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
= = = =
48 bit
= = = =
56 bit
+++++
Blowfish algoritmi kaliti uzunligi qanday?
= = = =
#O'zgaruvchan
= = = =
256 bit
= = = =
128 bit
= = = =
64 bit
+++++
Blowfish algoritmi raund akslantirishlari soni qancha?
= = = =
#16 marta
= = = =
32 marta
= = = =
12 marta
= = = =
Kirish bloki uzunligiga bog'liq
+++++
Blowfishda raund kaliti uzunligi qancha?
= = = =
#32 bit
= = = =

24 bit
= = = =
16 bit
= = = =
128 bit
+++++
Blowfish algoritmi qanday tur kriptotizimga kiradi?
= = = =
#Simmetrik
= = = =
Asimmetrik
= = = =
Kompozitsiyali
= = = =
Modifikatsiyalangan
+++++
Qanday manbaa asosida raund kalitlari yaratiladi?
= = = =
#Kirish bloki uzunligiga bog'liq holda
= = = =
Dastlabki berilgan blok asosida
= = = =
Maxfiy kalit asosida
= = = =
Shifrlangan blok asosida
+++++
Berilgan algoritmning kriptobardoshliligi nimaga asoslangan?
= = = =
#Kalit uzunligiga
= = = =
Mahfiy kalitni bilishga
= = = =
Shifrlash jarayonini bajarilish vaqtiga
= = = =
Shifrlash sikllari soniga
+++++
Shifrlash qanday amallar orqali amalga oshiriladi?
= = = =
#Chekli maydonda qo'shish mod 232 va mod 2 bo'yicha
= = = =
Chekli maydonda qo'shish mod 232 bo'yicha
= = = =
Mos bitlarni qo'shish mod 2 bo'yicha
= = = =
Chekli maydonda qo'shish mod 232 va mod 2 bo'yicha, hamda bitlarni surish

+++++
Blowfishda S-bloklar soni va o'lchami qanday?
= = = =
#Har biri: 4, 256 bit
= = = =
Har biri: 8, 32 bit
= = = =
Har biri: 4, 128 bit
= = = =
Har biri: 6, 64 bit
+++++
RSA algoritmida n-ochiq kalit, d-maxfiy kalit bo'lsa, qaysi formula shifirlash jarayonini ifodalaydi?
= = = =
C=Memodn
= = = =
M=Cdmodn
= = = =
M= Ce*dmodn
= = = =
M=Ce modn
+++++
RSA algoritmida n-ochiq kalit, d-maxfiy kalit bo'lsa, ular uchun qaysi shart o'rinli?
= = = =
#e va d o'zaro tub sonlar;
= = = =
Ushbu Me va Cd ifodalar barcha M < n uchun oson hisolanadiga1n bo'lishi k1erak;
= = = =
e va d-kalitlarga bog'liq holda yana shunday p va q -sonlari mavjud bo'lib, ular o'zaro tub bo'lishi kerak;
= = = =
e va d -o'zaro tub bo'lmasligi kerak
+++++
RSA algoritmining maxfiy kalitini topish qanday masalani echish murakkabligiga asoslanadi?
= = = =
#Katta sonni tub ko'paytuvchilarga ajratish masalasining murakkabligiga;
= = = =
p va q -tub sonlarni tanlash murakkabligiga;
= = = =
Eyler funksiyasinianiqlashning murakkabligiga;
= = = =
Diskret logarifimni xisoblash murakkabligiga;
+++++
RSA algoritmi maxfiy kaliti uzunligi qancha?

= = = =
#Ochiq kalit va Eyler funksiyasi bilan aniqlanadi;
= = = =
Ixtiyoriy;
= = = =
Ochiq kalit uzunligi bilan aniqlanadi
= = = =
Ochiq kalit uzunligiga teng;
+++++
Berilgan shifrlash algoritmi kaliti qanday asosga ko'ra yaratiladi?
= = = =
#Ixtiyoriy
= = = =
Berilgan blok asosida
= = = =
Shifrlangan blok asosida
= = = =
Shifrlash sikllari soni asosid
+++++
RSA shifrlash algoritmida foydalaniladigan sonlarning spektori o'lchami qanday?
= = = =
#p va q -sonlarning ko'paytmasini ifodalovchi sonning spektoriga teng;
= = = =
65536
= = = =
65535
= = = =
65537
+++++
Berilgan algoritmning kriptobardoshligi qanday aniqlanadi?
= = = =
#Kalit uzunligi bilan
= = = =
Shifrlash jarayoni uchun ketgan vaqt bilan
= = = =
Shifrlash sikllari soni bilan
= = = =
Etarli katta butun sonni tub ko'paytuvchilarga ajratish masalasining murakkabligiga
+++++
DES, GOST 28147-89 algoritmlari i-shifrlash bloki uzunligi qancha?
= = = =
#32 bit;
= = = =
64 bit;
= = = =

24 bit;
= = = =
16 bit;
+++++
DES algoritmi kaliti uzunligi qancha?
= = = =
#64 bit;
= = = =
56 bit;
= = = =
48 bit;
= = = =
128 bit;
+++++
DES algoritmi akslantirishlari raundlari soni qancha?
= = = =
#16;
= = = =
48;
= = = =
32;
= = = =
12;
+++++
DES da E-kengaytirish funksiyasining mohiyati qanday?
= = = =
#32 bitli Ri-1 blokni 48 bitli E(Ri-1) blokka akslantiradi;
= = = =
Ri-1 -blok bitlarini takrorlashdan iborat;
= = = =
32 bitli ki -kalitni 48 bitgacha kengaytiradi;
= = = =
16 bitli ki kalitni 32 bitgacha kengaytiradi;
+++++
DES algoritmi Si - bloki vazifasi nimadan iborat?
= = = =
#48 bitli blokni 32 bitli blokka siqishdan iborat;
= = = =
56 bitli kalit blokini 48 bitli blokka siqishdan iborat;
= = = =
64 bitli kalit blokini 48 bitli blokka siqishdan iborat;
= = = =
32 bitli kalit blokini 16 bitli blokka siqishdan iborat;
+++++
DES algoritmi dastlabki o'rin almashtirish jadvalining o'lchami qanday?

= = = =
#8 x 8;
= = = =
6 x 8;
= = = =
4 x 8;
= = = =
8 x 12;
+++++
DES algoritmi shifrlash blokining chap va o'ng qism bloklarining o'lchami qancha?
= = = =
#Chap qism blok 32 bit, o'ng qism blok 32 bit;
= = = =
Chap qism blok 32 bit, o'ng qism blok 48 bit;
= = = =
Chap qism blok 64 bit, o'ng qism blok 64 bit;
= = = =
Chap qism blok 16 bit, o'ng qism blok 16 bit;
+++++
DES algoritmida raund kalitlari uzunligi qancha?
= = = =
#48 bit;
= = = =
24 bit;
= = = =
32 bit;
= = = =
16 bit;
+++++
DES algoritmida E-kengaytirish akslantirishining mohiyati qanday?
= = = =
#32 bitli kirish blokini 48 bitli raund kalitiga mod2 maydonda qo'shish uchun 32 bitli blok 48 bitga kengaytiriladi
= = = =
32 bitli kirish blokini 48 bitli raund kalitiga mod48 maydonda qo'shish uchun 32 bitli blok 48 bitga kengaytiriladi.
= = = =
32 bitli kirish blokini 48 bitli raund kalitiga mod32 maydonda qo'shish uchun 32 bitli blok 48 bitga kengaytiriladi.
= = = =
32 bitli kirish blokini 56 bitli raund kalitiga mod2 maydonda qo'shish uchun 32 bitli blok 56 bitga kengaytiriladi.
+++++
DES algoritmida Si - bloklarning vazifasi nimadan iborat?
= = = =

