Z.T.XUDOYKULOV, O.ALLANOV,
I.M.BOYQUZIYEV, I.S.OLIMOV,
O.O.TURSUNOV, U.U.TOJIAKBAROVA

KRIPTOGRAFIYA 2

O‘ZBEKISTON RESPUBLIKASI RAQAMLI
TEXNOLOGIYALAR VAZIRLIGI

MUHAMMAD AL-XORAZMIY NOMIDAGI TOSHKENT
AXBOROT TEXNOLOGIYALARI UNIVERSITETI

Z.T.XUDOYKULOV, O.....
I.S.OLIMOV, O.O.TURSUNOV, U.U.TOJIAKBAROVA

KRIPTOGRAFIYA 2

O‘zbekiston Respublikasi Oliy va o‘rta maxsus ta'lim vazirligi tomonidan o‘quv qo‘llanma sifatida tavsiya etilgan

"LESSON-PRESS" nashriyoti
TOSHKENT 2023

UDK: 004.056.5(075.8)
UDK: 003.26(075)
BBK: 32.973.26-018

Taqrizchilar:

K.A.Tashev – texnika fanlari nomzodi, dotsent, Muhammad al-Xorazmiy nomidagi Toshkent axborot texnologiyalari universiteti ilmiy-ishlar va innovatsiyalar bo'yicha prorektori.

M.M.Kadirov – PhD, Islom Karimov nomidagi Toshkent davlat texnika universiteti Axborot texnologiyalari kafedrasi dotsenti.

Kriptografiya 2: *O'quv qo'llanma* / Z.T.Xudoykulov, O.M.Allanov, I.M.Boyquziyev, I.S.Olimov, O.O.Tursunov, U.U.Tojiakbarova; – T.: "LESSON-PRESS" nashriyoti", 2023. – 187 b.

O'quv qo'llanma Kriptografiya 1 nomli o'quv qo'llanmaning davomi bo'lib, unda sonlar nazariyasi muammolari, tub sonlar va ularni generatsiyalash usullari, ochiq kalitli shifrlash algoritmlari, ochiq kalitli shifrlarga asoslangan himoya mexanizmlari, elektron raqamli imzo tizimlari, kriptografik protokollar, tasodifiy qiymatlarni generatsiyalash usullari, statistik testlar to'plami, zamonaviy kriptografik protokollar, bulutli hisoblash tizimlarida foydalanilgan shifrlash algoritmalari hamda kvant kriptografiyasining nazariy va amaliy asoslari muhokama etilgan.

O'quv qo'llanma 5330300 – "Axborot xavfsizligi (sohalar bo'yicha)" yo'nalishi bo'yicha ta'lim olayotgan talabalar uchun tavsiya etiladi, hamda faoliyati axborot xavfsizligini ta'minlash bilan bog'liq bo'lgan mutaxassislarning keng doirasi uchun ham foydali bo'lishi mumkin.

MUHAMMAD AL-XORAZMIY NOMIDAGI TOSHKENT AXBOROT TEXNOLOGIYALARI UNIVERSITETINING 2023 YIL 29 AVGUSTDAGI 895-22-SONLI BUYRUG'IGA ASOSAN NASHR QILISHGA RUXSAT BERILDI

ISBN 978-9910-05-007-7

MUQADDIMA

So‘ngi yillarda axborot kommunikatsiya texnologiyalari sohasining jadal rivojlanishi turli manbalardan tez va osonlik bilan axborot olish imkoniyatini taqdim etmoqda. Davlat muassasalari, tijorat korxonalari va jismoniy shaxslar masofadan turib axborot xizmatlarini taqdim etmoqdalar va ulardan foydalanmoqdalar. Turli ma’lumotlarni, to‘lov haqidagi ma’lumotlar, tashkilotga oid ma’lumotlar va shaxsiy ma’lumotlarni tarmoq bo‘ylab uzatilishi, foydalanilayotgan axborot tizimiga ma’lum xavfsizlik talablarini shakllantirish zaruriyatini qo‘yadi.

Shu sababli axborotni ishlash, uzatish, saqlash jarayonida uning xavfsizligini ta’minlash maqsadida, mazkur soha bilan shug‘ullanuvchi xodimlar jalb qilinmoqda va ishonchli himoya mexanizmlaridan foydalanishga alohida e’tibor berilmoqda. Ishonchli himoyani ta’minlashda matematik isbotga asoslangan mexanizmlardan biri – *kriptografiya* hisoblanadi.

Keyingi yillarda kriptologiya yo‘nalishini rivojlantirishga davlatimiz tomonidan katta ahamiyat berilmoqda. Xususan, O‘zbekiston Respublikasi Prezidentining 2022-yil 28-yanvardagi PF-60-son “2022-2026-yillarga mo‘ljallangan Yangi O‘zbekistonning taraqqiyot strategiyasi to‘g‘risidagi” Farmonida “Kiberjinoyatchilikning oldini olish tizimini yaratish” maqsadi ham belgilangan.. Bundan tashqari, O‘zbekiston Respublikasi Prezidentining 2007-yil 3-aprelda qabul qilingan «O‘zbekiston Respublikasida axborotning kriptografik himoyasini tashkil etish chora-tadbirlari to‘g‘risida”gi PQ-614-son Qarorida belgilangan asosiy vazifalardan biri axborotni muhofaza qilish sohasida yuqori malakali kadrlarni tayyorlashdan iborat bo‘lib, buning uchun axborot xavfsizligi va kriptografiya yo‘nalishlarida davlat tilida ta’lim olayotgan talabalar, tadqiqotchilar va ilmiy xodimlar uchun mo‘ljallangan o‘quv qo‘llanmalar, darsliklar, uslubiy qo‘llanmalar va kitoblar chop etish muhim ahamiyat kasb etadi. Mazkur o‘quv qo‘llanma ana shu sohada bajarilgan ishlardan biri hisoblanadi.

Qo‘llanmaning birinchi bobida sonlar nazariyasiga oid muammolar, butun sonni faktorlash muammosi, diskret logarifmlash muammosi, elliptik egri chiziqda diskret logarifmlash muammosi va ularni yechish usullari haqida ma’lumotlar keltirilgan.

Ikkinchi bob ochiq kalitli shifrlash algoritmlari parametrlarini generatsiyalashga bag‘ishlangan hamda tub sonlarni generatsiyalash

usullari, tublikka tekshirishning birlamchi testlari, Solovay – Strassen testi, Rabin – Miller testiga oid ma'lumotlar keltirilgan.

Uchinchi bobda tasodifiy bitlar generatori, xususan, kriptografik psevdotasodifiy sonlar generatori, entropiya to'plovchilar, statistik testlar: DIEHARD testlar to'plami, NIST statistik testlar to'plami, tasodifiy ketma-ketliklarni entropiyasini o'lchash usullariga oid ma'lumotlar keltirilgan.

Qo'llanmaning to'rtinchi bobi ochiq kalitli shifrlash algoritmlariga bag'ishlangan bo'lib, unda RSA algoritmi, El-Gamal algoritmi, Diffi-Xellman kalitni ochiq taqsimlash algoritmi hamda takomillashgan ochiq kalitli shifrlash sxemalari haqida ma'lumotlar keltirilgan.

Beshinchi bob elektron raqamli imzo tizimlariga bag'ishlangan bo'lib, unda elektron raqamli imzo nima, uning xususiyatlari, ishlash prinsipi, klassik elektron raqamli imzo algoritmalari, elektron raqamli imzo standartlari va ochiq kalitli kriptografik tizimlardan foydalanishdagi muammolar haqida so'z yuritilgan.

Qo'llanmaning oltinchi bobida kriptografik protokollar haqida so'z boradi, xususan, kriptografik protokol, uning xususiyatlari, kriptografik algoritmlarni amalga oshirish usullari, dasturiy, apparat-dasturiy kriptografik himoya vositalari, sodda autentifikatsiya protokollari, SSH protokoli, SSL/TLS protokoli, IPSec protokoli haqida ma'lumotlar keltirilgan.

Yettinchi bob bulutli hisoblashda mavjud kriptografik algoritmlar, xususan, gomomorfik shifrlash usullari, attributga asoslangan shifrlash usullari, qidirish imkoniyatiga ega shifrlash, identifikatorga asoslangan shifrlash haqida ma'lumotlar keltirilgan.

Qo'llanmaning sakkizinchi bobi kvant kriptografiyasi asoslariga bag'ishlangan bo'lib, unda kvant nazariyasi, kvant kriptografiyasi asoslari, kvant kriptografiyasi protokollari hamda kvant kompyuterlari haqida ma'lumotlar keltirilgan.

I BOB. SONLAR NAZARIYASIGA OID MUAMMOLAR

Ushbu bobda ochiq kalitli kripografik tizimlarni yaratishda asos bo'lgan matematik muammolar bilan tanishib chiqiladi.

1.1. Butun sonni faktorlash muammosi

Simmetrik shifrlash algoritmlari ma'lumotni shifrlashda tezkor hisoblansada, ulardagi kalitlarni taqsimlash muammosini yechish uchun boshqa kriptografik algoritmlardan foydalanish talab etiladi. Mazkur muammoning yechimi klassik va zamonaviy algebrada olingan ilmiy natijalar asosida yaratilgan *ochiq kalitli kriptotizimlar*ning yaratilishi bilan hal etildi.

Ochiq kalitli shifrlash usullarini yaratishda odatda hozirda yechimi mavjud bo'lmagan matematik muammolardan foydalaniladi. Bu matematik muammolar odatda *bir tomonlama funksiya* sifatida ifodalanadi. Bir tomonlama funksiya deb, o'ziga teskari bo'lgan funksiya mavjud bo'lmagan funksiyaga aytiladi.

Ochiq kalitli shifrlash algoritmlarini yaratishda hozirda 1.1-jadvalda keltirilgan matematik muammolardan foydalanilmoqda.

1.1-jadval

Muammo turi bo'yicha ochiq kalitli kriptotizimlar tasnifi

Muammo	Bayoni
1	2
Faktorlash	Butun sonni faktorlash muammosi: butun musbat n soni berilgan, uning tub bo'lgan bo'luvchilarini topish kerak: ya'ni, $n = p_1^{e_1} p_2^{e_2} \cdots p_k^{e_k}$ ko'rinishda yozish kerak, bu yerda p^i - turli tub sonlar va har biri $e_i \geq 1$.
RSA muammosi (RSAP)	RSA muammosi (RSA inversiya kabi ma'lum): ikkita turli p va q toq sonlarning ko'paytmasi bo'lgan butun musbat n soni, $gcd(e,(p-1)(q-1)) = 1$ ga teng bo'lgan butun musbat e soni va butun c berilgan, shunday butun m ni topish kerakki, unda $m^e \equiv c(modn)$ bo'lsin.
Kvadratik chegirma muammosi (*Quadratic residuosity*	Kvadratik chegirma muammosi: toq murakkab butun n va $\left(\frac{a}{n}\right) = 1$ Yakobi belgisiga ega bo'lgan butun a soni berilgan, a soni n modul bo'yicha kvadratik chegirma ekanligi yoki chegirma emasligi aniqlansin.

Muammo	Bayoni
1	2
problem, QRP)	. .
n moduli bo'yicha kvadrat ildiz (*Square roots modulo*, SQROOT)	n moduli bo'yicha kvadrat ildiz: murakkab butun n soni va $a \in Q_n$ (n moduli bo'yicha kvadratik chegirma to'plami) berilgan, n moduli bo'yicha a dan shunday butun kvadratik ildiz x soni topilsinki, unda $x^2 = a(modn)$ bo'lsin.
Diskret logarifm muammosi (*Discrete logarithm problem*, DLP)	Diskret logarifm muammosi: tub son p uchun, chekli maydon Z_p^* da hosil qiluvchi (generator) element α hamda $\beta \in Z_p^*$ berilgan bo'lsa, shunday $0 \leq x \leq p-2$ bo'lgan butun x son topilsinki, unda $\alpha^x \equiv \beta(modp)$ bo'lsin, bu yerda x – daraja ko'rsatkichi.
Umumlashgan diskret logarifm muammosi (*Generalized discrete logarithm problem*, GDLP)	Umumlashgan diskret logarifm muammosi: n tartibli chekli siklik gruppa G, G ning hosil qiluvchisi α va $\beta \in G$ element berilgan, shunday $0 \leq x \leq n-1$ bo'lgan butun x soni topilsinki, unda $\alpha^x = \beta$ bo'lsin.
Diffi- Xellman muammosi (*Diffie-Hellman problem*, DHP)	Diffi-Xellman muammosi: tub son p, Z_p^* hosil qiluvchisi - α va $\alpha^a(modp)$ va $\alpha^b(modp)$ elementlari berilgan, $\alpha^{ab}(modp)$ topilsin.
Umumlashgan Diffi- Xellman muammosi (*Generalized Diffie-Hellman*	Umumlashgan Diffi-Xellman muammosi: chekli siklik gruppa G, G hosil qiluvchisi - α va gruppa elementlari α^a va α^b lar berilgan, α^{ab} topilsin.

Muammo	Bayoni
1	2
problem, GDHP)	
Qism to'plam -yig'indisi (*Subset sum problem*, SUBSET-SUM)	Qism to'plam-yig'indisi muammosi: butun musbat sonlar to'plami $\{a_1, a_2, \dots, a_n\}$ va butun musbat son S berilgan, yig'indisi S ga teng bo'lgan a_j qism to'plam mavjudligi yoki yo'qligi aniqlansin.
Elliptik egri chiziqda diskret logarifm muammosi (*Elliptic Curve Discrete Logarithm Problem*, ECDLP)	Elliptik egri chiziqli diskret logarifm muammosi: E elliptik egri chiziq, F_p chekli maydon va $P, Q \in E(F_p)$ nuqtalar berilgan. $Q = [k]P$ shartni qanoatlantiruvchi k butun sonni topish talab etiladi, agarda u mavjud bo'lsa.
Daraja parametri muammosi	*1-ta'rif.* Agar parametrli gruppa $(F_n; ®)$ da tashuvchi F_n ning elementi y berilgan bo'lsa, unda parametr R, daraja ko'rsatkichi e va element a topilsin. 2-ta'rif. Agar parametrli gruppa $(F_n; ®)$ da tashuvchi F_n ning elementlari va a berilgan bo'lsa, unda parametr R va daraja ko'rsatkichi e topilsin. Bu yerda F_n– n ta butun sonlardan tuzilgan chekli to'plam, $y \equiv a^{\backslash e} (mod\ n)$, \e – a ni parametr R bilan e-darajasi ramzi, $\varphi(n) > R > 1$, element a esa $a^{\backslash \omega} (mod\ n) \equiv 0$ shartini faqat $\omega = q$ bo'lgandagina qanoatlantiradi, $q - \varphi(n)$ ning butun sonli bo'luvchisi, $\varphi(n)$ – Eyler pi-funksiyasi, $n \in \{p, p_1 * p_2\}$, p, p_1, p_2 – tub sonlar.

Ko'plab ochiq kalitli kriptografik tizimlar butun sonni faktorlash muammosiga asoslanadi. Unga RSA, Rabin ochiq kalitli kriptotizimlarini

misol keltirish mumkin. Ushbu bo'limda ushbu muammoni yechish usullari bilan tanishib chiqiladi.

Butun sonni faktorlash muammosiga 1.1-jadvalda ta'rif berildi. Umumiy holda sonni tub yoki murakkab son ekanligini aniqlash muammosi, faktorlashga qaraganda oson hisoblanadi. Shu bois, sonni faktorlashdan oldin uni murakkabligini tekshirish talab etiladi. Sonlarni tublikka tekshirish usullari bilan keyingi bobda tanishib chiqiladi.

Mazkur muammoni yechishning qator usullari mavjud bo'lib, ularning barchasi dastlab sonning kichik tub bo'luvchilarini aniqlashga asoslanadi. Umumiy holda butun sonni faktorlash algoritmlarini *maxsus* va *umumiy* guruhlarga ajratish mumkin.

Birinchi guruhga oid algoritmlarning ishlash vaqti faktorlanuvchi sonning xususiyatlariga, uning o'lchami, shakli va h. bog'liq bo'ladi. Faktorlash uchun sarflangan vaqt esa foydalanilgan algoritmga bog'liq bo'ladi. Ushbu guruhga quyidagi algoritmlarni kiritish mumkin:

- birlamchi bo'lish (trial division);
- Pollardning Ro algoritmi (Pollard's rho);
- Elliptik egri chiziq algoritmi (elliptic curve algorithm);
- Pollardning $p-1$ algoritmi va h.

Boshqa tomondan, umumiy guruhga tegishli algoritmlarning ishlash vaqti faqat n sonining uzunligiga bog'liq bo'ladi. Ushbu guruhga tegishli algoritmlarga kvadratik g'alvir (quadratic sieve) va maydon g'alvirining umumiy soni (general number field sieve) algoritmlarini misol keltirish mumkin.

Maxsus guruhga tegishli algoritmlar samarali hisoblansada, har ikkala guruhga tegishli algoritmlardan ma'lum ketma-ketlikda foydalanish tavsiya etiladi. Quyida ushbu foydalanish tartibi keltirilgan:

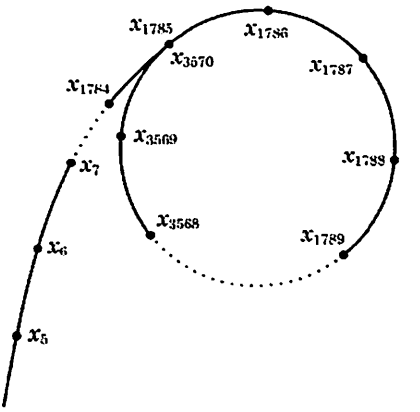
1. b_1 dan kichik bo'lgan tub sonlarga birlamchi bo'lish.
2. Shundan so'ng, Pollardning Ro algoritmini qo'llab b_2 ($b_2 > b_1$) dan kichik bo'lgan ixtiyoriy tub faktorlarni topish.
3. Elliptik egri chiziq algoritmini qo'llab b_3 ($b_3 > b_2$) dan kichik bo'lgan ixtiyoriy tub faktorlarni topish.
4. Va nihoyat, umumiy guruhga tegishli bo'lgan algoritmlardan birini qo'llash.

Birlamchi bo'lish. Olingan n sonini murakkabligini tekshirishda sarflanadigan vaqtni kamaytirish uchun dastlab "kichik" tub sonlarga bo'lish amalga oshiriladi. Bu yerda, "kichik" qiymat n sonining uzunligiga bog'liq bo'ladi. Tezkor holatda $\sqrt{n}$ gacha bo'lgan tub sonlarga

bo‘lish amalga oshiriladi. Agar ushbu holat amalga oshirilsa, n soni to‘liq faktorlanadi. Buning uchun esa, agar n soni o‘zaro teng uzunlikdagi ikki tub sonlarni ko‘paytmasi bo‘lsa, $\sqrt{n}$ marta bo‘lish talab etiladi. Masalan, faktorlanishi kerak bo‘lgan butun soni $n = 12$ ga teng bo‘lsa, uni bo‘luvchi sonlar 1, 2, 3, 4, 6, va 12 ga teng bo‘ladi. Ushbu ketma-ketlikdan eng yuqori darajali tub sonlarni tanlash orqali sonni faktorlash mumkin bo‘ladi: $12 = 3 \times 4 = 3 \times 2^2$.

Pollardning Ro algoritmi. Ushbu algoritm maxsus guruhga tegishli algoritm bo‘lib, murakkab sonning kichik faktorlarini topishga mo‘ljallangan. Ro algoritmi (ρ - algoritm) Jon Pollard tomonidan 1975 yilda, butun sonni faktorlash maqsadida taklif etilgan. Ushbu algoritm Floydning ketma-ketlikdagi sikl uzunligini aniqlash algoritmiga va tug‘ilgan kun paradoksining ba’zi xususiyatlariga asoslangan. Ushbu algoritm kichik ko‘paytuvchilardan iborat bo‘lgan murakkab sonlarni faktorlashda eng samarali usullardan hisoblanadi. Algoritm murakkabligi $O(N^{1/4})$ sifatida baholangan.

Pollardning Ro algoritmi biror n – elementidan boshlab siklni tashkil qiluvchi ketma-ketliklarni quradi. Ushbu holatni yunoncha ρ belgisi sifatida ifodalash mumkin (1.1-rasm).



1.1-rasm. Yunoncha ρ belgisi sifatida ifodalangan ketma-ketliklar

Faraz qilaylik $f: S \to S$ tasodifiy funksiya bo‘lsin (S chekli to‘plam bo‘lib, soni n ga teng). Bundan tashqari, x_0 element S ning tasodifiy elementi bo‘lsin va $x_0, x_1, x_2, \ldots$ ketma-ketliklar $i \geq 0$ uchun $x_{i+1} = f(x_i)$ orqali aniqlangan bo‘lsin. S to‘plam chekli bo‘lgani bois, ketma-ketlik siklik (takrorlanuvchan) bo‘ladi. Bunda sikl boshlanishigacha

bo'lgan ketma-ketlikdagi elementlar soni (ρ belgisining dumi) ko'pi bilan $\sqrt{\pi n/8}$ ga teng bo'lsa, siklning uzunligi ham ko'pi bilan $\sqrt{\pi n/8}$ ga teng bo'ladi. Sikl mavjud bo'lgani bois, turli o'rindagi elementlar o'zaro teng bo'ladi (kolliziya hodisasi, i va j o'rindagi elementlar teng bo'lishi: $x_i = x_j$) va bu holat turli kriptotahlil usullari, butun sonni faktorlash, diskret logarifmlash, uchun murakkablikni oshiradi. Kolliziya hodisasini topish uchun *Floydning ketma-ketlikdagi sikl uzunligini aniqlash algoritmi*dan foydalaniladi.

Ushbu algoritm "toshbaqa va quyon" ham deb nomlanib, Robert Floyd tomonidan taklif etilgan. Ushbu usulda, dastlabki (x_1, x_2) juftlikdan foydalangan holda biror m uchun $x_m = x_{2m}$ ga teng bo'lgunga qadar, iterativ tarzda (x_i, x_{2i}) lar hisoblanadi. Agar ketma-ketlikning "dumi" λ ga va siklning uzunligi μ ga teng bo'lsa, $m = \mu(1 + \lfloor \lambda/\mu \rfloor)$ holda birinchi $x_m = x_{2m}$ holat kuzatiladi. Bu yerda, $\lambda < m \leq \lambda + \mu$ o'rinli bo'lib, ushbu algoritmning ishlash vaqti $O(\sqrt{n})$ ga teng.

Faraz qilaylik, p soni n butun murakkab sonning tub ko'paytuvchisi bo'lsin. Pollardning Ro algoritmi n faktorlashda $i \geq 0$ uchun $x_0 = 2$, $x_{i+1} = f(x_i) = x_i^2 + 1 \; mod \; p$ tenglik bilan ifodalanuvchi $x_0, x_1, x_2, \ldots$ butun ketma-ketliklardan ikki marta takrorlangan elementlarni topishni amalga oshiradi. Floydning ketma-ketlikdagi sikl uzunligini aniqlash algoritmi $x_m \equiv x_{2m} (mod \; p)$ shartni qanoatlantiruvchi x_m va x_{2m} elementlarni topish uchun xizmat qiladi. p soni n butun murakkab sonning tub bo'luvchisi, biroq, u nomalum bo'lgani bois, bu $x_i \; mod \; n$ tenglikni hisoblash va $\gcd(x_m - x_{2m}, n) > 1$ shartni tekshirish orqali amalga oshiriladi. Agar $\gcd(x_m - x_{2m}, n) < n$ bo'lsa, n sonining trivial bo'lmagan faktori mavjud ($\gcd(x_m - x_{2m}, n) = n$ sharti o'rinli bo'lish ehtimoli juda past).

Pollardning Ro algoritmining ketma-ketligi quyida keltirilgan:

Pollardning Ro algoritmi

Kirish: tub sonning darajasi bo'lmagan murakkab n soni.

Chiqish: ± 1 va $\pm n$ ga teng bo'lmagan (trivial bo'lmagan) d faktorni topish.

1. $a \leftarrow 2, b \leftarrow 2$ ni o'rnatish.
2. $i = 1,2, \ldots$ lar uchun quyidagilarni hisoblash:

   2.1. $a \leftarrow a^2 + 1 \; mod \; n, \; b \leftarrow b^2 + 1 \; mod \; n, \; b \leftarrow b^2 + 1 \; mod \; n$ hisoblash.

   2.2. $d = \gcd(a - b, n)$ ni hisoblash.

2.3. Agar $1 < d < n$ bo'lsa, d ni qaytarish va siklni muvaffaqqiyatli tugatish.

2.4. Agar $d = n$ bo'lsa, siklni muvaffaqqiyatsiz tugatish.

$n = 455459$ ga teng holat uchun ushbu algoritmni amalga oshirilish tartibi quyida keltirilgan:

a	b	d
5	26	1
26	2871	1
677	179685	1
2871	155260	1
44380	416250	1
179685	43670	1
121634	164403	1
155260	247944	1
44567	68343	743

Shunday qilib, $n = 455459$ sonini faktorlari 743 va 455459/743=613 ga teng.

1.2. Diskret logarifmlash muammosi

Shunday x – butun son topilsinki: $a^x \equiv b(mod\ r)$ (1.1)

tenglik o'rinli bo'lsin. Bu yerda r-tub son va (1.1) tenglama (Z /pZ) gruppada qaraladi. (1.1) tenglamaning yechimi $x = log_a b$ - ni quyidagi formula orqali topish mumkin:

$$log_a b \equiv \sum_{j=1}^{p-2} (1 - a^j)^{-1} b^j \ (mod\ p-1)$$

Biroq, bu formula bilan yechimni topish masalasi bevosita «mumkin bo'lgan barcha holatlarni ko'rib chiqish» kabi usulga o'xshash bo'lgani uchun ham amalda bu formula qo'llanilmaydi. Quyida keltiriladigan algoritm esa hisoblashlar sonini qisqartirib yechimni topishning samarali usulini beradi.

Diskret logarifmlash algoritmi:

1-Qadam. Quyidagi son hisoblansin

$H := [p^{1/2}] + 1$

2-Qadam. Quyidagi son hisoblansin

$C \equiv a^H \pmod p$

3- Qadam. u, $0 \le u \le H$ sonli qiymatlari uchun $C^u \pmod p$ jadval tuzilsin. Bu qiymatlarni tartiblab chiqilsin.

4 – Qadam. Keyingi jadval esa $b*a^v \pmod p$, $0 \le v \le H$ qiymatlar uchun tuzilib tartiblansin.

5- Qadam. Birinchi va ikkinchi jadvalda teng chiqqan u, v elementlar olinsin.

6- Qadam. Javob sifatida

$x \equiv H*u - v \pmod{(p-1)}$

olinsin.

Misol 1. Quyidagi $3^x \equiv 15 \pmod{17}$ ifodadan x- ni toping.

Yechish: Bevosita tekshirib ko'rish mumkinki, x=6 bu tenglikni qanoatlantiradi. Haqiqatan $3^6 = 729$; $729 = 42*17 + 15$.

Shuni ta'kidlash kerakki bizni faqat butun yechimlar qiziqtiradi. Shuning uchun ham (1) ifodadan butun x-ni topish masalasi murakkab hisoblanadi.

Bu misolni yechish jarayoni yuqoridagi algoritm orqali quyidagicha amalga oshiriladi.

1-qadam. $H := [p^{1/2}] + 1$, $H = 5$.

2-qadam. $C \equiv a^H \pmod p$, $C = 3^5 \pmod{17} = 5$.

3-qadam. $5^u \pmod{17}$, $1 \le u \le 5$ jadval qiymatlarini hisoblaymiz:

$u = 1, 5 \pmod{17} = 5$

$u = 2, 25 \pmod{17} = 8$

$u = 3, 125 \pmod{17} = 6$

$u = 4, 625 \pmod{17} = 13$

$u = 5, 3125 \pmod{17} = 6$

Bu qiymatlarni tartiblasak: 5,6,8,13 .

4-qadam. $15*3^v \pmod{17}$, $0 \le v \le 5$ jadval qiymatlarini hisoblaymiz:

$v = 1, 45 \pmod{17} = 1$

$v = 2, 15*9 \pmod{17} = 16$

$v = 3, 15*27 \pmod{17} = 14$

$v = 4, 15*81 \pmod{17} = 8$

$v = 5, 15*243 \pmod{17} = 7$

Bu qiymatlarni tartiblasak: 7,8,11,14,16.

5-qadam. Ikkita jadval natijalari ustma-ust tushgan u, v – elementlarni tanlab olamiz.

Yani, u =2, v = 4.

6-qadam. Javob :

$$x \equiv H*u - v \pmod{(p-1)}$$

yani $x \equiv 5*2 - 4 \pmod{16} = 6 \pmod{16}$, $x = 6$.

Misol 2. Berilgan ifodadan x –ni toping

$3^x \equiv 7 \pmod{13}$.

Yechish. Bevosita tekshirib ko'rish mumkinki butun x-soni mavjud emas. Buni ham yuqoridagi algoritm orqali tekshiramiz : a = 3, b =7, p = 13

1)$H := [p^{1/2}] + 1$, H= 4.

2)$C \equiv a^H \pmod{p}$, $C = 3^4 \pmod{13} = 3$.

3)$3^u \pmod{13}$, $1 \le u \le 4$ jadval qiymatlarini hisoblaymiz:

u =1, $3 \pmod{17} = 3$

u=2, $9 \pmod{17} = 9$

u=3, $27 \pmod{17} = 10$

u=4, $81 \pmod{17} = 3$

4)$7*3^v \pmod{13}$, $0 \le v \le 4$ jadval qiymatlarini hisoblaymiz :

v= 0, $7 \pmod{13} = 7$

v=1, $21 \pmod{17} = 4$

v=2, $21*3 \pmod{17} = 12$

v=3, $7*27 \pmod{17} = 2$

v=4, $7*81 \pmod{17} = 4$

5)Ikkita jadval natijalari ustma-ust tushgan u, v –elementlarni tanlab olamiz. Biroq bunday qiymatlar mavjud emas ekan.

6)Javob butun yechim yo'q degan xulosaga kelamiz.

1.3. Elliptik egri chiziqda nuqtalarni qo'shish

So'nggi yillarda elliptik egri chiziqlar kriptografiyada keng tadbiq qilinmoqda. Bu bo'limda elliptik egri chiziqlar haqida umumiy ma'lumotlar, ularning koordinatalar sistemasidagi o'rni va xossalari, hamda ularda yotuvchi ratsional koordinatali nuqtalar ustida chekli maydonlarda bajariladigan amallar bilan tanishib chiqamiz.

Ta'rif. Biror K-chekli maydonda olingan elliptik egri chiziq deb, Veyershtrass tenglamasi deb ataluvchi quyidagi

$$y^2 + a_1xy + a_3y = x^3 + a_2x^2 + a_4x + a_6 (1.2)$$

tenglik orqali aniqlanuvchi egri chiziqqa aytiladi, bu yerda: $a_1, a_2, a_3, a_4, a_5, a_6 \in K$.

Elliptik egri chiziq odatda E yoki E/K bilan belgilanadi va elliptik egri chiziqqa tegishli nuqtalar, ya'ni (1.2) tenglama yechimlari shu elliptik egri chiziqning affin nuqtalari deyiladi.

Ta'rif.

Ushbu $E: f(x,y) = y + a_1xy + a_3y - x^3 - a_2x^2 - a_4x - a_6 = 0$ - elliptik egri chiziqqa tegishli bo'lgan $P(x_0, y_0) \in E$ nuqta silliq deyiladi, agar quyidagi shartlardan bittasi o'rinli bo'lsa:

$f_x'(x_0, y_0) \neq 0$ yoki $f_y'(x_0, y_0) \neq 0$. (1.3)

Ta'rif. E (yoki E/K) –elliptik egri chiziq silliq deb ataladi, agar uning har bir affin nuqtasi silliq bo'lsa.

Misol 1. $y^2 = x^3$-eliptik egri chiziq uchun (0;0) nuqta silliq nuqta emasligi ko'rsatilsin.

Yechish.

$f(x, y) = y^2 - x^3$, $f_x' = -3x^2$, $f_x' = 2y$

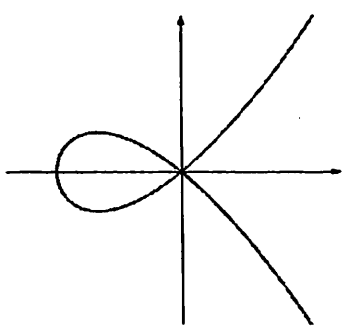
U holda (1.3) shartga nisbatan ziddiyatga kelamiz, natijada (0;0) nuqta haqiqatan ham silliq nuqta bo'la olmas ekan.

Misol 2. $y^2 = x^3 + x^2$ -eliptik egi chiziq uchun (0;0) nuqta silliq nuqta emas ekanligi ko'rsatilsin.

Haqiqatan,

$f(x,y) = y^2 - x^3 - x^2$, $f_x' = -3x^2 - 2x$, $f_y' = 2y$

bo'lib, (1.3) shartga nisbatan ziddiyatga kelamiz. Natijada (0; 0) nuqta haqiqatan ham silliq nuqta bo'la olmas ekan. Uning grafigi quyidagicha:



1.2-rasm. $y^2=x^3+x^2$ elliptik egri chiziq grafigi

Biz bundan keyin elliptik egri chiziqlarning umumiy kanonik ko'rinishi hisoblangan quyidagi tenglama bilan ish ko'ramiz:

$$y^2 = x^3 + ax^2 + bx + c, \qquad (1.4)$$

bu yerda $a, b, c \in Z$ va $p(x) = x^3 + ax^2 + bx + c$, ko'phad karrali ildizga ega emas deb qaraladi.

Elliptik egri chiziqlarning grafiklari. Yuqorida keltirilgan (1.4) ko'rinishdagi egri chiziq grafigiga ega bo'lish uchun

$$y = \sqrt{x^3 + ax^2 + bx + c}, \qquad (1.5)$$

chizish va Ox – o'qiga nisbatan simmetrik akslantirish lozim. (1.5) grafigini chizish uchun esa kvadrat ildizsiz ko'rinishdagi funksiya $z = x^3 + ax^2 + bx + c$ grafigini chizib olish kerak bo'ladi.

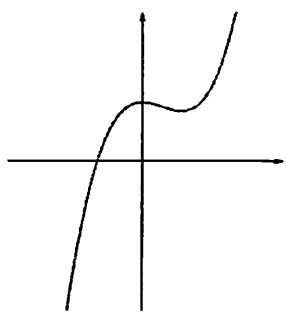
Yuqorida talab etilgan shartga muvofiq (1.4) funksiya Ox-o'qida karrali ildizga ega emas. U holda $x^3 + ax^2 + bx + c = 0$ uchinchi tartibli tenglama uchun Kordano formulasiga ko'ra yoki bitta, yoki uchta haqiqiy ildizga ega va bu ildizlar turlicha bo'ladi.

Demak, $y = x^3 + ax^2 + bx + c$ funksiya grafigi quyidagi ikkita holdan kelib chiqib ifodalanadi:

a) tenglama bitta yechimga ega, ya'ni funksiya grafigi Ox –o'qini bitta nuqtada kesib o'tadi;

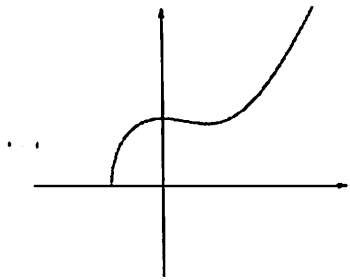
b) tenglama uchta yechimga ega, ya'ni funksiya grafigi Ox –o'qini uchta nuqtada kesib o'tadi.

Keltirilgan a) hol uchun $y = x^3 + ax^2 + bx + c$, funksiya grafigi quyidagi ko'rinishga ega:



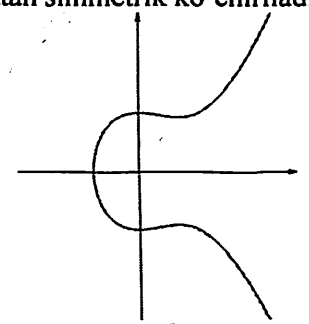
1.3-rasm. a holat uchün funksiya grafigi

Bu grafikdan (1.5) funksiya grafigini olish uchun, kvadrat ildiz ostidagi ifodaning manfiy bo'lmagan qiymatlar sohasiga mos keluvchi - aniqlanish sohasi qismini



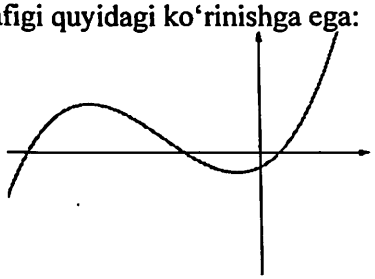
1.4-rasm. $y = \sqrt{x^3 + ax^2 + bx + c}$ *funksiya grafigi*

Ox - o'qiga nisbatan simmetrik ko'chiriladi, ya'ni:



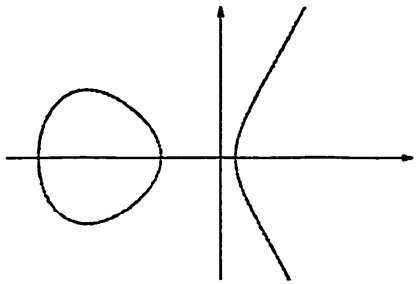
1.5-rasm. $y^2 = x^3 + ax^2 + bx + c$ *funksiya grafigi*

Uchta haqiqiy ildizga ega bo'lgan b) hol uchun $z = x^3 + ax^2 + bx + c$, funksiya grafigi quyidagi ko'rinishga ega:



1.6-rasm. b holat uchun funksiya grafigi

Xuddi yuqoridagi fikr va mulohazalarga ko'ra bu grafikdan (1.5) funksiya grafigini olish uchun, kvadrat ildiz ostidagi ifodaning manfiy bo'lmagan qiymatlar sohasiga mos keluvchi - aniqlanish sohasi qismini Ox - o'qiga nisbatan simmetrik ko'chiriladi, natijada grafik ellips va giperboladan iborat bo'lgan ikkita qismlar bilan ifodalanadi:



1.7-rasm. (1.5) tenglik grafigi

Elliptik egri chiziqqa tegishli ratsional nuqtalarni aniqlash usullari. Hozirgi kunda $y^2 = x^3 + ax^2 + bx + c$, tenglamaning barcha ratsional yechimlarini topish matematikada noma'lumligicha qolib kelmoqda. Lekin, bugungi kunda kriptografiya fanida unchalik effektiv bo'lmasa ham quyidagi ikkita usuldan foydalaniladi. Quyida ushbu usullar bilan batafsil tanishamiz.

1- usul. Tanlangan $y^2=x^3+ax+b$ tenglamaga x_i qiymatlar berib, tenglamaning o'ng tomoni to'la kvadrat tashkil qilishi tekshiriladi. Agar qandaydir x_k qiymatda to'la kvadrat tashkil qilsa, u holda tenglamaga tegishli nuqta koordinatalarini

$$(x_k;y_k = \pm\sqrt{x_k^3 + ax_k + b}) \qquad (1.6)$$

juftliklar bilan fiksirlanadi. Bu usul tenglama koeffisentlariga biror shart avvaldan berilgan holda yaxshi natija beradi. Ya'ni koeffisentlarga mos tenglama xosil qilib, shu tenglamaga tegishli nuqta qidirish usuli hisoblanadi.

Misol:

$a = 2, b = -3$ bo'lsin, ya'ni tenglama: $y^2 = x^3 + 2x - 3$ ko'rinishga ega. (1.5) formulaga ko'ra, $x = 2$ bo'lganda, $y = \sqrt{2^3 + 2 * 2 - 3} = 3$.

Demak, $y^2 = x^3 + 2x - 3$ tenglama *P(2, 3)* ratsional nuqtaga ega.

2- usul. Bu usul topilishi kerak bo'lgan nuqtaga biror shart qo'yilganda foydalaniladigan usul hisoblanadi. Ya'ni nuqta koordinatalari (x,y) va tenglamaning bitta *a*–koeffisentini fiksirlab: $(a, x, y \in R)$,

$$b = y^2 - x3^3 - ax \qquad (1.7)$$

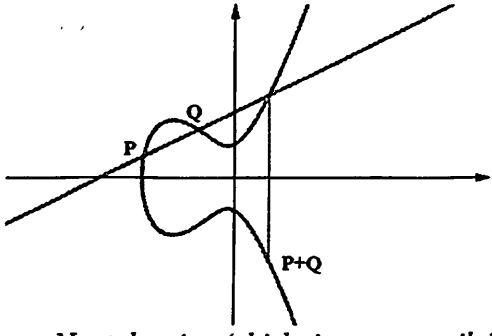
formula orqali *b*–koeffisiyent hisoblanib topiladi va shu koeffisent asosida tenglama quriladi. Buni quyidagi misolda ko'rish mumkin.

Misol: Agar $a = 2, P(x,y) = (1,2)$ berilgan bo'lsa, u holda (1.7) formulaga ko'ra: $b = 2^2 - 1^3 - 2 * 1 = -1$.

Demak, *P(1, 2)* nuqta $y^2 = x^3 + 2x - 1$ ga tegishli ratsional nuqta hisoblanadi.

Elliptik egri ,chiziqlarning ratsional nuqtalarini qo'shish. $E: y = x^3 + ax^2 + bx + c$, elliptik egri chiziqda $P(x_1, y_1)$, $Q(x_2, y_2)$ nuqtalar berilgan bo'lsin. Bu nuqtalar orqali to'g'ri chiziq o'tkazamiz. U holda o'tkazilgan chiziq, *E*- egri chiziqni uchinchi nuqtada kesib o'tadi. Bu $B(x_3, y_3)$ nuqtani Ox - o'qiga simmetrik ko'chiramiz va hosil bo'lgan:

$B'(x_3, -y_3) = P(x_1, y_1) + Q(x_2, y_2)$ nuqtani, $P(x_1, y_1)$ va $Q(x_2, y_2)$ nuqtalarning elliptik egri chiziq ustida qo'shish deb e'lon qilamiz:



1.8-rasm. Nuqtalarni qo'shishning geometrik ifodalanishi

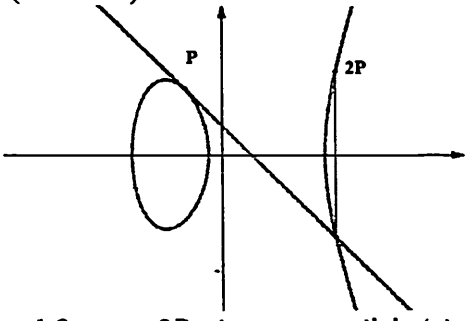
1.8-rasmda $x^3 + ax^2 + bx + c = 0$ tenglama bitta yechimga ega bo'lgan hol uchun misol sifatida keltirilgan.

Izoh. Albatta har doim ham $P(x_1, y_1)$ va $Q(x_2, y_2)$ nuqtalar orqali o'tuvchi chiziq *E*-egri chiziqni uchinchi nuqtada kesib o'tavermaydi. Masalan, o'tkazmoqchi bo'layotgan chiziq ikkita nuqta orqali Ox -o'qiga vertikal bo'lib qolsa, u holda egri chiziqni uchinchi nuqtada kesib o'tmaydi (1.10-rasm).

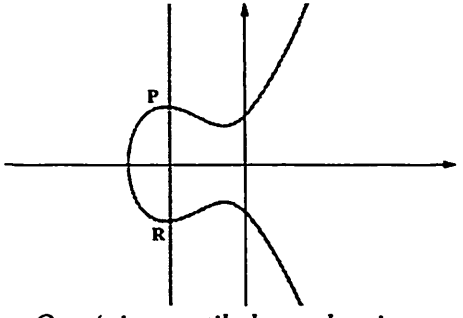
Ikkita nuqta orqali o'tuvchi chiziq egri chiziqni uchinchi nuqtada kesib o'tmaydigan holi alohida ko'rib o'tiladi.

Demak, $P(x_1, y_1) \neq Q(x_2, y_2) \neq 0$ bo'lganda ularning yig'indisini $P(x_1, y_1) + Q(x_2, y_2)$ topish ko'rib chiqildi. $P + P =?$ qanday amalga oshiriladi? Buning uchun elliptik egri chiziqdagi *P* -nuqta orqali urinma chiziq o'tkaziladi. Bu urinma chiziq elliptik egri chiziq grafigidagi ikkinchi qismni (giperbola qismida) biror nuqtada kesib o'tadi. Ana shu kesib o'tgan nuqtani Ox -o'qiga simmetrik ko'chiriladi va bu nuqtani $2P$

deb e'lon qilinadi (1.9-rasm):



1.9-rasm. 2P-ning geometrik ko'rinishi



1.10-rasm. Ox o'qiga vertikal nuqalarni geometrik ko'rinishi

Xuddi shunday, $3P$-ni topish uchun, $3P = P + 2P$ va hokazo, $4P = P + 3P$, $5P = 4P + P$ nuqtalarni topish ham yuqoridagi kabi amalga oshiriladi.

Elliptik egri chiziqning nuqtalarini qo'shish formulalari. Yuqorida ko'rib o'tilganlarga muvofiq, agar $P, Q \in E$ nuqtalar bo'lsa. Ular orqali kesuvchi chiziq o'tkazib, bu kesuvchi chiziq E -egri chiziqni biror uchinchi $R(x_3, y_3)$ nuqtada kesib o'tadi.

Tasdiq. Agar $P, Q \in E$ nuqtalar ratsional nuqtalar bo'lsa, u holda $R(x_3, y_3)$ nuqta ham ratsional nuqta bo'ladi.

Isboti. $P, Q \in E$ nuqtalar orqali o'tuvchi chiziq umumiy ko'rinishi: $y = kx + d$ bo'lib, bu yerda k, d – hozircha noma'lum. Bu noma'lumlar quyidagicha topiladi, ya'ni $P(x_1, y_1)$, $Q(x_2, y_2)$ nuqtalardan $y = kx + d$ chiziq o'tadi. Bundan esa quyidagilar kelib chiqadi:

$$\begin{cases} y_1 = kx_1 + d \\ y_2 = kx_2 + d \end{cases} \Rightarrow y_1 - y_2 = k(x_1 - x_2) \quad k = \frac{y_1 - y_2}{x_1 - x_2}$$

Shuningdek,

$$d = y_1 - kx_1 = y_1 - \left(\frac{y - y_2}{x - x_2}\right) \cdot x_1 = \frac{y_2x_1 - y_1x_2}{x_1 - x_2}$$

o'rinli. Demak, biz $u = k\,x + d$ chiziqni tiklab oldik. Keyingi qadamda, $u = kx+d$–ni $y^2 = x^3 + ax^2 + bx + c$, elliptik egri chiziq tenglamasiga olib borib qo'yamiz, ya'ni

$$(kx + d)^2 = x^3 + ax^2 + bx + c,$$
$$x^3 + (a - k^2)x^2 + (b - 2kd)x + c - d^2 = 0,$$

u holda uchinchi tartibli tenglama uchun Viyet teoremasiga ko'ra:

$$x_1 + x_2 + x_3 = k^2 - a$$

bo'lib, bu oxirgi tenglikda x_1, x_2 ratsional sonlar, u holda x_3 - ham ratsional, hamda $y_3 = kx_3 + d$ ifodadan esa y_3 ham ratsional bo'ladi. Demak, tasdiq isbot qilindi.

Bu keltirilgan tasdiq isbotidan esa $P + Q$ yig'indi nuqta koordinatasini hisoblash formulasini keltirib chiqarish mumkin. $P + Q$ nuqta R – nuqtani Ox - o'qiga simmetrik ko'chirishdan hosil bo'lar edi. Natijada biz qidirayotgan nuqtaning koordinatalarini (u, v)–deb belgilasak, bu koordinatalar quyidagi formulalar orqali topiladi:

$$u = k^2 - a - x_1 - x_2,$$
$$v = -ku - d = -(k(u - x_1) + y_1),$$

chunki $u = x_3, v = -y_3$. Bu formulalarga $k = \frac{y_1 - y_2}{x_1 - x_2}$ ifoda qo'yilsa:

$$\begin{cases} v = \frac{y_1 - y_2}{x_1 - x_2}(-u + x_1) - y_1. \\ u = \frac{(y_1 - y_2)^2}{(x_1 - x_2)^2} - (a + x_1 + x_2), \end{cases} \tag{1.8}$$

tengliklarga ega bo'lamiz. Bu formulalar $x_1 \neq x_2$ bo'lganda ma'noga ega bo'ladi.

Agar $x_1 = x_2$ bo'lsa, $y = kx + d$ chiziq sifatida urinma o'tkazilib, quyidagicha formulaga kelamiz:

$$\begin{cases} u = -2x_1 - a + \frac{(3x_1^2 + 2ax_1 + b)^2}{4y_1^2}, \\ v = -y_1 - \frac{3x_1^2 + 2ax_1 + b}{2y_1}(u - x_1). \end{cases} \tag{1.9}$$

Shunday qilib, hech bo'lmasa bitta P- ratsional nuqta elliptik egri chiziqdagi nuqta bo'lsa, u holda (1.8), (1.9) formulalar orqali $2P, 3P, 4P, \ldots$ va hokazolarni topish mumkin ekan.

Shuni alohida ta'kidlash kerakki, (1.8) va (1.9) formulalar (1.4) tenglamaga nisbatan keltirib chiqarildi. Endi elliptik egri chiziqning kriptografiyada keng qo'llaniladigan $y^2 = x^3 + ax + b$ tenglamasi uchun ratsional nuqtalarini qo'shish formulalarini keltirib o'tamiz:

$$\begin{cases} u = \frac{(y_1-y_2)^2}{(x_1-x_2)^2} - x_1 - x_2, \\ v = -y_1 + \frac{y_1-y_2}{x_1-x_2}(x_1-u). \end{cases} \quad (1.10)$$

bu yerda, $x_1 \neq x_2$.

Agar $x_1 = x_2$ bo'lsa, u holda

$$\begin{cases} u = \frac{(3x_1^2+a)^2}{4y_1^2} - 2x_1, \\ v = -y_1 - \frac{3x_1^2+a}{2y_1}(x_1-u). \end{cases} \quad (1.11)$$

Misol -3. Agar elliptik egri chiziq tenglamasi $y^2 = x^3 - 2$, undagi nuqta $P(3,5)$ bo'lsa, u holda ushbu nuqtalar: $2P = ?, 3P = ?, 4P = ?, 5P = ?$ topilsin.

Yechish. Yuqoridagi (1.9) formulaga muvofiq:

$$y^2 = x^3 + ax^2 + bx + c, a = 0, b = 0;$$

$$u = -2x_1 - a + \frac{(3x_1^2+2ax_1+b)^2}{4y_1^2} = \frac{129}{100};$$

$$v = -y_1 - \frac{3x_1^2+2ax_1+b}{2y_1}(u-x_1) = -\frac{383}{100};$$

demak, $2P = \left(\frac{129}{100}; -\frac{383}{100}\right)$.

Natijada (1.9) formuladan foydalanib: $3P, 4P, 5P$ – larni hisoblash mumkin, yani $u_n = nP$ – nuqtaning birinchi koordinatasini olsak, u holda:

$$u_1 = 3, u_2 = \frac{129}{100}, u_3 = \frac{164323}{29241}$$

$$u_4 = \frac{2340922881}{58675600}, u_5 = \frac{307326105747363}{160280942564521}$$

Shu hisoblashlarni davom ettirsak, u_{11} ga borganda 71 xonali songa to'qnash kelamiz.

1.4. Elliptik egri chiziq nuqtasi tartibi

Oldingi bo'limda agar $P \in E$ bo'lsa, nP – ni topish, ya'ni

$$nP = P + P + \ldots\ldots + P$$

ko'rib chiqilgan edi. Biroq bu qo'shish jarayonida quyidagi ikkita holat bo'lishi mumkin:

1. Biror n – chi qadamda $nP = 0$ tenglik bajarilishi mumkin;
2. $2P, 3P, 4P$ va hokazo nP – nuqtalar har xil qiymatga ega bo'lishi mumkin.

Ta'rif. Agar $mP \neq 0$, barcha $m < n$ bajarilib, $nP = 0$ bo'lsa, u holda P – nuqta n – chekli tartibga ega deyiladi.

Misol. $y^2 = x^3 + 4$, $P(0,2)$ nuqta $n = 3$ tartibli ekanligi ko'rsatilsin.

Yechish. Haqiqatan $a = b = 0$, (1.8) formulaga ko'ra:

$$u = 0$$

$$v = -2$$

$$2P = (0;-2), 3P = 2P + P = (0;-2) + (0;2) = (0;0)$$

bu esa elliptik egri chiziq nuqtasi tartibi ta'rifi bilan ustama-ust tushdi, ya'ni $n=3$ ekan. Bevosita tekshirib ko'rish mumkinki:

1) $y^2 = x^3 + 1, P(2,3), n = 6.$

2) $y^2 = x^3 - 43x + 166, P(3,8), n = 7.$

Izoh. 1901 yilda fransuz matematigi A.Puankare (1854- 1912) quyidagi gipotezani ilgari surgan.

Gipoteza. Har doim cheksiz tartibli $P_1, P_2, \ldots\ldots P_k$ chekli ratsional nuqtalar topish mumkinki, har qanday P- ratsional nuqta shu ratsional nuqtalar orqali ifodalanadi:

$$P = n_1P_1 + \ldots\ldots + n_kP_k + Q,$$

Bu yerda $n_1, \ldots . n_k$ - butun sonlar P – nuqta uchun bir qiymatli aniqlanadi, Q – esa chekli tartib ega bo'lgan nuqta. Bu yerdagi k - soni egri chiziq rangi deyiladi.

1922 yilda ingliz matematigi L.Mordell, Puankare gipotezasi isbotini keltiradi. Biroq, bu isbot egri chiziq rangini topishning usulini bermas edi. Faqatgina 1995 yilda elliptik egri chiziq rangini juda murakkab analitik konstruksiya yordamida topish mumkinligi ko'rsatildi.

Ta'rif. E EECh ga tegishli bo'lgan P nuqtaning tartibi deb $[k]P = O$ shartni bajaruvchi eng kichik natural k soniga aytiladi.

Nuqtalarni qo'shish quyidagi xossalarga ega:

0. $[0]P = O$;
1. $[1]P = P$;
2. $[n + m]P = [n]P + [m]P$;
3. $[-n]P = -([n]P)$.

Ma'lumki, agar $z \neq 0$ bo'lsa, $y^2 = z(mod\, p)$ tenglama ikkita yechimga ega bo'lishi mumkin. Agar bu yechimlar y_1 va y_2 bo'lsa, u holda $y_1 = -y_2$ tenglik bajariladi. Agar $y_2 < 0$ bo'lsa, u holda $y_2 + p$ ham yuqoridagi tenglamaning yechimi bo'ladi.

Teorema 1. P va $(-P)$ nuqtalarning tartiblari teng bo'ladi.

Misol 1. F_{97} maydon ustida aniqlangan $y^2 = x^3 + 46x + 74$ EECh larning nuqtalarini tartiblarini topamiz. Biz uni quyidagi jadvalda keltiramiz.

x	y_1	y_2	$ord(P)$
1	11	86	16
4	15	82	4
6	9	88	80
8	9	88	40
9	21	76	10
10	46	51	8
15	29	68	80
19	12	85	80
20	19	78	80
22	26	71	8
24	8	89	40
27	12	85	16
30	18	79	40
32	48	49	40
34	28	69	80
35	6	91	20
37	7	90	80
43	46	51	80
44	46	51	80
46	2	95	20
49	45	52	5
51	12	85	10
52	22	75	80
57	0	0	2
60	14	83	40
63	25	72	40
64	35	62	16
65	47	50	40
66	24	73	20
67	42	55	80
70	2	95	80
75	32	65	20
76	41	56	80
78	2	95	80
83	9	88	16
85	5	92	80
88	17	80	40

90	31	66	5
94	43	54	80
96	30	67	80

Berilgan maydonning koordinatalar tekisligida nuqtalari soni 9410 ga teng. Yuqoridagi jadvaldan EECh ga tegishli nuqtalar soni 81 ta ekanligi kelib chiqadi (nol nuqta bilan birga). Demak, tekislikdagi barcha nuqtalar EECh ga tegishli bo'lmas ekan, ya'ni x ning barcha qiymatlarida $y^2 = x^3 + 46x + 74(mod\ 9\ 7)$ tenglama yechimga ega bo'lavermaydi. Masalan, $x = 2$ hol uchun. Agar bu qiymatni tenglamaga olib borib qo'yilsa $y^2 = 77(mod\ 9\ 7)$ tenglamaga kelinadi. Bu tenglama yechimga ega yoki yo'qligini aniqlash uchun Lejandr simvolidan foydalaniladi:

$$L\left(\frac{77}{97}\right) = (-1)^{\frac{77-1}{2}\frac{97-1}{2}} L\left(\frac{97}{77}\right) = L\left(\frac{20}{77}\right) = L\left(\frac{4\cdot 5}{77}\right) =$$

$$(-1)^{\frac{77-1}{2}\frac{5-1}{2}} L\left(\frac{77}{5}\right) = L\left(\frac{2}{5}\right) = (-1)^{\frac{5^2-1}{8}} = -1$$ Demak, $x = 2$ holda $y^2 = 77(mod\ 9\ 7)$ tenglama yechimga ega emas ekan.

