# 24-Mavzu: AXBOROTLARNI HIMOYALASHNING KRIPTOGRAFIK USULLARI

**Reja:**

Axborot xavfsizligi

Axborot xavfsizligiga tahdidlarning asosiy turlari

Kriptografik axborot himoyasi tamoyillari

***Tayanch so'z va iboralar:*** *axborot xavfsizli, axborot maxfiyli, axborot butligi, «maskarad», yekyordam, kriptotahliliy xujum*

**Axborot xavfsizligi**

Kriptografik tizimlarning tasnifi

Kriptografiya fan sifatida. Asosiy tushunchalar. Ushbu mavzu bilan biz axborot xavfsizligining kriptografik usullarini o'rganishni boshlaymiz.

Kriptografiya - bu uning tarkibini yashirishga qaratilgan ma'lumotni o'zgartirish usullarini o'rganadigan fundamental fan.

"Kriptografiya" so'zi (kriptografiya) yunoncha "kryptus" so'zlaridan - maxfiy, "grafen" - yozish, ya'ni yozishni anglatadi. so'zma-so'z "kriptografiya".

Kriptoanaliz - bu kriptografik xakerlik usullarini o'rganadigan fan.

Kriptologiya - bu shifrlar va ularning chidamliligini o'rganadigan fan.

Kriptologiya \u003d Kriptografiya + Kriptanaliz

Kriptografiya tarixi bir necha ming yilliklarga borib taqaladi. Birinchi shifrlash tizimlari miloddan avvalgi to'rtinchi ming yillikda yozish bilan bir vaqtda paydo bo'lgan.

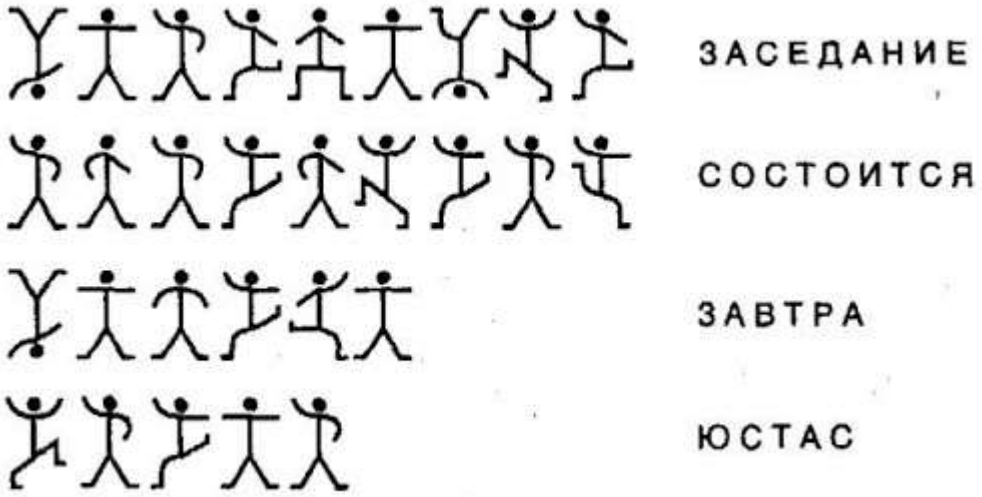
Devid Kohn "Taniqli shifrli xakerlar" kriptovalyutaga bag'ishlangan epik kitobida miloddan avvalgi 1900 yilda Misrda kriptografiyani va miloddan avvalgi 500 yilda Injilni yozgan. Qadimgi Yunoniston va qadimgi Rimda kriptografiya allaqachon faoliyatning turli sohalarida, ayniqsa jamoat sohalarida keng qo'llanilgan edi. (Yuliy Tsezar, Galliy urushi haqidagi yozuvlar, miloddan avvalgi 1-asr.) O'rta asrlarning qorong'i yillarida shifrlash amaliyoti qat'iy ishonch bilan saqlangan. Salib yurishlari yillarida Papa bilan birga xizmat qilgan kriptograflar bir yillik ishdan so'ng jismoniy halokatga duchor bo'lishdi.

Qadimgi davrlardan 1949 yilgacha kriptologiyaning rivojlanish davri odatda ilmiygacha bo'lgan kriptologiya davri deb nomlanadi, chunki o'sha davrlarning yutuqlari sezgi asosida va dalillar bilan qo'llab-quvvatlanmagan. O'shanda kriptologiya deyarli fan sifatida emas, balki san'at sifatida ham qo'llanilgan.


