5330300-Axborot xavfsizligi yo'nalishi bakalavr talabalari uchun "Kriptografiya 2" fanidan TESTLAR

№ 1.
Manba:
Qiyinlik darajasi – 1

Kriptologiya qanday yo'nalishlarga bo'linadi?
kriptografiya va kriptotahlil
kriptografiya va kriptotizim
kripto va kriptotahlil
kriptoanaliz va kriptotizim

№ 2. Na'muna uchun test
Manba:
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:
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:
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:
Qiyinlik darajasi – 1

Shifrlash orqali ma'lumotning qaysi xususiyati ta'minlanadi?
maxfiyligi
butunliligi
ishonchliligi
foydalanuvchanligi

№ 6.
Manba:
Qiyinlik darajasi – 1

Ochiq kalitli kriptotizimlar kim tomonidan kashf qilingan?
U.Diffie va M.Hellman
Rivest va Adlman
Shamir va Rivest
U.DIffie va Rivest

№ 7.
Manba:
Qiyinlik darajasi – 1

Kriptologiya necha yo‘nalishga bo‘linadi?
2
14
16
18

№ 8.
Manba:
Qiyinlik darajasi – 1

Kriptologiya so‘zining ma’nosi?
cryptos – maxfiy, logos – ilm
cryptos – kodlash, logos – ilm
cryptos – kripto, logos – yashiraman
cryptos – maxfiy, logos – kalit

№ 9.
Manba:
Qiyinlik darajasi – 1

Ochiq kalitli kriptotizimlar ma'lumotni qanday xususiyatini taminlaydi?
maxfiyligini
butunligini
foydalanuvchanligini
ma'lumotni autentifikatsiyasini

№ 10.
Manba:
Qiyinlik darajasi – 1

Kriptotizimlar kalitlar soni bo‘yicha necha turga bo‘linadi?
2
4
6
8

№ 11.
Manba:
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:
Qiyinlik darajasi – 1

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

№ 13.
Manba:
Qiyinlik darajasi – 1

Ochiq kalitli kriptotizimlarda qanday turdagi kalitlardan foydalanadi?
ochiq va maxfiy kalitlardan
maxfiy kalitlar juftidan
maxfiy kalitni uzatishni talab etmaydi
ochiq kalitni talab etmaydi

№ 14.
Manba:
Qiyinlik darajasi – 1

Assimetrik kriptotizimlarda necha kalitdan foydalaniladi?
2 ta
3 ta
4 ta
kalit ishlatilmaydi

№ 15.
Manba:
Qiyinlik darajasi – 1

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

№ 16.
Manba:
Qiyinlik darajasi – 1

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

№ 17.
Manba:
Qiyinlik darajasi – 1

Ochiq kalitni kriptotizimlarda nechta kalitdan foydalanadi?
ikkita
bitta

uchta
kalitdan foydalanilmaydi

№ 18.
Manba:
Qiyinlik darajasi – 1

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

№ 19.
Manba:
Qiyinlik darajasi – 1

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

№ 20.
Manba:
Qiyinlik darajasi – 1

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

№ 21.
Manba:
Qiyinlik darajasi – 1

Qanday sonlar tub sonlar hisoblanadi?
1 va o’ziga bo’linadigan sonlarlar
barcha toq sonlar
juft bo’lmagan sonlar
2 ga bo’linmaydigan sonlar

№ 22.
Manba:
Qiyinlik darajasi – 1

Sonlarni tublikka tekshirish algoritmlari nechta sinfga bo'linadi?
ikkita sinfga
uchta sinfga
bitta sinfga
sinflarga bo'linmaydi

№ 23.
Manba:
Qiyinlik darajasi – 1

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

№ 24.
Manba:
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. Shnorr

№ 25.
Manba:
Qiyinlik darajasi – 1

Ochiq kalitli shifrlash algoritmi keltirilgan qatorni toping?
RSA
AES
DES
RC4

№ 26.
Manba:
Qiyinlik darajasi – 1

Ochiq kalitli shifrlash algoritmi keltirilgan qatorni toping?
El-Gamal
AES
DES
RC4

№ 27.
Manba:
Qiyinlik darajasi – 1

Shifrlash orqali ma'lumotning qaysi xususiyati ta'minlanadi?
maxfiyligi
butunliligi
ishonchliligi
foydalanuvchanliligi

№ 28.
Manba:
Qiyinlik darajasi – 1

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

№ 29.
Manba:
Qiyinlik darajasi – 1

Faqat simmetrik algoritm keltirilgan qatorni ko’rsating?
AES
RSA
El-Gamal
Barcha javoblar to’g’ri

№ 30.
Manba:
Qiyinlik darajasi – 1

Kriptotizimlar kalitlar soni bo’yicha nechta turga bo’linadi?
2
3
4
5

№ 31.
Manba:
Qiyinlik darajasi – 1

Kriptotizimlar kalitlar soni bo’yicha qanday turga bo’linadi?
simmetrik va assimetrik
simmetrik va bitta kalitli
3 kalitli kriptotizimlar
assimetrik va 2 ta kalitli

№ 32.
Manba:
Qiyinlik darajasi – 1

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

№ 33.
Manba:
Qiyinlik darajasi – 1

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

№ 34.
Manba:
Qiyinlik darajasi – 1

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

№ 35.
Manba:
Qiyinlik darajasi – 1

Sonlarni tublikka tekshiruvchi algoritmlar necha sinfga bo’linadi?
2
3
4
5

№ 36.
Manba:
Qiyinlik darajasi – 1

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

№ 37.
Manba:
Qiyinlik darajasi – 1

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

№ 38.
Manba:
Qiyinlik darajasi – 1

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

№ 39.
Manba:
Qiyinlik darajasi – 1

1 ga va o’ziga bo’linadigan sonlar qanday sonlar hisoblanadi?
tub sonlar
murakkab sonlar
toq sonlar
juft sonlar

№ 40.