Yuqorida ko'rib o'tganimizdek F maydon ustida aniqlangan E EECh unda aniqlangan qo'shish amaliga nisbatan gruppa tashkil etar ekan. Bu EECh ga tegishli nuqta qism gruppa tashkil etishini quyidagi teorema aniqlaydi.

Teorema 2. Bizga E elliptik egri chiziqqa tegishli bo'lgan P nuqta berilgan bo'lib, uning tartibi $ord(P) = n$ tub bo'lsin. U holda $\langle P\rangle = \{O, P, [2]P, [3]P, \ldots, [n-1]P\}$ to'plam $E(F)$ ning siklik qism gruppasi bo'ladi.

Misol 2. F_{29} maydon ustida aniqlangan $E: y^2 = x^3 + 4x + 20$ EECh berilgan bo'lsin. $P = (1,5)$ nuqtaning tartibi 37 ga teng bo'lib, bu nuqta aniqlagan qism gruppa $E(F_{29})$ gruppaning o'zi bilan ustma-ust tushadi, ya'ni bu nuqta $E(F_{29})$ gruppaning generatori bo'ladi.

$[0]P = O$	$[8]P = (8,10)$	$[16]P = (0,22)$	$[24]P = (16,2)$	$[32]P = (6,17)$
$[1]P = (1,5)$	$[9]P = (14,23)$	$[17]P = (27,2)$	$[25]P = (19,16)$	$[33]P = (15,2)$
$[2]P = (4,19)$	$[10]P = (13,23)$	$[18]P = (2,23)$	$[26]P = (10,4)$	$[34]P = (20,26)$
$[3]P = (20,3)$	$[11]P = (10,25)$	$[19]P = (2,6)$	$[27]P = (13,6)$	$[35]P = (4,10)$
$[4]P = (15,27)$	$[12]P = (19,13)$	$[20]P = (27,27)$	$[28]P = (14,6)$	$[36]P = (1,24)$
$[5]P = (6,12)$	$[13]P = (16,27)$	$[21]P = (0,7)$	$[29]P = (8,19)$	
$[6]P = (17,19)$	$[14]P = (5,22)$	$[22]P = (3,28)$	$[30]P = (24,7)$	

$[7]P = (24,22)$ $[15]P = (3,1)$ $[23]P = (5,7)$ $[31]P = (17,10)$

Ko'rib o'tganimizdek F maydon ustida aniqlangan E elliptik egri chiziqning nuqtalari $F \times F = \{(x,y): x,y \in F\}$ to'plamning qism to'plami bo'ladi. Demak, E elliptik egri chiziqning nuqtalari tashkil etgan gruppa $F \times F$ ning qandaydir qism to'plamiga teng bo'ladi. Bu qism to'plamni aniqlash uchun bizga quyidagi teorema yordam beradi. $(A,*)$ va $(B,\circ)$ algebraik strukturalar berilgan bo'lsin. Ularning to'g'ri yig'indisi deganda $A \oplus B = \{(x,y): x \in A, y \in B\}$ to'plamga aytiladi va bu to'plam ham algebraik struktura bo'ladi. Bu algebraik strukturada amal quyidagicha aniqlanadi: $(x_1,y_1) \oplus (x_2,y_2) = (x_1 * x_2, y_1 \circ y_2)$.

Teorema 3. E elliptik egri chiziq F_q maydon ustida berilgan bo'lsin. Bu maydon nuqtalari aniqlagan $E(F_q)$ gruppa $Z_{n_1} \oplus Z_{n_2}$ ga izomorf bo'ladi, bu yerda n_1 va n_2 lar bir qiymatli aniqlangan va n_2 soni n_1 va $q-1$ larning bo'luvchisi.

$y^2 = x^3 + ax^2 + bx + c$ -elliptik egri chiziq ratsional nuqtalarini topishning effektiv usulini topish hozirgi kunda sonlar nazariyasining muhim muammolaridan biri hisoblanadi. Biroq egri chiziqqa tegishli bitta nuqta topilsa, qolganlari 1.3 - bo'limda keltirilgan formulalar orqali aniqlanadi.

Bugungi kunda EECh ning nuqtalari soni $\#E(F_p)$ ni hisoblashning Shuf (Rene Schoof, 1985) metodi va uning modifikasiyalangan varianti bo'lgan SEA algoritmlari mavjud. Shuf metodi EECh ning nuqtalari sonini topishning birinchi polinomial metodi hisoblanadi va uning qiyinchilik darajasi p modul bo'yicha $O(log^6 p)$ ta operasiyaga teng. Ushbu metodni tushunishda muhim tushuncha va teoremalar bilan tanishib chiqamiz..

Teorema 4. $\#E(F_p)$ uchun

$$p + 1 - 2\sqrt{p} \le \#E(F_p) \le p + 1 + 2\sqrt{p}$$

tengsizliklar o'rinli.

Demak, $\#E(F_p) = p + 1 - t$ deb olishimiz mumkin, bunda $|t| \le 2\sqrt{p}$ bo'lib u $\#E(F_p)$ uchun Frobenuis izi deb ataladi.

$\#E(F_p)$ hisoblashning asl mohiyatini tushunish uchun uning eng oddiy usulini keltiramiz. $\#E(F_q)$ ***ni hisoblashning oddiy usuli.*** Bu usulda avvalo har bir $x \in F_q$ uchun $z = x^3 + ax + b$ hisoblanadi va z ning F_q maydonda kvadratik chegirma ekanligi tekshiriladi. Agar $z = 0$

bo'lsa, u holda $(x,0) \in E$ bo'ladi. Agar shunday $y \in F_q$ topilib, $y^2 \equiv z(mod\, p)$ tenglik o'rinli bo'lsa, u holda bu tenglikni qanoatlantiruvchi va absissasi x ga teng faqat ikkita nuqta mavjud, ya'ni $(x,y),(x,-y) \in E$ munosabat o'rinli bo'ladi. EECh dagi nuqtalar sonini aniqlashda quyidagi teorema o'rinli.

Teorema 5. F_p maydonda aniqlangan $y^2 = x^3 + ax + b$ EECh ning nuqtalari soni $\#E(F_p) = p + 1 + \sum_{x=0}^{p-1}\left(\frac{x^3+ax+b}{p}\right)$ ga teng, bu yerda $(\cdot)$ – Lejandr simvoli.

Lekin, bu usulni p juda kichik tub son bo'lgan holda ECh ning nuqtalar sonini topishda qo'llash mumkin.

Ma'lumki $m \geq 3$ hol uchun $[m]P$ nuqtaning koordinatalarini hisoblash juda ko'p amallarni bajarishni talab qiladi. EECh da $[m]P$ hisoblashning rekursiv formulasi ham mavjud, ya'ni $m \geq 2$ va $P = (x,y)$ bo'lsa

$$[m]P = \left(\frac{\psi_m^2 x - \psi_{m-1}\psi_{m+1}}{\psi_m^2}, \frac{\psi_{m+2}\psi_{m-1}^2 - \psi_{m-2}\psi_{m+1}^2}{4y\psi_m^3}\right) \qquad (1.12)$$

formula o'rinli bo'ladi, bunda

$$\psi_{-1} = -1,\ \ \psi_0 = 0,\ \ \psi_1 = 1,\ \ \psi_2 = 2y,\ \ \psi_3 = 3x^4 + 6ax^2 + 12bx - a^2,$$

$$\psi_4 = 4y(x^6 + 5ax^4 + 20bx^3 - 5a^2x^2 - 4abx - 8b^2 - a^3),$$

$$\psi_{2m+1} = \psi_{m+2}\psi_m^3 - \psi_{m-1}\psi_{m+1}^3,\ m \geq 2,\ m \geq 3$$

bo'lib, $\psi_m(x,y)$ ko'phad m -tartibli bo'luvchi ko'phad deb ataladi. Barcha ψ bo'luvchi ko'phadlarning koeffisentlari p modul bo'yicha hisoblanadi. Yuqorida keltirilgan rekursiv formulaga ko'ra m -tartibli bo'luvchi ko'phadni hisoblashni $O(log\, m)$ qadamda bajarish mumkin. Eslatib o'tamizki m toq bo'lgan hollar uchun ψ_m ko'phad faqat x o'zgaruvchiga bog'liq bo'lib qoladi.

Teorema 6. $\psi_n(x,y) = 0$ tenglik faqat va faqat tartibi n ga karrali bo'lgan $P = (x,y)$ nuqtalar uchun bajariladi.

Ma'lumki, F_p maydon ustida berilgan $y^2 = x^3 + ax + b$ EECh uchun Xasse teoremasidan $\#E(F_p) = p + 1 - t$ ga egamiz. Quyidagi teorema $\#E(F_p) = p + 1 - t$ tenglikdagi p va t parametrlar orasidagi bog'lanishni ifodalaydi.

$\varphi_q((x,y)) = (x^q, y^q)$ tenglik bilan aniqlanuvchi $\varphi_q: E(\overline{F_q}) \to E(\overline{F_q})$ akslantirish ***Frobenuis endomorfizmi*** deyiladi. Har qanday $P \in$

$E(\overline{F}_q)$ nuqta uchun $\varphi_q^2 - t\varphi_q + q = 0$ tenglik o'rinli. Boshqacha aytganda quyidagi teorema o'rinli bo'ladi.

Teorema 7. (Frobenuis endomorfizmining xossasi). Ixtiyoriy $P(x,y) \in E_p(a,b)$ uchun quyidagi tenglik o'rinli bo'ladi

$$(x^{p^2}, y^{p^2}) + [p](x,y) = [t](x^p, y^p), \qquad (1.13)$$

bu formuladagi qo'shish ECh dagi nuqtalarni qo'shishni bildiradi.

Shuf algoritmini o'rganishda l-tartibli torsion (burilish) nuqta tushunchasiga duch kelamiz. Shuning uchun bu tushunchani keltirib o'tamiz. Agar EECh dagi P nuqta uchun $[l]P = O$ bo'lsa, P nuqta $l-$ tartibli torsion nuqta deyiladi va barcha l -tartibli torsion nuqtalar to'plami $E[l]$ orqali belgilanadi. Manbalarda $\#E[l] = l^2$ tenglik o'rinli va $E[l]$ to'plam $E(F_p)$ ning qism gruppasi bo'lishi ta'kidlangan.

l -tartibli torsion nuqtalar va l -tartibli $\psi_l(x,y)$ bo'luvchi ko'phad orasida ham bog'lanish mavjud bo'lib, bu bog'lanish quyidagi teoremada keltiriladi.

Teorema 8. $P(x,y)$ nuqtaning l- tartibli torsion nuqta bo'lishi uchun $\psi_l(x,y) = 0$ bo'lishi zarur va yetarlidir.

Misol 3. $y^2 = x^3 + 2x + 6(mod\,7)$ ECh ning nuqtalari sonini toping.

Yechish. Birinchi oddiy usuldan foydalanib ko'ramiz. Buning uchun x ga 0 dan 6 gacha bo'lgan qiymatlarni berib chiqamiz. So'ngra bu qiymatlarga mos y ning qiymatlarini topamiz. Buning uchun z_7 ning elementlarini kvadratlarini yozib chiqamiz:

$0^2 = 0,\ 1^2 = 1,\ 2^2 = 4,\ 3^2 = 2,\ 4^2 = 2,\ 5^2 = 4,\ 6^2 = 1.$

Yuqorida hisoblanganlarga ko'ra $E_7(2,6)$ ning nuqtalarini topamiz:

$x = 0$ y mavjud emas
$x = 1$ $y = 3, y = -3 = 4$
$x = 2$ $y = 2, y = -2 = 5$
$x = 3$ $y = 2, y = -2 = 5$
$x = 4$ $y = 1, y = -1 = 6$
$x = 5$ $y = 1, y = -1 = 6$
$x = 6$ y mavjud emas

Topilgan nuqtalarga cheksiz nuqtani qo'shsak, $\#E_7(2,6) = 11$ ga ega bo'lamiz.

EECh larni kriptografiyada qo'llanilishida $\#E(F_p)$ ning katta tub son yoki katta tub son va kichik sonning ko'paytmasiga teng bo'lishi talab qilinadi. Bu talabning muhimligi Lagranj va Xasse teoremalariga

asoslanadi. Lagranj teoremasiga ko'ra elementning tartibi gruppa tartibining bo'luvchisi bo'ladi. Lagranj va Xasse teoremalariga ko'ra esa agar $\{k_i\}$ lar EECh ning n ta nuqtasining tartiblari bo'lsa, u holda shunday r soni topilib $p+1-2\sqrt{p} \le r \cdot lcm(\{k_i\}) \le p+1+2\sqrt{p}$ tengsizliklar o'rinli bo'ladi. Agar bunday r yagona bo'lsa, u holda $\#E(F_p) = r \cdot lcm(\{k_i\})$ tenglik o'rinli bo'ladi.

Misol 4. Faraz qilaylik F_{97} maydon ustida $y^2 = x^3 + 46x + 74$ EECh berilgan bo'lsin. Xasse teoremasiga ko'ra $97 - 2 \cdot 9 = 79 \le \#E(F_{97}) \le 117 = 97 + 2 \cdot 9$ munosabatlar o'rinli bo'ladi. Bu EECh ga tegishli $P = (64,35)$ va $Q = (46,95)$ nuqtalarni qaraylik. Bu nuqtalarning tartiblari quyidagicha bo'ladi: $ord(P) = 16$, $ord(Q) = 20$. Yuqoridagi qayd qilingan tasdiqqa ko'ra $79 \le r \cdot lcm(ord(P), ord(Q)) \le 117$ tengsizlik o'rinli bo'ladi va $lcm(16,20) = 80$ ekanligidan $r = 1$ tenglik kelib chiqadi. Demak, $\#E(F_{97}) = 80$.

Agar $\#E(F_p)$ ma'lum bo'lsa, $\#E(F_{p^n})$ ni hisoblash mumkin. Haqiqatan ham, faraz qilaylik $\#E(F_p) = p + 1 - t$ bo'lsin.

Teorema 9. $\#E(F_{p^n})$ ni hisoblash uchun $x^2 - tx + p = (x - \alpha)(x - \beta)$ tenglikni qanoatlantiruvchi α, β lar topiladi va ular uchun $\#E(F_{p^n}) = p^n + 1 - (\alpha^n + \beta^n)$ tenglik o'rinli bo'ladi. Agar p juda katta son bo'lsa $s_n = \alpha^n + \beta^n$ miqdor quyidagi rekkurent formula bilan berilgan ketma-ketlik orqali topiladi: $s_0 = 2$, $s_1 = t$, $s_{n+1} = ts_n - ps_{n-1}$.

Agar $\#E(F_p) = p + 1 - 2d$ bo'lsin, u holda teorema 2.3.2 ga ko'ra α va β kompleks sonlar topilib $p = \alpha\beta$ va $-2d = \alpha + \beta$ tengliklar o'rinli bo'ladi.

Tasdiq. Agar F_2 maydonda aniqlangan ECh $y^2 + xy = x^3 + ax^2 + b$ tenglik orqali berilgan bo'lsa, u holda $\#E(F_2) \in \{2,4\}$ munosabat o'rinli bo'ladi. Yuqoridagilardan esa har qanday k uchun, $\#E(F_2) = 2$ va $\#E(F_2) = 4$ lar uchun mos ravishda, quyidagi tengliklar o'rinli bo'ladi:

$$\#E(F_{2^k}) = 2^k + 1 - 2^{\frac{k}{2}+1}\left\lfloor \cos\left(k \arctan\left(\pm\sqrt{7}\right)\right)\right\rfloor \quad (1.14).$$

Isboti. Agar $a, b = 0$ bo'lsa, u holda $y^2 + xy = x^3$ ECh tenglamasi faqat bitta (0,0) yechimga ega bo'ladi. Cheksiz uzoqlikdagi nuqtani hisobga olsak $\#E(F_2) = 2$ bo'ladi. $GF(2)$ maydonda aniqlangan ECh ning nuqtalari soni uchun $\#E(F_2) = 2 + 1 - 2d$ tenglik o'rinli

ekanligidan $-2d=-1$ ga ega bo'lamiz. $\begin{cases}\alpha+\beta=-1\\ \alpha\beta=2\end{cases}$ tenglamalar sistemasini yechsak $\alpha=\frac{-1\pm\sqrt{-7}}{2}$ va $\beta=\frac{-1\mp\sqrt{-7}}{2}$ yechimlarga ega bo'lamiz. Topilgan bu qiymatlardan $\#E(F_{2^k})=2^k+1-\frac{(1-\sqrt{-7})^k+(1+\sqrt{-7})^k}{2^k}$ ga ega bo'lamiz. Bu ifodani soddalashtirish uchun kompleks sonning trigonometrik ko'rinishi va uni darajaga oshirish xossasidan foydalaniladi. Shulardan kelib chiqqan holda bu formulalarni keltirib o'tamiz. Bizga biror $z=a+ib\in C$ kompleks son berilgan bo'lsin. Uning trigonometrik ko'rinishi $z=r(\cos\phi+i\sin\phi)$ bo'lib, bunda $\phi=arctan\frac{b}{a}$, $r=|z|=\sqrt{a^2+b^2}$. Agar $z=r(\cos\phi+i\sin\phi)$ bo'lsa, $z^k=r^k(\cos(k\phi)+i\sin(k\phi))$ tenglik o'rinli bo'ladi. Yuqorida keltirilgan formulalardan foydalanib $z_1=1-\sqrt{-7}=1-\sqrt{7}i$ va $z_2=1+\sqrt{-7}=1+\sqrt{7}i$ sonlarning darajalarini hisoblasak, mos ravishda $z_1^k=\left(\sqrt{8}\right)^k\left[\cos\left(k\,arctan\sqrt{7}\right)-i\sin\left(k\,arctan\sqrt{7}\right)\right]$ va $z_1^k=\left(\sqrt{8}\right)^k\left[\cos\left(k\,arctan\sqrt{7}\right)+i\sin\left(k\,arctan\sqrt{7}\right)\right]$ larga ega bo'lamiz. Natijada esa $\#E(F_{2^k})=2^k+1-2^{\frac{k}{2}+1}\left[\cos\left(k\,arctan\sqrt{7}\right)\right]$ kelib chiqadi.

Agar $a=b=1$ bo'lsa, $\#E(F_2)=4$ va $-2d=1$ bo'ladi. $\begin{cases}\alpha+\beta=1\\ \alpha\beta=2\end{cases}$ tenglamalar sistemasi $\alpha=\frac{1\pm\sqrt{-7}}{2}$ va $\beta=\frac{1\mp\sqrt{-7}}{2}$ yechimlarga ega. Natijada $\#E(F_{2^k})=2^k+1-2^{\frac{k}{2}+1}\left[\cos\left(k\,arctan(-\sqrt{7})\right)\right]$ ga ega bo'lamiz. Tasdiq isbot bo'ldi.

Xuddi shunday maydon xarakteristikasi 3 ga teng hol uchun ham ECh nuqtalarini topish formulasini keltiramiz.

Tasdiq. Agar F_3 maydonda aniqlangan ECh ning j -invarianti noldan farqli bo'lsa, u holda $\#E(F_3)\in\{1,2,3,4,5,6,7\}$ munosabat o'rinli bo'ladi. Bu holda ECh ning F_{3^k} dagi nuqtalari soni quyidagicha aniqlash mumkin:

1) ixtiyoriy k va $\#E(F_3)=5$, $\#E(F_3)=3$ lar uchun mos ravishda $\#E(F_{3^k})=3^k+1-2\cdot3^{\frac{k}{2}}\left[\cos\left(k\,arctan\left(\pm\sqrt{11}\right)\right)\right]$ bo'ladi;

2) ixtiyoriy k va $\#E(F_3)=6$, $\#E(F_3)=2$ lar uchun mos ravishda $\#E(F_{3^k})=3^k+1-2\cdot3^{\frac{k}{2}}\left[\cos\left(k\,arctan\left(\pm\sqrt{2}\right)\right)\right]$ bo'ladi;

3) ixtiyoriy k va $\#E(F_3)=7$, $\#E(F_3)=1$ lar uchun mos ravishda $\#E(F_{3^k})=3^k+1-2\cdot 3^{\frac{k}{2}}\left|cos\left(k\,arctan\left(\pm 3^{-\frac{1}{2}}\right)\right)\right|$ bo'ladi;

4) $\#E(F_3)=4$ va k – juft, k – toq lar uchun mos ravishda $\#E(F_{3^k})=\begin{cases}3^k+1-2\cdot(-3)^{\frac{k}{2}}\\ 3^k+1\end{cases}$ bo'ladi.

Isboti. Koeffisiyentlari $a,b,c\in F_3$ bo'lgan $y^2=x^3+ax^2+bx+c$ tenglik bilan aniqlangan ECh ning nuqtalari $\#E(F_3)\in\{1,2,3,4,5,6,7\}$ bo'ladi. $\#E(F_3)$ ning qiymatlar $a,b,c\in F_3$ koeffisiyentlarga bog'liq ravishda har xil bo'ladi (1–jadval). $\#E(GF(3))=4$ tenglik $a,b,c\in F_3$ larning ko'p qiymatlarida o'rinli bo'ladi. Shuning uchun faqatgina $\#E(F_3)=4$ holni isbotini qaraymiz. Qolgan hollar ham shunga o'xshash isbotlanadi.

1.2–jadval

$\#E(GF(3))$	EECh ning koeffisiyentlari		
	a	b	c
1	0	2	2
2	2	0	2
	2	1	2
	2	2	0
3	1	1	2
4	0	0	0
	0	0	1
	0	0	2
	0	1	0
	0	1	1
	0	1	2
	0	2	0
	1	0	0
	1	0	2
	1	1	0
	1	2	0
	1	2	1
	1	2	2
5	2	0	0
	2	0	1
	2	1	0

$\#E(GF(3))$	EECh ning koeffisiyentlari		
	a	b	c
	2	1	1
	2	2	1
	2	2	2
6	1	1	1
7	0	2	1
	1	0	1

$\#E(F_3) = 4$ ekanligidan, $-2d = 0$ ga ega bo'lamiz. Bundan esa $\begin{cases}\alpha + \beta = 0 \\ \alpha\beta = 3\end{cases}$ tenglamalar sistemasiga ega bo'lamiz. bu sistemaning yechimlari $\alpha = \pm\sqrt{-3}$ va $\beta = \mp\sqrt{-3}$ bo'ladi. Bu qiymatlardan $\#E(F_{3^k}) = 3^k + 1 - \left(\left(\sqrt{-3}\right)^k + \left(-\sqrt{-3}\right)^k\right)$ ga ega bo'lamiz. Demak,

$$\#E(F_{3^k}) = \begin{cases}3^k + 1 - 2 \cdot (-3)^{\frac{k}{2}}, k - \text{juft} \\ 3^k + 1, k - \text{toq}\end{cases}$$

tenglik o'rinli ekan. Teorema 9 isbot bo'ldi.

F_p maydon ustida aniqlangan $E: y^2 = x^3 + ax + b$ EECh kriptografik talablarga javob berishi uchun quyidagilar bajarilishi lozim:

1. $t = \lfloor log\, p \rfloor + 1 \geq 160$
2. $a, b \neq 0 (mod\, p)$ va $4a^3 + 27b^2 \neq 0 (mod\, p)$
3. $\#E(F_p)$ – deyarli tub son
4. $(p^k - 1)\, mod\, q = 0$ shart biror $k = \overline{1,31}$ uchun bajarilsa 2-qadamga qaytilsin
5. $p = q$ bo'lsa, 2-qadamga qaytilsin
6. G generator nuqta topilsin.

Nazorat savollari

1. Butun sonni faktorlash muammosini yechish usullari haqida ayting?
2. Pollardning Ro algoritmini tushuntiring?
3. Diskret logarifmlash muammosini yechish usullarini ayting?
4. Elliptik egri chiziqda nuqtalar qanday qo'shiladi?
5. Elliptik egri chiziq deb qanday chiziqqalarga aytiladi?
6. Elliptik egri chiziqda nuqta tartibi qanday aniqlanadi?

II BOB. OCHIQ KALITLI SHIFRLASH ALGORITMLARI PARAMETRLARI

2.1. Tub sonlar va ularning ayrim xossalari

Ochiq kalitli kriptotizimlarning asosiy tashkil etuvchi elementlaridan biri yetarlicha katta (150 va undan ortiq xonali) tub sonlardan foydalanishidir. Bunday kriptotizimlarda malumotlarni shifrlash va rasshifroklalash jarayonini amalga oshirish algoritmlarini amaliy qo'llanishlarini ta'minlash uchun katta razryadli sonlarni tub yoki tub emasligini aniqlab olish usullarini bilish muhim hisoblanadi.

Quyida ochiq kalitli kriptotizmlar asosi bilan bog'liq bo'lgan sonlar nazariyasining ayrim ta'rif va tasdiqlari isbotsiz keltiriladi.

Ta'rif 1. Berilgan p natural son tub deyiladi, agarda $p > 1$ bo'lib, u bir va o'zidan boshqa natural bo'luvchilarga ega bo'lmasa.

Odatda tub sonlar p va q lar bilan belgilanib, tub sonlarga quyidagilar misol bo'la oladi:
29, 53, 79, 89, 97, 113, 151, 163, 419, 877, 1063, 1439, 1913, 1999, 2003, 2081, 2609, 2887, 3181, 3217, 3517, 3797, 4423, 4999, 5039, 5227, 5659, 5878, 5981.

Ta'rif 2. Bir va o'zidan boshqa sonlarga ham bo'linadigan sonlar murakkab sonlar deyiladi.

Ta'rifdan ko'rinadiki, 1 soni tub soniga kirmaydi. Shuningdek, murakkab son ham emas.

Teorema 1. Har bir $n > 1$ natural sonning 1 dan farqli eng kichik bo'luvchisi p tub sondir.

Teorema 2. Har qanday n natural son berilgan p tub songa yoki bo'linadi yoki u bilan o'zaro tubdir.

Teorema 3. Agar $a \cdot b$ ko'paytma biror p tub songa bo'linsa, u holda ko'paytuvchilardan kamida bittasi p -ga bo'linadi.

Natija. Agar bir necha sonlarning ko'paytmasi p tub songa bo'linib, uning barcha ko'paytuvchilari tub sonlardan iborat bo'lsa, ko'paytuvchilarning biri p-ga tengdir.

Teorema (arifmetikaning asosiy teoremasi) 4. Har bir $n > 1$ natural son tub son yoki tub son ko'paytmasi shaklida yoziladi, agarda bu ko'paytmada ko'paytuvchilarning o'rni etiborga olinmasa, u holda bu ko'paytma yagona bo'ladi.

Teorema 5. Tub sonlar to'plami cheksizdir.

Tub sonlarning keltirilgan xossalaridan foydalanish va ularning ochiq kalitli algoritmlarda yetarlicha katta qiymatlarda ishlatilishi, katta qiymatli berilgan butun sonlarni elementar hamda maxsus ko'rinshga ega bo'lgan sonlarning tub ekanligini aniqlash usullaridan foydalanishni taqazo etadi. Bunday usullardan ayrimlari quyida keltiriladi.

1-usul.

Teorema 5. Ixtiyoriy n natural sonning eng kichik tub bo'luvchisi $\sqrt{n}$ dan oshmaydi.

Misol 1. $n = 89$ shu sonning tub ekanligini yuqoridagi teoremaga asosan quyidagicha tekshiriladi.

Yechish. $\sqrt{89} < 10$ demak, 2, 3, 4, 5, 6, 7, 8, 9 sonlarga ketma-ket bo'lib chiqiladi. Agar berilgan n natural son shu sonlardan birortasiga bo'linsa, uholda berilgan son murakkab, aks holda esa tub son deb e'lon qilinadi. Javob $n = 89$ tub son.

2-usul.

Ushbu usul Eratosfen g'alviri deb atalib, bu usulda berilgan N natural songa ko'ra, shu songacha bo'lgan tub sonlar ro'yxatini topish mumkin bo'ladi, ya'ni agar N dan katta bo'lmagan barcha tub sonlarni topish kerak bo'lsa, avvalo ikkidan boshlab, N gacha bo'lgan barcha natural sonlar yozib chiqiladi. Hosil bo'lgan jadvalda ikkidan keyin har bir ikkinchisini, uchdan keyin har bir uchunchisini, beshdan keyin har bir beshinchisini, 7 dan keyin har bir yettinchisini va h.k. Bu jarayonni $\sqrt{N}$ - dan ortmaydigan r tub songacha davom ettirib, r-ga bo'linadigan sonlar o'chiriladi. O'chirilmay qolgan sonlar N dan ortmaydigan tub sonlar bo'ladi. Chunki, N dan ortmaydigan barcha karrali sonlar o'chirib tashlandi.

Misol 2. $N = 200$ bo'lsin, u holda $13 < \sqrt{200}$ bo'ladi. 2 dan 200 gacha bo'lgan intervaldagi tub sonlarni topish uchun 2 va 199 gacha bo'lgan barcha toq sonlar yoziladi. Keyin yuqoridagidek 3, 5, 7, 11, 13- ga karali bo'lganlari o'chirilib, quyidagi hosil qilinadi:

2, 3, 5, 7, 11, 13, 17, 19, 23, 29, 31, 37, 41, 43, 47, 53, 59, 61, 67, 71, 73, 79, 83, 89, 97, 101, 103, 107, 109, 113, 127, 131, 137, 139, 149, 151, 157. 163, 167, 173, 179, 181, 191 ,193, 197, 199.

Demak, 200 dan kichik tub sonlarning umumiy soni 46 ta ekan.

Ta'rif 3. Quyidagi ko'rinishdagi sonlar: $F_n = 2^{2^n} + 1$, bu yerda, $n \geq 0$, Ferma sonlari deyiladi.

Masalan, bevosita ishonch hosil qilish mumkinki F_0, F_1, F_2, F_3, F_4 sonlar tub sonlar bo'ladi, lekin, yana qaysi n-lar uchun Ferma sonlari tub bo'ladi degan savolga, quyidagi teorema javob beradi.

Teorema 6. $k = F_n$ soni $n > 0$ bo'lganda tub bo'ladi faqat va faqat, $3^{(k-1)/2} \equiv -1(mod\ k)$ o'rinli bo'lsa.

Hozirgi vaqtda n=5, 6, 7, 8, 9, 10, 11, 12, 15, 16, 18, 23, 36, 38, 73 qiymatlarda Ferma sonlari murakkab ekanligi ma'lum.

Misol 3. $n = 3$ uchun $F_n = 2^{2^n} + 1$ sonini tub ekanligi isbot qilinsin.

Yechish. F_3=257, $(F_3-1)/2$=128. U holda keltirilgan algoritmga ko'ra, $3^{128}(\text{mod } 257) = (3^8)^{16}(\text{mod } 257) = 6561^{16} (\text{mod } 257) = (136^2)^8 (\text{mod } 257) = 249^8 (\text{mod } 257) = (249^2)^4 (\text{mod } 257) = 64^4 (\text{mod } 257) = 256(\text{mod } 257) = -1(\text{mod } 257)$;

Demak, 257 soni tub son ekan.

Ta'rif 4. Quyidagi ko'rinishdagi sonlar $M_p = 2^p - 1$, bu yerda, p-tub son, - Mersen sonlari deb ataladi.

Masalan, p = 2, 3, 5, 7, 13, 17, 19 lar uchun Mersen sonlari tub son. Biroq, p =11, 23, 29 bo'lganda esa Mersen sonlari murakkab son bo'ladi.

Mersen sonlari tub bo'lishligi uchun quyidagi teorema o'rinli.

Teorema 7. $M_p = 2^p - 1$, p-tub son va $p > 2$. Quyidagi ketma-ketlik ko'rib chiqiladi:

$L_0, L_1, L_2, \ldots\ldots$

$L_0 = 4, L_{j+1} \equiv (L_j{}^2 - 2)(mod\ M_p)$

Berilgan, M_p – soni tub bo'ladi, faqat va faqat $L_{p-2} \equiv 0\ (mod\ M_p)$ bo'lsa.

Misol-4. r=13 bo'lsa, Mersen soni tub son bo'lishligi ko'rsatilsin.

Yechish. $M_{13}=2^{13}-1$= 8192-1=8191. Keltirilgan algoritm bo'yicha: $L_0 = 4, L_{j+1} \equiv (L_j{}^2 - 2)(mod\ M_p)$, j=1,2,.....11 gacha hisoblab chiqiladi:

L_0=4, L_1=14, L_2=194, L_3=4870, L_4=3953, L_5=5970, L_6=1857, L_7=36, L_8=1294, L_9=3490, L_{10}=128, L_{11}=16382 (mod 8191)=0.

Demak, algoritm shartlari bajarildi, ya'ni 8191 soni tub ekan.

Quyida ko'rib chiqadigan algoritm umumiy ko'rinishda berilgan natural son tub bo'lishini aniqlab beruvchi algoritmlardan biri bo'lib, Lukas algoritmi deb ham yuritiladi.

Teorema (Lukas). Agar n – natural son uchun shunday a – butun son mavjud bo'lib:

$a^{n-1} \equiv 1\ (mod\ n)$ va $a^{n-1/p} \neq 1\ (mod\ n)$ har bir tub r – soni n – 1-ning bo'luvchisi bo'lgan. U holda n – tub son bo'ladi.

Misol 5. Agar n=113 bo'lsa, uning tub son ekanligi Lukas algoritmi yordamida tekshirilsin.

Yechish:

Aytaylik, a=3 bo'lsin. U holda $n-1=112$ bo'lib, $112=2^4\times7$. $3^{112}(\text{mod}113)=3^{8\times14}(\text{mod}113)=6561^{14}(\text{mod}113)=7^{14}(\text{mod}113)=823543^2$ $(\text{mod}113)=112^2(\text{mod}113)=1$;

Demak, Lukas algoritmi shartlari bajarildi, ya'ni n=113 soni tub ekan.

2.2. Tub sonlarni generatsiyalash usullari

Tub sonlarning keltirilgan xossalaridan foydalanish va ularning asimmetrik algoritmlarda yetarlicha katta qiymatlarda ishlatilishi, katta qiymatli berilgan butun sonlarni elementar hamda maxsus ko'rinishga ega bo'lgan sonlarning tub ekanligini aniqlash usullaridan foydalanishni taqozo etadi. Bunday usullardan ayrimlarini ko'rib chiqamiz.

1- usul.

Teorema 5. Ixtiyoriy n natural sonning eng kichik tub bo'luvchisi $\sqrt{n}$ dan oshmaydi.

Misol 1. n = 89 shu sonning tub ekanligini yuqoridagi teoremaga asosan quyidagicha tekshiramiz.

Yechish. $\sqrt{89} < 10$ demak, 2,3,4,5, 6,7,8,9 sonlarga ketma-ket bo'lib ko'ramiz. Agar berilgan n natural son shu sonlardan birortasiga bo'linsa, u holda berilgan son murakkab, aks holda esa tub son deb elon qilinadi. Javob n =89 tub son.

2- usul.

Eratosfen g'alviri deb ataladi. Bu usulda berilgan N natural songa ko'ra, shu songacha bo'lgan tub sonlar ro'yxatini topish mumkin bo'ladi, yani agar N dan katta bo'lmagan barcha tub sonlarni topish kerak bo'lsa, avvalo ikkidan boshlab, N gacha bo'lgan barcha natural sonlarni yozib chiqamiz, hosil bo'lgan jadvalda ikkidan keyin har bir ikkinchisini, uchdan keyin har bir uchinchisini, beshdan keyin har bir beshinchisini , 7

dan keyin har bir yettinchisini va h.k. Bu jarayonni $\sqrt{N}$ dan ortmaydigan r tub songacha davom ettirib, r ga bo'linadigan sonlarni o'chiramiz. O'chirilmay qolgan sonlar N dan ortmaydigan tub sonlar bo'ladi, chunki biz N dan ortmaydigan barcha karrali sonlarni o'chirib tashladik.

Misol 2. N = 200 bo'lsin, u holda $13<\sqrt{200}$ bo'ladi.

2 dan 200 gacha bo'lgan intervaldagi tub sonlarni topish uchun 2 va 199 gacha bo'lgan barcha toq sonlarni yozamiz. Keyin yuqoridagidek 3, 5 , 7,11,13 ga karali bo'lganlarini o'chirib, quyidagini hosil qilamiz:

2, 3, 5, 7, 11, 13, 17, 19, 23, 29, 31, 37, 41, 43, 47, 53, 59, 61, 67, 71, 73, 79, 83, 89, 97, 101, 103, 107, 109, 113, 127, 131, 137, 139, 149, 151, 157, 163, 167 , 173, 179, 181, 191, 193, 197, 199.

Demak, 200 dan kichik tub sonlarning umumiy soni 46 ta ekan.

Tarif 3. Quyidagi ko'rinishdagi sonlar:

$F_k = 2^{2^k} + 1$, $k=0,1,2,...$ Ferma sonlari deyiladi.

Masalan. Bevosita ishonch hosil qilish mumkinki F_0, F_1, F_2 , F_3, F_4 sonlar tub sonlar bo'ladi, lekin yana qaysi k - lar uchun Ferma sonlari tub bo'ladi degan savol bo'lsa, bu savolga quyidagi teorema javob beradi.

Teorema 6. $n = F_k$ soni $k > 0$ bo'lganda tub bo'ladi faqat va faqat, $3^{(n-1)/2} \equiv -1 \pmod n$ o'rinli bo'lsa.

Hozirgi vaqtda k=5,6,7,8,9,10,11,12,15,16,18,23,36,38,73 qiymatlarda Ferma sonlari murakkab ekanligi malum[11] .

Misol -3. $F_k = 2^{2^k} + 1$, $k=3$ bo'lganda tub ekanligi isbot qilinsin.

Yechish. $F_3 = 257$, $(F_3 - 1) : 2 = 128$. U holda keltirilgan algoritmga ko'ra:

$3^{128} \pmod{257} = (3^8)^{16} \pmod{257} = 6561^{16} \pmod{257} = (136^2)^8 \pmod{257} = 249^8 \pmod{257} = (249^2)^4 \pmod{257} = 64^4 \pmod{257} = 256 \pmod{257} = -1 \pmod{257}$;

Demak, 257 soni tub son ekan.

Tarif 4. Quyidagi ko'rinishdagi sonlar $M_r = 2^r - 1$, r- tub son tub bo'lsa. U holda bunday sonlar Mersen sonlari deb ataladi.

Masalan r=2,3,5,7,13,17,19 bo'lganda Mersen sonlari tub son . Biroq r=11,23, 29 bo'lganda esa Mersen sonlari murakkab ekanliklari aniqlanilgan.

Shuni takidlash lozimki, Mersen sonlari juda kam miqdorda topilgan bo'lib, 2001 yil 39 –chi Mersen soni topilgan va bu son $M_{13466917}$ iboratdir.

Mersen sonlari tub bo'lishligi uchun quyidagi tasdiq o'rinli.

Teorema 7. $M_r = 2^r - 1$, r- tub son va $r > 2$. Quyidagicha ketma-ketlikni qaraymiz: L_0 , L_1 , L_2 .....

$L_0 = 4$, $L_{j+1} \equiv (L_j^2 - 2) ((\mod M_p)$

Berilgan M_r – soni tub bo'ladi faqat va faqat $L_{r-2} \equiv 0(\mod M_p)$ bo'lsa.

Misol-4. r=13 bo'lsa, Mersen soni tub son bo'lishligi ko'rsatilsin.

Yechish. $M_{13} = 2^{13} - 1 = 8192\text{-}1 = 8191$. Keltirilgan algoritm bo'yicha:

$L_0 = 4$, $L_{j+1} \equiv (L_j^2 - 2) ((\mod M_p)$

J = 1,2,.....11 gacha hisoblab chiqamiz:

$L_0 = 4$, $L_1 = 14$, $L_2 = 194$, $L_3 = 4870$, $L_4 = 3953$, $L_5 = 5970$, $L_6 = 1857$, $L_7 = 36$, $L_8 = 1294$, $L_9 = 3490$, $L_{10} = 128$, $L_{11} = 16382 (\mod 8191) = 0$.

Demak, algoritm shartlari bajarildi, yani 8191 soni tub ekan.

Quyida ko'rib chiqadigan algoritm umumiy ko'rinishda berilgan natural son tub bo'lishini aniqlab beruvchi algoritmlardan biri bo'lib, Lukas algoritmi deb ham yuritiladi.

Teorema (Lukas). Agar n – natural son uchun shunday a – butun son mavjud bo'lib: $a^{n-1} \equiv 1 (\mod n)$ va $a^{n-1/r} \neq 1 (\mod n)$ har bir tub r – soni n -1 ning bo'luvchisi bo'lgan. U holda n – tub son bo'ladi.

Misol 5. Agar $n = 113$ bo'lsa, uning tub son ekanligi Lukas algoritmi yordamida tekshirilsin.

Yechish.

Aytaylik, a=3 bo'lsin. U holda n -1 = 112 bo'lib, $112 = 2^4 * 7$.

$3^{112} (\mod 113) = 3^{8*14} (\mod 113) = 6561^{14} (\mod 113) = 7^{14} (\mod 113) = 823543^2 (\mod 113) = 112^2 (\mod 113) = 1$;

Demak, Lukas algoritmi shartlari bajarildi, yani n = 113 soni tub ekan.

2.3. Sonlarni tublikka tekshirishning birlamchi testlari

Sonlarni tublikka tekshirishning ehtimollik algoritmlari:

- Ferma testi;
- Solavey Shtrassen testi;
- Rabbi-Milner testi;
- Beyl-pomerens testi;
- Lukas testi;
- Poklington testi;
- Prot testi;
- Frobenius.

Tub sonlar ochiq kalitli kriptografik tizimlarda juda muhim va zarur bo'lib, ixtiyoriy hajmdagi tub sonlardan foydalanadi. Tub sonlar kalitlarni generatsiya qilishda va ochiq parametrlarni hosil qilishda foydalaniladi. Olingan biror son, n dan kichik bo'lgan tub sonlarning taqribiy miqdori quyidagi tenglik bilan o'lchanadi:

$$n/\ln n$$

Tub sonlarni generatsiya qilish murakkab vazifa bo'lib, uni samarali amalga oshirish uchun biroz "hiyla" ishlatiladi. Boshqa so'z bilan aytilganda "n soni tubmi ?" degan savolga javob beriladi.

Tub sonlarni generatsiyalashdagi noto'g'ri usullardan biri bu – tub sonni topib keyin uni faktorlash bo'lib, juda ham ko'p vaqt oladi. Amalda ko'plab sonlarni tublikga tekshiruvchi testlar mavjud bo'lib, quyida sonlarni tublikka tekshiruvchi algoritmlar bilan tanishib chiqiladi.

Solovey – Shtrassen testi. Robert Solovey va Volker Shtrassen tomonidan ishlab chiqilgan ushbu ehtimoliy tublikka tekshirish algoritmi bo'lib, unda p sonini tublikka tekshirish uchun Yakobi belgilaridan foydalaniladi:

-dastlab p dan kichik bo'lgan tasodifiy a soni tanlanadi;

-agar $EKUB(a,p) \neq 1$, u holda p testdan o'ta olmaydi, u murakkab son;

-$j = a^{(p-1)/2} mod p$ ni hisoblanadi;

-Yakobi belgisi J(a,p) hisoblanadi;

-agar $j \neq J(a,p)$ bo'lsa, u holda p aniq tub emas;

-agar $j = J(a,p)$ bo'lsa, u holda 50 % dan yuqori bo'lmagan ehtimollik bilan p tub son emas.

Yuqoridagi ketma – ketlik t marta turli a sonlar bilan amalga oshiriladi. Bu holda murakkab toq sonlarning barcha t marta testlash davomida testdan o'tish ehtimoli $1/2^t$ dan yuqori bo'lmaydi.

Lehman. Yuqorida kabi testlashga asoslangan usullardan biri *Lehman* tomonidan ishlab chiqilgan va uni ketma – ketligi quyida keltirilgan:

-dastlab p dan kichik bo'lgan tasodifiy a soni tanlanadi;

-$a^{(p-1)/2} mod p$ ni hisoblanadi;

-agar $a^{(p-1)/2} mod p \neq 1$ ёки $-1 \; mod \; p$ ga, u holda p aniq tub son emas;

-agar $a^{(p-1)/2} mod p = 1$ ёки $-1 \; mod \; p$ bo'lsa, u holda 50 % dan yuqori bo'lmagan ehtimollik bilan p tub son emas.

Ushbu testlashda ham murakkab toq sonlarning testdan o'tish ehtimoli Solovey – Shtrassen testidagi kabi bo'ladi.

Rabin – Miller testi. Amalda eng tezkor algoritm sifatidagi qaraladigan tublikga tekshirish usuli sanalib, bu algoritm Maykl Rabin va Gari Millerlar tomonidan yaratilgan. Ushbu testlash usuli ketma – ketligi quyidagicha:

1. testlash uchun p son olinadi;
2. shundan so'ng p-1 ni 2 soni necha marta bo'lishini anglatuvchi b soni hisoblanadi (ya'ni, 2^b soni $p-1$ ni bo' luvchisi bo'lgandagi b ning eng katta qiymati);
3. shundan so'ng $p = 1 + 2^b * m$ tenglikdan m hisoblanadi;
4. p dan kichik bo'lgan a soni tanlanadi;
5. $j = 0$ ga o'rnatiladi va $z = a^m mod p$ hisoblanadi;
6. agar $z = 1$ bo'lsa yoki $z = p - 1$ ga teng bo'lsa, u holda p testdan o'tadi va u tub bo'lishi mumkin;
7. agar $j > 0$ bo'lsa va $z = 1$ bo'lsa, u holda p tub son emas;
8. $j = j + 1$ o'rnatiladi. Agar $j < b$ va $z \neq p - 1$ bo'lsa, $z = z^2 mod p$ o'rnatiladi va 7 – qadamga o'tiladi. Agar $z = p - 1$ ga teng bo'lsa, p testdan o'tadi va u tub son bo'lishi mumkin;
9. agar $j = b$ va $z \neq p - 1$ ga teng bo'lsa, u holda p testlashdan o'ta olmaydi.

Ushbu testlash usulida murakkab toq sonni yolg'ondan o'tish ehtimoli juda past. a sonning ¾ qismi test natijasi to'g'riligini tasdiqlaydi. Bu shuni tasdiqlaydiki murakkab sonlarning t marta testlashdan o'tish ihtimoli $1/4^t$ ga teng bo'ladi. Bu albatta, taxminiy fikr bo'lib, amalda 256 – bitli sonlarni 6 marta testlashda xatolik bo'lishi ehtimoli $1/2^{51}$ ga teng bo'ladi (2.1 - jadval).

2.1 – jadval

DSA algoritmi uchun Rabin – Miller testi orqali testlashning minimal iteratsiyasi

Parametrlar	**Faqat Rabin – Miller testlash orqali**
p:1024 bit; q: 160 bit. Xatolik ehtimoli=2^{-80}	p va q lar uchun: 40
p:2048 bit; q: 224 bit.	p va q lar uchun: 56

Parametrlar	Faqat Rabin – Miller testlash orqali
Xatolik ehtimoli=2^{-112}	
p:2048 bit; q: 256 bit. Xatolik ehtimoli=2^{-112}	p va q lar uchun: 56
p:3072 bit; q: 256 bit. Xatolik ehtimoli=2^{-128}	p va q lar uchun: 64

Tub sonlarni tekshirishni amalga oshirish. Amalda sonlarni tublikga testlash juda ham tezkor amalda oshiriladi:

1. n – bitli tasodifiy p soni generatsiya qilinadi;
2. ushbu sonning eng kichik va eng katta pozisiyasidagi bitlarga 1 o'rnatiladi (eng kichik pozisiyaga 1 ni o'rnatish sonni toqligini, eng katta pozisiyasida o'rnatilgan 1 esa to'liq n bitli bo'lishini ta'minlaydi);
3. p sonni kichik tub sonlar, 2,3,5,7,11 va h.larga bo'linadi, bunda odatda 2000 dan kichik bo'lgan barcha tub sonlardan foydalanadi;
4. agar 3 bosqich natijasida p son tub deb topilsa, ba'zi a sonlarga ko'ra Rabin – Miller testi amalga oshiriladi (odatda testlashni 5 marta amalga oshirish yetarli);
5. 4 bosqich natijasiga ko'ra p son tub deb topilsa, testlash tugatiladi, aks holda, boshqa p tub son olinadi va qaytadan jarayonlar amalga oshiriladi.

Nazorat savollari

1. Tub son va uning xususiyatlari haqida ayting?
2. Tub sonlarga misollar keltiring?
3. Tub sonlarning kriptografiyada tutgan o'rni?
4. Tub sonlarni generatsiyalash usullari haqida ayting?
5. Tub sonlarni tublikka tekshirishning birlamchi testlari haqida ayting?
6. Solovey – Shtrassen testi haqida ayting?
7. Rabin-Miller testi haqida ayting?

III BOB. TASODIFIY BITLAR KETMA-KETLIGINI GENERATSIYALASH

3.1. Tasodifiy bitlar generatori

Axborot xavfsizligida talab qilingan tasodifiy sonlarni hosil qilish muammosini bartaraf etishda quyidagi usullardan foydalaniladi:

Xavfsiz bo'lmagan tasodifiy sonlar generatori. Bu turdagi generatorlar kriptografik psevdo-tasodifiy sonlar generatori hisoblanmaydi. Mazkur turdagi generatorlardan foydalanilganda hujumchi hosil qilinuvchi qiymatlarni oldindan bilishi mumkin bo'ladi.

Bu turdagi generatorlarga misol sifatida aksariyat dasturlash tillarida mavjud $rand()$ yoki $random()$ funksiyalarini (chiziqli kongurent generatorlarga asoslangan) keltirish mumkin. Bundan tashqari "Mersen Twister" generatori ham ushbu toifaga tegishli bo'lib, qator tizimlarda va dasturiy vositalarga (masalan, Matlab, Excel, PHP, Python va hak.) keng qo'llaniladi. Bu turdagi generatorlar yuqori darajadagi entropiyaga ega kalitlarni generatsiya qila olmasligi bilan zaif sanaladi. Ushbu generator 1997 yilda Makoto Matsumoto va Takuji Nishimuralar tomonidan yaratilgan.

Quyida "Mersen Twister" algoritmining umumiy ifodasi keltirilgan:

$$x_{k+n} := x_{k+m} \oplus \left(\left(x_k^u || x_{k+1}^l\right) A\right)$$

"Mersene Twister" generatorining 32 bitli tizim uchun mo'ljallangan shaklida quyidagi parametrlardan foydalanilgan:

$(w,\ n,\ m,\ r) = (32, 624, 397, 31)$;

$a = 9908\text{B}0\text{DF}_{16}$;

$(u,\ d) = (11, \text{FFFFFFFF}_{16})$;

$(s, b) = (7, 9\text{D}2\text{C}5680_{16})$;

$(t, c) = (15, \text{EFC}60000_{16})$;

$l = 18$.

Bu yerda: w- so'z uzunligi (bitda), n – takrorlanish darajasi, m – foydalaniluvchi o'rta so'z, r – bir so'zning ikkiga bo'linish nuqtasi, a – twist matrisasi uchun koeffisent, b, c – almashtirish bit maskalari, s, t – almashtirishdashi siljitish bitlari, u, d, l – qo'shimcha siljitish va maska parametrlari. Umumiy holda ushbu generatorning psevdokodi quyidagicha:

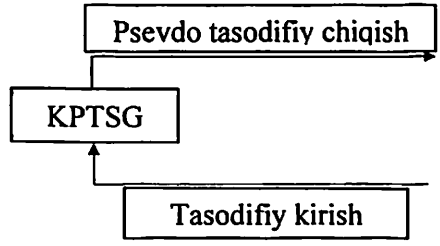
```
// generator holatini saqlash uchun n uzunlikdagi massivni yaratish
  int[0..n-1] MT
```

```
    int index := n+1
    const int lower_mask = (1 << r) - 1
    const int upper_mask = lowest w bits of (not
lower_mask)

    // Dastlabki seed qiymatdan generatorni
ishlatish
    function seed_mt(int seed) {
      index := n
      MT[0] := seed
      for i from 1 to (n - 1) {
        MT[i] := lowest w bits of (f * (MT[i-1]
xor (MT[i-1] >> (w-2))) + i)
      }
    }

    // MT[index] dan qiymatlarni ajratish
    // har n tada twist() ni chaqirish
    function extract_number() {
      if index >= n {
        if index > n {
         error "Generator was never seeded"
         }
        twist()
      }

      int y := MT[index]
      y := y xor ((y >> u) and d)
      y := y xor ((y << s) and b)
      y := y xor ((y << t) and c)
      y := y xor (y >> l)

      index := index + 1
      return lowest w bits of (y)
    }
    // x_i lar ketma-ketligidan keyingi n
qiymatni generatsiya qilish
    function twist() {
      for i from 0 to (n-1) {
```

```
        int x := (MT[i] and upper_mask)
             + (MT[(i+1) mod n] and lower_mask)
        int xA := x >> 1
        if (x mod 2) != 0 {
          xA := xA xor a
        }
        MT[i] := MT[(i + m) mod n] xor xA
      }
      index := 0
    }
```

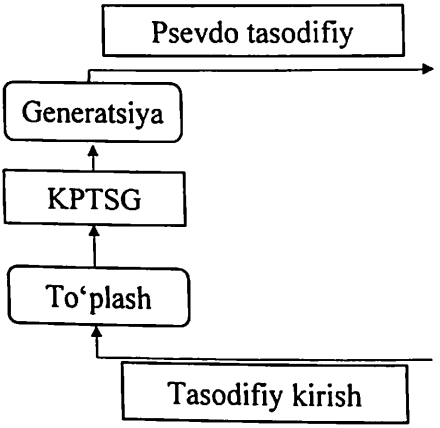
Ushbu generatorda almashtirish funksiyasi sifatida bir tomonlama funksiyadan foydalanilmaganiligi sababli, xavfsiz emas deb qaraladi. Ushbu generatorning keyingi versiyalarida tezkorlini oshirishga harakat qilingan (Tiny MT).

Kriptografik psevdotasodifiy sonlar generatori (KPTSG). Mazkur usulga asosan xavfsiz yagona boshlang'ich qiymat (seed) ni kiritish orqali kriptografik algoritm talab etilgan uzunlikdagi tasodifiy qiymatlarni generatsiya qilib beradi. Ushbu holat aksariyat hollarda tasodifiy qiymatlarni generatsiya qilishdagi asosiy yechim sifatida qaraladi. Umumiy holda KPTSGlarni 3.1-rasmdagi kabi tasvirlash mumkin.



3.1-rasm. KPTSGlarni umumiy ko'rinishi

Tasodifiy hodisalar manbasidan olingan qiymatlar dastlab to'plash jarayoni orqali ma'lum vaqt to'planib boriladi. Ushbu to'plangan ma'lumotlar orqali generator holati yangilanadi va shundan so'ng generatsiyalash jarayonida psevdotasodifiy chiqishlar hosil qilinadi (3.2-rasm).



