5330300-Axborot xavfsizligi yo’nalishi bakalavr talabalari uchun “Kriptografiya 1” 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.
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

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:
Qiyinlik darajasi – 1

Kriptologiya necha yo‘nalishga bo‘linadi?
2
4
6
8

№ 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

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

№ 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

Ma’lumotlarni kodlash va dekodlashda necha kalitdan foydalanadi?
kalit ishlatilmaydi
4 ta
2 ta
3 ta

№ 13.
Manba:
Qiyinlik darajasi – 1

Simmetrik kriptotizimlarda necha kalitdan foydalaniladi?
1 ta
3 ta
4 ta
kalit ishlatilmaydi

№ 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

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:
Qiyinlik darajasi – 1

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 o‘rniga qo‘yish va o‘rin almashtirish akslantirishlarning kombinatsiyalaridan birgalikda foydalaniladigan algoritmlar
shifrlash jarayonida kalitlarning o‘rni almashtiriladigan algoritmlarga

№ 19.
Manba:
Qiyinlik darajasi – 1

O‘rniga qo‘yish shifrlash algoritmlari necha sinfga bo‘linadi?
2
4
6
8

№ 20.
Manba:
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:

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:

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:

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:

Qiyinlik darajasi – 1

RC4 oqimli shifrlash algoritmi asosan qayerda qo‘llaniladi?
simsiz aloqa vositalaridagi mavjud WEP protokolida
mobil aloqa standarti GSM protokolida
inernet trafiklarini shifrlashda
radioaloqa tarmoqlarda

№ 25.

Manba:

Qiyinlik darajasi – 1

A5/1 oqimli shifrlash algoritmida dastlabki kalit uzunligi nechi bitga teng?
64

512
192
256

№ 26.
Manba:
Qiyinlik darajasi – 1

A5/1 oqimli shifrlash algoritmida har bir qadamda kalit oqimining qanday qiymatini hosil qiladi?
bir biti
bir bayti
64 biti
8 bayti

№ 27.
Manba:
Qiyinlik darajasi – 1

RC4 oqimli shifrlash algoritmida har bir qadamda kalit oqimining qanday qiymatini hosil qiladi?
bir baytini
bir bitini
64 bitini
8 baytini

№ 28.
Manba:
Qiyinlik darajasi – 1

Blokli shifrlash algoritmlari arxitekturasi jihatidan qanday tarmoqlarga bo‘linadi?
Feystel va SP
SP va Petri
Feystel va Petri
Kvadrat va iyerarxik

№ 29.
Manba:
Qiyinlik darajasi – 1

Blokli simmetrik shifrlash algoritmlari raund funksiyalarida qanday amallar bajariladi?
ARX
PRX
RPT
XOR

№ 30.
Manba:
Qiyinlik darajasi – 1

ARX amali nimalardan iborat?
add, rotate, xor
mod, rotate, xor
add, mod, xor

add, rotate, mod

№ 31.
Manba:
Qiyinlik darajasi – 2

DES shifrlash algoritmi qaysi tarmoqqa asoslangan holda ishlaydi?
Feystel tarmog‘iga asoslangan holda
SPN tarmog‘iga asoslangan holda
Lai-Massey tarmog‘iga asoslangan holda
hech qanday tarmoqqa asoslanmaydi

№ 32.
Manba:
Qiyinlik darajasi – 2

DES shifrlash algoritmida raundlar soni nechta?
16
32
64
128

№ 33.
Manba:
Qiyinlik darajasi – 2

DES shifrlash algoritmida kalit uzunligi necha bitga teng?
56
512
192
256

№ 34.
Manba:
Qiyinlik darajasi – 2

DES shifrlash algoritmida har bir raunda necha bitli raund kalitlaridan foydalaniladi?
48
56
64
32

№ 35.
Manba:
Qiyinlik darajasi – 2

AES algoritmida shifrlash kalitining uzunligi necha bitga teng?
128, 192, 256 bit
128, 156, 256 bit
128, 192 bit
256, 512 bit