Manba:
Qiyinlik darajasi – 1

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

№ 41.
Manba:
Qiyinlik darajasi – 1

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

№ 42.
Manba:
Qiyinlik darajasi – 1

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

№ 43.
Manba:
Qiyinlik darajasi – 1

Raqamli imzoni shakllantirish muolajasi qaysi algoritmga tegishli?
ERI algoritmiga
kodlash algoritmiga
shifrlash algoritmiga
steganografiya algoritmiga

№ 44.
Manba:
Qiyinlik darajasi – 1

ECDSA-2000 qaysi davlat standarti hisoblanadi?
AQSH
Rossiya
O'zbekiston
Kanada

№ 45.
Manba:
Qiyinlik darajasi – 1

O'zDSt 1092:2009 standarti qaysi davlat standarti hisoblanadi?
O'zbekiston
AQSH
Rossiya

Kanada

№ 46.
Manba:
Qiyinlik darajasi – 1

ГОСТ Р 34.10-94 standarti qaysi davlat standarti hisoblanadi?
Rossiya
O’zbekiston
AQSH
Kanada

№ 47.
Manba:
Qiyinlik darajasi – 1

Seans kalitli hamda seans kalitsiz rejimlarda ishlidigan standartni ko’rsating?
O’zDSt 1092:2009
ECDSA-2000
ГОСТ Р 34.10-94
DSA

№ 48.
Manba:
Qiyinlik darajasi – 1

DSA qanday standart hisoblanadi?
ERI standarti
shifrlash standarti
kodlash standarti
steganografik standart

№ 49.
Manba:
Qiyinlik darajasi – 1

O’zDSt 1092:2009 qanday standart hisoblanadi?
ERI standarti
shifrlash standarti
kodlash standarti
steganografik standart

№ 50.
Manba:
Qiyinlik darajasi – 1

ГОСТ Р 34.10-94 qanday standart hisoblanadi?
ERI standarti
kodlash standarti
steganografik standart
shifrlash standarti

№ 51.
Manba:
Qiyinlik darajasi – 2

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

faktorizatsiyalash va diskret logarifmlash algoritmlariga
modulyar arifmetika murakkabligiga asoslangan algoritmlarga
diskret lografmlash murakkabligiga asoslangan algorimtlarga
faktorizatsiyalash murakkabligiga asoslangan algorimtlarga

№ 52.
Manba:
Qiyinlik darajasi – 2

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

№ 53.
Manba:
Qiyinlik darajasi – 2

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

№ 54.
Manba:
Qiyinlik darajasi – 2

Faqat tub son keltirilgan qatorni toping?
3, 5
5, 15
16, 2
3, 18

№ 55.
Manba:
Qiyinlik darajasi – 2

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

№ 56.
Manba:
Qiyinlik darajasi – 2

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

№ 57.
Manba:
Qiyinlik darajasi – 2

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

№ 58.
Manba:
Qiyinlik darajasi – 2

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

№ 59.
Manba:
Qiyinlik darajasi – 2

Diffie-Helman algoritmi qanday matematik murakkablikka asoslanadi?
diskret logarifmlash murakkabligiga
faktorlash murakkabligiga
elliptik egri chiziqda diskret logarifmlash murakkabligiga
elliptik egri chiziqda faktorlash murakkabligiga

№ 60.
Manba:
Qiyinlik darajasi – 2

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

№ 61.
Manba:
Qiyinlik darajasi – 2

Faqat tub son keltirilgan qatorni toping?
2, 5
5, 25
16, 3
3, 21

№ 62.
Manba:
Qiyinlik darajasi – 2

ERI algoritmlari nechta muolajadan iborat?
ikkita

bitta asosiy
uchta
to'rtta

№ 63.
Manba:
Qiyinlik darajasi – 2

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

№ 64.
Manba:
Qiyinlik darajasi – 2

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

№ 65.
Manba:
Qiyinlik darajasi – 2

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

№ 66.
Manba:
Qiyinlik darajasi – 2

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

№ 67.
Manba:
Qiyinlik darajasi – 2

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

№ 68.
Manba:
Qiyinlik darajasi – 2

Diskret logarifmlash murakkabligiga asoslangan algoritm keltirilgan qatorni ko'rsating?
Diffie-Hellman, EL-Gamal algoritmi
RSA algoritmi
EL-Gamal algoritmi
Diffie-Hellman algoritmi