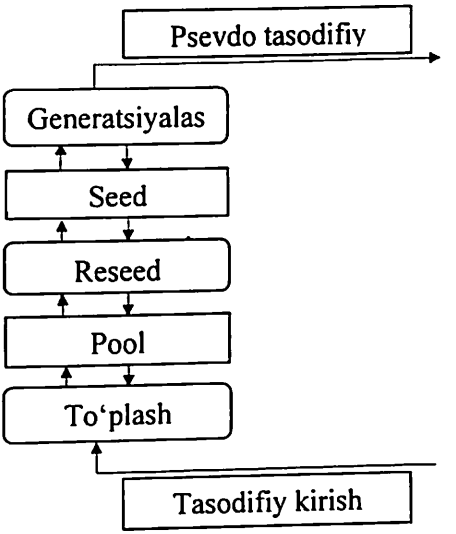
3.2-rasm. KPTSGning takshiliy jarayonlari

KPTSGning holat jarayoni muhim ahamiyatga ega bo‘lib, qator qism bosqichlardan iborat. Dastlab kiritilgan tasodifiy qiymatlar *pool* deb ataluvchi yig‘uvchida to‘planib boradi va u davomi amalga oshiriladi. Yig‘uvchi *pool* to‘plangan qiymatlar asosida generator ichki holati yangilanadi (*reseed*). Shundan so‘ng har bir generatsiya qilingan psevdotasodifiy blokdan so‘ng, *seed* jarayoni orqali generator ichki holati qaytadan yangilanadi. Bunda generatorning chiqish qiymatidan foydalaniladi. Umumiy holda *seed* va *reseed* jarayonlarining asosiy farqi ularning generator ichki holatini yangilashda foydalanadigan qiymatlarida. Boshqa so‘z bilan aytganda, *reseed* jarayonida ichki holat *pool* dagi qiymatlar asosida yangilansa, *seed* jarayoni generatsiyalash jarayonidan foydalangan holda uni amalga oshiradi.

DSA KPTSG. Digital Signature Standard (DSA) standartida elektron raqamli imzo algoritmi bilan birgalikda algoritmning zarur bo‘lgan parametrlarini hosil qilish uchun foydalaniladigan sodda PTSG ham keltirilgan. Ushbu algoritm SHA1 (yoki DES algoritmi) xesh funksiyasiga asoslanganda $N = 160$ yoki uning boshqa ($160 \leq N \leq 512$) qiymatlaridan ham foydalanilishi mumkin. $N = 160$ hol uchun generatorning ishlash ketma-ketligi quyidagicha:

1. KPTSG uzluksiz o‘zgarib turuvchi holat X_i dan iborat.
2. KPTSG tanlovga ko‘ra kirish qiymati W_i ni qabul qiladi. Agar bu qiymat amalga oshirilmasa, u holda u nolga teng deb olinadi.
3. KPTSG har bir chiqish bloki uchun quyidagilarni amalga oshiradi:

a. $output[i] = hash((W_i + X_i) mod 2^{160})$;
b. $X_{i+1} = (X_i + output[i] + 1) mod 2^{160}$.



3.3-rasm. Umumiy KPTSG, doimiy ichki holatni yangilab borish jarayoni

DSA KPTSG. Digital Signature Standard (DSA) standartida elektron raqamli imzo algoritmi bilan birgalikda algoritmning zarur bo'lgan parametrlarini hosil qilish uchun foydalaniladigan sodda PTSG ham keltirilgan. Ushbu algoritm SHA1 (yoki DES algoritmi) xesh funksiyasiga asoslanganda $N = 160$ yoki uning boshqari qiymatlaridan $(160 \leq N \leq 512)$ ham foydalanilishi mumkin. $N = 160$ hol uchun generatorning ishlash ketma-ketligi quyidagicha:

4. KPTSG uzluksiz o'zgarib turuvchi holat X_i dan iborat.
5. KPTSG tanlovga ko'ra kirish qiymati W_i ni qabul qiladi. Agar bu qiymat amalga oshirilmasa, u holda u nolga teng deb olinadi.
6. KPTSG har bir chiqish bloki uchun quyidagilarni amalga oshiradi:
   a. $output[i] = hash((W_i + X_i) mod 2^{160})$;
   b. $X_{i+1} = (X_i + output[i] + 1) mod 2^{160}$.

RSA REF KPTSG. RSAREF 2.0 hujjatida keltirilgan KPTSGi ikki amaldan: MD5 asosida xeshlash va $mod 2^{128}$ bo'yicha qo'shishdan iborat. Ushbu PTSGning amalga oshirish ketma-ketligi quyidagicha:

1. 128 bitli sanoq C_i berilgan bo'lsin.
2. Agar dastlabki kirish qiymati X_i bo'lsa, $C_{i+1} = (C_i + MD5(X_i))mod2^{128}$ hisoblanadi.
3. Psevdotasodifiy ketma-ketlik quyidagicha hisoblanadi:
   a. $output[i] = MD5(C_i)mod2^{128}$;
   b. $C_{i+1} = (C_i + 1)mod2^{128}$.

Entropiya to'plovchilar. Ushbu tizimlar odatda "haqiqiy" tasodifiy sonlar *generatori deb ham yuritiladi* va ular turli manbalardan tasodifiy qiymatlar (entropiya)ni to'playdi hamda bevosita taqdim etadi. Ular aksariyat hollarda xavfsiz deb qaralsada, qiymatlarni generatsiya qilish tezligi past.

CryptGenRandom. Ushbu kriptografik PTSGi Microsoft CryptoAPI ichida mavjud bo'lib, Windows OTdagi barcha ilovalar undan foydalanishi mumkin. Ushbu generator gibrid sanalib, entropiya to'plovchi va PTSGlaridan iborat.

Ushbu generatordan kriptografik algoritmlar sifatida RC4 oqimli shifrlash algoritmi va SHA1 xesh-funksiyasi foydalanilgan. Ushbu generator algoritmi yoki ochiq kodi chop etilmagan bo'lib, dizassamberlash natijasida olingan psevdokodi quyidigicha:

```
CryptGenRandom (Buffer , Len)
while (Len >0) {
    R := R ⊕ get_next_20_rc4_bytes ()
    State := State ⊕ R
    T := SHA -1'(State)
    Buffer := Buffer | T
        // | denotes concatenation
    R[0..4] := T[0..4]
        // copy 5 least significant bytes
    State := State + R + 1
    Len := Len - 20
}
```

Unga asosan har bir siklda 20 baytli tasodifiy qiymat hosil bo'ladi. Generatorning asosiy holati ikkita registor R va $State$ dan iborat. Ushbu ikki registor holati har bir siklda yangilanib boradi va chiqish qiymatni hosil qiladi.

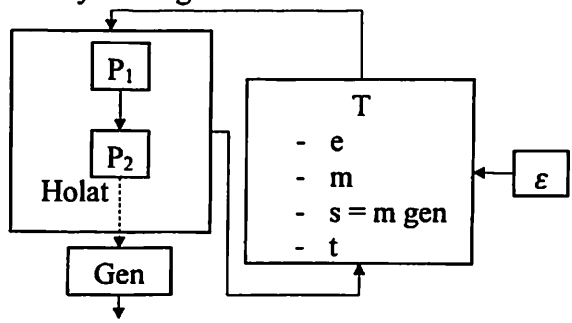
Ushbu generatorning entropiya to'plovchi qismi operatsion tizimning turli manbalaridan 3584 baytgacha ma'lumotni yig'ishi aytib

o'tilgan. Ushbu to'plangan ma'lumotlar "katta xesh funksiya" (VeryLargeHash) deb ataluvchi funksiya yordamida 80 baytga aylantiriladi.

/dev/random. Ushbu tasodifiy sonlar generatori Linux OT muhiti uchun eng keng tarqalgan bo'lib, u Teodor Tso tomonidan ishlab chiqilgan va ushbu generator Linux 1.3.30 dan boshlab OT o'zak qismiga aylangan. Ushbu tasodifiy sonlar genaratori turli manbalardan keladigan entropiya qiymatlarini yig'ishga asoslangan. Talab etilgan tasodifiy qiymat to'plangandan so'ng, generator chiqish qiymatini taqdim etadi. Shuning uchun ushbu generator talab qilingan qiymat mavjud bo'lmaganda bloklangan holatda bo'ladi.

Bundan tashqari ushbu algoritm asosida yaratilgan */dev/urandom* generatori mavjud bo'lib, u entropiya to'plovchi va KPTSGlari mujassamlashganidan iborat.

/dev/random generatori ikkita "pul" (pool) dan iborat. Birlamchi pul $\mathcal{P}_1$ tashqi hodisalar manbai $\mathcal{E}$ dan keluvchi entropiyani to'plash uchun foydalanilsa, ikkinchi pul $\mathcal{P}_2$ tasodifiy qiymatlarni generatsiya qilish uchun foydalaniladi. Bunda baytlar $\mathcal{P}_1$ dan $\mathcal{P}_2$ ga ko'chirib o'tkaziladi. "Pul"lar bilan aralashtirishni amalga oshirish uchun ikkita funksiya mavjud bo'lib, ulardan biri m – aralashtirish funksiyasi va gen – generatsiyalash funksiyasi sanaladi. Aralashtirish funksiyasi pulga kirishda foydalanilsa, generatsiya funksiyasi esa chiqishda tasodifiy ketma-ketliklarni hosil qilishda foydalanadi. Ikki pulning o'lchami 64 ga karrali bo'lgan bitdan iborat bo'lib, siqish funksiyasi sifatida CRC-32 funksiyasidan foydalanilgan.

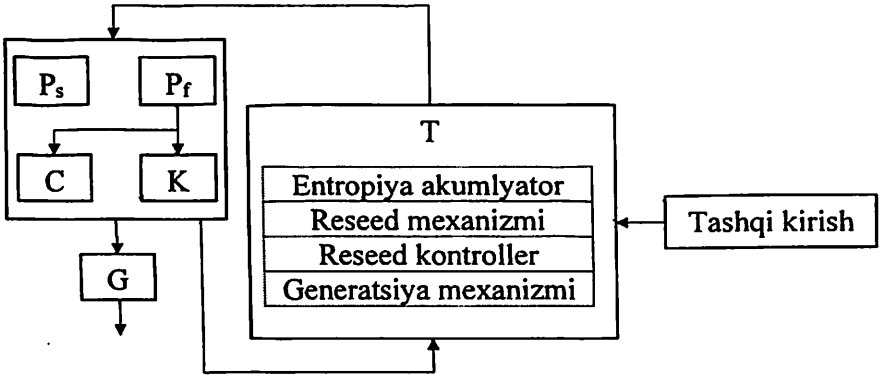


3.4-rasm. /dev/randomning umumiy strukturasi

Yarrow. Ushbu generator tasodifiy sonlar generatorini qurish uchun umumiy konsepsiya bo'lib, Counterpane Systems tashkilotida N.Fergusson, J. Kelsey va B.Shnayerlar tomonidan ishlab chiqilgan.

Ushbu konsepsiyaga asosan kriptografik xesh – funksiya asosida to'ldiriluvchi ikkita pul: *tezkor (fast)*, P_f va *sekin (slow)*, P_s to'ldirib boriladi. Ulardan blokli simmetrik shifrlash algoritmining kaliti K hosil qilinadi va u bilan ortib boruvchi sanagich qiymati C shifrlanadi. Ushbu konsepsiyaga ko'ra tanlangan xesh funksiya kriptografik xesh funksiya talablariga javob berishi va blokli simmetrik shifrlash algoritmi ham bardoshli bo'lishi talab etiladi. Xususan, Yarrow-160 da 160-bitli SHA1 xesh funksiyasi va 3DES algoritmidan foydalanilgan.

Yarrow konsepsiyasi 3.5-rasmda keltirilgan 4 ta komponentdan iborat. *Entropy Accumulator* jarayonida tashqi manbalardan kiruvchi ma'lumotlarni ikkita pulga joylashtirish va entropiyani hisoblashdan iborat. *Reseed Mechanism* jarayonida holat talabdagi kabi bo'lsa pullardan yangi kalit hosil qilinadi. *Reseed Control* mexanizmi esa *Reseed Mechanism* uchun yetarli entropiya to'planganini aniqlash uchun foydalaniladi. *Generation Mechanism* jarayonida hosil bo'lgan kalit va sanoq qiymatiga ko'ra tasodifiy baytlar ketma-ketligi hosil qilinadi.



3.5-rasm. Yarrowning umumiy tuzilishi

Ushbu generatorning bardoshliligi hosil qilingan xesh funksiyadan olingan xesh qiymat uzunligi m va kalit uzunligi k larning eng kichigining qiymatiga teng bo'ladi. Ya'ni, kalit 3DES uchun $k = 192$ va SHA1 xesh funksiya uchun $m = 160$ ligidan, generatorning bardoshligini 160 bitga teng deb qarash mumkin.

3.2. Statistik testlar

Axborot xavfsizligida tasodifiy sonlar generatoridan hosil bo'lgan ketma-ketliklarni tasodifiylik darajasini tekshirish uchun mos aniqlash

usuli mavjud bo'lishi zarur. Hozirgi kunda tadqiqotchilar tomonidan qurilmaga yoki dasturiy ta'minotga asoslangan yangi tasodifiy sonlar generatorlari ishlab chiqilmoqda. Biroq, ulardan hosil bo'lgan tasodifiy qiymatlarga baho bermasdan turib, amalda foydalanish tavsiya etilmaydi.

Tasodifiy sonlar generatoridan hosil bo'lgan qiymatlarni statistik testlash usullari asosida testlashdan keng foydalanilib, odatda quyidagi turdagi statistik testlar to'plamidan keng qo'llaniladi (3.1-jadval).

3.1-jadval

Statistik testlar to'plami va ularning xususiyatlari

№	Manba/ muallif	Testlar to'plami nomi	To'plam-dagi testlar soni
1.	Donald Knuth/ Stanford University	The Art Of Computer Programming Vol. 2 Seminumerical Algorithms	11 ta
2.	George Marsaglia/Florida State University	DIEHARD	15 ta
3.	Helen Gustafson, et. al./ Queensland University of Technology	Crypt-XS	6 ta
4.	Alfred Menezes, et. al./CRC Press, Inc.	Handbook of Applied Cryptography	
5.	Pierre L'Ecuyer, Richard Simard/ Université de Montréal	TestU01's test batteries	SmallCrush (10) Crush (96 ta) BigCrush (106 ta)
6.	Andrew Rukhin, et. al./NIST ITL	NIST Statistical Test Suite	15 ta

Donald Knuz tomonidan yozilgan "The Art of Computer Programming, Seminumerical Algorithms, Volume 2" nomli kitobda, muallif qator emperik testlarni keltirib o'tgan. Jumladan, *chastota* (frequency), *ketma-ketlik* (serial), *oraliq* (gap), *poker* (poker), *kupon to'plovchi* (coupon collector's), *o'rin almashtirish* (permutation), *yugirish* (run), *t ning maksimumi* (maximum-of-t), *kolliziya* (collision), *tug'ulgan*

kun oralig'i (birthday spacings) va *ketma-ketlik korrelasiyasi* (serial correlation) testlar.

DIEHARD testlar to'plami Djorj Marsaliya tomonidan ishlab chiqilgan bo'lib, 15 ta statistik testlardan: *tug'ulgan kun oralig'i* (birthday spacings), *bog'liqlikni almashtirish* (overlapping permutations), *matrisa rangini o'lchash* (ranks of 31x31, 32x32, 6x8 matrices), *"20-bitli so'zda maymun" testi* (monkey tests on 20-bit Words, monkey tests OPSO), *OQSO, DNA, ketma-ketlikdagi birlar sonini aniqlash* (count the 1's in a stream of bytes), *maxsus baytdagi birlar sonini aniqlash* (count the 1's in specific bytes), *minimal distansiya* (minimum distance), *tasodifiy sferalar* (random spheres), *siqish* (squeeze), *bog'liqliklar yig'indisi* (overlapping sums), *yugurish* (runs) va *kraps* (craps) iborat.

Crypt-XS statistik testlar to'plami Avstraliyadagi Kvinslend Texnologiyalar universitetining Axborot xavfsizligi tadqiqotlar markazidagi tadqiqotchilar tomonidan ishlab chiqilgan va u *chastota* (frequency), *binar hosila* (binary derivative), *nuqtalarni almashtirish* (change point), *yugirishlar* (runs), *ketma-ketlik murakkabligi* (sequence complexity) va *chiziqli murakkablik* (linear complexity) testlaridan iborat bo'lgan.

NIST statistik testlar to'plami (NIST Statistical Test Suite) NIST institutining Kompyuter xavfsizligi va Statistik injineriya bo'limlari tomonidan ishlab chiqilgan. Ushbu to'plam o'zida 15 ta statistik testlarni mujassamlashtirgan:

1. Chastota (Frequency) testi;
2. Bloklar uchun chastota (Frequency Test within a Block) testi;
3. Yugurishlar (Runs) testi;
4. Blok ichidagi eng uzun yugurish (Longest Run of Ones in a Block) testi;
5. Birlik matrisa rangini hisoblash (Binary Matrix Rank) testi;
6. Diskret Furye almashtirishlari (Discrete Fourier Transform) testi;
7. Davriy bo'lmagan qismlar (Non-overlapping Template Matching) testi;
8. Davriy bo'lgan qismlar (Overlapping Template Matching) testi;
9. Maurerning «Universal statistik» (Maurer's «Universal Statistical») testi;
10. Chiziqli murakkablik (Linear Complexity) testi;
11. Davomiylik (Serial) testi;
12. Taxminiy entropiya (Approximate Entropy) testi;
13. Ortib boruvchi yig'indi (Cumulative Sums) testi;

14. Tasodifiy tashriflar (Random Excursions) testi;
15. Tasodifiy tashriflar varianti (Random Excursions Variant) testi.

Ushbu bo'limda NIST statistik testlar to'plami bilan yaqindan tanishib chiqiladi. Mazkur testlar to'plami yordamida yagona tasodifiy qiymatni tasodifiylikka tekshirish ketma-ketligi 3.2-jadvalda aks ettirilgan. Ushbu ketma-ketlik umumiy testlash ssenariysini aks ettirgan bo'lib, NIST statistik testlar to'plamidan foydalanib testlashda muhim ahamiyatga ega.

3.2-jadval

Yagona binar ketma-ketlikni baholash muolajasi

Qadam va qadam jarayon	Izoh
Sizning nulevoy gipoteza holatingiz.	Binar ketma-ketlikni tasodifiy deb faraz qiling.
Statistik testlar ketma-ketligini amalga oshirish.	Testlash bitlar kesimida amalga oshiriladi.
P – qiymatni hisoblash.	$P \in [0,1]$ ga tegishli.
P – qiymatni α ga solishtirish.	$\alpha \in (0.001,0.01]$ kabi kelgilang. Agar $P \geq \alpha$ bo'lsa, testdan o'tgan, aks holda o'ta olmagan.

Mazkur testlash to'plamida kiritilgan har bir test usuli aynan bir maqsadga qaratilgan bo'lib, aynan bir holat bo'yicha baho beradi. Quyidagi 3.3-jadvalda har bir testning maqsadi va baho beruvchi asosiy zaiflik tomoni aks ettirilgan.

3.3-jadval

NIST statistik testlar to'plamining xususiyatlari

№	Statistik test	Zaiflikni aniqlash
1.	Frequency	Bir yoki nolni juda ko'pligini.
2.	Cumulative Sums	Ketma-ketlik boshlanishida bir yoki nolni juda ko'pligini.
3.	Longest Runs Of Ones	Birlarni uzoq vaqtli davomiyligi taqsimotining og'ishini.
4.	Runs	Bitlar ketma-ketligida tezkor (sekin) birdan nolga va aksincha o'tishlarni ko'rsatuvchi yugirishlarning umumiy katta (kichik) sonini.
5.	Rank	Mos tasodifiy ketma-ketlikdan qism takroriyligi natijasidagi rang taqsimotini og'ishini.

№	Statistik test	Zaiflikni aniqlash
6.	Spectral	Bitlar ketma-ketligidagi takrorlanish xususiyatini.
7.	Non-overlapping Template Matchings	Kesishmagan shablonlarni qanchalik ko'p paydo bo'lishini.
8.	Overlapping Template Matchings	Birlarning *m* bitli yugirishlarni paydo bo'lishini.
9.	Universal Statistical	Siqilishini (biror qoniniyatga asoslanishini).
10.	Random Excursions	Tasodifiy yurishda yagona holatga o'tishlar sonini taqsimotining og'ishini.
11.	Random Excursion Variant	Yagona holatga turli holatlardan o'tishlarning umumiy soni taqsimotining og'ishini.
12.	Approximate Entropy	*m* bit uzunlikdagi so'zlar taqsimotining bir xil emasligini.
13.	Serial	*m* bit uzunlikdagi so'zlar taqsimotining bir xil emasligini. Approximate Entropyga o'xshash.
14.	Linear Complexity	Cheklangan uzunlikdagi (qism) qator uchun chiziqli murakkablikning taqsimotidan og'ishini.

Har bir testni amalga oshirish uchun unga talab etilgan uzunlikdagi tasodifiy qiymat kiritilishi talab etiladi. NIST tomonidan keltirilgan har bir test uchun kiritiladigan tasodifiy qiymatlarga minimal uzunlik talabi qo'yilgan (3.4-jadval).

3.4-jadval

NIST statistik testlariga kirish qiymatlariga uzunlik talabi

№	Statistik test	Minimal kirish qiymat uzunligi (bit)
1.	Chastota (Frequency) testi	100
2.	Bloklar uchun chastota (Frequency Test within a Block) testi	100
3.	Yugurishlar (Runs) testi	100
4.	Blok ichidagi eng uzun yugurish (Longest Run of Ones in a Block) testi	128
5.	Birlik matrisa rangini hisoblash (Binary Matrix Rank) testi	38912

№	Statistik test	Minimal kirish qiymat uzunligi (bit)
6.	Diskret Furye almashtirishlari (Discrete Fourier Transform) testi	1000
7.	Davriy bo'lmagan qismlar (Non-overlapping Template Matching) testi	10^6
8.	Davriy bo'lgan qismlar (Overlapping Template Matching) testi	10^6
9.	Maurerning «Universal statistik» (Maurer's «Universal Statistical») testi	387840
10.	Chiziqli murakkablik (Linear Complexity) testi	10^6
11.	Davomiylik (Serial) testi	128
12.	Taxminiy entropiya (Approximate Entropy) testi	100
13.	Ortib boruvchi yig'indi (Cumulative Sums) testi	100
14.	Tasodifiy tashriflar (Random Excursions) testi	10^6
15.	Tasodifiy tashriflar varianti (Random Excursions Variant) testi	10^6

Tasodifiy ketma-ketliklar entropiyasini o'lchash usullari. Generatsiya qilingan psevdotasodifiy ketma-ketliklarni statistik testlar orqali tekshirish bilan har doim ham ularga aniq baho berib bo'lmaydi. Kalitlarni tasodifiy darajasini tekshirishda odatda ularning entropiya qiymatini o'lchash muhim ahamiyat kasb etadi.

NIST SP 800-90B nashridagi entropiyani o'lchash usuli. Ushbu nashrda *min-Entropy – minimal entropiya* usuli keltirilgan bo'lib, uning ketma-ketligi quyidagicha:

1. Tasodifiy sonlar generatoridan hosil qilingan ketma-ketliklar ma'lum bloklarga ajratilib, to'plam shaklida ifodalanadi. Bunda agar blok uchunligi n bit bo'lsa, to'plamdagi bloklar soni N kamida 2^n ga teng bo'lishi zarur.

2. To'plam ichida eng ko'p takrorlangan qiymat C_{max} ga o'zlashtiriladi.

3. Ushbu qiymat uchun ehtimollik $p_{max} = {}^{C_{max}}/_{N}$ ga teng bo'ladi.

4. Chegara qiymat $C_{chegara} = C_{max} + 2.3\sqrt{N * p_{max}(1 - p_{max})}$ tenglik orqali hisoblanadi.

5. Chegar qiymat uchun entropiya $H = -\log_2({}^{C_{chegara}}/_{N})$ tenglik orqali hisoblanadi.

6. Yakuniy minimal – entropiya = min (n, H) ga ya'ni, ikki qiymatning eng kichigiga teng bo'ladi.

/dev/random generatorida entropiyani o'lchash. Ushbu algoritmda muallif tomonidan isbotga ega bo'lmagan quyidagi entropiyani hisoblash tengligidan foydalanilgan:

$$\Delta_n^1 = time_n - time_{n-1},$$
$$\Delta_n^2 = \Delta_n^1 - \Delta_{n-1}^1,$$
$$\Delta_n^3 = \Delta_n^2 - \Delta_{n-1}^2,$$
$$\Delta_n = \min(|\Delta_n^1|, |\Delta_n^2|, |\Delta_n^3|),$$
$$entropy_n = log_2(\left[\frac{\Delta_n}{2}\right] (mod\ 2^{12})).$$

$time_n$ o'zgaruvchisi biror manbadagi tashqi hodisani vaqt belgisini ifodalaydi. Har bir manba o'zining $\{time_n\}_{n\geq 0}$ ketma-ketliklariga ega. $mod\ 2^{12}$ dan foydalanish esa entropiya qiymatini ko'pi bilan 12 bitga teng bo'lishini bildiradi.

Yarrow generatorida entropiyani o'lchash. Mualliflar tomonidan mazkur algoritm uchun entropiyani to'plash uchun o'zgacha usuldan foydalanilgan. Har bir hodisalar manbasi uchun alohida entropiyani o'lchash sanog'i qo'yilgan bo'lib, har bir generatorning ichki holati yangilangandan so'ng, ular nolga olib kelingan.

Ushbu generatorning keyingi avlodi sanalmish *Fortuna* generatorida esa hodisalar manbasidan kelgan qiymatlarni 32 ta pulga taqsimlangan holda saqlash va ulardan generator ichki holatini yangilashda o'zgacha usuldan foydalanish orqali entropiyani hisoblash yo'lidan voz kechilgan.

Bundan tashqari entropiyani hisoblashda ko'plab usullardan foydalanilgan bo'lib, ular ichida EGD (Entropy Gathering Daemon) entropiya to'plovchisida foydalanilgan yondashuv muhim ahamiyat kasb etadi. Ushbu yondashuvga ko'ra manbadan olingan har bir bayt uchun bir bit entropiyaga ega deb faraz qilingan.

Umumiy holda mavjud entropiyani o'lchash usullarini turli statistik usullarga va farazlarga asoslanilganini yoki uni hisoblashdan voz kechilganligini ko'rish mumkin.

Nazorat savollari

1. Tasodifiy qiymatlar va ularning kriptografiyadagi o'rni?
2. Xavfsiz bo'lmagan tasodifiy bitlar generatori haqida ayting?
3. Tasodifiy va psevdotasodifiy sonlar generatori haqida ayting?
4. Kriptografik psevdotasodifiy sonlar generatori haqida ayting?
5. ANSI X9.17 KPTSG haqida ayting?
6. Entropiya to'plovchilar va ularning xususiyatlari?
7. Statistik testlar nima va ularning asosiy maqsadi nima?
8. DIAHARD testlar to'plami haqida ayting?
9. NIST statistik testlar to'plami haqida ayting?
10. Tasodifiy ketma-ketliklarni entropiyasini o'lchash usullari?
11. Yarrow generatorida entropiyani o'lchash tartibi?

IV. OCHIQ KALITLI SHIFRLASH ALGORITMLARI

4.1. RSA ochiq kalitli shifrlash algoritmi

Simmetrik kalitli kriptoalgoritmlar asosida yaratilgan kriptotizim axborot-kommunikatsiya tarmoqlarida ma'lumotlar almashinuvining muhofazasini ta'minlash masalalarini yechishda qanchalik ishonchli bo'lmasin, baribir undan amalda foydalanish jarayonida ayrim qo'shimcha xavfsizlikni ta'minlash masalalari kelib chiqib, ularning yechilishi talab etiladi. Shunday masalalardan biri kalitlarni tizim foydalanuvchilariga tarqatish masalasidir. Ishlab chiqilgan bardoshli kalitlarni tizim foydalanuvchilariga yetkazish xavfsizligi kafolatli ta'minlangan bo'lishi talab etiladi. Buning uchun esa qo'shimcha holda yana biror boshqa kriptotizimdan foydalanishga to'g'ri keladi. Bu masala yechimining qo'shimcha kriptotizimdan foydalanmay hal etilishi klassik va zamonaviy algebrada olingan ilmiy natijalar asosida yaratilgan *ochiq kalitli kriptotizim*larning vujudga kelishi bilan amalga oshirildi.

Ochiq kalitli kriptotizimlar bundan 32 yil muqaddam AQSh olimlari U. Diffi va M. Xellman tomonidan kashf etilgan bo'lib, ular katta sonli chekli to'plamlarda bir tomonlama funksiyalardan foydalanishga asoslangan. U. Diffi va M. Xellmanning 1976 yilda bosilib chiqqan "Kriptologiyada yangi yo'nalishlar" maqolasida ilgari surilgan "maxfiy kalitni uzatishni talab etmaydigan amaliy bardoshli maxfiy tizimlarni tuzish mumkin" degan fikri kriptologiyada Ochiq kalitli kriptotizimlarning yuzaga kelishi hamda ularning rivojlanish davrining boshlanishiga sabab bo'ldi.

Ochiq kalitli kriptotizimlarning yuzaga kelishi simmetrik tizimlarda yechilmay qolgan maxfiy shifrlash kalitlarini tarqatish va elektron raqamli imzo tizimlarini yaratish hamda qator zamonaviy masalalarni yechish imkoniyatini berdi.

Ochiq kalitli kriptotizimlar simmetrik kriptotizimlarga nisbatan o'nlab marta katta uzunlikdagi (*512*, *1024*, *2048*, *4096* bitli) kalitlardan foydalanadi va shu sabab yuzlab marta sekinroq ishlaydi. Ochiq kalitli kriptotizimlarning matematik asosida bir tomonlama oson hisoblanadigan funksiyalar (modul bo'yicha diskret darajaga oshirish funksiyasi, egri chiziqli elliptik va sh.k.) yotadi. Ochiq kalitli kriptotizimlar axborot xavfsizligining barcha muammolarini yechib berishga qodir hisoblanadi.

Ochiq kalitli kriptotizim mohiyati har bir foydalanuvchi uchun birini bilgan holda ikkinchisini topish, yechilishi murakkab bo'lgan masala bilan bog'liq kalitlar juftligini yaratishdan iborat. Bu juftlikni

tashkil etuvchi kalitlardan biri ochiq (oshkora), ikkinchisi maxfiy (shaxsiy) deb e'lon qilinadi. Ochiq kalit oshkora e'lon qilinadi, maxfiy kalit faqat uning egasigagina ma'lum bo'ladi. Biror foydalanuvchining ochiq kalitini bilgan holda uning maxfiy kalitini topishning amaliy jihatdan mumkin emasligi, yechilishi murakkab bo'lgan masalaning hal etilishini talab qilishi bilan kafolatlanadi. Ochiq ma'lumot, shu ma'lumotni olishi kerak bo'lgan foydalanuvchining ochiq kaliti bilan shifrlanib unga uzatiladi. Shifrlangan ma'lumotni olgan foydalanuvchi faqat uning o'ziga ma'lum bo'lgan maxfiy kalit bilan uni rasshifroklalash, ochiq ma'umotga ega bo'ladi.

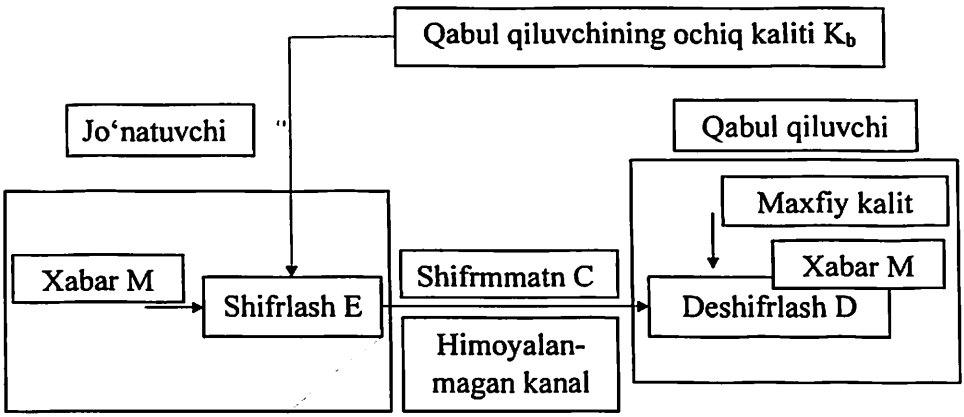
Ochiq kalitli kriptotizimlar algoritmlari ularning asosini tashkil etuvchi bir tomonli funksiyalar bilan farqlanadi. Ammo har qanday bir tomonli funksiya ham ochiq kalitli kriptotizimlar yaratish uchun va ulardan amaldagi axborot tizimida maxfiy aloqa xizmatini o'rnatish algoritmini qurish uchun qulaylik tug'dirmaydi.

Bir tomonli funksiyalarni aniqlanish ta'rifida nazariy jihatdan teskarisi mavjud bo'lmagan funksiyalar emas balki, berilgan funksiyaga teskari bo'lgan funksiyaning qiymatlarini hisoblash amaliy jihatdan maqsadga muvofiq bo'lmagan funksiyalar tushuniladi. Shuning uchun ma'lumotning ishonchli muhofazasini ta'minlovchi ochiq kalitli kriptotizimlarga muhim bo'lgan quyidagi talablar qo'yiladi:

1. Dastlabki ochiq ma'lumotni shifrma'lumot ko'rinishiga o'tkazish bir tomonli jarayon va shifrlash kaliti bilan shifr ma'lumotni ochish(rasshifrovkalash) mumkin emas, ya'ni shifrlash kalitini bilish shifr ma'lumotni rasshifrovkalash uchun yetarli emas.

2. Ochiq kalitning ma'lumligiga asoslanib, maxfiy kalitni zamonaviy fan va texnika yutuqlari yordamida aniqlash uchun ko'p sarf-harajatlar talab etadi. Bunda, shifrni ochish uchun bajarilishi kerak bo'ladigan eng kam miqdordagi amallar sonini aniqlash muhimdir.

Assimetrik shifrlash usullari ma'lumotlarni shifrlashda va rasshifrovkalashda alohida alohida kalitlardan foydalanadi. Shuning uchun ularda kalitlarni taqsimlash muammosi mavjud emas (4.1 – rasm).



4.1 - rasm. Assimetrik shifrlash usullarining umumiy ko'rinishi

Assimetrik shirflash algoritmlaridan foydalanib ma'lumotlarni shirflash quyidagi jarayonlardan iborat:

1. Kalitlar generatsiyasi.

B foydalanuvchi k_B maxfiy kalit asosida K_B ochiq kalitni generatsiya qiladi. Ochiq kalit K_B ochiq tarmoq orqali A foydalanuvchiga yoki tarmoqning boshqa foydalanuvchilariga uzatadi.

2. Ma'lumotlarni shirflash.

A foydalanuvchi yoki tarmoqning boshqa foydalanuvchisi K_B ochiq kalitdan foydalangan holda ochiq ma'lumotni shifrlaydi va uni ochiq tarmoq orqali yuboradi.

3. Shifr ma'lumotni rasshifrovkalash.

B foydalanuvchi qabul qilingan shifrmatnni o'zining k_B maxfiy kalit bilan rasshifrovkalaydi va ochiq matnga ega bo'ladi.

Assimetrik shifrlash usullarini yaratishda odatda hozirda yechimi mavjud bo'lmagan matematik muaamodan foydalaniladi. Bu matematik muammolar odatda bir tomonlama funksiya sifatida ifodalanadi. Bir tomonlama funksiya deb, o'ziga teskari bo'lgan funksiya mavjud bo'lmagan funksiyaga aytiladi.

Ma'lumki, eng ko'p foydalanib kelingan Ochiq kalitli tizimlarga bardoshliligi uchta muammoning, ya'ni faktorlash, diskret logarifmlash va EECh gruppasida diskret logarifmlash murakkabligi muammolaridan biri bilan belgilanadigan kriptotizimlar kiradi. Bular bilan bir qatorda qo'shimcha maxfiylikka ega bo'lgan Ochiq kalitli kriptotizimlar ham yuzaga kelmoqda.

RSA shifrlash algoritmi. Diffi va Xelman kriptografiya sohasida yangicha yondashishni targ'ib qilib, ochiq kalitli kriptotizimlarning barcha talablariga javob beradigan kriptografik algoritm yaratish taklifi bilan chiqdi. Birinchilardan bo'lib bunga javoban 1997 yil Ron Rayvets (Ron Rivest), Adi Shamir (Adi Shamir) va Len Adlmen (Len Adlmen)lar shu vaqtgacha tan olingan va amaliy keng qo'llanib kelingan ochiq kalitli shifrlash algoritm sxemasini taklif qildi va bu algoritm ularning nomi sharafiga RSA algoritmi deb ataldi. RSA algoritmi faktorlash murakkabligiga asoslangan shifrlash algoritmi hisoblanadi.

Rayvest, Shamir va Adlmen tomonidan yaratilgan sxema daraja ko'rsatkichiga asoslangan. Ochiq matn bloklarga ajratilib shifrlanadi, har bir blok ba'zi berilgan n sonidan kichik bo'lgan ikkilik qiymatga ega bo'ladi. Bundan kelib chiqadiki blok uzunligi $log_2(n)$dan kichik yoki teng bo'lishi kerak. Umuman olganda amaliyotda blok uzunligi 2^kga teng deb olinadi, bu yerda $2^k < n \leq 2^{k+1}$. Ochiq matn M bloki va shifrlangan matn C bloki uchun shifrlash va rasshifrovkalash quyidagi formula bilan hisoblash mumkin.

$$M = M^e mod n,$$

$$M = C^d mod n = (M^e)^d mod n = M^{ed} mod n.$$

Jo'natuvchi ham, qabul qiluvchi ham n ni qiymatini bilishi kerak. Jo'natuvchi e ni qiymatini, qabul qiluvchi esa faqat d ni qiymatini bilishadi. Ushbu sxema ochiq kalitli shifrlash algoritmi hisoblanadi, $KU=\{e,n\}$- ochiq kalit va $KR=\{d,n\}$-maxfiy kalit hisoblanadi.Bu algoritm ochiq kalit yordamida shifrlanishi uchun, quyidagi talablar bajarilishi kerak.

1. Shunday e, d va n qiymatlar mavjud bo'lish kerakki, barcha $M < n$ uchun $M^{ed} = Mmodn$ tenglik o'rinli bo'lishi kerak.

2. Barcha $M < n$ uchun M^e va C^d ning hisoblash oson bo'lishi kerak.

3. Amaliy jihatdan e va n ni bilmasdan turib d ni qiymatini bilish mumkin bo'lmasligi kerak.

Birinchi shartga binoan quyidagi munosabatni topish kerak

$$M^{ed} = Mmodn.$$

Eyler funksiyasiga asosan: har qanday ikkita p va q tub son va har qanday n va m butun sonlar uchun, $n=p*q$ va $0 < m < n$, va ixtiyoriy k butun son uchun quyidagi munosabat bajariladi.

$$m^{k\varphi(n)+1} = m^{k(p-1)(q-1)+1} \equiv m \bmod n,$$

Bu yerda $\varphi(n)$ Eyler funksiyasi bo'lib, n dan kichik va n bilan o'zaro tub bo'lgan musbat butun son. Eyler funksiyasi $\varphi(n)$ bilan o'zaro tub bo'lgan e son tanlab olinadi va talab qilinayotgan munosabat quyidagi shart asosida bajariladi.

$$e * d = k\varphi(n) + 1.$$

Bu quyidagi munosabat bilan ekvivalent:

$$e * d \equiv 1 \, mod\varphi(n),$$

$$d \equiv e^{-1} mod\varphi(n),$$

e va d, $\varphi(n)$modul bo'yicha o'zaro teskari son, ya'ni $gcd(\varphi(n), e) = 1$.

Yuqorida keltirilgan parametrlar asosida RSA sxemasini quyidagicha tasniflash mumkin:

p va q - tub sonlar (maxfiy, tanlab olinadi),

$n=p*q$ (ochiq, hisoblanadi),

shunday e, $gcd(\varphi(n), e) = 1, 1 < e, \varphi(n)$ (ochiq, tanlab olinadi),

$d \equiv e^{-1} mod\varphi(n)$ (maxfiy, hisoblanadi).

Maxfiy kalit $\{d, n\}$ dan, ochiq kalit esa $\{e, n\}$ dan iborat bo'ladi. Faraz qilaylik A foydalanuvchi ochiq kalitini elon qildi va B foydalanuvchi unga M xabarni jo'natmoqchi. B foydalanuvchi $C = M^e(modn)$hisoblab Cni jo'natadi. Shifrlangan matnni qabul qilgan A foydalanuvchi $M = C^d(modn)$ yordamida rasshifrovkalab dastlabki ochiq matnga ega bo'ladi.

Misol.

1. Ikkita tub son tanlab olinadi, $p=7$ va$q=17$.
2. $n=p*q=7*17$ hisoblanadi.
3. Eyler funksiyasi hisoblanadi $\varphi(n) = (p-1) * (q-1) = 96$.
4. Eyler funksiyasi $\varphi(n) = 96$ bilan o'zaro tub bo'lgan va undan kichkina bo'lgan e tanlab olinadi; bizni, misolimizda $e = 5$.
5. $d * e = 1mod\ 96$ va $d < 96$ shartni qanoatlantiruvchi d soni topiladi. $d = 77, 77 * 5 = 385 = 4 * 96 + 1$.

Natijada ochiq kalit $KU = \{5,119\}$ va yopiq kalit $KR = \{77,119\}$ hosil bo'ladi. Yuqoridagi misolda ochiq matn qiymati $M = 19$ olingan. Shifrlash formulasiga ko'ra ochiq matn qiymati ochiq kalit qiymati yordamida darajaga ko'tarilib, n modul bo'yicha qiymati olinadi, ya'ni 19 soni 5 darajaga ko'tariladi, natijada 2476099 hosil bo'ladi. Natijani 119 ga bo'linsa, qoldiq 66 ga teng bo'ladi. $19^5 = 66\ mod\ 119$ va shuning uchun ham shifrlangan matn 66 ga teng bo'ladi. Rasshifrovkalash uchun esa shifrlangan matn qiymati maxfiy kalit qiymati yordamida darajaga

ko'tarilib, n modul bo'yicha qiymati olinadi, ya'ni $66^{77} = 19\ mod\ 119$ hisoblanadi va dastlabki ochiq matn qiymatiga ega bo'linadi, ya'ni 19 ga.

Kalitlarni hisoblash. Ochiq kalitli kriptotizimlarga kalitlarni generatsiya qilish muhim ahamiyat kasb etadi. Har bir tomon ikkitadan kalit generatsiya qilishi kerak bo'ladi. Buni amalga oshirish uchun esa quyidagi vazifalarni bajarish kerak bo'ladi:

- ikkita p va q dan iborat tub son aniqlab olish;
- ikkinchisini hisoblash uchun, e yoki d sonlaridan birini tanlash.

Birinchi bo'lib p va q ni tanlash prosedurasini ko'rib o'tilsa. $n = p * q$ qiymati hammaga ma'lumligini inobatga olgan holda, p va q ni qiymatini to'liq tanlash usulida topish imkoniyatiga yo'l qo'ymaslik uchun, bu tub sonlar yetarli darajada katta bo'lishi kerak. Shu bilan bir qatorda katta tub sonlarni topish metodi amaliy jihatdan unumli bo'lishi kerak. Hozirgi kungacha samaradorligi yaxshi bo'lgan, ihtiyoriy katta sondagi tub sonni hisoblash metodi ishlab chiqilmagan. Bu metodlarda ko'proq taxminan istalgan uzunlikdagi va aniqlikdagi, tanlab olingan toq sonni tublikka tekshirish prosedurasi yotadi. Agar tanlab olingan son tub bo'lib chiqmasa, toki tub son tanlab olinmaguncha davom etadi. Sonlarni tublikka tekshiruvchi bir qator testlar mavjud bo'lib, bu testlarining deyarli barchasi ehtimollik xarakteriga ega. Ya'ni testlash natijasi berilgan butun sonni ehtimoliy tubligini aniqlaydi. To'liq ishonch bo'lmasligiga qaramasdan, bunday testlarning bajarilishi, ishonchliligi ta'minlanganligi ehtimoli birga yaqin bo'ladi.

RSA algoritmining himoyalanganligi. RSA algoritmining uch xil mumkin bo'lgan kriptotihlil usuli mavjud bo'lib, ular quyidagilardan iborat:

- Oddiy tanlash usuli. Bunda barcha mumkin bo'lgan maxfiy kalitlarni tekshirish taklif qilinadi.
- Matematik analiz. Shunday bir nechta usullar mavjud bo'lib, ularning hammasi ikkita tub sonli ko'paytmaning ko'paytuvchilarini topishga ekvivalent.
- Vaqt sarfi bo'yicha analiz. Shifrlash algorimining bajarilishiga ketgan vaqtni analiz qilishga qaratilgan.

Oddiy tanlash usuliga qarshi himoya RSA da ham, qolgan barcha kriptotizimlardagidek katta hajmdagi kalitlarni ishlatishdir. Bunday yondashishda e va d qancha katta bitdan iborat bo'lsa shuncha yaxshi. Lekin kalitlarni generatsiya qilishda murakkab hisoblashlarni ishlatish hamda shifrlash/rasshifrovkalash kalitlarining uzunligining katta bo'lishi tizimni sekin ishlashiga olib keladi.

RSA kriptotahlilida 3 xil matematik yondashuvni ajratib ko'rsatish mumkin.

- n-ni ikkita tub ko'paytuvchilarga ajratish. Bu o'z navbatida $\varphi(n) = (p-1)*(q-1)$hisoblashni, bu esa $d = e^{-1}(mod\varphi(n))$ ni aniqlab olish imkonini beradi.
- Oldindan p va q ni hisoblamasdan turib, to'g'ridan to'g'ri $\varphi(n)$ aniqlash.
- Oldindan $\varphi(n)$ ni aniqlamasdan turib, to'g'ridan to'g'ri d ni aniqlash.

Ko'p hollarda RSA shifri kriptotahlilida n qiymatni ikkita tub ko'paytuvchiga ajratish masalasi muhokama qilinadi. Berilgan n bo'yicha $\varphi(n)$ ni aniqlash masalasi bilan n ni ko'paytuvchilarga ajratish masalasi bilan ekvivalent hisoblanadi. Hozirgi kundagi ma'lum algoritmlarda e va n orqali d ni aniqlash muammosiga ketadigan vaqt bilan, ko'paytuvchilarga ajratish muammosiga ketadigan vaqt bir xil.

Vaqtga asoslangan hujumda kiruvchi ma'lumotning hajmiga bog'liq holda kompyuterda amalga oshiriladigan hisoblashlar vaqti turlicha bo'ladi. Shuning uchun hujumchi kiruvchi ma'lumot asosida uni hisoblash uchun sarflanadigan vaqtni taxmin qilishi mumkin. Shuningdek, kriptografik algoritmlarda hisoblash vaqti algoritm turi, kalit uzunligi, kompyuterning hisoblash imkoniyatiga bog'liq holda turli xil bo'lishi mumkin. Bitta so'rovni qayta ishlash uchun ketgan vaqtning sirqib chiqishi asosida umumiy vaqtni aniqlashga erishish mumkin. Ushbu vaqt asosida hujumchi tizim va kriptografik algoritm haqidagi ko'pgina ma'lumotlarni bilib olishi mumkin.

Sonni darajaga ko'tarib hisoblash Diffi-Xelman va RSA algoritmlarida mavjud. $R = y^x mod\, n$, n – ochiq kalitning bir qismi (RSA) yoki o'zgarmas son (Diffi-Xelman) va y olinadi. Hujumchining asosiy maqsadi x – maxfiy kalitni qo'lga kiritish. Bir nechta y uchun $y^x mod\, n$ ni hisoblaydi. $w - x$ kalitning bit uzunligi. Uning algoritmini quyidagicha keltirish mumkin:

Let $s_0 = 1$
For k=0 upto w-1:
  If (bit k of x) is 1 then
    Let $R_k = (s_k \cdot y) mod n$
  Else
    Let $R_k = s_k$
  Let $s_{k+1} = R_k^2 mod\, n$

EndFor

Return (R_{w-1})

Hujum natijasida $0, \ldots, (b-1)$ bitlari ma'lum bo'lgan holda, b ni aniqlashga harakat qilinadi. Barcha daraja ko'rsatkichlarini olish uchun $b = 0$ dan boshlash lozim.

x ning birinchi bitini bilish asosida, *For* siklining birinchi ketma-ketligini aniqlashi va s_b, belgisini hisoblashga erishishi mumkin. Keyingi sikl x ning birinchi nomalum bitiga qaratiladi. Agar 1 ga teng bo'lsa, $R_b = (s_b * y) mod\ n$ hisoblash amalga oshiriladi, 0 ga teng bo'lsa, keyingisiga o'tkazib yuboriladi.

Qoldiq haqidagi Xitoy teoremasi. $N = p * q$ berilgan va $p, q > 1$ o'zaro tub sonlar bo'lsa, unda,

$Z_N \simeq Z_p x Z_q$ va $Z_N^* \simeq Z_p^* x Z_q^*$.

Bu yerda, $\simeq$ izomofirzmni anglatadi. Ya'ni, $G \simeq H$ bo'lsa, G dan H ga izomofirzm deb o'qiladi hamda G va H to'plamlarining turi va o'lchami o'zaro teng.

f funksiyasi $x \in \{0, \ldots, N-1\}$ elementlarini birlashtiradi va (x_q, x_p) juftligi uchun $x_q \in \{0, \ldots, q-1\}$ va $x_p \in \{0, \ldots, p-1\}$ o'rinli bo'lsa unda,

$$f(x) \stackrel{def}{=} ([x mod p], [x mod q]).$$

Shuning uchun, f funksiyasi Z_N dan $Z_p x Z_q$ga izomorfizm va Z_N^* dan $Z_p^* x Z_q^*$ ga izomorfizm.

Isboti.

Agar $x \in Z_N$ unda (x_p, x_q) elementlari uchun $f(x)$ chiquvchi qiymat sanaladi. Bu yerda, $x_q \in Z_q$ va $x_p \in Z_p$. Shuningdek, $x \in Z_N^*$ bo'lsa, $(x_p, x_q) \in Z_p^* x Z_q^*$. Ammo, $x_p \notin Z_p^*$ chunki, gcd $([x mod p], p) \neq 1$ shartni qanoatlantiradi. Ammo, gcd $(x, p) \neq 1$. Bu esa, gcd $(x, N) \neq 1$ ni yuzaga keltiradi, chunki $x \in Z_N^*$.

Yuqorida f funksiyasi Z_N dan $Z_p x Z_q$ga va Z_N^* dan $Z_p^* x Z_q^*$ga izomorfizm ekanligi keltirildi. Birinchi navbatda f funksiyasi birga-bir jarayonni amalga oshirishini isbotlash talab etiladi. Aytaylik, $f(x) = (x_p, x_q) = f(x')$ unda $x = x_p = x' mod p$ va $x = x_q = x' mod q$. Bu esa, $(x - x')$ sonining p va q sonlariga bo'linishini ta'minlaydi. Shuningdek, $\gcd(p, q) = 1$ va $pq = N$ soni $(x - x')$ ga bo'linadi. Ammo,$x, x' \in Z_N$ uchun $x = x' mod N$ o'rinli. Bu esa, $x = x'$ va f birga-bir funksiya ekanligini anglatadi. $|Z_N| = N = p \cdot q = |Z_p| \cdot |Z_q|$, bu yerda,

Z_N, Z_p, Z_q ning o'lchami teng. Bundan kelib chiqib shuni aytish mumkinki, f birga-bir funksiya hamda ikki tomonlama xususiyatni ta'minlaydi.

f funksiya uchun quyidagi tenglik hosil qilinadi:

$$f(a+_N b) = ([(a+_N b) mod p], [(a+_N b) mod q]) =$$
$$= ([(a+b) mod p], [(a+b) mod q]) =$$
$$= ([a mod p], [a mod q]) \boxplus ([b mod p], [b mod q]) = f(a) \boxplus f(b).$$

Keltirilgan tenglikda $p|N$ bo'lganda, $[[X mod N] mod p] = [[X mod p] mod p]$ qoidasidan foydalanilgan.

Kengaytirilgan Qoldiq haqidagi Xitoy teoremasida $p_1, p_2, \dots, p_l$ o'zaro tub sonlar bo'lsa, $i \neq j$ uchun $\gcd(p_i, p_j) = 1$ va $N \stackrel{def}{=} \prod_{i=1}^{l} p_i$ bo'lsa, unda

$Z_N \simeq Z_{p_1} \text{x} \dots \text{x} Z_{p_l}$ va $Z_N^* \simeq Z_{p_1}^* \text{x} \dots \text{x} Z_{p_l}^*$.

Izomorfizm xususiyati yuqoridagi kabi hisoblanadi.

4.2. El-Gamal ochiq kalitli shifrlash algoritmi

Ushbu ochiq kalitli shifrlash algoritmi diskert logarifmlash muammosiga asoslangan bo'lib, kalitlar uzunligi teng bo'lgan holda bardoshligi RSA algoritmi bardoshligiga teng.

Kalit generatori. El-Gamal algoritmida kalit generatori quyidagi bosqichlardan iborat:

-p – katta tub son tanlanadi;

-$g<p$ shartni qanoatlantiruvchi g butun son tanlanadi;

-*maxfiy kalit* sifatida $a<p$ shartni qanoatlantiruvchi butun son tanlanadi;

-*ochiq kalit* sifatida $y = g^a mod p$ hisoblanadi;

-ochiq kalitlar jufti (y, g, p) ma'lumotni shifrlovchi tomonlarga yoki ixtiyoriy odamlarga tarqatiladi.

Ochiq matnni shifrlash. Shifrlanishi kerak bo'lgan M ochiq matn va ochiq kalitlar juftiga ega foydalanuvchi quyidagi ketma – ketlikdagi amallarni bajaradi:

- r sonidan kichik bo'lgan va $EKUB(k, p-1) = 1$ shartni bajaruvchi k -sonini tanlab olinadi;
- k son asosida $r = g^k mod p$ hisoblanadi;
- ochiq matnning har bir belgisi uchun $c = M * y^k mod p$ tenglikni hisoblash orqali shifrmatn olinadi;

- shifrlash amalga oshirilgach, k son o'chirib tashlanadi va qabul qiluvchiga *(r, c)* juftlik yuboriladi.

Shifrmatnni rasshifrovkalash. Shifrmatn va maxfiy kalitga ega foydalanuvchi quyidagi ketma – ketliklarni bajarish orqali ochiq matnga ega bo'ladi:

- qabul qilingan ma'lumotlar asosida $m = c * r^{p-a-1} mod p$ ochiq matn hisoblanadi.

Ushbu algoritm asosida sodda misol quyida keltirilgan:

A tomon o'zining maxfiy kaliti asosida ochiq kalit juftini hosil qiladi va uni B tomonga yuboradi. Olingan qiymatlar quyidagilar:

$g = 3;\ p = 31;\ a = 4; y = g^a mod p = (3^4) mod 31 = 19.$ Bu yerda (p, g, y) – ochiq kalitlar jufti va a maxfiy kalit.

Shifrlash. Bu bosqich A tomonning ochiq kalitlariga esa B tomondan amalga oshiriladi. Ochiq ma'lumot sifatida M=CDEF (2,3,4,5 –alfavitdani o'rni) olinib, $EKUB(k, p-1) = 1$ shartni qanoatlantiruvchi $k=7$ tanlandi. Shundan so'ng quyidagilar hisoblanadi:

$r = g^k mod p$ =(3^7)mod31=17;

$C_1 = m * y^k mod p$ =2 * (19^7)$mod 31 = 14$;

$C_2 = m * y^k mod p$ =3 * (19^7)$mod 31 = 21$;

$C_3 = m * y^k mod p$ =4 * (19^7)$mod 31 = 28$;

$C_4 = m * y^k mod p$ =5 * (19^7)$mod 31 = 4$;

Shundan so'ng C_i= { C_1, C_2, C_3, C_4 } lardan iborat C_i va r A tomonga yuboriladi.

Rasshifrovkalash. Bu jarayon maxfiy kalitga ega bo'lgan A tomondan amalga oshiriladi va ochiq matn olinadi:

$M_1 = C_1 * r^{p-a-1} mod p = 14 * 17^{(31-1-4)} \text{mod} 31 = 2;$

$M_2 = C_2 * r^{p-a-1} mod p = 21 * 17^{(31-1-4)} \text{mod} 31 = 3;$

$M_3 = C_3 * r^{p-a-1} mod p = 28 * 17^{(31-1-4)} \text{mod} 31 = 4;$

$M_4 = C_4 * r^{p-a-1} mod p = 4 * 17^{(31-1-4)} \text{mod} 31 = 5.$

Bu yerda diskert logarifmlash muammosi sifatida ochiq kalitlar jufti berilganda $y = g^a mod p$ tenglamadan a maxfiy kalitni topish mumkin, hozirda ushbu muammoning optimal usuli mavjud emas.