Ikkinchi Jahon urushi kriptografiya tarixida burilish nuqtasi bo'lgan: agar urushdan oldin kriptografiya ancha tor maydon bo'lgan bo'lsa, urushdan keyin u keng faoliyat sohasiga aylandi.

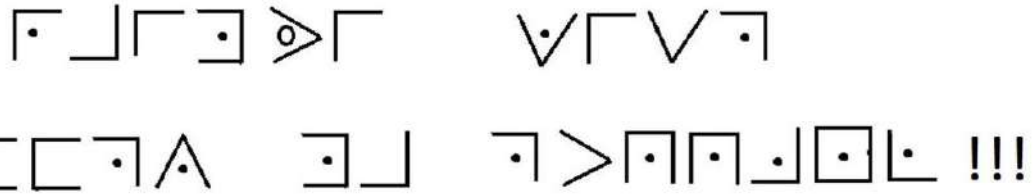
1949 yilda Klod Shannonning "Maxfiy tizimlardagi aloqa nazariyasi" maqolasi maxfiy maxfiy kalitlar bilan ilmiy kriptologiyaning yangi davrining boshlanishini belgiladi. Ushbu ajoyib ishda Shannon kriptografiyani axborot nazariyasi bilan bog'ladi.

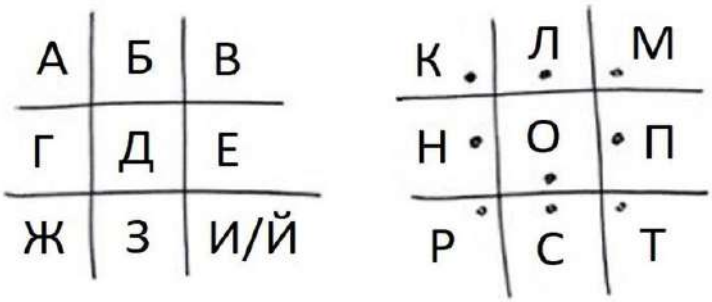
So'nggi 25-30 yil ichida kriptografiyani rivojlantirish sohasida faollik oshdi, ochiq ilmiy tadqiqotlar jadal o'sdi. Shu vaqtgacha kriptografiya faqat harbiy va razvedka maqsadlarida ishlatilgan.

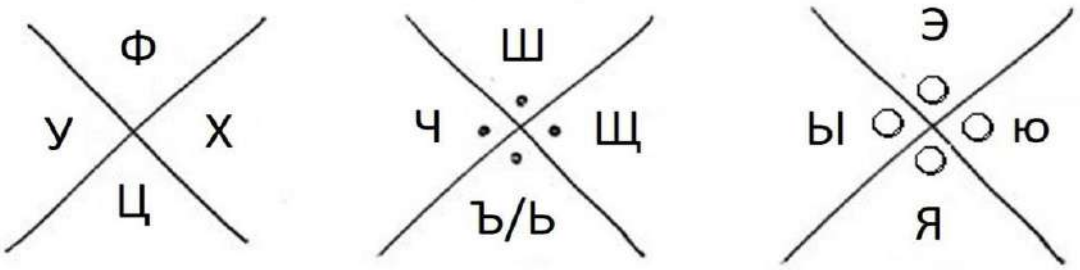



70-yillarda kriptografiyaning keyingi rivojlanishiga jiddiy ta'sir ko'rsatadigan ikkita voqea yuz berdi. Birinchidan, ma'lumotlarni shifrlash bo'yicha birinchi

standart (DES) qabul qilindi (va e'lon qilindi!). Ikkinchidan, amerikalik matematiklar U.Diffi va M.Xellmanning ishidan so'ng "yangi kriptografiya" paydo bo'ldi - ochiq kalitli kriptografiya. Ushbu ikkala voqea tez rivojlanayotgan aloqa vositalarining, shu jumladan himoya qilish uchun oson va ishonchli ishonchli kriptografik vositalarning zarur bo'lgan mahalliy va global kompyuter tarmoqlarining ehtiyojlaridan kelib chiqqan. Kriptografiya nafaqat harbiy, diplomatik, davlat sohalarida, balki tijorat, bank va boshqa sohalarda ham keng talabga aylandi.




Steganografiya - bu xabarning mavjudligini yashirish uchun mo'ljallangan usullar to'plami.

