

**O'ZBEKISTON RESPUBLIKASI AXBOROT TEXNOLOGIYALARI
VA KOMMUNIKATSIYALARINI RIVOJLANTIRISH VAZIRLIGI**

**MUHAMMAD AL-XORAZMIY NOMIDAGI TOSHKENT
AXBOROT TEXNOLOGIYALARI UNIVERSITETI**

MUSTAQIL ISH

Guruh: 011-18

Bajardi: Rakhimov M.B

Variant 11

Mavzu : Simmetrik va assimetrik kriptotizimlarning qiyosiy tahlili

Reja:

- 1. Kirish*
- 2. Simmetrik kriptotizimlar*
- 3. Asimetrik kriptotizimlar*
- 4. Xulosa*

KIRISH

“Istalgan axborot xavfsizlik tizimini buzish mumkin, faqatgina bu shunga ketadigan harajat, vaqt va mehnatiga arziyidigan ma’lumot bo’lsa!”

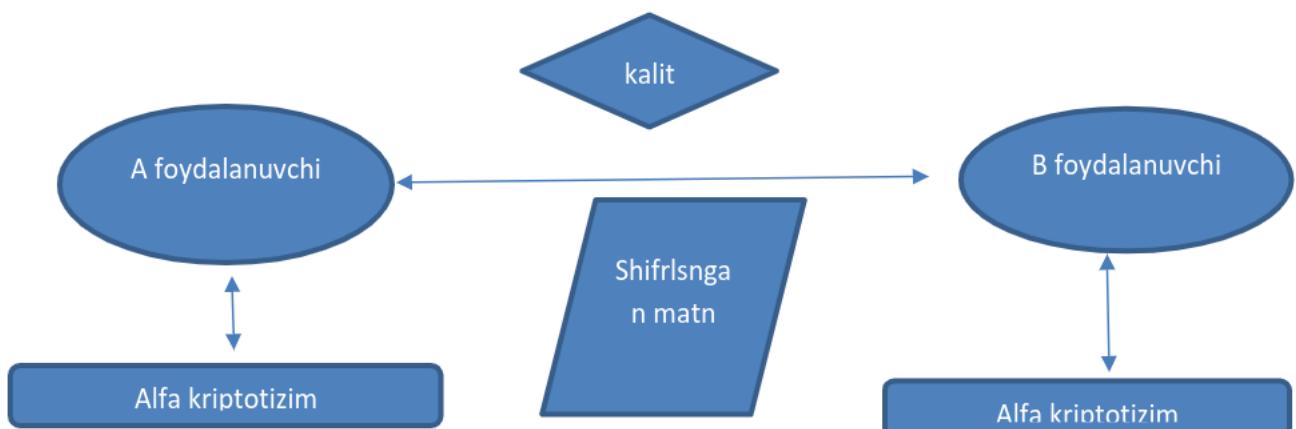
Norbert Viner.

Axborot axborot xavfsizligini ta’minlashda eng ishonchli vasotalardan biri axborotni kriptografik himoya qilish vositalari hisoblanadi. Shu bois Respublikamizda bu yo’nalish jadal sur’atlar bilan rivojlanmoqda. Prezidentimizning 2007 yil 3 – aprelda qabul qilgan “O’zbekiston Respublikasida axborotning kriptografik himoyasini tashkil etish chora-tadbirlari to’g’risidagi” PQ – 614 – son qarori shular jumlasidandir.

Axborot-kommunikatsiya tizimida ma’lumotlarni maxfiy yoki konfidensial almashuv jarayoni uchun kriptografik tizimlar yaratish bilan bir qatorda shu tizimda bardoshli kalitlar yaratish masalasini ishonchli hal etish muhim o’rin tutadi. Chunki tanlangan kriptotizim murakkab va ishonchli bo‘lishi undan amalda foydalanish jarayonlari bardoshli kalitlarni generatsiya qilish masalasi bilan bog‘liqdir.

Simmetrik kriptotizimlar bu shunday kriptoshifrlash tizimiki unda shifrlash ham deshifrlash ham aynan bir kalit yordamida amalga oshiriladi. Bu kriptotizim asimetrik kriptotizimlar vujudga kelmasi turib faqatgina simmetrik tizimlardan foydalanilgan. Algoritmning kaliti o'zaro ma'lumotlar almashinayotgan tomonlarning har ikkalasi uchun ham boshqalardan sir saqlanishi kerak. Ma'lumotlarni qaysi simmetrik kriptotizim asosida shifrlanishi bu ikki tomon tomonidan ma'lumot almashinishi oldin bajarish kerak

Simmetrik tizimning strukturasi



Simmetrik kriptotizimlarning turlari:

Simmetrik kriptotizimlarga qo'yidagi algiritmlarni misol qilib keltirishimiz mumkin:

1- Blokli shifrlash algoritmlari:

- AES (Advanced Encryption Standard)
- DES (Data Encryption Standard)
- 3DES (Triple-DES)
- RC2 (Rivest shifri)
- RC5
- Blowfish
- Twofish
- NUSH
- IDEA (International Data Encryption Algorithm, Xalqaro ma'lumotlanri shifrlash algoritmi)
- CAST
- Kuznechik

2- Potokli yoki Oqimli shifrlash algoritmlari:

- RC4
- SEAL (Software Efficient Algorithm)
- WAKE (World Auto Key Encryption algorithm)

Bu kalit orqali ham shifrlanadi ham deshifrlanadi. Bu tizimning xavfi shundaki agar bu kalit mahfiy kanaldan tutib olinsa tutib olingan matnni bemalol deshifrlash imkonini paydo bo'ladi. Aynan anashu xolat asimmetrik kriptotizimni kelib chiqishiga sabab bo'ldi. Bu kalitlar bilan mavjud bo'lgan muammoni 1976 yilda yechimini topishdi. Asimmetrik kriptotizimda ochiq kalit va yopiq kalit tushunchasi kirib keldi. Bu g'oyani Amerikalik kriptografikachilar Uitfeld Diffi va Martin Xellman tomonidan kiritishdi. Ochiq kalitni ommaviy uzatish mumkin, yopiq kalitni esa ochiq

kalitni yuboruvchini o'zida yashirin xolda qoladi. Bu jarayon qanday bo'ladi? Matnni qabul qilib oluvchi ikki xil kaliti bo'ladi: Ommaviy kalit va Maxfiy kalit. Bu shaxs matn yuboruvchi shaxsga faqatgina ochiq kalitni uzatadi. Matnni yubormoqchi bo'lgan shaxs esa shu ochiq kalit bilan matnni shifrlaydi va uzatadi. Matnni qabul qilib olgan shaxs o'zining maxfiy kaliti bilan matnni deshifrlaydi. Mabodo ochiq kalitni dushman qo'lga kiritganda ham uni deshifrlay olmaydi.