№ 36.
Manba:
Qiyinlik darajasi – 2

AES shifrlash algoritmida raundlar soni nechaga teng bo‘ladi?
10, 12, 14
14, 16, 18
18, 20, 22
22, 24, 26

№ 37.
Manba:
Qiyinlik darajasi – 2

AES algoritmida raundlar soni nimaga bo‘gliq?
kalit uzunligiga
kiruvchi blok uzunligi va matn qiymatiga
foydalanilgan vaqtiga
kiruvchi blok uzunligiga

№ 38.
Manba:
Qiyinlik darajasi – 2

AES algoritmida nechta akslantirishlardan foydalaniladi?
4
2
5
6

№ 39.
Manba:
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:
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:

Qiyinlik darajasi – 2

Xesh qiymatlarni yana qanday atash mumkin?
dayjest
funksiya
imzo
raqamli imzo

№ 42.
Manba:
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:
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:
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:
Qiyinlik darajasi – 2

Xesh funsiyalarga 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:
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:
Qiyinlik darajasi – 2

CRC-3 tizimida CRC qiymatini hisoblash jarayonida ma'lumotga nechta nol biriktiriladi?
3
6
9
12

№ 48.
Manba:
Qiyinlik darajasi – 2

CRC-4 tizimida CRC qiymatini hisoblash jarayonida ma’lumotga nechta nol biriktiriladi?
4
8
12
16

№ 49.
Manba:
Qiyinlik darajasi – 2

CRC-5 tizimida CRC qiymati hisoblash jarayonida ma’lumotga nechta nol biriktiriladi?
5
10
15
20

№ 50.
Manba:
Qiyinlik darajasi – 2

CRC-6 tizimida CRC qiymati hisoblash jarayonida ma’lumotga nechta nol biriktiriladi?
6
12
18
24

№ 51.
Manba:
Qiyinlik darajasi – 2

Qaysi maxfiylikni ta’minlash usulida kalitdan foydalanilmaydi?
kodlash
shifrlash
steganografiya

autentifikatsiya

№ 52.
Manba:
Qiyinlik darajasi – 2

Ximoyalanuvchi ma’lumot boshqa bir ma’lumotni ichiga yashirish orqali maxfiyligini ta’minlaydigan usul qaysi?
steganografiya
kodlash
shifrlash
autentifikatsiya

№ 53.
Manba:
Qiyinlik darajasi – 2

Baytlar kesimida shifrlashni amalga oshiradigan algoritm keltirilgan qatorni ko’rsating?
RC4
A5/1
SHA1
MD5

№ 54.
Manba:
Qiyinlik darajasi – 2

Bitlar kesimida shifrlashni amalga oshiradigan algoritm keltirilgan qatorni ko’rsating?
A5/1
RC4
SHA1
MD5

№ 55.
Manba:
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:
Qiyinlik darajasi – 2

Sezar shifrlash algoritmi qaysi turdagi akslantirishga asoslangan?
o’rniga qo’yish
o’rin almashtirish
kompozitsion
aralash

№ 57.
Manba:
Qiyinlik darajasi – 2

Vijiner shifrlash algoritmi qaysi turdagi akslantirishga asoslanadi?
o’rniga qo’yish
o’rin almashtirish
kompozitsion
aralash

№ 58.
Manba:
Qiyinlik darajasi – 2

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

№ 59.
Manba:
Qiyinlik darajasi – 2

16 raund davom etadigan blokli shifrlash algoritmi ko’rsating?
DES
AES
A5/1
RC4

№ 60.
Manba:
Qiyinlik darajasi – 2

10 raund davom etadigan blokli shifrlash algoritmi ko’rsating?
AES
DES
A5/1
RC4

№ 61.
Manba:
Qiyinlik darajasi – 2

Qanday algoritmlarda chiqishda doim fiksirlangan uzunlikdagi qiymat chiqadi?
xesh algoritmlarda
shifrlash algoritmlarida
kodlash algoritmlarida
steganografik algoritmlarda

