

$\phi(n)$  ni topish qiyinligi  $n$  sonining ... qiyinligiga bog'liq.

====

#Faktorlash

====

farajalash

====

ayrish

====

ildizlash

++++

$6 \bmod 11$  ning javobini toping

====

#1

====

2

====

3

====

4

++++

Eyler teoremasining nechanchi versiyasi RSA kriptografik tizimida foydalaniladi.

====

#ikkinchi

====

uchunchi

====

to'rtinchi

====

beshinchi

++++

" $M_p = 2^p - 1$ " formulasini kim aniqlagan ?

====

#Mersen

====

ferma

====

eyler

====

shopen

++++

Mersen formulasi nima uchun kerak ?

====

#Barcha tub sonlarni aniqlab beradi

====

barcha butun sonlarni aniqlab beradi

====

barcha manfiy sonlarni aniqlab beradi

====

sonlarning ildizini hisoblab beradi

++++

“Ferma tub sonlari topish formulasi” rostdan ham aniq tub sonlarni hisoblab bera oladimi ?

====

#Yo‘q

====

ha

====

albatta

====

aniq emas

++++

Quyidagi qaysi algoritm sonlarni tublikka tekshirishda effektiv hisonlanadi ?

====

#Determinicimk algoritmi

====

ferma algoritmi

====

dyron algoritmi

====

mersel algoritmi

++++

Ferma va kvadrat ildiz testlarinig kombinatsiyasidan tashkil topgan tekshirish usuli ?

====

#Rabbin – Miltter

====

faktORIZatsiyalash

====

2 karra ildiz olish

====

ayirish – ildiz olish

++++

Pollard usuli – ...

====

#Tub ko'paytuvchilarga ajratish algoritmini ifodalaydi hamda berilgan sonning tub ekanligini aniqlash imkonini beradi.

====

murakkab ko'paytuvchilarga ajratish algoritmini ifodalaydi hamda berilgan sonning tub ekanligini aniqlash imkonini beradi.

====

tub ko'paytuvchilarga ajratish algoritmini ifodalaydi hamda berilgan sonning murakkab ekanligini aniqlash imkonini beradi.

====

murakkab ko'paytuvchilarga ajratish algoritmini ifodalaydi hamda berilgan sonning juft ekanligini aniqlash imkonini beradi.

++++

RSA shifrlash algoritmi qachon o'ylab topilgan ?

====

#1997 – yili

====

1998 – yili

=====

1999 – yili

=====

2000 – yili

+++++

Ochiq kalitli kriptotizimlar ... akslantirishlarga (funksiyalarga) asoslanadi.

=====

#Bir tomonlama

=====

ko'p tomonlama

=====

2 tomonlama

=====

3 tomonlama

+++++

Qaysi shifrlash algoritmi kalitlar uzunligi teng bo'lgan holdabardoshligi RSA shifrlash algoritmi bardoshligiga teng ?

=====

#Eg – gamal

=====

poklington

=====

eyler

=====

mdr

+++++

$f(x) = a^x \pmod{p}$  formula qaysi algoritm uchun o'rinli ?

=====

#Diffi – xelman

=====

eyler

=====

Dyson

====

mdr

++++

Elleptik egri chiziq tenglama yechimlari shu nuqtaning ... deyiladi.

====

#Affin nuqtalari

====

chet nuqtalari

====

proporsional nuqtalari

====

ekstrimum nuqtalari

++++

Quyidagi algoritmlardan qaysi biri Algoritmning xavfsizligi katta tub sonlarga va ko'paytuvchilarga ajratish muammosiga asoslangan.

====

#Rabbin

====

eyker

====

Pailler

====

sezar

++++

Rabbin shifrlash algoritmi qachon chop etilgan ?

====

#1979 – yili

====

1980 – yili

====

1981 – yili

====

1982 – yili

++++

Rabbin shifrlash algoritmi kim tomonidan ishlab chiqilgan ?

=====

#Maykl Rabbin

=====

Tom Rabin

=====

Eric Rabin

=====

Robert Rabin

++++

Qanday shifrlash algoritmlari bitta (bir xil) elektron hujjatga har xil ERIni qo'yish imkoniyatini bermaydi ?

=====

#Ochiq kalitli

=====

yopiq kalitli

=====

ko'p qulfli

=====

shifr kalitli

++++

Ishonchliliganing yuqoriligi va shaxsiy kompyuterlarda amalga oshirilishining qulayligi bilan ajralib turuvchi raqamli imzo algoritmi nechanchi yilda El Gamal tomonidan ishlab chikildi ?

=====

#1984

=====

1985

=====

1986

=====

1987

++++

RSA kriptografik standartining standart raqami nima ?

====

#PKCS#1

====

PKCS#2

====

PKCS#3

====

PKCS#4

++++

ChangeCipherSpec Protocol nima vazifani bajaradi ?

====

#Ushbu protokol asosida aloqa kanali himoyalaniadi.

====

ushbu protokol asosida to'liq kanali himoyalaniadi.