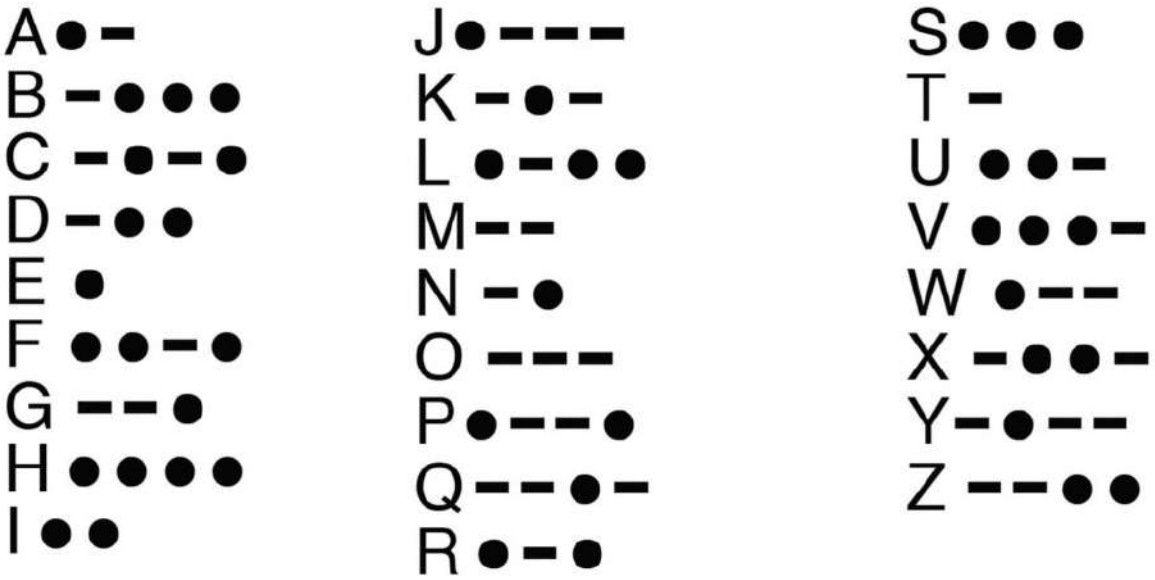
Masalan:

1. Yashirin xabarni etkazishi uchun oddiy matnda so'zlar yoki harflarni tartibga solish.
2. Belgilarni belgilash.
3. Ko'rinmas siyoh.
4. Ponksiyon qog'ozi.
5. Tuzatish lentasi yordamida chiziqlar orasida bosib chiqarish.

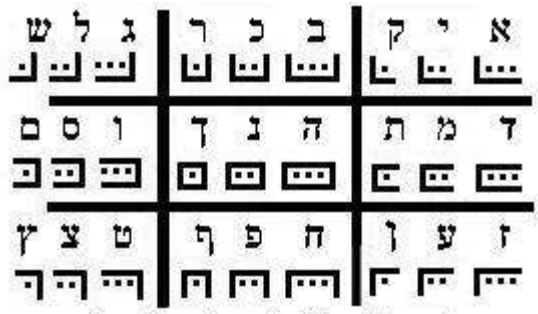
Bunday usullarning o'zi arxaik ko'rinishga ega, ammo ularning zamonaviy ekvivalentlari mavjud. Masalan, CD-ning video ramkalaridagi ahamiyatsiz bitlardan foydalangan holda xabarlarni yashirish.

Hozirgi vaqtda bunday operatsiyalarni amalga oshirishga imkon beradigan ko'plab dasturiy paketlar ishlab chiqilgan. Steganografiyaning afzalligi shundaki, u nafaqat ularning mazmunini, balki xabarlarni uzatish haqiqatini ham yashira

oladi. Darhaqiqat, shifrlashning o'zi shubhali - bu yashirish kerak bo'lgan narsa borligini anglatadi.




Bugungi kunda shifrlashning 2 turi keng tarqalgan:
An'anaviy
Ochiq kalitlarni shifrlash.



Еврейский шифр "Аик-Бекар".

**An'anaviy shifrlash jarayoni ikkita tarkibiy qismni o'z ichiga oladi:**

1. Shifrlash algoritmi.
2. Kalit oddiy matndan mustaqil bo'lgan qiymatdir.

Algoritmni bajarishda erishilgan natija ishlatiladigan kalitga bog'liq. Kalitni o'zgartirish shifr matnini o'zgartiradi.

An'anaviy shifrlashning kuchi bir qancha omillarni aniqlaydi:

1. Shifrlash algoritmining murakkabligi (shunchaki murakkab bo'lishi kerak, shunda faqat shifrlangan matn bo'lsa, xabarni shifrlash mumkin emas).
2. Kalit xavfsizligi an'anaviy shifrlash ishonchliligining asosiy omili. Algoritmning o'zi yashirin bo'lishi mumkin.