№ 62.
Manba:

Qiyinlik darajasi – 2

Vernam shifrlash algoritm asosi qaysi mantiqiy hisoblashga asoslangan
XOR
ARX
ROX
XRA

№ 63.
Manba:
Qiyinlik darajasi – 2

Chastotalar tahlili kriptotahlil usuli samarali ishlidigan algorimtlar keltirilgan qatorni belgilang?
Sezar, Affin
Vernam
Vijiner
RC4

№ 64.
Manba:
Qiyinlik darajasi – 2

Simmetrik shifrlash algorimtlarida qanday muammo mavjud?
kalitni uzatish
kalit generatsiyalash
kalitni saqlash
kalitni yo’q qilish

№ 65.
Manba:
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:
Qiyinlik darajasi – 2

Foydanaluvchanlikni ta’minlash bu-?
ruxsat etilmagan “bajarishdan” himoyalash
ruxsat etilmagan “yozishdan” himoyalash
ruxsat etilmagan “o‘qishdan” himoyalash
ruxsat berilgan “amallarni” bajarish

№ 67.
Manba:
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:
Qiyinlik darajasi – 2

.... kriptotizimni shifrlash va rasshifrovkalash uchun sozlashda foydalaniladi.
kalit
ochiq matn
alifbo
algoritm

№ 69.
Manba:
Qiyinlik darajasi – 2

Agar ochiq ma’lumot shifrlansa, natijasi .... bo‘ladi.
shifrmatn
ochiq matn
noma’lum
kod

№ 70.
Manba:
Qiyinlik darajasi – 2

Rasshifrovkalash jarayonida kalit va ..... kerak bo‘ladi
shifrmatn
ochiq matn
kodlash
alifbo

№ 71.
Manba:
Qiyinlik darajasi – 3

Ma’lumotni sakkizlik sanoq tizimidan o‘n oltilik sanoq tizimiga o‘tkazish bu?
kodlash
shifrlash
yashirish
rasshifrovkalash

№ 72.
Manba:
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:
Qiyinlik darajasi – 3

Ikki kalitli deyilganda qaysi kriptotizim nazarda tutiladi?
ochiq kalitli kriptotizim
simmetrik kriptotizim
xesh funksiyalar
MAC tizimlari

№ 74.
Manba:
Qiyinlik darajasi – 3

Ma’lumotni mavjudligini yashirishni maqsad qilgan bilim sohasi bu?
steganografiya
kriptografiya
kodlash
kriptotahlil

№ 75.
Manba:
Qiyinlik darajasi – 3

Ma’lumotni konfidensialligini ta’minlash uchun ..... zarur.
shifrlash
kodlash
deshifrlash
rasshifrovkalash

№ 76.
Manba:
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:
Qiyinlik darajasi – 3

Qadimiy davr klassik shifriga quyidagilarning qaysi biri tegishli?
Sezar
kodlar kitobi
Enigma shifri
DES, AES shifri

№ 78.

Manba:
Qiyinlik darajasi – 3

Kompyuter davriga tegishli shifrlarni aniqlang?
DES, AES shifri
kodlar kitobi
Sezar
Enigma shifri

№ 79.
Manba:
Qiyinlik darajasi – 3

.... shifrlar blokli va oqimli turlarga ajratiladi
simmetrik
ochiq kalitli
assimetrik
klassik

№ 80.
Manba:
Qiyinlik darajasi – 3

Tasodifiy ketma-ketliklarni generatsiyalashga asoslangan shifrlash turi bu?
oqimli shifrlar
blokli shifrlar
ochiq kalitli shifrlar
assimetrik shifrlar

№ 81.
Manba:
Qiyinlik darajasi – 3

Ochiq matn qismlarini takror shifrlashga asoslangan usul bu?
blokli shifrlar
oqimli shifrlar
ochiq kalitli shifrlar
assimetrik shifrlar

№ 82.
Manba:
Qiyinlik darajasi – 3

A5/1 shifri qaysi turga mansub?
oqimli shifrlar
blokli shifrlar
ochiq kalitli shifrlar
assimetrik shifrlar

