'iy nazar muvaffaqiyatli o'rnatilishini asosidir

OSI modeli nechta sathga ajraladi? 7

Fizik sathning vazifasi nimadan iborat Qurilma, signal va

binar o'zgartirishlar

Ilova sathning vazifasi nimadan iborat Ilovalarni

tarmoqqa ulanish jarayoni

Kanal sathning vazifasi nimadan iborat Fizik manzillash

Tarmoq sathning vazifasi nimadan iborat Yo'lni aniqlash

va mantiqiy manzillash

TCP/IP modeli nechta sathdan iborat 4

Quyidagilarninf qaysi biri Kanal sathi protokollari

Ethernet, Token Ring, FDDI, X.25, Frame Relay, RS-232,

v.35.

Quyidagilarninf qaysi biri tarmoq sathi protokollari . IP,

ICMP, ARP, RARP

Quyidagilarninf qaysi biri transport sathi protokollari

TCP, UDP, RTP

Quyidagilarninf qaysi biri ilova sathi protokollari HTTP,

Telnet, FTP, TFTP, SNMP, DNS, SMTP va hak

TCP/IP modelining kanal sathiga OSI modelining qaysi

sathlari mos keladi Kanal, Fizik

TCP/IP modelining tarmoq sathiga OSI modelining qaysi

sathlari mos keladi Tarmoq

TCP/IP modelining transport sathiga OSI modelining

qaysi sathlari mos keladi Tramsport

TCP/IP modelining ilova sathiga OSI modelining qaysi

sathlari mos keladi llova, taqdimot, seans

Quyidagilardan lokal tarmoqqa berilgan ta’rifni belgilang.

Kompyuterlar va ularni bog’lab turgan qurilmalardan

iborat bo’lib, ular odatda bitta tarmoqda bo’ladi.

Quyidagilardan mintaqaviy tarmoqqa berilgan ta’rifni

belgilang. . Odatda ijaraga olingan telekommunikatsiya

liniyalaridan foydalanadigan tarmoqlardagi tugunlarni birbiriga bog’laydi.

Quyidagilardan MAN tarmoqqa berilgan ta’rifni

belgilang. Bu tarmoq shahar yoki shaharcha bo’ylab

tarmoqlarning o’zaro bog’lanishini nazarda tutadi

Quyidagilardan shaxsiy tarmoqqa berilgan ta’rifni

belgilang. Qisqa masofalarda qurilmalar o’rtasida

ma’lumot almashinish imkoniyatini taqdim etadi

Quyidagilardan qaysi biri tarmoqning yulduz

topologiyasiga berilgan Tarmoqda har bir kompyuter yoki

tugun markaziy tugunga individual bog’langan bo’ladi

Quyidagilardan qaysi biri tarmoqning shina

topologiyasiga berilgan Tarmoqda yagona kabel barcha

kompyuterlarni o’zida birlashtiradi

Quyidagilardan qaysi biri tarmoqning halqa

topologiyasiga berilgan Yuboriluvchi va qabul qilinuvchi

ma’lumot TOKYeN yordamida manziliga yetkaziladi

Quyidagilardan qaysi biri tarmoqning mesh

topologiyasiga berilgan Tarmoqdagi barcha kompyuter va

tugunlar bir-biri bilan o’zaro bog’langan bo’ladi

Tarmoq kartasi nima? Hisoblash qurilmasining ajralmas

qismi bo’lib, qurilmani tarmoqqa ulash imkoniyatini

taqdim etadi

Repetir nima? Odatda signalni tiklash yoki qaytarish

uchun foydalaniladi

Hub nima? Tarmoq qurilmasi bo’lib, ko’plab tarmoqlarni

ulash uchun yoki LAN segmentlarini bog’lash uchun

xizmat qiladi

Switch nima? Ko’plab tarmoqlarni ulash uchun yoki LAN

segmentlarini bog’lash uchun xizmat qiladi. Qabul

qilingan signalni barcha chiquvchi portlarga emas balki

paketda manzili keltirilgan portga uzatadi

Router nima? Qabul qilingan ma'lumotlarni tarmoq

sathiga tegishli manzillarga ko'ra (IP manzil) uzatadi

DNS tizimlari. Host nomlari va internet nomlarini IP

manzillarga o'zgartirish yoki teskarisini amalga oshiradi

TCP bu- ... Transmission Control Protocol

UDP bu-... User datagram protocol

Tarmoq xavfsizligiga tahdidlar tavsiflangan bandni

belgilang Ichki, tashqi

Tarmoq xavfsizligining buzilishi natijasida biznes

faoliyatining buzilishi qanday oqibatlarga olib keladi

Biznes jarayonlarni to'xtab qolishiga olib keladi

Tarmoq xavfsizligining buzilishi natijasida ishlab

chiqarishning yo'qolishi qanday oqibatlarga olib keladi

Hujum natijasida ishlab chiqarishi yo'qolgan hollarda uni

qayta tiklash ko'p vaqt talab qiladi va bu vaqtda ishlab

chiqarish to'xtab qoladi

Tarmoq xavfsizligining buzilishi natijasida maxfiylikni

yo'qolishi qanday oqibatlarga olib keladi Konfidensial

axborotni chiqib ketishi natijasida, tashkilot shaxsiy

ma'lumotlarini yo'qolishi mumkin

Tarmoq xavfsizligining buzilishi natijasida axborotning

o'g'irlanishi qanday oqibatlarga olib keladi Tashkilot

xodimlarining shaxsiy va ishga oid ma'ulmotlarini

kutilmaganda oshkor bo'lishi ushbu xodimlarga bevosita

ta'sir qiladi

Quyidagi ta'riflardan qaysi biri tarmoqning texnologik

zaifligini ifodalaydi Tarmoq qurilmalari, switch yoki

routerlardagi autentifikatsiya usullarining yetarlicha

bardoshli bo'lmasligi

Quyidagi ta'riflardan qaysi biri tarmoqning sozlanishdagi

zaifligini ifodalaydi tizim xizmatlarini xavfsiz bo'lmagan

tarzda sozlanishi, joriy sozlanish holatida qoldirish,

parollarni noto'g'ri boshqarilishi

Quyidagi ta'riflardan qaysi biri tarmoqning xavfsizlik

siyosatidagi zaifligini ifodalaydi. Xavfsizlik siyosatidagi



zaiflikni yuzaga kelishiga tashkilotning xavfsizlik

siyosatida qoidalar va qarshi choralarni noto'g'ri ishlab chiqilgani sabab bo'ladi.

Asosan tarmoq, tizim va tashkilot haqidagi axborot olish maqsadda amalga oshiriladigan tarmoq hujumi qaysi

Razvedka hujumlari

Ma'lumotlarni zaxira nusxalash bu – ... Muhim bo'lgan axborot nusxalash yoki saqlash jarayoni bo'lib, bu ma'lumot yo'qolgan vaqtda qayta tiklash imkoniyatini beradi

Zarar yetkazilgandan keyin tizimni normal ish holatiga qaytarish va tizimda saqlanuvchi muhim ma'lumotni yo'qolishidan so'ng uni qayta tiklash uchun qanday

amaldan foydalanamiz Zaxira nusxalash

Ma'lumotlarni inson xatosi tufayli yo'qolish sababiga ta'rif bering Qasddan yoki tasodifiy ma'lumotni o'chirib yuborilishi, ma'lumotlarni saqlash vositasini to'g'ri joylashtirilmagani yoki ma'lumotlar bazasini xatolik bilan boshqarilganligi.

Zahira nusxalash strategiyasi nechta bosqichni o'z ichiga oladi? 5

Zaxiralash uchun zarur axborotni aniqlash nechta bosqichda amalga oshiriladi. 4

Zaxira nusxalovchi vositalar tanlashdagi narx xuusiyatiga berilgan ta'rifni nelgilash Har bir tashkilot o'zining budjetiga mos bo'lgan zaxira nusxalash vositasiga ega bo'lishi shart.

RAID texnologiyasining transkripsiyasi qanday. Random Array of Independent Disks

RAID texnologiyasida nechta satx mavjud 6

OSI modelining birinchi sathi qanday nomlanadi Fizik sath

OSI modelining ikkinchi sathi qanday nomlanadi Kanal sathi

OSI modelining uchinchi sathi qanday nomlanadi Tarmoq sathi

OSI modelining oltinchi sathi qanday nomlanadi

Taqdimlash sathi

OSI modelining ettinchi sathi qanday nomlanadi Amaliy sath

Elektr signallarini qabul qilish va uzatish vazifalarini OSI modelining qaysi sathi bajaradi Fizik sath

Keltirilgan protokollarning qaysilari transport sathi protokollariga mansub TCP,UDP

OSI modelining fizik sathi qanday funktsiyalarni bajaradi

Elektr signallarini uzatish va qabul qilish

OSI modelining amaliy sathi qanday funktsiyalarni bajaradi Klient dasturlari bilan o'zaro muloqotda bo'lish

12 gacha bo'lgan va 12 bilan o'zaro tub bo'lgan sonlar soni nechta? 8 ta

Yevklid algoritmi qanday natijani beradi? Sonning eng katta umumiy bo'luvchisini topish

Qanday sonlar tub sonlar deb yuritiladi? Faqatgina 1 ga va o'ziga bo'linadigan sonlar tub sonlar deyiladi.

To'liq zaxiralash To'liq va o'sib boruvchi usullarning mujassamlashgan ko'rinishi bo'lib, oxirgi zaxiralangan nusxadan boshlab bo'lgan o'zgarishlarni zaxira nusxalab boradi. • Amalga oshirish to'liq zaxiralashga qaraganda tez amalga oshiriladi. • Qayta tikla

O'sib boruvchi zaxiralash Zaxiralangan ma'lumotga nisbatan o'zgarish yuz berganda zaxirilash amalga oshiriladi. • Oxirgi zaxira nusxalash sifatida ixtiyoriy zaxiralash usuli bo'lishi mumkin (to'liq saxiralashdan). •

Saqlash uchun kam hajm va amalga oshiris

Differensial zaxiralash Ushbu zaxiralashda tarmoqqa bog'lanishamalga oshiriladi. • Iliq zaxiralashda, tizim yangilanishi davomiy yangilanishni qabul qilish uchun ulanadi

Ushbu jarayon ma'lumot qanday yo'qolgani, ma'lumotni qayta tiklash dasturiy vositasi va ma'lumotni tiklash manzilini qayergaligiga bog'liq bo'ladi. Qaysi jarayon Ma'lumotlarni qayta tiklash

Antivirus dasturlarini ko'rsating? Drweb, Nod32,

Kaspersky

Wi-Fi tarmoqlarida quyida keltirilgan qaysi shifrlash

protokollaridan foydalaniladi wep, wpa, wpa2

Axborot himoyalangan qanday sifatlarga ega bo'lishi

kerak? ishonchli, qimmatli va to'liq

Axborotning eng kichik o'lchov birligi nima? bit

Virtual xususiy tarmoq – bu? VPN

Xavfli viruslar bu - ... kompyuter ishlashida jiddiy

nuqsonlarga sabab bo'luvchi viruslar

Mantiqiy bomba – bu ... Ma'lum sharoitlarda zarar

keltiruvchi harakatlarni bajaruvchi dastur yoki uning

alohida modullari

Rezident virus... tezkor xotirada saqlanadi

DIR viruslari nimani zararlaydi? FAT tarkibini zararlaydi

.... kompyuter tarmoqlari bo'yicha tarqalib,

komlg'yuterlarning tarmoqdagi manzilini aniqlaydi va u

yerda o'zining nusxasini qoldiradi «Chuvalchang» va

replikatorli virus

Mutant virus... shifrlash va deshifrlash algoritmlaridan

iborat- to'g'ri javob

Fire Wall ning vazifasi... tarmoqlar orasida aloqa

o'rnatish jarayonida tashkilot va Internet tarmog'i orasida

xavfsizlikni ta'minlaydi

Kompyuter virusi nima? maxsus yozilgan va zararli

dastur

Kompyuterning viruslar bilan zararlanish yo'llarini

ko'rsating disk, maxsus tashuvchi qurilma va kompyuter

tarmoqlari orqali

Troyan dasturlari bu... virus dasturlar

Kompyuter viruslari xarakterlariga nisbatan necha turga

ajraladi? 5

Antiviruslarni, qo'llanish usuliga ko'ra... turlari mavjud

detektorlar, faglar, vaktsinalar, privivkalar, revizorlar,

monitorlar

Axborotni himoyalash uchun ... usullari qo'llaniladi.

kodlashtirish, kriptografiya, stegonografiya

Stenografiya mahnosi... sirli yozuv

...sirli yozuvning umumiy nazariyasini yaratdiki, u fan sifatida stenografiyaning bazasi hisoblanadi K.Shennon

Kriptologiya yo'nalishlari nechta? 2

Kriptografiyaning asosiy maqsadi... maxfiylik, yaxlitlilikni ta'minlash

Zararli dasturiy vositalarni aniqlash turlari nechta 3

Signaiurana asoslangan ...bu fayldan topilgan bitlar qatori bo'lib, maxsus belgilarni o'z ichiga oladi. Bu o'rinda ularning xesh qiymatlari ham signatura sifatida xizmat qilishi mumkin.

O'zgarishni aniqlashga asoslangan Zararli dasturlar biror joyda joylashishi sababli, agar tizimdagi biror joyga o'zgarishni aniqlansa, u holda u zararlanishni ko'rsatishi mumkin

Anomaliyaga asoslangan Noodatiy yoki virusga o'xshash yoki potensial zararli harakatlari yoki xususiyatlarni topishni maqsad qiladi

Antiairuslar qanday usulda viruslarni aniqlaydi

Signaturaga asoslangan

Viruslar - o'zini o'zi ko'paytiradigan programma bo'lib, o'zini boshqa programma ichiga, kompyuterning yuklanuvchi sektoriga yoki hujjat ichiga biriktiradi

Rootkitlar- ushbu zararli dasturiy vosita operatsion tizim tomonidan aniqlanmasligi uchun ma'lum harakatlarini yashiradi

Backdoorlar - zararli dasturiy kodlar bo'lib, hujumchiga autentifikatsiyani amalga oshirmasdan aylanib o'tib tizimga kirish imkonini beradi, maslan, administrator parolisiz imtiyozga ega bo'lish

Troyan otlari- bir qarashda yaxshi va foydali kabi ko'rinuvchi dasturiy vosita sifatida ko'rinsada, yashiringan zararli koddan iborat bo'ladi

Ransomware- mazkur zararli dasturiy ta'minot qurbon kompyuterida mavjud qimmatli fayllarni shifrlaydi yoki

qulflab qo'yib, to'lov amalga oshirilishini talab qiladi  
Resurslardan foydalanish usuliga ko'ra viruslar qanday  
turlarga bo'linadi Virus parazit, Virus cherv  
Zararlagan obyektlar turiga ko'ra Dasturiy, yuklanuvchi,  
Makroviruslar, multiplatformali viruslar  
Faollashish prinsipiga ko'ra Resident, Norezident  
Dastur kodini tashkil qilish yondashuviga ko'ra  
Shifrlangan, shifrlanmagan, Polimorf  
Shifrlanmagan viruslar o'zini oddiy dasturlar kabi  
ko'rsatadi va bunda dastur kodida hech qanday  
qo'shimcha ishlashlar mavjud bo'lmaydi.

$P=31$ ,  $q=29$  eyler funksiyasida  $f(p,q)$  ni hisoblang 840  
 $256 \bmod 25 = ?$  6

bu yaxlit «butun»ni tashkil etuvchi bog'liq yoki o'zaro  
bog'langan tashkil etuvchilar guruhi nima deyiladi. Tizim  
Tashkilotni himoyalash maqsadida amalga oshirilgan  
xavfsizlik nazoratini tavsiflovchi yuqori sathli hujjat yoki  
hujjatlar to'plami nima deyiladi Xavfsizlik siyosati  
RSA shifrlash algoritmda foydalaniladigan sonlarning  
spektori o'lchami qanday?  $p$  va  $q$  –sonlarning  
ko'paytmasini ifodalovchi sonning spektoriga teng;  
DES algoritmi akslantirishlari raundlari soni qancha? 16;  
DES algoritmi shifrlash blokining chap va o'ng qism  
bloklarining o'lchami qancha? CHap qism blok 32 bit,  
o'ng qism blok 32 bit;

Simmetrik va asimmetrik shifrlash algoritmlarining  
qanday mohiyatan farqli tomonlari bor? SHifrlash va  
deshifrlash jarayonlari uchun kalitlarni generatsiya qilish  
qoidalariga ko'ra farqlanadi

19 gacha bo'lgan va 19 bilan o'zaro tub bo'lgan sonlar  
soni nechta? 18 ta

10 gacha bo'lgan va 10 bilan o'zaro tub bo'lgan sonlar  
soni nechta? 4 ta

Eyler funsiyasida (1) qiymati nimaga teng? 0

Eyler funksiyasida 60 sonining qiymatini toping. 59

Eyler funksiyasi yordamida 1811 sonining qiymatini

toping. 1810

97 tub sonmi? Tub

Quyidagi modulli ifodani qiymatini toping ( $148 + 14432$ )

mod 256. 244

Quyidagi sonlarning eng katta umumiy bo'luvchilarini

toping. 88 i 220 44

Quyidagi ifodani qiymatini toping.  $-17 \bmod 11$  5

2 soniga 10 modul bo'yicha teskari sonni toping.  $\emptyset$

Tashkilotning maqsadlari va vazifalari hamda xavfsizlikni

ta'minlash sohasidagi tadbirlar tavsiflanadigan yuqori

darajadagi reja nima? Kiberxavfsizlik siyosati

Kiberxavfsizlik siyosati tashkilotda nimani ta'minlaydi?

tashkilot masalalarini yechish himoyasini yoki ish

jarayoni himoyasini ta'minlaydi

Kiberxavfsizlikni ta'minlash masalalari bo'yicha

xavfsizlik siyosati shablonlarini ishlab chiqadigan

yetakchi tashkilotni aniqlang SANS (System

Administration Networking and Security)

Korxonaning davomli muvaffaqiyat bilan faoliyat

yuritishini ta'minlashga mo'ljallangan strukturalangan va

o'zaro bog'langan harakatlar to'plami- ... Strategiya

Tahdidlarning muvaffaqiyatli amalga oshirilishiga imkon

beruvchi har qanday omil – bu ... Zaiflik

ISO/IEC 27002:2005 – .... Axborot texnologiyasi.

Xavfsizlikni ta'minlash metodlari. Axborot xavfsizligini

boshqarishning amaliy qoidalari

O'zDStISO/IEC 27005:2013 – .... Axborot texnologiyasi.

Xavfsizlikni ta'minlash usullari. Axborot xavfsizligi

risklarini boshqarish

Axborot xavfsizligi arxitekturasining nechta satxi bor? 3

Rahbariy hujjat. Ma'lumotlar uzatish tarmog'ida axborot

xavfsizligini ta'minlash to'g'risida Nizom - Xujjat

raqamini toping RH 45-215:2009

Davlat hokimiyati va boshqaruv organlarining axborot

xavfsizligini ta'minlash dasturini ishlab chiqish tartibi -

Xujjat raqamini toping RH 45-185:2011

Davlat organlari saytlarini joylashtirish uchun  
provayderlar serverlari va texnik maydonlarning axborot  
xavfsizligini ta'minlash darajasini aniqlash tartibi - Xujjat  
raqamini toping RH 45-193:2007

Aloqa va axborotlashtirish sohasida axborot xavfsizligi.

Atamalar va ta'riflar - Xujjat raqamini toping TSt 45-  
010:2010

Quyidagilardan qaysi standart aloqa va axborotlashtirish  
sohasida axborot xavfsizligidagi asosiy atama va  
ta'riflarni belgilaydi? TSt 45-010:2010

Sub'ekt identifikatorini tizimga yoki talab qilgan  
sub'ektga taqdim qilish jarayoni nima? Identifikatsiya  
Foydalanuvchini (yoki biror tomonni) tizimdan  
foydalanish uchun ruxsati mavjudligini aniqlash jarayoni  
nima? Autentifikatsiya

Identifikatsiya va autentifikatsiyadan o'tgan  
foydalanuvchilarga tizimda bajarishi mumkin bo'lgan  
amallarga ruxsat berish jarayoni – nima deyiladi?

Avtorizatsiya

Identifikatsiya nima? Sub'ekt identifikatorini tizimga yoki  
talab qilgan sub'ektga taqdim qilish jarayoni

Autentifikatsiya nima? Foydalanuvchini (yoki biror  
tomonni) tizimdan foydalanish uchun ruxsati mavjudligini  
aniqlash jarayoni

Avtorizatsiya nima? Identifikatsiya va autentifikatsiyadan  
o'tgan foydalanuvchilarga tizimda bajarishi mumkin  
bo'lgan amallarga ruxsat berish jarayoni

... - Faqat foydalanuvchiga ma'lum va biror tizimda  
autentifikatsiya jarayonidan o'tishni ta'minlovchi biror  
axborot Parol

Smart karta o'lchamidagi, kichik xajmdagi xotira va  
xisoblash imkoniyatiga ega bo'lgan, o'zida parol yoki  
kalitni saqlovchi qurilma nima deb ataladi? Token,

Smartkarta

Smartkarta nima asosida autentifikatsiyalaydi? Something  
you have

Faqat bir marta foydalaniluvchi, xar bir sessiya uchun o'zgarib turadigan parol nima deyiladi? One-time password (OTP)

Foydalanuvchining tarmoqdagi harakatini, shu jumladan, uning resurslardan foydalanishga urinishini qayd etish nima deb ataladi? Ma'murlash

Amaldagi qonunchilikka mos ravishda texnik, dasturiy va dasturiy-texnik vositalar yordamida axborot xavfsizligining nokriptografik usullari bilan ta'minlashni inobatga oluvchi axborot himoyasi nima? Axborotning texnik himoyasi

Nazorat hududi – bu ... Qo'riqlanuvchi soha bo'lib, uning ichida kommunikatsiya qurilmalari hamda axborot tarmog'ining lokal tarkibiy qurilmalarini birlashtiruvchi barcha nuqtalar joylashadi

Texnik himoya vositalari – bu ... Texnik qurilmalar, komplekslar yoki tizimlar yordamida ob'ektni himoyalashdir

Bu axborotni tutib olish qurilmasi bo'lib, ularda uzatuvchi qurilma sifatida kontaktli mikrofonlardan foydalaniladi Stetoskoplar

Xesh funksiya to'g'ri ko'rsatilgan javobni aniqlang.

MD5

MD5, SHA1, Tiger xesh funktsiyalari uchun blok uzunligi necha baytga teng? 64 bayt

Sub'ektni ob'ektga ishlash qobiliyatini aniqlash – nima?

Foydalanishni boshqarish

Foydalanishni boshqarishda sub'ekt bu - .... Inson, dastur, jarayon

Foydalanishni boshqarishning qaysi usuli tizimdagi shaxsiy ob'ektlarni ximoyalash uchun qo'llaniladi?

Discretionary access control DAC

Foydalanishni boshqarishning qaysi usulidan asosan operatsion tizimlarda qo'llaniladi? Discretionary access control DAC

Foydalanishni boshqarishning qaysi usulida



foydalanishlar sub'ektlar va ob'ektlarni

klassifikatsiyalashga asosan boshqariladi? Mandatory

access control MAC

Foydalanishni boshqarishning qaysi usulida xavfsizlik

markazlashgan tarzda xavfsizlik siyosati m'muri

toimonidan amalga oshiriladi? Mandatory access control

MAC

Foydalanishni boshqarishning qaysi usulida xar bir

foydalanuvchini foydalanish ruxsatini belgilash o'rniga

rol uchun ob'ektlardan foydalanish ruxsatini ko'rsatish

yetarli bo'ladi? Role-based access control RBAC

Foydalanishni boshqarishning qaysi usulida sub'ekt va

ob'ektlarga tegishli xuquqlarni ma'murlash oson kechadi?

Role-based access control RBAC

Firibgarlikni oldini olish uchun bir shaxs toimonidan

ko'plab vazifalarni bajarishga ruxsat bermaslik zarur. Bu

muammo foydalanishni boshqarishni qaysi usulida

bartaraf etiladi? Role-based access control RBAC

Ob'ekt va sub'ektlarning attributlari, ular bilan mumkin

bo'lgan amallar va so'rovlarga mos keladigan muxit

uchun qoidalarni taxlil qilish asosida foydalanishni

boshqarish - .... Attribute based access control ABAC

Attribute based access control ABAC usuli attributlari

qaysilar? Foydalanuvchi attributlari, Resurs attributlari,

Ob'ekt va muxit attributlari

Foydalanishni boshqarishning qaysi usulida ruxsatlar va

xarakatni kim bajarayotganligi to'g'risidagi xolatlar

"agar, u xolda" buyrug'idan tashkil topgan qoidalarga

asoslanadi? Attribute based access control ABAC

XASML standart foydalanishni boshqarishning qaysi

usulida qo'llaniladi? Attribute based access control

ABAC

XASML standartida qoida nima? Maqsad, ta'sir, shart,

majburiyat va maslaxatlar

XASML standartida maqsad nima? Sub'ekt ob'ekt ustida

nima xarakat qilishi

Lampsonning foydalanishni boshqarish matritsasi

nimalardan tashkil topgan? Imtiyozlar ro'yxati

Access control list va Capability list bu nimaning asosiy elementi xisoblanadi? Lampson matritsasining

Lampson matritsasining satrlarida nima ifodalanadi?

Sub'ektlar

Foydalanishni boshqarishning mantiqiy vositalari

infratuzilma va uning ichidagi tizimlarda ... uchun

foydalaniladi. Mandat, Tasdiqlash, Avtorizatsiya

SHaxsiy simsiz tarmoq standartini aniqlang. Bluetooth,

IEEE 802.15, IRDA

Lokal simsiz tarmoq standartini aniqlang. IEEE 802.11,

Wi-Fi, HiperLAN

Regional simsiz tarmoq standartini aniqlang. IEEE

802.16, WiMAX

Global simsiz tarmoq standartini aniqlang. CDPD, 2G,

2.5G, 3G, 4G, 5G

Bluetooth, IEEE 802.15, IRDA standartida ishlovchi

simsiz tarmoq turini aniqlang. SHaxsiy simsiz tarmoq

IEEE 802.11, Wi-Fi, HiperLAN standartida ishlovchi

simsiz tarmoq turini aniqlang. Lokal simsiz tarmoq

IEEE 802.16, WiMAX standartida ishlovchi simsiz

tarmoq turini aniqlang. Regional simsiz tarmoq

CDPD, 2G, 2.5G, 3G, 4G, 5G standartida ishlovchi

simsiz tarmoq turini aniqlang. Global simsiz tarmoq

Bluetooth qanday chastota oralig'ida ishlaydi? 2.4-2.485

Ggts

Wi-Fi qanday chastota oralig'ida ishlaydi? 2.4-5 Ggts

WiMax tarmog'ining tezligi qancha? 1 Gbit/sekund

Quyidagilardan qaysi biri MITM xujumiga tegishli xattixarakat ximoblanadi? Aloqa seansini konfidentsialligini va yaxlitligini buzish

WiMAX tarmoq arxitekturasini nechta tashkil etuvchidan

iborat? 5

WiMAX tarmoq arxitekturasini qaysi tashkil etuvchidan

iborat? Base station, Subscriber station, Mobile station,

Relay station, Operator network

GSM raqamli mobil telefonlarining nechanchi avlodi  
uchun ishlab chiqilgan protokol? Ikkinchi avlodi  
GSM standarti qaysi tashkilot tomonidan ishlab  
chiqilgan? European telecommunications standards  
institute

.... – oʻzida IMSI raqamini, autentifikatsiyalash kaliti,  
foydalanuvchi maʼlumoti va xavfsizlik algoritmlarini  
saqlaydi. Sim karta

Rutoken S qurilmasining ogʻirligi qancha? 6.3 gramm  
True Crypt dasturi qaysi algoritmlardan foydalanib  
shifrlaydi? AES, Serpent, Twofish

Maʼlumotni saqlash vositalarida saqlangan maʼlumot  
konfidentsialligini aniqlash qaysi dasturiy shifrlash  
vositalarining vazifasi? Disc encryption software  
BestCrypt dasturi qaysi algoritmlardan foydalanib  
shifrlaydi? AES, Serpent, Twofish

AxCrypt dasturi qaysi algoritmlardan foydalanib  
shifrlaydi? AES-256

Qogʻoz koʻrinishidagi axborotlarni yoʻq qilish  
qurilmasining nomini kiriting. Shredder

Maʼlumotlarni bloklarga boʻlib, bir qancha (kamida  
ikkita) qattiq diskda rezerv nusxasini yozish qaysi  
texnologiya? RAID 0

Qaysi texnologiyada maʼlumotni koʻplab nusxalari bir  
vaqtda bir necha disklarga yoziladi? RAID 1

Qaysi texnologiyada maʼlumotlarni bir necha disklarda  
bayt satxida ajratilgan xolda yoziladi? RAID 3

Qaysi texnologiyada maʼlumotlarni bir necha disklarda  
bayt satxida ajratilgan xolda yoziladi va nazorat bitlari  
ham ular ichida taqsimlanadi? RAID 5

Disk zararlanganda “qaynoq almashtirish” yordamida uni  
almashtirish mumkin. Bu xususiyat qaysi texnologiyaga  
tegishli? RAID 50

Zaxiralashning qanday turlari mavjud? Toʻliq, oʻsib  
boruvchi, differentsial

IOS, Android, USB xotiralardan maʼlumotlarni tiklash

uchun qaysi dasturdan foydalaniladi? EASEUS Data

recovery wizard

Foydalanuvchi ma'lumotlarini qo'lga kirituvchi va uni

xujumchiga yuboruvchi dasturiy kod nima? Spyware

Operatsion tizim tomonidan aniqlanmasligi uchun

ma'lum xarakatlarni yashirish nima deyiladi? Rootkits

Qurbon kompyuterda mavjud qimmatli fayllarni

shifrlaydi yoki qulflab qo'yib to'lov amalga oshirishni

talab qiladi. Bu qaysi zararli dastur? Ransomware

Quyidagilardan o'zidan ko'payishi yo'q bo'lganlarini

belgilang. Mantiqiy bomba, Trojan oti, Backdoors

Viruslar resurslardan foydalanish usuliga ko'ra qanday

turlarga bo'linadi? Virus parazitlar, virus chervlar

Viruslar zararlangan ob'ektlar turiga ko'ra qanday

turlarga bo'linadi? Dasturiy, yuklanuvchi, makroviruslar,

ko'p platformali

Viruslar faollashish printsipiga ko'ra qanday turlarga

bo'linadi? Rezident, norezident

Viruslar dastur kodini tashkil qilish yondoshuviga ko'ra

qanday turlarga bo'linadi? SHifrlangan, shifrlanmagan,

polimorf

Dastlabki virus nechanchi yilda yaratilgan? 1988

ILOVEYOU virusi keltirgan zarar qancha? 10 mlrd.

Dollar

CodeRed virusi keltirgan zarar qancha? 2 mlrd. Dollar

Melissa virusi keltirgan zarar qancha? 80 million dollar

NetSky virusi keltirgan zarar qancha? 18 mlrd. Dollar

MyDoom virusi keltirgan zarar qancha? 38 mlrd. Dollar

Risk monitoring ..... ni paydo bo'lish imkoniyatini

aniqlaydi. Yangi risklar

..... riskni tutuvchi mos nazorat usuli amalga

oshirilganligini kafolatlaydi. Risk monitoring

Axborot xavfsizligi siyosatining necha hil turi bor? 3

Internetdan foydalanish siyosatining nechta turi mavjud?

4

Nomuntazam siyosat (Promiscuous Policy) nima? Tizim

resurslaridan foydalanishda hech qanday cheklovlar

qo'ymaydi

Paranoid siyosati (Paranoid Policy) – bu .... Hamma

narsa ta'qiqlanadi

Ruxsat berishga asoslangan siyosat (Permissive Policy) –

bu ... Faqat ma'lum hizmatlar/hujumlar/harakatlar

boklanadi

Ehtiyotkorlik siyosati (Prudent Policy) – bu .... Barcha

hizmatlar blokirovka qilingandan so'ng bog'lanadi

Tizim resurslaridan foydalanishda hech qanday

cheklovlar qo'ymaydi. Bu qaysi xavfsizlik siyosatiga hos?

Nomuntazam siyosat (Promiscuous Policy)

Barcha hizmatlar blokirovka qilingandan so'ng

bog'lanadi. Bu qaysi xavfsizlik siyosatiga hos?

Ehtiyotkorlik siyosati (Prudent Policy)

Faqat ma'lum hizmatlar/hujumlar/harakatlar boklanadi.

Bu qaysi xavfsizlik siyosatiga hos? Ruxsat berishga

asoslangan siyosat (Permissive Policy)

Hamma narsa ta'qiqlanadi. Bu qaysi xavfsizlik siyosatiga

hos? Paranoid siyosati (Paranoid Policy)

Tizim arxitekturasining turlari nechta? 5

Internet, havo hujumidan mudofaa, transport tizimlari

qaysi tizim arxitekturasiga xos? Hamkorlik tizimlari

arxitekturas

Cloud computing texnologiyasining nechta asosiy turi

mavjud? 3

Raqamli soatlar qaysi texnologiyaga tegishli? O'rnatilgan

tizimlar (Embedde systems)

Xavfsizlikning asosiy yo'nalishlarini sanab o'ting.

\*Axborot xavfsizligi, Iqtisodiy xavfsizlik, Mudofaa

xavfsizligi, Ijtimoiy xavfsizlik, Ekologik xavfsizlik

Axborot xavfsizligining asosiy maqsadlaridan biri- bu...

\*Axborotlarni o'g'irlanishini, yo'qolishini,

soxtalashtirilishini oldini olish

Konfidentsiallikga to'g'ri ta'rif keltiring. \*axborot

inshonchliligi, tarqatilishi mumkin emasligi, maxfiyligi

kafolati;

Yaxlitlikni buzilishi bu - ... \*Soxtalashtirish va o'zgartirish

... axborotni himoyalash tizimi deyiladi. \*Axborotning zaif tomonlarini kamaytiruvchi axborotga ruxsat etilmagan kirishga, uning chiqib ketishiga va yo'qotilishiga to'sqinlik qiluvchi tashkiliy, texnik, dasturiy, texnologik va boshqa vosita, usul va choralarning

Kompyuter virusi nima? \*maxsus yozilgan va zararli dastur

Axborotni himoyalash uchun ... usullari qo'llaniladi.

\*kodlashtirish, kriptografiya, stegonografiya

Stenografiya ma'nosi... \*sirli yozuv

Kriptografiyaning asosiy maqsadi... \*maxfiylik, yaxlitlikni ta'minlash

SMTP - Simple Mail Transfer protokol nima? \*elektron pochta protokoli

SKIP protokoli... \*Internet protokollari uchun kriptokalitlarning oddiy boshqaruvi

Kompyuter tarmog'ining asosiy komponentlariga nisbatan xavf-xatarlar... \*uzilish, tutib qolish, o'zgartirish, soxtalashtirish

...ma'lumotlar oqimini passiv hujumlardan himoya qilishga xizmat qiladi. \*konfidentsiallik

Foydalanish huquqini cheklovchi matritsa modeli bu...

\*Bella La-Padulla modeli

Kompyuter tarmoqlarida tarmoqning uzoqlashtirilgan elemenlari o'rtasidagi aloqa qaysi standartlar yordamida amalga oshiriladi? \*TCP/IP, X.25 protokollar

Himoya tizimi kompleksligiga nimalar orqali erishiladi?

\*Xuquqiy tashkiliy, muhandis, texnik va dasturiy matematik elementlarning mavjudligi orqali

Kalit – bu ... \*Matnni shifrlash va shifrini ochish uchun kerakli axborot

Qo'yish, o'rin almashtirish, gammalash kriptografiyaning

qaysi turiga bog'liq? \*simmetrik kriptotizimlar

Autentifikatsiya nima? \*Ma'lum qilingan foydalanuvchi, jarayon yoki qurilmaning haqiqiy ekanligini tekshirish muolajasi

Identifikatsiya bu- ... \*Foydalanuvchini uning identifikatori (nomi) bo'yicha aniqlash jarayoni

O'rin almashtirish shifri bu - ... \*Murakkab bo'lmagan kriptografik akslantirish

Simmetrik kalitli shifrlash tizimi necha turga bo'linadi. \*2 turga

Kalitlar boshqaruvi 3 ta elementga ega bo'lgan axborot almashinish jarayonidir bular ... \*hosil qilish, yig'ish, taqsimlash

Kriptologiya - \*axborotni qayta akslantirib himoyalash muammosi bilan shug'ullanadi

Kriptografiyada alifbo – \*axborot belgilarini kodlash uchun foydalaniladigan chekli to'plam

Simmetrik kriptotizimlarda ... jumlani davom ettiring  
\*shifrlash va shifrni ochish uchun bitta va aynan shu kalitdan foydalaniladi

Kriptobardoshlilik deb ... \*kalitlarni bilmasdan shifrni ochishga bardoshlilikni aniqlovchi shifrlash tavsifi

Elektron raqamli imzo deb – \*xabar muallifi va tarkibini aniqlash maqsadida shifrmatnga qo'shilgan qo'shimcha

Kriptografiya – \*axborotni qayta akslantirishning matematik usullarini izlaydi va tadqiq qiladi

Kriptografiyada matn – \*alifbo elementlarining tartiblangan to'plami

Kriptoanaliz – \*kalitlarni bilmasdan shifrni ochishga bardoshlilikni aniqlovchi shifrlash tavsifi

Shifrlash – \*akslantirish jarayoni: ochiq matn deb nomlanadigan matn shifrmatnga almashtiriladi

Kalit taqsimlashda ko'proq nimalarga e'tibor beriladi?  
\*Tez, aniq va maxfiyligiga

Faol hujum turi deb... \*Maxfiy uzatish jarayonini uzib qo'yish, modifikatsiyalash, qalbaki shifr ma'lumotlar

tayyorlash harakatlaridan iborat jarayon

Blokli shifrlash- \*shifrlanadigan matn blokiga

qo'llaniladigan asosiy akslantirish

Simmetrik kriptotizimning uzluksiz tizimida ... \*ochiq

matnning har bir harfi va simvoli alohida shifrlanadi

Kripto tizimga qo'yiladigan umumiy talablardan biri

\*shifr matn uzunligi ochiq matn uzunligiga teng bo'lishi

kerak

Berilgan ta'riflardan qaysi biri asimmetrik tizimlarga xos?

\*Asimmetrik kriptotizimlarda  $k_1 \neq k_2$  bo'lib,  $k_1$  ochiq

kalit,  $k_2$  yopiq kalit deb yuritiladi,  $k_1$  bilan axborot

shifrlanadi,  $k_2$  bilan esa deshifrlanadi

Yetarlicha kriptoturg'unlikka ega, dastlabki matn

simvollarini almashtirish uchun bir necha alfavitdan

foydalanishga asoslangan almashtirish usulini belgilang

\*Vijener matritsasi, Sesar usuli

Akslantirish tushunchasi deb nimaga aytiladi? \*1-

to'plamli elementlariga 2-to'plam elementalriga mos

bo'lishiga

Simmetrik guruh deb nimaga aytiladi? \*O'rin

almashtirish va joylashtirish

Qo'yish, o'rin almashtirish, garmalash kriptografiyaning

qaysi turiga bog'liq? \*simmetrik kriptosistemalar

Xavfli viruslar bu - ... \*kompyuter ishlashida jiddiy

nuqsonlarga sabab bo'luvchi viruslar

Mantiqiy bomba – bu ... \*Ma'lum sharoitlarda zarar

keltiruvchi harakatlarni bajaruvchi dastur yoki uning

aloqida modullari

Elektron raqamli imzo tizimi qanday muolajalarni amalga

oshiradi? \*raqamli imzoni shakllantirish va tekshirish

muolajasi

Shifrlashning kombinatsiyalangan usulida qanday

kriptotizimlarning kriptografik kalitlaridan foydalaniladi?

\*Simmetrik va asimmetrik

Axborot himoyasi nuqtai nazaridan kompyuter

tarmoqlarini nechta turga ajratish mumkin? \*Korporativ



va umumfoydalanuvchi

Elektromagnit nurlanish va ta'sirlanishlardan

himoyalaniş usullari nechta turga bo'linadi? \*Sust va faol

Internetda elektron pochta bilan ishlash uchun TCP/IPga asoslangan qaysi protokoldan foydalaniladi? \*SMTP, POP yoki IMAR

Axborot resursi – bu? \*axborot tizimi tarkibidagi elektron shakldagi axborot, ma'lumotlar banki, ma'lumotlar bazasi

Shaxsning, o'zini axborot kommunikatsiya tizimiga tanishtirish jarayonida qo'llaniladigan belgilar ketmaketligi bo'lib, axborot kommunikatsiya tizimidan foydalanish huquqiga ega bo'lish uchun

foydalaniluvchining maxfiy bo'lmagan qayd yozuvi – bu?

\*login

Uning egasi haqiqiylikini aniqlash jarayonida tekshiruv axboroti sifatida ishlatiladigan belgilar ketma-ketligi (maxfiy so'z) – bu? \*parol

Identifikatsiya jarayoni qanday jarayon? \* axborot tizimlari obyekt va subhektlariga uni tanish uchun nomlar (identifikator) berish va berilgan nom bo'yicha solishtirib uni aniqlash jarayoni

Autentifikatsiya jarayoni qanday jarayon? \*obyekt yoki subhektning unga berilgan identifikatorga mosligini tekshirish va belgilar ketmaketligidan iborat maxfiy kodini tekshirish orqali aslligini aniqlash

Avtorizatsiya jarayoni qanday jarayon?

\*foydalanuvchining resursdan foydalanish huquqlari va ruxsatlarini tekshirish jarayoni

Ro'yxatdan o'tish bu? \*foydalanuvchilarni ro'yxatga olish va ularga dasturlar va ma'lumotlarni ishlatishga huquq berish jarayoni

Axborot qanday sifatlarga ega bo'lishi kerak? \*ishonchli, qimmatli va to'liq

Axborotning eng kichik o'lchov birligi nima? \*bit

Elektron hujjatning rekvizitlari nechta qismdan iborat?

\*4

Axborotlarni saqllovchi va tashuvchi vositalar qaysilar?

\*fleshka, CD va DVD disklar

Imzo bu nima ? \*hujjatning haqiqiyligini va yuborgan fizik shaxsga tegishli ekanligini tasdiqlaydigan insonning fiziologik xususiyati.

Muhr bu nima? \*hujjatning haqiqiyligini va biror bir yuridik shaxsga tegishli ekanligini tasdiqlovchi isbotdir

DSA – nima \*Raqamli imzo algoritmi

El Gamal algoritmi qanday algoritm \*Shifrlash algoritmi va raqamli imzo algoritmi

Sezarning shifrlash sistemasining kamchiligi

\*Harflarning soʻzlarda kelish chastotasini yashirmaydi

Axborot xavfsizligi va xavfsizlik sanʼati haqidagi fan .... deyiladi? \*Kriptografiya

Tekstni boshqa tekst ichida maʼnosini yashirib keltirish bu - \*steganografiya

Shifrttekstni ochiq tekstga akslantirish jarayoni nima deb ataladi? \*Deshifrlash

..... – hisoblashga asoslangan bilim sohasi boʻlib, buzgʻunchilar mavjud boʻlgan sharoitda amallarni kafolatlash uchun oʻzida texnologiya, inson, axborot va jarayonni mujassamlashtirgan. \*Kiberxavfsizlik

Risk \*Potensial foyda yoki zarar

Tahdid nima?

\*Tashkilotga zarar yetkazishi mumkin boʻlgan istalmagan hodisa.

Kodlash nima? \*Maʼlumotni osongina qaytarish uchun hammaga

ochiq boʻlgan sxema yordamida maʼlumotlarni boshqa formatga oʻzgartirishdir

Shifrlash nima? Maʼlumotni osongina qaytarish uchun hammaga

ochiq boʻlgan sxema yordamida maʼlumotlarni boshqa formatga oʻzgartirishdir

Axborotni shifrnı ochish (deshifrlash) bilan qaysi fan

shug'ullanadi Kriptoanaliz

Qaysi juftlik RSA algoritmining ochiq va yopiq

kalitlarini ifodalaydi  $\{d, e\}$  – ochiq,  $\{e, n\}$  – yopiq;

Zamonaviy kriptografiya qanday bo'limlardan iborat?

Elektron raqamli imzo; kalitlarni boshqarish

Kriptografik usullardan foydalanishning asosiy

yo'nalishlari nimalardan iborat? uzatilyotgan xabarlarni

haqiqiylikni aniqlash

Shifr nima? \* Shifrlash va deshifrlashda foydalaniladigan

matematik funktsiyadan iborat bo'lgan kriptografik

algoritm

Ochiq kalitli kriptotizimlarning mohiyati nimadan iborat?

\*Ochiq kalitli kriptotizimlarda bir-biri bilan matematik

bog'langan 2 ta – ochiq va yopiq kalitlardan foydalaniladi

Oqimli shifrlashning mohiyati nimada? Oqimli shifrlash

birinchi navbatda axborotni bloklarga bo'lishning imkoni

bo'lmagan hollarda zarur,

Qandaydir ma'lumotlar oqimini har bir belgisini shifrlab,

boshqa belgilarini kutmasdan kerakli joyga jo'natish

uchun oqimli shifrlash zarur, Oqimli shifrlash algoritmlari

ma'lumotlarni bitlar yoki belgilar bo'yicha shifrlaydi

Simmetrik algoritmlarni xavfsizligini ta'minlovchi

omillarni ko'rsating. \*uzatilyotgan shifrlangan xabarni

kalitsiz ochish mumkin bo'lmashligi uchun algoritm yetarli

darajada bardoshli bo'lishi lozim, uzatilyotgan xabarni

xavfsizligi algoritmni maxfiyligiga emas

Kriptotizim qaysi komponentlardan iborat? \*ochiq

matnlar fazosi  $M$ , Kalitlar fazosi  $K$ ,

Shifmatnlar fazosi  $C$ ,  $E_k : M \rightarrow C$  (shifrlash uchun) va  $D_k :$

$C \rightarrow M$  (deshifrlash uchun) funktsiyalar

Asimmetrik kriptotizimlar qanday maqsadlarda

ishlatiladi? \*shifrlash, deshifrlash, ERI yaratish va

tekshirish, kalitlar almashish uchun

Kriptografik elektron raqamli imzolarda qaysi kalitlar

ma'lumotni yaxlitligini ta'minlashda ishlatiladi. \*ochiq

kalitlar

Xesh-funksiyaning natijasi ... Kiruvchi xabar uzunligidan

uzun xabar

RSA algoritmi qanday jarayonlardan tashkil topgan

\*Kalitni generatsiyalash; Shifrlash; Deshifrlash.

Ma'lumotlar butunligi qanday algoritmlar orqali amalga

oshiriladi \*Xesh funksiyalar

To'rtta bir-biri bilan bog'langan bog'lamlar strukturasi

(kvadrat shaklida) qaysi topologiya turiga mansub \*Xalqa

Qaysi topologiya birgalikda foydalanilmaydigan muhitni

qo'llamasligi mumkin? \*to'liq bog'lanishli

Kompyuterning tashqi interfeysi deganda nima

tushuniladi? \*kompyuter bilan tashqi qurilmani

bog'lovchi simlar va ular orqali axborot almashinish

qoidalar to'plamlari

Lokal tarmoqlarda keng tarqalgan topologiya turi qaysi?

\*Yulduz

Ethernet kontsentratori qanday vazifani bajaradi

\*kompyuterdan kelayotgan axborotni qolgan barcha

kompyuterga yo'naltirib beradi

OSI modelida nechta satx mavjud \*7

OSI modelining to'rtinchi satxi qanday nomlanadi

\*Transport satxi

OSI modelining beshinchi satxi qanday nomlanadi

\*Seanslar satxi

OSI modelining birinchi satxi qanday nomlanadi \*Fizik

satx

OSI modelining ikkinchi satxi qanday nomlanadi \*Kanal

satxi

OSI modelining uchinchi satxi qanday nomlanadi

\*Tarmoq satxi

OSI modelining oltinchi satxi qanday nomlanadi

\*Taqdimlash satxi

OSI modelining yettinchi satxi qanday nomlanadi

\*Amaliy satx

OSI modelining qaysi satxlari tarmoqqa bog'liq satxlar

hisoblanadi \*fizik, kanal va tarmoq satxlari

OSI modelining tarmoq satxi vazifalari keltirilgan

qurilmalarning qaysi birida bajariladi \*Marshrutizator

Elektr signallarini qabul qilish va uzatish vazifalarini OSI

modelining qaysi satxi bajaradi \*Fizik satx

Ma'lumotlarni uzatishning optimal marshrutlarini

aniqlash vazifalarini OSI modelining qaysi satxi bajaradi

\*Tarmoq satxi

Keltirilgan protokollarning qaysilari tarmoq satxi

protokollariga mansub \*IP, IPX

Keltirilgan protokollarning qaysilari transport satxi

protokollariga mansub \*TCP,UDP

OSI modelining fizik satxi qanday funksiyalarni bajaradi

\*Elektr signallarini uzatish va qabul qilish

OSI modelining amaliy satxi qanday funksiyalarni

bajaradi \*Klient dasturlari bilan o'zaro muloqotda bo'lish

Keltirilgan protokollarning qaysilari kanal satxi

protokollariga mansub \*Ethernet, FDDI

Keltirilgan protokollarning qaysilari taqdimlash satxi

protokollariga mansub \*SNMP, Telnet

Identifikatsiya, autentifikatsiya jarayonlaridan o'tgan

foydalanuvchi uchun tizimda bajarishi mumkin bo'lgan

amallarga ruxsat berish jarayoni bu... \*Avtorizatsiya

Autentifikatsiya faktorlari nechta 4

Faqat foydalanuvchiga ma'lum va biror tizimda

autentifikatsiya jarayonidan o'tishni ta'minlovchi biror

axborot nima Login

Ko'z pardasi, yuz tuzilishi, ovoz tembri- bular

autentifikatsiyaning qaysi faktoriga mos belgilar? Biron

nimaga egalik asosida

barcha kabel va tarmoq tizimlari; tizim va kabellarni fizik

nazoratlash; tizim va kabel uchun quvvat manbai; tizimni

madadlash muhiti. Bular tarmoqning qaysi satxiga kiradi?

\*Fizik satx

Fizik xavfsizlikda Yong'inga qarshi tizimlar necha turga

bo'linadi \*2

Avtorizatsiya tushunchasi odatda qaysi tushuncha bilan

sinonim sifatida ham foydalanadi? \*Foydalanishni

boshqarish

Foydalanishni boshqarish –bu... Subyektni Subyektga ishlash qobiliyatini aniqlashdir.

Foydalanishni boshqarishda inson, dastur, jarayon va xokazolar nima vazifani bajaradi? Obyekt

Foydalanishna boshqarishda ma'lumot , resurs, jarayon nima vazifani bajaradi ? \*Obyekt

Foydalanishna boshqarishning nechta usuli mavjud? \*4

Foydalanishni boshqarishning qaysi usulida tizimdagi shaxsiy Obyektlarni himoyalash uchun qo'llaniladi

ABAC

Foydalanishni boshqarishning qaysi modelida Obyekt egasining o'zi undan foydalanish huquqini va kirish turini o'zi belgilaydi ABAC

Foydalanishni boshqarishning qaysi usulida

foydalanishlar Subyektlar va Obyektlarni

klassifikatsiyalashga asosan boshqariladi. ABAC

Foydalanishni boshqarishning mandatli modelida

Obyektning xavfsizlik darajasi nimaga bog'liq..

Tashkilotda Obyektning muhimlik darajasi bilan yoki yuzaga keladigan foyda miqdori bilan bilan xarakterlanadi

MAC usuli bilan foydalanishni boshqarishda xavfsizlik markazlashgan holatda kim tomonidan amalga oshiriladi

\*xavfsizlik siyosati ma'muri

Agar Subyektning xavfsizlik darajasida Obyektning xavfsizlik darajasi mavjud bo'lsa, u holda uchun qanday amalga ruxsat beriladi Yozish

Agar Subyektning xavfsizlik darajasi Obyektning xavfsizlik darajasida bo'lsa, u holda qanday amalga ruxsat beriladi. \*Yozish

Foydalanishni boshqarishning qaysi modelida har bir

Obyekt uchun har bir foydalanuvchini foydalanish ruxsatini belgilash o'rniga, rol uchun Obyektlardan

foydalanish ruxsati ko'rsatiladi? ABAC

Rol tushunchasiga ta'rif bering. \*Muayyan faoliyat turi

bilan bog'liq harakatlar va majburiyatlar to'plami sifatida

belgilanishi mumkin

Foydalanishni boshqarishning qaysi usuli - Obyektlar va

Subyektlarning atributlari, ular bilan mumkin bo'lgan

amallar va so'rovlarga mos keladigan muhit uchun

qoidalarini tahlil qilish asosida foydalanishlarni

boshqaradi. \*ABAC

XACML foydalanishni boshqarishni qaysi usulining

standarti? \*ABAC

Biometrik autentifikatsiyalash usullari an'anaviy

usullarga nisbatan avfzalliklari qaysi javobda to'g'ri

ko'rsatilgan? \*barchasi

Axborotning kriptografik himoya vositalari necha turda?

4

Dasturiy shifrlash vositalari necha turga bo'linadi \*4

Diskni shifrlash nima uchun amalga oshiriladi?

\*Ma'lumotni saqlash vositalarida saqlangan ma'lumot

konfidensialligini ta'minlash uchun amalga oshiriladi

Ma'lumotlarni yo'q qilish odatda necha hil usulidan

foydalaniladi? 8

Kompyuter tarmoqlari bu – \*Bir biriga osonlik bilan

ma'lumot va resurslarni taqsimlash uchun ulangan

kompyuterlar guruhi

Tarmoq modeli –bu.. ikki

Matematik modellar to'plami

OSI modelida nechta tarmoq satxi bor \*7

OSI modeli 7 satxi bu \*Ilova

OSI modeli 1 satxi bu Ilova

OSI modeli 2 satxi bu Ilova

TCP/IP modelida nechta satx mavjud \*4

Qanday tarmoq qisqa masofalarda qurilmalar o'rtasida

ma'lumot almashinish imkoniyatini taqdim etadi? Lokal

Tarmoq kartasi bu... \*Hisoblash qurilmasining ajralmas

qismi bo'lib, qurilmani tarmoqqa ulash imkoniyatini

taqdim etadi.

Switch bu... Hisoblash qurilmasining ajralmas qismi

bo'lib, qurilmani tarmoqqa ulash imkoniyatini taqdim etadi.

Hab bu... Hisoblash qurilmasining ajralmas qismi bo'lib, qurilmani tarmoqqa ulash imkoniyatini taqdim etadi.

Tarmoq repiteri bu... Hisoblash qurilmasining ajralmas qismi bo'lib, qurilmani tarmoqqa ulash imkoniyatini taqdim etadi.

Qanday tizim host nomlari va internet nomlarini IP manzillarga o'zgartirish yoki teskarisini amalga oshiradi.

\*DNS tizimlari

..... protokoli ulanishga asoslangan protokol bo'lib, internet orqali ma'lumotlarni almashinuvchi turli ilovalar uchun tarmoq ulanishlarini sozlashga yordam beradi.

\*TCP

.... protokolidan odatda o'yin va video ilovalar tomonidan keng foydalaniladi. \*UDP

Qaysi protokol ma'lumotni yuborishdan oldin aloqa o'rnatish uchun zarur bo'lgan manzil ma'lumotlari bilan ta'minlaydi. TCP

Tarmoq taxdidlari necha turga bo'linadi 2

Qanday xujum asosiy hujumlarni oson amalga oshirish uchun tashkilot va tarmoq haqidagi axborotni to'plashni maqsad qiladi; \*Razvedka hujumlari

Qanday xujum hujumchi turli texnologiyalardan foydalangan holda tarmoqqa kirishga harakat qiladi

Razvedka hujumlari

Qanday xujum da hujumchi mijozlarga, foydalanuvchilarga va tashkilotlarda mavjud bo'lgan biror xizmatni cheklashga urinadi; Razvedka hujumlari

Qanday xujumdp zararli hujumlar tizim yoki tarmoqqa bevosita va bilvosita ta'sir qiladi; Razvedka hujumlari

RSA elektron raqamli imzo algoritmidagi ochiq kalit e qanday shartni qanoatlantirishi shart? \*e soni Eyler funksiyasi - bilan o'zaro tub

RSA elektron raqamli imzo algoritmidagi yopiq kalit d qanday hisoblanadi? Bu yerda p va q tub sonlar,  $n=pq$ , -



Eyler funksiyasi,e-ochiq kalit \*

Elektron raqamli imzo algoritmi qanday bosqichlardan iborat bo'ladi? \*Imzo qo'yish va imzoni tekshirishdan Imzoni haqiqiyligini tekshirish qaysi kalit yordamida amalga oshiriladi? \*Imzo muallifining ochiq kaliti yordamida

Tarmoq modeli-bu... \*Ikki hisoblash tizimlari orasidagi aloqani ularning ichki tuzilmaviy va texnologik asosidan qat'iy nazar

muvaffaqiyatli o'rnatilishini asosidir

OSI modeli nechta satxga ajraladi? 2

Fizik satxning vazifasi nimadan iborat \*Qurilma, signal va binar o'zgartirishlar

Ilova satxning vazifasi nimadan iborat Qurilma, signal va binar o'zgartirishlar

Kanal satxning vazifasi nimadan iborat Qurilma, signal va binar o'zgartirishlar

Tarmoq satxning vazifasi nimadan iborat Qurilma, signal va binar o'zgartirishlar

TCP/IP modeli nechta satxdan iborat \*4

Quyidagilarninf qaysi biri Kanal satxi protokollari

\*Ethernet, Token Ring, FDDI, X.25, Frame

Relay, RS-232, v.35.

Quyidagilarninf qaysi biri tarmoq satxi protokollari

Ethernet, Token Ring,FDDI, X.25, Frame

Relay, RS-232, v.35.

Quyidagilarninf qaysi biri transport satxi protokollari

Ethernet, Token Ring,FDDI, X.25, Frame

Relay, RS-232, v.35.

Quyidagilarninf qaysi biri ilova satxi protokollari

Ethernet, Token Ring,FDDI, X.25, Frame

Relay, RS-232, v.35.

TCP/IP modelining kanal satxiga OSI modelining qaysi satxlari mos keladi \*Kanal, Fizik

TCP/IP modelining tarmoq satxiga OSI modelining qaysi satxlari mos keladi Kanal, Fizik

TCP/IP modelining transport satxiga OSI modelining

qaysi satxlari mos keladi Kanal, Fizik

TCP/IP modelining ilova satxiga OSI modelining qaysi

satxlari mos keladi Kanal, Fizik

Quyidagilardan lokal tarmoqqa berilgan ta'rifni

belgilang. \*Kompyuterlar va ularni bog'lab turgan

qurilmalardan iborat bo'lib, ular odatda bitta tarmoqda

bo'ladi.

Quyidagilardan mintaqaviy tarmoqqa berilgan ta'rifni

belgilang. Kompyuterlar va ularni bog'lab turgan

qurilmalardan iborat bo'lib, ular odatda bitta tarmoqda

bo'ladi.

Quyidagilardan MAN tarmoqqa berilgan ta'rifni

belgilang. Kompyuterlar va ularni bog'lab turgan

qurilmalardan iborat bo'lib, ular odatda bitta tarmoqda

bo'ladi.

Quyidagilardan shaxsiy tarmoqqa berilgan ta'rifni

belgilang. Kompyuterlar va ularni bog'lab turgan

qurilmalardan iborat bo'lib, ular odatda bitta tarmoqda

bo'ladi.

Quyidagilardan qaysi biri tarmoqning yulduz

topologiyasiga berilgan \*Tarmoqda har bir kompyuter

yoki tugun Markaziy tugunga individual bog'langan

bo'ladi

Quyidagilardan qaysi biri tarmoqning shina

topologiyasiga berilgan Tarmoqda har bir kompyuter yoki

tugun markaziy tugunga individual bog'langan bo'ladi

Quyidagilardan qaysi biri tarmoqning halqa

topologiyasiga berilgan Tarmoqda har bir kompyuter yoki

tugun markaziy tugunga individual bog'langan bo'ladi

Quyidagilardan qaysi biri tarmoqning mesh

topologiyasiga berilgan Tarmoqda har bir kompyuter yoki

tugun markaziy tugunga individual bog'langan bo'ladi

Tarmoq kartasi nima? \*Hisoblash qurilmasining ajralmas

qismi bo'lib, qurilmani tarmoqqa ulash imkoniyatini

taqdim etadi

Repetir nima? Hisoblash qurilmasining ajralmas qismi bo'lib, qurilmani tarmoqqa ulash imkoniyatini taqdim etadi

Hub nima? Hisoblash qurilmasining ajralmas qismi bo'lib, qurilmani tarmoqqa ulash imkoniyatini taqdim etadi

Switch nima? Hisoblash qurilmasining ajralmas qismi bo'lib, qurilmani tarmoqqa ulash imkoniyatini taqdim etadi

Router nima? Hisoblash qurilmasining ajralmas qismi bo'lib, qurilmani tarmoqqa ulash imkoniyatini taqdim etadi

DNS tizimlari. \*Host nomlari va internet nomlarini IP manzillarga o'zgartirish yoki teskarisini amalga oshiradi

TCP bu- ... \*Transmission Control Protocol

UDP bu-... User domain protocol

IP protokolining necha xil versiyasi mavjud? 1

Tarmoq xavfsizligiga tahdidlar tavsiflangan bandni belgilang \*Ichki, tashqi

Tarmoq xavfsizligining buzilishi natijasida biznes faoliyatining buzilishi qanday oqibatlarga olib keladi

\*Biznes jarayonlarni to'xtab qolishiga olib keladi

Tarmoq xavfsizligining buzilishi natijasida ishlab chiqarishning yo'qolishi qanday oqibatlarga olib keladi

Biznesda ixtiyoriy hujum biznes jarayonlarni to'xtab qolishiga olib keladi

Tarmoq xavfsizligining buzilishi natijasida maxfiylikni yo'qolishi qanday oqibatlarga olib keladi  
Biznesda ixtiyoriy hujum biznes jarayonlarni to'xtab qolishiga olib keladi

Tarmoq xavfsizligining buzilishi natijasida axborotning o'g'irlanishi qanday oqibatlarga olib keladi  
Biznesda ixtiyoriy hujum biznes jarayonlarni to'xtab qolishiga olib keladi

Quyidagi ta'riflardan qaysi biri tarmoqning texnologik zaifligini ifodalaydi \*Tarmoq qurilmalari, switch yoki

routerlardagi autentifikatsiya

usullarining yetarlicha bardoshli bo'lmashligi

Quyidagi ta'riflardan qaysi biri tarmoqning sozlanishdagi

zaifligini ifodalaydi Tarmoq qurilmalari, switch yoki

routerlardagi autentifikatsiya

usullarining yetarlicha bardoshli bo'lmashligi

Quyidagi ta'riflardan qaysi biri tarmoqning xavfsizlik

siyosatidagi zaifligini ifodalaydi. Tarmoq qurilmalari,

switch yoki routerlardagi autentifikatsiya usullarining

yetarlicha bardoshli bo'lmashligi

Asosan tarmoq, tizim va tashkilot haqidagi axborot olish

maqsadda amalga oshiriladigan tarmoq hujumi qaysi

\*Razvedka hujumlari

Razvedka hujumiga berilgan ta'rifni aniqlang \*Asosiy

hujumlarni oson amalga oshirish uchun tashkilot va

tarmoq haqidagi axborotni to'plashni maqsad qiladi;

Kirish hujumiga berilgan ta'rifni aniqlang asosiy

hujumlarni oson amalga oshirish uchun tashkilot va

tarmoq haqidagi axborotni to'plashni maqsad qiladi;

DOS hujumiga berilgan ta'rifni aniqlang asosiy

hujumlarni oson amalga oshirish uchun tashkilot va

tarmoq haqidagi axborotni to'plashni maqsad qiladi;

Zararli hujumga berilgan ta'rifni aniqlang asosiy

hujumlarni oson amalga oshirish uchun tashkilot va

tarmoq haqidagi axborotni to'plashni maqsad qiladi;

Razvetka hujumari necha turga bo'linadi 1

Qaysi hujum jarayoni TCP/IP tarmog'ida paketlarni tutib

olish, dekodlash, tekshirish va tarjima qilishni o'z ichiga

oladi \*Paketlarni snifferlash

Tarmoqlaro ekranni OSI modeli bo'yicha qanday

turlarga bo'lindi? \*• paket filterlari tarmoq satxida

ishlaydi; ekspert paketi filterlari – transport sahida

ishlaydi; ilova proksilari – ilova satxida

Tarmoqlaro ekranni foydalanilgan texnologiyasi

bo'yicha qanday turlarga bo'lindi? paket filterlari tarmoq

satxida ishlaydi; ekspert paketi filterlari – transport sahida

ishlaydi; ilova proksilari – ilova satxida

Tarmoqlaro ekranni bajarilishiga ko'ra qanday turlarga bo'lindi? paket filterlari tarmoq satxida ishlaydi; ekspert paketi filterlari – transport sahida ishlaydi; ilova proksilari – ilova satxida

Tarmoqlaro ekranni ulanish sxemasi bo'yicha qanday turlarga bo'lindi? paket filterlari tarmoq satxida ishlaydi; ekspert paketi filterlari – transport sahida ishlaydi; ilova proksilari – ilova satxida

Paket filterlari tarmoqlararo ekrani vazifasi nima?

\*Tarmoq satxida paketlarni

tahlillashga asoslan;

Ilova proksilari tarmoqlararo ekrani vazifasi nima?

Tarmoq satxida paketlarni tahlillashga asoslan;

Ekspert paket filterlari tarmoqlararo ekrani vazifasi nima?

Tarmoq satxida paketlarni tahlillashga asoslan;

Quyidagilardan qaysi biri paket filterlari tarmoqlararo ekrani kamchiligini ifodalaydi. \*Bu turdagi tarmoqlararo ekran TCP aloqani tekshirmaydi. Ilova satxi ma'lumotlarni, zararli dasturlarni va hak. tekshirmaydi.

Quyidagilardan qaysi biri ekspert paket filterlari tarmoqlararo ekrani kamchiligini ifodalaydi. Bu turdagi tarmoqlararo ekran TCP aloqani tekshirmaydi. Ilova satxi ma'lumotlarni, zararli dasturlarni va hak. tekshirmaydi.

Simsiz tarmoqlarning nechta turi mavjud 5

Bluetooth qanday simsiz tarmoq turiga kiradi. Global

Wifi qanday simsiz tarmoq turiga kiradi. Global

LTE, CDMA, HSDPA qanday simsiz tarmoq turiga kiradi. \*Global

WiMAX qanday simsiz tarmoq turiga kiradi. Global

Bluetooth texnologiyasida autentifikatsiya bu... Ikki autentifikatsiyalangan tarmoqda ma'lumotni almashinish jarayonida tinglashdan va uchunchi tomondan bo'ladigan hujumlardan himoyalash uchun shifrlash amalga oshirish.

Bluetooth texnologiyasida konfidensiallik bu... \*Ikki

autentifikatsiyalangan tarmoqda ma’ulmotni almashinish jarayonida tinglashdan va uchunchi tomondan bo’ladigan hujumlardan himoyalash uchun shifrlash amalga oshirish.

Bluetooth texnologiyasida avtorizatsiya bu... Ikki

autentifikatsiyalangan tarmoqda ma’ulmotni almashinish jarayonida tinglashdan va uchunchi tomondan bo’ladigan hujumlardan himoyalash uchun shifrlash amalga oshirish.

GSM bu ..- \*Global System for Mobile Communications

Simsiz tarmoq Bluetooth ishlash rejimlari nechta? 2

Kompyuterda hodisalar haqidagi ma’lumot qayerda saqlanadi? \*hodisalar jurnaliga

Windows operatsion tizimida xatolik hodisasiga berilgan ta’rifni belgilang. \*Ma’lumotni yo’qotish yoki

funksionallikni yo’qotish kabi muhim muammoni ko’rsatadigan voqea. Masalan, agar xizmat ishga tushirish paytida yuklana olmasa, xatolik hodisasi qayd

Windows operatsion tizimida ogohlantirish hodisasiga berilgan ta’rifni belgilang. Ma’lumotni yo’qotish yoki funksionallikni yo’qotish kabi muhim muammoni ko’rsatadigan voqea. Masalan, agar xizmat ishga tushirish paytida yuklana olmasa, xatolik hodisasi

Windows operatsion tizimida axborot hodisasiga berilgan ta’rifni belgilang. Ma’lumotni yo’qotish yoki funksionallikni yo’qotish kabi muhim muammoni ko’rsatadigan voqea. Masalan, agar xizmat ishga tushirish paytida yuklana olmasa, xatolik hodisasi qayd

Windows operatsion tizimida muvaffaqiyatli audit hodisasiga berilgan ta’rifni belgilang. Ma’lumotni yo’qotish yoki funksionallikni yo’qotish kabi muhim muammoni ko’rsatadigan voqea. Masalan, agar xizmat ishga tushirish paytida yuklana olmasa, xatolik ho

Windows operatsion tizimida muvaffaqiyatsiz audit hodisasiga berilgan ta’rifni belgilang. Ma’lumotni yo’qotish yoki funksionallikni yo’qotish kabi muhim muammoni ko’rsatadigan voqea. Masalan, agar xizmat ishga tushirish paytida yuklana olmasa, xatolik

Ma'lumotlarni zaxira nusxalash bu – ...

\*Muhim bo'lgan axborot nusxalash yoki saqlash jarayoni bo'lib, bu ma'lumot yo'qolgan vaqtda qayta tiklash imkoniyatini beradi

Zarar yetkazilgandan keyin tizimni normal ish holatiga qaytarish va tizimda saqlanuvchi muhim ma'lumotni yo'qolishidan so'ng uni qayta tiklash uchun qanday amaldan foydalanamiz \*Zaxira nusxalash

Ma'lumotlarni inson xatosi tufayli yo'qolish sababiga ta'rif bering \*Qasddan yoki tasodifiy ma'lumotni o'chirib yuborilishi, ma'lumotlarni saqlash vositasini to'g'ri joylashtirilmagani yoki ma'lumotlar bazasini xatolik bilan boshqarilganligi.

Ma'lumotlarni g'arazli hatti harakatlar yo'qolish sababiga ta'rif bering Qasddan yoki tasodifiy ma'lumotni o'chirib yuborilishi, ma'lumotlarni saqlash vositasini to'g'ri joylashtirilmagani yoki ma'lumotlar bazasini xatolik bilan boshqarilganligi.

Ma'lumotlarni tasodifiy sabablar tufayli yo'qolish sababiga ta'rif bering Qasddan yoki tasodifiy ma'lumotni o'chirib yuborilishi, ma'lumotlarni saqlash vositasini to'g'ri joylashtirilmagani yoki ma'lumotlar bazasini xatolik bilan boshqarilganligi.

Ma'lumotlarni tabiiy ofatlar tufayli yo'qolish sababiga ta'rif bering Qasddan yoki tasodifiy ma'lumotni o'chirib yuborilishi, ma'lumotlarni saqlash vositasini to'g'ri joylashtirilmagani yoki ma'lumotlar bazasini xatolik bilan boshqarilganligi.

Zahira nusxalash strategiyasi nechta bosqichni o'z ichiga oladi? 7

Zaxiralash uchun zarur axborotni aniqlash nechta bosqichda amalga oshiriladi. \*4

Zaxira nusxalovchi vositalar tanlashdagi narx xususiyatiga berilgan ta'rifni nelgilash \*Har bir tashkilot o'zining budjetiga mos bo'lgan zaxira nusxalash vositasiga ega bo'lishi shart.

Zaxira nusxalovchi vositalar tanlashdagi ishonchlilik  
xususiyatiga berilgan ta'rifni aniqlash Har bir tashkilot  
o'zining budjetiga mos bo'lgan zaxira nusxalash  
vositasiga ega bo'lishi shart.

Zaxira nusxalovchi vositalar tanlashdagi tezlik  
xususiyatiga berilgan ta'rifni aniqlash Har bir tashkilot  
o'zining budjetiga mos bo'lgan zaxira nusxalash  
vositasiga ega bo'lishi shart.

Zaxira nusxalovchi vositalar tanlashdagi  
foydalanuvchanlik xususiyatiga berilgan ta'rifni aniqlash  
Har bir tashkilot o'zining budjetiga mos bo'lgan zaxira  
nusxalash vositasiga ega bo'lishi shart.

Zaxira nusxalovchi vositalar tanlashdagi qulaylik  
xususiyatiga berilgan ta'rifni aniqlash Har bir tashkilot  
o'zining budjetiga mos bo'lgan zaxira nusxalash  
vositasiga ega bo'lishi shart.

RAID texnologiyasining transkripsiyasi qanday.

Redundant Array of Independent Disks

RAID texnologiyasida nechta satx mavjud 3

RAID 0: diskni navbatlanishi bu-.. \*Ma'lumotni  
bloklarga bo'lib, bir qancha qattiq diskda ularni yozadi, U  
IO unumdorligini yuklamani ko'plab kanal va disk  
drayverlariga bo'lish orqali yaxshilaydi. Agar disk  
buzilsa, ma'lumotni tiklab bo'lmaydi. • Kamida ikkita

RAID 1: diskni navbatlanishi bu-.. Ma'lumotni bloklarga  
bo'lib, bir qancha qattiq diskda ularni yozadi, U IO  
unumdorligini yuklamani ko'plab kanal va disk  
drayverlariga bo'lish orqali yaxshilaydi.

Agar disk buzilsa, ma'lumotni tiklab bo'lmaydi. • Kamida  
ikkita disk talab qilinadi

RAID 3: diskni navbatlanishi bu-.. Ma'lumotni bloklarga  
bo'lib, bir qancha qattiq diskda ularni yozadi, U IO  
unumdorligini yuklamani ko'plab kanal va disk  
drayverlariga bo'lish orqali yaxshilaydi.

Agar disk buzilsa, ma'lumotni tiklab bo'lmaydi. • Kamida  
ikkita disk talab qilinadi



RAID 5: diskni navbatlanishi bu-.. Ma'lumotni bloklarga bo'lib, bir qancha qattiq diskda ularni yozadi, U IO unumdorligini yuklamani ko'plab kanal va disk drayverlariga bo'lish orqali yaxshilaydi.

Agar disk buzilsa, ma'lumotni tiklab bo'lmaydi. • Kamida ikkita disk talab qilinadi

RAID 10: diskni navbatlanishi bu-.. \*Gibrid satx bo'lib, RAID 1 va RAID 0

satxlaridan iborat va kamida 4 ta diskni talab etadi

RAID 50: diskni navbatlanishi bu-.. Gibrid satx bo'lib, RAID 1 va RAID 0

satxlaridan iborat va kamida 4 ta diskni talab etadi

Ma'lumotlarni nusxalash usullari necha xil usulda amalga oshiriladi? \*3

Issiq zaxiralash usuliga berilgan ta'rifni belgilang.