Bu matnni deshifrlash uchun kompyuterda yillab vaqt kerak bo'ladi. Kalitlarni tanlashda qancha katta tub sonlar tanlansa, qadamlar soni shuncha ko'payadi. Kompyutering hisoblashiga ham ancha qiyinchilik tug'diradi. Bu tizimlarga RSA va Al-Gamal shifrlash tizimlari kiradi. Bu tizimlar berilgan qiymatlar ustida matematik arifmetik amal bo'lgan modulli bo'lish yoki boshqacha qilib aytganda qoldiqli bo'lish asosida yaratilgan va shu rusumda ishlaydi. Bu tizimlarni zamonaviy axborot texnologiyalarda ERI (Elektron raqamli imzo) ham deb yuritiladi. Aslida esa bu Elektron raqamli imzo va Autentifikatsiya tizimlar asosida ochiq va yopiq kalitlarga asoslangan kriptografik tizim. Autentifikatsiya bu ma'lumotlarning egasini aniq shu muallifligini tasdiqllovchi tizimdir. Misol qilib keltirsak: foydalanuvchi o'zing parol va login bilan himoyalangan ma'lumotlar bazasiga kirayotganda uning parol va logini aniqligini tekshirishda, electron hujjatlarni aniq yuboruvchining o'ziga tegishli ekanligini isbotlovchi ochiq kalitli raqamli imzoni tekshirishda juda ko'p ishlatiladi. Kriptografiyada kriptotizimlarning o'zlarining kalitlarga qo'fyiladigan parametrlari mavjud. Bular turli xil shartlarni qanoatlantirishida. Bizga ma'lum bir algoritm berilgan bo'lsin, algoritmning funksiyasi $y = f(x)$ bo'lib, u x argument qabul qilsin. Kriptotizimning qandayligiga qarab x -argumentga shu kriptotizimlarning kalitga qo'yiladigan shartlari, qanday parametrlarga bo'y sunushi mavjud bo'ladi. RSA, Elgamal, Rabin va shunga o'xshagan kriptotizimlari algoritmlarida kalitlar tub sonlar asosida qurilishi kerak. Aynan tub sonning katta yoki kichikligi, aniq tub sonligi kalitning parametrlari xisoblanadi. Asimetrik kriptotizimlar bir tomonli funksiyalardan tashkil topgan ekan, bu funksiyalarning argumentiga qo'yadigan va shifrlash jarayonida shifrlagan ma'lumotni deshifrlashda murakkabligini oshiradigan parametrlarni xosil qiladi. Bu matematiklar tomonidan yaratilib kelinib,

funksiyalarning aniqlanish sohasi, qiymatlar sohasi kabi tushunchalarni o'z ichiga oladi.

Bir tomonlama funksiyalar. Bu funksiyalarning bir tomonlama deyilishi sabab shuki, bu funksiyalar bir tomonlama ishlatalgan 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. $f(x)_z = y$. Ko'rinish qoldiki x ixtiyoriy $X (0, 1, \dots, N)$ 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 $f(x)_z$ ma'lum bir funksiyamiz orqali xosil qilgan funksiyamiz qiymati y ma'lum $Y (0, 1, \dots, N)$ 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 « $f(x)_z = y$ » funksiyamizni qiymatini teskari funksiya orqali jarayonni boshida hosil qiluvchi « $f(y)_z^{-1} = x$ » ya'ni x ni topib olib bo'lmaydi. Bu maxfiy xolatga keltirishga ishlataladigan 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.

RSA algoritmi. Bu algoritm asimmetrik kriptotizim hisoblanadi va juda ko'p o'zligini tasdiqlash tizimlarda ishlataladi. 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. Massachusetts 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 algoritmn RSA deb nomlashdi. RSA bu uning yaratuvchilarini sharafiga qo'yilgan ismlarning bosh harflaridir R - Rivest, S - Shamil, A – Adleman -> RSA. Keling bu algoritmn ishlash usulini qadamlarga bo'lib tatbiq qilsak:

1-Qadamda 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: $\varphi(n) = (p-1) * (q-1) = 9167368$
- Ochiq eksponentani tanlaymiz: $e = 3$
- Yopiq eksponentani tanlaymiz: $d = e^{-1} \text{ mod } \varphi(n), d = 6111579$
- 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:

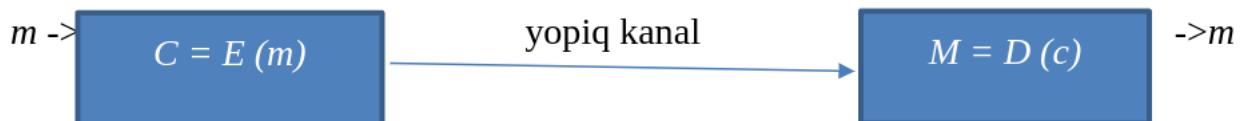
- Biror bir matnni tanlaymiz: $m = 111111$
- Shifrlangan matn holatga keltirish uchun hisoblash jarayonini o'tkazamiz: $c = E(m) = m^e \text{ mod } n = 111111^3 \text{ mod } 9173503 = 4051753$

3-Qadamda matnni yopiq kalitlar yordamida ochiq holatga keltirish:

$$m = D(c) = c^d \text{ mod } n = 4051753^{6111579} \text{ mod } 9173503 = 111111$$

Ochiq kalit orqali shifrlab junatmoqda yopiq kaliti orqali deshifrlamoqda.