№ 83.
Manba:
Qiyinlik darajasi – 3

Qaysi algoritmlar simmetrik blokli shifrlarga tegishli?
AES, DES
A5/1, AES
Sezar, AES
Vijiner, DES

№ 84.
Manba:
Qiyinlik darajasi – 3

Simmetrik kriptotizimlarning asosiy kamchiligi bu?
kalitni taqsimlash zaruriyati
shifrlash jarayonining ko‘p vaqt olishi
kalitlarni esda saqlash murakkabligi
algoritmlarning xavfsiz emasligi

№ 85.
Manba:
Qiyinlik darajasi – 3

Faqat simmetrik blokli shifrlarga xos bo‘lgan atamani aniqlang?
blok uzunligi
kalit uzunligi
ochiq kalit
kodlash jadvali

№ 86.
Manba:
Qiyinlik darajasi – 3

Sezar shifrlash usuli qaysi akslantirishga asoslangan?
o‘rniga qo‘yish
o‘rin almashtirish
ochiq kalitli shifrlarga
kombinatsion akslantirishga

№ 87.
Manba:
Qiyinlik darajasi – 3

Kerxgofs prinsipiga ko‘ra kriptotizimning to‘liq xavfsiz bo‘lishi faqat qaysi kattalik nomalum bo‘lishiga asoslanishi kerak?
kalit
algoritm
shifrmatn
protokol

№ 88.
Manba:
Qiyinlik darajasi – 3

Shifrlash va deshifrlashda alohida kalitlardan foydalanuvchi kriptotizimlar bu?

ochiq kalitli kriptotizimlar
simmetrik kriptotizimlar
bir kalitli kriptotizimlar
xesh funksiyalar

№ 89.
Manba:
Qiyinlik darajasi – 3

Simmetrik shifrlar axborotni qaysi xususiyatlarini ta’minlashda foydalaniladi?
konfidensiallik va yaxlitlilik
konfidensiallik va foydalanuvchanlik
foydalanuvchanlik va yaxlitlik
foydalanuvchanlik

№ 90.
Manba:
Qiyinlik darajasi – 3

Ochiq kalitli shifrlar axborotni qaysi xususiyatlarini ta’minlashda foydalaniladi?
konfidensiallik va yaxlitlilik
konfidensiallik va foydalanuvchanlik
foydalanuvchanlik va yaxlitlik
foydalanuvchanlik

№ 91.
Manba:
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:
Qiyinlik darajasi – 3

Ochiq kalitli shifrlashda deshifrlash qaysi kalit asosida amalga oshiriladi?
shaxsiy kalit
ochiq kalit
kalitdan foydalanilmaydi
umumiy kalit

№ 93.
Manba:
Qiyinlik darajasi – 3

Quyidagi ta’rif qaysi atamaga tegishli: “maxfiy kodlarni”ni yaratish bilan shug‘ullanadigan soha-bu?
kriptografiya
kriptologiya

kriptotahlil
kripto

№ 94.
Manba:
Qiyinlik darajasi – 3

Quyidagi ta’rif qaysi atamaga tegishli: “maxfiy kodlarni”ni buzish bilan shug‘ullanadigan soha-bu?
kriptotahlil
kriptografiya
kriptologiya
kripto

№ 95.
Manba:
Qiyinlik darajasi – 3

Kriptotizimni boshqaradigan vosita?
kalit
algoritm
stegokalit
kriptotizim boshqarilmaydi

№ 96.
Manba:
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:
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:
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:
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:
Qiyinlik darajasi – 3

Qanday algorimtlar qaytmas xususiyatiga ega hisoblanadi?
xesh funksiyalar
elektron raqamli imzo algoritmlari
simmetrik kriptotizimlar
ochiq kalitli kriptotizimlar

№ 101.
Manba:
Qiyinlik darajasi – 1

RC4 shifrlash algoritmi qaysi turga mansub?
oqimli shifrlar
blokli shifrlar
ochiq kalitli shifrlar
assimetrik shifrlar

