**O’ZBEKISTON RESPUBLIKASI AXBOROT TEXNOLOGIYALARI**

**VA KOMMUNIKATSIYALARINI RIVOJLANTIRISH VAZIRLIGI**

**MUHAMMAD AL-XORAZMIY NOMIDAGI**

**TOSHKENT AXBOROT TEXNOLOGIYALARI UNIVERSITETI**

**Shifrlash algoritmlarini dasturiy va apparat amalga oshirishning samarali usullari**

mavzusidagi

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| **MAGISTRLIK ISHI** | | | | | |
|  | Magistr |  | \_\_\_\_\_\_\_\_\_  imzo |  | Ahmadov U.S.  F.I.SH. |
|  |  |  |  |  |  |
|  | Rahbar |  | \_\_\_\_\_\_\_\_\_\_ imzo |  | Axmedova O.P.  F.I.SH. |
|  |  |  |  |  |  |

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **MUNDARIJA** | | | | |
| **Kirish……………………………………………………………….…….** | | |
| **1.** | **Ma’lumotlarni шифрлаш алгоритмларининг бардошлилигига оид талаблар ……....................** | |
| 1.1. | | Axborotlarni шифрлаш алгоритмлари таснифи ............................................. |
| 1.2. | | Simmetrik shifrlash algoritmlari қиёсий таҳлили |
| 1.3. | | Assimmetrik shifrlash algoritmlariнинг математик асослари…..……………………………….  1-боб бўйича хулосалар |

**2. Kriptografik apparat va dasturiy vositalar taдқиқи…………………………**

2.1. Kriptografik модулларга оид хавфсизлик талаблари ....……………………………………

2.2. Kriptografik dasturiy vositalarнинг қиёсий tahlili………………………………………

2.3. Kriptografik apparat vositalarнинг tahlili …………………………………………………………

3.

**Kirish**

Hozirgi kunda axborot texnologiyalari jadal tarzda rivojlanib borayotgan bir vaqtda, axborot almashinuvi xam juda katta tezlik bilan rivojlanib bormoqda.

Elektron ko‘rinishdagi ma’lumotlarni hajmini ortishi, uni saqlash bilan bog‘liq bo‘lgan muammolar hajmini ham ortishiga olib keladi. Ushbu muammolarni hal qilishda mavjud bo‘lgan usullar esa, kundan-kunga yangilanaveradi. Shunga qarmasdan axborot xavfsizligini ta'minlashda qadimda ham foydalanilagan va hozirda ham foydalanilayotgan usullardan biri bu - kriptografik himoya usullaridir. Kriptografik himoya usullari o‘zining ishonchlililigi, samaradorligi va foydalanish darajasi qamrovi kengligi bilan boshqa usullardan farq qiladi. Hozirda axborot xavfsizligini ta’minlashning har bir jabhasida kriptografik usullardan foydalanilmoqda. Bu esa uning muhimligidan darak beradi.

Kriptografiya - axborotlarni aslidan o‘zgartirilgan holatga akslantirish uslublarini topish va takomillashtirish bilan shug‘ullanadi. Dastlabki sistemalashgan kriptografik uslublar eramiz boshida, Yuliy Sezarning ish yuritish yozishmalarida uchraydi. U, biror ma’lumotni maxfiy holda, biror kishiga yetkazmoqchi bo‘lsa, alfavitning birinchi harfini alfavitning to‘rtinchi harfi bilan, ikkinchisini beshinchisi bilan va hokazo shu tartibda almashtirib matnning asli holatidan shifrlangan matn holatiga o‘tkazgan.

Axborotlarning muhofazasi masalalari bilan kriptologiya (kryptos- maxfiy, logos- ilm) fani shug‘ullanadi. Kriptologiya maqsadlari o‘zaro qarama-qarshi bo‘lgan ikki yo‘nalishga ega: - kriptografiya va kriptoanaliz.

Kriptografiyaning ochiq ma’lumotlarni shifrlash masalalarini matematik uslublari bilan shug‘ullanishi to‘g‘risida yuqorida aytib o‘tildi.

Kriptoanaliz esa shifrlash uslubini (kalitini yoki algoritmini) bilmagan holda shifrlangan ma’lumotni asli holatini (mos keluvchi ochiq ma'lumotni) topish masalalarini yechish bilan shug‘ullanadi.

Hozirgi zamon kriptografiyasi quyidagi to‘rtta bo‘limni o‘z ichiga oladi:

1) Simmetrik kriptotizimlar.

2) Ochiq kalit algoritmiga asoslangan kriptotizimlar.

3) Elektron raqamli imzo kriptotizimlari.

4) Kriptotizimlar uchun kriptobardoshli kalitlarni ishlab chiqish va ulardan foydalanishni boshqarish.

Kriptografik uslublardan foydalanishning asosiy yo‘nalishlari: maxfiy ma’lumotlarni ochiq aloqa kanali bo‘yicha muhofaza qilgan holda uzatish, ularning haqiqiyligini ta’minlash, axborotlarni (elektron hujjatlarni, elektron ma’lumotlar jamg‘armasini) kompyuterlar tizimi xotirasida shifrlangan holda saqlash va shu kabi masalalarning yechimlarini o‘z ichiga oladi.

**1.1 Axborotlarni kriptografik himoyalash**

Axborotning himoyalashning aksariyat mexanizmlari asosini shifrlash tashkil etadi. Axborotni shifrlash deganda ochiq axborotni (dastlabki matnni) shifrlangan axborotga o’zgartirish (shifrlash) va aksincha (rasshifrovka qilish) jarayoni tushuniladi.

Axborotni qayta akslantirish yordamida himoyalash muammosi inson ongini uzoq vaqtlardan buyon bezovta qilib kelgan. Kriptografiya tarixi – inson tili tarixi bilan tengdosh. Hatto dastlabki xat yozish ham o’z-o’zicha kriptografik tizim hisoblangan, chunki qadimgi jamiyatda faqat alohida shaxslargina xat yozishni bilganlar. Qadimgi Yegipet va Qadimgi Hindistonning ilohiy kitoblari bunga misol bo’la oladi.

Xat yozishning keng tarqalishi natijasida kriptografiya alohida fan sifatida vujudga keldi. Dastlabki kriptotizimlardan eramizning boshlaridayoq foydalanilgan. Sezar o’z xatlarida tizimli shifrlardan foydalangan.