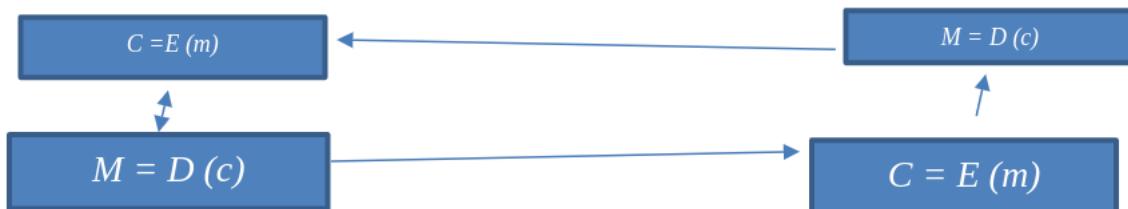
Kanallar orqali ma'lumot o'tishi



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.



El-gamal Kriptotizimi. EL-GAMAL matnni maxfiy xolatga keltirish usuli asimetrik 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 $y = g^x \text{ mod } p$

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 qiymatimizdan 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 $a = g^k \text{ mod } p$ va $b = y^k M \text{ mod } p$
3. Bu (a, b) sonlari shifrlangan matn hisoblanadi. Ko'rinish 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.

$$M = b * \left(\frac{1}{(a^x) \text{ mod } p} \right) * p.$$

$$\text{Bunda } \left(\frac{1}{(a^x) \text{ mod } p} \right) = g^{-kx} \text{ (mod } p\text{)}$$

shundan kelib chiqadiki,

$$b * (a^x)^{-1} = (y^k M) g^{-kx} = (g^{xk} M) g^{-xk} = M \text{ (mod } p\text{).}$$

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

$$\ll M = b * (a^{x-1}) \text{ mod } p = b * a^{(p-1-x)} \text{ mod } p \gg.$$

Kriptobardoshlik va hususiyati

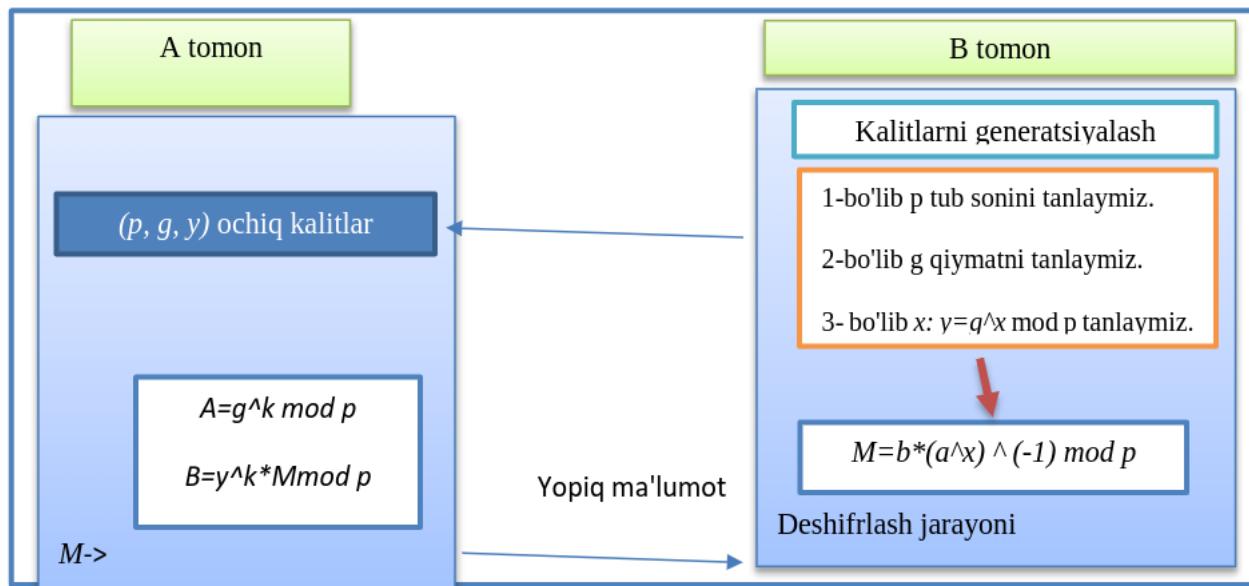
Ochiq kalitli kriptotizimlar xazirgi kunda himoya jihatdan eng qulay tizimlar bo'lib kelmoqda. El-gamal tizimi ham shularning ichiga kiradi. uning algoritmi hisoblashlarning qiyinlik darajasi diskret logarifmlashga borar ekan, unda p, g, y ma'lum bo'lib x ni qanoatlantiruvchi tenglik topish ancha murakkab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

$$y \equiv g^x \pmod{p}.$$

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:

Birlamchi ma'lumot almashish sxemasi



Asimmetrik kriptotizimlarning simmetrik kriptotizimlarga qaraganda kamchiligi:

- Algoritmga o'zgartirish qiyin. Bu hammasi Diffi va Hellman qonunlari asosida bo'lishi, sonlarni qiymatlariga beriladigan shartlarni qanoatlantirishi kerak.
- Juda uzun kalitlat. Pastki jadvalda simmetrik kriptotizimlarning va asimmetrik kriptotizim bo'lgan RSA kalitlarining uzunligi keltirilgan:

1.1-jadval. Simmetrik va assimetrik kriptotizimlarning kalit o'lchovlari

Simmetrik kriptotizimlarning uzunligi (bit o'lchov birligida)	RSA kriptotizimining uzunligi (bit o'lchov birligida)
56	384
64	512
80	768
112	1792
128	2304

Shifrlash-deshifrlash asimmetrik kriptozimlarda, simmetrik kriptotizimlarga shifrlash- deshifrlash, nisbatan juda sekin bajariladi.

Juda ko'p resurslar talab qiladi. Bu asimmetrik algoritmlarning ichiga bir nazar tashlasak juda ko'p arifmetik amallar va shartlarni ko'rishimiz mumkin.