№ 69.
Manba:
Qiyinlik darajasi – 2

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

№ 70.
Manba:
Qiyinlik darajasi – 2

Karlmaykl sonlari qaysi tublikka tekshiruvchi algoritmlarda doim bajariladi?
Ferma testida
Solovey-Shtrassen testida
Eyler testida
Rabbin testida

№ 71.
Manba:
Qiyinlik darajasi – 2

RSA algoritmida p, q tub sonlar bo’lsa, modul qiymati N qanday topiladi?
N=p*q
N=p/q
N=q/p
N=p-q

№ 72.
Manba:
Qiyinlik darajasi – 2

Amerikaning nechta ERI standarti mavjud?
2 ta
1 ta
3 ta
mavjud emas

№ 73.
Manba:
Qiyinlik darajasi – 2

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

№ 74.
Manba:
Qiyinlik darajasi – 2

O’zbekistonning nechta ERI standarti mavjud?
1 ta
2 ta
3 ta
mavjud emas

№ 75.
Manba:
Qiyinlik darajasi – 2

O’zbekistonning qanday ERI standarti mavjud?
O’zDSt 1092:2009
DSA
ECDSA-2000
ГОСТ Р 34.10-94

№ 76.
Manba:
Qiyinlik darajasi – 2

Qaysi kalit orqali ERI qo’yiladi?
shaxsiy kalit orqali
ochiq kalit orqali
kalit ishtirok etmaydi
ikkala kalit birgalikda ishtirok etadi

№ 77.
Manba:
Qiyinlik darajasi – 2

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

№ 78.
Manba:
Qiyinlik darajasi – 2

Diffie-Hellman algoritmi qanday hujumga bardoshsiz hisoblanadi?
o’rtada turgan odam hujumiga
chastotalar tahlili hujumiga
yon kanal tahlili hujumiga
to’liq tanlash hujumiga

№ 79.
Manba:
Qiyinlik darajasi – 2

Qaysi algoritm o’rtada turgan odam hujumiga bardoshsiz hisoblanadi?
Diffie-Hellman
RSA
ElGamal
DSA

№ 80.
Manba:
Qiyinlik darajasi – 2

Sonlarni tublikka tekshirishda qaysi algoritm samarali hisoblanadi?
Rabin Milner
Solovey Shtrassen
Ferma
Eyler

№ 81.
Manba:
Qiyinlik darajasi – 2

Sonlarni tublikka tekshirishda qaysi algoritm Karlmaykl sonlarida ham to’gri ishlaydi?
Ferma algoritmida
Solovey Shtrassen algoritmida
Rabin-Milner algoritmida
Eyler algoritmida

№ 82.
Manba:
Qiyinlik darajasi – 2

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

№ 83.
Manba:
Qiyinlik darajasi – 2

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

№ 84.
Manba:
Qiyinlik darajasi – 2

“Psevdotub” termini qaysi algoritmlarda ishlatiladi
sonlarni tublikka tekshirish algoritmlarida
shifrlash algoritmlarida
steganografik algoritmlarda
kodlash algoritmlarida

№ 85.
Manba:
Qiyinlik darajasi – 2

“soxta tublikka guvoh” termini qaysi algoritmlarda ishlatiladi
sonlarni tublikka tekshirish algoritmlarida
shifrlash algoritmlarida
steganografik algoritmlarda
kodlash algoritmlarida

№ 86.
Manba:
Qiyinlik darajasi – 2

“murakkabligiga guvoh” termini qaysi algoritmlarda ishlatiladi
sonlarni tublikka tekshirish algoritmlarida
shifrlash algoritmlarida
kodlash algoritmlarida
steganografik algoritmlarda

№ 87.
Manba:
Qiyinlik darajasi – 2

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)))

№ 88.
Manba:
Qiyinlik darajasi – 2

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)

№ 89.
Manba:
Qiyinlik darajasi – 2

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)

№ 90.
Manba:
Qiyinlik darajasi – 2

Faktorlash muammosini yechishning Pollard usulida tanlanadigan funksiya qanday ko’rinishda bo'ladi?
kvadratik polinom
chiziqli polinom
kubik polinom
funksiya argementiga bog'liq emas

№ 91.
Manba:
Qiyinlik darajasi – 2

Faktorlash muammosini yechishning Pollard usulida eng kichik polinom qanday tanlanadi?
x^2+1
x+1
x
x^2

№ 92.
Manba:
Qiyinlik darajasi – 2

Faktorlash muammosini yechishning Pollard usulida funksiya argumenti boshlangich qiymati nechiga teng bo'ladi?
2
1
3
0

№ 93.
Manba:
Qiyinlik darajasi – 2

Ochiq kalitli RSA shifrlash algoritmida ochiq kalit "e" qanday topiladi?
φ(N) bilan o'zaro tub va undan kichik bo'lgan son tanlanadi
φ(N) dan kichik tub son tanlanadi
φ(N) dan katta tub son tanlanadi
φ(N) ning tub ko'paytuvchilaridan biri tanlanadi

№ 94.
Manba:
Qiyinlik darajasi – 2

Ochiq kalitli RSA shifrlash algoritmida maxfiy kalit qanday topiladi?
e*d=1 mod φ(p*q) taqqoslamadan
e*d=1 mod N
e*d=1 mod φ(p-1)
e*d=1 mod φ((p-1)(q-1))