Kriptografik tizimlar birinchi va ikkinchi jahon urushlarida jadal rivojlandi. Urush yillaridan so’ng va hozirga qadar hisoblash vositalarining jadal rivojlanishi kriptografik usullar yaratishni tezlashtirdi va ularning mukammalligini oshirdi.

Bir tomondan, kompyuter tarmoqlaridan foydalanish kengaydi, jumladan, Internet global tarmog’i. Bu tarmoqda begona shaxslardan himoyalanishi zarur bo’lgan hukumat, harbiy, tijorat va shaxsiy xarakterga ega bo’lgan axborotning katta hajmi harakatlanadi.

Boshqa tomondan, qudratli kompyuterlar, tarmoqli va neyronli hisoblash texnologiyalarining paydo bo’lishi ochish mumkin emas deb hisoblangan kriptografik tizimlarning obro’siga putur yetkazdi.

Kriptologiya – axborotni qayta akslantirib himoyalash muammosi bilan shug’ullanadi (kryptos – maxfiy, sirli, logos - fan). Kriptologiya ikki yo’nalishga bo’linadi – kriptografiya va kriptoanaliz. Bu ikki yo’nalishning maqsadlari qarama-qarshi.

Kriptografiya – axborotni qayta akslantirishning matematik usullarini izlaydi va tadqiq qiladi.

Kriptoanaliz – kalitni bilmasdan shifrlangan matnni ochish imkoniyatlarini o’rganadi.

Bu kitobda asosiy e’tibor kriptografik usullarga qaratilgan.

Zamonaviy kriptografiya quyidagi to’rtta bo’limlarni o’z ichiga oladi:

1. Simmetrik kriptotizimlar.
2. Ochiq kalitli kriptotizimlar.
3. Elektron imzo tizimlari.
4. Kalitlarni boshqarish.

Kriptografik usullardan foydalanishning asosiy yo’nalishi – maxfiy axborotning aloqa kanalidan uzatish (masalan, elektron pochta), uzatiladigan xabarning uzunligini o’rnatish, axborotni (hujjatlarni, ma’lumotlar bazasini) shifrlangan holda raqamli vositalarda saqlash.

SHunday qilib, kriptografiya axborotni shunday qayta ishlash imkonini beradiki, bunda uni qayta tiklash faqat kalitni bilgandagina mumkin.

Shifrlash va deshifrlashda qatnashadigan axborot sifatida biror alifbo asosida yozilgan matnlar qaraladi. Bu terminlar ostida quyidagilar tushuniladi.

Alifbo – axborot belgilarini kodlash uchun foydalaniladigan chekli to’plam.

Matn – alifbo elementlarining tartiblangan to’plami.

Zamonaviy ATlarida qo’llaniladigan alifbolarga misol sifatida quyidagilarni keltirish mumkin:

1. Z33 alifbosi – rus alifbosining 32 harflari va bo’sh joy belgisi;
2. Z256 alifbosi – ASCII va KOI-8 standart kodlariga kiruvchi belgilar;
3. Binar alifbo - Z2={0, 1}
4. Sakkizlik yoki o’n oltilik alifbolar.

SHifrlash – akslantirish jarayoni: ochiq matn deb ham nomlanadigan matn shifrmatnga almashtiriladi.

Kriptografik tizim

Deshifrlash – shifrlashga teskari jarayon. Kalit asosida shifrmatn ochiq matnga akslantiriladi.

Kalit – matnni shifrlash va shifrini ochish uchun kerakli axborot.

Kriptografik tizim – ochiq matnni akslantirishning T oilasini o’zida mujassamlashtiradi. Bu oila a’zolari k bilan indekslanadi yoki belgilanadi. k parametr kalit hisoblanadi. K kalitlar fazosi – bu kalitning mumkin bo’lgan qiymatlari to’plami. Odatda kalit alifbo harflari ketma-ketligidan iborat bo’ladi.

Kriptotizimlar simmetrik va ochiq kalitli tizimlarga bo’linadi.

Simmetrik kriptotizimlarda shifrlash va shifrni ochish uchun bitta va aynan shu kalitdan foydalaniladi.

Ochiq kalitli kriptotizimlarda bir-biriga matematik usullar bilan bog’langan ochiq va yopiq kalitlardan foydalaniladi. Axborot ochiq kalit yordamida shifrlanadi, ochiq kalit barchaga oshkor qilingan bo’ladi, shifrni ochish esa faqat yopiq kalit yordamida amalga oshiriladi, yopiq kalit faqat qabul qiluvchigagina ma’lum.

Kalitlarni tarqatish va kalitlarni boshqarish terminlari axborotni akslantirish tizimlari jarayoniga tegishli. Bu iboralarning mohiyati foydalanuvchilar o’rasida kalit yaratish va tarqatishdir.

Elektron raqamli imzo deb – xabar muallifi va tarkibini aniqlash maqsadida shifrmatnga qo’shilgan qo’shimchaga aytiladi (elektron xujjatdagi mazkur elektron xujjat axborotini elektron raqamli imzoning yopiq kalitidan foydalangan xolda maxsus o’zgartirish natijasida xosil qilingan hamda elektron raqamli imzoning ochiq kaliti yordamida elektron xujjatdagi axborotda xatolik yo’qligini aniqlash va elektron raqamli imzo yopiq kalitining egasini identifikatsiya qilish imkoniyatini beradigan imzo).

Kriptobardoshlilik deb kalitlarni bilmasdan shifrni ochishga bardoshlilikni aniqlovchi shifrlash tavsifiga aytiladi.

Kriptobardoshlilikning bir necha ko’rsatkichlari bo’lib, ular:

1. barcha mumkin bo’lgan kalitlar soni;
2. kriptoanaliz uchun zarur bo’lgan o’rtacha vaqt.

Kriptografik akslantirish unga mos keluvchi algoritm va k kalit qiymati bilan aniqlanadi. Axborotni himoyalash maqsadida samarali shifrlash kalitni yashirin saqlashga va shifrning kriptobardoshliligiga bog’liq.

Deyarli tub son – tub bo’lish ehtimoli 1 ga yaqin.

Belgi – axborotni fiksirlangan uzunlikdagi ko’rinishi

SHA – Secure Hash Algorithm ma’lumotni xeshlash algoritmi

vaqtinchalik shtempel - vaqtni belgilab qo’yish mexanizmi

Diffi - Xellman algoritmi – ikki abonent o’rtasida o’zaro kalit almashinish algoritmi

Autentifikatsiya – shaxsini haqqoniyligini tasdiqlash.