1.2-jadval. Algoritmlarning o'zaro bir biri bilan solishtirilishi:

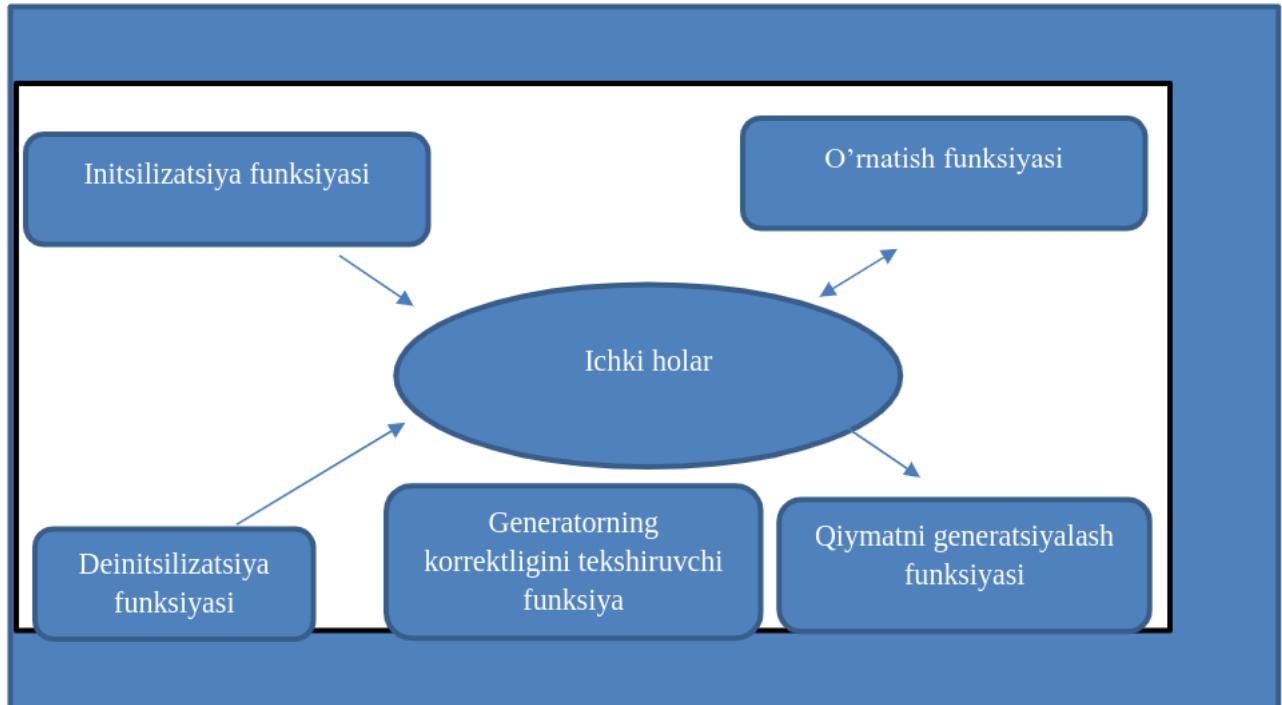
	Kalit	Qo'llanishi	Kriptobardoshliliqi, MIPS	Izoh
RSA	4096 bitgacha	Shifrlash va imzoda	1300-bit kalit uchun $2,7 \cdot 10^{28}$	o'zida juda ko'p standartlarni mujassam etadi.
ElGamal	4096 bitgacha	Shifrlash va imzoda	1300-bit kalit uchun $2,7 \cdot 10^{28}$	Murakkab diskret logarifmik hisoblashlarga

				asoslangan tizim
DSA	1024 bitgacha	Faqat imzoda qo'llanadi		ANB tomonidan o'ylab chiqilgan bo'lib, diskret logarifmlashga asoslangan
ECDSA	4096 bitgacha	Shifrlash va imzoda	Tezlik va kriptobardoshliligi RSA nikida ko'ra yuqori	Zamonaviy yo'nalish bo'lib juda ko'p matematiklar bular ustida ishlamoqda

1.1. 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 aytildi. Psevdatosidifiy generatorlar qo'yidagi ko'rinishlarga ajratiladi: oddiy arifmetik, kriptografik sindirilgan yoki buzilgan va oxirgisi kriptobardoshli. Bularning umumiyligi 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



RANDU – bu psevdatosodifiy sonlar generatori bo’lib, u 1960 – yildan to’liq foydalanishga kirib kelgan. Bu $V_{j+1} \equiv (65539_j) \text{mod } 2^{31}$ holatda bo’lib, bu yerda V_0 toq sondir.

Psevdatosodifiy sonlar quyidagi ko’rinishda hisoblanadi:

$X_j \equiv V_j / 2^{31}$ bu algoritm xozirda ham eng taniqli algoritm hisoblanadi.

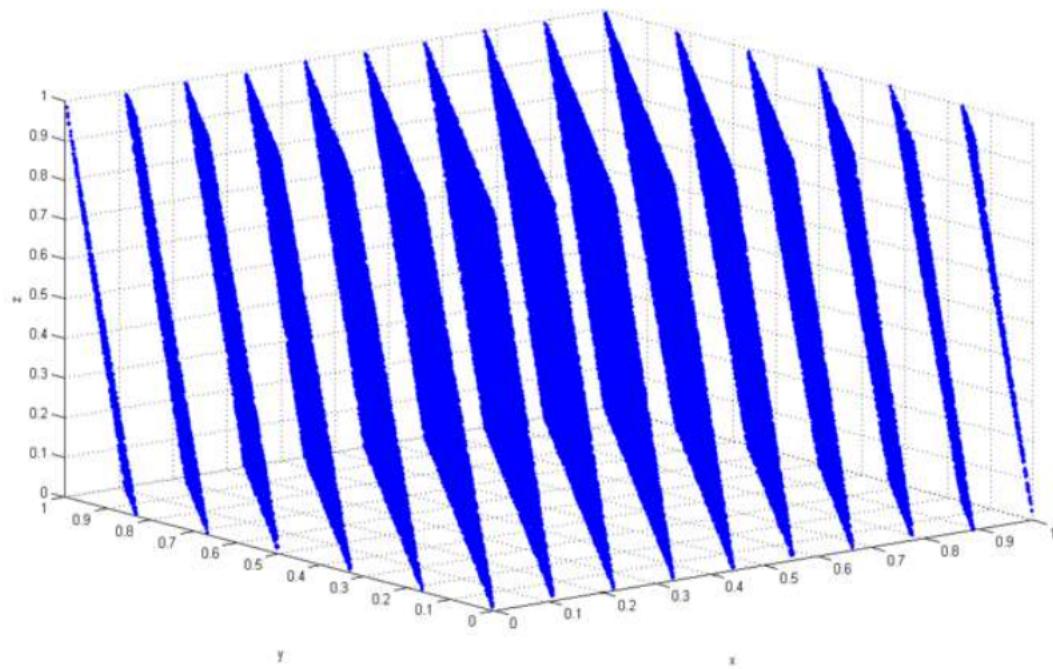
$$x_{k+2} = (2^{16} + 3)x_{k+1} = (2^{16} + 3)^2 x_k$$