El-Gamal shifrlash algorimi xavfsizligi va unga bo'ladigan hujumlar. Ushbu algoritmga qaratilgan hujumlarni aktiv va passiv turlarga ajratish mumkin.

Passiv hujum. El-Gamal shifrlash algorimida berilgan quyidagi ketma-ketlikdan x noma'lumni topishga asoslangan. $p, \alpha, \beta, = \alpha^d,\ k_E =$

α^i va $y = x\beta^i$. Diffi Xellman algoritmining murakkabligi ham aynan shunga asoslangan.

Bobning maxfiy kalitini qidirish asosida x ni qayta tiklash.

$$"d = \log_\alpha \beta \, modp$$

Agar parametrlar to'g'ri tanlansa, faqatgina hisoblash murakkabligiga bog'liq bo'lib qoladi. Ushbu qadam muvofaqiyatli amalga oshirilsa, x ni quyidagi formula orqali hisoblashi mumkin:

$$x \equiv y(k_E^d)^{-1} modp$$

Boshqa tarafdan, Bobning d maxfiy elementi asosida Alisaning quyidagi tasodifiy i elementini hisoblashi mumkin:

$$i = \log_\alpha k \, modp$$

Bu asosida x ni quyidagi formula orqali hisoblashi mumkin:

$$x \equiv y(\beta^i)^{-1} modp$$

Har ikki holatda ham hujumchi chekli guruhda diskret logarifm muammosini yechishi lozim. Bundan tashqari uning xavfsizligini oshirish uchun Elliptik egri chiziqlar va Indeksni hisoblash usullarini kiritish hamda p ning o'lchami kamida 1024 bit bo'lishi lozim.

Aktiv hujum. Asimmetirik kriptotizimlarda ochiq kalitlarning egasi ma'lum va ochiq tarmoqda uzatiladi. Hujumchi o'rtadagi odam hujumini qo'llagan holda Alisadan kelgan xabarni o'zgartirib Bobga va aksincha jo'natish orqali maxfiy kalitni olishga harakat qilishi mumkin.

Uning boshqa zaifligi sifatida ikki tomon o'rtasidagi maxfiy element i takror foydalanilmaydi. Tasavvur qilaylik Alisa x_1 va x_2 xabarlarni shifrlash uchun i qiymatdan foydalangan. Ushbu holatda ikki niqob kalit $k_M = \beta^i$ bir xil bo'lishi lozim. Alisa ikkita shifr ma'lumotni uzatadi: (y_1, k_E) va (y_2, k_E). Agar hujumchi birinchi xabarni taxmin qila olsa, unda niqob kalitni quyidagicha hisoblaydi:

$$k_M = y_1 x_1^{-1}$$

Bu asosida x_2 xabarlarni quyidagicha hisoblaydi:

$$x_2 = y_2 k_M^{-1} modp.$$

Boshqa xabarlar ham i qiymat yordamida shifrlanadi va shu yo'l asosida qayta tiklanadi.

Diffi Xellman kalitlarni taqsimlash algoritmi. U. Diffi va M.Ye. Xellmanning kalitlarni ochiq taqsimlash sistemasi ochiq kalitli boshqa kriptotizimlar kabi maxfiy kalitni maxfiy kanal orqali uzatilishining hojati yo'qligini ta'minlaydi, ammo autentifikatsiya masalasini yechmaydi va o'rtadagi odam hujumiga bardoshsiz. Ushbu kalitlarni almashish algoritmi ko'pgina tekin va pulli turdagi protokollarda (SSH, TLS, IPSec)

qo'llaniladi. Diffi Xellman algoritmi uchun quyidagi o'rin almashtirish o'rinli:

$$k = (a^x)^y = (a^y)^x modp$$

Ushbu k qiymat maxfiy hisoblanib, uni sessiya kaliti sifatida foydalanish mumkin. 4.1-jadvalda Diffi Xellman algoritmi mohiyati va unga misol keltirilgan.

4.1-jadval

Misol

Alisa	Hujumchi	Bob
Alisa va Bob ikkita g, p (p>g) sonni hosil qiladi. p=11, g=7	Buzg'unchiga ham p=11, g=7 ma'lum.	Alisa va Bob ikkita g, p (p>g) sonni hosil qiladi. p=11, g=7
Alisa o'zining maxfiy kalitini hosil qiladi. X_A=6		Bob o'zining maxfiy kalitini hosil qiladi. X_B=9
$Y_A=g^{X(A)}(modp)$ $Y_A=7^6 mod11=4$	⟶ ⟵	$Y_B=g^{X(B)}(modp)$ $Y_B=7^9 mod11=8$
Alisa Y_B=8 ni qabul qiladi.	Buzg'unchiga ham Y_A =4, Y_B = 8 ma'lum.	Bob Y_A=4 ni qabul qiladi.
Maxfiy kalit = $Y_B^{X_A} modp$ Maxfiy kalit = $8^6 mod11 = 3$		Maxfiy kalit = $Y_A^{X_B} modp$ Maxfiy kalit = $4^9 mod11 = 3$

Bu yerda, p va g sonlari ikki tomon uchun ma'lum bo'lib, p>g shartni qanoatlantirishi lozim. Tanlangan X_A va X_B=9 sonlari (2, ..., p-2) oraliqda bo'lishi talab etiladi. Shuningdek, p – katta tub son.

Diffi Xellman kalitlarni taqsimlash algoritmi xavfsizligi. Ushbu algoritm xavfsizligini *o'rtadagi odam hujumi* asosida tahlil etish mumkin. Chunki u α va p sonlarini biladi va Alisa va Bob o'rtasidagi seans kalitini olishga harakat qiladi. Shuningdek hujumchida ikki tomonning ochiq kalitlari ham mavjud. U $k = \alpha^{ab}$ ni hisoblash imkoniyatiga egami degan savol qo'yiladi. Bu yerda, $A = \alpha^a$ va $B = \alpha^b$. Ushbu muammo Diffi Xellman muammosi deb nomlanadi.

Takomillashgan Diffi Xellman muammosi. G chekli siklik guruh berilgan. $\alpha \in G$ va $A = \alpha^a$ va $B = \alpha^b$ sonlar G ga tegishli. α^{ab} ni hisoblash Diffi Xellman muammosi hisoblanadi.

Muhokamalar. Diffi-Xellman kalitlarni taqsimlash sxemasi ANSI X9.42 da standartlashtirilgan va TLS kabi bir qancha protokollarda

qo'llaniladi. Ushbu algoritm ikkita tomon o'rtasida kalitlarni almashishga mo'ljallangan bo'lib, guruh ichida esa, birlashgan Diffi-Xellman kalitlarni taqsimlash sxemasidan foydalanish mumkin.

El-Gamal ochiq kalitli shifrlash algoritmi GnuPG, OpenSSL, PGP va boshqa shu kabi kriptografik dasturlarda qo'llaniladi.

4.3. Takomillashgan ochiq kalitli shifrlash sxemalari

Takomillashgan ochiq kalitli shifrlash sxemalari sifatida Pailler, Goldvasser-Mikali va Rabin shifrlash sxemalarini keltirish mumkin. Ushbu sxemalarni kelajakda amaliyotga tadbiq etish katta natijalarni taqdim etadi.

– Rabin shifrlash sxemasi yashirin yo'llar orqali bir tomonlama almashtirish xususiyati asosida ochiq kalitli kriptotizimlarni qurishga qaratilgan.

– Pailler shifrlash sxemasi gomomorfik shifrlash algoritmlariga asoslangan va natijada ko'pgina algoritmlardan tashkil topgan mujassamlashgan kriptografik algoritmlarni ishlab chiqishga erishish mumkin.

– Goldvasser-Mikali sxemasi tanlangan ochiq matnlar asosidagi hujum (CPA) xavfsizligiga asoslanadi. Ushbu sxema ham gomomorfik shifrlash algoritmlari va sonlar nazariyasidan foydalanadi.

Rabin shifrlash sxemasi. Ochiq kalitlar kriptotizim va u modul bo'yicha kvadrat ildizni hisobash murakkabligi asoslangan. U yashirin yo'llar orqali bir tomonlama funksiya xususiyatiga ega.

Yashirin yo'llar orqali bir tomonlama funksiya. f bir tomonlama funksiya yordamida X to'plamdan Y to'plamga o'tishni anglatadi. Bu yerda yashirin yo'llar xususiyatlarini qo'llaydigan bo'lsak, ixtiyoriy $y \in IMf$, $x \in X$ uchun $f(x) = y$ teskari funksiya hosil bo'ladi. Ushbu funksiya asimmetrik shifrlashga asoslangan RSA, Rabin, El-Gamalya, McEliece, NTRUEncrypt va Polly Cracker kabi kriptografik algoritm va tizimlarda qo'llaniladi. Elektron raqamli imzoni qurishda foydalaniladi. Uning bardoshlilikni ta'minlashning asosiy xususiyati shundan iboratki, kirishda qo'llanilgan funksiyani bilmasdan uning teskarisini hisoblash imkoniyati mavjud emas. Ushbu funksiyani quyidagicha hisoblash mumkin:

$$f: \{0,1\}^{l(n)} \times \{0,1\}^{n} \rightarrow \{0,1\}^{m(n)}.$$

Bu yerda, $\{0,1\}^{l(n)}$ – ochiq kalitlar to'plami, $\{0,1\}^{m(n)}$ – n bitdan iborat chiquvchi qiymat. Quyidagi shartlar bajarilganda yashirin yo'llar orqali bir tomonlama deb nomlanadi:

1. Bir tomonlama xususiyatiga ega bo'lishi.

2. Samarali algoritm asosida M xabardar $M`$ hisoblanadi va bir nechta $Z$ kalitlar uchun $f(M) = f(M`)$ shart bajarilishi lozim.

3. Ma'lum M xabar va $f(M)$ asosida $f(M) = f(M`)$ tengligini bilgan holda $M \neq M`$ ni hisoblash murakkab jarayon.

Uning uchta asosiy ko'rinishi mavjud:

"Barchasi ammo biri" (All-but-one) yashirin yo'llar orqali bir tomonlama funksiya. Yashirin yo'llar orqali bir nechta bir tomonlama funksiyalar asosida quriladi va yetarli darajada axborotlar yo'qolishi yuzaga keladi. "Barchasi ammo biri" funksiyasi B to'plam bilan bog'liq va uning elementlari shox deb nomlanadi. Ushbu funksiya yo'qotish shoxi deb nomlangan b^* ($b^* \in$ B) elementini qabul qiladi va $g(\cdot,\cdot)$ funksiya hamda t yashirin o'tishni chiqaradi. g funksiya ixtiyoriy $b \neq b^*$ shox uchun $g(b,\cdot)$ yashirin kirishni ta'minlaydi. Bu yerda, $g(b,\cdot)$ – yo'qotish funksiyasi. Bundan tashqari, g funksiyasining xususiyatidan kelib chiqib, yo'qotish shoxi maxfiy sanaladi.

"Barchasi ammo N ta" (All-but-N) yashirin yo'llar orqali bir tomonlama funksiya. Ushbu funksiya N ta yo'qotish shoxlariga ega va qolganlari yashirish kirishni anglatadi. U yo'qotish shoxlari asosida shifrlangan ma'lumotni aniq ifodalashda qo'llaniladi. Boshqa shifrlangan ma'lumotlar yashirin funksiyalar asosida amalga oshiriladi. Yo'qotish shoxlari kalit uzunligiga mos bo'ladi, shuning uchun hujumchi yo'qotish funksiyasiga ega barcha shoxlarni qidirishda qo'pol kuch hujumidan foydalanadi. Ushbu yondashuvning asosiy kamchiligi sifatida, kalitlarning bardoshliligi N chiziqli ekanligini keltirish mumkin.

"Barchasi ammo ko'pchiligi" (All-but-many) yashirin yo'llar orqali bir tomonlama funksiya. Uning "Barchasi ammo N ta" yondoshuvidan asosiy farqi shundaki, rasshifrovkalash rasshifrovkalashda ko'p sonli yashirin shoxlardan foydalaniladi.

Quyida yashirin yo'llar orqali bir tomonlama funksiyaga misollar keltirilgan:

RSA algoritmi. RSA shifrlash algoritmida $n = p \cdot q$, lekin n soni ma'lum bo'lgan holatda p va q sonlarini hisoblash murakkab jarayon. Ma'lumotni shifrlash $E(m) = m^e mod n$ orqali amalga oshiriladi va e

soni $(p-1)*(q-1)$ ga o'zaro tub. p va q yashirin kirish sonlarini bilgan holatda, E^{-1} teskari funksiyani hisoblash oson.

Polli Kreker algoritmi. U quyidagi bosqichlardan tashkil topgan:

1. A tomon chekli maydondan tasodifiy son tanlaydi.

2. A tomon ushbu vektor berilgan nuqtada nolga intiladigan ko'phad tuzadi.

3. B tomon $p = \sum q_i * p_i$ yig'indini hosil qiladi.

4. B tomon A tomonga $p + m$ sonini jo'natadi.

Rabin shifrlash algoritmi yordamida shifrlangan ma'lumonti rasshifrovkalash katta sonlarning faktorlash muammosi kabi murakkab jarayon. Unda N modul bo'yicha kvadrat ildizni hisoblash murakkab. Faktorlash muammosi va kvadrat ildiz hisoblash bir-biriga o'xshash jarayon, ya'ni:

– N soning tub bo'luvchilari ma'lum bo'lgan holda, N modul bo'yicha kvadrat ildizni hisoblash mumkin.

– N modul bo'yicha kvadrat ildizi hisoblangan va N sonini tub ko'paytuvchilarga ajratishga erishish mumkin.

Rabin shifrlash algoritmida ochiq va yopiq kalitlardan foydalaniladi. Kalitlarni generatsiyalash quyidagi qadamlardan tashkil topgan:

katta, tub bo'lgan va $p \equiv q \equiv 3 \ mod \ 4$ shartni qanoatlantiradigan p va q sonlari olinadi;

$n = p * q$ hisoblanadi;

n ochiq kalit, p va q yopiq kalit.

Shifrlash. Ma'lumotni shifrlash quyidagi formula asosida amalga oshiriladi:

$$c = m^2 mod n$$

Ushbu algoritmda modul bo'yicha ko'paytirish amalidan foydalanganligi bois, RSA algoritmiga nisbatan tezroq amalga oshiriladi.

Misol. $m = 20$ bo'lsa, unda shifrlangan ma'lumot quyidagi ko'rinishga ega bo'ladi:

$c = m^2 mod \ n = 20^2 mod \ 77 = 400 mod \ 77 = 15.$

Rasshifrovkalash. Rasshifrovkalash uchun p va q yopiq kalitlar kerak. Rasshifrovkalash quyidagicha amalga oshiriladi:

Evklid algoritmi asosida $y_p * p + y_q * q = 1$ tenglikdan y_p va y_q sonlarini aniqlash lozim.

Qoldiq haqidagi Xitoy teoremasi asosida quyidagi 4 ta sonni hisoblash talab etiladi:

$$r_1 = (y_p * p * m_q + y_q * q * m_p) \ mod \ n$$

$$r_2 = n - r_1$$
$$r_3 = (y_p * p * m_q - y_q * q * m_p) \bmod n$$
$$r_4 = n - r_3$$

Ulardan biri haqiqiy ochiq matnni ifodalaydi. Rasshifrovkalash natijasida $m \in \{64,20,13,57\}$ sonlar kelib chiqadi va ildizlardan biri m xabarni ifodalaydi.

Matnni rasshifrovkalashda to'g'ri variantdan tashqari uchta yolg'on natija ham olinadi. Bu esa, Rabin kriptotizimining asosiy noqulayligi sanaladi va bu esa amaliyotda keng qo'llanilishiga to'siq bo'ladi.

Agar ochiq axborot matndan iborat bo'lsa, uni rasshifrovkalash murakkab jarayon emas, ammo ERI yoki tasodifiy bitlar ketma-ketligidan iborat bo'lsa, qator muammolarni yuzaga keltiradi. Uni bartaraf etish uchun shifrlashdan oldin ochiq matnga belgi qo'yish talab etiladi.

RSA shifrlash algoritmida xabarning darajasi katta songa ko'tarilsa, Rabinda esa, xabar son qiymatining kvadrati hisoblanadi. Shuning uchun uning tezligi yuqori hamda RSA bilan teng kriptobardoshlilikni ta'minlaydi.

Hujumchi ochiq kalit n ni faktorlash muammosini yechib, shifrlangan matnni ochishga erishishi mumkin. Shuningdek, Rabin shifrlash algoritmi tanlangan shifrmatnlar hujumiga bardoshsiz sanaladi.

Pailler shifrlash sxemasi. Paskal Peye tomonidan 1999 yilda yaratilgan. Ikkita tub sondan tashkil topgan sonning faktorlash muammosiga asoslangan. Masalan, 27, 37, 67, 73 va h.k. ushbu algoritm qo'shishga asoslangan Gomomorfik kriptotizimlarga asoslangan, ya'ni ochiq kalit va shifrmatn ma'lum bo'lgan holda, m_1 va m_2 ochiq matnga mos holda, $m_1 + m_2$ ochiq ma'lumotning shifrmatnini hisoblash mumkin.

Dastlab algoritmda modul bo'yicha bo'linishdan olingan qoliqdan ildiz hisoblashga qaratilgan. Uning 2006 yilda taklif etilgan usulida tasdiqlangan o'rin almashishlar evaziga samaradorligi va xavfsizligi yanada oshirilgan.

Algoritm quyidagi jarayonlardan tashkil topgan:

Kalitlarni generatsiyalash:

1. $\gcd(p * q, (p-1) * (q-1)) = 1$ shartni bajaruvchi p va q katta tub sonlar tanlanadi.
2. $n = p * q$ va $\lambda = lcm(p-1, q-1)$ hisoblanadi.
3. $g \in Z_{n^2}^*$ shartni qanoatlantirgan tasodifiy butun g soni tanlanadi.

4. $\mu = (L(g^{\lambda} \bmod n^2))^{-1} \bmod n$ hisoblanadi. Bu yerda, $L(u) = div(\frac{u-1}{n})$.

Ochiq kalitlar – (n, g).

Yopiq kalitlar - (λ, μ).

Shifrlash:

1. $m \in Z_n$ bo'lgan m xabarni shifrlash talab etiladi.
2. . $r \in Z_n^*$ bo'lgan r tasodifiy son tanlanadi.
3. $c = g^m * r^n \bmod n^2$ formula asosida shifrmatn hisoblanadi.

Rasshifrovkalash:

1. $c \in Z_{n^2}^*$ bo'lgan c shifrmatn qabul qilinadi.
2. $m = L(c^{\lambda} \bmod n^2) \cdot \mu \bmod n$ yordamida rasshifrovkalash amalga oshiriladi.

Elektron raqamli imzo uchun quyidagicha qo'laniladi:

$h: N \to \{0,1\}^k \in Z_{n^2}^*$ xesh qiymat hosil qilinadi.

m xabarni imzolash quyidagicha amalga oshiriladi,

$$s_1 = \frac{L(h(m)^{\lambda} \bmod n^2)}{L(g^{\lambda} \bmod n^2)} \bmod n$$

$$s_2 = (h(m) g^{-s_1})^{\frac{1}{n} \bmod \lambda} \bmod n$$

Elektron raqamli imzo (s_1 va s_2) juftligidan iborat.

Imzoni tekshirishda quyidagi shart bajarilsa u haqiqiy sanaladi:

$$h(m) = g^{s_1} s_2^n \bmod n^2.$$

Gomomorfik xususiyati. Peye algoritmining boshqa algoritmlardan asosiy farqli jihati, uning gomomorfik xususiyatga egaligi sanaladi. Ochiq ma'lumotlarni gomomorfik qo'shish quyidagicha amalga oshiriladi.

$$D(E(m_1, r_1) \cdot E(m_2, r_2) \bmod n^2) = m_1 + m_2 \bmod n.$$

Shifrmatnni g^{m_2} ga ko'paytirish natijasida ochiq matnga mos yig'indini qo'lga kiritamiz.

$$D(E(m_1, r_1) \cdot g^{m_2} \bmod n^2) = m_1 + m_2 \bmod n.$$

Peye shifrlash sxemasi elektron ovoz berishda, elektron lotoreyada va elektron valyuta tizimlarida qo'llaniladi.

Elektron ovoz berish. Peye shifrlash sxemasini qo'llash asosida bir nechta nomzoddan iborat jarayonlarda ovoz berishni tashkil etish mumkin va u quyidagi qadamlardan tashkil topgan:

1. N – saylovchilar soni va $k \in N$ hamda $N < 2^k$.
2. Saylovchi i nomzodga ovoz berishi uchun $2^{k(i-1)}$ sonini shifrlaydi va saylov koordinatoriga jo'natiladi.

3. Natijalarni hisoblash uchun, koordinator saylovchilar tomonidan shifrlangan barcha ma'lumotlarni rasshifrovkalaydi. Birinchi k bit birinchi nomzod uchun berilgan ovozlar sonini anglatadi, ikkinchi va undan keyingi nomzodlar uchun ham shu kabi hisoblanadi.

Elektron lotoreya. Peye shifrlash sxemasini qo'llash asosida elektron lotoreya quyidagicha amalga oshiriladi:

1. Lotoreyada N ta o'yin bor va har biri o'zining yagona raqamiga ega, $n \in \{0, 1, \ldots, N\}$.

2. Har bir o'yinchi tasodifiy son tanlaydi, uni shifrlaydi va o'yin tashkilotchisiga jo'natadi.

3. Yutuqli raqamni tanlash uchun, barcha shifrma'lumotlar rasshifrovkalanadi, ularning s yig'indisi hisoblanadi va g'olib $s \bmod n$ formula orqali aniqlanadi. Uni qalbakilashtirish imkoniyati deyarli mavjud emas yoki murakkab jarayon.

Elektron valyuta. Peye algoritmi o'z-o'zini yashirish xususiyatiga ega. Ya'ni, ochiq ma'lumotga o'zgartirish kiritmasdan shifrmatnni o'zgartirish imkoniyati mavjud. Uning bu xususiyatidan *ecash* kabi elektron valyuta tizimini ishlab chiqishda qo'llash mumkin. Natijada, kredit karta raqamini oshkor etmagan holda online savdoni amalga oshiriladi. Elektron lotoreya kabi haridorning ma'lumotlari shifrlanadi.

Goldvasser-Mikali shifrlash sxemasi. Shafi Goldvasser va Silvio Mikali tomonidan 1982 yilda yaratilgan ochiq kalitli shifrlash algoritmi. U yetarli darajada bardoshli bo'lsada, shifrmatn ochiq matndan 100 martagacha uzun bo'lganligi uchun samarasiz sanaladi. Algoritm bardoshliligini baholash uchun semantik bardoshlilik tushunchasi kiritilgan. Shifrlangan ma'lumot uni buzish uchun hech qanday foydali va yordamchi ma'lumotni taqdim etmaydi. Goldvasser va Mikali yashirin kirishli bir tomonlama funksiyalar shifrmatn haqidagi ma'lumotlarni berkitish samaradorligi past ekanligini ko'rsatib berishgan. Ushbu shifrlash sxemasi ehtimolli shifrlashni taqdim etadi.

*Ehtimolli shifrlash, bu shifrmatn asosida ochiq ma'lumot haqida axborot olishning mumkin emasligi.

Algoritm quyidagi jarayonlardan tashkil topgan:

Kalitlarni generatsiyalash: A tomon quyidagi qadamlarni amalga oshiradi.

1. $|p| = |q|$ shartni qanoatlantiruvchi p va q tasodifiy sonlar hosil qilinadi.

2. $N = p \cdot q$ hisoblanadi.

3. $\left(\frac{y}{p}\right) = \left(\frac{y}{q}\right) = -1$ shartni qanoatlantiruvchi y tasodifiy son ajratib olinadi. Bu yerda, $y \in J(N) nQR_N$.

Ochiq kalitlar – (N, y).

Yopiq kalitlar – (p, q).

Shifrlash. A tomonga $m = b_1, b_2, \ldots, b_l$ qatorini jo'natish uchun B tomon quyidagi jarayon amalga oshiriladi:

$for(i = 1, 2, \ldots, l)$
{
$x \leftarrow_U Z_N^*;$
$if(b_i == 0)\ c_i \leftarrow x^2 (mod\ N);$
$else\ c_i \leftarrow yx^2 (mod N);$
}

B tomon A tomonga $E_N(m) \leftarrow (c_1, c_2, \ldots, c_l)$ xabarini jo'natadi.

Rasshifrovkalash. $c_1, c_2, \ldots, c_l$ ketma-ketlikni qabul qilgan A tomon quyidagi qadamlarni bajaradi:

$for(i = 1,2, \ldots, l)$
{
$if(c_i \in QR_N) b_i \leftarrow 0;$
$b_i \leftarrow 1;$
}
$set\ m \leftarrow (b_1, b_2, \ldots, b_l).$

l bit ma'lumotni shifrlash uchun $O(l(\log_2 N)^2)$ bit hisoblashlarni amalga oshirish lozim. Bu esa, vaqtga bog'liq muammoni keltirib chiqaradi. Bir bit ochiq ma'lumotga $\log_2 N$ bit shifr ma'lumot mos keladi.

Xavfsizligi. Ushbu algoritm xatosiz ko'p sonli tasodifiy bitlar asosida shifrlangan ma'lumotni hosil qiladi. "Nol" belgilari ochiq matnda QR_N ko'phad asosida, "Bir" belgilar esa, $\frac{J_N(1)}{QR_N}$ ko'phad asosida taqsimlanadi.

Nazorat savollari

1. RSA algoritmining ishlash tartibi haqida ayting?
2. Assimetrik shifrlash algoritmining ishlash prinsipi, afzalligi va kamchiliklari?
3. Qoldiq haqidagi Xitoy teoremasi haqida ayting?
4. El-Gamal ochiq kalitli shifrlash algoritmi haqida ayting?

5. Diffi-Xelman kalitlarni ochiq taqsimlash algoritmi haqida ayting?
6. Takomillashgan ochiq kalitli shifrlash sxemalari?
7. Rabin shifrlash sxemasi haqida ayting?
8. Pailler shifrlash sxemasi haqida ayting?

V. ELEKTRON RAQAMLI IMZO ALGORITMLARI

5.1. Elektron raqamli imzo va uning ishlash prinsipi

Kriptografik sxemalar odatda ikki masalani yechishga yo'naltirilgan: Shifrlash (AES, 3DES yoki RSA), kalitlarni taqsimlash (Diffi-Helman yoki EECh).

Alisa va Bob simmetrik blokli shifrlash algoritmlari yordamida maxfiy ma'lumotlarni almashishlari mumkin. Buning uchun ikki tomon uchun ham umumiy bo'lgan simmetrik shifrlash kaliti bo'lishi lozim. Ushbu kalit yordamida ma'lumot ham shifrlanadi, ham rasshifrovka qilinadi. Shuning uchun ushbu kalitni hujumchining qo'liga tushishidan himoyalash lozim. Ammo simmetrik kriptotizimlar ishtirokchilarning o'zini xavfsizligini yetarli darajada himoya qila olmaydi.

Aloqa boshlanishidan oldin simmetrik shifrlash kaliti Diffi-Xellman kabi kalitlarni almashish ochiq kalitli kriptotizimi yordamida almashiladi. Shuningdek, ushbu sxemada uchinchi tomon Bobdan kelgan ma'lumotni o'zgartirib Alisaga va aksincha amallarni bajarsa, maxfiy ma'lumot buzg'unchining qo'liga tushishi yoki uni o'zgartirishi mumkin. Ushbu holatda ishonchli uchinchi tomon yordamida ularning haqiqiyligini tekshirish va jo'natilgan xabarning egasini aniqlash lozim. Buning ochiq kalitli kriptotizimlarga mansub Elektron raqamli imzo (ERI) algoritmlaridan foydalanish mumkin.

ERI ishlash prinsipi. Elektron raqamli imzo - elektron matnga ilova qilinadigan kriptografik almashtirishdan iborat bo'lib, uzatilgan xabarning butunligini va imzolovchining haqiqiy yoki haqiqiy emasligini aniqlash imkonini beradi.

Qabul qilib olingan ma'lumotlarning haqiqiy yoki haqiqiy emasligini aniqlash masalasi, ya'ni ma'lumotlar autentifikatsiyasi masalasi quyidagicha aniqlanadi.

Har qanday yozma xat yoki hujjatning oxirida shu hujjatni tuzuvchisi yoki tuzish uchun javobgar bo'lgan shaxsning imzosi bo'lishi tabiiy holdir. Bunday holat odatda quyidagi ikkita maqsaddan kelib chiqadi. Birinchidan, ma'lumotni olgan tomon o'zida mavjud imzo na'munasiga olingan ma'lumotdagi imzoni solishtirgan holda shu ma'lumotning haqiqiyligiga ishonch hosil qiladi. Ikkinchidan, shaxsiy imzo ma'lumot xujjatiga yuridik jihatdan mualliflikni kafolatlaydi. Bunday kafolat esa savdo–sotiq, ishonchnoma, majburiyat va shu kabi bitimlarda alohida muhimdir.

Hujjatlardagi qo'yilgan shaxsiy imzolarni soxtalashtirish nisbatan murakkab bo'lib, shaxsiy imzolarning mualliflarini hozirgi zamonaviy ilg'or kriminalistika uslublaridan foydalanish orqali aniqlash mumkin. Ammo elektron raqamli imzo xususiyatlari bundan farqli bo'lib, ikkilik sanoq sistemasi xususiyatlari bilan belgilanadigan xotira registrlari bitlariga bog'liq. Xotira bitlarining ma'lum bir ketma-ketligidan iborat bo'lgan elektron imzoni ko'chirib biror joyga qo'yish yoki o'zgartirish kompyuterlar asosidagi aloqa tizimlarida murakkablik tug'dirmaydi.

Bugungi yuqori darajada rivojlangan butun dunyo sivilizasiyasida hujjatlar, jumladan maxfiy hujjatlarning ham, elektron ko'rinishda ishlatilishi va aloqa tizimlarida uzatilishi keng qo'llanilib borilayotganligi elektron hujjatlar va elektron imzolarning haqiqiyligini aniqlash masalalarining muhimligini keltirib chiqarmoqda.

Ochiq kalitli kriptografik tizimlar qanchalik qulay va kriptobardoshli bo'lmasin, autentifikatsiya masalasining to'la yechilishiga javob bera olmaydi. Shuning uchun autentifikatsiya uslubi va vositalari kriptografik algoritmlar bilan birgalikda kompleks holda qo'llanilishi talab etiladi.

Quyida ikkita (A) va (B) foydalanuvchilarning aloqa munosabatlarida autentifikatsiya tizimi raqib tomonning o'z maqsadi yo'lidagi qanday xatti-harakatlaridan va kriptotizim foydalanuvchilarining foydalanish protokolini o'zaro buzilishlardan saqlashi kerakligini ko'rsatuvchi holatlar ko'rib chiqiladi.

Rad etish. Foydalanuvchi (A) foydalanuvchi (B) ga haqiqatan ham ma'lumot jo'natgan bo'lib, uzatilgan ma'lumotni rad etishi mumkin.

Bunday qoida buzilishining (tartibsizlikning) oldini olish maqsdida elektron (raqamli) imzodan foydalaniladi.

Modifikatsiyalash (o'zgartirish). Foydalanuvchi (B) qabul qilib olingan ma'lumotni o'zgartirib, shu o'zgartirilgan ma'lumotni foydalanuvchi (A) yubordi, deb ta'kidlaydi (da'vo qiladi).

Soxtalashtirish. Foydalanuvchi (B)ning o'zi ma'lumot tayyorlab, bu sohta ma'lumotni foydalanuvchi (A) yubordi deb da'vo qiladi.

Faol modifikasiyalash (o'zgartirish). (A) va (B) foydalanuvchilarning o'zaro aloqa tarmog'iga uchinchi bir (V) foydalanuvchi noqonuniy tarzda bog'lanib, ularning o'zaro uzatayotgan ma'lumotlarini o'zgartirgan holda deyarli uzluksiz uzatib turadi.

Niqoblash (imitatsiyalash). Uchinchi foydalanuvchi (B) foydalanuvchi (B)ga foydalanuvchi (A) nomidan ma'lumot jo'natadi. Yuqorida sanab o'tilgan: modifikatsiyalash, soxtalashtirish, faol

modifikasiyalash, niqoblash kabi aloqa tizimi qoidalarining buzilishini oldini olish maqsadida raqamli signaturadan – raqamli imzo va uzatiladigan ma'lumotning biror qismini to'la o'z ichiga oluvchi raqamli shifrmatndan iborat bo'lgan ma'lumotdan foydalaniladi.

Takrorlash. Foydalanuvchi (B) foydalanuvchi (A) tomonidan foydalanuvchi (B)ga jo'natilgan ma'lumotni takroran (B)ga jo'natadi. Bunday noqonuniy xatti–harakat aloqa usulidan banklar tarmoqlarida elektiron hisob–kitob tizimidan foydalanishda noqonuniylik bilan o'zgalar pullarini talon-taroj qilishda foydalaniladi. Ana shunday noqonuniy usullardan muhofazalanish uchun quyidagi chora - tadbirlari ko'riladi.

- imitatsiyalashga bardoshlilik – imitabardoshlilik;
- kriptotizimga kirayotgan ma'lumotlarni muhofaza maqsadlaridan kelib chiqib tartiblash.

Elektron raqamli imzo aloqa tizimlarida bir necha tur qoida buzilishlaridan muhofaza qilishni ta'minlaydi, ya'ni:

- maxfiy kalit faqat foydalanuvchi (A)ning o'zigagina ma'lum bo'lsa, u holda foydalanuvchi (B) tomonidan qabul qilib olingan ma'lumotni faqat (A) tomonidan jo'natilganligini rad etib bo'lmaydi;
- qonun buzar (raqib tomon) maxfiy kalitni bilmagan holda modifikatsiyalash, soxtalashtirish, faol modifikatsiyalash, niqoblash va boshqa shu kabi aloqa tizimi qoidalarining buzilishiga imkoniyat tug'dirmaydi;
- aloqa tizimidan foydalanuvchilarning o'zaro bog'liq holda ish yuritishi munosabatidagi ko'plab kelishmovchiliklarni bartaraf etadi va bunday kelishmovchiliklar kelib chiqqanda vositachisiz aniqlik kiritish imkoniyati tug'iladi.

Ko'p hollarda uztilayotgan ma'lumotlarni shifrlashga zarurat bo'lmaydi, uni elektron raqamli imzo bilan tasdiqlash kerak bo'ladi. Bunday holatlarda ochiq matn jo'natuvchining yopiq kaliti bilan shifrlanib, olingan shifrmatn ochiq matn bilan birga jo'natiladi. Ma'lumotni qabul qilib olgan tomon jo'natuvchining ochiq kaliti yordamida shifrmatnni rasshifrovkalab, ochiq matn bilan solishtirishi mumkin.

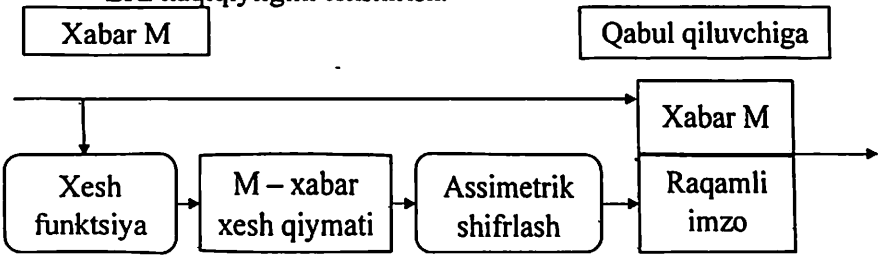
Asimmetrik shirflash algoritmlari yuqorida isbotlanganidek, katta hajmdagi ma'lumotlarni shifrlashda keng qo'llanilmaydi. Asimmetrik shifrlash algoritmlari kriptografiya sohasida asosan elektron raqamli imzo tizimlarida keng foydalaniladi.

ERI algoritmlari quyidagi vazifalarni bajaradi:

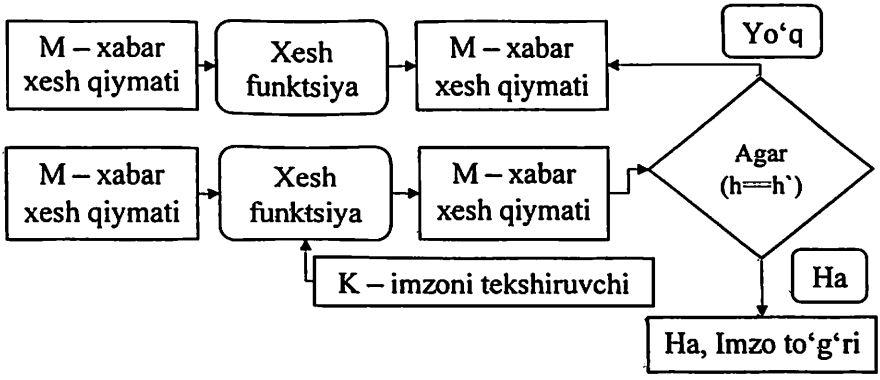
- imzo chekilgan ma'lumot butunligini;
- elektron hujjatga raqamli imzo qo'ygan subyektning mualliflikdan bosh tortmasligini ta'minlaydi;
- elektron hujjat manbaining haqiqiyligini aniqlash.

ERI tizimi quyidagi ikki jarayondan iborat (5.1, 5.2 - rasmlar):

- ERIni shakllantirish;
- ERI haqiqiyligini tekshirish.



5.1- rasm. Elektron raqamli imzoni shakllantirish jarayoni



5.2 - rasm. Elektron raqamli imzoni tekshirish jarayoni

ERI sxemalarining yuqoridagi vazifalarga qo'shimacha quyidagi imkoniyatlari mavjud:

Identifikatsiya va autentifikatsiya. Shaxs, kompyuter yoki kredit kartalarini tanib olish va haqiqiyligini tekshirish.

Ruxsatlarni nazoratlash. Huquqi bor foydalanuvchilarga manbaalardan foydalanishiga ruhsat berish.

Foydalanuvchanlik. Elektron tizimlardan foydalanish imkoniyatini ta'minlaydi.

Audit. Mavjud hodisalarning log fayllari asosida xavfsizlikka aloqador elementlar haqida dalillar to'plash va tahlillash.

Fizik xavfsizlik. Fizik urinish va harakatlardan himoyalash.

Anonimlik. Foydalanuvchini oshkor etish yoki uning nomidan noto'g'ri foydalanishdan himoyalash.

5.2. RSA algoritmiga asoslangan ERI

RSA algoritmiga asoslangan ERI algoritmini ortiqcha qiyinchiliksiz amalga oshirsa bo'ladi. Buning uchun shifrlash va deshirflash uchun foydalanilgan kalitlardan teskarisiga va ma'lumotning o'rnida uning xesh qiymatdan foydalanishning o'zi yetarli (5.3 - rasm).

ERI ni shakllantirish	**ERI ni tekshirish**
$H(M)^d mod n = P$ Bu yerda: H(M) – ma'lumotning xesh qiymati; d – imzo qo'yish kaliti (yopiq kalit); n,e – ochiq kalit; P – imzo.	$P^e mod n = H`(M)$ $\begin{cases} H`(M) \equiv & \text{Haqiqiy} \\ H`(M) \not\equiv & \text{Haqiqiy emas} \end{cases}$

5.3– rasm. RSA asosida ERI algoritmi

RSA algoritmi yordamida shifrlashda qo'llaniladigan kalitlar teskarisi tarzda foydalaniladi. Ya'ni, d – imzo qo'yish (shifrlash) va e – imzoni tekshirish (deshirflash) uchun foydalaniladi.

Isboti. RSA algoritmida quyidagi tenglik bajarilganida uning haqiqiyligi isbotlanadi:

$$P^e = (x^d)^e = x^{de} \equiv x \bmod n.$$

Chunki, ochiq va yopiq kalitlar o'rtasida quyidagi tenglik o'rinli:

$$d\,e \equiv 1 \bmod \varphi(n).$$

$x \in Z_n$ butun son va hisoblashdan keyin ham butun son bo'ladi. RSA algoritmi ochiq kalitli bo'lganligi bois, qabul qiluvchi yopiq kalit orqali shifrlangan ma'lumotni rasshifrovkalaydi. Elektron raqamli imzoda esa, imzo egasi yopiq kalit asosida x xabarni imzolaydi.

Misol. Bob $x = 4$ xabarni shifrlaydi va Alisaga tasdiqlash uchun jo'natadi. Uning sxemasi quyida keltirilgan:

Alisa		**Bob**
		p=3 va q=11 sonlari tanlanadi $n = p * q = 33$ hisoblanadi $\varphi(n) = (3-1) * (11-1) = 20$ $e = 3$ tanlanadi $d \equiv e^{-1} \equiv 7 \bmod 20$

Alisa		Bob
	$(n,e) = (33,3)$ ⟵	
		$x = 4$ xabarni imzolash $s = x^d \equiv 4^7 \equiv 16\ mod\ 33$
	$(x,s) = (4,16)$ ⟵	
Tasdiqlash: $x` = s^e \equiv 16^3$ $\equiv 4\ mod\ 33$ $x` \equiv x\ mod\ 33$ Demak imzo haqiqiy		

RSA asosidagi ERI xavfsizligi. Ochiq kalitli kriptotizimlarda kalitlarning autentifikatsiyasi asosiy xavfsizlik muammosi hisoblanadi. Ya'ni, haqiqiy foydalanuvchining ochiq kaliti uning juft yopiq kalitiga mos kelishi lozim. Agar hujumchi Alisa o'rnidan ma'lumotni imzolasa, Alisaning ochiq kaliti (sertifikati) asosida uni tekshirish mumkin. Unga qaratilgan asosiy hujumlar maxfiy kalitni hisoblashga urinadi. Buning uchun n sonini tashkil etuvchi p va q tub sonlarining faktorizatsiya muammosini yechish lozim. Uni bartaraf etish uchun katta o'lchamdagi sonlar tanlanishi lozim (Masalan, 1024 bit yoki undan kattaroq).

Qalbakilashtirish hujumi. Bobdan kelgan imzoni ushlab qoladi va hujumchi o'zining ochiq kaliti va imzosini jo'natadi. Alisa esa ushbu xabar Bob tomonidan jo'natilgan deb o'ylaydi. Bu kabi hujumlarni oldini olish uchun RSA to'ldirish (padding) sxemalaridan foydalanish lozim. RSA to'ldirishda Bob ma'lumot uzatish uchun aynan format yoki oldindan kelishilgan uzunlikni tanlashi mumkin. Bu esa, o'z-o'zidan hujumchiga nomalum.

5.3. El-Gamal algoritmiga asoslangan ERI

Amalda El-Gamal shifrlash usuliga asoslangan ERI algoritmalari keng qo'llaniladi. U RSA algoritmidan farqli o'laroq diskret logarifm muammosiga asoslangan. Bu usulda asoslangan ERI da kalitlarni generatsiyalash shifrlashdagi kabi amalga oshiriladi. Imzo qo'yish va imzoni tekshirish jarayonlari quyidagi kabi amalga oshiriladi (5.4-rasm).

ERI ni shakllantirish	ERI ni tekshirish
$r \equiv \alpha^{k_E} mod p$ $s = (x - dr){k_E}^{-1} mod(p-1)$ Bu yerda:	$\beta^r r^s mod p \equiv \alpha^x mod p$ tenglik o'rinli bo'lsa imzo haqiqiy, aks holda yo'q.

ERI ni shakllantirish	ERI ni tekshirish
x – ma'lumot; k_E – imzo qo'yish kaliti (maxfiy kalit); k_E - EKUB (k_E, p-1)=1 ga teng butun son; (r,s) – imzo.	Bu yerda: $\beta = \alpha^d mod p$ – ochiq kalit. $d \in \{2,3,\ldots,p-2\}$.

5.4 – rasm. El-Gamal asosidagi ERI

Uning xavfsizligi diskret logarifm muammosi asosida isbotlanadi va p soni sifatida 1024 bitdan katta bo'lgan va tub sonlarni generatsiyalash usullari asosida olingan sonni olish lozim. Xuddi shunday maxfiy kalit ham tasodifiy sonlarni generatsiyalash asosida hosil qilinadi.

Isboti. Qabul qiluvchida haqiqiy imzo va ochiq kalit bo'lsa, imzoni oson tekshirishi mumkin. (r,s) – imzo parametrlari berilgan bo'lsa, quyidagi tekshirish tengligini keltirish o'rinli:

$$\beta^r r^s \equiv (\alpha^d)^r (\alpha^{k_E})^s mod\ p \equiv \alpha^{dr+k_E s} mod\ p.$$

Agar α^x uchun quyidagi tenglik bajarilsa, demak, imzo haqiqiy:

$$\alpha^x = \alpha^{dr+k_E s} mod\ p.$$

Ferma teoremasiga asosan, tenglikning ikki tomonini eksponentlash asosida quyidagi tenglikka ega bo'linadi:

$$x \equiv dr + k_E s\ mod\ .p - 1.$$

$$s \equiv (x - dr){k_E}^{-1} mod\ p - 1.$$

Misol. Bob xabarni imzolaydi va Alisaga tasdiqlash uchun jo'natadi. Uning sxemasi quyida keltirilgan:

Alisa		Bob
		$p = 29, \alpha = 2, d = 12$ va $\beta = \alpha^d \equiv 7\ mod\ 29$
	$\xleftarrow{(p,\alpha,\beta) = (29,2,7)}$	
		$x = 26$ xabar $k_E = 5$ $r \equiv \alpha^{k_E} mod p \equiv 2^5 9$ $\equiv 3 mod\ 29$

Alisa		Bob
		$s = (x - dr)k_E{}^{-1} mod(p - 1) \equiv (-10) \cdot 17 \equiv 26\ mod\ 28$
	$(x,(r,s)) = (26,(3,26))$	
Tekshirish: $\beta^r r^s \equiv 7^3 \cdot 3^{26} \equiv 22\ mod\ 29$ $\alpha^x \equiv 2^{26} \equiv 22\ mod\ 29$ Imzo haqiqiy.		

El-Gamal asosidagi ERI xavfsizligi. Agar hujumchi diskret logarifmni hisoblash imkoniyatiga ega bo'lsa, unda a orqali maxfiy kalitni hosil qilishi mumkin. Natijada, xuddi qonuniy foydalanuvchi kabi xabarlarni imzolashi mumkin. Ularni oldini olish uchun diskret logarifm muammosida keltirilgan shartlarga amal qilish lozim. Olinayotgan sonlar belgilangan guruhlarga tegishli bo'lishiga qat'iy rioya etish talab etiladi.

Vaqtinchaik kalitdan qayta foydalanish. k kalitni qayta qo'llash asosida maxfiy kalitni hisoblashga asoslangan.

Qalbakilashtirish hujumi. RSA algoritmiga o'xshab, ixtiyoriy x xabar uchun qalbaki imzo shakllantiriladi. Hujumchi Bobning o'rnidan o'zini haqiqiy deb tanishtiradi va imzoni jo'natadi. Agar xabar xeshlangan bo'lsa, unda bu hujum ish bermaydi.

5.4. ERI standartlari

DSA ERI algoritmi. 1991-yilda NIST (National Institute of Standard and Technology) tomonidan DSA (Digital Signature Algorithm) algoritmiga asoslangan DSS (Digital Signature Standard) ERI standarti yaratildi. Ushbu algoritm chekli maydonda diskret logarifmlash muammosiga asoslangan. Xesh funksiya sifatida SHA1 standartidan foydalanilgan.

Imzoni shakllantirish:

1. Imzolanuvchi M ma'lumotni imzolashda quyidagi ketma – ketliklar bajariladi:

a. p – tub son tanlanadi ($2^{1023} < p < 2^{1024}$ va bit uzunligi 64 ga karrali);
b. q - tub son tanlanadi ($2^{159} < q < 2^{160}$ va $p-1$ ning bo'luvchisi);
c. $0 < h < p$ va $h^{(p-1)/q} \bmod p > 1$ shartlarni qanoatlantiruvchi h kattalik asosida $g = h^{(p-1)/q} \bmod p$ butun son hisoblanadi;
d. x – maxfiy kalit orqali, $y = q^x \bmod p$ ochiq kalit hisoblanadi (bu yerda: 0<x<q);
e. ma'lumotning xesh qiymatini hisoblanadi (H(M) – ma'lumot xesh qiymati [1;q] oraliqda).

2. Ma'lumot jo'natuvchisi tasodifiy k sonini tanlaydi ($0 < k < q$ shart bilan). Ushbu kattalik imzo shallantirilgandan so'ng o'chirib tashlanadi.
3. M ma'lumotni imzolari quyidagilarga teng bo'ladi:

$$r = g^k \bmod p \bmod q,$$
$$s = k^{-1}(xr + H(M)) \bmod q.$$

Hosil qilingan kattaliklar (r, s) malumot M ga qo'shib imzoni tekshiruvchi tomonga yuboriladi.

Imzoni tekshirish jarayoni:

Qabul qilingan M' ma'lumot va unga qo'yilgan imzo (r', s') asosida imzoni tekshirish jarayoni amalga oshiriladi. Bu ikki bosqichdan iborat. Agar imzo birinchi bosqichdagi tekshiruvdan o'ta olmasa, unda ikkinchi bosqichga o'tmaydi.

1. Qabul qilingan imzolar uchun $0 < s' < q$ yoki $0 < r' < q$ shart tekshiriladi. Bu shart bajarilsa ikkinchi bosqichga o'tiladi.
2. Ikkinchi bosqich quyidagilardan iborat:
   a. $v = (s')^{-1} (mod\ q)$ hisoblanadi.
   b. $z_1 = H(M')\ v \bmod q, \quad z_2 = r'\ v \bmod q$ qiymatlar hisoblanadi.
   c. Shundan so'ng $u = g^{z_1} y^{z_1} \bmod p \bmod q$ qiymat hisoblanadi.
   i. Agar $r' = u$ tenglik bajarilsa, u holda qo'yilgan elektron raqamli imzo haqiqiy ($M = M'$) bo'ladi. Aks holda imzo qalbaki deb topiladi.

EECh asosidagi ERI algoritmi. EECh asosidagi ochiq kalitli kriptotizimlar tub sonlar faktorizasiyasi yoki diskret logarifm muammosiga nisbatan xavfsizligi yuqori ekanligi isbotlangan. Ya'ni 160-256 bit kalit uzunlikdagi xavfsizligi RSA yoki El-Gamalning

1024-3072 bit kalitga teng. Ularga misol sifatida EC DSA va GOST R 34.10-2001 standartlarini keltirish mumkin.

EC DSA raqamli imzo algoritmi.

Imzoni generatsiya qilish algoritmi. Boshlang'ich ma'lumotlar: M - imzolanishi kerak bo'lgan ma'lumot, berilgan parametrlar va imzo kaliti. Natija: imzo (r, s).

1) $1 \leq k \leq n-1$ intervaldan tasodifiy k soni tanlanadi, bu yerda G nuqta tartibi $n > max\{2^{160}, 4\sqrt{p}\}$ shartni qanoatlantiruvchi tub son bo'lishi kerak.

2) $(x_1, y_1) := [k]G$ hisoblanadi.

3) $r := x_1 \, mod \, n$ hisoblanadi.

4) Agar $r = 0$ bo'lsa, u holda 1-qadamga boriladi, aks holda keyingi qadamga o'tiladi.

5) $z := k^{-1} \, mod \, n$ hisoblanadi.

6) $e := h(M)$ hisoblanadi.

7) $s := z(e + dr) \, mod \, n$ hisoblanadi.

8) Agar $s = 0$ bo'lsa, u holda 1-qadamga boriladi.

9) M-ma'lumot imzosi - (r, s) juftligidan iborat.

Imzoni tekshirish algoritmi. Boshlang'ich ma'lumotlar: M - ma'lumot, berilgan parametrlar, imzoni tekshirish kaliti va M-ma'lumot imzosi. Natija: imzo haqiqiyligi yoki qalbakiligi haqidagi tasdiq.

1)Agar $1 \leq r, s \leq n-1$ shart bajarilmasa, u holda imzo qalbaki va imzoni tekshirish algoritmi tugatiladi.

2)$e := h(M)$ hisoblanadi.

3)$w := s^{-1} \, mod \;\; n$ hisoblanadi.

4)$u_1 := ew \;\; mod \;\; n$ hisoblanadi.

5)$u_2 := rw \;\; mod \;\; n$ hisoblanadi.

6)$X := [u_1]G + [u_2]Q = (x_1, y_1)$ hisoblanadi.

7)Agar $r = x_1 \;\; mod \;\; n$ shart bajarilsa, u holda imzo haqiqiy, aks holda imzo qalbaki va imzoni tekshirish algoritmi tugatiladi.

GOST R 34.10-2001 EECh ERI standarti.

Imzoni generasiya qilish. Boshlang'ich ma'lumotlar: M ma'lumot, berilgan (elliptik chiziqqa aloqador) parametrlar va imzo maxfiy kaliti. Ushbu algoritmda Elliptik egri chiziq tenglamasi $p > 2^{255}$ shartni qanoatlantiruvchi tub xarakteristikali F_p maydonda deb qaraldi. Natija, imzo (r, s).

Imzoni generasiya qilish qadamlari:

1. $1 \le k \le n-1$ intervaldan ixtiyoriy k soni tanlansin, bu yerda G nuqta tartibi $2^{254} < n < 2^{256}$ shartni qanoatlantiruvchi son.

2. $(x_1,y_1)= [k]G$ hisoblansin, ya'ni tanlangan egri chiziqqa tegishli G nuqtani k marta qo'shilsin.

3. $r=x_1 \bmod n$ hisoblansin. Agar $r=0$ bo'lsa, 1-qadamga qaytilsin va boshqa k soni tanlansin.

4. M ma'lumotning xesh funksiyasi hisoblansin, ya'ni $e=H(M)$. Agar $H(M) \bmod n=0$ bo'lsa, u holda $H(M) \bmod n=1$ deb olinsin.

5. $0< d <n$ intervaldan olingan d maxfiy kalit asosida $s=(dr+ke) \bmod n$ hisoblab topilsin.

6. Agar $s=0$ bo'lsa, 1-qadamga qaytilsin va boshqa k soni tanlansin.

7. Hosil bo'lgan (r,s) sonlar juftligi M ma'lumotga qo'yilgan imzo hisoblanadi.

Imzoni tekshirish. Boshlang'ich ma'lumotlar M ma'lumot, berilgan (elliptik chiziqqa aloqador) parametrlar, imzoni tekshirish kaliti va M ma'lumot imzosi-(r,s). Natija: imzo haqiqiyligi yoki qalbakiligi haqidagi tasdiq.

Imzoni tekshirish qadamlari:

1. Agar $1 \le r, s \le n-1$ bajarilmasa, u holda imzo qalbaki va tekshirishni shu yerda to'xtatish mumkin.

2. $e= H(M)$ hisoblansin.

3. $w= H(M)^{(n-2)} \bmod n$ hisoblansin.

4. $u_1 = s\,w \bmod q$ hisoblansin.

5. $u_2 = (n-r)\,w \bmod n$ hisoblansin.

6. $X=[u_1]\,G+[u_2]\,Q=(x_1,y_1)$ hisoblansin.

7. Agar $x_1 \bmod n = r$ bo'lsa, imzo haqiqiy, aks holda imzo qalbaki va algoritm to'xtatiladi.

Muhokama: ERI imzo ochiq kalitli shifrlash algoritmlariga asoslangan, masalan RSA. Ammo DSA kabi algoritmlar mavjudki, ularni ma'lumotlarni shifrlash maqsadida qo'llab bo'lmaydi. DSA va RSA kabi algoritmlarining imzo sxemasida 1024 bitdan katta sonlar tanlanishi lozim. ECDSA kabi EEChga asoslangan algoritmlar uchun esa, kamida 160-256 bit olinishi maqsadga muvofiq.