====

ushbu protokol asosida shifr kanali himoyalaniadi.

====

ushbu protokol asosida xabarlar kanali himoyalaniadi.

++++

Application Data Protocol nima vazifani bajaradi ?

====

#Ushbu protokol ilova sathidan ma'lumotni olib, uni maxfiy kanal orqali yuborishni ta'minlaydi.

====

ushbu protokol tarmoq sathidan ma'lumotni olib, uni maxfiy kanal orqali yuborishni ta'minlaydi.

====

ushbu protokol fizik sathidan ma'lumotni olib, uni maxfiy kanal orqali yuborishni ta'minlaydi.

====

ushbu protokol ilova sathidan ma'lumotni olib, uni ochiq kanal orqali yuborishni ta'minlaydi.

++++

Handshake protocol nima vazifani bajaradi ?

====

#Ushbu protokol TLS protokolida asosiy protokollarda biri sanalib, bu protokol orqali xavfsizlik parametrlari uzatiladi.

====

ushbu protokol UTP protokolida asosiy protokollarda biri sanalib, bu protokol orqali xavfsizlik parametrlari uzatiladi.

====

ushbu protokol TCP protokolida asosiy protokollarda biri sanalib, bu protokol orqali xavfsizlik parametrlari uzatiladi.

====

ushbu protokol TLS protokolida asosiy protokollarda biri sanalib, bu protokol orqali ma'lumot parametrlari uzatiladi.

++++

HelloRequest nima vazifani bajaradi ?

====

#Ushbu xabar orqali server handshake protokolini qayta yuklaydi

====

ushbu xabar orqali client handshake protokolini qayta yuklaydi

====

ushbu xabar orqali server handshake protokolini yangilaydi

====

ushbu xabar orqali server handshake protokolini o'chiradi

++++

Gomomorfik shifrlash nima ?

====

#Bu har qanday ma'lumotlarni qayta ishlash va boshqarish paytida shifrlangan holda qolishga imkon beradigan shifrlash usuli

====

bu har qanday ma'lumotlarni qayta ishlash va boshqarish paytida shifrn olib tashlashga imkon beradigan shifrlash usuli

====

bu har qanday ma'lumotlarni qayta ishlash va boshqarish paytida shifrlangan holda qolishga imkon beradigan usuli

++++

bu har ayrim ma'lumotlarni qayta ishlash va boshqarish paytida shifrlangan holda qolishga imkon beradigan shifrlash usuli



++++

Gomomorfik shifrlash qachon kelib chiqqan ?

=====

#1978 – yilda

=====

1981 – yilda

=====

1982 – yilda

1983 – yilda

++++

Blokli shifrlash algoritmlari arxitekturasini jihatidan qanday tarmoqlarga bo'linadi?

=====

#Feystel va SP

=====

sp va petri

=====

feystel va petri

=====

kvadrat va iyerarxik

++++

A5/1 oqimli shifrlash algoritmidan har bir qadamda kalit oqimining qanday qiymatini hosil qiladi?

=====

#bir bit

=====

bir bayt

=====

64 bit

=====

8 bayt

++++

Blokli simmetrik shifrlash algoritmlari raund funksiyalarida qanday amallar bajariladi?

=====

#ArX

=====

PRX

=====

RPT

=====

XOR

+++++

ARX amali nimalardan iborat?

=====

#Add, rotate, xor

=====

mod, rotate, xor

=====

add, mod, xor

=====

add, rotate, mod

+++++

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

+++++

DES shifrlash algoritmda raundlar soni nechta?

=====

#16

=====

32

=====

64

=====

128

+++++

DES shifrlash algoritmda kalit uzunligi necha bitga teng?

=====

#56

=====

512

=====

192

=====

256

+++++

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

=====

#48

=====

56

=====

64

=====

98

+++++

AES algoritmda shifrlash kalitining uzunligi necha bitga teng?

=====

#128, 192, 256 bit

=====

1028, 254, 256 bit

=====

128, 1024 bit

=====

2048, 512 bit

+++++

AES shifrlash algoritmda raundlar soni nechaga teng bo'ladi?

=====

#10, 12, 14

=====

14, 16, 18

=====

18, 20, 22

=====

22, 24, 26

+++++

AES algoritmda raundlar soni nimaga bo'g'liq?

=====

#Kalit uzunligiga

=====

kiruvchi blok uzunligi va matn qiymatiga

=====

foydalanilgan vaqtiga

=====

kiruvchi blok uzunligiga

+++++

AES algoritmidan nechta akslantirishlardan foydalaniladi?

=====

#4

=====

5

=====

8

=====

6

+++++

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

+++++

Xesh funksiyalar qanday maqsadlarda ishlatiladi?

=====

#Ma'lumotni to'liqligini nazoratlash va ma'lumot manbaini autentifikatsiyalashda

=====

ma'lumotni maxfiylikni nazoratlash va ma'lumot manbaini haqiqiylikni tekshirishda

=====

ma'lumotni butunligini nazoratlashda

=====

ma'lumot manbaini autentifikatsiyalashda

+++++

Xesh qiymatlarni yana qanday atash mumkin?