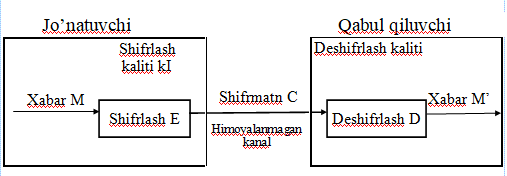
1.1.1 Kriptotizimlarga qo’yilgan talablar

Ma’lumotlarni kriptografik akslantirish jarayoni dasturiy va apparatli amalga oshirilishi mumkin. Apparatli ta’minot qimmat, ammo u sermahsullik, oddiylik, himoyalanganlik kabi afzalliklarga ega. Dasturiy ta’minot foydalanishga qulayligi uchun ko’proq amaliy hisoblanadi.

Amalga oshirish usullariga bog’liq bo’lmagan holda axborotni himoyalashning zamonaviy kriptografik tizimlariga quyidagi umumiy talablar qo’yiladi:

1. shifrlash algoritmini bilish shifrmatn kriptobardoshliligini tushirib yubormasligi lozim. Barcha kriptotizimlar bu talabga javob berishi kerak;
2. shifrlangan xabarning biror qismi va unga mos ochiq matn asosida kalitni aniqlash uchun zarur bo’lgan amallar soni mumkin bo’lgan umumiy kalitlarga sarflanadigan amallar sonidan kam bo’lmasligi kerak;
3. shifrlangan matndan ochiq matnni hosil qilish uchun mumkin bo’lgan kalitlar to’plamini to’la ko’rib chiqish amallari soni qat’iy past ko’rsatkichga ega bo’lishi va zamonaviy kompyuterlar imkoniyatlari chegarasidan chiqib ketishi kerak;
4. shifrlash algoritmini bilish himoyaga ta’sir qilmasligi kerak;
5. kalitdagi yoki boshlang’ich ochiq matndagi kichik o’zgarishlar shifrlangan matnni tubdan o’zgartirib yuborishi kerak;
6. shifrlash algoritmining tarkibiy elementlari o’zgarmas bo’lishi lozim;
7. shifrlash jarayonida qo’shilgan qo’shimcha bitlar shifrmatnda bir butunligini saqlashi va yetarlicha yashirilgan bo’lishi talab etiladi;
8. shifrmatn uzunligi ochiq matn uzunligiga teng bo’lishi kerak;
9. shifrlash jarayonida ketma-ket qo’llaniladigan kalitlar o’rtasida o’zaro oddiy va oson bog’liqlik bo’lmasligi kerak;
10. mumkin bo’lgan kalitlar to’plamidagi ixtiyoriy kalit, shifrmatnning kriptobardoshliligini ta’minlashi kerak;
11. algoritm ham dasturiy, ham apparatli realizatsiyaga qulay, va kalit uzunligining o’zgarishi, shifrlash algoritmining sifatini pasaytirmasligi kerak.

Shifrlash kriptotizimining umumlashtirilgan sxemasi



1-rasm.

Uzatiluvchi axborot matni M kriptografik o’zgartirish Yek1 yordamida shifrlanadi, natijada shifrmatn C olinadi:



**1.2 Simmetrik shifrlash algoritmlari**

Simmetrik shifrlash algoritmlarida ma’lumotni shifrlash uchun ham,parolni hal qilish uchun bir xil kalitdan foydalanishni o'z ichiga oladi. Simmetrik algoritmlarga ikkita asosiy talab qo'llaniladi: shifrlash ob'ektidagi barcha statistik qonuniyatlarning to'liq yo'qolishi va chiziqlilikning yetishmasligi. Simmetrik tizimlarni blok va oqim tizimlariga bo'lish odatiy holdir.

Blok tizimlarida dastlabki ma'lumotlar bloklarga bo'linadi, so'ngra kalit yordamida transformatsiya qilinadi.

Oqim tizimlarida ma'lum bir ketma-ketlik (chiquvchi gamma) hosil bo'ladi, keyinchalik u xabarning ustiga joylashtiriladi va ma'lumotlar gamma hosil bo'lganda oqim tomonidan shifrlanadi. Simmetrik kriptosistemadan foydalangan holda aloqa sxemasi rasmda ko'rsatilgan.

Bu yerda M - ochiq matn, K - yopiq kanal orqali uzatiladigan maxfiy kalit, En (M) - shifrlash, Dk (M) - parolni hal qilish

Odatda, simmetrik shifrlashda dastlabki ma'lumotlarning almashtirishlari va almashtirishlarining murakkab va ko'p bosqichli kombinatsiyasi qo'llaniladi va bu yerda ko'plab qadamlar (o'tish) bo'lishi mumkin va ularning har biri "o'tish tugmachasi" ga mos kelishi kerak.

O'rnini bosish operatsiyasi simmetrik shifr uchun birinchi talabni bajaradi, ma'lum bir qonunga binoan xabar bitlarini aralashtirish orqali har qanday statistik ma'lumotlardan xalos bo'ladi. Almashtirish ikkinchi talabni bajarish uchun zarur - algoritmga nochiziqlik berish. Bunga ma'lum hajmdagi xabarning ma'lum bir qismini asl qiymatga murojaat qilish orqali standart qiymatga almashtirish orqali erishiladi.

Simmetrik tizimlar assimetriklardan afzalliklari va kamchiliklariga ega. Simmetrik shifrlarning afzalliklariga yuqori shifrlash tezligi, bir xil kuchga ega bo'lgan kichikroq talab qilinadigan kalit uzunligi, katta bilim va amalga oshirish qulayligi kiradi. Simmetrik algoritmlarning kamchiliklari, avvalambor, kalit almashinuvi paytida kalit sirining buzilishi ehtimoli katta bo'lganligi va katta tarmoqdagi kalitlarni boshqarish murakkabligi sababli kalitlarni almashtirishning murakkabligi deb hisoblanadi.

**1.2.1Simmetrik shifrlash algoritmlariga misollar:**

* GOST 28147-89 - ichki shifrlash standarti
* 3DES (Triple-DES, triple DES)
* RC6 (Rivesta kodi)
* Ikki baliq
* SEED - Koreys shifrlash standarti
* Camellia - Yapon shifrlash standarti
* CAST (Carlisle Adams va Stafford Tavares dasturchilarining bosh harflaridan)
* XTEA - bu amalga oshirishning eng oson algoritmi
* AES - Amerika shifrlash standarti
* DES - bu AESgacha bo'lgan AQSh ma'lumotlarini shifrlash standarti

Mavjud barcha kriptografik usullar quyidagi sinflarga ajratiladi:

*Simmetrik*

*kriptotizimlar*

*Gammalash*

*Podstanovkalar*

*Blokli shifrlar*

*Perestanovkalar*

1-sxema.