№ 102.
Manba:
Qiyinlik darajasi – 1

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

№ 103.
Manba:
Qiyinlik darajasi – 1

ARX amali qaysi shifrlash algoritmlarida foydalaniladi?
Blokli shifrlashda
Ochiq kalitli shifrlashda

Assimetrik shifrlashda
Ikki kalitli shifrlashda

№ 104.
Manba:
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:
Qiyinlik darajasi – 1

Qaysi algoritm har bir qadamda bir bayt qiymatni shifrlaydi?
RC4
A5/1
RSA
AES

№ 106.
Manba:
Qiyinlik darajasi – 1

Qaysi algorimtda har bir qadamda bir bit qiymatni shifrlaydi?
A5/1
RC4
RSA
AES

№ 107.
Manba:
Qiyinlik darajasi – 1

AES algoritmi qaysi tarmoq asosida qurilgan?
SP
Feystel
Petri
Petri va SP

№ 108.
Manba:
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:
Qiyinlik darajasi – 1

AES shifrlash algoritmi nomini kengaytmasini ko‘rsating?
Advanced Encryption Standard
Advanced Encoding Standard
Advanced Encryption Stadium
Always Encryption Standard

№ 110.
Manba:
Qiyinlik darajasi – 1

A5/1 shifrlash algoritmi bu?
oqimli shifrlash algoritmi
ochiq kalitli shifrlash algoritmi
assimetrik shifrlash algoritmi
blokli shifrlash algoritmi

№ 111.
Manba:
Qiyinlik darajasi – 1

RC4 shifrlash algoritmi bu?
oqimli shifrlash algoritmi
ochiq kalitli shifrlash algoritmi
asimetrik shifrlash algoritmi
blokli shifrlash algoritmi

№ 112.
Manba:
Qiyinlik darajasi – 1

DES shifrlash algoritmi bu?
blokli shifrlash algoritmi
oqimli shifrlash algoritmi
ochiq kalitli shifrlash algoritmi
asimetrik shifrlash algoritmi

№ 113.
Manba:
Qiyinlik darajasi – 1

AES shifrlash algoritmi bu?
blokli shifrlash algoritmi
oqimli shifrlash algoritmi
ochiq kalitli shifrlash algoritmi
asimetrik shifrlash algoritmi

№ 114.

Manba:
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:
Qiyinlik darajasi – 1

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

№ 116.
Manba:
Qiyinlik darajasi – 1

A5/1 oqimli shifrlash algoritmida maxfiy kalit necha registrga bo’linadi?
3
4
5
6

№ 117.
Manba:
Qiyinlik darajasi – 1

A5/1 oqimli shifrlash algoritmida X registr uzunligi nechi bitga teng?
19
17
16
15

№ 118.
Manba:
Qiyinlik darajasi – 1

A5/1 oqimli shifrlash algoritmida Y registr uzunligi nechi bitga teng?
22
21
19
20

№ 119.
Manba:
Qiyinlik darajasi – 1

A5/1 oqimli shifrlash algoritmida Z registr uzunligi nechi bitga teng?
23
20
19
18

№ 120.
Manba:
Qiyinlik darajasi – 1

Qaysi xesh algoritmda xesh qiymat 128 bitga teng bo’ladi?
MD5
SHA1
CRC
MAC

№ 121.
Manba:
Qiyinlik darajasi – 1

Qaysi xesh algoritmda xesh qiymat 160 bitga teng bo’ladi?
SHA1
MD5
CRC
MAC

№ 122.
Manba:
Qiyinlik darajasi – 1

Xeshlash algoritmlarini ko‘rsating?
SHA1, MD5, O‘z DSt 1106
RSA, DSA, El-gamal
DES, AES, Blovfish
O‘z DSt 1105, ГОСТ 28147-89, FEAL