Amalda ko'plab davlatlar o'zining ERI standartlariga ega. Ularga quyidagilarni kiritish mumkin:

- El-Gamalga asoslangan DSA standarti (AQSh);
- El-Gamalga asoslangan GOST R 34.10-94 standarti (Rossiya);
- EECh asoslangan ECDSA -2000 standarti (AQSh);
- EECh asoslangan GOST R 34.10-2001 standarti (Rossiya);

- Parametrli darajaga ko'tarish va EECh asoslangan O'zDSt 1092:2009 standarti (O'zbekiston Respublikasi).

5.5. Ochiq kalitli shifrlardan foydalanish muammolari

Shifrlash algoritmlari yordamida ma'lumot konfidensialligini ta'minlashga erishish mumkin. Ushbu masalani hal etishda asimmetrik shifrlash algoritmlaridan foydalanish quyidagi afzallik va kamchiliklarni keltirib chiqaradi:

Afzalligi:

– Maxfiy kalitni ochiq kanallar yordamida ochiq holda uzatish almashish mumkin. Kalitni almashish uchun maxsus, himoyalangan kanallardan foydalanish shart emas.

– Rasshifrovkalash kaliti xabarni qabul qiluvchi tomonidan generatsiyalanadi va uni ochiq tarmoqda jo'natish shart emas. Natijada maxfiy kalit konfidensiyalligi ta'minlanadi.

– Katta tarmoqlarda kalitlar soni simmetrik shifrlash algoritmlariga qaraganda soni kam.

Kamchiligi:

– Algoritmga o'zgartirish kiritish murakkab.

– Yuqori bardoshlilikni ta'minlash uchun uzun kalitlardan foydalanish lozim. 5.2-jadvalda simmetrik va asimmetrik shifrlash algoritmlarida teng bardoshlilik uchun mos kalit uzunliklari keltirilgan.

5.2-jadval

Simmetrik va asimmetrik shifrlash algoritmlari uchun kalit uzunliklari

Simmetrik kalit uzunligi (bit)	Asimmetrik kalit uzunligi (bit)
56	384
64	512
80	768
112	1792
128	2304

– Shifrlash va rasshifrovkalash tezligi simmetrik shifrlash algoritmlariga nisbatan past.

– Ma'lumotni shifrlash uchun katta hisoblash mashinalarini talab etadi, shuning uchun asimmetrik shifrlash algoritmlaridan Elektron raqamli imzoda ma'lumotning xesh qiymatini imzolashda va gibrid shifrlash algoritmlarida seans kalitni almashish maqsadlarida foydalaniladi.

Nazariy jihatdan matematik kriptobardoshliligi isbotlanmagan.

Nazorat savollari

1. Elektron raqamli imzo va uning ishlash prinsipi haqida ayting?
2. Elektron raqamli imzo qaysi hujumlarga nisbatan himoyani ta'minlaydi?
3. RSA algoritmiga asoslangan elektron raqamli imzo algoritmi haqida ayting?
4. El-Gamal algoritmiga asoslangan elektron raqamli imzo algoritmi haqida ayting?
5. Elektron raqamli imzo standartlari haqida ayting?
6. Elliptik egri chiziqqa asoslangan elektron raqamli imzo standartlari haqida ayting?

VI. KRIPTOGRAFIK PROTOKOLLAR

6.1. Kriptografik algoritmlardan foydalanish

Protokol va uning vazifalari. Ikki yoki undan ortiq tomonlar bajaradigan, biror-bir masalani yechish uchun loyihalashtirilgan harakatlar ketma-ketligi protokol hisoblanadi. Protokollar ishlashini namoyish qilish bir-nechta ishtirokchilar yordamida amalga oshiriladi (6.1-jadval).

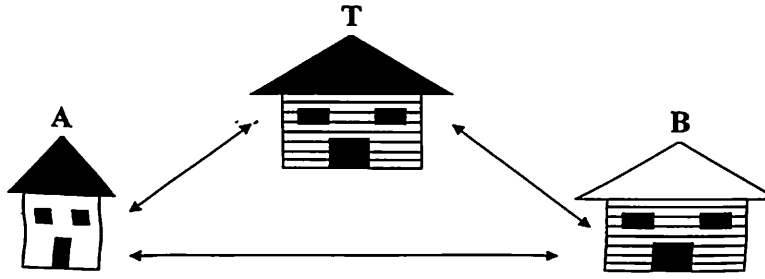
6.1-jadval

Protokol ishtirokchilari

Ishtirokchilar	Faoliyati	Belgilanishi
Alisa	Barcha protokollarning birinchi ishtirokchisi	**A**
Bob	Barcha protokollarning ikkinchi ishtirokchisi	**B**
Kerol	Uch va to'rt tomonli protokollar ishtirokchisi	**K**
Dev	To'rt tomonli protokollar ishtirokchisi	**D**
Trent	Ishonchli vositachi	**T**
Eva	Passiv buzg'unchi	**E**
Mellori	Yomon niyatli aktiv buzg'unchi	**M**

Jarayondagi asosiy ishtirokchilar – **A** va **B** bo'lib, ular umumiy qabul qilingan barcha ikki tomonlama protokollarni bajaradilar. Qoida bo'yicha barcha protokollarni **A** inisializasiya qiladi, **B** esa javob beradi. Agar protokol 3 va 4 tomonlar ishtirokini talab qilsa, **K** va **D** qo'shiladi. Boshqa ishtirokchilar maxsus yordamchi rolni bajarishadi.

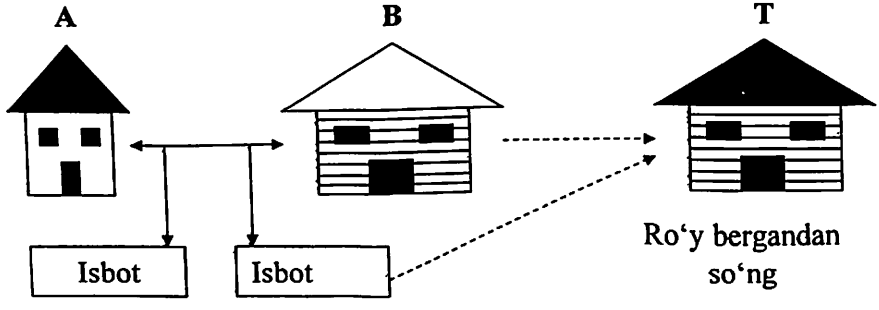
Vositachi yordamidagi protokollar. Vositachi deb protokolni bajarilishini yakuniga yetkazishga ishonch bildirilgan manfaatdor bo'lmagan uchinchi tomonga aytiladi (6.1-rasm). Vositachining "manfaatdor bo'lmasligi" protokol bajarilishining natijasi hamda protokol ishtirokchisining hech biri u uchun ahamiyatga ega emasligini bildiradi. "Ishonch bildirish" so'zi protokolning barcha ishtirokchilari vositachining so'zlarini haqiqat deb qabul qilishini, uning hamma harakatlarini to'g'ri deb bilishligini, bundan tashqari vositachi protokoldagi o'zining qismini bajarishi "ishonchlilik"ni bildiradi. Vositachilar bir-biriga ishonchi bo'lmagan 2 tomonga protokolni bajarilishiga yordam beradilar.



6.1-rasm. Vositachi yordamidagi protokol

Arbitrli protokollar. Vositachini yollash katta mablag‘ talab etganligi uchun, vositachi ishtirok etgan protokollarni ancha patroq darajali ikkita qism protokolga ajratish mumkin. Birinchisi vositachisiz protokol hisoblanadi, bunda tomonlar protokolni bajarish niyatida bo‘lgan hollardagina ishlaydi. Ikkinchisi, faqat ayrim hollarda ijro etiladigan – qachon tomonlar orasida kelishmovchilik kelib chiqsa, vositachi yordamidagi protokollar hisoblanadi. Bu protokolda maxsus turdagi vositachi ishtirok etadi – bu arbitr (6.2-rasm).

Arbitr xuddi vositachi kabi qiziqmaydigan va protokolning ishonchli uchinchi tomoni hisoblanadi. Vositachidan farqli ravishda u har bir protokolning bajarilishida ishtirok etishi shart emas. Arbitr faqat protokolning to‘g‘ri bajarilganligini tekshirish uchun taklif qilinadi.



6.2-rasm. Arbitli protokol

O‘ziga yetarli protokollar - eng yaxshi protokol turi hisoblanadi (6.3-rasm). Tomonlar to‘g‘riligi protokollarning o‘zi bilan kafolatlanadi. Protokolning bajarilishi uchun vositachi kerak emas. Kelishmovchiliklarning mavjud emasligini protokol konstruksiyasining

o‘zi ta’minlaydi. Agar tomonlarning biri g‘irromlik qilishga harakat qilsa, boshqa tomon shu zahoti aldovni aniqlaydi va protokol bajarilishi to‘xtatiladi.

6.3-rasm. O‘ziga yetarli protokol

Kriptografik protokollar nazariyasi. Kriptografik protokol tushunchasi kriptografiyaning asosiy tushunchalaridan biri hisoblanadi va u maxfiylik, haqiqiylikni tekshirish, yaxlitlik va insonlar tomonidan qilinadigan buzg‘unchilik muammolarini hal etishda muhim ahamiyat kasb etadi. Kriptografik algoritmlar va usullarni aniq bir muammolarni yechishda qo‘llay olish uchun kriptografik protokollar haqida to‘liq ma’lumotga ega bo‘lish talab etiladi.

Kriptografik protokol kriptoalgoritmdan va shifrlash kalitlaridan foydalanishni belgilab beradigan qoidalar va proseduralar to‘plamidir. Tomonlar bir-biriga ishonib do‘st bo‘lishi mumkin yoki aksincha bir-biriga ishonmasligi, ya’ni buzg‘unchi bo‘lishi mumkin. Kriptografik protokol tarkibiga ma’lum bir kriptografik algoritm kiradi, ammo protokollar faqatgina maxfiylikni ta’minlash uchun mo‘ljallanmagan. Protokollarda kriptografiyani ishlatishdan maqsad firibgarlik va noqonuniy eshitishni aniqlash yoki unga yo‘l qo‘ymaslik.

Ba’zi protokollarda ishtirokchilardan biri ikkinchisini aldashi mumkin. Boshqa protokollarda esa buzg‘unchi protokolni buzishi yoki undagi maxfiy ma’lumotni bilib olishi mumkin.

Kriptografik protokolning har bir ishtirokchisi ma’lum algoritmlar ketma-ketligiga mos ravishda ish bajaradi. Har bir ishtirokchi tomonidan bajariladigan amal quyidagicha bo‘lishi mumkin:

– boshqa ishtirokchiga (yoki ishtirokchilar guruhiga) *xabarni yuborish;*

– boshqa ishtirokchidan *xabar qabul qilish;*

– *ichki amal,* ya’ni ishtirokchilar amalga oshiradigan ba’zi hisoblash ishlari.

Kriptografik protokol ishtirokchilari 3 sinfga bo‘linadi:

1. *Odatdagi (qonuniy) ishtirokchilar* (**A, B** va hokazo belgilar ko'rinishida ifodalanadi, indekslar bilan ham kelishi mumkin).

2. *Ishonchli vositachi* (**T** belgisi ko'rinishida ifodalanadi, indeks bilan ham kelishi mumkin).

3. Quyidagi ikki sinfga bo'linuvchi *buzg'unchilar:*

a) *Passiv buzg'unchilar* (**Y** belgisi ko'rinishida ifodalanadi, indeks bilan ham kelishi mumkin).

Passiv buzg'unchi boshqa ishtirokchilarga yuborgan xabarni ushlab olishi, o'g'irlashi va tahlil qilishi mumkin.

b) *Aktiv buzg'unchilar* (**M** belgisi ko'rinishida ifodalanadi, indeks bilan ham kelishi mumkin).

Aktiv buzg'unchi quyidagi amallarni bajarishi mumkin:

– boshqa ishtirokchilarga yuborilgan xabarni ushlab olishi va tahlil qilishi;

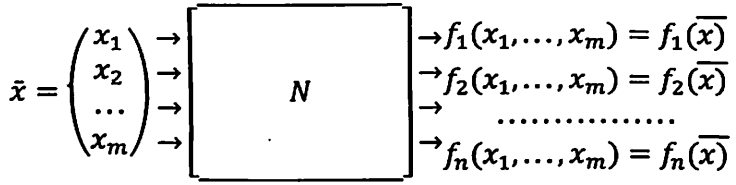
– yuborilgan xabarni o'zgartirishi yoki o'chirishi;

– yangi xabarni hosil qilib, boshqa ishtirokchilarga yuborishi;

– o'zini boshqa ishtirokchi qilib ko'rsatishi (bunday aktiv buzg'unchilarni *firibgar* deb nomlashadi).

Shunday qilib kriptografik protokol – bu shunday protokolki, unda kriptografik algoritmlar qo'llaniladi va u biror bir kriptografik masalani yechish uchun xizmat qiladi.

Nazariy kriptografiyada protokol m ta kirish va $n \le m$ ta chiqishga ega bo'lgan "qora quti" sifatida qaraladi (6.4-rasm):



6.4-rasm. Nazariy kriptografiyada protokol sxemasi

Kriptografik protokollarning berilgan talablarga ko'ra to'g'ri tuzilishi odatda ikki maqsadni ko'zlaydi: tashqaridagi buzg'unchidan himoya qilishni va o'zaro bir birini aldashdan himoya qilishni. Kriptografik protokollar – bu ishtirokchilar orasidagi shunday o'zaro bog'lanish protsedurasiki, uning natijasida qonuniy ishtirokchilar o'z maqsadlariga erishadilar, buzg'unchi esa maqsadiga yeta olmaydi.

Bitta protokol aynan bitta ishtirok etuvchi shaxslar tomonidan biror vaqt oralig'ida bir necha marta bajarilishi mumkin. Seans – bu

protokolning bir marta bajarilishi. Protokol raundi – bu bir martali ikki tomonlama xabar yuborish. Raund kontekstiga bog'liq holda ikki yoki undan ortiq xabarlarni jo'natishni o'z ichiga olishi mumkin. Ba'zan protokolning ichida siklik konstruksiyalar ham uchraydi: bunda bir martali siklning bajarilishi raund deb ataladi.

Kriptografik protokollarning tavsifi, odatda ishtirokchilarning hatti-harakati tavsifidan tashqari talab qilinayotgan algoritmlarning xarakteristikalarini, protokolning to'g'ri ishlashi uchun talab qilinadigan boshlang'ich shartlarni o'z ichiga oladi.

Kriptografik protokolning xossalari bir necha sinflarga bo'linadi. Quyidagi sinfdagi xossalar eng dolzarb hisoblanadi.

1. *Aniqlik*, ya'ni:

– kriptografik protokol ishtirokchilari tomonidan amalga oshiriladigan hisoblashlarning to'g'riligi;

– ishtirokchilar tomonidan hisoblangan natijalarning berilgan o'zaro nisbatga mos kelishi;

– va hokazo.

Ushbu xossasi asosiy hisoblanadi, chunki ularning buzilishi natijasida, hattoki kriptografik protokol qolgan hamma xossalarga ega bo'lsa ham, uni ishlatib bo'lmaydi.

2. *Xavfsizlik*. Ushbu xossa sinfi bir necha sinflarga bo'linadi. Ulardan eng dolzarblari quyidagilar:

– Yaxlitlik, ya'ni qonuniy ishtirokchilar almashinadigan xabarni buzg'unchi tomonidan o'zgartirish harakatlari KPni bajarish jarayonida aniqlanishidan iborat;

– Maxfiylik, ya'ni KP ishi jarayonida axborotning mualliflashtirilmagan tarzda chiqib ketishining oldi olinganligidan iborat: kriptografik protokol ishlab turgan ixtiyoriy paytda buzg'unchi shifrlangan xabarni tarkibi bilan tanishish imkoni bo'lmasligi kerak.

– Turg'unlik ma'lum xatti-harakatlardan ishtirokchining hatti-harakatlarini rad etishda va kriptografik protokol bajarilib turgan muhitda kutilmagan xatti-harakati holatida namoyon bo'ladi.

Shuningdek ushbu xossalar sinfiga kriptografik protokol ishlab turgan kompyuter tizimida nosozlikdan so'ng normal ishlashini tezda ta'minlash qobiliyati kiradi.

3. *Samaradorlik* - kriptografik protokol ishlashi jarayonida xotira va vaqt resurslaridan samarali foydalanish. Kriptografik protokol dagi amalga oshirilgan algoritmlarning optimalligi.

4. *Adaptasiya* – ichki strukturasini o'zgartirmasdan uni sozlagichi yordamida o'zgartirish yo'li bilan kriptografik protokol muhitining ozgina o'zgarishiga moslashuvchanligi.

5. *Hujjatlashtirilganlik* - uni ishlatish shartida muhim o'zgarish bo'lganda kriptografik protokolga tezda o'zgartirish kiritishga imkon beruvchi kriptografik protokol tavsifining tiniq va aniq hujjatlashtirilganligi (Masalan, juda ko'p mumkin bo'lgan kirish ma'lumotlarini kengaytirish yoki toraytirish holatida).

6. *Mobillilik va moslashuvchanlik,* ya'ni kriptografik protokolning turli konfiguratsiya va platformalarda yaxshi ishlash qobiliyati.

Xavfli ochiq kompyuter tarmoqlarida va taqsimlangan kompyuter tarmoqlarida o'zaro xavfsiz ma'lumot almashinuvini tashkillashtirish muhim vazifalardan biri bo'lib, uni hal qilish uchun kriptografik protokoldan foydalanish mumkin.

Kriptografik protokollar quyidagi asosiy vazifalarni bajaradi:

– ma'lumotlar manbasining autentifikatsiyasi;
– tomonlar autentifikatsiyasi;
– ma'lumotlar maxfiyligi;
– rad etishning mumkin bo'lmasligi;
– qabul qilganlikning isboti bilan rad etishning mumkin bo'lmasligi;
– manbaning isboti bilan rad etishning mumkin bo'lmasligi;
– ma'lumotlar yaxlitligi;
– qayta tiklashsiz ulanishning yaxlitligini ta'minlash;
– qayta tiklashli ulanishning yaxlitligini ta'minlash;
– foydalanishni chegaralash.

Kriptografik protokollarni bajaradigan asosiy vazifalariga qarab umumiy holda quyidagicha sinflash mumkin:

– shifrlash protokollari;
– ERI protokoli;
– Identifikatsiya /autentifikatsiya protokoli;
– kalitlarni autentifikatsiya qilib tarqatish protokoli.

Shifrlash protokollari. Bu sinfdagi protokol asosini shifrlash/shifrni ochishning simmetrik yoki assimmetrik algoritmi tashkil etadi. Shifrlash algoritmi jo'natuvchi xabarni yuborayotganda amalga oshiriladi, natijada xabar ochiq holatdan shifrlangan holatga almashtiriladi. Shifrni ochish algoritmi qabul qiluvchi xabarni

olayotganda amalga oshiriladi, natijada xabar shifrlangan holatdan ochiq holatga almashtiriladi. Shu tarzda maxfiylik xususiyati ta'minlanadi.

Odatda simmetrik shifrlash/shifrni ochish algoritmlarida uzatilayotgan xabarlarning yaxlitlik xossasini saqlash uchun, uzatishda va qabul qilishda shifrlash kaliti qo'llaniladigan imitohimoya qo'shimchalarini tekshirishni imitohimoya qo'shimchalarini hisoblovchi algoritmlar bilan birga qo'llaniladi. Asimmetrik shifrlash/shifrni ochish algoritmlarini qo'llaganda yaxlitlik xossasi alohida ERIni hisoblash orqali, uzatishda va qabul qilishdą qabul qilingan xabarni rad eta olmaslik va haqiqiylikni ta'minlovchi ERIni tekshirish yordamida amalga oshiriladi.

ERI protokoli. Bu sinfdagi protokol asosini yuborishda yuboruvchining yopiq kaliti yordamida ERIni hisoblash, qabul qilishda ochiq ma'lumotnomadan olinadigan va o'zgartirishdan himoyalangan yopiq kalitga mos ochiq kalit yordamida ERIni tekshirish algoritmlari tashkil etadi. Protokolni tekshirish natijasi ijobiy bo'lganda, qabul qilingan xabar, uning ERIsi va mos ochiq kalitlarni arxivlash amali bilan tugallanadi. Agar ERI rad qila olmaslik xususiyati uchun emas, balki faqat yaxlitlik va qabul qilingan xabarning haqiqiyligini ta'minlash uchun qo'llanilsa, arxivlash amali bajarilmasligi mumkin. Bu holda tekshiruvdan so'ng ERI o'sha zahotiyoq yoki kutish davri chegarasi tugashi bilan o'chirib tashlanadi.

Identifikatsiya/autentifikatsiya protokoli. Bu sinfdagi protokol asosini identifikatorga ega bo'lgan identifikatsiya qilinuvchi ob'yektning faqatgina qayd etilgan obyektga ma'lum bo'lgan maxfiy axborotni bilishligini tekshiradigan ba'zi algoritm tashkil etadi. Bunda tekshirish usuli bilvosita hisoblanadi, ya'ni bu maxfiy axborotni taqdim qilmasdan amalga oshiriladi.

Odatda har bir obyektning nomi (identifikatori) himoyalangan ma'lumotlar bazasiga yozilgan tizimdagi huquq va vositalar ro'yxati bilan bog'lanadi. Bu holatda identifikatsiya protokoli identifikatsiya qilingan obyekt buyurtirgan xizmatning vakolatli ekanligini tekshiradigan APgacha kengaytirilishi mumkin.

Agar identifikatsiya protokolida ERI ishlatilsa, u holda maxfiy axborot sifatida ERIning maxfiy kaliti ishlatiladi. ERIni tekshirish yopiq kalitni aniqlashga yo'l qo'ymaydigan, lekin bu yopiq kalitni ERI muallifiga ma'lum bo'lishiga ishonch hosil qiladigan ma'lumot bo'lgan unga mos ochiq kalit yordamida amalga oshiriladi.

Autentifikatsiya qilingan kalitlarni taqsimlash protokoli. Bu sinfdagi protokol ishtirokchilarni autentifikatsiya qilishni generatsiyalash va kanal bo'yicha kalitlarni taqsimlash protokoli bilan qo'shilib ketadi. Protokol ikki yoki uch ishtirokchilardan iborat: uchinchi ishtirokchi bo'lib, kalitlarni taqsimlash va generatsiyalash markazi xizmat qiladi (*s* server). Protokol 3 bosqichdan iborat: generatsiya, qayd etish (registratsiya) va kommunikatsiya. Generatsiya bosqichida *s* server tizimning parametrlari qiymatlarini, shuningdek o'zining ochiq va yopiq kalitini ham generatsiyalaydi. Qayd qilish bosqichida *s* server hujjatlar bo'yicha ishtirokchilarni (shaxsan o'zining kelishi yoki vakolatli shaxslar orqali) identifikatsiya qiladi. Buning uchun *s* server har bir obyekt uchun kalit va/yoki identifikatsiyalovchi axborotni generatsiya qiladi va kerakli tizim konstantalari va *s* serverining ochiq kalitidan (zaruriy holatda) iborat bo'lgan xavfsizlik ma'lumotini shakllantiradi. Kommunikatsiya bosqichida umumiy seans kalitini shakllantirish bilan yakunlanadigan o'zining autentifikatsiya qilingan kalitlar almashinuvi protokolini amalga oshiradi.

Kriptografik dasturiy vositalar. Axborot xavfsizligini ta'minlash uchun uni kriptografik almashtirishni amalga oshiruvchi apparat, dasturiy yoki apparat-dasturiy vosita *axborotni kriptografik muhofaza qilish vositasi* deyiladi.

Dasturiy ta'minot majmuasiga kiruvchi va axborotni muhofaza qilish uchun mo'ljallangan maxsus dastur *axborotni muhofaza qilishning dasturiy vositasi* deb ataladi.

Kriptografik dasturiy vositalarda kriptografik algoritmlar yuqori yoki quyi darajadagi dasturlash tillarida amalga oshiriladi. Dasturiy vositalardagi amallar odatda kompyuter xotirasida bajariladi. Dasturiy vositani kriptobardoshliligi kriptoalgoritmni qanchalik aniqlik bilan amalga oshirilganiga bog'liq. Kriptografik dasturiy vositalarga apparat vositalar kabi keng qamrovli shartlar qo'yilmasada, quyidagi muhim o'ziga xos xususiyatlarga ega bo'lishi shart:

– vazifalarni qo'shimcha nazorat qilish imkoniyati mavjudligi, chunki ko'p hollarda dasturiy vositalar apparat vositalarga qaraganda ancha sust ishlashi kuzatiladi;

– yopiq matnlarda xatolarni nazorat qilish imkoniyatii mavjudligi;

– kalitlarni ishonchli saqlanilishini ta'minlash imkoniyati;

– mavjud dasturiy vositani o'zgartirish imkoniyati va qo'shimchalar qo'shish imkoniyati;

Kriptografik dasturiy vositalar quyidagi vazifalarni bajaradi:

– foydalanuvchilarni identifikatsiya/autentifikatsiyadan o'tkazish;

– operatsion tizim va dasturiy vositalarni kriptografik himoyasini ta'minlash;

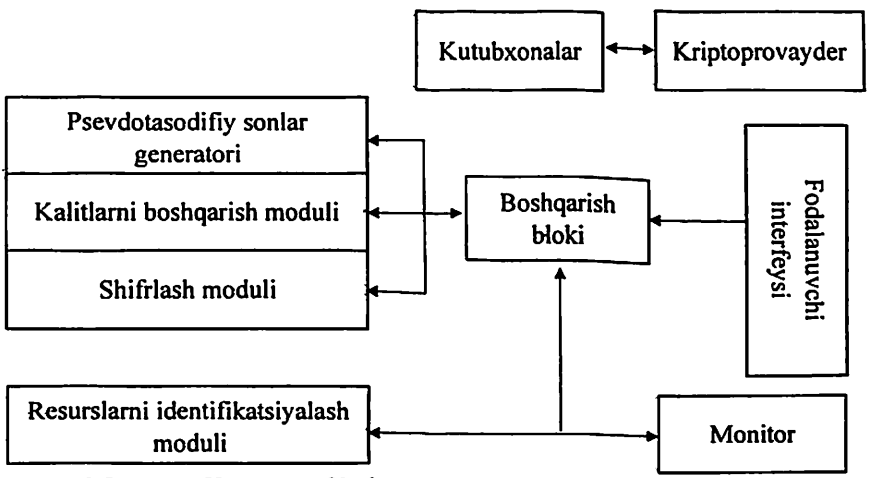
– psevdotasodifiy ketma-ketliklarni hosil qilish;

– ma'lumotlarni shifrlash;

– kalitlarni tashkil etish, tekshirish, elektron raqamli imzo va dasturiy kodlarni ko'chirishdan himoyalash uchun;

– kalit uzatilishida xavfsizlikni ta'minlashda.

Kriptografik dasturiy vositalarning tuzilishi 6.5-rasmda keltirilgan.



6.5-rasm. Kriptografik dasturiy vositalarning umumiy sxemasi

Kriptografik dasturiy vositalarning umumiy sxemasidagi qismlarning vaziflari.

Boshqarish bloki dasturiy vositaning alohida qismlarini birlashtiradi, tashqaridan kiruvchi buyruqlarni ichki modul bilan bog'laydi.

Kalitlarni boshqarish moduli kalit ma'lumotlarni hosil qilishda, foydalanuvchini identifikatsiya/autentifikatsiyadan o'tkazishda foydalaniladi.

Psevdotasodifiy ketma-ketlik generatori tasodifiy bo'lgan bitlar ketma-ketligini hosil qilishda foydalaniladi.

Kriptografik dasturiy modul kutubxonalari amaliy vazifalarni hal etadi va dasturiy vositani sozlashda foydalaniladi.

Foydalanuvchi interfeysi foydalanuvchiga dasturiy muhitdan foydalanishga qulaylik tug'diradi va ichki modulga ma'lumot kritishda va natijani foydalanuvchiga ko'rsatish uchun foydalaniladi.

Shunday qilib, dasturiy kriptografik himoya vositalari quyidagi o'ziga xos xususiyatlarga ega:

– ushbu dasturiy kriptografik himoya vositalari boshqa qurilmalarda saqlangan bo'lishi mumkin;

– blokli shifrlash algoritmlarida blok o'lchami fayl segmenti o'lchamini oshirishi mumkin, natijada esa fayl o'lchami ortishi mumkin;

– dasturiy kriptografik himoya vositalarining shifrlash tezligi apparat vositalar tezligiga qaraganda past bo'lishi mumkin, chunki barcha hisoblashlar markaziy prosessorda amalga oshiriladi.

6.2-jadvalda dasturiy kriptografik himoya vositalariga misollar keltirilgan.

6.2-jadval

Dasturiy kriptografik himoya vositalariga misollar

Guruhi	Misollar
Diskdagi ma'lumotlarni shifrlash tizimlari	Operatsion tizimning dasturiy vositalari, PGP, Secret Disk
Tarmoqda ma'lumotlarni shifrlash tizimlari	ZASTAVA kompleksi (VPN + dasturiy kriptografik vosita)
Elektron hujjatlarni haqiqiyligini aniqlash tizimlari	PGP
Kalitlarni boshqarish tizimlari	ZASTAVA server sertifikatlari

Kriptografik dasturiy vositalar himoyaning to'liqligiga kafolat bermasada, iqtisodiy tomondan foydali bo'lib, ixtiyoriy maxfiylik talab etilgan tizimlarda qo'llash imkonini beradi.

Axborotlarni himoyalashning kriptografik apparat-dasturiy vositasi apparat va dastur majmuasidan iborat bo'lib, 6.6-rasmda uning umumiy sxemasi keltirilgan. U quyidagi modullardan tashkil topgan:

– shifrlash bloki (asimmetrik shifrlash tizimlari dasturiy modullar, simmetrik shifrlashla apparat modullar uchun), dasturiy, apparat ko'rinishida yoki ularning kombinatsiyasi asosida amalga oshiriladi;

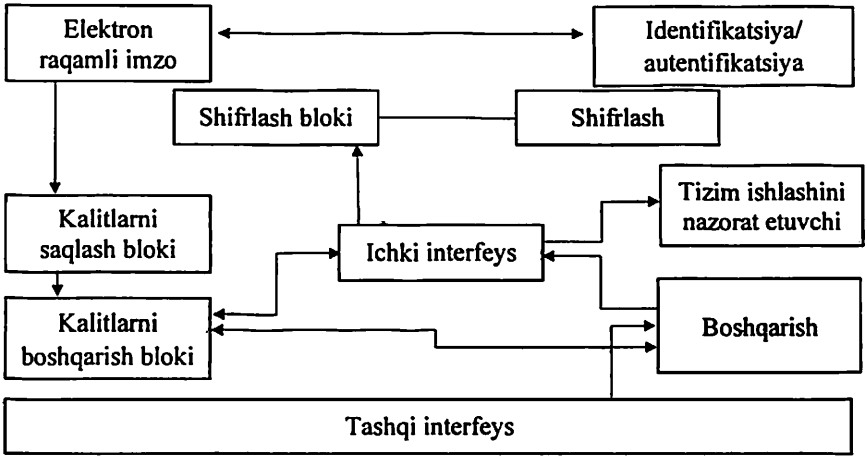
– elektron raqamli imzo bloki;

– kalitlarni boshqarish bloki;

– identifikatsiya/autentifikatsiya moduli;

– tashqi interfeysni boshqarish moduli;

– tizim ishlashini nazorat qiluvchi modul.



6.6-rasm. Kriptografik apparat-dasturiy himoya vositasining umumiy sxemasi

Apparat-dasturiy kriptografik vositalarni qurishda namunaviy tayanch sxema mavjud emas, chunki ushbu tizimni qurishda va samaradorligini oshirishda doim yangi usullar qidiriladi va tizim sxemasi o'zgarib turadi. Ushbu kriptografik himoya vositalari xavfsizlik siyosati va himoyalanadigan tizimga qo'yilgan talablardan kelib chiqib tanlanadi.

6.3-jadvalda kriptografik apparat-dasturiy vositalariga namunalari keltirilgan.

6.3-jadval

Kriptografik apparat-dasturiy vositalarga misollar

Guruhi	Misollar
Diskdagi ma'lumotlarni shifrlash tizimlari	Crypton Soft, GRYaDA
Tarmoqda ma'lumotlarni shifrlash tizimlari	Crypton ArcMail (KRIPTON platasida)
Elektron hujjatlarni haqiqiyligini aniqlash tizimlari	Crypton Sign, Crypton ArcMail (KRIPTON platasida)
Kalitlarni boshqarish tizimlari	Crypton Tools(KRIPTON platasida)

Quyida ayrim kriptografik apparat-dasturiy himoya vositalari keltirilgan:

ANKAD (KRIPTON). 20 yildan beri axborot xavfsizligi sohasida ishlab keladigan mashhur tashkilotlardan biridir. U keng ko'lamdagi xavfsizlik vositalarini (axborotning kriptografik himoya vositalarini, elektron raqamli imzo qurilmalarini, ruxsatsiz foydalanishni oldini olish uchun mo'ljallangan vositalarni, kompyuter resurslariga ruxsatni cheklash va h.k.) ishlab chiqaradi.

ANKAD firmasining himoya vositalari orqali quyidagi turdagi axborotlarni himoyalash mumkin:

– davlat sirlarini himoyalashda;

– shaxsiy ma'lumotlarni himoyalashda;

– konfidensial ma'lumotlarni himoyalashda;

– tijoratga oid ma'lumotlarni himoyalashda.

RUTOKEN. RUTOKEN – autentifikatsiyalash va ma'lumotlarni himoyalash tizimi bo'lib, rossiyada ishlab chiqilgan yoki xalqaro standartlarini qo'llaydi. U USB zanjir ko'rinishida bo'lib, kompyuterning USB portiga ulunadi. Hozirda RUTOKENning 32Kbayt va undan yuqori xotirali turlari qo'llanilmoqda.

RUTOKEN quyidagi vazifalarni bajaradi:

Autentifikatsiya:

– ma'lumotlar bazasi, WEB-serverlarda, VPN-tarmoqlarda parol orqali bo'ladigan autentifikatsiyani apparat-dasturiy autentifikatsiyaga almashtirish;

– pochta serverlari, ma'lumotlar bazasi serveri, Web-serverlar, fayl serverlar bilan bo'ladigan to'g'ridan-to'g'ri aloqani himoyalash.

Ma'lumotlarni himoyalash:

– ma'lumotlarni GOST 28147-89 standarti orqali shifrlash;

– elektron pochtani shifrlash, elektron raqamli imzo orqali himoyalash;

– kompyuterga bo'ladigan ruxsatlarni boshqarish.

Korporativ foydalanishda:

– amaliy dasturlar orqali elektron savdo-sotiq tizimida xizmat ma'lumotlarini, shaxsiy ma'lumotlarni, parollarni, raqamli sertifikatlarni, shifrlash parollarini saqlashda;

– RUTOKEN korparativ tizimlarda har xil turdagi axborotlarga bo'ladigan ruxsatlarni beruvchi yagona identifikator sifatida qo'llash.

KriptoPRO – kriptografik himoya vositalarini ishlab chiqaruvchi tashkiloti bo'lib, 2000 yilda tashkil topgan. Ushbu tashkilot kriptografik himoya vositalari, asosan ERI vositalarini ishlab chiqarib, jahon bozorida

KriptoPRO nomi ostida o'z mahsulotlari bilan mashhur. Ushbu tashkilot kriptografik himoya vositalari asosida asosan Rossiyada ishlab chiqarilgan standartlar va jahonda tan olingan standartlar yotadi.

KriptoPRO HSM kriptografik apparat-dasturiy vositasi quyidagi vazifalarni bajaradi:

– ERI tashkil etish va tekshirish;

– xesh qiymatni hisoblash;

– ma'lumotlar blokini shifrlash va rasshifrovkalash;

– kalitlarni hosil qilish va ularni saqlash;

– kriptografik xizmatlar uchun foydalanuvchilarni boshqarish;

Kriptoprosesor "GRYaDA-41". Ushbu kriptografik apparat-dasturiy himoya vositasi Ukraina davlat xavfsizlik xizmati tomonidan davlat organlari va tijorat tashkilotlarida xavfsizlikni ta'minlash maqsadida foydalaniladi. Ushbu vosita axborot xavfsizligini ta'minlashda kriptografik tizimlar, kalitlarni generatsiya qilish algoritmlari, shifrlash, xesh-funksiyani hisoblash, ERI shakllantirish va tekshirish hamda kriptografik protokollarni shakllantirish kabi tizimlardan foydalanilgan.

Ushbu himoya vositasi quyidagi imkoniyatlarni taqdim etadi:

– GOST 28147-89, FIPS 197 algoritmlari bilan shifrlash;

– DSTU 4145-2002, ISO/IEC 15946-2, GOST 34.310-95 algoritmlari orqali ERI shakllantirish va tekshirish;

– GOST 34.311-95 (SHA-1, SHA-2) bo'yicha xesh-funksiyani hisoblash;

– Diffi-Xelman (X9.42 i X9.63) protokoli asosida kalitlarni taqsimlash algoritmi;

– GOST 34.310-95, DSTU 4145-2002 ERI standarti va Diffi-Xelman ISO/IEC 15946-3 protokoli uchun ochiq va yopiq kalitlarni hosil qilish;

– GOST 28147-89 uchun seans kalitini, GOST 34.310-95 va DSTU 4145-2002 uchun psevdotasodifiy ketma-ketlikni hosil qilish;

– ma'lumotlarni himoyalangan shaklda tashqi xotira qurilmalarida saqlash;

– dasturiy ta'minotlarni to'liqligini va ishlash rejimini to'g'riligini ta'minlash.

E-XAT. O'zbekiston Respublikasida davlat tashkilotlari o'rtasida elektron hujjat almashish tizimi bo'lib, Unicon.uz korxonasi tomonidan ishlab chiqilgan. E-XAT himoyalangan elektron xat almashish tizimining asosiy vazifasi elektron xatlarning butunligini, maxfiyligini va

ishonchliligini, umuman aytganda foydalanuvchilar o'rtasidagi elektron xat hamda ovoz ma'lumotlarini uzatishdagi axborot himoyasini ta'minlab berish maqsadida ishlab chiqilgan.

E-XAT tizimida axborotni kriptografik himoya qilishning barcha usullaridan, ya'ni axborotni shifrlash/rasshifrovklash, elektron raqamli imzo qo'yish va uni tekshirish, maxfiy kalitlarni almashish kabilarda quyidagi algoritmlardan foydalanilgan:

– Elektron raqamli imzoda - O'zDST 1092:2009 «Axborot texnologiyasi. Axborotni kriptografik muhofazasi. Elektron raqamli imzoni shakllantirish va tekshirish jarayonlari» milliy standarti.

– Shifrlashda - O'zDST 1105:2009 «Axborot texnologiyasi. Axborotni kriptografik muhofazasi. Ma'lumotlarni shifrlash algoritmi» milliy standartlari asosida ishlab chiqilgan.

E-XAT uchta dasturiy ta'minot asosida ishlaydi:

– E-XAT serveri – foydalanuvchilarning xatlarini qabul qilish, saqlash va jo'natish;

– elektron raqamli imzo kalitlarini ro'yxatga olish markazi;

– E-XAT tizimining foydalanuvchi uchun dasturi.

E-KALIT katta bo'lmagan tashqi ko'rinishga ega USB-brelok bo'lib, foydalanuvchining shaxsiy kriptografik parametrlarini muhofazalangan ishonchli muhitda saqlanishini ta'minlaydi.

E-KALIT quyidagi imkoniyatlarni beradi:

– elektron raqamli imzoning shaxsiy parametrlari, ERI yopiq kalitlari, xeshlash kalitlari, shifrlash kalitlari, shuningdek ochiq parametrlarni (masalan, ochiq kalitlar sertifikati);

– identifikatsion ma'lumotlar (login va parol)ni bilish asosida qurilma xotirasi tarkibidan foydalanish uchun foydalanuvchini xavfsiz avtorizatsiya qilish;

– berilgan bir martalik parollarni tanlashga urinishda qurilma xotirasidan foydalana olishni blokirovka qilish;

– shaxsiy kompyuter tomonidan so'rov berilganida elektron raqamli imzo ochiq kalitining sertifikatini berish;

– foydalanuvchining shaxsiy kompyuterdagi kriptografik kalitlari va sertifikatlarini yuklash (masalan, ERI kalitlarini ro'yxatga olish markazining dasturidan);

– tasodifiy sonni xeshlash asosida foydalanuvchining identifikatsion ma'lumotlarini qurilmaga xavfsiz uzatish.

Qurilma va shaxsiy kompyuter o'rtasida axborot bilan almashuv maxsus kriptografik protokol bo'yicha amalga oshiriladi, bu USB shinasi ushlab olingan holda foydalanuvchining kriptografik kalitlari va identifikatsion ma'lumotlaridan ruxsatsiz foydalana olish imkoniyatini istisno etadi. Qurilma bilan komplektda Windows XP operatsion tizimi uchun maxsus drayver yetkazib beriladi.

S-FILES tizimi shaxsiy kompyuter yoki tashqi diskdagi papkalarga va fayllarga ruxsatsiz kirishdan muhofaza qilish, yaxlitlik va himoya qilish uchun mo'ljallangan. Fayl xavfsizligi kriptografik ma'lumotlarni shifrlash orqali ta'minlanadi. Ma'lumotlarning yaxlitligi foydalanuvchining elektron raqamli imzosi va ma'lumotlarni uzatish vositalaridan foydalangan holda ta'minlanadi.

6.2. Sodda autentifikatsiyalash protokollari

Alisa va Bob tarmoq orqali bog'langanda faraz qilaylik Alisa Bobga haqiqatan o'zi ekanligini isbotlashi kerak bo'lsin. Bu o'rinda Alisa va Bobni inson yoki mashina bo'lishini esdan chiqarmaslik zarur. Aniqki, tarmoq senariysi bo'lganda Alisa va Bobni o'zgarmas, mashina ekanligi ehtimoli yuqori.

Aksariyat hollarda Alisani Bobga haqiqiyligini isbotlashining o'zi etarli. Ammo ba'zida har ikkala tomon bir biriga o'zlarini haqiqiyligini isbotlashi talab etiladi. Bunda odatda Alisa Bobga o'zini haqiqiyligini tasdiqlashda va Bob Alisaga haqiqiyligini tasdiqlashda ham yagona protokoldan foydalaniladi. Ushbu bobda barcha xavfsizlik protokollari ham har doim xavfsiz emasligini misollar orqali ko'rib o'tiladi.

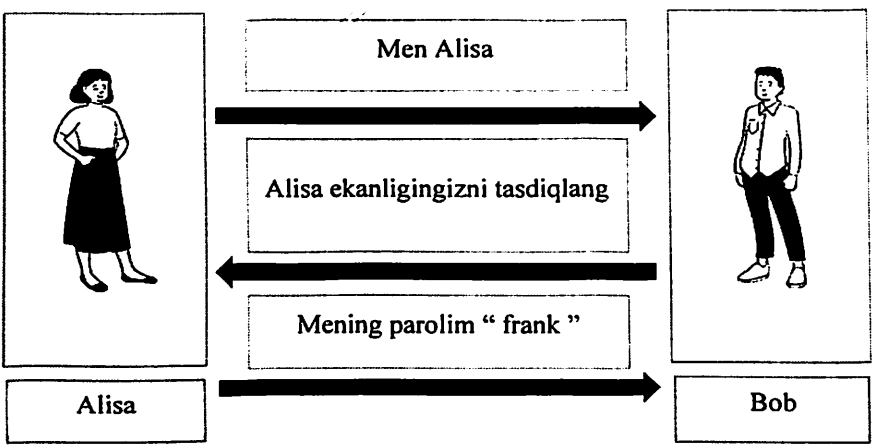
Autentifikatsiyadan tashqari ***sessiya kaliti*** ham ko'p holda talab etiladi. Sessiya kaliti simmetrik kalit bo'lib, autentifikatsiyani ta'minlagan holda joriy sessiyada uzatiladigan axborot maxfiyligi yoki butunligin ta'minlashda xizmat kilishi mumkin. Dastlab, faqat autentifikatsiyani amalga oshiruvchi protokollar bilan tanishib chiqiladi.

Xususiy hollarda, xavfsizlik protokollarida boshqa talablar ham bo'lishi mumkin. Masalan, protokolda ***ochiq kalitli tizimlardan, simmetrik tizimlardan yoki xesh –funksiyalardan foydalanish*** so'ralishi mumkin. Bundan tashqari, anonimlikni ta'minlovchi, haqiqatan rad etishni ta'minlovchi protokol talab etilishi mumkin.

Quyida dastlab yolg'iz kompyuter tizimida autentifikatsiyalashni ta'minlash bilan bog'liq muammolar bilan tanishib chiqiladi. Bu o'rinda ushbu protokollar o'zida ***xeshlash yoki "salting"*** kabi texnologiyalarini qamrab oladi. Biroq, tarmoq orqali autentifikatsiyalashni amalga

oshirganda jiddiy muammolar vujudga kelishi mumkin. Tarmoq orqali autentifikatsiyalash amalga oshirilganda buzg'unchi uchun imkoniyatlar ortadi. Tarmoq bo'ylab autentifikatsiya xabarlari uzatilganda ***buzg'unchi tomonidan uni qayta takrorlanishi, qo'shilishi, o'chirib tashlash yoki xabarni o'zgartirish*** holatlari bo'lishi mumkin.

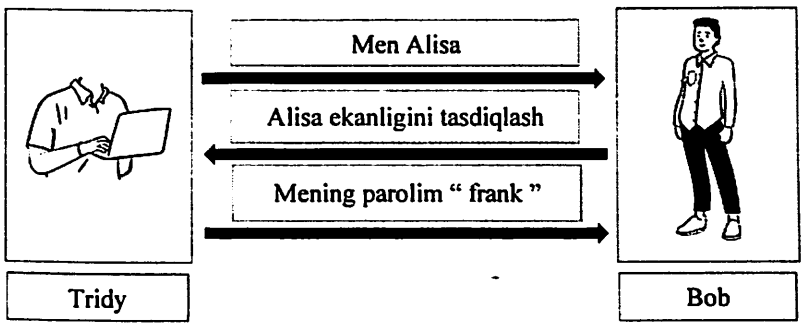
Birinchi ko'rinishdagi tarmoq orqali sodda autentifikatsiyalash imkonini beruvchi protokol 6.7-rasmda keltirilgan. Ushbu protokol uchta xabar uzatilishidan iborat bo'lib, dastlab Alisa Bob bilan aloqani o'rnatadi va unga o'z identifikatorini yuboradi. Shundan so'ng, Bob undan haqiqiyligini ta'minlashni talab etadi va Alisa unga o'z paroli bilan javob beradi. Parolga asosan Bob Alisani autentifikatsiyadan o'tkazadi.



6.7-rasm. Sodda autentifikatsiya protokoli

Ushbu protokol ko'rinishidan sodda ko'rinsada, unda jiddiy kamchilik mavjud. Agar Buzg'unchi, Tridi, tarmoqni kuzatish imkoniga ega bo'lsa, ushbu ma'lumotlardan qayta foydalanishi mumkin. Bunda Tridi ma'lumotlardan keyinchalik foydalanishi mumkin bo'ladi (6.8-rasm). Ushbu ***takrorlash hujumi*** jiddiy muammo olib keladi.

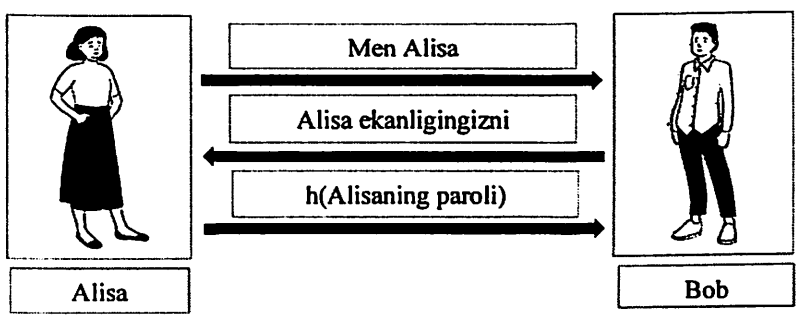
6.7-rasmda keltirilgan protokol bilan bog'liq bo'lgan muammolardan yana biri bu ***parolning ochiq yuborilishidir***. Agar Tridi tomonidan Alisani parolini kuzatish imkoni bo'lsa, u holda Tridi uning parolini bilishi mumkin. Ushbu muammo takrorlash hujumiga qaraganda ham jiddiy muammo bo'lib, Alisa ushbu paroldan ***boshqa qaydlar uchun ham foydalangan taqdirda***, yanada jiddiy muammo kelib chiqadi. Bundan tashqari, yana bir muammo bu ***autentifikatsiyalash uchun Bobni ham Alisaga tegishli parolni bilishi*** talab etilishidir.



6.8-rasm. Takrorlash hujumi

Bundan tashqari ushbu protokol ***samarasiz*** ham hisoblanadi. Ya'ni, barcha ma'lumotlarni yagona xabar orqali yuborish mumkin. Shundan qilib, ushbu protokol har tomonlama zaiflikga ega. Va nihoyat, 6.7 – rasmda keltirilgan protokol ***ikki tomonlama autentifikatsiyani*** ta'minlamaydi.

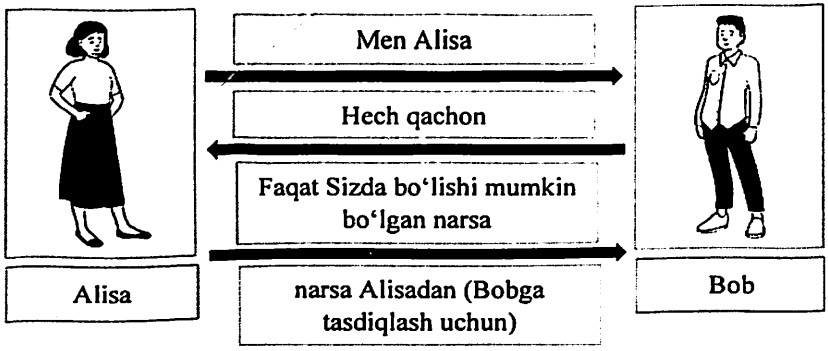
Keyingi ko'rinishdagi protokol 6.9-rasmda keltirilgan bo'lib, u yuqorida keltirilgan protokoldagi ***muammolarni bartaraf etgan***. Ushbu yangi protokolda, passiv kuzutuvchi Tridi Alisaga tegishli parolni bila olmaydi va Bob ham ushbu parolni bilishi talab etilmaydi. Bob Alisaga tegishli bo'lgan parolning xeshini bilishning o'zi yetarli.



6.9-rasm. Xesh asosida sodda autentifikatsiyalash protokoli

6.8-rasmda keltirilgan protokolda jiddiy muammo bu – ***takrorlash hujumining mavjudligidir***. Ya'ni, Tridi barcha yozishmalarni qayd etadi va ma'lum vaqtdan so'ng uni takrorlaydi. Bu holda Tridi Alisa sifatida autentifikatsiyadan o'tadi.

Alisani autentifikatsiyalash uchun Bob ***savol-javob*** mexanizmidan foydalanishga majbur. Ya'ni, Bob Alisaga savolni yuboradi va Alisadan keladigan javob asosida uni tekshiradi. Bu holda takrorlash hujumidan himoyalash uchun, Bob ***"bir martali sonlar (number used once, nonce)"dan*** foydalanishi shart. Ya'ni, Bob har safar unikal savolni yuboradi va unga mos javob hosil qilinadi. Bob qabul qilinayotgan javobni oldin yuborilmaganini aniqlash orqali takrorlash hujumi oldi olinadi yoki boshqa so'z bilan aytganda ***nonce*** javobni takrorlanmaslikni oldini oladi. Ushbu imkoniyatni taqdim etuvchi protokol 6.10-rasmda aks ettirilgan.

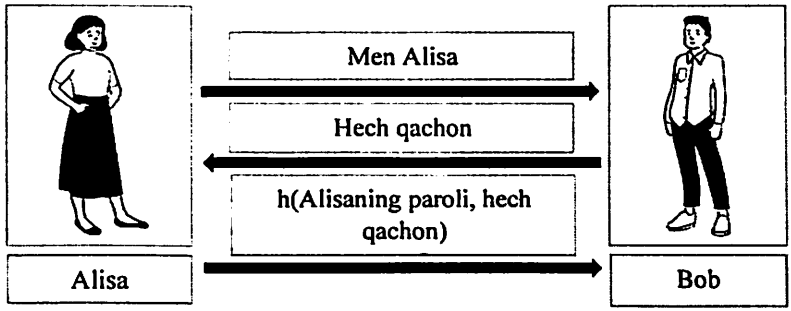


6.10-rasm. Umumiy autentifikatsiya

Dastlab Alisaning paroliga asoslangan holda autentifikatsiyalash protokoli taqdim etiladi. Bunda faraz qilaylik parolni Alisa biladi va Bob ham tekshirish uchun uni bilish imkoniga ega.

Takrorlash hujumiga bardoshli bo'lgan dastlabki protokol 6.11 – rasmda keltirilgan. Ushbu protokolda, *nonce* Bob tomonidan Alisaga yuboriladi. Alisa o'zining paroli va *nonce* ni xeshlash orqali javobni amalga oshiradi. Bu holda *nonce* xabar yangiligini va takrorlash hujumidan himoyalashni ta'minlaydi.

6.11-rasmda keltirilgan protokoldagi yagona muammo bu Bobni Alisaga tegishli parolni bilishi talab etiladi. Bundan tashqari, Alisa va Bob odatda inson ko'rinishda bo'lishdan ko'proq mashina bo'lishi mumkin va bu holda paroldan foydalanish mantiqsizdir. Bundan tashqari inson parolni esda saqlab yurishi uchun uni odatda murakkab tarzda tanlamaydi. Shuning uchun, Alisa va Bobni mashina bo'lishi ehtimolini hisobga olib parolni o'rniga kalitlardan foydalanish mumkin bo'ladi.

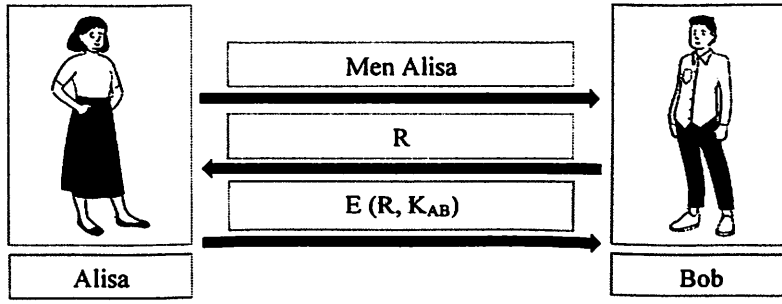


6.11-rasm. Savol-javob

Simmetrik kalitlar yordamida autentifikatsiya. Simmetrik kalitlarga asoslangan autentifikatsiyalashga o'tishdan oldin ma'lum belgilanishlar keltirib o'tiladi. Agar *ochiq matn R* bo'lsa va *kalit K* bo'lsa, u holda *shifrmatn S=E(P,K)* ga teng bo'ladi va ochiq matn *P=D(C,K)* ga teng bo'ladi. Bundan tashqari, ko'rib o'tilgan protokollarni tahlil qilganda unda foydalanilgan kriptografik algoritmlarni xavfsiz deb faraz qilinsin.

Faraz qilinsin, Alisa va Bob umumiy simmetrik kalit K_{AB} ga ega. Simmetrik kriptografiya bo'lgani sababli, kalitni boshqa tomonlar bilmaydi. Alisa o'zini Bobga autentifikatsiyadan o'tkazishda ushbu kalitni bilishidan foydalanadi. Bundan tashqari protokol takrorlash hujumidan himoyalashi shart.

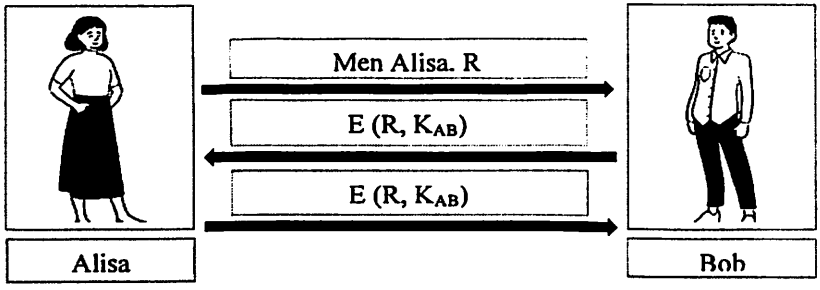
Simmetrik kalitga asoslangan autentifikatsiyalash protokolning birinchi ko'rinishi 6.12-rasmda keltirilgan. Ushbu protokol yuqorida keltirilgan parolga asoslangan savol-javob protokoligi analog bo'lib, farqli ravishda *nonce* va *parolni* xeshlash o'rniga, *tasodifiy qiymat R* ni simmetrik kalit K_{AB} bilan shifrlaydi.