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

$$x_{k+2} = (2^{32} + 6 * 2^{16} + 9)x_k = [6 * (2^{16} + 3) - 9]x_k$$

$$x_{k+2} = 6 * x_{k+1} - 9 * x_k$$

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



1.5. rasm. Random funksiyasining psevdatosodifiy sonlarni sonlar o'qidagi grafiki

1.4. Kvant kriptografiyası

Kvant kriptografiyası – bu xavfsizlik tizimini kvant fizikasiga asoslangan holda yaratilishi. Bu yo'malishdagi kriptografiyanı odatiy kriptografiyadan farqi shuki, klassik kriptografiya, matematik metodlarga asoslangan bo'lsa, kvant kriptografiyası kvant fizikasidagi ob'yektlarning informatsiyani xavfsizligiga javob berishiga asoslangan. Ma'lumotlarni yuborish, qabul qilish har doim fizik qurilmalar yordamida amalga oshiriladi. Axborot tashuvchilar elektr oqimidagi elektronlar, optic aloqadagi fotonlarni misol qilish mumkin. Kvant kriptografiyası texnologiyasi kvant tizimini xaddi-harakatini aniqlab bo'lmaslik tamoyillariga bo'y sunadi. Bu aniq bo'limgan tamoyil Geyzenbergni teoremasi bo'lib, unda bir vaqtning o'zida zarrachaning ham impulse ham kordinatasini boshqa fotonlarnikini aniqlab bo'lmay bir fotonni parametriga qarb aniqlab bo'lmaydi. Birinchi bor kvant obyektlari tomonidan axborotlarni ximoyalash 1970 – yilda Stiven Vizner tomonidan taklif qilingan. O'n yillarcha o'tgach IBM kompaniyasi hodimi Charliz Bennet va Monreall universiteti olimi Jil Brassar Viznerni ishi bilan tanishgach, ishaltilayotgan kvant

obyektlariga maxfiy kalitni ishlatalishni taklif etdilar. Ular 1984 – yilda esa kvant holati yordamidagi ximoyalangan kanalni yaratishni ntaklif qilib kiritishdi. Bundan keyin ular tomondan BB84 sxemasi taklif etilgan.

Maxfiy kalitni generatsiyalashning (BB84) oddiy algoritmi. Birinchi bo'lib foydalanuvchi tanlangan polyarizatsiya 0, 45, 90, 135° bo'yicha fotonni generatsiyalaydi. Qabul qiluvchi bu fotonlarni qabul qilib uni diogonal yoki perpendikulyar tarzda qutblantirani o'lchaydi. Keyin ochiq kanal orqali hisoblash natijalarini yoshirmagam holda har bir foton uchun qanday yondashganini bildiradi. Keyin esa foydalanuvchi va qabul qiluvchi qabul qiluvchining qaysi foronga nisbatan noto'g'ri yondashganini tashab ketishadi. Agar kvant kanalini tutib olishmasa, ma'lumotlar maxfiy kalit bilan va boshqa qutblangan ko'rinishda chiqadi. Chiqishda bitlarning ketma-ketlikda tartib bilan chiqadi: gorizontal yoki 45° li qutblari ikkilik "0" qiymatga, vertical va 135° li qutliligi ikkilik "1" qiymatni o'z ichiga oladi. Bu kvant kriptografik tizimini birlamchi kvant aloqasi deb ataymiz.

Alisa 4 ta mumkin bo'lган qutblanishni quyidagicha tanlaydi va jo'natadi.

	/	-	\	-	-	/		
--	---	---	---	---	---	---	--	--

Har bir foton uchun Bob tasodifiy hollarni tanlaydi.

+	+	*	*	+	*	*	*	*	+
---	---	---	---	---	---	---	---	---	---

Bob o'lchangan natijalarni hisoblaydi va maxfiy tarzda saqlaydi.

	-	/	\	-	/	/	/	
--	---	---	---	---	---	---	---	--

Bob ochiq holda qanday o'lchamalrn yoki hisoblanganda chiqqan natijalarni aniqlaganini bildiradi, Alisa esa qaysi o'lchamlar to'g'ri bo'lganini tekshirib xabar beradi.

V				V	V		V		V
---	--	--	--	---	---	--	---	--	---

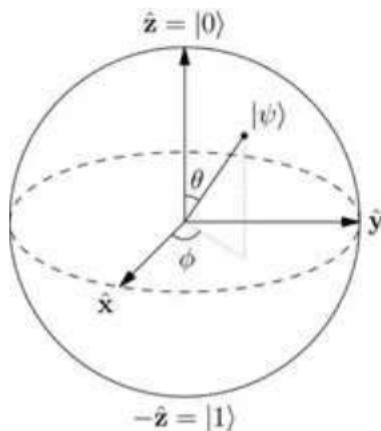
Alisa va Bob, Bob o'lchagan hamma to'g'ri ma'lumotlarni saqlab qoladi. Bu ma'lumotlar "0" va "1" holatga keltiriladi.

