**KRIPTOGRAFIYA 1**

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| **Qiyinlik darsjasi** | **Test topshirig`i** | **To`g`ri javob** | **Muqobil javob** | **Muqobil javob** | **Muqobil javob** |
| 1 | Sonning teskarisini toppish amali qanday algoritm yordamida amalga oshiriladi? | Kengaytirilgan Yevklid | Yevklid | Ferma teoremasi | Affin tizimi |
| 2 | Qaysi juftlik RSA algoritmining ochiq va yopiq kalitlarini ifodalaydi | {*d, e*} – ochiq, {*e, n*} – yopiq; | {*e, n*} – yopiq, {*d, n*} – ochiq; | {*d, n*} – yopiq, {*e, n*} – ochiq; | {*e, n*} – ochiq, {*d, n*} – yopiq; |
| 1 | DES shifrlash algoritmi bloki o‘lchami qanday | 64 bit | 128 bit | 48 bit | 56 bit |
| 1 | Blowfish algoritmi kaliti uzunligi qanday? | O‘zgaruvchan | 256 bit | 128 bit | 64 bit |
| 1 | Blowfish algoritmi raund akslantirishlari soni qancha? | 16 marta | 32 marta | 12 marta | Kirish bloki uzunligiga bog‘liq. |
| 1 | Blowfishda raund kaliti uzunligi qancha? | 32 bit | 24 bit | 16 bit | 128 bit |
| 1 | Blowfish algoritmi qanday tur kriptotizimga kiradi? | Simmetrik | Asimmetrik | Kompozitsiyali | Modifikatsiyalangan |
| 1 | Qanday manbaa asosida raund kalitlari yaratiladi? | Krish bloki uzunligiga bog‘liq holda. | Dastlabki berilgan blok asosida | Maxfiy kalit asosida | SHifrlangan blok asosida |
| 1 | Berilgan algoritmning kriptobardoshliligi nimaga asoslangan? | Kalit uzunligiga. | Mahfiy kalitni bilishga | SHifrlash jarayonini bajarilish vaqtiga | SHifrlash sikllari soniga |
| 2 | 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. |
| 2 | Blowfishda S-bloklar soni va o‘lchami qanday? | Har biri: 4, 256 bit | Har biri: 8, 32 bit | Har biri: 4, 128 bit | Har biri: 6, 64 bit |
| 2 | RSA algoritmida n-ochiq kalit, d-maxfiy kalit bo‘lsa, qaysi formula shifirlash jarayonini ifodalaydi? | C = Me mod n; | M = Cd mod n; | C = Med mod n; | C = Mn mod n. |
| 2 | RSA algoritmida n-ochiq kalit, d-maxfiy kalit bo‘lsa, ular uchun qaysi shart o‘rinli? | e va d o‘zaro tub sonlar; | Ushbu Me va Cd ifodalar barcha M < n uchun oson hisolanadiga1n bo‘lishi k1erak; | e va d-kalitlarga bog‘liq holda yana shunday p va q -sonlari mavjud bo‘lib, ular o‘zaro tub bo‘lishi kerak; | e va d –o‘zaro tub bo‘lmasligi kerak. |
| 1 | Qaysi juftlik RSA algoritmining ochiq va yopiq kalitlarini ifodalaydi | {d, n} – yopiq, {e, n} – ochiq; | {e, n} – yopiq, {d, n} – ochiq; | {d, e} – ochiq, {e, n} – yopiq; | {e, n} – ochiq, {d, n} – yopiq; |
| 1 | RSA algoritmining maxfiy kalitini topish qanday masalani echish murakkabligiga asoslanadi? | Katta sonni tub ko‘paytuvchilarga ajratish masalasining murakkabligiga; | p va q –tub sonlarni tanlash murakkabligiga; | Eyler funksiyasinianiqlashning murakkabligiga; | Diskret logarifimni xisoblash murakkabligiga; |
| 1 | RSA algoritmi maxfiy kaliti uzunligi qancha? | Ochiq kalit va Eyler funksiyasi bilan aniqlanadi; | Ixtiyoriy; | Ochiq kalit uzunligi bilan aniqlanadi; | Ochiq kalit uzunligiga teng; |
| 1 | Berilgan shifrlash algoritmi kaliti qanday asosga ko‘ra yaratiladi? | Ixtiyoriy | Berilgan blok asosida; | SHifrlangan blok asosida; | SHifrlash sikllari soni asosid |
| 1 | RSA shifrlash algoritmida foydalaniladigan sonlarning spektori o‘lchami qanday? | p va q –sonlarning ko‘paytmasini ifodalovchi sonning spektoriga teng; | 65536; | 65535; | 65537; |
| 2 | Berilgan algoritmning kriptobardoshligi qanday aniqlanadi? | Kalit uzunligi bilan; | SHifrlash jarayoni uchun ketgan vaqt bilan; | SHifrlash sikllari soni bilan; | Etarli katta butun sonni tub ko‘paytuvchilarga ajratish masalasining murakkabligiga; |
| 2 | DES, GOST 28147-89 algoritmlari i-shifrlash bloki uzunligi qancha? | 32 bit; | 64 bit; | 24 bit; | 16 bit; |
| 2 | DES algoritmi kaliti uzunligi qancha? | 64 bit; | 56 bit; | 48 bit; | 128 bit; |