№ 95.
Manba:
Qiyinlik darajasi – 2

Ochiq kalitli RSA shifrlash algoritmida qaysi parametrlar ochiq holda e'lon qilinadi?
N,e
e
N,d

d

№ 96.
Manba:
Qiyinlik darajasi – 2

Ochiq kalitli RSA shifrlash algoritmida "e" ochiq kalit, “d” shaxsiy kalit bo'lsa deshifrlash formulasi to'g'ri ko'rsatilgan qatorni belgilang?
M=C^d (mod N)
M=C^d (mod φ(N))
M=C^e (mod N)
M=C^e (mod φ(N))

№ 97.
Manba:
Qiyinlik darajasi – 2

Ochiq kalitli RSA shifrlash algoritmida "d" shaxsiy kalit, “e” ochiq kalit bo'lsa shifrlash formulasi to'g'ri ko'rsatilgan qatorni belgilang?
C=M^e (mod N)
C=M^e (mod φ(N))
C=M^d (mod φ(N))
C=M^d (mod N)

№ 98.
Manba:
Qiyinlik darajasi – 2

Ochiq kalitli RSA shifrlash algoritmida "p" tub son bo'lsa Eyler funskiyasi φ(p) qanday qiymat qaytaradi?
p-1
p
φ(p)
φ(p-1)

№ 99.
Manba:
Qiyinlik darajasi – 2

Ochiq kalitli RSA shifrlash algoritmida "p=7" tub son bo'lsa Eyler funskiyasi φ(p) qanday qiymat qaytaradi?
6
7
φ(7)
φ(6)

№ 100.
Manba:
Qiyinlik darajasi – 2

Ochiq kalitli El-Gamal shifrlash algoritmida "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

№ 101.
Manba:
Qiyinlik darajasi – 2

Ochiq kalitli El-Gamal shifrlash algoritmida ochiq kalit qanday hisoblanadi?
y=g^a (mod p), bu yerda g-birlamchi ildiz, a-maxfiy kalit, p-tub son
y=g^a (mod p), bu yerda g-soni (p-1) dan kichik butun son, a-maxfiy kalit, p-tub son
y=g^a (mod p), bu yerda g-soni p dan kichik butun son, a-maxfiy kalit, p-tub son
y=g^a (mod p), bu yerda g-soni (p-1) bilan o'zaro tub bo'lgan butun son, a-maxfiy kalit, p-tub son

№ 102.
Manba:
Qiyinlik darajasi – 2

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

№ 103.
Manba:
Qiyinlik darajasi – 2

"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

№ 104.
Manba:
Qiyinlik darajasi – 2

"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

№ 105.
Manba:
Qiyinlik darajasi – 2

"A" va "B" foydalanuvchilar ma'lumot almashmoqchi, "A" foydalanuvchi elektron hujjatga 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

№ 106.

Manba:
Qiyinlik darajasi – 2

"A" va "B" foydalanuvchilar ma'lumot almashmoqchi, "B" foydalanuvchi elektron hujjatga 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

№ 107.
Manba:
Qiyinlik darajasi – 2

Ochiq kalitli kriptotizimlarga asoslangan ERI algoritmida 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

№ 108.
Manba:
Qiyinlik darajasi – 2

ERI qaysi xususiyatni taminlamaydi?
Konfidensiallikni
Rad etishni oldini olishni
Yaxlitlikni
Ma’lumot egasi shaxsini ko’rsatishni

№ 109.
Manba:
Qiyinlik darajasi – 2

"A" va "B" foydalanuvchilar o'rtasida elektron ma'lumot almashinishida "rad etish" qoida buzlishi 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'zgartirilganligini rad etish
"A" foydalanuvchi yuborgan ma'lumotini yubormaganligini rad etishi

№ 110.
Manba:
Qiyinlik darajasi – 2

"A" va "B" foydalanuvchilar o'rtasida ma'lumot almashinishida qanday buzilishlar bo'lishi mumkin?
rad etish, modifikatsiyalash, soxtalashtirish, takrorlash
rad etish, modifikatsiyalash, soxtalashtirish, maxfiylashtirish, takrorlash
modifikatsiyalash, soxtalashtirish, maxfiylashtirish, takrorlash
rad etish, modifikatsiyalash, soxtalashtirish, maxfiylashtirish

№ 111.
Manba:
Qiyinlik darajasi – 2

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

2 ta
3 ta
4 ta
1 ta asosiy

№ 112.
Manba:
Qiyinlik darajasi – 2

Faktorlash muammosini yechishning Pollard algoritmida 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

№ 113.
Manba:
Qiyinlik darajasi – 2

RSA algoritmida p=3, q=11, e=3 bo'lganda maxfiy kalitni qiymati topilsin: e*d=1 mod φ(N)?
7
6
8
5