Mono- va ko’p alifboli o’rniga qo’yishlar (**podstanovkalar**).

Bir xil alifbodan foydalangan holda ochiq matnni boshqa matnga murakkab yoki qiyin qoida bo’yicha almashtirish o’rniga qo’yish hisoblanadi. Yuqori kriptobardoshlilikni ta’minlash uchun katta kalitlardan foydalanishga to’g’ri keladi.

O’rin almashtirishlar (**perestanovkalar**)

Bu ham uncha murakkab bo’lmagan kriptografik akslantirish hisoblanadi, odatda boshqa usullar bilan birgalikda foydalaniladi.

Gamma qo’shish (**Gammalash**)

Bu usulda kalit asosida generatsiya qilinadigan psevdotasodifiy sonlar ketma-ketligi ochiq matn ustiga qo’yiladi.

Blokli shifrlar shifrlanadigan matn blokiga qo’llaniladigan asosiy akslantirish usullarini (mumkin bo’lgan takrorlashlar va navbatlar bilan) tasvirlaydi. Blokli shifrlar yuqori kriptobardoshlilikka ega ekanligidan amalda u yoki bu sinf akslantirishidan ko’proq uchraydi. Amerika va Rossiyaning shifrlash standartlari aynan shu sinf shifrlariga asoslangan.

**1.2.2 DES shifrlash algoritmi**

Ma'lumotlarni shifrlash algoritmi DES (Data Encryption Standard) 1977 yilda nashr etilgan va hanuzgacha tijorat ma'lumotlarini himoya qilish tizimlarida ishlatiladigan keng tarqalgan simmetrik algoritm hisoblanadi.

DES algoritmi Feistel tarmoq metodologiyasiga muvofiq tuzilgan va o'zgaruvchan ketma-ketlik va almashtirishlar ketma-ketligidan iborat. DES algoritmi 64 bitli kalit yordamida 64 bitli ma'lumotlar bloklarini shifrlaydi, unda 56 bit muhim ahamiyatga ega (qolgan 8 ta paritiya uchun chek bitlar).

Shifrlash jarayoni 64 bitli blok bitlarining boshlang'ich almashtirishidan, shifrlashning 16 siklidan (turidan) va nihoyat, bitlarning so'nggi almashinuvidan iborat.

DES parolini hal qilish shifrlashga teskari bo'lib, teskari tartibda shifrlash amallarini takrorlash orqali amalga oshiriladi.

DES algoritmining asosiy afzalliklari:

* faqat 56 bit uzunlikdagi bitta kalit ishlatiladi;
* algoritmning nisbatan soddaligi yuqori ishlov berish tezligini ta'minlaydi;
* Xabarni bitta dasturiy ta'minot to'plami bilan shifrlashdan so'ng, parolni hal qilish uchun DES algoritmiga mos keladigan har qanday boshqa dasturiy ta'minot to'plamidan foydalanishingiz mumkin;
* algoritmning kriptografik kuchi aksariyat tijorat dasturlarining axborot xavfsizligini ta'minlash uchun etarli.

Zamonaviy mikroprotsessor texnologiyasi simmetrik blokli shifrlarni asosiy oqimi 40 bit bo'lgan yoriqlarni juda oqilona vaqt ichida yorib o'tishga imkon beradi. Bunday xakerlik uchun qo'pol kuch ishlatish usuli qo'llaniladi - barcha mumkin bo'lgan asosiy qiymatlarni to'liq sinovdan o'tkazish ("qo'pol kuch" usuli). Yaqin vaqtgacha DES nisbatan xavfsiz shifrlash algoritmi hisoblangan.

Blok algoritmlarini yangi, yanada mustahkam algoritmlarni ishlab chiqarish uchun birlashtirishning ko'plab usullari mavjud. Bunday usullardan biri bir nechta shifrlash - blokirovka algoritmidan bir necha marta turli xil tugmalar yordamida bir xil matnli blokni shifrlash. 3x shifrlash bilan siz uch xil tugmachadan foydalanishingiz mumkin.

3-DES (Triple DES) algoritmi DES algoritmining ishonchliligi yetarli emas deb hisoblangan holatlarda qo'llaniladi.

Bugungi kunda ikkita zamonaviy kriptografik kuchli shifrlash algoritmlari tobora ko'proq qo'llanilmoqda: ichki shifrlash standarti GOST 28147-89 va AQShning yangi kripto standarti - AES (Advanced Encryption Standard).

**1.2.3 GOST 28147-89 shifrlash standarti**

Shifrlash standarti GOST 28147-89 apparat va dasturiy ta'minotni amalga oshirish uchun mo'ljallangan, kriptografik talablarga javob beradi va himoyalangan ma'lumotlarning maxfiyligi darajasiga cheklovlar qo'ymaydi. GOST 28147-89 tomonidan aniqlangan ma'lumotlarni shifrlash algoritmi 256-bitli 64-bitli blok algoritmidir.

Shifrlanadigan ma'lumotlar 64 bitli bloklarga bo'linadi. Ushbu bloklar ikkita kichik bloklarga bo'lingan Nx va N2 Har biri 32 bit. Subblock / V ma'lum bir tarzda qayta ishlanadi, undan so'ng uning qiymati pastki blok qiymatiga qo'shiladi N2 (qo'shimcha 2-modul bilan amalga oshiriladi, ya'ni XOR mantiqiy operatsiyasi qo'llaniladi - "eksklyuziv yoki"), keyin subbloklar almashtiriladi. Ushbu transformatsiya algoritmning ishlash rejimiga qarab ma'lum bir necha marta ("dumaloqlar") - 16 yoki 32 marta amalga oshiriladi.Har bir turda ikkita operatsiya o'tkaziladi.Birinchi operatsiya tugmachani qoplashdir. Subblock / V tarkibiga 2 32 moduli qo'shilib, kalitning 32 bitli qismi qo'shiladi K x.To'liq shifrlash kaliti 32-bitli pastki tugmachalarning birikmasi sifatida ifodalanadi: K0, K1, K2, K3, K4, K5, K6, K7. Shifrlash jarayonida dumaloq raqamga va algoritmning ishlash rejimiga qarab ushbu pastki kalitlardan biri ishlatiladi.