| 1 | DES algoritmi akslantirishlari raundlari soni qancha? | 16; | 48; | 12; | 32; |
| 2 | DES da E-kengaytirish funksiyasining mohiyati qanday? | 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 kalitni 32 bitgacha kengaytiradi; |
| 2 | DES algoritmi Si – 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 kalit blokini 16 bitli blokka siqishdan iborat; |
| 2 | DES algoritmi dastlabki o‘rin almashtirish jadvalining o‘lchami qanday? | 8 x 8; | 4 x 8; | 6 x 8; | 8 x 12; |
| 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; |
| 2 | DES algoritmida raund kalitlari uzunligi qancha ? | 48 bit; | 24 bit; | 32 bit; | 16 bit; |
| 2 | 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 ; | 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 56 bitli raund kalitiga mod2 maydonda qo‘shish uchun 32 bitli blok 56 bitga kengaytiriladi. |
| 2 | DES algoritmida Si – 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 16 bitli blokka siqishdan iborat; |
| 1 | DES algoritmida bitlar o‘rinlarini almashtirilishini aniqlovchi boshlang‘ich jadval o‘lchami qanday? | 8 x 8; | 4 x 8; | 6 x 8; | 8 x 16; |
| 2 | DES algoritmida kalitlar generatsiyasi jadvali o‘lchovi qanday? | 8 x 8, algoritmda aniqlangan jadval bo‘yicha; | 4 x 8; | 6 x 8; | 8 x 8; |
| 1 | DES algoritmida 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. |
| 1 | DES algoritmida shifrlash natijasi qanday ifodalanadi? | Har biri 32 bitdan iborat bo‘lgan 2 qisimdan iborat; | Har biri 16 bitdan iborat bo‘lgan 4 qisimdan iborat; | Har biri 16 bitdan iborat bo‘lgan 2 qisimdan iborat; | Har biri 16 bitdan iborat bo‘lgan 6 qisimdan iborat; |
| 2 | GOST 28147-89 algoritmi kaliti uzunligi qancha? | 256 bit; | 128 bit; | 512 bit; | 64 bit; |
| 2 | GOST 28147-89 algoritmi raundlari soni qancha? | 32 ta; | 24 ta; | 48 ta; | 16 ta; |
| 2 | RSA algoritmining maxfiy kalitini topish qanday masalani echish murakkabligiga asoslanadi? | Katta sonni tub ko‘paytuvchilarga ajratish masalasining murakkabligiga; | p va q –tub sonlarni tanlash murakkabligiga; | Eyler funksiyasinianiqlashning murakkabligiga; | Diskret logarifimni xisoblash murakkabligiga; |
| 2 | RSA algoritmida n-ochiq kalit, d-maxfiy kalit bo‘lsa, qaysi formula shifirlash jarayonini ifodalaydi? | C = Me mod n; | M = Cd mod n; | C = Med mod n; | C = Mn mod n. |
| 2 | Blowfish shifrlash algoritmi bloki o‘lchami qancha? | 64 bit | 128 bit | 48 bit | 56 bit |
| 1 | Simmetrik shifrlash algoritmi bardoshligi nimaga asoslangan? | Kalit uzunligiga; | Mahfiy kalitni bilishga; | Ma’lumotnideshifrlash uchun ketadigan vaqtga; | Algoritm shifrlash raundlari soniga; |
| 1 | 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 tarqatish va aralashtirish beruvchi hamda elektron elementlarda qulay amalga oshirishni ta’minlaydigan barcha akslantirishlar asosida; |
| 1 | Ochiq ma’lumotni shifrlashning mohiyati nimadan iborat? | Ochiq ma’lumotning asl ma’nosini yashirishdan iborat. | Ochiq ma’lumotning asl ma’nosini oshkor qilishdan iborat | Ochiq ma’lumotning asl ma’nosini yashirish va oshkor qilishdan iborat | SHifr ma’lumotning asl ma’nosini yashirish va deshifrlashdan iborat |
| 2 | Qanday tur akslantirishlar mavjud va ularning farqlari qanday? | O‘rniga qo‘yish va o‘rin almashtirish, va ularning kombinatsiyalari | Faqat o‘rin almashtirish | Faqat kombinatsiyalashgan | Faqat o‘rniga qo‘yish |
| 2 | O‘rniga qo‘yish shifrlashning (akslantirishining) mohiyati qanday? | Ochiq ma’lumot belgilari shifr ma’lumot belgilariga kalit asosida almashtiriladi | Ochiq ma’lumot belgilari boshqa ochiq ma’lumot belgilariga almashtiriladi | Ochiq ma’lumot belgilari shifr ma’lumot belgilariga kalitsiz almashtiriladi | Ochiq ma’lumot belgilarini kalitsiz o‘rinlari almashtiriladi |