№ 114.
Manba:
Qiyinlik darajasi – 2

7 soni bilan o’zaro tub bo’lgan sonlarni ko’rsating?
2,3,6
14,2,5
1,7,5
6,21,2

№ 115.
Manba:
Qiyinlik darajasi – 2

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

№ 116.
Manba:
Qiyinlik darajasi – 2

Elliptik egri chiziqqa asoslangan Diffie Hellman algoritmi qanda matematik murakkablikka asoslanagan?
Elliptik egri chiziqda diskret logarifmlash murakkabligiga asoslangan
Diskret logarifmlash murakkabligiga asoslangan
Elliptik egri chiziqda nuqtlarni ikkilantirish murakkabligiga asoslangan
Elliptik egri chiziqda nuqtalarni qo’shish murakkabligiga asoslangan

№ 117.
Manba:
Qiyinlik darajasi – 2

Faktorlash muammosini bartaraf etuvchi usul keltirilgan qatorni ko’rsating?
Pollard usuli
Xitoy teoremasi
Pohlig-Hellman usulu
RSA usuli

№ 118.
Manba:
Qiyinlik darajasi – 2

Pollard usuli qanday turdagi matematik murakkablikni yechishda foydalaniladi?
faktorlash murakkabligini
diskret logarifmlash murakkabligini
elliptik egrzi chiziqda diskret logarifmlash murakkabligini
elliptik egrzi chiziqda faktorlash murakkabligini

№ 119.
Manba:
Qiyinlik darajasi – 2

RSA algoritmidagi matematik murakkablikni qanday usul orqali bartaraf qilish mumkin?
Pollard usuli
Xitoy teoremasi
Pohlig-Hellman usuli
RSA usuli

№ 120.
Manba:
Qiyinlik darajasi – 2

Diskret logarifmlash muammosini bartaraf etuvchi usul keltirilgan qatorni ko’rsating?
Pohlig-Hellman usuli
Pollard usuli
Xitoy teoremasi
RSA usuli

№ 121.
Manba:
Qiyinlik darajasi – 2

Pohlig-Hellman usuli qanday turdagi matematik murakkablikni yechishda foydalaniladi?
diskret logarifmlash murakkabligini
faktorlash murakkabligini
elliptik egrzi chiziqda faktorlash murakkabligini
daraja parameter murakkabligini

№ 122.
Manba:
Qiyinlik darajasi – 2

El-Gamal algoritmidagi matematik murakkablikni qanday usul orqali bartaraf qilish mumkin?
Pohlig-Hellman usulu

Pollard usuli
Xitoy teoremasi
El-Gamal usuli

№ 123.
Manba:
Qiyinlik darajasi – 2

Qoldiqlar haqidagi Xitoy teoremasidan qaysi algoritmda foydalaniladi?
Pohlig-Hellman algoritmida
Pollard algoritmida
RSA algoritmida
El-Gamal algoritmida

№ 124.
Manba:
Qiyinlik darajasi – 2

Diskret logarifm murakkabligini bartaraf etishda Pohlig-Hellman algoritmida yana qanday qo'shimcha usuldan foydalanadi?
qoldiqlar haqidagi Xitoy teoremasidan
Evklid algoritmidan
kengaytirilgan Evklid algoritmidan
parameter bo'yicha darajaga oshirishdan

№ 125.
Manba:
Qiyinlik darajasi – 2

RSA algoritmida maxfiy kalitni hisoblashda qaysi algoritmdan foydalanish mumkin?
Evklidning kengaytirilgan algoritmidan
qoldiqlar haqidagi Xitoy teoremasidan
parameter bo'yicha darajaga oshirishdan
Pohlig-Hellman algoritmidan

№ 126.
Manba:
Qiyinlik darajasi – 2

Faktorlash muammosiga asoslangan algoritmni ko'rsating?
RSA
El-Gamal
DSA
ECDSA

№ 127.
Manba:
Qiyinlik darajasi – 2

Elliptik egri chiziqda diskret logafimlash muammosiga asoslangan algoritmni ko'rsating?
ECDSA
EL-Gamal
DSA
RSA

№ 128.

Manba:
Qiyinlik darajasi – 2

Evklidning kengaytirilgan algoritmidan RSA shifrlash algoritmining qaysi parametrini hisoblashda foydalaniladi?
maxfiy kalitni
ochiq kalitni
tub sonlarni
modul qiymatini

№ 129.
Manba:
Qiyinlik darajasi – 2

Diffie-Hellman algoritmida 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)

№ 130.
Manba:
Qiyinlik darajasi – 2

El-Gamal shifrlash algoritmida 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)

№ 131.
Manba:
Qiyinlik darajasi – 2

RSA asosidagi ERI algoritmida qaysi kalit orqali elektron hujjatga imzo qo’yiladi?
maxfiy kalit orqali
ochiq kalit orqali
kalit ishlatilmaydi
imzo qo’lda qo’yiladi

№ 132.
Manba:
Qiyinlik darajasi – 2

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

№ 133.
Manba:
Qiyinlik darajasi – 2

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

№ 134.
Manba:
Qiyinlik darajasi – 2

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

№ 135.
Manba:
Qiyinlik darajasi – 2

Elliptik egri chiziqda nuqtalarni qo’shish qaysi algoritm bajariladi?
ECDSA
EL-Gamal
DSA
RSA

№ 136.
Manba:
Qiyinlik darajasi – 2

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

№ 137.
Manba:
Qiyinlik darajasi – 2

Malumotni shifrlash va deshifrlashda turli kalitlardan foydalanuvchi algoritmni ko’rsating?
RSA
AES
DES
RC4

№ 138.
Manba:
Qiyinlik darajasi – 2

Qanday kriptotizimlarda ochiq kalit kafolati talabi qo’yiladi?
ochiq kalitli kriptotizimlarda
bunday kriptotizim mavjud emas
simmetrik kriptotizimlarda
maxfiy kalitli kriptotizimlarda

№ 139.