=====

#Dayjest

====

funksiya

====

Imzo

====

raqamli imzo

++++

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

++++

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

++++

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

++++

Xesh funsiyalarga qanday turlarga bo'linadi?

====

#Kalitli va kalitsiz xesh funsiyalarga

====

kalitli va kriptografik bo'lmagan xesh funsiyalarga

====

kalitsiz va kriptografik bo'lmagan xesh funsiyalarga

====

kriptografik va kriptografik bo'lmagan xesh funsiyalarga

++++

Ma'lumotlarni autentifikatsiyalash kodlari deb qanday xesh funsiyalarga aytiladi?

====

#Kalitli xesh funsiyalarga

====

kalitsiz xesh funsiyalarga

====

kriptografik bo'lmagan xesh funsiyalarga

====

kriptografik xesh funsiyalarga

++++

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

====

#3

====

6

====

9

=====

12

+++++

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

=====

#4

=====

8

=====

12

=====

16

+++++

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

=====

#5

=====

10

=====

15

=====

20

+++++

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

=====

#6

=====

12

=====



18

=====

24

++++

Qaysi maxfiylikni ta'minlash usulida kalitdan foydalanilmaydi?

=====

#Kodlash

=====

shifrlash

=====

steganografiya

=====

autentifikatsiya

++++

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

=====

#Steganografiya

=====

kodlash

=====

shifrlash

=====

autentifikatsiya

++++

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

=====

#Rc4

=====

A5/1

=====

SHA1

=====

MD5

+++++

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

=====

#a5/1

=====

RC4

=====

SHA1

=====

MD5

+++++

Qaysi hujum turida barcha bo'lishi mumkin bo'lgan variantlar ko'rib chiqiladi?

=====

#Qo'pol kuch hujumi

=====

chastotalar tahlili

=====

analitik hujum

=====

sotsial injineriya

+++++

Sezar shifrlash algoritmi qaysi turdagi akslantirishga asoslangan?

=====

#O'rniga qo'yish

=====

o'rin almashtirish

=====

Kompozitsion

=====

aralash

++++

Vijiner shifrlash algoritmi qaysi turdagi akslantirishga asoslanadi?

=====

#O'rniga qo'yish

=====

o'rin almashtirish

=====

Kompozitsion

=====

aralash

++++

A5/1 oqimli shifrlash algoritmda registrarning surilishi qanday kattalikka bog'liq?

=====

#Maj funksiyasi qiymatiga

=====

kalit qiymatiga

=====

registr uzunligi qiymatiga

=====

hech qanday kattalikka bog'liq emas

++++

16 raund davom etadigan blokli shifrlash algoritmi ko'rsating?

=====

#DeS

=====

AES

=====

A5/1

=====

RC4

+++++

10 raund davom etadigan blokli shifrlash algoritmi ko'rsating?

=====

#AeS

=====

DES

=====

A5/1

=====

RC4

+++++

Qanday algoritmlarda chiqishda doim fiksirlangan uzunlikdagi qiymat chiqadi?

=====

#Xesh algoritmlarda

=====

shifrlash algoritmlarida

=====

kodlash algoritmlarida

=====

steganografik algoritmlarda

+++++

Vernam shifrlash algoritmi asosi qaysi mantiqiy hisoblashga asoslangan

=====

#XoR

=====

ARX

=====

ROX

=====

XRA

++++

Chastotalar tahlili kriptotahlil usuli samarali ishlidigan algorimtlar keltirilgan qatorni belgilang?

=====

#Sezar, Affin

=====

vernam

=====

Vijiner

=====

RC4

++++

Simmetrik shifrlash algorimtlarida qanday muammo mavjud?

=====

#Kalitni uzatish

=====

kalit generatsiyalash

=====

kalitni saqlash

=====

kalitni yo'q qilish

++++

Konfidensiallikni ta'minlash bu -?

=====

#Ruxsat etilmagan "o'qishdan" himoyalash

=====

ruxsat etilmagan "yozishdan" himoyalash

=====

ruxsat etilmagan “bajarishdan” himoyalash

=====

ruxsat berilgan “amallarni” bajarish

+++++

Foydalanuvchanlikni ta’minlash bu-?

=====

#Ruxsat etilmagan “bajarishdan” himoyalash

=====

ruxsat etilmagan “yozishdan” himoyalash

=====

ruxsat etilmagan “o’qishdan” himoyalash

=====

ruxsat berilgan “amallarni” bajarish

=====

Butunlikni ta’minlash bu - ?

=====

#Ruxsat etilmagan “yozishdan” himoyalash

=====

ruxsat etilmagan “bajarishdan” himoyalash

=====

ruxsat etilmagan “o’qishdan” himoyalash

=====

ruxsat berilgan “amallarni” bajarish

+++++

.... kriptotizimni shifrlash va rasshifrovkalash uchun sozlashda foydalaniladi.