Ikkinchi operatsiya - stolni almashtirish. Kalitni ustiga qo'ygandan so'ng, pastki birlik N ( 4 bitli 8 qismga bo'linadi, ularning har birining qiymati pastki blokning ushbu qismi uchun almashtirish jadvaliga muvofiq almashtiriladi. Keyin kichik blok 11 bitga chapga siljiydi.

Jadvalni almashtirish. 5-quti (Almashinish qutisi) ko'pincha zamonaviy shifrlash algoritmlarida qo'llaniladi, shuning uchun bunday operatsiya qanday tashkil etilganligini tushuntirishga arziydi.

5-qutini almashtirish bloki sakkizta almashtirish tugunidan iborat (5 ta almashtirish bloklari). O'rnini bosish blokiga kelish S 32 bitli vektor ketma-ket 4 bitli vektorlarga bo'linadi, ularning har biri mos keladigan tugun tomonidan 4 bitli vektorga aylantiriladi. Har bir almashtirish tuguni 0000 ... 1111 oralig'idagi 16 ta 4-bitli ikkilik raqamlarni almashtirish jadvali sifatida ifodalanishi mumkin. Kirish vektori jadvaldagi satrning manzilini bildiradi va bu qatordagi raqam chiqish vektori hisoblanadi. Keyin 4-bitli chiqish vektorlari ketma-ket 32-bitli vektorga birlashtiriladi. O'zgartirish tugunlari (almashtirish jadvallari) - bu kompyuter tarmog'i uchun umumiy bo'lgan va kamdan-kam o'zgarib turadigan asosiy elementlar. Ushbu almashtirish tugunlari sir saqlanishi kerak.

GOST 28147-89 tomonidan belgilangan algoritm to'rtta ish rejimini ta'minlaydi: oddiy almashtirish, geribildirim bilan gamma, gamma va simulyatorlar avlodi. Ular yuqorida tavsiflangan bir xil shifrlash transformatsiyasidan foydalanadilar, ammo rejimlarning maqsadi turlicha bo'lganligi sababli, bu konvertatsiya ularning har birida turli yo'llar bilan amalga oshiriladi.

GOST 28147-89 algoritmi juda mustahkam algoritmdir - hozirda uni oshkor qilish uchun yuqorida aytib o'tilgan "qo'pol kuch" usulidan samarali usullar taklif qilinmagan. Uning yuqori xavfsizligiga birinchi navbatda kalitning katta uzunligi - 256 bit tufayli erishiladi. Yashirin sinxronlash xabaridan foydalanganda samarali kalit uzunligi 320 bitgacha oshiriladi va almashtirish jadvalining maxfiyligi qo'shimcha bitlarni qo'shadi. Bundan tashqari, kriptografik kuch transformatsiyalar turlarining soniga bog'liq bo'lib, ulardan GOST 28147-89 bo'yicha 32 bo'lishi kerak (kirish ma'lumotlarining dispersiyasining to'liq samarasi 8 turdan so'ng erishiladi).

**1.2.4 AES shifrlash standarti**

1997 yilda Amerika Standartlar va Texnologiyalar Instituti (NIST) AES (Advanced Encryption Standard) nomli yangi simmetrik kriptoalgoritm standarti uchun tanlov e'lon qildi. Uning rivojlanishida dunyodagi eng yirik kriptologiya markazlari qatnashgan. Ushbu tanlov g'olibi aslida keyingi 10-20 yil davomida global kripto standartiga aylandi.

Kriptoalgoritmlarga - yangi AES standartiga nomzodlarga quyidagi talablar qo'yildi:

* algoritm nosimmetrik bo'lishi kerak;
* algoritm blok shifr bo'lishi kerak;
* algoritm blok uzunligi 128 bit bo'lishi va uchta asosiy uzunlikni qo'llab-quvvatlashi kerak: 128, 192 va 256 bit.

Bundan tashqari, kriptoalgoritmlarni ishlab chiquvchilarga quyidagilar tavsiya qilingan:

* ham apparatda (mikrochiplarda), ham dasturiy ta'minotda (shaxsiy kompyuterlar va serverlarda) osongina amalga oshiriladigan operatsiyalardan foydalaning;
* maqsadli 32-bitli protsessorlar;
* barcha manfaatdor shaxslar algoritmning mustaqil kriptanalizini mustaqil ravishda amalga oshirishlari va unda hech qanday hujjatsiz imkoniyatlar mavjudligiga ishonch hosil qilishlari uchun keraksiz ravishda shifr tuzilishini murakkablashtirmang.

Tanlov natijalari 2000 yil oktyabr oyida e'lon qilindi - Belgiyadan ikki kriptograf - Vinsent Raymen va Joan Daemen tomonidan ishlab chiqilgan Rijndael algoritmi g'olib bo'ldi. Rijndael algoritmi yangi AES ma'lumotlarni shifrlash standartiga aylandi.

AES algoritmi ma'lum bo'lgan simmetrik shifrlash algoritmlarining ko'pchiligiga o'xshamaydi, ularning tuzilishi "Feistel tarmog'i" deb nomlanadi va Rossiyaning GOST 28147-89 ga o'xshashdir. Mahalliy shifrlash standartidan farqli o'laroq, AES algoritmi qayta ishlangan ma'lumotlarning har bir blokini o'rnatilgan blok uzunligiga qarab 4x4, 4x6 yoki 4x8 o'lchamdagi ikki o'lchovli bayt massivi ko'rinishida aks ettiradi (shifrlangan axborot blokining bir necha belgilangan o'lchamlaridan foydalanishga ruxsat beriladi). Bundan tashqari, tegishli bosqichlarda transformatsiyalar mustaqil ustunlar yoki mustaqil satrlar yoki umuman alohida baytlar bo'yicha amalga oshiriladi.

AES algoritmi ma'lum turlardan iborat (10 dan 14 gacha - bu blok kattaligi va kalit uzunligiga bog'liq) va to'rtta transformatsiyani amalga oshiradi:

BS (ByteSub) - massivning har bir baytini jadvalga almashtirish ;

SR (ShiftRow) - qator qatorlarini siljitish. Ushbu operatsiyani bajarish paytida birinchi satr o'zgarishsiz qoladi, qolganlari esa massivning kattaligiga qarab belgilangan baytlar soniga chapga siljiydi. Masalan, 4x4 qator uchun 2, 3 va 4 qatorlar mos ravishda 1, 2 va 3 baytga siljiydi;

MS (MixColumn) - massivning mustaqil ustunlaridagi operatsiya, har bir ustun ma'lum bir qoidaga muvofiq (x) bilan belgilangan matritsaga ko'paytirilganda;

AK (AddRoundKey) - kalitni qo'shish. Massivning har bir bitiga dumaloq tugmachaning mos keladigan biti bilan 2-modul qo'shiladi, bu esa o'z navbatida shifrlash klavishasidan ma'lum usulda hisoblanadi.