Manba:
Qiyinlik darajasi – 2

Elektron raqamli imzo bo‘yicha birinchi standart?
DSS
RSA
DES
AES

№ 140.
Manba:
Qiyinlik darajasi – 2

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

№ 141.
Manba:
Qiyinlik darajasi – 2

Ochiq kalitni identifikatsiyalash jarayoni qaysi tizimga tegishli
ochiq kalitlar infratuzilmasiga
identifikatsiya tizimlariga
autentifikatsiya tizimlariga
simmetrik kriptotizimlarga

№ 142.
Manba:
Qiyinlik darajasi – 2

Ochiq kalitni taqsimlash jarayoni qaysi tizimga tegishli
ochiq kalitlar infratuzilmasiga
autentifikatsiya tizimlariga
simmetrik kriptotizimlarga
identifikatsiya tizimlariga

№ 143.
Manba:
Qiyinlik darajasi – 2

Shaxsiy kalitni maxfiyligini saqlash deganda nima tushiniladi?
kalitni boshqarish davomida tomonlardan maxfiy tarzda saqlanishi
kalitni to’g’riligiga kafolat berilishi
kalitlarni butunligini ta’minlanishi
kalitlni raqamli sertifikat bilan maxfiyligini ta’minlanishi

№ 144.
Manba:
Qiyinlik darajasi – 2

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

№ 145.
Manba:
Qiyinlik darajasi – 2

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

№ 146.
Manba:
Qiyinlik darajasi – 2

Foydalanuvchi nomi haqidagi ma’lumotlar nimada aks etishi kerak?
raqamli sertifikatda
raqamli imzoda
shifrlashda
kodlashda

№ 147.
Manba:
Qiyinlik darajasi – 2

Foydalanuchi ochiq kaliti nimada aks etishi kerak?
raqamli sertifikatda
raqamli imzoda
shifrlashda
kodlashda

№ 148.
Manba:
Qiyinlik darajasi – 2

Tashkilot imzosi nimada aks etishi kerak?
raqamli sertifikatda
shifrlashda
kodlashda
raqamli imzoda

№ 149.
Manba:
Qiyinlik darajasi – 2

X.509 standarti nima uchun mo’ljallangan?
ochiq kalitli infratuzilmalar uchun
raqamli imzo uchun
maxfiy kalit uchun
ochiq kalit uchun

№ 150.
Manba:
Qiyinlik darajasi – 2

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

X.509 standarti
DSA standarti
ECDSA standarti
RSA standarti

№ 151.
Manba:
Qiyinlik darajasi – 3

"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

№ 152.
Manba:
Qiyinlik darajasi – 3

"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

№ 153.
Manba:
Qiyinlik darajasi – 3

Malumotni shifrlash va deshifrlashda turli kalitlardan foydalanuvchi algoritmni ko’rsating?
El-Gamal
AES
DES
RC4

№ 154.
Manba:
Qiyinlik darajasi – 3

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

№ 155.
Manba:
Qiyinlik darajasi – 3

Nosimmetrik kriptografiya asosida birinchi bo‘lib elektron raqamli imzo bo‘yicha milliy standart yaratgan davlat?
AQSh
Germaniya
Rossiya

Koreya

№ 156.
Manba:
Qiyinlik darajasi – 3

Ochiq kalitli RSA shifrlash algoritmida "d" maxfiy kalit bo'lsa rasshifrovkalash formulasi to'g'ri ko'rsatilgan qatorni belgilang?
M=C^d (mod N)
M=C^d (mod φ(N))
M=C^e (mod N)
M=C^e (mod φ(N))

№ 157.
Manba:
Qiyinlik darajasi – 3

Ochiq kalitli RSA shifrlash algoritmida "e" ochiq kalit bo'lsa shifrlash formulasi to'g'ri ko'rsatilgan qatorni belgilang?
C=M^e (mod N)
C=M^e (mod φ(N))
C=M^d (mod φ(N))
C=M^d (mod N)

№ 158.
Manba:
Qiyinlik darajasi – 3

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

№ 159.
Manba:
Qiyinlik darajasi – 3

Qanday algoritm yordamida diskret logarifmlash muammosini bartaraf etiladi?
Polig-Hellman algoritmi
Diffie-Hellman algoritmi
Pollard algoritmi
Eyler-Ferma algoritmi

№ 160.
Manba:
Qiyinlik darajasi – 3

ERI algoritmlari qanday turdagi masalalarni yechishga imkon beradi?
ma'lumot yaxlitligini tekshirish, ma'lumot manbani autentifikatsiyalash hamda rad etishdan himoyalash
ma'lumot yaxlitligini tekshirish, ma'lumot manbani autentifikatsiyalash
ma'lumot manbani autentifikatsiyalash hamda rad etishdan himoyalash
ma'lumot yaxlitligini tekshirish, rad etishdan himoyalash