#48 bitli blokni 32 bitli blokka siqishdan iborat;
= = = =
56 bitli blokni 32 bitli blokka siqishdan iborat;
= = = =
64 bitli blokni 32 bitli blokka siqishdan iborat;
= = = =
32 bitli blokni 16 bitli blokka siqishdan iborat;
+++++
DES algoritmida bitlar o'rinlarini almashtirilishini aniqlovchi boshlang'ich jadval o'lchami qanday?
= = = =
#8 x 8;
= = = =
4 x 8;
= = = =
8 x 16;
= = = =
4 x 4;
+++++
DES algoritmida kalitlar generatsiyasi jadvali o'lchovi qanday?
= = = =
#8 x 8, algoritmda aniqlangan jadval bo'yicha;
= = = =
4 x 8;
= = = =
6 x 8;
= = = =
8 x 8;
+++++
DES algoritmida raund kalitlari bitlarini siljitish qanday amalga oshiriladi?
= = = =
#Raund kalitlari bitlarini siljitish berilgan jadval bo'yicha hamma raundlar uchun bir xil amalga oshiriladi.
= = = =
Siljitish 28 bitdan qilib ikkiga bo'lingan algoritmda berilgan jadval bo'yicha chapga siklik surish orqali\
amalga oshiriladi.
= = = =
Juft raundlar bo'yicha 2 bit chapga toq raundlar uchun 1 bit o'nga suriladi;
= = = =
Siljitish 16 bitdan qilib ikkiga bo'lingan algoritmda berilgan jadval bo'yicha chapga siklik surish orqali amalga oshiriladi.
+++++
DES algoritmida shifrlash natijasi qanday ifodalanadi?
= = = =

#Har biri 32 bitdan iborat bo'lgan 2 qisimdan iborat;
= = = =
Har biri 16 bitdan iborat bo'lgan 4 qisimdan iborat;
= = = =
Har biri 16 bitdan iborat bo'lgan 2 qisimdan iborat;
= = = =
Har biri 16 bitdan iborat bo'lgan 6 qisimdan iborat;
+++++
GOST 28147-89 algoritmi kaliti uzunligi qancha?
= = = =
#256 bit;
= = = =
128 bit;
= = = =
512 bit;
= = = =
64 bit;
+++++
GOST 28147-89 algoritmi raundlari soni qancha?
= = = =
#32 ta;
= = = =
24 ta;
= = = =
48 ta;
= = = =
16 ta;
+++++
RSA algoritmining maxfiy kalitini topish qanday masalani echish murakkabligiga asoslanadi?
= = = =
#Katta sonni tub ko'paytuvchilarga ajratish masalasining murakkabligiga;
= = = =
p va q -tub sonlarni tanlash murakkabligiga;
= = = =
Eyler funksiyasinianiqlashning murakkabligiga;
= = = =
Diskret logarifimni xisoblash murakkabligiga;
+++++
.....dan asosiy maqsad ma'lumotni maxfiyligini qolganlardan sir tutishdir.
= = = =
#Shifrlash
= = = =
Steganografiya
= = = =

Watermarking
= = = =
Kodlash
+++++
Simmetrik kalitli kriptotizimlar bu,
= = = =
#Bir kalitli kriptotizimlar
= = = =
Ko'p kalitli kriptotizimlar
= = = =
Assimmetrik kriptotizimlar
= = = =
Xesh funksiyalar
+++++
Ochiq kalitli kriptotizimlar bu,
= = = =
#Ikki kalitli kriptotizimlar
= = = =
Bir kalitli kriptotizimlar
= = = =
Ko'p kalitli kriptotizimlar
= = = =
Assimmetrik kriptotizimlar
+++++
Ma'lumotni ..... uning butunligini kafolatlash maqsadida amalga oshiriladi.
= = = =
#Xeshlash
= = = =
Kodlash
= = = =
Shifrlash
= = = =
Deshifrlash
+++++
..... da odatda kiruvchi ma'lumotning uzunligi o'zgaruvchan bo'lib, chiqishda o'zgarmas uzunlikdagi qiymatni qaytaradi.
= = = =
#Xesh funksiya
= = = =
Kodlash
= = = =
Shifrlash
= = = =
Stenanografiya
+++++

Odatda xesh funksiyalar kirishda ma'lumotdan tashqari hech qanday qiymatni talab etmagani bois ..... deb ham ataladi.
= = = =
#Kalitsiz kriptografik funksiyalar
= = = =
Kalitli kriptografik funksiyalar
= = = =
Elektron raqamli imzo (ERI) algoritmlari
= = = =
Gamilton algoritmlari
+++++
Qadimgi davr klassik shifrlari keltirilgan javoblarni belgilang.
= = = =
#Sezar, polibiya kvadrati
= = = =
Vijiner, atbash
= = = =
Zimmerman telegrami, enigma shifri, SIGABA mashinalari
= = = =
DES, AES, IDEA, RC4
+++++
O'rta davr klassik shifrlari keltirilgan javoblarni belgilang.
= = = =
#Vijiner, atbash
= = = =
Zimmerman telegrami, enigma shifri, SIGABA mashinalari
= = = =
DES, AES, IDEA, RC4
= = = =
Sezar, polibiya kvadrati
+++++
1 va 2-jahon urushi davri klassik shifrlari keltirilgan javoblarni belgilang.
= = = =
#Zimmerman telegrami, enigma shifri, SIGABA mashinalari
= = = =
DES, AES, IDEA, RC4
= = = =
Sezar, polibiya kvadrati
= = = =
Vijiner, atbash
+++++
Zamonaviy shifrlar keltirilgan javoblarni belgilang.
= = = =
#DES, AES, IDEA, RC4
= = = =

Sezar, polibiya kvadrati
= = = =
Vijiner, atbash
= = = =
Zimmerman telegrami, enigma shifri, SIGABA mashinalari
+++++
..... shifri nomi bilan tanilgan kriptotizim bardoshli shifrlash algoritmi hisoblanadi.
= = = =
#Bir martali bloknot yoki vernam
= = = =
Vijiner
= = = =
Atbash
= = = =
Polibiya kvadrati
+++++
Bir martali bloknot usulida ochiq matnga kalitni ..... amalida qo'shish orqali shifrmatn hosil qilinadi.
= = = =
#XOR
= = = =
OR
= = = =
NOT
= = = =
MOD
+++++
Kodlar kitobi orqali mashhur ..... shifrlangan.
= = = =
#Zimmermann telegrami
= = = =
SIGABA mashinasi
= = = =
Enigma shifri
= = = =
GOST 34791 standarti
+++++
Kodlar kitobi asosida shifrlash ..... akslantirishiga asoslangan.
= = = =
#O'rniga qo'yish
= = = =
Gammalashtirish
= = = =
Almashtirish

= = = =
Tahliliy o'zgartirish
+++++
..... hozirda amalda qo'llaniluvchi simmetrik blokli shifrlarni yaratishga asos bo'lgan.
= = = =
#Kodlar kitobi
= = = =
Bir martali bloknot
= = = =
Gammalashtirish
= = = =
Tahliliy o'zgartirish
+++++
..... o'z davrida yetarli xavfsizlikni ta'minlagan shifrlash usuli hisoblanadi.
= = = =
#Kodlar kitobi
= = = =
Bir martali bloknot
= = = =
Gammalashtirish
= = = =
Tahliliy o'zgartirish
+++++
..... kriptotizimlarda ma'lumotni shifrlashda va deshifrlashda yagona kalitdan foydalaniladi.
= = = =
#Simmetrik
= = = =
Assimmetrik
= = = =
Affin
= = = =
Xesh funksiya
+++++
#Simmetrik kriptotizimlar 2 guruhga ajratiladi:
= = = =
Simmetrik oqimli shifrlar, simmetrik blokli shifrlar
= = = =
Simmetrik oqimli shifrlar, assimmetrik blokli shifrlar
= = = =
Assimmetrik oqimli shifrlar, simmetrik blokli shifrlar
= = = =
Assimmetrik oqimli shifrlar, assimmetrik blokli shifrlar
+++++

7mod3=?
= = = =
#1
= = = =
2
= = = =
0
= = = =
3
+++++
14mod3=?
= = = =
#2
= = = =
1
= = = =
3
= = = =
0
+++++
2mod3=?
= = = =
#2
= = = =
1
= = = =
3
= = = =
0
+++++
-7mod3=?
= = = =
#2
= = = =
1
= = = =
0
= = = =
3
+++++
-2mod5=?
= = = =
#3
= = = =
0