=====

#Kalit

=====

ochiq matn

=====

alifbo

=====

algorithm

+++++

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

=====

#Shifrmtn

=====

ochiq matn

=====

noma'lum

=====

kod

+++++

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

=====

#Shifrmtn

=====

ochiq matn

=====

Kodlash

=====

alifbo

+++++

Ma'lumotni sakkizlik sanoq tizimidan o'n oltilik sanoq tizimiga o'tkazish bu?

=====

#Kodlash

=====

shifrlash

=====

yashirish

=====

rasshifrovkalash

+++++

Ma'lumotni shifrlash va deshifrlash uchun bir xil kalitdan foydalanuvchi tizim bu?

=====

#Simmetrik kriptotizim

=====

ochiq kalitli kriptotizim

=====

assimetrik kriptotizim

=====

xesh funksiyalar

+++++

Ikki kalitli deyilganda qaysi kriptotizim nazarda tutiladi?

=====

#Ochiq kalitli kriptotizim

=====

simmetrik kriptotizim

=====

xesh funksiyalar

=====

MAC tizimlari

+++++

Ma'lumotni mavjudligini yashirishni maqsad qilgan bilim sohasi bu?

=====

#Steganografiya

=====

kriptografiya

=====



kodlash

=====

kriptotahlil

+++++

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

=====

#Shifrlash

=====

kodlash

=====

deshifrlash

=====

rasshifrovkalash

+++++

Ma'lumotni uzatishda kriptografik himoya .....

=====

#Konfidensiallik va yaxlitlikni ta'minlaydi

=====

konfidensiallik va foydalanuvchanlikni ta'minlaydi

=====

foydalanuvchanlik va butunlikni ta'minlaydi

=====

konfidensiallikni ta'minlaydi

+++++

Qadimiy davr klassik shifriga quyidagilarning qaysi biri tegishli?

=====

#Sezar

=====

kodlar kitobi

=====

enigma shifri

=====

DES, AES shifri

+++++

Kompyuter davriga tegishli shifrlarni aniqlang?

=====

#DeS, AeS shifri

=====

kodlar kitobi

=====

Sezar

=====

enigma shifri

+++++

.... shifrlar blokli va oqimli turlarga ajratiladi

=====

#Simmetrik

=====

ochiq kalitli

=====

assimetrik

=====

klassik

+++++

Tasodifiy ketma-ketliklarni generatsiyalashga asoslangan shifrlash turi bu?

=====

#Oqimli shifrlar

=====

blokli shifrlar

=====

ochiq kalitli shifrlar

=====

assimetrik shifrlar

+++++

Ochiq matn qismlarini takror shifrlashga asoslangan usul bu?

=====

#Blokli shifrlar

=====

oqimli shifrlar

=====

ochiq kalitli shifrlar

=====

assimetrik shifrlar

+++++

A5/1 shifri qaysi turga mansub?

=====

#Oqimli shifrlar

=====

blokli shifrlar

=====

ochiq kalitli shifrlar

=====

assimetrik shifrlar

+++++

Qaysi algoritmlar simmetrik blokli shifrlarga tegishli?

=====

#AeS, DeS

=====

A5/1, AES

=====

Sezar, AES

=====

Vijiner, DES

+++++

Simmetrik kriptotizimlarning asosiy kamchiligi bu?

=====

#Kalitni taqsimlash zaruriyati

=====

shifrlash jarayonining ko'p vaqt olishi

=====

kalitlarni esda saqlash murakkabligi

=====

algoritmning xavfsiz emasligi

+++++

Faqat simmetrik blokli shifrlarga xos bo'lgan atamani aniqlang?

=====

#Blok uzunligi

=====

kalit uzunligi

=====

ochiq kalit

=====

kodlash jadvali

+++++

Sezar shifrlash usuli qaysi akslantirishga asoslangan?

=====

#O'rniga qo'yish

=====

o'rin almashtirish

=====

ochiq kalitli shifrlarga

=====

kombinatsion akslantirishga

+++++

Kerxgofs prinsipiga ko'ra kriptotizimning to'liq xavfsiz bo'lishi faqat qaysi kattalik nomalum bo'lishiga asoslanishi kerak?

=====

#Kalit

=====

algoritm

=====

shifrmavn

=====

protokol

+++++

Shifrlash va deshifrlashda alohida kalitlardan foydalanuvchi kriptotizimlar bu?

=====

#Ochiq kalitli kriptotizimlar

=====

simmetrik kriptotizimlar

=====

bir kalitli kriptotizimlar

=====

xesh funksiyalar

+++++

Simmetrik shifrlar axborotni qaysi xususiyatlarini ta'minlashda foydalaniladi?

=====

#Konfidensiallik va Yaxlitlilik

=====

konfidensiallik va foydalanuvchanlik

=====

foydalanuvchanlik va yaxlitlik

=====

foydalanuvchanlik

+++++

Ochiq kalitli shifrlar axborotni qaysi xususiyatlarini ta'minlashda foydalaniladi?