			\	-		/		
1			1	0		0		1

Kvant superpozitsiyasi. Kvant superpozitsiyasi kvant mexanikasi asosida paydo bo'lgan. Kvant mexanikasi 20 asrning global o'zgaruviga sabab bo'ldi desak xato bo'lmaydi. Chunki biz ishlatalayotgan har bir telefon, har bir kompyuter, har bir aqli hisoblash tizimlari, gadget yoki shunga o'xshash qurilmalar kvant mexanikasiz paydo bo'lmasdi. Bu davrlaning boshlanishi 1930 tillarga borib taqaladi. Bu kvant superpozitsiyasi mana man degan olimlarning ham miyasini tormozlantirib qo'ygan. Kvant superpozitsiyasiga bir misol keltirib unga yaxshilab e'tibor bersak gap nimada ketayotganligini anglab olamiz. Misol uchun: maqsad olma sotib olish mumkin bo'lsin, siz bitta olma sotib oldiz, men ham bitta olma sotib oldim. Biz birgalikda ikkita olma sotib oldik. Vazifa juda yaxshi bajarildi deylik. Ammo superpopzitsiyaning ham o'ziga yetarlicha muammosi bor.

Deylik biz olma sotib olmoqchimiz, ammo do'konda bor yo'g'i bir donagina olma qolgan. Unda biz hech qachon ikkita olma sotib ololmaymiz. Lekin yakka holda olma sotib olishimiz mumkin edi. Manabu endi olimlarning miyasiga urilgan kvant superpozitsiyasining qarashi edi. Bu ancha tushunmovchiliklarga olib keladi. Odatda fiziklar bu kvant superpozitsiyasiga quyidagicha qaraydilar: bir natijaga olib keluvchi shu birinchi holatga olib kelsa, ikkinchi najiga olib keluvchi jarayon shu ikkinchi jarayonning holatiga olib kelsa, ikkala jarayonning birgalikda harakati aniq natijaga olib keladi. Ammo kvant superpozitsiyasi klassik superpozitsiyasidan farqlanadi. Bu kvant teoremasi bilan uzlusiz bog'liqdir. Bizda ikkita quti bor deylik. Electron shu ikki qutining birida bo'ladi, ikkinchida esa yo'q. Albatta yo ikkinchisida bo'lib birinchisida bo'lmasligi ham mumkin. Kvant superpozitsiyasida esa bu elektron har ikkala qutida bir vaqtning uzida bo'ladi. Bu esa shu yuqorida qarashlarimizga bog'liq holda kvant superpozitsiyasining uning harakati haqida emas balki uning holatida ketayotganligini bilib olamiz. Shunday qilib kvant superpozitsiyasi bu zarrachaning bir vaqtning uzida ham holatlari, ham joylashganidir. Superpozitsiya ham bugungi kunda hozircha amalga oshirilmagan nazariyagini xolos.

Kubitlar



1.7-Rasm. Kubitning matematik tuzilishi

Kubitning polyar ko'rinishi. Kubit-bu kvantli razryad yoki kvant kompyuterida ma'lumot saqlovchi element. Kubit ham huddi bitdek ikki xil holatni o'z ichiga oladi. Bular: nol va 1. Shu holatlarni o'z ichiga olgan holatda superpozitsiyani egallab quyidagi tenglikni qanoatlantiradi:

$$|A^2| + |B^2| = 1.$$

Kubit so'zini birinchi bo'lib Amerika Qo'shma Shtatlarida Kenon kollejdan Ben Shumaxer foydalanishga kiritgan. Zvezdin esa buni qisqacha qilib q-bit deb yuritishni taklif qilgan. Ba'zi bir adabiyotlarda kvantbit degan atamalarni ham uchratish mumkin. Kubitlarning oddiy klassik bitlardan farqi oddiy bit 0 yoki 1 qiymatlarni qabul qilgan holda qayta ishlansa kubitlar esa bir vaqtning uzida ham bir ham nol qiymatga ega bo'ladi. Kubitlarning qutblanishi elektronlarniki bilan bir xil shaklda amalga oshadi.

Kubitlar ikki xil holatni bir vaqtning uzida qabul qilishiga qaramay uning koefisentlari elektronning qayerda joylashganini topishini ehtimolini beradi. 2ta qubit mumkin bo'lgan 4 xil holatda bo'ladi. 4ta qubit esa 16 ta holatni o'z ichiga oladi.

Bu qanday amalga oshadi:

Bizga ikki bit ma'lumot bo'lsin $00, 01, 10, 11$ bu shu ixtiyoriy ko'rinishlardan biri bo'ladi. Ammo kubitlarda bu to'rtta holat ham shu ikki kubitga tegishli bo'ladi. Buning matematik ko'rinishi:

$$2^n = n$$

Bu yerda n – kubitlar soni, 2^n esa u qabul qiladigan bitlar soni. Shunday qilib bilib oldikki kvantoviy kompyuter oddiy kompyuterden farqi u bir natijaga olib keluvchi jarayonni bir vaqtning o’zida turli xil usullar bilan yondasha oladigan kompyuterdir. Kompyuterlarning parallel ishlay olishi bugungi kunda shunchaki farazgina bo’lib kelmoqda. Kvant kompyuterlarning paydo bo’lishi kriptografiya olamida ochiq va yopiq kalitli asimetrik kriptotizimlarning yo’q bo’lib ketishiga olib keladi.

Shor algoritmi. Shor algoritmining xususiyati shundaki, bu algoritm yordamida ochiq kalitli kriptizimlarni buzish mumkin. Buning uchun bizga Shor algoritmini kvant kompyuterida yuritishimiz kerak xolos. Misol uchun RSA algoritmini olsak, unda M ochiq kalit bo’lib u ikki tub sonning ko’paytmasidan xosil bo’lgan. RSA shifrlash tizimini buzishning yo’llaridan biri M sonining ko’paytuvchilarini topishdir. M katta qiymatga ega bo’lganda klassik algoritmlardan foydalanish bu jarayonga hech qanday naf bermaydi. Bularga misol qilib Shanksning kvadratik forma metodi va Pollard va Shtrassen algoritmini keltirishimiz mumkin. Bu algoritmlar $M^{1/2}$ vaqtini talab qiladi.