| 2 | O‘rin almashtirish shifrlashning (akslantirishining) mohiyati qanday? | Ochiq ma’lumot belgilari o‘rinlari kalit asosida almashtiriladi | Ochiq ma’lumot belgilari boshqa ochiq ma’lumot belgilariga almashtiriladi | Ochiq ma’lumot belgilari bloklari o‘rinlari almashtiriladi | Ochiq ma’lumot belgilari shifr ma’lumot belgilariga kalitsiz almashtiriladi |
| 2 | Gammalashtirish shifrlashning (akslantirishining) mohiyati qanday? | Ochiq ma’lumot belgilari shifr ma’lumot belgilariga biror amal bajarish bilan almashtiriladi | Ochiq ma’lumot belgilari bloklari o‘rinlari almashtiriladi | Ochiq ma’lumot belgilari o‘rinlari kalit asosida almashtiriladi | Ochiq ma’lumot belgilari shifr ma’lumot belgilariga kalitsiz almashtiriladi |
| 2 | Uzliksiz shifrlashning mohiyati nimada? | Ochiq ma’lumot alfaviti belgilari shifr ma’lumot alfaviti belgilariga alohida-alohida almashtiriladi | Ochiq ma’lumot alfaviti belgilari bloklari shifr ma’lumot alfaviti belgilari bloklariga almashtiriladi | Ochiq ma’lumot alfaviti belgilari shifr ma’lumot alfaviti belgilari bloklariga almashtiriladi | Ochiq ma’lumot alfaviti belgilari bloklari shifr ma’lumot alfaviti belgilariga almashtiriladi |
| 2 | 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 bloklab akslantirish imkoniyatiga ega |
| 2 | Uzliksiz shifrlashning qanday kriptografik kamchiliklari bor? | Sinxronlash buzilganda shifrlanish xatolari tarqaladi | Sinxronlashbuzilganda shifrlanish xatolari tarqamaydi | Sinxronlashbuzilmaganda shifrlanish xatolari tarqaladi | Sinxronlash buzilganda shifrlanish xatolari qisman tarqaladi. |
| 2 | 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. | Aakslantirishlarini apparat qurilmalarini amalga oshirish samarali, ammo tezligi yuqori emas. |
| 2 | Psevdotasodifiy ketma-ketlik ishlab chiqaruvchi generatorlari o‘zaro qanday farqlanadi? | Generatorlar algoritmlari akslantirishlarining xossalari bo‘yicha | SHifr ma’lumot alfaviti belgilari chastotaviy xarakteristikalari bo‘yicha | SHifr ma’lumot alfaviti alohida belgilarining chastotaviy xarakteristikalari bo‘yicha | SHifr ma’lumot bloklari chastotaviy xarakteristikalari belgilari bo‘yicha |
| 1 | Ochiq kalitli shifrlash algoritmlari bilan qanday kriptografik masalalar echiladi? | Konfidensiallik va autentifikatsiya masalalarini | Konfidensiallik va to‘lalik (butunlik) | To‘lalik (butunlik) | Konfidensiallik |
| 1 | Asimmetrik kriptotizimlar qanday matematik asoslarga ega? | Asimmetrik algoritmlar yuqori tartibli chiziqli algebraik tenglamalar sistemasini chekli maydonlarda echishning hisoblash murakkabligimasalasiga asoslanadi | Asimmetrik algoritmlar elliptik egri chiziq nuqtalari ustida amallar bajarishning hisoblash murakkabligi masalasiga asoslanadi | Asimmetrik algoritmlar etarli katta natural sonni tub ko‘paytuvchilarga ajratishning hisoblash murakkabligi masalasiga asoslanadi | Asimmetrik algoritmlar xarakteristikasi etarli katta bo‘lgan chekli maydonlarda diskret logarifmlashni hisoblash murakkabligi masalasiga asoslanadi |
| 1 | Simmetrik va asimmetrik shifrlash algoritmlarining qanday mohiyatan farqli tomonlari bor? | SHifrlash va deshifrlash jarayonlarida kalitlardan foydalanish qoidalariga ko‘ra farqlanadi | SHifrlash va deshifrlash jarayonlari uchun kalitlarni generatsiya qilish qoidalariga ko‘ra farqlanadi | SHifrlash va deshifrlash jarayonlarida kalitlarni almashish qoidalariga ko‘ra farqlanadi | Bardoshlilikni ta’minlovchi asoslarining har xilligi bilan farqlanadi |
| 2 | Xesh-funksiya qanday kriptografik masalalarni echishga qo‘llaniladi? | To‘lalik (butunlik) masalasini echishga | ERI masalasini echishga | Identifikatsiya masalasini echishga | Konfidensiallik masalasini echishga |
| 2 | ERI bilan qanday kriptografik masalalar echiladi? | Autentifikatsiyalash va to‘lalikni (butunlikni) | Autentif ikatsiyalash va konfidensiallini | Autentifikatsiyalash va kalitlar taqsimotini | Autentifikatsiyalash va kalitlar generatsiyasini |