№ 123.
Manba:
Qiyinlik darajasi – 1

Qaysi algoritmda, algoritmning necha round bajarilishi ochiq matn uzunligiga bog’liq?
A5/1
MD5
SHA1
HMAC

№ 124.
Manba:
Qiyinlik darajasi – 1

A5/1 oqimli shifrlash algoritmida major qiymati hisoblash jarayonida, birinchi (X) registrning qaysi qiymati olinadi?

x8
x9
x10
x11

№ 125.
Manba:
Qiyinlik darajasi – 1

A5/1 oqimli shifrlash algoritmida major qiymati hisoblash jarayonida, ikkinchi (Y) registrning qaysi qiymati olinadi?
y10
y11
y12
y13

№ 126.
Manba:
Qiyinlik darajasi – 1

A5/1 oqimli shifrlash algoritmida major qiymati hisoblash jarayonida, uchinchi (Z) registrning qaysi qiymati olinadi?
z10
z11
z12
z13

№ 127.
Manba:
Qiyinlik darajasi – 1

Sezar shifrlash algoritmida shifrlash formulasi qanday?
C=(M+K) mod p
C=(M-K) mod p
C=(M*K) mod p
C=(M/K) mod p

№ 128.
Manba:
Qiyinlik darajasi – 1

Sezar shifrlash algoritmida rasshifrovkalash formulasi qanday?
M=(C-K) mod p
M=(C+K) mod p
M=(C*K) mod p
M=(C/K) mod p

№ 129.
Manba:
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:
Qiyinlik darajasi – 1

DES shifrlash algoritmi simmetrik turga mansub bo‘lsa, unda nechta kalitdan foydalaniladi?
1
2
3
4

№ 131.
Manba:
Qiyinlik darajasi – 2

AES shifrlash algoritmi simmetrik turga mansub bo‘lsa, unda nechta kalitdan foydalaniladi?
1
2
3
4

№ 132.
Manba:
Qiyinlik darajasi – 2

A5/1 shifrlash algoritmi simmetrik turga mansub bo‘lsa, unda nechta kalitdan foydalaniladi?
1
2
3
4

№ 133.
Manba:
Qiyinlik darajasi – 2

RC4 shifrlash algoritmi simmetrik turga mansub bo‘lsa, unda nechta kalitdan foydalaniladi?
1
2
3
4

№ 134.
Manba:
Qiyinlik darajasi – 2

DES shifrlash algoritmida S-bloklardan chiqqan qiymatlar uzunligi necha bitga teng bo‘ladi?
4
8

12
16

№ 135.
Manba:
Qiyinlik darajasi – 2

DES shifrlash algoritmida S-bloklarga kiruvchi qiymatlar uzunligi necha bitga teng bo‘ladi?
6
12
18
24

№ 136.
Manba:
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:
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:
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:
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:
Qiyinlik darajasi – 2

MD5 xesh funksiyasida chiquvchi qiymat uzunligi nechaga teng?
128
Ixtiyoriy
510
65

№ 141.
Manba:
Qiyinlik darajasi – 2

MD5 xesh funksiyasida kiruvchi ma’lumot uzunligi qanday bitli bloklarga bo‘linadi?
512
1024
2048
4096

№ 142.
Manba:
Qiyinlik darajasi – 2

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

№ 143.
Manba:
Qiyinlik darajasi – 2

MD5 xesh funksiyasida amallar necha raund davomida bajariladi?
64
128
256
512

№ 144.
Manba:
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:
Qiyinlik darajasi – 2

MD5 xesh funksiyasida initsializatsiya bosqichida nechta 32 bitli registrdan foydalanadi?
4
8
12
16

№ 146.
Manba:
Qiyinlik darajasi – 2

MD5 xesh funksiyasida initsializatsiya bosqichida 4 ta necha bitli registrlardan foydalanadi?
32
64
128
256

№ 147.
Manba:
Qiyinlik darajasi – 2

SHA1 xesh funksiyasida chiquvchi qiymat uzunligi nechaga teng?
160
Ixtiyoriy
512
256