\*Ushbu usulda foydalanuvchi tizimni boshqarayotgan vaqtda ham zaxira nusxalash jarayoni davom ettiriladi.

Mazkur zaxiralash usulini amalga oshirish tizimni harakatsiz vaqtini kamaytiradi.

Iliq zaxiralash usuliga berilgan ta'rifni belgilang. Ushbu usulda foydalanuvchi tizimni boshqarayotgan vaqtda ham zaxira nusxalash jarayoni davom ettiriladi.

Mazkur zaxiralash usulini amalga oshirish tizimni harakatsiz vaqtini kamaytiradi.

Sovuq zaxiralash usuliga berilgan ta'rifni belgilang.

Ushbu usulda foydalanuvchi tizimni boshqarayotgan vaqtda ham zaxira nusxalash jarayoni davom ettiriladi.

Mazkur zaxiralash usulini amalga oshirish tizimni harakatsiz vaqtini kamaytiradi.

Ichki zahiralash qanday amalga oshiriladi Ichki zahiralashda mahalliy yoki global serverlardan foydalaniladi

OSI modelining birinchi satxi qanday nomlanadi \*Fizik satx

OSI modelining ikkinchi satxi qanday nomlanadi \*Kanal satxi

OSI modelining uchinchi satxi qanday nomlanadi

\*Tarmoq satxi

OSI modelining oltinchi satxi qanday nomlanadi

\*Taqdimlash satxi

OSI modelining ettinchi satxi qanday nomlanadi

\*Amaliy satx

Elektr signallarini qabul qilish va uzatish vazifalarini

OSI modelining qaysi satxi bajaradi \*Fizik satx

Keltirilgan protokollarning qaysilari transport satxi

protokollariga mansub \*TCP,UDP

OSI modelining fizik satxi qanday funktsiyalarni

bajaradi \*Elektr signallarini uzatish va qabul qilish

OSI modelining amaliy satxi qanday funktsiyalarni

bajaradi \*Klient dasturlari bilan o'zaro muloqotda bo'lish

12 gacha bo'lgan va 12 bilan o'zaro tub bo'lgan sonlar

soni nechta? 6 ta

Yevklid algoritmi qanday natijani beradi? \*Sonning eng

katta umumiy bo'luvchisini topish

Qanday sonlar tub sonlar deb yuritiladi? \*Faqatgina 1 ga

va o'ziga bo'linadigan sonlar tub sonlar deyiladi.

To'liq zaxiralash Tiklashning tezligi yuqori. axira

nusxalash jarayonining sekin va ma'lumotni saqlash

uchun ko'p hajm talab etadi

O'sib boruvchi zaxiralash Tiklashning tezligi yuqori.

Zaxira nusxalash jarayonining sekin va ma'lumotni

saqlash uchun ko'p hajm talab etadi

Differensial zaxiralash Tiklashning tezligi yuqori. Zaxira

nusxalash jarayonining sekin va ma'lumotni saqlash

uchun ko'p hajm talab etadi

Ushbu jarayon ma'lumot qanday yo'qolgani, ma'lumotni

qayta tiklash dasturiy vositasi va ma'lumotni tiklash

anzilini qayergaligiga bog'liq bo'ladi. Qaysi jarayon

Ma'lumotlarni qayta tiklash

Antivirus dasturlarini ko'rsating? \*Drweb, Nod32,

Kaspersky

Wi-Fi tarmoqlarida quyida keltirilgan qaysi shifrlash

protokollaridan foydalaniladi \*wep, wpa, wpa2

Axborot himoyalangan qanday sifatlarga ega bo'lishi

kerak? \*ishonchli, qimmatli va to'liq

Axborotning eng kichik o'lchov birligi nima? \*bit

Virtual xususiy tarmoq – bu? \*VPN

Xavfli viruslar bu - ... \*kompyuter ishlashida jiddiy

nuqsonlarga sabab bo'luvchi viruslar

Mantiqiy bomba – bu ... \*Ma'lum sharoitlarda zarar

keltiruvchi harakatlarni bajaruvchi dastur yoki uning

alohida modullari

Rezident virus... \*tezkor xotirada saqlanadi

DIR viruslari nimani zararlaydi? \*FAT tarkibini

zararlaydi

.... kompyuter tarmoqlari bo'yicha tarqalib,

kompyuterning tarmoqdagi manzilini aniqlaydi va u yerda

o'zining nusxasini qoldiradi \*«Chuvalchang» va

replikatorli virus

Mutant virus... \*shifrlash va deshifrlash algoritmlaridan

iborat

Fire Wall ning vazifasi... \*tarmoqlar orasida aloqa

o'rnatish jarayonida tashkilot va Internet tarmog'i orasida

xavfsizlikni ta'minlaydi

Kompyuter virusi nima? \*maxsus yozilgan va zararli

dastur

Kompyuterning viruslar bilan zararlanish yo'llarini

ko'rsating \*disk, maxsus tashuvchi qurilma va kompyuter

tarmoqlari orqali

Troyan dasturlari bu... \*virus dasturlar

Kompyuter viruslari xarakterlariga nisbatan necha turga

ajraladi? \*5

Antiviruslarni, qo'llanish usuliga ko'ra... turlari mavjud

\*detektorlar, faglar, vaksinalar, privivkalar, revizorlar,

monitorlar

Axborotni himoyalash uchun ... usullari qo'llaniladi.

\*kodlashtirish, kriptografiya, stegonografiya

Stenografiya mahnosi... \*sirli yozuv

...sirli yozuvning umumiy nazariyasini yaratdiki, u fan  
sifatida stenografiyaning bazasi hisoblanadi \*K.Shennon  
Kriptologiya yo'nalishlari nechta? \*2  
Kriptografiyaning asosiy maqsadi... \*maxfiylik,  
yaxlitlilikni ta'minlash  
Zararli dasturiy vositalarni aniqlash turlari nechta \*3  
Signaiurana asoslangan \*....bu fayldan topilgan bitlar  
qatori bo'lib, maxsus belgilarni o'z ichiga oladi. Bu  
o'rinda ularning xesh  
qiymatlari ham signatura sifatida xizmat qilishi mumkin.  
O'zgarishni aniqlashga asoslangan ....bu fayldan topilgan  
bitlar qatori bo'lib, maxsus belgilarni o'z ichiga oladi. Bu  
o'rinda ularning xesh  
qiymatlari ham signatura sifatida xizmat qilishi mumkin.  
Anomaliyaga asoslangan ....bu fayldan topilgan bitlar  
qatori bo'lib, maxsus belgilarni o'z ichiga oladi. Bu  
o'rinda ularning xesh  
qiymatlari ham signatura sifatida xizmat qilishi mumkin.  
Antiairuslar qanday usulda viruslarni aniqlaydi  
Anomaliyaga asoslangan  
Viruslar - bir qarashda yaxshi va foydali kabi ko'rinuvchi  
dasturiy vosita sifatida ko'rinsada, yashiringan zararli  
koddan iborat bo'ladi  
Rootkitlar- bir qarashda yaxshi va foydali kabi  
ko'rinuvchi dasturiy vosita sifatida ko'rinsada,  
yashiringan zararli koddan iborat bo'ladi  
Backdoorlar - bir qarashda yaxshi va foydali kabi  
ko'rinuvchi dasturiy vositasifatida ko'rinsada, yashiringan  
zararli koddan iborat bo'ladi  
Trojan otlari- \*bir qarashda yaxshi va foydali kabi  
ko'rinuvchi dasturiy vosita sifatida ko'rinsada,  
yashiringan zararli koddan iborat bo'ladi  
Ransomware- bir qarashda yaxshi va foydali kabi  
ko'rinuvchi dasturiy vosita sifatida ko'rinsada,  
yashiringan zararli koddan iborat bo'ladi  
Resurslardan foydalanish usuliga ko'ra viruslar qanday

turlarga bo'linadi \*Virus parazit, Virus cherv

Zararlagan obyektlar turiga ko'ra Virus parazit, Virus cherv

Faollashish prinsipiga ko'ra Virus parazit, Virus cherv

Dastur kodini tashkil qilish yondashuviga ko'ra Virus parazit, Virus cherv

Shifrlanmagan viruslar \*o'zini oddiy dasturlar kabi

ko'rsatadi va bunda dastur kodida hech qanday

qo'shimcha ishlashlar mavjud bo'lmaydi.

Shifrlangan viruslar o'zini oddiy dasturlar kabi ko'rsatadi

va bunda dastur kodida hech qanday qo'shimcha

ishlashlar mavjud bo'lmaydi.

Polimorf viruslar o'zini oddiy dasturlar kabi ko'rsatadi va

bunda dastur kodida hech qanday qo'shimcha ishlashlar

mavjud bo'lmaydi.

Dasturiy viruslar-... bir vaqtning o'zida turli xildagi

Obyektlarni

zararlaydi. Masalan, OneHalf.3544 virusi ham MS-DOS

dasturlari ham qattiq diskning yuklanuvchi sektorlarini

zararlasa, Anarchy oilasiga tegishli viruslar MS-DOS va

Windows dasturlaridan tashqari, MS Word hujjatlarini

ham zararlay oladi.

Ko'p platformali viruslar \*bir vaqtning o'zida turli

xildagi Obyektlarni

zararlaydi. Masalan, OneHalf.3544 virusi ham MS-DOS

dasturlari ham qattiq diskning yuklanuvchi sektorlarini

zararlasa, Anarchy oilasiga tegishli viruslar MS-DOS va

Windows dasturlaridan tashqari, MS Word hujjatlarini

ham zararlay oladi.

Yuklanuvchi viruslar bir vaqtning o'zida turli xildagi

Obyektlarni

zararlaydi. Masalan, OneHalf.3544 virusi ham MS-DOS

dasturlari ham qattiq diskning yuklanuvchi sektorlarini

zararlasa, Anarchy oilasiga tegishli viruslar MS-DOS va

Windows dasturlaridan tashqari, MS Word hujjatlarini

ham zararlay oladi.

Makroviruslar-... bir vaqtning o'zida turli xildagi

Obyektlarni

zararlaydi. Masalan, OneHalf.3544 virusi ham MS-DOS dasturlari ham qattiq diskning yuklanuvchi sektorlarini zararlasi, Anarchy oilasiga tegishli viruslar MS-DOS va Windows dasturlaridan tashqari, MS Word hujjatlarini ham zararlay oladi.

Birinchi kompyuter virusi nima deb nomlangan Cherv

$P=31$ ,  $q=29$  eyler funksiyasida  $f(p,q)$  ni hisoblang  $*840$   
 $256 \bmod 25 = ?$  5

bu yaxlit «butun»ni tashkil etuvchi bog'liq yoki o'zaro bog'langan tashkil etuvchilar guruhi nima deyiladi.

\*Tizim

Tashkilotni himoyalash maqsadida amalga oshirilgan xavfsizlik nazoratini tavsiflovchi yuqori satxli hujjat yoki hujjatlar to'plami nima duvidadi Standart

RSA shifrlash algoritmda foydalaniladigan sonlarning spektori o'lchami qanday? 65535;

DES algoritmi akslantirishlari raundlari soni qancha?

\*16;

DES algoritmi shifrlash blokining chap va o'ng qism bloklarining o'lchami qancha? CHap qism blok 32 bit, o'ng qism blok 48 bit;

Simmetrik va asimmetrik shifrlash algoritmlarining qanday mohiyatan farqli tomonlari bor? SHifrlash va deshifrlash jarayonlarida kalitlardan foydalanish qoidalariga ko'ra farqlanadi

19 gacha bo'lgan va 19 bilan o'zaro tub bo'lgan sonlar soni nechta? 19 ta

10 gacha bo'lgan va 10 bilan o'zaro tub bo'lgan sonlar soni nechta? \*4 ta

Qaysi formula qoldiqli bo'lish qonunini ifodalaydi

Eyler funsiyasida (1) qiymati nimaga teng? \*0

Eyler funsiyasida 60 sonining qiymatini toping. 59

Eyler funsiyasi yordamida 1811 sonining qiymatini toping. \*1810

97 tub sonmi? \*Tub

Quyidagi modulli ifodani qiymatini toping

$(148 + 14432) \bmod 256$ . \*244

Quyidagi sonlarning eng katta umumiy bo'luvchilarini toping. 88 i 220 21

Quyidagi ifodani qiymatini toping.

$-17 \bmod 11$  6

2 soniga 10 modul bo'yicha teskari sonni toping. 3

I:

S: Xavfsizlikning asosiy yo'nalishlarini sanab o'ting.

+: Axborot xavfsizligi, Iqtisodiy xavfsizlik, Mudofaa xavfsizligi, Ijtimoiy xavfsizlik, Ekologik xavfsizlik

-: Axborot va Iqtisodiy xavfsizlik, Signallar havfsizligi, Mobil aloqa xavfsizligi, Dasturiy ta'minot xavfsizligi

-: Mudofaa xavfsizligi, Ijtimoiy xavfsizlik, Signallar havfsizligi, Mobil aloqa xavfsizligi, Ekologik xavfsizlik

-: Axborot xavfsizligi, Iqtisodiy xavfsizlik, Mudofaa xavfsizligi, Ijtimoiy xavfsizlik, Dasturiy ta'minot xavfsizligi, Ekologik xavfsizlik

I:

S: Axborot xavfsizligining asosiy maqsadlaridan biribu...

+: Axborotlarni o'g'irlanishini, yo'qolishini, soxtalashtirilishini oldini olish

-: Ob'yektga bevosita ta'sir qilish

-: Axborotlarni shifrlash, saqlash, yetkazib berish

-: Tarmoqdagi foydalanuvchilarni xavfsizligini ta'minlab berish

I:

S: Konfidentsiallikga to'g'ri ta'rif keltiring.

+: axborot inshonchliligi, tarqatilishi mumkin emasligi, maxfiyligi kafolati;

-: axborot konfidensialligi, tarqatilishi mumkinligi, maxfiyligi kafolati;

-: axborot inshonchliligi, tarqatilishi mumkin emasligi, parollanganligi kafolati;

-: axborot inshonchliligi, axborotlashganligi, maxfiyligi

kafolati;

I:

S: Yaxlitlikni buzilishi bu - ...

+: Soxtalashtirish va o'zgartirish

-: Ishonchsizlik va soxtalashtirish

-: Soxtalashtirish

-: Butunmaslik va yaxlitlanmaganlik

I:

S:... axborotni himoyalash tizimi deyiladi.

+: Axborotning zaif tomonlarini kamaytiruvchi axborotga

ruxsat etilmagan kirishga, uning chiqib ketishiga va

yo'qotilishiga to'sqinlik qiluvchi tashkiliy, texnik,

dasturiy, texnologik va boshqa vosita, usul va

choralarning kompleksi

-: Axborot egalari hamda vakolatli davlat organlari

shaxsan axborotning qimmatliligi, uning yo'qotilishidan

keladigan zarar va himoyalash mexanizmining narxidan

kelib chiqqan holda axborotni himoyalashning zaruriy

darajasi

-: Axborot egalari hamda vakolatli davlat organlari

shaxsan axborotning qimmatliligi, uning yo'qotilishidan

keladigan zarar va himoyalash mexanizmining zaruriy

darajasi hamda tizimning turini, himoyalash usullar va

vositalari

-: Axborotning zaif tomonlarini kamaytiruvchi axborotga

ruxsat etilmagan kirishga, uning chiqib ketishiga va

yo'qotilishiga to'sqinlik qiluvchi tashkiliy, texnik,

dasturiy, texnologik va boshqa vosita, usul

I:

S: Kompyuter virusi nima?

+: maxsus yozilgan va zararli dastur

-.exe fayl

-: boshqariluvchi dastur

-: Kengaytmaga ega bo'lgan fayl

I:

S: Kriptografiyaning asosiy maqsadi...



+: maxfiylik, yaxlitlilikni ta`minlash

-: ishonchlilik, butunlilikni ta`minlash

-: autentifikatsiya, identifikatsiya

-: ishonchlilik, butunlilikni ta`minlash, autentifikatsiya, identifikatsiya

I:

S: SMTP - Simple Mail Transfer protokol nima?

+: elektron pochta protokoli

-: transport protokoli

-: internet protokoli

-: Internetda ommaviy tus olgan dastur

I:

S: SKIP protokoli...

+: Internet protokollari uchun kriptokalitlarning oddiy boshqaruvi

-: Protokollar boshqaruvi

-: E-mail protokoli

-: Lokal tarmoq protokollari uchun kriptokalitlarning oddiy boshqaruvi

I:

S: Kompyuter tarmog'ining asosiy komponentlariga nisbatan xavf-xatarlar...

+: uzilish, tutib qolish, o'zgartirish, soxtalashtirish

-: o'zgartirish, soxtalashtirish

-: tutib qolish, o'zgarish, uzilish

-: soxtalashtirish, uzilish, o'zgartirish

I:

S: ...ma`lumotlar oqimini passiv hujumlardan himoya qilishga xizmat qiladi.

+: konfidentsiallik

-: identifikatsiya

-: autentifikatsiya

-: maxfiylik

I:

S: Foydalanish huquqini cheklovchi matritsa modeli bu...

+: Bella La-Padulla modeli

-:Dening modeli

-:Landver modeli

-:Huquqlarni cheklovchi model

I:

S: Kompyuter tarmoqlarida tarmoqning uzoqlashtirilgan elementlari o'rtasidagi aloqa qaysi standartlar yordamida amalga oshiriladi?

+: TCP/IP, X.25 protokollar

-:X.25 protokollar

-:TCP/IP

-:SMTP

I:

S: Autentifikatsiya nima?

+: Ma'lum qilingan foydalanuvchi, jarayon yoki qurilmaning haqiqiy ekanligini tekshirish muolajasi

-: Tizim meyoriy va g'ayritabiiy hollarda rejalashtirilgandek o'zini tutishligi holati

-: Istalgan vaqtda dastur majmuasining mumkinligini kafolati

-:Tizim noodatiy va tabiiy hollarda qurilmaning haqiqiy ekanligini tekshirish muolajasi

I:

S:Identifikatsiya bu- ...

+: Foydalanuvchini uning identifikatori (nomi) bo'yicha aniqlash jarayoni

-:Ishonchliligini tarqalishi mumkin emasligi kafolati

-:Axborot boshlang'ich ko'rinishda ekanligi uni saqlash, uzatishda ruxsat etilmagan o'zgarishlar

-:Axborotni butunligini saqlab qolgan holda uni elementlarini o'zgartirishga yo'l qo'ymaslik

I:

S:O'rin almashtirish shifri bu - ...

+: Murakkab bo'lmagan kriptografik akslantirish

-:Kalit asosida generatsiya qilish

-:Ketma-ket ochiq matnni ustiga qo'yish

-:Belgilangan biror uzunliklarga bo'lib chiqib shifrlash

I:

S: Simmetrik kalitli shifrlash tizimi necha turga bo'linadi.

+: 2 turga

-: 3 turga

-: 4 turga

-: 5 turga

I:

S: Kalitlar boshqaruvi 3 ta elementga ega bo'lgan axborot almashinish jarayonidir bular ...

+: hosil qilish, yig'ish, taqsimlash

-: ishonchliligi, maxfiyligi, aniqligi

-: xavfsizlik, tez ishlashi, to'g'ri taqsimlanishi

-: abonentlar soni, xavfsizligi, maxfiyligi

I:

S: Kriptologiya -

+: axborotni qayta akslantirib himoyalash muammosi

bilan shug'ullanadi

-: axborotni qayta akslantirishning matematik usullarini izlaydi va tadqiq qiladi

-: kalitni bilmasdan shifrlangan matnni ochish

imkoniyatlarini o'rganadi

-: kalitlarni bilmasdan shifrni ochishga bardoshlilikni

aniqlovchi shifrlash tavsifi

I:

S: Kriptografiya alifbo –

+: axborot belgilarini kodlash uchun foydalaniladigan

chekli to'plam

-: matnni shifrlash va shifrni ochish uchun kerakli axborot

-: xabar muallifi va tarkibini aniqlash maqsadida

shifratga qo'shilgan qo'shimcha

-: kalit axborotni shifrlovchi kalitlar

I:

S: Simmetrik kriptotizimlarda ... jumlani davom ettiring

+: shifrlash va shifrni ochish uchun bitta va aynan shu

kalitdan foydalaniladi

-: bir-biriga matematik usullar bilan bog'langan ochiq va

yopiq kalitlardan foydalaniladi

-:axborot ochiq kalit yordamida shifrlanadi, shifrni ochish

esa faqat yopiq kalit yordamida amalga oshiriladi

-:kalitlardan biri ochiq boshqasi esa yopiq hisoblanadi

I:

S: Kriptobardoshlilik deb ...

+: kalitlarni bilmasdan shifrni ochishga bardoshlilikni

aniqlovchi shifrlash tavsifi

-:axborotni qayta akslantirib himoyalash muammosi bilan  
shug'ullanadi

-:kalitni bilmasdan shifrlangan matnni ochish

imkoniyatlarini o'rganadi

-:axborotni qayta akslantirishning matematik usullarini

izlaydi va tadqiq qiladi

I:

S: Elektron raqamli imzo deb –

+: xabar muallifi va tarkibini aniqlash maqsadida

shifrmatnga qo'shilgan qo'shimcha

-:matnni shifrlash va shifrini ochish uchun kerakli axborot

-:axborot belgilarini kodlash uchun foydalaniladigan  
chekli to'plam

-:kalit axborotni shifrlovchi kalitlar

I:

S: Kriptografiya –

+: axborotni qayta akslantirishning matematik usullarini

izlaydi va tadqiq qiladi

-:axborotni qayta akslantirib himoyalash muammosi bilan  
shug'ullanadi

-:kalitni bilmasdan shifrlangan matnni ochish

imkoniyatlarini o'rganadi

-:kalitlarni bilmasdan shifrni ochishga bardoshlilikni

aniqlovchi shifrlash tavsifi

I:

S: Kriptografiyada matn –

+: alifbo elementlarining tartiblangan to'plami

-:matnni shifrlash va shifrini ochish uchun kerakli axborot

-:axborot belgilarini kodlash uchun foydalaniladigan

chekli to'plam

-:kalit axborotni shifrlovchi kalitlar

I:

S: Kriptoanaliz –

+: kalitlarni bilmasdan shifrnı ochishga bardoshlilikni

aniqllovchi shifrlash tavsifi

-:axborotni qayta akslantirishning matematik usullarini

izlaydi va tadqiq qiladi

-:axborotni qayta akslantirib himoyalash muammosi bilan

shug'ullanadi

-:kalitni bilmasdan shifrlangan matnnı ochish

imkoniyatlarini o'rganadi

I:

S: Shifrlash –

+: akslantirish jarayoni ochiq matn deb nomlanadigan

matn shifrmatnga almashtiriladi

-:kalit asosida shifrmatn ochiq matnga akslantiriladi

-:shifrlashga teskari jarayon

-:Almashtirish jarayoni bo'lib: ochiq matn deb

nomlanadigan matn o'girilgan holatga almashtiriladi

I:

S: Faol hujum turi deb...

+: Maxfiy uzatish jarayonini uzib qo'yish,

modifikatsiyalash, qalbaki shifrlar ma'lumotlar tayyorlash

harakatlaridan iborat jarayon

-:Maxfiy ma'lumotni aloqa tarmog'ida uzatilayotganda

eshitish, tahrir qilish, yozib olish harakatlaridan iborat

uzatilayotgan ma'lumotni qabul qiluvchiga

o'zgartirishsiz yetkazish jarayoni

-:Ma'lumotga o'zgartirish kiritmay uni kuzatish jarayoni

-:Sust hujumdan farq qilmaydigan jarayon

I:

S: Blokli shifrlash-

+: shifrlanadigan matn blokiga qo'llaniladigan asosiy

akslantirish

-:murakkab bo'lmagan kriptografik akslantirish

-:axborot simvollarini boshqa alfavit simvollari bilan almashtirish

-:ochiq matnning har bir harfi yoki simvoli alohida shifrlanishi

I:

S: Simmetrik kriptotizimning uzluksiz tizimida ...

+: ochiq matnning har bir harfi va simvoli alohida shifrlanadi

-:belgilangan biror uzunliklarga teng bo'linib chiqib shifrlanadi

-:murakkab bo'lmagan kriptografik akslantirish orqali shifrlanadi

-:ketma-ket ochiq matnlarni o'rniga qo'yish orqali shifrlanadi

I:

S: Kriptotizimga qo'yiladigan umumiy talablardan biri

+: shifr matn uzunligi ochiq matn uzunligiga teng bo'lishi kerak

-:shifrlash algoritmining tarkibiy elementlarini o'zgartirish imkoniyati bo'lishi lozim

-:ketma-ket qo'llaniladigan kalitlar o'rtasida oddiy va oson bog'liqlik bo'lishi kerak

-:maxfiylik o'ta yuqori darajada bo'lmoqligi lozim

I:

S: Berilgan ta'riflardan qaysi biri asimmetrik tizimlarga xos?

+: Asimmetrik kriptotizimlarda  $k_1 \neq k_2$  bo'lib,  $k_1$  ochiq kalit,  $k_2$  yopiq kalit deb yuritiladi,  $k_1$  bilan axborot shifrlanadi,  $k_2$  bilan esa deshifrlanadi

-:Asimmetrik tizimlarda  $k_1 = k_2$  bo'ladi, ya'ni  $k$  – kalit bilan axborot ham shifrlanadi, ham deshifrlanadi

-:Asimmetrik kriptotizimlarda yopiq kalit axborot almashinuvining barcha ishtirokchilariga ma'lum bo'ladi, ochiq kalitni esa faqat qabul qiluvchi biladi

-:Asimmetrik kriptotizimlarda  $k_1 \neq k_2$  bo'lib, kalitlar

hammaga oshkor etiladi

I:

S: Yetarlicha kriptoturg'unlikka ega, dastlabki matn  
simvollarini almashtirish uchun bir necha alfavitdan  
foydalanishga asoslangan almashtirish usulini belgilang

+: Vijener matritsasi, Sezar usuli

-:monoalfavitli almashtirish

-:polialfavitli almashtirish

-:o'rin almashtirish

I:

S: Akslantirish tushunchasi deb nimaga aytiladi?

+: 1-to'plamli elementlariga 2-to'plam elementlariga mos  
bo'lishiga

-:1-to'plamli elementlariga 2-to'plam elementlarini  
qarama-qarshiligiga

-:har bir elementni o'ziga ko'payimasiga

-:agar birinchi va ikkinchi to'plam bir qiymatga ega  
bulmasa

I:

S: Simmetrik guruh deb nimaga aytiladi?

+: O'rin almashtirish va joylashtirish

-:O'rin almashtirish va solishtirish

-:Joylashtirish va solishtirish

-:O'rin almashtirish va transportizatsiyalash

I:

S: Qo'yish, o'rin almashtirish, gammalash  
kriptografiyaning qaysi turiga bog'liq?

+: simmetrik kriptosistemalar

-:assimetrik kriptosistemalar

-:ochiq kalitli kriptosistemalar

-:autentifikatsiyalash

I:

S: Internetda elektron pochta bilan ishlash uchun  
TCP/IPga asoslangan qaysi protokoldan foydalaniladi?

+: SMTP, POP yoki IMAP

-:SKIP, ATM, FDDI

-:X.25 va IMAR

-:SMTP, TCP/IP

I:

S: Axborot resursi – bu?

+: axborot tizimi tarkibidagi elektron shakldagi axborot,  
 ma`lumotlar banki, ma`lumotlar bazasi

-:cheklanmagan doiradagi shaxslar uchun mo`ljallangan  
 hujjatlashtirilgan axborot, bosma, audio, audiovizual  
 hamda boshqa xabarlar va materiallar

-:identifikatsiya qilish imkonini beruvchi rekvizitlari  
 qo`yilgan holda moddiy jismda qayd etilgan axborot

-:manbalari va taqdim etilish shaklidan qathi nazar  
 shaxslar, predmetlar, faktlar, voqealar, hodisalar va  
 jarayonlar to`g`risidagi ma`lumotlar

I:

S: Shaxsning, o`zini axborot kommunikatsiya tizimiga  
 tanishtirish jarayonida qo`llaniladigan belgilar ketmaketligi bo`lib, axborot kommunikatsiya tizimidan  
 foydalanish huquqiga ega bo`lish uchun  
 foydalaniluvchining maxfiy bo`lmagan qayd yozuvi – bu?

+: login parol

-:identifikatsiya

-:maxfiy maydon

-: token

I:

S: Uning egasi haqiqiylikini aniqlash jarayonida tekshiruv  
 axboroti sifatida ishlatiladigan belgilar ketma-ketligi  
 (maxfiy so`z) – bu?

+: parol

-:login

-:identifikatsiya

-:maxfiy maydon foydalanuvchilarni ro`yxatga olish va  
 ularga dasturlar va ma`lumotlarni ishlatishga huquq berish  
 jarayoni

I:

S: Identifikatsiya jarayoni qanday jarayon?

+: axborot tizimlari obyekt va subhektlariga uni tanish



uchun nomlar (identifikator) berish va berilgan nom

bo'yicha solishtirib uni aniqlash jarayoni

-:obyekt yoki subhektni unga berilgan identifikatorga

mosligini tekshirish va belgilar ketmaketligidan iborat

maxfiy kodini tekshirish orqali aslligini aniqlash

-:foydalanuvchining resursdan foydalanish huquqlari va

ruxsatlarini tekshirish jarayoni

-:foydalanuvchilarni ro'yxatga olish va ularga dasturlar va

ma'lumotlarni ishlatishga huquq berish jarayoni

I:

S: Autentifikatsiya jarayoni qanday jarayon?

+: obyekt yoki subhektni unga berilgan identifikatorga

mosligini tekshirish va belgilar ketmaketligidan iborat

maxfiy kodini tekshirish orqali aslligini aniqlash

-:axborot tizimlari obyekt va subhektlariga uni tanish

uchun nomlar (identifikator) berish va berilgan nom

bo'yicha solishtirib uni aniqlash jarayoni

-:foydalanuvchining resursdan foydalanish huquqlari va

ruxsatlarini tekshirish jarayoni

-:foydalanuvchilarni ro'yxatga olish va ularga dasturlar va

ma'lumotlarni ishlatishga huquq berish jarayoni

I:

S: Ro'yxatdan o'tish bu?

+: foydalanuvchilarni ro'yxatga olish va ularga dasturlar

va ma'lumotlarni ishlatishga huquq berish jarayoni

-:axborot tizimlari ob'yekt va subhektlariga uni tanish

uchun nomlar (identifikator) berish va berilgan nom

bo'yicha solishtirib uni aniqlash jarayoni

-:ob'yekt yoki subhektni unga berilgan identifikatorga

mosligini tekshirish va belgilar ketmaketligidan iborat

maxfiy kodini tekshirish orqali aslligini aniqlash

-:foydalanuvchining resursdan foydalanish huquqlari va

ruxsatlarini tekshirish jarayoni

I:

S: Axborot qanday sifatlarga ega bo'lishi kerak?

+: ishonchli, qimmatli va to'liq

-:uzluksiz va uzlukli

-:ishonchli, qimmatli va uzlukli

-:ishonchli, qimmatli va uzluksiz

I:

S: Axborotning eng kichik o'lchov birligi nima?

+: bit

-:kilobayt

-:bayt

-:bitta simvol

I:

S: Elektron hujjatning rekvizitlari nechta qismdan iborat?

+: 4

-:5

-:6

-:7

I:

S: Axborotlarni saqlovchi va tashuvchi vositalar qaysilar?

+: fleshka, CD va DVD disklar

-:Qattiq disklar va CDROM

-:CD va DVD, DVDROM

-:Qattiq disklar va DVDROM

I:

S: Avtorizatsiya jarayoni qanday jarayon?

+: foydalanuvchining resursdan foydalanish huquqlari va ruxsatlarini tekshirish jarayoni

-:axborot tizimlari obyekt va subhektlariga uni tanish uchun nomlar (identifikator) berish va -berilgan nom bo'yicha solishtirib uni aniqlash jarayoni

-:obyekt yoki subhektni unga berilgan identifikatorga mosligini tekshirish va belgilar ketmaketligidan iborat maxfiy kodini tekshirish orqali aslligini aniqlash.

-: parollash jarayoni

I:

S: Kodlash nima?

+: Ma'lumotni osongina qaytarish uchun hammaga ochiq bo'lgan sxema yordamida ma'lumotlarni boshqa formatga

o'zgartirishdir

-:Ma'lumot boshqa formatga o'zgartiriladi, biroq uni faqat maxsus shaxslar qayta o'zgartirishi mumkin bo'ladi

-:Ma'lumot boshqa formatga o'zgartiriladi, barcha shaxslar kalit yordamida qayta o'zgartirishi mumkin bo'ladi

-:Maxfiy xabarni soxta xabar ichiga berkitish orqali aloqani yashirish hisoblanadi

I:

S: Shifrlash nima?

+: Ma'lumot boshqa formatga o'zgartiriladi, biroq uni faqat maxsus shaxslar qayta o'zgartirishi mumkin bo'ladi

-:Ma'lumotni osongina qaytarish uchun hammaga ochiq bo'lgan sxema yordamida ma'lumotlarni boshqa formatga o'zgartirishdir

-: Ma'lumot boshqa formatga o'zgartiriladi, barcha shaxslar kalit yordamida qayta o'zgartirishi mumkin bo'ladi

-:Maxfiy xabarni soxta xabar ichiga berkitish orqali aloqani yashirish hisoblanadi

I:

S: Axborotni shifrnı ochish (deshifrlash) bilan qaysi fan shug'ullanadi

+:Kriptoanaliz

-:Kartografiya

-:Kriptologiya

-:Adamar usuli

I:

S: Qaysi juftlik RSA algoritmining ochiq va yopiq kalitlarini ifodalaydi

+:  $\{d, n\}$  – yopiq,  $\{e, n\}$  – ochiq;

-:  $\{d, e\}$  – ochiq,  $\{e, n\}$  – yopiq;

-:  $\{e, n\}$  – yopiq,  $\{d, n\}$  – ochiq;

-:  $\{e, n\}$  – ochiq,  $\{d, n\}$  – yopiq;

I:

S: Zamonaviy kriptografiya qanday bo'limlardan iborat?

-: Elektron raqamli imzo; kalitlarni boshqarish

-: Simmetrik kriptotizimlar; ochiq kalitli kriptotizimlar;

+: Simmetrik kriptotizimlar; ochiq kalitli kriptotizimlar;

Elektron raqamli imzo; kalitlarni boshqarish

-: Simmetrik kriptotizimlar; ochiq kalitli kriptotizimlar;

kalitlarni boshqarish

I:

S: Shifr nima?

+: Shifrlash va deshifrlashda foydalaniladigan matematik

funktsiyadan iborat bo'lgan kriptografik algoritim

-: Kalitlarni taqsimlash usuli

-: Kalitlarni boshqarish usuli

-: Kalitlarni generatsiya qilish usuli

I:

S: Ochiq kalitli kriptotizimlarning mohiyati nimadan

iborat?

+: Ochiq kalitli kriptotizimlarda bir-biri bilan matematik

bog'langan 2 ta – ochiq va yopiq kalitlardan foydalaniladi

-: Ochiq kalitli kriptotizimlarda shifrlash va deshifrlashda

1 ta – kalitdan foydalaniladi

-: Ochiq kalitli kriptotizimlarda ma'lumotlarni faqat

shifrlash mumkin

-: Ochiq kalitli kriptotizimlarda ma'lumotlarni faqat

deshifrlash mumkin

I:

S: Oqimli shifrlashning mohiyati nimada?

+: Oqimli shifrlash birinchi navbatda axborotni bloklarga

bo'lishning imkoni bo'lmagan hollarda zarur,

-: Qandaydir ma'lumotlar oqimini har bir belgisini

shifrlab, boshqa belgilarini kutmasdan kerakli joyga

jo'natish uchun oqimli shifrlash zarur,

-: Oqimli shifrlash algoritmlari ma'lumotlarni bitlar yoki

belgilar bo'yicha shifrlaydi

-: Oqimli shifrlash birinchi navbatda axborotni bloklarga

bo'lishning imkoni bo'lmagan hollarda zarur,

I:

S: Simmetrik algoritmlarni xavfsizligini ta'minlovchi omillarni ko'rsating.

+: uzatilayotgan shifrlangan xabarni kalitsiz ochish mumkin bo'lmashligi uchun algoritm yetarli darajada bardoshli bo'lishi lozim, uzatilayotgan xabarni xavfsizligi algoritmni maxfiyligiga emas, balki kalitni maxfiyligiga bog'liq bo'lishi lozim,

-:uzatilayotgan xabarni xavfsizligi kalitni maxfiyligiga emas, balki algoritmni maxfiyligiga bog'liq bo'lishi lozim

-:uzatilayotgan xabarni xavfsizligi shifrlanayotgan xabarni uzunligiga bog'liq bo'lishi lozim

-:uzatilayotgan xabarni xavfsizligi shifrlanayotgan xabarni uzunligiga emas, balki shifrlashda foydalaniladigan arifmetik amallar soniga bog'liq bo'lishi lozim

I:

S: Asimmetrik kriptotizimlar qanday maqsadlarda ishlatiladi?

+: shifrlash, deshifrlash, ERI yaratish va tekshirish, kalitlar almashish uchun

-:ERI yaratish va tekshirish, kalitlar almashish uchun

-:shifrlash, deshifrlash, kalitlar almashish uchun

-: Heshlash uchun

I:

S: Kriptografik elektron raqamli imzolarda qaysi kalitlar ma'lumotni yaxlitligini ta'minlashda ishlatiladi.

+: ochiq kalitlar

-:yopiq kalitlar

-:seans kalitlari

-:Barcha tutdagi kalitlar

I:

S: Kompyuterning tashqi interfeysi deganda nima tushuniladi?

+: kompyuter bilan tashqi qurilmani bog'lovchi simlar va ular orqali axborot almashinish qoidalari to'plamlari

-:tashqi qurilmani kompyuterga bog'lashda ishlatiladigan

ulovchi simlar

-:kompyuterning tashqi portlari.

-:tashqi qurilma bilan kompyuter o'rtasida axborot

almashinish qoidalari to'plami

I:

S: Lokal tarmoqlarda keng tarqalgan topologiya turi

qaysi?

+: Yulduz

-:Xalqa

-:To'liqbog'langan

-:Umumiy shina

I:

S: Ethernet kontsentratori qanday vazifani bajaradi

+: kompyuterdan kelayotgan axborotni qolgan barcha

kompyuterga yo'naltirib beradi

-:kompyuterdan kelayotgan axborotni boshqa bir

kompyuterga yo'naltirib beradi

-:kompyuterdan kelayotgan axborotni xalqa bo'ylab

joylashgan keyingi kompyuterga

-:tarmoqning ikki segmentini bir biriga ulaydi

I:

S: OSI modelida nechta satx mavjud

+: 7

-:4

-:5

-:3

I:

S: OSI modelining to'rtinchi satxi qanday nomlanadi

+: Transport satxi

-:Amaliy satx

-:Seanslar satxi

-:Taqdimlash satxi

I:

S: OSI modelining beshinchi satxi qanday nomlanadi

+: Seanslar satxi

-:Tarmoq satxi

-:Fizik satx

-:Amaliy satx

I:

S: OSI modelining birinchi satxi qanday nomlanadi

+: Fizik satx

-:Seanslar satxi

-:Transport satxi

-:Taqdimlash satxi

I:

S: OSI modelining ikkinchi satxi qanday nomlanadi

+: Kanal satxi

-:Amaliy satxi

-:Fizik satx

-:Seanslar satxi

I:

S: OSI modelining uchinchi satxi qanday nomlanadi

+: Tarmoq satxi

-:Amaliy satx

-:Kanal satxi

-:Taqdimlash satxi

I:

S: OSI modelining oltinchi satxi qanday nomlanadi

+: Taqdimlash satxi

-:Amaliy satx

-:Seanslar satxi

-:Kanal satxi

I:

S: OSI modelining yettinchi satxi qanday nomlanadi

+: Amaliy satx

-:Seanslar satxi

-:Transport satxi

-:Taqdimlash satxi

I:

S: OSI modelining qaysi satxlari tarmoqqa bog'liq satxlar hisoblanadi

+: fizik, kanal va tarmoq satxlari

-:seans va amaliy satxlar

-:amaliy va taqdimlash satxlari

-:transport va seans satxlari

I:

S: OSI modelining tarmoq satxi vazifalari keltirilgan

qurilmalarning qaysi birida bajariladi

+: Marshrutizator

-:Ko'prik

-:Tarmoq adapter

-:Kontsentrator

I:

S: Elektr signallarini qabul qilish va uzatish vazifalarini

OSI modelining qaysi satxi bajaradi

+: Fizik satx

-:Kanal satxi

-:Tarmoq satxi

-:Transport satxi

I:

S: Ma'lumotlarni uzatishning optimal marshrutlarini

aniqlash vazifalarini OSI modelining qaysi satxi bajaradi

+: Tarmoq satxi

-:Kanal satxi

-:Amaliy satx

-:Transport satxi

I:

S: Keltirilgan protokollarning qaysilari tarmoq satxi

protokollariga mansub

+: IP, IPX

-:NFS, FTP

-:Ethernet, FDDI

-:TCP,UDP

I:

S: Keltirilgan protokollarning qaysilari transport satxi

protokollariga mansub

+: TCP,UDP



-:NFS, FTP

-:IP, IPX

-:Ethernet, FDDI

I:

S: OSI modelining fizik satxi qanday funksiyalarni bajaradi

+: Elektr signallarini uzatish va qabul qilish

-:Aloqa kanalini va ma'lumotlarni uzatish muxitiga murojaat qilishni boshqarish

-:Bog'lanish seansini yaratish, kuzatish, oxirigacha ta'minlash

-:Klient dasturlari bilan o'zaro muloqotda bo'lish

I:

S: Identifikatsiya, autentifikatsiya jarayonlaridan o'tgan foydalanuvchi uchun tizimda bajarishi mumkin bo'lgan amallarga ruxsat berish jarayoni bu...

+: Avtorizatsiya

-:Shifrlash

-:Identifikatsiya

-:Autentifikatsiya

I:

S: Autentifikatsiya faktorlari nechta

+: 3

-:4

-:5

-: 6

I:

S: Ko'z pardasi, yuz tuzilishi, ovoz tembri- bular autentifikatsiyaning qaysi faktoriga mos belgilar?

+: Biometrik autentifikatsiya

-:Biron nimaga egalik asosida

-:Biron nimani bilish asosida

-:Parolga asoslangan

I:

S: Barcha kabel va tarmoq tizimlari; tizim va kabellarni fizik nazoratlash; tizim va kabel uchun quvvat manbai;

tizimni madadlash muhiti. Bular tarmoqning qaysi satxiga

kiradi?

+: Fizik satx

-:Tarmoq satxi

-:Amaliy satx

-:Tadbiqiy sath

I:

S: Fizik xavfsizlikda Yong'inga qarshi tizimlar necha turga bo'linadi

+: 2

-:4

-:3

-:5

I:

S: Foydalanishni boshqarishda inson, dastur, jarayon va xokazolar nima vazifani bajaradi?

+: Subyekt

-:Obyekt

-:Tizim

-:Jarayon

I:

S: MAC usuli bilan foydalanishni boshqarishda xavfsizlik markazlashgan holatda kim tomonidan amalga oshiriladi

+: xavfsizlik siyosati ma'muri

-:Foydalaguvchining o'zi

-:Dastur tomonidan

-:Boshqarish amaalga oshirilmaydi

I:

S: Agar Subyektning xavfsizlik darajasida Obyektning xavfsizlik darajasi mavjud bo'lsa, u holda uchun qanday amalga ruxsat beriladi

+: O'qish

-:Yozish

-:O'zgartirish

-:Yashirish

I:

S: Agar Subyektning xavfsizlik darajasi Obyektning xavfsizlik darajasida bo'lsa, u holda qanday amalga ruxsat beriladi.

+: Yozish

-: O'qish

-: O'zgartirish

-: Yashirish

I:

S: Rol tushunchasiga ta'rif bering.

+: Muayyan faoliyat turi bilan bog'liq harakatlar va majburiyatlar to'plami sifatida belgilanishi mumkin

-: Foydalanishni boshqarish

-: Muayyan faoliyat turi bilan bog'liq imkoniyatlar to'plami sifatida belgilanishi mumkin

-: Vakolitlarni taqsimlash

I:

S: Foydalanishni boshqarishning qaysi usuli - Obyektlar va Subyektlarning atributlari, ular bilan mumkin bo'lgan amallar va so'rovlarga mos keladigan muhit uchun qoidalarni tahlil qilish asosida foydalanishlarni boshqaradi.

+: ABAC

-: MAC

-: DAC

-: RBAC

I:

S: Biometrik autentifikatsiyalash usullari an'anaviy usullarga nisbatan avfzalliklari qaysi javobda to'g'ri ko'rsatilgan?

+: barchasi

-: biometrik alomatlarining ishga layoqatli shaxsdan ajratib bo'lmavsligi

-: biometrik alomatlarini soxtalashtirishning qiyinligi

-: biometrik alomatlarini noyobligi tufayli autentifikatsiyalashning ishonchlilik darajasi yuqoriligi

I:

S: OSI modeli 7 satxi bu

+: Ilova

-:Seans

-:Fizik

-:Kanal

I:

S: OSI modeli 1 satxi bu

+: Fizik

-:Ilova

-:Seans

-:Kanal

I:

S: OSI modeli 2 satxi bu

+:Kanal

-: Fizik

-:Ilova

-:Seans

I:

S: TCP/IP modelida nechta satx mavjud

+: 4

-:3

-:2

-:8

I:

S: Qanday tarmoq qisqa masofalarda qurilmalar o'rtasida ma'lumot almashinish imkoniyatini taqdim etadi?

+: Shaxsiy tarmoq

-:Lokal

-:Mintaqaviy

-:CAMPUS

I:

S: Tarmoq kartasi bu...

+: Hisoblash qurilmasining ajralmas qismi bo'lib, qurilmani tarmoqqa ulash imkoniyatini taqdim etadi.

-:Tarmoq repetiri odatda signalni tiklash yoki qaytarish uchun foydalaniladi.

-:ko'plab tarmoqlarni ulash uchun yoki LAN

segmentlarini bog'lash uchun xizmat qiladi.

-:qabul qilingan signalni barcha chiquvchi portlarga emas balki paketda manzili keltirilgan portga uzatadi.

I:

S: Server xotirasidagi joyni bepul yoki pulli ijagara berish xizmati qanday ataladi?

+: Qabul qilingan signalni barcha chiquvchi portlarga emas balki paketda manzili keltirilgan portga uzatadi.

-:Hisoblash qurilmasining ajralmas qismi bo'lib, qurilmani tarmoqqa ulash imkoniyatini taqdim etadi.

-:Signalni tiklash yoki qaytarish uchun foydalaniladi.

-:Ko'plab tarmoqlarni ulash uchun yoki LAN segmentlarini bog'lash uchun xizmat qiladi.

I:

S: Hab bu...

+: ko'plab tarmoqlarni ulash uchun yoki LAN segmentlarini bog'lash uchun xizmat qiladi.

-:Hisoblash qurilmasining ajralmas qismi bo'lib, qurilmani tarmoqqa ulash imkoniyatini taqdim etadi.

-:Tarmoq repetiri odatda signalni tiklash yoki qaytarish uchun foydalaniladi.

-:qabul qilingan signalni barchachiquvchi portlarga emas balki paketda manzili keltirilgan portga uzatadi.

I:

S: Tarmoq repiteri bu...

+: Signalni tiklash yoki qaytarish uchun foydalaniladi.

-:Hisoblash qurilmasining ajralmas qismi bo'lib, qurilmani tarmoqqa ulash imkoniyatini taqdim etadi.

-:ko'plab tarmoqlarni ulash uchun yoki LAN segmentlarini bog'lash uchun xizmat qiladi.

-:qabul qilingan signalni barcha chiquvchi portlarga emas balki paketda manzili keltirilgan portga uzatadi.

I:

S: Qanday tizim host nomlari va internet nomlarini IP manzillarga o'zgartirish yoki teskarisini amalga oshiradi.

+: DNS tizimlari

-.TCP/IP

-.Ethernet

-.Token ring

I:

S: ..... protokoli ulanishga asoslangan protokol bo'lib,  
internet orqali ma'lumotlarni almashinuvchi turli ilovalar  
uchun tarmoq ulanishlarini sozlashga yordam beradi.

+: TCP

-.IP

-.HTTP

-.FTP

I:

S: .... protokolidan odatda o'yin va video ilovalar  
tomonidan keng foydalaniladi.

+: UDP

-.HTTP

-.TCP

-.FTP

I:

S: Qaysi protokol ma'lumotni yuborishdan oldin aloqa  
o'rnatish uchun zarur bo'lgan manzil ma'lumotlari bilan  
ta'minlaydi.

+: IP

-.TCP

-.HTTP

-.FTP

I:

S: Tarmoq taxdidlari necha turga bo'linadi

+: 4

-.2

-.3

-.5

I:

S: Qanday xujum asosiy hujumlarni oson amalga oshirish  
uchun tashkilot va tarmoq haqidagi axborotni to'plashni

maqsad qiladi;

+: Razvedka hujumlari

-:Kirish hujumlari

-:Xizmatdan voz kechishga undash (Denial of service, DOS) hujumlari

-:Zararli hujumlar

I:

S: Qanday xujum hujumchi turli texnologiyalardan foydalangan holda tarmoqqa kirishga harakat qiladi

+: Kirish hujumlari

-:Razvedka hujumlari

-:Xizmatdan voz kechishga undash (Denial of service, DOS) hujumlari

-:Zararli hujumlar

I:

S: Qanday xujum da hujumchi mijozlarga, foydalanuvchilarga va tashkilotlarda mavjud bo'lgan biror xizmatni cheklashga urinadi;

+: Xizmatdan voz kechishga undash (Denial of service, DOS) hujumlari

-:Razvedka hujumlari

-:Kirish hujumlari

-:Zararli hujumlar

I:

S: Qanday xujumdp zararli hujumlar tizim yoki tarmoqqa bevosita va bilvosita ta'sir qiladi;

+: Zararli hujumlar

-:Razvedka hujumlari

-:Kirish hujumlari

-:Xizmatdan voz kechishga undash (Denial of service, DOS) hujumlari

I:

S: RSA elektron raqamli imzo algoritmidagi ochiq kalit e qanday shartni qanoatlantirishi shart?

+: e soni Eyler funksiyasi -  $\phi(n)$  bilan o'zaro tub

-:e ning qiymati  $[1,n]$  kesmaga tegishli ixtiyoriy son

-:e soni ixtiyoriy tub son

-:e soni ixtiyoriy butun musbat son

I:

S: RSA elektron raqamli imzo algoritmidagi yopiq kalit d

qanday hisoblanadi? Bu yerda p va q tub sonlar,  $n=pq$ ,

$\phi(n)$ - Eyler funksiyasi, e-ochiq kalit

+:  $d=e^{-1} \bmod \phi(n)$

-:  $d=e^{-1} \bmod q$

-:  $d=e^{-1} \bmod q$

-:  $d=e^{-1} \bmod p$

I:

S: Elektron raqamli imzo algoritmi qanday bosqichlardan

iborat bo'ladi?

+: Imzo qo'yish va imzoni tekshirishdan

-:Faqat imzo qo'yishdan

-:Faqat imzoni tekshirishdan

-:Barcha javoblar to'g'ri

I:

S: Imzoni haqiqiyligini tekshirish qaysi kalit yordamida

amalg oshiriladi?

+: Imzo muallifining ochiq kaliti yordamida

-:Ma'lumotni qabul qilgan foydalanuvchining ochiq kaliti yordamida

-:Ma'lumotni qabul qilgan foydalanuvchining maxfiy kaliti yordamida

-:Imzo muallifining maxfiy kaliti yordamida

I:

S: Tarmoq modeli-bu...

+: Ikki hisoblash tizimlari orasidagi aloqani ularning ichki tuzilmaviy va texnologik asosidan qat'iy nazar muvaffaqiyatli o'rnatilishini asosidir

-:Global tarmoq qurish usullari

-:Lokal tarmoq qurish usullari

-:To'g'ri javob yo'q.

I:

S: OSI modeli nechta satxga ajraladi?



+: 7

-:2

-:4

-:3

I:

S: TCP/IP modelining kanal satxiga OSI modelining

qaysi satxlari mos keladi

+: Kanal, Fizik

-:Tarmoq

-:Transport

-:Ilova, taqdimot, seans.

I:

S: TCP/IP modelining tarmoq satxiga OSI modelining

qaysi satxlari mos keladi

+: Tarmoq

-:Kanal, Fizik

-:Transport

-:Ilova, taqdimot, seans.

I:

S: TCP/IP modelining transport satxiga OSI modelining

qaysi satxlari mos keladi

+: Transport

-:Kanal, Fizik

-:Tarmoq

-:Ilova, taqdimot, seans.

I:

S: TCP/IP modelining ilova satxiga OSI modelining qaysi

satxlari mos keladi

+: Ilova, taqdimot, seans

-:Kanal, Fizik

-:Tarmoq

-:Transport

I:

S: Quyidagilardan lokal tarmoqqa berilgan ta'rifni

belgilang.

+: Kompyuterlar va ularni bog'lab turgan qurilmalardan

iborat bo'lib, ular odatda bitta tarmoqda bo'ladi.

-:Odatda ijaraga olingan telekommunikatsiya liniyalaridan foydalanadigan tarmoqlardagi tugunlarni bir-biriga bog'laydi.

-:Bu tarmoq shahar yoki shaharcha bo'ylab tarmoqlarning o'zaro bog'lanishini nazarda tutadi

-:Qisqa masofalarda qurilmalar o'rtasida ma'lumot almashinish imkoniyatini taqdim etadi

I:

S: Quyidagilardan mintaqaviy tarmoqqa berilgan ta'rifni belgilang.

+: Odatda ijaraga olingan telekommunikatsiya liniyalaridan foydalanadigan tarmoqlardagi tugunlarni birbiriga bog'laydi.

-:Kompyuterlar va ularni bog'lab turgan qurilmalardan iborat bo'lib, ular odatda bitta tarmoqda bo'ladi.

-:Bu tarmoq shahar yoki shaharcha bo'ylab tarmoqlarning o'zaro bog'lanishini nazarda tutadi

-:Qisqa masofalarda qurilmalar o'rtasida ma'lumot almashinish imkoniyatini taqdim etadi.

I:

S: Repetir nima?

+: Odatda signalni tiklash yoki qaytarish uchun foydalaniladi

-:Tarmoq qurilmasi bo'lib, ko'plab tarmoqlarni ulash uchun yoki LAN segmentlarini bog'lash uchun xizmat qiladi

-: Hisoblash qurilmasining ajralmas qismi bo'lib, qurilmani tarmoqqa ulash imkoniyatini taqdim etadi

-:Ko'plab tarmoqlarni ulash uchun yoki LAN segmentlarini bog'lash uchun xizmat qiladi. Qabul qilingan signalni barcha chiquvchi portlarga emas balki paketda manzili keltirilgan portga uzatadi

I:

S: Hub nima?

+: Tarmoq qurilmasi bo'lib, ko'plab tarmoqlarni ulash uchun yoki LAN segmentlarini bog'lash uchun xizmat

qiladi

-:Hisoblash qurilmasining ajralmas qismi bo'lib,  
qurilmani tarmoqqa ulash imkoniyatini taqdim etadi,  
Odatda signalni tiklash yoki qaytarish uchun foydalaniladi

-:Ko'plab tarmoqlarni ulash uchun yoki LAN  
segmentlarini bog'lash uchun xizmat qiladi.

-:Qabul qilingan signalni barcha chiquvchi portlarga emas  
balki paketda manzili keltirilgan portga uzatadi

I:

S: Router nima?

+: Qabul qilingan ma'lumotlarni tarmoq satxiga tegishli  
manzillarga ko'ra (IP manzil) uzatadi.

-:Tarmoq qurilmasi bo'lib, ko'plab tarmoqlarni ulash  
uchun yoki LAN segmentlarini bog'lash uchun xizmat  
qiladi Hisoblash qurilmasining ajralmas qismi bo'lib,  
qurilmani tarmoqqa ulash imkoniyatini taqdim etadi

-:Ko'plab tarmoqlarni ulash uchun yoki LAN  
segmentlarini bog'lash uchun xizmat qiladi.

-:Qabul qilingan signalni barcha chiquvchi portlarga emas  
balki paketda manzili keltirilgan portga uzatadi

I:

S: Asosan tarmoq, tizim va tashkilot haqidagi axborot  
olish maqsadda amalga oshiriladigan tarmoq hujumi  
qaysi

+: Razvedka hujumlari

-:Kirish hujumlari

-:DOS hujumi

-:Zararli hujumlar

I:

S: Razvedka hujumiga berilgan ta'rifni aniqlang

+: Asosiy hujumlarni oson amalga oshirish uchun  
tashkilot va tarmoq haqidagi axborotni to'plashni maqsad  
qiladi;

-:hujumchi turli texnologiyalardan foydalangan holda  
tarmoqqa kirishga harakat qiladi hujumchi -:mijozlarga,  
foydalanuvchilarga va tashkilotlarda mavjud bo'lgan biror

xizmatni cheklashga urinadi;

-:zararli hujumlar tizim yoki tarmoqqa bevosita va bilvosita ta'sir qiladi;

I:

S: OSI modelining birinchi satxi qanday nomlanadi

+: Fizik satx

-:Seanslar satxi

-:Transport satxi

-:Taqdimlash satxi

I:

S: OSI modelining ikkinchi satxi qanday nomlanadi

+: Kanal satxi

-:Amaliy satxi

-:Fizik satx

-:Seanslar satxi

I:

S: OSI modelining uchinchi satxi qanday nomlanadi

+: Tarmoq satxi

-:Amaliy satx

-:Kanal satxi

-:Taqdimlash satxi

I:

S: OSI modelining oltinchi satxi qanday nomlanadi

+: Taqdimlash satxi

-:Amaliy satx

-:Seanslar satxi

-:Kanal satxi

I:

S: OSI modelining ettinchi satxi qanday nomlanadi

+: Amaliy satx

-:Seanslar satxi

-:Transport satxi

-:Taqdimlash satxi

I:

S: Elektr signallarini qabul qilish va uzatish vazifalarini

OSI modelining qaysi satxi bajaradi

+: Fizik satx

-:Kanal satxi

-:Tarmoq satxi

-:Transport satxi

I:

S: Keltirilgan protokollarning qaysilari transport satxi

protokollariga mansub

+: TCP,UDP

-:NFS, FTP

-:IP, IPX

-:Ethernet, FDDI

I:

S: OSI modelining fizik satxi qanday funksiyalarni

bajaradi

+: Elektr signallarini uzatish va qabul qilish

-:Aloqa kanalini va ma'lumotlarni uzatish muxitiga

murojat qilishni boshqarish

-:Bog'lanish seansini yaratish, kuzatish, oxirigacha  
ta'minlash

-:Klient dasturlari bilan o'zaro muloqotda bo'lish

I:

S: OSI modelining amaliy satxi qanday funksiyalarni

bajaradi

+: Klient dasturlari bilan o'zaro muloqotda bo'lish

-:Aloqa kanalini va ma'lumotlarni uzatish muxitiga

murojat qilishni boshqarish

-:Bog'lanish seansini yaratish, kuzatish, oxirigacha  
ta'minlash

-:Elektr signallariniuzatish va qabul qilish

I:

S: Yevklid algoritmi qanday natijani beradi?

+: Sonning eng katta umumiy bo'luvchisini toppish

-:Sonning turli bo'luvchilarini toppish

-:Sonning eng kichik umumiy karralisini toppish

-:Sonning eng katta umumiy bo'linuvchisini topish

I:

S: Qanday sonlar tub sonlar deb yuritiladi?

+: Faqatgina 1 ga va o'ziga bo'linadigan sonlar tub sonlar deyiladi.

-:O'zidan boshqa bo'luvchilari mavjud bo'lgan sonlar tub sonlar deyiladi.

-:Agar sonning 1 dan boshqa bo'luvchilari bo'lsa.

-:Faqatgina 1 ga o'ziga bo'linmaydigan sonlar tub sonlar deyiladi.

I:

S: OSI modelining birinchi satxi qanday nomlanadi

+: Fizik satx

-:Seanslar satxi

-:Transport satxi

-:Taqdimlash satxi

I:

S: OSI modelining ikkinchi satxi qanday nomlanadi

+: Kanal satxi

-:Amaliy satxi

-:Fizik satx

-:Seanslar satxi

I:

S: OSI modelining uchinchi satxi qanday nomlanadi

+: Tarmoq satxi

-:Amaliy satx

-:Kanal satxi

-:Taqdimlash satxi

I:

S: OSI modelining oltinchi satxi qanday nomlanadi

+: Taqdimlash satxi

-:Amaliy satx

-:Seanslar satxi

-:Kanal satxi

I:

S: OSI modelining ettinchi satxi qanday nomlanadi

+: Amaliy satx

-:Seanslar satxi

-:Transport satxi

-:Taqdimlash satxi

I:

S: Elektr signallarini qabul qilish va uzatish vazifalarini

OSI modelining qaysi satxi bajaradi

+: Fizik satx

-:Kanal satxi

-:Tarmoq satxi

-:Transport satxi

I:

S: Keltirilgan protokollarning qaysilari transport satxi  
protokollariga mansub

+: TCP,UDP

-:NFS, FTP

-:IP, IPX

-:Ethernet, FDDI

I:

S: OSI modelining fizik satxi qanday funksiyalarni  
bajaradi

+: Elektr signallarini uzatish va qabul qilish

-:Aloqa kanalini va ma'lumotlarni uzatish muxitiga  
murojat qilishni boshqarish

-:Bog'lanish seansini yaratish, kuzatish, oxirigacha  
ta'minlash

-:Klient dasturlari bilan o'zaro muloqotda bo'lish

I:

S: OSI modelining amaliy satxi qanday funksiyalarni  
bajaradi

+: Klient dasturlari bilan o'zaro muloqotda bo'lish

-:Aloqa kanalini va ma'lumotlarni uzatish muxitiga  
murojat qilishni boshqarish

-:Bog'lanish seansini yaratish, kuzatish, oxirigacha  
ta'minlash

-:Elektr signallarini uzatish va qabul qilish

I:

S: Yevklid algoritmi qanday natijani beradi?

+: Sonning eng katta umumiy bo'luvchisini toppish

-:Sonning turli bo'luvchilarini toppish

-:Sonning eng kichik umumiy karralisini toppish

-:Sonning eng katta umumiy bo'linuvchisini topish

I:

S: Qanday sonlar tub sonlar deb yuritiladi?

+: Faqatgina 1 ga va o'ziga bo'linadigan sonlar tub sonlar deyiladi.

-:O'zidan boshqa bo'luvchilari mavjud bo'lgan sonlar tub sonlar deyiladi.

-:Agar sonning 1 dan boshqa bo'luvchilari bo'lsa.

-:Faqatgina 1 ga o'ziga bo'linmaydigan sonlar tub sonlar deyiladi.

I:

S: Antivirus dasturlarini ko'rsating?

+: Drweb, Nod32, Kaspersky

-:arj, rar, pkzip, pkunzip

-:winrar, winzip, winarj

-:pak, lha

I:

S: Wi-Fi tarmoqlarida quyida keltirilgan qaysi shifrlash protokollaridan foydalaniladi

+: wep, wpa, wpa2

-:web, wpa, wpa2

-:wpa, wpa2

-:wpa, wpa2, wap

I:

S: Axborot himoyalangan qanday sifatlarga ega bo'lishi kerak?

+: ishonchli, qimmatli va to'liq

-:uzluksiz va uzlukli

-:ishonchli, qimmatli va uzlukli

-:ishonchli, qimmatli va uzluksiz

I:

S: Axborotning eng kichik o'lchov birligi nima?

+: bit



-:kilobayt

-:bayt

-:bitta simvol

I:

S: Virtual xususiy tarmoq – bu?

+: VPN

-:APN

-:ATM

-:Ad-hoc

I:

S: Xavfli viruslar bu - ...

+: kompyuter ishlashida jiddiy nuqsonlarga sabab

bo'luvchi viruslar

-:tizimda mavjudligi turli taassurot (ovoz, video) bilan

bog'liq viruslar, bo'sh xotirani kamaytirsada, dastur va

ma'lumotlarga ziyon yetkazmaydi

-:o'z-o'zidan tarqalish mexanizmi amalga oshiriluvchi

viruslar

-:dastur va ma'lumotlarni buzilishiga hamda kompyuter

ishlashiga zarur axborotni o'chirilishiga bevosita olib

keluvchi, muolajalari oldindan ishlash algoritmlariga

joylangan viruslar

I:

S: Mantiqiy bomba – bu ...

+: Ma'lum sharoitlarda zarar keltiruvchi harakatlarni

bajaruvchi dastur yoki uning alohida modullari

-:Viruslar va zarar keltiruvchi dasturlarni tarqatish

kanallari

-:Viruslar kodiga boshqarishni uzatish

-:Qidirishning passiv mexanizmlarini amalga oshiruvchi,

yahni dasturiy fayllarga tuzoq qo'yuvchi viruslar

I:

S: Rezident virus...

+: tezkor xotirada saqlanadi

-:to'liqligicha bajarilayotgan faylda joylashadi

-:ixtiyoriy sektorlarda joylashgan bo'ladi

-:alohida joyda joylashadi

I:

S: DIR viruslari nimani zararlaydi?

+: FAT tarkibini zararlaydi

-:com, exe kabi turli fayllarni zararlaydi

-:yuklovchi dasturlarni zararlaydi

-:Operatsion tizimdagi sonfig.sys faylni zararlaydi

I:

S:.... kompyuter tarmoqlari bo'yicha tarqalib,  
komlg'yuterlarning tarmoqdagi manzilini aniqlaydi va u  
yerda o'zining nusxasini qoldiradi

+: «Chuvalchang» va replikatorli virus

-:Kvazivirus va troyan virus

-:Troyan dasturi

-:Mantiqiy bomba

I:

S: Fire Wall ning vazifasi...

+: tarmoqlar orasida aloqa o'rnatish jarayonida tashkilot  
va Internet tarmog'i orasida xavfsizlikni ta'minlaydi

-:kompyuterlar tizimi xavfsizligini ta'minlaydi

-:Ikkita kompyuter o'rtasida aloqa o'rnatish jarayonida  
Internet tarmog'i orasida xavfsizlikni ta'minlaydi

-:uy tarmog'i orasida aloqa o'rnatish jarayonida tashkilot  
va Internet tarmog'i orasida xavfsizlikni ta'minlaydi

I:

S: Kompyuter virusi nima?

+: maxsus yozilgan va zararli dastur

-:..exe fayl

-:boshqariluvchi dastur

-:Kengaytmaga ega bo'lgan fayl

I:

S: Kompyuterning viruslar bilan zararlanish yo'llarini  
ko'rsating

+: disk, maxsus tashuvchi qurilma va kompyuter  
tarmoqlari orqali

-: faqat maxsus tashuvchi qurilma orqali

-: faqat kompyuter tarmoqlari orqali

-:zararlanish yo'llari juda ko'p

I:

S: Troyan dasturlari bu...

+: virus dasturlar

-:antivirus dasturlar

-:o'yin dasturlari

-:yangilovchi dasturlar

I:

S: Kompyuter viruslari xarakterlariga nisbatan necha turga ajraladi?

+: 5

-:4

-:2

-:3

I:

S: Antiviruslarni, qo'llanish usuliga ko'ra... turlari mavjud

+: detektorlar, faglar, vaktsinalar, privivkalar, revizorlar, monitorlar

-:detektorlar, falglar, revizorlar, monitorlar, revizatsiyalar

-:vaktsinalar, privivkalar, revizorlar, tekshiruvchilar

-:privivkalar, revizorlar, monitorlar, programma, revizorlar, monitorlar

I:

S: Stenografiya mahnosi...

+: sirli yozuv

-:sirli xat

-:maxfiy axborot

-:maxfiy belgi

I:

S: ...sirli yozuvning umumiy nazariyasini yaratdiki, u fan sifatida stenografiyaning bazasi hisoblanadi

+: K.Shennon

-:Sezar

-:U.Xill

-:Fon Neyman

I:

S: Kriptologiya yo'nalishlari nechta?

+: 2

-:3

-:4

-:5

I:

S: Kriptografiyaning asosiy maqsadi...

+: maxfiylik, yaxlitlikni ta'minlash

-:ishonchlilik, butunlikni ta'minlash

-:autentifikatsiya, identifikatsiya

-:ishonchlilik, butunlikni ta'minlash, autentifikatsiya,  
identifikatsiya

I:

S: DES algoritmi akslantirishlari raundlari soni qancha?

+: 16;

-:14;

-:12;

-:32;

I:

S: DES algoritmi shifrlash blokining chap va o'ng qism  
bloklarining o'lchami qancha?

+: CHap qism blok 32 bit, o'ng qism blok 32 bit;

-:CHap qism blok 32 bit, o'ng qism blok 48 bit;

-:CHap qism blok 64 bit, o'ng qism blok 64 bit;

-:CHap qism blok 16 bit, o'ng qism blok 16 bit;

I:

S: 19 gacha bo'lgan va 19 bilan o'zaro tub bo'lgan sonlar  
soni nechta?

+: 18 ta;

-:19 ta

-:11 ta

-:9 ta

I:

S: 10 gacha bo'lgan va 10 bilan o'zaro tub bo'lgan sonlar  
soni nechta?

+: 3 ta

-:7 ta

-:8 ta;

-:9 ta

I:

S: Qaysi formula qoldiqli bo'lish qonunini ifodalaydi

+:  $a = bq + r, 0 \leq r < b$ ,

-:  $a = p_1^{a_1} p_2^{a_2} p_3^{a_3} \dots p_k^{a_k}$

-:  $M = r_1^{k_1} r_2^{k_2}$ ;

-:  $M = v(k_1 + k_2)$

I:

S: Eyler funksiyasida  $p=11$  va  $q=13$  sonining qiymatini

toping.

+: 16

-:59

-:30

-:21

I:

S: Eyler funksiyasi yordamida 1811 sonining qiymatini

toping.

+: 1810

-:2111

-:16

-:524

I:

S: 97 tub sonmi?

+: Tub

-:murakkab

-:Natural

-:To'g'ri javob yo'q

I:

S: Quyidagi modulli ifodani qiymatini toping

$(148 + 14432) \bmod 256$ .

+: 244

-:200

-:156

:-154

I:

S: Quyidagi sonlarning eng katta umumiy bo'luvchilarini toping. 88 i 220

+: 44

:-21

:-42

:-20

I:

S: Quyidagi ifodani qiymatini toping.  $-16 \bmod 11$

+: 6

:-5

:-7

:-11

I:

S: 2 soniga 10 modul bo'yicha teskari sonni toping.

+:  $\emptyset$

:-3

:-10

:-25

I:

S: 2 soniga 10 modul bo'yicha teskari sonni toping.

+:  $\emptyset$

:-3

:-10

:-25

I:

S: DES da dastlabki kalit uzunligi necha bitga teng?

+:56 bit

:-128 bit

:-64 bit

:-32 bit

I:

S: DES da bloklar har birining uzunligi necha bitga teng?

+:32 bit

:-56 bit

-:48 bit

-:64 bit

I:

S: DES da raundlar soni nechta?

+:16

-:32

-:8

-:48

I:

S: Shifrlash kaliti noma'lum bo'lganda shifrlangan

ma'lumotni deshifrlash qiyinlik darajasini nima belgilaydi

+:kriptobardoshlik

-:Shifr matn uzunligi

-:Shifrlash algoritmi

-:Texnika va texnologiyalar

I:

S: Barcha simmetrik shifrlash algoritmlari qanday

shifrlash usullariga bo'linadi

+:blokli va oqimli

-:DES va oqimli

-:Feystel va Verman

-:SP- tarmoq va IP

I:

S: DES shifrlash algoritmida shifrlanadigan malumotlar

bloki necha bit?

+:64

-:32

-:48

-:56

I:

S: XOR amali qanday amal?

+:2 modul bo'yicha qo'shish

-:264 modul bo'yicha qo'shish

-:232 modul bo'yicha qo'shish

-:248 modul bo'yicha qo'shish

I:

S:  $4+31 \bmod 32$  ?

+:3

-:4

-:31

-:32

I:

S:  $21+20 \bmod 32$ ?

+:9

-:12

-:16

-:41

I:

S:  $12+22 \bmod 32$  ?

+:2

-:12

-:22

-:32

I:

S: AES algoritmi bloki uzunligi ... bitdan kam  
bo'lmisligi kerak.

+:128

-:512

-:256

-:192

I:

S: Xesh-:funktsiyani natijasi ...

+:fiksirlangan uzunlikdagi xabar

-:Kiruvchi xabar uzunligidagi xabar

-:Kiruvchi xabar uzunligidan uzun xabar

-:fiksirlanmagan uzunlikdagi xabar

I:

S:  $2+5 \bmod 32$  ?

+:7

-:32

-:2

-:5



I:

S: 97 tub sonmi?

+:Tub

-:murakkab

-:Natural

-:To'g'ri javob yo'q

I:

S: Ikkilik sanoq tizimida berilgan 10111 sonini o'nlik sanoq tizimiga o'tkazing.

+:23

-:20

-:21

-:19

I:

S: Quyidagi ifodani qiymatini toping.  $-17 \bmod 11$

+:5

-:6

-:7

-:11

I:

S: Diskni shifrlash nima uchun amalga oshiriladi?

+: Ma'lumotni saqlash vositalarida saqlangan ma'lumot konfidensialligini ta'minlash uchun amalga oshiriladi

-:Xabarni yashirish uchun amalga oshiriladi

-:Ma'lumotni saqlash vositalarida saqlangan ma'lumot butunligini ta'minlash uchun amalga oshiriladi

-:Ma'lumotni saqlash vositalarida saqlangan ma'lumot foydalanuvchanligini ta'minlash uchun amalga oshiriladi

I:

S: Ma'lumotlarni yo'q qilish odatda necha hil usulidan foydalaniladi?

+: 4

-:8

-:7

-:5

I:

S: OSI modelida nechta tarmoq satxi bor

+: 7

-:6

-:5

-:4

I:

S: Diskni shifrlash nima uchun amalga oshiriladi?

+: Ma'lumotni saqlash vositalarida saqlangan ma'lumot  
konfidensialligini ta'minlash uchun amalga oshiriladi

-:Xabarni yashirish uchun amalga oshiriladi

-:Ma'lumotni saqlash vositalarida saqlangan ma'lumot  
butunligini ta'minlash uchun amalga oshiriladi

-:Ma'lumotni saqlash vositalarida saqlangan ma'lumot  
foydalanuvchanligini ta'minlash uchun amalga oshiriladi

I:

S: Ma'lumotlarni yo'q qilish odatda necha hil usulidan  
foydalaniladi?