| 2 | Asimmetrik kriptotizim foydalanuvchilari kalitlari qanday generatsiya qilinadi? | Algoritmning yaratilishiga asos bo‘lgan hisoblash murakkabligi asosida | Mahfiy va ochiq kalitlarni tasodifiy tanlash bilan | Mahfiy kalitlarni tasodifiy tanlash bilan | Ochiq kalitlarni tasodifiy tanlash bilan |
| 2 | Kriptotizim foydalanuvchilariga ularning kalitlari qanday tarqatiladi? | Kalitlarni tarqatish protokolining maxsus asimmetrik algoritmlari asosida | Ixtiyoriy asimmetrik shifrlash algoritmi asosida | Kalitlarni tarqatish protokolining maxsus simmetrik algoritmlari asosida | Ixtiyoriy simmetrik shifrlash algoritmi asosida |
| 2 | Kriptotizim foydalanuvchilariga ularning kalitlarini tarqatish protokollarida ERIdan qanday foydalaniladi? | Kalit xeshlanadi, bu xesh qiymatga nisbatan ERI shakllantiriladi, kalit ifodasi va ERI birlashtirilib, xosil bo‘lgan kengaytirilgan ma’lumot shifrlanib ochiq kanal orqali uzatiladi | Uzatilishi kerak bo‘lgan kalit ifodasiga nisbatan ERI shakllantiriladi, kalit ifodasi va ERI birlashtirilib, xosil bo‘lgan kengaytirilgan ma’lumot shifrlanib ochiq kanal orqali uzatiladi | Kalit xeshlanadi, bu xesh qiymatga nisbatan ERI shakllantiriladi, xesh qiymat ifodasi va ERI birlashtirilib, xosil bo‘lgan kengaytirilgan ma’lumot shifrlanib ochiq kanal orqali uzatiladi | Kalit xeshlanadi, bu xesh qiymatga nisbatan ERI shakllantiriladi, xesh qiymat shifrlanib ochiq kanal orqali uzatiladi |
| 2 | DES i GOST 28147-89 shifrlash algoritmlarining qanday umumiylik tomonlari bor? | Har ikkisi ham Feystel tarmog‘iga asoslangan | Har ikkisi ham bir xil sondagi akslantirish raundlariga ega | Har ikkisi ham bir xil asosiy akslantirishlarga ega | Har ikkisi ham bir xil uzunlikdagi kalitga ega |
| 1 | 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 | Akslantiriladigan blok uzunligi bilan |
| 2 | RSA asimmetrik kriptotizim foydalanuvchilarining ochiq va mahfiy kalitlari qanday generatsiya qilinadi? | Tub sonlar ko‘paytmasidan iborat etarli katta natural sonning Eyler funksiyasi asosida | CHekli maydonda teskari element topishning Eyler-Ferma formulasi yoki Evklid algoritmi bo‘yicha generatsiya qilinadi | Xarakteristikasi etarli chekli maydonda diskret logarifimlashni hisoblashning murakkabligiasosida | CHekli maydonda berilgan chiziqli algebraik tenglamalar sistemasining echish murakkabligi asosida |
| 2 | El-Gamal asimmetrik kriptotizim foydalanuvchilarining ochiq va mahfiy kalitlari qanday generatsiya qilinadi? | Xarakteristikasi etarli chekli maydonda diskret logarifimlashni hisoblashning murakkabligiasosida | CHekli maydonda teskari element topishning Eyler-Ferma formulasi yoki Evklid algoritmi bo‘yicha generatsiya qilinadi | Tub sonlar ko‘paytmasidan iborat etarli katta natural sonning Eyler funksiyasi asosida | CHekli maydonda berilgan chiziqli algebraik tenglamalar sistemasining echish murakkabligi e. |
| 2 | Elliptik egri chiziqqa asoslanganasimmetrik kriptotizimlarning mohiyati qanday? | Elliptik egri chiziq irratsional kordinatali nuqtalari ustida amal bajarish murakkabliklariga asoslangan | Elliptik egri chiziq irratsional kordinatali nuqtalari ustida amal bajarish murakkabliklariga asoslangan | Elliptik egri chiziq haqiyqiy kordinatali nuqtalari ustida amal bajarish murakkabliklariga asoslangan | Elliptik egri chiziq irratsional kordinatali nuqtalarini qo‘shish amalini bajarish murakkabliklariga asoslangan |
| 2 | Axborot-kommunikatsiya tizimlarida kalitlar almashinuvining Diffi-Xelliman algoritmi mohiyati qanday? | Xarakteristikasi etarli chekli maydonda diskret logarifimlashni hisoblashning murakkabligi | asosida | Tub sonlar ko‘paytmasidan iborat etarli katta natural sonning Eyler funksiyasi asosida | CHekli maydonda teskari element topishning Eyler-Ferma formulasi yoki Evklid algoritmi bo‘yicha generatsiya qilinadi |