AES algoritmi boshqa algoritmlarga nisbatan bir qator afzalliklari tufayli ma'lumotlarni shifrlashning yangi standartiga aylandi. Avvalo, u barcha platformalarda yuqori tezlikda shifrlashni ta'minlaydi: dasturiy ta'minotda ham, apparatni amalga oshirishda ham. Bundan tashqari, uning ishlashi uchun resurs talablari minimaldir, bu uni hisoblash qobiliyatlari cheklangan qurilmalarda qo'llashda muhimdir.

AES algoritmining yagona kamchiligi uning noan'anaviy sxemasidir. Gap shundaki, "Feistel tarmog'iga" asoslangan algoritmlarning xususiyatlari yaxshi o'rganilgan va AES, aksincha, yashirin zaifliklarni o'z ichiga olishi mumkin, ularni faqat keng tarqalishi boshlanganidan bir muncha vaqt o'tgach topish mumkin.

Ma'lumotlarni shifrlash uchun boshqa simmetrik blok kriptoalgoritmlari ham qo'llaniladi. Ko'pgina blok simmetrik kriptalgoritmlar to'g'ridan-to'g'ri 64-bitli oddiy matnli kirishni 64-bitli shifrlangan matnga o'zgartiradi, ammo ma'lumotlar kamdan-kam hollarda 64 bit bilan cheklanadi.

Turli xil kriptografik masalalarni yechishda blok simmetrik algoritmidan foydalanish uchun to'rtta ish rejimi ishlab chiqilgan:

1. elektron kod kitobi EU B (Elektron kod kitobi);
2. Shifrlarni blokirovkalash;
3. shifrlangan matn haqida mulohazalar (shifrni qaytarib berish);
4. OFB chiqishi haqida mulohazalar (Chiqish uchun orqaga qaytarish).

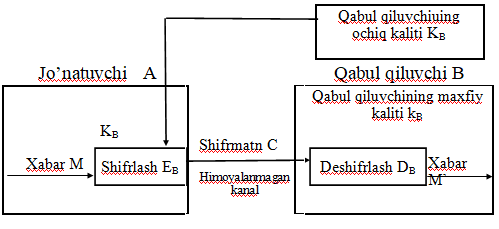
Ushbu ish rejimlari dastlab DES blok algoritmi uchun ishlab chiqilgan, ammo boshqa kripto blok algoritmlari ushbu rejimlarning har qandayida ishlashi mumkin.

**1.3 Assimmetrik shifrlash algoritmlari**

Asimmetrik kriptotizimlarda axborotni shifrlashda va rasshifrovka qilishda turli kalitlardan foydalaniladi:

* ochiq kalit K axborotni shifrlashda ishlatiladi, maxfiy kalit k dan hisoblab chiqariladi;
* maxfiy kalit k , uning jufti bo’lgan ochiq kalit yordamida shifrlangan axborotni rasshifrovka qilishda ishlatiladi.

Maxfiy va ochiq kalitlar juft-juft generatsiyalanadi. Maxfiy kalit egasida qolishi va uni ruxsatsiz foydalanishdan ishonchli ximoyalash zarur (simmetrik algoritmdagi shifrlash kalitiga o’xshab). Ochiq kalitning nusxalari maxfiy kalit egasi axborot almashinadigan kriptografik tarmoq abonentlarining har birida bo’lishi shart.



2-rasm.

Asimmetrik kriptotizimda shifrlangan axborotni uzatish quyidagicha amalga oshiriladi:

1. Tayyorgarlik bosqichi:

- abonent V juft kalitni generatsiyalaydi: maxfiy kalit kV va ochiq kalit KV;

- ochiq kalit KV abonent A ga va qolgan abonentlarga jo’natiladi.

2. A va V abonentlar o’rtasida axborot almashish:

- abonent A abonent Vning ochiq kaliti KV yordamida axborotni shifrlaydi va shifrmatnni abonent Vga jo’natadi;

- abonent V o’zining maxfiy kaliti kV yordamida axborotni rasshifrovka qiladi. Hech kim (shu jumladan abonent A ham) ushbu axborotni rasshifrovka qilaolmaydi, chunki abonent Vning mahfiy kaliti unda yo’q.

Asimmetrik kriptotizimda axborotni ximoyalash axborot qabul qiluvchi kaliti kV ning mahfiyligiga asoslangan.

Asimmetrik kriptotizimlarning asosiy hususiyatlari quyidagilar:

1. Ochiq kalitni va shifr matnni himoyalangan kanal orqali jo’natish mumkin, ya’ni niyati buzuq odamga ular ma’lum bo’lishi mumkin.

2. SHifrlash YeV : M ► C va rasshifrovka qilish DB: S ► M algoritmlari ochiq.

**1.3.1 Bir tomonlama funksiyalar.**

Bu funksiyalarning bir tomonlama deyilishi sabab shuki, bu funksiyalar bir tomonlama ishlatilgan holda matnni maxfiy holatga olib kelinib, ikkinchi tomondan uni ommaviy holatga olib kelishning iloji yuq. Bu ta'rifni yanada aniqroq qilib aytadigan bo'lsak bizga shunday *x* ga tegishli *X* argumentlar to'plami mavjud bo'lsin va shu X qiymatlar to'plamlaridan biror bir funksiya keltirib chiqaraylik. = y. Ko'rinib qoldiki x ixtiyoriy *X* (0,1………. *N*) sonlar oralig'ida joylashgan. Bu sonlar ichidan olingan ixtiyoriy sonlar biz e'lon qilgan ma'lum bir funksiyadan o'tib y qiymatni hosil qildi. Bu jarayongacha biz bu funksiyani bir tomonlama deb atay olmaymiz. Hamma gap shundaki bu funksiyani orqaga qaytirishning boshqa matematik muqobil usuli yo'q bo'lishi lozim. Yanada aniqrog' qilib aytadigan bo'lsak bizga ma'lum bir funksiyamiz orqali xosil qilgan funksiyamiz qiymati y ma'lum *Y (0, 1, …. N)* sonlar oralig'iga tegishli bo'lib uni funksiyasini teskari shaklga keltirib hisoblash ma'noga ega emas. Mana bunaqa funksiyalar hisoblashda ancha qiyinchilik keltiradi. Buni matematik jihatdan quyidagicha yozamiz: ma'lum bir x qiymat orqali keltirib chiqargan *« = y»* funksiyamizni qiymatini teskari funksiya orqali jarayonni boshida hosil qiluvchi «*! = x*» ya'ni x ni topib olib bo'lmaydi. Bu maxfiy xolatga keltirishga ishlatiladigan funksiyalarni bir tomonlama funksiyalar deb ataymiz. Bu funksiyalarning kriptografika yo'nalishiga paydo bo'lishiga sabab, yuqorida aytganimizdek Stamfordlik olimlar Uitfield Diffi va Martin Xellmanlar sababchi bo'ldi.