№ 161.
Manba:
Qiyinlik darajasi – 3

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

№ 162.
Manba:
Qiyinlik darajasi – 3

O'zDSt 1092:2009 standarti bu?
ERI standarti
Shifrlash standarti
Xesh funksiya standarti
Kalitni generatsiyalash standarti

№ 163.
Manba:
Qiyinlik darajasi – 3

DSA ERI standarti qanday murakkablikka asoslanadi?
diskret logarifmlash masalasini murakabligiga
faktorizatsiyalash masalasi murakkabligiga
elliptik egri chiziqlarga asoslangan diskret logarifmlash masalasi murakkabligiga
elliptik egri chiziqlarga asoslangan faktorizatsiyalash masalasi murakkabligiga

№ 164.
Manba:
Qiyinlik darajasi – 3

O'zDSt 1092:2009 ERI standarti birinchi algoritmi qanday murakkablikka asoslanadi?
daraja parametr muammosiga
diskret logarifmlash muammosiga
faktorizatsiyalash muammosiga
elliptik egri chiziqlarda faktorizatsiyalash murakkabligiga

№ 165.
Manba:
Qiyinlik darajasi – 3

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

№ 166.
Manba:
Qiyinlik darajasi – 3

Sonlarni tublikka tekshirishning Solovey-Shtrassen testida qanday kriteriyadan foydalanadi?
Eyler kriteriyasidan

Karlmaykl sonlari kriteriyasidan
Murakkab sonlar kriteriyasidan
Tub sonlar kriteriyasidan

№ 167.
Manba:
Qiyinlik darajasi – 3

Sonlarni tublikka tekshirishning Ferma testida qanday taqqoslamadan foydalaniladi?
a^(n-1)=1 (mod n)
a^(φ(n)-1)=1 (mod n)
a^(φ(n))=1 (mod n)
a^(n-1)≠1 (mod n)

№ 168.
Manba:
Qiyinlik darajasi – 3

Sonlarni tublikka tekshirishning Ferma testida qanday taqqoslama bajarilganda tekshirilayotgan son murakkab bo'ladi?
a^(n-1)≠1 (mod n)
a^(n-1)=1 (mod n)
a^(φ(n)-1)≠1 (mod n)
a^(φ(n)-1)=1 (mod n)

№ 169.
Manba:
Qiyinlik darajasi – 3

Sonlarni tublikka tekshirishning Solovey-Shtrassen testida qanday taqqoslamadan foydalanadi?
a^((p-1)/2)=(a/p) mod p
a^((p-1)/2)=1 mod p
a^((p-1)/2)≠(a/p) mod p
a^((p-1)/2)≠1 mod p

№ 170.
Manba:
Qiyinlik darajasi – 3

Sonlarni tublikka tekshirishning Solovey-Shtrassen testida qanday simvoldan foydalanadi?
Lejandr simvolidan
Karlmaykl simvolidan
Eyler simvolidan
Lukas simvolidan

№ 171.
Manba:
Qiyinlik darajasi – 3

Sonlarni tublikka tekshirishning Solovey-Shtrassen testida Lejandr simvoli qanday qiymatlarni qabul qilishi mumkin?
0,-1,1
0,1
0,-1
1, -1

№ 172.
Manba:
Qiyinlik darajasi – 3

2 lik sanoq tizimida 0101 soniga 1111 sonini 2 modul bo’yicha qo’shing?
1010
101
1111
1001

№ 173.
Manba:
Qiyinlik darajasi – 3

143mod17 nechiga teng?
7
6
5
8

№ 174.
Manba:
Qiyinlik darajasi – 3

-19mod11 nechiga teng?
3
5
4
2

№ 175.
Manba:
Qiyinlik darajasi – 3

Ochiq kalitli RSA shifrlash algoritmida "p=11" tub son bo'lsa Eyler funskiyasi $\varphi(p)$ qanday qiymat qaytaradi?
10
8
6
4

№ 176.
Manba:
Qiyinlik darajasi – 3

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

№ 177.
Manba:
Qiyinlik darajasi – 3

13 soni bilan o’zaro tub bo’lgan sonlarni ko’rsating?
5, 7

12, 26
14, 39
13 dan tashqari barcha sonlar

№ 178.
Manba:
Qiyinlik darajasi – 3

Ellipti egri chiziqlarda funksiya koeffitsentlari a, b qiymati qanday shartni qanoatlantirishi kerak?
4*a^3+27*b^2≠0
4*a^2+27*b^2≠0
4*a^3+27*b^3≠0
4*a^2+27*b^3≠0

№ 179.
Manba:
Qiyinlik darajasi – 3

Eyler kriteriyasidan qaysi algoritmda foydalanadi?
Solovey-Shtrassen algortmida
Ferma algoritmida
Rabbin Miller algoritmida
RSA algoritmida

№ 180.
Manba:
Qiyinlik darajasi – 3

Qaysi algoritm Karlmaykl sonlarini murakkab son sifatida aniqlaydi?
Solovey-Shtrassen algoritmi
Ferma algoritmi
Rabbin Miller algoritmi
RSA algoritmi

№ 181.
Manba:
Qiyinlik darajasi – 3

17 soni bilan o’zaro tub bo’lgan sonlarni ko’rsating?
16, 18
12, 34
14, 51
17 dan tashqari barcha sonlar

№ 182.
Manba:
Qiyinlik darajasi – 3

Faktorlash muammosi ifodalangan qatorni ko’rsating?
N=p*q;
Y=(g^a)modp;
N=SQRT(P);
Y=g^a;

№ 183.