=====

#Konfidensiallik va yaxlitlik

=====

konfidensiallik va foydalanuvchanlik

=====

foydalanuvchanlik va yaxlitlik

=====

foydalanuvchanlik

=====

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

=====

Ochiq kalitli shifrlashda deshifrlash qaysi kalit asosida amalga oshiriladi?

=====

#Shaxsiy kalit

=====

ochiq kalit

=====

kalitdan foydalanilmaydi

=====

umumiy kalit

+++++

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

=====

#Kriptografiya

=====

kriptologiya

=====

kriptotahlil

=====

kriptoanaliz

+++++

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

=====

#Kriptotahlil

=====

kriptografiya

=====

kriptologiya

=====

stenografiya

+++++

Kriptotizimni boshqaradigan vosita?

=====

#Kalit

=====

algoritm

=====

ategokalit

=====

kriptotizim boshqarilmaydi

+++++

Quyidagi ta'rif qaysi kriptotizimga tegishli: ochiq matnni shifrlashda hamda rasshifrovkalashda bitta maxfiy kalitdan foydalaniladi?

=====

#Simmetrik kriptotizimlar

=====

nosimmetrik kriptotizimlar

=====

ochiq kalitli kriptotizimlar

=====

assimetrik kriptotizimlar

+++++

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

+++++

Xesh funksiyalar nima maqsadda foydalaniladi?

=====

#Ma'lumotlar yaxlitligini ta'minlashda

=====

ma'lumot egasini autentifikatsiyalashda

=====



ma'lumot maxfiyligini ta'minlashda

=====

ma'lumot manbaini autentifikatsiyalashda

+++++

Chastotalar tahlili hujumi qanday amalga oshiriladi?

=====

#Shifr matnda qatnashgan harflar sonini aniqlash orqali

=====

shifr matnda eng kam qatnashgan harflarni aniqlash orqali

=====

ochiq matnda qatnashgan harflar sonini aniqlash orqali

=====

ochiq matnda eng kam qatnashgan harflarni aniqlash orqali

+++++

Qanday algoritmlar qaytmas xususiyatiga ega hisoblanadi?

=====

#Xesh funksiyalar

=====

elektron raqamli imzo algoritmlari

=====

simmetrik kriptotizimlar

=====

ochiq kalitli kriptotizimlar

+++++

RC4 shifrlash algoritmi qaysi turga mansub?oqimli shifrlar

=====

# Oqimli shifrlar

=====

blokli shifrlar

=====

ochiq kalitli shifrlar

=====

assimetrik shifrlar

++++

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

++++

ARX amali qaysi shifrlash algoritmlarida foydalaniladi?

=====

# Blokli shifrlashda

=====

ochiq kalitli shifrlashda

=====

assimetrik shifrlashda

=====

ikki kalitli shifrlashda

++++

Kerkxofs printsipi bo'yicha qanday taxminlar ilgari suriladi?

=====

# Kalitdan boshqa barcha ma'lumotlar barchaga ma'lum

=====

faqat kalit barchaga ma'lum

=====

barcha parametrlar barchaga ma'lum

=====

shifrlash kaliti barchaga ma'lum

+++++

Qaysi algoritm har bir qadamda bir bayt qiymatni shifrlaydi?

=====

# Rc4

=====

A5/1

=====

RSA

=====

AES

+++++

Qaysi algoritmtda har bir qadamda bir bit qiymatni shifrlaydi?

=====

# a5/1

=====

RC4

=====

RSA

=====

AES

+++++

AES algoritmi qaysi tarmoq asosida qurilgan?

=====

# SP

=====

feystel

=====

petri

=====

petri va SP

+++++

Elektron raqamli imzo bo'yicha birinchi O'z DSt 1092 qaysi korxona tomonidan ishlab chiqilgan?

=====

# UNICON.UZ

=====

INFOCOM

=====

UZTELECOM

=====

O'zR axborot texnologiyalari va kommunikatsiyalarini rivojlantirish vazirligi

+++++

AES shifrlash algoritmi nomini kengaytmasini ko'rsating?

=====

# Advanced Encryption Standard

=====

advanced encoding standard

=====

advanced encryption stadium

=====

always encryption standard

+++++

A5/1 shifrlash algoritmi bu?

=====

# Oqimli shifrlash algoritmi

=====

ochiq kalitli shifrlash algoritmi

=====

assimetrik shifrlash algoritmi

=====

blokli shifrlash algoritmi

+++++

RC4 shifrlash algoritmi bu?

=====

# Oqimli shifrlash algoritmi

=====

ochiq kalitli shifrlash algoritmi

=====

asimetrik shifrlash algoritmi

=====

blokli shifrlash algoritmi

+++++

DES shifrlash algoritmi bu?

=====

# Blokli shifrlash algoritmi

=====

oqimli shifrlash algoritmi

=====

ochiq kalitli shifrlash algoritmi

=====

asimetrik shifrlash algoritmi

+++++

AES shifrlash algoritmi bu?