+: 4

-:8

-:7

-:5

I:

S: OSI modelida nechta tarmoq satxi bor

+: 7

-:6

-:5

-:4

I:

S: "Axborot erkinligi prinsiplari va kafolatlari  
to'g'risida"gi qonun moddadan iborat

+:16

-:18

-:11

-:14

I:

S: Kompyuter etikasi instituti notijoriy tashkilot

tomonidan texnologiyani axloqiy nuqta nazardan targ'ib

qilish bo'yicha nechta etika qoidalari keltirilgan

+:10

-:18

-:11

-:14

I:

S: Kiberjinoyatchilik bu —. . .

+: Kompyuter yoki boshqa qurilmalarga qarshi qilingan  
yoki kompyuter va boshqa qurilmalar orqali qilingan  
jinoiy faoliyat.

-: Kompyuter o'yinlari

-: Faqat banklardan pul o'g'irlanishi

-: autentifikatsiya jarayonini buzish

I:

S: Fishing nima?

+: Internetdagi firibgarlikning bir turi bo'lib, uning  
maqsadi foydalanuvchining maxfiy ma'lumotlaridan,  
login/parol, foydalanish imkoniyatiga ega bo'lishdir.

-: Ma'lumotlar bazalarini xatoligi

-: Mualliflik huquqini buzilishi

-: Lug'at orqali xujum qilish.

I:

S: Bag nima?

+: Dasturiy ta'minotni amalga oshirish bosqichiga tegishli  
bo'lgan muammo

-: Mualliflik huquqini buzilishi

-: Dasturlardagi ortiqcha reklamalar

-: Autentifikatsiya jarayonini buzish

I:

S: Nuqson nima?

+: Dasturni amalga oshirishdagi va loyixalashdagi  
zaifliklarning barchasi nuqsondir

-: Dasturiy ta'minotni amalga oshirish bosqichiga tegishli  
bo'lgan muammo

-: Dasturlardagi ortiqcha reklamalar

-: Autentifikatsiya jarayonini buzish

I:

S: Quyidagilardan qaysi birida xavfsiz dasturlash tillari keltirilgan.

+: C#, Scala, Java

-: C, C#, java

-: C++, Scala, Java

-: Misra-C, Java, c++

I:

S: Quyidagilardan qaysi biri dasturiy maxsulotlarga qo'yiladigan xavfsizlik talablari hisoblanadi.

+: Vazifaviy, novazifaviy, qolgan talablar

-: Qolgan talablar, anaviy taablar, etika talablari

-: Vazifaviy, novazifaviy, etika talablari.

-: Vazifaviy, etika talablari, foydalanuvchanlik talablari.

I:

S: Dasturiy ta'minotda kirish va chiqishga aloqador bo'lgan talablar qanday talablar sirasiga kiradi?

+:Vazifaviy

-: Novazifaviy

-: Etika talablari

-: Qolgan talablar

I:

S: Dasturda tizim amalga oshirishi kerak bo'lgan vazifalar bu..

+:Vazifaviy

-: Novazifaviy

-: Etika talablari

-: Qolgan talablar

I:

S: Risklarni boshqarishda risklarni aniqlash jarayoni bu-..

+: Tashkilot xavfsizligiga ta'sir qiluvchi tashqi va ichki risklarning manbasi, sababi, oqibati va haklarni aniqlash.

-: Risklarni baholash bosqichi tashkilotning risk darajasini baholaydi va risk ta'siri va ehtimolini o'lchashni ta'minlaydi.

-: Risklarni davolash bu – aniqlangan risklar uchun mos nazoratni tanlash va amalga oshirish jarayoni.

-: Risk monitoringi yangi risklarni paydo bo'lish imkoniyatini aniqlash.

I:

S: Tizim ishlamay turganda yoki foydalanuvchilar ma'lumot bilan ishlamay turganda zahiralash amalga oshirilsa .... deb ataladi.

+: "Sovuq saxiralash"

-: "Issiq zaxiralash"

-: "Iliq saxiralash"

-: "To'liq zaxiralash"

I:

S: Agar axborotning o'g'irlanishi moddiy va ma'naviy boyliklarning yo'qotilishi bilan bog'liq bo'lsa bu nima deb yuritiladi?

+: Jinoyat sifatida baholanadi

-: Rag'bat hisoblanadi

-: Buzgunchilik hisoblanadi

-: Guruhlar kurashi hisoblanadi

I:

S: Asimmetrik kriptotizimlarda axborotni shifrlashda va rasshifrovka qilish uchun qanday kalit ishlatiladi?

+: Ikki kalit

-: Bitta kalit

-: Elektron raqamli imzo

-: Foydalanuvchi identifikatori

I:

S: Axborot xavfsizligida axborotning bahosi qanday aniqlanadi?

+: Axborot xavfsizligi buzulgan taqdirda ko'rilishi mumkin bo'lgan zarar miqdori bilan

-: Axborot xavfsizligi buzulgan taqdirda axborotni foydalanuvchi uchun muhurligi bilan

-: Axborotni noqonuniy foydalanishlardan o'zgartirishlardan va yo'q qilishlardan himoyalanganligi

bilan

-:Axborotni saqlovchi, ishlovchi va uzatuvchi apparat va dasturiy vasitalarning qiymati bilan}

I:

S:Axborot xavfsizligiga bo'ladigan tahdidlarning qaysi biri maqsadli (atayin) tahdidlar deb hisoblanadi?

+:Strukturalarni ruxsatsiz modifikatsiyalash

-:Tabiiy ofat va avariya

-:Texnik vositalarning buzilishi va ishlamasligi

-:Foydalanuvchilar va xizmat ko'rsatuvchi hodimlarning hatoliklari}

I:

S:Axborot xavfsizligiga bo'ladigan tahdidlarning qaysi biri tasodifiy tahdidlar deb hisoblanadi?

+:Texnik vositalarning buzilishi va ishlamasligi

-:Axborotdan ruxsatsiz foydalanish

-:Zararkunanda dasturlar

-:An'anaviy josuslik va diversiya haqidagi ma'lumotlar tahlili}

I:

S:Axborot xavfsizligini ta'minlovchi choralarni ko'rsating?

+:1-huquqiy, 2-tashkiliy-ma'muriy, 3-injener-texnik

-:1-axloqiy, 2-tashkiliy-ma'muriy, 3-fizikaviy-kimyoviy

-:1-dasturiy, 2-tashkiliy-ma'muriy, 3-huquqiy

-:1-aparat, 2-texnikaviy, 3-huquqiy}

I:

S:Axborot xavfsizligining huquqiy ta'minoti qaysi me'yorlarni o'z ichiga oladi

+:Xalqaro va milliy huquqiy me'yorlarni

-:Tashkiliy va xalqaro me'yorlarni

-:Ananaviy va korporativ me'yorlarni

-:Davlat va nodavlat tashkilotlarime'yorlarni}

I:

S:Axborotni uzatish va saqlash jarayonida o'z strukturasi va yoki mazmunini saqlash xususiyati nima deb ataladi?

+: Ma'lumotlar butunligi

-:Axborotning konfidentsialligi

-:Foydalanuvchanligi

-:Ixchamligi}

I:

S:Axborotning buzilishi yoki yo'qotilishi xavfiga olib  
keluvchi himoyalanuvchi ob'ektga qarshi qilingan  
xarakatlar qanday nomlanadi?

+:Tahdid

-:Zaiflik

-:Hujum

-:Butunlik}

I:

S:Biometrik autentifikatsiyalashning avfzalliklari-bu:

+:Biometrik alomatlarining noyoblighi

-:Bir marta ishlatilishi

-:Biometrik alomatlarni o'zgartirish imkoniyati

-:Autentifikatsiyalash jarayonining soddalighi

I:

S: Foydalanish huquqlariga (mualliflikka) ega barcha  
foydalanuvchilar axborotdan foydalana olishliklari-bu:

+:Foydalanuvchanligi

-:Ma'lumotlar butunligi

-:Axborotning konfidentsialligi

-:Ixchamlighi

I:

S:Global simsiz tarmoqning ta'sir doirasi qanday?

+:Butun dunyo bo'yicha

-:Binolar va korpuslar

-:O'rtacha kattalikdagishahar

-:Foydalanuvchi yaqinidagi tarmoq

I:

S: Foydalanuvchini identifikatsiyalashda qanday  
ma'lumotdan foydalaniladi?

+:Identifikatori

-:Telefon raqami

-:Parol

-:Avtorizatsiyasi

I:

S: Foydalanuvchining tarmoqdagi harakatlarini va resurslardan foydalanishga urinishini qayd etish-bu:

+:Ma`murlash

-:Autentifikatsiya

-:Identifikatsiya

-:Sertifikatsiyalash

I:

S: Kompyuter tizimini ruxsatsiz foydalanishdan himoyalashni, muhim kompyuter tizimlarni rezervlash, o'g'irlash va diversiyadan himoyalashni ta'minlash rezerv elektr manbai, xavfsizlikning maxsus dasturiy va apparat vositalarini ishlab chiqish va amalga

+:Injener-texnik

-:Molyaviy

-:Tashkiliy-ma'muriy

-:Huquqiy

I:

S: Ma'lum qilingan foydalanuvchi, jarayon yoki qurilmaning haqiqiy ekanligini tekshirish muolajasi-bu:

+:Autentifikatsiya

-:Identifikatsiya

-:Ma`murlash (accounting)

-:Avtorizatsiya

I:

S: O'zini tarqatishda kompyuter tarmoqlari va elektron pochta protokollari va komandalaridan foydalanadi—bu:

+:Tarmoq viruslari

-:Pochta viruslari

-:Fayl viruslari

-:Protokol viruslari

I:

S: Qanday viruslar xavfli hisoblanadi?

+:kompyuter ishlashida jiddiy nuqsonlarga olib keluvchi



-:Jiddiy nuqsonlarga olib kelmaydigan ammo

foydalanuvchini chalg'itadigan.

-:Katta viruslar va odatda zararli dasturlar

-:Passiv viruslar

I:

S: Rezident bo'lmagan viruslar qachon xotirani

zararlaydi?

+:Faqat faollashgan vaqtida

-:Faqat o'chirilganda

-:Kompyuter yoqilganda

-:Tarmoq orqali ma'lumot almashishda

I:

S: Simli va simsiz tarmoqlar orasidagi asosiy farq

nimadan iborat?

+:Tarmoq chetki nuqtalari orasidagi mutlaqo

nazoratlamaydigan xudud

-:Tarmoq chetki nuqtalari orasidagi xududning kengligi

asosida qurilmalarholati

-:Himoya vositalarining chegaralanganligi

-:Himoyani amalga oshirish imkoniyati yo'qligi va

ma'lum protokollarning ishlatilishi

I:

S: Simmetrik shifrlashning noqulayligi – bu:

+:Maxfiy kalitlar bilan ayirboshlash zaruriyatidir

-:Kalitlar maxfiyligi

-:Kalitlar uzunligi

-:SHifrlashga ko'p vaqt sarflanishi va ko'p yuklanishi

I:

S: Simsiz tarmoqlarni kategoriyalarini to'g'ri ko'rsating?

+:Simsiz shaxsiy tarmoq (PAN), simsiz lokal tarmoq

(LAN), simsiz regional tarmoq (MAN) va Simsiz global

tarmoq (WAN)

-:Simsiz internet tarmoq (IAN )va Simsiz telefon tarmoq

(WLAN), Simsiz shaxsiy tarmoq (PAN) va Simsiz global

tarmoq (WIMAX)

-:Simsiz internet tarmoq (IAN) va uy simsiz tarmog'i

-:Simsiz chegaralanmagan tarmoq (LAN), simsiz kirish

nuqtalari

I:

S: Sub`ektga ma`lum vakolat va resurslarni berish

muolajasi-bu:

+:Avtorizatsiya

-:Haqiqiylikni tasdiqlash

-:Autentifikatsiya

-:Identifikatsiya

I:

S: Tarmoq operatsion tizimining to'g'ri konfiguratsiyasini

madadlash masalasini odatda kim hal etadi?

+:Tizim ma'muri

-:Tizim foydalanuvchisi

-:Korxona raxbari

-:Operator

I:

S: Tarmoqlararo ekran texnologiyasi-bu:

+:Ichki va tashqi tarmoq o'rtasida filtr va himoya

vazifasini bajaradi

-:Ichki va tashqi tarmoq o'rtasida axborotni o'zgartirish

vazifasini bajaradi

-:Qonuniy foydalanuvchilarni himoyalash

-:Ishonchsiz tarmoqdan kirishni boshqarish}

I:

S: Xizmat qilishdan voz kechishga undaydigan

taqsimlangan hujum turini ko'rsating?

+:DDoS (Distributed Denial of Service) hujum

-:Tarmoq hujumlari

-:Dastur hujumlari asosidagi (Denial of Service) hujum

-:Virus hujumlari}

I:

S: Uyiştirilmagan tahdid, ya'ni tizim yoki dasturdagi

qurilmaning jismoniy xatoligi – bu...

+:Tasodifiy tahdid

-:Uyiştirilgan tahdid

-:Faol tahdid

-:Passiv tahdid

I:

S: Axborot xavfsizligi qanday asosiy xarakteristikalariga ega?

+:Butunlik, konfidentsiallik, foydalana olishlik

-:Butunlik, himoya, ishonchlilikni urganib chiqishlilik

-:Konfidentsiallik, foydalana olishlik

-:Himoyalanganlik, ishonchlilik, butunlik

}

I:

S: Tizim ishlamay turganda yoki foydalanuvchilar ma'lumot bilan ishlamay turganda zahiralash amalga oshirilsa .... deb ataladi.

+: "Sovuq saxiralash"

-: "Issiq zaxiralash"

-: "Iliq saxiralash"

-: "To'liq zaxiralash"

I:

S: Agar foydalanuvchi tizimda ma'lumot bilan ishlash vaqtida ham zahiralash amalga oshirilishi .... deb ataladi?

+: "Issiq zaxiralash"

-: "Sovuq saxiralash"

-: "Iliq saxiralash"

-: "To'liq zaxiralash"

I:

S: Ma'lumotlarni zahira nusxasini saqlovchi va tikovchi dasturni belgilang

+: HandyBackup

-: Recuva, R.saver

-: Cryptool

-: Eset32

I:

S: O'chirilgan, formatlangan ma'lumotlarni tikovchi dasturni belgilang.

+: Recuva, R.saver

-:HandyBakcup

-:Cryptool

-:Eset32

I:

S: Virtuallashtirishga qaratilgan dasturiy vositalarni belgilang.

+:VMware, VirtualBox

-:HandyBakcup

-:Eset32

-:Cryptool

I:

S: Cloud Computing texnologiyasi nechta katta turga ajratiladi?

+:3 turga

-:2 turga

-:4 turga

-:5 turga

I:

S: O'rnatilgan tizimlar-bu...

+:Bu ko'pincha real vaqt hisoblash cheklovlariga ega bo'lgan kattaroq mexanik yoki elektr tizimidagi maxsus funksiyaga ega, boshqaruvchidir

-:Korxona ichki tarmog'iga ulangan korporativ tarmog'idan bo'ladigan hujumlardan himoyalash

-:Korxona ichki tarmog'ini Internet global tarmog'idan ajratib qo'yish

-:Bu ko'pincha global tizimda hisoblash cheklovlariga ega bo'lgan mexanik yoki elektr tizimidagi maxsus funksiyaga ega qurilmadir

I:

S: Axborotdan oqilona foydalanish kodeksi qaysi tashkilot tomonidan ishlab chiqilgan?

+:AQSH sog'liqni saqlash va insonlarga xizmat ko'rsatish vazirligi

-:AQSH Mudofaa vazirligi

-:O'zbekiston Axborot texnologiyalari va

kommunikatsiyalarni rivojlantirish vazirligi

-:Rossiya kiberjinoyatlarga qarshu kurashish davlat  
qo'mitasi

I:

S: Axborotdan oqilona foydalanish kodeksi nechanchi yil  
ishlab chiqilgan?

+:1973 yil

-:1980 yil

-:1991 yil

-:2002 yil

I:

S: Kompyuter bilan bog'liq falsafiy soha bo'lib,  
foydalanuvchilarning xatti-harakatlari, kompyuterlar  
nimaga dasturlashtirilganligi va umuman insonlarga va  
jamiyatga qanday ta'sir ko'rsatishini o'rgatadigan soha  
nima deb ataladi?

+:Kiberetika

-:Kiberhuquq

-:Kiberqoida

-:Kiberxavfsizlik

I:

S: Kompyuter yoki boshqa qurilmalarga qarshi qilingan  
yoki kompyuter va boshqa qurilmalar orqali qilingan  
jinoyat-...

+:Kiberjinoyat

-:Kibersport

-:Kiberterror

-:Hakerlar uyushmasi

I:

S: Tarmoqlararo ekran paket filtrlari qaysi sathda  
ishlaydi?

+:Tarmoq sathida

-:Ilova sathida

-:Kanal sathida

-:Fizik sathida

I:

S: Tarmoqlararo ekran ekspert paketi filtrlari qaysi sathda ishlaydi?

+:Transport sathida

-:Ilova sathida

-:Kanal sathida

-:Fizik sathida

I:

S: Spam bilan kurashishning dasturiy uslubida nimalar ko'zda tutiladi?

+:Elektron pochta qutisiga kelib tushadigan ma'lumotlar dasturlar asosida filtrlanib cheklanadi

-:Elektron pochta qutisiga kelib tushadigan spamlar me'yoriy xujjatlar asosida cheklanadi va bloklanadi

-:Elektron pochta qutisiga kelib tushadigan spamlar ommaviy ravishda cheklanadi

-:Elektron pochta qutisiga kelib spamlar mintaqaviy hududlarda cheklanadi

I:

S: Ma'lumotlarni yo'qolish sabab bo'luvchi tabiiy tahdidlarni ko'rsating

+:Zilzila, yong'in, suv toshqini va hak

-:Quvvat o'chishi, dasturiy ta'minot to'satdan o'zgarishi yoki qurilmani to'satdan zararlanishi

-:Tashkilotdagi muhim ma'lumotlarni modifikatsiyalanishi yoki o'g'irlanishi

-:Qasddan yoki tasodifiy ma'lumotni o'chirib yuborilishi, ma'lumotlarni saqlash vositasini to'g'ri joylashtirilmagani

I:

S: Ma'lumotlarni tasodifiy sabablar tufayli yo'qolish sababini belgilang

+:Quvvat o'chishi, dasturiy ta'minot to'satdan o'zgarishi yoki qurilmani to'satdan zararlanishi

-:Tashkilotdagi muhim ma'lumotlarni modifikatsiyalanishi yoki o'g'irlanishi

-:Ma'lumotlarni saqlash vositasini to'g'ri joylashtirilmagani yoki ma'lumotlar bazasini xatolik bilan

boshqarilganligi.

-:Zilzila, yong'in, suv toshqini va hak

I:

S: Ma'lumotlarni inson xatosi tufayli yo'qolish sababini belgilang.

+:Ma'lumotlarni saqlash vositasini to'g'ri joylashtirilmagani yoki ma'lumotlar bazasini xatolik bilan boshqarilganligi.

-:Tashkilotdagi muhim ma'lumotlarni modifikatsiyalanishi yoki o'g'irlanishi

-:Quvvat o'chishi, dasturiy ta'minot to'satdan o'zgarishi yoki qurilmani to'satdan zararlanishi

-:Zilzila, yong'in, suv toshqini va hak

I:

S: Ma'lumotlarni g'arazli hatti harakatlar yo'qolish sababini ko'rsating.

+:Tashkilotdagi muhim ma'lumotlarni modifikatsiyalanishi yoki o'g'irlanishi

-:Quvvat o'chishi, dasturiy ta'minot to'satdan o'zgarishi yoki qurilmani to'satdan zararlanishi

-:Ma'lumotlarni saqlash vositasini to'g'ri joylashtirilmagani yoki ma'lumotlar bazasini xatolik bilan boshqarilganligi.

-:Zilzila, yong'in, suv toshqini va hak

I:

S: Kompyuterda hodisalar haqidagi ma'lumot qayerda saqlanadi?

+:Hodisalar jurnaliga

-:Operativ xotiraga

-:Kesh xotiraga

-:Vaqtinchalik faylga

I:

S: Internet orqali masofada joylashgan kompyuterga yoki tarmoq resurslariga DoS hujumlari uyushtirilishi natijasida..

+:Foydalanuvchilar kerakli axborot resurlariga murojaat

qilish imkoniyatidan mahrum qilinadilar

-:Foydalanuvchilarning maxfiy axborotlari kuzatilib,  
masofadan buzg'unchilarga etkaziladi

-:Axborot tizimidagi ma'lumotlar bazalari o'g'irlanib  
ko'lga kiritilgach, ular yo'q qilinadilar

-:Foydalanuvchilar axborotlariga ruxsatsiz o'zgartirishlar  
kiritilib, ularning yaxlitligi buziladi

I:

S: Dasturlarni buzish va undagi mualliflik huquqini  
buzush uchun yo'naltirilgan buzg'unchi bu - ... .

+:Krakker

-:Hakker

-:Virus bot

-:Ishonchsiz dasturchi

I:

S: Antivirus dasturiy vositalari viruslarni tahlil qilishiga  
ko'ra necha turga bo'linadi?

+:2 turga: fayl Signaturaga va evristikaga asoslangan

-:2 turga: faol va passiv

-:2 turga: pulli va pulsiz

-:2 turga: litsenziyali va ochiq

I:

S: "Parol", "PIN" kodlarni xavfsizlik tomonidan  
kamchiligi nimadan iborat?

+:Foydalanish davrida maxfiylik kamayib boradi

-:Parolni esda saqlash kerak bo'ladi

-:Parolni almashtirish jarayoni murakkabligi

-:Parol uzunligi soni cheklangan

I:

S: Yaxlitlikni buzilishi bu - ...

+:Soxtalashtirish va o'zgartirish

-:Ishonchsizlik va soxtalashtirish

-:Soxtalashtirish

-:Butunmaslik va yaxlitlanmaganlik

I:

S: Tarmoqda joylashgan fayllar va boshqa resurslardan



foydalanishni taqdim etuvchi tarmoqdagi kompyuter

nima?

+:Server

-:Bulutli tizim

-:Superkompyuter

-:Tarmoq

I:

S: Tahdid nima?

+:Tizim yoki tashkilotga zarar yetkazishi mumkin bo'lgan istalmagan hodisa.

-:Tashkilot uchun qadrli bo'lgan ixtiyoriy narsa

-:Bu riskni o'zgartiradigan harakatlar bo'lib

-:Bu noaniqlikning maqsadlarga ta'siri

I:

S: Risk nima?

+:Potensial kuchlanish yoki zarar

-:Potensial foyda yoki zarar

-:Tasodifiy taxdid

-:Katta yo'qotish

I:

S: Qaysi tarmoq kabelining axborot uzatish tezligi yuqori hisoblanadi?

+:Optik tolali

-:O'rama juft

-:Koaksial

-:Telefon kabeli

I:

S: Nima uchun autentifikatsiyalashda parol ko'p qo'llaniladi?

+:Sarf xarajati kam, almashtirish oson

-:Parolni eslab qolish oson

-:Parolni o'g'rishlash qiyin

-:Serverda parollarni saqlash oson

I:

S: Elektron xujjatlarni yo'q qilish usullari qaysilar?

+:Shredirlash, magnitsizlantirish, yanchish

- :Yoqish, ko'mish, yanchish
- :Shredirlash, yoqish, ko'mish
- :Kimyoviy usul, yoqish.

I:

S: Elektron raqamli imzo algoritmi qanday bosqichlardan iborat bo'ladi?

- +:Imzo qo'yish va imzoni tekshirishdan
- :Faqat imzo qo'yishdan
- :Faqat imzoni tekshirishdan
- :Kalitlarni taqsimlashdan

I:

S: Elektron pochtaga kirishda foydalanuvchi qanday autentifikatsiyalashdan o'tadi?

- +:Parol asosida
- :Smart karta asosida
- :Biometrik asosida
- :Ikki tomonlama

I:

S: Qaysi javobda xavfsizlik siyosatini amalga oshirishdagi Jazolar bosqichiga to'g'ri ta'rif berilgan.

- : tashkilot o'z siyosatini ishlab chiqishdan oldin o'z aktivlari uchun risklarni baholashi shart
- : tashkilot o'z xavfsizlik siyosatini ishlab chiqishdan oldin umumiy qoidalarni o'rnatilish shart
- : yangi xavfsizlik siyosatini ishlab chiqish yoki mavjudiga qo'shimcha kiritish jarayonida boshqaruvchi bo'lishi shart
- +: ma'lum tashkilotlarda tashkilotlarda qat'iy siyosatlar mavjud. Agar xodimlar ushbu siyosatlarga amal qilmasa, ularga qarshi bir qancha choralar qo'llaniladi.

I:

S: Qaysi javobda xavfsizlik siyosatini amalga oshirishdagi Xodimlarni o'rgatish bosqichiga to'g'ri ta'rif berilgan.

- : tashkilot o'z siyosatini ishlab chiqishdan oldin o'z aktivlari uchun risklarni baholashi shart
- : tashkilot o'z xavfsizlik siyosatini ishlab chiqishdan

oldin umumiy qoidalarini o'rnatilish shart

-: yangi xavfsizlik siyosatini ishlab chiqish yoki  
mavjudiga qo'shimcha kiritish jarayonida boshqaruvchi  
bo'lishi shart

+: xodimlarga tashkilot xavfsizlik siyosati davomli  
ravishda o'rgatilishi shart

I:

S: Galstuk babochka usuli nima?

+: Risklarni baholash usuli

-: Risklarni qabul qilish usuli

-: shifrlash algoritmi

-: Risklarni hosil qilish usuli.

I:

S: Lotin alifbosida DADA so'zini 3 kalit bilan  
shifrlagandan so'ng qaysi so'z hosil bo'ladi. A=0,  
B=1....Z=25.

+:GDGD

-: NANA

-: GPGP

-: FDFD

I:

S: Lotin alifbosida NON so'zini 3 kalit bilan  
shifrlagandan so'ng qaysi so'z hosil bo'ladi. A=0,  
B=1....Z=25.

+:GDGD

-: NANA

+: QRQ

-: FDFD

I:

S: Fizik to'siqlarni o'rnatish , Xavfsizlik qo'riqchilarini  
ishga olish, Fizik qulflar qo'yishni amalga oshirish  
qanday nazorat turiga kiradi?

+:Fizik nazorat

-: Texnik nazorat

-: Ma'muriy nazorat

-: Tashkiliy nazorat

I:

S: Ruxsatlarni nazoratlash, "Qopqon", Yong'inga qarshi tizimlar, Yoritish tizimlari, Ogohlantirish tizimlari , Quvvat manbalari, Video kuzatuv tizimlari, Qurollarni aniqlash, Muhitni nazoratlash amalga oshirish qanday nazorat turiga kiradi?

-: Fizik nazorat

+: Texnik nazorat

-: Ma'muriy nazorat

-: Tashkiliy nazorat

I:

S: Qoida va muolajalarni yaratish, Joylashuv arxitekturasini loyihalash, Xavfsizlik belgilari va ogohlantirish signallari, Ishchi joy xavfsizligini ta'minlash, Shaxs xavfsizligini ta'minlash amalga oshirish qanday nazorat turiga kiradi?

-: Fizik nazorat

-: Texnik nazorat

+: Ma'muriy nazorat

-: Tashkiliy nazorat

I:

S: Ikkilik sanoq tizimida qanday raqamlardan foydalanamiz?

+: Faqat 0 va 1

-: Faqat 1

-: Faqat 0

-: Barcha raqamlardan

I:

S: AES shifrlash algoritmi necha rounddan iborat

+: 10, 12, 14

-: 10,14,16

-: 12,14,16

-: 16

I:

S: Hodisalar daraxti usuli nima?

+: Risklarni baholash usuli

-: Risklarni qabul qilish usuli

-: shifrlash algoritmi

-: Risklarni hosil qilish usuli

I:

S: Yuliy Sezar ma'lumotlarni shifrlashda alfavit xarflarni nechtaga surib shifrlagan?

+:3 taga

-:4 taga

-:2 taga

-:5 taga

I:

S: WiMAX qanday simsiz tarmoq turiga kiradi.

+: Regional

-: Lokal

-: Global

-: Shaxsiy

I:

S: Wi-Fi necha Gs chastotali to'liqida ishlaydi?

+: 2.4-5 Gs

-: 2.4-2.485 Gs

-: 1.5-11 Gs

-: 2.3-13.6 Gs

I:

S: Quyidagi parollarning qaysi biri "bardoshli parol"ga kiradi?

+: Onx458&hdsh)

+: 12456578

+: salomDunyo

+: Mashina777

I:

S: Parollash siyosatiga ko'ra parol tanlash shartlari qanday?

+: Kamida 8 belgi: katta va kichik xavflar, sonlar ,

kamida bitta maxsus simvol qo'llanishi kerak. -: Kamida 8

belgi: katta va kichik xavflar, sonlar qo'llanishi kerak.

-: Kamida 6 belgi: katta xarflar, sonlar , kamida bitta

maxsus simvol qo'llanishi kerak.

-: Kamida 6 belgi: katta va kichik xarflar, kamida bitta maxsus simvol qo'llanishi kerak.

1. Avtorizatsiya tushunchasi odatda qaysi tushuncha bilan sinonim sifatida ham foydalanadi?

Foydalanishni boshqarish

2. To'rtta bir-biri bilan bog'langan bog'lamlar strukturasi (kvadrat shaklida) qaysi topologiya turiga mansub?

Xalqa

3. Ko'z pardasi, yuz tuzilishi, ovoz tembri, -bular autentifikatsiyaning qaysi faktoriga mos belgilar?

Biometrik autentifikatsiya

5. Ruxsatlarni nazoratlash, "Qopqon", Yong'inga qarshi tizimlar, Yoritish tizimlari, Ogohlantirish tizimlari, Quvvat manbalari, Video kuzatuv tizimlari, Qurollarni aniqlash, Muhitni nazoratlash amalga oshirish qanday nazorat turiga kiradi?

Texnik nazorat

6. Ma'lumotlarni yo'qolish sabab bo'luvchi tabiiy tahdidlarni ko'rsating

Zilzila, yong'in, suv toshqini va hak.

7. Token, Smartkartalarda xavfsizlik tomonidan kamchiligi nimada?

Qurilmalarni ishlab chiqarish murakkab jarayon

8. Foydalanishni boshqarish –bu...

Sub'ektni Sub'ektga ishlash qobiliyatini aniqlashdir.

9. Ro'yxatdan o'tish-bu...

foydalanuvchilarni ro'yxatga olish va ularga dasturlar va ma'lumotlarni ishlatishga huquq berish jarayoni

10. MAC usuli bilan foydalanishni boshqarishda xavfsizlik markazlashgan holatda kim tomonidan amalga oshiriladi?

Xavfsizlik siyosati ma'muri

11. MD5, SHA1, SHA256, O'z DSt 1106:2009- qanday algoritmlar deb ataladi?

Shifrlash

12. Shifr nima?

Shifrlash va deshifrlashda foydalaniladigan matematik funktsiyadan iborat bo'lgan kriptografik algoritmlar

13. Ethernet kontsentratori qanday vazifani bajaradi?

kompyuterdan kelayotgan axborotni qolgan barcha kompyuterga yo'naltirib beradi

14. Tekstni boshqa tekst ichida ma'nosini yashirib

keltirish nima deb ataladi?

steganografiya

15. Qaysi juftlik RSA algoritmining ochiq va yopiq

kalitlarini ifodalaydi?

$\{d, n\}$  – yopiq,  $\{e, n\}$  – ochiq;

16. Zimmermann telegrami, Enigma shifri, SIGABA

kriptografiyaning qaysi davriga to'g'ri keladi?

1-2 jahon urushu davri

17. Ochiq kalitli kriptotizimlarning mohiyati nimadan

iborat?

Ochiq kalitli kriptotizimlarda bir-biri bilan matematik

bog'langan 2 ta – ochiq va yopiq kalitlardan foydalaniladi

18. ....–hisoblashga asoslangan bilim sohasi bo'lib,

buzg'unchilar mavjud bo'lgan sharoitda amallarni

kafolatlash uchun o'zida texnologiya, inson, axborot va

jarayonni mujassamlashtirgan.

Kiberxavfsizlik

19. Kriptografiyaning asosiy maqsadi nima?

maxfiylik, yaxlitlikni ta'minlash

20. Foydalanishni boshqarishning qaysi usuli – Ob'ektlar

va Sub'ektlarning atributlari, ular bilan mumkin bo'lgan

amallar va so'rovlarga mos keladigan muhit uchun

qoidalarini tahlil qilish asosida foydalanishlarni

boshqaradi.

ABAC

1. Avtorizatsiya tushunchasi odatda qaysi tushuncha bilan

sinonim sifatida ham foydalanadi?

Foydalanishni boshqarish

2. To'rtta bir-biri bilan bog'langan bog'lamlar strukturasi

(kvadrat shaklida) qaysi topologiya turiga mansub?

Xalqa

3. Ko'z pardasi, yuz tuzilishi, ovoz tembri, -bular autentifikatsiyaning qaysi faktoriga mos belgilar?

Biometrik autentifikatsiya

5. Ruxsatlarni nazoratlash, "Qopqon", Yong'inga qarshi tizimlar, Yoritish tizimlari, Ogohlantirish tizimlari, Quvvat manbalari, Video kuzatuv tizimlari, Qurollarni aniqlash, Muhitni nazoratlash amalga oshirish qanday nazorat turiga kiradi?

Texnik nazorat

6. Ma'lumotlarni yo'qolish sabab bo'luvchi tabiiy tahdidlarni ko'rsating

Zilzila, yong'in, suv toshqini va hak.

9. Ro'yxatdan o'tish-bu...

foydalanuvchilarni ro'yxatga olish va ularga dasturlar va ma'lumotlarni ishlatishga huquq berish jarayoni

10. MAC usuli bilan foydalanishni boshqarishda xavfsizlik markazlashgan holatda kim tomonidan amalga oshiriladi?

Xavfsizlik siyosati ma'muri

12. Shifr nima?

Shifrlash va deshifrlashda foydalaniladigan matematik funktsiyadan iborat bo'lgan kriptografik algoritim

13. Ethernet kontsentratori qanday vazifani bajaradi?

kompyuterdan kelayotgan axborotni qolgan barcha kompyuterga yo'naltirib beradi

14. Tekstni boshqa tekst ichida ma'nosini yashirib keltirish nima deb ataladi?

steganografiya

15. Qaysi juftlik RSA algoritmining ochiq va yopiq kalitlarini ifodalaydi?

$\{d, n\}$  – yopiq,  $\{e, n\}$  – ochiq;

16. Zimmermann telegrami, Enigma shifri, SIGABA kriptografiyaning qaysi davriga to'g'ri keladi?

1-2 jahon urushu davri



17. Ochiq kalitli kriptotizimlarning mohiyati nimadan iborat?

Ochiq kalitli kriptotizimlarda bir-biri bilan matematik bog'langan 2 ta – ochiq va yopiq kalitlardan foydalaniladi

18. ....–hisoblashga asoslangan bilim sohasi bo'lib, buzg'unchilar mavjud bo'lgan sharoitda amallarni kafolatlash uchun o'zida texnologiya, inson, axborot va jarayonni mujassamlashtirgan.

Kiberxavfsizlik

19. Kriptografiyaning asosiy maqsadi nima?

maxfiylik, yaxlitlilikni ta'minlash

1. Ma'lumotlarni zahira nusxasini saqlovchi va tikovchi dasturni belgilang.

HandyBackup

2. Makroviruslar nimalarni zararlaydi?

Ma'lum dasturlash tilida yozilgan va turli ofis ilovalari – MS Word hujjati, MS Excel elektron jadvali, Corel Draw tasviri, fayllarida joylashgan "makroslar" yoki "skriptlar"ni zararlaydi.

3. Ehtiyotkorlik siyosati (Prudent Policy) – bu ....

Barcha xizmatlar blokirovka qilingandan so'ng bog'lanadi

4. Qaysi siyosatga ko'ra faqat ma'lum xavfli xizmatlar/hujumlar yoki harakatlar bloklanadi?

Ruxsat berishga asoslangan siyosat

5. Nuqson atamasiga berilgan ma'noni ko'rsating.

Dasturni amalga oshirishdagi va loyixalashdagi zaifliklarning barchasi

6. Hamma narsa ta'qiqlanadi. Bu qaysi xavfsizlik siyosatiga hos?

Paranoid siyosati (Paranoid Policy)

7. "Axborot olish va kafolatlari va erkinligi to'g'risda"gi

Qonuni qachon kuchga kirgan?

1997 yil 24 aprel

8. Adware-zararli dastur vazifasi nimadan iborat?

marketing maqsadida yoki reklamani namoyish qilish

uchun foydalanuvchini ko'rish rejimini kuzutib boruvchi  
dasturiy ta'minot.

9. Axborot xavfsizligiga bo'ladigan tahdidlarning qaysi  
biri maqsadli (atayin) tahdidlar deb hisoblanadi?

Strukturalarni ruxsatsiz modifikatsiyalash

10. Axborot xavfsizligi boshqaruv tizimida "Aktiv" so'zi  
nimani anglatadi?

Axborot xavfsizligida tashkilot uchun qimmatbaho  
bo'lgan va himoyalaniishi lozim bo'lgan narsalar

11. Fishing (ing. Fishing – baliq ovlash) bu...

Internetdagi firibgarlikning bir turi bo'lib, uning maqsadi  
foydalanuvchining maxfiy ma'lumotlaridan, login/parol,  
foydalanish imkoniyatiga ega bo'lishdir.

12. Ma'lumotlarni zaxira nusxalash bu – ...

Muhim bo'lgan axborot nusxalash yoki saqlash jarayoni.

13. .... riskni tutuvchi mos nazorat usuli amalga  
oshirilganligini kafolatlaydi.

Risk monitoring

14. O'chirilgan yoki formatlangan ma'lumotlarni tikovchi  
dasturni belgilang.

Recuva, R.saver

15. "Avtorizatsiya" atamasi qaysi tushuncha bilan  
sinonim sifatida ham foydalanadi?

Foydalanishni boshqarish

16. Kiberetika tushunchasi:

Kompyuter va kompyuter tarmoqlarida odamlarning  
etikasi

17. Rootkits-qanday zararli dastur?

ushbu zararli dasturiy vosita operatsion tizim tomonidan  
aniqlanmasligi uchun ma'lum harakatlarini yashiradi.

18. "Fishing" tushunchasi:

Tashkilot va odamlarning maxsus va shaxsiy  
ma'lumotlarini olishga qaratilgan internet-hujumi

19. Enterprise Information Security Policies, EISP-bu...

Tashkilot axborot xavfsizligi siyosati

20. Asosan tarmoq, tizim va tashkilot haqidagi axborot

olish maqsadda amalga oshiriladigan tarmoq hujumi

qaysi?

Razvedka hujumlari

1. Hamma narsa ta'qiqlanadi. Bu qaysi xavfsizlik

siyosatiga hos?

Paranoid siyosati (Paranoid Policy)

2. Spam bilan kurashishning dasturiy uslubida nimalar

ko'zda tutiladi?

Elektron pochta qutisiga kelib tushadigan ma'lumotlar

dasturlar asosida filtrlanib cheklanadi.

3. Axborot xavfsizligida axborotning bahosi qanday

aniqlanadi?

Axborot xavfsizligi buzilgan taqdirda ko'rilishi mumkin

bo'lgan zarar miqdori bilan

4. Antiviruslarni, qo'llanish usuliga ko'ra... turlari

mavjud?

detektorlar, faglar, vaktsinalar, privivkalar, revizorlar,

monitorlar

5. "Axborotlashtirish to'g'risida"gi Qonunning maqsadi

nimadan iborat?

Axborotlashtirish, axborot resurslari va axborot

tizimlaridan foydalanish sohasidagi munosabatlarni

tartibga solish.

6. Ma'lumotlarni bloklarga bo'lib, bir qancha (kamida

ikkita) qattiq diskda rezerv nusxasini yozish qaysi

texnologiya?

RAID 0

7. "Avtorizatsiya" atamasi qaysi tushuncha bilan sinonim

sifatida ham foydalanadi?

Foydalanishni boshqarish

8. "Elektron hujjat" tushunchasi haqida to'g'ri ta'rif

berilgan qatorni ko'rsating.

Elektron shaklda qayd etilgan, elektron raqamli imzo

bilan tasdiqlangan va elektron hujjatning uni

identifikatsiya qilish imkoniyatini beradigan boshqa

rekvizitlariga ega bo'lgan axborot elektron hujjatdir

9. Doktorlar, detektorlarga xos bo'lgan ishni bajargan holda zararlangan fayldan viruslarni chiqarib tashlaydigan va faylni oldingi holatiga qaytaradigan dasturiy ta'minot nomini belgilang.

Faglar

10. Dastlabki virus nechanchi yilda yaratilgan?

1986

11. Rezident virus...

tezkor xotirada saqlanadi

12. Zaiflik – bu...

tizimda mavjud bo'lgan xavfsizlik muammoasi bo'lib, ular asosan tizimning yaxshi shakllantirilmaganligi yoki sozlanmaganligi sababli kelib chiqadi.

13. Asosan tarmoq, tizim va tashkilot haqidagi axborot olish maqsadda amalga oshiriladigan tarmoq hujumi qaysi?

Razvedka hujumlari

14. Virusning signaturasi (virusga taalluqli baytlar ketmaketligi) bo'yicha operativ xotira va fayllarni ko'rish natijasida ma'lum viruslarni topuvchi va xabar beruvchi dasturiy ta'minot nomi nima deb ataladi?

Detektorlar

15. Makroviruslar nimalarni zararlaydi?

Ma'lum dasturlash tilida yozilgan va turli ofis ilovalari – MS Word hujjati, MS Excel elektron jadvali, Corel Draw tasviri, fayllarida joylashgan “makroslar” yoki “skriptlar”ni zararlaydi.

16. Texnik himoya vositalari – bu ...

Texnik qurilmalar, komplekslar yoki tizimlar yordamida ob'ektni himoyalashdir

17. Kompyuter yoki boshqa qurilmalarga qarshi qilingan yoki kompyuter va boshqa qurilmalar orqali qilingan jinoyat-...

Kiberjinoyat deb ataladi

19. Issue-Specific Security Policies, ISSP-bu...

Muammofa qaratilgan xavfsizlik siyosati

20. Axborot xavfsizligin ta'minlashda birinchi darajadagi

me'yoriy hujjat nomini belgilang.

qonunlar

1. Foydalanishni boshqarishning qaysi usuli – Ob'ektlar va Sub'ektlarning atributlari, ular bilan mumkin bo'lgan amallar va so'rovlarga mos keladigan muhit uchun qoidalarini tahlil qilish asosida foydalanishlarni boshqaradi.

ABAC

2. MAC usuli bilan foydalanishni boshqarishda xavfsizlik markazlashgan holatda kim tomonidan amalga oshiriladi?

Xavfsizlik siyosati ma'muri

3. Kriptografiyaning asosiy maqsadi nima?

maxfiylik, yaxlitlikni ta'minlash

4. Uning egasi haqiqiylikni aniqlash jarayonida tekshiruv axboroti sifatida ishlatiladigan belgilar ketma-ketligi (maxfiy so'z) – nima?

parol

5. Global simsiz tarmoqda qaysi standartlar ishlaydi?

CDPD, 4G

6. Autentifikatsiya faktorlari nechta?

3 ta

8. Kriptografiyada matn –bu..

alifbo elementlarining tartiblangan to'plami

9. Stenografiya ma'nosi qanday?

sirli yozuv

11. Axborot xavfsizligiga bo'ladigan tahdidlarning qaysi biri tasodifiy tahdidlar deb hisoblanadi?

Texnik vositalarning buzilishi va ishlamasligi

12. Ochiq kalitli kriptotizimlarning mohiyati nimadan iborat?

Ochiq kalitli kriptotizimlarda bir-biri bilan matematik bog'langan 2 ta – ochiq va yopiq kalitlardan foydalaniladi

13. Ma'lumotlar butunligi qanday algritmlar orqali amalga oshiriladi?

Xesh funksiyalar

14. WiMAX qanday simsiz tarmoq turiga kiradi?

Regional

15. Simmetrik shifrlashning noqulayligi – bu:

Maxfiy kalitlar bilan ayirboshlash zaruriyatidir

16. Ma'lumotlarni yo'qolish sabab bo'luvchi tabiiy

tahdidlarni ko'rsating

Zilzila, yong'in, suv toshqini va hak.

17. Ma'lumotlarni tasodifiy sabablar tufayli yo'qolish

sababini belgilang

Quvvat o'chishi, dasturiy ta'minot to'satdan o'zgarishi

yoki qurilmani to'satdan zararlanishi

18. Ko'z pardasi, yuz tuzilishi, ovoz tembri, -bular

autentifikatsiyaning qaysi faktoriga mos belgilar?

Biometrik autentifikatsiya

1. Yuliy Sezar ma'lumotlarni shifrlashda alfavit xarflarni

nechtaga surib shifrlagan?

3 taga

2. Kriptotizimga qo'yiladigan umumiy talablardan biri

nima?

shifr matn uzunligi ochiq matn uzunligiga teng bo'lishi

kerak

3. Autentifikatsiya faktorlari nechta?

3 ta

4. Axborot xavfsizligining asosiy maqsadlaridan biri-bu...

Axborotlarni o'g'irlanishini, yo'qolishini,

soxtalashtirilishini oldini olish

5. Ma'lumotlarni inson xatosi tufayli yo'qolish sababini

belgilang.

Ma'lumotlarni saqlash vositasini to'g'ri

joylashtirilmagani yoki ma'lumotlar bazasini xatolik bilan

boshqarilganligi.

6. Qaysi tarmoq kabelining axborot uzatish tezligi yuqori

hisoblanadi?

Optik tolali

7. Ma'lumotlar butunligi qanday algritmlar orqali amalga

oshiriladi?

Xesh funksiyalar

8. Zimmermann telegrami, Enigma shifri, SIGABA

kriptografiyaning qaysi davriga to'g'ri keladi?

1-2 jahon urushu davri

9. Foydalanishni boshqarishning qaysi usuli – Ob'ektlar

va Sub'ektlarning atributlari, ular bilan mumkin bo'lgan

amallar va so'rovlarga mos keladigan muhit uchun

qoidalarni tahlil qilish asosida foydalanishlarni

boshqaradi.

ABAC

10. Ochiq kalitli kriptotizimlarning mohiyati nimadan

iborat?

Ochiq kalitli kriptotizimlarda bir-biri bilan matematik

bog'langan 2 ta – ochiq va yopiq kalitlardan foydalaniladi

11. Sub'ektga ma'lum vakolat va resurslarni berish

muolajasi-bu:

Avtorizatsiya

12. Kriptografiyaning asosiy maqsadi nima?

maxfiylik, yaxlitlikni ta'minlash

13. Identifikatsiya bu- ...

Foydalanuvchini uning identifikatori (nomi) bo'yicha

aniqlash jarayoni

14. Fire Wall ning vazifasi...

Tarmoqlar orasida aloqa o'rnatish jarayonida tashkilot va

Internet tarmog'i orasida xavfsizlikni ta'minlaydi

15. Kiberjinoyatchilik bu – . . .

Kompyuter yoki boshqa qurilmalarga qarshi qilingan yoki

kompyuter va boshqa qurilmalar orqali qilingan jinoiy

faoliyat.

16. Berilgan ta'riflardan qaysi biri asimmetrik tizimlarga

xos?

Asimmetrik kriptotizimlarda  $k_1 \neq k_2$  bo'lib,  $k_1$  ochiq kalit,

$k_2$  yopiq kalit deb yuritiladi,  $k_1$  bilan axborot shifrlanadi,

$k_2$  bilan esa deshifrlanadi

17. Biometrik autentifikatsiyalashning avfzalliklari-bu:

Biometrik parametrlarning noyobligi

18. "Parol", "PIN" kodlarni xavfsizlik tomonidan

kamchiligi nimadan iborat?

Foydalanish davrida maxfiylik kamayib boradi

19. Kriptografiyada kalitning vazifasi nima?

1. Spyware-qanday zararli dastur?

Foydalanuvchi ma'lumotlarini qo'lga kirituvchi va uni hujumchiga yuboruvchi dasturiy kod.

2. Axborot xavfsizligin ta'minlashda birinchi darajadagi me'yoriy hujjat nomini belgilang.

Qonunlar

3. Adware-zararli dastur vazifasi nimadan iborat?

marketing maqsadida yoki reklamani namoyish qilish uchun foydalanuvchini ko'rish rejimini kuzutib boruvchi dasturiy ta'minot.

4. Ma'lumotlarni zahira nusxasini saqlovchi va tikovchi dasturni belgilang.

HandyBackup

5. Qaysi texnologiyada ma'lumotlarni bir necha disklarda bayt satxida ajratilgan xolda yoziladi va nazorat bitlari ham ular ichida taqsimlanadi?

RAID 5

6. Axborot xavfsizligi boshqaruv tizimida "Aktiv" so'zi nimani anglatadi?

Axborot xavfsizligida tashkilot uchun qimmatbaho bo'lgan va himoyalaniishi lozim bo'lgan narsalar

7. Dasturlarni buzish va undagi mualliflik huquqini buzush uchun yo'naltirilgan buzg'unchi bu - ... .

Kraker

8. Qaysi siyosatga ko'ra hamma narsa ta'qiqlanadi?

Paranoid siyosat

9. .... riskni tutuvchi mos nazorat usuli amalga oshirilganligini kafolatlaydi.

Risk monitoring

10. Ehtiyotkorlik siyosati (Prudent Policy) – bu ....

Barcha xizmatlar blokirovka qilingandan so'ng bog'lanadi

11. Xizmat qilishdan voz kechishga undaydigan



taqsimlangan hujum turini ko'rsating?

DDoS (Distributed Denial of Service) hujum

12. Kiberetika tushunchasi:

Kompyuter va kompyuter tarmoqlarida odamlarning etikasi

13. "Elektron hujjat" tushunchasi haqida to'g'ri ta'rif berilgan qatorni ko'rsating.

Elektron shaklda qayd etilgan, elektron raqamli imzo bilan tasdiqlangan va elektron hujjatning uni identifikatsiya qilish imkoniyatini beradigan boshqa rekvizitlariga ega bo'lgan axborot elektron hujjatdir

14. "Avtorizatsiya" atamasi qaysi tushuncha bilan sinonim sifatida ham foydalanadi?

Foydalanishni boshqarish

15. Polimorf viruslar tushunchasi to'g'ri ko'rsating.

Viruslar turli ko'rinishdagi shifrlangan viruslar bo'lib, o'zining ikkilik shaklini nusxadan-nusxaga o'zgartirib boradi

16. Rezident virus...

tezkor xotirada saqlanadi

17. Hamma narsa ta'qiqlanadi. Bu qaysi xavfsizlik siyosatiga hos?

Paranoid siyosati (Paranoid Policy)

1. Kiberetika tushunchasi:

Kompyuter va kompyuter tarmoqlarida odamlarning etikasi

2. "Avtorizatsiya" atamasi qaysi tushuncha bilan sinonim sifatida ham foydalanadi?

Foydalanishni boshqarish

3. Doktorlar, detektorlarga xos bo'lgan ishni bajargan holda zararlangan fayldan viruslarni chiqarib tashlaydigan va faylni oldingi holatiga qaytaradigan dasturiy ta'minot nomini belgilang.

Faglar

4. Zararli dasturlar qanday turlarga bo'linadi?

Dasturdagi zaifliklar(atayin qilingan) va zararli

dasturlar(atayin qilingan)

5. Aksariyat tijorat tashkilotlari uchun ichki tarmoq

xavfsizligini taminlashning zaruriy sharti-bu...

Tarmoqlararo ekranlarning o'rnatilishi

6. Bag atamasini nima ma'noni beradi?

Dasturiy ta'minotni amalga oshirish bosqichiga tegishli

bo'lgan muammo

7. Tashkilotni himoyalash maqsadida amalga oshirilgan

xavfsizlik nazoratini tavsiflovchi yuqori sathli hujjat yoki

hujjatlar to'plami nima deyiladi?

Xavfsizlik siyosat

8. Ma'lumotlarni zahira nusxasini saqlovchi va tikovchi

dasturni belgilang.

HandyBackup

9. DIR viruslari nimani zararlaydi?

FAT tarkibini zararlaydi

10. .... riskni tutuvchi mos nazorat usuli amalga

oshirilganligini kafolatlaydi.

Risk monitoring

11. Nuqson atamasiga berilgan ma'noni ko'rsating.

Dasturni amalga oshirishdagi va loyixalashdagi

zaifliklarning barchasi

12. "Axborot olish kafolatlari va erkinligi to'g'risida"gi

Qonunning 10-moddasi mazmuni qanday?

Axborot manbaini oshkor etmaslik

13. Qaysi siyosat turli hisoblash resurslaridan to'g'ri

foydalanishni belgilaydi?

Maqbul foydalanish siyosati

14. Axborot xavfsizligi boshqaruv tizimida "Aktiv" so'zi

nimani anglatadi?

Axborot xavfsizligida tashkilot uchun qimmatbaho

bo'lgan va himoyalaniishi lozim bo'lgan narsalar

15. O'chirilgan yoki formatlangan ma'lumotlarni tikovchi

dasturni belgilang.

Recuva, R.saver

16. Qaysi texnologiyada ma'lumotlarni bir necha

disklarda bayt satxida ajratilgan xolda yoziladi?

RAID 3

17. Xavfsizlikni ta'minlashning bir yoki bir necha tizimi hamda loyihalashni nazoratlash va ulardan foydalanish xususida to'liq tasavvurga ega shaxs kim deb ataladi?

Xavfsizlik ma'muri (admin)

19. Ma'lumotlarni bloklarga bo'lib, bir qancha (kamida ikkita) qattiq diskda rezerv nusxasini yozish qaysi texnologiya?

RAID 0

20. Qaysi siyosatda Administrator xavfsiz va zarur xizmatlarga individual ravishda ruxsat beradi?

Extiyotkorlik siyosati

1. Ma'lumotlarni yo'qolish sabab bo'luvchi tabiiy tahdidlarni ko'rsating

Zilzila, yong'in, suv toshqini va hak.

2. Shaxsning, axborot kommunikatsiya tizimidan foydalanish huquqiga ega bo'lish uchun foydalaniluvchining maxfiy bo'lmagan qayd yozuvi – bu...

login

3. Berilgan ta'riflardan qaysi biri asimmetrik tizimlarga xos?

Asimmetrik kriptotizimlarda  $k_1 \neq k_2$  bo'lib,  $k_1$  ochiq kalit,  $k_2$  yopiq kalit deb yuritiladi,  $k_1$  bilan axborot shifrlanadi,  $k_2$  bilan esa deshifrlanadi

6. Zimmermann telegrami, Enigma shifri, SIGABA kriptografiyaning qaysi davriga to'g'ri keladi?

1-2 jahon urushu davri

7. Wi-Fi necha Gs chastotali to'lqinda ishlaydi?

2.4-5 Gs

8. Wi-Fi tarmoqlarida quyida keltirilgan qaysi shifrlash protokollaridan foydalaniladi.

WEP, WPA, WPA2

11. Konfidentsiallikga to'g'ri ta'rif keltiring.

axborot inshonchliligi, tarqatilishi mumkin emasligi,

maxfiyligi kafolati;

12. Autentifikatsiya nima?

Ma'lum qilingan foydalanuvchi, jarayon yoki qurilmaning haqiqiy ekanligini tekshirish muolajasi

13. Axborotni uzatish va saqlash jarayonida o'z

strukturalari va yoki mazmunini saqlash xususiyati nima deb ataladi?

Ma'lumotlar butunligi

14. ....–hisoblashga asoslangan bilim sohasi bo'lib,

buzg'unchilar mavjud bo'lgan sharoitda amallarni

kafolatlash uchun o'zida texnologiya, inson, axborot va jarayonni mujassamlashtirgan.

Kiberxavfsizlik

15. Qaysi juftlik RSA algoritmining ochiq va yopiq

kalitlarini ifodalaydi?

$\{d, n\}$  – yopiq,  $\{e, n\}$  – ochiq;

16. Kodlash nima?

Ma'lumotni osongina qaytarish uchun hammaga ochiq

bo'lgan sxema yordamida ma'lumotlarni boshqa formatga o'zgartirishdir

17. Qo'yish, o'rin almashtirish, g'ammalash

kriptografiyaning qaysi turiga bog'liq?

simmetrik kriptotizimlar

18. Kriptografiyada kalitning vazifasi nima?

Matnni shifrlash va shifrini ochish uchun kerakli axborot

19. To'rtta bir-biri bilan bog'langan bog'lamlar

strukturalari (kvadrat shaklida) qaysi topologiya turiga mansub?

Xalqa

20. Axborot xavfsizligiga bo'ladigan tahdidlarning qaysi

biri tasodifiy tahdidlar deb hisoblanadi?

Texnik vositalarning buzilishi va ishlamasligi

1. Konfidentsiallikga to'g'ri ta'rif keltiring.

axborot inshonchiligi, tarqatilishi mumkin emasligi,

maxfiyligi kafolati;

2. Foydalanishni boshqarish –bu...

Sub'ektni Ob'ektga ishlash qobilyatini aniqlashdir.

3. Uning egasi haqiqiyligini aniqlash jarayonida tekshiruv  
axboroti sifatida ishlatiladigan belgilar ketma-ketligi  
(maxfiy so'z) – nima?

parol

4. To'rtta bir-biri bilan bog'langan bog'lamlar strukturasi  
(kvadrat shaklida) qaysi topologiya turiga mansub?

Xalqa

5. Kodlash nima?

Ma'lumotni osongina qaytarish uchun hammaga ochiq  
bo'lgan sxema yordamida ma'lumotlarni boshqa formatga  
o'zgartirishdir

6. Lokal tarmoqlarda keng tarqalgan topologiya turi  
qaysi?

Yulduz

7. Axborotni uzatish va saqlash jarayonida o'z strukturasi  
va yoki mazmunini saqlash xususiyati nima deb ataladi?

Ma'lumotlar butunligi

8. Wi-Fi necha Gs chastotali to'lqinda ishlaydi?

2.4-5 Gs

9. Yaxlitlikni buzilishi bu - ...

Soxtalashtirish va o'zgartirish

10. Zimmermann telegrami, Enigma shifri, SIGABA  
kriptografiyaning qaysi davriga to'g'ri keladi?

1-2 jahon urushu davri

11. Axborot xavfsizligiga bo'ladigan tahdidlarning qaysi  
biri maqsadli (atayin) tahdidlar deb hisoblanadi?

Strukturalarni ruxsatsiz modifikatsiyalash

12. Kriptotizimga qo'yiladigan umumiy talablardan biri  
nima?

shifr matn uzunligi ochiq matn uzunligiga teng bo'lishi  
kerak

13. Risk nima?

Potensial foyda yoki zarar

14. Assimmetrik kriptotizimlar qanday maqsadlarda  
ishlatiladi?

Shifrlash, deshifrlash, ERI yaratish va tekshirish, kalitlar almashish uchun

15. Ma'lumotlarni yo'q qilish odatda necha xil usulidan foydalaniladi?

4 xil

16. MAC usuli bilan foydalanishni boshqarishda xavfsizlik markazlashgan holatda kim tomonidan amalga oshiriladi?

Xavfsizlik siyosati ma'muri

17. Quyidagilardan mintaqaviy tarmoqqa berilgan ta'rifni belgilang.

Odatda ijaraga olingan telekommunikatsiya liniyalaridan foydalanadigan tarmoqlardagi tugunlarni bir-biriga bog'laydi.

3. Ehtiyotkorlik siyosati (Prudent Policy) – bu ....

Barcha xizmatlar blokirovka qilingandan so'ng bog'lanadi

4. Axborot xavfsizligin ta'minlashda birinchi darajadagi me'yoriy hujjat nomini belgilang.

Qonunlar

5. Rootkits-qanday zararli dastur?

ushbu zararli dasturiy vosita operatsion tizim tomonidan aniqlanmasligi uchun ma'lum harakatlarini yashiradi.

6. Qaysi texnologiyada ma'lumotni ko'plab nusxalari bir vaqtda bir necha disklarga yoziladi?

RAID 1

7. "Axborotlashtirish to'g'risida"gi Qonunning maqsadi nimadan iborat?

Axborotlashtirish, axborot resurslari va axborot tizimlaridan foydalanish sohasidagi munosabatlarni tartibga solish.

8. Hamma narsa ta'qiqlanadi. Bu qaysi xavfsizlik siyosatiga hos?

Paranoid siyosati (Paranoid Policy)

10. Qaysi siyosatga ko'ra hamma narsa ta'qiqlanadi?

Paranoid siyosat

11. Tizim ishlamay turganda yoki foydalanuvchilar ma'lumot bilan ishlamay turganda zahiralash amalga oshirilsa .... deb ataladi.

"Sovuq saxiralash"

12. Virusning signaturasi (virusga taalluqli baytlar ketmaketligi) bo'yicha operativ xotira va fayllarni ko'rish natijasida ma'lum viruslarni topuvchi va xabar beruvchi dasturiy ta'minot nomi nima deb ataladi?

Detektorlar

13. Dasturlarni buzish va undagi mualliflik huquqini buzush uchun yo'naltirilgan buzg'unchi bu - ... .

Kraker

14. "Fishing" tushunchasi:

Tashkilot va odamlarning maxsus va shaxsiy ma'lumotlarini olishga qaratilgan internet-hujumi

15. O'zbekiston Respublikasi hududida turli ijtimoiy tarmoqlar platformalari cheklanishiga "Shaxsga doir ma'lumotlar to'g'risida"gi Qonunning qaysi moddasi sabab qilib olingan?

27(1)-modda. O'zbekiston Respublikasi fuqarolarining shaxsga doir ma'lumotlariga ishlov berishning alohida shartlari

16. Ma'lumotlarni zaxira nusxalash bu – ...

Muhim bo'lgan axborot nusxalash yoki saqlash jarayoni.

17. Fishing (ing. Fishing – baliq ovlash) bu...

Internetdagi firibgarlikning bir turi bo'lib, uning maqsadi foydalanuvchining maxfiy ma'lumotlaridan, login/parol, foydalanish imkoniyatiga ega bo'lishdir.

18. Dastlabki virus nechanchi yilda yaratilgan?

1986

19. "Backdoors"-qanday zararli dastur?

zararli dasturiy kodlar bo'lib, hujumchiga autentifikatsiyani amalga oshirmasdan aylanib o'tib tizimga kirish imkonini beradi, maslan, administrator parolisiz imtiyozga ega bo'lish

20. Kiberetika tushunchasi:

Kompyuter va kompyuter tarmoqlarida odamlarning

etikasi

3. Ma'lumotlarni yo'q qilish odatda necha xil usulidan foydalaniladi?

4 xil

4. Ko'z pardasi, yuz tuzilishi, ovoz tembri, -bular autentifikatsiyaning qaysi faktoriga mos belgilar?

Biometrik autentifikatsiya

5. Rol tushunchasiga ta'rif bering.

Muayyan faoliyat turi bilan bog'liq harakatlar va majburiyatlar to'plami sifatida belgilanishi mumkin

6. Identifikatsiya bu- ...

Foydalanuvchini uning identifikatori (nomi) bo'yicha aniqlash jarayoni

7. Shifr nima?

Shifrlash va deshifrlashda foydalaniladigan matematik funktsiyadan iborat bo'lgan kriptografik algoritim

8. Ma'lumotlarni inson xatosi tufayli yo'qolish sababini belgilang.

Ma'lumotlarni saqlash vositasini to'g'ri joylashtirilmagani yoki ma'lumotlar bazasini xatolik bilan boshqarilganligi.

10. Stenografiya ma'nosi qanday?

sirli yozuv

11. OSI modelida nechta sath mavjud?

7 ta

12. Kriptografiyada kalitning vazifasi nima?

Matnni shifrlash va shifrini ochish uchun kerakli axborot

13. Qanday tarmoq qisqa masofalarda qurilmalar o'rtasida ma'lumot almashinish imkoniyatini taqdim etadi?

Shaxsiy tarmoq

15. Risk nima?

Potensial foyda yoki zarar

16. Kodlash nima?

Ma'lumotni osongina qaytarish uchun hammaga ochiq bo'lgan sxema yordamida ma'lumotlarni boshqa formatga o'zgartirishdir



17. Foydalanishni boshqarishning qaysi usuli – Ob'ektlar va Sub'ektlarning atributlari, ular bilan mumkin bo'lgan amallar va so'rovlarga mos keladigan muhit uchun qoidalarni tahlil qilish asosida foydalanishlarni boshqaradi.

ABAC

18. Shaxsning, axborot kommunikatsiya tizimidan foydalanish huquqiga ega bo'lish uchun foydalaniluvchining maxfiy bo'lmagan qayd yozuvi – bu...

login

19. Zamonaviy kriptografiya qanday bo'limlardan iborat?

Simmetrik kriptotizimlar; ochiq kalitli kriptotizimlar;

Elektron raqamli imzo; kalitlarni boshqarish

1. Spam bilan kurashishning dasturiy uslubida nimalar ko'zda tutiladi?

Elektron pochta qutisiga kelib tushadigan ma'lumotlar dasturlar asosida filtrlanib cheklanadi.

2. Ma'lumotlarni bloklarga bo'lib, bir qancha (kamida ikkita) qattiq diskda rezerv nusxasini yozish qaysi texnologiya?

RAID 0

3. Tizim ishlamay turganda yoki foydalanuvchilar ma'lumot bilan ishlamay turganda zahiralash amalga oshirilsa .... deb ataladi.

"Sovuq saxiralash"

4. Xavfsizlikni ta'minlashning bir yoki bir necha tizimi hamda loyihalashni nazoratlash va ulardan foydalanish xususida to'liq tasavvurga ega shaxs kim deb ataladi?

Xavfsizlik ma'muri (admin)

5. Qaysi texnologiyada ma'lumotlarni bir necha disklarda bayt satxida ajratilgan xolda yoziladi va nazorat bitlari ham ular ichida taqsimlanadi?

RAID 5

6. Tashkilotni himoyalash maqsadida amalga oshirilgan xavfsizlik nazoratini tavsiflovchi yuqori sathli hujjat yoki

hujjatlar to'plami nima deyiladi?

Xavfsizlik siyosat

7. Fishing (ing. Fishing – baliq ovlash) bu...

Internetdagi firibgarlikning bir turi bo'lib, uning maqsadi foydalanuvchining maxfiy ma'lumotlaridan, login/parol, foydalanish imkoniyatiga ega bo'lishdir.

8. Bag atamasini nima ma'noni beradi?

Dasturiy ta'minotni amalga oshirish bosqichiga tegishli bo'lgan muammo

9. "Backdoors"-qanday zararli dastur?

zararli dasturiy kodlar bo'lib, hujumchiga autentifikatsiyani amalga oshirmasdan aylanib o'tib tizimga kirish imkonini beradi, maslan, administrator parolisiz imtiyozga ega bo'lish

10. Dastlabki virus nechanchi yilda yaratilgan?

1986

11. Virusning signaturasi (virusga taalluqli baytlar ketmaketligi) bo'yicha operativ xotira va fayllarni ko'rish natijasida ma'lum viruslarni topuvchi va xabar beruvchi dasturiy ta'minot nomi nima deb ataladi?

Detektorlar

12. Risk monitoringi ..... ni paydo bo'lish imkoniyatini aniqlaydi.

Yangi risklar

13. Ransomware qanday zarar keltiradi?

mazkur zararli dasturiy ta'minot qurbon kompyuterida mavjud qimmatli fayllarni shifrlaydi yoki qulflab qo'yib, to'lov amalga oshirilishini talab qiladi.

14. O'zbekiston Respublikasi hududida turli ijtimoiy tarmoqlar platformalari cheklanishiga "Shaxsga doir ma'lumotlar to'g'risida"gi Qonunning qaysi moddasi sabab qilib olingan?

27(1)-modda. O'zbekiston Respublikasi fuqarolarining shaxsga doir ma'lumotlariga ishlov berishning alohida shartlari

15. Texnik himoya vositalari – bu ...

Texnik qurilmalar, komplekslar yoki tizimlar yordamida

ob'ektni himoyalashdir

17. Enterprise Information Security Policies, EISP-bu...

Tashkilot axborot xavfsizligi siyosati

18. Qaysi siyosatga ko'ra hamma narsa ta'qiqlanadi?

Paranoid siyosat

19. "Fishing" tushunchasi:

Tashkilot va odamlarning maxsus va shaxsiy

ma'lumotlarini olishga qaratilgan internet-hujumi

20. Axborot xavfsizligining huquqiy ta'minoti qaysi

me'yorlarni o'z ichiga oladi?

Xalqaro va milliy huquqiy me'yorlarni

1. "Fishing" tushunchasi:

Tashkilot va odamlarning maxsus va shaxsiy

ma'lumotlarini olishga qaratilgan internet-hujumi

2. Dasturlarni buzish va undagi mualliflik huquqini

buzush uchun yo'naltirilgan buzg'unchi bu - ... .

Kraker

3. Agar foydalanuvchi tizimda ma'lumot bilan ishlash

vaqtida ham zahiralash amalga oshirilishi .... deb ataladi?

"Issiq zaxiralash"

4. Xizmat qilishdan voz kechishga undaydigan

taqsimlangan hujum turini ko'rsating?

DDoS (Distributed Denial of Service) hujum

5. Nuqson atamasiga berilgan ma'noni ko'rsating.

Dasturni amalga oshirishdagi va loyixalashdagi

zaifliklarning barchasi

6. Risklarni identifikatsiya qilishdan maqsad nima?

Potensial zarar yetkazadigan ehtimoliy insidentlarni

prognozlash va bu zarar qay tarzda olinishi mumkinligi

to'g'risida tasavvurga ega bo'lish

7. Dastlabki virus nechanchi yilda yaratilgan?

1986

8. Rootkits-qanday zararli dastur?

ushbu zararli dasturiy vosita operatsion tizim tomonidan

aniqlanmasligi uchun ma'lum harakatlarini yashiradi.

9. Qaysi siyosatga ko'ra hamma narsa ta'qiqlanadi?

Paranoid siyosat

10. Ko'p platformali viruslar bu...

Bir vaqtning o'zida turli xildagi ob'ektlarni zararlaydi.

Masalan, OneHalf.3544 virusi ham MS-DOS dasturlari ham qattiq diskning yuklanuvchi sektorlarini zararlaydi

11. "Axborot olish kafolatlari va erkinligi to'g'risida"gi

Qonunning 10-moddasi mazmuni qanday?

Axborot manbaini oshkor etmaslik

12. Risk monitoringi ..... ni paydo bo'lish imkoniyatini aniqlaydi.

Yangi risklar

13. "Elektron hujjat" tushunchasi haqida to'g'ri ta'rif berilgan qatorni ko'rsating.

Elektron shaklda qayd etilgan, elektron raqamli imzo bilan tasdiqlangan va elektron hujjatning uni

identifikatsiya qilish imkoniyatini beradigan boshqa

rekvizitlariga ega bo'lgan axborot elektron hujjatdir

15. O'zbekiston Respublikasi hududida turli ijtimoiy tarmoqlar platformalari cheklanishiga "Shaxsga doir ma'lumotlar to'g'risida"gi Qonunning qaysi moddasi sabab qilib olingan?

27(1)-modda. O'zbekiston Respublikasi fuqarolarining shaxsga doir ma'lumotlariga ishlov berishning alohida shartlari

16. Qaysi texnologiyada ma'lumotlarni bir necha disklarda bayt satxida ajratilgan xolda yoziladi va nazorat bitlari ham ular ichida taqsimlanadi?

RAID 5

17. Axborot xavfsizligiga bo'ladigan tahdidlarning qaysi biri maqsadli (atayin) tahdidlar deb hisoblanadi?

Strukturalarni ruxsatsiz modifikatsiyalash

18. "Backdoors"-qanday zararli dastur?

zararli dasturiy kodlar bo'lib, hujumchiga

autentifikatsiyani amalga oshirmasdan aylanib o'tib

tizimga kirish imkonini beradi, maslan, administrator

parolisiz imtiyozga ega bo'lish

19. Botnet-nima?

internet tarmog'idagi obro'sizlantirilgan kompyuterlar bo'lib, taqsimlangan hujumlarni amalga oshirish uchun hujumchi tomonidan foydalaniladi.

20. Axborot xavfsizligida axborotning bahosi qanday aniqlanadi?

Axborot xavfsizligi buzulgan taqdirda ko'rilishi mumkin bo'lgan zarar miqdori bilan

Windows OT lokal xavfsizlik siyosatini sozlash oynasiga o'tish uchun "Buyruqlar satri"ga quyidagi so'rovlardan qaysi biri kiritiladi?