= = = =
1
= = = =
2
+++++
RSA ochiq kalitli shifrlash algoritmi mualliflari ..... bo'lgan uchta olim sharafiga qo'yilgan.
= = = =
#Rivest, Shamir, Adleman
= = = =
Ravir, Shamir, Adelman
= = = =
Riavir, Shanel, Adleman
= = = =
Rivest, Shamer, Adelman
+++++
RSA algoritmi katta sonlarni ..... ga asoslanadi.
= = = =
#Faktorlash muammosi
= = = =
Generatsiyalash
= = = =
Tub ko'paytuvchilarga ajratish
= = = =
Qoldiq
+++++
RSA algoritmida quyidagi jarayonlar mavjud:
= = = =
#Kalitni generatsiyalash, shifrlash, deshifrlash
= = = =
Kalitni generatsiyalash, shifrlash, qoldiq
= = = =
Kalitni generatsiyalash, deshifrlash, qoldiq
= = = =
Shifrlash, deshifrlash, qoldiq
+++++
Xesh qiymat M ma'lumot uchun qanday ko'rinishda hisoblanadi?
= = = =
#h(M)
= = = =
H(M)
= = = =
(M)
= = = =
h(m)

+++++
MAC bu,
= = = =
#Message authentication code
= = = =
Message authentication computer
= = = =
Message avtorization code
= = = =
Message avtorization computer
+++++
MAC bu,
= = = =
#Xabarlarni autentifikatsiyalash kodi
= = = =
Xabarlarni avtorizatsiyalash kompyuteri
= = = =
Xabarlarni avtorizatsiyalash kodi
= = = =
Xabarlarni avtorizatsiyalash kompyuteri
+++++
Elektron raqamli imzo (ERI) bu,
= = = =
#Elektron hujjatdagi mazkur elektron hujjat axborotini elektron raqamli imzoning yopiq kalitidan foydalangan holda maxsus o'zgartirish natijasida hosil qilingan hamda elektron raqamli imzoning ochiq kaliti yordamida elektron hujjatdagi axborotda xatolik yo'qligini aniqlash va elektron raqamli imzo yopiq kalitining egasini identifikatsiya qilish imkoniyatini beradigan imzo.
= = = =
Elektron hujjatdagi mazkur elektron hujjat axborotini elektron raqamli imzoning yopiq kalitidan foydalangan holda maxsus o'zgartirish natijasida hosil qilingan hamda elektron raqamli imzo yopiq kalitining egasini identifikatsiya qilish imkoniyatini beradigan imzo.
= = = =
Elektron hujjatdagi mazkur elektron hujjat axborotini elektron raqamli imzoning yopiq kalitidan foydalangan holda maxsus o'zgartirish natijasida hosil qilingan hamda elektron raqamli imzoning ochiq kaliti yordamida elektron hujjatdagi axborotda xatolik yo'qligini aniqlash imkoniyatini beradigan imzo.
= = = =
Elektron hujjatdagi mazkur elektron hujjat axborotini elektron raqamli imzoning yopiq kalitidan foydalangan holda maxsus o'zgartirish va elektron raqamli imzo yopiq kalitining egasini identifikatsiya qilish imkoniyatini beradigan imzo.
+++++
PKI bu,
= = = =

#Public key infrastructure
= = = =
Public key international
= = = =
Public kase international
= = = =
Public kase infrastructure
+++++
PKI bu,
= = = =
#Ochiq kalitlar infratuzilmasi
= = = =
Ochiq kalitlar birligi
= = = =
Ochiq kalitlar guruhi
= = = =
Ochiq kalitlar innovatsiyasi
+++++
SA bu,
= = = =
#Certificate authorit
= = = =
Certificate authentication
= = = =
Certificate avtorization
= = = =
Certificate identification
+++++
SA bu,
= = = =
#Sertifikat markazi
= = = =
Sertifikat autentifikatsiyasi
= = = =
Sertifikat avtorizatsiyasi
= = = =
Sertifikat identifikatsiyasi
+++++
Raqamli sertifikat bu,
= = = =
#Ochiq kalit sertifikati
= = = =
Yopiq kalit sertifikati
= = = =
Sertifikatlar byurosi

= = = =
Setifikatlar markazi
+++++
Raqamli sertifikat bu,
= = = =
#Qisqacha sertifikat
= = = =
Yopiq kalit sertifikati
= = = =
Sertifikatlar byurosi
= = = =
Setifikatlar markazi
+++++
..... foydalanuvchining ismi va uning ochiq kalitidan iborat bo'ladi.
= = = =
#Raqamli sertifikat
= = = =
Yopiq kalit sertifikati
= = = =
Sertifikatlar byurosi
= = = =
Setifikatlar markazi
+++++
..... odatda tomoni odatda uchinchi tomon (trusted third party yoki TTP) sifatida qaraladi.
= = = =
#Certificate authorit (CA)
= = = =
Certificate authentication (CA)
= = = =
Certificate avtorization (CA)
= = = =
Certificate identification (CI)
+++++
Ruxsatlarni nazoratlash sohasi quyidagi qism sohalardan iborat:
= = = =
#Identifikatsiya, autentifikatsiya, avtorizatsiya
= = = =
Identifikatsiya, autentifikatsiya, ma'murlash
= = = =
Identifikatsiya, avtorizatsiya, ma'murlash
= = = =
autentifikatsiya, avtorizatsiya, ma'murlash
+++++
..... shaxsni kimdir deb davo qilish jarayoni.

= = = =
#Identifikatsiya
= = = =
Autentifikatsiya
= = = =
Avtorizatsiya
= = = =
Ma'murlash
+++++
"Men Bahodirman" identifikatorni toping.
= = = =
#Bahodir
= = = =
Men
= = = =
Men Bahodirman
= = = =
Bu yerda identifikator ko'rsatilmagan
+++++
..... subyekt identifikatorini tizimga yoki talab qilgan subyektga taqdim etish jarayoni.
= = = =
#Identifikatsiya
= = = =
Autentifikatsiya
= = = =
Avtorizatsiya
= = = =
Ma'murlash
+++++
..... foydalanuvchini (yoki biror tomonni) tizimdan foydalanish uchun ruxsati mavjudligini aniqlash jarayoni.
= = = =
#Autentifikatsiya
= = = =
Avtorizatsiya
= = = =
Ma'murlash
= = = =
Identifikatsiya
+++++
..... foydalanuvchi yoki subyektni haqiqiyligini tekshirish jarayoni.
= = = =
#Autentifikatsiya
= = = =

Avtorizatsiya
= = = =
Ma'murlash
= = = =
Identifikatsiya
+++++
..... identifikatsiya, autentifikatsiya jarayonlaridan o'tgan foydalanuvchi uchun tizimda bajarishi mumkin bo'lgan amallarga ruxsat berish jarayonidir.
= = = =
#Avtorizatsiya
= = = =
Ma'murlash
= = = =
Identifikatsiya
= = = =
Autentifikatsiya
+++++
..... binar qaror - ya'ni, ruxsat beriladi yoki yo'q.
= = = =
#Autentifikatsiya
= = = =
Ma'murlash
= = = =
Identifikatsiya
= = = =
Avtorizatsiya
+++++
..... esa tizimning turli resurslariga foydalanishni cheklash uchun foydalanuvchi qoidalar to'plami haqidagi = = = =
#barcha narsa.
= = = =
Avtorizatsiya
= = = =
Ma'murlash
= = = =
Identifikatsiya
= = = =
Autentifikatsiya
+++++
..... siz kimsiz?
= = = =
#Identifikatsiya
= = = =
Autentifikatsiya
= = = =

Avtorizatsiya
= = = =
Ma'murlash
+++++
..... siz haqiqatdan ham sizmisiz?
= = = =
#Autentifikatsiya
= = = =
Ma'murlash
= = = =
Identifikatsiya
= = = =
Avtorizatsiya
+++++
..... sizga buni bajarishga ruxsat bormi?
= = = =
#Avtorizatsiya
= = = =
Ma'murlash
= = = =
Identifikatsiya
= = = =
Autentifikatsiya
+++++
..... faqat foydalanuvchiga ma'lum va biror tizimda autentifikatsiya jarayonidan o'tishni ta'minlovchi biror = = = =
#axborot.
= = = =
Parol
= = = =
Smartkarta
= = = =
Token
= = = =
Kalit
+++++
..... kredit karta o'lchamidagi qurilma bo'lib, kichik hajmdagi xotira va hisoblash imkoniyatiga ega.
= = = =
#Smartkarta
= = = =
Token
= = = =
Kalit
= = = =