=====

# Blokli shifrlash algoritmi

=====

oqimli shifrlash algoritmi

=====

ochiq kalitli shifrlash algoritmi

=====

asimetrik shifrlash algoritmi

+++++

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

=====

# Kalitlar soni bilan

=====

matematik murakkabligi bilan

=====

farq qilmaydi

=====

biri maxfiylikni ta'minlasa, biri butunlikni ta'minlaydi

+++++

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

=====

# 2

=====

3

=====

4

=====

5

+++++

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

=====

# 3

=====

4

=====

5

=====

6

+++++

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

=====

# 19

=====

21

=====

23

=====

26

+++++

A5/1 oqimli shifrlash algoritmida Y registr uzunligi nechi bitga teng?

=====

# 22

=====

24

=====

25

=====

28

+++++

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

=====

# 23

=====

26

=====

32

=====

24

+++++

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

=====

# MD5

=====

ShA1

=====

CRC

=====

MAC

+++++

Qaysi xesh algoritmda xesh qiymat 160 bitga teng bo'ladi?

=====

# SHA1

=====

MD5

=====

CRC

=====

MAC

+++++

Xeshlash algoritmlarini ko'rsating?

=====

# SHA1, MD5, O'z DSt 1106

=====

rsa, dsa, el-gamal

=====



des, aes, blowfish

=====

O'z DSt 1105, ГОСТ 28147-89, FEAL

+++++

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

=====

# A5/1

=====

MD5

=====

SHA1

=====

HMAC

+++++

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

=====

# x8

=====

x9

=====

x10

=====

x11

+++++

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

=====

# y10

=====

y11

====

y12

====

y13

++++

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

====

# z10

====

z11

====

z12

====

z13

++++

Sezar shifrlash algoritmda shifrlash formulasi qanday?

====

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

====

$c = (m - k) \bmod p$

====

$c = (m * k) \bmod p$

====

$c = (m / k) \bmod p$

++++

Sezar shifrlash algoritmda rasshifrovkalash formulasi qanday?

====

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

====

$m = (c + k) \bmod p$

=====

$m = (c * k) \bmod p$

=====

$m = (c / k) \bmod p$

+++++

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

+++++

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

=====

# 1

=====

2

=====

3

=====

4

+++++

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

=====

# 1

=====

2

=====

3

=====

4

+++++

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

=====

# 1

=====

2

=====

3

=====

4

+++++

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

=====

# 1

=====

2

=====

3

=====

4

+++++

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

=====

# 4

=====

8

=====

12

=====

16

+++++

DES shifrlash algoritmidagi S-bloklarga kiruvchi qiymatlar uzunligi necha bitga teng bo'ladi?

=====

# 6

=====

12

=====

18

=====

24

+++++

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

+++++

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

++++

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

++++

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

++++

MD5 xesh funksiyasida chiquvchi qiymat uzunligi nechaga teng?

====

# 128

=====

256

=====

510

=====

160

+++++

MD5 xesh funksiyasida kiruvchi ma'lumot uzunligi qanday bitli bloklarga bo'linadi?

=====

# 512

=====

1024

=====

2048

=====

4096

+++++

Faqat AQSH davlatiga tegishli kriptografik standartlar nomini ko'rsating?

=====

# AES, DES

=====

AES, GOST 28147-89

=====

DES, O'z DST 1105-2009

=====

SHA1, GOST 3412-94

+++++

MD5 xesh funksiyasida amallar necha raund davomida bajariladi?

=====

# 64

=====

128

=====

256

=====

512

+++++

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

=====

# "UNICON.UZ" DUK

=====

"O'zstandart" agentligi

=====

Davlat Soliq Qo'mitasi

=====

Kadastr agentligi

+++++

MD5 xesh funksiyasida initsializatsiya bosqichida nechta 32 bitli registrdan foydalanadi?

=====

# 4

=====

8

=====

12

=====

16

+++++

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

=====



# 32

=====

64

=====

128

=====

256

+++++

SHA1 xesh funksiyasida chiquvchi qiymat uzunligi nechaga teng?

=====

# 160

=====

1024

=====

512

=====

256

+++++

SHA1 xesh funksiyasida kiruvchi ma'lumot uzunligi qanday bitli bloklarga bo'linadi?

=====

# 512

=====

1024

=====

2048

=====

4096

+++++

Faqat xesh funksiyalar nomi keltirilgan qatorni ko'rsating?

=====

# SHA1, MD5

=====

sha1, des

=====

md5, AES

=====

MAC, A5/1

+++++

SHA1 xesh funksiyasida amallar nechi raund davomida bajariladi?

=====

# 80

=====

128

=====

256

=====

512

+++++

Sonning teskarisini toppish amali qanday algoritm yordamida amalga oshiriladi?

=====

# Kengaytirilgan Yevklid

=====

Yevklid

=====

Ferma teoremasi

=====

Affin tizimi

+++++

DES shifrlash algoritmi bloki o'lchami qanday

=====

# 64 bit

=====

128 bit

=====

1024 bit

=====

256 bit

+++++

43 mod 21 ning javobini toping.