J:secpol.msc

№	Savol				
1	Qanday funksiyalar asosiy akslantirishlar deyiladi	Aralashtirish va tarqatish xususiyatlariga ega bo'lgan funksiyalar	Simmetrik blokli shifrlash funksiyalari	Shifrlanishi kerak bo'lgan funksiyalar	Xesh funksiyalar
2	Shifr ...	:Kalitdan foydalangan holda almashtirish uchun amalga oshiriladigan qayta almashtirishlar majmui	Axborotning xavfsizligini ta'minlab saqlash hamda uzatish tizimlarini yaratish	U aloqa kanallari orqali axborotning xavfsizligini ta'minlab saqlash hamda uzatish tizimlarini yaratish	Alifbod foydalanm holda almashtirish uchun amalga oshiriladi qayta almashtirishlar majmui
3	ochiq ma'lumotni shifrlash va deshifrlash jarayonini tashkil etuvchi amallar majmui bo'lib, alifbo belgilarini almashtirish ketma ketligidan iborat	:Kriptografik tizim	:Shifrlash	:Deshifrlash	:Kriptobardoshlilik
4	:... shifrlash kaliti noma'lum bo'lgan holda shifrlangan ma'lumotni deshifrlashning qiyinlik darajasini belgilaydi	:Kriptobardoshlilik	:Kriptografik tizim	:Deshifrlash	:Shifrlash
5	Kriptotizimlar qanday turlarga bo'linadi?	:Simmetrik va asimmetrik kriptotizim	:Ochiq kalitli kriptotizim, Elektron raqamli imzo	:Kalitlarni taqsimlash va boshqarish	:Kriptografik kriptotizimlar
6	Axborotni aslidan o'zgartirilgan holatga akslantirish uslublarini topish va takomillashtirish bilan shug'ullanadigan fan nima deb ataladi?	:Kriptografiya	:Kriptotizimlar	:Kriptotahlil	:Ochiq kriptotizimlar infratuzilmi
7	DES algoritmidagi dastlabki raund kaliti necha bitga teng?	:48 bit	:56 bayt	:32 bit	:64 bit
8	DES da dastlabki kalit uzunligi necha bitga teng?	:56 bit	:128 bit	:64 bit	:32 bit
9	DES da blok har birining uzunligi necha bitga teng?	:32 bit	:56 bit	:48 bit	:64 bit
10	DES da raundlar soni nechta?	6:40	134:40:00	14:40	118:40:00
11	DES da S blok kanday funktsiya bajaradi?	:6 bitli blokni 4 bitga almashtiradi	:8 bitli blokni 4 bitga almashtiradi	:6 bitli blokni 6 bitga almashtiradi	:4 bitli blokni 4 bitga almashtiradi
12	DES da blok E kengaytirilishidan	kalit bilan XOR amali bilan qo'shiladi	kalit bilan mod32 bo'yicha qo'shiladi	kalit bilan ko'paytiriladi	S boxlar ajratiladi

	so'ng kaday amal bajariladi?				
13	DES qaysi tarmog' asosida ishlaydi	:Feystel tarmog'i asosida	:Khafre Blowfish	:GOST 28147 89	:AES FIPS
14	DES da IP jadval qanday ish bajaradi?	:Berilgan jadval bo'yicha bitlarning o'rnini aralashtiradi	:Bitlarni chapga yoki o'nga n birlik suradi	:mod $2^{32}$ buyicha qo'shiladi	:raund ka generasiya
15	DES da shifrlangan matn bloki necha bitdan iborat buladi?	:64 bit	:128 bit	:256 bit	:56 bi
16	DES da S bloklar soni nechta?	14:40	16:40	6:40	10:40
17	Kriptotizim – bu	:shifrlash jarayonini tashkil etuvchi barcha amallar majmui	:Oddiy boshqaruv tizimi	:Shifrlashni amalga oshiradigan tizim	:Yashirin
18	: DES shifrlash algoritmi nechanchi yilda yaratilgan	:1976 yilda	:1980 yilda	:1989 yilda	:1987 yi
19	Shifrlash kaliti noma'lum bo'lganda shifrlangan ma'lumotni deshifrlash qiyinlik darajasini nima belgilaydi	:kriptobardoshlik	:Shifr matn uzunligi	:Shifrlash algoritmi	:Texnika texnologiy
20	Klassik shifrlash algoritmlari necha turga bo'linadi	19:40	18:40	20:40	17:40
21	O'rniga qo'yish shifrlash algoritmi nechta turga bo'linadi	20:40	19:40	18:40	17:40
22	Ochiq matndagi bitta belgi o'rniga shifr mantdagi bitta belgi mos qo'yilsa, bunday o'rniga qo'yish algoritmi nima deyiladi	:bir qiymatli	:Ko'p qiymatli	:O'rin almashtirish	:Mosli
23	Shifrlashda ishlatiladigan kalitlar qanday bo'ladi	:simmetrik va asimmetrik	:Uzun	:Murakkab va oson	:Uzun va o
24	Kriptotahlil bilan shug'ullanuvchi insonlar kimlar?	:kriptoanalitiklar	:Shifrchilar	:Hakkerlar	:Dasturch
25	Agar A alfavit m ta elementdan iborat bo'lsa, u holda A to'plamdagi barcha o'rniga qo'yishlar soni nimaga teng bo'ladi?	:m!	:m2	:2m	:mm
26	Shifrlash algoritmlarida samarali tarqatish akslantirishi uchun, odatda, qanday akslantirishdan foydalaniladi	:S blok	:IP	:IP 1	:Siljitis

27	Kriptotizim – bu	:shifrlash jarayonini tashkil etuvchi barcha amallar majmui	:Oddiy boshqaruv tizimi	:Shifrlashni amalga oshiradigan tizim	:Yashirinlik
28	O'rniga qo'yish – almashtirish tarmoqlariga asoslangan shifrlash algoritmi qanday ataladi	:SP– tarmoq	:Feystel tarmog'i	:Vijener	:Feystel Verman
29	AES shifrlash standartining mualliflari kimlar	:Ridjmen va Deimen	:Feystel va Pascal	:Vijener va Verman	:Feystel Verman
30	Barcha simmetrik shifrlash algoritmlari qanday shifrlash usullariga bo'linadi	:blokli va oqimli	:DES va oqimli	:Feystel va Verman	:SP– tarmoq
31	DES shifrlash algoritmda kalit uzunligi va blok uzunligi mos holda qancha bo'lishi kerak	:56 bit, 64 bit	:64 bit, 64 bit	:32 bit, 64 bit	:56 bit, 32 bit
32	DES shifrlash algoritmi nechta rejimda ishlashi belgilab qo'yilgan	:4 ta	:3 ta	:2 ta	:5 ta
33	Shifrlanuvchi bloklar bir biriga bog'liq bo'lmagan holda alohida shifrlash algoritmi orqali qayta ishlanadigan DES shifrlash algoritmining rejimi qaysi	:ECB	:CBC	:CFB	:OFB
34	DES shifrlash algoritmi qaysi tarmoqqa asoslangan	:Feystel tarmog'i	:SP tarmoqlari	:FROG tarmog'i	:HPC tarmog'i
35	DES shifrlash algoritmda kalitlar fazosi necha bitdan iborat	110:40:00	102:40:00	134:40:00	118:40:00
36	DES shifrlash algoritmda shifrlanadigan ma'lumotlar bloki necha bit?	102:40:00	134:40:00	118:40:00	110:40:00
37	DES shifrlash algoritmda shifrlash jarayoni nimalardan iborat?	:kiruvchi blok, boshlang'ich almashtirish, 16 raundli shifrlash va yakuniy almashtirish	:Kalitlar fazosi, shifrlash, 32 raundli shifrlash va yakuniy almashtirish	:Boshlang'ich almashtirish, kalitlar fazosi, shifrlash	:Kiruvchi blok, yakuniy almashtirish, shifrlash
38	DES shifrlash algoritmda i raundi necha bitli kalitdan foydalaniladi?	118:40:00	110:40:00	102:40:00	134:40:00
39	XOR amali qanday amal?	:2 modul bo'yicha qo'shish	:264 modul bo'yicha qo'shish	:232 modul bo'yicha qo'shish	:248 modul bo'yicha qo'shish



40	DES shifrlash algoritmda kengaytirish funksiyasi qanday vazifani bajaradi?	:32 bitli blokni 48 bitli blokka kengaytiradi	:64 bitli blokni 56 bitli blokka almashtiradi	:Berilgan blokni 2 ga ko`paytiradi	:Bu algoritmda kengaytirish funksiyasi
41	DES shifrlash algoritmi necha rejimda ishlaydi?	18:40	14:40	6:40	134:40:00
42	DES shifrlash algoritmi kalitlarni kodlashda qaysi rejimdan foydalanadi?	:ECB rejimi	:CBC rejimi	:CFB rejimi	:OFB rejimi
43	DES shifrlash algoritmda S bloklar nima uchun ishlatiladi?	:48 bitli blokni 32 bitli blokka aylantirish uchun	:Kalitlarni saralash uchun	:Ochiq matnni tekshirish uchun	:DES da S bloklari ishlatilma
44	DES shifrlash algoritmda nechta S blok bor?	14:40	6:40	10:40	118:40:00
45	Sezar shifrlash usulini ko`rsating.	:(m k)mod26 m harf tartib raqami, k kalit	:(m k)mod25 m ixtiyoriy son, k kalit	:(m k 26)mod2	:(mk)mod26
46	DES shifrlash algoritmda ochiq matn necha bitdan bloklarga ajratiladi?	102:40:00	134:40:00	6:40	14:40:00
47	DES shifrlash algoritmda shifrlash funksiyasini hosil qilishda nimalardan foydalaniladi?	:E kengaytirish funksiyasi, kalit, S bloklardan, P almashtirishdan	:Ochiq matn, kalit, shifmatndan	:Kalitning o`zidan	:Shifrlash funksiyasi
48	Xavfsizlik siyosati quyidagilar asosida yaratiladi	:tashkilot ma`lumot tizimlarining umumiy tavsiflari asosida	:o`zaro yaqin tashkilotlarning siyosatini o`rganish asosida	:sintez asosida	:tavakalchilik tahlili asosida
49	Shifrlashtirish so`zining ma`nosi nima?	:Shifrlashtirish – almashtirish jarayoni bo`lib, berilgan matn shifrlangan matn bilan almashtiriladi.	:Shifrlashtirish – almashtirish jarayoni bo`lib, berilgan matn jadval bilan almashtiriladi.	:Shifrlashtirish – almashtirish jarayoni bo`lib, berilgan matn lotincha matn bilan almashtiriladi.	:Shifrlashtirish – almashtirish jarayoni bo`lib, berilgan matn inglizcha matn bilan almashtiriladi.
50	Deshifrlashtirish so`zining ma`nosi nima?	:Deshifrlashtirish – shifrlashtirishga teskari jarayon. Kalit asosida shifrlangan matn o`z holatiga uzgartiriladi.	:Deshifrlashtirish – bu matn ma`lumotlarini o`zgartirish uchun ikkilik kodi.	:Deshifrlashtirish – bu grafik ma`lumotlarni o`zgartirish uchun sakkizlik kodi.	:Deshifrlashtirish – bu grafik ma`lumotlarni o`zgartirish uchun sakkizlik kodi.
51	Alfavit – bu	:axborotni kodlashtirish uchun ishlatiladigan chekli belgilar to`plami.	:axborotni kodlashtirish uchun ishlatiladigan diskret va cheksiz belgilar to`plami.	:axborotni kodlashtirish uchun ishlatiladigan diskret belgilar to`plami.	:axborotni kodlashtirish uchun ishlatiladigan cheksiz belgilar to`plami.
52	Kalit – bu?	:kalit – matnlarni shifrlash va deshifrlash uchun kerak bo`lgan axborot	:kalit – matnlarni o`zgartirish uchun kerak bo`lgan ma`lumot	:kalit – matnlarni kodlashtirish uchun kerak bo`lgan amal	:kalit – matnlarni shifrlash va deshifrlash uchun kerak bo`lgan

53	Simmetrik kriptotizimlarda shifrlash va deshifrlashda qanday kalit ishlatiladi?	:Bir xil kalit	:Alohida kalitlar	:Har xil kalitlar	:Ochiq
54	Ochiq kalitli tizimda shifrlash va deshifrlash uchun qanday kalit ishlatiladi?	:ochiq va yopiq	:Ochiq	:yopiq	:Bir xil kalit
55	Kriptomustahkamlik – bu	:Shifrnin deshifrlashga nisbatan mustahkamligini xarakterlaydi	:Identifikatorning deshifrlashga nisbatan mustahkamligini xarakterlaydi	:Kodning deshifrlashga nisbatan mustahkamligini xarakterlaydi	:Kodning deshifrlashga nisbatan mustahkamligini xarakterlaydi
56	Axborotni himoyalash maqsadida shifrlashning effektivligi quyidagilarga bog'liq?	:Shifrnin kriptomustahkamligi va kalitning sirini saqlashga	:Shifrnin kriptomustahkamligiga	:kodning sirini saqlashga	:Identifikatorning sirini saqlashga
57	Shifrlangan ma'lumot o'qilishi mumkin faqat	:Kaliti berilgan bo'lsa	:Kodi berilgan bo'lsa	:Identifikatori berilgan bo'lsa	:Shifri berilgan bo'lsa
58	Shifrlangan xabarning ma'lum qismi va unga mos keluvchi ochiq matn bo'yicha ishlatilgan shifrlash kalitining kerakli jarayonlar sonini aniqlash quyidagilardan iborat	:Mumkin bo'lgan kalitlarning umumiy sonidan kam bo'lmagan	:mumkin bo'lgan kalitlarning diskret sonidan kam bo'lmagan	:mumkin bo'lgan kalitlarning haqiqiy sonidan kam bo'lmagan	:mumkin bo'lgan kalitlarning mavhum sonidan kam bo'lmagan
59	Kalitlarni sezgarsiz o'zgartirish quyidagilarga olib kelishi mumkin	:bitta va bir xil kalitdan foydalanganda ham shifrlangan xabarlar sezilarli darajada o'zgarishga ega bo'ladi	:Xatto bir xil kalitni ishlatganda ham shifrlangan ma'lumot ko'rinishi sezilarli bo'ladi	:Xatto bir xil kalitni ishlatganda shifrlangan ma'lumot ko'rinishi sezilarli va sezgarsiz bo'ladi	:Xatto bitta xil kalitni ishlatganda shifrlangan ma'lumot ko'rinishi sezilarli bo'ladi
60	Quyidagilar bo'lmasligi kerak	:shifrlash jarayonida muntazam qo'llanadigan kalitlar orasida sodda va osongina aniqlash mumkin bo'lgan bog'liqlik	:shifrlash jarayonida muntazam qo'llanadigan identifikatorlar orasida sodda va aniqlash mumkin bo'lgan bog'liqlik	:Shifrlash jarayonida muntazam qo'llanadigan shifrlar orasida sodda va osongina aniqlash mumkin bo'lgan bog'liqlik	:shifrlash jarayonida muntazam qo'llanadigan kodlar orasida sodda va osongina aniqlash mumkin bo'lgan bog'liqlik
61	Mumkin bo'lgan to'plamlardan olingan har qanday kalitlar ... ni ta'minlaydi	:axborotni ishonchli himoyalash	:Komp'yuterni ishonchli himoyalash	:faylni ishonchli himoyalash	:axborot va ma'lumotni ishonchli himoyalash

62	Simmetrik kriptotizim uchun qanday usullar qo'llaniladi?	:o`rin almashtirish, gammalash, blokli shifrlash	:Monoalfavitli almashtirish, o`rnini almashtirish, gammalash	:Ko`p alfavitli almashtirish, o`rnini almashtirish, gammalash	:o`rnini almashtirish, gammirlash, identifikatsiya
63	Sezar almashtirishning mazmuni qanday izohlanadi?	:Sezar almashtirish monoalfavitli guruhiga qarashli	:Sezar` almashtirish ko`p alfavitli guruhiga qarashli	:Sezar` almashtirish blokli shifrlash guruhiga qarashli	:Sezar almashtirish gammalash guruhiga qarashli
64	Axborotni kodlash uchun foydalaniladigan chekli sondagi belgilar to'plami ... deb ataladi	:Alifbo	:Matn	:Kalit	:Axborot
65	Alifboning elementlaridan (belgilaridan) tashkil topgan tartiblangan tuzilma ... deb ataladi	:Matn	:Axborot	:Alifbo	:Kalit
66	Dastlabki ma'lumotni bevosita shifrlash va deshifrlash uchun zarur manba ... deb ataladi	:Kalit	:Alifbo	:Axborot	:Matn
67	Ochiq matn deb ataluvchi dastlabki ma'lumotni shifrlangan ma'lumot (kriptogramm holatiga o'tkazish jarayoni ... deb ataladi	:Shifrlash	:Deshifrlash	Kriptografik tizim	:Kriptobardoshlilik
68	Shifrlashga teskari bo'lgan jarayon, ya'ni kalit yordamida shifrlangan ma'lumotni dastlabki holatga o'tkazish ... deb ataladi	:Deshifrlash	:Tahlil qilish	:Kriptografik tizim	:Kriptobardoshlilik
69	... ochiq ma'lumotni shifrlash va deshifrlash jarayonini tashkil etuvchi amallar majmui bo'lib, alifbo belgilarini almashtirish ketma ketligidan iborat.	:Kriptografik tizim	:Shifrlash	:Deshifrlash	:Kriptobardoshlilik
70	... shifrlash kaliti noma'lum bo'lgan holda shifrlangan ma'lumotni deshifrlashning qiyinlik darajasini belgilaydi.	<b>:Kriptobardoshlilik</b>	:Tahlil qilish	:Deshifrlash	:Kriptografiya

7 1	Quyidagilardan qaysi biri matn jo'natilgan shaxsga qabul qilingan elektron matnning va matnni raqamli imzolovchining haqiqiy yoki nohaqiqiylikini aniqlash imkonini beradi?	:Elektron raqamli imzo	:Simmetrik kriptotizim	:Kalitlarni taqsimlash va boshqarish	:Ochiq kriptotizim
7 2	Qaysi kriptotizimda shifrlash uchun ham va deshifrlash uchun ham bir xil kalitdan foydalaniladi?	:Simmetrik kriptotizim	:Elektron raqamli imzo	:Ochiq kalitli kriptotizim	:Kalitlarni taqsimlash va boshqarish
7 3	... kriptobardoshli kalitlarni ishlab chiqish (yoki yaratish), ularni saqlash, hamda kalitlarni foydalanuvchilar orasida muhofazalangan holda taqsimlash jarayonlarini o'z ichiga oladi.	:Kalitlarni taqsimlash va boshqarish	:Elektron raqamli imzo	:Ochiq kalitli kriptotizim	:Simmetrik kriptotizim
7 4	Ochiq kalitli kriptotizimlarda qanday kalitlar foydalaniladi?	:ochiq va yopiq kalitlar	:Qo'shimcha kalitlar	:Yopiq kalitlar	:Ochiq kriptotizim
7 5	Kriptologiya maqsadlari o'zaro qarama qarshi bo'lgan ikkita yo'nalishiga ega. Bular qaysilar?	:Kriptografiya va kriptotahlil	:Simmetrik va asimmetrik kriptotizim	:Kalitlarni taqsimlash va boshqarish	:Ochiq kriptotizim Elektron raqamli imzo
7 6	Kriptotizimlar ikki qismga bo'linadi. Bular qaysilar?	:Simmetrik va asimmetrik kriptotizim	:Kriptografiya va kriptotahlil	:Kalitlarni taqsimlash va boshqarish	:Ochiq kriptotizim Elektron raqamli imzo
7 7	Axborotni aslidan o'zgartirilgan holatga akslantirish uslublarini topish va takomillashtirish bilan shug'ullanadigan fan qaysi?	:Kriptografiya	:Kriptotizimlar	:Kriptologiya	:Kriptotizimlar
7 8	Axborotni muxofaza qilish masalalari bilan shug'ullanadigan fan bo'lib Cryptos maxfiy, logos ilm degan ma'noni anglatadigan fan qaysi?	:Kriptologiya	:Kriptografiya	:Kriptotizimlar	:Kriptotizimlar

79	Kriptotahlilchilarni maxfiyligi ta'minlangan ma'lumotlarga ega bo'lish, ularni deshifrlash chora tadbirlarini amalga oshirishga bo'lgan hatti harakatlar (hujumlar)i qaysi turlarga bo'linadi?	:faol (aktiv) va faol bo'lmagan (passiv) hujumlar	:Kriptografiya va kriptotahlil	:Simmetrik va asimmetrik kriptotizim	:Kalitlar taqsimlash boshqari
80	Teskarisi mavjud bo'lmagan akslantirishlar qanday akslantirishlar deyiladi.	:Bir tomonlama	:Ko'p tomonlama	:Inyektiv	:Syurek
81	Ma'lumotlarni himoyalash deganda nima tushiniladi?	:Ma'lumotlarga ruxsat etilmagan kirishlardan himoyalash	:Himoyalash uchun maxsus disketalarni ishlab chiqish	:Ma'lumotlar xavfsizligini ta'minlashga yo'naltirilgan tashkiliy ishlar	:Himoya uchun ma himoyal omborlari y
82	Ma'lumotni qonuniy manbadan olingaligini kafolatlovchi va oluvchining haqiqiyiligini tasdiqlovchi xizmat qanday nomlanadi?	:autentifikatsiya	:butunlik	:maxfiylik	:nobutur
83	Zamonaviy kriptografiya qanday bo'limlardan iborat?	:Simmetrik kriptotizimlar; ochiq kalitli kriptotizimlar; Elektron raqamli imzo; kalitlarni boshqarish	:Simmetrik kriptotizimlar; ochiq kalitli kriptotizimlar;	:Electron raqamli imzo; kalitlarni boshqarish	:Simmet kriptotizin ochiq kal kriptotizin kalitlarni boshqari
84	Kriptografik usullardan foydalanishning asosiy yo'nalishlari nimalardan iborat?	:Aloqa kanali orqali maxfiy axborotlarni uzatish (masalan, elektron pochta orqali), uzatiliyotgan xabarlarini haqiqiyiligini aniqlash,	:tashuvchilarda axborotlarni shifrlangan ko'rinishda saqlash (masalan, hujjatlarni, ma'lumotlar bazasini)	:Aloqa kanali orqali maxfiy axborotlarni uzatish (masalan, elektron pochta orqali) uzatiliyotgan xabarlarini haqiqiyiligini aniqlash	:tashuvchi axborotla shifrlang ko'rinishda s (masala hujjatlar ma'lumo bazasini
85	Shifr nima?	:Shifrlash va deshifrlashda foydalaniladigan matematik funktsiyadan iborat bo'lgan kriptografik algoritm	:Kalitlarni taqsimlash usuli	:Kalitlarni boshqarish usuli	:Kalitlar generatsiya usuli
86	$12 \cdot 11 \bmod 16$ ?	15:40	10:40	11:40	6:40
87	$13 \cdot 4 \bmod 26$ ?	5:40	4:40	1:40	140:40:
88	DES algoritmiga muqobil bo'lgan	:Uch karrali DES, IDEA, Rijndael	:Uch karrali DES	:IDEA	:Rijnda

	algoritmni ko'rsating.				
89	DES algoritmining asosiy muammosi nimada?	:kalit uzunligi 56 bit. Bugungu kunda ushbu uzunlik algoritmnining kriptobardoshliligi uchun yetarli emas	:DES algoritmi bo'yicha shifrlash 16 raunddan iborat. Bu algoritmnining kriptobardoshliligi uchun yetarli emas	:Ushbu algoritm Feystel tarmog'iga asoslangan, shu sababli unda shifrlash qiyin	:Ushbu al SP tarmog asoslangan sababli u shifrlash c
90	Xabarning autentifikatori sifatida ishlatilishi uchun xesh funktsiya qanday talablarga mos kelishi kerak?	:Keltirilganlarning barchasiga mos kelishi kerak	:xesh funktsiya H ixtiyoriy uzunlikdagi ma'lumotlar blokiga qo'llanilishi va u fiksirlangan uzunlikdagi chiqishni ta'minlashi lozim.	: $H(M)$ ixtiyoriy M uchun nisbatan oson hisoblanishi lozim. Xesh kod h ning ixtiyoriy berilgan qiymati uchun $H(M)=h$ tenglik bajariluvchi M ni topish mumkin bo'lmasin.	:Ixtiyoriy x berilgan qi uchun $H(y)$ tenglik bajar y'x ni top mumkin bo'l Shunind $H(y)=H(x)$ bajariluvchi jo'ftlikni to mumkin bo'l
91	MD5 qanday xossalarga ega?	:Xesh kodning har bir biti kirishdagi har bir bitning funktsiyasidir. 128 bitli xesh kod uchun MD5 nisbatan kuchli xesh funktsiya hisoblanadi	:Xesh kodning har bir biti kirishdagi har bir bitning funktsiyasidir	:128 bitli xesh kod uchun MD5 nisbatan kuchli xesh funktsiya hisoblanadi	:128 bitli xe uchun M nisbatan k xesh funk hisoblanm
92	SHA 1 algoritmining bajarilishi qanday mantiqdan iborat?	:Algoritm kirishda maksimal uzunligi 264 bit bo'lgan xabarni qabul qilib, chiqishda uzunligi 160 bit bo'lgan xabarning daydjestini yaratadi	:Algoritm kirishda maksimal uzunligi 264 bit bo'lgan xabarni qabul qilib, chiqishda uzunligi 200 bit bo'lgan xabarning daydjestini yaratadi	:Algoritm kirishda maksimal uzunligi 264 bitbo'lgan xabarni qabul qilib, chiqishda uzunligi 170 bit bo'lgan xabarning daydjestini yaratadi	:Algoritm k maksimal uz 264 bitbo' xabarni qabu chiqishda uz 110 bit bo' xabarni daydjestini y
93	MD5 xesh funktsiya qanaqa xarakteristikaga ega?	:daydjesti uzunligi 128 bit; Blok uzunligi 512 bit; Iteratsiya soni – 64 (har birida 16 iteratsiya bo'lgan 4 ta tsikl); Elementar mantiqiy funktsiyalar soni – 4; Qo'shimcha konstantalar sonu – 64.	:daydjesti uzunligi 128 bit; Blok uzunligi 512 bit; Iteratsiya soni – 64 (har birida 16 iteratsiya bo'lgan 4 ta tsikl); Elementar mantiqiy funktsiyalar soni – 3; Qo'shimcha konstantalar sonu – 56.	:daydjesti uzunligi 128 bit; Blok uzunligi 512 bit; Iteratsiya soni – 64 (har birida 16 iteratsiya bo'lgan 4 ta tsikl); Elementar mantiqiy funktsiyalar soni – 4; Qo'shimcha konstantalar sonu – 72.	:daydjesti u 128 bit; E uzunligi 5 Iteratsiya so (har birida iteratsiya bo ta tsikl); Ele mantiqi funktsiyalar 5; Qo'shir konstantalar 64.

94	SHA 1 xesh funktsiya qanaqa xarakteristikaga ega?	:Daydjesti uzunligi 160 bit; Blok uzunligi 512 bit; Iteratsiya soni – 80; Elementar mantiqiy funktsiyalar soni – 3; Qo'shimcha konstantalar sonu – 4.	:daydjesti uzunligi 160 bit; Blok uzunligi 512 bit; Iteratsiya soni – 60; Elementar mantiqiy funktsiyalar soni – 4; Qo'shimcha konstantalar sonu – 2.	:daydjesti uzunligi 160 bit; Blok uzunligi 512 bit; Iteratsiya soni – 100; Elementar mantiqiy funktsiyalar soni – 2; Qo'shimcha konstantalar sonu – 4.	:daydjesti uzunligi 160 bit; Blok uzunligi 512 bit; Iteratsiya soni – 100; Elementar mantiqiy funktsiyalar soni – 3; Qo'shimcha konstantalar sonu – 6.
95	4 31 mod 32 ?	19:40	18:40	135:40:00	134:40:00
96	21 20mod32?	13:40	10:40	6:40	125:40:00
97	SHA 256 xesh funktsiya qanaqa xarakteristikaga ega?	:Xabar uzunligi 264 bit; Blok uzunligi 512 bit; So'z uzunligi 32 bit; Xabar daydjesti uzunligi 256 bit	:Xabar uzunligi 262 bit; Blok uzunligi 512 bit; So'z uzunligi 28 bit; Xabar daydjesti uzunligi 256 bit	:Xabar uzunligi 260 bit; Blok uzunligi 512 bit; So'z uzunligi 32 bit; Xabar daydjesti uzunligi 256 bit	:Xabar uzunligi 266 bit; Blok uzunligi 512 bit; So'z uzunligi 32 bit; Xabar daydjesti uzunligi 256 bit
	SHA 512 xesh funktsiya qanaqa xarakteristikaga ega?	:Xabar uzunligi 2128 bit; Blok uzunligi 1024 bit; So'z uzunligi 64 bit; Xabar daydjesti uzunligi 512 bit	:Xabar uzunligi 2128 bit; Blok uzunligi 1024 bit; So'z uzunligi 62 bit; Xabar daydjesti uzunligi 508 bit	:Xabar uzunligi 2128 bit; Blok uzunligi 1024 bit; So'z uzunligi 64 bit; Xabar daydjesti uzunligi – 510 bit	:Xabar uzunligi 2128 bit; Blok uzunligi 1024 bit; So'z uzunligi 64 bit; Xabar daydjesti uzunligi 508 bit
99	Nisbatan mashhur bo'lgan xesh funktsiyalarni ko'rsating.	:MD2, MD4, MD5, SHA	:GOST 28147, DES, AES, SERPENT	:DES, O'zDSt1106:2006, AES	:O'zDSt1109:2006, MD2, SHA, MARS
100	Davlat yoki xalqaro standart sifatida ishlatilayotgan blokli shifrlash algoritmlarini ko'rsating.	:DES, GOST28147, CAST, AES	:DES, GOST28147, CAST	:RC4, CAST, AES	:DES, GOST28147, CAST, AES
101	S box lar nima uchun yaratilgan?	:Ochiq matn va shifratmatn orasidagi bog'liqlikni yuqotish uchun	:shifrlash jarayonini soddalashtirish uchun	:deshifrlash jarayonini soddalashtirish uchun	:kalitlar generatsiya qilish uchun soddalashtirish uchun
102	12 22 mod 32 ?	20:40	10:40	0:40	134:40:00
103	... shifrida shifrlanayotgan matn belgilari boshqa alifbo belgilariga almashadi	:o'rniga qo'yish	:o'rin almashtirish	:gammalashtirish	:analitik almashtirish asoslangan
104	... shifrida shifrlanayotgan matn belgilari qandaydir qoidaga asosan shifrlanayotgan matnning boshqa belgilariga almashadi	:o'rin almashtirish	:o'rniga qo'yish	:gammalashtirish	:analitik almashtirish asoslangan

105	... shifrida shifrlanayotgan matn belgilari shifrning gammasi deb ataluvchi qandaydir tasodifiy ketma ketlikning belgilari bilan qo'shiladi	:gammalashtirish	:o'rin almashtirish	:o'rniga qo'yish	:analitik almashtirish asoslangan
106	... shifrida shifrlanayotgan matn belgilari analitik qoida (formulaga) asosan almashadi.	:analitik almashtirishga asoslangan	:o'rin almashtirish	:o'rniga qo'yish	:gammalashtirish
107	Simmetrik algoritmlarni xavfsizligini ta'minlovchi omillarni ko'rsating.	:uzatilayotgan shifrlangan xabarni kalitsiz ochish mumkin bo'lmashligi uchun algoritm yetarli darajada bardoshli bo'lishi lozim, uzatilayotgan xabarni xavfsizligi algoritmni maxfiyligiga emas, balki kalitni maxfiyligiga bog'liq bo'lishi lozim,	:uzatilayotgan xabarni xavfsizligi kalitni maxfiyligiga emas, balki algoritmni maxfiyligiga bog'liq bo'lishi lozim	:uzatilayotgan xabarni xavfsizligi shifrlanayotgan xabarni uzunligiga bog'liq bo'lishi lozim	:uzatilayotgan xabarni xavfsizligi shifrlanayotgan xabarni uzunligiga bog'liq bo'lishi lozim
108	Kriptotizim quyidagi komponentlardan iborat:	:ochiq matnlar fazosi M, Kalitlar fazosi K, Shifratmatnlar fazosi C, Ek : $M \oplus C$ (shifrlash uchun) va Dk: $C \oplus M$ (deshifrlash uchun) funksiyalar	:Shifratmatnlar fazosi C, Ek: $M \oplus C$ (shifrlash uchun) va Dk: $C \oplus M$ (deshifrlash uchun) funksiyalar	:ochiq matnlar fazosi M, shifratmatnlar fazosi C	:ochiq matnlar fazosi M, shifratmatnlar fazosi C
109	$2 \cdot 5 \bmod 32$ ?	15:40	134:40:00	20:40	17:40
110	Serpent, Square, Twofish, RC6 algoritmlari qaysi turiga mansub?	:simmetrik blokli algoritmlar	:Oqimli shifrlash	:asimmetrik algoritmlar	:elektron raqamli imzo algoritmlari
111	Rijndael algoritmi S box uzunligi necha bit?	38:40:00	34:40:00	30:40:00	24:40:00
112	Simmetrik shifrlash algoritmlari blokli deyiladi, agar ...	:shifrlashda ochiq matn fiksirlangan uzunlikdagi bloklarga bo'linsa	:Algoritm Feystel tarmog'i asosida qurilsa	:Algoritmda S boxdan foydalanilsa	:Algoritmda chiziqli almashtirish foydalanilsa
113	To'g'ri mulohazani tanlang.	:Rijndael algoritmi Feystel tarmog'iga asoslanmagan	:Rijndael algoritmi 4 shoxli Feystel tarmog'iga asoslangan	:Rijndael algoritmi 6 shoxli Feystel tarmog'iga asoslangan	:Rijndael algoritmi 8 shoxli Feystel tarmog'iga asoslangan
114	Xesh funksiyani natijasi ...	:fiksirlangan uzunlikdagi xabar	:Kiruvchi xabar uzunligidagi xabar	:Kiruvchi xabar uzunligidan uzun xabar	:fiksirlangan uzunlikdagi xabar



1 1 5	AES algoritmi bloki uzunligi ... bitdan kam bo'lmashligi kerak.	38:40:00	345:20:00	89:20:00	25:20:00
1 1 6	Zamonaviy kriptografiya qanday bo'limlardan iborat?	:Simmetrik kriptotizimlar; ochiq kalitli kriptotizimlar; Elektron raqamli imzo; kalitlarni boshqarish	:Simmetrik kriptotizimlar; ochiq kalitli kriptotizimlar;	:Electron raqamli imzo; kalitlarni boshqarish	:Simmetrik kriptotizimlar; ochiq kalitli kriptotizimlar; kalitlarni boshqarish
1 1 7	Kriptografik usullardan foydalanishning asosiy yo'nalishlari nimalardan iborat?	:Aloqa kanali orqali maxfiy axborotlarni uzatish (masalan, elektron pochta orqali), uzatiliyotgan xabarlarini haqiqiylikni aniqlash, tashuvchilarda axborotlarni shifrlangan ko'rinishda saqlash (masalan, hujjatlarni, ma'lumotlar bazasini)	:Aloqa kanali orqali maxfiy axborotlarni uzatish (masalan, elektron pochta orqali)	:uzatiliyotgan xabarlarini haqiqiylikni aniqlash	:tashuvchilarda axborotlarni shifrlangan ko'rinishda saqlash (masalan, hujjatlarni, ma'lumotlar bazasini)
1 1 8	Shifr nima?	:Shifrlash va deshifrlashda foydalaniladigan matematik funktsiyadan iborat bo'lgan kriptografik algoritmlar	:Kalitlarni taqsimlash usuli	:Kalitlarni boshqarish usuli	:Kalitlarni generatsiya qilish usuli
1 1 9	Himoyalangan yoki xavfsizlikni ta'minlovchi protokol qanday protokol?	:Hech bo'lmaganda bitta xavfsizlik funksiyasini qo'llab quvvatlashni ta'minlovchi protokol	:Kommunikatsion protokol	:Ko'p ishtirokchili protokol	:Kalit almash tiruvchi protokol
1 2 0	Protokol xavfsizligi nimalarda o'z ifodasini topadi?	:Xavfsizlikni xarakterlovchi xossalari (maxfiylik, butunlik...) kafolati ta'minlanishida	:Protokoldan begonalar xabar topishining oldini olishda	:Protokollar xavfsizlikni ta'minlamaydi	:Protokollar maxfiy kalitlarni ishlatilmasdan
1 2 1	Kriptografik protokol bu	:Bajarilish jarayonida ishtirokchilar tomonidan kriptografik algoritmlardan foydalanadigan protokol	:Bajarilish jarayonida ishtirokchilar tomonidan kriptografik algoritmlardan foydalanmaydigan protokol	:Maxfiy kalitlar ishlatilmaydigan protokol	:Faqatgina maxfiy axborotlarni uzatish uchun asoslangan protokol

1 2 2	Tashqaridan kuzatib, xabarlarini bilib olishga va protokol bajarilishini buzishga urinuvchi qanday ataladi	:Raqib tomon	:Buzg'unchi	:Ishtirokchi	:Foydalan
1 2 3	Kriptografik protokollarni qanday guruhlash mumkin	:Ishtirokchilar soniga va uzatilayotgan xabar soniga ko'ra	:Xavfsizlikni ta'minlash darajasiga ko'ra	:Qo'llanilgan algoritmlar turiga qarab	:Kriptogr protokoll guruhlar ajratilma
1 2 4	Ishtirokchilar soniga ko'ra kriptografik protokollar qanday turlarga bo'linadi?	: Ikki tomonlama; Uchtomonlama; Ko'ptomonlama.	:Umumiy va yakka tartibdagi protokollar	:Oddiy va ko'p tomonlama protokollar	:Uchtomon
1 2 5	S box lar nima uchun yaratilgan?	:ochiq matn va shifrmtn orasidagi bog'liqlikni yuqotish uchun	:shifrlash jarayonini soddalashtirish uchun	:deshifrlash jarayonini soddalashtirish uchun	:kalitlar generatsiya o soddalashtirish uchun
1 2 6	Oqimli shifrlashning mohiyati nimada?	:Oqimli shifrlash birinchi navbatda axborotni bloklarga bo'lishning imkoni bo'lmagan hollarda zarur, Qandaydir ma'lumotlar oqimini har bir belgisini shifrlab, boshqa belgilarini kutmasdan kerakli joyga jo'natish uchun oqimli shifrlash zarur, Oqimli shifrlash algoritmlari ma'lumotlarnbi bitlar yoki belgilar bo'yicha shifrlaydi	:Oqimli shifrlash birinchi navbatda axborotni bloklarga bo'lishning imkoni bo'lmagan hollarda zarur, Qandaydir ma'lumotlar oqimini har bir belgisini shifrlab, boshqa belgilarini kutmasdan kerakli joyga jo'natish uchun oqimli shifrlash zarur	:Qandaydir ma'lumotlar oqimini har bir belgisini shifrlab, boshqa belgilarini kutmasdan kerakli joyga jo'natish uchun oqimli shifrlash zarur, Oqimli shifrlash algoritmlari ma'lumotlarnbi bitlar yoki belgilar bo'yicha shifrlaydi	:Oqimli shifrlash birinchi navbatda axborotni bloklarga bo'lishning imkoni bo'lmagan hollarda zarur, Oqimli shifrlash algoritmlari ma'lumotlarnbi bitlar yoki belgilar bo'yicha shifrlaydi
1 2 7	Almashtirishlar turiga ko'ra shifrlarni qanday guruhlarga ajratish mumkin?	:o'rniga qo'yish shifri, o'rin almashtirish shifri, gammalashtirish shifri, analitik almashtirishga asoslangan shifr	:o'rniga qo'yish shifri, o'rin almashtirish shifri, gammalashtirish shifri,	:o'rniga qo'yish shifri, o'rin almashtirish shifri, analitik almashtirishga asoslangan shifr	:o'rin almashtirish shifri, gammalashtirish shifri, analitik almashtirishga asoslangan shifr
1 2 8	... shifrida shifrlanayotgan matn belgilari boshqa alifbo belgilariga almashadi	:o'rniga qo'yish	:o'rin almashtirish	:gammalashtirish	:analitik almashtirishga asoslangan
1 2 9	... shifrida shifrlanayotgan matn belgilari shifrnin gammasi deb ataluvchi qandaydir tasodifiy ketma ketlikning belgilari bilan qo'shiladi	:gammalashtirish	:o'rin almashtirish	:o'rniga qo'yish	:analitik almashtirishga asoslangan

1 3 0	... shifrd shifrlanayotgan matn belgilari analitik qoida (formul ga asosan almashadi	:analitik almashtirishga asoslangan	:o'rin almashtirish	:o'rniga qo'yish	:gammalashtirish
1 3 1	Simmetrik algoritm xavfsizligini ta'minlovchi omillarni ko'rsating.	:uzatilayotgan shifrlangan xabarni kalitsiz ochish mumkin bo'lmasligi uchun algoritm yetarli darajada bardoshli bo'lishi lozim, uzatilayotgan xabarni xavfsizligi algoritmni maxfiyligiga emas, balki kalitni maxfiyligiga bog'liq bo'lishi lozim,	:uzatilayotgan xabarni xavfsizligi kalitni maxfiyligiga emas, balki algoritmni maxfiyligiga bog'liq bo'lishi lozim	:uzatilayotgan xabarni xavfsizligi shifrlanayotgan xabarni uzunligiga bog'liq bo'lishi lozim	:uzatilayotgan xabarni xavfsizligi shifrlanayotgan xabarni uzunligiga bog'liq bo'lishi lozim
1 3 2	Kriptotizim quyidagi komponentlardan iborat:	:ochiq matnlar fazosi M, Kalitlar fazosi K, Shifmatnlar fazosi C, Ek : M ® C (shifrlash uchun) va Dk: C®M (deshifrlash uchun) funktsiyalar	:Shifmatnlar fazosi C, Ek: M®C (shifrlash uchun) va Dk: C®M (deshifrlash uchun) funktsiyalar	:ochiq matnlar fazosi M, shifmatnlar fazosi C	:ochiq matnlar fazosi M, shifmatnlar fazosi C
1 3 3	4 31 mod 32 ?	19:40	18:40	135:40:00	134:40:00
1 3 4	DES algoritmiga muqobil bo'lgan algoritmni ko'rsating.	:Uch karrali DES, IDEA, Rijndael	:Uch karrali DES	:IDEA	:Rijndael
1 3 5	DES algoritmining asosiy muammosi nimada?	:kalit uzunligi 56 bit. Bugungu kunda ushbu uzunlik algoritmning kriptobardoshliligi uchun yetarli emas	:DES algoritmi bo'yicha shifrlash 16 raunddan iborat. Bu algoritmning kriptobardoshliligi uchun yetarli emas	:Ushbu algoritm Feystel tarmog'iga asoslangan, shu sababli unda shifrlash qiyin	:Ushbu algoritm SP tarmog'iga asoslangan, shu sababli unda shifrlash qiyin
1 3 6	Simmetrik blokli shifrlash rejimlarini ko'rsating.	:ECB Electronic Codebook, CBC Cipher Block Chaining, CFB Cipher Feedback, OFB Output Feedback	:ECB Electronic Codebook, CBC Cipher Block Chaining,	:CFB Cipher Feedback, OFB Output Feedback	:CBC Cipher Block Chaining, CFB Cipher Feedback
1 3 7	Asimmetrik kriptotizimlar qanday maqsadlarda ishlatiladi?	:shifrlash, deshifrlash, ERI yaratish va tekshirish, kalitlar almashish uchun	:shifrlash, deshifrlash	:ERI yaratish va tekshirish, kalitlar almashish uchun	:shifrlash, deshifrlash, ERI yaratish va tekshirish

1 3 8	Diffi Xellman algoritmining maqsadi nimada?	:algoritimning maqsadi keyinchalik qandaydir simmetrik shifrlash algoritmidagi foydalanish uchun 2 ta foydalanuvchilar tomonidan kalitlarni xavfsiz almashishida	:algoritimning maqsadi diskret logarifmlarni hisoblashda	:algoritimning maqsadi shifrlash jarayonida algoritimning kriptobardoshligini oshirish uchun kalitlar uzunligini oshirishda	:algoritim maqsadi sonlarni ko'paytuvchi ajratishda
1 3 9	12 22 mod 32 ?	20:40	10:40	0:40	134:40:00
1 4 0	Rijndael algoritmi S box uzunligi necha bit?	38:40:00	34:40:00	30:40:00	24:40:00
1 4 1	: Simmetrik shifrlash algoritmlari blokli deyiladi, agar ...	:shifrlashda ochiq matn fiksirlangan uzunlikdagi bloklarga bo'linadi	:Algoritim Feystel tarmog'i asosida qurilsa	:Algoritmda S boxdan foydalanilsa	:Algoritim chiziqli almashtirish foydalanadi
1 4 2	To'g'ri mulohazani tanlang.	:Rijndael algoritmi Feystel tarmog'iga asoslanmagan	:Rijndael algoritmi 4 shoxli Feystel tarmog'iga asoslangan	:Rijndael algoritmi 6 shoxli Feystel tarmog'iga asoslangan	:Rijndael algoritmi 8 shoxli Feystel tarmog'iga asoslangan
1 4 3	Xesh funktsiyani natijasi ...	:fiksirlangan uzunlikdagi xabar	:Kiruvchi xabar uzunligidagi xabar	:Kiruvchi xabar uzunligidan uzun xabar	:fiksirlangan uzunlikdagi xabar
1 4 4	AES algoritmi bloki uzunligi ... bitdan kam bo'lmasligi kerak.	38:40:00	345:20:00	89:20:00	25:20:00
1 4 5	2 5 mod 32 ?	15:40	134:40:00	20:40	17:40
1 4 6	MD5 qanday xossalarga ega?	:Xesh kodning har bir biti kirishdagi har bir bitning funktsiyasidir. 128 bitli xesh kod uchun MD5 nisbatan kuchli xesh funktsiya hisoblanadi	:Xesh kodning har bir biti kirishdagi har bir bitning funktsiyasidir	:128 bitli xesh kod uchun MD5 nisbatan kuchli xesh funktsiya hisoblanadi	:128 bitli xesh kod uchun MD5 nisbatan kuchli xesh funktsiya hisoblanadi
1 4 7	SHA 1 algoritmining bajarilishi qanday mantiqdan iborat?	:Algoritim kirishda maksimal uzunligi 264 bit bo'lgan xabarni qabul qilib, chiqishda uzunligi 160 bit bo'lgan xabarning daydjestini yaratadi	:Algoritim kirishda maksimal uzunligi 264 bit bo'lgan xabarni qabul qilib, chiqishda uzunligi 200 bit bo'lgan xabarning daydjestini yaratadi	:Algoritim kirishda maksimal uzunligi 264 bit bo'lgan xabarni qabul qilib, chiqishda uzunligi 170 bit bo'lgan xabarning daydjestini yaratadi	:Algoritim kirishda maksimal uzunligi 264 bit bo'lgan xabarni qabul qilib, chiqishda uzunligi 110 bit bo'lgan xabarning daydjestini yaratadi

1 4 8	MD5 xesh funksiya qanaqa xarakteristikaga ega?	:daydjesti uzunligi 128 bit; Blok uzunligi 512 bit; Iteratsiya soni – 64 (har birida 16 iteratsiya bo'lgan 4 ta tsikl); Elementar mantiqiy funktsiyalar soni – 4; Qo'shimcha konstantalar sonu – 64.	:daydjesti uzunligi 128 bit; Blok uzunligi 512 bit; Iteratsiya soni – 64 (har birida 16 iteratsiya bo'lgan 4 ta tsikl); Elementar mantiqiy funktsiyalar soni – 3; Qo'shimcha konstantalar sonu – 56.	:daydjesti uzunligi 128 bit; Blok uzunligi 512 bit; Iteratsiya soni – 64 (har birida 16 iteratsiya bo'lgan 4 ta tsikl); Elementar mantiqiy funktsiyalar soni – 4; Qo'shimcha konstantalar sonu – 72.	:daydjesti uzunligi 128 bit; Blok uzunligi 512 bit; Iteratsiya soni – 64 (har birida 16 iteratsiya bo'lgan 4 ta tsikl); Elementar mantiqiy funktsiyalar soni – 5; Qo'shimcha konstantalar sonu – 64.
1 4 9	12 11 mod 16 ?	15:40	10:40	11:40	6:40
1 5 0	RIJNDAEL algoritmi qancha uzunligdagi kalitlarni qo'llab quvvatlaydi.	:128 bitli, 192 bitli, 256 bitli	:128 bitli, 192 bitli,	:192 bitli, 256 bitli	:128 bitli, 256 bitli
1 5 1	Identifikasiyalash va autentifikasiyalash bu?	:Foydalanuvchilarni ro'yxatdan o'tkazish tartibi va ro'yxatdan o'tish ma'lumotlarini tekshirish tartibi	:sertifikatlar va ochiq kalitlarning yashash siklini boshqarish jarayonida tomonlarning harakatlarini belgilab beradi;	:xodimlarga, asbob uskunalar va texnik vositalar joylashtiriladigan xonalarga nisbatan qo'yiladigan talablarni belgilaydi;	:maxfiy kalitlarni yashash siklini boshqarish jarayonida tomonlarning harakatlarini belgilab beradi;
1 5 2	Blowfish shifrlash algoritmi bloki o'lchami qanday?	:64 bit	:128 bit	:48 bit	:56 bit
1 5 3	Blowfish algoritmi kaliti uzunligi qanday?	:O'zgaruvchan	:256 bit	:128 bit	:64 bit
1 5 4	Blowfish algoritmi raund akslantirishlari soni qancha?	:16 marta	:32 marta	:18 marta	:Kirish bloki uzunligiga bog'liq
1 5 5	Blowfish algoritmi qanday tur kriptotizimga kiradi?	:Simmetrik	:Asimmetrik	:Kompozitsiyali	:Modifikatsiyalan
1 5 6	Qanday manbaa asosida raund kalitlari yaratiladi?	:Krish bloki uzunligiga bog'liq holda.	:Dastlabki berilgan blok asosida	:Maxfiy kalit asosida	:SHifrlangan ma'lumot asosida
1 5 7	Berilgan algoritmnin kriptobardoshlilik nimaga asoslangan?	:Kalit uzunligiga.	:Mahfiy kalitni bilishga	:SHifrlash jarayonini bajarilish vaqtiga	:SHifrlash soniga
1 5 8	SHifrlash qanday amallar orqali amalga oshiriladi?	:CHEkli maydonda qo'shish mod 232 va mod 2 bo'yicha	:CHEkli maydonda qo'shish mod 232 bo'yicha	:Mos bitlarni qo'shish mod 2 bo'yicha	:CHEkli maydonda qo'shish mod 232 va mod 2 bo'yicha hamda bitlarni surish
1 5 9	DES, GOST 28147 89 algoritmlari shifrlash bloki uzunligi qancha?	:32 bit;	:64 bit;	:48 bit;	:16 bit;

1 6 0	<i>E kengaytirish funksiyasining mohiyati qanday?</i>	:32 bitli Ri 1 blokni 48 bitli E(Ri 1) blokka akslantiradi;	:Ri 1 blok bitlarini takrorlashdan iborat;	:32 bitli ki –kalitni 48 bitgacha kengaytiradi;	:16 bitli ki 32 bitgacha kengaytiradi;
1 6 1	DES algoritmi $S_i$ – bloki vazifasi nimadan iborat?	:48 bitli blokni 32 bitli blokka siqishdan iborat;	:56 bitli kalit blokini 48 bitli blokka siqishdan iborat;	:64 bitli kalit blokini 48 bitli blokka siqishdan iborat;	:32 bitli blokini 16 bitli blokka siqishdan iborat;
1 6 2	DES algoritmi dastlabki o‘rin almashtirish jadvalining o‘lchami qanday?	:8 x 8;	:4 x 8;	:6 x 8;	:8 x 12;
1 6 3	97 tub sonmi?	:Tub	:murakkab	:Natural	:To‘g‘ri javob berish yo‘q
1 6 4	Ikkilik sanoq tizimida berilgan 10111 sonini o‘nlik sanoq tizimiga o‘tkazing.	23:40	2:40	1:40	3:40
1 6 5	Quyidagi modulli ifodani qiymatini toping. $(125 \cdot 45) \bmod 10$ .	17:40	7:40	4:40	141:40:00
1 6 6	Quyidagi modulli ifodani qiymatini toping. $(148 - 14432) \bmod 256$ .	77:20:00	33:20:00	10:40:00	12:40:00
1 6 7	Quyidagi ifodani qiymatini toping. $17 \bmod 11$	17:40	16:40	15:40	11:40
1 6 8	Sonning teskarisini topish amali qanday algoritm yordamida amalga oshiriladi?	:Kengaytirilgan Yevklid	:Yevklid	:Ferma teoremasi	:Affin tizim
1 6 9	Multiplikativ teskarilash deb nimaga aytiladi?	:Modul ustida ko‘paytirish bo‘yicha teskarilash	:Modul ustida qo‘shish bo‘yicha teskarilash	:Modul ustida qo‘shish bo‘yicha ko‘paytirish amali	:Modul ustida ko‘paytirish bo‘yicha qo‘shish amali
1 7 0	Sonning o‘zi va uning modul multiplikativ teskarisining ko‘paytmasi nechaga teng	21:40	22:40	20:40	15:40
1 7 1	: DES algoritmi shifrlash blokining chap va o‘ng qism bloklarining o‘lchami qancha?	:CHap qism blok 32 bit, o‘ng qism blok 32 bit;	:CHap qism blok 32 bit, o‘ng qism blok 48 bit;	:CHap qism blok 64 bit, o‘ng qism blok 64 bit;	:CHap qism blok 16 bit, o‘ng qism blok 16 bit;
1 7 2	SHifrlash bloki uzunligi qancha ?	:32 bit;	:64 bit;	:48 bit;	:16 bit;
1 7 3	DES algoritmi kalit uzunligi qancha?	:56 bit;	:64 bit;	:48 bit;	:128 bit;
1 7 4	: DES algoritmi akslantirish raundlari soni qancha?	:16 ta;	:14 ta;	:12 ta;	:32 ta;

175	DES algoritmidagi E akslantirishining mohiyati qanday?	:32 bitli kirish blokini 48 bitli raund kalitiga mod2 maydonda qo'shish uchun 32 bitli blok 48 bitga kengaytiriladi ;	:32 bitli kirish blokini 48 bitli raund kalitiga mod48 maydonda qo'shish uchun 32 bitli blok 48 bitga kengaytiriladi.	:32 bitli kirish blokini 48 bitli raund kalitiga mod32 maydonda qo'shish uchun 32 bitli blok 48 bitga kengaytiriladi.	:32 bitli kirish blokini 48 bitli raund kalitiga mod2 maydonda qo'shish uchun 32 bitli blok 48 bitga kengaytiriladi.
176	$S_i$ – bloklarning vazifasi nimadan iborat?	:48 bitli blokni 32 bitli blokka siqishdan iborat;	:56 bitli blokni 32 bitli blokka siqishdan iborat;	:64 bitli blokni 32 bitli blokka siqishdan iborat;	:32 bitli blokni 32 bitli blokka siqishdan iborat;
177	DES algoritmidagi Bitlar o'rinlarini almashtirilishini aniqlovchi boshlang'ich jadval o'lchami qanday?	:8 x 8;	:4 x 8;	:6 x 8;	:8 x 16;
178	SHifrlash algoritmi chap va o'ng bloklarining o'lchami qanday?	:CHap blok 32 bit, o'ng blok 32 bit;	:CHap blok 32 bit, o'ng blok 48 bit;	:CHap blok 64 bit, o'ng blok 64 bit;	:CHap blok 64 bit, o'ng blok 64 bit;
179	Raund kalitlari bitlarini siljitish qanday amalga oshiriladi?	:Raund kalitlari bitlarini siljitish berilgan jadval bo'yicha hamma raundlar uchun bir xil amalga oshiriladi.	:Siljitish 28 bitdan qilib ikkiga bo'lingan algoritmda berilgan jadval bo'yicha chapga siklik surish orqali amalga oshiriladi.	:Juft raundlar bo'yicha 2 bit chapga toq raundlar uchun 1 bit o'nga suriladi;	:Siljitish 16 bitdan qilib ikkiga bo'lingan algoritmda berilgan jadval bo'yicha chapga siklik surish orqali amalga oshiriladi.
180	DES algoritmi kaliti uzunligi qancha.	:64 bit;	:48 bit;	:56 bit;	:128 bit;
181	DES algoritmi akslantirishlari raundlari soni qancha?	:16;	:32;	:14;	:12;
182	: Blowfish shifrlash algoritmi bloki o'lchami qancha?	:64 bit	:128 bit	:48 bit	:56 bit
183	: Blowfish algoritmi kaliti uzunligi qancha?	:O'zgaruvchan	:256 bit	:128 bit	:64 bit
184	Simmetrik shifrlash algoritmi bardoshligi nimaga asoslangan?	:Kalit uzunligiga;	:Mahfiy kalitni bilishga;	:Ma'lumotni shifrlash uchun ketadigan vaqtga;	:Algoritmi shifrlash raundlari soniga;
185	Qanday amallar asosida blokli shifrlash akslantirishlari yaratiladi?	: mod 2 bo'yicha qo'shish asosida;	:Ko'paytirish asosida;	:mod 2 bo'yicha qo'shish va ko'paytirish asosida;	:Samarali ta'lim va aralashtirish beruvchi hadda elektro elementlarda amalga oshirilgan ta'minlaydigan barcha akslantirish asosida;

186	Bloklab shifrlashning asosiy yutuqlari nimalarda namoyon bo'ladi?	:SHifrlangan ma'lumotga ochiq ma'lumotning chastotaviy xususiyatlari o'tmaydi	:SHifrlangan ma'lumotga ochiq ma'lumotning chastotaviy xususiyatlari to'la o'tadi	:SHifrlangan ma'lumotga ochiq ma'lumotning chastotaviy xususiyatlari qisman o'tmaydi	:SHifrlangan ma'lumotga ochiq ma'lumotning chastotaviy xususiyatlari qisman o'tmaydi
187	O'rniga qo'yish va o'rin almashtirish shifrlarining mohiyatan farqi qanday?	:SHifrlangan ma'lumot alfavitida	:Ochiq va shifrlangan ma'lumotlar alfavitlarida	:Foydalaniladigan kalit uzunligida	:Ochiq ma'lumot alfavitida
188	Oddiy o'rniga qo'yish shifrlari bardoshligi qanday aniqlanadi?	:SHifrlangan ma'lumot alfavit belgilarining barcha mumkin bo'lgan holatlari soni bilan	:Algoritmni amalga oshirish uchun bajariladigan barcha mumkin bo'lgan amallar soni bilan	:Algoritmni amalga oshirish uchun bajariladigan barcha mumkin bo'lgan akslantirishlar soni bilan	:Algoritmni amalga oshirish uchun bajariladigan barcha mumkin bo'lgan akslantirishlar soni bilan
189	Uzliksiz shifrlashning qanday kriptografik qulaylik va samaradorlik tomonlari bor?	:Tezligi yuqori va akslantirishlari apparat qurilmalarda qulay amalga oshirilish imkoniyatiga ega	:Tezligi yuqori va akslantirishlari dasturiy ta'minoti qulay amalga oshirilish imkoniyatiga ega	:Tezligi yuqori va akslantirishlari yuqori kriptobardoshlilikka ega	:Tezligi yuqori va akslantirishlari yuqori kriptobardoshlilikka ega
190	Uzliksiz shifrlashning qanday kriptografik kamchiliklari bor?	:Sinxronlash buzilganda shifrlanish xatolari tarqaladi	:Sinxronlash buzilgan da shifrlanish xatolari tarqamaydi	:Sinxronlash buzilmagan da shifrlanish xatolari tarqaladi	:Sinxronlash buzilgan da shifrlanish xatolari tarqalaydi
191	Uzliksiz shifrlash algoritmlarida siljitish registrlarining qo'llanishini mohiyati nimada?	:Tezligi yuqori va akslantirishlarini apparat qurilmalarini amalga oshirish samarali	:Tezligi yuqori va akslantirishlarini apparat qurilmalarini amalga oshirish samarasiz	:Tezligi yuqori emas, ammo akslantirishlarini apparat qurilmalarini amalga oshirish samarali.	:Tezligi yuqori va akslantirishlarini apparat qurilmalarini amalga oshirish samarali.
192	Xesh funksiya qanday kriptografik masalalarni echishga qo'llaniladi?	:To'ralik (butunlik) masalasini echishga	:ERI masalasini echishga	:Identifikatsiya masalasini echishga	:Konfidens masalasini echishga
193	Blokli simmetrik kalitli shifrlash algoritmlarining bardoshligi qanday parametr bilan aniqlanadi?	:Algoritm kaliti uzunligi bilan	:SHifrlangan va ochiq ma'lumotlar uzunliklari bilan aniqlanadi	:Raund kalitlari uzunliklari bilan	:Akslantirish blok uzunligi bilan
194	Agar $a=19$ bo'lsa, u holda unga teskari bo'lgan sonni xarakteristikasi 26 bo'lgan maydonda hisoblang.	11:40	:17 va 19	:19 va 11	:13 va 19



195	Kriptografiya va kriptotahlil yo'nalishlari mohiyatan qanday farqlarga ega?	:Kriptografiya yo'nalishi ochiq ma'lumot asl holatini yashirish bilan, kriptotahlil yo'nalishi esa shifr ma'lumotga mos keluvchi ochiq ma'lumotni kalit noma'lum bo'lganda topish masalalari echimlari bilan shug'illanadi	:Har ikkala yo'nalish ham ochiq ma'lumot asl mazmunini yashirish va oshkor qilish masalalari echimlari bilan shug'illanadi	:Har ikkala yo'nalish ham kalit noma'lum bo'lganda shifr ma'lumot asl mazmunini yashirish va oshkor qilish masalalari echimlari bilan shug'illanadi	:Kriptotahlil yo'nalishi ochiq ma'lumot asl holatini yashirish bilan, kriptotahlil yo'nalishi esa shifr ma'lumotga mos keluvchi ochiq ma'lumotni kalit noma'lum bo'lganda topish masalalari echimlari bilan shug'illanadi
196	MD5 xesh algoritmi xesh qiymat uzunligi nechchiga teng?	:128 bit	:32 bit	:64 bit	:256 bit
197	MD5 xesh algoritmining raundlar soni nechchiga teng?	18:40	19:40	16:40	17:40
198	AES shifrlash standartining mualliflari kimlar	:Ridjmen va Deimen	:Feystel va Pascal	:Vijener va Verman	:Feystel va Verman
199	XOR amali qanday amal?	:2 modul bo'yicha qo'shish	:264 modul bo'yicha qo'shish	:232 modul bo'yicha qo'shish	:248 modul bo'yicha qo'shish
200	Kalit – bu?	:kalit – matnlarni shifrlash va deshifrlash uchun kerak bo'lgan axborot	:kalit – matnlarni o'zgartirish uchun uchun kerak bo'lgan ma'lumot	:kalit – matnlarni kodlashtirish uchun uchun kerak bo'lgan amal	:kalit – matnlarni shifrlash va deshifrlash uchun kerak bo'lgan
201	Sonning moduli qaysi matematik ifoda orqali aniqlanadi	Qoldiqli bo'lish	Logarifmlash	Faktorlash	Elliptik chiziqlar
202	O'zaro teskari sonlar ko'paytmasi nimaga teng.	0	1	cheksiz	bo'sh to'p
203	OpenSSL nima?	Secure Sockets Layer (SSL) va kriptografiya vositalarini amalga oshiruvchi asosiy dasturdir	Drayver	Shifrlash kaliti	Dehshifrlash kaliti
204	RC4 qanday algoritmi	Simmetrik oqimli shifrlash algoritmi	Simmetrik blokli shifrlash algoritmi	Assimmetrik shifrlash algoritmi	Elektron raqamli imzo
205	A5/1 qanday algoritmi	Simmetrik oqimli shifrlash algoritmi	Simmetrik blokli shifrlash algoritmi	Assimmetrik shifrlash algoritmi	Elektron raqamli imzo
206	MD5 algoritmidagi hesh qiymat uzunligi necha bitga teng	128	256	65	512

Kriptologiya qanday yo‘nalishlarga bo‘linadi?=====

#kriptografiya va kriptotahlil=====

kriptografiya va kriptotizim=====

kripto va kriptotahlil=====

kriptoanaliz va kriptotizim

++++

Kriptologiya nima bilan shug‘ullanadi?=====

#maxfiy kodlarni yaratish va buzish ilmi bilan=====

maxfiy kodlarni buzish bilan=====

maxfiy kodlarni yaratish bilan=====

maxfiy kodlar orqali ma’lumotlarni yashirish bilan

++++

Kriptografiya nima bilan shug‘ullanadi?=====

#maxfiy kodlarni yaratish bilan=====

maxfiy kodlarni buzish bilan=====

maxfiy kodlar orqali ma’lumotlarni yashirish bilan=====

shifrlash uslublarini bilmagan holda shifrlangan ma’lumotni asl holatini topish bilan

++++

Kriptotahlil nima bilan shug‘ullanadi?=====

#maxfiy kodlarni buzish bilan=====

maxfiy kodlarni yaratish bilan=====

maxfiy kodlar orqali ma’lumotlarni yashirish bilan=====

shifrlash uslublarini bilmagan holda shifrlangan ma’lumotni asl holatini topish bilan

++++

Shifrlash orqali ma’lumotning qaysi xususiyati ta’minlanadi?=====

#maxfiyligi=====

Butunliligi=====

Ishonchliligi=====

foydalanuvchanligi

++++

Ochiq kalitli kriptotizimlar kim tomonidan kashf qilingan?=====

#U.Diffie va M.Hellman=====

Rivest va Adlman=====

Shamir va Rivest=====

U.Diffie va Rivest

++++

Kriptologiya necha yo‘nalishga bo‘linadi?=====

#2=====

14=====

16=====

18

++++

Kriptologiya so‘zining ma’nosi?=====

#cryptos – maxfiy, logos – ilm=====

cryptos – kodlash, logos – ilm=====

cryptos – kriptologiya, logos – yashiraman=====

cryptos – maxfiy, logos – kalit

++++

Ochiq kalitli kriptotizimlar ma'lumotni qanday xususiyatini taminlaydi?=====

#maxfiyligini=====

Butunligini=====

Foydalanuvchanligini=====

ma'lumotni autentifikatsiyasini

++++

Kriptotizimlar kalitlar soni bo‘yicha necha turga bo‘linadi?=====

#2=====

4=====

6=====

8

++++

Kriptotizimlar kalitlar soni bo‘yicha qanday turga bo‘linadi?=====

#simmetrik va assimetrik turlarga=====

simmetrik va bir kalitli turlarga=====

3 kalitli turlarga=====

assimetrik va 2 kalitli turlarga

++++

Simmetrik kriptotizimlardagi qanday muammoni ochiq kalitli kriptotizimlar bartaraf etdi?=====

#maxfiy kalitni uzatish muammosini=====

kalitni generatsiyalash muammosini=====

ochiq kalitni uzatish muammosini=====

kalitlar juftini hosil qilish muammosini

++++

Ochiq kalitli kriptotizimlarda qanday turdagi kalitlardan foydalanadi?=====

#ochiq va maxfiy kalitlardan=====

maxfiy kalitlar juftidan=====

maxfiy kalitni uzatishni talab etmaydi=====

ochiq kalitni talab etmaydi

++++

Assimetrik kriptotizimlarda necha kalitdan foydalaniladi?=====

#2 ta=====

3 ta=====

4 ta=====

kalit ishlatilmaydi

++++

Kerkxofs printsipi nimadan iborat?=====

#kriptografik tizim faqat kalit noma'lum bo'lgan taqdirdagina maxfiylik ta'minlanadi=====

kriptografik tizim faqat yopiq bo'lgan taqdirdagina maxfiylik ta'minlanadi=====

kriptografik tizim faqat kalit ochiq bo'lgan taqdirdagina maxfiylik ta'minlanadi=====

kriptografik tizim faqat ikkita kalit ma'lum bo'lgan taqdirdagina maxfiylik ta'minlanadi

++++

Kalit bardoshliligi bu -?=====

#eng yaxshi ma'lum algoritm bilan kalitni topish murakkabligidir=====

eng yaxshi ma'lum algoritm yordamida yolg'on axborotni ro'kach qilishdir=====

nazariy bardoshlilik=====

amaliy bardoshlilik

++++

Ochiq kalitni kriptotizimlarda nechta kalitdan foydalanadi?=====

#Ikkita=====

Bitta=====

Uchta=====

kalitdan foydalanilmaydi

++++

Ochiq kalitli kriptotizimlarda qaysi kalit orqali ma'lumot shifrlanadi?=====

#ochiq kalit orqali=====

maxfiy kalit orqali=====

ma'lumot shifrlanmaydi=====

ushbu tizimda kalitdan foydalanilmaydi

++++

Ochiq kalitli kriptotizimda, qaysi kalit orqali ma'lumot rasshifrovkalanadi?=====

#maxfiy kalit orqali=====

ochiq kalit orqali=====

ma'lumot shifrlanmaydi=====

ushbu tizimda kalitdan foydalanilmaydi

++++

Ochiq kalitli kriptotizimlarda asosan qanday turdagi sonlar bilan ishlaydi?=====

#tub sonlar bilan=====

kasr sonlar bilan=====

chekli maydonda kasr sonlar=====

faqat manfiy sonlar

++++

Qanday sonlar tub sonlar hisoblanadi?=====

#1 va o'ziga bo'linadigan sonlarlar=====

barcha toq sonlar=====

juft bo'lmagan sonlar=====

2 ga bo'linmaydigan sonlar

++++

Sonlarni tublikka tekshirish algoritmlari nechta sinfga bo'linadi?=====

#ikkita sinfga=====

uchta sinfga=====

bitta sinfga=====

sinflarga bo'linmaydi

++++

Kriptotahlil nima bilan shug'ullanadi? =====

#kalit yoki algoritmi bilmagan holda shifrlangan ma'lumotga mos keluvchi ochiq ma'lumotni topish bilan =====

ochiq ma'lumotlarni shifrlash masalalarining matematik uslublari bilan=====

maxfiy kodlarni yaratish bilan=====

maxfiy kodlar orqali ma'lumotlarni yashirish bilan

++++

RSA algoritmining mualliflarini ko'rsating=====

#R. Rayvest, A. Shamir, L. Adleman=====

Diffi va M. Xellman=====

R. Rayvest, K. Xellman, L. Adleman=====

L. Adleman, El Gamal, K. Shnorr

++++

Ochiq kalitli shifrlash algoritmi keltirilgan qatorni toping? =====

#RSA=====

AES=====

DES=====

RC4

++++

Ochiq kalitli shifrlash algoritmi keltirilgan qatorni toping?=====

#El-Gamal=====

AES=====

DES=====

RC4

++++

Shifrlash orqali ma'lumotning qaysi xususiyati ta'minlanadi?=====

#Maxfiyligi=====

Butunliligi=====

Ishonchliligi=====

Foydalanuvchanliligi

++++

Kriptografiya bu -?=====

#axborotni o'zgartirish vositalari va usullarini o'rganadigan fan=====

axborot mazmunidan beruxsat erkin foydalanishdan muhofazalash=====

axborotni buzishning oldini olish=====

axborot almashtirish vosita va usullari bilan shug'ullanadigan fan sohasi

++++

Faqat simmetrik algoritm keltirilgan qatorni ko'rsating?=====

#AES=====

RSA=====

El-Gamal=====

Barcha javoblar to'g'ri

++++

Kriptotizimlar kalitlar soni bo'yicha nechta turga bo'linadi?=====

#2=====

3=====

4=====

++++

Kriptotizimlar kalitlar soni bo'yicha qanday turga bo'linadi?=====

#simmetrik va assimetrik=====

simmetrik va bitta kalitli=====

3 kalitli kriptotizimlar=====

assimetrik va 2 ta kalitli

++++

Ferma testi qanday turdagi tublikka testlovchi algoritm hisoblanadi?=====

#ehtimollik testlar tarkibiga kiruvchi algoritm=====

aniqlashtirilgan testlar tarkibiga kiruvchi algoritm=====

taqribiy testlar tarkibiga kiruvchi algoritm=====

tublikka teslovchi algoritm hisoblanmaydi

++++

Solovey Shtrassen testi qanday turdagi tublikka testlovchi algoritm hisoblanadi?=====

#ehtimollik testlar tarkibiga kiruvchi algoritm=====

aniqlashtirilgan testlar tarkibiga kiruvchi algoritm=====

taqribiy testlar tarkibiga kiruvchi algoritm=====

tublikka teslovchi algoritm hisoblanmaydi

++++

Rabbi-Milner testi qanday turdagi tublikka testlovchi algoritm hisoblanadi?=====

#ehtimollik testlar tarkibiga kiruvchi algoritm=====

aniqlashtirilgan testlar tarkibiga kiruvchi algoritm=====

taqribiy testlar tarkibiga kiruvchi algoritm=====

tublikka teslovchi algoritm hisoblanmaydi

++++

Sonlarni tublikka tekshiruvchi algoritmlar necha sinfga bo'linadi?=====

#2=====

3=====

4=====

5

++++

Sonlarni tublikka tekshiruvchi algoritmlar qanday sinfga bo'linadi?=====

#aniqlashtirilgan va ehtimolli testlar=====

aniqlashtirilgan va taqribiy testlar=====

taqribiy va ehtimolli testlar=====

aniqlashtirilgan, ehtimolli va taqribiy testlar

++++

Sonlarni tublikka tekshiruvchi ehtimollikka asoslangan algoritmlar keltirilgan qatorni ko'rsating?=====

#Ferma, Solovey Shtrassen, Rabbi-Milner=====

Ferma, Solovey Shtrassen, Eyler=====

Eyler, Solovey Shtrassen, Rabbi-Milner=====

Ferma, Eyler, Rabbi-Milner

++++

Elliptik egriz chiqizlarda nuqtalar usitda qanday ammalar bajariladi?=====

#nuqtalarni qo'shish va nuqtalarni ikkilantirish=====

nuqtalarni qo'shish va nuqtalarni ko'paytirish=====

nuqtalarni qo'shish va nuqtalarni bo'lish=====

nuqtalarni ayirish va nuqtalarni ko'paytirish

++++

1 ga va o'ziga bo'linadigan sonlar qanday sonlar hisoblanadi?=====

#tub sonlar=====

murakkab sonlar=====

toq sonlar=====

juft sonlar

Elektron hujjat manbaini haqiqiyligini qaysi amal orqali amalga oshiriladi?=====

#ERI orqali amalga oshiriladi=====

shifrlash algoritmi orqali amalga oshiriladi=====

kodlash orqali amalga oshiriladi=====

autentifikatsiya orqali amalga oshiriladi

++++

Elektron hujjat yaxlitligini (o'zgarmasligini) tekshirish qaysi amal orqali amalga oshiriladi?=====

#ERI orqali amalga oshiriladi=====

kodlash orqali amalga oshiriladi=====

shifrlash algoritmi orqali amalga oshiriladi=====

autentifikatsiya orqali amalga oshiriladi

++++

Elektron hujjatni mualliflikdan bosh tortmasligini qaysi amal orqali amalga oshiriladi?=====

#ERI orqali amalga oshiriladi=====

kodlash orqali amalga oshiriladi=====

autentifikatsiya orqali amalga oshiriladi=====

shifrlash algoritmi orqali amalga oshiriladi

++++

Raqamli imzoni shakllantirish muolajasi qaysi algoritmga tegishli?=====

#ERI algoritmiga=====

kodlash algoritmiga=====

shifrlash algoritmiga=====

steganografiya algoritmiga

++++

ECDSA-2000 qaysi davlat standarti hisoblanadi?=====



#AQSH=====

Rossiya=====

O'zbekiston=====

Kanada

++++

O'zDSt 1092:2009 standarti qaysi davlat standarti hisoblanadi?=====

#O'zbekiston=====

AQSH=====

Rossiya=====

Kanada

++++

ГОСТ Р 34.10-94 standarti qaysi davlat standarti hisoblanadi?=====

#Rossiya=====

O'zbekiston=====

AQSH=====

Kanada

++++

Seans kalitli hamda seans kalitsiz rejimlarda ishlidigan standartni ko'rsating?=====

#O'zDSt 1092:2009=====

ECDSA-2000=====

ГОСТ Р 34.10-94=====

DSA

++++

DSA qanday standart hisoblanadi?=====

#ERI standarti=====

shifrlash standarti=====

kodlash standarti=====

steganografik standart

++++

Ochiq kalitli kriptotizimlar qanday turdagi matematik murakkablikka asoslangan algoritmlarga bo'linadi?=====

#faktorizatsiyalash va diskret logarifmlash algoritmlariga=====

modulyar arifmetika murakkabligiga asoslangan algoritmlarga=====

diskret logarifmlash murakkabligiga asoslangan algorimtlarga=====

faktorizatsiyalash murakkabligiga asoslangan algorimtlarga

++++

Ochiq kalitli kriptotizimlarning bardoshligini ta'minlashda qanday murakkab muammo turiga asoslanadi?=====

#faktorlash, diskret logarifmlash, elliptik egri chiziqda diskret logarifmlash=====

faktordash, diskret logarifmlash=====

faktordash, diskret logarifmlash, elliptik egri chiziqda faktORIZatsiyalash=====

faktordash, diskret logarifmlash, modulyar arifmetikaga

++++

Ehtimolli testlar sonlarni tublikka tekshirishda qanday natijani beradi?=====

#tekshirilayotgan son tub yoki tubmasligi haqida ehtimollik bilan javob beradi=====

tekshirilayotgan son tub yoki tubmasligi haqida kafolatlangan aniq javob beradi=====

tekshirilayotgan son tub yoki tubmasligi haqida tasodifiy ravishda javob beradi=====

tekshirilayotgan son tub yoki tubmasligini 0 va 1 qiymatlarga qarab javob beradi

++++

Sonlarni tublikka tekshirishning ehtimolli algoritmlariga quyidagilarning qaysilari kiradi?=====

#Ferma, Rabbi-Milner, Poklington testlari=====

Rabbi-Milner, Solovey-Shtrassen, Pollard testlari=====

Ferma, Solovey-Shtrassen, Pollard testlari=====

Rabbi Milner, Poklington, Pollard testlari

++++

Ochiq kalitli RSA shifrlash algoritmi bardoshliligi qanday matematik muammo turiga asoslangan?=====

#faktordash murakkabligiga=====

diskret logarifmlash murakkabligiga=====

elliptik egri chiziqlarda faktORIZatsiyalash murakkabligiga=====

elliptik egri chiziqlarda faktORIZatsiyalash murakkabligiga

++++

Ochiq kalitli El-Gamal shifrlash algoritmi qanday matematik murakkablikka asoslanadi?=====

#diskret logarifmlash murakkabligiga=====

faktordash murakkabligiga=====

elliptik egri chiziqda diskret logarifmlash murakkabligiga=====

elliptik egri chiziqda faktordash murakkabligiga

++++

Diffie-Helman algoritmi qanday matematik murakkablikka asoslanadi?=====

#diskret logarifmlash murakkabligiga=====

faktordash murakkabligiga=====

elliptik egri chiziqda diskret logarifmlash murakkabligiga=====

elliptik egri chiziqda faktordash murakkabligiga

++++

Diffie-Hellman qanday algoritm hisoblanadi?=====

#kalitlarni ochiq taqsimlash algoritmi=====

ochiq kalitli shifrlash algoritmi=====

diskret logarifmlash murakkabligiga asoslangan shifrlash algoritmi=====

faktirlash murakkabligiga asoslangan kalitlarni ochiq taqsimlash algoritmi

++++

ERI algoritmlari qanday muolajalardan iborat?=====

#imzoni shakllantirish, imzoni tekshirish=====

imzoni shakllantirish, imzo qo'yish va imzoni tekshirish=====

imzoni shakllantirish va imzo qo'yish=====

imzo qo'yish

++++

Ochiq kalitli kriptotizimlarda elektron hujjatlarga imzo qo'yish qaysi kalit orqali amalga oshiriladi?=====

#shaxsiy kalit orqali=====

ochiq kalit orqali=====

imzo qo'yilishi kalitga bog'liq emas=====

imzo qo'lda qo'yiladi

++++

Ochiq kalitli kriptotizimlarda elektron hujjatlarga qo'yilgan imzoni tekshirish qaysi kalit orqali amalga oshiriladi?=====

#ochiq kalit orqali=====

maxfiy kalit orqali=====

imzo qo'yilishi kalitga bog'liq emas=====

imzo qo'lda qo'yiladi

++++

Diskret logarifmlash murakkabligiga asoslangan algoritm keltirilgan qatorni ko'rsating?=====

#Diffie-Hellman, EL-Gamal algoritmi=====

RSA algoritmi=====

EL-Gamal algoritmi=====

Diffie-Hellman algoritmi

++++

Faktirlash murakkabligiga asoslangan algoritm keltirilgan qatorni ko'rsating?=====

#RSA=====

El-Gamal =====

Diffie-Hellman=====

DSA

++++

Karlmaykl sonlari qaysi tublikka tekshiruvchi algoritmlarda doim bajariladi?=====

#Ferma testida=====

Solovey-Shtrassen testida=====

Eyler testida=====

Rabbin testida

++++

Ochiq kalitli RSA shifrlash algoritmda maxfiy kalit qanday topiladi?=====

# $e*d=1 \bmod (p*q)$  taqqoslamadan=====

$e*d=1 \bmod N$ =====

$e*d=1 \bmod \varphi(p-1)$ =====

$e*d=1 \bmod \varphi((p-1)(q-1))$

++++

Ochiq kalitli RSA shifrlash algoritmda qaysi parametrlar ochiq holda e'lon qilinadi?=====

# $N, e$ =====

$e$ =====

$N, d$ =====

$d$

++++

Ochiq kalitli RSA shifrlash algoritmda "e" ochiq kalit, "d" shaxsiy kalit bo'lsa deshifrlash formulasi to'g'ri ko'rsatilgan qatorni belgilang?=====

# $M=C^d \bmod N$ =====

$M=C^d \bmod \varphi(N)$ =====

$M=C^e \bmod N$ =====

$M=C^e \bmod \varphi(N)$

++++

Ochiq kalitli RSA shifrlash algoritmda "d" shaxsiy kalit, "e" ochiq kalit bo'lsa shifrlash formulasi to'g'ri ko'rsatilgan qatorni belgilang?=====

# $C=M^e \bmod N$ =====

$C=M^e \bmod \varphi(N)$ =====

$C=M^d \bmod \varphi(N)$ =====

$C=M^d \bmod N$

++++

Ochiq kalitli El-Gamal shifrlash algoritmda "p" tub son bo'lsa maxfiy kalit qanday tanlanadi?=====

# $(p-1)$  bilan o'zaro tub bo'lgan  $(1, p-1)$  intervaldagi butun son=====

$p$  bilan o'zaro tub bo'lgan  $(1, p-1)$  intervaldagi butun son=====

$(1, p-1)$  intervaldagi tub son=====

$(p-1)$  bilan o'zaro tub bo'lgan  $(1, p)$  intervaldagi butun son

++++

Ochiq kalitli El-Gamal shifrlash algoritmda ochiq kalit qanday hisoblanadi?=====

# $y=g^a \bmod p$ , bu yerda  $g$ -birlamchi ildiz,  $a$ -maxfiy kalit,  $p$ -tub son=====

$y=g^a \bmod p$ , bu yerda  $g$ -soni  $(p-1)$  dan kichik butun son,  $a$ -maxfiy kalit,  $p$ -tub son=====

$y=g^a \bmod p$ , bu yerda  $g$ -soni  $p$  dan kichik butun son,  $a$ -maxfiy kalit,  $p$ -tub son=====

$y = g^a \pmod{p}$ , bu yerda  $g$ -soni  $(p-1)$  bilan o'zaro tub bo'lgan butun son,  $a$ -maxfiy kalit,  $p$ -tub son

++++

Ochiq kalitli kriptotizimlarga asoslangan kalitlarni taqsimlash Diffie-Hellman algoritmi ishlash prinsipi qanday?=====

#umumiy maxfiy kalitni hosil qilishga asoslangan=====

ochiq va yopiq kalitlar juftini hosil qilishga asoslangan=====

maxfiy kalitni uzatishni talab etmaydigan prinsipga asoslangan=====

ochiq kalitlarni hosil qilishga asoslangan

++++

"A" va "B" foydalanuvchilar ma'lumot almashmoqchi, "A" foydalanuvchi "B" tomondan qabul qilgan ma'lumotni imzosini tekshirishda qaysi kalitdan foydalanadi?=====

#"B" foydalanuvchining ochiq kalitidan=====

"B" foydalanuvchining maxfiy kalitidan=====

"A" foydalanuvchi o'zining ochiq kalitidan=====

"A" foydalanuvchini o'zining maxfiy kalitidan

++++

RSA algoritmidagi  $p=3$ ,  $q=11$ ,  $e=3$  bo'lganda maxfiy kalitni qiymati topilsin:  $e \cdot d \equiv 1 \pmod{\varphi(N)}$ ?=====

#7=====

6=====

8=====

5

++++

Faktorlash muammosini bartaraf etuvchi usul keltirilgan qatorni ko'rsating?=====

#Pollard usuli=====

Xitoy teoremasi=====

Pohlig-Hellman usulu=====

RSA usuli

++++

Pollard usuli qanday turdagi matematik murakkablikni yechishda foydalaniladi?=====

#faktorlash murakkabligini=====

diskret logarifmlash murakkabligini=====

elliptik egrzi chiziqda diskret logarifmlash murakkabligini=====

elliptik egrzi chiziqda faktorlash murakkabligini

++++

RSA algoritmidagi matematik murakkablikni qanday usul orqali bartaraf qilish mumkin?=====

#Pollard usuli=====

Xitoy teoremasi=====

Pohlig-Hellman usuli=====

RSA usuli

++++

Diskret logarifmlash muammosini bartaraf etuvchi usul keltirilgan qatorni ko'rsating?=====

#Pohlig-Hellman usuli=====

Pollard usuli=====

Xitoy teoremasi=====

RSA usuli

++++

Pohlig-Hellman usuli qanday turdagi matematik murakkablikni yechishda foydalaniladi?=====

#diskret logarifmlash murakkabligini=====

faktirlash murakkabligini=====

elliptik egrzi chiziqda faktirlash murakkabligini=====

daraja parameter murakkabligini

++++

Evklidning kengaytirilgan algoritmidan RSA shifrlash algoritmining qaysi parametrini hisoblashda foydalaniladi?=====

#maxfiy kalitni=====

ochiq kalitni=====

tub sonlarni=====

modul qiymatini

++++

Diffie-Hellman algoritmidan qaysi parametrlar ochiq holda e'lon qilinadi?=====

#p va g tub sonlarni( $p > g$ )=====

p tub sonni=====

p va g toq sonlarni( $p > g$ )=====

p va g juft sonlarni( $p > g$ )

++++

Axborot xavfsizligining pasayishi nimani anglatadi?