An'anaviy (klassik) kriptografiyada XIX asrda shakllangan asosiy qoida - Kirkxof qoidalari qabul qilinadi:

Shifrning mustahkamligi faqat kalitning xavfsizligi bilan belgilanishi kerak.

An'anaviy shifrlashning bu xususiyati uning keng tarqalganligini va tan olinishini belgilaydi. Chunki algoritmni sir saqlashning hojati yo'q, ishlab chiqaruvchilar ko'plab zamonaviy tizimlar bilan jihozlangan arzon, ommabop chiplar ko'rinishida shifrlash algoritmlarini amalga oshirishlari mumkin.

An'anaviy kriptotizim modelini batafsilroq ko'rib chiqing.

Simmetrik kriptosistemaning an'anaviy modelining nazariy asoslari birinchi marta 1949 yilda Klod Shannon tomonidan taqdim etilgan.

Manba aniq matnli xabarni yaratadi:

X oddiy elementning xi elementlari n harflaridan iborat ba'zi cheklangan A alifbosidagi belgilardir:

An'anaga ko'ra, ingliz tilidagi 26 harfdan iborat alifbo ishlatilgan, ammo bugungi kunda (0,1) ikkilik alifbosi ko'proq ishlatiladi.

Shifrlash uchun kalit quyidagi shaklda yaratiladi:

K \u003d [k1, k2, ..., kj]

Agar kalit xabarning o'zi bilan bir joyda yaratilgan bo'lsa, uni yashirin kanallar orqali qabul qiluvchiga yuborish kerak. Yoki kalit uchinchi tomon tomonidan yaratilgan bo'lib, u kalitni xabarni yuboruvchiga va qabul qiluvchiga ishonchli etkazib berishi kerak.

Shifrlash algoritmidan foydalanib, X va K ga ega bo'lgan holda, shifrlangan matn hosil bo'ladi

Y \u003d [y1, y2, ..., yn]

Buni formula sifatida yozish mumkin:

Y kodlash algoritmini E tekis matn X ga K tugmachasi yordamida erishiladi.

Teskari aylantirish:

2. Kriptotizim turlari

shifrlash kriptografiyasi algoritmi

Kriptografik tizimlarning tasnifi quyidagi uchta xususiyatga asoslanadi:

Ishlatilgan tugmalar soni.

Oddiy matnni shifrlangan holatga o'tkazish operatsiyalari turi.

Oddiy matnni qayta ishlash usuli.

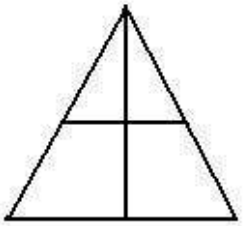
Simmetrik kriptosistemalar;

Asimmetrik kriptosistemalar.

Agar jo'natuvchi va oluvchi bir xil kalitdan foydalansa, shifrlash tizimi nosimmetrik, bitta kalitli tizim, maxfiy kalit bilan tizim, an'anaviy shifrlash sxemasi deb ataladi. (Masalan, DES, CAST, RC5, IDEA, Blowfish, klassik shifrlar);

Agar jo'natuvchi va qabul qilgich turli xil kalitlardan foydalansa, tizim asimmetrik, ikkita kalitli tizim, ochiq kalitlarni shifrlash sxemasi deb ataladi. (RSA, El Gamal).

Масонская латиница и схема ее построения

Алфавит розенкрейцеров AMORC и схема построения

**2) Oddiy matnni shifrlangan joyga o'zgartirish operatsiyalari turlari bo'yicha.**

Shifokor shifrlari - Shifrlash oddiy matnning har bir elementini (bitlar, harflar, bitlar yoki harflar guruhlari) boshqa element bilan almashtirishga asoslangan. (Tsezar, Playfayer, Xill);

Permutatsiya shifrlari - shifrlash aniq matn elementlarining ketma-ketligini o'zgartirishga asoslangan. (Ladder, ustunlarni qayta tartiblash);

Ishlab chiqarish shifrlari - shifrlash bir necha almashtirish va almashtirish operatsiyalarining kombinatsiyasiga asoslangan. Ishlab chiqarish shifrlari ko'pgina zamonaviy zamonaviy shifrlash tizimlarida qo'llaniladi. (DES).