| 2 | Agar a=19 bo‘lsa, u holda unga teskari bo‘lgan sonni xarakteristikasi 26 bo‘lgan maydonda hisoblang. | 11 | 17 va 19 | 19 va 11 | 13 va 19 |
| 1 | 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, kriptografiya yo‘nalishi esa shifr ma’lumotga mos keluvchi ochiq ma’lumotni kalit noma’lum bo‘lganda topish masalalari echimlari bilan shug‘illanadi |
| 1 | kalitni bilmagan holda axborotni shifrini ochish (deshifrlash) bilan qaysi fan shug’ullanadi | Kriptoanaliz | Kartografiya; | Kriptologiy++a. | Adamar usuli |
| 2 | Eyler funksiyasi yordamida 1811 sonining qiymatini toping. | 1810 | 2111 | 16 | 524 |
| 2 | sonlari nima deb ataladi | Ferma sonlari | Eyler sonlari | Mersenn sonlari ; | Feystal sonlari |
| 2 | Quyidagi taqqoslamalardan qaysi biri o’rinli |  |  |  |  |
| 2 | yagona yechimga ega bo’lishi uchun qanday shart bajarilishi kerak |  |  |  |  |
| 1 | AES shifrlash standartining mualliflari kimlar | Ridjmen va Deimen | Feystel va Pascal | Vijener va Verman | Feystel va Verman |
| 1 | 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 |
| 1 | RSA algoritmi qanday maqsadda ishlatiliadi? | ochiq kalitli kriptotizimlarda ma’lumotlarni shifrlashning mustaqil vositasi sifatida, ERI tizimida foydalanuvchilarni | autenfikatsiya vositasi sifatida, asosiy tizimlarda kalitlarni taqsimlash vositasi | ochiq kalitli kriptotizimlarda ma’lumotlarni shifrlashning mustaqil vositasi sifatida | ERI tizimida foydalanuvchilarni autenfikatsiya vositasi sifatida asosiy tizimlarda kalitlarni taqsimlash vositasi |
|  |  |  |  |  |  |
| 2 | 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 - 36 bit; Xabar daydjesti uzunligi - 256 bit |
| 2 | 4+31 mod 32 ? | 3 | 2 | 31 | 32 |
| 2 | 12+22 mod 32 ? | 2 | 1 | 22 | 32 |
| 2 | 2+5 mod32 ? | 7 | 32 | 2 | 15 |
| 1 | AES algoritmi bloki uzunligi … bitdan kam bo’lmasligi kerak. | 128 | 512 | 256 | 64 |
| 1 | MD5 xesh algoritmi xesh qiymat uzunligi nechchiga teng? | 128 bit | 32 bit | 64 bit | 256 bit |
| 2 | Uzluksiz shifrlash algoritmlari asosini nima tashkil etadi? | Psevdotasodifiy ketma-ketlik | Elleptik egri chiziklar | Feystel tarmogi | Tugri javob keltirilmagan |
| 2 | Uzunligi 128 bitdan kam bo‘lmagan kalitlarning mumkin bo‘lgan barcha variantlari soni nechta | 2^128 | 256 | 2^256 | 1024 |
| 1 | Kalitni bilmasdan axborotni shifrni ochish (deshifrlash) bilan qaysi fan shug’ullanadi | Kriptoanaliz | Kartografiya; | Kriptologiy++a. | Adamar usuli |
| 1 | Asimmetrik kriptotizim foydalanuvchilarining ochiq va mahfiy kalitlari qanday generatsiya qilinadi? | Algoritm asoslangan hisoblash murakkabligini ta’minlovchi noma’lum parametrga bog‘liq holda | Algoritm asoslangan maxsus protokol bo‘yicha | Algoritm asoslangan hisoblash murakkabligini ta’minlovchi barchaga ma’lum parametrga bog‘liq holda | Algoritm asoslangan hisoblash murakkabligini ta’minlovchi faqat mahfiy kalit egasiga ma’lum bo‘lgan parametrga bog‘liq holda |
| 1 | Xesh-funksiya qanday xossalarga ega bo‘lishi kerak? | Bir tomonlamalik xossasiga ega bo‘lishi kerak | Teskarisi mavjud bo‘lmasligi kerak | O‘zaro birqiymatlilik xossasiga | Teng qiymatlilik xossasiga |
| 1 | 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 |
| 1 | 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 |
| 2 | Sonning o’zi va uning modul multiplikativ teskarisining ko’paytmasi nechaga teng | 1 | 0 | 2 | 7 |
| 2 | Sonning teskarisini toppish amali qanday algoritm yordamida amalga oshiriladi? | Kengaytirilgan Yevklid | Yevklid | Ferma teoremasi | Affin tizim |
| 1 | Quyidagi ifodani qiymatini toping. -17mod11 | 5 | 6 | 7 | 11 |