=====#axborot [xavfsizligi](#)

=====ma'lumotlarning tartibsizligi

=====ma'lumotlarning mas'uliyatsizligi

=====ichki xavfsizlik

+++++

Tashkilotning iqtisodiy xavfsizligini ta'minlash muammosining eng muhim tarkibiy qismlaridan biri bu

=====#Axborot texnologiyalari (IT) va tizimlar (IS) xavfsizligi

=====Axborot texnologiyalari (IT) xavfsizligi

=====Axborot tizimlarining xavfsizligi (IS)

=====Texnik tizimlarning xavfsizligi (TS)

+++++

Axborot tizimlari va texnologiyalarini rivojlantirish, joriy qilish va ulardan foydalanishning ajralmas qismi hisoblanadi

=====#Axborot xavfsizligi

=====kriptografiya

=====steganografiya

=====autentifikatsiya

+++++

Zamonaviy dasturlash texnologiyasi sizni mutlaqo xatosiz va xavfsiz dasturlarni yaratishga imkon beradimi?

=====#emas

=====Ha

=====noma'lum

=====savol noto'g'ri

+++++

Huquqiy hujjatlar talablariga yoki ma'lumot egalari tomonidan o'rnatilgan talablarga muvofiq mulkka tegishli va himoya qilinishi kerak bo'lgan ma'lumotlar

=====#himoyalangan ma'lumotlar

=====maxfiy ma'lumotlar

=====keraksiz ma'lumotlar

=====foydali ma'lumotlar

+++++

Axborot egalari bo'lishi mumkin:

=====#davlat, yuridik shaxs, shaxslar guruhi, yakka shaxs.

=====davlat xizmatchisi, yuridik shaxs, shaxslar guruhi, jismoniy shaxs.

=====davlat, yuridik shaxs, shaxslar guruhi, alohida aktsiyadorlik jamiyati.

=====davlat, yuridik shaxs, shaxslar guruhi, alohida kompaniya.

+++++

Axborotni qayta ishlashning avtomatlashtirilgan tizimlari nima uchun kerak?

=====#ma'lumotlarni saqlash, qayta ishlash va uzatish uchun

=====ma'lumotlarni saqlash, yangilash va yashirish uchun

=====ma'lumotlarni saqlash, qayta ishlash va shifrlash uchun

=====ma'lumotlarni saqlash, qayta ishlash va tahlil qilish uchun

+++++

Axborot xavfsizligini buzishning potentsial yoki real xavfini keltirib chiqaradigan shartlar va omillar to'plami

=====#Tahdid (axborot xavfsizligi)

=====Maxfiylikni buzish

=====Hodisa

=====Hujum

+++++

Axborot xavfsizligiga tahdidning bevosita sababi bo'lgan sub'ekt (shaxs, moddiy ob'ekt yoki jismoniy hodisa)

=====#Axborot xavfsizligiga tahdid manbai

=====Texnik xavfsizlik manbai

=====Virus hujumining manbasi

=====Xodimlarning manbasi

+++++

Axborot tizimining xususiyati, unda ishlov beriladigan axborotga tahdidlarni amalga oshirishga imkon beradi

=====#Zaiflik (axborot tizimi)

=====Xaker hujumi

=====Hodisa

=====Qayta rasmiylashtirish

+++++

Yashirin yoki mahfiy axborotni amalga oshirish natijasida shaxs, shaxslar guruhi yoki u mo'ljallanmagan har qanday tashkilot uchun foydalanish mumkin bo'lgan tahdid

=====#Maxfiylikka tahdid (oshkor qilish tahdidi)

=====Butunlik uchun tahdid

=====Texnik tahdid

=====Xaker hujumi

+++++

Amalga oshirilishi natijasida ma'lumotlar o'zgartirilishi yoki yo'q qilinishi mumkin bo'lgan tahdid

=====#Butunlik uchun tahdid

=====Virusli hujum xavfi

=====Tarmoq tahdidi

=====Texnik tahdid

+++++

Tashkilotni o'z faoliyatida yo'naltiradigan hujjatlashtirilgan qoidalar, protseduralar, amaliyotlar yoki axborot xavfsizligi sohasidagi ko'rsatmalar to'plami

=====#Xavfsizlik [siyosati](#)

=====Davlat siyosati

=====Korporativ etika

=====Ko'rsatmalar

+++++

Amalga oshirilishi avtomatlashtirilgan tizim mijozlariga xizmat ko'rsatishni rad etishga, tajovuzkorlarning o'z xohishlariga ko'ra manbalardan ruxsatsiz foydalanishiga olib keladigan tahdid hisoblanadi.

=====#Xizmat tahdidini rad etish (mavjud tahdid)

=====Texnik muammo

=====Tizimning favqulodda to'xtashi

=====Hujum



+++++

Uning maxfiyligi, ochiqqligi va yaxlitligi ta'minlanadigan axborot xavfsizligi holati

=====#Axborot xavfsizligi  
=====#Ma'lumot xavfsizligi  
=====#Operatsion tizim xavfsizligi  
=====#Shaxsiy ma'lumotlar xavfsizligi

+++++

Axborotni himoya qilish usuli

=====#axborotni himoya qilishning muayyan printsiplari va vositalarini qo'llash tartibi va qoidalari.  
=====#axborotni texnik himoya qilishning muayyan printsiplari va vositalarini qo'llash tartibi va qoidalari.  
=====#ma'lum bir algoritmlar va axborot xavfsizligi vositalarini qo'llash tartibi va qoidalari.  
=====#axborotni himoya qilishning ayrim algoritmlarini qo'llash tartibi va qoidalari.

+++++

Apparat, dasturiy ta'minot, dasturiy ta'minot va apparat, axborotni himoya qilish uchun mo'ljallangan yoki ishlatiladigan materiallar va (yoki) materiallar

=====#Axborot xavfsizligi vositasi  
=====#Axborotni nusxalash vositasi  
=====#Axborot uzatish vositasi  
=====#Shaxsiy ma'lumotlarni uzatish vositasi

+++++

Axborotni kriptografik o'zgartirish orqali himoya qilish

=====#kriptografik ma'lumotlarni himoya qilish  
=====#antivirus ma'lumotlarini himoya qilish  
=====#ma'lumotlarni steganografik himoya qilish  
=====#axborotni texnik himoya qilish

+++++

Ruxsat berilgan shaxslarning kirib borishi yoki kirishiga to'sqinlik qiladigan vositalar to'plami va tashkiliy choralar yordamida axborotni himoya qilish himoya qilinadigan obyekt hisoblanadi.

=====#axborotni jismoniy himoya qilish  
=====#axborotni dasturiy himoyasi  
=====#antivirus ma'lumotlarini himoya qilish  
=====#oddiy ma'lumotlarni himoya qilish

+++++

Muayyan tarmoq tugunini o'chirishga qaratilgan hujum turi (Xizmatni rad etish - DoS)

=====#xizmatdan bosh tortish  
=====#"ma'lumotlarga kirishni rad etish"  
=====#"ma'lumotlarga kirishni rad etish"  
=====#"parolga kirish taqiqlandi"

+++++

Kriptovalyutatsiya atamasini birinchi bo'lib kiritgan olimni ko'rsating

=====#F. Fridman

=====#Aristotel

=====#Shannon

=====#Aliqushchi

+++++

IV asrda "antiscital" dekifrlash qurilmasini kim yaratgan. Mil. Avv.

=====#Aristotel

=====#Sokrat

=====#Ptolemey

=====#Spital

+++++

Qaysi olimning kitobida chastota kriptovalyutasi to'g'risida birinchi ma'lum eslatma mavjud?

=====#Al-Kindi

=====#Aristotel

=====#Umar Xayyom

=====#Mirzo Ulug'bek

+++++

Qur'on matni asosida arab tilidagi harflarning chastota jadvalini birinchi bo'lib kim aniqlagan?

=====#Shihab al-Kalkasandi

=====#Umar Xayyom

=====#Mirzo Ulug'bek

=====#Imom Buxoriy

+++++

Axborotni shifrlash va shifrlash usullarini qaysi fan rivojlantirmoqda?

=====#Kriptologiya

=====#Informatika

=====#Matematika

=====#Fizika

+++++

DES shifrlash algoritmi qaysi tarmoqqa asoslangan holda ishlaydi?

=====#Feystel tarmog'iga asoslangan holda

=====#SPN tarmog'iga asoslangan holda

=====#hech qanday tarmoqqa asoslanmaydi

=====#Lai-Massey tarmog'iga asoslangan holda

+++++

Quyida keltirilgan xususiyatlarning qaysilari xesh funksiyaga mos?

=====#chiqishda fiksirlangan uzunlikdagi qiymatni beradi  
=====chiqishda bir xil qiymatni beradi  
=====kolliziyaga ega  
=====chiqishdagi qiymat bilan kiruvchi qiymatlar bir xil bo'ladi

+++++

Quyida keltirilgan xususiyatlarning qaysilari xesh funksiyaga mos?

=====#ixtiyoriy olingan har xil matn uchun xesh qiymatlar bir xil bo'lmaydi  
=====ixtiyoriy olingan bir xil matn uchun qiymatlar bir xil bo'lmaydi  
=====ixtiyoriy olingan har xil matn uchun xesh qiymatlar bir xil bo'ladi  
=====ixtiyoriy olingan har xil xesh qiymat uchun dastlabki ma'lumotlar bir xil bo'ladi

+++++

DES shifrlash algoritmidan har bir raunda necha bitli raund kalitlaridan foydalaniladi?

=====#48  
=====56  
=====64  
=====32

+++++

Qaysi hujum turida barcha bo'lishi mumkin bo'lgan variantlar ko'rib chiqiladi?

=====#qo'pol kuch hujumi  
=====sotsial injineriya  
=====analitik hujum  
=====chastotalar tahlili

+++++

Ma'lumotlarni autentifikatsiyalash kodlari deb qanday xesh funksiyalarga aytiladi?

=====#kalitli [xesh funksiyalarga](#)  
=====kalitsiz xesh funksiyalarga  
=====kriptografik bo'lmagan xesh funksiyalarga  
=====kriptografik xesh funksiyalarga

+++++

AES algoritmidan raundlar soni nimaga bo'g'liq?

=====#kalit uzunligiga  
=====kiruvchi blok uzunligiga  
=====foydalanilgan vaqtiga  
=====kiruvchi blok uzunligi va matn qiymatiga

+++++

A5/1 oqimli shifrlash algoritmidan registrlarning surilishi qanday kattalikka bog'liq?

=====#maj funksiyasi qiymatiga

====kalit qiymatiga  
====registr uzunligi qiymatiga  
====hech qanday kattalikka bog'liq emas

+++++  
16 raund davom etadigan blokli shifrlash algoritmi ko'rsating?

====#DES  
====AES  
====RC4  
====A5/1

+++++  
10 raund davom etadigan blokli shifrlash algoritmi ko'rsating?

====#AES  
====DES  
====RC4  
====A5/1

+++++  
Xesh qiymatlarni yana qanday atash mumkin?

====#dayjest  
====funksiya  
====imzo  
====raqamli imzo

+++++  
Ximoyalanuvchi ma'lumot boshqa bir ma'lumotni ichiga yashirish orqali maxfiyligini ta'minlaydigan usul qaysi?

====#steganografiya  
====kodlash  
====shifrlash  
====autentifikatsiya

+++++  
Baytlar kesimida shifrlashni amalga oshiradigan algoritm keltirilgan qatorni ko'rsating?

====#RC4  
====A5/1  
====MD5  
====SHA1

+++++  
Kolliziya deb nima nisbatan aytiladi?

====#ikkita har xil matn uchun bir xil xesh qiymat mos kelishi  
====ikkita bir xil matn uchun bir xil xesh qiymat mos kelishi  
====ikkita har xil matn uchun har xil xesh qiymat mos kelishi

====ikkita bir xil matn uchun bir xil xesh qiymat mos kelmasligiga

+++++

Konfidensiallikni ta'minlash bu -?

====#ruxsat etilmagan "o'qishdan" himoyalash

====ruxsat etilmagan "yozishdan" himoyalash

====ruxsat etilmagan "bajarishdan" himoyalash

====ruxsat berilgan "amallarni" bajarish

+++++

Sezar shifrlash algoritmi qaysi turdagi akslantirishga asoslangan?

====#o'rniga qo'yish

====o'rin almashtirish

====aralash

====kompozitsion

+++++

CRC-3 tizimida CRC qiymatini hisoblash jarayonida ma'lumotga nechta nol biriktiriladi?

====#3

====6

====12

====9

+++++

.... kriptotizimni shifrlash va rasshifrovkalash uchun sozlashda foydalaniladi.

====#kalit

====ochiq matn

====algoritm

====alifbo

+++++

CRC-5 tizimida CRC qiymati hisoblash jarayonida ma'lumotga nechta nol biriktiriladi?

====#5

====10

====15

====20

+++++

Rasshifrovkalash jarayonida kalit va ..... kerak bo'ladi

====#shifrmtn

====ochiq matn

====kodlash

====alifbo

+++++

Kriptologiya qanday yoʻnalishlarga boʻlinadi?

=====#kriptografiya va kriptotahlil

=====#kripto va kriptotahlil

=====#kriptografiya va kriptotizim

=====#kriptoanaliz va kriptotizim

+++++

Kriptotizimlar kalitlar soni boʻyicha necha turga boʻlinadi?

=====#2

=====#6

=====#4

=====#8

+++++

Kriptografiya nima bilan shugʻullanadi?

=====#maxfiy kodlarni yaratish bilan

=====#maxfiy kodlar orqali maʼlumotlarni yashirish

=====#bilan maxfiy kodlarni buzish bilan

=====#shifrlash uslublarini bilmagan holda shifrlangan maʼlumotni asl holatini topish bilan

+++++

Kerkxofs printsipi nimadan iborat?

=====#kriptografik tizim faqat kalit nomaʼlum boʻlgan taqdirdagina maxfiylik taʼminlanadi

=====#kriptografik tizim faqat yopiq boʻlgan taqdirdagina maxfiylik taʼminlanadi

=====#kriptografik tizim faqat ikkita kalit maʼlum boʻlgan taqdirdagina maxfiylik taʼminlanadi

=====#kriptografik tizim faqat kalit ochiq boʻlgan taqdirdagina maxfiylik taʼminlanadi

+++++

Shifrlash orqali maʼlumotning qaysi xususiyati taʼminlanadi?

=====#maxfiyligi

=====#ishonchliligi

=====#butunliligi

=====#foydalanuvchanligi

+++++

Oʻrniga qoʻyish shifrlash sinfiga qanday algoritmlar kiradi?

=====#shifrlash jarayonida ochiq maʼlumot alfavit belgilari shifr maʼlumot =====belgilariga almashtiriladigan algoritmlar

=====#shifrlash jarayonida ochiq maʼlumot alfaviti belgilarining oʻrinlar almashtiriladigan algoritmlar

=====#shifrlash jarayonida kalitlarning oʻrni almashtiriladigan algoritmlarga

=====#shifrlash jarayonida oʻrniga qoʻyish va oʻrin almashtirish akslantirishlarning kombinatsiyalaridan birgalikda foydalaniladigan algoritmlar

+++++

Kriptologiya necha yo‘nalishga bo‘linadi?

=====#2

====4

====8

====6

+++++

Kriptologiya so‘zining ma‘nosi?

=====#cryptos – maxfiy, logos – ilm

====cryptos – maxfiy, logos – kalit

====cryptos – kriptologiya, logos – yashiraman

====cryptos – kodlash, logos – ilm

+++++

O‘rniga qo‘yish shifrlash algoritmlari necha sinfga bo‘linadi?

=====#2

====6

====4

====8

+++++

O‘rniga qo‘yish shifrlash algoritmlari qanday sinfga bo‘linadi?

=====#bir qiymatli va ko‘p qiymatli shifrlash

====bir qiymatli shifrlash

====ko‘p qiymatli shifrlash

====uzluksiz qiymatli shifrlash

+++++

Kriptologiya nima bilan shug‘ullanadi?

=====#maxfiy kodlarni yaratish va buzish ilmi bilan

====maxfiy kodlarni yaratish bilan

====maxfiy kodlarni buzish bilan

====maxfiy kodlar orqali ma‘lumotlarni yashirish bilan

+++++

Ma‘lumotlarni kodlash va dekodlashda necha kalitdan foydalanadi?

=====#kalit ishlatilmaydi

====3 ta

====2 ta

====4 ta

+++++

Simmetrik kriptotizimlarda necha kalitdan foydalaniladi?

=====#1 ta  
====3 ta  
====kalit ishlatilmaydi  
====4 ta

+++++  
Kriptotahlil nima bilan shugʻullanadi?

=====#maxfiy kodlarni buzish bilan  
====shifrlash uslublarini bilmagan holda shifrlangan ma'lumotni asl holatini topish bilan  
====maxfiy kodlar orqali ma'lumotlarni yashirish bilan  
====maxfiy kodlarni yaratish bilan shifrlash uslublarini bilmagan holda shifrlangan ma'lumotni asl holatini topish bilan

+++++  
A5/1 oqimli shifrlash algoritmidagi dastlabki kalit uzunligi nechki bitga teng?

=====#64  
====192  
====512  
====256

+++++  
Steganografiya ma'lumotni qanday maxfiylashtiradi?

=====#maxfiy xabarni soxta xabar ichiga berkitish orqali  
====maxfiy xabarni kriptografik kalit yordamida shifrlash orqali  
====maxfiy xabarni kodlash orqali  
====maxfiy xabarni shifrlash orqali

+++++  
Shifrlash algoritmlari akslantirish turlariga qarab qanday turlarga bo'linadi?

=====#o'rniga qo'yish, o'rin almashtirish va kompozitsion akslantirishlarga  
====o'rniga qo'yish, o'rin almashtirish va surish akslantirishlariga  
====o'rniga qo'yish va o'rin almashtirish akslantirishlariga  
====o'rniga qo'yish, sirush va kompozitsion shifrlash akslantirishlariga

+++++  
Blokli shifrlash algoritmlari arxitekturasini jihatidan qanday tarmoqlarga bo'linadi?

=====#Feistel va SP  
====Feistel va Petri  
====SP va Petri  
====Kvadrat va iyerarxik

+++++  
Zamonaviy kriptografiya qaysi bo'limlarni o'z ichiga oladi?



=====#simmetrik kriptotizimlar, ochiq kalitli kriptotizimlar, elektron raqamli imzo kriptotizimlari, kriptobardoshli kalitlarni ishlab chiqish va boshqarish

====simmetrik kriptotizimlar, ochiq kalit algoritmiga asoslangan kriptotizimlar, elektron raqamli imzo kriptotizimlari, foydalanuvchilarni ro'yxatga olish

====simmetrik kriptotizimlar, ochiq kalit algoritmiga asoslangan kriptotizimlar, elektron raqamli imzo kriptotizimlari, foydalanuvchilarni identifikatsiya qilish

====simmetrik kriptotizimlar, ochiq kalit algoritmiga asoslangan kriptotizimlar, elektron raqamli imzo kriptotizimlari, foydalanuvchilarni autentifikatsiyalash

+++++

ARX amali nimalardan iborat?

=====#add, rotate, xor

====add, rotate, mod

====add, mod, xor

====mod, rotate, xor

+++++

Tasodifiy ketma-ketliklarni generatsiyalashga asoslangan shifrlash turi bu?

=====#oqimli shifrlar

====blokli shifrlar

====ochiq [kalitli shifrlar](#)

====assimetrik shifrlar

+++++

Qanday algoritmlarda chiqishda doim fiksirlangan uzunlikdagi qiymat chiqadi?

=====#xesh algoritmlarda

====kodlash algoritmlarida

====shifrlash algoritmlarida

====steganografik algoritmlarda

+++++

Ma'lumotni shifrlash va deshifrlash uchun bir xil kalitdan foydalanuvchi tizim bu?

=====#simmetrik kriptotizim

====ochiq [kalitli kriptotizim](#)

====assimetrik kriptotizim

====xesh funksiyalar

+++++

Ikki kalitli deyilganda qaysi kriptotizim nazarda tutiladi?

=====#ochiq kalitli kriptotizim

====simmetrik kriptotizim

====xesh funksiyalar

====MAC tizimlari

+++++

Simmetrik shifrlash algoritmlarida qanday muammo mavjud?

=====#kalitni uzatish  
=====#kalit generatsiyalash  
=====#kalitni yo'q qilish  
=====#muammo yo'q

+++++

Sezar shifrlash usuli qaysi akslantirishga asoslangan?

=====#o'rniga qo'yish  
=====#o'rin almashtirish  
=====#ochiq kalitli shifrlarga  
=====#kombinatsion akslantirishga

+++++

Ma'lumotni uzatishda kriptografik himoya .....

=====#konfidensiallik va yaxlitlikni ta'minlaydi  
=====#konfidensiallik va foydalanuvchanlikni ta'minlaydi  
=====#konfidensiallikni ta'minlaydi  
=====#foydalanuvchanlik ta'minlaydi va butunlikni

+++++

Butunlikni ta'minlash bu - ?

=====#ruxsat etilmagan "yozishdan" himoyalash  
=====#ruxsat etilmagan "bajarishdan" himoyalash  
=====#ruxsat etilmagan "o'qishdan" himoyalash  
=====#ruxsat berilgan "amallarni" bajarish

+++++

Shifrlash va deshifrlashda alohida kalitlardan foydalanuvchi kriptotizimlar bu?

=====#ochiq kalitli kriptotizimlar  
=====#simmetrik kriptotizimlar  
=====#bir kalitli kriptotizimlar  
=====#xesh funksiyalar

+++++

Agar ochiq ma'lumot shifrlansa, natijasi .... bo'ladi.

=====#shifrmavn  
=====#ochiq matn  
=====#noma'lum  
=====#kod

+++++

Ochiq kalitli shifrlar axborotni qaysi xususiyatlarini ta'minlashda foydalaniladi?

=====#konfidensiallik va yaxlitlilik  
=====#konfidensiallik va foydalanuvchanlik  
=====#foydalanuvchanlik va yaxlitlik  
=====#foydalanuvchanlik

+++++

MD5 xesh funksiyasida kiruvchi ma'lumot uzunligi qanday bitli bloklarga bo'linadi?

=====#512  
=====#1024  
=====#2048  
=====#4096

+++++

add amalining ma'nosi nima?

=====#modul asosida qo'shish  
=====#XOR amali  
=====#surish (siklik surish, mantiqiy surish)  
=====#akslantirish

+++++

SHA1 xesh funksiyasida initsializatsiya bosqichida 5 ta necha bitli registrlardan foydalanadi?

=====#32  
=====#64  
=====#128  
=====#256

+++++

O'zbekistonda kriptografiya sohasida faoliyat yurituvchi tashkilot nomini ko'rsating?

=====#"UNICON.UZ" DUK  
=====#"O'zstandart" agentligi  
=====#Kadastr agentligi  
=====#Davlat Soliq Qo'mitasi

+++++

Faqat simmetrik shifrlash algoritmlari nomi keltirilgan qatorni ko'rsating?

=====#AES, A5/1  
=====#SHA1, DES  
=====#MD5, AES  
=====#HMAC, RC4

+++++

HMAC tizimida kalit qiymati blok uzunligiga teng bo'lganda ma'lumotga qanday biriktiriladi?

=====#kalit qiymati o'zgartirilmagan holda ma'lumotga [biriktiriladi](#)

====kalit qiymati blok uzunligiga teng bo'lguncha nol qiymat bilan to'ldirilib hosil bo'lgan qiymat ma'lumotga  
biriktiriladi

====kalitni xesh qiymati hisoblanib, unga blok uzunligiga teng bo'lguncha nol qiymat qo'shiladi va yangi hosil bo'lgan  
qiymat ma'lumotga biriktiriladi

====xesh funksiyalarda kalit qiymatida foydalanilmaydi

+++++

DES shifrlash algoritmda rasshifrovkalashda birinchi raunda qaysi kalitdan foydalaniladi?

====#16-raund kalitidan

====1-raund kalitidan

====1-raunda kalitdan foydalanilmaydi

====dastlabki kalitdan

+++++

SHA1 xesh funksiyasida kiruvchi ma'lumot uzunligi qanday bitli bloklarga bo'linadi?

====#512

====1024

====2048

====4096

+++++

AES shifrlash algoritmda blok uzunligi 128, kalit uzunligi 192 bit bo'lsa raundlar soni nechta bo'ladi?

====#12

====10

====14

====6

+++++

AES shifrlash algoritmda nechta akslantirishdan foydalanadi?

====#4

====3

====2

====akslantirishdan foydalanilmaydi

+++++

GSM tarmog'ida foydalaniluvchi shifrlash algoritmi nomini ko'rsating?

====#A5/1

====dastlabki kalitdan

====AES

====DES

+++++

WEP protokolida (Wi-Fi tarmog'ida) foydalaniluvchi shifrlash algoritmi nomini ko'rsating?

====#RC4

====DES  
====SHA1  
====A5/1

+++++  
rotate amalining ma'nosi nima?

====#surish (siklik surish, mantiqiy surish)  
====modul asosida qo'shish  
====XOR amali  
====Akslantirish

+++++  
SHA1 xesh funksiyasida to'ldirish bitlarini qo'shishda ma'lumot uzunligi 512 modul bo'yicha qanday son bilan taqqoslanadigan qilib to'ldiriladi?

====#448  
====1002  
====988  
====772

+++++  
HMAC tizimida kalit qiymati blok uzunligidan kichik bo'lganda ma'lumotga qanday biriktiriladi?

====#kalit qiymati blok uzunligiga teng bo'lguncha nol qiymat bilan to'ldirilib hosil bo'lgan qiymat ma'lumotga biriktiriladi  
====kalitni xesh qiymati hisoblanib, unga blok uzunligiga teng bo'lguncha nol qiymat qo'shiladi va yangi hosil bo'lgan qiymat ma'lumotga biriktiriladi  
====kalit qiymati o'zgartirilmagan holda ma'lumotga biriktiriladi  
====xesh funksiyalarda kalit qiymatida foydalanilmaydi

+++++  
Kolliziya hodisasi qaysi turdagi algoritmlarga xos?

====#xesh funksiyalar  
====ochiq kalitli shifrlash algoritmlari  
====kalitlarni boshqarish tizimlari  
====simmetrik shifrlash algoritmlari

+++++  
AES shifrlash algoritmidan shifrlash jarayonida qanday akslantirishdan foydalaniladi?

====#SubBytes, ShiftRows, MixColumns va AddRoundKey  
====SubBytes, ShiftRows va AddRoundKey  
====SubBytes, MixColumns va AddRoundKey  
====MixColumns, ShiftRows, SubBytes

+++++  
Faqat blokli simmetrik shifrlash algoritmlari nomi keltirilgan qatorni ko'rsating?

=====#AES, DES  
=====A5/1, RC4  
=====A5/1, MD5  
=====SHA1, RC4

+++++

Vernam shifrlash algoritmidagi shifr matn  $C=101$  ga, kalit  $K=111$  ga teng bo'lsa shifr matn qiymati qanday bo'ladi?

=====#010  
=====101  
=====111  
=====110

+++++

Quyidagi ifoda nechta yechimga ega?  $3 \cdot x = 2 \pmod{7}$ .

=====#bitta yechimga ega  
=====ikkita yechimga ega  
=====yechimga ega emas  
=====uchta yechimga ega

+++++

$143 \pmod{17}$  nechiga teng?

=====#7  
=====6  
=====5  
=====8

+++++

Blokli shifrlash rejimlari qaysi algoritmlarda qo'llaniladi?

=====#AES, DES  
=====Sezar, Affin  
=====MD5, SHA1  
=====A5/1, RC4

+++++

MD5 xesh algoritmidagi nechta 32 bitli statik qiymatdan foydalanadi?

=====#4  
=====8  
=====12  
=====16

+++++

Sezar shifrlash algoritmidagi ochiq matn  $M=3$  ga, kalit  $K=7$  ga teng hamda  $p=26$  ga teng bo'sa shifr matn qiymati neciga teng bo'ladi?

=====#10  
====16  
====18  
====22

+++++

Qaysi xesh algoritmda 64 raund amal bajariladi?

=====#MD5  
====MAC  
====CRC  
====SHA1

+++++

DES shifrlash standarti qaysi davlat standarti?

=====#AQSH  
====Rossiya  
====Buyuk Britaniya  
====Germaniya

+++++

Qaysi blokli shifrlash algoritmda raund kalit uzunligi qiymatiga bo'g'liq?

=====#AES  
====IDEA  
====DES  
====RSA

+++++

A5/1 oqimli shifrlash algoritmda  $x_{18}=1$ ,  $y_{21}=0$ ,  $z_{22}=1$  ga teng bo'lsa kalitni qiymatini toping

=====#0  
====1  
====2  
====3

+++++

Kolliziya hodisasi deb nimaga aytiladi?

=====#ikki xil matn uchun bir xil xesh qiymat chiqishi  
====ikki xil matn uchun ikki xil xesh qiymat chiqishi  
====bir xil matn uchun ikki xil xesh qiymat chiqishi  
====bir xil matn uchun bir xil xesh qiymat chiqishi bir xil matn uchun bir xil xesh qiymat chiqishi

+++++

3 sonini 5 chekli maydonda teskarisini toping?

=====#2

====3  
====4  
====5

+++++

Bir qiymatli shifrlash qanday amalga oshiriladi?

====#ochiq ma'lumot alfaviti belgilarining har biriga shifr ma'lumot alfavitining bitta belgisi mos qo'yiladi  
====ochiq ma'lumot alfaviti belgilarining har biriga shifr ma'lumot alfavitining ikkita yoki undan ortiq chekli sondagi belgilari mos qo'yiladi  
====ochiq ma'lumot alfaviti belgilarining har ikkitasiga shifr ma'lumot alfavitining ikkita yoki undan ortiq chekli sondagi belgilari mos qo'yiladi  
====ochiq ma'lumot alfaviti belgilarining har juftiga shifr ma'lumot alfavitining bitta belgisi mos qo'yiladi

+++++

DES shifrlash algoritmida raundlar soni nechta?

====#16  
====64  
====32  
====128

+++++

DES shifrlash algoritmida kalit uzunligi necha bitga teng?

====#56  
====256  
====192  
====512

+++++

RC4 oqimli shifrlash algoritmi asosan qayerda qo'llaniladi?

====#simsiz aloqa vositalaridagi mavjud WEP protokolida  
====radioaloqa tarmoqlarda  
====internet trafiklarini shifrlashda  
====mobil aloqa standarti GSM protokolida

+++++

Xesh funksiyalarga qanday turlarga bo'linadi?

====#kalitli va kalitsiz xesh funksiyalarga  
====kalitli va kriptografik bo'lmagan xesh funksiyalarga  
====kalitsiz va kriptografik bo'lmagan xesh funksiyalarga  
====kriptografik va kriptografik bo'lmagan xesh funksiyalarga

+++++

AES shifrlash algoritmida raundlar soni nechaga teng bo'ladi?

====#10, 12, 14



====14, 16, 18  
====18, 20, 22  
====22, 24, 26

+++++

A5/1 oqimli shifrlash algoritmda har bir qadamda kalit oqimining qanday qiymatini hosil qiladi?

====#bir biti  
====bir bayti  
====64 biti  
====8 bayti

+++++

CRC-4 tizimida CRC qiymatini hisoblash jarayonida ma'lumotga nechta nol biriktiriladi?

====#4  
====8  
====16  
====12

+++++

Blokli simmetrik shifrlash algoritmlari raund funksiyalarida qanday amallar bajariladi?

====#ARX  
====PRX  
====XOR  
====RPT

+++++

CRC-6 tizimida CRC qiymati hisoblash jarayonida ma'lumotga nechta nol biriktiriladi?

====#6  
====12  
====18  
====24

+++++

Qaysi maxfiylikni ta'minlash usulida kalitdan foydalanilmaydi?

====#kodlash  
====shifrlash  
====autentifikatsiya  
====steganografiya

+++++

Vernam shifrlash algoritmi asosi qaysi mantiqiy hisoblashga asoslangan

====#XOR  
====ARX  
====ROX

=====XRA

+++++

Chastotalar tahlili kriptotahlil usuli samarali ishlidigan algorimtlar keltirilgan qatorni belgilang?

=====#Sezar, Affin

=====Vernam

=====Vijiner

=====RC4

+++++

Bitlar kesimida shifrlashni amalga oshiradigan algoritm keltirilgan qatorni ko'rsating?

=====#A5/1

=====SHA1

=====RC4

=====MD5

+++++

Ma'lumotni konfidensialligini ta'minlash uchun ..... zarur.

=====#shifrlash

=====kodlash

=====rasshifrovkalash

=====deshifrlash

+++++

Foydanaluvchanlikni ta'minlash bu-?

=====#ruxsat etilmagan "bajarishdan" himoyalash

=====ruxsat etilmagan "yozishdan" himoyalash

=====ruxsat etilmagan "o'qishdan" himoyalash

=====ruxsat berilgan "amallarni" bajarish

+++++

Vijiner shifrlash algoritmi qaysi turdagi akslantirishga asoslanadi?

=====#o'rniga qo'yish

=====o'rin almashtirish

=====kompozitsion

=====aralash

+++++

Kompyuter davriga tegishli shifrlarni aniqlang?

=====#DES, AES shifri

=====kodlar kitobi

=====Sezar

=====Enigma shifri

+++++

.... shifrlar blokli va oqimli turlarga ajratiladi

=====#simmetrik  
=====#ochiq **kalitli**  
=====#klassik  
=====#assimetrik

+++++

DES shifrlash algoritmi bu?

=====#blokli shifrlash algoritmi  
=====#oqimli shifrlash algoritmi  
=====#ochiq **kalitli shifrlash algoritmi**  
=====#asimetrik shifrlash algoritmi

+++++

Ma'lumotga elektron raqamli imzo qo'yish hamda uni tekshirish qanday amalga oshiriladi?

=====#Ma'lumotga raqamli imzo qo'yish maxfiy kalit orqali, imzoni tekshirish ochiq kalit orqali amalga oshiriladi  
=====#Ma'lumotga raqamli imzo qo'yish ochiq kalit orqali, imzoni tekshirish maxfiy kalit orqali amalga oshiriladi  
=====#Ma'lumotga raqamli imzo qo'yish maxfiy kalit orqali, imzoni tekshirish yopiq kalit orqali amalga oshiriladi  
=====#Ma'lumotga raqamli imzo qo'yish hamda uni tekshirish maxfiy kalit orqali amalga oshiriladi

+++++

A5/1 oqimli shifrlash algoritmidagi Z registr uzunligi nechti bitga teng?

=====#23  
=====#18  
=====#19  
=====#20

+++++

Kerkxofs printsipi bo'yicha qanday taxminlar ilgari suriladi?

=====#Kalitdan boshqa barcha ma'lumotlar barchaga ma'lum  
=====#Faqat kalit barchaga ma'lum  
=====#Barcha parametrlar barchaga ma'lum  
=====#Shifrlash kaliti barchaga ma'lum

+++++

Qaysi algoritm har bir qadamda bir bayt qiymatni shifrlaydi?

=====#RC4  
=====#A5/1  
=====#RSA  
=====#AES

+++++

A5/1 oqimli shifrlash algoritmidagi maxfiy kalit nechta registrga bo'linadi?

=====#3  
=====#6

=====5  
=====4

+++++

AES algoritmi qaysi tarmoq asosida qurilgan?

=====#SP  
=====Feystel  
=====Petri va SP  
=====Petri

+++++

Elektron raqamli imzo bo'yicha birinchi O'z DSt 1092 qaysi korxona tomonidan ishlab chiqilgan?

=====#UNICON.UZ  
=====INFOCOM  
=====UZTELECOM  
=====O'zR axborot texnologiyalari va kommunikatsiyalarini rivojlantirish vazirligi

+++++

AES shifrlash algoritmi nomini kengaytmasini ko'rsating?

=====#Advanced Encryption Standard  
=====Advanced Encoding Standard  
=====Advanced Encryption Stadium  
=====Always Encryption Standard

+++++

A5/1 shifrlash algoritmi bu?

=====#oqimli shifrlash algoritmi  
=====blokli shifrlash algoritmi  
=====assimetrik shifrlash algoritmi  
=====ochiq kalitli shifrlash algoritmi

+++++

RC4 shifrlash algoritmi qaysi turga mansub?

=====#oqimli shifrlar  
=====blokli shifrlar  
=====ochiq kalitli shifrlar  
=====assimetrik shifrlar

+++++

Xeshlash algoritmlarini ko'rsating?

=====#SHA1, MD5, O'z DSt 1106  
=====RSA, DSA, El-gamal  
=====DES, AES, Blovfish

====O‘z DSt 1105, FOCT 28147-89, FEAL

+++++

AES shifrlash algoritmi bu?

====#blokli shifrlash algoritmi

====oqimli shifrlash algoritmi

====ochiq kalitli shifrlash algoritmi

====asimetrik shifrlash algoritmi

+++++

ARX amali qaysi shifrlash algoritmlarida foydalaniladi?

====#Blokli shifrlashda

====Ikki kalitli shifrlashda

====Assimetrik shifrlashda

====Ochiq kalitli shifrlashda

+++++

Kriptotizimlar kalitlar soni bo‘yicha nechta turga bo‘linadi?

====#2

====3

====4

====5

+++++

A5/1 oqimli shifrlash algoritmidagi major qiymati hisoblash jarayonida, uchinchi (Z) registrning qaysi qiymati olinadi?

====#z10

====z11

====z12

====z13

+++++

A5/1 oqimli shifrlash algoritmidagi X registr uzunligi nechti bitga teng?

====#19

====16

====17

====15

+++++

Qaysi algoritmda har bir qadamda bir bit qiymatni shifrlaydi?

====#A5/1

====RC4

====RSA

====AES

+++++

Mantiqiy XOR amalining asosi qanday hisoblashga asoslangan?

=====#mod2 bo'yicha qo'shishga

====mod2 bo'yicha ko'paytirishga

====mod2 bo'yicha darajaga ko'tarishga

====mod2 bo'yicha bo'lishga

+++++

Qaysi xesh algoritmda xesh qiymat 128 bitga teng bo'ladi?

=====#MD5

====SHA1

====CRC

====MAC

+++++

Qaysi xesh algoritmda xesh qiymat 160 bitga teng bo'ladi?

=====#SHA1

====MD5

====CRC

====MAC

+++++

Faqat AQSH davlatiga tegishli kriptografik standartlar nomini ko'rsating?

=====#AES, DES

====AES, FOCT 28147-89

====DES, O'z DST 1105-2009

====SHA1, FOCT 3412-94

+++++

RC4 shifrlash algoritmi simmetrik turga mansub bo'lsa, unda nechta kalitdan foydalaniladi?

=====#1

====2

====3

====4

+++++

A5/1 oqimli shifrlash algoritmda major qiymati hisoblash jarayonida, birinchi (X) registrning qaysi qiymati olinadi?

=====#x8

====x9

====x10

====x11

+++++

DES shifrlash algoritmda S-bloklarga kiruvchi qiymatlar uzunligi necha bitga teng bo'ladi?

=====#6  
====12  
====24  
====18

+++++

MD5 xesh funksiyasida initsializatsiya bosqichida 4 ta necha bitli registrlardan foydalanadi?

=====#32  
====64  
====128  
====256

+++++

Imitatsiya turidagi hujumlarda ma'lumotlar qanday o'zgaradi?

=====#ma'lumot qalbakilashtiriladi  
====ma'lumot yo'q **qilinadi**  
====ma'lumot ko'chirib olinadi  
====ma'lumot dublikat qilinadi

+++++

Sezar shifrlash algoritmidan rasshifrovkalash formulasi qanday?

=====# $M = (C - K) \bmod p$   
==== $M = (C + K) \bmod p$   
==== $M = (C * K) \bmod p$   
==== $M = (C / K) \bmod p$

+++++

Faqat xesh funksiyalar nomi keltirilgan qatorni ko'rsating?

=====#SHA1, MD5  
====SHA1, DES  
====MD5, AES  
====HMAC, A5/1

+++++

MD5 xesh funksiyasida chiquvchi qiymat uzunligi nechaga teng?

=====#128  
====Ixtiyoriy  
====510  
====65

+++++

AES shifrlash algoritmi simmetrik turga mansub bo'lsa, unda nechta kalitdan foydalaniladi?

=====#1  
====2  
====3

=====4

+++++

SHA1 xesh funksiyasida initsializatsiya bosqichida nechta registrdan foydalanadi?

=====#5

=====10

=====15

=====20

+++++

MD5 xesh funksiyasida amallar nechta raund davomida bajariladi?

=====#64

=====128

=====512

=====256

+++++

DES shifrlash algoritmidan S-bloklardan chiqqan qiymatlar uzunligi nechta bitga teng bo'ladi?

=====#4

=====8

=====12

=====16

+++++

MD5 xesh funksiyasida initsializatsiya bosqichida nechta 32 bitli registrdan foydalanadi?

=====#4

=====8

=====12

=====16

+++++

Faqat oqimli simmetrik shifrlash algoritmlari nomi keltirilgan qatorni ko'rsating?

=====#A5/1, RC4

=====AES, DES

=====SHA1, RC4

=====A5/1, MD5

+++++

SHA1 xesh funksiyasida chiquvchi qiymat uzunligi nechaga teng?

=====#160

=====Ixtiyoriy

=====512

=====256



+++++

O'zgartirish turidagi hujumlarda ma'lumotlar qanday o'zgaradi?

=====#modifikatsiya qilinadi

=====#ma'lumot yo'q qilinadi

=====#ma'lumot dublikat qilinadi

=====#ma'lumot ko'chirib olinadi

+++++

AES standarti qaysi algoritm asoslangan?

=====#Rijndael

=====#RC6

=====#Twofish

=====#Serpent

+++++

SHA1 xesh funksiyasida amallar nechi raund davomida bajariladi?

=====#80

=====#128

=====#256

=====#512

+++++

2 lik sanoq tizimida 0101 soniga 1111 sonini 2 modul bo'yicha qo'shing?

=====#1010

=====#0101

=====#1001

=====#1111

+++++

AES shifrlash standarti qaysi davlat standarti?

=====#AQSH

=====#Rossiya

=====#Buyuk Britaniya

=====#Germaniya

+++++

Qaysi algoritmda maj kattaligi ishlatiladi?

=====#A5/1

=====#RC4

=====#SHA1

=====#MD5

+++++

Qalbakilashtirish hujumi qaysi turdagi hujum turiga kiradi?

=====#Immitatsiya  
=====#o'zgartirish  
=====#Fabrication  
=====#modification

+++++  
SHA1 xesh funksiyasi qaysi davlat standarti?

=====#AQSH  
=====#Rossiya  
=====#Germaniya  
=====#Buyuk Britaniya

+++++  
Qayday akslantirishdan foydalanilsa chastotalar tahlili kriptotahlil usuliga bardoshli bo'ladi

=====#bigram akslantirishidan  
=====#o'rniga qo'yish akslantirishidan  
=====#o'rin almashtirish akslantirishidan  
=====#xech qanday akslantirishdan foydalanish shart emas

+++++  
SHA1 xesh algoritmda nechta 32 bitli statik qiymatdan foydalanadi?

=====#5  
=====#10  
=====#15  
=====#20

+++++  
A5/1 oqimli shifrlash algoritmda maj(1,0,1) ga teng bo'lsa maj kattalik qiymatini toping?

=====#1  
=====#0  
=====#2  
=====#3

+++++  
SHA1 xesh funksiyada 102 bitli ma'lumot berilganda to'ldirish bitlari qanday to'ldiriladi?

=====#bir bit 1, 345 ta 0, ma'lumot uzunligi qiymatining 64 bitli qiymati bilan  
=====#bir bit 1, 345 ta 0, ma'lumot uzunligining dastlabki 64 bitli qiymati bilan  
=====#bir bit 1, 409 ta 0, ma'lumot uzunligi qiymatining 64 bitli qiymati bilan  
=====#bir bit 1, 409 ta 0, ma'lumot uzunligining dastlabki 64 bitli qiymati bilan

+++++  
Qaysi blokli shifrlash algoritmda 8 ta statik S-box lardan foydalaniladi?

=====#DES

====RSA  
====RC4  
====A5/1

+++++

Kriptotizimlar kalitlar soni bo'yicha qanday turga bo'linadi?

====#simmetrik va assimetrik turlarga  
====assimetrik va 2 kalitli turlarga  
====3 kalitli turlarga  
====simmetrik va bir kalitli turlarga

+++++

Ko'p qiymatli shifrlash qanday amalga oshiriladi?

====#ochiq ma'lumot alfaviti belgilarining har biriga shifr ma'lumot alfavitining ikkita yoki undan ortiq chekli sondagi belgilari mos qo'yiladi  
====ochiq ma'lumot alfaviti belgilarining har ikkitasiga shifr ma'lumot alfavitining ikkita yoki undan ortiq chekli sondagi belgilari mos qo'yiladi  
====ochiq ma'lumot alfaviti belgilarining har biriga shifr ma'lumot alfavitining bitta belgisi mos qo'yiladi  
====ochiq ma'lumot alfaviti belgilarining har juftiga shifr ma'lumot alfavitining bitta belgisi mos qo'yiladi

+++++

A5/1 oqimli shifrlash algoritmi asosan qayerda qo'llaniladi?

====#mobil aloqa standarti GSM protokolida  
====simsiz aloqa vositalaridagi mavjud WEP protokolida  
====internet trafiklarini shifrlashda  
====radioaloqa tarmoqlarida

+++++

Assimetrik kriptotizimlarda necha kalitdan foydalaniladi?

====#2 ta  
====3 ta  
====4 ta  
====kalit ishlatilmaydi

+++++

AES algoritmda shifrlash kalitining uzunligi necha bitga teng?

====#128, 192, 256 bit  
====128, 156, 256 bit  
====256, 512 bit  
====128, 192 bit

+++++

Kalit bardoshliligi bu -?

====#eng yaxshi ma'lum algoritm bilan kalitni topish murakkabligidir

====eng yaxshi ma'lum algoritm yordamida yolg'on axborotni ro'kach qilishdir  
====amaliy bardoshlilik  
====nazariy bardoshlilik

+++++

RC4 oqimli shifrlash algoritmda har bir qadamda kalit oqimining qanday qiymatini hosil qiladi?

====#bir baytini  
====bir bitini  
====64 bitini  
====8 baytini

+++++

AES algoritmda nechta akslantirishlardan foydalaniladi?

====#4  
====2  
====5  
====6

+++++

Qanday funksiyalarga xesh funksiya deyiladi?

====#ixtiyoriy uzunlikdagi ma'lumotni biror fiksirlangan uzunlikga o'tkazuvchi funksiyaga aytiladi  
====ma'lumot baytlarini boshqa qiymatlarga almashtiruvchi funksiyaga aytiladi  
====ma'lumot bitlarini boshqa qiymatlarga almashtiruvchi funksiyaga aytiladi  
====ixtiyoriy uzunlikdagi ma'lumotni bit yoki baytlarini zichlashtirib beruvchi funksiyaga aytiladi

+++++

Xesh funksiyalar qanday maqsadlarda ishlatiladi?

====#ma'lumotni to'liqligini nazoratlash va ma'lumot manbaini autentifikatsiyalashda  
====ma'lumot manbaini autentifikatsiyalashda  
====ma'lumotni butunligini nazoratlashda  
====ma'lumotni maxfiylikini nazoratlash va ma'lumot manbaini haqiqiylikini tekshirishda

+++++

Ma'lumotni sakkizlik sanoq tizimidan o'n oltilik sanoq tizimiga o'tkazish bu?

====#kodlash  
====rasshifrovkalash  
====yashirish  
====shifrlash

+++++

A5/1 shifri qaysi turga mansub?

====#oqimli shifrlar  
====blokli shifrlar  
====ochiq kalitli shifrlar

=====assimetrik shifrlar

+++++

Qaysi algoritmlar simmetrik blokli shifrlarga tegishli?

=====#AES, DES

=====A5/1, AES

=====Vijiner, DES

=====Sezar, AES

+++++

Ma'lumotni mavjudligini yashirishni maqsad qilgan bilim sohasi bu?

=====#steganografiya

=====kriptografiya

=====kodlash

=====kriptotahlil

+++++

Faqat simmetrik blokli shifrlarga xos bo'lgan atamani aniqlang?

=====#blok uzunligi

=====kalit uzunligi

=====ochiq kalit

=====kodlash jadvali

+++++

Quyidagi ta'rif qaysi atamaga tegishli: "maxfiy kodlarni"ni buzish bilan shug'ullanadigan soha-bu?

=====#kriptotahlil

=====kripto

=====kriptologiya

=====kriptografiya

+++++

Qadimiy davr klassik shifriga quyidagilarning qaysi biri tegishli?

=====#Sezar

=====kodlar kitobi

=====Enigma shifri

=====DES, AES shifri

+++++

Quyidagi ta'rif qaysi kriptotizimga tegishli: ochiq matnni shifrlashda hamda rasshifrovkalashda mos holda ochiq va maxfiy kalitdan foydalanadi?

=====#ochiq kalitli kriptotizimlar

=====maxfiy kalitli kriptotizimlar

=====simmetrik kriptotizimlar

====elektron raqamli imzo tizimlari

+++++

Simmetrik shifrlar axborotni qaysi xususiyatlarini ta'minlashda foydalaniladi?

====#konfidensiallik va yaxlitlik

====konfidensiallik va foydalanuvchanlik

====foydalanuvchanlik va yaxlitlik

====foydalanuvchanlik

+++++

Qanday algoritmlar qaytmas xususiyatiga ega hisoblanadi?

====#xesh funksiyalar

====elektron raqamli imzo algoritmlari

====simmetrik kriptotizimlar

====ochiq kalitli kriptotizimlar

+++++

Ochiq matn qismlarini takror shifrlashga asoslangan usul bu?

====#blokli shifrlar

====oqimli shifrlar

====assimetrik shifrlar

====ochiq kalitli shifrlar

+++++

Ochiq kalitli shifrlashda deshifrlash qaysi kalit asosida amalga oshiriladi?

====#shaxsiy kalit

====ochiq kalit

====kalitdan foydalanilmaydi

====umumiy kalit

+++++

Quyidagi ta'rif qaysi atamaga tegishli: "maxfiy kodlarni"ni yaratish bilan shug'ullanadigan soha-bu?

====#kriptografiya

====kriptologiya

====kriptotahlil

====kripto

+++++

Simmetrik kriptotizimlarning asosiy kamchiligi bu?

====#kalitni taqsimlash zaruriyati

====kalitlarni esda saqlash murakkabligi

====shifrlash jarayonining ko'p vaqt olishi

====algoritmlarning xavfsiz emasligi

+++++

Kriptotizimni boshqaradigan vosita?

=====#kalit

=====algoritm

=====stegokalit

=====kriptotizim boshqarilmaydi

+++++

Quyidagi ta'rif qaysi kriptotizimga tegishli: ochiq matnni shifrlashda hamda rasshifrovkalashda bitta maxfiy kalitdan foydalaniladi?

=====#simmetrik kriptotizimlar

=====nosimmetrik kriptotizimlar

=====ochiq kalitli kriptotizimlar

=====assimetrik kriptotizimlar

+++++

Kerxgofs prinsipiga ko'ra kriptotizimning to'liq xavfsiz bo'lishi faqat qaysi kattalik nomalum bo'lishiga asoslanishi kerak?

=====#kalit

=====protokol

=====shifrmtn

=====Algoritm

+++++

Xesh funksiyalar nima maqsadda foydalaniladi?

=====#ma'lumotlar yaxlitligini ta'minlashda

=====ma'lumot egasini autentifikatsiyalashda

=====ma'lumot maxfiyligini ta'minlashda

=====ma'lumot manbaini autentifikatsiyalashda

+++++

Chastotalar tahlili hujumi qanday amalga oshiriladi?

=====#shifr matnda qatnashgan harflar sonini aniqlash orqali

=====shifr matnda eng kam qatnashgan harflarni aniqlash orqali

=====ochiq matnda qatnashgan harflar sonini aniqlash orqali

=====ochiq matnda eng kam qatnashgan harflarni aniqlash orqali

+++++

Xesh funksiyaga tegishli bo'lgan talabni aniqlang?

=====#bir tomonlama funksiya bo'lishi

=====chiqishda ixtiyoriy uzunlikda bo'lishi

=====turli kirishlar bir xil chiqishlarni akslantirishi

=====kolliziyaga bardoshli bo'lmasligi

+++++

RC4 shifrlash algoritmi bu?

=====#oqimli shifrlash algoritmi

=====#ochiq kalitli shifrlash algoritmi

=====#blokli shifrlash algoritmi

=====#asimetrik shifrlash algoritmi

+++++

A5/1 shifrlash algoritmi simmetrik turga mansub bo'lsa, unda nechta kalitdan foydalaniladi?

=====#1

=====#2

=====#3

=====#4

+++++

Qaysi algoritmda, algoritmnining necha round bajarilishi ochiq matn uzunligiga bog'liq?

=====#A5/1

=====#MD5

=====#HMAC

=====#SHA1

+++++

Simmetrik va ochiq kalitli kriptotizimlar asosan nimasi bilan bir biridan farq qiladi?

=====#kalitlar soni bilan

=====#matematik murakkabligi bilan

=====#farq qilmaydi

=====#biri maxfiylikni ta'minlasa, biri butunlikni ta'minlaydi

+++++

A5/1 oqimli shifrlash algoritmidagi major qiymati hisoblash jarayonida, ikkinchi (Y) registrning qaysi qiymati olinadi?

=====#y10

=====#y11

=====#y12

=====#y13

+++++

Kalitli xesh funksiyalar qanday turdagi hujumlardan himoyalaydi?

=====#imitatsiya va o'zgartirish turidagi hujumlardan

=====#ma'lumotni oshkor qilish turidagi hujumlardan

=====#DDOS hujumlaridan

=====#foydalanishni buzishga qaratilgan hujumlardan

+++++

Sezar shifrlash algoritmidagi shifrlash formulasi qanday?



===== $C=(M+K) \bmod p$   
===== $C=(M-K) \bmod p$   
===== $C=(M*K) \bmod p$   
===== $C=(M/K) \bmod p$

+++++

A5/1 oqimli shifrlash algoritmda Y registr uzunligi nechi bitga teng?

=====#22  
=====20  
=====19  
=====21

+++++

Kalitli xesh funksiyalardan foydalanish nimani kafolatlaydi?

=====#fabrikatsiyani va modifikatsiyani oldini oladi  
=====ma'lumot yo'q qilinadi  
=====ma'lumot dublikat qilinadi  
=====ma'lumot ko'chirib olinadi

+++++

DES shifrlash algoritmi simmetrik turga mansub bo'lsa, unda nechta kalitdan foydalaniladi?

=====#1  
=====2  
=====3  
=====4

+++++

AES tanlovi g'olibi bo'lgan algoritm nomini ko'rsating?

=====Rijndael  
=====IDEA  
=====Blowfish  
=====Twofish

+++++

AES shifrlash algoritmda 128 bitli ma'lumot bloki qanday o'lchamdagi jadvalga solinadi?

=====#4x4  
=====4x6  
=====6x4  
=====6x6

+++++

A5/1 oqimli shifrlash algoritmda maj(1,0,1) ga teng bo'lsa qaysi registrlar suriladi?

=====#birinchi va uchunchi registrlar suriladi

====faqat ikkinchi registr suriladi  
====birinchi va ikkinchi registrlar suriladi  
====faqat birinchi resgistr suriladi

+++++

GSM tarmog'ida foydalaniluvchi shifrlash algoritmi nomini ko'rsating?

====#A5/1  
====DES  
====RC4  
====AES

+++++

HMAC tizimida kalit qiymati blok uzunligidan katta bo'lganda ma'lumotga qanday biriktiriladi?

====#kalitni xesh qiymati hisoblanib, unga blok uzunligiga teng bo'lguncha nol qiymat qo'shiladi va yangi hosil bo'lgan qiymat ma'lumotga biriktiriladi  
====kalit qiymati blok uzunligiga teng bo'lguncha nol qiymat bilan to'ldirilib hosil bo'lgan qiymat ma'lumotga biriktiriladi  
====kalit qiymati o'zgartirilmagan holda ma'lumotga biriktiriladi  
====xesh funksiyalarda kalit qiymatidan foydalanilmaydi

+++++

Qaysi xesh algoritmda 80 raund amal bajariladi?

====#SHA1  
====CRC  
====MD5  
====MAC

+++++

Affin shifrlash algoritmda  $a=2$ ,  $b=3$ ,  $p=26$  hamda ochiq matn  $x=4$  ga teng bo'lsa, shifr matn qiymatini toping?

====#11  
====27  
====41  
====31

+++++

MD5 xesh funksiyada 48 bitli ma'lumot berilganda to'ldirish bitlari qanday to'ldiriladi?

====#bir bit 1, 399 ta 0, ma'lumot uzunligi qiymatining 64 bitli qiymati bilan  
====bir bit 1, 399 ta 0, ma'lumot uzunligining dastlabki 64 bitli qiymati bilan  
====bir bit 1, 463 ta 0, ma'lumot uzunligi qiymatining 64 bitli qiymati bilan  
====bir bit 1, 463 ta 0, ma'lumot uzunligining dastlabki 64 bitli qiymati bilan

+++++

AES shifrlash algoritmda ochiq matn bilan dastlab qanday amal bajariladi?

====#ochiq matn dastlabki kalit bilan XOR amali bajariladi

====ochiq matn birinchi raund kalit bilan XOR amali bajariladi  
====ochiq matn ustida dastlab SubBytes akslantirishi amali bajariladi  
====ochiq matn ustida dastlab ShiftRows akslantirishi amali bajariladi

+++++

Vernam shifrlash algoritmda ochiq matn M=101 ga, kalit K=111 ga teng bo'lsa shifr matn qiymati qanday bo'ladi?

====#010  
====101  
====111  
====110

?Konfidensiallikni ta'minlash bu - ?

+ruxsatsiz o'qishdan himoyalash.  
-ruxsatsiz yozishdan himoyalash.  
-ruxsatsiz bajarishdan himoyalash.  
-ruxsat etilgan amallarni bajarish.

?Foydalanuvchanlikni ta'minlash bu - ?

+ruxsatsiz bajarishdan himoyalash.  
-ruxsatsiz yozishdan himoyalash.  
-ruxsatsiz o'qishdan himoyalash.  
-ruxsat etilgan amallarni bajarish.

?Yaxlitlikni ta'minlash bu - ?

+ruxsatsiz yozishdan himoyalash.  
-ruxsatsiz o'qishdan himoyalash.  
-ruxsatsiz bajarishdan himoyalash.  
-ruxsat etilgan amallarni bajarish.

?Jumlani to'ldiring. Hujumchi kabi fikrlash ... kerak.

+bo'lishi mumkin bo'lgan **xavfni oldini olish uchun**  
-kafolatlangan amallarni ta'minlash uchun  
-ma'lumot, axborot va tizimdan foydalanish uchun  
-ma'lumotni aniq va ishonchli ekanligini bilish uchun

?Jumlani to'ldiring. Tizimli fikrlash ... uchun kerak.

+kafolatlangan amallarni ta'minlash  
-bo'lishi mumkin bo'lgan xavfni oldini olish  
-ma'lumot, axborot va tizimdan foydalanish  
-ma'lumotni aniq va ishonchli ekanligini bilish

?Axborot xavfsizligida risk bu?

+Manbaga zarar keltiradigan ichki yoki tashqi zaiflik ta'sirida tahdid qilish ehtimoli.  
-U yoki bu faoliyat jarayonida nimaga erishishni xoxlashimiz.  
-Tashkilot uchun qadrlil bo'lgan ixtiyoriy narsa.  
-Tizim yoki tashkilotga zarar yetkazishi mumkin bo'lgan istalmagan hodisa.

?Axborot xavfsizligida tahdid bu?

- +Aktivga zarar yetkazishi mumkin bo'lgan istalmagan hodisa.
- Noaniqlikning maqsadlarga ta'siri.
- U yoki bu faoliyat jarayonida nimaga erishishni xohlashimiz.
- Tashkilot uchun qadrlı bo'lgan ixtiyoriy narsa.

?Axborot xavfsizligida aktiv bu?

- +Tashkilot yoki foydalanuvchi uchun qadrlı bo'lgan ixtiyoriy narsa.
- Tizim yoki tashkilotga zarar yetkazishi mumkin bo'lgan istalmagan hodisa.
- Noaniqlikning maqsadlarga ta'siri.
- U yoki bu faoliyat jarayonida nimaga erishishni xohlashimiz.

?Axborot xavfsizligida zaiflik bu?

- +Tahdidga sabab bo'luvchi tashkilot aktivi yoki boshqaruv tizimidagi nuqson.
- Tashkilot uchun qadrlı bo'lgan ixtiyoriy narsa.
- Tizim yoki tashkilotga zarar yetkazishi mumkin bo'lgan istalmagan hodisa.
- Noaniqlikning maqsadlarga ta'siri.

?Axborot xavfsizligida boshqarish vositasi bu?

- +Natijasi zaiflik yoki tahdidga ta'sir qiluvchi riskni o'zgartiradigan harakatlar.
- Bir yoki bir nechta tahdidga sabab bo'luvchi tashkilot aktivi yoki boshqaruv tizimidagi kamchilik.
- Tashkilot uchun qadrlı bo'lgan ixtiyoriy narsa.
- Tizim yoki tashkilotga zarar yetkazishi mumkin bo'lgan istalmagan hodisa.

?Har qanday vaziyatda biror bir hodisani yuzaga kelish ehtimoli qo'shilsa ....

- +risk paydo bo'ladi.
- hujum paydo bo'ladi.
- tahdid paydo bo'ladi.
- aktiv paydo bo'ladi.

?Jumlani to'ldiring. Denial of service (DOS) hujumi axborotni .... xususiyatini buzushga qaratilgan.

- +foydalanuvchanlik
- butunlik
- konfidensiallik
- ishonchlilik

?Jumlani to'ldiring. ... sohasi tashkil etuvchilar xavfsizligi, aloqa xavfsizligi va dasturiy ta'minotlar xavfsizligidan iborat.

- +Tizim xavfsizligi
- Ma'lumotlar xavfsizligi
- Inson xavfsizligi
- Tashkilot xavfsizligi

?Kriptologiya so'ziga berilgan to'g'ri tavsifni toping?

- +Maxfiy shifrlarni yaratish va buzish fani va sanati.
- Maxfiy shifrlarni yaratish fani va sanati.

- Maxfiy shifrlarni buzish fani va sanati.
- Axborotni himoyalash fani va sanati.

?.... kriptotizimni shifrlash va deshifrlash uchun sozlashda foydalaniladi.

- +Kriptografik kalit
- Ochiq matn
- Alifbo
- Algoritm

?Kriptografiya so ziga berilgan to g ri tavsifni toping?

- +Maxfiy shifrlarni yaratish fani va sanati.
- Maxfiy shifrlarni yaratish va buzish fani va sanati.
- Maxfiy shifrlarni buzish fani va sanati.
- Axborotni himoyalash fani va sanati.

?Kriptotahlil so ziga berilgan to g ri tavsifni toping?

- +Maxfiy shifrlarni buzish fani va sanati.
- Maxfiy shifrlarni yaratish fani va sanati.
- Maxfiy shifrlarni yaratish va buzish fani va sanati.
- Axborotni himoyalash fani va sanati.

?..... axborotni ifodalash uchun foydalaniladigan chekli sondagi belgilar to plami.

- +Alifbo
- Ochiq matn
- Shifrmtn
- Kodlash

?Ma lumot shifrlansa, natijasi .... bo ladi.

- +shifrmtn
- ochiq matn
- nomalum
- kod

?Deshifrlash uchun kalit va ..... kerak bo ladi.

- +shifrmtn
- ochiq matn
- kodlash
- alifbo

?Ma lumotni shifrlash va deshifrlashda yagona kalitdan foydalanuvchi tizim bu -

- +simmetrik kriptotizim.
- ochiq kalitli kriptotizim.
- asimetrik kriptotizim.
- xesh funksiyalar.

?Ikki kalitli kriptotizim bu -

- +ochiq kalitli kriptotizim.
- simmetrik kriptotizim.
- xesh funksiyalar.
- MAC tizimlari.

?Axborotni mavjudligini yashirish bilan shug'ullanuvchi fan sohasi bu -

- +steganografiya.
- kriptografiya.
- kodlash.
- kriptotahlil.

?Axborotni foydalanuvchiga qulay tarzda taqdim etish uchun ..... amalga oshiriladi.

- +kodlash
- shifrlash
- yashirish
- deshifrlash

?Jumlani to'ldiring. Ma'lumotni konfidentsialligini ta'minlash uchun ..... zarur.

- +shifrlash
- kodlash
- dekodlash
- deshifrlash

?Ma'lumotni mavjudligini yashirishda .....

- +steganografik algoritmdan foydalaniladi.
- kriptografik algoritmdan foydalaniladi.
- kodlash algoritmidan foydalaniladi.
- kriptotahlil algoritmidan foydalaniladi.

?Xesh funksiyalar - .... funksiya.

- +kalitsiz kriptografik
- bir kalitli kriptografik
- ikki kalitli kriptografik
- ko'p kalitli kriptografik

?Jumlani to'ldiring. Ma'lumotni uzatishda kriptografik himoya .....