6.12-rasm. Simmetrik kalit asosida autentifikatsiya protokoli

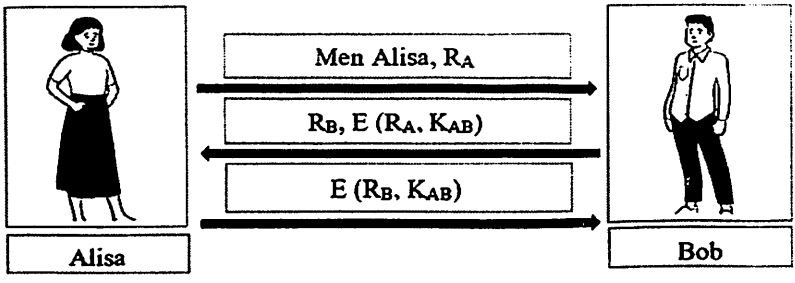
6.12-rasmda keltirilgan protokolda, Alisa R qiymatni kalit K_{AB} bilan shifrlay olishi sababli (Tridi esa shifrlay olmaydi), Bob uni autentifikatsiya qiladi. Buning uchun Bob to'g'ri shifrlanganini bilishining o'zi yetarli. Ushbu protokol *tasodifiy qiymat* R dan foydalanilgani bois takrorlash hujumidan himoyalaydi. Biroq ushbu protokol ikki tomonlama autentifikatsiyalashni amalga oshirmaydi. Shuning uchun keyingi topshiriq sifatida ikki tomonlama autentifikatsiyalash vazifasi olinadi.

Ikki tomonlama autentifikatsiyalash imkoniyatini beruvchi protokolning dastlabki ko'rinishi 6.13 – rasmda aks ettirilgan. Bu protokol samarali va simmetrik kalitdan foydalangan bo'lsada, unda ham zaiflik mavjud. Uchinchi xabar ikkinchi xabar bilan bir xil bo'lib, u yuboruvchi haqida xech narsani isbotlay olmaydi, ya'ni, yuboruvchi Alisami yoki Tridimi?



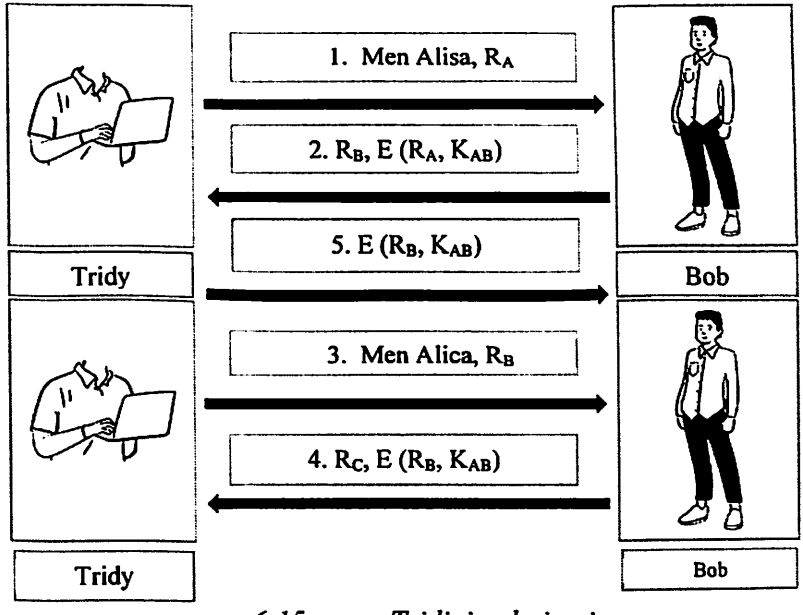
6.13-rasm. Ikki tomonlama autentifikatsiyami

Ikki tomonlama autentifikatsiyalashning xavfsiz usuli bu 6.12-rasmda keltirilgan protokol bo'lib, faqat jarayonni ikki marta takrorlash talab etiladi, ya'ni, bir marta Alisani autentifikatsiyalash uchun keyingi marta Bobni autentifikatsiyalash uchun. Ushbu protokolning umumiy ko'rinishi 6.14-rasmda aks ettirilgan. Bunda bir nechta xabarlarni birlashtirish orqali samaradorlik oshirilgan.



6.14-rasm. Xavfsiz ikki tomonlama autentifikatsiya

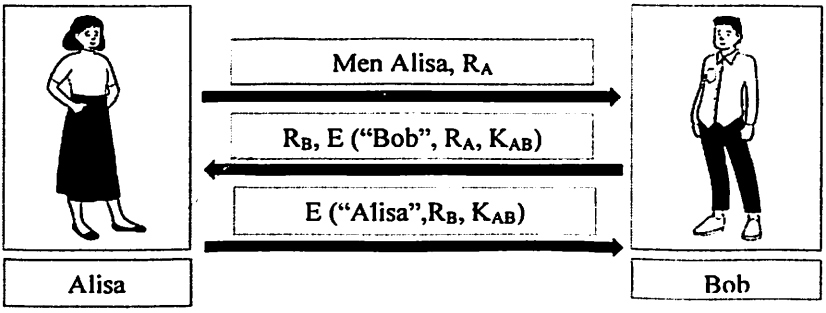
Ushbu protokol ko'rinishidan hayratlanarli bo'lsada, MiG-in-the-middle hujumiga o'xshash hujumga bardoshsizdir. Ushbu hujum 6.15-rasmda aks ettirilgan. Bunda Tridi Bob bilan aloqani Alisa nomidan o'rnatadi va R_A ni Bobga yuboradi. Protokolga asosan Bob uni shifrlaydi va uni R_B ga qo'shib, Tridiga yuboradi. Bu holda Tridi kalitni bilmasligi sababli, uni shifrlay olmaydi. Biroq Tridi malakali bo'lganligi sababli, Bob bilan yangi aloqani o'rnatadi va unga yana Alisa ekanligini aytadi. Shuning bilan birga R_B ni o'zini tasodifiy qiymati sifatida Bobga yuboradi. Protokolga asosan Bob $E(R_B,K_{AB})$ ni shifrlaydi va Tridiga yuboradi. Tridi esa ushbu ma'lumotdan birinchi bog'lanishni tugallash uchun foydlanadi. Tridi ikkinchi ulanishdan chiqib ketadi va birinchi ulanish asosida Alisa sifatida autentifikatsiyadan o'tadi.



6.15-rasm. Tridining hujumi

Umumiy holda xulosa shundan iboratki, bir tomonlama autentifikatsiyalashda foydalanilgan protokol ikki tomonlama autentifikatsiyalash uchun o'rinli emas.

6.16-rasm va 6.17-rasmlarda keltirilgan xavfsiz bo'lmagan ikki tomonlama autentifikatsiyalash protokolini kichik o'zgarishga uchragan ko'rinishi keltirilgan. Bunga asosan, foydalanuvchining identifikatori *nonce*ga qo'shilib, shifrlanadi. Ushbu kichik o'zgarish 6.15-rasmda keltirilgan tahdidga bardoshli bo'lishni ta'minlaydi.



6.16-rasm. Bardoshli ikki tomonlama autentifikatsiyalash protokoli

Yuqorida keltirilgan protokollardan shunday xulosa chiqadiki, protokolni ikki tomonda ham bir xil narsani bajarishi yaxshi g'oya emas.

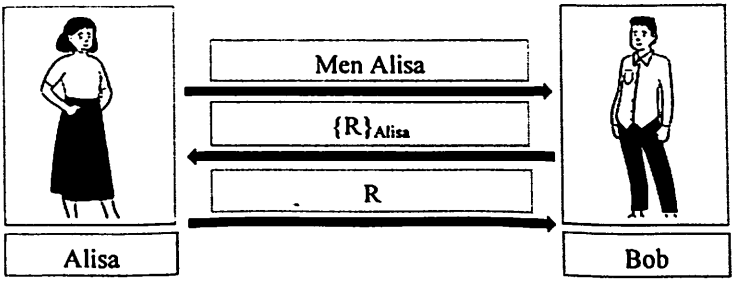
Ochiq kalitdan foydalangan holda autentifikatsiya. Bundan oldingi bo'limda simmetrik kalitga asoslangan xavfsiz ikki tomonlama autentifikatsiyalash protokoli ko'rib o'tgan edik. Ushbu bo'limda bu vazifani ochiq kalitni kriptografik tizimlar yordamida amalga oshirish masalasi bilan tanishib o'tiladi. Bundan oldin quyidagi belgilanishlar olinadi. Alisaga tegishli bo'lgan ochiq kalit bilan ma'lumot M ni shifrlash $C=\{M\}_{Alisa}$ kabi belgilansa, shunga asosan ochiq matnni $M=[C]_{Alisa}$ kabi belgilanadi. Imzolashda maxfiy kalitdan foydalaniladi va shifrlash/rasshifrovkalash jarayonlari imzolash/imzoni tekshirish jarayonlari teskari bo'lgani uchun

$$[\{M\}_{Alisa}]_{Alisa} = M \text{ va } \{[M]_{Alisa}\}_{Alisa} = M.$$

Ochiq kalitli kriptografik tizimlarda ochiq kalit bilan ixtiyoriy kishi ixtiyoriy amalni bajarishi mumkin va bunda maxfiy kalitdan faqat Alisa foydalanishi mumkin bo'ladi.

Ochiq kalitli kriptografiyaga asoslangan autentifikatsiyalash protokolining birinchi ko'rinishi 6.17-rasmda aks ettirilgan. Ushbu protokol Alisa maxfiy kalit bilan shifrmatnni rasshifrovkalay olgani va R ni uchinchi xabarda yuborgani uchun Bobga Alisani autentifikatsiyalash imkonini beradi. Bunda R tasodifiy qiymat Bob tomonidan generatsiya qilingani bois, takrorlash hujumida himoyalangan. Shuning uchun, Tridi

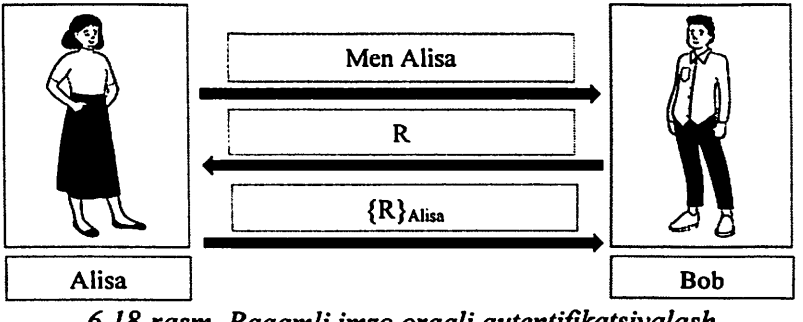
birinchi ulanishdan qayd etgan ma'lumotlarni keyingi ulanishlarda foydalana olmaydi



6.17-rasm. Ochiq kalit asosida autentifikatsiyalash

Biroq, Alisa autentifikatsiyada foydalangan kalitni shifrlashda ham foydalansa, 6.17-rasmda keltirilgan protokolda jiddiy muammo bo'lishi aniq. Faraz qilaylik, Tridiga oldinroq tutib olingan Alisani ochiq kaliti bilan shifrlangan xabar bor, $C=\{M\}_{Alisa}$. Keyin, Tridi o'zini Bob kabi tutib, C ni 2 xabarda Alisaga yuboradi va Alisa uni rasshifrovkalab Tridiga qaytarib yuboradi. Tridi nuqtai nazaridan, bundan yaxshiroq biror narsaga erishish imkonsiz. Buning qulaylik tomoni shundaki, yagona kalit juftini ham ma'lumotni shifrlashda va imzolashda foydalanmaslik zarur.

6.17-rasmda keltirilgan protokolda ochiq kalitni shifrlashdan foydalanilgan. Ushbu protokolni imzolash orqali ham amalga oshirish mumkinmi ? Ha. Uning umumiy ko'rinishi 6.18-rasmda keltirilgan.



6.18-rasm. Raqamli imzo orqali autentifikatsiyalash

Ushbu protokol 6.17-rasmda keltirilgan protokolda mavjud bo'lgan zaiflikga ega. Ushbu protokolda, agar Tridi o'zini Bob kabi tutsa, unda Alisa tomonidan imzolangan biror ma'lumotga ega bo'ladi. Ushbu

muammoning yechimi bu imzolashda va shifrlashda turli kalit juftlaridan foydalanishdir.

6.3. SSH protokoli

Secure Shell protokoli. SSH protokoli aloqa tarmog'ida, masofadan turib amal bajarish, ikki tarmoq foydalanuvchisi orasida xavfsiz kanal hosil qilish uchun foydalaniladigan kriptografik tarmoq protokolidir. Ushbu algoritm xavfsiz tarmoq orqali maxfiy aloqani tashkil etish uchun foydalaniladi va bunda SSH klient va SSH server orasida xavfsiz kanal hosil qilinadi. Ushbu protokolning ikki SSH-1 va SSH-2 variantlari mavjud.

Ushbu protokol Unix yoxud LINUX sistemalariga resurslarga murojaatni amalga oshirishda foydalaniladigan asosiy yutilitalardan sanalib, WINDOWS operatsion tizimi foydalanuvchilari uchun ham moslashtirilgan. Ushbu protokol Telnet yoki boshqa xavfsiz bo'lmagan protokollar (Bekreley rsh, rexec, rlogin) o'rnini bosish maqsadida ishlab chiqilgan. Ushbu protokolda shifrlashdan foydalanish orqali ma'lumotning butunligi va konfidensialligini ta'minlash amalga oshirilgan (Lekin, Edvard Snovden tomonidan bazida NSA (National Security Agency) tomonidan SSHni rasshifrovkalash orqali ma'lumotdan yashirincha foydalanilgan deb ham aytilgan).

SSH protokoli quyidagi imkoniyatlarni beradi:

- Xavfsiz login bilan bog'lanishni;
- Xavfsiz ma'lumot almashishni ochiq (ishonchsiz) kanal orqali amalga oshirishni ta'minlaydi.

SSH protokollari quyidagilarga asoslanadi:

- Ochiq kalitli shifrlash algoritmlariga yoki
- Raqamli sertifikatlarga yoki
- Parollarga.

Ushbu protokolning ikki turdagi varianti, pullik va bepul turlari mavjud.

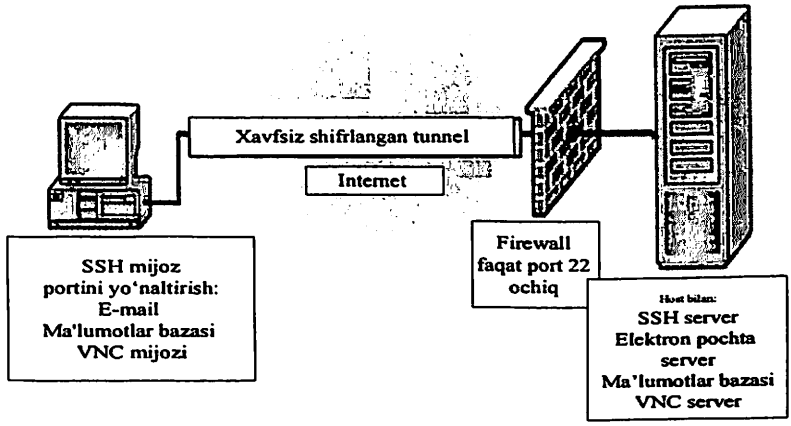
SSH vazifalari

- Xavfsiz buyruq-oynasi (command-shell)
- Xavfsiz fayl transferi
- Port forwarding

Xavfsiz Command-shell. Command shell tizimi Linux, Unix, Windows operatsion tizimlarda mavjud bo'lib, asosan dasturiy vositalarni

yuklashda va boshqa buyruqlarni bajarishda foydalaniladi. Xavfsiz command-shell ilovasi masofadan turib, buyruqlarni bajarishda, fayllarni tahrir qilishda, katalog tarkibini ko'rishda va ma'lumot bazasini boshqarishda foydalanilishi mumkin. Ushbu tizimdan tarmoq administratori masofadan turib, o'z vazifalarini bajarishda, xizmatlarni boshqarishda va boshqa amallarni bajarishda foydalanishi mumkin. Bunda barcha buyruqlar xavfsiz kanal orqali yuboriladi.

Port forwarding. SSH ning ushbu imkoniyati, TCP/IP xizmati orqali amalga oshiriluvchi, e-mail, istemolchi ma'lumoti bazasi va hokazo. ilovalardan xavfsiz kanal orqali foydalanish uchun zamin yaratadi. Ushbu xizmat ba'zida tunellash kabi xizmatni amalga oshirib, TCP/IP ilovalarini xavfsiz kanal orqali amalga oshiradi. Port forwarding xizmati o'rnatilgandan so'ng, himoyalangan kanal orqali bir tomondan (foydalanuvchi qism) ikkinchi tomonga (server tomonga) ma'lumot jo'natiladi. Bunda hosil qilingan yagona himoyalangan kanal orqali ko'plab ilovalar ma'lumotlari yuborilishi mumkin. Ba'zi ilovalarni boshqarishda buyruqlar oynasini o'zi yetarli sanalmaydi, grafik interfeys orqali boshqarish talab etiladi. Ushbu holda SSH ushbu xizmati orqali masofadagi ilova bilan kriptografik himoyalangan kanal hosil qilinadi. Bunga misol qilib, Virtual Network Client (VNC) ni misol qilib olish mumkin (6.18-rasm).

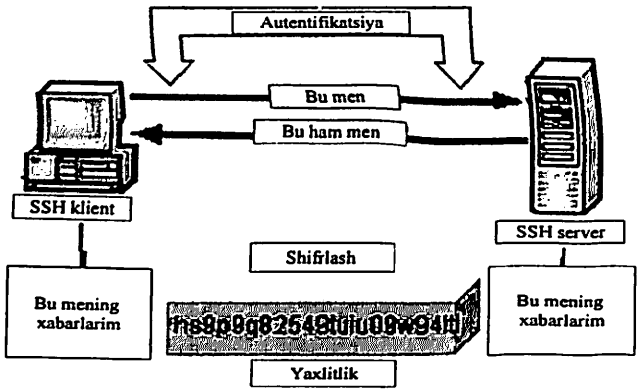


6.18-rasm. Virtual Network Client (VNC)

Xavfsiz fayl transferi. Secure File Transfer Protocol (SFTP) protokoli SSH protokoli asosida ishlab chiqilgan bo'lib, bunda FTP protokolida mavjud ko'plab zaifliklar oldi olingan. Birinchidan SFTP foydalanuvchi login/parolini va yuborilayotgan ma'lumotini shifrlab jo'natadi. Ikkinchidan ushbu protokol SSH ning porti (22 port) orqali ishlaydi. Bundan tashqari FTP protokolida mavjud bo'lgan Network Address Translations (NAT) muammosi uchramaydi.

SSH ning protokol asosi

- Foydalanuvchi autentifikatsiyasi (User authentication);
- Hostga asoslangan autentifikatsiyalash (Host authentication);
- Ma'lumotni shifrlash;
- Ma'lumot butunligi.



6.19-rasm. SSH ning protokol asosi

Foydalanuvchi autentifikatsiyasi (User authentication). Foydalanuvchini haqiqiyligini ta'minlashda SSH tizimi quyidagi turdagi autentifikatsiyalash vositalaridan foydalaniladi:

- Parol asosida;
- Ochiq kalitli shifrlash algoritmlariga asoslangan autentifikatsiyalash usullari;
- Kerberos, NTLM va boshqalar.

Parol asosida autentifikatsiyalash. Ushbu usul boshqa autentifikatsiyalash usullariga qaraganda ko'p uchrab, bunda parol va logini asosida foydalanuvchi haqiqiyligi ta'minlanadi. Ba'zi protokollar, FTP, Telnet protokollari login va parolni kanalda ochiq holatda yuboradi.

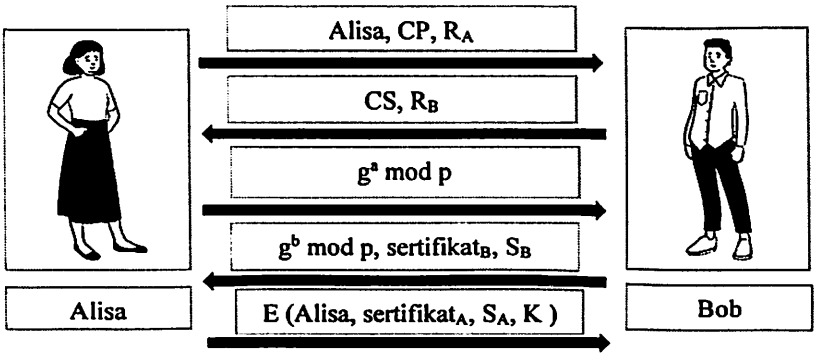
Bu esa buzg'unchiga tarmoqni tinglash va ularni qo'lga kiritish imkonini beradi. Bundan farqli ravishda SSH protokolida login va parol tarmoqda shifrlangan holatda yuboriladi.

SSH_MSG_USERAUTH_REQUEST
- Foydalanuvchi ismi
- Xizmat nomi
- Parol
- FALSE (bayroq holati FALSE)
- Parol

Ushbu so'rovga server quyidagicha javob berishi mumkin:
SSH_MSG_USERAUTH_FAILURE,
SSH_MSG_USERAUTH_SUCCESS, yoki
SSH_MSG_USERAUTH_PASSWD_CHANGEREQ

Ochiq kalitli shifrlash algoritmlariga asoslangan autentifikatsiyalash usullari. Ushbu usul SSH tizimida keng foydalaniladigan autentifikatsiyalash usullaridan biridir. Bunda kalit uzunligi 1024 bitdan 2048 bit oralig'ida bo'ladi. Ushbu usulda foydalanuvchi ochiq kalitlari serverda saqlanadi. Bundan tashqari foydalanuvchi maxfiy kalitga mos parolga ega bo'lib, buzg'unchi maxfiy kalitni bilganda ham parolsiz tizimni boshqara olmaydi.

Quyida sertifikatlarga asoslangan soddalashtirilgan SSH protokoli keltirilgan (6.20-rasm):

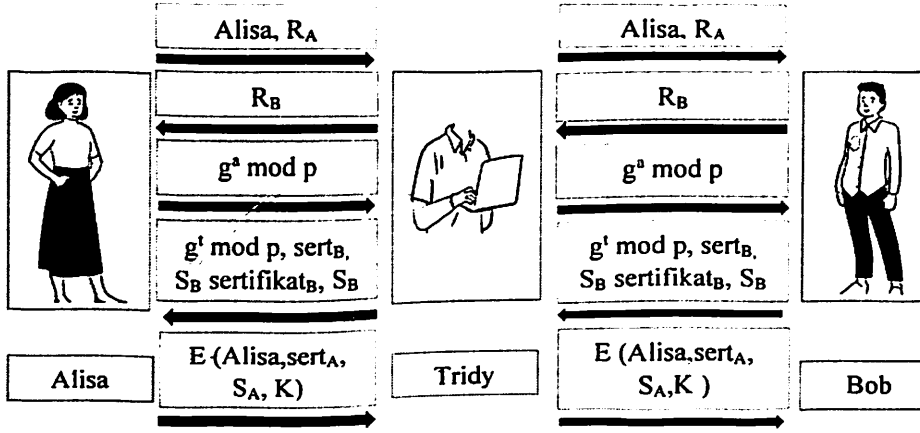


6.20-rasm. SSH protokoli

Bu yerda:
CP = " crypto proposed ", and CS = " crypto selected"

$H = h$ (Alisa, Bob, CP, CS, R_A, R_B, g^a mod p, g^b mod p, g^{ab} mod p,)
$S_B = [H]_{Bob}$
$S_A = [H, Alica, certificate_A]_{Alica}$
$K = g^{ab}$ mod p

SSH da MIM hujumi



6.21-rasm. SSH protokolida MITM hujumi

Alisa quyidagini hisoblaydi:

$H_a = h$ *(Alisa, Bob, CP, CS,* R_A, R_B, g^a *mod p,* g^t *mod p,* g^{at} *mod p,)*

Ammo Bob quyidagiga imzo chekadi:

$H_b = h$ *(Alisa, Bob, CP, CS,* R_A, R_B, g^t *mod p,* g^b *mod p,* g^{bt} *mod p,)*

Host asoslangan autentifikatsiyalash (Host authentication). Ushbu usulda foydalanuvchi hostiga asoslangan holda autentifikatsiyalash amalga oshiriladi. Agar bir nechta foydalanuvchilar bir mashinada bo'lsa u holda ular uchun yagona host kaliti mavjud bo'lib, autentifikatsiyalash aynan shu kalitga asoslangan holda amalga oshiriladi. Ushbu holda foydalanuvchi o'zining shaxsiy kaliti va shaxsini ta'minlash uchun sertifikatini yuboradi. Server esa ochiq kalitni aynan shu foydalanuvchiga tegishli yoki tegishli emasligini va imzoni haqiqiyligini tekshiradi.

SSH_MSG_USERAUTH_REQUEST

- Foydalanuvchi ismi;

- Xizmat nomi;
- "hostbased";
- Ochiq kalitli algoritm nomi;
- Mijoz hosti uchun sertifikat va ochiq kalit;
- Mijoz hosti nomi;
- Mijoz hostida foydalanuvchi ismi;
- Imzo (sessiya raqami, va hak).

Ma'lumotni shifrlash. Yuborilayotgan ma'lumot boshqalar tushuna olmasligi uchun shifrlash algoritmlari yordamida shifrlanadi. Bunda SSH protokoli blokli shifrlash algoritmlari sanalgan (DES, 3DES, Blowfish, AES, va Twofish) lardan foydalanadi. Ma'lumot almashinishdan oldin ikki tomon orasida foydalanilanishi kerak bo'lgan kripografik algoritmlar kelishib olinadi. Autentifikatsiya jarayonidan so'ng, umumiy kalit tanlanib, ushbu kalit asosida foydalanuvichilar ma'lumotni shifrlab yuborishadi.

Ma'lumot butunligi. Ma'lumot uzatilish jarayonida buzg'unchi tomonidan ma'lumotni yo'q qilinishga urinish yoki ma'lumotni o'zgartirish holatlari kuzatiladi. Ushbu holatlarni oldini olish va tekshirish uchun SSH tizimlarida ma'lumot butunligini ta'minlash algoritmlari foydalaniladi. SSH1 protokolida ma'lumotni butunligini tekshirishda oddiy 32 bitli CRC ma'lumotni tekshirish tizimidan foydalanilgan bo'lsa, SSH2 tizimida esa MAC (Message Authentication Code) tizimlaridan foydalanilgan.

CRC (Cyclic Redundancy Check). Ushbu tizim ma'lumotni butunligini tekshirishda xatolikni tekshiruvchi kodlardan foydalanadi. Ushbu tizim W. Wesley Peterson tomonidan 1961-yilda ixtiro qilingan bo'lib, 32 bitli CRC tizim Ethernet uchun foydalaniladi.

Misol o'rnida 14 bitli ma'lumot va 3-bitli CRC tizimidan x^3+x+1 ko'phadiga asoslangan holda olib, ma'lumot dastlab ikkilik ko'rinishda o'tkaziladi.

M=11010011101100 va CRC 1011 ga teng. Dastlab ma'lumot bitiga CRC bitiga mos ravishda 0 va 1 lar qo'shiladi.

11010011101100 000 <--- input right padded by 3 bits
1011 <--- divisor (4 bits) = x^3+x+1

01100011101100 000 <--- result

Har bir CRC qo'shilganda natija uzunligi bir bitga kamayadi. Ushbu ketma-ketlik ma'lumot uzunligi to'liq 0 bo'lmagunga qadar davom ettiriladi va to'ldirilgan 0lar soniga teng bo'lgan qoldiq natija olinadi.

```
11010011101100 000
1011
01100011101100 000
 1011
00111011101100 000
  1011
00010111101100 000
   1011
00000001101100 000
     1011
00000000110100 000
      1011
00000000011000 000
       1011
00000000001110 000
        1011
00000000000101 000
         101 1
---------------
00000000000000 100
```

Ushbu olingan 100 qiymat qoldiq sanalib, ma'lumot uchun CRC qiymatni bildiradi.

Ma'lumotni tekshirish jarayoni ham yuqoridagi jarayonga o'xshash bo'lib, faqat qo'shiladigan bitlarning birinchi birlik bitga o'zgartiriladi.

```
11010011101100 100      <--- ma'lumot & tekshiruvchi qiymat bilan
1011                <--- bo'luvchi
01100011101100 100          <--- natija
 1011               <--- bo'luvchi ...
00111011101100 100

.....
```

00000000001110 100
1011
00000000000101 100
101 1
---
0 <— qoldiq

Agar natijaviy qoldiq 0 ga teng bo'lsa, kelgan ma'lumot o'zgarmagan aks holda o'zgargan deb topiladi.

Amalda ko'plab foydalaniladigan CRC ko'phadi uzunliklari quyidagicha:

- 9 bit (CRC-8);
- 17 bit (CRC-16);
- 33 bit (CRC-32);
- 65 bit (CRC-64).

SSH protokolida quyidagi kriptografik algoritmlardan foydalanilgan:

- TCP o'rniga SCTP protokoli qo'llanilgan;
- ECDSA ERI algoritmi;
- ECDH kalit almashinish protokoli;
- UMAC tizimi, ma'lumotni butunligini tekshirish uchun (HMAC o'rniga).

6.4. SSL/TLS protokoli

Transport Layer Security (TLS) dastlab yaratilgan Secure Sockets Layer (SSL) protokolining davomchisi sanalib, kompyuter tarmog'ida aloqa xavfsizligini ta'minlash uchun yaratilgan va bir nechta kriptografik protokollar va algoritmlardan tashkil topgan. Ushbu protokolda X.509 sertifikatidan foydalanilgan bo'lib, tomonlarni autentifikatsiyalashda assimetrik shifrlash algoritmlaridan foydalaniladi.

X.509 sertifikati. Kriptografiyada X.509 standarti ochiq kalitli infratuzilmalar (public key infrastructure (PKI)) va imtiyozga asoslangan boshqarish infratuzilmalari (Privilege Management Infrastructure (PMI)) uchun mo'ljallangan.

Ushbu X.509 v3 sertifikatining tuzilishi quyidagicha:

- **Certificate**
  - **Version** (versiya)
  - **Serial Number** (serial raqami)
  - **Algorithm ID** (algoritm ID si)

- **Issuer** (sertifikat beruvchi tashkilot, emitent)
- **Validity** (amal qilish muddati)
  - **Not Before**
  - **Not After**
- **Subject** (sertifikat oluvchi tashkilot, istemolchi)
- **Subject Public Key Info** (istemolchi ochiq kalit ma'lumoti)
  - **Public Key Algorithm** (ochiq kalit algoritmi)
  - **Subject Public Key** (ochiq kalit)
- **Issuer Unique Identifier (optional)** (emitentning takrorlanmas identifikatori)
- **Subject Unique Identifier (optional)** (istemolchining takrorlanmas identifikatori)
- **Extensions (optional)** (kengaytirilgan imkoniyatlari)
  - ...

- **Certificate Signature Algorithm** (sertifikatda foydalanilgan ERI algoritmi)
- **Certificate Signature** (sertifikat qo'yilgan imzo)

Misol tariqasida quyida OpenSSL asosida hosil qilingan sertifikat berilgan:

$ openssl x509 -in freesoft-certificate.pem -noout -text

Certificate:

Data:

Version: 1 (0x0)

Serial Number: 7829 (0x1e95)

Signature Algorithm: md5WithRSAEncryption

Issuer: C=ZA, ST=Western Cape, L=Cape Town, O=Thawte Consulting cc,
OU=Certification Services Division,
CN=Thawte Server CA/emailAddress=server-certs@thawte.com

Validity

Not Before: Jul 9 16:04:02 1998 GMT

Not After : Jul 9 16:04:02 1999 GMT

Subject: C=US, ST=Maryland, L=Pasadena, O=Brent Baccala, OU=FreeSoft, CN=www.freesoft.org/emailAddress=baccala@freesoft.org

Subject Public Key Info:

Public Key Algorithm: rsaEncryption

RSA Public Key: (1024 bit)
Modulus (1024 bit):
00:b4:31:98:0a:c4:bc:62:c1:88:aa:dc:b0:c8:bb:
33:35:19:d5:0c:64:b9:3d:41:b2:96:fc:f3:31:e1:
66:36:d0:8e:56:12:44:ba:75:eb:e8:1c:9c:5b:66:
70:33:52:14:c9:ec:4f:91:51:70:39:de:53:85:17:
16:94:6e:ee:f4:d5:6f:d5:ca:b3:47:5e:1b:0c:7b:
c5:cc:2b:6b:c1:90:c3:16:31:0d:bf:7a:c7:47:77:
8f:a0:21:c7:4c:d0:16:65:00:c1:0f:d7:b8:80:e3:
d2:75:6b:c1:ea:9e:5c:5c:ea:7d:c1:a1:10:bc:b8:
e8:35:1c:9e:27:52:7e:41:8f
Exponent: 65537 (0x10001)
Signature Algorithm: md5WithRSAEncryption
93:5f:8f:5f:c5:af:bf:0a:ab:a5:6d:fb:24:5f:b6:59:5d:9d:
92:2e:4a:1b:8b:ac:7d:99:17:5d:cd:19:f6:ad:ef:63:2f:92:
ab:2f:4b:cf:0a:13:90:ee:2c:0e:43:03:be:f6:ea:8e:9c:67:
d0:a2:40:03:f7:ef:6a:15:09:79:a9:46:ed:b7:16:1b:41:72:
0d:19:aa:ad:dd:9a:df:ab:97:50:65:f5:5e:85:a6:ef:19:d1:
5a:de:9d:ea:63:cd:cb:cc:6d:5d:01:85:b5:6d:c8:f3:d9:f7:
8f:0e:fc:ba:1f:34:e9:96:6e:6c:cf:f2:ef:9b:bf:de:b5:22:
68:9f

Sertifikatning eng so‘ngi bandida (Signature Algorithm) sertifikatning undan yuqorigi bandida joylashgan ma’lumotga qo‘yilgan imzo va imzo qo‘yish uchun foydalanilgan algoritm nomi keltirilgan. Ushbu imzoni sertifikat beruvchi tashkilot o‘zining maxfiy kaliti asosida amalga oshiradi.

Internet tarmoq protokollari orasida olinganda, SSL/TLS protokoli ilova (Application) sathida ishlaydi. Ushbu sathni OSI modelida ekvivalent bo‘lgan sathlarda ifodalansa, SSL/TLS 5-seans (session) sathdan boshlanadi va oltinchi (presentation) sathda ishlaydi. Sessiya sathida amalga oshirilayotgan sessiya uchun umumiy kalitni va shifrlash algoritmlarini tanlash uchun assimetrik shifrlash algoritmlari yordamida handshake (qo‘l berib ko‘rishish) jarayoni amalga oshiriladi. Shundan so‘ng oltinchi sathda hosil qilingan umumiy kalit bilan simmetrik shifrlash asosida aloqa kanallari maxfiyligi ta’minlanadi. Har ikki SSL/TLS protokol yarim transport sathida ishlaydi, ya’ni paketni shifrlashda.

TLS (yoki SSL) protokoli kliyent-server arxitekturasida ishlaydi va kliyent serverga ulunish uchun TLS aloqani o'rnatilganligini ko'rsatishi shart. Buning uchun odatda ikki usuldan foydalaniladi:

- TLS bog'lanishlar uchun alohida port berish (masalan, HTTPS uchun 443 port orqali);
- Protokolga asoslangan usul.

Klient va server TLS bog'lanishidan foydalanishga roziligini "qo'l siqish" (handshake) amaliyoti orqali bildiradi. Ushbu jarayon davomida kliyent va server xavfsiz aloqani tashkil etish uchun kerakli bo'lgan ko'plab parametrlarni kelishib oladilar:

-Ushbu jarayon dastlab kliyent serverga TLS bog'lanishni amalga oshirgandan so'ng boshlanib, unda serverga foydalinilishi mumkin bo'lgan kriptografik algoritmlarning ro'yxatini yuboradi.

-Server qabul qilingan ro'yxatdan kerakli algoritmlarni tanlaydi.

-Shundan so'ng server o'zining ochiq kalitidan tashkil topgan va ishonarli tashkilot tomonidan berilgan raqamli sertifikatini yuboradi.

-Kliyent bog'lanishni boshlashdan oldin kelgan sertifikatni haqiqiyligini tekshiradi.

-Shundan so'ng, kliyent maxfiy aloqani hosil qilish uchun kerakli bo'ladigan sessiya kalitini hosil qilish uchun foydalaniladigan tasodifiy sonni serverning ochiq kaliti bilan shifrlab yuboradi.

- Qabul qilingan tasodifiy son orqali har ikkala tomon shifrlash va rasshifrovkalash uchun kerakli bo'lgan kalitni hosil qiladi.

Natijada himoyalangan aloqa hosil qilinadi va aloqa tugagunga qadar ikki tomon orasidagi ma'lumot shifrlangan holda uzatiladi.

Tarmoqda ma'lumotni xavfsizligini ta'minlash muammosini hal qilishga urinishlar natijasida Netscape tomonidan SSL protokolining birinchi versiyasi ishlab chiqildi ammo ommaga foydalanish uchun tarqatilmadi. Sababi, ushbu birinchi versiyada jiddiy xavfsizlik muamosi mavjud edi. Shundan so'ng ushbu kamchiliklar bartaraf etilib, 1995 yilda ikkinchi versiya shaklida amalda foydalanish uchun taqdim etildi. Ushbu ikkinchi versiya ham amalda jiddiy kamchiliklarga egaligi aniqlanib, 1996 yilda SSLv3.0 versiyasi taqdim etildi.

Shundan so'ng SSLv3.0 da mavjud kamchiliklar bartaraf etilib, 1999 yilda TLS 1.0 taqdim etildi. SSLv3.0 va TLS 1.0 o'rtasida katta farq mavjud bo'lmay, TLS 1.0 protokoli SSLv3.0 ga qaraganda o'zining moslashuvchanligi bilan ajralib turdi.

TLS 1.1 protokoli 2006 yil aprel oyida ommaga taqdim etildi va oldingi versiyadan asosiy farqi, cipher-block chaining (CBC) rejimiga qarshi himoya usuli qo'shildi.

TLS 1.2 protokoli 2008 yil avgust oyida taqdim etilib, quyidagi o'zgarishlarni o'zida mujassam etgan:

-MD5-SHA-1 algoritmlari SHA-256 algoritmi bilan almashtirilgan;

-Ushbu protokoldan boshlab shifrlash algoritmi sifatida AES shifrlash algoritmi qo'shildi.

-Autentifikatsiyalash shifrlash algoritmi sifatida Galois/Counter Mode (GCM) rejimiga asoslangan AES algoritmidan foydalanila boshlandi.

Hozirgi kunda kelib, TLS 1.3 protokoli ustida ishlar amalga oshirilmoqda va unda odingi versiyalarga mavjud zaif algoritmlar almashtirilishi ko'zga tutilmoqda.

TLS/SSL protokolida foydalanilgan raqamli sertifikatlarni yaratuvchi, uchinchi ishonchli tomon sifatida qatnashgan tashkilotlarning 2015 yil boshidagi ko'rsatkichi quyida ko'rsatilgan:

O'rin	Tashkilot	Foydalanilishi	Bozordagi ulushi
1.	Comodo	6.6%	33.6%
2.	Symantec Group	6.5%	33.2%
3.	Go Daddy Group	2.6%	13.2%
4.	GlobalSign	2.2%	11.3%
5.	DigiCert	0.6%	2.9%

Kalit taqsimlash protokollari. Kliyent-server orasida himoyalangan kanal hosil qilinishidan oldin, ikki tomon orasida umumiy kalit hosil qilinishi va keyinchalik barcha aloqalar ushbu kalit bilan shifrlanishi zarur. Amalda quyidagi kalit taqsimlash protokollari foydalaniladi: RSA asosida ochiq kalit va maxfiy kalitdan foydalanish orqali (TLS handshake protokolida foydalanilgan TLS_RSA protokoli), Diffie-Hellman (TLS_DH), vaqtinchalik Diffie-Hellman (TLS_DHE), Elliptic Curve Diffie-Hellman (TLS_ECDH), vaqtinchalik Elliptic Curve Diffie-Hellman (TLS_ECDHE), anonim Diffie-Hellman (TLS_DH_anon), oldindan kelishilgan kalit asosida (pre-shared key (TLS_PSK)) va xavfsiz tasodifiy parol (Secure Remote Password (TLS_SRP)) asosida amalga oshiriladi.

TLS_DH_anon va TLS_ECDH_anon usullari “o‘rtada turgan odam” (Man-in-the-middle attack) hujumiga bardoshsiz bo‘lib, amalda ularning o‘rnida TLS_DHE vaTLS_ECDHE butunlay xavfsizlikni (forward secrecy) ta’minlash maqsadida foydalaniladi.

Quyidagi jadvalda protokol versiyalarida foydalanilgan kalitlarni taqsimlash protokollari keltirilgan.

Algoritmlar	SSL 2.0	SSL 3.0	TLS 1.0	TLS 1.1	TLS 1.2
RSA	Bor	Bor	Bor	Bor	Bor
DH-RSA					
DHE-RSA (forward secrecy)		Bor	Bor	Bor	Bor
ECDH-RSA					
ECDHE-RSA (forward secrecy)			Bor	Bor	Bor
DH-DSS					
DHE-DSS (forward secrecy)		Bor	Bor	Bor	Bor
ECDH-ECDSA					
ECDHE-ECDSA (forward secrecy)			Bor	Bor	Bor
PSK					
PSK-RSA					
DHE-PSK (forward secrecy)			Bor	Bor	Bor
ECDHE-PSK (forward secrecy)					
SRP					
SRP-DSS			Bor	Bor	Bor
SRP-RSA					
Kerberos			Bor	Bor	Bor
DH-ANON (insecure)			Bor	Bor	Bor
ECDH-ANON (insecure)			Bor	Bor	Bor
GOST R 34.10-94 / 34.10-2001			Bor	Bor	Bor

Kalit taqsimlash protokollari asosida hosil qilingan kalit bilan quyidagi simmetrik shifrlash algoritmlari yordamida ma’lumotni shifrlab

jo'natiladi. Jadvalda mashhur hujum turlariga qarshi protokolning holati keltirilgan. Bu yerda:

N/A – mavjud emas, S – xavfsiz, D – shartlarni kamaytirishga bog'liq, L – kam darajada xavfsiz.

Shifrlash algoritmi			Protokol versiyasi				
Turi	**Algoritm**	**Kalit uzunligi**	**SSL 2.0**	**SSL 3.0**	**TLS 1.0**	**TLS 1.1**	**TLS 1.2**
Blokli shifrlash algoritmlari	AES GCM	256, 128	N/A	N/A	N/A	N/A	S
	AES CCM		N/A	N/A	N/A	N/A	S
	AES CBC		N/A	N/A	D	S	S
	Camellia GCM	256, 128	N/A	N/A	N/A	N/A	S
	Camellia CBC		N/A	N/A	D	S	S
	ARIA GCM	256, 128	N/A	N/A	N/A	N/A	S
	ARIA CBC		N/A	N/A	D	S	S
	SEED CBC	128	N/A	N/A	D	S	S
	3DES EDE CBC	112	I	I	L	L	L
	GOST 28147-89 CNT	256	N/A	N/A	S	S	S
	IDEA CBC	128	I	I	D	S	N/A
	DES CBC	56	I	I	I	I	N/A
	RC2 CBC	40	I	I	I	N/A	N/A
Oqimli shifrlash	ChaCha20-Poly1305	256	N/A	N/A	N/A	N/A	S
	RC4	128	I	I	I	I	I

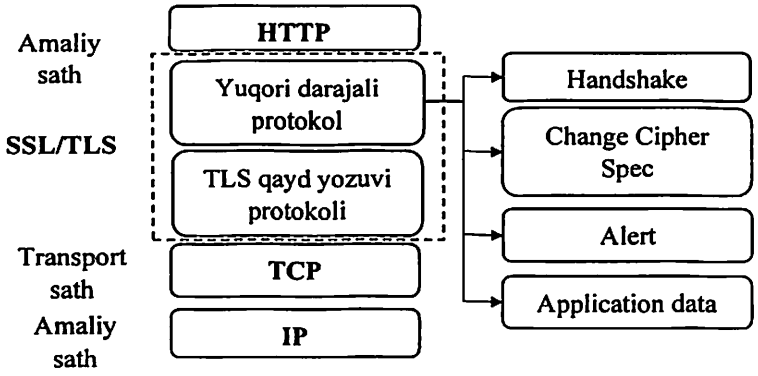
Quyida esa ma'lumotni autentifikatsiyalash kodlarini SSL/TLS protokol versiyalarida ishlatilish holati keltirilgan.

Algoritm	**SSL 2.0**	**SSL 3.0**	**TLS 1.0**	**TLS 1.1**	**TLS 1.2**

HMAC-MD5	Ha	Ha	Ha	Ha	Ha
HMAC-SHA1	Yo‘q	Ha	Ha	Ha	Ha
HMAC-SHA256/384	Yo‘q	Yo‘q	Yo‘q	Yo‘q	Ha
AEAD	Yo‘q	Yo‘q	Yo‘q	Yo‘q	Ha
GOST 28147-89 IMIT	Yo‘q	Yo‘q	Ha	Ha	Ha
GOST R 34.11-94	Yo‘q	Yo‘q	Ha	Ha	Ha

Hozirda yuqorida nomlari keltirilgan SSL/TLS protokol versiyalari amalda foydalanilmoqda va quyidagi jadvalda ularning web cahifalarda foydalanish ko‘rsatkichlari va ularning xavfsizlik xususiyati keltirilgan.

Protokol versiyasi	**Web sahifalarda qo‘llab quvatlanishi**	**Xavfsizlik ko‘rsatkichi**
SSL 2.0	14.4% (–0.5%)	Xavfsiz emas
SSL 3.0	47.3% (–3.1%)	Xavfsiz emas
TLS 1.0	99.7% (±0.0%)	Algoritm turiga bog‘liq
TLS 1.1	51.5% (+1.6%)	Algoritm turiga bog‘liq
TLS 1.2	54.5% (+1.8%)	Algoritm turiga bog‘liq



SSL/TLS sathining quyi tashkil etuvchi protokoli (TLS qayd yozuvi protokoli), dastlabki ma’lumotni fragmentlarga ajratish, sozlanishga ko‘ra fragment ma’lumotni siqish, siqilgan ma’lumotga uning MAC qiymatini qo‘shish, hosil bo‘lgan ma’lumot juftini shifrlash algoritmi yordamida shifrlash va unga TLS qayd yozuvi sarlavhasini qo‘shish amallaridan hosil bo‘ladi.

Yuqori darajali protokol. Ushbu protokol TLS qayd yozuvi protokoli ustida joylashtirilgan bo'lib, u to'rtta protokoldan iborat. Har bir protokol o'zining maxsus vazifasiga ega bo'lib, ular alohida yoki birgalikda ham foydalanilishi mumkin.

Handshake protokoli. Ushbu protokol har ikki tomonda bir-birini autentifikatsiyalash, foydalaniladigan kriptografik algoritmlarni kelishish va boshqa bog'lanish parametlarini almashish imkonini beradi. Ushbu protokol kliyent va server orasida almashinuvchi to'rtta xabarlar majmuasidan iborat. Har bir xabarlar majmuasi alohida paket holatida yuboriladi. Quyida ushbu protokolning umumiy ko'rinishi keltirilgan.

Certificate (server)	Barcha kalit almashinish algoritmlari uchun zarur
ServerKeyExchange	Ba'zi hollarda, masalan Diffi-Xelman algoritmida zarur
CertificateRequest	Kliyent autentifikatsiyasi talab etilganda zarur.
Certificate (client)	CertificateRequest so'roviga javob berishda zarur.
CertificateVerify	Kliyent Certificate yuborilganda zarur.

ChangeCipherSpec Protocol: ushbu protokol asosida aloqa kanali himoyalanadi.

Alert Protocol: ushbu xabar berish protokoli, barcha protokol natijalarini e'lon qilishda foydalaniladi.

Application Data Protocol: ushbu protokol ilova sathidan ma'lumotni olib, uni maxfiy kanal orqali yuborishni ta'minlaydi.

TLS qayd yozuvi formati.

Ushbu format uchta maydondan iborat bo'lib, uning asosida yuqori darajali protokol quriladi.

- Byte 0: TLS qayd yozuvi turi.
- Bytes 1-2:TLS protokol versiyasi (major/minor).
- Bytes 3-4: qayd yozuvidagi ma'lumot uzunligi (o'zidan tashqari). Maksimal qiymati 16384 bit yoki 16Kbit.

TLS qayd yozuvi turi	Versiyasi		Ma'lumot uzunligi		yuqori darajali protokol
	major	minor	(bits 15..8)	(bits 7..0)	

TLS qayd yozuvi turi

Hex	Dec	Tyri
0x14	20	ChangeCipherSpec

0x15	21	Alert
0x16	22	Handshake
0x17	23	Application
0x18	24	Heartbeat

Protokol versiyasi

Hex	Dec	Protokol versiyasi
0x0300	3,0	SSL 3.0
0x0301	3,1	TLS 1.0
0x0302	3,2	TLS 1.1
0x0303	3,3	TLS 1.2

Handshake protokol formati. Ushbu protokol TLS protokolida asosiy protokollarda biri sanalib, bu protokol orqali xavfsizlik parametrlari uzatiladi. Ushbu protokol orqali o'n bir turdagi xabar uzatilashi mumkin.

Byte +0	Byte +1	Byte +2	Byte +3
22			
Versiya		Uzunlik	
Minor	Major	(bits 15..8)	(bits 7..0)
Xabar turi	Handshake ma'lumoti uzunligi		
	(bits 23..16)	(bits 15..8)	(bits 7..0)
Handshake ma'lumoti			
Xabar turi	Handshake ma'lumoti uzunligi		
	(bits 23..16)	(bits 15..8)	(bits 7..0)
Handshake ma'lumoti			

Handshake ma'lumoti uzunligi. Ushbu maydon uzunligi 3 bayt bo'lib, faqat Handshake ma'lumoti uzunligini bildiradi, sarlavhani o'z ichiga olmagan holda. Bitta TLS yozishmasida bir nechta Handshake ma'lumoti bo'lishi mumkin.

Handshake protokolida xabar turi quyidagicha bo'lishi mumkin:

Xabar turi		
Dec	**Hex**	**Tasnif**
0	0x00	HelloRequest
1	0x01	ClientHello
2	0x02	ServerHello
4	0x04	NewSessionTicke
11	0x0b	Certificate
12	0x0c	ServerKeyExchange
13	0x0d	CertificateRequest
14	0x0e	ServerHelloDone
15	0x0f	CertificateVerify
16	0x10	ClientKeyExchange
20	0x14	Finished

HelloRequest: ushbu xabar orqali server handshake protokolini qayta yuklaydi. Ushbu xabar ko'p foydalanilmasada, agar bog'lanish uzoq vaqt davom ettirilsa, kalitni zaifligi ortadi. Shunday vaziyatda seans kalitini qaytadan hosil qilish va bog'lanishni qayta qurish uchun foydalaniladi.

Byte +0	Byte +1	Byte +2	Byte +3
22			
Versiya		Uzunlik	
Minor	Major	4 bit	
0	Handshake ma'lumoti uzunligi		
	0 bit		

ClientHello: Handshake protokoli odatda ushbu xabardan boshlanib, ushbu xabar orqali kriptografik algoritmlar ro'yxati, siqish usullari va kengaytmalar ro'yxati yuboriladi. Bundan tashqari ushbu xabar, sessiyani qaytadan yuklash uchun ham ishlatiladi.

Byte +0	Byte +1	Byte +2	Byte +3
22			
Versiya		Uzunlik	
Major	Minor	Ma'lumotga bog'liq holda	
01	Handshake ma'lumoti uzunligi		
	3 bayt		
SSL/TLS versiyasi (major/minor)		32 bitli tasodifiy kalit	

SessionId uzunligi	Max 32 bitli SessionId
Kriptografik algoritmlar ro'yxati	
Siqish usullari	Kengaytmalar

ServerHello: ushbu xabar xam **ClientHello** ga o'xshash bo'lib, farqli tomoni kriptografik algoritmlar ro'yxati va siqish usullari maydonidadir. Agar SessionId>0 bo'lsa, u holda kliyent ushbu parametrdan kelajakda foydalanadi.

Byte +0	Byte +1	Byte +2	Byte +3
22			
Versiya		Uzunlik	
Major	Minor	Ma'lumotga bog'liq holda	
02	Handshake ma'lumoti uzunligi		
	3 bayt		
SSL/TLS versiyasi (major/minor)		32 bitli tasodifiy kalit	
SessionId uzunligi	Max 32 bitli SessionId		
Kriptografik algoritmlar ro'yxati			
Siqish usullari		Kengaytmalar	

Certificate: ushbu xabar ochiq kalit sertifikatidan tashkil topgan. Ushbu sertifikat TLS protokolida sertifikat iyerarxiyasi va PKI dan foydalanish imkonini beradi.

Byte +0	Byte +1	Byte +2	Byte +3
22			
Versiya		Uzunlik	
Major	Minor	Ma'lumotga bog'liq holda	
11	Handshake ma'lumoti uzunligi		
	3 bayt		
Sertifikatlar ketma-ketligi uzunligi		Sertifikat uzunligi	
sertifikat	...bir nechta sertifikatlar		

ServerKeyExchange. Ushbu xabar o'zida kalit almashinish protokollari parametrlarini saqlab, ushbu protokol asosida almashingan kalit asosida semmetrik shifrlash algoritmlari uchun kalit hosil qilinadi.

Ushbu xabar tanlovga ko'ra amalga oshiriladi. Odatda sertificate xabari orqali umumiy kalit asosida qilinadi.

Byte +0	Byte +1	Byte +2	Byte +3
22			
Versiya		Uzunlik	
Major	Minor	Ma'lumotga bog'liq holda	
12	Handshake ma'lumoti uzunligi		
	3 bayt		
Algoritm parametrlari			

CertificateRequest. Ushbu xabar server kliyentdan autentifikatsiyadan o'tishni talab qilganda bajariladi. Ushbu xabar umuman olganda, veb xizmatlar uchun ko'p talab etilmasada, ba'zida talab etiladi. Bundan tashqari, ushbu xabar orqali kliyent o'zining sertifikat versiyasi va qaysi tashkilot tomonidan berilgani haqidagi ma'lumot yuboriladi.

Byte +0	Byte +1	Byte +2	Byte +3
22			
Versiya		Uzunlik	
Major	Minor	Ma'lumotga bog'liq holda	
13	Handshake ma'lumoti uzunligi		
	3 bayt		
Sertifikat tipi uzunligi	Sertifikat avtorlari uzunligi	Sertifikat avtorining nomi	.....

ServerHelloDone. Ushbu xabar server tomon handshake protokilini ishini tugatganda yuboriladi. Ushbu xabar o'zida ortiqcha ma'lumotni olmaydi.

Byte +0	Byte +1	Byte +2	Byte +3
22			
Versiya		Uzunlik	
Major	Minor	Ma'lumotga bog'liq holda	
14	Handshake ma'lumoti uzunligi		
	0 bayt		

ClientKeyExchange. Ushbu xabar serverni hosil qilinayotgan simmetrik kalit bilan ta'minlash uchun parametrlarni yuborishda

foydalaniladi. Ushbu xabardani algoritmlar ServerKeyExchange xabariga yuborilgan algoritmlar bilan mos keladi.

Byte +0	Byte +1	Byte +2	Byte +3
22			
Versiya		Uzunlik	
Major	Minor	Ma'lumotga bog'liq holda	
16	Handshake ma'lumoti uzunligi		
	3 bayt		
Algoritm parametrlari			

CertificateVerify. Ushbu xabar orqali kliyent server kalitini uning sertifikatiga mosligini tekshiradi. Ushbu xabar imzolangan xeshdan tashkil topadi. Ushbu xabar CertificateRequest so'rovi yuborilgan holda va Certificate xabarini tasdiqlash uchun foydalaniladi.