| 2 | Quyidagi modulli ifodani qiymatini toping. (148 + 14432) mod 256. | 244 | 200 | 156 | 154 |
| 2 | Quyidagi modulli ifodani qiymatini toping. (12545)mod10. | 5 | 15 | 18 | 25 |
| 2 | Ikkilik sanoq tizimida berilgan 10111 sonini o’nlik sanoq tizimiga o’tkazing. | 23 | 22 | 11 | 10 |
| 2 | Quyidagi XOR amali natijasini hisoblang. | 000111 | 000101 | 110011 | 000001 |
| 1 | 97 tub sonmi? | Tub | murakkab | Natural | haqiqiy son |
| 1 | Simmetrik kriptotizimlarda shifrlash va deshifrlashda qanday kalit ishlatiladi? | Bir xil kalit | Alohida kalitlar | Har xil kalitlar | Ochiq |
| 1 | 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 |
| 1 | Kriptotahlil bilan shug’ullanuvchi insonlar kimlar? | kriptoanalitiklar | Shifrchilar | Hakkerlar | Dasturchilar |
| 1 | Shifrlash kaliti noma’lum bo’lganda shifrlangan ma’lumotni deshifrlash qiyinlik darajasini nima belgilaydi | kriptobardoshlik | Shifr matn uzunligi | Shifrlash algoritmi | Texnika va texnologiyalar |
| 2 | DES shifrlash algoritmi nechanchi yilda yaratilgan | 1976-yilda | 1980-yilda | 1989-yilda | 1987-yilda |
| 2 | 2 soniga 10 modul bo’yicha teskari sonni toping. |  | 10 | 25 |  |
| 2 | Eyler funksiyasida 60 sonining qiymatini toping. | 59 | 30 | 16 | 21 |
| 1 | Barcha shifrlash algoritmlari qanday shifrlash usullariga bo’linadi | 1. blokli va oqimli | 2. DES va oqimli | 3. Feystel va Verman | 4. SP− tarmoq va IP |
| 1 | Deshifrlashtirish so`zining ma`nosi nima? | 1. Deshifrlashtirish – shifrlashtirishga teskari jarayon. Kalit asosida shifrlangan matn o`z holatiga uzgartiriladi. | 2. Deshifrlashtirish – bu matn ma`lumotlarini o`zgartirish uchun ikkilik kodi. | 3. Deshifrlashtirish – bu grafik ma`lumotlarni o`zgartirish uchun sakkizlik kodi. | 4. Deshifrlashtirish – bu grafik va matnli ma`lumotlarni o`zgartirish uchun sakkizlik kodi |
| 1 | Dastlabki ma’lumotni bevosita shifrlash va deshifrlash uchun zarur manba … deb ataladi | Kalit | Alifbo | Axborot | Matn |
| 1 | Axborotni muxofaza qilish masalalari bilan shug’ullanadigan fan bo’lib kryptos- maxfiy, logos-ilm degan ma’noni anglatadigan fan qaysi? | Kriptologiya | Kriptografiya | Kriptotizimlar | Kriptotahlil |
| 1 | 2+5 mod32 ? | 7 | 32 | 2 | 5 |
| 2 | Serpent, Square, Twofish, RC6 algoritmlari qaysi turiga mansub? | simmetrik blokli algoritmlar | Oqimli shifrlash | asimmetrik algoritmlar | elektron raqamli imzo algoritmlari |
| 1 | Ochiq kalitlar infratuzilmasini qanday maqsadda ishlatiladi? | Axborotlarni maxfiyligini va butunligini ta’minlash maqsadida | Axborotlarni saqlash va qayta ishlash maqsadida | Axborot almashish va ishlab chiqish maqsadida | Axborotlarni maxfiyligini ta’minlash maqsadida |
| 1 | Xesh-funktsiyani natijasi … | fiksirlangan uzunlikdagi xabar | Kiruvchi xabar uzunligidagi xabar | Kiruvchi xabar uzunligidan uzun xabar | fiksirlanmagan uzunlikdagi xabar |
| 1 | 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 |
| 2 | 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 chiziqsiz almashtirishdan foydalanilsa |
| 2 | 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, kalitlar almashish uchun |
| 2 | Elektron raqamli imzo nima? | Xabarni qabul qiluvchi xabarni muallifini (jo’natuvchini) va xabarni haqiqiyligini tekshirish imkonini beruvchi xabarga qo’shib jo’natiladigan kriptografik almashtirish | Ochiq kalitli kriptotizim | Simmetrik kriptografik algoritm | Asimmetrik kriptografik algoritm |
| 2 | Quyida keltirilgan algoritmlardan ochiq kalitli kriptotizimlarni ko’rsating: RSA, DES, O’z DSt 1105:2009, GOST 28147 El-Gamal. | RSA, El-Gamal | O’zDSt 1105:2009, GOST 28147 | O’z DSt 1105:2009, El-Gamal | RSA, DES |
| 2 | Kriptografik tizimlar yordamida xavfsizlikning ta’minlashning amaliy masalalarini yechish uchun mo’ljallangan protokol qaysi? | Amaliy kriptografik protokoli | Shartnomani imzolash protokoli | Diffie Xellman protokoli | Tanga tashlash protokoli |