- +konfidentsiallik va butunlikni ta'minlaydi.
- konfidentsiallik va foydalanuvchanlikni ta'minlaydi.
- foydalanuvchanlik va butunlikni ta'minlaydi.
- konfidentsiallik ta'minlaydi.

?Jumlani to'ldiring. ... kompyuter davriga tegishli shifrlarga misol bo'la oladi.

- +DES, AES shifri
- Sezar shifri
- Kodlar kitobi
- Enigma shifri

?.... kriptografik shifrlash algoritmlari blokli va oqimli turlarga ajratiladi.

- +Simmetrik
- Ochiq kalitli
- Asimmetrik
- Klassik davr

?Jumlani to'ldiring. .... shifrlar tasodifiy ketma-ketliklarni generatsiyalashga asoslanadi.

- +Oqimli
- Blokli
- Ochiq kalitli
- Asimmetrik

?Ochiq matn qismlarini takroriy shifrlovchi algoritmlar bu -

- +blokli shifrlar
- oqimli shifrlash
- ochiq kalitli shifrlar
- asimmetrik shifrlar

?A5/1 shifri bu -

- +oqimli shifr.
- blokli shifr.
- ochiq kalitli shifr.
- asimmetrik shifr

?Quyidagi muammolardan qaysi biri simmetrik kriptotizimlarga xos.

- +Kalitni taqsimlash zaruriyati.
- Shifrlash jarayonining ko'p vaqt olishi.
- Kalitlarni esda saqlash murakkabligi.
- Foydalanuvchilar tomonidan maqbul ko'rilmaligi.

?Quyidagi atamalardan qaysi biri faqat simmetrik blokli shifrlarga xos?

- +Blok uzunligi.
- Kalit uzunligi.
- Ochiq kalit.
- Kodlash jadvali.

?Jumlani to'ldiring. Sezar shifri .... akslantirishga asoslangan.

- +o'riniga qo'yish
- o'rin almashtirish
- ochiq kalitli
- kombinatsion

?Kriptotizimning to'liq xavfsiz bo'lishi Kerxgofs prinsipiga ko'ra qaysi kattalikning nomalum bo'lishiga asoslanadi?

- +Kalit.
- Algoritm.

- Shifratn.
- Protokol.

?Shifrlash va deshifrlashda turli kalitlardan foydalanuvchi shifrlar bu -

- +ochiq kalitli shifrlar.
- simmetrik shifrlar.
- bir kalitli shifrlar
- xesh funksiyalar.

?Agar simmetrik kalitning uzunligi 64 bit bo'lsa, jami bo'lishi mumkin bo'lgan kalitlar soni nechta?

- +264
- 64!
- 642
- 263

?Axborotni qaysi xususiyatlari simmetrik shifrlar yordamida ta'minlanadi.

- +Konfidentsiallik va butunlik.
- Konfidentsiallik.
- Butunlik va foydalanuvchanlik.
- Foydalanuvchanlik va konfidentsiallik.

?Axborotni qaysi xususiyatlari ochiq kalitli shifrlar yordamida ta'minlanadi.

- +Konfidentsiallik.
- Konfidentsiallik, butunlik va foydalanuvchanlik.
- Butunlik va foydalanuvchanlik.
- Foydalanuvchanlik va konfidentsiallik.

?Elektron raqamli imzo tizimi.

- +MAC tizimlari.
- Simmetrik shifrlash tizimlari.
- Xesh funksiyalar.
- Butunlik va foydalanuvchanlik.

?Qaysi ochiq kalitli algoritim katta sonni faktorlash muammosiga asoslanadi?

- +RSA algoritmi.
- El-Gamal algoritmi.
- DES.
- TEA.

?Rad etishdan himoyalashda ochiq kalitli kriptotizimlarning qaysi xususiyati muhim hisoblanadi.

- +Ikkita kalitdan foydalanilgani.
- Matematik muammoga asoslanilgani.
- Ochiq kalitni saqlash zaruriyati mavjud emasligi.
- Shaxsiy kalitni saqlash zarurligi.

?Quyidagi talablardan qaysi biri xesh funksiyaga tegishli emas.



- +Bir tomonlama funktsiya bo'lmashi kerak.
- Amalga oshirishdagi yuqori tezlik.
- Turli kirishlar turli chiqishlarni akslantirishi.
- Kolliziyaga bardoshli bo'lishi.

?Quyidagi xususiyatlardan qaysi biri elektron raqamli imzo tomonidan ta'minlanadi?

- +Axborot butunligini va rad etishdan himoyalash.
- Axborot konfidentsialligini va rad etishdan himoyalash.
- Axborot konfidentsialligi.
- Axborot butunligi.

?Faqat ma'lumotni butunligini ta'minlovchi kriptotizimlarni ko'rsating.

- +MAC (Xabarlarini autentifikatsiya kodlari) tizimlari.
- Elektron raqamli imzo tizimlari.
- Ochiq kalitli kriptografik tizimlar.
- Barcha javoblar to'g'ri.

?Foydalanuvchini tizimga tanitish jarayoni bu?

- +Identifikatsiya.
- Autentifikatsiya.
- Avtorizatsiya.
- Ro'yxatga olish.

?Foydalanuvchini haqiqiylikni tekshirish jarayoni bu?

- +Autentifikatsiya.
- Identifikatsiya.
- Avtorizatsiya.
- Ro'yxatga olish.

?Tizim tomonidan foydalanuvchilarga imtiyozlar berish jarayoni bu?

- +Avtorizatsiya.
- Autentifikatsiya.
- Identifikatsiya.
- Ro'yxatga olish.

?Parolga asoslangan autentifikatsiya usulining asosiy kamchiligini ko'rsating?

- +Esda saqlash zaruriyati.
- Birga olib yurish zaruriyati.
- Almashtirib bo'lmashlik.
- Qalbakilashtirish mumkinligi.

?Biron narsani bilishga asoslangan autentifikatsiya deyilganda quyidagilardan qaysilar tushuniladi.

- +PIN, Parol.
- Token, mashinaning kaliti.
- Yuz tasviri, barmoq izi.
- Biometrik parametrlar.

?Tokenga asoslangan autentifikatsiya usulining asosiy kamchiligini ayting?

- +Doimo xavfsiz saqlab olib yurish zaruriyati.
- Doimo esada saqlash zaruriyati.
- Qalbakilashtirish muammosi mavjudligi.
- Almashtirib bo'lmazlik.

?Esda saqlashni va olib yurishni talab etmaydigan autentifikatsiya usuli bu -

- +biometrik autentifikatsiya.
- parolga asoslangan autentifikatsiya.
- tokenga asoslangan autentifikatsiya.
- ko p faktorli autentifikatsiya.

?Qaysi biometrik parametr eng yuqori universallik xususiyatiga ega?

- +Yuz tasviri.
- Ko'z qorachig'i.
- Barmoq izi.
- Qo'l shakli.

?Qaysi biometrik parametr eng yuqori takrorlanmazlik xususiyatiga ega?

- +Ko'z qorachig'i.
- Yuz tasviri.
- Barmoq izi.
- Qo'l shakli.

?Quyidagilardan qaysi biri har ikkala tomonning haqiqiyligini tekshirish jarayonini ifodalaydi?

- +Ikki tomonlama autentifikatsiya.
- Ikki faktorli autentifikatsiya.
- Ko'p faktorli autentifikatsiya.
- Biometrik autentifikatsiya.

?Parolga asoslangan autentifikatsiya usuliga qaratilgan hujumlarni ko'rsating?

- +Parollar lug'atidan foydalanish asosida hujum, yelka orqali qarash hujumi, zararli dasturlardan foydalanish asosida hujum.
- Fizik o'g'irlash hujumi, yelka orqali qarash hujumi, zararli dasturlardan foydalanish asosida hujum.
- Parollar lug'atidan foydalanish asosida hujum, yelka orqali qarash hujumi, qalbakilashtirish hujumi.
- Parollar lug'atidan foydalanish asosida hujum, bazadagi parametrlarni almashtirish hujumi, zararli dasturlardan foydalanish asosida hujum.

?Tokenga asoslangan autentifikatsiya usuliga qaratilgan hujumlarni ko'rsating?

- +Fizik o'g'irlash, mobil qurilmalarda zararli dasturlardan foydalanishga asoslangan hujumlar
- Parollar lug'atidan foydalanish asosida hujum, yelka orqali qarash hujumi, zararli dasturlardan foydalanish asosida hujum
- Fizik o'g'irlash, yelka orqali qarash hujumi, zararli dasturlardan foydalanishga asoslangan hujumlar
- Parollar lug'atidan foydalanish asosida hujum, bazadagi parametrlarni almashtirish hujumi, zararli dasturlardan foydalanish asosida hujum

?Foydalanuvchi parollari bazada qanday ko'rinishda saqlanadi?

- +Xeshlangan ko rinishda.
- Shifrlangan ko rinishda.
- Ochiq holatda.
- Bazada saqlanmaydi.

?Agar parolning uzunligi 8 ta belgi va har bir o rinda 128 ta turlicha belgidan foydalanish mumkin bo lsa, bo lishi mumkin bo lgan jami parollar sonini toping.

- +1288
- 8128
- 128!
- 2128

?Parolni "salt" (tuz) kattaligidan foydalanib xeshlashdan (h(password, salt)) asosiy maqsad nima?

- +Buzg unchiga ortiqcha hisoblashni talab etuvchi murakkablikni yaratish.
- Buzg unchi topa olmasligi uchun yangi nomalum kiritish.
- Xesh qiymatni tasodifiylik darajasini oshirish.
- Xesh qiymatni qaytmaslik talabini oshirish.

?Quyidagilardan qaysi biri tabiiy tahdidga misol bo ladi?

- +Yong in, suv toshishi, harorat ortishi.
- Yong in, o g irlik, qisqa tutashuvlar.
- Suv toshishi, namlikni ortib ketishi, bosqinchilik.
- Bosqinchilik, terrorizm, o g irlik.

?Qaysi nazorat usuli axborotni fizik himoyalashda inson faktorini mujassamlashtirgan?

- +Ma muriy nazoratlash.
- Fizik nazoratlash.
- Texnik nazoratlash.
- Apparat nazoratlash.

?Faqat ob ektning egasi tomonidan foydalanishga mos bo lgan mantiqiy foydalanish usulini ko rsating?

- +Diskretion foydalanishni boshqarish.
- Mandatli foydalanishni boshqarish.
- Rolga asoslangan foydalanishni boshqarish.
- Attributga asoslangan foydalanishni boshqarish.

?Qaysi usul ob ektlar va sub ektlarni klassifikatsiyalashga asoslangan?

- +Mandatli foydalanishni boshqarish.
- Diskretion foydalanishni boshqarish.
- Rolga asoslangan foydalanishni boshqarish.
- Attributga asoslangan foydalanishni boshqarish.

?Biror faoliyat turi bilan bog liq harakatlar va majburiyatlar to plami bu?

- +Rol.
- Imtiyoz.
- Daraja.
- Imkoniyat.

?Qoida, siyosat, qoida va siyosatni mujassamlashtirgan algoritmlar, majburiyatlar va maslahatlar kabi tushunchalar qaysi foydalanishni boshqarish usuliga aloqador.

- +Attributga asoslangan foydalanishni boshqarish.
- Rolga asoslangan foydalanishni boshqarish.
- Mandatli foydalanishni boshqarish.
- Diskretion foydalanishni boshqarish.

?Bell-Lapadula modeli axborotni qaysi xususiyatini ta minlashni maqsad qiladi?

- +Konfidensiallik.
- Butunlik.
- Foydalanuvchanlik.
- Ishonchlilik.

?Biba modeli axborotni qaysi xususiyatini ta minlashni maqsad qiladi?

- +Butunlik.
- Konfidensiallik.
- Foydalanuvchanlik.
- Maxfiylik.

?Qaysi turdagi shifrlash vositasida barcha kriptografik parametrlar kompyuterning ishtirokisiz generatsiya qilinadi?

- +Apparat.
- Dasturiy.
- Simmetrik.
- Ochiq kalitli.

?Qaysi turdagi shifrlash vositasida shifrlash jarayonida boshqa dasturlar kabi kompyuter resursidan foydalanadi?

- +Dasturiy.
- Apparat.
- Simmetrik.
- Ochiq kalitli.

?Yaratishda biror matematik muammoga asoslanuvchi shifrlash algoritmini ko rsating?

- +Ochiq kalitli shifrlar.
- Simmetrik shifrlar.
- Blokli shifrlar.
- Oqimli shifrlar.

?Xesh funksiyalarda kolliziya hodisasi bu?

- +Ikki turli matnlarning xesh qiymatlarini bir xil bo lishi.
- Cheksiz uzunlikdagi axborotni xeshlay olishi.
- Tezkorlikda xeshlash imkoniyati.
- Turli matnlar uchun turli xesh qiymatlarni hosil bo lishi.

?64 ta belgidan iborat Sezar shifrlash usulida kalitni bilmasdan turib nechta urinishda ochiq matnni aniqlash mumkin?

- +63
- 63!

-32  
-322

?Elektron raqamli imzo muolajalarini ko rsating?

- +Imzoni shakllantirish va imkoni tekshirish.
- Shifrlash va deshifrlash.
- Imzoni xeshlash va xesh matnni deshifrlash.
- Imzoni shakllartirish va xeshlash.

? "Yelka orqali qarash" hujumi qaysi turdagi autentifikatsiya usuliga qaratilgan.

- +Parolga asoslangan autentifikatsiya.
- Tokenga asoslangan autentifikatsiya.
- Biometrik autentifikatsiya.
- Ko z qorachig iga asoslangan autentifikatsiya.

?Sotsial injineriyaga asoslangan hujumlar qaysi turdagi autentifikatsiya usuliga qaratilgan.

- +Parolga asoslangan autentifikatsiya.
- Tokenga asoslangan autentifikatsiya.
- Biometrik autentifikatsiya.
- Ko z qorachig iga asoslangan autentifikatsiya.

?Yo qolgan holatda almashtirish qaysi turdagi autentifikatsiya usuli uchun eng arzon.

- +Parolga asoslangan autentifikatsiya.
- Tokenga asoslangan autentifikatsiya.
- Biometrik autentifikatsiya.
- Ko z qorachig iga asoslangan autentifikatsiya.

?Qalbakilashtirish hujumi qaysi turdagi autentifikatsiya usuliga qaratilgan.

- +Biometrik autentifikatsiya.
- Biror narsani bilishga asoslangan autentifikatsiya.
- Biror narsaga egalik qilishga asoslangan autentifikatsiya.
- Tokenga asoslangan autentifikatsiya

?Axborotni butunligini ta minlash usullarini ko rsating.

- +Xesh funksiyalar, MAC.
- Shifrlash usullari.
- Assimetrik shifrlash usullari, CRC tizimlari.
- Shifrlash usullari, CRC tizimlari.

?Quyidagilardan qaysi biri to liq kompyuter topologiyalarini ifodalamaydi.

- +LAN, GAN, OSI.
- Yulduz, WAN, TCP/IP.
- Daraxt, IP, OSI.
- Shina, UDP, FTP.

?OSI tarmoq modeli nechta sathdan iborat?

- +7
- 4
- 6
- 5

?TCP/IP tarmoq modeli nechta sathdan iborat?

- +4
- 7
- 6
- 5

?Hajmi bo'yicha eng kichik hisoblangan tarmoq turi bu -

- +PAN
- LAN
- CAN
- MAN

?IPv6 protokolida IP manzilni ifodalashda necha bit ajratiladi.

- +128
- 32
- 64
- 4

?IP manzilni domen nomlariga yoki aksincha almashtirishni amalga oshiruvchi xizmat bu-

- +DNS
- TCP/IP
- OSI
- UDP

?Natijasi tashkilotning amallariga va funksional harakatlariga zarar keltiruvchi hodisalarning potensial paydo bo'lishi bu?

- +Tahdid.
- Zaiflik.
- Hujum.
- Aktiv.

?Zaiflik orqali AT tizimi xavfsizligini buzish tomon amalga oshirilgan harakat bu?

- +Hujum.
- Zaiflik.
- Tahdid.
- Zararli harakat.

?Quyidagilardan qaysi biri tarmoq xavfsizligi muammolariga sabab bo'lmaydi?

- +Routerlardan foydalanmaslik.
- Qurilma yoki dasturiy vositani noto'g'ri sozlanish.
- Tarmoqni xavfsiz bo'lmagan tarzda va zaif loyihalash.
- Tug'na texnologiya zaifligi.

?Tarmoq xavfsizligini buzulishi biznes faoliyatga qanday ta'sir qiladi?

- +Biznes faoliyatning buzilishi, huquqiy javobgarlikka sababchi bo'ladi.
- Axborotni o'g'irlanishi, tarmoq qurilmalarini fizik buzilishiga olib keladi.
- Maxfiylikni yo'q qilishi, tarmoq qurilmalarini fizik buzilishiga olib keladi.
- Huquqiy javobgarlik, tarmoq qurilmalarini fizik buzilishiga olib keladi.

?Razvedka hujumlari bu?

- +Asosiy hujumlarni oson amalga oshirish uchun tashkilot va tarmoq haqidagi axborotni to'plashni maqsad qiladi.
- Turli texnologiyalardan foydalangan holda tarmoqqa kirishga harakat qiladi.
- Foydalanuvchilarga va tashkilotlarda mavjud bo'lgan biror xizmatni cheklashga urinadi.
- Tizimni fizik buzishni maqsad qiladi.

?Kirish hujumlari bu?

- +Turli texnologiyalardan foydalangan holda tarmoqqa kirishga harakat qiladi.
- Asosiy hujumlarni oson amalga oshirish uchun tashkilot va tarmoq haqidagi axborotni to'plashni maqsad qiladi.
- Foydalanuvchilarga va tashkilotlarda mavjud bo'lgan biror xizmatni cheklashga urinadi.
- Tarmoq haqida axborotni to'plash hujumchilarga mavjud bo'lgan potensial zaiflikni aniqlashga harakat qiladi.

?Xizmatdan voz kechishga qaratilgan hujumlar bu?

- +Foydalanuvchilarga va tashkilotlarda mavjud bo'lgan biror xizmatni cheklashga urinadi.
- Turli texnologiyalardan foydalangan holda tarmoqqa kirishga harakat qiladi.
- Asosiy hujumlarni oson amalga oshirish uchun tashkilot va tarmoq haqidagi axborotni to'plashni maqsad qiladi.
- Tarmoq haqida axborotni to'plash hujumchilarga mavjud bo'lgan potensial zaiflikni aniqlashga harakat qiladi.

?Paketlarni snifferlash, portlarni skanerlash va Ping buyrug'ini yuborish hujumlari qaysi hujumlar toifasiga kiradi?

- +Razvedka hujumlari.
- Kirish hujumlari.
- DOS hujumlari.
- Zararli dasturlar yordamida amalga oshiriladigan hujumlar.

?O'zini yaxshi va foydali dasturiy vosita sifatida ko'rsatuvchi zararli dastur turi bu?

- +Trojan otlari.
- Adware.
- Spyware.
- Backdoors.

?Marketing maqsadida yoki reklamani namoyish qilish uchun foydalanuvchini ko'rish rejimini kuzutib boruvchi zararli dastur turi bu?

- +Adware.
- Trojan otlari.
- Spyware.
- Backdoors.

?Himoya mexanizmini aylanib o'tib tizimga ruxsatsiz kirish imkonini beruvchi zararli dastur turi bu?

- +Backdoors.
- Adware.

- Troyan otlari.
- Spyware.

?Paket filterlari turidagi tarmoqlararo ekran vositasi OSI modelining qaysi sathida ishlaydi?

- +Tarmoq sathida.
- Transport sathida.
- Ilova sathida.
- Kanal sathida.

?Tashqi tarmoqdagi foydalanuvchilardan ichki tarmoq resurslarini himoyalash qaysi himoya vositasining vazifasi hisoblanadi.

- +Tarmoqlararo ekran.
- Antivirus.
- Virtual himoyalangan tarmoq.
- Router.

?Ichki tarmoq foydalanuvchilarini tashqi tarmoqqa bo'lgan murojaatlarini chegaralash qaysi himoya vositasining vazifasi hisoblanadi.

- +Tarmoqlararo ekran.
- Antivirus.
- Virtual himoyalangan tarmoq.
- Router.

?2 lik sanoq tizimida 11011 soniga 11010 sonini 2 modul bo'yicha qo'shish?

- +00001
- 10000
- 01100
- 11111

?2 lik sanoq tizimida 11011 soniga 00100 sonini 2 modul bo'yicha qo'shish?

- +11111
- 10101
- 11100
- 01001

?2 lik sanoq tizimida 11011 soniga 11010 sonini 2 modul bo'yicha qo'shish?

- +00001
- 10000
- 01100
- 11111

?Axborot saqlagich vositalaridan qayta foydalanish xususiyatini saqlab qolgan holda axborotni yo'q qilish usuli qaysi?

- +Bir necha marta takroran yozish va maxsus dasturlar yordamida [saqlagichni tozalash](#)
- Magnitsizlantirish
- Formatlash
- Axborotni saqlagichdan o'chirish



?Elektron ma'lumotlarni yo'q qilishda maxsus qurilma ichida joylashtirilgan saqlagichning xususiyatlari o'zgartiriladigan usul bu ...

- +magnitsizlantirish.
- shredirlash.
- yanchish.
- formatlash.

?Yo'q qilish usullari orasidan ekologik jihatdan ma'qullanmaydigan va maxsus joy talab qiladigan usul qaysi?

- +Yoqish
- Maydalash
- Ko'mish
- Kimyoviy ishlov berish

?Kiberjinoyatchilik bu - ?

+Kompyuter yoki boshqa qurilmalarga qarshi qilingan yoki kompyuter va boshqa qurilmalar orqali qilingan jinoiy faoliyat.

- Kompyuterlar bilan bog'liq falsafiy soha bo'lib, foydalanuvchilarning xatti-harakatlari, kompyuterlar nimaga dasturlashtirilganligi va umuman insonlarga va jamiyatga qanday ta'sir ko'rsatishini o'rganadi.
- Hisoblashga asoslangan bilim sohasi bo'lib, buzg'unchilar mavjud bo'lgan sharoitda amallarni kafolatlash uchun o'zida texnologiya, inson, axborot va jarayonni mujassamlashtirgan.
- Tizimlarni, tarmoqlarni va dasturlarni raqamli hujumlardan himoyalash amaliyoti.

?Kiberetika bu - ?

+Kompyuterlar bilan bog'liq falsafiy soha bo'lib, foydalanuvchilarning xatti-harakatlari, kompyuterlar nimaga dasturlashtirilganligi va umuman insonlarga va jamiyatga qanday ta'sir ko'rsatishini o'rganadi.

- Kompyuter yoki boshqa qurilmalarga qarshi qilingan yoki kompyuter va boshqa qurilmalar orqali qilingan jinoiy faoliyat.
- Hisoblashga asoslangan bilim sohasi bo'lib, buzg'unchilar mavjud bo'lgan sharoitda amallarni kafolatlash uchun o'zida texnologiya, inson, axborot va jarayonni mujassamlashtirgan.
- Tizimlarni, tarmoqlarni va dasturlarni raqamli hujumlardan himoyalash amaliyoti.

?Shaxsiy simsiz tarmoqlar qo'llanish sohasini belgilang

- +Tashqi qurilmalar kabellarining o'rnida
- Binolar va korxonalar va internet orasida belgilangan simsiz bog'lanish
- Butun dunyo bo'yicha internetdan foydalanishda
- Simli tarmoqlarni mobil kengaytirish

?VPNning texnik yechim arxitekturasiga ko'ra turlari keltirilgan qatorni aniqlang?

- +Korporativ tarmoq ichidagi VPN; masofadan foydalaniluvchi VPN; korporativ tarmoqlararo VPN
- Kanal sathidagi VPN; tarmoq sathidagi VPN; seans sathidagi VPN
- Marshrutizator ko'rinishidagi VPN; tarmoqlararo ekran ko'rinishidagi VPN
- Dasturiy ko'rinishdagi VPN; maxsus shifrlash protsessoriga ega apparat vosita ko'rinishidagi VPN

?Axborotning konfidentsialligi va butunligini ta'minlash uchun ikki uzal orasida himoyalangan tunelni quruvchi himoya vositasi bu?

- +Virtual Private Network
- Firewall

- Antivirus
- IDS

?Qanday tahdidlar passiv hisoblanadi?

- +Amalga oshishida axborot strukturasi va mazmunida hech narsani o zgartirmaydigan tahdidlar
- Hech qachon amalga oshirilmaydigan tahdidlar
- Axborot xavfsizligini buzmaydigan tahdidlar
- Texnik vositalar bilan bog liq bo lgan tahdidlar

?Quyidagi qaysi hujum turi razvedka hujumlari turiga kirmaydi?

- +Ddos
- Paketlarni snifferlash
- Portlarni skanerlash
- Ping buyrug ini yuborish

?Trafik orqali axborotni to plashga harakat qilish razvedka hujumlarining qaysi turida amalga oshiriladi?

- +Passiv
- DNS izi
- Lug atga asoslangan
- Aktiv

?Portlarni va operatsion tizimni skanerlash razvedka hujumlarining qaysi turida amalga oshiriladi?

- +Aktiv
- Passiv
- DNS izi
- Lug atga asoslangan

?Paketlarni snifferlash, portlarni skanerlash, ping buyrug ini yuborish qanday hujum turiga misol bo ladi?

- +Razvedka [hujumlari](#)
- Xizmatdan voz kechishga undash hujumlari
- Zararli hujumlar
- Kirish hujumlari

?DNS serverlari tarmoqda qanday vazifani amalga oshiradi?

- +Xost nomlari va internet nomlarini IP manzillarga o zgartirish va teskarisini amalga oshiradi
- Ichki tarmoqqa ulanishga harakat qiluvchi boshqa tarmoq uchun kiruvchi nuqta vazifasini bajaradi
- Tashqi tarmoqqa ulanishga harakat qiluvchi ichki tarmoq uchun chiqish nuqtasi vazifasini bajaradi
- Internet orqali ma lumotlarni almashinuvchi turli ilovalar uchun tarmoq ulanishlarini sozlash funksiyasini amalga oshiradi

?Markaziy xab yoki tugun orqali tarmoqni markazlashgan holda boshqarish qaysi tarmoq topologiyasida amalga oshiriladi?

- +Yulduz
- Shina
- Xalqa
- Mesh

?Quyidagilardan qaysilari ananaviy tarmoq turi hisoblanadi?

- +WAN, MAN, LAN
- OSI, TCP/IP
- UDP, TCP/IP, FTP
- Halqa, yulduz, shina, daraxt

?Quyidagilardan qaysilari tarmoq topologiyalari hisoblanadi?

- +Halqa, yulduz, shina, daraxt
- UDP, TCP/IP, FTP
- OSI, TCP/IP
- SMTP, HTTP, UDP

?Yong inga qarshi tizimlarni aktiv chora turiga quyidagilardan qaysilari kiradi?

- +Yong inni aniqlash va bartaraf etish tizimi
- Minimal darajada yonuvchan materiallardan foydalanish
- Yetarlicha miqdorda qo shimcha chiqish yo llarini mavjudligi
- Yong inga aloqador tizimlarni to g ri madadlanganligi

?Yong inga qarshi kurashishning aktiv usuli to g ri ko rsatilgan javobni toping?

- +Tutunni aniqlovchilar, alangani aniqlovchilar va issiqlikni aniqlovchilar
- Binoga istiqomat qiluvchilarni yong in sodir bo lganda qilinishi zarur bo lgan ishlar bilan tanishtirish
- Minimal darajada yonuvchan materiallardan foydalanish, qo shimcha etaj va xonalar qurish
- Yetarli sondagi qo shimcha chiqish yo llarining mavjudligi

?Yong inga qarshi kurashishning passiv usuliga kiruvchi choralarni to g ri ko rsatilgan javobni toping?

- +Minimal darajada yonuvchan materiallardan foydalanish, qo shimcha etaj va xonalar qurish
- Tutun va alangani aniqlovchilar
- O t o chirgich, suv purkash tizimlari
- Tutun va alangani aniqlovchilar va suv purkash tizimlari

?Fizik himoyani buzilishiga olib keluvchi tahdidlar yuzaga kelish shakliga ko ra qanday guruhlariga bo linadi?

- +Tabiiy va sun iy
- Ichki va tashqi
- Aktiv va passiv
- Bir faktorlik va ko p faktorli

?Quyidagilarnig qaysi biri tabiiy tahdidlarga misol bo la oladi?

- +Toshqinlar, yong in, zilzila
- Bosqinchilik, terrorizm, o g irlik
- O g irlik, toshqinlar, zilzila
- Terorizm, toshqinlar, zilzila

?Quyidagilarnig qaysi biri sun iy tahdidlarga misol bo la oladi?

- +Bosqinchilik, terrorizm, o g irlik
- Toshqinlar, zilzila, toshqinlar
- O g irlik, toshqinlar, zilzila
- Terorizm, toshqinlar, zilzila

?Kolliziya hodisasi deb nimaga aytiladi?

- +Ikki xil matn uchun bir xil xesh qiymat chiqishi
- ikki xil matn uchun ikki xil xesh qiymat chiqishi
- bir xil matn uchun bir xil xesh qiymat chiqishi
- bir xil matn uchun ikki xil xesh qiymat chiqishi

?GSM tarmog'ida foydalaniluvchi shifrlash algoritmi nomini ko'rsating?

- +A5/1
- DES
- AES
- RC4

?O'zbekistonda kriptografiya sohasida faoliyat yurituvchi tashkilot nomini ko'rsating?

- +"UNICON.UZ" DUK
- "O'zstandart" agentligi
- Davlat Soliq Qo'mitasi
- Kadastr agentligi

?RC4 shifrlash algoritmi simmetrik turga mansub bo'lsa, unda nechta kalitdan foydalaniladi?

- +1
- 2
- 3
- 4

?A5/1 shifrlash algoritmi simmetrik turga mansub bo'lsa, unda nechta kalitdan foydalaniladi?

- +1
- 2
- 3
- 4

?AES shifrlash algoritmi simmetrik turga mansub bo'lsa, unda nechta kalitdan foydalaniladi?

- +1
- 2
- 3
- 4

?DES shifrlash algoritmi simmetrik turga mansub bo'lsa, unda nechta kalitdan foydalaniladi?

- +1
- 2
- 3
- 4

?A5/1 oqimli shifrlash algoritmida maxfiy kalit necha registrga bo'linadi?

- +3
- 4

-5  
-6

?Faqat simmetrik blokli shifrlarga xos bo'lgan atamani aniqlang?

+blok uzunligi  
-kalit uzunligi  
-ochiq kalit  
-kodlash jadvali

?A5/1 shifri qaysi turga mansub?

+oqimli shifrlar  
-blokli shifrlar  
-ochiq kalitli shifrlar  
-assimetrik shifrlar

?.... shifrlar blokli va oqimli turlarga ajratiladi

+simmetrik  
-ochiq kalitli  
-assimetrik  
-klassik

?Quyida keltirilgan xususiyatlarning qaysilari xesh funksiyaga mos?

+ixtiyoriy olingan har xil matn uchun xesh qiymatlar bir xil bo'lmaydi  
-ixtiyoriy olingan bir xil matn uchun qiymatlar bir xil bo'lmaydi  
-ixtiyoriy olingan har xil matn uchun xesh qiymatlar bir xil bo'ladi  
-ixtiyoriy olingan har xil xesh qiymat uchun dastlabki ma'lumotlar bir xil bo'ladi

?Quyida keltirilgan xususiyatlarning qaysilari xesh funksiyaga mos?

+chiqishda fiksirlangan uzunlikdagi qiymatni beradi  
-chiqishda bir xil qiymatni beradi  
-chiqishdagi qiymat bilan kiruvchi qiymatlar bir xil bo'ladi  
-kolliziyaga ega

?Xesh qiymatlarni yana qanday atash mumkin?

+dayjest  
-funksiya  
-imzo  
-raqamli imzo

?A5/1 oqimli shifrlash algoritmidagi dastlabki kalit uzunligi nechki bitga teng?

+64  
-512  
-192  
-256

?A5/1 oqimli shifrlash algoritmi asosan qayerda qo'llaniladi?

- +mobil aloqa standarti GSM protokolida
- simsiz aloqa vositalaridagi mavjud WEP protokolida
- internet trafiklarini shifrlashda
- radioaloqa tarmoqlarida

?Assimetrik kriptotizimlarda necha kalitdan foydalaniladi?

- +2 ta
- 3 ta
- 4 ta
- kalit **ishlatilmaydi**

?Simmetrik kriptotizimlarda necha kalitdan foydalaniladi?

- +1 ta
- 3 ta
- 4 ta
- kalit ishlatilmaydi

?Kriptotizimlar kalitlar soni bo'yicha qanday turga bo'linadi?

- +simmetrik va assimetrik turlarga
- simmetrik va bir kalitli turlarga
- 3 kalitli turlarga
- assimetrik va 2 kalitli turlarga

?Kriptologiya qanday yo'nalishlarga bo'linadi?

- +kriptografiya va kriptotahlil
- kriptografiya va kriptotizim
- kripto va kriptotahlil
- kriptoanaliz va kriptotizim

?Qaysi chora tadbirlar virusdan zararlanish holatini kamaytiradi?

- +Barcha javoblar to'g'ri
- Faqat litsenziyalı dasturiy ta'minotdan foydalanish.
- Kompyuterni zamonaviy antivirus dasturiy vositasi bilan ta'minlash va uni doimiy yangilab borish.
- Boshqa kompyuterda yozib olingan ma'lumotlarni o'qishdan oldin har bir saqlagichni antivirus tekshiruvidan o'tkazish.

?Antivirus dasturiy vositalari zararli dasturlarga qarshi to'liq himoyani ta'minlay olmasligining asosiy sababini ko'rsating?

- +Paydo bo'layotgan zararli dasturiy vositalar sonining ko'pligi.
- Viruslar asosan antivirus ishlab chiqaruvchilar tomonidan yaratilishi.
- Antivirus vositalarining samarali emasligi.
- Aksariyat antivirus vositalarining pullik ekanligi.

?...umumiy tarmoqni ichki va tashqi qismlarga ajratib himoyalash imkonini beradi.

- +Tarmoqlararo ekran
- Virtual himoyalangan tarmoq
- Global tarmoq
- Korxona tarmog'i

?RSA algoritmidagi  $p=5$ ,  $q=13$ ,  $e=7$  ga teng bo'lsa, shaxsiy kalitni hisoblang?

- +7
- 13
- 65
- 35

?..... hujumida hujumchi o'rnatilgan aloqaga suqilib kiradi va aloqani bo'ladi. Nuqtalar o'rniga mos javobni qo'ying.

- +O'rnatilgan odam.
- Qo'pol kuch.
- Parolga qaratilgan.
- DNS izi.

?Agar ob'ektning xavfsizlik darajasi sub'ektning xavfsizlik darajasidan kichik yoki teng bo'lsa, u holda O'qish uchun ruxsat beriladi. Ushbu qoida qaysi foydalanishni boshqarish usuliga tegishli.

- +MAC
- DAC
- RMAC
- ABAC

?GSM tarmog'ida ovozli sozlashuvlarni shifrlash algoritmi bu?

- +A5/1
- DES
- FOCT
- RSA

?RSA algoritmidagi ochiq kalit  $e=7$ ,  $N=35$  ga teng bo'lsa,  $M=2$  ga teng ochiq matnni shifrlash natijasini ko'rsating?

- +23
- 35
- 5
- 7

?RSA algoritmidagi ochiq kalit  $e=7$ ,  $N=143$  ga teng bo'lsa,  $M=2$  ga teng ochiq matnni shifrlash natijasini ko'rsating?

- +128
- 49
- 11
- 7

?Jumlani to'ldiring. Agar axborotning o'zgarishi moddiy va ma'naviy boyliklarning yo'qotilishiga olib kelsa.

- +jinoyat sifatida baholanadi.
- rag'bat hisoblanadi.
- buzg'unchilik hisoblanadi.
- guruhlar kurashi hisoblanadi.

?Jumlani to'ldiring. Simli va simsiz tarmoqlar orasidagi asosiy farq ...

- +tarmoq chetki nuqtalari orasidagi mutlaqo nazoratlamaydigan xudud mavjudligi.
- tarmoq chetki nuqtalari orasidagi xududning kengligi.

- himoya vositalarining chegaralanganligi.
- himoyani amalga oshirish imkoniyati yo'qligi.

?Jumlani to'ldiring. Simmetrik shifrlash algoritmlari ochiq ma'lumotdan foydalanish tartibiga ko'ra ...

- +blokli va oqimli turlarga bo'linadi.
- bir kalitli va ikki kalitli turlarga bo'linadi.
- Feistel tarmog'iga asoslangan va SP tarmog'iga asoslangan turlarga bo'linadi.
- murakkablikka va tizimni nazariy yondoshuvga asoslangan turlarga bo'linadi.

?Jumlani to'ldiring. Tarmoqlararo ekranning vazifasi ...

- +ishonchli va ishonchsiz tarmoqlar orasida ma'lumotlarga kirishni boshqarish.
- tarmoq hujumlarini aniqlash.
- trafikni taqiqlash.
- tarmoqdagi xabarlar oqimini uzish va ulash.

?Faktorlash muammosi asosida yaratilgan assimetrik shifrlash usuli?

- +RSA
- El-Gamal
- Elliptik egri chiziqqa asoslangan shifrlash
- Diffi-Hellman

?Eng zaif simsiz tarmoq protokolini ko'rsating?

- +WEP
- WPA
- WPA2
- WPA3

?Axborotni shifrlashdan maqsadi nima?

- +Maxfiy xabar mazmunini yashirish.
- Ma'lumotlarni zichlashtirish, siqish.
- Ma'lumotlarni yig'ish va sotish.
- Ma'lumotlarni uzatish.

?9 soni bilan o'zaro tub bo'lgan sonlarni ko'rsating?

- +10, 8
- 6, 10
- 18, 6
- 9 dan tashqari barcha sonlar

?12 soni bilan o'zaro tub bo'lgan sonlarni ko'rsating?

- +11, 13
- 14, 26
- 144, 4
- 12 dan tashqari barcha sonlar

?13 soni bilan o'zaro tub bo'lgan sonlarni ko'rsating?



- +5, 7
- 12, 26
- 14, 39
- 13 dan tashqari barcha sonlar

?Jumlani to'ldiring. Autentifikatsiya tizimlari asoslanishiga ko'ra ... turga bo'linadi.

- +3
- 2
- 4
- 5

?...umumiy tarmoqni ichki va tashqi qismlarga ajratib himoyalash imkonini beradi.

- +Tarmoqlararo ekran
- Virtual himoyalangan tarmoq
- Global tarmoq
- Korxona tarmog'i

?Antivirus dasturiy vositalari zararli dasturlarga qarshi to'liq himoyani ta'minlay olmasligining asosiy sababini ko'rsating?

- +Paydo bo'layotgan zararli dasturiy vositalar sonining ko'pligi.
- Viruslar asosan antivirus ishlab chiqaruvchilar tomonidan yaratilishi.
- Antivirus vositalarining samarali emasligi.
- Aksariyat antivirus vositalarining pullik ekanligi.

?Qaysi chora tadbirlar virusdan zararlanish holatini kamaytiradi?

- +Barcha javoblar to'g'ri
- Faqat litsenzyali dasturiy ta'minotdan foydalanish.
- Kompyuterni zamonaviy antivirus dasturiy vositasi bilan ta'minlash va uni doimiy yangilab borish.
- Boshqa kompyuterda yozib olingan ma'lumotlarni o'qishdan oldin har bir saqlagichni antivirus tekshiruvidan o'tkazish.

?Virus aniq bo'lganda va xususiyatlari aniq ajratilgan holatda eng katta samaradorlikka ega zararli dasturni aniqlash usulini ko'rsating?

- +Signaturaga asoslangan usul
- O'zgarishga asoslangan usul
- Anomaliyaga asoslangan usul
- Barcha javoblar to'g'ri

?Signatura (antiviruslarga aloqador bo'lgan) bu-?

- +Fayldan topilgan bitlar qatori.
- Fayldagi yoki katalogdagi o'zgarish.
- Normal holatdan tashqari holat.
- Zararli dastur turi.

?Zararli dasturiy vositalarga qarshi foydalaniluvchi dasturiy vosita bu?

- +Antivirus
- VPN

- Tarmoqlararo ekran
- Brandmauer

?Kompyuter viruslarini tarqalish usullarini ko'rsating?

- +Ma lumot saqlovchilari, Internetdan yuklab olish va elektron pochta orqali.
- Ma lumot saqlovchilari, Internetdan yuklab olish va skaner qurilmalari orqali.
- Printer qurilmasi, Internetdan yuklab olish va elektron pochta orqali.
- Barcha javoblar to'g'ri.

?Qurbon kompyuteridagi ma lumotni shifrlab, uni deshifrlash uchun to'lovni amalga oshirishni talab qiluvchi zararli dastur bu-?

- +Ransomware.
- Mantiqiy bombalar.
- Rootkits.
- Spyware.

?Internet tarmog'idagi obro' sizlantirilgan kompyuterlar bu-?

- +Botnet.
- Backdoors.
- Adware.
- Virus.

?Biror mantiqiy shartni tekshiruvchi trigger va foydali yuklamadan iborat zararli dastur turi bu-?

- +Mantiqiy bombalar.
- Backdoors.
- Adware.
- Virus.

?Buzg'unchiga xavfsizlik tizimini aylanib o'tib tizimga kirish imkonini beruvchi zararli dastur turi bu-?

- +Backdoors.
- Adware.
- Virus.
- Trojan otlari.

?Ma lumotni to'liq qayta tiklash qachon samarali amalga oshiriladi?

- +Saqlagichda ma lumot qayta yozilmagan bo'lsa.
- Ma lumotni o'chirish Delete buyrug'i bilan amalga oshirilgan bo'lsa.
- Ma lumotni o'chirish Shifr+Delete buyrug'i bilan amalga oshirilgan bo'lsa.
- Formatlash asosida ma lumot o'chirilgan bo'lsa.

?Ma lumotni zaxira nusxalash nima uchun potensial tahdidlarni paydo bo'lish ehtimolini oshiradi.

- +Tahdidchi uchun nishon ko'payadi.
- Saqlanuvchi ma lumot hajmi ortadi.
- Ma lumotni butunligi ta'minlanadi.
- Ma lumot yo'qolgan taqdirda ham tiklash imkoniyati mavjud bo'ladi.

?Qaysi xususiyatlar RAID texnologiyasiga xos emas?

- +Shaxsiy kompyuterda foydalanish mumkin.
- Serverlarda foydalanish mumkin.
- Xatoliklarni nazoratlash mumkin.
- Disklarni "qaynoq almashtirish" mumkin.

?Qaysi zaxira nusxalash vositasi oddiy kompyuterlarda foydalanish uchun qo'shimcha apparat va dasturiy vositani talab qiladi?

- +Lentali disklar.
- Ko'chma qattiq disklar.
- USB disklar.
- CD/DVD disklar.

?Ma'lumotlarni zaxira nusxalash strategiyasi nimadan boshlanadi?

- +Zarur axborotni tanlashdan.
- Mos zaxira nusxalash vositasini tanlashdan.
- Mos zaxira nusxalash usulini tanlashdan.
- Mos RAID sathini tanlashdan.

?Jumlani to'ldiring. .... - muhim bo'lgan axborot nusxalash yoki saqlash jarayoni bo'lib, bu ma'lumot yo'qolgan vaqtda qayta tiklash imkoniyatini beradi.

- +Ma'lumotlarni zaxira nusxalash
- Kriptografik himoya
- VPN
- Tarmoqlararo ekran

?Paket filteri turidagi tarmoqlararo ekran vositasi nima asosida tekshirishni amalga oshiradi?

- +Tarmoq sathi parametrlari asosida.
- Kanal sathi parametrlari asosida.
- Ilova sathi parametrlari asosida.
- Taqdimot sathi parametrlari asosida.

?Jumlani to'ldiring. ... texnologiyasi lokal simsiz tarmoqlarga tegishli.

- +WI-FI
- WI-MAX
- GSM
- Bluetooth

?Jumlani to'ldiring. Kriptografik himoya axborotning ... xususiyatini ta'minlamaydi.

- +Foydalanuvchanlik
- Butunlik
- Maxfiylik
- Autentifikatsiya

?Jumlani to'ldiring. Parol kalitidan .... farq qiladi.

- +tasodifiylik darajasi bilan
- uzunligi bilan

- belgilari bilan
- samaradorligi bilan

?Parolga "tuz"ni qo shib xeshlashdan maqsad?

- +Tahdidchi ishini oshirish.
- Murakkab parol hosil qilish.
- Murakkab xesh qiymat hosil qilish.
- Ya na bir maxfiy parametr kiritish.

?Axborotni foydalanuvchanligini buzishga qaratilgan tahdidlar bu?

- +DDOS tahdidlar.
- Nusxalash tahdidlari.
- Modifikatsiyalash tahdidlari.
- O rtaga turgan odam tahdidi.

?Tasodifiy tahdidlarni ko rsating?

- +Texnik vositalarning buzilishi va ishlamasligi.
- Axborotdan ruxsatsiz foydalanish.
- Zararkunanda dasturlar.
- An anaviy josuslik va diversiya.

?Xodimlarga faqat ruxsat etilgan saytlardan foydalanishga imkon beruvchi himoya vositasi bu?

- +Tarmoqlararo ekran.
- Virtual Private Network.
- Antivirus.
- Router.

?Qaysi himoya vositasi yetkazilgan axborotning butunligini tekshiradi?

- +Virtual Private Network.
- Tarmoqlararo ekran.
- Antivirus.
- Router.

?Qaysi himoya vositasi tomonlarni autentifikatsiyalash imkoniyatini beradi?

- +Virtual Private Network.
- Tarmoqlararo ekran.
- Antivirus.
- Router.

?Foydalanuvchi tomonidan kiritilgan taqiqlangan so rovni qaysi himoya vositasi yordamida nazoratlash mumkin.

- +Tarmoqlararo ekran.
- Virtual Private Network.
- Antivirus.
- Router.

?Qaysi himoya vositasi mavjud **IP - paketni to liq shifrlab**, unga yangi IP sarlavha beradi?

- +Virtual Private Network.
- Tarmoqlararo ekran.
- Antivirus.
- Router.

?Ochiq tarmoq yordamida himoyalangan tarmoqni qurish imkoniyatiga ega himoya vositasi bu?

- +Virtual Private Network.
- Tarmoqlararo ekran.
- Antivirus.
- Router.

?Qaysi himoya vositasida mavjud paket shifrlangan holda yangi hosil qilingan mantiqiy paket ichiga kiritiladi?

- +Virtual Private Network.
- Tarmoqlararo ekran.
- Antivirus.
- Router.

?Qaysi himoya vositasi tarmoqda uzatilayotgan axborotni butunligi, maxfiyligi va tomonlar autentifikatsiyasini ta'minlaydi?

- +Virtual Private Network.
- Tarmoqlararo ekran.
- Antivirus.
- Router.

?Qaysi tarmoq himoya vositasi tarmoq manzili, identifikatorlar, interfeys manzili, port nomeri va boshqa parametrlar yordamida filtrlashni amalga oshiradi.

- +Tarmoqlararo ekran.
- Antivirus.
- Virtual himoyalangan tarmoq.
- Router.

?Web-sahifa bu...

- +Yagona adresga ega bo'lgan, brauzer yordamida ochish va ko'rish imkoniyatiga ega bo'lgan hujjatdir
- Tarmoqqa ulangan kompyuterda, klientga belgilangan umumiy vazifalarni bajarish uchun foydalaniluvchi sahifadir
- Klient-server arxitekturasiga asosidagi, keng tarqalgan Internetning axborot xizmati
- HTML kodlari to'plami

?Web-sayt nima?

- +Aniq maqsad asosida mantiqiy bog'langan web-sahifalar birlashmasi
- Klient-server texnologiyasiga asoslangan, keng tarqalgan internetning axborot xizmatidir
- A va B
- Yagona adresga ega bo'lgan hujjat hisoblanib, uni ochish (brauzer yordamida) va o'qish imkoniyati mavjud

?WWW nechta komponentdan tashkil topgan?

-3  
-2

?WWWning komponentlari qaysi javobda to'g'ri berilgan?

+Dasturiy/texnik vositalar, HTML, HTTP, URI  
-HTML, FTP, WWW  
-HTML, CSS, PHP  
-HTML, JavaScript, JQuery, PHP

?Hozirgi kunda WWWning nechta versiyasi mavjud?

+4  
-3  
-5  
-2

?Web 1.0 ning rivojlanish davrini toping?

+1990-2000 yy.  
-2000-2005 yy.  
-1980-1990 yy.  
-2010-2015 yy.

?Web 2.0 ning rivojlanish davrini toping?

+2000-2010 yy.  
-2010-2020 yy.  
-2020-2030 yy.  
-1990-2000 yy.

?Web 3.0 ning rivojlanish davrini toping?

+2010-2020 yy.  
-2000-2010 yy.  
-2020-2030 yy.  
-1990-2000 yy.

?Web 4.0 ning rivojlanish davrini toping?

+2020-2030 yy.  
-2000-2010 yy.  
-2010-2020 yy.  
-1990-2000 yy.

?HTML teglar necha xil bo'ladi?

+Juft, toq, maxsus teglar  
-Toq teglari  
-Juft teglari  
-Ko'rinishi ko'p

?Qaysi teg HTML hujjatning tanasini ifodalaydi?

- +body
- html
- head
- title

?Qaysi teg hujjatning stilini ifodalash uchun ishlatiladi?

- +style
- head
- isindex
- body

?Qaysi teg HTML hujjatni ifodalaydi?

- +html
- body
- meta
- isindex

?Qaysi teg HTML hujjat sarlavhasini ifodalaydi?

- +head
- meta
- title
- body

?Havola to g ri ko rsatilgan qatorni toping.

- +havola
- havola
- havola
- Ekranni tozalash

?

---

tegi nimani ifodalaydi?

- +Gorizontal chiziq chizish
- Yangi satrga o tish
- qo shtirnoq
- Ekranni tozalash

?Jadval hosil qilish uchun qaysi tegdan foydalaniladi?

+



?Jadval ustunlarini birlashtirish atributi qaysi javobda keltirilgan?

?Jadval satrlarini birlashtirish atributi qaysi javobda keltirilgan?

?HTML da shrift o lchamini o zgartirish uchun qaysi tegdan foydalaniladi?

-  
-  
-

?  
tegi nimani ifodalaydi?

+Yangi satrga o tish  
-"uzilish"  
-qo shirnoq  
-Ekranni tozalash

?  
tegi nima uchun qo llaniladi?

+matnni paragraflarga ajratish uchun  
-Sarlavhani ifodalash uchun  
-Obyektni ko rsatilgan joyga o rnatish va shu nuqtadan bo sh satrga matnni davom ettirish uchun qo llaniladi  
-Tartibsiz ro yxat hosil qilish uchun

?Rasmlar bilan ishlash teglarini qaysi javobda berilgan?

+Img, map, area, [picture](#)  
-Image, map, a, picture  
-Image, form, area, photo  
-Img, iframe, areas, picture

? tegining vazifasi nima?

+Matnni ajratilgan shaklda aniqlash  
-Matnni o chirilgan shaklda belgilash  
-Matnni tagiga chizilgan shaklda belgilash  
-Matnni qiya shaklda belgilash

? tegining vazifasi nima?

+Matnni tagiga chizilgan shaklda belgilash  
-Matnni o chirilgan shaklda belgilash  
-Matnni ajratilgan shaklda aniqlash  
-Matnni qiya shaklda belgilash

? tegining vazifasi nima?



- +Matnni o'chirilgan shaklda belgilash
- Matnni tagiga chizilgan shaklda belgilash
- Matnni ajratilgan shaklda aniqlash
- Matnni qir shaklda belgilash

?

tegini nimani ifodalaydi?

- +Tartiblanmagan ro'yxat
- Tartiblangan ro'yxat
- Jadval yacheykasi
- Yangi qatorga o'tish

?

matni nimani ifodalaydi?

- +Teg kvadrat shaklidagi ro'yxat hosil qiladi
- Teg aylana shaklidagi ro'yxat hosil qiladi
- Teg alifbo ko'rinishdagi ro'yxatni hosil qiladi
- Teg raqamli ko'rinishdagi ro'yxatni hosil qiladi

?

matni nimani ifodalaydi?

- +Teg I., II., III., IV. va h.k ko'rinishdagi ro'yxatni hosil qiladi
- Teg raqamli ko'rinishdagi ro'yxatni hosil qiladi
- Teg kvadrat shaklidagi ro'yxat hosil qiladi
- Teg 1., 2., 3., 4. va h.k ko'rinishdagi ro'yxatni hosil qiladi

?

tegining majburiy atributini toping

- +src
- title
- href
- type

?Qaysi teg forma ichida qayerga ma'lumot kiritilishini ifodalaydi?

+

=

=

=

?HTMLda forma elementlariga kiritilgan qiymatlarni tozalash uchun qaysi elementdan foydalaniladi?

- +reset
- text
- hidden
- submit

?Qaysi teg formada ma'lumot kiritishda foydalanuvchi bir nechta variantlardan birini tanlashdan foydalanishni ifodalaydi?

+
☐
atributi bilan

-
atributi bilan

-
☐
atributi bilan

-
atributi bilan

?Formada parol kiritish kerak bo'lsa qaysi kiritish elementidan foydalanishga to'g'ri keladi?

+password
-☐
-
-

- - - +colspan -rowspan -cellpadding -cols +rowspan -colspan -cellpadding -rows +

TESTLAR

**№ 1.**

**Manba:** Kiberxavfsizlik asoslari: O'quv qo'llanma/S.K.Ganiev, A.A.Ganiev, Z.T.Xudoyqulov; – T.: "Iqtisod-Moliya", 2021. – 228 b..

**Qiyinlik darajasi – 1**

Kriptologiya qanday yo'nalishlarga bo'linadi?
kriptografiya va kriptotahlil
kriptografiya va kriptotizim
kripto va kriptotahlil
kriptoanaliz va kriptotizim

**№ 2.**

**Manba:** Kiberxavfsizlik asoslari: O'quv qo'llanma/S.K.Ganiev, A.A.Ganiev, Z.T.Xudoyqulov; – T.: "Iqtisod-Moliya", 2021. – 228 b..

**Qiyinlik darajasi – 1**

Kriptologiya nima bilan shug'ullanadi?
maxfiy kodlarni yaratish va buzish ilmi bilan
maxfiy kodlarni buzish bilan
maxfiy kodlarni yaratish bilan
maxfiy kodlar orqali ma'lumotlarni yashirish bilan

**№ 3.**

**Manba:** Kiberxavfsizlik asoslari: O'quv qo'llanma/S.K.Ganiev, A.A.Ganiev, Z.T.Xudoyqulov; – T.: "Iqtisod-Moliya", 2021. – 228 b..

**Qiyinlik darajasi – 1**

Kriptografiya nima bilan shug'ullanadi?
maxfiy kodlarni yaratish bilan
maxfiy kodlarni buzish bilan
maxfiy kodlar orqali ma'lumotlarni yashirish bilan
shifrlash uslublarini bilmagan holda shifrlangan ma'lumotni asl holatini topish bilan

**№ 4.**

**Manba:** Kiberxavfsizlik asoslari: O'quv qo'llanma/S.K.Ganiev, A.A.Ganiev, Z.T.Xudoyqulov; – T.: "Iqtisod-Moliya", 2021. – 228 b..

**Qiyinlik darajasi – 1**

Kriptotahlil nima bilan shug'ullanadi?
maxfiy kodlarni buzish bilan
maxfiy kodlarni yaratish bilan
maxfiy kodlar orqali ma'lumotlarni yashirish bilan
shifrlash uslublarini bilmagan holda shifrlangan ma'lumotni asl holatini topish bilan

**№ 5.**

**Manba:** Kiberxavfsizlik asoslari: O'quv qo'llanma/S.K.Ganiev, A.A.Ganiev, Z.T.Xudoyqulov; – T.: "Iqtisod-Moliya", 2021. – 228 b..

**Qiyinlik darajasi – 1**

Shifrlash orqali ma'lumotning qaysi xususiyati ta'minlanadi?
maxfiyligi
butunliligi
ishonchliligi
foydalanuvchanligi

**№ 6.**

**Manba:** Kiberxavfsizlik asoslari: O'quv qo'llanma/S.K.Ganiev, A.A.Ganiev, Z.T.Xudoyqulov; – T.: "Iqtisod-Moliya", 2021. – 228 b..

**Qiyinlik darajasi – 1**

Steganografiya ma'lumotni qanday maxfiylashtiradi?
maxfiy xabarni soxta xabar ichiga berkitish orqali
maxfiy xabarni kriptografik kalit yordamida shifrlash orqali
maxfiy xabarni shifrlash orqali
maxfiy xabarni kodlash orqali

**№ 7.**

**Manba:** Kiberxavfsizlik asoslari: O'quv qo'llanma/S.K.Ganiev, A.A.Ganiev, Z.T.Xudoyqulov; – T.: "Iqtisod-Moliya", 2021. – 228 b..

**Qiyinlik darajasi – 1**

Kriptologiya necha yoʻnalishga boʻlinadi?
2
4
6
8

#### **№ 8.**

**Manba:** Kiberxavfsizlik asoslari: Oʻquv qoʻllanma/S.K.Ganiev, A.A.Ganiev, Z.T.Xudoyqulov; – T.: “Iqtisod-Moliya”, 2021. – 228 b..

#### **Qiyinlik darajasi – 1**

Kriptologiya soʻzining maʼnosi?
cryptos – maxfiy, logos – ilm
cryptos – kodlash, logos – ilm
cryptos – kript, logos – yashiraman
cryptos – maxfiy, logos – kalit

#### **№ 9.**

**Manba:** Kiberxavfsizlik asoslari: Oʻquv qoʻllanma/S.K.Ganiev, A.A.Ganiev, Z.T.Xudoyqulov; – T.: “Iqtisod-Moliya”, 2021. – 228 b..

#### **Qiyinlik darajasi – 1**

Zamonaviy kriptografiya qaysi boʻlimlarni oʻz ichiga oladi?
simmetrik kriptotizimlar, ochiq kalitli kriptotizimlar, elektron raqamli imzo kriptotizimlari, kriptobardoshli kalitlarni ishlab chiqish va boshqarish
simmetrik kriptotizimlar, ochiq kalit algoritmiga asoslangan kriptotizimlar, elektron raqamli imzo kriptotizimlari, foydalanuvchilarni roʻyxatga olish
simmetrik kriptotizimlar, ochiq kalit algoritmiga asoslangan kriptotizimlar, elektron raqamli imzo kriptotizimlari, foydalanuvchilarni autentifikatsiyalash
simmetrik kriptotizimlar, ochiq kalit algoritmiga asoslangan kriptotizimlar, elektron raqamli imzo kriptotizimlari, foydalanuvchilarni identifikatsiya qilish

#### **№ 10.**

**Manba:** Kiberxavfsizlik asoslari: Oʻquv qoʻllanma/S.K.Ganiev, A.A.Ganiev, Z.T.Xudoyqulov; – T.: “Iqtisod-Moliya”, 2021. – 228 b..

#### **Qiyinlik darajasi – 1**

Kriptotizimlar kalitlar soni bo'yicha necha turga bo'linadi?
2
4
6
8

### **№ 11.**

**Manba:** Kiberxavfsizlik asoslari: O'quv qo'llanma/S.K.Ganiev, A.A.Ganiev, Z.T.Xudoyqulov; – T.: "Iqtisod-Moliya", 2021. – 228 b..

### **Qiyinlik darajasi – 1**

Kriptotizimlar kalitlar soni bo'yicha qanday turga bo'linadi?
simmetrik va assimetrik turlarga
simmetrik va bir kalitli turlarga
3 kalitli turlarga
assimetrik va 2 kalitli turlarga

### **№ 12.**

**Manba:** Kiberxavfsizlik asoslari: O'quv qo'llanma/S.K.Ganiev, A.A.Ganiev, Z.T.Xudoyqulov; – T.: "Iqtisod-Moliya", 2021. – 228 b..

### **Qiyinlik darajasi – 1**

Ma'lumotlarni kodlash va dekodlashda necha kalitdan foydalanadi?
kalit ishlatilmaydi
4 ta
2 ta
3 ta

### **№ 13.**

**Manba:** Kiberxavfsizlik asoslari: O'quv qo'llanma/S.K.Ganiev, A.A.Ganiev, Z.T.Xudoyqulov; – T.: "Iqtisod-Moliya", 2021. – 228 b..

### **Qiyinlik darajasi – 1**

Simmetrik kriptotizimlarda necha kalitdan foydalaniladi?
1 ta

3 ta
4 ta
kalit ishlatilmaydi

#### **№ 14.**

**Manba:** Kiberxavfsizlik asoslari: O'quv qo'llanma/S.K.Ganiev, A.A.Ganiev, Z.T.Xudoyqulov; – T.: "Iqtisod-Moliya", 2021. – 228 b..

#### **Qiyinlik darajasi – 1**

Assimetrik kriptotizimlarda necha kalitdan foydalaniladi?
2 ta
3 ta
4 ta
kalit ishlatilmaydi

#### **№ 15.**

**Manba:** Kiberxavfsizlik asoslari: O'quv qo'llanma/S.K.Ganiev, A.A.Ganiev, Z.T.Xudoyqulov; – T.: "Iqtisod-Moliya", 2021. – 228 b..

#### **Qiyinlik darajasi – 1**

Kerxofs printsiplari nimadan iborat?
kriptografik tizim faqat kalit noma'lum bo'lgan taqdirdagina maxfiylik ta'minlanadi
kriptografik tizim faqat yopiq bo'lgan taqdirdagina maxfiylik ta'minlanadi
kriptografik tizim faqat kalit ochiq bo'lgan taqdirdagina maxfiylik ta'minlanadi
kriptografik tizim faqat ikkita kalit ma'lum bo'lgan taqdirdagina maxfiylik ta'minlanadi

#### **№ 16.**

**Manba:** Kiberxavfsizlik asoslari: O'quv qo'llanma/S.K.Ganiev, A.A.Ganiev, Z.T.Xudoyqulov; – T.: "Iqtisod-Moliya", 2021. – 228 b..

#### **Qiyinlik darajasi – 1**

Kalit bardoshliligi bu -?
eng yaxshi ma'lum algoritmlar bilan kalitni topish murakkabligidir
eng yaxshi ma'lum algoritmlar yordamida yolg'on axborotni ro'kach qilishdir
nazariy bardoshlilik

**№ 17.**

**Manba:** Kiberxavfsizlik asoslari: O'quv qo'llanma/S.K.Ganiev, A.A.Ganiev, Z.T.Xudoyqulov; – T.: "Iqtisod-Moliya", 2021. – 228 b..

**Qiyinlik darajasi – 1**

Shifrlash algoritmlari akslantirish turlariga qarab qanday turlarga bo'linad?
o'rniga qo'yish, o'rin almashtirish va kompozitsion akslantirishlarga
o'rniga qo'yish va o'rin almashtirish akslantirishlariga
o'rniga qo'yish, o'rin almashtirish va surish akslantirishlariga
o'rniga qo'yish, sirush va kompozitsion shifrlash akslantirishlariga

**№ 18.**

**Manba:** Kiberxavfsizlik asoslari: O'quv qo'llanma/S.K.Ganiev, A.A.Ganiev, Z.T.Xudoyqulov; – T.: "Iqtisod-Moliya", 2021. – 228 b..

**Qiyinlik darajasi – 1**

O'rniga qo'yish shifrlash sinfiga qanday algoritmlar kiradi?
shifrlash jarayonida ochiq ma'lumot alfaviti belgilari shifr ma'lumot belgilariga almashtiriladigan algoritmlar
shifrlash jarayonida ochiq ma'lumot alfaviti belgilarining o'rinlar almashtiriladigan algoritmlar
shifrlash jarayonida o'rniga qo'yish va o'rin almashtirish akslantirishlarning kombinatsiyalaridan birgalikda foydalaniladigan algoritmlar
shifrlash jarayonida kalitlarning o'rni almashtiriladigan algoritmlarga

**№ 19.**

**Manba:** Kiberxavfsizlik asoslari: O'quv qo'llanma/S.K.Ganiev, A.A.Ganiev, Z.T.Xudoyqulov; – T.: "Iqtisod-Moliya", 2021. – 228 b..

**Qiyinlik darajasi – 1**

O'rniga qo'yish shifrlash algoritmlari necha sinfga bo'linadi?
2
4
6



**№ 20.**

**Manba:** Kiberxavfsizlik asoslari: O'quv qo'llanma/S.K.Ganiev, A.A.Ganiev, Z.T.Xudoyqulov; – T.: "Iqtisod-Moliya", 2021. – 228 b..

**Qiyinlik darajasi – 1**

O'rniga qo'yish shifrlash algoritmlari qanday sinfga bo'linadi?
bir qiymatli va ko'p qiymatli shifrlash
ko'p qiymatli shifrlash
bir qiymatli shifrlash
uzluksiz qiymatli shifrlash

**№ 21.**

**Manba:** Z.T. Xudoyqulov, Sh.Z. Islomov, U.R. Mardiyev. "Kriptografiya 1: o'quv qo'llanma" – Тошкент, 2021 – 206 bet.

**Qiyinlik darajasi – 1**

Bir qiymatli shifrlash qanday amalga oshiriladi?
ochiq ma'lumot alfaviti belgilarining har biriga shifr ma'lumot alfavitining bitta belgisi mos qo'yiladi
ochiq ma'lumot alfaviti belgilarining har biriga shifr ma'lumot alfavitining ikkita yoki undan ortiq chekli sondagi belgilari mos qo'yiladi
ochiq ma'lumot alfaviti belgilarining har ikkitasiga shifr ma'lumot alfavitining ikkita yoki undan ortiq chekli sondagi belgilari mos qo'yiladi
ochiq ma'lumot alfaviti belgilarining har juftiga shifr ma'lumot alfavitining bitta belgisi mos qo'yiladi

**№ 22.**

**Manba:** Z.T. Xudoyqulov, Sh.Z. Islomov, U.R. Mardiyev. "Kriptografiya 1: o'quv qo'llanma" – Тошкент, 2021 – 206 bet.

**Qiyinlik darajasi – 1**

Ko'p qiymatli shifrlash qanday amalga oshiriladi?
ochiq ma'lumot alfaviti belgilarining har biriga shifr ma'lumot alfavitining ikkita yoki undan ortiq chekli sondagi belgilari mos qo'yiladi
ochiq ma'lumot alfaviti belgilarining har ikkitasiga shifr ma'lumot alfavitining ikkita yoki undan ortiq chekli sondagi belgilari mos qo'yiladi

ochiq ma'lumot alfaviti belgilarining har biriga shifr ma'lumot alfavitining bitta belgisi mos qo'yiladi
ochiq ma'lumot alfaviti belgilarining har juftiga shifr ma'lumot alfavitining bitta belgisi mos qo'yiladi

### **№ 23.**

**Manba:** Kiberxavfsizlik asoslari: O'quv qo'llanma/S.K.Ganiev, A.A.Ganiev, Z.T.Xudoyqulov; – T.: "Iqtisod-Moliya", 2021. – 228 b..

#### **Qiyinlik darajasi – 1**

A5/1 oqimli shifrlash algoritmi asosan qayerda qo'llaniladi?
mobil aloqa standarti GSM protokolida
simsiz aloqa vositalaridagi mavjud WEP protokolida
internet trafiklarini shifrlashda
radioaloqa tarmoqlarida

### **№ 24.**

**Manba:** Z.T. Xudoyqulov, Sh.Z. Islomov, U.R. Mardiyev. "Kriptografiya 1: o'quv qo'llanma" – Тошкент, 2021 – 206 bet.

#### **Qiyinlik darajasi – 1**

RC4 oqimli shifrlash algoritmi asosan qayerda qo'llaniladi?
simsiz aloqa vositalaridagi mavjud WEP protokolida
mobil aloqa standarti GSM protokolida
internet trafiklarini shifrlashda
radioaloqa tarmoqlarda

### **№ 25.**

**Manba:** Z.T. Xudoyqulov, Sh.Z. Islomov, U.R. Mardiyev. "Kriptografiya 1: o'quv qo'llanma" – Тошкент, 2021 – 206 bet.

#### **Qiyinlik darajasi – 1**

A5/1 oqimli shifrlash algoritmida dastlabki kalit uzunligi nechi bitga teng?
64
512
192

**№ 26.**

**Manba:** Z.T. Xudoyqulov, Sh.Z. Islomov, U.R. Mardiyev. “Kriptografiya 1: o’quv qo’llanma” – Toshkent, 2021 – 206 bet.

**Qiyinlik darajasi – 1**

A5/1 oqimli shifrlash algoritmda har bir qadamda kalit oqimining qanday qiymatini hosil qiladi?
bir biti
bir bayti
64 biti
8 bayti

**№ 27.**

**Manba:** Z.T. Xudoyqulov, Sh.Z. Islomov, U.R. Mardiyev. “Kriptografiya 1: o’quv qo’llanma” – Toshkent, 2021 – 206 bet.

**Qiyinlik darajasi – 1**

RC4 oqimli shifrlash algoritmda har bir qadamda kalit oqimining qanday qiymatini hosil qiladi?
bir baytini
bir bitini
64 bitini
8 baytini

**№ 28.**

**Manba:** Z.T. Xudoyqulov, Sh.Z. Islomov, U.R. Mardiyev. “Kriptografiya 1: o’quv qo’llanma” – Toshkent, 2021 – 206 bet.

**Qiyinlik darajasi – 1**

Blokli shifrlash algoritmlari arxitekturasini jihatidan qanday tarmoqlarga bo’linadi?
Feystel va SP
SP va Petri
Feystel va Petri
Kvadrat va iyerarxik

**№ 29.**

**Manba:** Kiberxavfsizlik asoslari: O'quv qo'llanma/S.K.Ganiev, A.A.Ganiev, Z.T.Xudoyqulov; – T.: "Iqtisod-Moliya", 2021. – 228 b..

**Qiyinlik darajasi – 1**

RSA algoritmining mualliflarini ko'rsating
R. Rayvest, A. Shamir, L. Adleman
Diffi va M. Xellman
R. Rayvest, K. Xellman, L. Adleman
L. Adleman, El Gamal, K. Shnorrr

**№ 30.**

**Manba:** Kiberxavfsizlik asoslari: O'quv qo'llanma/S.K.Ganiev, A.A.Ganiev, Z.T.Xudoyqulov; – T.: "Iqtisod-Moliya", 2021. – 228 b..

**Qiyinlik darajasi – 1**

Ochiq kalitli shifrlash algoritmi keltirilgan qatorni toping?
RSA
AES
DES
RC4

**№ 31.**

**Manba:** Kiberxavfsizlik asoslari: O'quv qo'llanma/S.K.Ganiev, A.A.Ganiev, Z.T.Xudoyqulov; – T.: "Iqtisod-Moliya", 2021. – 228 b..

**Qiyinlik darajasi – 2**

Ochiq kalitli shifrlash algoritmi keltirilgan qatorni toping?
El-Gamal
AES
DES
RC4

**№ 32.**

**Manba:** Kiberxavfsizlik asoslari: O'quv qo'llanma/S.K.Ganiev, A.A.Ganiev, Z.T.Xudoyqulov; – T.: "Iqtisod-Moliya", 2021. – 228 b..

**Qiyinlik darajasi – 2**

DES shifrlash algoritmda raundlar soni nechta?
16
32
64
128

**№ 33.**

**Manba:** Kiberxavfsizlik asoslari: O'quv qo'llanma/S.K.Ganiev, A.A.Ganiev, Z.T.Xudoyqulov; – T.: "Iqtisod-Moliya", 2021. – 228 b..