Parol
+++++
Biometrik parametrlar insonning o'zi uchun ..... kalit sifatida xizmat qiladi.
= = = =
#Kalit
= = = =
Parol
= = = =
Smartkarta
= = = =
Token
+++++
..... biometrik parametr barcha foydalanuvchilarda bo'lishi shart.
= = = =
#Universal bo'lishi
= = = =
Farqli bo'lish
= = = =
O'zgarmaslik
= = = =
To'planuvchanlik
+++++
..... tanlangan biometrik parametr barcha insonlar uchun farq qilishi shart.
= = = =
#Farqli bo'lish
= = = =
To'planuvchanlik
= = = =
Universal bo'lishi
+++++
..... tanlangan biometrik parametr vaqt o'tishi bilan o'zgarmay qolishi shart.
= = = =
#O'zgarmaslik
= = = =
To'planuvchanlik
= = = =
Universal bo'lishi
= = = =
Farqli bo'lish
+++++
..... fizik xususiyat osonlik bilan to'planuvchi bo'lishi shart. Amalda fizik xususiyatni to'planuvchanligi, insonning jarayonga e'tibor berishiga ham bog'liq bo'ladi.
= = = =
#To'planuvchanlik

= = = =
Universal bo'lishi
= = = =
Farqli bo'lish
= = = =
O'zgarmaslik
+++++
Agar tomonlardan biri ikkinchisini autentifikatsiyadan o'tkazsa, ... deb ataladi.
= = = =
#Bir tomonlama autentifikatsiya
= = = =
Ikki tomonlama autentifikatsiya
= = = =
Bir faktorli autentifikatsiya
= = = =
Ko'p faktorli autentifikatsiya
+++++
"Elektron pochtadan foydalanish davomida faqat server foydalanuvchini haqiqiyligini tekshiradi" qaysi turdagi = = = =
#autentifikatsiya.
= = = =
Bir tomonlama autentifikatsiya
= = = =
Ikki tomonlama autentifikatsiya
= = = =
Bir faktorli autentifikatsiya
= = = =
Ko'p faktorli autentifikatsiya
+++++
Agar har ikkala tomon bir-birini autentifikatsiyadan o'tkazsa, u holda ..... deb ataladi.
= = = =
#Ikki tomonlama autentifikatsiya
= = = =
Bir faktorli autentifikatsiya
= = = =
Ko'p faktorli autentifikatsiya
= = = =
Bir tomonlama autentifikatsiya
+++++
"Elektron to'lovlarni amalga oshirishda esa ham server foydalanuvchini autentifikatsiyadan o'tkazadi ham
foydalanuvchi serverni autentifikatsiyadan o'tkazadi" qaysi turdagi autentifikatsiya.
= = = =
#Ikki tomonlama autentifikatsiya

= = = =
Bir faktorli autentifikatsiya
= = = =
Ko'p faktorli autentifikatsiya
= = = =
Bir tomonlama autentifikatsiya
+++++
Pochtaga kirishda faqat parolni bilsangiz siz autentifikatsiyadan o'ta olasiz. Bu qaysi turdagi autentifikatsiya.
= = = =
#Bir faktorli autentifikatsiya
= = = =
Ko'p faktorli autentifikatsiya
= = = =
Bir tomonlama autentifikatsiya
= = = =
Ikki tomonlama autentifikatsiya
+++++
Tekshirish faqat bitta faktor bo'yicha (masalan parol) amalga oshiriladi. Bu qaysi turdagi autentifikatsiya.
= = = =
#Bir faktorli autentifikatsiya
= = = =
Ko'p faktorli autentifikatsiya
= = = =
Bir tomonlama autentifikatsiya
= = = =
Ikki tomonlama autentifikatsiya
+++++
Mazkur muammoni bartaraf etish uchun, birinchi faktorga qo'shimcha qilib, yana boshqa faktorlardan foydalanish mumkin. Bu qaysi turdagi autentifikatsiya.
= = = =
#Ko'p faktorli autentifikatsiya
= = = =
Bir tomonlama autentifikatsiya
= = = =
Ikki tomonlama autentifikatsiya
= = = =
+++++
Foydalanuvchi dastlab tizimga o'z ovozi orqali autentifikatsiyadan o'tadi va undan so'ng parol bo'yicha autentifikatsiyadan o'tkaziladi. Bu qaysi turdagi autentifikatsiya.
= = = =
#Ko'p faktorli autentifikatsiya
= = = =

Bir tomonlama autentifikatsiya
= = = =
Ikki tomonlama autentifikatsiya
= = = =
Bir faktorli autentifikatsiya
+++++
Plastik kartadan to'lovni amalga oshirishdagi autentifikatsiya.
= = = =
#Ko'p faktorli autentifikatsiya
= = = =
Bir tomonlama autentifikatsiya
= = = =
Ikki tomonlama autentifikatsiya
= = = =
Bir faktorli autentifikatsiya
+++++
Dastlab foydalanuvchida plastik kartani o'zini bor bo'lishini talab etadi va ikkinchidan uni PIN kodini bilishni talab etadi. Bu qaysi turdagi autentifikatsiya.
= = = =
#Ko'p faktorli autentifikatsiya
= = = =
Bir tomonlama autentifikatsiya
= = = =
Ikki tomonlama autentifikatsiya
= = = =
Bir faktorli autentifikatsiya
+++++
..... usuli faktorlardan bittasi qalbakilashtirilgan taqdirda ham autentifikatsiya jarayonini buzilmasligiga olib keladi.
= = = =
#Ko'p faktorli autentifikatsiya
= = = =
Bir tomonlama autentifikatsiya
= = = =
Ikki tomonlama autentifikatsiya
= = = =
Bir faktorli autentifikatsiya
+++++
..... faqat bir marta foydalanuvchi parol bo'lib, har bir sessiya uchun o'zgarib turadi.
= = = =
#One time password (OTP)
= = = =
Smartkarta
= = = =

Token
= = = =
Kalit
+++++
Turli mobayl ilovalarida to'lovlarni amalga oshirishda SMS xabar ko'rinishida ..... lar kelishi mumkin.
= = = =
#One time password (OTP)
= = = =
Smartkarta
= = = =
Token
= = = =
Kalit
+++++
..... ga asoslangan autentifikatsiya oddiy statik parolga qaraganda yuqori xavfsizlik darajasiga ega.
= = = =
#One time password (OTP)
= = = =
Smartkarta
= = = =
Token
= = = =
Kalit
+++++
..... odatda ikkinchi faktor sifatida foydalaniladi.
= = = =
#One time password (OTP)
= = = =
Smartkarta
= = = =
Token
= = = =
Kalit
+++++
Vaqtni sinxronlashga asoslangan dasturiy OTP generatori bu,
= = = =
#Google Authenticator
= = = =
Smartkarta
= = = =
Token
= = = =
Certificate authenticator

+++++
Hujumning mazkur turi tokenni yoki smart kartani o'g'irlashni maqsad qiladi. Bu,
= = = =
#Fizik o'g'irlash
= = = =
Qalbakilashtirish
= = = =
Dasturiy ko'rinishdagi tokenlarning zararli dasturlarga bardoshsizligi
= = = =
Ma'lumotlar bazasidagi biometrik parametrlarni almashtirish
+++++
Ba'zi tokenlar dasturiy ko'rinishda bo'lib, mobil qurilmalarda ishlaydi va shu sababli zararli dastur tomonidan boshqarilishi mumkin. Bu,
= = = =
#Dasturiy ko'rinishdagi tokenlarning zararli dasturlarga bardoshsizligi
= = = =
Ma'lumotlar bazasidagi biometrik parametrlarni almashtirish
= = = =
Fizik o'g'irlash
= = = =
Qalbakilashtirish
+++++
Yuzlari o'xshash bo'lgan Hasan o'rniga Husan autentifikatsiyadan o'tishi bu,
= = = =
#Qalbakilashtirish
= = = =
Dasturiy ko'rinishdagi tokenlarning zararli dasturlarga bardoshsizligi
= = = =
Ma'lumotlar bazasidagi biometrik parametrlarni almashtirish
= = = =
Fizik o'g'irlash
+++++
Sifati yuqori bo'lgan foydalanuvchi yuz tasviri mavjud rasm bilan tizimni aldashi bu,
= = = =
#Qalbakilashtirish
= = = =
Dasturiy ko'rinishdagi tokenlarning zararli dasturlarga bardoshsizligi
= = = =
Ma'lumotlar bazasidagi biometrik parametrlarni almashtirish
= = = =
Fizik o'g'irlash
+++++
Ushbu hujum bevosita foydalanuvchilarni biometrik parametrlari saqlangan bazaga qarshi amalga oshiriladi.