| 2 | Kriptografik protokol asosini numa tashkil qiladi? | Kriptografik algoritm va almashtirishlar | Kriptoanaliz usullari va vositalari | Dasturiy vositalar | Kriptografiya va kriptoanaliz |
| 2 | Protokol nima? | Ikki yoki undan ortiq tomonlar tomonidan aniq bir masalani yechish uchun zarur harakatlar tartibi | Ikki yoki undan ortiq tomonlar tomonidan aniq bir masalani yechish uchun tuzilgan dasturiy ta’minot | Ikki yoki undan ortiq tomonlar tomonidan aniq bir maqsadga yo’naltirilgan aloqa | Ishtirokchilar kelishuvi bayonnomasi |
| 2 | Hujjatni ERIni tekshirish nimaga keltiriladi? | hujjatni xesh-yig’indisini hisoblashga, imzodagi xesh-yig’indini rasshifrovka qilishga va ushbu 2 miqdorlarni solishtirishga | ushbu hujjatni xesh-yig’indisini hisoblashga, electron raqamli imzoda foydalanilgan ochiq kalitni solishtirishga | electron raqamli imzoda foydalanilgan ochiq kalitni solishtirishga | electron raqamli imzodagi xesh-yig’indini rasshifrovka qilishga |
| 2 | Shifr nima? | Shifrlash va deshifrlashda foydalaniladigan matematik funktsiyadan iborat bo’lgan krptografik algoritm | Kalitlarni taqsimlash usuli | Kalitlarni boshqarish usuli | Kalitlarni generatsiya qilish usuli |
| 1 | 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 | Kriptotizim quyidagi komponentlardan iborat: | ochiq matnlar fazosi M, Kalitlar fazosi K, Shifrmatnlar fazosi C, *Ek*: *M → C* (shifrlash uchun) va *Dk*: *C→M* (deshifrlash uchun) funktsiyalar | Shifrmatnlar fazosi C, *Ek*: *M→C* (shifrlash uchun) va *Dk*: *C→M* (deshifrlash uchun) funktsiyalar | ochiq matnlar fazosi M, shifrmatnlar fazosi C | ochiq matnlar fazosi M, kalitlar fazosi K |
| 1 | … 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 almashtirishga asoslangan |
| 1 | Nisbatan mashhur bo’lgan xesh-funksiyalarni ko’rsating. | MD2, MD4, MD5, SHA | GOST 28147, DES, AES, SERPENT | DES, O’zDSt1106:2006, AES | O’zDSt1092:2005, MD2, SHA, MARS |
| 1 | Kriptomustahkamlikning  qanaqa ko‘rsatkichlari  mavjud | –mumkin bo‘lg*a*n  kalitlar soni; –  kripto tahlil uchun  kerakli o‘rtacha vaqt; | –mumkin bo‘lgan  kalitlar soni; –  kripto tahlil uchun  kerakli boshlang‘ich  vaqt; | –mumkin bo‘lgan  kalitlar soni; –  kripto tahlil uchun  kerakli oxirgi  vaqt; | barcha javoblar to‘g‘ri |
| 1 | Shifrlangan ma’lumot  o‘qilishi mumkin faqat | Kaliti berilgan  bo‘ls*a* | Kodi berilgan bo‘lsa | Identifikatori  berilgan bo‘lsa | Shifri berilgan  bo‘lsa |
| 1 | Shifrlash jarayonida  ma’lumotga  kiritiladigan qo‘shimcha  bitlar | to‘liq va ishonchli  yashiringan bo‘lishi  ker*a*k | to‘liq bo‘lmagan va  ishonchli yashiringan  bo‘lishi kerak | to‘liq bo‘lmagan va  ishonchsiz  yashiringan bo‘lishi  kerak | barcha javoblar to‘g‘ri |
| 1 | Shifrlangan matnning  Uzunligi | Berilgan matnning  uzunligiga teng  bo‘lishi sh*a*rt | Shifrning  uzunligiga teng  bo‘lishi shart | Shifrning  uzunligiga teng  bo‘lmasligi shart | Berilgan matnning  uzunligiga teng  bo‘lmasligi shart |
| 1 | Quyidagilar bo‘lmasligi  Kerak | shifrlash jarayonida  muntazam  qo‘llanadigan  kalitlar orasida  sodda va osongina aniqlash mumkin  bo‘lg*a*n 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 |
| 2 | Kalitlar kanday  taksimlanadi: | Generatsiya  markazini yaratish va  kalitlarni  taksimlash va  kalitlarni tugri  almashlash yuli bil*a*n | Korrektirovka  markazini yaratish va  kalitlarni  taksimlash va  kalitlarni tugri  almashlash yuli bilan | Loyixalash  markazini yaratish  va kalitlarni  taksimlash va  kalitlarni tugri  almashlash yuli  bilan | Tugri javob yuk |
| 1 | Ma’lumotlarni  himoyalash deb nimaga  aytiladi | ma’lumotlarga  ruxsat etilmagan  kirishlardan  himoyal*a*nish | himoyalash uchun  maxsus disketalarni  ishlab chiqish | ma’lumotlar  xavfsizligini  ta’minlashga  yo‘naltirilgan  kompleks tashkiliy  ishlar | himoyalash uchun  maxsus kitoblar  ishlab chiqish |