**Qiyinlik darajasi – 2**

DES shifrlash algoritmda kalit uzunligi necha bitga teng?
56
512
192
256

**№ 34.**

**Manba:** Z.T. Xudoyqulov, Sh.Z. Islomov, U.R. Mardiyev. "Kriptografiya 1: o'quv qo'llanma" – Тошкент, 2021 – 206 bet.

**Qiyinlik darajasi – 2**

DES shifrlash algoritmda har bir raunda necha bitli raund kalitlaridan foydalaniladi?
48
56
64
32

**№ 35.**

**Manba:** Z.T. Xudoyqulov, Sh.Z. Islomov, U.R. Mardiyev. "Kriptografiya 1: o'quv qo'llanma" – Тошкент, 2021 – 206 bet.

**Qiyinlik darajasi – 2**

AES algoritmda shifrlash kalitining uzunligi necha bitga teng?
--

128, 192, 256 bit
128, 156, 256 bit
128, 192 bit
256, 512 bit

### № 36.

**Manba:** Z.T. Xudoyqulov, Sh.Z. Islomov, U.R. Mardiyev. “Kriptografiya 1: o’quv qo’llanma” – Toshkent, 2021 – 206 bet.

### Qiyinlik darajasi – 2

AES shifrlash algoritmda raundlar soni nechaga teng bo’ladi?
10,12,14
14, 16, 18
18, 20, 22
22, 24, 26

### № 37.

**Manba:** Z.T. Xudoyqulov, Sh.Z. Islomov, U.R. Mardiyev. “Kriptografiya 1: o’quv qo’llanma” – Toshkent, 2021 – 206 bet.

### Qiyinlik darajasi – 2

AES algoritmda raundlar soni nimaga bo’g’liq?
kalit uzunligiga
kiruvchi blok uzunligi va matn qiymatiga
foydalanilgan vaqtiga
kiruvchi blok uzunligiga

### № 38.

**Manba:** Z.T. Xudoyqulov, Sh.Z. Islomov, U.R. Mardiyev. “Kriptografiya 1: o’quv qo’llanma” – Toshkent, 2021 – 206 bet.

### Qiyinlik darajasi – 2

AES algoritmda nechta akslantirishlardan foydalaniladi?
4
2

5
6

### № 39.

**Manba:** Z.T. Xudoyqulov, Sh.Z. Islomov, U.R. Mardiyev. “Kriptografiya 1: o’quv qo’llanma” – Toshkent, 2021 – 206 bet.

### Qiyinlik darajasi – 2

Qanday funksiyalarga xesh funksiya deyiladi?
ixtiyoriy uzunlikdagi ma’lumotni biror fiksirlangan uzunlikga o’tkazuvchi funksiyaga aytiladi
ixtiyoriy uzunlikdagi ma’lumotni bit yoki baytlarini zichlashtirib beruvchi funksiyaga aytiladi
ma’lumot bitlarini boshqa qiymatlarga almashtiruvchi funksiyaga aytiladi
ma’lumot baytlarini boshqa qiymatlarga almashtiruvchi funksiyaga aytiladi

### № 40.

**Manba:** Z.T. Xudoyqulov, Sh.Z. Islomov, U.R. Mardiyev. “Kriptografiya 1: o’quv qo’llanma” – Toshkent, 2021 – 206 bet.

### Qiyinlik darajasi – 2

Xesh funksiyalar qanday maqsadlarda ishlatiladi?
ma’lumotni to’liqligini nazoratlash va ma’lumot manbaini autentifikatsiyalashda
ma’lumotni maxfiyligini nazoratlash va ma’lumot manbaini haqiqiyligini tekshirishda
ma’lumotni butunligini nazoratlashda
ma’lumot manbaini autentifikatsiyalashda

### № 41.

**Manba:** Z.T. Xudoyqulov, Sh.Z. Islomov, U.R. Mardiyev. “Kriptografiya 1: o’quv qo’llanma” – Toshkent, 2021 – 206 bet.

### Qiyinlik darajasi – 2

Xesh qiymatlarni yana qanday atash mumkin?
dayjest
funksiya
imzo
raqamli imzo

**№ 42.**

**Manba:** Z.T. Xudoyqulov, Sh.Z. Islomov, U.R. Mardiyev. “Kriptografiya 1: o’quv qo’llanma” – Toshkent, 2021 – 206 bet.

**Qiyinlik darajasi – 2**

Quyida keltirilgan xususiyatlarning qaysilari xesh funksiyaga mos?
chiqishda fiksirlangan uzunlikdagi qiymatni beradi
chiqishda bir xil qiymatni beradi
chiqishdagi qiymat bilan kiruvchi qiymatlar bir xil bo’ladi
kolliziyaga ega

**№ 43.**

**Manba:** Z.T. Xudoyqulov, Sh.Z. Islomov, U.R. Mardiyev. “Kriptografiya 1: o’quv qo’llanma” – Toshkent, 2021 – 206 bet.

**Qiyinlik darajasi – 2**

Quyida keltirilgan xususiyatlarning qaysilari xesh funksiyaga mos?
ixtiyoriy olingan har xil matn uchun xesh qiymatlar bir xil bo’lmaydi
ixtiyoriy olingan bir xil matn uchun qiymatlar bir xil bo’lmaydi
ixtiyoriy olingan har xil matn uchun xesh qiymatlar bir xil bo’ladi
ixtiyoriy olingan har xil xesh qiymat uchun dastlabki ma’lumotlar bir xil bo’ladi

**№ 44.**

**Manba:** Z.T. Xudoyqulov, Sh.Z. Islomov, U.R. Mardiyev. “Kriptografiya 1: o’quv qo’llanma” – Toshkent, 2021 – 206 bet.

**Qiyinlik darajasi – 2**

Kolliziya deb nima nisbatan aytiladi?
ikkita har xil matn uchun bir xil xesh qiymat mos kelishi
ikkita bir xil matn uchun bir xil xesh qiymat mos kelishi
ikkita har xil matn uchun har xil xesh qiymat mos kelishi
ikkita bir xil matn uchun bir xil xesh qiymat mos kelmasligiga

**№ 45.**

**Manba:** Z.T. Xudoyqulov, Sh.Z. Islomov, U.R. Mardiyev. “Kriptografiya 1: o’quv qo’llanma” – Toshkent, 2021 – 206 bet.



### Qiyinlik darajasi – 2

Xesh funksiyalarga qanday turlarga bo'linadi?
kalitli va kalitsiz xesh funksiyalarga
kalitli va kriptografik bo'lmagan xesh funksiyalarga
kalitsiz va kriptografik bo'lmagan xesh funksiyalarga
kriptografik va kriptografik bo'lmagan xesh funksiyalarga

#### № 46.

**Manba:** Z.T. Xudoyqulov, Sh.Z. Islomov, U.R. Mardiyev. “Kriptografiya 1: o'quv qo'llanma” – Тошкент, 2021 – 206 bet.

### Qiyinlik darajasi – 2

Ma'lumotlarni autentifikatsiyalash kodlari deb qanday xesh funksiyalarga aytiladi?
kalitli xesh funksiyalarga
kalitsiz xesh funksiyalarga
kriptografik bo'lmagan xesh funksiyalarga
kriptografik xesh funksiyalarga

#### № 47.

**Manba:** Z.T. Xudoyqulov, Sh.Z. Islomov, U.R. Mardiyev. “Kriptografiya 1: o'quv qo'llanma” – Тошкент, 2021 – 206 bet.

### Qiyinlik darajasi – 2

CRC-3 tizimida CRC qiymatini hisoblash jarayonida ma'lumotga nechta nol biriktiriladi?
3
6
9
12

#### № 48.

**Manba:** Z.T. Xudoyqulov, Sh.Z. Islomov, U.R. Mardiyev. “Kriptografiya 1: o'quv qo'llanma” – Тошкент, 2021 – 206 bet.

### Qiyinlik darajasi – 2

CRC-4 tizimida CRC qiymatini hisoblash jarayonida ma'lumotga nechta nol biriktiriladi?
--

4
8
12
16

**№ 49.**

**Manba:** Z.T. Xudoyqulov, Sh.Z. Islomov, U.R. Mardiyev. “Kriptografiya 1: o’quv qo’llanma” – Toshkent, 2021 – 206 bet.

**Qiyinlik darajasi – 2**

CRC-5 tizimida CRC qiymati hisoblash jarayonida ma’lumotga nechta nol biriktiriladi?
5
10
15
20

**№ 50.**

**Manba:** Z.T. Xudoyqulov, Sh.Z. Islomov, U.R. Mardiyev. “Kriptografiya 1: o’quv qo’llanma” – Toshkent, 2021 – 206 bet.

**Qiyinlik darajasi – 2**

CRC-6 tizimida CRC qiymati hisoblash jarayonida ma’lumotga nechta nol biriktiriladi?
6
12
18
24

**№ 51.**

**Manba:** Z.T. Xudoyqulov, Sh.Z. Islomov, U.R. Mardiyev. “Kriptografiya 1: o’quv qo’llanma” – Toshkent, 2021 – 206 bet.

**Qiyinlik darajasi – 2**

Qaysi maxfiylikni ta’minlash usulida kalitdan foydalanilmaydi?
kodlash
shifrlash

steganografiya
autentifikatsiya

### № 52.

**Manba:** Z.T. Xudoyqulov, Sh.Z. Islomov, U.R. Mardiyev. “Kriptografiya 1: o’quv qo’llanma” – Toshkent, 2021 – 206 bet.

### Qiyinlik darajasi – 2

Ximoyalanuvchi ma’lumot boshqa bir ma’lumotni ichiga yashirish orqali maxfiyligini ta’minlaydigan usul qaysi?
steganografiya
kodlash
shifrlash
autentifikatsiya

### № 53.

**Manba:** Z.T. Xudoyqulov, Sh.Z. Islomov, U.R. Mardiyev. “Kriptografiya 1: o’quv qo’llanma” – Toshkent, 2021 – 206 bet.

### Qiyinlik darajasi – 2

Baytlar kesimida shifrlashni amalga oshiradigan algoritm keltirilgan qatorni ko’rsating?
RC4
A5/1
SHA1
MD5

### № 54.

**Manba:** Z.T. Xudoyqulov, Sh.Z. Islomov, U.R. Mardiyev. “Kriptografiya 1: o’quv qo’llanma” – Toshkent, 2021 – 206 bet.

### Qiyinlik darajasi – 2

Bitlar kesimida shifrlashni amalga oshiradigan algoritm keltirilgan qatorni ko’rsating?
A5/1
RC4
SHA1
MD5

**№ 55.**

**Manba:** Z.T. Xudoyqulov, Sh.Z. Islomov, U.R. Mardiyev. “Kriptografiya 1: o’quv qo’llanma” – Toshkent, 2021 – 206 bet.

**Qiyinlik darajasi – 2**

Qaysi hujum turida barcha bo’lishi mumkin bo’lgan variantlar ko’rib chiqiladi?
qo’pol kuch hujumi
chastotalar tahlili
analitik hujum
sotsial injineriya

**№ 56.**

**Manba:** Z.T. Xudoyqulov, Sh.Z. Islomov, U.R. Mardiyev. “Kriptografiya 1: o’quv qo’llanma” – Toshkent, 2021 – 206 bet.

**Qiyinlik darajasi – 2**

Sezar shifrlash algoritmi qaysi turdagi akslantirishga asoslangan?
o’rniga qo’yish
o’rin almashtirish
kompozitsion
aralash

**№ 57.**

**Manba:** Z.T. Xudoyqulov, Sh.Z. Islomov, U.R. Mardiyev. “Kriptografiya 1: o’quv qo’llanma” – Toshkent, 2021 – 206 bet.

**Qiyinlik darajasi – 2**

Vijiner shifrlash algoritmi qaysi turdagi akslantirishga asoslanadi?
o’rniga qo’yish
o’rin almashtirish
kompozitsion
aralash

**№ 58.**

**Manba:** Z.T. Xudoyqulov, Sh.Z. Islomov, U.R. Mardiyev. “Kriptografiya 1: o’quv qo’llanma” – Тошкент, 2021 – 206 bet.

**Qiyinlik darajasi – 2**

A5/1 oqimli shifrlash algoritmda registrlarning surilishi qanday kattalikka bog’liq?
maj funksiyasi qiymatiga
kalit qiymatiga
registr uzunligi qiymatiga
hech qanday kattalikka bog’liq emas

**№ 59.**

**Manba:** Z.T. Xudoyqulov, Sh.Z. Islomov, U.R. Mardiyev. “Kriptografiya 1: o’quv qo’llanma” – Тошкент, 2021 – 206 bet.

**Qiyinlik darajasi – 2**

16 raund davom etadigan blokli shifrlash algoritmi ko’rsating?
DES
AES
A5/1
RC4

**№ 60.**

**Manba:** Z.T. Xudoyqulov, Sh.Z. Islomov, U.R. Mardiyev. “Kriptografiya 1: o’quv qo’llanma” – Тошкент, 2021 – 206 bet.

**Qiyinlik darajasi – 2**

10 raund davom etadigan blokli shifrlash algoritmi ko’rsating?
AES
DES
A5/1
RC4

**№ 61.**

**Manba:** Z.T. Xudoyqulov, Sh.Z. Islomov, U.R. Mardiyev. “Kriptografiya 1: o’quv qo’llanma” – Тошкент, 2021 – 206 bet.

**Qiyinlik darajasi – 2**

Qanday algoritmlarda chiqishda doim fiksirlangan uzunlikdagi qiymat chiqadi?
xesh algoritmlarda
shifrlash algoritmlarida
kodlash algoritmlarida
steganografik algoritmlarda

### № 62.

**Manba:** Z.T. Xudoyqulov, Sh.Z. Islomov, U.R. Mardiyev. “Kriptografiya 1: o’quv qo’llanma” – Тошкент, 2021 – 206 bet.

### Qiyinlik darajasi – 2

Vernam shifrlash algoritmi asosi qaysi mantiqiy hisoblashga asoslangan
XOR
ARX
ROX
XRA

### № 63.

**Manba:** Z.T. Xudoyqulov, Sh.Z. Islomov, U.R. Mardiyev. “Kriptografiya 1: o’quv qo’llanma” – Тошкент, 2021 – 206 bet.

### Qiyinlik darajasi – 2

Chastotalar tahlili kriptotahlil usuli samarali ishlidigan algorimtlar keltirilgan qatorni belgilang?
Sezar, Affin
Vernam
Vijiner
RC4

### № 64.

**Manba:** Z.T. Xudoyqulov, Sh.Z. Islomov, U.R. Mardiyev. “Kriptografiya 1: o’quv qo’llanma” – Тошкент, 2021 – 206 bet.

### Qiyinlik darajasi – 2

Simmetrik shifrlash algorimtlarida qanday muammo mavjud?
kalitni uzatish

kalit generatsiyalash
kalitni saqlash
kalitni yo'q qilish

#### **№ 65.**

**Manba:** Z.T. Xudoyqulov, Sh.Z. Islomov, U.R. Mardiyev. “Kriptografiya 1: o’quv qo’llanma” – Тошкент, 2021 – 206 bet.

#### **Qiyinlik darajasi – 2**

Konfidensiallikni ta’minlash bu -?
ruxsat etilmagan “o’qishdan” himoyalash
ruxsat etilmagan “yozishdan” himoyalash
ruxsat etilmagan “bajarishdan” himoyalash
ruxsat berilgan “amallarni” bajarish

#### **№ 66.**

**Manba:** Z.T. Xudoyqulov, Sh.Z. Islomov, U.R. Mardiyev. “Kriptografiya 1: o’quv qo’llanma” – Тошкент, 2021 – 206 bet.

#### **Qiyinlik darajasi – 2**

Foydalanuvchanlikni ta’minlash bu-?
ruxsat etilmagan “bajarishdan” himoyalash
ruxsat etilmagan “yozishdan” himoyalash
ruxsat etilmagan “o’qishdan” himoyalash
ruxsat berilgan “amallarni” bajarish

#### **№ 67.**

**Manba:** Z.T. Xudoyqulov, Sh.Z. Islomov, U.R. Mardiyev. “Kriptografiya 1: o’quv qo’llanma” – Тошкент, 2021 – 206 bet.

#### **Qiyinlik darajasi – 2**

Butunlikni ta’minlash bu - ?
ruxsat etilmagan “yozishdan” himoyalash
ruxsat etilmagan “bajarishdan” himoyalash

ruxsat etilmagan “o’qishdan” himoyalash
ruxsat berilgan “amallarni” bajarish

### № 68.

**Manba:** Z.T. Xudoyqulov, Sh.Z. Islomov, U.R. Mardiyev. “Kriptografiya 1: o’quv qo’llanma” – Toshkent, 2021 – 206 bet.

### Qiyinlik darajasi – 2

.... kriptotizimni shifrlash va rasshifrovkalash uchun sozlashda foydalaniladi.
kalit
ochiq matn
alifbo
algoritm

### № 69.

**Manba:** Z.T. Xudoyqulov, Sh.Z. Islomov, U.R. Mardiyev. “Kriptografiya 1: o’quv qo’llanma” – Toshkent, 2021 – 206 bet.

### Qiyinlik darajasi – 2

Agar ochiq ma’lumot shifrlansa, natijasi .... bo’ladi.
shifrmtn
ochiq matn
noma’lum
kod

### № 70.

**Manba:** Z.T. Xudoyqulov, Sh.Z. Islomov, U.R. Mardiyev. “Kriptografiya 1: o’quv qo’llanma” – Toshkent, 2021 – 206 bet.

### Qiyinlik darajasi – 2

Rasshifrovkalash jarayonida kalit va ..... kerak bo’ladi
shifrmtn
ochiq matn
kodlash
alifbo

### № 71.



**Manba:** Z.T. Xudoyqulov, Sh.Z. Islomov, U.R. Mardiyev. “Kriptografiya 1: o’quv qo’llanma” – Toshkent, 2021 – 206 bet.

**Qiyinlik darajasi – 3**

Ma’lumotni sakkizlik sanoq tizimidan o’n oltilik sanoq tizimiga o’tkazish bu?
kodlash
shifrlash
yashirish
rasshifrovkalash

**№ 72.**

**Manba:** Z.T. Xudoyqulov, Sh.Z. Islomov, U.R. Mardiyev. “Kriptografiya 1: o’quv qo’llanma” – Toshkent, 2021 – 206 bet.

**Qiyinlik darajasi – 3**

Ma’lumotni shifrlash va deshifrlash uchun bir xil kalitdan foydalanuvchi tizim bu?
simmetrik kriptotizim
ochiq kalitli kriptotizim
assimetrik kriptotizim
xesh funksiyalar

**№ 73.**

**Manba:** Д.Е. Акбаров. Ахборот хавфсизлигини таъминлашнинг криптографик усуллари ва уларнинг қўлланишлари. Тошкент. “Ўзбекистон маркаси”, 2009. – 432 б.

**Qiyinlik darajasi – 3**

Ikki kalitli deyilganda qaysi kriptotizim nazarda tutiladi?
ochiq kalitli kriptotizim
simmetrik kriptotizim
xesh funksiyalar
MAC tizimlari

**№ 74.**

**Manba:** Z.T. Xudoyqulov, Sh.Z. Islomov, U.R. Mardiyev. “Kriptografiya 1: o’quv qo’llanma” – Toshkent, 2021 – 206 bet.

**Qiyinlik darajasi – 3**

Ma'lumotni mavjudligini yashirishni maqsad qilgan bilim sohasi bu?
steganografiya
kriptografiya
kodlash
kriptotahlil

**№ 75.**

**Manba:** Z.T. Xudoyqulov, Sh.Z. Islomov, U.R. Mardiyev. "Kriptografiya 1: o'quv qo'llanma" – Тошкент, 2021 – 206 bet.

**Qiyinlik darajasi – 3**

Ma'lumotni konfidensialligini ta'minlash uchun ..... zarur.
shifrlash
kodlash
deshifrlash
rasshifrovkalash

**№ 76.**

**Manba:** Z.T. Xudoyqulov, Sh.Z. Islomov, U.R. Mardiyev. "Kriptografiya 1: o'quv qo'llanma" – Тошкент, 2021 – 206 bet.

**Qiyinlik darajasi – 3**

Ma'lumotni uzatishda kriptografik himoya .....
konfidensiallik va yaxlitlikni ta'minlaydi
konfidensiallik va foydalanuvchanlikni ta'minlaydi
foydalanuvchanlik va butunlikni ta'minlaydi
konfidensiallikni ta'minlaydi

**№ 77.**

**Manba:** Z.T. Xudoyqulov, Sh.Z. Islomov, U.R. Mardiyev. "Kriptografiya 1: o'quv qo'llanma" – Тошкент, 2021 – 206 bet.

**Qiyinlik darajasi – 3**

Qadimiy davr klassik shifriga quyidagilarning qaysi biri tegishli?
Sezar

kodlar kitobi
Enigma shifri
DES, AES shifri

### № 78.

**Manba:** .E. Акбаров. Ахборот хавфсизлигини таъминлашнинг криптографик усуллари ва уларнинг қўлланишлари. Тошкент. "Ўзбекистон маркаси ", 2009. – 432 б.

### Qiyinlik darajasi – 3

Kompyuter davriga tegishli shifrlarni aniqlang?
DES, AES shifri
kodlar kitobi
Sezar
Enigma shifri

### № 79.

**Manba:** Z.T. Xudoyqulov, Sh.Z. Islomov, U.R. Mardiyev. "Kriptografiya 1: o'quv qo'llanma" – Тошкент, 2021 – 206 bet.

### Qiyinlik darajasi – 3

.... shifrlar blokli va oqimli turlarga ajratiladi
simmetrik
ochiq kalitli
assimetrik
klassik

### № 80.

**Manba:** Z.T. Xudoyqulov, Sh.Z. Islomov, U.R. Mardiyev. "Kriptografiya 1: o'quv qo'llanma" – Тошкент, 2021 – 206 bet.

### Qiyinlik darajasi – 3

Tasodifiy ketma-ketliklarni generatsiyalashga asoslangan shifrlash turi bu?
oqimli shifrlar
blokli shifrlar
ochiq kalitli shifrlar

**№ 81.**

**Manba:** Z.T. Xudoyqulov, Sh.Z. Islomov, U.R. Mardiyev. “Kriptografiya 1: o’quv qo’llanma” – Тошкент, 2021 – 206 bet.

**Qiyinlik darajasi – 3**

Ochiq matn qismlarini takror shifrlashga asoslangan usul bu?
blokli shifrlar
oqimli shifrlar
ochiq kalitli shifrlar
assimetrik shifrlar

**№ 82.**

**Manba:** Z.T. Xudoyqulov, Sh.Z. Islomov, U.R. Mardiyev. “Kriptografiya 1: o’quv qo’llanma” – Тошкент, 2021 – 206 bet.

**Qiyinlik darajasi – 3**

A5/1 shifri qaysi turga mansub?
oqimli shifrlar
blokli shifrlar
ochiq kalitli shifrlar
assimetrik shifrlar

**№ 83.**

**Manba:** Z.T. Xudoyqulov, Sh.Z. Islomov, U.R. Mardiyev. “Kriptografiya 1: o’quv qo’llanma” – Тошкент, 2021 – 206 bet.

**Qiyinlik darajasi – 3**

Qaysi algoritmlar simmetrik blokli shifrlarga tegishli?
AES, DES
A5/1, AES
Sezar, AES
Vijiner, DES

**№ 84.**

**Manba:** Z.T. Xudoyqulov, Sh.Z. Islomov, U.R. Mardiyev. “Kriptografiya 1: o’quv qo’llanma” – Тошкент, 2021 – 206 bet.

**Qiyinlik darajasi – 3**

Simmetrik kriptotizimlarning asosiy kamchiligi bu?
kalitni taqsimlash zaruriyati
shifrlash jarayonining ko’p vaqt olishi
kalitlarni esda saqlash murakkabligi
algoritmning xavfsiz emasligi

**№ 85.**

**Manba:** Z.T. Xudoyqulov, Sh.Z. Islomov, U.R. Mardiyev. “Kriptografiya 1: o’quv qo’llanma” – Тошкент, 2021 – 206 bet.

**Qiyinlik darajasi – 3**

Faqat simmetrik blokli shifrlarga xos bo’lgan atamani aniqlang?
blok uzunligi
kalit uzunligi
ochiq kalit
kodlash jadvali

**№ 86.**

**Manba:** Z.T. Xudoyqulov, Sh.Z. Islomov, U.R. Mardiyev. “Kriptografiya 1: o’quv qo’llanma” – Тошкент, 2021 – 206 bet.

**Qiyinlik darajasi – 3**

Sezar shifrlash usuli qaysi akslantirishga asoslangan?
o’rniga qo’yish
o’rin almashtirish
ochiq kalitli shifrlarga
kombinatsion akslantirishga

**№ 87.**

**Manba:** Z.T. Xudoyqulov, Sh.Z. Islomov, U.R. Mardiyev. “Kriptografiya 1: o’quv qo’llanma” – Тошкент, 2021 – 206 bet.

**Qiyinlik darajasi – 3**

Kerxgofs prinsipiga ko'ra kriptotizimning to'liq xavfsiz bo'lishi faqat qaysi kattalik nomalum bo'lishiga asoslanishi kerak?
kalit
algoritm
shifrmata
protokol

### **№ 88.**

**Manba:** Z.T. Xudoyqulov, Sh.Z. Islomov, U.R. Mardiyev. "Kriptografiya 1: o'quv qo'llanma" – Toshkent, 2021 – 206 bet.

### **Qiyinlik darajasi – 3**

Shifrlash va deshifrlashda alohida kalitlardan foydalanuvchi kriptotizimlar bu?
ochiq kalitli kriptotizimlar
simmetrik kriptotizimlar
bir kalitli kriptotizimlar
xesh funksiyalar

### **№ 89.**

**Manba:** Z.T. Xudoyqulov, Sh.Z. Islomov, U.R. Mardiyev. "Kriptografiya 1: o'quv qo'llanma" – Toshkent, 2021 – 206 bet.

### **Qiyinlik darajasi – 3**

Simmetrik shifrlar axborotni qaysi xususiyatlarini ta'minlashda foydalaniladi?
konfidensiallik va yaxlitlik
konfidensiallik va foydalanuvchanlik
foydalanuvchanlik va yaxlitlik
foydalanuvchanlik

### **№ 90.**

**Manba:** Z.T. Xudoyqulov, Sh.Z. Islomov, U.R. Mardiyev. "Kriptografiya 1: o'quv qo'llanma" – Toshkent, 2021 – 206 bet.

### **Qiyinlik darajasi – 3**

Ochiq kalitli shifrlar axborotni qaysi xususiyatlarini ta'minlashda foydalaniladi?
konfidensiallik va yaxlitlik

konfidensiallik va foydalanuvchanlik
foydalanuvchanlik va yaxlitlik
foydalanuvchanlik

### **№ 91.**

**Manba:** Z.T. Xudoyqulov, Sh.Z. Islomov, U.R. Mardiyev. “Kriptografiya 1: o’quv qo’llanma” – Тошкент, 2021 – 206 bet.

### **Qiyinlik darajasi – 3**

Xesh funksiyaga tegishli bo’lgan talabni aniqlang?
bir tomonlama funksiya bo’lishi
kolliziyaga bardoshli bo’lmasligi
turli kirishlar bir xil chiqishlarni akslantirishi
chiqishda ixtiyoriy uzunlikda bo’lishi

### **№ 92.**

**Manba:** Z.T. Xudoyqulov, Sh.Z. Islomov, U.R. Mardiyev. “Kriptografiya 1: o’quv qo’llanma” – Тошкент, 2021 – 206 bet.

### **Qiyinlik darajasi – 3**

Ochiq kalitli shifrlashda deshifrlash qaysi kalit asosida amalga oshiriladi?
shaxsiy kalit
ochiq kalit
kalitdan foydalanilmaydi
umumiy kalit

### **№ 93.**

**Manba:** Z.T. Xudoyqulov, Sh.Z. Islomov, U.R. Mardiyev. “Kriptografiya 1: o’quv qo’llanma” – Тошкент, 2021 – 206 bet.

### **Qiyinlik darajasi – 3**

Quyidagi ta’rif qaysi atamaga tegishli: “maxfiy kodlarni”ni yaratish bilan shug’ullanadigan soha-bu?
kriptografiya
kriptologiya
kriptotahlil

kripto
--------

**№ 94.**

**Manba:** Z.T. Xudoyqulov, Sh.Z. Islomov, U.R. Mardiyev. “Kriptografiya 1: o’quv qo’llanma” – Toshkent, 2021 – 206 bet.

**Qiyinlik darajasi – 3**

Quyidagi ta’rif qaysi atamaga tegishli: “maxfiy kodlarni”ni buzish bilan shug’ullanadigan soha-bu?
kriptotahlil
kriptografiya
kriptologiya
kripto

**№ 95.**

**Manba:** Z.T. Xudoyqulov, Sh.Z. Islomov, U.R. Mardiyev. “Kriptografiya 1: o’quv qo’llanma” – Toshkent, 2021 – 206 bet.

**Qiyinlik darajasi – 3**

Kriptotizimni boshqaradigan vosita?
kalit
algoritm
stegokalit
kriptotizim boshqarilmaydi

**№ 96.**

**Manba:** Z.T. Xudoyqulov, Sh.Z. Islomov, U.R. Mardiyev. “Kriptografiya 1: o’quv qo’llanma” – Toshkent, 2021 – 206 bet.

**Qiyinlik darajasi – 3**

Quyidagi ta’rif qaysi kriptotizimga tegishli: ochiq matnni shifrlashda hamda rasshifrovkalashda bitta maxfiy kalitdan foydalaniladi?
simmetrik kriptotizimlar
nosimmetrik kriptotizimlar
ochiq kalitli kriptotizimlar
assimetrik kriptotizimlar



**№ 97.**

**Manba:** Z.T. Xudoyqulov, Sh.Z. Islomov, U.R. Mardiyev. "Kriptografiya 1: o'quv qo'llanma" – Toshkent, 2021 – 206 bet.

**Qiyinlik darajasi – 3**

Quyidagi ta'rif qaysi kriptotizimga tegishli: ochiq matnni shifrlashda hamda rasshifrovkalashda mos holda ochiq va maxfiy kalitdan foydalanadi?
ochiq kalitli kriptotizimlar
maxfiy kalitli kriptotizimlar
simmetrik kriptotizimlar
elektron raqamli imzo tizimlari

**№ 98.**

**Manba:** .E. Akbarov. Axborot xavfsizligini ta'minlashning kriptografik usullari va ularning qullanihlari. Toshkent. "Ўзбекистон маркаси ", 2009. – 432 б.

**Qiyinlik darajasi – 3**

Xesh funksiyalar nima maqsadda foydalaniladi?
ma'lumotlar yaxlitligini ta'minlashda
ma'lumot egasini autentifikatsiyalashda
ma'lumot maxfiyligini ta'minlashda
ma'lumot manbaini autentifikatsiyalashda

**№ 99.**

**Manba:** Z.T. Xudoyqulov, Sh.Z. Islomov, U.R. Mardiyev. "Kriptografiya 1: o'quv qo'llanma" – Toshkent, 2021 – 206 bet.

**Qiyinlik darajasi – 3**

Chastotalar tahlili hujumi qanday amalga oshiriladi?
shifr matnda qatnashgan harflar sonini aniqlash orqali
shifr matnda eng kam qatnashgan harflarni aniqlash orqali
ochiq matnda qatnashgan harflar sonini aniqlash orqali
ochiq matnda eng kam qatnashgan harflarni aniqlash orqali

**№ 100.**

**Manba:** .E. Акбаров. Ахборот хавфсизлигини таъминлашнинг криптографик усуллари ва уларнинг қўлланишлари. Тошкент. "Ўзбекистон маркаси", 2009. – 432 б.

**Qiyinlik darajasi – 3**

Qanday algoritmlar qaytmas xususiyatiga ega hisoblanadi?
xesh funksiyalar
elektron raqamli imzo algoritmlari
simmetrik kriptotizimlar
ochiq kalitli kriptotizimlar

**№ 101.**

**Manba:** Z.T. Xudoyqulov, Sh.Z. Islomov, U.R. Mardiyev. "Kriptografiya 1: o'quv qo'llanma" – Тошкент, 2021 – 206 bet.

**Qiyinlik darajasi – 1**

RC4 shifrlash algoritmi qaysi turga mansub?
oqimli shifrlar
blokli shifrlar
ochiq kalitli shifrlar
assimetrik shifrlar

**№ 102.**

**Manba:** Z.T. Xudoyqulov, Sh.Z. Islomov, U.R. Mardiyev. "Kriptografiya 1: o'quv qo'llanma" – Тошкент, 2021 – 206 bet.

**Qiyinlik darajasi – 1**

Ma'lumotga elektron raqamli imzo qo'yish hamda uni tekshirish qanday amalga oshiriladi?
Ma'lumotga raqamli imzo qo'yish maxfiy kalit orqali, imzoni tekshirish ochiq kalit orqali amalga oshiriladi
Ma'lumotga raqamli imzo qo'yish ochiq kalit orqali, imzoni tekshirish maxfiy kalit orqali amalga oshiriladi
Ma'lumotga raqamli imzo qo'yish maxfiy kalit orqali, imzoni tekshirish yopiq kalit orqali amalga oshiriladi
Ma'lumotga raqamli imzo qo'yish hamda uni tekshirish maxfiy kalit orqali amalga oshiriladi

**№ 103.**

**Manba:** Z.T. Xudoyqulov, Sh.Z. Islomov, U.R. Mardiyev. “Kriptografiya 1: o’quv qo’llanma” – Тошкент, 2021 – 206 bet.

**Qiyinlik darajasi – 1**

ARX amali qaysi shifrlash algoritmlarida foydalaniladi?
Blokli shifrlashda
Ochiq kalitli shifrlashda
Assimetrik shifrlashda
Ikki kalitli shifrlashda

**№ 104.**

**Manba:** Z.T. Xudoyqulov, Sh.Z. Islomov, U.R. Mardiyev. “Kriptografiya 1: o’quv qo’llanma” – Тошкент, 2021 – 206 bet.

**Qiyinlik darajasi – 1**

Kerkxofs printsipi bo’yicha qanday taxminlar ilgari suriladi?
Kalitdan boshqa barcha ma’lumotlar barchaga ma’lum
Faqat kalit barchaga ma’lum
Barcha parametrlar barchaga ma’lum
Shifrlash kaliti barchaga ma’lum

**№ 105.**

**Manba:** Z.T. Xudoyqulov, Sh.Z. Islomov, U.R. Mardiyev. “Kriptografiya 1: o’quv qo’llanma” – Тошкент, 2021 – 206 bet.

**Qiyinlik darajasi – 1**

Qaysi algoritm har bir qadamda bir bayt qiymatni shifrlaydi?
RC4
A5/1
RSA
AES

**№ 106.**

**Manba:** Z.T. Xudoyqulov, Sh.Z. Islomov, U.R. Mardiyev. “Kriptografiya 1: o’quv qo’llanma” – Тошкент, 2021 – 206 bet.

**Qiyinlik darajasi – 1**

Qaysi algoritmda har bir qadamda bir bit qiymatni shifrlaydi?
A5/1
RC4
RSA
AES

**№ 107.**

**Manba:** Z.T. Xudoyqulov, Sh.Z. Islomov, U.R. Mardiyev. “Kriptografiya 1: o’quv qo’llanma” – Тошкент, 2021 – 206 bet.

**Qiyinlik darajasi – 1**

AES algoritmi qaysi tarmoq asosida qurilgan?
SP
Feistel
Petri
Petri va SP

**№ 108.**

**Manba:** Z.T. Xudoyqulov, Sh.Z. Islomov, U.R. Mardiyev. “Kriptografiya 1: o’quv qo’llanma” – Тошкент, 2021 – 206 bet.

**Qiyinlik darajasi – 1**

Elektron raqamli imzo bo’yicha birinchi O’z DSt 1092 qaysi korxona tomonidan ishlab chiqilgan?
UNICON.UZ
INFOCOM
UZTELECOM
O’zR axborot texnologiyalari va kommunikatsiyalarini rivojlantirish vazirligi

**№ 109.**

**Manba:** Z.T. Xudoyqulov, Sh.Z. Islomov, U.R. Mardiyev. “Kriptografiya 1: o’quv qo’llanma” – Тошкент, 2021 – 206 bet.

**Qiyinlik darajasi – 1**

AES shifrlash algoritmi nomini kengaytmasini ko’rsating?
Advanced Encryption Standard

Advanced Encoding Standard
Advanced Encryption Stadium
Always Encryption Standard

**№ 110.**

**Manba:** Z.T. Xudoyqulov, Sh.Z. Islomov, U.R. Mardiyev. “Kriptografiya 1: o’quv qo’llanma” – Toshkent, 2021 – 206 bet.

**Qiyinlik darajasi – 1**

A5/1 shifrlash algoritmi bu?
oqimli shifrlash algoritmi
ochiq kalitli shifrlash algoritmi
assimetrik shifrlash algoritmi
blokli shifrlash algoritmi

**№ 111.**

**Manba:** Z.T. Xudoyqulov, Sh.Z. Islomov, U.R. Mardiyev. “Kriptografiya 1: o’quv qo’llanma” – Toshkent, 2021 – 206 bet.

**Qiyinlik darajasi – 1**

RC4 shifrlash algoritmi bu?
oqimli shifrlash algoritmi
ochiq kalitli shifrlash algoritmi
asimetrik shifrlash algoritmi
blokli shifrlash algoritmi

**№ 112.**

**Manba:** Z.T. Xudoyqulov, Sh.Z. Islomov, U.R. Mardiyev. “Kriptografiya 1: o’quv qo’llanma” – Toshkent, 2021 – 206 bet.

**Qiyinlik darajasi – 1**

DES shifrlash algoritmi bu?
blokli shifrlash algoritmi
oqimli shifrlash algoritmi
ochiq kalitli shifrlash algoritmi

**№ 113.**

**Manba:** Z.T. Xudoyqulov, Sh.Z. Islomov, U.R. Mardiyev. “Kriptografiya 1: o’quv qo’llanma” – Тошкент, 2021 – 206 bet.

**Qiyinlik darajasi – 1**

AES shifrlash algoritmi bu?
blokli shifrlash algoritmi
oqimli shifrlash algoritmi
ochiq kalitli shifrlash algoritmi
asimetrik shifrlash algoritmi

**№ 114.**

**Manba:** Z.T. Xudoyqulov, Sh.Z. Islomov, U.R. Mardiyev. “Kriptografiya 1: o’quv qo’llanma” – Тошкент, 2021 – 206 bet.

**Qiyinlik darajasi – 1**

Simmetrik va ochiq kalitli kriptotizimlar asosan nimasi bilan bir biridan farq qiladi?
kalitlar soni bilan
matematik murakkabligi bilan
farq qilmaydi
biri maxfiylikni ta’minlasa, biri butunlikni ta’minlaydi

**№ 115.**

**Manba:** Z.T. Xudoyqulov, Sh.Z. Islomov, U.R. Mardiyev. “Kriptografiya 1: o’quv qo’llanma” – Тошкент, 2021 – 206 bet.

**Qiyinlik darajasi – 1**

Kriptotizimlar kalitlar soni bo’yicha nechta turga bo’linadi?
2
3
4
5

**№ 116.**

**Manba:** Z.T. Xudoyqulov, Sh.Z. Islomov, U.R. Mardiyev. “Kriptografiya 1: o’quv qo’llanma” – Тошкент, 2021 – 206 bet.

**Qiyinlik darajasi – 1**

A5/1 oqimli shifrlash algoritmida maxfiy kalit necha registrga bo’linadi?
3
4
5
6

**№ 117.**

**Manba:** T. Xudoyqulov, Sh.Z. Islomov, U.R. Mardiyev. “Kriptografiya 1: o’quv qo’llanma” – Тошкент, 2021 – 206 bet.

**Qiyinlik darajasi – 1**

A5/1 oqimli shifrlash algoritmida X registr uzunligi nechi bitga teng?
19
17
16
15

**№ 118.**

**Manba:** Z.T. Xudoyqulov, Sh.Z. Islomov, U.R. Mardiyev. “Kriptografiya 1: o’quv qo’llanma” – Тошкент, 2021 – 206 bet.

**Qiyinlik darajasi – 1**

A5/1 oqimli shifrlash algoritmida Y registr uzunligi nechi bitga teng?
22
21
19
20

**№ 119.**

**Manba:** Z.T. Xudoyqulov, Sh.Z. Islomov, U.R. Mardiyev. “Kriptografiya 1: o’quv qo’llanma” – Тошкент, 2021 – 206 bet.

**Qiyinlik darajasi – 1**

A5/1 oqimli shifrlash algoritmda Z registr uzunligi nechi bitga teng?
23
20
19
18

**№ 120.**

**Manba:** Z.T. Xudoyqulov, Sh.Z. Islomov, U.R. Mardiyev. “Kriptografiya 1: o’quv qo’llanma” – Тошкент, 2021 – 206 bet.

**Qiyinlik darajasi – 1**

Qaysi xesh algoritmda xesh qiymat 128 bitga teng bo’ladi?
MD5
SHA1
CRC
MAC

**№ 121.**

**Manba:** Z.T. Xudoyqulov, Sh.Z. Islomov, U.R. Mardiyev. “Kriptografiya 1: o’quv qo’llanma” – Тошкент, 2021 – 206 bet.

**Qiyinlik darajasi – 1**

Qaysi xesh algoritmda xesh qiymat 160 bitga teng bo’ladi?
SHA1
MD5
CRC
MAC

**№ 122.**

**Manba:** Z.T. Xudoyqulov, Sh.Z. Islomov, U.R. Mardiyev. “Kriptografiya 1: o’quv qo’llanma” – Тошкент, 2021 – 206 bet.

**Qiyinlik darajasi – 1**

Xeshlash algoritmlarini ko’rsating?
SHA1, MD5, O’z DSt 1106



RSA, DSA, El-gamal
DES, AES, Blowfish
O'z DSt 1105, ГОСТ 28147-89, FEAL

### № 123.

**Manba:** Z.T. Xudoyqulov, Sh.Z. Islomov, U.R. Mardiyev. “Kriptografiya 1: o’quv qo’llanma” – Тошкент, 2021 – 206 bet.**Qiyinlik darajasi – 1**

Qaysi algoritmda, algoritmning necha round bajarilishi ochiq matn uzunligiga bog’liq?
A5/1
MD5
SHA1
HMAC

### № 124.

**Manba:** Z.T. Xudoyqulov, Sh.Z. Islomov, U.R. Mardiyev. “Kriptografiya 1: o’quv qo’llanma” – Тошкент, 2021 – 206 bet.

### Qiyinlik darajasi – 1

A5/1 oqimli shifrlash algoritmda major qiymati hisoblash jarayonida, birinchi (X) registrning qaysi qiymati olinadi?
x8
x9
x10
x11

### № 125.

**Manba:** Z.T. Xudoyqulov, Sh.Z. Islomov, U.R. Mardiyev. “Kriptografiya 1: o’quv qo’llanma” – Тошкент, 2021 – 206 bet.**Qiyinlik darajasi – 1**

A5/1 oqimli shifrlash algoritmda major qiymati hisoblash jarayonida, ikkinchi (Y) registrning qaysi qiymati olinadi?
y10
y11
y12

**№ 126.**

**Manba:** Z.T. Xudoyqulov, Sh.Z. Islomov, U.R. Mardiyev. “Kriptografiya 1: o’quv qo’llanma” – Toshkent, 2021 – 206 bet. **Qiyinlik darajasi – 1**

A5/1 oqimli shifrlash algoritmda major qiymati hisoblash jarayonida, uchinchi (Z) registrning qaysi qiymati olinadi?
z10
z11
z12
z13

**№ 127.**

**Manba:** Z.T. Xudoyqulov, Sh.Z. Islomov, U.R. Mardiyev. “Kriptografiya 1: o’quv qo’llanma” – Toshkent, 2021 – 206 bet.

**Qiyinlik darajasi – 1**

Sezar shifrlash algoritmda shifrlash formulasi qanday?
$C=(M+K) \bmod p$
$C=(M-K) \bmod p$
$C=(M*K) \bmod p$
$C=(M/K) \bmod p$

**№ 128.**

**Manba:** Z.T. Xudoyqulov, Sh.Z. Islomov, U.R. Mardiyev. “Kriptografiya 1: o’quv qo’llanma” – Toshkent, 2021 – 206 bet.

**Qiyinlik darajasi – 1**

Sezar shifrlash algoritmda rasshifrovkalash formulasi qanday?
$M=(C-K) \bmod p$
$M=(C+K) \bmod p$
$M=(C*K) \bmod p$
$M=(C/K) \bmod p$

**№ 129.**

**Manba:** Z.T. Xudoyqulov, Sh.Z. Islomov, U.R. Mardiyev. “Kriptografiya 1: o’quv qo’llanma” – Toshkent, 2021 – 206 bet.

**Qiyinlik darajasi – 1**

Mantiqiy XOR amalining asosi qanday hisoblashga asoslangan?
mod2 bo’yicha qo’shishga
mod2 bo’yicha ko’paytirishga
mod2 bo’yicha darajaga ko’tarishga
mod2 bo’yicha bo’lishga

**№ 130.**

**Manba:** .E. Akbarov. Axborot xavfsizligini ta’minlashning kriptografik usullari va ularning qullanihlari. Toshkent. “Ўзбекистон маркаси “, 2009. – 432 б.

**Qiyinlik darajasi – 1**

DES shifrlash algoritmi simmetrik turga mansub bo’lsa, unda nechta kalitdan foydalaniladi?
1
2
3
4

**№ 131.**

**Manba:** .E. Akbarov. Axborot xavfsizligini ta’minlashning kriptografik usullari va ularning qullanihlari. Toshkent. “Ўзбекистон маркаси “, 2009. – 432 б.

**Qiyinlik darajasi – 2**

AES shifrlash algoritmi simmetrik turga mansub bo’lsa, unda nechta kalitdan foydalaniladi?
1
2
3
4

**№ 132.**

**Manba:** .E. Akbarov. Axborot xavfsizligini ta’minlashning kriptografik usullari va ularning qullanihlari. Toshkent. “Ўзбекистон маркаси “, 2009. – 432 б.

**Qiyinlik darajasi – 2**

A5/1 shifrlash algoritmi simmetrik turga mansub bo'lsa, unda nechta kalitdan foydalaniladi?
1
2
3
4

**№ 133.**

**Manba:** Z.T. Xudoyqulov, Sh.Z. Islomov, U.R. Mardiyev. "Kriptografiya 1: o'quv qo'llanma" – Toshkent, 2021 – 206 bet.

**Qiyinlik darajasi – 2**

RC4 shifrlash algoritmi simmetrik turga mansub bo'lsa, unda nechta kalitdan foydalaniladi?
1
2
3
4

**№ 134.**

**Manba:** Z.T. Xudoyqulov, Sh.Z. Islomov, U.R. Mardiyev. "Kriptografiya 1: o'quv qo'llanma" – Toshkent, 2021 – 206 bet.

**Qiyinlik darajasi – 2**

DES shifrlash algoritmda S-bloklardan chiqqan qiymatlar uzunligi necha bitga teng bo'ladi?
4
8
12
16

**№ 135.**

**Manba:** Z.T. Xudoyqulov, Sh.Z. Islomov, U.R. Mardiyev. "Kriptografiya 1: o'quv qo'llanma" – Toshkent, 2021 – 206 bet.

**Qiyinlik darajasi – 2**

DES shifrlash algoritmda S-bloklarga kiruvchi qiymatlar uzunligi necha bitga teng bo'ladi?
6
12

18
24

### № 136.

**Manba:** Z.T. Xudoyqulov, Sh.Z. Islomov, U.R. Mardiyev. “Kriptografiya 1: o’quv qo’llanma” – Toshkent, 2021 – 206 bet.

### Qiyinlik darajasi – 2

Kalitli xesh funksiyalar qanday turdagi hujumlardan himoyalaydi?
imitatsiya va o’zgartirish turidagi hujumlardan
ma’lumotni oshkor qilish turidagi hujumlardan
foydalanishni buzishga qaratilgan hujumlardan
DDOS hujumlaridan

### № 137.

**Manba:** Z.T. Xudoyqulov, Sh.Z. Islomov, U.R. Mardiyev. “Kriptografiya 1: o’quv qo’llanma” – Toshkent, 2021 – 206 bet.

### Qiyinlik darajasi – 2

Imitatsiya turidagi hujumlarda ma’lumotlar qanday o’zgaradi?
ma’lumot qalbakilashtiriladi
ma’lumot yo’q qilinadi
ma’lumot dublikat qilinadi
ma’lumot ko’chirib olinadi

### № 138.

**Manba:** Z.T. Xudoyqulov, Sh.Z. Islomov, U.R. Mardiyev. “Kriptografiya 1: o’quv qo’llanma” – Toshkent, 2021 – 206 bet.

### Qiyinlik darajasi – 2

O’zgartirish turidagi hujumlarda ma’lumotlar qanday o’zgaradi?
modifikatsiya qilinadi
ma’lumot yo’q qilinadi
ma’lumot dublikat qilinadi
ma’lumot ko’chirib olinadi

**№ 139.**

**Manba:** Z.T. Xudoyqulov, Sh.Z. Islomov, U.R. Mardiyev. “Kriptografiya 1: o’quv qo’llanma” – Toshkent, 2021 – 206 bet.

**Qiyinlik darajasi – 2**

Kalitli xesh funksiyalardan foydalanish nimani kafolatlaydi?
fabrikatsiyani va modifikatsiyani oldini oladi
ma’lumot yo’q qilinadi
ma’lumot dublikat qilinadi
ma’lumot ko’chirib olinadi

**№ 140.**

**Manba:** .E. Akbarov. Axborot xavfsizligini ta’minlashning kriptografik usullari va ularning qullaniшlari. Toshkent. “Ўзбекистон маркаси “, 2009. – 432 б.

**Qiyinlik darajasi – 2**

MD5 xesh funksiyasida chiquvchi qiymat uzunligi nechaga teng?
128
Ixtiyoriy
511
65

**№ 141.**

**Manba:** Z.T. Xudoyqulov, Sh.Z. Islomov, U.R. Mardiyev. “Kriptografiya 1: o’quv qo’llanma” – Toshkent, 2021 – 206 bet.

**Qiyinlik darajasi – 2**

MD5 xesh funksiyasida kiruvchi ma’lumot uzunligi qanday bitli bloklarga bo’linadi?
512
1023
2047
4095

**№ 142.**

**Manba:** .E. Akbarov. Axborot xavfsizligini ta’minlashning kriptografik usullari va ularning qullaniшlari. Toshkent. “Ўзбекистон маркаси “, 2009. – 432 б.

### Qiyinlik darajasi – 2

Faqat AQSH davlatiga tegishli kriptografik standartlar nomini ko'rsating?
AES, DES
AES, GOST 28147-89
DES, O'z DST 1105-2009
SHA1, GOST 3412-94

#### № 143.

**Manba:** Z.T. Xudoyqulov, Sh.Z. Islomov, U.R. Mardiyev. "Kriptografiya 1: o'quv qo'llanma" – Toshkent, 2021 – 206 bet.

### Qiyinlik darajasi – 2

MD5 xesh funksiyasida amallar necha raund davomida bajariladi?
64
128
256
512

#### № 144.

**Manba:** Z.T. Xudoyqulov, Sh.Z. Islomov, U.R. Mardiyev. "Kriptografiya 1: o'quv qo'llanma" – Toshkent, 2021 – 206 bet.

### Qiyinlik darajasi – 2

O'zbekistonda kriptografiya sohasida faoliyat yurituvchi tashkilot nomini ko'rsating?
"UNICON.UZ" DUK
"O'zstandart" agentligi
Davlat Soliq Qo'mitasi
Kadastr agentligi

#### № 145.

**Manba:** Z.T. Xudoyqulov, Sh.Z. Islomov, U.R. Mardiyev. "Kriptografiya 1: o'quv qo'llanma" – Toshkent, 2021 – 206 bet.

### Qiyinlik darajasi – 2

MD5 xesh funksiyasida initsializatsiya bosqichida nechta 32 bitli registrdan foydalanadi?
---

4
8
12
16

**№ 146.**

**Manba:** Z.T. Xudoyqulov, Sh.Z. Islomov, U.R. Mardiyev. “Kriptografiya 1: o’quv qo’llanma” – Toshkent, 2021 – 206 bet.

**Qiyinlik darajasi – 2**

MD5 xesh funksiyasida initsializatsiya bosqichida 4 ta necha bitli registrlardan foydalanadi?
32
64
128
256

**№ 147.**

**Manba:** Z.T. Xudoyqulov, Sh.Z. Islomov, U.R. Mardiyev. “Kriptografiya 1: o’quv qo’llanma” – Toshkent, 2021 – 206 bet.

**Qiyinlik darajasi – 2**

SHA1 xesh funksiyasida chiquvchi qiymat uzunligi nechaga teng?
160
Ixtiyoriy
512
256

**№ 148.**

**Manba:** Z.T. Xudoyqulov, Sh.Z. Islomov, U.R. Mardiyev. “Kriptografiya 1: o’quv qo’llanma” – Toshkent, 2021 – 206 bet.

**Qiyinlik darajasi – 2**

SHA1 xesh funksiyasida kiruvchi ma’lumot uzunligi qanday bitli bloklarga bo’linadi?
512
1024



2048
4096

### № 149.

**Manba:** Z.T. Xudoyqulov, Sh.Z. Islomov, U.R. Mardiyev. “Kriptografiya 1: o’quv qo’llanma” – Toshkent, 2021 – 206 bet.

### Qiyinlik darajasi – 2

Faqat xesh funksiyalar nomi keltirilgan qatorni ko’rsating?
SHA1, MD5
SHA1, DES
MD5, AES
HMAC, A5/1

### № 150.

**Manba:** Z.T. Xudoyqulov, Sh.Z. Islomov, U.R. Mardiyev. “Kriptografiya 1: o’quv qo’llanma” – Toshkent, 2021 – 206 bet.

### Qiyinlik darajasi – 2

SHA1 xesh funksiyasida amallar nechti raund davomida bajariladi?
80
128
256
512

### № 151.

**Manba:** Z.T. Xudoyqulov, Sh.Z. Islomov, U.R. Mardiyev. “Kriptografiya 1: o’quv qo’llanma” – Toshkent, 2021 – 206 bet.

### Qiyinlik darajasi – 2

Faqat simmetrik shifrlash algoritmlari nomi keltirilgan qatorni ko’rsating?
AES, A5/1
SHA1, DES
MD5, AES
HMAC, RC4

**№ 152.**

**Manba:** Z.T. Xudoyqulov, Sh.Z. Islomov, U.R. Mardiyev. “Kriptografiya 1: o’quv qo’llanma” – Toshkent, 2021 – 206 bet.

**Qiyinlik darajasi – 2**

SHA1 xesh funksiyasida initsializatsiya bosqichida nechta registrdan foydalanadi?
5
10
15
20

**№ 153.**

**Manba:** Z.T. Xudoyqulov, Sh.Z. Islomov, U.R. Mardiyev. “Kriptografiya 1: o’quv qo’llanma” – Toshkent, 2021 – 206 bet.

**Qiyinlik darajasi – 2**

SHA1 xesh funksiyasida initsializatsiya bosqichida 5 ta necha bitli registrlardan foydalanadi?
32
64
128
256

**№ 154.**

**Manba:** Z.T. Xudoyqulov, Sh.Z. Islomov, U.R. Mardiyev. “Kriptografiya 1: o’quv qo’llanma” – Toshkent, 2021 – 206 bet.

**Qiyinlik darajasi – 2**

SHA1 xesh funksiyasida to’ldirish bitlarini qo’shishda ma’lumot uzunligi 512 modul bo’yicha qanday son bilan taqqoslanadigan qilib to’ldiriladi?
448
772
988
1002

**№ 155.**

**Manba:** Z.T. Xudoyqulov, Sh.Z. Islomov, U.R. Mardiyev. “Kriptografiya 1: o’quv qo’llanma” – Тошкент, 2021 – 206 bet.

**Qiyinlik darajasi – 2**

Faqat simmetrik shifrlash algoritmlari nomi keltirilgan qatorni ko’rsating?
AES, A5/1
SHA1, DES
MD5, AES
HMAC, RC4

**№ 156.**

**Manba:** Z.T. Xudoyqulov, Sh.Z. Islomov, U.R. Mardiyev. “Kriptografiya 1: o’quv qo’llanma” – Тошкент, 2021 – 206 bet.

**Qiyinlik darajasi – 2**

Faqat oqimli simmetrik shifrlash algoritmlari nomi keltirilgan qatorni ko’rsating?
A5/1, RC4
AES, DES
A5/1, MD5
SHA1, RC4

**№ 157.**

**Manba:** Z.T. Xudoyqulov, Sh.Z. Islomov, U.R. Mardiyev. “Kriptografiya 1: o’quv qo’llanma” – Тошкент, 2021 – 206 bet.

**Qiyinlik darajasi – 2**

DES shifrlash algoritmda rasshifrovkalashda birinchi raunda qaysi kalitdan foydalaniladi?
16-raund kalitidan
1-raund kalitidan
dastlabki kalitdan
1-raunda kalitdan foydalanilmaydi

**№ 158.**

**Manba:** Z.T. Xudoyqulov, Sh.Z. Islomov, U.R. Mardiyev. “Kriptografiya 1: o’quv qo’llanma” – Тошкент, 2021 – 206 bet.

### Qiyinlik darajasi – 2

Faqat blokli simmetrik shifrlash algoritmlari nomi keltirilgan qatorni ko'rsating?
AES, DES
A5/1, RC4
A5/1, MD5
SHA1, RC4

#### № 159.

**Manba:** Z.T. Xudoyqulov, Sh.Z. Islomov, U.R. Mardiyev. "Kriptografiya 1: o'quv qo'llanma" – Тошкент, 2021 – 206 bet.

### Qiyinlik darajasi – 2

AES standarti qaysi algoritm asoslangan?
Rijndael
Serpent
Twofish
RC6

#### № 160.

**Manba:** Z.T. Xudoyqulov, Sh.Z. Islomov, U.R. Mardiyev. "Kriptografiya 1: o'quv qo'llanma" – Тошкент, 2021 – 206 bet.

### Qiyinlik darajasi – 2

AES shifrlash algoritmida nechta akslantirishdan foydalanadi?
4
3
2
akslantirishdan foydalanilmaydi

#### № 161.

**Manba:** Z.T. Xudoyqulov, Sh.Z. Islomov, U.R. Mardiyev. "Kriptografiya 1: o'quv qo'llanma" – Тошкент, 2021 – 206 bet.

### Qiyinlik darajasi – 2

GSM tarmog'ida foydalaniluvchi shifrlash algoritmi nomini ko'rsating?
---

A5/1
DES
AES
RC4

### № 162.

**Manba:** Z.T. Xudoyqulov, Sh.Z. Islomov, U.R. Mardiyev. “Kriptografiya 1: o’quv qo’llanma” – Toshkent, 2021 – 206 bet.

#### Qiyinlik darajasi – 2

add amalining ma’nosi nima?
modul asosida qo’shish
surish (siklik surish, mantiqiy surish)
XOR amali
akslantirish

### № 163.

**Manba:** Z.T. Xudoyqulov, Sh.Z. Islomov, U.R. Mardiyev. “Kriptografiya 1: o’quv qo’llanma” – Toshkent, 2021 – 206 bet.

#### Qiyinlik darajasi – 2

rotate amalining ma’nosi nima?
surish (siklik surish, mantiqiy surish)
modul asosida qo’shish
XOR amali
Akslantirish

### № 164.

**Manba:** Z.T. Xudoyqulov, Sh.Z. Islomov, U.R. Mardiyev. “Kriptografiya 1: o’quv qo’llanma” – Toshkent, 2021 – 206 bet.

#### Qiyinlik darajasi – 2

HMAC tizimida kalit qiymati blok uzunligidan katta bo’lganda ma’lumotga qanday biriktiriladi?
kalitni xesh qiymati hisoblanib, unga blok uzunligiga teng bo’lguncha nol qiymat qo’shiladi va yangi hosil bo’lgan qiymat ma’lumotga biriktiriladi

kalit qiymati blok uzunligiga teng bo'lguncha nol qiymat bilan to'ldirilib hosil bo'lgan qiymat ma'lumotga biriktiriladi
kalit qiymati o'zgartirilmagan holda ma'lumotga biriktiriladi
xesh funksiyalarda kalit qiymatidan foydalanilmaydi

#### **№ 165.**

**Manba:** Z.T. Xudoyqulov, Sh.Z. Islomov, U.R. Mardiyev. “Kriptografiya 1: o'quv qo'llanma” – Тошкент, 2021 – 206 bet.

#### **Qiyinlik darajasi – 2**

HMAC tizimida kalit qiymati blok uzunligidan kichik bo'lganda ma'lumotga qanday biriktiriladi?
kalit qiymati blok uzunligiga teng bo'lguncha nol qiymat bilan to'ldirilib hosil bo'lgan qiymat ma'lumotga biriktiriladi
kalitni xesh qiymati hisoblanib, unga blok uzunligiga teng bo'lguncha nol qiymat qo'shiladi va yangi hosil bo'lgan qiymat ma'lumotga biriktiriladi
kalit qiymati o'zgartirilmagan holda ma'lumotga biriktiriladi
xesh funksiyalarda kalit qiymatida foydalanilmaydi

#### **№ 166.**

**Manba:** Z.T. Xudoyqulov, Sh.Z. Islomov, U.R. Mardiyev. “Kriptografiya 1: o'quv qo'llanma” – Тошкент, 2021 – 206 bet.

#### **Qiyinlik darajasi – 2**

HMAC tizimida kalit qiymati blok uzunligiga teng bo'lganda ma'lumotga qanday biriktiriladi?
kalit qiymati o'zgartirilmagan holda ma'lumotga biriktiriladi
kalit qiymati blok uzunligiga teng bo'lguncha nol qiymat bilan to'ldirilib hosil bo'lgan qiymat ma'lumotga biriktiriladi
kalitni xesh qiymati hisoblanib, unga blok uzunligiga teng bo'lguncha nol qiymat qo'shiladi va yangi hosil bo'lgan qiymat ma'lumotga biriktiriladi
xesh funksiyalarda kalit qiymatida foydalanilmaydi

#### **№ 167.**

**Manba:** Z.T. Xudoyqulov, Sh.Z. Islomov, U.R. Mardiyev. “Kriptografiya 1: o'quv qo'llanma” – Тошкент, 2021 – 206 bet.

#### **Qiyinlik darajasi – 2**

AES shifrlash algoritmda shifrlash jarayonida qanday akslantirishdan foydalaniladi?
SubBytes, ShiftRows, MixColumns va AddRoundKey
SubBytes, ShiftRows va AddRoundKey
SubBytes, MixColumns va AddRoundKey
MixColumns, ShiftRows, SubBytes

### № 168.

**Manba:** Z.T. Xudoyqulov, Sh.Z. Islomov, U.R. Mardiyev. “Kriptografiya 1: o’quv qo’llanma” – Тошкент, 2021 – 206 bet.

### Qiyinlik darajasi – 2

AES shifrlash algoritmda ochiq matn bilan dastlab qanday amal bajariladi?
ochiq matn dastlabki kalit bilan XOR amali bajariladi
ochiq matn birinchi raund kalit bilan XOR amali bajariladi
ochiq matn ustida dastlab SubBytes akslantirishi amali bajariladi
ochiq matn ustida dastlab ShiftRows akslantirishi amali bajariladi

### № 169.

**Manba:** Z.T. Xudoyqulov, Sh.Z. Islomov, U.R. Mardiyev. “Kriptografiya 1: o’quv qo’llanma” – Тошкент, 2021 – 206 bet.

### Qiyinlik darajasi – 2

AES shifrlash algoritmda blok uzunligi 128, kalit uzunligi 192 bit bo’lsa raundlar soni nechta bo’ladi?
12
10
14
6

### № 170.

**Manba:** Z.T. Xudoyqulov, Sh.Z. Islomov, U.R. Mardiyev. “Kriptografiya 1: o’quv qo’llanma” – Тошкент, 2021 – 206 bet.

### Qiyinlik darajasi – 2

AES tanlovi g’olibi bo’lgan algoritm nomini ko’rsating?
Rijndael

Twofish
Blowfish
IDEA

**№ 171.**

**Manba:** Z.T. Xudoyqulov, Sh.Z. Islomov, U.R. Mardiyev. “Kriptografiya 1: o’quv qo’llanma” – Toshkent, 2021 – 206 bet.

**Qiyinlik darajasi – 3**

AES shifrlash algoritmidagi 128 bitli ma’lumot bloki qanday o’lchamdagi jadvalga solinadi?
4x4
4x6
6x4
6x6

**№ 172.**

**Manba:** Z.T. Xudoyqulov, Sh.Z. Islomov, U.R. Mardiyev. “Kriptografiya 1: o’quv qo’llanma” – Toshkent, 2021 – 206 bet.

**Qiyinlik darajasi – 3**

WEP protokolidagi (Wi-Fi tarmog’ida) foydalaniluvchi shifrlash algoritmi nomini ko’rsating?
RC4
DES
SHA1
A5/1

**№ 173.**

**Manba:** Z.T. Xudoyqulov, Sh.Z. Islomov, U.R. Mardiyev. “Kriptografiya 1: o’quv qo’llanma” – Toshkent, 2021 – 206 bet.

**Qiyinlik darajasi – 3**

AES shifrlash standarti qaysi davlat standarti?
AQSH
Rossiya
Buyuk Britaniya
Germaniya



**№ 174.**

**Manba:** Z.T. Xudoyqulov, Sh.Z. Islomov, U.R. Mardiyev. “Kriptografiya 1: o’quv qo’llanma” – Toshkent, 2021 – 206 bet.

**Qiyinlik darajasi – 3**

SHA1 xesh funksiyasi qaysi davlat standarti?
AQSH
Rossiya
Buyuk Britaniya
Germaniya

**№ 175.**

**Manba:** Z.T. Xudoyqulov, Sh.Z. Islomov, U.R. Mardiyev. “Kriptografiya 1: o’quv qo’llanma” – Toshkent, 2021 – 206 bet.

**Qiyinlik darajasi – 3**

DES shifrlash standarti qaysi davlat standarti?
AQSH
Rossiya
Buyuk Britaniya
Germaniya

**№ 176.**

**Manba:** Z.T. Xudoyqulov, Sh.Z. Islomov, U.R. Mardiyev. “Kriptografiya 1: o’quv qo’llanma” – Toshkent, 2021 – 206 bet.

**Qiyinlik darajasi – 3**

Kolliziya hodisasi qaysi turdagi algoritmlarga xos?
xesh funksiyalar
ochiq kalitli shifrlash algoritmlari
simmetrik shifrlash algoritmlari
kalitlarni boshqarish tizimlari

**№ 177.**

**Manba:** Z.T. Xudoyqulov, Sh.Z. Islomov, U.R. Mardiyev. “Kriptografiya 1: o’quv qo’llanma” – Тошкент, 2021 – 206 bet.

**Qiyinlik darajasi – 3**

MD5 xesh funksiyada 48 bitli ma’lumot berilganda to’ldirish bitlari qanday to’ldiriladi?
bir bit 1, 399 ta 0, ma’lumot uzunligi qiymatining 64 bitli qiymati bilan
bir bit 1, 399 ta 0, ma’lumot uzunligining dastlabki 64 bitli qiymati bilan
bir bit 1, 463 ta 0, ma’lumot uzunligi qiymatining 64 bitli qiymati bilan
bir bit 1, 463 ta 0, ma’lumot uzunligining dastlabki 64 bitli qiymati bilan

**№ 178.**

**Manba:** Z.T. Xudoyqulov, Sh.Z. Islomov, U.R. Mardiyev. “Kriptografiya 1: o’quv qo’llanma” – Тошкент, 2021 – 206 bet.

**Qiyinlik darajasi – 3**

SHA1 xesh funksiyada 102 bitli ma’lumot berilganda to’ldirish bitlari qanday to’ldiriladi?
bir bit 1, 345 ta 0, ma’lumot uzunligi qiymatining 64 bitli qiymati bilan
bir bit 1, 345 ta 0, ma’lumot uzunligining dastlabki 64 bitli qiymati bilan
bir bit 1, 409 ta 0, ma’lumot uzunligi qiymatining 64 bitli qiymati bilan
bir bit 1, 409 ta 0, ma’lumot uzunligining dastlabki 64 bitli qiymati bilan

**№ 179.**

**Manba:** Z.T. Xudoyqulov, Sh.Z. Islomov, U.R. Mardiyev. “Kriptografiya 1: o’quv qo’llanma” – Тошкент, 2021 – 206 bet.

**Qiyinlik darajasi – 3**

Quyidagi ifoda nechta yechimga ega? $3 \cdot x = 2 \pmod{7}$ .
bitta yechimga ega
ikkita yechimga ega
yechimga ega emas
uchta yechimga ega

**№ 180.**

**Manba:** Z.T. Xudoyqulov, Sh.Z. Islomov, U.R. Mardiyev. “Kriptografiya 1: o’quv qo’llanma” – Тошкент, 2021 – 206 bet.

**Qiyinlik darajasi – 3**

2 lik sanoq tizimida 0101 soniga 1111 sonini 2 modul bo'yicha qo'shing?
1010
0101
1111
1001

**№ 181.**

**Manba:** Z.T. Xudoyqulov, Sh.Z. Islomov, U.R. Mardiyev. "Kriptografiya 1: o'quv qo'llanma" – Тошкент, 2021 – 206 bet.

**Qiyinlik darajasi – 3**

143mod17 nechiga teng?
7
6
5
8

**№ 182.**

**Manba:** Z.T. Xudoyqulov, Sh.Z. Islomov, U.R. Mardiyev. "Kriptografiya 1: o'quv qo'llanma" – Тошкент, 2021 – 206 bet.

**Qiyinlik darajasi – 3**

A5/1 oqimli shifrlash algoritmida maj(1,0,1) ga teng bo'lsa qaysi registrlar suriladi?
birinchi va uchunchi registrlar suriladi
faqat ikkinchi registr suriladi
birinchi va ikkinchi registrlar suriladi
faqat birinchi resgistr suriladi

**№ 183.**

**Manba:** Z.T. Xudoyqulov, Sh.Z. Islomov, U.R. Mardiyev. "Kriptografiya 1: o'quv qo'llanma" – Тошкент, 2021 – 206 bet.

**Qiyinlik darajasi – 3**

Qalbakilashtirish hujumi qaysi turdagi hujum turiga kiradi?
Immitatsiya

o'zgartirish
Fabrication
modification

#### **№ 184.**

**Manba:** Z.T. Xudoyqulov, Sh.Z. Islomov, U.R. Mardiyev. "Kriptografiya 1: o'quv qo'llanma" – Тошкент, 2021 – 206 bet.

#### **Qiyinlik darajasi – 3**

Sezar shifrlash algoritmidagi ochiq matn $M=3$ ga, kalit $K=7$ ga teng hamda $p=26$ ga teng bo'sa shifr matn qiymati neciga teng bo'ladi?
10
16
18
22

#### **№ 185.**

**Manba:** Z.T. Xudoyqulov, Sh.Z. Islomov, U.R. Mardiyev. "Kriptografiya 1: o'quv qo'llanma" – Тошкент, 2021 – 206 bet.

#### **Qiyinlik darajasi – 3**

Qayday akslantirishdan foydalanilsa chastotalar tahlili kriptotahlil usuliga bardoshli bo'ladi
bigram akslantirishidan
o'rniga qo'yish akslantirishidan
o'rin almashtirish akslantirishidan
hech qanday akslantirishdan foydalanish shart emas

#### **№ 186.**

**Manba:** Z.T. Xudoyqulov, Sh.Z. Islomov, U.R. Mardiyev. "Kriptografiya 1: o'quv qo'llanma" – Тошкент, 2021 – 206 bet.

#### **Qiyinlik darajasi – 3**

Affin shifrlash algoritmidagi $a=2$ , $b=3$ , $p=26$ hamda ochiq matn $x=4$ ga teng bo'lsa, shifr matn qiymatini toping?
11

27
31
41

**№ 187.**

**Manba:** Z.T. Xudoyqulov, Sh.Z. Islomov, U.R. Mardiyev. “Kriptografiya 1: o’quv qo’llanma” – Toshkent, 2021 – 206 bet.

**Qiyinlik darajasi – 3**

A5/1 oqimli shifrlash algoritmida maj(1,0,1) ga teng bo’lsa maj kattalik qiymatini toping?
1
0
2
3

**№ 188.**

**Manba:** Z.T. Xudoyqulov, Sh.Z. Islomov, U.R. Mardiyev. “Kriptografiya 1: o’quv qo’llanma” – Toshkent, 2021 – 206 bet.

**Qiyinlik darajasi – 3**

A5/1 oqimli shifrlash algoritmida $x_{18}=1$ , $y_{21}=0$ , $z_{22}=1$ ga teng bo’lsa kalitni qiymatini toping
0
1
2
3

**№ 189.**

**Manba:** Z.T. Xudoyqulov, Sh.Z. Islomov, U.R. Mardiyev. “Kriptografiya 1: o’quv qo’llanma” – Toshkent, 2021 – 206 bet.

**Qiyinlik darajasi – 3**

Vernam shifrlash algoritmida ochiq matn $M=101$ ga, kalit $K=111$ ga teng bo’lsa shifr matn qiymati qanday bo’ladi?
010
101
111

**№ 190.**

**Manba:** Z.T. Xudoyqulov, Sh.Z. Islomov, U.R. Mardiyev. “Kriptografiya 1: o’quv qo’llanma” – Toshkent, 2021 – 206 bet.

**Qiyinlik darajasi – 3**

Vernam shifrlash algoritmda shifr matn C=101 ga, kalit K=111 ga teng bo’lsa shifr matn qiymati qanday bo’ladi?
010
101
111
110

**№ 191.**

**Manba:** Z.T. Xudoyqulov, Sh.Z. Islomov, U.R. Mardiyev. “Kriptografiya 1: o’quv qo’llanma” – Toshkent, 2021 – 206 bet.

**Qiyinlik darajasi – 3**

3 sonini 5 chekli maydonda teskarisini toping?
2
3
4
5

**№ 192.**

**Manba:** Z.T. Xudoyqulov, Sh.Z. Islomov, U.R. Mardiyev. “Kriptografiya 1: o’quv qo’llanma” – Toshkent, 2021 – 206 bet.

**Qiyinlik darajasi – 3**

Qaysi algoritmda maj kattaligi ishlatiladi?
A5/1
RC4
MD5
SHA1

**№ 193.**

**Manba:** Z.T. Xudoyqulov, Sh.Z. Islomov, U.R. Mardiyev. “Kriptografiya 1: o’quv qo’llanma” – Тошкент, 2021 – 206 bet.

**Qiyinlik darajasi – 3**

MD5 xesh algoritmda nechta 32 bitli statik qiymatdan foydalanadi?
4
8
12
16

**№ 194.**

**Manba:** Z.T. Xudoyqulov, Sh.Z. Islomov, U.R. Mardiyev. “Kriptografiya 1: o’quv qo’llanma” – Тошкент, 2021 – 206 bet.

**Qiyinlik darajasi – 3**

SHA1 xesh algoritmda nechta 32 bitli statik qiymatdan foydalanadi?
5
10
15
20

**№ 195.**

**Manba:** Z.T. Xudoyqulov, Sh.Z. Islomov, U.R. Mardiyev. “Kriptografiya 1: o’quv qo’llanma” – Тошкент, 2021 – 206 bet.

**Qiyinlik darajasi – 3**

Qaysi xesh algoritmda 64 raund amal bajariladi?
MD5
SHA1
CRC
MAC

**№ 196.**

**Manba:** Z.T. Xudoyqulov, Sh.Z. Islomov, U.R. Mardiyev. “Kriptografiya 1: o’quv qo’llanma” – Тошкент, 2021 – 206 bet.

### Qiyinlik darajasi – 3

Qaysi xesh algoritmda 80 raund amal bajariladi?
SHA1
MD5
CRC
MAC

#### № 197.

**Manba:** Z.T. Xudoyqulov, Sh.Z. Islomov, U.R. Mardiyev. “Kriptografiya 1: o’quv qo’llanma” – Toshkent, 2021 – 206 bet.

### Qiyinlik darajasi – 3

Qaysi blokli shifrlash algoritmda raund kalit uzunligi qiymatiga bo’g’liq?
AES
DES
IDEA
RSA

#### № 198.

**Manba:** .E. Akbarov. Axborot xavfsizligini ta’minlashning kriptografik usullari va ularning qullaniшlari. Toshkent. “Ўзбекистон маркаси”, 2009. – 432 б.

### Qiyinlik darajasi – 3

Qaysi blokli shifrlash algoritmda 8 ta statik S-box lardan foydalaniladi?
DES
RC4
RSA
A5/1

#### № 199.

**Manba:** Z.T. Xudoyqulov, Sh.Z. Islomov, U.R. Mardiyev. “Kriptografiya 1: o’quv qo’llanma” – Toshkent, 2021 – 206 bet.

### Qiyinlik darajasi – 3

Kolliziya hodisasi deb nimaga aytiladi?
---



ikki xil matn uchun bir xil xesh qiymat chiqishi
ikki xil matn uchun ikki xil xesh qiymat chiqishi
bir xil matn uchun bir xil xesh qiymat chiqishi
bir xil matn uchun ikki xil xesh qiymat chiqishi

**№ 200.**

**Manba:** Z.T. Xudoyqulov, Sh.Z. Islomov, U.R. Mardiyev. “Kriptografiya 1: o’quv qo’llanma” – Toshkent, 2021 – 206 bet.

**Qiyinlik darajasi – 3**

Blokli shifrlash rejimlari qaysi algoritmlarda qo’llaniladi?
AES, DES
Sezar, Affin
A5/1, RC4
MD5, SHA1

### Foydalanilgan adabiyotlar

1. Z.T. Xudoyqulov, Sh.Z. Islomov, U.R. Mardiyev. “Kriptografiya 1: o’quv qo’llanma” – Toshkent, 2021 – 206 bet.
2. Д.Е. Акбаров. Ахборот хавфсизлигини таъминлашнинг криптографик усуллари ва уларнинг қўлланишлари. Тошкент. “Ўзбекистон маркаси”, 2009. – 432 б.
3. Kiberxavfsizlik asoslari: O’quv qo’llanma/S.K.Ganiev, A.A.Ganiev, Z.T.Xudoyqulov; – T.: “Iqtisod-Moliya”, 2021. – 228 b.