Byte +0	Byte +1	Byte +2	Byte +3
22			
Versiya		Uzunlik	
Major	Minor	Ma'lumotga bog'liq holda	
15	Handshake ma'lumoti uzunligi		
	3 bayt		
Imzolangan xesh			

Finished. Ushbu xabar orqali TLS muolajasi tugallanganligi va tanlangan shifrlash algoritmlari aktivlashganligini ko'rsatiladi. Ushbu xabar oldingi barcha handshake protokol xabarlarini o'z ichiga oladi.

Byte +0	Byte +1	Byte +2	Byte +3
22			
Versiya		Uzunlik	
Major	Minor	Ma'lumotga bog'liq holda	
20	Handshake ma'lumoti uzunligi		
	3 bayt		
Imzolangan xesh			

ChangeCipherSpec protokol formati. Ushbu protokol bitta xabardan iborat bo'lib, paketning shifrlanganligini bildiradi. TLS protokoli butun TLS qayd yozuvi ma'lumotini inkapsusiyalaydi.

Byte +0	Byte +1	Byte +2	Byte +3

20		
Versiya		Uzunlik
Major	Minor	1 bit
1		

Alert protokoli. Handshaking va application turidagi protokol o'z ishini normal holatda tugatmagan holda Alert protokoli orqali xabar beriladi. Shunga qaramasdan, ushbu xabar har bir turlagi protokol bilan birgalikda yuboriladi. Agar ushbu xabar ma'lumoti "fatal error" bo'lsa, u holda sessiya zudlik bilan yopiladi. Agar xabar ma'lumoti "warning" bo'lsa, u holda masofadagi foydalanuvchi talabiga ko'ra sessiyani tugatish yoki tugatmaslik tanlanadi.

Byte +0	Byte +1	Byte +2	Byte +3
21			
Versiyasi		Uzunligi	
Major	Minor	0	2
Daraja		Tasnif	

Daraja. Ushbu maydon Alert ni darajasini ko'rsatadi. Yuqorida aytib o'tilganidek, ikki turdagi Alert mavjud.

Kodi	Daraja turi	Bog'lanish holati
1	warning	Bog'lanish yoki xavfsizlik o'zgaruvchan bo'lishi mumkin.
2	fatal	Bog'lanish yoki xavfsizlik xavfli bo'lishi mumkin, tiklib bo'lmas xatolik yuz bergan.

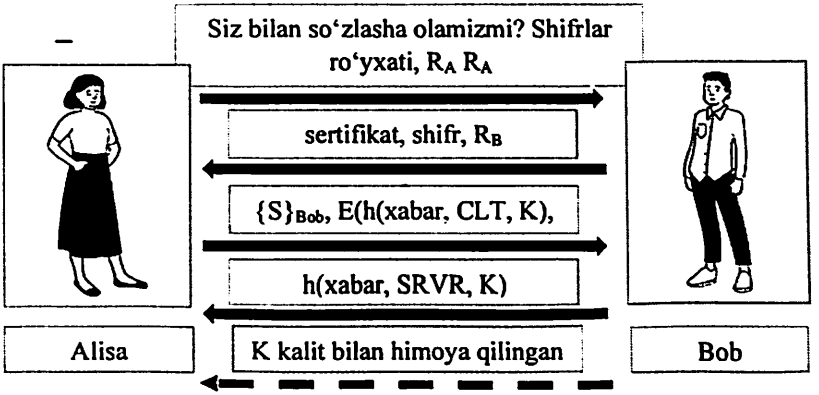
Agar jarayon normal holatda o'z ishini tugatgan taqdirda ham, biror bir daraja turi qaytariladi. Jarayonning qanday tugaganligi esa tasnif asosida aniqlanadi. Quyida tasnif jadvali keltirilgan.

Kodi	Tasnif	Daraja
0	Close notify	warning/fatal
10	Unexpected message	fatal
20	Bad record MAC	fatal
21	Decryption failed	fatal
22	Record overflow	fatal
30	Decompression failure	fatal

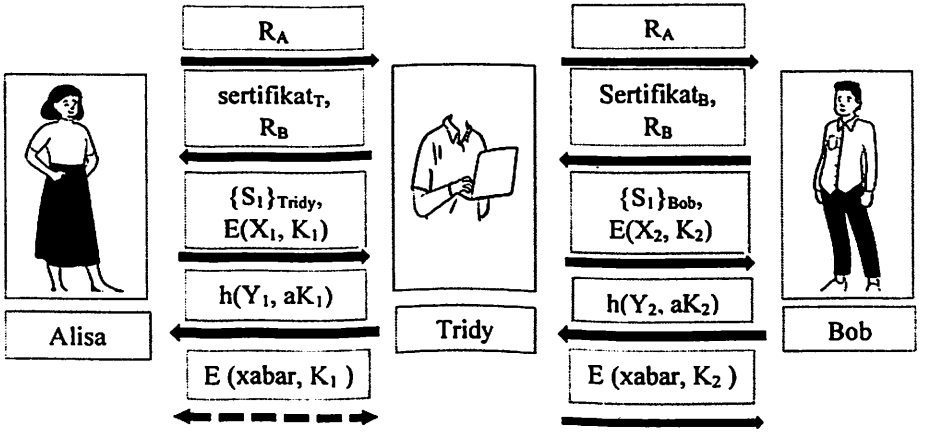
Kodi	Tasnif	Daraja
40	Handshake failure	fatal
41	No certificate	warning/fatal
42	Bad certificate	warning/fatal
43	Unsupported certificate	warning/fatal
44	Certificate revoked	warning/fatal
45	Certificate expired	warning/fatal
46	Certificate unknown	warning/fatal
47	Illegal parameter	fatal
48	Unknown CA (Certificate authority)	fatal
49	Access denied	fatal
50	Decode error	fatal
51	Decrypt error	warning/fatal
60	Export restriction	fatal
70	Protocol version	Fatal
71	Insufficient security	Fatal
80	Internal error	Fatal
90	User canceled	fatal
100	No renegotiation	warning
110	Unsupported extension	warning
111	Certificate unobtainable	warning
112	Unrecognized name	warning/fatal
113	Bad certificate status response	Fatal
114	Bad certificate hash value	Fatal
115	Unknown PSK identity (used in TLS-PSK and TLS-SRP)	Fatal
120	No Application Protocol	Fatal

ApplicationData protokoli. Ushbu protokol ma'lumotni shifrlab jo'natuvchi protokol sanalib, ma'lumot va uning MAS qiymati birgalikda shifrlanib yuboriladi.

Soddalashgan holda SSL/TLS protokoli ishlash prinsipi quyidagicha:



dastlabki maxfiy kalit.
$K = h(S,R_A,R_B)$
"msgs" – oldingi barcha xabarlar.
CLNTva SRVR lar o'zgarmaslar.



6.5. IPSec protokoli

Internet Protocol Security (IPsec) protokol tizimlari Internet Protocol (IP) bog'lanishlarini xavfsizligini jo'natilayotgan har bir paketni shifrlash orqali ta'minlaydi. Ushbu protokol sessiya boshlanishida ikki tomonlama autentifikatsiyani amalga oshiradi va keyinchalik umumiy kriptografik kalitga ega bo'linadi. IPSec protokoli ma'lumot oqimlari

himoyasini ikki host orasida (host-to-host), ikki tarmoq orasida (network-to-network) va host va tarmoq orasida (network-to-host).

Ushbu protokol OSI modelining tarmoq sathida ishlaydi va tarmoq sathida autentifikatsiyalashni, ma'lumot autentifikatsiyasini, ma'lumot butunligini, ma'lumot maxfiyligini va ma'lumotni takrorlashdan himoyalashni qo'llab quvatlaydi.

Ipsec protokollar to'plami ochiq standart sanalib, u quyidagi turli vazifalarni bajaruvchi quyidagi funksiyalardan iborat:

Sarlavha autentifikatsiyasi (Authentication Headers (AH)) funksiya vazifasi bog'lanish yaxlitligi, IP datagrammasi uchun ma'lumot autentifikatsiyasi va takrorlashga asoslangan hujumlarning oldini olishdan iborat. Umuman olganda IPsec ning ushbu vazifasi orqali faqat ma'lumot butunligi ta'minlanadi.

Xavfsizlik yuki inkapsulyatsiyasi (Encapsulating Security Payloads (ESP)) funksiyasi esa ma'lumotni konfidensialligini, ma'lumot butunligini va boshqa bir qator vazifalarni bajaradi.

Xavfsizlik to'plami (Security Associations (SA)) funksiyasi vazifasi yuqoridagi ikkita funksiyaga kerakli bo'lgan barcha kriptografik algoritmlar to'plamini o'zida saqlaydi. Internet Security Association and Key Management Protocol (ISAKMP) tizimi esa autentifikatsiyalash va kalit almashinish jarayoni amalga oshiradi.

Sarlavha autentifikatsiyasi (Authentication Headers (AH)). Ushbu funksiya vazifasi bog'lanish butunligini va IP paketi ma'lumotlari haqiqiyligini ta'minlashda foydalaniladi. Bundan tashqari u ma'lumotni qayta yuborish hujumiga qarshi himoyalashda foydalaniladi.

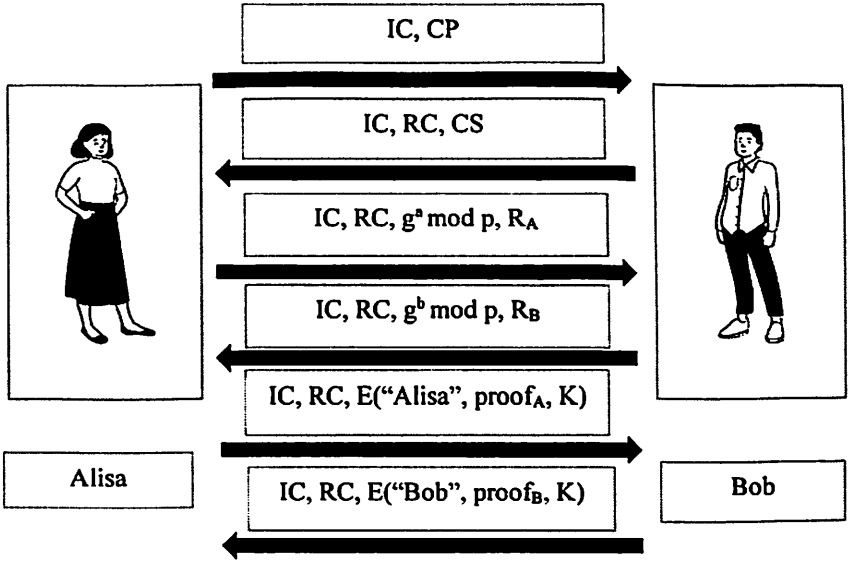
Xavfsizlik to'plami (Security Associations (SA)). IPsec ning ushbu vazifasi orqali dastlab ikki tomonlama autentifikatsiya va sessiya kalitlarini almashish amalga oshiriladi va shundan so'ng asosiy amallar bajariladi. Bu bosqichni amalga oshirishda quyidagi usullardan foydalaniladi:

- ochiq kalitli shifrlash (haqiqiy) asosida
  - o asosiy rejim
  - o agressiv rejim
- ochiq kalitli shifrlash (shakllantirilgan) asosida
  - o asosiy rejim
  - o agressiv rejim
- ochiq kalitli imzolash asosida
  - o asosiy rejim
  - o agressiv rejim

- simmetrik shifrlash asosida
  - o asosiy rejim
  - o agressiv rejim

Ushbu bosqichda ochiq kalitli shifrlash va ularga asoslangan imzolash algoritmlaridan foydalanishdan asosiy maqsad, kalitni maxfiy saqlanishidir. Bunda maxfiy kalit faqat bir tomonda maxfiy holatda saqlanadi. Sessiya kalitini hosil qilishda esa Diffi-Xelman kalitlarni ochiq taqsimlash algoritmidan foydalanadi.

Ochiq kalitli shifrlash algoritmlari asosida imzolashga asoslangan (asosiy rejim):

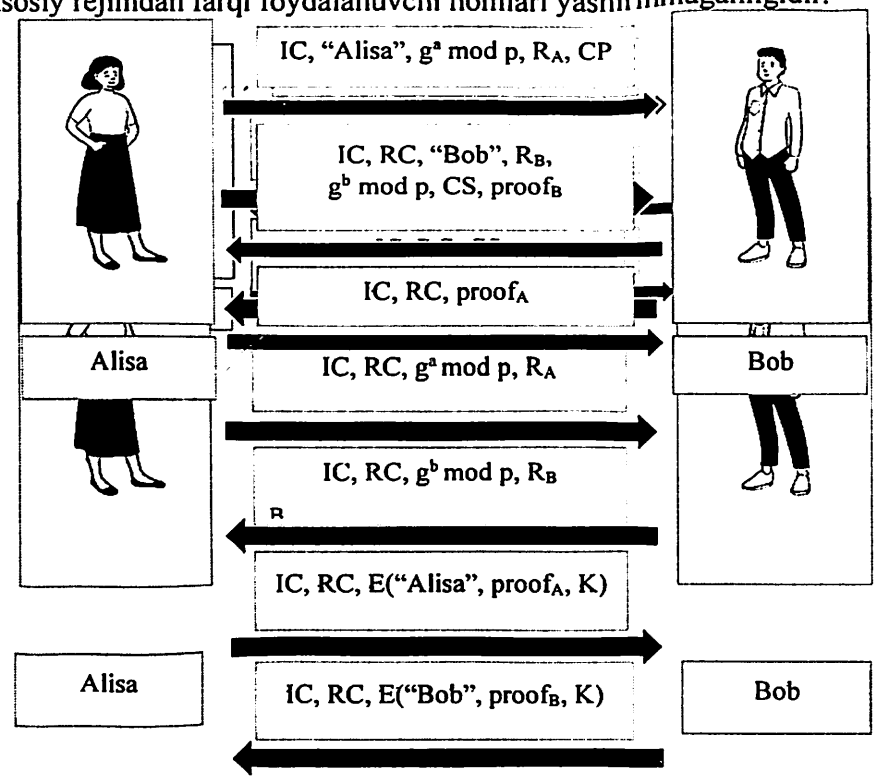


Bu yerda:

- CP = taklif etilgan kriptografik algoritmlar ro'yxati (crypto proposed), CS = tanlangan kriptografik algoritmlar ro'yxati (crypto selected).
- IC = initiator "cookie", RC = responder "cookie", Ushbu ikki parametr DDOS hujumni oldini olishda foydalaniladi.
- $K = h(IC,RC,g^{ab} \bmod p, R_A, R_B)$
- $SKEYID = h(R_A, R_B, g^{ab} \bmod p)$
- $proofA = [h(SKEYID, g^a \bmod p, g^b \bmod p, IC, RC, CP, \text{"Alisa"})]_{Alisa}$

Ochiq kalitli shifrlash algoritmlari asosida imzolashga asoslangan (agressiv rejim):

Asosiy rejimdan farqi foydalanuvchi nomlari yashirinmaganligidir.



Simmetrik kalitli shifrlash algoritmlari asosida imzolashga asoslangan (asosiy rejim):

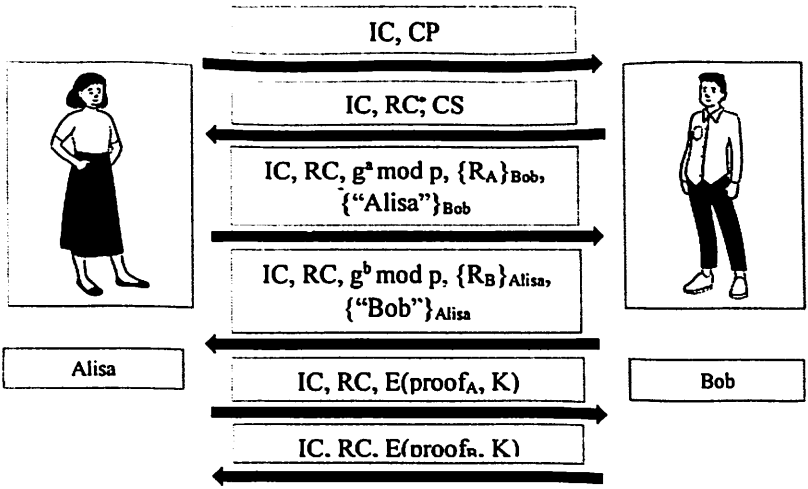
Bu yerda:

- K_{AB}= simmetrik almashingan kalit
- $K = h(IC,RC,g^{ab} \bmod p,R_A,R_B,K_{AB})$
- $SKEYID = h(K, g^{ab} \bmod p)$
- $proofA = h(SKEYID,g^a \bmod p,g^b \bmod p,IC,RC,CP,\text{"Alisa"})$

Ushbu protokolda Alisa o'zining ismini 5 chi xabarda jo'natmoqda. Alisaning identifikatori K kalit bilan shifrlanmoqda. Bob ushbu K kalitni topish uchun esa K_{AV} ni bilishi kerak. K_{AV} bilish uchun esa u Alisa bilan gaplashayotganini bilishi shart.

Simmetrik kalitli shifrlash algoritmlari asosida imzolashga asoslangan (agressiv rejim):

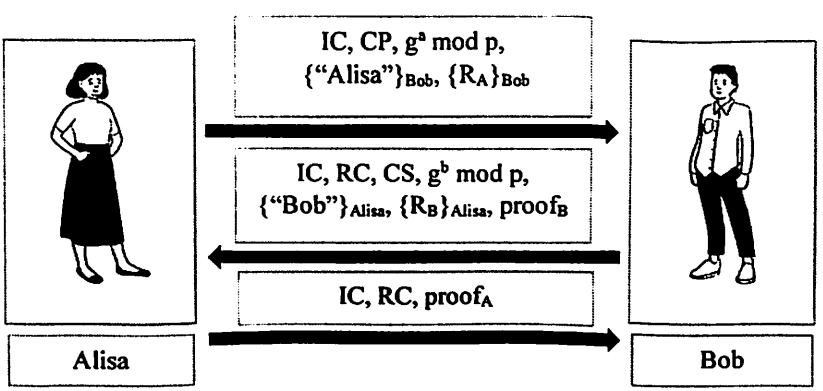
Ushbu protokolda ham foydalanuvchini nomini yashirish amalga oshirilmagan ammo asosiy rejimda uchraydigan muammo mavjud emas.



Ochiq kalitli shifrlash algoritmlariga asoslangan (asosiy rejim):

CP = crypto proposed, CS = crypto selected
IC = initiator "cookie", RC = responder "cookie"
K = h(IC,RC,g^{ab}mod p,R_A,R_B)
SKEYID = h(R_A, R_B, g^{ab}mod p)
proofA= h(SKEYID,g^amod p,g^bmod p,IC,RC,CP,"Alisa")

Ochiq kalitli shifrlash algoritmlari asosida imzolashga asoslangan (agressiv rejim):



Nazorat savollari

1. Kriptografik algoritmlarni amalga oshirish usullari haqida ayting?
2. Kriptografik protokol va unga qo'yilgan talablar?
3. Kriptografik protokol turlari?
4. Kriptografik dasturiy vositalar va ularning arxitekturasi?
5. Kriptografik apparat-dasturiy vositalarga misollar ayting?
6. Sodda autentifikatsiyalash protokollari va ularga misollar keltiring?
7. SSH protokoli va uning ishlash prinsipi?
8. CRC funksiyalar va ularning ishlash haqida ayting?
9. SSL/TLS protokoli va uning ishlash prinsipi?
10. X509 sertifikati va uning tuzilishi?
11. IPSec protokoli, uning ishlash prinsipi va foydalanilgan autentifikatsiya usullari?

VII. BULUTLI HISOBLASH TIZIMLARIDA KRIPTOGRAFIK ALGORITMLARDAN FOYDALANISH

7.1. Gomomorfik shifrlash usullari

Bulutli hisoblash ma'lumot, fayl saqlovchilar, ilovalar uchun dinamik infratuzilmani ta'minlash uchun lokal yoki global tarmoqqa ulangan ko'p sonli tizimlardan tashkil topgan. Bu texnologiya o'zi bilan birga, hisoblashda xarajatlarni kamaytirish, ilovalar hosti, ma'lumot saqlovchilar va ma'lumot uzatishda katta imkoniyatlarni olib keladi.

Bulutli hisoblash texnologiyasi quyidagi 3 ta katta turga ajratiladi:

Dasturiy ta'minot xizmati (Software-as-a-Service, SaaS): Ushbu modelda foydalanuvchiga tugallangan dasturiy ta'minot taklif etilib, bulut tizimida bitta xizmat asosida ko'plab foydalanuvchilarga xizmat ko'rsatiladi. Bulutli hisoblashning ushbu modelida foydalanuvchi kichik ilova – brauzer orqali tizimni boshqaradi. SaaS tizimi o'zida ko'plab ilovalarni qamrab olib, ular, ofis ilovalari, turli messenjerlar, to'lovni amalga oshiruvchi maxsus ilovalar, ma'lumotlarni boshqaruvchi tizim ilovalari, boshqaruvchi ilovalarni o'z ichiga oladi.

Platforma xizmati (Platform-as-a-Service, PaaS): PaaS xizmatida istemolchi IaaS xizmatidan foydalanib qurilgan tizim ustida, o'zining istagan dasturiy vositani yaratish imkoniniga ega bo'ladi. Ushbu imkoniyatlar dasturlarlash tillari, maxsus dasturlar yoki boshqa qo'shimcha ilovalar ko'rinishida bo'ladi. Qisqa qilib aytganda PaaS xizmati IaaS tizimida ixtiyoriy dasturlash tillaridan foydalangan holda yangi dasturlarni yaratish imkoniyatini beradi.

Infratuzulma xizmati (Infrastructure-as-a-Service, IaaS): Ma'lumotlar infratuzilmasi boshqa tizimlar, telefon tizimlari, yo'l tizimlari kabi samarali model tomon harakatlanyapti. Infratuzulma xizmati tashkilotlarni internet tarmog'i orqali ma'lumot saqlash tizimlari va hisoblash tizimlari bilan ta'minlab, istemolchi o'zi uchun kerakli infratuzulmani qurishda IaaS xizmati ta'minlagan, serverlar, ma'lumotlarni saqlash tizimlari, ma'lumot markazlari, tarmoq jihozlari va boshqalardan foydalanishi mumkin.

Bulutli hisoblash tizimlarida konfidensial ma'lumotlarni saqlash uchun maxsus shifrlash algoritmlaridan foydalanish talab etiladi.

Shifrlash algoritmlarining asosiy maqsadi ikki tomon o'rtasida himoyalanmagan kanal orqali maxfiy ma'lumotlarni hujumchidan himoyalangan holda jo'natish. Ishonchsiz uchinchi tomon sifatida

hujumchi shifrmatnni olishi va hozirgi kundagi hisoblash imkoniyatlaridan foydalangan holda uni ochishi mumkin. Axborot hajmining ortishi va ko'p sonli markazlashmagan axborot tizimlarining ko'payishi gomomorfik shifrlash algoritmlaridan foydalanishni taqozo etmoqda.

Bulutli axborotni saqlash tizimlarida axborot jo'natuvchi tomonidan shifrlanadi va serverga jo'natadi. Agar u ustida biror amal bajarilishi lozim bo'lsa, unda ushbu axborotni rasshifrovkalash lozim. Agar gomomorfik shifrlash algoritmlaridan foydalanilsa ularni rasshifrovkalash shart emas. Gomomorfik shifrlash axborotni bulutli tizimlarda saqlashda uning butunligi, konfidensiyalligi va foydalanuvchanligini ta'minlashda yangi sohalarni ochib beradi. Bulutli hisoblash tizimlarida qo'yilgan vazifani yechishda unga mos algoritmlar tahlillanadi. Shifrlangan ma'lumotlarni ko'paytirish uchun RSA yoki El-Gamal va qo'shish uchun Peye algoritmidan foydalanish maqsadga muvofiq. Agar to'liq gomomorfik shifrlashdan foydalanilsa, unda hisoblash parametrlar sonini chegaralash lozim. Ushbu holatda xatolar soni maxfiy parametrdan ortib ketsa, to'g'ri rasshifrovkalash amalga oshmasligi mumkin.

Ya'ni ikki shifrma'lumot ustida amalga oshirilgan gomomorfik amallar ochiq holdagi ushbu ma'lumotlar ustida bajarilgan natija bilan bir xil bo'ladi. Shuning uchun shirfma'lumot orqali uni ochmasdan ixtiyoriy jarayonlarni amalga oshirish mumkin. Gomomorfik shifrlash algoritmlari qisman va to'liq turlarga bo'linadi.

Qisman gomomorfik shifrlash algoritmlari amallardan birini bajarishi mumkin: qo'shish yoki ko'paytirish.

To'liq gomomorfik shifrlash algoritmlari gomomorfizm xususiyati asosida ikki amalni ham birga qo'llash imkoniyatiga ega.

Gomomorfik shifrlash. Ular ochiq va unga mos shifrmantlar ustida bir nechta algebraik amallarni bajarishni nazarda tutadi. Unda shifrlash funksiyasi quyidagicha amalga oshiriladi:

$$E(k,t)$$

Bu yerda, k – shifrlash kaliti, t – shifrlanishi lozim bo'lgan ochiq matn. E - gomomorfik shifrlash funksiyasi hisoblanib, t_1 va t_2 ochiq ma'lumotlar ustida M algoritmdan foydalaningan holda $c = M(E(k,t_1),E(k,t_2))$ hisoblanadi va uni deshirflash natijasida $t_1 * t_2$ ochiq ma'lumotga ega bo'lamiz.

Agar t_1 va t_2 ochiq ma'lumotlar ko'paytirish amali yordamida hisoblangan. Xuddi shunday $c = E(k,t_1) * E(k,t_2)$ shifrmatn ham

hisoblangan va u rasshifrovkalansa $t_1 * t_2$ natija olinadi. Ushbu holatda boshqa kalitdan foydalanilsa, undan chiqqan natija $t_1 * t_2$ ekanligini tekshirishning imkoniyati mavjud emas.

Ixtiyoriy shifrlash algoritmi kalit generatsiyasi, shifrlash va rasshifrovkalash qadamlaridan tashkil topgan. Ammo gomomorfik shifrlashda hisoblash qadami ham mavjud:

Kalit generatsiyasi. Shifrlash uchun yopiq va rasshifrovkalash uchun ochiq kalitlarni generatsiyalashni o'z ichiga oladi.

Shifrlash. Ochiq ma'lumot maxfiy kalit bilan shifrlanadi va shifrma'lumot ochiq kalit bilan birga serverga jo'natiladi.

Hisoblash. Serverda shifrmatn ustida F funksiya va ochiq kalit yordamida hisoblashlar amalga oshiriladi va natijani mijozga jo'natadi.

Rasshifrovkalash. Mijoz serverdan olgan qiymat asosida maxfiy kalit bilan shifrma'lumotni rasshifrovkalaydi.

Agar, E – shifrlash funksiyasi, D – rasshifrovkalash funksiyasi, t_1 va t_2 -ochiq ma'lumotlar "+" – qo'shish va "*" ko'paytirish amali bo'lsa, unda quyidagi hisoblash o'rinli:

Qo'shish gomomorfik xususiyati:

$$D(E(t_1) * E(t_2)) = t_1 * t_2$$

Ko'paytirish gomomorfik xususiyati:

$$D(E(t_1) + E(t_2)) = t_1 + t_2$$

Agar tizmi *to'liq* gomomorfik bo'lsa, ya'ni qo'shish va ko'paytirish birgalikda ishlatilsa quyidagicha amalga oshiriladi:

$$D(E(t_1) * E(t_2)) = t_1 * t_2,\ D(E(t_1) + E(t_2)) = t_1 + t_2$$

Qisman gomomorfik shifrlash usulini turli kriptografik algoritmlarga qo'llash.

RSA kriptotizimi. RSA ochiq kalitli kriptotizim sanaladi. Agar p – RSA ning moduli, t – ochiq ma'lumot, k – ochiq kalit, unda shifrlash funksiyasi quyidagicha bo'ladi:

$$E(t) = t^k \bmod p$$

Unda gomomorfik hisoblash (ko'paytirish) quyidagicha bo'ladi:

$$E(t_1) * E(t_2) = t_1^k * t_2^k \bmod p = (t_1 t_2)^k \bmod p = E(t_1 t_2)$$

El-Gamal kriptotizimi. Ushbu algoritm ham ochiq kalitli kriptotizim va diskret logarifm muammosiga asoslangan. Uning gomomorfik ko'rinishi ochiq ma'lumotlar ustida ko'paytirish amali asosida hisoblanadi. Agar:

$E(y, g, \{r_1\}, t_1) = (y^{r_1} t_1, g^{r_1})$ va $E(y, g, \{r_2\}, t_2) = (y^{r_2} t_2, g^{r_2})$ bo'lsa, unda, $E(y, g, \{r_1, r_2\}, t_1, t_2)$ quyidagicha ko'rinishda bo'ladi:

$$(y^{r_1}y^{r_2}t_1t_2, g^{r_1}g^{r_2})$$

Goldvasser-Mikali kriptotizimi. m modul bo'yicha E shifrlash funksiyasi b bit uchun $E(b) = x^b r^2 mod\ m$. Bu yerda, x – ochiq ma'lumot, r – tasodifiy son, $r \in \{0, \dots, m-1\}$. Unda gomomorfik shifrlash qo'shish amali orqali quyidagicha bo'ladi:

$$E(b_1) * E(b_2) = x^{b_1} r_1^2 x^{b_2} r_2^2 = x^{b_1+b_2}(r_1 r_2)^2 = E(b_1 \oplus b_2)$$

Bu yerda, $\oplus$ - *G(2)* asosida qo'shishni anglatadi.

Peye kriptotizimi. Agar ochiq kalit m moduli asosida va g – tasodifiy son bo'lsa, unda shifrlash funksiyasi quyidagicha hisoblanadi:

$$E(t) = g^t r^m\ mod\ m^2$$

Bu yerda, $r \in \{0, \dots, m-1\}$. Unda gomomorfik shifrlash qo'shish amali orqali quyidagicha bo'ladi:

$$E(t_1) * E(t_2) = (g^{t_1} r_1^m) * (g^{t_2} r_2^m)\ mod\ m^2$$
$$= g^{t_1+t_2}(r_1 r_2)^m\ mod\ m^2 = E(t_1 + t_2)$$

Benalo kriptotizimi. Agar ochiq kalit m moduli asosida bo'lsa, unda shifrlash funksiyasi quyidagicha bo'ladi:

$$E(t) = g^t r^c\ mod\ m$$

Bu yerda, $r \in \{0, \dots, m-1\}$. Unda gomomorfik shifrlash qo'shish amali orqali quyidagicha bo'ladi:

$$E(t_1) * E(t_2) = (g^{t_1} r_1^c) * (g^{t_2} r_2^c)\ mod\ m = g^{t_1+t_2}(r_1 r_2)^c\ mod\ m$$
$$= E(t_1 + t_2)$$

Gomomorfik shifrlash algoritmlari bulutli hisoblash tizimlaridan tashqari quyidagi sohalarda qo'llash mumkin:

Elektron ovoz berish. U gomomorfik shifrlash qo'llanilgan ilg'or sohalardan sanaladi. Ovoz beruvchilarning ovozi shifrlanadi va shifr ma'lumotlar ustida amallar bajariladi. Benalo ovoz berish tizimi quyidagi bosqichlardan tashkil topgan:

1. Har bir ovoz beruvchi ishtirokchi o'zining ovozini gomomorfik xususiyatlar asosida maxfiy taqsimlash sxemasi asosida ajratadi va tanlangan nomzodga yo'naltiradi.

2. Nomzodlar ovozni qabul qiladi: qabul qilingan ovozlarning yig'indisi qisman maxfiy hisoblanadi.

Asosiy ishonchli odam ishtirokchilar jo'natgan ovozlar asosida to'plangan qisman maxfiy yig'indi asosida ovozlarning natijasini hisoblaydi.

7.2. Attributga asoslangan shifrlash

Attributga asoslangan shifrlash ochiq kalitli kriptotizimning bir ko'rinishi hisoblanib, rasshifrovkalashda qo'llaniladigan yopiq kalit qo'shimcha ma'lumotlarga (lavozim, yashash joyi, qayd yozuvi turi) bog'liq. Uning sxemasi 2005 yilda Sahai va Waters tomonidan taklif etilgan. Ushbu sxemada ma'lumot jo'natuvchi, qabul qiluvchi va uchinchi ishonchli tomon ishtirok etadi.

Kalitlar o'rnatilgan atributlar to'plami asosida hosil qilinadi. Agar tizimga foydalanuvchi yangi atribut bilan qo'shilsa, atribut to'plamga kiritiladi hamda ochiq va yopiq kalitlar qaytadan hosil qilinadi. Xabar jo'natuvchi ma'lumotni ochiq kalit va bir nechta atributlar yordamida shifrlaydi. Qabul qiluvchi ishonchli uchinchi tomondan olgan yopiq kaliti asosida shifrlangan ma'lumotni rasshifrovkalaydi. Bunda, qabul qiluvchidagi atributlar soni d o'rnatilgan talabni bajarishi lozim. Masalan, ma'lumotni shifrlash atributlari quyidagicha: {"Kriptologiya kafedrasi", "O'qituvchi", "Talaba"} va $d = 2$. Ma'lumotni rasshifrovkalash uchun uchtadan ikkita atribut mavjud bo'lishi lozim, demak talab bajarildi.

Ruxsatlar tuzilishi:

$\{P_1, P_2, \dots, P_n\}$ – atributlar to'plami. $\mathbb{A} \subseteq 2^{\{P_1, P_2, \dots, P_n\}}$ monoton deb nomlanadi, agar $\forall B, C: B \in \mathbb{A}, B \subseteq C \rightarrow C \in \mathbb{A}$ qanoatlantirilsa.

Ruxsatlar tuzilmasi bo'sh bo'lmagan $\mathbb{A}$ $\{P_1, P_2, \dots, P_n\}$ to'plam ositini o'z ichiga oladi. $\mathbb{A}$ – avtorizasiyalangan va avtorizasiyalanmagan atributlar to'plamini o'z ichiga oladi. Shifrlash sxemasini boshlashda monoton ruxsatlar tuzilmasidan foydalaniladi. 2007 yilda monoton bo'lmagan tuzilma samarasiz ekanligi isbotlangan.

Algoritm ishlashi quyidagicha:

G_1 va G_2 – ikki argumentli guruh, p – to'plam va g - G_1 guruhining generatori.

$e: G_1 \times G_2 \rightarrow G_2$ - ikki argumentli guruhning tasvirlanishi.

d – chegaraviy qiymat.

Algoritm to'rt asosiy qadamdan tashkil topgan.

Ochiq va universal kalitlarni hosil qilish:

Uchinchi ishonchli tomon tasodifiy holda $t_1, t_2, \dots, t_n$ va Z_q chekli maydondan y ni tanlaydi hamda quyidagi formula asosida ochiq kalitni hisoblaydi.

$$PK = (T_1 = g^{t_1}, \dots, T_n = g^{t_n}, Y = e(g,g)^y).$$

Bu yerda, g – bir nechta p (tub son) tartibli ikki argumentli G_1 guruhini hosil qilish. Shuningdek ushbu bosqichda $MK = (t_1, t_2, ..., t_n)$ universal kaliti hosil qilinadi.

Yopiq kalitni hosil qilish:

Ishonchli tomon har bir U foydalanuvchi uchun yopiq kalit generatsiya qiladi. A_U – foydalanuvchining atributlar to'plami. Tasodifiy holatda darajasi $d-1$ bo'lgan q ko'phad tanlanadi va $q(0) = y$ bajariladi. Undu uning yopiq kaliti quyidagicha hisoblanadi:

$$D = \{D_i = g^{\frac{q(i)}{t_i}}\} \forall i \in A_U.$$

Shifrlash:

Ma'lumot egasi $M \in G_2$ xabarni $A_C T$ atributlar to'plami va $s \in Z_q$ tasodifiy tanlangan son orqali shifrlaydi.

$CT = (A_{CT}, E = MY^s = e(g,g)^{ys}, \{E_i = g^{t_i s}\} \forall i \in A_U)$.

Rasshifrovkalash:

Agar $i \in A_U \cap A_C T$ dan $|A_U \cap A_C T| \geq d$ shart bajarilsa, quyidagi tenglikni bajarish uchun d tasodifiy atribut tanlanadi.

$$e(E_i, D_i) = e(g,g)^{q(i)s}$$

$$Y^s = e(g,g)^{q(0)s} = e(g,g)ys$$

$$M = \frac{E}{Y^s}$$

Natijada, rasshifrovkalangan M xabarga ega bo'linadi.

Ushbu sxemada yopiq kalitlar sirni bo'lishish mexanizmi asosida generatsiyalanadi. Sirning bir qismi foydalanuvchining yopiq kaliti D_i komponentasiga biriktiriladi. Yopiq kalit tasodifiy $q(i)$ ko'phadga mos keladi. Natijada, foydalanuvchilarning so'zlashuvini kuzatish asosida bir nechta yopiq kalitlarni barlashtirish asosida yangi yopiq kalitni aniqlash imkoniyati mavjud emas.

Qidirish (Predicate) imkoniyatiga ega shifrlash. Shifrma'lumot va yopiq kalit o'rtasidagi funksional bog'liqlikka asoslangan. Yopiq kalit F bashorat qilish funksiyasiga bog'liq va u $F(I) = 1$ bo'lgan holatda I atribut bilan bog'liq ma'lumotni rasshifrovkalashda qo'llanilishi mumkin.

An'anaviy asimmetrik shifrlash tizimlarida rasshifrovkalashni amalga oshiruvchi tomon ochiq va yopiq kalitlarni generatsiyalaydi. Ochiq kalitni ma'lumotni shifrlab jo'natuvchi tomonga (yoki tomonlarga) taqdim etadi. Natijada, jo'natuvchi ma'lumotni ochiq kalit bilan shifrlaydi va qabul qiluvchiga yuboradi. Qabul qiluvchi o'zida mavjud ochiq kalitning yopiq sherigi bilan rasshifrovkalaydi. Shuningdek, ushbu ochiq kalit bilan kirib kelgan boshqa shifrlangan ma'lumotlarni ham

rasshifrovkalay oladi. Lekin, ma'lumotni shifrlash imkoniyatini chekli sondagi foydalanuvchilarga taqdim etish yangi usullardan foydalanishni talab etadi. Bashorat qilishga asoslangan shifrlash algoritmlaridan ushbu masalani hal etishda foydalanish mumkin.

Bashoratga asoslangan shifrlash sxemasi to'rt asosiy bosqichdan tashkil topgan:

1. Mos holda ochiq va yopiq kalitlarni generatsiyalash: PK va SK.

2. F bashorat fuknsiyasi asosida yopiq kalitni generatsiyalash: $GenKey(SK, F) = S_K$.

3. M xabarni PK ochiq kaliti va I atribut yordamida shifrlanadi: $E_{PK}(I, M) = C$.

4. F bashorat funksiyasi va I atribut o'rtasidagi aloqa mavjudligi aniqlanganda C xabarni rasshifrovkalab M xabarga ega bo'lish mumkin:

$$F(I) = 1, D_{SK_f}(C) = M.$$

$$F(I) = 0, D_{SK_f}(C) = \emptyset.$$

Ushbu sxemada shifrlangan ma'lumot $\bar{x}$ vektor va yopiq kalit esa, $\bar{v}$ vektor bilan bog'langan. Rasshifrovkalash jarayonida vektorlarning skalyar ko'paytmasi $\bar{x} \cdot \bar{v} = 0 \, mod \, N$ shartni qanoatlantirishi lozim. Ushbu tenglikni tekshirish jarayonida foydalanuvchi $\bar{x}$ vektor haqida hech qanday axborot olmasligi lozim. Buning uchun N tartibli ikki argumentli guruh qo'llaniladi. N uchta tub sonning ko'paytmasidan hosil qilinadi. Quyida ushbu sxema haqida batafsil keltiriladi:

Ochiq va yopiq kalitlarni generatsiyalash:

1. p, q, r tub sonlar tanlanadi va G guruh hisoblanadi: $G = G_p \times G_q \times G_r$.

2. Ikki argumentli guruh tanlanadi: $\hat{e}: G \times G \to G_t$.

3. Tasodifiy son tanlanadi: $R_{1,i}, R_{2,i} \in G_r, h_{1,i}, h_{2,i} \in G_p, i = \overline{1,n}, R_0 \in G_r$.

4. Ochiq kalit ma'lumotlar to'plamidan tashkil topgan:

$PK = (N, G, G_t, \hat{e}, g_p, g_q, Q = g_q \cdot R_0, H_{1,i} = h_{1,i} \cdot R_{1,i}, H_{2,i} = h_{2,i} \cdot R_{2,i}, j = \overline{1,n})$.

5. Yopiq kalit: $SK = (p, q, r, g_q, h_{1,i}, h_{2,i}, j = \overline{1,n})$.

Bog'liq yopiq kalitni generatsiyalash:

1. Bashorat n o'lchamli $\bar{v}$ vektor ko'rinishida ifodalanadi.

2. Tasodifiy sonlar tanlanadi:

$$r_{1,i}, r_{2,i}, \in Z_p, i = \overline{1,n}, R_5 \in G_r, f_1, f_2 \in Z_q, Q_6 \in G_q.$$

3. Bog'liq yopiq kalit quyidagicha bo'ldai:

$SK_{\bar{v}} = (K = R_5 * Q_6 * \prod_{i=1}^{n} h_{1,i}^{-r_{1,i}} \cdot h_{2,i}^{-r_{2,i}}, K_{1,i} = g_p^{r_{1,i}} \cdot g_q^{f_{1,v_i}}, K_{2,i} = g_p^{r_{2,i}} \cdot g_q^{f_{2,v_i}})$.

Shifrlash:

1. $\vec{x} = (x_1, \dots, x_n), x_i \in Z_N$.
2. Tasodifiy sonlar tanlanadi: $s, \alpha, \beta \in Z_N, R_{3,i}, R_{4,i} \in G_r$.
3. Shifrma'lumot:

$$C = (C_0 = g_p^s, C_{1,i} = H_{1,i}^s \cdot Q^{\alpha x_i} \cdot R_{3,i}, C_{2,i} = H_{2,i}^s \cdot Q^{\beta x_i} \cdot R_{4,i})$$

Rasshifrovkalash:

Ushbu holatda rasshifrovkalash natijasi sifatida 1 olinadi:

$$\hat{e}(C_0, K) \cdot \prod_{i=1}^{n} \hat{e}(C_{1,i}, K_{1,i}) \cdot \hat{e}(C_{1,i}, K_{1,i}) = 1$$

7.3. Qidirish imkoniyatli shifrlash

Axborotni himoyalangan holda qidirish. Gomomorfik shifrlash qidiruv tizimlaridan olingan ma'lumotning konfidensialligini ta'minlagan holda ajratib berish imkoniyatini beradi. Xizmat so'rovni qabul qiladi, qayta ishlaydi va natijani so'rovning ichini tushunmasdan qaytaradi. Uyida ma'lumotlar bazasidan axborotni uning indeksi orqali ajratib olish misoli keltirilgan.

Masalan, $v_1, v_2, \dots, v_n$ - yozuvlar indeksi. $v_i \in \{0,1\}$, $c_1, c_2, \dots, c_i, \dots, c_{2^n}$ – ma'lumotlar bazasidagi indeksga ega yozuvlar.

Talab etilgan yozuvni tanlash uchun F funksiyani hisoblash lozim:

$$F = (v_1, v_2, \dots, v_n; c_1, c_2, \dots, c_i, \dots, c_{2^n}) =$$
$$= c_1\big((v_1 \oplus 1) \otimes (v_2 \oplus 1) \otimes \dots \otimes (v_n \oplus 1)\big) +$$
$$+ c_2\big((v_1 \oplus 1) \otimes (v_2 \oplus 1) \otimes \dots \otimes (v_n \oplus 1)\big) +$$
$$+ c_3\big((v_1 \oplus 1) \otimes (v_2 \oplus 1) \otimes \dots \otimes (v_n \oplus 1)\big) +$$
$$+ \dots +$$
$$+ c_{2^n}(v_1 \otimes v_2 \otimes \dots \otimes v_n)$$

Agar barcha c_i gomomorfik shifrlash yordamida shifrlangan bo'lsa, F shifrma'lumotlar asosida gomomorfik hisoblanishi mumkin. Buning uchun, mijoz $v_1, v_2, \dots, v_n$ indeksni bit bo'yisa shifrlashi va serverga jo'natishi lozim. Bu yerda, gomomorfik shifrlash usulining ham qo'shish, ham ko'paytirish xususiyati birgalikda amalga oshiriladi.

Simsiz markazlashmagan aloqa tarmog'ini himoyalash. Bunga MANET tarmog'i misol bo'lishi mumkin va u mobil qurilmalardan tashkil topgan. Har bir qurilma ixtiyoriy holda xohlagan yo'nalishda

harakatlanishi mumkin va ixtiyoriy holatda qo'shni qurilma bilan aloqa o'rnata oladi. Uning asosiy muammosi aloqa xavfsizligini ta'minlash. Ushbu holatda gomomorfik shifrlashdan foydalanilishi mumkin. Ushbu holatda kanallar o'rtasidagi amallar shifrma'lumotlar ustida bajariladi. Kanallar o'rtasida samarali yo'lni aniqlash uchun chiziqli amallardan foydalanish lozim. Mavjud gomomorfik shifrlash algoritmlari shifrma'lumotlar ustidagi amallarni hujumchi egallashiga yo'l qo'ymaydi. Shuning uchun trafikni tahlil qilish asosida xabar yo'nalishini aniqlashnig imkoniyati mavjud emas.

Smart kartalar uchun autsorsing xizmatlari. Hozirgi kunda o'zining ichida operatsion tizim mavjud universal kartalar keng tarqalmoqda. Ular yordamida bir nechta xizmatlardan foydalanish mumkin. Ko'pchilik ilovalarda hisoblashlar kartada emas, gomomorfik amalga oshiriladi. Masalan xizmat provayderlari yoki biometrik tekshiruvlar katta trafikni talab etadi. Shuning uchun ushbu ma'lumotlarni gomomorfik shifrlash algoritmlaridan foydalangan holda, tashqi qurilmalarda saqlash maqsadga muvofiq.

Qayta aloqa tizimlari. Foydalanuvchilarning anomalligi va oraliq hisoblash natijalarini berkitish maqsadida gomomorfik shifrlash algoritmlaridan foydalaniladi. Tizim o'qituvchining faoliyati haqida talabalardan anonim so'rov o'tkazishi mumkin. So'rov shirflangan holda saqlanadi va ixtiyoriy qayta aloqa uchun anonim holatda foydalanilishi mumkin.

Dasturiy mahsulotlarni himoyalash uchun uni murakkablashtirish. Uning asosiy maqsadi dastur kodi yoki uning arxitekturasini tushinib bo'lmaydigan holatga o'tkazish. An'anaviy kompyuter arxitekturasi ikkilik qatorlardan tashkil topgan va gomomorfik shifrlash usullarini qo'llash asosida uning ichki strukturasi to'liq berkitilishiga erishiladi.

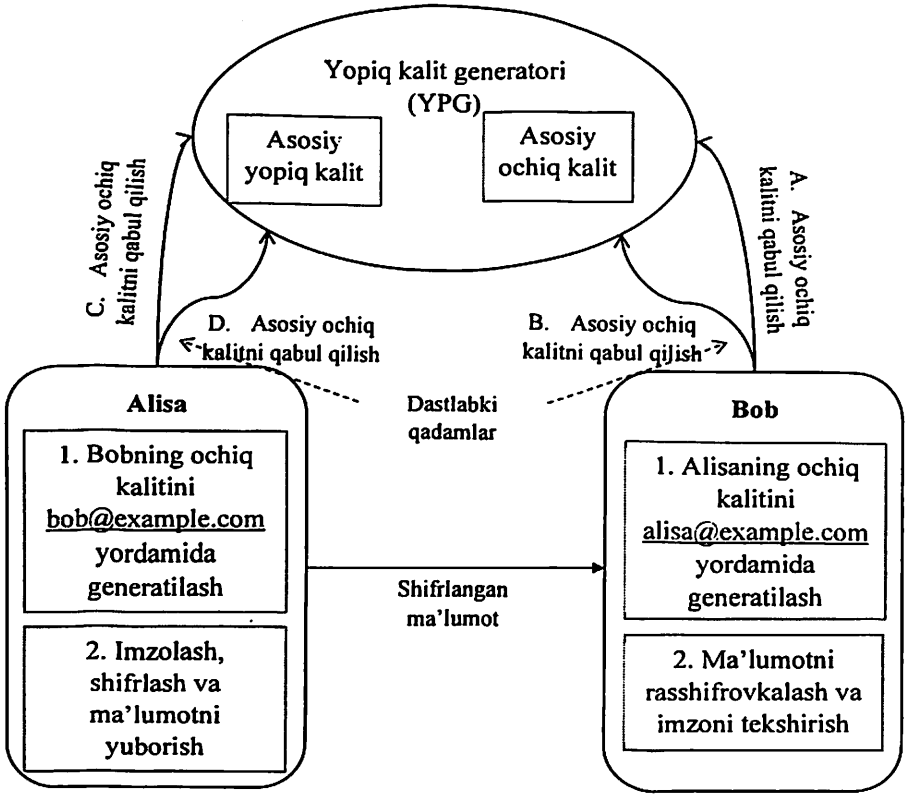
Bundan tashqari reklama sohasida iste'molchilarni himoyalashda, tibbiyot ilovalarida, moliyaviy hisobotlarda, kriminalistik rasmlarni tanib olishda qo'llaniladi.

7.4. Identifikatorga asoslangan shifrlash

Asimmetrik kriptotizim bo'lib, ochiq kalit foydalanuvchi nomiga bog'liq bir nechta unikal ma'lumotlar asosida generatsiyalanadi. Ushbu ma'lumotlar sifatida foydalanuvchi nomi, elektron manzil, telefon raqami va boshqa shu kabilarni kiritish mumkin. 1984 yilda Adi Shamir tomonidar identifikatorga asoslangan imzo va elektron pochtaga asoslangan ochiq kalitlar infratuzilmasini ishlab chiqqan lekin ommaga

umumiy sxemani ma'lum qilmagan. Uning birinchi amaliy qo'llanilishi 2001 yilda amalga oshirilgan.

Ixtiyoriy tomonda foydalanuvchining biror identifikatori asosida kalitlarni generatsiyalash va kalitlarni almashmasdan xabarlarni xavfsiz almashish hamda imzoni tekshirishga asoslangan. Kalitlarni generatsiyalash va taqsimlash markazlari har bir foydalanuvchi uchun smart karta taqdim etadi. Karta mikroprosessor, kirish va chiqish porti, tezkor va doimiy xotira hamda shifrlash, rasshifrovkalash, imzolash va imzoni tekshirish dasturlarini o'z ichiga oladi. U ma'lum foydalanuvchilar doirasida, tashkilot hodimlari o'rtasida foydalanilishi mumkin.



6.21-rasm. Identifikatorga asoslangan shifrlash algoritmining sxemasi

6.21-rasmda identifikatorga asoslangan shifrlash algoritmining sxemasi keltirilgan. A tomon smart kartadan foydalangan holda xabarni imzolaydi va barcha ma'lumotlarni qabul qiluvchining identifikatori

asosida shifrlaydi va B tomonga yuboradi. Qabul qiluvchi smart karta yordamida yopiq kalitdan foydalanib xabarni rasshifrovkalaydi va jo'natuvchining identifikatori asosida imzoni tekshiradi. Xavfsizlikni ta'minlash maqsadida yopiq kalitlar kalitlarni taqsimlash markazlarida generatsiyalanishi lozim.

Ushbu kriptotizimning bardoshliligi quyidagilarga bog'liq:

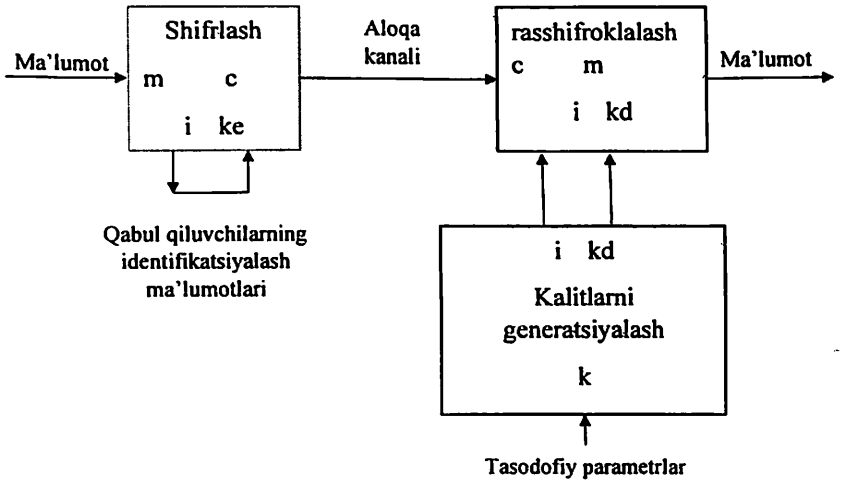
– asosiy kriptografik funksiyalarning bardoshliligiga;

– uchinchi tomonda saqlanadigan axborotlar (kalit)ning ishonchliligiga;

– yangi foydalanuvchilarga smart karta taqdim etishdan oldin uni diqqat bilan tekshirish;

– smart kartani o'g'irlatish, yo'qotish, ko'paytirish va ruxsatsiz foydalanishdan himoyalash lozim.

6.22-rasmda identifikatorga asoslangan shifrlash algoritmining sxemasi keltirilgan bo'lib, unda k_e – shifrlash kaliti, k_d – rasshifroklalash kaliti va i – identifikatsion ma'lumot. Agar $k_e = i$ bo'lsa, rasshifroklalash kaliti i va tasodifiy k soni asosida $k_d = f(i,k)$ hisoblanadi.



6.22-rasm. Identifikatorga asoslangan shifrlash algoritmida kalitlardan foydalanish

Identifikatorga asoslangan shifrlash algoritmi asosida imzolash quyidagicha amalga oshiriladi:

$$s^e = i * t^{f(t,m)} \ (mod\ n).$$

Bu yerda, m – xabar, (s,t) – imzo, i – foydalanuvchining identifikatsion ma'lumoti, n – ikkita katta tub sonning ko'paytmasi (RSA kabi), e - $\varphi(n)$ bilan o'zaro tub bo'lgan katta tub son.

n, e parametrlari va f funksiya uchinchi ishonchli tomonda tanlanadi va ikki tomon uchun ham bir xil. f funksiyasining algoritmik tavsifi o'zining shaxsiy smart kartasida amalga oshiriladi. n sonining tub ko'paytuvchilari ochiq kalitlarni generatsiyalash serverida saqlanadi. Foydalanuvchilar bir-biridan i – foydalanuvchining identifikatsion ma'lumoti asosida farqlanadi. i soniga mos keluvchi yagona g yopiq kalit $g^e = i\ (mod\ n)$ tenglikni qanoatlantiradi. Ushbu kalit serverda oson hisoblanadi, ammo e kalitni hech kim hisoblashi mumkin emas.

Har bir m xabar ko'p sonli (s,t) imzo juftligiga ega, shuning uchun, (s,t) juftligini tasodifiy tanlash samarasiz. Har bir juftlik uchun $s^e = i * t^{f(t,m)}\ (mod\ n)$ tenglikni hisoblash talab etiladi. Bu esa, hisoblash uchun ko'p vaqt talab etadi.

Foydalanuvchi m xabarni imzolashi uchun tasodifiy r sonini tanlaydi va $t = r^e (mod\ n)$ ni hisoblaydi va imzo formulasini quyidagicha yozish mumkin:

$$s^e = g^e * r^{ef(t,m)}\ (mod\ n).$$

Natijada e soni ishtirokisiz quyidagiga ega bo'lish mumkin:

$$s = s * r^{f(t,m)}\ (mod\ n).$$

Hozirgi kunda elliptik egri chiziqlarga va ikki argumentli juftliklarga asoslangan ko'rinishlari mavjud. Amaliyotda quyidagi sxemalar keng qo'llaniladi:

– Boneh–Franklin sxemasi (BF-IBE);

– Sakai–Kasahara sxemasi (SK-IBE);

– Boneh-Boyen sxemasi (BB-IBE).