Shor algoritmining ishlash tamoyili. Shor algoritmining asosi shuki, u kvant kompyuterlaridagi birlik ma'lumotlarni-kubitlarni-bir qancha qiymatlarni qabul qilishiga va chalkashliklarni topib bartaraf etishga undaydi. Shuning uchun ham u kubitlarni tejagan holda hisoblashlarni amalga oshiradi. Shor algoritmining ishlash tamoyilini ikkiga bo’lish mumkin:

- Bir muncha ma'lum bir funksiyalarni topishni ko'p
- Bu funksiyaning davrini kvantli tarzda topish

Qo’yingki:

M -bizda shunday sonki, toq sonning ildizi bo’lmasisin va bu sonni biz ko’paytuvchilarga ajratishimiz kerak bo’lsin.

N - ishlatilayotgan registrning xotirasining hajmi

Bit ko'rinihsidagi o'lchami n ning M o'lchamidan 2 barobar kattadir. Aniqrog'i,

$$M^2 < N = 2^n < 2M^2$$

t- Ixtiyoriy parametr, unda

$$1 < t < M \text{ va } \gcd(t, M) = 1,$$

bu yerda \gcd -umumiyligi bo'luvchi. Bu yerda aytib o'tish lozimki t, M, N aniqlangan bo'lib, bizga faqatgina t ixtiyoriy son uchun r funksiyaning davrini topishimiz kerak.

Klassik algoritm. Bu yerda r shunda minimalki u $t^r = 1 \pmod{M}$ t ning M bo'yicha modulli tartibi hisoblanadi. r qatori $f(x) = t^x \pmod{M}$, bu yerda $x = 0, 1, 2, \dots, N-1$ funfsiyasining qatoridir. Unga ko'ra agar r ni t funksiya orqali samarali aniqlab olsak, RSA shifrlash tizimidagi M ning bo'luvchilarini $\log_2 M$ dan $1 - M^{-m}$ vaqt oraliq'igacha aniqlab olish mumkin bo'ladi. Shunday qilib davom etamiz $r = 0 \pmod{2}$, $t^{r/2} \neq -1 \pmod{M}$ unda $\gcd(t^{r/2} + 1, M)$ - M ning bo'luvchisi. Bunda $\geq 1 - 1/2^{k-1}$ ehtimoli k ning qiymati toq bo'lmaganda kelib chiqadi. Shuning uchun ham $t \geq 1 - M^{-m}$ shartni qanoatlantirib $O(\lg M)$ urinishdan kelib chiqadi. Bir urinishning eng uzun hisoblanish- $t^{r/2} ga$ teng bo'ladi.

Kvant algoritmi. Kvant algoritmini ro'yobga keltirish uchun sxemada ikkita registr kerak bo'ladi X va Y . boshida bular kubitlarning 0 holatidagi aksini uz ichiga olgan holda bo'ladi. X registr x funksiyaning $f(x)$ argumentlarni joylashishi uchun xizmat ko'rsatadi. Y registr esa r davri bo'yicha $f(x)$ funksiyaning qiymatlarini saqlash uchun ishlatiladi. Kvantli hisoblash 4 qadamdan iborat:

- Birinchi qadam. Adamar operatsiyasidan foydalanib hamma superpozitsiyasini X registr uchun boshlang'ich holatini joylahstirgan holda hisoblashni bajaramiz. Va ikkala registrning holati quyidagi ko'rinishga keladi:

$$\frac{1}{\sqrt{N}} \sum_{x=0}^{N-1} |x, 0\rangle$$

- Ikkinci qadam. Ikkala registr uchun Unitar o'zgarishni hisoblaymiz:

$$\frac{1}{\sqrt{N}} \sum_{x=0}^{N-1} |x, 0\rangle \xrightarrow{U_f} \frac{1}{\sqrt{N}} \sum_{x=0}^{N-1} |x, t^x \pmod{M}\rangle$$

Ikkala registrning o'rtasidagi bog'liqlikning holatidir.

Uchunchi qadam. Furye qatori bizga shunday Uniter uzgarishini beradiki u kvant registrlarni holatini bizga namoyon qiladi.

$$\exists \sum_{x=0}^{N-1} f(x)|x\rangle$$

Va

$$\sum_{k=0}^{N-1} \tilde{f}(k)|k\rangle$$

$$QFT_N : \sum_{x=0}^{N-1} f(x)|x\rangle \Rightarrow \sum_{k=0}^{N-1} \tilde{f}(k)|k\rangle$$

bunda Furye o'zgarishi Amplituda $f(x)$ uziga

$$\tilde{f}(k) = \frac{1}{N} \sum_{x=0}^{N-1} \exp(2\pi i kx/N) f(x)$$

ko'rinishni oladi. Uchunchi qadamda birinchi registrni holati ustida Furye uzgarishi amali bajarilib unda quyidagi holatni olamiz:

$$\frac{1}{N} \sum_{x=0}^{N-1} \sum_{k=0}^{N-1} \exp(2\pi i kx/N) |k, t^x \bmod M\rangle$$

- To'rtinchi qadam. Bu qadamda birinchi registrning o'lchamini olamiz:

$$|0,0\rangle \otimes I, |1,1\rangle \otimes I, |1,1\rangle \otimes I, \dots, |N-1,N-1\rangle \otimes I$$

Va natijada ko'rindikli

$$|k, k^t \bmod M\rangle,$$

$$\left| \frac{1}{N} \sum_{x: t^x \equiv k^t \bmod M} \exp(2\pi i kx/N) \right|^2$$

Va bunda quyidagi yaqinlashishni amalga oshiramiz k/N dan

$$r' < M < \sqrt{N}:$$

$$\left| \frac{k}{N} - \frac{d'}{r'} \right| < \frac{1}{2N}$$

Va r ning o'rniga r' dan foydalanib ko'ramiz:

- Agar $r' \equiv 0 \pmod{2}$ bo'lsa, unda $\gcd(t^{r'/2} \pm 1, M)$
- Agar r' toq bo'lmasa yoki toq bo'lsa M ning bo'luvchisi topilmasa, unda $O(\lg \lg M)$ ni huddi shu t qiymati orqali qayta yana bir bajariladi.