=====

# 1

=====

0.5

=====

3

=====

7

+++++

?  $F_{2^k+1}$ ,  $F_{2^k}$   $k=0,1,\dots$  sonlari nima deb ataladi ?

=====

# Ferma sonlari

=====

Euler sonlari

=====

el – gamal sonlari

=====

Vijner sonlari

+++++

$a^{(-1)^x} \pmod n$  yagona yechimga ega bo'lishi uchun qanday shart bajarilishi kerak

=====

# EKUB(a,n)=1;

=====

ekuk(a, n) = - 2 ;

=====

ekub (a, n) < 1.5

=====

ekub (a, n) <= 3

+++++

(12+22) mod 32 ?

=====

# 2

=====

5

=====

6

=====

8

+++++

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

+++++

17 mod 11 ning javobini toping.

=====

# 6

====

4

====

2

====

7

++++

34 sonini 2 lik sanoq tizimiga o'tkazing.

====

# 1000102

====

1001102

====

1001002

====

1100102

++++

Kriptotahlil bilan shug'ullanuvchi insonlar kimlar?

====

# Kriptoanalitiklar

====

shifrchilar

====

hakkerlar

====

dasturchilar

++++

Deshifrlashtirish so`zining ma`nosi nima?

====

# Deshifrlashtirish – shifrlashtirishga teskari jarayon. Kalit asosida shifrlangan matn o`z holatiga uzgartiriladi.

=====

deshifrlashtirish – bu matn ma`lumotlarini o`zgartirish uchun ikkilik kodi.

=====

deshifrlashtirish – bu grafik ma`lumotlarni o`zgartirish uchun sakkizlik kodi.

=====

deshifrlashtirish – bu grafik va matnli ma`lumotlarni o`zgartirish uchun sakkizlik kodi

+++++

$(2+5) \bmod 32$  ning javobini toping.

=====

# 7

=====

3

=====

8

=====

1

+++++

Shifr nima?

=====

# Shifrlash va deshifrlashda foydalaniladigan matematik funktsiyadan iborat bo`lgan krptografik algoritm

=====

kalitlarni taqsimlash usuli

=====

kalitlarni boshqarish usuli

=====

kalitlarni generatsiya qilish usuli

+++++

$256 \bmod 256$  ning javobini toping.

====

# 0

====

1

====

2

====

4

++++

A soni B soniga bo'linishi qanday ifodalanadi ?

====

#  $B \mid A$  orqali idodalanadi ;

====

$a \mid b$  orqali idodalanadi

====

$b \% a$  orqali idodalanadi

====

$b \nmid a$  orqali ifodalanadi

++++

Ikki a va b butun sonlarning umumiy bo'luvchisi deb nimaga aytiladi ?

====

# Ushbu ikki sonni bo'luvchi musbat butun soniga aytiladi.

====

ushbu ikki sonni bo'linuvchi musbat butun soniga aytiladi.

====

ushbu ikki songa ko'payuvchibutun musbat soniga aytiladi.

====

to'g'ri javob berilmagan.

++++

Umumiy bo'luvchi (d) qanday belgilaniladi ? a, b – butun sonlar

====

#  $\text{Gcd}(a,b)=d$

====

$\text{gcd}(d,b)=a$

====

$\text{gcd}(b,d)=a$

====

$\text{gcd}(a,b)=d$

++++

Sinovning natijasi yetarlicha katta ehtimollik bilan haqiqiy bo'lsa, u holda qanday test deyiladi ?

====

# Ehtimolli test

====

aniqlashti-rilgan test

====

kafolatli test

====

aniqlashti-rilmagan test

++++

Rossiya ERI standarti berilgan variantni ko'rsating.

====

# ГОСТ Р 34.10-94

====

ECDSA-2000

====

O'zDSt 1092:2009

====

E1092:2009

++++

DSA ERI loyihasi nechanchi yili muhokamaga qo'yildi ?



====

# 1991 – yili

====

1992 – yili

====

1995 – yili

====

1998 – yili

++++

Ochiq kalitli shifrlash algoritmlari bilan qanday kriptografik masalalar echiladi?

====

# Konfidensiallik va autentifikatsiya masalalarini

====

konfidensiallik va toʻlalik (butunlik)

====

faqat toʻlalik (butunlik)

====

faqat konfidensiallik

++++

Elliptik egri chiziqqa asoslangan asimmetrik 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 haqiqiy kordinatali nuqtalari ustida amal bajarish murakkabliklariga asoslangan

====

elliptik egri chiziq irratsional kordinatali nuqtalarini qoʻshish amalini bajarish murakkabliklariga asoslangan

++++

Blowfish algoritmi qanday tur kriptotizimga kiradi?

=====

# Simmetrik

=====

asimmetrik

=====

kompozitsiyali

=====

modifikatsiyalangan

++++

223 sonini tub ekanini tekshiring.

=====

# Tub son

=====

murakkab son

=====

mukammal son

=====

irratsional son

++++

RSA algoritmi qanday maqsadda ishlatiladi?