1. Axborot xavfsizligining qaysi xususiyati ma’lumotni maxfiyligini ta’minlaydi? – Konfidensiallik.

2. A5/1 oqimli shifrlash algoritmida kiruvchi kalit uzunligi qancha bo’ladi? – 64.

3. A5/1 oqimli shifrlash algoritmida kiruvchi kalit nechta qismga ajratiladi? – 3.

4. A5/1 oqimli shifrlash algoritmida kiruvchi kalit 1 qism uzunligi nechki bit bo’ladi? – 19.

5. A5/1 oqimli shifrlash algoritmida Z registrning boqarish biti qaysi - 11

6. ARX amali nimalardan iborat? – add, rotate, xor.

7. AES algoritmida shifrlash kalitining uzunligin qanday? – 128,192,256 bit.

8. Axborot xavfsizligining qaysi xususiyati ma'lumotni butunligini ta'minlaydi? – butunlik.
9. DES shifrlash algoritmda kalit uzunligi nechi – 56.
10. DES shifrlash algoritmda qanday amallardan foydalaniladi? -
11. DES shifrlash algoritmda raundlar soni nechta – 16.
12. DES shifrlash algoritmda kiruvchi blok uzunligi nechi – 64.
13. DES shifrlash algoritmi qaysi tarmoqqa asoslangan holda ishlaydi? – feystel tarmog'iga asoslangan holda.
14. Ma'lumotlarni shifratga o'girish jarayoni bu – Daslabki ma'lumotlarni kalit yordamida shifrlangan ma'lumotlarga almashtirish.
15. Ma'lumotlar maxfiyligi qaysi usullar orqali ta'minlandi? – Kriptografik usullar asosida.
16. Oqimli shifrlash algoritmlariga qaysi algoritmlar kiradi? – A5, RC4.
17. Quyida keltirilgan kriptotaxlil usullaridan qaysi biri orqali maqsadga tezroq erishiladi? – Qo'pol kuch hujumi.
18. Simmetrik shifrlash algoritmi qanday turlarga bo'linadi? – uzluksiz va blokli.
19. Simmetrik shifrlash algoritmi necha turga bo'linadi? – 2.
20. Simmetrik kriptotizimlarda nechta kalitdan foydalaniladi? – 1 ta.
21. Kriptografiyaning ta'rifi qaysi bo'limdaa to'g'ri keltirilgan? – kriptografik almashtirishlarni o'rganivchi fan.
22. Klassik kriptotaxlil bu – y shifratndan x ochiq matnni ajratib olish yoki shifratndan k kalitni tiklash ilmi.
23. Kriptologiya nechta yo'nalishga bo'linadi? – 2.
24. Kriptologiya qaysi yo'nalishlarga bo'linadi? – Kriptografiya va kriptozanaliz.
25. Kriptoalgoritmning bardoshliligi bu – kriptoalgoritmning uni oshkor etishga bo'lgan [turli urunishlarga](#), ya'ni unga bo'ladigan hujumlarga qarshi tura olish qobiliyati.
26. Kriptotaxlil usullaridan biri bo'lgan to'liq tanlash hujumi qanday amalga oshiriladi? – shifrlash algoritmini qora quti sifatida ko'rib barcha bo'lishi mumkin bo'lgan kalitlarni tekshirib chiqadi.

27. Kriptografiya bu – Axborotni o'zgartirish [prinsiplari](#), vositalari va usullarini o'rganadigan ilmiy fan.
28. Kriptotaxlil usullaridan biri bo'lgan analitik hujumi qanday amalga oshiriladi? – shifrlash algoritmining ichki tuzilishidan foydalaniladi.
29. Ko'p qiymatli shifrlash qanday amalga oshiriladi? – ochiq ma'lumot alfaviti belgilarining har biriga shifr ma'lumot alfavitining 2 ta yoki undan ortiq chekli sondagi belgilari mos qo'yiladi.
30. Kriptoanaliz nima bilan shug'ullanadi? – Shifrlash uslubini bilmagan holda shifrlangan ma'lumotni asl holatini topish masalalarini yechish bilan shug'ullanadi.
31. Kriptografik o'zgartirish bu – parametrlarning bir qismi maxfiy holda bo'lgan kriptografik algoritm bo'yicha ma'lumotlarni almashtirish.
32. O'rniga qo'yish shifrlash sinfiga qanday algoritmlar kiradi? – shifrlash jarayonida ochiq ma'lumot alfaviti belgilari shifr ma'lumot alfaviti belgilariga almashtiriladigan algoritmlar.
33. O'rniga qo'yish shifrlash algoritmi qanday sinfga bo'linadi? – bir qiymatli va ko'p qiymatli shifrlash.
34. O'rniga qo'yish shifrlash algoritmi nechta sinfga bo'linadi? – 2.
35. 2 lik sanoq tizimida 11011 soniga 11011 sonini 2 modul bo'yicha qo'shing – 00000.
36. 2 lik sanoq tizimida 0101 soniga 1111 sonini 2 modul bo'yicha qo'shing – 1010.
37. 2 lik sanoq tizimida 101101 soniga 001110 sonini 2 modul bo'yicha qo'shing – 100011.
38.  $-8 \bmod 7$  nechiga teng? – 6.
39.  $-21 \bmod 13$  nechiga teng – 5.
40.  $-19 \bmod 11$  nechiga teng - 3.
41. 2 lik sanoq tizimida 11011 soniga 10110 sonini 2 modul bo'yicha qo'shing – 01101.

**1. RSA ning DSA dan ustunligi nimada?**

u kamroq resurslardan foydalanadi va tezroq shifrlashni amalga oshiradi, chunki u nosimmetrik tugmachalardan foydalanadi

**3.  $12+11 \bmod 16$  ?**

7

**4. XOR amali qanday amal?**

2 modul bo'yicha qo'shish

**5. Barcha simmetrik shifrlash algoritmlari qanday shifrlash usullariga bo'linadi**

DES va oqimli

**6. Ma'lumki tasodifiy ketma-ketlik belgilariga qo'shilgan asl matnning qanday belgilari bor?**

analitik transformatsiya algoritmi

**7. DES algoritmining asosiy muammosi nimada?**

kalit uzunligi 56 bit. Bugungu kunda ushbu uzunlik algoritmning kriptobardoshliligi uchun yetarli emas

**8. Vijiner jadvali bo'yicha matnning dekodlanishini tashkil etuvchi ketma-ketliklar soni:**

4

**9. Kriptotizimlar qanday turlarga bo'linadi?**

Simmetrik va asimmetrik kriptotizim

**10. Odatda elektron imzo nima deyiladi?**

uning matnga biriktirilgan kriptografik o'zgarishi

**11. DES qaysi tarmog' asosida ishlaydi**

Feystel tarmog'i asosida

**13. Ma'lumotni qonuniy manbadan olingaligini kafolatlovchi va oluvchining haqiqiylikini tasdiqlovchi xizmat qanday nomlanadi?**

autentifikatsiya

**15. Kriptanalizning maqsadi:**

Kriptografik algoritmda almashtirish funktsiyalari sonini ko'paytirish

**16. Kriptanalizning maqsadi:**

Kriptografik algoritmda almashtirish funktsiyalari sonini kamaytirish

**17. Zamonaviy kriptografik axborot xavfsizligi tizimlariga qo'yiladigan talablar:**

kalitlar o'rtasida oddiy va oson o'rnatiladigan bog'liqliklar bo'lmasligi kerak

**18. Kriptosistemalar qanday turlarga bo'linadi?**

barcha javoblar to'g'ri

**19. Alfavit nima?**

ma'lumotni kodlash uchun ishlatiladigan belgilarning cheklangan to'plami

## 20. Simmetrik kriptosistemalarda shifrlash va shifr matnni ochish uchun ishlatiladigan kalitlar soni:

2

---

1. DES-dagi samarali kalit uzunligi:

16

2. Assimetrik kripto tizimlarida ishlatiladigan kalitlarning soni:

2

3. Alifbo namunalarini tanlang:

Z256 – belgilardan ASCII KOI-8

4. Xavfsizlik matnini tiklash uchun sizga quyidagilardan qaysilari kerak?

kalit

5. DES algoritmining asosiy muammosi nimada?

kalit uzunligi 56 bit. Bugungu kunda ushbu uzunlik algoritmning kriptobardoshliligi uchun yetarli emas

6. Simmetrik kriptosistemalarda shifrlash va shifr matnni ochish uchun ishlatiladigan kalitlar soni:

1

7. Kriptografik quvvat nima?

shriftning kalitini bilmasdan uning parolini hal qilishga chidamliligini aniqlaydigan xususiyati

8. DES shifrlash algoritmida kalit uzunligi va blok uzunligi mos holda qancha bo'lishi kerak

56 bit, 64 bit

9. DES algoritmiga muqobil bo'lgan algoritmni ko'rsating.

Rijndael

10. Shifrlash nima?

asl matnni shifrlangan matnga o'tkazish jarayoni

11. Elektron raqamli imzo yaratish uchun nima ishlatilishini tanlang:

## jo'natuvchining ochiq kaliti

12. Qaysi kriptotizimda shifrlash uchun ham va deshifrlash uchun ham bir xil kalitdan foydalaniladi?

Simmetrik kriptotizim

13. Kriptotizimlar qanday turlarga bo'linadi?

Simmetrik va asimmetrik kriptotizim

16.  $13+4 \bmod 26$ ?

17

17. Assimetrik kriptotizimda shifrlash uchun ishlatiladigan kalit nomi:

maxfiy

18. Odatda elektron imzo nima deyiladi?

uning matnga biriktirilgan kriptografik o'zgarishi

20. Asosiy zamonaviy shifrlash usullari:

RC4, Vijniner

---

1. Zamonaviy kriptografik axborot xavfsizligi tizimlariga qo'yiladigan talablar:

kalitlar o'rtasida oddiy va oson o'rnatiladigan bog'liqliklar bo'lmasligi kerak

2. Assimetrik kriptotizimda shifrlash uchun ishlatiladigan kalit nomi:

yarim ochiq

3. Simmetrik kriptosistemalarda shifrlash va shifr matnni ochish uchun ishlatiladigan kalitlar soni:

1

5. Matn nima?

kodlash uchun ishlatiladigan cheklangan to'plam

6. Vijniner jadvali bo'yicha matnning dekodlanishini tashkil etuvchi ketma-ketliklar soni:

2

7. Kriptografik quvvat nima?

shriftning kalitini bilmasdan uning parolini hal qilishga chidamliligini aniqlaydigan xususiyati

8. Kriptotizimlar qanday turlarga bo'linadi?

Simmetrik va asimmetrik kriptotizim

9. Shifrlashda birinchi bo'lib qaysi matndan foydalanilgan?

Misr yozuvi

10. DES-dagi samarali kalit uzunligi:

56

11. XOR amali qanday amal?

2 modul bo'yicha qo'shish

12. Shifrlash kuchini oshirish uchun ishlatiladigan viginer jadvallari:

jadvalning barcha (birinchi tashqari) qatorlarida harflar istalgan tartibda

13.  $12+11 \bmod 16$  ?

7

14. Kriptografik quvvat ko'rsatkichlari bilan nima bog'liqligini tanlang:

barcha mumkin bo'lgan kalitlar soni

15. Ma'lumotni qonuniy manbadan olingaligini kafolatlovchi va oluvchining haqiqiyligini tasdiqlovchi xizmat qanday nomlanadi?

autentifikatsiya

16. Ochiq kalit tizimida kalitlarning bir-biriga qanday bog'liqligini tanlang:

matematik jihatdan

17. Windows-da saqlanadigan maxfiy ma'lumotlar:

tarmoq manbalariga kirish uchun internetga sertifikatlar va tarmoq resurslariga kirish uchun shifrlangan parollar

18. DES shifrlash algoritmidagi kalit uzunligi va blok uzunligi mos holda qancha bo'lishi kerak

56 bit, 64 bit

19. Qaysi kriptotizimda shifrlash uchun ham va deshifrlash uchun ham bir xil kalitdan foydalaniladi?

Simmetrik kriptotizim

20. Elektron raqamli imzo yaratish uchun nima ishlatilishini tanlang:

jo'natuvchining shaxsiy kaliti

---

1. Almashtirish usulining mohiyati:

barchasi to'g'ri

2. Shifrlashda birinchi bo'lib qaysi matndan foydalanilgan?

Misr yozuvi

3. Shifrlash kuchini oshirish uchun ishlatiladigan viginer jadvallari:

jadvalning barcha (birinchi tashqari) qatorlarida harflar istalgan tartibda

4. Ma'lumotni qonuniy manbadan olingaligini kafolatlovchi va oluvchining haqiqiyligini tasdiqlovchi xizmat qanday nomlanadi?

autentifikatsiya

5. Ma'lumki tasodifiy ketma-ketlik belgilariga qo'shilgan asl matnning qanday belgilari bor?

almashtirish algoritmi

6. Ochiq kalit tizimida kalitlarning bir-biriga qanday bog'liqligini tanlang:

matematik jihatdan

7.  $12+11 \bmod 16$  ?

7

9. RSA ning DSA dan ustunligi nimada?

U bir martalik shifrlash maydonchalarini ishlatadi

10. Elektron raqamli imzo yaratish uchun nima ishlatilishini tanlang:

jo'natuvchining shaxsiy kaliti

11. Kriptosistemalar qanday turlarga bo'linadi?



barcha javoblar to'g'ri

12. Xavfsizlik matnini tiklash uchun sizga quyidagilardan qaysilari kerak?

kalit

13. Assimetrik kriptotizimlarida ishlatiladigan kalitlarning soni:

2

14. DES qaysi tarmog' asosida ishlaydi

Feistel tarmog'i asosida

15. Simmetrik kriptosistemalarda shifrlash va shifr matnini ochish uchun ishlatiladigan kalitlar soni:

1

16. Odatda elektron imzo nima deyiladi?

uning matnga biriktirilgan kriptografik o'zgarishi

17.  $13+4 \bmod 26$ ?

17

18. DES algoritmgaga muqobil bo'lgan algoritmgani ko'rsating.

Uch karrali DES

19. Vijnier jadvali bo'yicha matnning dekodlanishini tashkil etuvchi ketma-ketliklar soni:

4

20. Alfavit nima?

ma'lumotni kodlash uchun ishlatiladigan belgilarning cheklangan to'plami

1. Barcha simmetrik shifrlash algoritmlari qanday shifrlash usullariga bo'linadi

blokli va oqimli

2. Ma'lumki tasodifiy ketma-ketlik belgilariga qo'shilgan asl matnning qanday belgilari bor?

gamma algoritmi

3. Kriptosistemalar qanday turlarga bo'linadi?

barcha javoblar to'g'ri

4. Simmetrik kriptosistemalarda shifrlash va shifr matnni ochish uchun ishlatiladigan kalitlar soni:  
1
5. Kriptografik quvvat ko'rsatkichlari bilan nima bog'liqligini tanlang:  
barcha mumkin bo'lgan kalitlar soni
6. Matn nima?  
alifbo elementlarining tartiblangan to'plami
7. DES da blok E kengaytirilishidan so'ng kanday amal bajariladi?  
kalit bilan XOR amali bilan qo'shiladi
8. Kriptografik quvvat nima?  
shriftning kalitini bilmasdan uning parolini hal qilishga chidamliligini aniqlaydigan xususiyati
9. Kriptotizimlar qanday turlarga bo'linadi?  
Simmetrik va asimmetrik kriptotizim
10. Shifrlash kuchini oshirish uchun ishlatiladigan viginer jadvallari:  
jadvalning barcha (birinchi tashqari) qatorlarida harflar istalgan tartibda
11. Qaysi kriptotizimda shifrlash uchun ham va deshifrlash uchun ham bir xil kalitdan foydalaniladi?  
Simmetrik kriptotizim
12. Kriptanalizning maqsadi:  
Algoritmning mustahkamligini aniqlash
13. Ma'lumotni qonuniy manbadan olingaligini kafolatlovchi va oluvchining haqiqiylikini tasdiqlovchi xizmat qanday nomlanadi?  
autentifikatsiya
14. DES algoritmgiga muqobil bo'lgan algoritmni ko'rsating.  
IDEA
15. Zamonaviy kriptografik axborot xavfsizligi tizimlariga qo'yiladigan talablar:

kalitlar o'rtasida oddiy va oson o'rnatiladigan bog'liqliklar bo'lmasligi kerak

16. DES shifrlash algoritmda kalit uzunligi va blok uzunligi mos holda qancha bo'lishi kerak  
56 bit, 64 bit

17.  $13+4\text{mod}26$ ?  
17

18. Alifbo namunalarini tanlang:  
Z256 – belgilardan ASCII KOI-8

19. Shifrlashda birinchi bo'lib qaysi matndan foydalanilgan?  
Misr yozuvi

20. Windows-da saqlanadigan maxfiy ma'lumotlar:  
tarmoq manbalariga kirish uchun internetga sertifikatlar va tarmoq resurslariga kirish uchun shifrlangan parollar

---

Asosiy zamonaviy shifrlash usullari:  
RSA, DES

2. Windows-da saqlanadigan maxfiy ma'lumotlar:  
tarmoq manbalariga kirish uchun internetga sertifikatlar va tarmoq resurslariga kirish uchun shifrlangan parollar

3. DES-dagi samarali kalit uzunligi:  
56

4. Shifrlash nima?  
asl matnni shifrlangan matnga o'tkazish jarayoni

5. DES da blok E kengaytirilishidan so'ng kanday amal bajariladi?  
kalit bilan XOR amali bilan qo'shiladi

6. Elektron raqamli imzo nimani yaxshiroq tavsiflashini tanlang:  
Bu qolda yozilgan imzoni electron hujjatga otkazish usuli

7. Simmetrik kriptosistemalarda shifrlash va shifr matnni ochish uchun ishlatiladigan kalitlar soni:

1

8. Kriptanalizning maqsadi:

Algoritmning mustahkamligini aniqlash

9. Shifrlashda birinchi bo'lib qaysi matndan foydalanilgan?

Misr yozuvi

10. Qaysi kriptotizimda shifrlash uchun ham va deshifrlash uchun ham bir xil kalitdan foydalaniladi?

Simmetrik kriptotizim

11. Alfavit nima?

ma'lumotni kodlash uchun ishlatiladigan belgilarning cheklangan to'plami

12. Deshifrlash nima?

teskari matnni shifrlangan matnga o'tkazish jarayoni

13. Kriptografik quvvat ko'rsatkichlari bilan nima bog'liqligini tanlang:

barcha mumkin bo'lgan kalitlar soni

14.  $12+11 \bmod 16$  ?

7

15. Kriptosistemalar qanday turlarga bo'linadi?

barcha javoblar to'g'ri

16. Shifrlash necha yil oldin paydo bo'lgan?

to'rt ming yil oldin

17. Ma'lumki tasodifiy ketma-ketlik belgilariga qo'shilgan asl matnning qanday belgilari bor?

gamma algoritmi

18 Kriptanalizning maqsadi:

algoritmning mustahkamligini aniqlash

19. Ma'lumotni qonuniy manbadan olingaligini kafolatlovchi va oluvchining haqiqiylikini tasdiqlovchi xizmat qanday nomlanadi?

autentifikatsiya

20. Kriptografik quvvat nima?

shriftning kalitini bilmasdan uning parolini hal qilishga chidamliligini aniqlaydigan xususiyati

---

1. DES qaysi tarmog' asosida ishlaydi

Feystel tarmog'i asosida

2. Assimetrik kripto tizimlarida ishlatiladigan kalitlarning soni

2

3. DES-dagi samarali kalit uzunligi:

56

4. DES shifrlash algoritmda kalit uzunligi va blok uzunligi mos holda qancha bo'lishi kerak

56 bit, 64 bit

5. Elektron raqamli imzo yaratish uchun nima ishlatilishini tanlang:

jo'natuvchining shaxsiy kaliti

6. Kriptanalizning maqsadi:

Algoritmning mustahkamligini aniqlash

7. RSA ning DSA dan ustunligi nimada?

Bu blok shifr va oqim shifridan yaxshiroqdir

8. Odatda elektron imzo nima deyiladi?

uning matnga biriktirilgan kriptografik o'zgarishi

9. Kriptanalizning maqsadi:

algoritmning mustahkamligini aniqlash

10. Elektron raqamli imzo nimani yaxshiroq tavsiflashini tanlang:

Bu qo'lda yozilgan imzoni elektron hujjatga o'tkazish usuli

11. Alifbo namunalarini tanlang:

Z256 – belgilardan ASCII KOИ-8

12. Shifrlash nima?

asl matnni shifrlangan matnga o'tkazish jarayoni

13. Kriptotizimlar qanday turlarga bo'linadi?

Simmetrik va asimmetrik kriptotizim

14. Kriptografik quvvat ko'rsatkichlari bilan nima bog'liqligini tanlang:

barcha mumkin bo'lgan kalitlar soni

15. Kriptografik quvvat nima?

shriftning kalitini bilmasdan uning parolini hal qilishga chidamliligini aniqlaydigan xususiyati

16. DES algoritmiga muqobil bo'lgan algoritmni ko'rsating.

Uch karrali DES, IDEA, Rijndael

17. DES algoritmining asosiy muammosi nimada?

kalit uzunligi 56 bit. Bugungu kunda ushbu uzunlik algoritmning kriptobardoshliligi uchun yetarli emas

18. XOR amali qanday amal?

2 modul bo'yicha qo'shish

19. Barcha simmetrik shifrlash algoritmlari qanday shifrlash usullariga bo'linadi

blokli va oqimli

20. Qaysi kriptotizimda shifrlash uchun ham va deshifrlash uchun ham bir xil kalitdan foydalaniladi?

Simmetrik kriptotizim

DES shifrlash algoritmi simmetrik turga mansub bo'lsa, unda nechta kalitdan foydalaniladi?

=====

# 1

=====

2

=====

3

=====

4

+++++

AES shifrlash algoritmi simmetrik turga mansub bo'lsa, unda nechta kalitdan foydalaniladi?

=====

# 1

=====

2

=====

3

=====

4

+++++

A5/1 shifrlash algoritmi simmetrik turga mansub bo'lsa, unda nechta kalitdan foydalaniladi?

=====

# 1

=====

2

=====

3

=====

4

+++++

RC4 shifrlash algoritmi simmetrik turga mansub bo'lsa, unda nechta kalitdan foydalaniladi?

=====

# 1

=====

2

=====

3

=====

4

+++++

DES shifrlash algoritmidan S-bloklardan chiqqan qiymatlar uzunligi necha bitga teng bo'ladi?

=====

# 4

=====

8

=====

12

=====

16

+++++

DES shifrlash algoritmidan S-bloklarga kiruvchi qiymatlar uzunligi necha bitga teng bo'ladi?

=====



# 6

=====

12

=====

18

=====

24

+++++

AES shifrlash algoritmida 128 bitli ma'lumot bloki qanday o'lchamdagi jadvalga solinadi?

=====

# 4x4

=====

4x6

=====

6x4

=====

6x6

+++++

Blokli shifrlash rejimlari qaysi algoritmlarda qo'llaniladi?

=====

#AES, DES

=====

Sezar, Affin

=====

A5/1, RC4

=====

MD5, SHA1

+++++

$2+5 \bmod 32=?$

=====

#7

=====

5

=====

2

=====

32

+++++

$26+7 \bmod 26=?$

=====

#7

=====

26

=====

33

=====

19

+++++

Rijndael algoritmi S-box uzunligi necha bit?

=====

#128

=====

132

=====

136

=====

+++++

Qaysi blokli shifrlash algoritmida 8 ta statik S-box lardan foydalaniladi?

=====

#DES

=====

RC4

=====

RSA

=====

A5/1

+++++

WEP protokolida (Wi-Fi tarmog'ida) foydalaniluvchi shifrlash algoritmi nomini ko'rsating?

=====

# RC4

=====

DES

=====

SHA1

=====

A5/1

+++++

Faqat oqimli simmetrik shifrlash algoritmlari nomi keltirilgan qatorni ko'rsating?

=====

# A5/1, RC4

=====

AES, DES

=====

A5/1, MD5

=====

SHA1, RC4

+++++

Faqat blokli simmetrik shifrlash algoritmlari nomi keltirilgan qatorni ko'rsating?

=====

# AES, DES

=====

A5/1, RC4

=====

A5/1, MD5

=====

SHA1, RC4

+++++

AES standarti qaysi algoritm asoslangan?

=====

# Rijndael

=====

Serpent

=====

Twofish

=====

RC6

+++++

GSM tarmog'ida foydalaniluvchi shifrlash algoritmi nomini ko'rsating?

=====

# A5/1

=====

DES

=====

AES

=====

RC4

+++++

add amalining ma'nosi nima?

=====

# modul asosida qo'shish

=====

surish (siklik surish, mantiqiy surish)

=====

XOR amali

=====

akslantirish

+++++

rotate amalining ma'nosi nima?

=====

# surish (siklik surish, mantiqiy surish)

=====

modul asosida qo'shish

=====

XOR amali

=====

Akslantirish

+++++

AES tanlovi g‘olibi bo‘lgan algoritm nomini ko‘rsating?

=====

# Rijndael

=====

Twofish

=====

Blowfish

=====

IDEA

+++++

Faqat AQSH davlatiga tegishli kriptografik standartlar nomini ko‘rsating?

=====

# AES, DES

=====

AES, FOCT 28147-89

=====

DES, O‘z DST 1105-2009

=====

SHA1, FOCT 3412-94

+++++

O‘zbekistonda kriptografiya sohasida faoliyat yurituvchi tashkilot nomini ko‘rsating?

=====

# “UNICON.UZ” DUK

=====

“O‘zstandart” agentligi

=====

Davlat Soliq Qo‘mitasi

=====

Kadastr agentligi

+++++

Simmetrik va ochiq kalitli kriptotizimlar asosan nimasi bilan bir biridan farq qiladi?

=====

# kalitlar soni bilan

=====

matematik murakkabligi bilan

=====

farq qilmaydi

=====

biri maxfiylikni ta’minlasa, biri butunlikni ta’minlaydi

+++++

Kriptotizimlar kalitlar soni bo‘yicha nechta turga bo‘linadi?

=====

# 2

=====

3

=====

4

=====

5

+++++

Faqat simmetrik shifrlash algoritmlari nomi keltirilgan qatorni ko'rsating?

=====

# AES, A5/1

=====

SHA1, DES

=====

MD5, AES

=====

HMAC, RC4

+++++

Quyidagi ta'rif qaysi kriptotizimga tegishli ochiq matnni shifrlashda hamda rasshifrovkalashda mos holda ochiq va maxfiy kalitdan foydalanadi?

=====

# ochiq kalitli kriptotizimlar

=====

maxfiy kalitli kriptotizimlar

=====

simmetrik kriptotizimlar

=====

elektron raqamli imzo tizimlari

+++++

Simmetrik kriptotizimlarning asosiy kamchiligi bu?

=====

# kalitni taqsimlash zaruriyati

=====

shifrlash jarayonining ko'p vaqt olishi

=====



kalitlarni esda saqlash murakkabligi

=====

algoritmning xavfsiz emasligi

+++++

Faqat simmetrik blokli shifrlarga xos bo'lgan atamani aniqlang?

=====

# blok uzunligi

=====

kalit uzunligi

=====

ochiq kalit

=====

kodlash jadvali

+++++

Sezar shifrlash usuli qaysi akslantirishga asoslangan?

=====

# o'rniga qo'yish

=====

o'rin almashtirish

=====

ochiq kalitli shifrlarga

=====

kombinatsion akslantirishga

+++++

Shifrlash va deshifrlashda alohida kalitlardan foydalanuvchi kriptotizimlar bu?

=====

# ochiq kalitli kriptotizimlar

=====

simmetrik kriptotizimlar

=====

bir kalitli kriptotizimlar

=====

xesh funksiyalar

+++++

Simmetrik shifrlar axborotni qaysi xususiyatlarini ta'minlashda foydalaniladi?

=====

# konfidensiallik va yaxlitlik

=====

konfidensiallik va foydalanuvchanlik

=====

foydalanuvchanlik va yaxlitlik

=====

foydalanuvchanlik

+++++

Kriptotizimni boshqaradigan vosita?

=====

# kalit

=====

algoritm

=====

stegokalit

=====

kriptotizim boshqarilmaydi

+++++

Chastotalar tahlili hujumi qanday amalga oshiriladi?

=====

# shifr matnda qatnashgan harflar sonini aniqlash orqali

=====

shifr matnda eng kam qatnashgan harflarni aniqlash orqali

=====

ochiq matnda qatnashgan harflar sonini aniqlash orqali

=====

ochiq matnda eng kam qatnashgan harflarni aniqlash orqali

+++++

RC4 shifrlash algoritmi qaysi turga mansub?

=====

# oqimli shifrlar

=====

blokli shifrlar

=====

ochiq kalitli shifrlar

=====

assimetrik shifrlar

+++++

Kerkxofs printsi bo'yicha qanday taxminlar ilgari suriladi?

=====

# Kalitdan boshqa barcha ma'lumotlar barchaga ma'lum

=====

Faqat kalit barchaga ma'lum

=====

Barcha parametrlar barchaga ma'lum

=====

Shifrlash kaliti barchaga ma'lum

+++++

Qaysi algoritim har bir qadamda bir bayt qiymatni shifrlaydi?

=====

# RC4

=====

A5/1

=====

RSA

=====

AES

+++++

Qaysi algorimtda har bir qadamda bir bit qiymatni shifrlaydi?

=====

# A5/1

=====

RC4

=====

RSA

=====

AES

+++++

AES algoritmi qaysi tarmoq asosida qurilgan?

=====

# SP

=====

Feystel

=====

Petri

=====

Petri va SP

+++++

AES shifrlash algoritmi nomini kengaytmasini ko'rsating?

=====

# Advanced Encryption Standard

=====

Advanced Encoding Standard

=====

Advanced Encryption Stadium

=====

Always Encryption Standard

+++++

A5/1 shifrlash algoritmi bu?

=====

# oqimli shifrlash algoritmi

=====

ochiq kalitli shifrlash algoritmi

=====

assimetrik shifrlash algoritmi

=====

blokli shifrlash algoritmi

+++++

RC4 shifrlash algoritmi bu?

=====

# oqimli shifrlash algoritmi

=====

ochiq kalitli shifrlash algoritmi

=====

asimetrik shifrlash algoritmi

=====

blokli shifrlash algoritmi

+++++

DES shifrlash algoritmi bu?

=====

# blokli shifrlash algoritmi

=====

oqimli shifrlash algoritmi

=====

ochiq kalitli shifrlash algoritmi

=====

asimetrik shifrlash algoritmi

+++++

AES shifrlash algoritmi bu?

=====

# blokli shifrlash algoritmi

=====

oqimli shifrlash algoritmi

=====

ochiq kalitli shifrlash algoritmi

=====

asimetrik shifrlash algoritmi

+++++

Mantiqiy XOR amalining asosi qanday hisoblashga asoslangan?

=====

# mod2 bo'yicha qo'shishga

=====

mod2 bo'yicha ko'paytirishga

=====

mod2 bo'yicha darajaga ko'tarishga

=====

mod2 bo'yicha bo'lishga

+++++

AES shifrlash standarti qaysi davlat standarti?

=====

# AQSH

=====

Rossiya

=====

Buyuk Britaniya

=====

Germaniya

Kolliziya hodisasi qaysi turdagi algoritmlarga xos?

=====

#xesh funksiyalar

=====

ochiq kalitli shifrlash algoritmlari

=====

simmetrik shifrlash algoritmlari

=====

kalitlarni boshqarish tizimlari

+++++

DES da S blok kanday funktsiya bajaradi?

=====

#6 bitli blokni 4 bitga almashtiradi

=====

8 bitli blokni 4 bitga almashtiradi

=====

6 bitli blokni 6 bitga almashtiradi

=====

4 bitli blokni 8 bitga almashtiradi

+++++

MD5 xesh funktsiyada 48 bitli ma'lumot berilganda to'ldirish bitlari qanday to'ldiriladi?

=====

#bir bit 1, 399 ta 0, ma'lumot uzunligi qiymatining 64 bitli qiymati bilan

=====

bir bit 1, 399 ta 0, ma'lumot uzunligining dastlabki 64 bitli qiymati bilan

=====

bir bit 1, 463 ta 0, ma'lumot uzunligi qiymatining 64 bitli qiymati bilan

=====

bir bit 1, 463 ta 0, ma'lumot uzunligining dastlabki 64 bitli qiymati bilan

+++++



SHA1 xesh funksiyada 102 bitli ma'lumot berilganda to'ldirish bitlari qanday to'ldiriladi?

=====

#bir bit 1, 345 ta 0, ma'lumot uzunligi qiymatining 64 bitli qiymati bilan

=====

bir bit 1, 345 ta 0, ma'lumot uzunligining dastlabki 64 bitli qiymati bilan

=====

bir bit 1, 409 ta 0, ma'lumot uzunligi qiymatining 64 bitli qiymati bilan

=====

bir bit 1, 409 ta 0, ma'lumot uzunligining dastlabki 64 bitli qiymati bilan

+++++

Quyidagi ifoda nechta yechimga ega?  $3 \cdot x = 2 \pmod{7}$ .

=====

#bitta yechimga ega

=====

ikkita yechimga ega

=====

yechimga ega emas

=====

uchta yechimga ega

+++++

2 lik sanoq tizimida 0101 soniga 1111 sonini 2 modul bo'yicha qo'shing?

=====

#1010

=====

0101

=====

1111

=====

1001

+++++

143mod17 nechiga teng?

=====

#7

=====

6

=====

5

=====

8

+++++

A5/1 oqimli shifrlash algoritmida maj(1,0,1) ga teng bo'lsa qaysi registrlar suriladi?

=====

#birinchi va uchunchi registrlar suriladi

=====

faqat ikkinchi registr suriladi

=====

birinchi va ikkinchi registrlar suriladi

=====

faqat birinchi resgistr suriladi

+++++

Qalbakilashtirish hujumi qaysi turdagi hujum turiga kiradi?

=====

#Immitatsiya

=====

o'zgartirish

=====

Fabrication

=====

Chastotaviy tahlil

+++++

Sezar shifrlash algoritmida ochiq matn  $M=3$  ga, kalit  $K=7$  ga teng hamda  $p=26$  ga teng bo'sa shifr matn qiymati neciga teng bo'ladi?

=====

#10

=====

16

=====

18

=====

22

+++++

Qayday akslantirishdan foydalanilsa chastotalar tahlili kriptotahlil usuliga bardoshli bo'ladi

=====

#bigram akslantirishidan

=====

o'rniga qo'yish akslantirishidan

=====

o'rin almashtirish akslantirishidan

=====

xech qanday akslantirishdan foydalanish shart emas

+++++

Affin shifrlash algoritmda  $a=2$ ,  $b=3$ ,  $p=26$  hamda ochiq matn  $x=4$  ga teng bo'lsa, shifr matn qiymatini toping?

=====

#11

=====

27

=====

31

=====

41

+++++

A5/1 oqimli shifrlash algoritmda  $maj(1,0,1)$  ga teng bo'lsa maj kattalik qiymatini toping?

=====

#1

=====

0

=====

2

=====

3

+++++

A5/1 oqimli shifrlash algoritmda  $x_{18}=1$ ,  $y_{21}=0$ ,  $z_{22}=1$  ga teng bo'lsa kalitni qiymatini toping

=====

#0

=====

1

=====

2

=====

+++++

Vernam shifrlash algoritmida ochiq matn  $M=101$  ga, kalit  $K=111$  ga teng bo'lsa shifr matn qiymati qanday bo'ladi?

=====

#010

=====

101

=====

111

=====

110

+++++

Vernam shifrlash algoritmida shifr matn  $C=101$  ga, kalit  $K=111$  ga teng bo'lsa shifr matn qiymati qanday bo'ladi?

=====

#010

=====

101

=====

111

=====

110

+++++

3 sonini 5 chekli maydonda teskarisini toping?

=====

#2

=====

3

=====

4

=====

5

+++++

Qaysi algoritmda maj kattaligi ishlatiladi?

=====

#A5/1

=====

RC4

=====

MD5

=====

SHA1

+++++

MD5 xesh algoritmida nechta 32 bitli statik qiymatdan foydalanadi?

=====

#4

=====

8

=====

12

=====

16

+++++

SHA1 xesh algoritmda nechta 32 bitli statik qiymatdan foydalanadi?

=====

#5

=====

10

=====

15

=====

20

+++++

Qaysi xesh algoritmda 64 raund amal bajariladi?

=====

#MD5

=====

SHA1

=====

CRC

=====

MAC

+++++

Qaysi xesh algoritmda 80 raund amal bajariladi?

=====

#SHA1

=====

MD5

=====

CRC

=====

MAC

+++++

Kolliziya hodisasi deb nimaga aytiladi?

=====

#ikki xil matn uchun bir xil xesh qiymat chiqishi

=====

ikki xil matn uchun ikki xil xesh qiymat chiqishi

=====

bir xil matn uchun bir xil xesh qiymat chiqishi

=====

bir xil matn uchun ikki xil xesh qiymat chiqishi

+++++

Xesh-funktsiyani natijasi ...

=====

#fiksirlangan uzunlikdagi xabar

=====

Kiruvchi xabar uzunligidagi xabar

=====

Kiruvchi xabar uzunligidan uzun xabar

=====

+++++

OpenSSL nima?

=====

#Secure Sockets Layer (SSL) va kriptografiya vositalarini amalga oshiruvchi asosiy dasturdir



=====

Drayver

=====

Shifrlash kaliti

=====

Dehsifrlash kaliti

+++++

Sonning moduli qaysi matematik ifoda orqali aniqlanadi

=====

#Qoldiqli bo'lish

=====

Logarifmlash

=====

Faktorlash

=====

Darajaga oshirish

+++++

XOR amali qanday amal?

=====

#2 modul bo'yicha qo'shish

=====

$2^{64}$  modul bo'yicha qo'shish

=====

$2^{32}$  modul bo'yicha qo'shish

=====

$2^{48}$  modul bo'yicha qo'shish

+++++

AES shifrlash standartining mualliflari kimlar

=====

#Ridjmen va Deimen

=====

Feystel va Pascal

=====

Vijener va Verman

=====

Feystel va Verman

+++++

Agar  $a=19$  bo'lsa, u holda unga teskari bo'lgan sonni modul26 bo'lgan maydonda hisoblang.

=====

#11

=====

17 va 19

=====

19 va 11

=====

13 va 19

+++++

Agar  $a=9$  bo'lsa, u holda unga teskari bo'lgan sonni modul26 bo'lgan maydonda hisoblang.

=====

#3

=====

17 va 19

=====

19 va 11

=====

13 va 19

+++++

Alfavit – bu

=====

#axborotni shifrlash uchun ishlatiladigan chekli belgilar to`plami.

=====

axborotni kodlashtirish uchun ishlatiladigan diskret va cheksiz belgilar to`plami.

=====

axborotni kodlashtirish uchun ishlatiladigan diskret belgilar to`plami.

=====

axborotni kodlashtirish uchun ishlatiladigan cheksiz belgilar to`plami

+++++

Kalit – bu?

=====

#kalit – matnlarni shifrlash va deshifrlash uchun kerak bo`lgan axborot

=====

kalit – matnlarni o`zgartirish uchun uchun kerak bo`lgan ma`lumot

=====

kalit – matnlarni kodlashtirish uchun uchun kerak bo`lgan amal

=====

kalit – matnlarni shifrlash va deshifrlash uchun kerak bo`lgan fayl

+++++

Axborotni shifrlash uchun foydalaniladigan chekli sondagi belgilar to'plami ... deb ataladi

=====

#Alifbo

=====

Matn

=====

Kalit

=====

Axborot

+++++

Dastlabki ma'lumotni bevosita shifrlash va deshifrlash uchun zarur manba ... deb ataladi

=====

#Kalit

=====

Alifbo

=====

Axborot

=====

Tuzilma

+++++

..... shifrlash kaliti noma'lum bo'lgan holda shifrlangan ma'lumotni deshifrlashning qiyinlik darajasini belgilaydi.

=====

#Kriptobardoshlilik

=====

Tahlil qilish

=====

Deshifrlash

=====

## Kriptografik tizim

+++++

$12+11 \bmod 16$  ?

=====

#7

=====

12

=====

11

=====

23

+++++

RIJNDAEL algoritmi qancha uzunligdagi kalitlarni qo'llab quvvatlaydi.

=====

#128 bitli, 192 bitli, 256 bitli

=====

128 bitli, 192 bitli,

=====

192 bitli, 256 bitli

=====

128 bitli, 256 bitli

+++++

Ikkiilik sanoq tizimida berilgan 10111 sonini o'nlik sanoq tizimiga o'tkazing.

=====

#23

=====

20

=====

21

=====

19

+++++

Ikkilik sanoq tizimida berilgan 1010 sonini o'nlik sanoq tizimiga o'tkazing.

=====

#10

=====

20

=====

22

=====

19

+++++

Quyidagi modulli ifodani qiymatini toping.  $(125 \cdot 45) \bmod 10$ .

=====

#5

=====

15

=====

18

=====

25

+++++

Quyidagi modulli ifodani qiymatini toping.  $(125 \cdot 25) \bmod 10$ .

=====

#5

=====

15

=====

18

=====

25

+++++

Quyidagi ifodani qiymatini toping.  $-17 \bmod 11$

=====

#5

=====

6

=====

7

=====

11

+++++

Quyidagi ifodani qiymatini toping.  $-19 \bmod 26$

=====

#5

=====

6

=====

7

=====

11

+++++

10 raund davom etadigan blokli shifrlash algoritmi ko'rsating?

=====

# AES

=====

DES

=====

A5/1

=====

RC4

+++++

Vernam shifrlash algoritm asosi qaysi mantiqiy hisoblashga asoslangan

=====

# XOR

=====

ARX

=====

ROX

=====

XRA

+++++

Simmetrik shifrlash algorimtlarida qanday muammo mavjud?

=====

# kalitni uzatish

=====

kalit generatsiyalash

=====

kalitni saqlash

=====



kalitni yo'q qilish

+++++

Konfidensiallikni ta'minlash bu -?

=====

# ruxsat etilmagan "o'qishdan" himoyalash

=====

ruxsat etilmagan "yozishdan" himoyalash

=====

ruxsat etilmagan "bajarishdan" himoyalash

=====

ruxsat berilgan "amallarni" bajarish

+++++

Foydanaluvchanlikni ta'minlash bu -?

=====

# ruxsat etilmagan "bajarishdan" himoyalash

=====

ruxsat etilmagan "yozishdan" himoyalash

=====

ruxsat etilmagan "o'qishdan" himoyalash

=====

ruxsat berilgan "amallarni" bajarish

+++++

Butunlikni ta'minlash bu - ?

=====

# ruxsat etilmagan "yozishdan" himoyalash

=====

ruxsat etilmagan “bajarishdan” himoyalash

=====

ruxsat etilmagan “o‘qishdan” himoyalash

=====

ruxsat berilgan “amallarni” bajarish

+++++

.... kriptotizimni shifrlash va rasshifrovkalash uchun sozlashda foydalaniladi.

=====

# kalit

=====

ochiq matn

=====

alifbo

=====

algoritm

+++++

Agar ochiq ma’lumot shifrlansa, natijasi .... bo‘ladi.

=====

# shifrmtn

=====

ochiq matn

=====

noma’lum

=====

kod

+++++

Rasshifrovkalash jarayonida kalit va ..... kerak bo‘ladi

=====

# shifrmtn

=====

ochiq matn

=====

kodlash

=====

alifbo

+++++

Ma’lumotni sakkizlik sanoq tizimidan o‘n oltilik sanoq tizimiga o‘tkazish bu?

=====

# kodlash

=====

shifrlash

=====

yashirish

=====

rasshifrovkalash

+++++

Qaysi algoritmlar simmetrik blokli shifrlarga tegishli?

=====

# AES, DES

=====

A5/1, AES

=====

Sezar, AES

=====

Vijiner, DES

+++++

A5/1 oqimli shifrlash algoritmida maxfiy kalit necha registrga bo'linadi?

=====

# 3

=====

4

=====

5

=====

6

+++++

A5/1 oqimli shifrlash algoritmida X registr uzunligi nechi bitga teng?

=====

# 19

=====

17

=====

16

=====

15

+++++

A5/1 oqimli shifrlash algoritmida Y registr uzunligi nechi bitga teng?

=====

# 22

=====

21

=====

19

=====

20

+++++

A5/1 oqimli shifrlash algoritmida Z registr uzunligi nechi bitga teng?

=====

# 23

=====

20

=====

19

=====

18

+++++

Sezar shifrlash algoritmida shifrlash formulasi qanday?

=====

#  $C=(M+K) \bmod p$

=====

$C=(M-K) \bmod p$

=====

$C=(M*K) \bmod p$

=====

$C=(M/K) \bmod p$

+++++

Sezar shifrlash algoritmda rasshifrovkalash formulasi qanday?

=====

#  $M = (C - K) \bmod p$

=====

$M = (C + K) \bmod p$

=====

$M = (C * K) \bmod p$

=====

$M = (C / K) \bmod p$

+++++

DES shifrlash algoritmda kalit uzunligi necha bitga teng?

=====

# 56

=====

512

=====

192

=====

256

+++++

DES shifrlash algoritmda har bir raunda necha bitli raund kalitlaridan foydalaniladi?

=====

# 48

=====

56

=====

64

=====

32

+++++

Qaysi blokli shifrlash algoritmda raund kalit uzunligi qiymatiga bo'g'liq?

=====

#AES

=====

DES

=====

IDEA

=====

RSA

+++++

AES algoritmda shifrlash kalitining uzunligi necha bitga teng?

=====

# 128, 192, 256 bit

=====

128, 156, 256 bit

=====

128, 192 bit

=====

256, 512 bit

+++++

Kriptologiya qanday yo'nalishlarga bo'linadi?

=====

# kriptografiya va kriptotahlil

=====

kriptografiya va kriptotizim

=====

kripto va kriptotahlil

=====

kriptoanaliz va kriptotizim

+++++

Kriptologiya nima bilan shug'ullanadi?

=====

# maxfiy kodlarni yaratish va buzish ilmi bilan

=====

maxfiy kodlarni buzish bilan

=====

maxfiy kodlarni yaratish bilan

=====

maxfiy kodlar orqali ma'lumotlarni yashirish bilan

+++++

Kriptografiya nima bilan shug'ullanadi?

=====

# maxfiy kodlarni yaratish bilan

=====

maxfiy kodlarni buzish bilan

=====

maxfiy kodlar orqali ma'lumotlarni yashirish bilan

=====

shifrlash uslublarini bilmagan holda shifrlangan ma'lumotni asl holatini topish bilan



+++++

Kriptotahlil nima bilan shug'ullanadi?

=====

# maxfiy kodlarni buzish bilan

=====

maxfiy kodlarni yaratish bilan

=====

maxfiy kodlar orqali ma'lumotlarni yashirish bilan

=====

shifrlash uslublarini bilmagan holda shifrlangan ma'lumotni asl holatini topish bilan

+++++

Shifrlash orqali ma'lumotning qaysi xususiyati ta'minlanadi?

=====

# maxfiyligi

=====

butunliligi

=====

ishonchliligi

=====

foydalanuvchanligi

+++++

Steganografiya ma'lumotni qanday maxfiylashtiradi?

=====

# maxfiy xabarni soxta xabar ichiga berkitish orqali

=====

maxfiy xabarni kriptografik kalit yordamida shifrlash orqali

=====

maxfiy xabarni shifrlash orqali

=====

maxfiy xabarni kodlash orqali

+++++

Kriptologiya necha yo‘nalishga bo‘linadi?

=====

# 2

=====

4

=====

6

=====

8

+++++

Kriptologiya so‘zining ma’nosi?

=====

# cryptos – maxfiy, logos – ilm

=====

cryptos – kodlash, logos – ilm

=====

cryptos – kriptologiya, logos – yashiraman

=====

cryptos – maxfiy, logos – kalit

+++++

Ximoyalanuvchi ma'lumot boshqa bir ma'lumotni ichiga yashirish orqali maxfiyligini ta'minlaydigan usul qaysi?

=====

# steganografiya

=====

kodlash

=====

shifrlash

=====

autentifikatsiya

+++++

Baytlar kesimida shifrlashni amalga oshiradigan algoritm keltirilgan qatorni ko'rsating?

=====

# RC4

=====

A5/1

=====

SHA1

=====

MD5

+++++

Zamonaviy kriptografiya qaysi bo'limlarni o'z ichiga oladi?

=====

# simmetrik kriptotizimlar, ochiq kalitli kriptotizimlar, elektron raqamli imzo kriptotizimlari, kriptobardoshli kalitlarni ishlab chiqish va boshqarish

=====

simmetrik kriptotizimlar, ochiq kalit algoritmiga asoslangan kriptotizimlar, elektron raqamli imzo kriptotizimlari, foydalanuvchilarni ro'yxatga olish

=====

simmetrik kriptotizimlar, ochiq kalit algoritmiga asoslangan kriptotizimlar, elektron raqamli imzo kriptotizimlari, foydalanuvchilarni autentifikatsiyalash

=====

simmetrik kriptotizimlar, ochiq kalit algoritmiga asoslangan kriptotizimlar, elektron raqamli imzo kriptotizimlari, foydalanuvchilarni identifikatsiya qilish

+++++

Kriptotizimlar kalitlar soni bo'yicha necha turga bo'linadi?

=====

# 2

=====

4

=====

6

=====

8

+++++

Kriptotizimlar kalitlar soni bo'yicha qanday turga bo'linadi?

=====

# simmetrik va assimetrik turlarga

=====

simmetrik va bir kalitli turlarga

=====

3 kalitli turlarga

=====

assimetrik va 2 kalitli turlarga

+++++

Ma'lumotlarni kodlash va dekodlashda necha kalitdan foydalanadi?

=====

# kalit ishlatilmaydi

=====

4 ta

=====

2 ta

=====

3 ta

+++++

Simmetrik kriptotizimlarda necha kalitdan foydalaniladi?

=====

# 1 ta

=====

3 ta

=====

4 ta

=====

kalit ishlatilmaydi

+++++

Assimetrik kriptotizimlarda necha kalitdan foydalaniladi?

=====

# 2 ta

=====

3 ta

=====

4 ta

=====

kalit ishlatilmaydi

+++++

Kalit bardoshliligi bu -?

=====

# eng yaxshi ma'lum algoritm bilan kalitni topish murakkabligidir

=====

eng yaxshi ma'lum algoritm yordamida yolg'on axborotni ro'kach qilishdir

=====

nazariy bardoshlilik

=====

amaliy bardoshlilik

+++++

O'rniga qo'yish shifrlash sinfiga qanday algoritmlar kiradi?

=====

# shifrlash jarayonida ochiq ma'lumot alfaviti belgilari shifr ma'lumot belgilariga almashtiriladigan algoritmlar

=====

shifrlash jarayonida ochiq ma'lumot alfaviti belgilarining o'rinlar almashtiriladigan algoritmlar

=====

shifrlash jarayonida o'rniga qo'yish va o'rin almashtirish akslantirishlarning kombinatsiyalaridan birgalikda foydalaniladigan algoritmlar

=====

shifrlash jarayonida kalitlarning o'rni almashtiriladigan algoritmlarga

+++++

O'rniga qo'yish shifrlash algoritmlari qanday sinfga bo'linadi?

=====

# bir qiymatli va ko'p qiymatli shifrlash

=====

ko'p qiymatli shifrlash

=====

bir qiymatli shifrlash

=====

uzluksiz qiymatli shifrlash

+++++

Ko'p qiymatli shifrlash qanday amalga oshiriladi?

=====

# ochiq ma'lumot alfaviti belgilarining har biriga shifr ma'lumot alfavitining ikkita yoki undan ortiq chekli sondagi belgilari mos qo'yiladi

=====

ochiq ma'lumot alfaviti belgilarining har ikkitasiga shifr ma'lumot alfavitining ikkita yoki undan ortiq chekli sondagi belgilari mos qo'yiladi

=====

ochiq ma'lumot alfaviti belgilarining har biriga shifr ma'lumot alfavitining bitta belgisi mos qo'yiladi

=====

ochiq ma'lumot alfaviti belgilarining har juftiga shifr ma'lumot alfavitining bitta belgisi mos qo'yiladi

+++++

A5/1 oqimli shifrlash algoritmi asosan qayerda qo'llaniladi?

=====

# mobil aloqa standarti GSM protokolida

=====

simtsiz aloqa vositalaridagi mavjud WEP protokolida

=====

internet trafiklarini shifrlashda

=====

radioaloqa tarmoqlarida

+++++

RC4 oqimli shifrlash algoritmi asosan qayerda qo'llaniladi?

=====

# simsiz aloqa vositalaridagi mavjud WEP protokolda

=====

mobil aloqa standarti GSM protokolda

=====

internet trafiklarini shifrlashda

=====

radioaloqa tarmoqlarda

+++++

A5/1 oqimli shifrlash algoritmida dastlabki kalit uzunligi nechi bitga teng?

=====

# 64

=====

512

=====

192

=====

256

+++++

A5/1 oqimli shifrlash algoritmida har bir qadamda kalit oqimining qanday qiymatini hosil qiladi?

=====

# bir biti

=====

bir bayti

=====

64 biti

=====

8 bayti



+++++

RC4 oqimli shifrlash algoritmda har bir qadamda kalit oqimining qanday qiymatini hosil qiladi?

=====

# bir baytini

=====

bir bitini

=====

64 bitini

=====

8 baytini

+++++

Blokli shifrlash algoritmlari arxitekturalari jihatidan qanday tarmoqlarga bo'linadi?

=====

# Feystel va SP

=====

SP va Petri

=====

Feystel va Petri

=====

Kvadrat va iyerarxik

+++++

DES shifrlash algoritmda raundlar soni nechta?

=====

# 16

=====

32

=====

64

=====

128

+++++

AES algoritmda raundlar soni nimaga bo'g'liq?

=====

# kalit uzunligiga

=====

kiruvchi blok uzunligi va matn qiymatiga

=====

foydalanilgan vaqtiga

=====

kiruvchi blok uzunligiga

+++++

Qaysi maxfiylikni ta'minlash usulida kalitdan foydalanilmaydi?

=====

# kodlash

=====

shifrlash

=====

steganografiya

=====

autentifikatsiya

+++++

Bitlar kesimida shifrlashni amalga oshiradigan algoritm keltirilgan qatorni ko'rsating?

=====

# A5/1

=====

RC4

=====

SHA1

=====

MD5

+++++

Qaysi hujum turida barcha bo'lishi mumkin bo'lgan variantlar ko'rib chiqiladi?

=====

# qo'pol kuch hujumi

=====

chastotalar tahlili

=====

analitik hujum

=====

sotsial injineriya

+++++

Sezar shifrlash algoritmi qaysi turdagi akslantirishga asoslangan?

=====

# o'rniga qo'yish

=====

o'rin almashtirish

=====

kompozitsion

=====

aralash

+++++

Vijiner shifrlash algoritmi qaysi turdagi akslantirishga asoslanadi?

=====

# o'rniga qo'yish

=====

o'rin almashtirish

=====

kompozitsion

=====

aralash

+++++

A5/1 oqimli shifrlash algoritmida registrlarning surilishi qanday kattalikka bog'liq?

=====

# maj funksiyasi qiymatiga

=====

kalit qiymatiga

=====

registr uzunligi qiymatiga

=====

hech qanday kattalikka bog'liq emas

+++++

16 raund davom etadigan blokli shifrlash algoritmi ko'rsating?

=====

# DES

=====

AES

=====

A5/1

=====

RC4

+++++

Ma'lumotni shifrlash va deshifrlash uchun bir xil kalitdan foydalanuvchi tizim bu?

=====

# simmetrik kriptotizim

=====

ochiq kalitli kriptotizim

=====

assimetrik kriptotizim

=====

xesh funksiyalar

+++++

Ikki kalitli deyilganda qaysi kriptotizim nazarda tutiladi?

=====

# ochiq kalitli kriptotizim

=====

simmetrik kriptotizim

=====

xesh funksiyalar

=====

MAC tizimlari

+++++

Ma'lumotni mavjudligini yashirishni maqsad qilgan bilim sohasi bu?

=====

# steganografiya

=====

kriptografiya

=====

kodlash

=====

kriptotahlil

+++++

Ma'lumotni konfidensialligini ta'minlash uchun ..... zarur.

=====

# shifrlash

=====

kodlash

=====

deshifrlash

=====

rasshifrovkalash

+++++

Ma'lumotni uzatishda kriptografik himoya .....

=====

# konfidensiallik va yaxlitlikni ta'minlaydi

=====

konfidensiallik va foydalanuvchanlikni ta'minlaydi

=====

foydalanuvchanlik va butunlikni ta'minlaydi

=====

konfidensiallikni ta'minlaydi

+++++

Qadimiy davr klassik shifriga quyidagilarning qaysi biri tegishli?

=====

# Sesar

=====

kodlar kitobi

=====

Enigma shifri

=====

DES, AES shifri

+++++

Kompyuter davriga tegishli shifrlarni aniqlang?

=====

# DES, AES shifri

=====

kodlar kitobi

=====

Sesar

=====

Enigma shifri

+++++

.... shifrlar blokli va oqimli turlarga ajratiladi

=====

# simmetrik

=====

ochiq kalitli

=====

assimetrik

=====

klassik

+++++

Tasodifiy ketma-ketliklarni generatsiyalashga asoslangan shifrlash turi bu?

=====

# oqimli shifrlar

=====

blokli shifrlar

=====

ochiq kalitli shifrlar

=====

assimetrik shifrlar

+++++

Ochiq matn qismlarini takror shifrlashga asoslangan usul bu?

=====

# blokli shifrlar

=====

oqimli shifrlar

=====

ochiq kalitli shifrlar

=====

assimetrik shifrlar



+++++

A5/1 shifri qaysi turga mansub?

=====

# oqimli shifrlar

=====

blokli shifrlar

=====

ochiq kalitli shifrlar

=====

assimetrik shifrlar

+++++

RC/4 shifri qaysi turga mansub?

=====

# oqimli shifrlar

=====

blokli shifrlar

=====

ochiq kalitli shifrlar

=====

assimetrik shifrlar

+++++

Pollard usuli qanday matematik muammoni yechadi?

=====

# Faktorlash

=====

Diskret logarifmlash

=====

Ratsional nuqtalarni aniqlash

=====

Sonning kvadrat ildizini hisoblash

+++++

Kvadratik g'alvir usuli qanday matematik muammoni yechadi?

=====

# Faktorlash

=====

Diskret logarifmlash

=====

Ratsional nuqtalarni aniqlash

=====

Kvadrat ildiz

+++++

Sonlarni tublikka tekshirish algoritmlari nechta sinfga bo'linadi?

=====

#ikkita sinfga

=====

uchta sinfga

=====

bitta sinfga

=====

sinflarga bo'linmaydi

+++++

RSA algoritmining mualliflarini ko'rsating

=====

#R. Rayvest, A. Shamir, L. Adleman

=====

Diffi va M. Xellman

=====

R. Rayvest, K. Xellman, L. Adleman

=====

L. Adleman, El Gamal, K. Shnorr

+++++

Ochiq kalitli shifrlash algoritmi keltirilgan qatorni toping?

=====

#RSA

=====

AES

=====

DES

=====

RC4

+++++

Ochiq kalitli shifrlash algoritmi keltirilgan qatorni toping?

=====

#El-Gamal

=====

AES

=====

DES

=====

RC4

+++++

Faqat simmetrik algoritm keltirilgan qatorni ko'rsating?

=====

#AES

=====

RSA

=====

El-Gamal

=====

Barcha javoblar to'g'ri

+++++

Faktorlash muammosini yechishning Pollard usulida eng kichik polinom qanday tanlanadi?

=====

#x^2+1

=====

x+1

=====

X

=====

x^2

+++++

Ferma testi qanday turdagi tublikka testlovchi algoritm hisoblanadi?

=====

#ehtimollik testlar tarkibiga kiruvchi algoritm

=====

aniqlashtirilgan testlar tarkibiga kiruvchi algoritm

=====

taqribiy testlar tarkibiga kiruvchi algoritm

=====

tublikka teslovchi algoritm hisoblanmaydi

+++++

Solovey Shtrassen testi qanday turdagi tublikka testlovchi algoritm hisoblanadi?

=====

#ehtimollik testlar tarkibiga kiruvchi algoritm

=====

aniqlashtirilgan testlar tarkibiga kiruvchi algoritm

=====

taqribiy testlar tarkibiga kiruvchi algoritm

=====

tublikka teslovchi algoritm hisoblanmaydi

+++++

Rabbi-Milner testi qanday turdagi tublikka testlovchi algoritm hisoblanadi?

=====

#ehtimollik testlar tarkibiga kiruvchi algoritm

=====

aniqlashtirilgan testlar tarkibiga kiruvchi algoritm

=====

taqribiy testlar tarkibiga kiruvchi algoritm

=====

tublikka teslovchi algoritm hisoblanmaydi

+++++

Elliptik egriz chiqizlarda nuqtalar usitda qanday ammalar bajariladi?

=====

#nuqtalarni qo'shish va nuqtalarni ikkilantirish

=====

nuqtalarni qo'shish va nuqtalarni ko'paytirish

=====

nuqtalarni qo'shish va nuqtalarni bo'lish

=====

nuqtalarni ayirish va nuqtalarni ko'paytirish

+++++

1 ga va o'ziga bo'linadigan sonlar qanday sonlar hisoblanadi?

=====

#tub sonlar

=====

murakkab sonlar

=====

toq sonlar

=====

juft sonlar

+++++

Elektron hujjat manbaini haqiqiyligini qaysi amal orqali amalga oshiriladi?

=====

#ERI orqali amalga oshiriladi

=====

shifrlash algoritmi orqali amalga oshiriladi

=====

kodlash orqali amalga oshiriladi

=====

autentifikatsiya orqali amalga oshiriladi

+++++

Elektron hujjat manbaini yaxlitligini tekshirish qaysi amal orqali amalga oshiriladi?

=====

#ERI orqali amalga oshiriladi

=====

shifrlash algoritmi orqali amalga oshiriladi

=====

kodlash orqali amalga oshiriladi

=====

autentifikatsiya orqali amalga oshiriladi

+++++

Elektron hujjatda mualliflikdan bosh tortmasligini tekshirish qaysi amal orqali amalga oshiriladi?

=====

#ERI orqali amalga oshiriladi

=====

shifrlash algoritmi orqali amalga oshiriladi

=====

kodlash orqali amalga oshiriladi

=====

autentifikatsiya orqali amalga oshiriladi

+++++

Faktorlash muammosini yechishning Pollard usulida funksiya argumenti boshlangich qiymati nechiga teng bo'ladi?

=====

#2

=====

1

=====

3

=====

0

+++++

Raqamli imzoni shakllantirish muolajasi qaysi algoritmgaga tegishli?

=====

#ERI algoritmgaga

=====

kodlash algoritmgaga

=====

shifrlash algoritmgaga

=====

steganografiya algoritmgaga

+++++

O'zDSt 1092:2009 standarti qaysi davlat standarti hisoblanadi?

=====

#O'zbekiston

=====

AQSH

=====

Rossiya

=====

Kanada

+++++

ГОСТ Р 34.10-94 standarti qaysi davlat standarti hisoblanadi?

=====

O'zbekiston

=====

AQSH

=====

#Rossiya

=====

Kanada

+++++

DSA qanday standart hisoblanadi?

=====

#ERI standarti

=====

shifrlash standarti

=====

kodlash standarti

=====

steganografik standart

+++++

Ochiq kalitli kriptotizimlarning matematik asosi nimaga asoslangan?

=====

#oson hisoblanadigan bir tomonlama funksiyalarga

=====

modulyar arifmetikaga

=====

faktORIZatsiyalashga

=====

diskret logarifmlashga

+++++

Faqat tub son keltirilgan qatorni toping?

=====

#3, 5

=====

5, 15



=====

16, 2

=====

3, 18

+++++

Ehtimolli testlar sonlarni tublikka tekshirishda qanday natijani beradi?

=====

#tekshirilayotgan son tub yoki tubmasligi haqida ehtimollik bilan javob beradi

=====

tekshirilayotgan son tub yoki tubmasligi haqida kafolatlangan aniq javob beradi

=====

tekshirilayotgan son tub yoki tubmasligi haqida tasodifiy ravishda javob beradi

=====

tekshirilayotgan son tub yoki tubmasligini 0 va 1 qiymatlarga qarab javob beradi

+++++

Ochiq kalitli RSA shifrlash algoritmi bardoshliligi qanday matematik muammo turiga asoslangan?

=====

#faktorlash murakkabligiga

=====

diskret logarifmlash murakkabligiga

=====

elliptik egri chiqizlarda faktorizatsiyalash murakkabligiga

=====

elliptik egri chiziqlarda faktorizatsiyalash murakkabligiga

+++++

Ochiq kalitli Rabin shifrlash algoritmi bardoshliligi qanday matematik muammo turiga asoslangan?

=====

#faktorlash murakkabligiga

=====

diskret logarifmlash murakkabligiga

=====

elliptik egri chiqizlarda faktorizatsiyalash murakkabligiga

=====

elliptik egri chiziqlarda faktorizatsiyalash murakkabligiga

+++++

Ochiq kalitli El-Gamal shifrlash algoritmi bardoshliligi qanday matematik muammo turiga asoslangan?

=====

faktorlash murakkabligiga

=====

#diskret logarifmlash murakkabligiga

=====

elliptik egri chiqizlarda faktorizatsiyalash murakkabligiga

=====

elliptik egri chiziqlarda faktorizatsiyalash murakkabligiga

+++++

Diffie-Helman algoritmi qanday matematik murakkablikka asoslanadi?

=====

faktorlash murakkabligiga

=====

#diskret logarifmlash murakkabligiga

=====

elliptik egri chiqizlarda faktorizatsiyalash murakkabligiga

=====

elliptik egri chiziqlarda faktorizatsiyalash murakkabligiga

+++++

ERI algoritmlari qanday muolajalalardan iborat?

=====

#imzoni shakllantirish, imzoni tekshirish

=====

imzoni shakllantirish, imzo qo'yish va imzoni tekshirish

=====

imzoni shakllantirish va imzo qo'yish

=====

imzo qo'yish

+++++

Ochiq kalitli kriptotizimlarda elektron hujjatlarga imzo qo'yish qaysi kalit orqali amalga oshiriladi?

=====

#shaxsiy kalit orqali

=====

ochiq kalit orqali

=====

imzo qo'yilishi kalitga bog'liq emas

=====

imzo qo'lda qo'yiladi

+++++

RSA shifrlash algoritmidan tanlangan p va q sonlarga qanday talab qo'yiladi?

=====

#tub bo'lishi

=====

o'zaro tub bo'lishi

=====

butun son bo'lishi

=====

toq son bo'lishi

+++++

Diskret logarifmlash murakkabligiga asoslangan algoritmlar keltirilgan qatorni ko'rsating?

=====

#Diffie-Hellman, EL-Gamal algoritmi

=====

RSA algoritmi

=====

EL-Gamal algoritmi

=====

## Diffie-Hellman algoritmi

+++++

RSA algoritmidagi  $p$ ,  $q$  tub sonlar bo'lsa, modul qiymati  $N$  qanday topiladi?

=====

# $N=p*q$

=====

$N=p/q$

=====

$N=q/p$

=====

$N=p-q$

+++++

RSA shifrlash algoritmidagi qaysi parametrlar ochiq holda e'lon qilinadi?

=====

#ochiq kalit –  $e$ , hamda modul qiymati -  $N$

=====

maxfiy kalit –  $d$ , hamda modul qiymati –  $N$

=====

ochiq kalit –  $e$ , hamda tub sonlar –  $p, q$

=====

maxfiy kalit –  $d$ , hamda tub sonlar –  $p, q$

+++++

Diffie-Hellman algoritmi qanday hujumga bardoshsiz hisoblanadi?

=====

#o'rtada turgan odam hujumiga

=====

chastotalar tahlili hujumiga

=====

yon kanal tahlili hujumiga

=====

to'liq tanlash hujumiga

+++++

Qaysi algoritim o'rtada turgan odam hujumiga bardoshsiz hisoblanadi?

=====

#Diffie-Hellman

=====

RSA

=====

ElGama

=====

DSA

+++++

Qanday sonlar murakkab sonlar deyiladi?

=====

#ko'paytuvchilarga ajraladigan sonlar murakkab sonlar deyiladi

=====

ko'paytuvchilarga ajralmaydigan sonlar murakkab sonlar deyiladi

=====

ko'paytuvchilarga ajralmaydigan toq sonlar sonlar murakkab sonlar deyiladi

=====

ko'paytuvchilarga ajraladigan juft sonlar murakkab sonlar deyiladi

+++++

Ochiq kalitli RSA shifrlash algoritmida ochiq kalit "e" qanday topiladi?

=====

# $\varphi(N)$  bilan o'zaro tub va undan kichik bo'lgan son tanlanadi

=====

$\varphi(N)$  dan kichik tub son tanlanadi

=====

$\varphi(N)$  dan katta tub son tanlanadi

=====

$\varphi(N)$  ning tub ko'paytuvchilaridan biri tanlanadi

+++++

Ochiq kalitli RSA shifrlash algoritmda maxfiy kalit qanday topiladi?

=====

# $e*d=1 \bmod \varphi(p*q)$  taqqoslamadan

=====

$e*d=1 \bmod N$

=====

$e*d=1 \bmod \varphi(p-1)$

=====

$e*d=1 \bmod \varphi((p-1)(q-1))$

+++++

Ochiq kalitli RSA shifrlash algoritmda "e" ochiq kalit, "d" shaxsiy kalit bo'lsa deshifrlash formulasi to'g'ri ko'rsatilgan qatorni belgilang?

=====

# $M=C^d \bmod N$

=====

$M=C^d \bmod \varphi(N)$

=====

$M=C^e \bmod N$

=====

$M=C^e \bmod \varphi(N)$

+++++

Ochiq kalitli RSA shifrlash algoritmda "d" shaxsiy kalit, "e" ochiq kalit bo'lsa shifrlash formulasi to'g'ri ko'rsatilgan qatorni belgilang?

=====

# $C=M^e \bmod N$

=====

$C=M^e \bmod \varphi(N)$

=====

$C=M^d \bmod \varphi(N)$

=====

$C=M^d \bmod N$

+++++

Ochiq kalitli RSA shifrlash algoritmida "p" tub son bo'lsa Eyler funskiyasi  $\varphi(p)$  qanday qiymat qaytaradi?

=====

#p-1

=====

P

=====

$\varphi(p)$

=====

$\varphi(p-1)$

+++++

Ochiq kalitli RSA shifrlash algoritmida "p=7" tub son bo'lsa Eyler funskiyasi  $\varphi(p)$  qanday qiymat qaytaradi?

=====

#6

=====

7

=====

$\varphi(7)$

=====

$\varphi(6)$

+++++

Faktorlash muammosini bartaraf etuvchi usul keltirilgan qatorni ko'rsating?

=====

#Pollard usuli

=====

Xitoy teoremasi

=====

Pohlig-Hellman usuli

=====

RSA usuli

+++++

RSA algoritmidagi matematik murakkablikni qanday usul orqali bartaraf qilish mumkin?

=====

#Pollard usuli

=====

Xitoy teoremasi

=====

Pohlig-Hellman usuli

=====

RSA usuli

+++++

Diskret logarifmlash muammosini bartaraf etuvchi usul keltirilgan qatorni ko'rsating?

=====

#Pohlig-Hellman usuli

=====

Pollard usuli

=====

Xitoy teoremasi

=====

RSA usuli

+++++

Pohlig-Hellman usuli qanday turdagi matematik murakkablikni yechishda foydalaniladi?

=====

#diskret logarifmlash murakkabligini

=====

faktirlash murakkabligini

=====

elliptik egrzi chiziqda faktirlash murakkabligini

=====

daraja parameter murakkabligini

+++++



El-Gamal algoritmidagi matematik murakkablikni qanday usul orqali bartaraf qilish mumkin?

=====

#Pohlig-Hellman usulu

=====

Pollard usuli

=====

Xitoy teoremasi

=====

El-Gamal usuli

+++++

Malumotni shifrlash va deshifrlashda turli kalitlardan foydalanuvchi algoritmni ko'rsating?

=====

#RSA

=====

AES

=====

DES

=====

RC4

+++++

Aniqlashtirilgan testlar sonlarni tublikka tekshirishda qanday natijani beradi?

=====

#tekshirilayotgan son tub yoki tubmasligi haqida kafolatlangan aniq javob beradi

=====

tekshirilayotgan son tub yoki tubmasligi haqida tasodifiy ravishda javob beradi

=====

tekshirilayotgan son tub yoki tubmasligi haqida ehtimollik bilan javob beradi

=====

tekshirilayotgan son tub yoki tubmasligini 0 va 1 oraliqdagi qiymatlarga qarab javob beradi

+++++

Sonlarni tublikka tekshirishning Ferma testida qanday taqqoslamadan foydalaniladi?

=====

$a^{n-1} \equiv 1 \pmod{n}$

=====

$a^{\varphi(n)-1} \equiv 1 \pmod{n}$

=====

$a^{\varphi(n)} \equiv 1 \pmod{n}$

=====

$a^{n-1} \not\equiv 1 \pmod{n}$

+++++

Faktorlash – bu

=====

#Berilgan sonning tub ko‘paytuvchilarini topish

=====

Sonlar nazariyasining eng dastlabki masalalaridan biri

=====

Berilgan sonni biror amal yoki xususiyatga ko‘ra uning tashkil etuvchilari orqali ifodalanishi

=====

Berilgan to‘plamni uning tashkil etuvchilari orqali ifodalanishi

+++++

Kriptanaliz bilan ishlashadigan odamlar kimlar?

=====

# kriptografik tahlilchilar

=====

Shifr

=====

Hakkerlar

=====

dasturchilar

+++++

Brute force hujumi bu...

=====

#Mumkin bo'lgan barcha qiymatlarni haqiqiy qiymat aniqlanguncha tanlashga asoslangan hujum

=====

Lug'at hujumi

=====

O'rniga qo'yish

=====

Aktiv hujum

+++++

Kalit bardoshliligi bu....

=====

#ma'lum algoritmi bilan kalitni topish murakkabligi

=====

Yolg'on axborotni ro'kach qilish

=====

Tegishli matematik masalalarning yetarlicha o'rganilmaganligi

=====

Kalitlarni yetarlicha uzunlikka ega bo'lmasligi

+++++

Nazariy bardoshlilik bu....

=====

ma'lum algoritmi bilan kalitni topish murakkabligi

=====

Yolg'on axborotni ro'kach qilish

=====

#Tegishli matematik masalalarning yetarlicha o'rganilmaganligi

=====

Kalitlarni yetarlicha uzunlikka ega bo'lmasligi