Nidderayterning kriptozimi. Bu tizim yuqori keltirgan asimmetrik kriptotizimlardan ko'ra, shor algortimiga bardoshliroq asimmetrik tizimdir. Bu tizim ham o'zining ochiq kalitiga ega. U 1986-yili Xarald Niderraytor tomondan yaratilgan. Bu tizimning McEliece kriptotizimidan farqi, uning tekshiruvchi matritsaning kodidan foydalanishidadir. Bu tizim elektron raqamli imzo yarata olib, rsa tizimini asosiy raqobatchisi va undan keeyingi asosiy nomzod hisoblanadi. Bu tizim shor algoritmi hujumiga o'ta bardoshliligi bilan RSA dan yaxshiroqdir.

Kalitni generatsiyalashi

1. Alisa (n, k) larni tanlaydi C kodni $CF(q)$ Galua maydoni asosida tanalydi.
2. Alias $(n - k) \times n$ tekshiruvchi H matritsani C kodi asosida generatsiya qiladi.
3. Alisa $GF(q)$ maydoni orqali $n \times n$ matritsani P ga mo'ljallab oladi. Va $(n - k) \times (n - k)$ ixtiyoriy tarzda olib uni hisoblab S ni chiqaradi.
4. Alisa $(n - k) \times n$ matritsani hisoblani hisoblaydi $H = shP$
5. Alisaning ochiq kaliti (H, t) , yopiq kaliti esa (s^{-1}, H, p^{-1})

Xulosa

Ushbu bitiruv ishini bajarish jarayonida shifrlash algoritmlari uchun kalitli axborotlarni generatsiya qilish masalalari tadqiq qilindi.

Shuningdek, shaxsiy kalitlarni generatsiya qilish va ularni himoyalash muammolari;

smart-kartalarda shaxsiy kalitlarni saqlash va ulardan foydalanish;

kalitlarni kartochkada va kartochkadan tashqarida generatsiya qilish kabi masalalar yoritilgan.

Bitiruv ishini bajarish jarayonida C# dasturlash tilida foydalanuvchilar uchun kalit juftligini yaratuvchi dastur tuzildi. Foydalanuvchilarni shaxsiy kalitlarini himoyalashda o‘rin almashtirish usulidan foydalangan holda kalitlarni shifrllovchi dastur tuzilgan. RSA algoritmida keltirilgan barcha matematik amallar dasturga kiritildi. Microsoft Visual Studio 2017 muhitining imkoniyatlaridan keng foydalanilgan tarzda dasturni konsol holatidan visual holatga olibkelindi.

Mazmunan xavfsizlik faoliyatiga falsaviy yondashadigan bo’lsak, xavf borligi uchun ham xavfsizlik bor. Buning jarayonning teskari jarayoni mantiqan to’g’ri kelmaydi. Biror bir axborotga tajovvuz bo’lmasa uning xavfsizligiga bo’lgan talab bo’lmaydi. Assimmetrik kriptotizimlar xozirgi kunlardagina o’z havfsizligini saqlab turibdi. Kvant kompyuterlari yaratilishi yillar o’tgan sari amalga oshirish mumkinligi yanada o’sib, assimmetrik kriptotizimlarning tanazzulga yuz tutish ehtimoli shunchalik oshmoqda. Ungacha esa assimmetrik kriptotizimlardan keng ko’llamda foydalanish mumkin. Bu butun dunyo uchun ayniqsa O’zbekiston Respublikasida qo’llanib kelinayotgan axborot texnologiyalarni xavfsizligi uchun katta muhim omildir. Xavfsizlik sferasida har bir kichik detalga global tarzda qarab yondashish lozim. Aynan kichik muammolar yig’ilib katta muammolarni yuzaga keltiradi. Shuning uchun ham ma’lumotning qiymatiga qarab uning assimmetrik kriptotizimlarning kalitlarini generatsiyalashda ularning bardoshlilik razryadiga katta e’tibor berish kerak bo’ladi.

FOYDALANILGAN ADABIYOTLAR RO'YXATI

1. I.A. Karimov «Yuksak manaviyat - Yengilmas kuch»
2. Akbarov D. Y. Axborot xavfsizligini ta'minlashning kriptografik usullari va ularning qo'llanilishi: Toshkent - «O'zbekiston markasi» nashriyoti - 2009.
3. Алферов А.П., Зубов А.Ю., Кузьмин А.С., Черемушкин А.В. Основы криптографии: Учебное пособие. – М.: Гелиос АРВ, 2002. – 480 с.
4. Ефремов П. Смарт-технологии в Интернете-ближайшая перспектива // Банковские технологии. -1997. -Июнь. -С. 108-109.
5. Иванов М.А. Криптографические методы защиты информации в компьютерных системах и сетях. -М.: КУДИЦ-ОБРАЗ, 2001. -363 с.
6. Лапонина О.Р. Основы сетевой безопасности: криптографические алгоритмы и протоколы взаимодействия: Курс лекций: Учебное пособие /Под ред. В.А. Сухомлина. -М.: Интернет-Ун-т Информ. Технологий, 2005. -604 с.
7. Мао, Венбо. Современная криптография. Теория и практика. Перевод с английского и ред. Д.А.Клюшина. -М.: Вильямс, 2005. -763 с.
8. Математические и компьютерные основы криптологии: Учебное пособие /Харин Ю.С., Берник В.И., Матвеев Г.В., Агиевич С.В. -Минск: Новое знание, 2003. -381с.
9. Молдовян А.А., Молдовян Н.А., Советов Б.Я. Криптография. – СПб.: Изд-во «Лань», 2001. – 224с.
10. Молдовян Н.А., Молдовян А.А. Введение в крипtosистемы с открытым ключом: Учебное пособие. -СПб.: БХВ-Петербург, 2005. -286с.
11. Полевой Н. Смарт-карта секретного доступа //Конфидент. 1997. №5. - С. 91-93.
12. Романец Ю.В., Тимофеев П.А., Шаньгин В.Ф. Защита информации в компьютерных системах и сетях. – М.: Радио и связь, 1999.
13. Рябко Б.Я., Фионов А.Н. Криптографические методы защиты информации: Учебное пособие для вузов. -М.: Горячая линия-Телеком. 2005. -229 с.