=====

# 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

++++

$(20 \cdot 10) \bmod 21$  ifodaning qiymatini toping.

=====

# 11

=====

12

=====

13

=====

17

++++

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

=====

# 32

=====

64

=====

128

=====

256

++++

AES standarti qaysi algoritmgaga asoslangan?

===

# Rijndael

=====

serpent

=====

twofish

=====

rc6

++++

Shifrlangan matnning uzunligi – ...

=====

# Berilgan matnning uzunligiga teng bo'lishi shart

=====

shifrnig uzunligiga teng bo'lishi shart

=====

shifrnig uzunligiga teng bo'lmasligi shart

=====

berilgan matnning uzunligiga teng bo'lmasligi shart

++++

Blokli shifrlash rejimlari qaysi algoritmlarda qo'llaniladi?

=====

# AES, DES

=====

Sezar, Affin

=====

A5/1, RC4

=====

MD5, SHA1

++++

Qaysi kriptotizimda shifrlash uchun ham va deshifrlash uchun ham bir xil kalitdan foydalaniladi

=====

# Simmetrik kriptotizim

=====

elektron raqamli imzo

=====

kalitlarni taqsimlash va boshqarish

=====

ochiq kalitli kriptotizim

++++

RSA algoritmi maxfiy kaliti uzunligi qanday aniqlanadi ?

=====

# Ochiq kalit va Eyler funksiyasi bilan aniqlanadi;

=====

ixtiyoriy tarzda;

=====

ochiq kalit uzunligi bilan aniqlanadi;

=====

ochiq kalit uzunligiga teng;

++++

Sezar algoritmidagi alifbo belgilarini nechtaga surish orqali shifrlangan.

=====

# 2 ta surish orqali

=====

10 ta surish orqali

=====

4 ta surish orqali

=====

5 ta surish orqali

=====

++++

Eng ko'p foydalaniladigan autentifikatsiyalash asosi-bu:

=====

# Parol

=====

biometrik parametrlar

=====

smart karta

=====

elektron raqamli imzo

++++

Elektron raqamli imzo qaysi algoritmlar asosida ishlab chiqiladi?

=====

# El-Gamal, RSA

=====

aes (advanced encryption standart)

=====

kerberos

=====

des(data encryption standart)

++++

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

=====

# A5/1

=====

DES

=====

AES

=====

RC4

=====

++++

Amerika ERI standarti berilgan variantni ko'rsating.

=====

# ECDSA-2000

=====

O'zDSt 1092:2009

=====

Rus – 2001

====

E1092:2009

++++

O'zb standartida xesh-funksiya necha bit uzunlikda bo'ladi ?

====

# 256

====

512

====

1024

====

2048

++++

803 sonini tublikka tekshiring.

====

# Tub son

====

mukammal son

====

murakkab son

====

juft son

++++

Qaysi algoritm Sonlarni tublikka tekshirishning ehtimollik algoritmlariga zid ?

====

# Alex testi

====

ferma testi

====

luxas testi

====

poklington testi

++++

Diffi – Xellman algoritmi funksiyasini ko'rsating.

====

#  $K = (a^x)^y = (a^y)^x \bmod p$

====

$k = (a^{(x+1)})^y = (a^y)^{x+1} \bmod p$

====

$k = (a^x)^{(y+1)} = (a^y)^{x+1} \bmod p$

====

$k = (a^p)^y = (a^y)^x \bmod x$

++++

Kriptografik protokol asosini nima tashkil qiladi?

====

# Kriptografik algoritm va almashtirishlar

====

kriptoanaliz usullari va vositalari

====

dasturiy vositalar

====

kriptografiya va kriptoanaliz

++++

Protokol nima?

====

# Ikki yoki undan ortiq tomonlar tomonidan aniq bir masalani yechish uchun zarur harakatlar tartibi

====

ikki yoki undan ortiq tomonlar tomonidan qandaydir bir masalani yechish uchun tuzilgan dasturiy ta'minot

====



ikki yoki undan ortiq tomonlar tomonidan aniq bir maqsadga yo'naltirilgan aloqa  
ishtirokchilar kelishuvi bayonnomasi

++++

25 mod 4 ning qiymatini toping.

=====

# 9

=====

10

=====

25

=====

21

++++

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

=====

# Bitta yechimga ega

=====

ikkita yechimga ega

=====

yechimga ega emas

=====

uchta yechimga ega

++++

$(30+45) \pmod{91}$

=====

# 75

=====

85

=====

95

=====

100

++++

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

++++

$(5+15)*2 \bmod 4$  ning qiymatini hisoblang.

=====

# 0

=====

1

=====

2

=====

3

++++

DES shifrlash standarti qaysi davlat standarti?

=====

# AQSH

=====

Rossiya

=====

Buyuk Britaniya

====

Germaniya

++++

DES algoritmda bitlar o'rinlarini almashtirilishini aniqlovchi boshlang'ich jadval o'lchami qanday?

====

# 8 x 8

====

8 x 1

====

8 x 2

====

8 x 3

++++