= = = =
#Ma'lumotlar bazasidagi biometrik parametrlarni almashtirish
= = = =
Qalbakilashtirish
= = = =
Dasturiy ko'rinishdagi tokenlarning zararli dasturlarga bardoshsizligi
= = = =
Fizik o'g'irlash
+++++
Ushbu hujumda tanlangan foydalanuvchini biometrik parametrlari hujumchini biometrik parametrlari bilan almashtiriladi.
= = = =
#Ma'lumotlar bazasidagi biometrik parametrlarni almashtirish
= = = =
Qalbakilashtirish
= = = =
Dasturiy ko'rinishdagi tokenlarning zararli dasturlarga bardoshsizligi
= = = =
Fizik o'g'irlash
+++++
Mashhur parolni buzuvchi vositalar:
= = = =
#Password Crackers, Password Portal, L0phtCrack and LC4, John the Ripper
= = = =
Password Crackers, Antivitask manager, Avast
= = = =
Doctor web, Antivitask manager, Avast
= = = =
Doctor web, eset nod, Avast
+++++
Adminlar ushbu vositalardan foydalanish orqali parollarni tekshirish zarar, bular
= = = =
#3Password Crackers, Password Portal, L0phtCrack and LC4, John the Ripper
= = = =
Password Crackers, Antivitask manager, Avast
= = = =
Doctor web, Antivitask manager, Avast
= = = =
Doctor web, eset nod, Avast
+++++
Tabiiy tahdidlarni ko'rsating:
= = = =
#Toshqinlar, yong'inlar, zilzila, harorat va namlik
= = = =

Vandalizm, qurilmaning yoqolishi, fizik qurilmalarning buzilishi, o'g'irlash, sotsial injeneriya, tizimlarni ruxsat etilmagan nazoratlash
= = = =
Vandalizm, qurilmaning yoqolishi, zilzila, harorat va namlik
= = = =
Toshqinlar, yong'inlar, fizik qurilmalarning buzilishi, o'g'irlash
+++++
Sun'iy tahdidlarni ko'rsating:
= = = =
#Vandalizm, qurilmaning yoqolishi, fizik qurilmalarning buzilishi, o'g'irlash, sotsial injeneriya, tizimlarni ruxsat etilmagan nazoratlash
= = = =
Vandalizm, qurilmaning yoqolishi, zilzila, harorat va namlik
= = = =
Toshqinlar, yong'inlar, fizik qurilmalarning buzilishi, o'g'irlash
= = = =
Toshqinlar, yong'inlar, zilzila, harorat va namlik
+++++
Fizik xavfsizlikni nazoratlash tashkilot axborot aktivlarini va binolaridan foydalanishni ..... ga yordam beradi.
= = = =
#Kuzatish, qaydlash, nazoratlash
= = = =
Ma'muriy nazorat, qaydlash, nazoratlash
= = = =
Kuzatish, qaydlash, fizik nazorat
= = = =
Kuzatish, ma'muriy nazorat, fizik nazorat
+++++
Ma'muriy nazorat bu,
= = = =
#3Qoida va muolajalarni yaratish, joylashuv arxitekturasini loyihalash, xavfsizlik belgilari va ogohlantirish signallari, ishchi joy xavfsizligini ta'minlash, shaxs xavfsizligini ta'minlash
= = = =
Fizik to'siqlarni o'rnatish, xavfsizlik qo'riqchilarini ishga olish, fizik qulflar
= = = =
Ruxsatlarni nazoratlash, "qopqon", yong'inga qarshi tizimlar, yoritish tizimlari, ogohlantirish tizimlari, quvvat manbaalari, video kuzatuv tizimlari, qurollarni aniqlash, muhitni nazoratlash
= = = =
Qoida va muolajalarni yaratish, joylashuv arxitekturasini loyihalash, xavfsizlik qo'riqchilarini ishga olish, fizik qulflar, quvvat manbaalari, video kuzatuv tizimlari, qurollarni aniqlash, muhitni nazoratlash
+++++

Fizik nazorat bu,
= = = =
#Fizik to'siqlarni o'rnatish, xavfsizlik qo'riqchilarini ishga olish, fizik qulflar
= = = =
Qoida va muolajalarni yaratish, joylashuv arxitekturasini loyihalash, xavfsizlik belgilari va ogohlantirish signallari, ishchi joy xavfsizligini ta'minlash, shaxs xavfsizligini ta'minlash
= = = =
Ruxsatlarni nazoratlash, "qopqon", yong'inga qarshi tizimlar, yoritish tizimlari, ogohlantirish tizimlari, quvvat manbaalari, video kuzatuv tizimlari, qurollarni aniqlash, muhitni nazoratlash
= = = =
Qoida va muolajalarni yaratish, joylashuv arxitekturasini loyihalash, xavfsizlik qo'riqchilarini ishga olish, fizik qulflar, quvvat manbaalari, video kuzatuv tizimlari, qurollarni aniqlash, muhitni nazoratlash
+++++
Texnik nazorat bu,
= = = =
#Ruxsatlarni nazoratlash, "qopqon", yong'inga qarshi tizimlar, yoritish tizimlari, ogohlantirish tizimlari, quvvat manbaalari, video kuzatuv tizimlari, qurollarni aniqlash, muhitni nazoratlash
= = = =
Qoida va muolajalarni yaratish, joylashuv arxitekturasini loyihalash, xavfsizlik qo'riqchilarini ishga olish, fizik qulflar, quvvat manbaalari, video kuzatuv tizimlari, qurollarni aniqlash, muhitni nazoratlash
= = = =
Qoida va muolajalarni yaratish, joylashuv arxitekturasini loyihalash, xavfsizlik belgilari va ogohlantirish signallari, ishchi joy xavfsizligini ta'minlash, shaxs xavfsizligini ta'minlash
= = = =
Fizik to'siqlarni o'rnatish, xavfsizlik qo'riqchilarini ishga olish, fizik qulflar
+++++
..... subyektni obyektga ishlash qobiliyatini aniqlash.
= = = =
#Foydalanishni boshqarish
= = = =
Subyekt
= = = =
Obyekt
= = = =
Ma'murlash
+++++
..... bu inson, dastur, jarayon va hokazo bo'lishi mumkin.
= = = =
#Subyekt

= = = =
Obyekt
= = = =
Ma'murlash
= = = =
Foydalanishni boshqarish
+++++
..... bu ma'lumot, resurs, jarayon va hokazo bo'lishi mumkin.
= = = =
#Obyekt
= = = =
Ma'murlash
= = = =
Foydalanishni boshqarish
= = = =
Subyekt
+++++
DAC (Discretionary access control) bu,
= = = =
#Diskretsion foydalanishni boshqarish usuli
= = = =
Mandatli foydalanishni boshqarish usuli
= = = =
Rolga asoslangan foydalanishni boshqarish usuli
= = = =
Atributlarga asoslangan foydalanishni boshqarish usuli
+++++
MAC (Mandatory access control) bu,
= = = =
#Mandatli foydalanishni boshqarish usuli
= = = =
Rolga asoslangan foydalanishni boshqarish usuli
= = = =
Atributlarga asoslangan foydalanishni boshqarish usuli
= = = =
Diskretsion foydalanishni boshqarish usuli
+++++
RBAC (Role-based access control) bu,
= = = =
#Rolga asoslangan foydalanishni boshqarish usuli
= = = =
Atributlarga asoslangan foydalanishni boshqarish usuli
= = = =
Diskretsion foydalanishni boshqarish usuli
= = = =