**3) oddiy matnni qayta ishlash usuliga ko'ra.**

Blokli shifrlar - Shifrlash deyiladi, unda mantiqiy shifrlash birligi oddiy matnning bloki bo'lib, o'zgartirilgandan so'ng bir xil uzunlikdagi shifr teksti olinadi. Masalan: DES, Feistel shifri.

· Oqimli shifr - bu oddiy matnning barcha elementlarini ketma-ket, ketma-ket (bit bilan, bayt-bayt bilan) shifrlash demakdir. Klassik oqim shifrlariga Vizhener shifrlari (avtomatik kalit tanlash bilan) va Vernam kiradi.

Blok shifrlari ancha yaxshi o'rganilgan. Ularning in-linega qaraganda ancha kengroq ekanligi ishoniladi. An'anaviy shifrlash sxemasidan foydalanadigan ko'p tarmoq dasturlari blok shifrlardan foydalanadi.

**3.** Kripto hujumlari turlari va algoritmlarning mustahkamligi

(X) va / yoki kalitni (K) qayta qurish jarayoni kriptovalyutiya deb ataladi.

Agar kalitni real vaqtda topishga imkon beradigan protsedura topilsa, shifrlash algoritmi ochilgan deb hisoblanadi.

Oshkor qilish algoritmining murakkabligi kriptosistemaning muhim xususiyatlaridan biridir va kriptografik barqarorlik deb ataladi.

Eng qadimgi va sodda ma'lum bo'lgan yovvoyi karifat shifri Yuliy Tsezarning shifri. Tsezar kodida alifboning har bir harfi bir alfavitda 3 pozitsiyada joylashgan harf bilan almashtiriladi.

Umumiy holda, siljish har qanday bo'lishi mumkin (1 dan 25 gacha). Agar har bir harfga raqamli ekvivalent berilgan bo'lsa, u holda:

Y \u003d Ek (X) \u003d (x + k) mod26

Biz Qaysarning umumiy algoritmini olamiz.

13 harfni o'ngga siljitish bilan Qaysarning shifri rot13 bilan belgilanadi.

Bunday shifrni parametrlarni oddiy ketma-ket ro'yxatga olish orqali aniqlash mumkin. Oddiy raqamlashni ishlatish quyidagilar bilan asoslanadi:

shifrlash va shifrlash algoritmlari ma'lum;

faqat 25 variant;

oddiy matnning tili.

Aksariyat hollarda tarmoqlarni himoya qilishda 1) emas, balki 2) amalga oshiriladi. Muhim belgi 3). Agar dastlabki matn oldindan siqilgan bo'lsa, unda bu tanib olishni ancha qiyinlashtiradi.

Kriptovalyutada shifrni ochishning yana bir imkoniyati mavjud (ro'yxatlash variantlaridan tashqari). Agar kriptovalyutada oddiy matnning mohiyati to'g'risida tushuncha bo'lsa, siz tegishli tilda matnlarga xos bo'lgan xarakteristik xususiyatlar to'g'risidagi ma'lumotlardan foydalanishingiz mumkin (statistik usullar). Masalan, alifbo harflarining paydo bo'lishi chastotalarini tahlil qilish.

Mono-alifbo shifrlarini ochish oson, chunki ular asl alifbo harflaridan foydalanish chastotasini meros qilib oladilar. Matnni shifrlangan matnni almashtirish usullari yordamida kamroq ko'rinadigan qilish uchun siz quyidagilardan foydalanishingiz mumkin.

ko'p harfli shifrlash, ya'ni. oddiy matnning individual belgilarini emas, balki bir nechta belgilar kombinatsiyasini almashtirish;

bir nechta alifbolar.

Ko'p harfli shifrlash usuliga asoslangan eng taniqli shifrlardan biri bu Playfair shifri. Unda oddiy matnning katta harflari (ikki harfning kombinatsiyasi) alohida birliklar sifatida ko'rib chiqilib, ular shifr matnning berilgan bigramlariga aylantiriladi. Bigramlarning chastotasini tahlil qilish yanada murakkabroq. Uzoq vaqt davomida Playfayer kodini buzib bo'lmaydi, deb ishonishgan. U Birinchi Jahon urushi paytida Britaniya Armiyasidagi shifrlash standarti bo'lib xizmat qildi va hatto AQShda Ikkinchi Jahon urushi paytida ham ishlatilgan.

Ko'p harfli shifrga misol sifatida Hill shifri ham kiradi (1929). Bu algoritmga asoslanib, har bir ketma-ketlikdagi oddiy matnni harflari m-ni shifr matniga almashtiradi.