**1.3.2 RSA algoritmi.**

Bu algoritm asimmetrik kriptotizim hisoblanadi va juda ko’p o’zligini tasdiqlash tizimlarda ishlatiladi. Bu tizimni ochiq kalitli kriptotizimlar ham deb atashadi. 1976 yilgi Diffi va Hellmanning maqolasi chiqqandan keyin kriptografika yo'nalshida juda katta o'zgarishlar kiritildi degan edik. Shu o'zgarishlar biri RSA algoritmidir. Massachusets texnalogiya universitetini olimlari bo'lgan Ronald Rives, Adi Shamir va Leo Adleman Diffi va Hellmanlarning e'lon qilgan maqolasini o'qib chiqib, o'zlarining algoritmlarini ishlab chiqmoqchi bo'lishadi. Bu ochiq kalitli tizimni ishlab chiqish jarayonida 40 tadan ortiq funksiyalar, tizimlar o'ylab chiqiladi. Ularning ichidan nihoyat bitta algoritm tanlashadi. Bu algoritm katta tub sonlarni juda oson topadi va ularni bir - biriga ko'paytiradi. Bu algoritmni RSA deb nomlashdi. RSA bu uning yaratuvchilarini sharafiga qo'yilgan ismlarning bosh harflaridir R - Rivest, S - Shamil, A – Adleman -> RSA. Keling bu algoritmni ishlash usulini qadamlarga bo'lib tatbiq qilsak:

**1-Qadam**da kalitni generatsiyalash deb yurutamiz:

* ikkita xar hil tub sonlarni olamiz: *p* = 3557, *q* = 2579
* ularni bir-biriga ko'paytmasini hisoblaymiz*:n = p \* q* = *3557 \* 25799173503*
* Eyler funksiyasini hisoblaymiz: *φ (n)* = (*p*-1) \* (*q*-1*)* = *9167368*
* Ochiq eksponentani tanlaymiz: *e* = 3
* Yopiq eksponentani tanlaymiz: *d =* *mod φ (n), d* = *6111579*
* Ochiq kalitni e'lon qilamiz: {*e, n*} = {3,9173503}
* Yopiq kalitni o'zimizga saqlab qo'yamiz: {*d, n*} = *{6111579,9173503}*

**2-Qadam** Matnni ochiq kalitlar orqali maxfiy xolatga keltirish:

* Biror bir matnni tanlaymiz: *m* = *111111*
* Shifrlangan matn holatga keltirish uchun hisoblash jarayonini o'tkazamiz: *c*=*E*(*m*) = *mod n* = *mod 9173503 = 4051753*

**3-Qadam**da matnni yopiq kalitlar yordamida ochiq holatga keltirish:

*m* = *D(c)* = = = 111111

Ochiq kalit orqali shifrlab junatmoqda yopiq kaliti orqali deshifrlamoqda.

**Kanallar orqali ma'lumot o'tishi**

*M = D (c)*

*C = E (m)*

*m* -> yopiq kanal ->*m*

2-sxema.

Matnni olish uchun 1-foydalanuvchi 2 –ma'lumot yuboruvchiga faqatgina ochiq kalitni yuborib matnni shu kalit qiymati bilan maxfiy xolatga keltirilgandan so'ngina aloqa kanali orqali qabul qilmoqda. Bu xolatni vaqt bo'yicha yoki har bir xabar almashish bo'yicha seanslab qo'yishimiz mumkin. Bunda matnni oluvchi ya'ni yopiq kalitga ega bo'lgan shaxs har bir matn olish jarayonida alohida, alohida ochiq kalitlar junatib turishi kerak. Bu jarayonni ikki tomonlama ko'rinishi ham mavjud bunda har ikkala tomon ham uzining kalitlariga ega bo'ladi.

**Ikki foydalanuvchi o'zaro aloqasi**

Har ikkala tomon ham matnlarni deshifrlaydi va shifrlaydi.

*M = D (c)*

*C =E (m)*

*C = E (m)*

*M = D (c)*

3-sxema.

**El-gamal Kriptotizimi.** EL-GAMAL matnni maxfiy xolatga keltirish usuli asimmetrik tarzda maxfiylash tizimlaridan biri bo'lib, u Amerika Qo'shma Shtatlarining (DSA) va Rossiya Federatsiyasining (GOST R 34.10-94) Elektron raqamli imzosining asosida yotadi. El-Gamal usuli kriptografika olamiga 1985 yilda Taher El-Gamal tomonidan namoyish qilinadi. Taher El-Gamal Diffi va Hellmanlarning tizimini yanada mukammallashtiradi. Bu tizim autentifikatsiya va matnni maxfiy xolatga keltirish bilan bog'liq jarayonlarda keng qo'llashga mo'ljallangan bo'ladi. El-Gamalning usulini RSA usulidan farqi shundan iborat ediki, Taher o'zining tizimi patent olmagan sababli bu usuldan foydalanish juda arzon bo'lib qolgan edi. Litsenziya uchun biror bir summa talab qila olamagan. Va shunday ham fikrlar borki bu tizim Diffi va Hellmanlarning patenti tasiri ostida turadi. Bu tkriptografik tizimning ham qadam orqali tartiblaymiz va nimalardan tashkil etganini o'rganamiz:

**1-qadam**. Kalitlarni generatsiyalash:

1. Biror bir *p* tub sonini tanlaymiz
2. Biror bir butun *g* sonini tanlaymiz
3. Tasodifiy biror bir butun son tanlaymizki bu son yuqoridagi keltirgan *p* songacha tegishli soxaga kirsin. Bu sonni x bilan belgilab olamiz *1 <x <p*
4. Hisoblaymiz *y = mod p*

Ochiq kalitlar to'plami bu *y, p, g,* yopiq kalit esa faqatgina x ning o'zi xolos.