Mandatli foydalanishni boshqarish usuli
+++++
ABAC (Attribute-based access control) bu,
= = = =
#Atributlarga asoslangan foydalanishni boshqarish usuli
= = = =
Diskretsion foydalanishni boshqarish usuli
= = = =
Mandatli foydalanishni boshqarish usuli
= = = =
Rolga asoslangan foydalanishni boshqarish usuli
+++++
Foydalanishni boshqarishning mazkur usuli tizimdagi shaxsiy obyektlarni himoyalash uchun qo'llaniladi. Bu,
= = = =
#DAC usuli
= = = =
MAC usuli
= = = =
RBAC usuli
= = = =
ABAC usuli
+++++
Bu usulga ko'ra obyekt egasining o'zi undan foydalanish huquqini va kirish turini o'zi belgilaydi.
= = = =
#DAC usuli
= = = =
MAC usuli
= = = =
RBAC usuli
= = = =
ABAC usuli
+++++
..... da subyektlar tomonidan obyektlarni boshqarish subyektlarning identifikatsiya axborotiga asoslanadi.
= = = =
#DAC usuli
= = = =
MAC usuli
= = = =
RBAC usuli
= = = =
ABAC usuli
+++++

UNIX operatsion tizimida fayllarni himoyalashda, fayl egasi qolganlarga o'qish (r), yozish (w) va bajarish (x) amallaridan bir yoki bir nechtasini berishi mumkin. Bu qaysi usul?
= = = =
#DAC usuli
= = = =
MAC usuli
= = = =
RBAC usuli
= = = =
ABAC usuli
+++++
..... da obyektning egasi xavfsizlik siyosatini quradi va kimga foydalanish uchun ruxsat berilishini aniqlaydi.
= = = =
#DAC usuli
= = = =
MAC usuli
= = = =
RBAC usuli
= = = =
ABAC usuli
+++++
..... da foydalanishlar subyektlar va obyektlarni klassifikatsiyalashga asosan boshqariladi.
= = = =
#MAC usuli
= = = =
RBAC usuli
= = = =
ABAC usuli
= = = =
DAC usuli
+++++
Ushbu usulda tizimning har bir subyekti va obyekti bir nechta xavfsizlik darajasiga ega bo'ladi.
= = = =
#MAC usuli
= = = =
RBAC usuli
= = = =
ABAC usuli
= = = =
DAC usuli
+++++

Ushbu usulda obyektning xavfsizlik darajasi tashkilotda obyektning muhimlik darajasi bilan yoki yo'qolgan taqdirda keltiradigan zarar miqdori bilan xarakterlanadi.
= = = =
#MAC usuli
= = = =
RBAC usuli
= = = =
ABAC usuli
= = = =
DAC usuli
+++++
Ushbu usulda subyektning xavfsizlik darajasi unga ishonish darajasi bilan belgilanadi.
= = = =
#MAC usuli
= = = =
RBAC usuli
= = = =
ABAC usuli
= = = =
DAC usuli
+++++
..... bilan foydalanishni boshqarishda xavfsizlik markazlashgan holatda xavfsizlik siyosati ma'muri tomonidan amalga oshiriladi.
= = = =
#MAC usuli
= = = =
RBAC usuli
= = = =
ABAC usuli
= = = =
DAC usuli
+++++
..... o'rnatilgan tizimlar xavfsizlik siyosati ma'muriga tashkilot bo'ylab xavfsizlik siyosatini amalga oshirish imkoniyatini beradi.
= = = =
#3MAC usuli
= = = =
RBAC usuli
= = = =
ABAC usuli
= = = =
DAC usuli
+++++

..... da foydalanishni boshqarishning asosiy g'oyasi tizimning ishlash logikasini tashkilotda kadrlar vazifasiga yaqinlashtirish.
= = = =
#RBAC usuli
= = = =
ABAC usuli
= = = =
DAC usuli
= = = =
MAC usuli

+++++
..... da har bir obyekt uchun har bir foydalanuvchini foydalanish ruxsatini belgilash o'rniga, rol uchun obyektlardan foydalanish ruxsatini ko'rsatish yetarli.
= = = =
#RBAC usuli
= = = =
ABAC usuli
= = = =
DAC usuli
= = = =
MAC usuli
+++++
..... da foydalanuvchilar o'z navbatida o'zlarining rollarini ko'rsatishadi.
= = = =
#RBAC usuli
= = = =
ABAC usuli
= = = =
DAC usuli
= = = =
MAC usuli
+++++
..... obyektlar va subyektlarning atributlari, ular bilan mumkin bo'lgan amallar va so'rovlarga mos keladigan muhit uchun qoidalarni tahlil qilish asosida foydalanishlarni boshqaradi.
= = = =
#ABAC usuli
= = = =
DAC usuli
= = = =
MAC usuli
= = = =
RBAC usuli
+++++

Avtorizatsiyaning klassik ko'rinishi ..... ning foydalanishni boshqarish matritsasidan boshlanadi.
= = = =
#Lampson
= = = =
Rivest
= = = =
Shamir
= = = =
Adlemann
+++++
ACL (Access control list) bu,
= = = =
#Foydalanishni boshqarish ro'yxati
= = = =
Imtiyozlar ro'yxati
= = = =
Foydalanishni boshqarish matritsasi
= = = =
Sertifikat markazi
+++++
C-list (Capability list) bu,
= = = =
#Imtiyozlar ro'yxati
= = = =
Foydalanishni boshqarish matritsasi
= = = =
Sertifikat markazi
= = = =
Foydalanishni boshqarish ro'yxati
+++++
Tartibsiz yordamchi bu,
= = = =
#Ko'p jabhalarda klassik xavfsizlik muammosi hisoblanadi
= = = =
Ko'p jabhalarda klassik xavfsizlik muammosi hisoblanmaydi
= = = =
Zamonaviy xavfsizlik muammosi hisoblanmaydi
= = = =
Zamonaviy xavfsizlik muammosi hisoblanadi
+++++
..... bir-biriga osonlik bilan ma'lumot va resurslarni taqsimlash uchun ulangan kompyuterlar guruhi.
= = = =
#Kompyuter tarmoqlari

= = = =
Internet
= = = =
Protokol
= = = =
Intranet
+++++
..... ikki hisoblash tizimlari orasidagi aloqani ularning ichki tuzilmaviy va texnologik asosidan qat'iy nazar muvaffaqqiyatli o'rnatilishini asosidir.
= = = =
#Tarmoq modeli
= = = =
Internet
= = = =
Protokol
= = = =
Intranet
+++++
..... modeli tarmoq bo'ylab ma'lumotlar almashinuvini aniqlashtirish uchun taqdim etilgan model.
= = = =
#3OSI
= = = =
OTP
= = = =
TCP
= = = =
IP
+++++
Fizik sath vazifasi:
= = = =
#Qurilma, signal va binar o'zgartirishlar
= = = =
Fizik manzillash
= = = =
Yo'lni aniqlash va mantiqiy manzillash
= = = =
Nuqta-nuqta ulanish, ishonchlilik va oqimni nazoratlash
+++++
Kanal sath vazifasi:
= = = =
#Fizik manzillash
= = = =
Yo'lni aniqlash va mantiqiy manzillash
= = = =

Nuqta-nuqta ulanish, ishonchlilik va oqimni nazoratlash
= = = =
Qurilma, signal va binar o'zgartirishlar
+++++
Tarmoq sath vazifasi:
= = = =
#Yo'lni aniqlash va mantiqiy manzillash
= = = =
Nuqta-nuqta ulanish, ishonchlilik va oqimni nazoratlash
= = = =
Qurilma, signal va binar o'zgartirishlar
= = = =
Fizik manzillash
+++++
Transport sath vazifasi:
= = = =
#Nuqta-nuqta ulanish, ishonchlilik va oqimni nazoratlash
= = = =
Qurilma, signal va binar o'zgartirishlar
= = = =
Fizik manzillash
= = = =
Yo'lni aniqlash va mantiqiy manzillash
+++++
Seans sath vazifasi:
= = = =
#Host osti ulanish, ilovalar orasida ulanishlarni boshqarish
= = = =
Qurilma, signal va binar o'zgartirishlar
= = = =
Fizik manzillash
= = = =
Yo'lni aniqlash va mantiqiy manzillash
+++++
Taqdimot sath vazifasi:
= = = =
#Ma'lumotni taqdim etish, shifrlash va deshifrlash, mashinaga mos tilga o'girish va teskarisi
= = = =
Host osti ulanish, ilovalar orasida ulanishlarni boshqarish
= = = =
Qurilma, signal va binar o'zgartirishlar
= = = =
Fizik manzillash
+++++