Oddiy monoalfabetik shifrni takomillashtirishning imkoniyatlaridan biri ma'lum sharoitlarga qarab bir nechta monoalfabetik almashtirishlardan foydalanishdir. Bunday shifrlash usullaridan foydalanishga asoslangan shifrlar oilasiga polialfabetik shifrlar deyiladi. Ular quyidagi xususiyatlarga ega:

monoalfabetik bog'liqliklar to'plamidan foydalanadi;

ushbu bosqichda shifrlash uchun qaysi konversiyalash qo'llanilishi kerak bo'lgan kalit mavjud.

Polyalfabetik yovvoyi belgilar shifrlari XV asrda ixtiro qilingan. Leon Battista Alberti. Ular XIX asrga qadar mashhur bo'lgan, ular xakerlik qila boshlaganlarida.

Ushbu turdagi eng mashhur va sodda algoritm Vigenere shifri (in-line).

Kriptovalyutaning statistik usullaridan (ya'ni harflarning paydo bo'lish chastotasi bo'yicha) eng yaxshi himoya bu oddiy matnning uzunligiga teng,

ammo statistik nuqtai nazardan sodda matndan farq qiladigan kalit so'zni tanlashdir. Bunday tizim 1918 yilda AT&T muhandisi Gilbert Vernem tomonidan taklif qilingan. Vernam algoritmida shifrlangan matn oddiy matn va kalit uchun XOR operatsiyasini ozgina bajarib yaratiladi.

Buzilib bo'lmaydigan mukammal shifr bo'lishi mumkinmi? Ishoning yoki ishonmang, mutlaq shifrlash usuli mavjud.

Jozef Moborn Vernamning sxemasini mutlaqo ishonchli qiladigan yaxshilanishni ixtiro qildi. U tasodifiy ravishda xabar uzunligiga teng kalitni yaratishni taklif qildi. Har bir kalit belgisi faqat bir marta va bitta xabarda ishlatiladi. Chiqish bu aniq matn bilan statistik aloqasi bo'lmagan tasodifiy ketma-ketlikdir. Sxema bir martalik lenta yoki bir martali ishlatiladigan daftar deb ataladi. Bu xakerlik uchun qarz bermaydi, chunki shifr matnida hech qanday oddiy matn yo'q. Biroq, bir martalik tugmachani ishlatish juda qiyin, chunki jo'natuvchi va qabul qiluvchida bitta tasodifiy kalit bo'lishi kerak, uni amalda bajarish qiyin.

Ideal shifr tushunchasini Shannon o'z asarlarida kiritgan. U o'z oldiga statistik usullarga asoslangan kriptovalyutani urinishlarining oldini olish vazifasini qo'ydi. Ideal shifr - bu oddiy matnning barcha statistik qonunlarini shifr matnida yashiradigan shifr.

Agar shifrlangan matnda oddiy matnni bir xil qayta tiklash uchun etarli ma'lumotlar bo'lmasa, shifrlash sxemasi mutlaqo xavfsiz (so'zsiz himoyalangan) deb nomlanadi.

Bu shuni anglatadiki, dushman matnni ochish uchun qancha vaqt sarflashidan qat'i nazar, u shifr matnida oddiy matnni tiklash uchun zarur ma'lumotga ega bo'lmagani uchun uni shifrlay olmaydi.

Shifrlash algoritmi bera oladigan maksimal qiymat kamida quyidagi shartlardan birini bajarishdir:

1) shifrni buzish qiymati shifrlangan ma'lumotlarning narxidan oshib ketadi;

2) Shifrni yorish uchun zarur bo'lgan vaqt, ma'lumot tegishli bo'lgan vaqtdan oshib ketadi.

**Agar shifrlash sxemasi ushbu ikkita shartga javob bersa, u hisoblash xavfsiz deb nomlanadi.**

An'anaviy shifrlash sxemalari uchun kriptovalyutaning barcha shakllari shifrlangan matnda ko'rinadigan oddiy matnning tuzilishidagi ba'zi xarakterli xususiyatlarni saqlab qolish asosida ishlab chiqilgan.

Ochiq kalitlar sxemalari uchun kriptanaliz mutlaqo boshqacha - kalit juftlarini bog'laydigan matematik bog'liqliklar mantiqiy asoslar yordamida, kalitlardan birini bilib, ikkinchisini topishga imkon berishiga asoslanadi.

Kripto hujumlarining asosiy turlari:

Shifr matniga hujum.


2.3-rasm - Foydalanish vositalari.