**2-qadam**. Shifrlash jarayoni:

Bunda M matnimiz *p* qiymatimimzdan kichik bo'lishi kerak

1. Sessiya kalitini tanlaymiz. Bu shunday son *k* bo'lishi kerakki u *1<k<p-1* oralig'ida yotsin.
2. *a* va *b* sonlarni hisoblaymiz *a =* va *b =*
3. Bu (*a, b*) sonlari shifrlangan matn hisoblanadi. Ko'rinib turibdiki El-Gamal ususli bilan hosil qilingan matn boshlang'ich maxfiylashtirilmagan *M* matndan 2 barobar uzun.

**3-qadam**. Matnni ommaviy o'qib bo'ladigan holatga keltirish (Deshifrlash)

x maxfiy kalitni bilgan holda *a* va *b* qiymatlarni formula orqali hisoblaymiz.

*M=b \* (.*

Bunda (

shundan kelib chiqadiki,

= ()= ()=M (mod *p*).

Va ko'proq bunday hisoblashlarda quyidagi sodda xolatga keltirilgan formula juda mos keladi:

« *M = b*».

Kriptobardoshlik va hususiyati

Ochiq kalitli kriptotizimlar xazirgi kunda himoya jihatdan eng qulay tizimlar bo'lib kelmoqda. El-gamal tizimi ham shularnig ichiga kiradi. uning algoritmi hisoblashlarning qiyinlik darajasi diskret logarifmlashga borar ekan, unda *p, g, y* ma'lum bo'lib *x* ni qanoatlantiruvchi tenglik topish ancha murakkab bo'ladi:

*y (mod p).*

Xozirda El-gamal sxemasi asosida ko'plab qo'shimcha algoritmlar paydo bo'lmoqda. Bularga misol qilib: DSA, ECDSA, KCDSA, Shnorra sxemasi.

Foydalanuvchilar orasida malumotlarni maxfiy holatga keltirish, almashish va birlamchi holatga keltirish sxemasi quyidagicha bo'ladi:

Yopiq ma'lumot

B tomon

A tomon

Deshifrlash jarayoni

*M*->

shifrlash

1-bo'lib p tub sonini tanlaymiz.

2-bo'lib g qiymatni tanlaymiz.

3- bo'lib *x: y=g^x* mod p tanlaymiz.

Kalitlarni generatsiyalash

*(p, g, y)* ochiq kalitlar

*A=g^k mod p*

*B=y^k\*Mmod p*

*M=b\*(a^x) ^ (-1) mod p*

4-sxema.

**1.3.3 Psevdotasodifiy sonlar generasiyasiga asoslangan algoritmlar.**

Bu sonlar generatori shunday algoritmki, uning chiqayotgan elementlari bir-biriga bog’liq bo’lmaydi. Va hech qanaqa ayniyat bilinmaydi. Tasodifiy sonlar manbayini toppish juda qiyin. Kriptografiyada psevdotasodifiy – psevdotasodofiy bitlarning kelishidan va har xil oqimli shifrlarni keltirib chiqarishiga aytiladi. Psevdatosidifiy generatorlar qo’yidagi ko’rinishlarga ajratiladi: oddiy arifmetik, kriptografik sindirilgan yoki buzilgan va oxirgisi kriptobardoshli. Bularning umumiy bir narsaga yo’naltirilgan, oddiy metodlar bilan sonlar generatsiyasini sirini topish mumkin bo’lmasligi. Deyarli ko’pchilik kriptotizimlar psevdatasodifiy sonlar generatsiyasidan foydalanishadi. Ayniqsa kalit ishlab chiqishda. Inson shun kalitlarni generatsiyalovchi dasturiy ta’minot yozarkan, har bir kriptozimning hsartlarini inobatga olgan holda algoritmlarni tuzadi, masalan asimmetrik kriptotizimlarda tub sonlar qatnashi kerak, simmetrikda esa birlik yoki o’nlik sonlardan yuqori yoki usuliga qarab qadamlar ko’pligi qanoatlantirilishi kerak. Psevdotasodifiy sonlar generatori funksiyasini mexanizmini ko’rzmiz:

**Random psevdatosodifiy sonlar generatsiyasi strukturasi**

O’rnatish funksiyasi

Initsializatsiya funksiyasi

Qiymatni generatsiyalash funksiyasi

Deinitsializatsiya funksiyasi

Generatorning korrektligini tekshiruvchi funksiya

5-sxema.

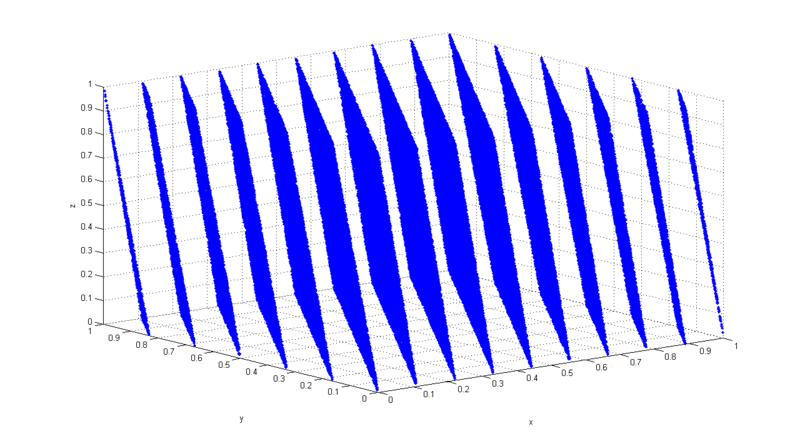
**RANDU** – bu psevdotasodifiy sonlar generatori bo’lib, u 1960 – yildan to’liq foydalanishga kirib kelgan. Bu holatda bo’lib, bu yerda toq sondir.

Psevdotasodifiy sonlar quyidagi ko’rinishda hisoblanadi:

bu algoritm xozirda ham eng taniqli algoritm hisoblanadi.

Kvadrat ko’paytuvchilarni ochib chiqqandan so’ng quyidagi formulaga ega bo’lamiz:

Bu algoritmdan bilinib uch o’lchovli koordinatada yotib, uncha katta bo’lmagan qirrada yoki silliq sirtda yotadi.



3-rasm. Random funksiyasining psevdotasodifiy sonlarni sonlar o'qidagi grafiki