Ilova sathi vazifasi:
= = = =
#Ilovalarni tarmoqqa ulanish jarayoni
= = = =
Ma'lumotni taqdim etish, shifrlash va deshifrlash, mashinaga mos tilga o'girish va teskarisi
= = = =
Host osti ulanish, ilovalar orasida ulanishlarni boshqarish
= = = =
Qurilma, signal va binar o'zgartirishlar
+++++
"Yuqori sath protokollarini o'zida saqlaydi, taqdim etish, kodlash va muloqotni nazoratlash", qaysi sath vazifasi?
= = = =
#Ilova sathi
= = = =
Transport sathi
= = = =
Tarmoq sathi
= = = =
Kanal sathi
+++++
"Tomonlar orasida mantiqiy ulanishni o'rnatadi va transport xizmatini ta'minlaydi", bu qaysi sath vazifasi?
= = = =
#Transport sathi
= = = =
Tarmoq sathi
= = = =
Kanal sathi
= = = =
Ilova sathi
+++++
"Manba tarmoqdan masofadagi tarmoqga ma'lumotlarni uzatish bilan tarmoqlararo paket almashinuvini amalga oshiradi", bu qaysi sath vazifasi?
= = = =
#Tarmoq sathi
= = = =
Kanal sathi
= = = =
Ilova sathi
= = = =
Transport sathi
+++++

"Bir xil tarmoqda ikkita hostlar orasida Internet sathi bo'ylab ma'lumot oqishini ta'minlaydi", bu qaysi sath vazifasi?
= = = =
#Kanal sathi
= = = =
Ilova sathi
= = = =
Transport sathi
= = = =
Tarmoq sathi
+++++
Ilova sathi protokollarini ko'rsating?
= = = =
#HTTP, Telnet, FTP, TFTP, SNMP, DNS, SMTP
= = = =
TCP, UDP, RTP
= = = =
IP, ICMP, ARP, RARP
= = = =
Ethernet, Token Ring, FDDI, X.25, Frame Relay, RS-232
+++++
Transport sathi protokollarini ko'rsating?
= = = =
#TCP, UDP, RTP
= = = =
IP, ICMP, ARP, RARP
= = = =
Ethernet, Token Ring, FDDI, X.25, Frame Relay, RS-232
= = = =
HTTP, Telnet, FTP, TFTP, SNMP, DNS, SMTP
+++++
Tarmoq sathi protokollarini ko'rsating?
= = = =
#IP, ICMP, ARP, RARP
= = = =
Ethernet, Token Ring, FDDI, X.25, Frame Relay, RS-232
= = = =
HTTP, Telnet, FTP, TFTP, SNMP, DNS, SMTP
= = = =
TCP, UDP, RTP
+++++
Kanal sathi protokollarini ko'rsating?
= = = =
#Ethernet, Token Ring, FDDI, X.25, Frame Relay, RS-232
= = = =

HTTP, Telnet, FTP, TFTP, SNMP, DNS, SMTP
= = = =
TCP, UDP, RTP
= = = =
IP, ICMP, ARP, RARP
+++++
Tahdid bu,
= = = =
#Natijasi tashkilotning amallariga va funksional harakatlariga zarar keltiruvchi va ularni uzib qo'yuvchi oshkor bo'lmagan hodisalarning potensial paydo bo'lishidir.
= = = =
Portlaganida tizim xavfsizligini buzuvchi kutilmagan va oshkor bo'lmagan hodisalarga olib keluvchi kamchilik, loyihalashdagi yoki amalga oshirishdagi xatolik.
= = = =
Zaiflik orqali AT tizimi xavfsizligini buzish tomon amalga oshirilgan harakat.
= = = =
Ishdan bo'shab ketgan xodim taqsimlangan diskdan haligacha foydalanish imkoniyatiga ega bo'lishi mumkinligi.
+++++
Zaiflik bu,
= = = =
#Portlaganida tizim xavfsizligini buzuvchi kutilmagan va oshkor bo'lmagan hodisalarga olib keluvchi kamchilik, loyihalashdagi yoki amalga oshirishdagi xatolik.
= = = =
Zaiflik orqali AT tizimi xavfsizligini buzish tomon amalga oshirilgan harakat.
= = = =
Ishdan bo'shab ketgan xodim taqsimlangan diskdan haligacha foydalanish imkoniyatiga ega bo'lishi mumkinligi.
= = = =
Natijasi tashkilotning amallariga va funksional harakatlariga zarar keltiruvchi va ularni uzib qo'yuvchi oshkor bo'lmagan hodisalarning potensial paydo bo'lishidir.
+++++
Haqiqiy shifrlanmagan ma'lumot bu,
= = = =
#ochiq matn
= = = =
shifrmatn
= = = =
deshifrlash
= = = =
kalit
+++++
Haqiqiy ma'lumotni qayta tiklash jarayoni bu,

= = = =
#deshifrlash
= = = =
ochiq matn
= = = =
Kalit
= = = =
kriptoanaliz
+++++
Kodlashtirish bu,
= = = =
#axborotni bir tizimdan boshqa tizimga ma'lum bir belgilar yordamida belgilangan tartib bo'yicha o'tkazish jarayoniga aytiladi.
= = = =
mahfiy xabar mazmunini shifrlash, ya'ni ma'lumotlarni maxsus algoritm bo'yicha o'zgartirib, shifrlangan matnni yaratish yo'li bilan axborotga ruxsat etilmagan kirishga to'siq qo'yish usuliga aytiladi.
= = = =
axborotni qayta akslantirishning matematik usullarini izlaydi va tadqiq qiladi.
= = = =
matnni shifrlash va shifrini ochish uchun kerakli axborot.
+++++
Kriptografiya bu,
= = = =
#mahfiy xabar mazmunini shifrlash, ya'ni ma'lumotlarni maxsus algoritm bo'yicha o'zgartirib, shifrlangan matnni yaratish yo'li bilan axborotga ruxsat etilmagan kirishga to'siq qo'yish usuliga aytiladi.
= = = =
axborotni bir tizimdan boshqa tizimga ma'lum bir belgilar yordamida belgilangan tartib bo'yicha o'tkazish jarayoniga aytiladi.
= = = =
kalitni bilmasdan shifrlangan matnni ochish imkoniyatlarini o'rganadi.
= = = =
esa axborotni ikkilik sanoq sistemasidagi "0" va "1" lardan iborat raqamli ko'rinishidir. Agar axborotni shifrlash va uni qayta tiklash uchun bir xil kalitdan foydalanilsa bunday shifrlash usuli simmetrik shifrlash usuli deyiladi.
+++++
Kalit bu,
= = = =
#matnni shifrlash va shifrini ochish uchun kerakli axborot.
= = = =
axborotni qayta akslantirishning matematik usullarini izlaydi va tadqiq qiladi.
= = = =
kalitni bilmasdan shifrlangan matnni ochish imkoniyatlarini o'rganadi.
= = = =

esa axborotni ikkilik sanoq sistemasidagi "0" va "1" lardan iborat raqamli ko'rinishidir. Agar axborotni
shifrlash va uni qayta tiklash uchun bir xil kalitdan foydalanilsa bunday shifrlash usuli simmetrik
shifrlash usuli deyiladi.
+++++
..... shifrlarda ma'lumotni shifrlash va deshifrlash uchun bir xil kalitdan foydalaniladi.
= = = =
#Cimmetrik
= = = =
Assimetrik
= = = =
Elektron raqamli imzo
= = = =
Vijiner
+++++
..... kriptotizimlarda shifrlash va deshifrlash uchun turlicha kalitlardan foydalaniladi.
= = = =
#Assimetrik
= = = =
Simmetrik
= = = =
Elektron raqamli imzo
= = = =
Xesh funksiya
+++++
..... bu maxfiy xabarni soxta xabar ichiga berkitish orqali aloqani yashirish hisoblanadi.
= = = =
#Stenanografiya
= = = =
Kriptografiya
= = = =
Kriptoanaliz
= = = =
Xesh funksiya
+++++
..... da esa jo'natuvchi faqat ochiq matn ko'rinishidagi xabar yuborishi mumkin, bunda u xabarni ochiq tarmoq (masalan, Internet) orqali uzatishdan oldin shifrlangan matnga o'zgartiradi.
= = = =
#Kriptografiya
= = = =