№ 148.
Manba:
Qiyinlik darajasi – 2

SHA1 xesh funksiyasida kiruvchi ma’lumot uzunligi qanday bitli bloklarga bo‘linadi?
512
1024
2048
4096

№ 149.
Manba:
Qiyinlik darajasi – 2

Faqat xesh funksiyalar nomi keltirilgan qatorni ko‘rsating?
SHA1, MD5
SHA1, DES
MD5, AES
HMAC, A5/1

№ 150.
Manba:
Qiyinlik darajasi – 2

SHA1 xesh funksiyasida amallar nechi raund davomida bajariladi?
80
128
256
512

№ 151.
Manba:
Qiyinlik darajasi – 2

Faqat simmetrik shifrlash algoritmlari nomi keltirilgan qatorni ko‘rsating?
AES, A5/1
SHA1, DES
MD5, AES
HMAC, RC4

№ 152.
Manba:
Qiyinlik darajasi – 2

SHA1 xesh funksiyasida initsializatsiya bosqichida nechta registrdan foydalanadi?
5
10
15
20

№ 153.
Manba:
Qiyinlik darajasi – 2

SHA1 xesh funksiyasida initsializatsiya bosqichida 5 ta necha bitli registrlardan foydalanadi?
32
64
128
256

№ 154.
Manba:
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:
Qiyinlik darajasi – 2

Faqat simmetrik shifrlash algoritmlari nomi keltirilgan qatorni ko‘rsating?
AES, A5/1

SHA1, DES
MD5, AES
HMAC, RC4

№ 156.
Manba:
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:
Qiyinlik darajasi – 2

DES shifrlash algoritmida rasshifrovkalashda birinchi raunda qaysi kalitdan foydalaniladi?
16-raund kalitidan
1-raund kalitidan
dastlabki kalitdan
1-raunda kalitdan foydalanilmaydi

№ 158.
Manba:
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:
Qiyinlik darajasi – 2

AES standarti qaysi algoritm asoslangan?
Rijndael
Serpent
Twofish
RC6

№ 160.
Manba:
Qiyinlik darajasi – 2

AES shifrlash algoritmida nechta akslantirishdan foydalanadi?
4
3
2
akslantirishdan foydalanilmaydi

№ 161.
Manba:
Qiyinlik darajasi – 2

GSM tarmog‘ida foydanalaniluvchi shifrlash algoritmi nomini ko‘rsating?
A5/1
DES
AES
RC4

№ 162.
Manba:
Qiyinlik darajasi – 2

add amalining ma’nosi nima?
modul asosida qo‘shish
surish (siklik surish, mantiqiy surish)
XOR amali
akslantirish

№ 163.
Manba:
Qiyinlik darajasi – 2

rotate amalining ma’nosi nima?
surish (siklik surish, mantiqiy surish)
modul asosida qo‘shish
XOR amali
Akslantirish

№ 164.
Manba:
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:
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:
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:
Qiyinlik darajasi – 2

AES shifrlash algoritmida shifrlash jarayonida qanday akslantirishdan foydalaniladi?
SubBytes, ShiftRows, MixColumns va AddRoundKey
SubBytes, ShiftRows va AddRoundKey
SubBytes, MixColumns va AddRoundKey
MixColumns, ShiftRows, SubBytes

№ 168.
Manba:
Qiyinlik darajasi – 2

AES shifrlash algoritmida 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:
Qiyinlik darajasi – 2

AES shifrlash algoritmida blok uzunligi 128, kalit uzunligi 192 bit bo‘lsa raundlar soni nechta bo‘ladi?
12
10
14
6

№ 170.
Manba:
Qiyinlik darajasi – 2

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

Rijndael
Twofish
Blowfish
IDEA

№ 171.
Manba:
Qiyinlik darajasi – 3

AES shifrlash algoritmida 128 bitli ma’lumot bloki qanday o‘lchamdagi jadvalga solinadi?
4x4
4x6
6x4
6x6