Manba:
Qiyinlik darajasi – 3

DES shifrlash algoritmi…
Simmetrik blokli shifr.
Ochiq kalitli shifr.
Assimetrik shifr.
Ikki kalitli shifr.

№ 184.
Manba:
Qiyinlik darajasi – 3

AQSH ning elektron raqamli imzo standartini ko‘rsating
DSS
DSA
RSA
ESIGN

№ 185.
Manba:
Qiyinlik darajasi – 3

Xeshlash algoritmlaridan qaysi xususiyatni ta’minlashda foydalaniladi?
Butunlik
Maxfiylik
Foydalanuvchanlik
Autentifikatsiya

№ 186.
Manba:
Qiyinlik darajasi – 3

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

№ 187.
Manba:
Qiyinlik darajasi – 3

Eng katta umumiy bo‘luvchi qanday belgilanadi?
EKUB(*a, b)*
EKUD
EKUK
EKUK(a,b)

№ 188.
Manba:
Qiyinlik darajasi – 3

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

№ 189.
Manba:
Qiyinlik darajasi – 3

O‘z DSt 1092 standartida qanday amallardan foydalanilgan?
Parametr bilan ko‘paytirish, parametr bilan darajaga ko‘tarish, parametr bilan teskarilash
Ko‘paytirish, darajaga ko‘tarish, teskarilash
Qo‘shish ayirish ko‘paytirish, bo‘lish
Qo‘shish, bo‘lish, ayirish, darajaga ko‘tarish

№ 190.
Manba:
Qiyinlik darajasi – 3

O‘z DSt 1092 standarti qanday matematik murakkablik asosida yaratilgan?
Parametrli algebra
Elliptik egri chiziqli diskret logarifm
Diskret logarifmlashni hisoblash
Tub ko‘paytuvchilarga ajratish

№ 191.
Manba:
Qiyinlik darajasi – 3

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

№ 192.
Manba:
Qiyinlik darajasi – 3

Sonlarni tublikka tekshirishning Solavey-Shtrassen testida qanday simvoldan foydalanadi?
Lejandr simvolidan
Karlmaykl simvolidan
Eyler simvolidan
Lukas simvolidan

№ 193.
Manba:
Qiyinlik darajasi – 3

Sonlarni tublikka tekshirishning Solavey-Shtrassen testida Lejandr simvoli qiymati qanday aniqlanadi?
(a/p)
(p/a)
(p-1)/2
(a-1)/2

№ 194.
Manba:

Qiyinlik darajasi – 3

ГОСТ Р 34. 10-2001 elektron raqamli imzo algoritmida qaysi xesh-funksiyadan foydalaniladi?
ГОСТ Р 34.11-94
O‘z DSt 1106
A5
SHA-256

№ 195.
Manba:
Qiyinlik darajasi – 3

Elektron raqamli imzo algoritmlari bardoshligini yanada oshirishda qanday funksiyalardan foydalaniladi?
Xesh-funksiya
Matematik funksiya
Bir tomonlama funksiya
Logarifmik funksiya

№ 196.
Manba:
Qiyinlik darajasi – 3

EC DSA elektron raqamli imzo algoritmi qanday matematik murakkablik asosida yaratilgan?
Elliptik egri chiziqli diskret logarifm
Diskret logarifmlashni hisoblash
Tub ko‘paytuvchilarga ajratish
Chiziqli algebraik tenglamalar sistemasini yechish

№ 197.
Manba:
Qiyinlik darajasi – 3

DSA algoritmidan qanday maqsadda foydalaniladi?
Elektron raqamli imzo
Autentifikatsiya
Shifrlash
Xeshlash

№ 198.
Manba:
Qiyinlik darajasi – 3

DSSda qaysi algoritmdan foydalanilgan?
Toxir El Gamal algoritmi
K. Shnorr
RSA
ESIGN

№ 199.
Manba:
Qiyinlik darajasi – 3

El Gamal algoritmidan qanday maqsadda foydalaniladi?
Shifrlash va elektron raqamli imzo
Autentifikatsiya va xeshlash

Shifrlash
Elektron raqamli imzo

№ 200.
Manba:
Qiyinlik darajasi – 3

RSA algoritmidan qanday maqsadda foydalaniladi?
Shifrlash va elektron raqamli imzo
Autentifikatsiya va xeshlash
Shifrlash
Elektron raqamli imzo

Foydalanilgan adabiyotlar

1. Z.T. Xudoyqulov, Sh.Z. Islomov, U.R. Mardiyev. “Kriptografiya 1: o’quv qo’llanma” – Тошкент, 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.