Kriptoanaliz
= = = =
Xesh funksiya
= = = =
Ctenanografiya
+++++
..... shifrlash usuli bo'yicha boshlang'ich matn belgilarining matnning ma'lum bir qismi doirasida maxsus qoidalar yordamida o'rinlari almashtiriladi.
= = = =
#O'rinlarini almashtirish
= = = =
Taxliliy o'zgartirish
= = = =
Gammalashtirish
= = = =
Almashtirish
+++++
..... shifrlash usuli bo'yicha boshlang'ich matn belgilari foydalanilayotgan yoki boshqa bir alifbo belgilariga almashtiriladi.
= = = =
#Almashtirish
= = = =
O'rinlarini almashtirish
= = = =
Taxliliy o'zgartirish
= = = =
Gammalashtirish
+++++
..... usuli bo'yicha boshlang'ich matn belgilari shifrlash gammasi belgilari, ya'ni tasodifiy belgilar ketma-ketligi bilan birlashtiriladi.
= = = =
#Gammalashtirish
= = = =
Almashtirish
= = = =
O'rinlarini almashtirish
= = = =
Taxliliy o'zgartirish
+++++
..... usuli bo'yicha boshlang'ich matn belgilari analitik formulalar yordamida o'zgartiriladi, masalan, vektorni matritsaga ko'paytirish yordamida. Bu yerda vektor matndagi belgilar ketma-ketligi bo'lsa, matritsa esa kalit sifatida xizmat qiladi.
= = = =
#Taxliliy o'zgartirish
= = = =

Gammalashtirish
= = = =
Almashtirish
= = = =
O'rinlarini almashtirish
+++++
Shifrlashning qaysi usullariga binoan dastlabki axborot simvollariga mos keluvchi raqam kodlarini ketma-ketligi gamma deb ataluvchi qandaydir simvollar ketma-ketligiga mos keluvchi kodlar ketma-ketligi bilan ketma-ket jamlanadi.
= = = =
#Additiv
= = = =
Kombinatsiyalangan
= = = =
Almashtirish
= = = =
O'rinlarini almashtirish
+++++
Ushbu standart - kriptografik algoritm, elektron ma'lumotlarni himoyalashga mo'ljallangan.
= = = =
#Ma'lumotlarni shifrlash algoritmi
= = = =
DES
= = = =
SHA
= = = =
El-gamal
+++++
Asimmetrik shifrlashning birinchi va keng tarqalgan kriptoalgoritmi .....1993 yilda standart sifatida qabul qilindi.
= = = =
#RSA
= = = =
DES
= = = =
SHA
= = = =
El-gamal
+++++
Elektron raqamli imzo tizimi ikkita asosiy muolajani amalga oshiradi:
= = = =
#raqamli imzoni shakllantirish muolajasi, raqamli imzoni tekshirish muolajasi
= = = =
raqamli imzoni tekshirish muolajasi, raqamli imzoni buzish muolajasi

= = = =
raqamli imzoni shakllantirish muolajasi, raqamli imzoni kolliziyaga tekshirish muolajasi
= = = =
raqamli imzoni kolliziyaga tekshirish muolajasi, raqamli imzoni tekshirish muolajasi
+++++
1977 yilda AQSH da yaratilgan ..... birinchi va dunyoda mashhur elektron raqamli imzo tizimi hisoblanadi.
= = = =
#RSA tizimi
= = = =
DES tizimi
= = = =
SHA tizimi
= = = =
El-gamal tizimi
+++++
Ishonchliligining yuqoriligi va shaxsiy kompyuterlarda amalga oshirilishining qulayligi bilan ajralib turuvchi raqamli imzo algoritmli 1984 yilda ..... tomonidan ishlab chiqildi.
= = = =
#El-Gamal
= = = =
Raman
= = = =
Shamil
= = = =
Adelman
+++++
Kriptologiya bu,
= = = =
#Maxfiy kodlarni yaratish va buzish fani va san'ati
= = = =
Maxfiy kodlarni yaratish bilan shug'ullanadi
= = = =
Maxfiy kodlarni buzish bilan shug'ullanadi
= = = =
Maxfiy kodlarni analitik tahlili bilan shug'ullanadi
+++++
Kriptografiya bu,
= = = =
#Maxfiy kodlarni yaratish bilan shug'ullanadi
= = = =
Maxfiy kodlarni buzish bilan shug'ullanadi

= = = =
Maxfiy kodlarni analitik tahlili bilan shug'ullanadi
= = = =
Maxfiy kodlarni yaratish va buzish fani va san'ati
+++++
Kriptotahlil bu,
= = = =
#Maxfiy kodlarni buzish bilan shug'ullanadi
= = = =
Maxfiy kodlarni analitik tahlili bilan shug'ullanadi
= = = =
Maxfiy kodlarni yaratish va buzish fani va san'ati
= = = =
Maxfiy kodlarni yaratish bilan shug'ullanadi
+++++
..... ma'lumotni osongina qaytarish uchun hammaga (hattoki hujumchiga ham) ochiq bo'lgan sxema yordamida ma'lumotlarni boshqa formatga o'zgartirishdir.
= = = =
#Kodlash
= = = =
Shifrlash
= = = =
Steganografiya
= = = =
Watermarking
+++++
..... ma'lumotlardan foydalanish qulayligini ta'minlash uchun amalga oshiriladi va hammaga ochiq bo'lgan sxemalardan foydalaniladi.
= = = =
#Kodlash
= = = =
Shifrlash
= = = =
Steganografiya
= = = =
Watermarking
+++++
..... jarayonida ham ma'lumot boshqa formatga o'zgartiriladi, biroq uni faqat maxsus shaxslar (deshifrlash kalitiga ega bo'lgan) qayta o'zgartirishi mumkin bo'ladi.
= = = =
#Shifrlash
= = = =
Steganografiya
= = = =

Watermarking
= = = =
Kodlash
+++++
.....dan asosiy maqsad ma'lumotni maxfiyligini ta'minlash bo'lib, uni qayta o'zgartirish ba'zi shaxslar (deshifrlash kalitiga ega bo'lgan) qayta o'zgartirishi mumkin bo'ladi.
= = = =
#Shifrlash
= = = =
Steganografiya
= = = =
Watermarking
= = = =
Kodlash
+++++
..... bu maxfiy xabarni soxta xabar ichiga berkitish orqali aloqani yashirish hisoblanadi.
= = = =
#Stenanografiya
= = = =
Shifrlash
= = = =
Watermarking
= = = =
Kodlash
+++++
.....ning asosiy g'oyasi bu - bu maxfiy ma'lumotlarning mavjudligi haqidagi shubhani oldini olish hisoblanadi.
= = = =
#Stenanografiya
= = = =
Shifrlash
= = = =
Watermarking
= = = =
Kodlash
+++++
Ochiq kalitlar infratuzilmasini qanday maqsadda ishlatiladi?
= = = =
#Axborotlarni maxfiyligini va butunligini ta'minlash maqsadid
= = = =
Axborotlarni saqlash va qayta ishlash maqsadida
= = = =
Axborot almashish va ishlab chiqish maqsadida

= = = =
Axborotlarni maxfiyligini ta'minlash maqsadida
+++++
Xesh-funktsiyani natijasi ...
= = = =
#fiksirlangan uzunlikdagi xabar
= = = =
Kiruvchi xabar uzunligidagi xabar
= = = =
Kiruvchi xabar uzunligidan uzun xabar
= = = =
fiksirlanmagan uzunlikdagi xabar
+++++
To'g'ri mulohazani tanlang.
= = = =
#Rijndael algoritmi Feystel tarmog'iga asoslanmagan
= = = =
Rijndael algoritmi 4 shoxli Feystel tarmog'iga asoslangan
= = = =
Rijndael algoritmi 6 shoxli Feystel tarmog'iga asoslangan
= = = =
Rijndael algoritmi 8 shoxli Feystel tarmog'iga asoslangan