| 1 | Alfavit – bu | axborotni kodlashtirish uchun ishlatiladigan chekli belgilar to‘plami. | axborotni kodlashtirish uchun ishlatiladigan diskret va cheksiz belgilar. | axborotni kodlashtirish uchun ishlatiladigan diskret belgilar to‘plami. | axborotni kodlashtirish uchun ishlatiladigan cheksiz belgilar to‘plami. |
| 2 | ERIning umumiy tan olingan sxemasi (modeli) nechta jarayonni o‘z ichiga oladi: | 3 | 2 | 4 | 5 |
| 1 | RSA elektron raqamli imzo algoritmidagi ochiq kalit e qanday shartni qanoatlantirishi shart? | e soni Eyler funksiyasi -bilan o‘zaro tub | e ning qiymati [1,n] kesmaga tegishli ixtiyoriy son | e soni ixtiyoriy tub son | e soni ixtiyoriy butun musbat son |
| 2 | RSA elektron raqamli imzo algoritmidagi yopiq kalit  d qanday hisoblanadi? Bu yerda p va q tub sonlar,n=pq,- Eyler funksiyasi,e-ochiq kalit. |  |  |  |  |
| 2 | 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 |
| 1 | Kaysi kriptotizimda shifrlash uchun ham va deshifrlash uchun ham bir xil kalitdan foydalaniladi | Simmetrik kriptotizim | Elektron raqamli imzo | Kalitlarni taqsimlash va boshqarish | Ochiq kalitli kriptotizim |
| 1 | Simmetrik shifrlashda qanday amallar orqali amalga oshiriladi? | CHekli maydonda qo‘shish  mod  va mod 2 bo‘yicha | CHekli maydonda qo‘shish  mod  bo‘yicha | Mos bitlarni qo‘shish  mod 2 bo‘yicha | CHekli maydonda qo‘shish  mod  va mod 2 bo‘yicha, hamda bitlarni surish. |
| 2 | Qanday manbaa asosida raund kalitlari yaratiladi? | Krish bloki uzunligiga bog‘liq holda. | Dastlabki berilgan blok asosida | Maxfiy kalit asosida | SHifrlangan blok asosida |
| 2 | RSA algoritmi maxfiy kaliti uzunligi qancha? | Ochiq kalit va Eyler funksiyasi bilan aniqlanadi; | Ixtiyoriy; | Ochiq kalit uzunligi bilan aniqlanadi; | Ochiq kalit uzunligiga teng; |
| 2 | Kriptotizim foydalanuvchilariga ularning kalitlari qanday tarqatiladi? | Kalitlarni tarqatish protokolining maxsus asimmetrik algoritmlari asosida | Ixtiyoriy asimmetrik shifrlash algoritmi asosida | Kalitlarni tarqatish protokolining maxsus simmetrik algoritmlari asosida | Ixtiyoriy simmetrik shifrlash algoritmi asosida |
| 2 | S-box lar nima uchun yaratilgan? | ochiq matn va shifrmatn orasidagi bog’liqlikni yuqotish uchun | shifrlash jarayonini soddalashtirish uchun | deshifrlash jarayonini soddalashtirish uchun | kalitlarni generatsiya qilishni soddalashtirish uchun |
| 1 | Sezar algoritmida alifbo belgilarini nechtaga surish orqali shifrlangan. | 3 | 4 | 5 | 2 |
| 1 | Bir marta ishlatilganidan parol–bu: | Biоmetrik autentifikatsiya | Parоl asоsidagi autentifikatsiya | Biografiya asоsidagi autentifikatsiya | Smart-karta asоsida autentifikatsiya |
| 2 | Autentifikatsiya prоtоkоllariga bo’ladigan asоsiy hujumlarni ko’rsating? | Autentifikatsiya almashinuvining taraflarini almashtirib qo’yish, majburian kechikish, matn tanlashli hujumlar | Xizmat ko’rsatishdan vоz kechish hujumlari | Kоmp yuter tizimini ishdan chiqaruvchi hujumlar | DOS va DDOS hujumlar |
| 2 | 256 mod 256 ni hisoblang | 0 | 25 | 2 | 1 |
| 2 | Nomlari ketma – ketligi to‘g‘ri ko‘yilgan jarayonlarni ko‘rsating? | Identifikatsiya, Audentifikatsiya, avtorizatsiya, maьmurlash | Audentifikatsiya identifikatsiya Avtorizatsiya. maьmurlash | Avtorizatsiya audentifikatsiya identifikatsiya maьmurlash | Maьmurlash identifikatsiya Avtorizatsiya audentifikatsiya |
| 1 | Eng ko’p foydalaniladigan autentifikatsiyalash asosi-bu: | Parol | Biometrik parametrlar | smart karta | Elektron rakamli imzo |
| 2 | Elektron raqamli imzo qaysi algoritmlar asosida ishlab chiqiladi? | El-Gamal, RSA | AES (Advanced Encryption Standart) | Kerberos | DES(Data Encryption Standart) |