№ 172.
Manba:
Qiyinlik darajasi – 3

WEP protokolida (Wi-Fi tarmog‘ida) foydanalaniluvchi shifrlash algoritmi nomini ko‘rsating?
RC4
DES
SHA1
A5/1

№ 173.
Manba:
Qiyinlik darajasi – 3

AES shifrlash standarti qaysi davlat standarti?
AQSH
Rossiya
Buyuk Britaniya
Germaniya

№ 174.
Manba:
Qiyinlik darajasi – 3

SHA1 xesh funksiyasi qaysi davlat standarti?
AQSH
Rossiya
Buyuk Britaniya
Germaniya

№ 175.
Manba:
Qiyinlik darajasi – 3

DES shifrlash standarti qaysi davlat standarti?
AQSH
Rossiya
Buyuk Britaniya
Germaniya

№ 176.
Manba:
Qiyinlik darajasi – 3

Kolliziya hodisasi qaysi turdagi algoritmlarga xos?
xesh funksiyalar
ochiq kalitli shifrlash algoritmlari
simmetrik shifrlash algoritmlari
kalitlarni boshqarish tizimlari

№ 177.
Manba:
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:
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:
Qiyinlik darajasi – 3

Quyidagi ifoda nechta yechimga ega? 3*x=2 mod 7.
bitta yechimga ega
ikkita yechimga ega
yechimga ega emas
uchta yechimga ega

№ 180.
Manba:
Qiyinlik darajasi – 3

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

№ 181.

Manba:
Qiyinlik darajasi – 3

143mod17 nechiga teng?
7
6
5
8

№ 182.
Manba:
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:
Qiyinlik darajasi – 3

Qalbakilashtirish hujumi qaysi turdagi hujum turiga kiradi?
Immitatsiya
o’zgartirish
Fabrication
modification

№ 184.
Manba:
Qiyinlik darajasi – 3

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

№ 185.
Manba:
Qiyinlik darajasi – 3

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

№ 186.
Manba:

Qiyinlik darajasi – 3

Affin shifrlash algoritmida 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:
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:
Qiyinlik darajasi – 3

A5/1 oqimli shifrlash algoritmida x18=1, y21=0, z22=1 ga teng bo’lsa kalitni qiymatini toping
0
1
2
3

№ 189.
Manba:
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
110

№ 190.
Manba:
Qiyinlik darajasi – 3

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

№ 191.
Manba:

Qiyinlik darajasi – 3

3 sonini 5 chekli maydonda teskarisini toping?
2
3
4
5

№ 192.
Manba:
Qiyinlik darajasi – 3

Qaysi algoritmda maj kattaligi ishlatiladi?
A5/1
RC4
MD5
SHA1

№ 193.
Manba:
Qiyinlik darajasi – 3

MD5 xesh algoritmida nechta 32 bitli statik qiymatdan foydalanadi?
4
8
12
16

№ 194.
Manba:
Qiyinlik darajasi – 3

SHA1 xesh algoritmda nechta 32 bitli statik qiymatdan foydalanadi?
5
10
15
20

№ 195.
Manba:
Qiyinlik darajasi – 3

Qaysi xesh algoritmda 64 raund amal bajariladi?
MD5
SHA1
CRC
MAC

№ 196.
Manba:
Qiyinlik darajasi – 3

Qaysi xesh algoritmda 80 raund amal bajariladi?

SHA1
MD5
CRC
MAC

№ 197.
Manba:
Qiyinlik darajasi – 3

Qaysi blokli shifrlash algoritmida raund kalit uzunligi qiymatiga bo’gliq?
AES
DES
IDEA
RSA

№ 198.
Manba:
Qiyinlik darajasi – 3

Qaysi blokli shifrlash algoritmida 8 ta statik S-box lardan foydalaniladi?
DES
RC4
RSA
A5/1

№ 199.
Manba:
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:
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” – 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.

Масъул:	**Мардиев У.Р.**
Масъул:	**Турсунов О.О.**
Кафедра мудири:	**Худойқулов З.Т.**
Декан:	**Иргашева Д.Я.**