Ushbu sxemaning afzalligi ochiq kalitlar foydalanuvchining identifikatori asosida generatsiyalanadi va seans boshlangandan keyin identifikatorni o'zgartira olmaydi. Ochiq kalitlarning xavfsizligi ta'minlansa, yopiq kalit ham xavfsiz sanaladi.

Muhokama: Bulutli hisoblash tizimlarida ma'lumotlar xavfsizligini ta'minlashda qo'llanniladigan algoritmlar tezligi yuqori va xavfsizligi kafolatlangan bo'lishi talab etiladi. Tizimda to'liq gomomorfik shifrlashlarni qo'llash natijasida tizimning unumdorligi pasayadi. Hozirgi kunda unumdorlikni oshirishning ikki yo'li mavjud:

– cheklangan gomomorfik amallardan foydalanish;

– "Shifrma'lumotni qadoqlash usuli" dan foydalanish.

Birinchi usulda qo'shish yoki ko'paytirish amallarining faqat bittasidan foydalanish nazarda tutilgan. Ikkinchi holatda esa, bir marta qo'llanilgan hisoblash keyingi o'rinlarda faqat takrorlanishi lozim.

Nazorat savollari

1. Bulutli hisoblash tizimlari va ularda mavjud xizmat modellari?
2. Gomomorfik shifrlash va uning mohiyati?
3. Attributga asoslangan shifrlash nima va uning ishlash prinsipi haqida ayting?
4. Qidirishga imkoniyatiga ega shifrlash nima?

VIII. KVANT KRIPTOGRAFIYASI ASOSLARI

8.1. Kvant nazariyasi

Ma'lumotni shifrlashning simmertik va asimmetrik algoritmlarining bir nechta afzallik va kamchilik jihatlari mavjud. Birgina RSA asimmetrik shifrlash algoritmida katta sonlarning faktorlash muammosi mavjud. Ushbu muammoni tezkorlik bilan hal etishga qaratilgan algoritm mavjud emas. 1994-yilda ushbu muammoni kvant kompyuterlarida yechish Sho tomonidan taklif etilgan. "Kvant parallellashtirish" usuli asosida mavjud usullarga nisbatan tez ishlashi isbotlab berilgan. Shuningdek, kvant kompyuterlarining amaliyotga joriy etilishi RSA kabi shifrlash algoritmlarining xavfsizligiga ham jiddiy ziyon keltiradi.

Yaqin vaqtlargacha kvant kriptografiyasi nazariy asoslangan va amaliy jihatdan esa, savdo maqsadlarida va uzoq masofalarga axborotlarni yetkazishda optik to'lqinlardan foydalanilgan. 1989-yilda birinchi marta laboratoriya sharoitida kvant kalitlarni almashish testdan o'tkaziladi. Kalitlarni almashishda optik to'lqinli muhitdan foydanilgan. 1995 yilda esa optik to'lqinlardan foydalangan holda 1,1 kmdan 23 kmgacha oraliqqa suv ostida kalitlarni almashish amalga oshirildi. NIST o'z tadqiqotlarida ushbu masofani 184 kmgacha uzaytirgan.

CeBIT-2002 birinchi kvant kritogarfiyasiga asoslangan savdo maqsadida ishlab chiqilgan kalitlarni almashish tizimi hisoblanadi va uning yordamida 27,9 - 117,6 kbit/s tezlik bilan 67 km masofaga kalitni almashishga erishilgan.

Id Quantique tomonidan ishlab chiqilgan Vectis tizmi AES shifrlash algoritmi uchun 128, 192 va 256 bitli kalitlarni generatsiya qilib VPN tunel orqali 100 km masofagacha 100 Gs chastotada almashishini ta'minlagan.

Kvant fizikasi klassik usullardan kvant zarrasi va uning holati asosida ifodalanadi. Kvant holati haqidagi ma'lumot aniq koordinatia o'lchami, og'irligi va maydonning qaysi qismida joylashgaligiga qarab farqlanadi. Uning xususiyatlaridagi kamchilik hisoblash murakkabliklarini keltirib chiqarishi mumkin. Kvant nazariyasiga o'tishdan oldin yorug'likning to'g'ri chiziqli tarqalish qonuni keltirish lozim. Unga ko'ra, optikaviy bir jinsli muhitda yorug'lik nuri to'g'ri chiziqli tarqaladi, chunki nuqtaviy yorug'lik manbai bilan shaffof bo'lmagan buyumlar yoritilganda, buyumlar shaklida aniq soya hosil bo'ladi. Yorug'lik nurlari to'lqin uzunligiga yaqin bo'lgan o'lchamli buyumlar yoritilganda bu qonundan chetlashish kuzatiladi.

Yorug'lik nuri tabiati to'g'risidagi birinchi tasavvurlar qadimgi greklar va misrliklarda paydo bo'lgan. XVII asr oxiriga kelib yorug'likning ikkita nazariyasi I.Nyuton tomonidan korpuskulyar nazariya va R.Guk va X.Gyuygens tomonidan to'lqin nazariyasi shakllana boshladi.

Gyuygens prinsipiga asosan, to'lqin yetib borgan har bir nuqta ikkilamchi to'lqinlar manbaiga aylanadi, manbani o'rab oluvchi egri chiziq keyingi momentdagi to'lqin fronti holatini belgilaydi. Gyuygens prinsipiga asoslanib yorug'likning qaytish va sinish qonunlarini osonlikcha isbotlash mumkin.

Kvant mexanikasi, asosan Plank gipotezasi, Shredinger, Geyzenberg, Dirak va Eynshteynlarning ilmiy ishlariga asoslangandir.

M. Plank tomonidan taklif etilgan gipotezaga asosan, yorug'likning nurlanishi va yutilishi uzluksiz bo'lmay, diskret xususiyatga ega, ya'ni aniq kvantlardan iboratdir. Bu kvant energiyasi quyidagicha ifodalanadi:

$$\varepsilon_0 = h\nu.$$

Bu yerda, h – Plank doimiysi. Plank gipotezasi qora jismning issiqlik nurlanishini ham oson tushuntira oldi.

1905 yilda A.Eynshteyn yorug'likning kvant nazariyasini kashf etdi. Bu nazariyaga asosan, yorug'lik nurlanishi va tarqalishi fotonlar – yorug'lik kvantlari oqimi ko'rinishida sodir bo'ladi.

De Broyl to'lqinlarini va Geyzenberg noaniqlik munosabatlarini izohlash quyidagi fikrga olib keldi:

- kvant mexanikasida mikrozarrachalarning har xil kuch maydonlaridagi harakatini ta'riflovchi harakat tenglamasi zarrachalarning to'lqin xususiyatini yoritib berishi zarur bo'ladi.

Asosiy tenglama $\psi(x,y,z,t)$ to'lqin funksiyasiga nisbatan va elektromagnit to'lqinlarni xarakterlovchi to'lqin tenglamasiga o'xshash bo'lishi kerak. Bunday tenglama *Shredingerning* umumiy tenglamasi deb ataladi va quyidagi ko'rinishga ega bo'ladi:

$$-\frac{\hbar}{2m}\Delta\psi + U(x,y,z,t)\psi = i\hbar\frac{\partial\psi}{\partial t}.$$

Bu yerda, $\hbar = \frac{h}{2\pi}$, m – zarracha massasi, Δ – Laplas operatori, $\Delta\psi = \frac{\partial^2\psi}{\partial x^2} + \frac{\partial^2\psi}{\partial y^2} + \frac{\partial^2\psi}{\partial z^2}$, i – mavhum birlik, $U(x,y,z,t)$ – kuch maydonidagi zarrachaning potensial funksiyasi, $\psi(x,y,z,t)$ – zarrachaning to'lqin funksiyasi.

8.2. Kvant kriptografiyasining asoslari

Kvant kalitlarni almashishning ikkita asosiy yo'nalishi farqlanadi:

Birinchi yo'nalish. Ikkita nomutanosib kvantning farqlash mumkin emaslik tamoyili. Ixtiyoriy ikki darajali kvant-mehanik tizimini chiziqli superpozisiya ko'rinishida tasvirlash mumkin.

$$|\psi\succ=\alpha|0\succ+\beta|0\succ$$

Bu yerda, uning xususiya holati $|0\succ$ va $|0\succ$. α va β koeffisentlar.

$$|\alpha|^2+|\beta|^2=1$$

Uning xavfsizligi nomalum kvant holatining ko'paytirishning imkoniyati mavjud emaslik nazariyasi bilan isbotlanadi. Ya'ni, kvant mehanikasining yagonalik va chiziqli xususiyatlari borki, kiruvchi holatga aniqlik kiritilmasdan uning aniq nus'xasini yaratish imkonsiz. Unga BB84 protokolini misol keltirish mumkin.

Ikkinchi yo'nalish kvant xususiyatlarini aralashtirishga asoslangan. Ikkita kvant-mexanik tizim korrelyatsiya holatida joylashadi va birinchi tizimda berilgan so'rov natijasi ikkinchisida hosil bo'ladi. Ushbu aralash holatdan hech biri bitta holatda turmaydi. Uni quyidagicha ifodalash mumkin:

$$|\psi_0\succ=\frac{|01\succ-|10\succ}{\sqrt{2}}$$

Ko'rilgan ikki holatdan birida $|01\succ$ yoki $|10\succ$ natijasi qaytariladi. Boshqa tizimostilarida teskari holatda, ya'ni, $|1\succ$ bo'lsa, $|0\succ$ qabul qilinadi va aksincha. Unga misol sifatida EPR(E91) protokolini keltirish mumkin.

Kvant nazariyasiga asoslangan barcha kalitlarni almashish protokollari ushbu ikki yo'nalishdan biriga tegishli holda amalga oshiriladi.

8.3. Kvant kriptografiyasi protokollari

Bitta fotonning holatiga bog'liq bo'lgan kodlashga asoslangan ko'plab kvant kriptografiyasi protokollari mavjud. BB84, B92, BB84(4+2), Goldenberg-Vaydman, Koashi-Imoto kabi algoritmlarni misol keltirish mumkin. Kvant xususiyatlarini aralashtirishga asoslangan yagona protokol bu - E91.

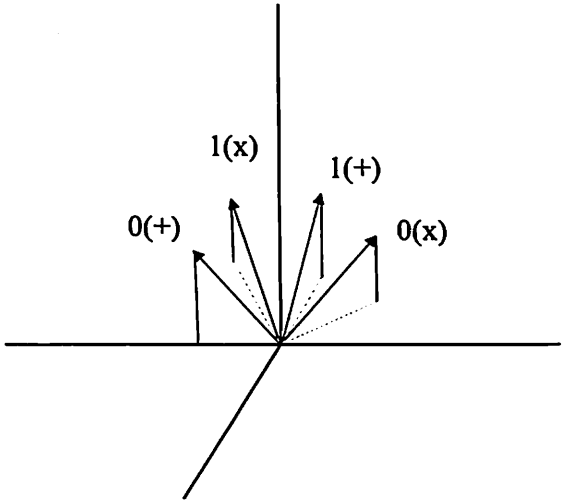
BB84 kvant protokoli. Unda kvantning to'rtta asosiy holati asos qilib olinadi. Alisa jo'natilayotgan bitga bog'liq bo'lmagan holda, «1» uchun 90° yoki 135° hamda «0» 45° yoki 0° li polyarizasiyalar tanlanadi. Kvantning bir jufti $0(|0(+)\succ)$ va $1(|1(+)\succ)$ kvant holatiga mos keladi

va «+» asosni ifodalaydi. Kvantning boshqa bir jufti 0(|0(x) >) va 1(|1(x) >) kvant holatiga mos keladi va «x» asosni ifodalaydi. Ikkita bazisning ichki holati ortogonal, ammo turli asoslarning holati juft ortogonol bo'lmagan sanaladi.

Tizimning kvant holati quyidagicha ifodalanishi mumkin:

$$|0_x\rangle = \frac{1}{\sqrt{2}}(|0_+\rangle + |1_+\rangle, |1_x\rangle) = \frac{1}{\sqrt{2}}(|0_+\rangle - |1_+\rangle)$$

Bu yerda, $|0_+\rangle$ va $|1_+\rangle$ «+» asosda va $|0_x\rangle$ va $|1_x\rangle$ «x» asos uchun mos holda «0» va «1» belgilarini kodlamoqda. Quyidagi 8.1-rasmda bazislarning 45° ga burilgan holi tasvirlangan.



8.1-rasm. BB84 protokolidagi fotonlarning polyarizatsiya holati

Kalitlarni hosil qilish bosqichlari:

1. Alisa tasodifiy holatda asoslardan birini tasodifiy tanlaydi. Asosning ichiga holatlardan birini 0 va 1 ga mos holda tanlaydi va fotonlarni jo'natadi.

8.2-rasm. Turli polyarizasiyali fotonlar

2. Bob Alisaga bog'liq bo'lmagan holda har bir fotonga mos asosni tanlaydi: to'g'ri chiziqli (+) yoki dioganal (x) asos.

8.3-rasm. Tanlangan o'lchamlar

Bob o'lchash natijasini o'zida saqlaydi.

|	-	/	\	-	/	/	/	|

8.4-rasm. O'lchash natijasi

3. Bob ochiq kanal orqali har bir turdagi foton uchun qo'llagan o'lchamini jo'natadi. Ammo, o'lchash natijasi sir saqlanadi.

4. Alisa ochiq kanal orqali Bobga kiruvchi asosga qanday o'lchamdan foydalanilganini jo'natadi.

V			V	V		V		V

8.5-rasm. To'g'ri o'lchamlar

5. Ishtirokchilar faqat mos kelgan asoslarni qoldiradi. Ular 0 yoki 1 bit belgilarini ifodaydi. Natijaa kalit 8.6-rasmdagi holatda olinadi.

|			\	-		/		|
1			1	0		0		1

8.6-rasm. To'g'ri o'lchamlar natijasida olingan kalit ketma-ketligi

Mos kelgan holatlar tahminan kiruvchi xabarning yarmiga ($n = \frac{1}{2}$) teng bo'ladi. Quyidagi 8.1-jadvalda BB84 protokoli asosida kvant kalitlarini hosil qilish misoli keltirilgan.

8.1-jadval

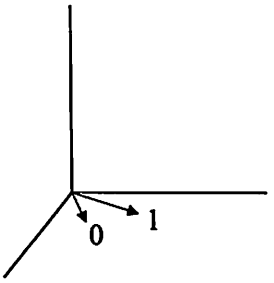
BB84 protokoli asosida kvant kalitlarini hosil qilish

Alisaning ikkilik signali	0	1	0	1
Alisaning polyarizasiya signali	↔	↕	⇘	⇗
Bobda tekshirilishi	✣	✣	✣	✣
Bobning ikkilik signali	0	1	?	?

O'rtadagi yo'qotish va xalaqitlar natijasida o'rtacha 50% foton ro'yhatdan o'tkaziladi.

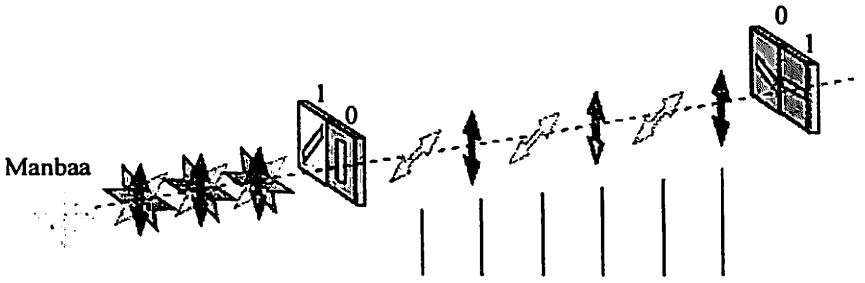
Takomillashgan tizimlarda xatolarni aniqlash va maxfiylikni oshirishning turli usullaridan foydalaniladi.

B92 kvant protokoli. Ushbu protokolda foton 0 va 1 belgilarini ifodalashi uchun ikki turdagi polyarizasiyadan foydalanadi. $|\varphi_0>$ va $|\varphi_1>$. Bu yerda, $<\varphi_0|\varphi_1> \neq 0$. $+45^0$ ga burilgan foton 1 bitni va 0^0 (V) ga burilgan foton esa, 0 bitni ifodalaydi. Quyidagi 8.7-rasmda uning grafik sxemasi keltirilgan.



8.7-rasm. B92 protokolidagi polyarizatsiya holatlari

B92 protokolining algoritmi



Alisaning ikkilik signali	1	0	1	0	1	0
Alisaning polyarizasiya signali	+45	V	+45	V	+45	V
	0		0		0	
Bobning polyarizasiya signali	+45	+45	H	H	H	+45
	0	0				0
Bobning ikkilik signali	0	0	1	1	1	0
Bobdagi natija	N	N	Y	N	Y	N

8.8-rasm. B92 protokoli asosida kvant kalitini hosil qilish

Alisa 0^0 va 45^0 (0 va 1) polyarizasiya yo'nalishidagi fotonlarni jo'natadi. Fotonlar ketma-ketligi tasodifiy yo'naltirilgan. Bob esa, fotonlarni 90^0 va 135^0 (45^0) polyarizasiya yo'nalishida qabul qiladi. Agar Alisadan kelgan fotonlar 90^0 li polyarizasiya orqali tahlil qilinsa, u filtrdan o'tmaydi. Agar ushbu filtr 45^0 ga teng bo'lsa, 0,5 ehtimollik bilan o'tadi.

Bob polyarizasiyani tahlil qilishi uchun «+» yoki «x» asosdan birini tasodifiy qo'llash orqali aniqlanadi. Agar Bob jo'natilgan fotonni ortogonol yo'nalishda tahlil qilgan bo'lsa, ushbu foton qanday belgini o'zida ifodalaganini bilishi mumkin: 1- mos foton o'tkazilmagan, 0 – mos foton 0,5 ehtimollik bilan o'tkazilmagan. Agar Bob jo'natilgan fotonni

ortogonol bo'lmagan yo'nalishda tahlil qilgan bo'lsa, ushbu foton qanday belgini o'zida ifodalaganini bilishi mumkin: 0 – agar foton muvafaqqiyatli qabul qilingan va 0 ni qabul qiladi. 1- *H* yo'nalishda qabul qilingan.

Quyida B92 protokoli asosida kalit generatsiyasi 8.2-jadvalda keltirilgan.

8.2-jadval

B92 protokoli asosida kalit generatsiyasi

Alisaning ikkilik signali	1	0	1	0
Alisaning polyarizasiya signali	↗	↕	↗	↕
Bobning polyarizasiya signali	↘	↘	↔	↔
Bobning ikkilik signali	0	0	1	1
Bobdagi natija	-	-	+	-

Birinchi va to'rtinchi ustunda ortogonol jo'natilgan, shuning uchun qabul qilishda tushib qolgan. Ikkinchi va uchinchi ustunda ortogonol bo'lmagan, shuning uchun to'g'ri qabul qilingan.

Olti holatli protokol. Bitta asosli BB84 protokoli quyidagicha tasvirlanadi:

$$|0_C>=\frac{1}{\sqrt{2}}(|0>+i|1>),\frac{1}{\sqrt{2}}(|0>-i|1>)$$

Ushbu holatdan tashqari yana ikkita polyarizasiya yo'nalishi mavjud: o'ng aylana va chap aylana. Bunda Bob qabul qilgan fotonlarni hisoblashi lozim. Olti holatli kvant protokolini formallashtirish 8.3-jadvalda keltirilgan.

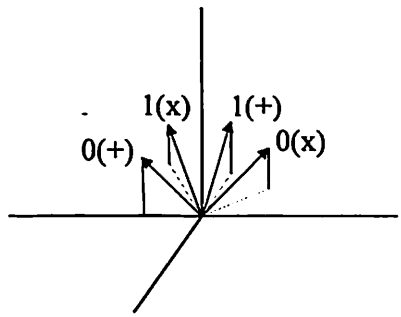
8.3-jadval

Olti holatli kvant protokolini formallashtirish

Alisaning ikkilik signali	1	0	1	0	1	0
Alisaning polyarizasiya signali	↗	↕	↔	↘	↺	↻
Bobda tekshirilishi	✣	✣	✣	✣	✣	✣
Bobning ikkilik signali	?	0	1	?	?	?

Bob fotonlarning minimal sonini qabul qiladi. Ya'ni umumiy fotonlarning uchdan bir (1/3) qismini qabul qiladi. Boshqacha qilib aytganda jo'natilgan fotonlarning 33% qismi qabul qilinadi.

BB84(4+2) kvant protokoli. BB84 va B92 prtotokollarining o'rtasidagi protokol hisoblanadi. Unda «0» va «1» bitlarni ifodalash uchun 4 ta kvant holati 2 ta asosda qo'llaniladi. Har bir asos holati ortogonol bo'lmagan usulda olinadi. Uning grafik ko'rinishi 8.10-rasmda keltirilgan.



8.10-rasm. BB84(4+2) prtokolida qo'llaniladigan polyarizasiya holati

Alisa tasodifiy holda asoslardan birini tanlaydi. Asosning ichida ham, tasodifiy holatda 0 yoki 1 tanlanadi va ular kvant kanaliga yo'naltiriladi. Bob bog'liq bo'lmagan holda iki o'lchamni tanlaydi. Bir nechta xabarlar almashilgandan keyin, har bir jo'natmada qo'llanilgan asoslarga aniqlik kiritiladi. Jo'natmadagi mos kelmagan asoslar tashlab yuboriladi. Qolgan jo'natmalarning raqami ochiqlanadi va uning kirish holati aniqlanmaganini bildiradi. Qolgan jo'natmalardan xatolarni tuzatish kodlari va maxfiylikni oshirish usullari yordamida maxfiy kalit hosil qilinadi. Bob qabul qilgan fotonlar 8.4-jadvalda keltirilgan.

8.4-jadval

BB84(4+2) protokolini formallashirish

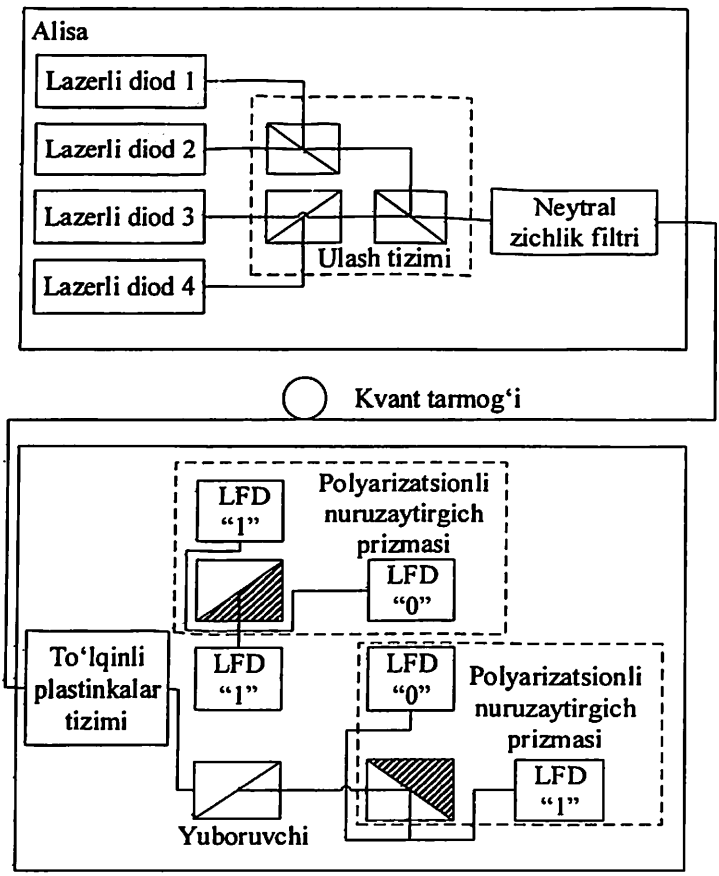
Alisaning ikkilik signali	0	1	0	1	0	1	0	1
Alisaning polyarizasiya signali	↔	↕	↘	↗	↔	↕	↘	↗
Bobda tekshirilishi	X	X	X	X	X	X	X	X
Bobning ikkilik signali	0	?	?	1	0	?	?	1

Natijada 50% fotonlarni qabul qilishga erishiladi.

Kvant kalitlarni almashish sxemasi. Hozirda kvant holatlarini kodlashning uchta turidan foydalaniladi: polyarizasiya, fazo va vaqtinchalik siljishlarni kodlash.

Polyarizasiyalri kodlash tizim tuzilmasi. Unga misol sifatida BB84 protokolini keltirish mumkin va 8.11-rasmda uning 4 ta holatli turi sxemasi keltirilgan.

Alisa stansiyasi 1 ns vaqt oralig'i bilan o'rganadigan 4 ta lazerli dioddan tashkil topgan. Fotonlar polyarizasiyasi -45^0, 0^0, $+45^0$ va 90^0 dan iborat. Bitta bitni jo'natish uchun lazer diodlaridan biri faollashtiriladi. Fotonlari kamida bir marta foydalaniladi va qadrsizlantiriladi. Bundan keyin Bob yo'nalishidagi fotonlar o'rganiladi. Bob fotonlarni to'g'i aniqlashi uchun optik aloqadagi asoslarni saqlash lozim.



8.11-rasm. Polyarizasiyalri kodlash tizim tuzilmasi

Impulslar plastinalardan dastlabki polyarizasiya holatini qayta tiklash uchun plastinalardan o'tkaziladi. Keyin impulslar, chiziqli yoki

dioganal yo'nalishini aniqlash uchun tahlildan o'tkaziladi. Fotonlar ortogonol asosda tekshiriladi (LFD). Fotonlar polyarizasiyasi to'lqin plastinasidan o'tgandan keyin 45^0ga buriladi. Ushbu vaqtda qolgan fotonlar yorug' polyarizasion prizmadan (LFD) o'tkaziladi.

Foton polyarizasiyasi $+45^0$ holatda bo'lishi lozim. Shundan so'ng, u Alisaga jo'natiladi va uning polyarizasiyasi tasodifiy holda optik tolada akslanadi. Bobda to'lqin plastinkalari polyarizasiya o'zgarishini to'ldiruvchi qilib o'rnatilishi lozim.

Ushbu sxemada to'rtta lazer va ikkita polyarizasiya holatidan foydalanilgan.

Fazoli kodlash tizimi tuzilishi. Polyarizasiyalarning barqaror emasligi polyarizasiyali kodlashtirishda murakkabliklar tug'diradi. Shuning uchun Bennet tomonidan fazoli kodlash tizimi yaratilgan. Fotonlarni qabul qilish va ularning tahlili interferometr qurilmalarida amalga oshiriladi.

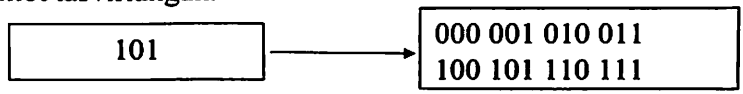
Vaqtinchalik kodlash tizimi strukturasi. Kvant kriptografisida vaqt oraliqlaridan foydalanish Sergey Molotkov tomonidan taklif etilgan. «0» va «1» bitlarni jo'natish uchun ayni vaqt oralig'idan foydalaniladi va ushbu vaqt har bir jnatmada almashinadi. Natijada ortogonol bo'lmagan hususyati kelib chiqadi. Natijada, interferometr qurilamalaridan foydalanishni bekor qiladi.

8.4. Kvant kompyuteri

Kvant mehanikasining imkoniyatlaridan foydalangan holda ma'lumotlarni tezkorlik bilan almashish va qayta ishlash uchun kvant kompyuteridan foydalanish 1981 yilda Yuriy Mannin tomonidan taklif etilgan. An'anaviy kompyuterlardan farqli ravishda "0" va "1" lar ustida emas, kubitlar ustida ma'lumot almashadi.

Kubit – kvant kompyuterlarida axborot saqlash turi. Kubit ham axborot biti kabi ikkita holatda bo'ladi: $|1\succ$ va $|0\succ$.

8.12-rasmda oddiy va kvant kompyuterlarning registridagi ma'lumot tasvirlangan.



8.12-rasm. Oddiy va kvant kompyuterlarning registridagi ma'lumot

Kvant kompyuterlari ko'plab imkoniyatlarni taqdim etsada, hozircha faqat nazariy jihatdan tasdiqlangan. 2010 yilda ayrim algoritmlarni qo'llagan holda amaliy tajribalar o'tkazilgan. Kvant qurilmalari ba'zi moddalarning sub-atom darajasida yoki keskin sovuq haroratga tutilganda reaksiyaga tayanadi. Googlening qurilmasi ichidagi metal ham deyarli -460 darajagacha muzlatilgan.

Ushbu turdagi kompyuterlar uchun yuqori darajali Quipper dasturlash tilida amallar bajariladi. Undagi hisoblashlar mahsus kvant algoritmlari yordamida amalga oshiriladi.

Agar klassik prosessorlar har bir seansda $|0>, |1>, \dots, N$ holatlardan birida bo'lsa, kvant prosessorlari har bir seansda barcha holatlarda bo'la oladi. Ushbu kvant holati kvant superposisiyasi deb nomlanadi va quyidagicha ifodalanadi:

$$|\Psi>=\sum_{j=0}^{N-1}\lambda_j|j>.$$

Bu yerda, $|j>$ - har bir holat, λ_j – amplituda.

Muhokama: Kvant kriptografiyasi konfidensiallikni ta'minlash borasida o'z o'rniga ega. Ohirgi paytlarda Toshiba, NEC, IBM, Hewlett Packard, Mitsubishi, NTT kabi tashkilotlar kvant kriptografiyasiga asoslangan tizimlarni ishlab chiqishga kirishgan. MagiQ, IdQuantique va Smart Quantum kabi kichik tashkilotlar katta natijalarga erishgan.

Kvant kriptografisini rivojlantirish uchun matematiklar, fiziklar va sxematexniklar birgalikda kurashishi lozim.

Nazorat savollari

1. Kvant nazariyasi haqida ayting?
2. Kvant kalitlarni almashinish haqida ayting?
3. Kvant kriptografiyasida mavjud kalitlarni taqsimlash protokollari haqida ayting?
4. Kvant kompyuteri va uning xususiyatlari?

FOYDALANILGAN ADABIYOTLAR

1. A.J.Menezes, P.C. van Oorschot, S.A.Vanstone. Handbook of Applied Cryptography. CRC Press, 2001, 816 p.
2. Шнайер Б. Прикладная криптография. Протоколы, алгоритмы, исходные тексты на языке Си. –М.: издательство ТРИУМФ, 2003 -816 стр.
3. S.K.Ganiev, A.A.Ganiev, Z.T.Xudoyqulov. Kiberxavfsizlik asoslari: O‘quv qo‘llanma. – T.: “Iqtisod-Moliya”, 2021. – 228 b.
4. S.K.Ganiev, T.A.Kuchkarov. Tarmoq xavfsizligi (Mobil tarmoq xavfsizligi). O‘quv qo‘llanma. –T.: «Aloqachi», 2019, 140 b.
5. S.K.Ganiev, M.M.Karimov, Z.T.Xudoyqulov, M.M.Kadirov. Axborot xavfsizligi bo‘yicha atama va tushunchalarning rus, o‘zbek va ingliz tillaridagi izohli lug‘ati. –T.: «Iqtisod-moliya», - 2017, 480 bet.
6. S.K.Ganiev, M.M.Karimov, K.A.Tashev. Axborot xavfsizligi. –T.: «Fan va texnologiya», 2016, 372 bet.
7. S.K.Ganiev, M.M.Karimov, K.A.Tashev. Axborot xavfsizligi. Axborot-kommunikatsion tizimlar xavfsizligi. O‘quv qo‘llanma. –T.: «Aloqachi», 2008, 382 bet.
8. Stamp M. Information security: principles and practice // John Wiley & Sons, 2011, -P. – 606.
9. D.Y.Akbarov, P.F.Xasanov, X.P.Xasanov, O.P.Axmedova, I.U.Xolimtoyeva. Kriptografiyaning matematik asoslari. O‘quv qo‘llanma. –T.: «Aloqachi», 2019, 192 bet.
10. Akbarov D.Y. Axborot xavfsizligini ta’minlashning kriptografik usullari va ularning qo‘llanilishi // Toshkent, 2008, 394 bet.
11. Шаньгин, В. Ф. Информатsионная безопасность компьютерных систем и сетей : Учеб. пособие / В.Ф. Шаньгин. — Москва : ИД «ФОРУМ» : ИНФРА-М, 2017. — 416 с.
12. А.П. Алферов, А.Ю. Зубов, А.С. Кузьмин, А.В. Черемушкин. Основы криптографии: Учебное пособие, 2-е изд. –М.: Гелиос АРВ, 2002.-480 с.
13. Xasanov X.P. Takomillashgan diamatritsalar algebralari va parametrli algebra asosida kriptotizimlar yaratish usullari va algoritmlari. –Toshkent, 2008. - 208 bet.

ATAMALARNING RUS, O'ZBEK VA INGLIZ TILLARIDAGI IZOHLI LUG'ATI

Авторизatsiя - представление пользователю определенных прав доступа на основе положительного результата его аутентификатsiи в системе.

Avtorizatsiya – tizimda foydalanuvchiga, uning ijobiy autentifikatsiyasiga asosan, ma'lum foydalanish huquqlarini taqdim etish.

Authorization – granting the user certain access rights based on the positive result of authentication in the system.

Администратор защиты - субъект доступа, ответственный за защиту автоматизированной системы от несанкционированного доступа к информатsiи.

Himoya ma'muri – avtomatlashtirilgan tizimni axborotdan ruxsatsiz foydalanishdan himoyalashga javobgar foydalanish subyekti.

Security administrator - the subject of the access responsible for the protection of the automated system against unauthorized access to the information.

Администратор системы - лицо, отвечающее за эксплуататsiю системы и поддержание ее в работоспособном состоянии.

Tizim ma'muri – tizimni ekspluatatsiyasiga va uning ishga layoqatlik holatini ta'minlashga javobgar shaxs.

System administrator – a person who is responsible for operation of the system and keeping it in an appropriate working condition.

Актив - 1. Информатsiя или ресурсы, подлежащие защите. 2. Все, что имеет ценность для организатsiи. 3. Главное приложение, общая система поддержки, высоко авторитетная программа, материальная часть, миссия критической систем, персонал, оборудование или логически связанная группа систем.

Aktiv - 1. Himoyalanuvchi axborot yoki resurslar. 2. Tashkilot uchun qiymatli barcha narsalar. 3. Bosh ilova, umumiy madadlovchi tizim, yuqori nufuzli dastur, moddiy qism, kritik tizim missiyasi, xodimlar, jihozlar yoki mantiqiy bog'langan tizimlari guruhi.

Asset - 1. Information or resources that should be protected. 2. Anything that has value to the organization. 3. A major application, general support system, high impact program, physical plant, mission critical system, personnel, equipment, or a logically related group of systems.

Активная угроза - угроза преднамеренного несанкционированного изменения состояния системы.
Faol tahdid – tizim holatini atayin ruxsatsiz o'zgartirish tahdidi.
Active threat – a threat that can make a deliberate unauthorized change to the system.

Алгоритм шифрования - алгоритм криптографический, реализующий функцию шифрования. В случае шифрсистем блочных получается использованием алгоритма шифрования блочного базового в конкретном режиме шифрования.
Shifrlash algoritmi - shifrlash funksiyasini amalga oshiruvchi kriptografik algoritm. Blokli shifrtizim holida shifrlashning muayyan rejimida shifrlashning bazaviy blokli algoritmidan foydalanib hosil qilinadi.
Encryption algorithm - a cryptographic algorithm that implements the function of encryption. In the case of block cipher system is obtained using the algorithm of the base block encryption in a particular mode of encryption.

Алгоритм криптографический - алгоритм, реализующий вычисление одной из функций криптографических.
Kriptografik algoritm – kriptografik funksiyalardan birini hisoblashni amalga oshiruvchi algoritm.
Cryptographic algorithm - the algorithm that implements the calculation of one cryptographic functions.

Алгоритм расшифрования - алгоритм криптографический, обратный к алгоритму шифрования и реализующий функцию расшифрования.
Rasshifrovkalash algoritmi – rasshifrovkalash funksiyasini amalga oshiruvchi va shifrlash algoritmiga teskari algoritm.

Decryption algorithm – the cryptographic algorithm which is inverse to the encryption algorithm that implements the decryption function.

Алгоритм хеширования - в криптографии - алгоритм, реализующий хеш-функцию криптографическую. В математике и программировании - алгоритм преобразования строк символов, как правило, уменьшающий длину строки и такой, что значение каждого символа выходной строки зависит сложным образом от большого количества входных символов (в идеале - от всех). Обычно, алгоритм хеширования преобразует строки произвольной длины в строки фиксированной длины.

Xeshlash algoritmi – kriptografiyada kriptografik xesh-funksiyani amalga oshiruvchi algoritm. Matematika va dasturlashda – odatda, satr uzunligini kamaytiruvchi simvollar satrini o'zgartiruvchi algoritm. Chiqish yo'li satrining har bir simvolining qiymati kirish yo'li simvollarining katta soniga (idealda – barchasiga) murakkab tarzda bog'liq. Odatda xeshlash algoritmi ixtiyoriy uzunlikdagi satrni belgilangan uzunlikdagi satrga o'zgartiradi.

Hashing algorithm – in cryptography, an algorithm that implements the cryptographic hash function. In mathematics and computer programming - algorithm for converting strings of characters, generally reducing the length of the string and such that the value of each symbol of the output string depends in a complex way from a large number of input characters (ideally all). Usually, hashing algorithm converts strings of arbitrary length to strings of fixed length.

Алгоритм цифровой подписи - асимметричный алгоритм, используемый для цифровой подписи данных.

Raqamli imzo algoritmi - ma'lumotlarni raqamli imzolash uchun foydalaniluvchi asimetrik algoritm.

Digital signature algorithm – asymmetric algorithm used for digitally signing data.

Алгоритм шифрования RSA - алгоритм шифрования, предложенный в 1978 г. Р. Райвестом, А. Шамиром и Л. Адлеманом и предназначенный для построения шифрсистем асимметричных.

RSA shifrlash algoritmi – 1978 yili R. Rayvest, A Shamir va L.Adleman tomonidan taklif etilgan va asimetrik shifr tizimlarini qurishga mo'ljallangan shifrlash algoritmi.
RSA encryption algorithm - the encryption algorithm proposed in 1978 by R. Rivest, A. Shamir and L. Adleman and is designed to build asymmetric ciphers.

Анализ - изучение значимости полученных данных и доказательственной ценности к случаю.
Tahlil – olingan ma'lumotlarning muhimligi va vaziyat uchun isbotlanganlik qiymatini o'rganish.
Analysis – the examination of acquired data for its significance and probative value to the case.

Анализаторы сетевые (сниффер) - программы, осуществляющие «прослушивание» трафика сетевого и автоматическое выделение из трафика сетевого имен пользователей, паролей, номеров кредитных карт, другой подобной информатsiи.
Tarmoq tahlillagichlari (sniffer) – tarmoq trafigini "tinglash"ni va tarmoq trafigidan avtomatik tarzda foydalanuvchilar ismini, parollarni, kredit kartalar nomerini, shu kabi boshqa axborotni ajratib olishni amalga oshiruvchi dasturlar.
Network analyzers (sniffer) - programs that listen on network traffic and automatic allocation of network traffic usernames, passwords, credit card numbers, and other such information.

Антивирус - программа, обнаруживающая или обнаруживающая и удаляющая вирусы. Если вирус удалить не удается, то зараженная программа уничтожается. Еще - программа, предназначенная для защиты от вирусов, обнаружения зараженных программных модулей и системных областей, а также восстановления исходного состояния зараженных объектов.
Antivirus – viruslarni aniqlovchi yoki aniqlovchi va yo'q qiluvchi dastur. Agar virus yo'q qilinmasa, zaharlangan dastur yo'q qilinadi. Yana – viruslardan himoyalashga, zaxarlangan dasturiy modullar va tizimli

makonlarni aniqlashga, hamda zaxarlangan obyektlarning dastlabki holatini tiklashga mo'ljallangan dastur.
Antivirus - the program that detect or detect and remove viruses. If virus remove not possible, then the infected program is destroyed. Another program, designed to protect against viruses, detecting infected software modules and system areas as well as restore the original state of infected object.

Аппаратное средство защиты информатsии - специальное защитное устройство или приспособление, входящее в комплект технического средства обработки информатsии.
Axborotni himoyalashning apparat vositasi – axborotni ishlovchi texnik vositasi komplekti tarkibiga kiruvchi maxsus himoyalovchi qurilma yoki moslama.
Hardware data protection - a special protective device or fixture included in the kit technical tools of information processing.

Апплеты вредоносные - небольшие приложения, которые автоматически загружаются и выполняются, и которые реализуют несанкционированные функции информатsионной системы.
Zararli appletlar - axborot tizimida ruxsat etilmagan funksiyalarni amalga oshiruvchi, avtomatik yuklanuvchi va bajariluvchi kichik ilovalar.
Malicious applets – small application that are automatically downloaded and executed and that perform an unauthorized function on an information system.

Архитектура IT безопасности - описание принципов безопасности и общего подхода для соблюдения принципов, управляющих системой проектирования безопасности.
AT xavfsizlik arxitekturasi - xavfsizlikni loyihalash tizimini boshqaruvchi tamoyillariga rioya qilish uchun xavfsizlik tamoyillarining va umumiy yondashishning tavsifi.
IT security architecture – a description of security principles and an overall approach for complying with the principles that drive the system design.

Архитектура информатsionной безопасности - встроенная, неотъемлемая часть архитектуры предприятия, описывающая структуру и поведение процессов безопасности, систем информатsionной безопасности, персональных и организатsionных подразделений, с указанием их выравнивание с целью и стратегическими планами предприятия.

Axborot xavfsizligining arxitekturasi - tashkilot xavfsizlik jarayonlari strukturasi va ishlash rejimini, axborot xavfsizligi tizimlarini, shaxsiy va tashkiliy bo'linmalarini, ularni tashkilot missiyasi va strategik rejalariga tenglashtirishni ko'rsatish bilan tavsiflovchi tashkilot arxitekturasining o'rnatilgan, ajratib bo'lmas qismi.

Information security architecture – an embedded, integral part of the enterprise architecture that describes the structure and behavior for an enterprise's security processes, information security systems, personnel and organizational sub-units, showing their alignment with the enterprise's mission and strategic plans.

Атака «противник в середине» — атака на протокол криптографический, в которой противник C выполняет этот протокол как с участником A, так и с участником B. Противник C выполняет сеанс с участником A от имени B, а с участником B от имени A. В процессе выполнения противник пересылает сообщения от A к B и обратно, возможно, подменяя их. В частности, в случае протокола аутентификатsii абонента успешное осуществление атаки «противник в середине» позволяет противнику аутентифицировать себя для B под именем A.

«Dushman o'rtada» hujumi – kriptografik protokolga hujum bo'lib, bunda dushman C ushbu protokolni ishtirokchi A va ishtirokchi B bilan bajaradi. Dushman C ishtirokchi A bilan seansni ishtirokchi B nomidan, ishtirokchi B bilan esa ishtirokchi A nomidan bajaradi. Bajarish jarayonida dushman ishtirokchi A dan ishtirokchi V ga va aksincha xabarni, ehtimol, o'zgartirib uzatadi. Xususan, abonentni autentifikatsiyalash protokoli holida «dushman o'rtada» hujumining muvafaaqiyatli amalga oshirilishi dushmanga ishtirokchi B uchun o'zini ishtirokchi A nomidan autentifikatsiyalashga imkon beradi.

Attack "the opponent in the middle" - attack on a cryptographic protocol in which the enemy with this protocol performs as a party A and party B with C. Enemy performs session with party A on behalf of B, and a participant on behalf of A. During runtime opponent forwards messages from A to B and back, possibly replacing them attacks. In particular, in the case of an authentication protocol is connected to the success of the attack "the opponent in the middle" allows authenticate itself to the enemy in the name of A.

Атака на отказ в обслуживании — атака с целью вызвать отказ системы, то есть создать такие условия, при которых легитимные пользователи не смогут получить доступ к предоставляемым системой ресурсам, либо этот доступ будет значительно затруднён.
Xizmat qilishdan voz kechishga undaydigan hujum – tizim buzilishiga sabab bo'luvchi hujum, ya'ni shunday sharoitlar tug'diradiki, qonuniy foydalanuvchi tizim taqdim etgan resurslardan foydalana olmaydi yoki foydalanish anchagina qiyinlashadi.
Denial-of-service attack - attack intended to cause a system failure, that is, to create conditions under which legitimate users will not be able to access the system-provided resources, or this access much more difficult.

Атака пассивная — атака на криптосистему или протокол криптографический, при которой противник и/или нарушитель наблюдает и использует передаваемые сообщения шифрованные, но не влияет на действия пользователей законных.
Passiv hujum – kriptotizmga yoki kriptografik protokolga hujum bo'lib, bunda dushman va/yoki buzg'unchi uzatiluvchi shifrlangan axborotni kuzatadi va ishlatadi, ammo qonuniy foydalanuvchilar harakatiga ta'sir etmaydi.
Passive attack - attack on a cryptosystem or a cryptographic protocol in which enemy and/or the offender observes and uses the transmitted messages are encrypted, but does not affect the user's actions legitimate.

Атака со словарем паролей — атака на криптосистему, основанная на переборе значений пароля.

Parollar lug'atiga asoslangan hujum – parol qiymatlarini saralashga asoslangan kriptotizimga hujum.
Attack with a dictionary of passwords - the attack on the cryptosystem based on iterating the value of a password.

Аутентификатор - средство аутентификатsii, представляющее отличительный признак пользователя. Средствами аутентификатsii пользователя могут быть дополнительные кодовые слова, биометрические данные и другие отличительные признаки пользователя.
Autentifikator – foydalanuvchining farqli alomatini ifodalovchi autentifikatsiya vositasi. Qo'shimcha kod so'zlari, biometrik ma'lumotlar va foydalanuvchining boshqa farqli alomatlari autentifikatsiya vositalari bo'lishi mumkin.
Authenticator - means of authentication that represents the distinctive attribute of the user. Means of user authentication can be additional code word, biometric data and other identifying features of the user.

Аутентификатsiя - проверка идентификатsii пользователя, устройства или другого компонента в системе, обычно для принятия решения о разрешении доступа к ресурсам системы; проверка целостности хранящихся или передающихся данных для обнаружения их несанкционированной модификатsii.
Autentifikatsiya – odatda tizim resurslaridan foydalanishga ruxsat etish xususida qaror qabul uchun foydalanuvchining, qurilmaning yoki tizimning boshqa tashkil etuvchisining identifikatsiyasini tekshirish; saqlanuvchi va uzatuvchi ma'lumotlarning ruxsatsiz modifikatsiyalanganligini aniqlash uchun tekshirish.
Authentication - checking the identification of user, device, or other component in the system, typically for decision-making about access to system resources; check the integrity of stored or transmitted data to detect unauthorized modification.

Аутентификатsiя биометрическая — способ аутентификатsii абонента (пользователя), основанный на проверке его биометрических характеристик (отпечатков пальцев, геометрии

руки, лица, голоса, рисунка сетчатки глаза и т. п.). К преимуществам данного метода относится неотделимость биометрических характеристик от пользователя: их нельзя забыть, потерять или передать другому пользователю.

Biometrik autentifikatsiya – abonentni (foydalanuvchini) uning biometrik xarakteristikasi (barmoq izlari, panja geometriyasi, yuzi, ovozi, ko'z pardasining to'ri va h.) asosidagi autentifikatsiyalash usuli. Ushbu usulning afzalligi – biometrik xarakteristikalarni foydalanuvchidan ajratib bo'lmasligi. Ularni esdan chiqarishning, yo'qotishning yoki boshqa foydalanuvchiga berishning iloji yo'q.

Biometric authentication - the method of authentication of a subscriber (user), based on a verification of biometric characteristics (fingerprints, hand geometry, face, voice, eye retina image, etc.). The advantages of this method is the inseparability of biometric characteristics from user: they cannot be forgotten, lost or transferred to another user.

Аутентификатsiя двухфакторная — аутентификатsiя пользователей на основе двух разнородных факторов, как правило, на основе того, что знает пользователь, и того, чем он владеет (например, на основе пароля и физического идентификатора).

Ikki faktorli autentifikatsiya – foydalanuvchilarni ikkita turli faktorlar asosida autentifikatsiyalash, odatda, foydalanuvchi biladigan narsa va egalik qiladigan narsa (masalan, parol va fizik identifikatori) asosida.

Two-factor authentication - user authentication on the basis of two unrelated factors, as a rule, on the basis of what he knows and what he knows (e.g., password-based and physical ID).

Аутентификатsiя на основе паролей одноразовых — технология аутентификатsii с помощью паролей одноразовых, для получения которых могут использоваться: алгоритм генератsii на основе односторонней функции, специальные устройства – токены, либо технология OOB (out of band), основанная на передаче пароля одноразового с использованием дополнительного канала, отличного от того, по которому пользователь осуществляет доступ к прикладной системе.

Bir martali parollar aosidagi autentifikatsiya - bir martali parollar yordamida autentifikatsiyalash texnologiyasi. Bir martali parollarni olishda quydagilar ishlatilishi mumkin: bir tomonlama funksiya asosida generatsiyalash algoritmi, maxsus qurilmalar-tokenlar, yoki bir martali parolni, foydalanuvchi tatbiqiy tizimdan foydalanishda ishlatiladigan kanaldan farqli, kanal orqali uzatishga asoslangan OOB (out of band) texnologiyasi.
One time password based authentication - technology authentication using one time passwords, which can be used: the generation algorithm based on one-way functions, special device – taken, or technology OOB (out of band) based on the transmission password disposable using additional channels, other than where the user accesses the application system.

Аутентификатsiя сообщений - добавление к блоку данных контрольного поля для обнаружения любых изменений в данных. При вычислении значений этого поля используется ключ, известный только приемнику данных.
Xabarlar autentifikatsiyasi – ma'lumotlarda har qanday o'zgarishlarni aniqlash maqsadida ma'lumotlar blokiga nazorat hoshiyasini qo'shish. Ushbu hoshiya qiymatini hisoblashda faqat ma'lumotlar priyemnigiga ma'lum kalitlar ishlatiladi.
Message authentication - adding control data to the data field to detect any changes in the data. The values of this field using a key known only to receiver data.

База данных - совокупность данных, организованных по определенным правилам, предусматривающим общие принципы описания, хранения и манипулирования данными, независимо от прикладных программ. Является информатsионной моделью предметной области. База данных, как правило, представляются тремя уровнями абстракции: внешним, концептуальным и внутренним.
Ma'lumotlar bazasi - tatbiqiy dasturlarga bog'liq bo'lmagan holda ma'lumotlarni tavsiflashning, saqlashning va manipulyatsiyalashning umumiy tamoyillarini ko'zda tutuvchi, ma'lum qoidalar bo'yicha tashkil

etilgan ma'lumotlar majmui. Predmet sohasining informatsion modeli hisoblanadi. Ma'lumotlar bazasi odatda abstraksiyaning tashqi, konseptual va ichki satxlari orqali ifodalanadi.
Database - a collection of data organized according to certain rules, providing general principles for describing, storing and manipulating data independent of the application programs. An information domain model. The database, usually presented in three levels of abstraction: external, conceptual and internal.

Безопасность - свойство системы противостоять внешним или внутренним дестабилизирующим факторам, следствием воздействия которых могут быть нежелательные ее состояния или поведение. Еще - состояние, в котором файлы данных и программы не могут быть использованы, просмотрены и модифицированы неавторизованными лицами (включая персонал системы), компьютерами или программами.
Xavfsizlik - ta'siri natijasida nomaqbul holatlarga olib keluvchi atayin yoki tasodifiy, ichki va tashqi beqarorlovchi faktorlarga qarshi tizimning tura olish xususiyati. Yana - ma'lumotlar fayllarining va dasturlarning avtorizatsiyalanmagan shaxslar (jumladan tizim xodimi), kompyuterlar yoki dasturlar tomonidan ishlatilishi, ko'rib chiqilishi va modifikatsiyalanishi mumkin bo'lmagan holat.
Security - the property of a system to withstand external or internal destabilizing factors, the effect of which may be unwanted state or behaviour. Still - a state in which the data files and programs may not be used, viewed and modified by unauthorized persons (including the system staff), computers or software.

Безопасность информатsии - состояние информатsии, при котором исключаются случайные или преднамеренные несанкционированные воздействия на информатsию или несанкционированное ее получение; еще - состояние уровня защищенности информатsии при ее обработке техническими средствами, обеспечивающее сохранение таких ее качественных характеристик (свойств) как секретность (конфиденциальность), целостность и доступность.

Axborot xavfsizligi - axborot holati bo'lib, unga binoan axborotga tasodifiy yoki atayin ruxsatsiz ta'sir etishga yoki ruxsatsiz uning olinishiga yo'l qo'yilmaydi; yana - axborotni texnik vositalar yordamida ishlanishida uning maxfiylik (konfidensiallik), yaxlitlik va foydalanuvchanlik kabi xarakteristikalarini (xususiyatlarini) saqlanishini ta'minlovchi axborotning himoyalanish darajasi holati.
Information security - status information, which excludes accidental or deliberate tampering or unauthorized information receive it, also - the state of security level information when processing technical means to ensure the preservation of its quality characteristics (properties) such as secrecy (confidentiality), integrity, and availability.

Безопасность информатsионная общества - то же, что и «безопасность, информатsионная личности» применительно к организованному коллективу людей и к обществу в целом.
Jamiyat axborot xavfsizligi – "shaxs axborot xavfsizligi" kabi, uyushgan odamlar kollektiviga va umuman, jamiyatga qo'llaniladi.
Society information security - what "safety information personality" when applied to organized team of people and to society as a whole.

Безопасность информатsионной сети - меры, предохраняющие информатsионную сеть от несанкционированного доступа, случайного или преднамеренного вмешательства в нормальные действия или попыток разрушения ее компонентов.
Axborot tarmog'i xavfsizligi – axborot tarmog'ini ruxsatsiz foydalanishdan, me'yoriy harakatlariga tasodifiy yoki atayin aralashishdan yoki komponentlarini buzishga urinishdan saqlash choralari.
Network security - measures that protect the information network from unauthorized access, accidental or deliberate interference in normal activities or attempts the destruction of its components.

Брандмауэр - метод защиты сети от угроз безопасности, исходящих от других систем и сетей, с помощью централизатsии доступа к сети и контроля за ним аппаратно-программными средствами; еще - является защитным барьером, состоящим из нескольких

компонентов (например, маршрутизатора или шлюза, на котором работает программное обеспечение брандмауэра).
Tarmoqlararo ekran – apparat-dasturiy vositalar yordamida tarmoqdan foydalanishni markazlashtirish va uni nazoratlash yo'li bilan tarmoqni boshqa tizimlardan va tarmoqlardan keladigan xavfsizlikka tahdidlardan himoyalash usuli; yana - bir necha komponentlardan (masalan, tarmoqlararo ekran dasturiy ta'minoti ishlaydigan marshrutizator yoki shlyuzdan) tashkil topgan ximoya to'sig'i hisoblanadi.
Firewall - a method of protecting a network against security threats from other systems and networks, through centralizing network access and control hardware and software; - is a protective barrier consisting of several components (e.g., router or gateway running firewall software).

Кибер инфраструктура - включает электронную информатsiю и коммуникатsionные системы, и службы и информатsiю, содержавшуюся в этих системах и службах.
Kiber infrastruktura – elektron axborot, kommunikatsiya tizimlari, xizmatlar va bu tizimlar va xizmatlarda mavjud axborotni o'z ichiga oladi.
Cyber infrastructure – includes electronic information and communications systems and services and the information contained in these systems and services.

Кибер инцидент - действия, использующие компьютерные сети, приводящие к фактическому или потенциальному ущербу в информатsionной системе и/или содержащейся в ней информатsии.
Kiber insident – axborot tizimi va/yoki undagi axborotga aniq yoki potensial zarar yetkazilishiga sabab bo'luvchi, kompyuter tarmoqlaridan foydalanuvchi harakatlar.
Cyber incident – actions taken using computer networks that result in an actual or potentially adverse effect on an information system and/or the information residing therein.

Кибер-атака - атака, через киберпространство, предназначенная для использования предприятием киберпространства в целях, отключения, уничтожения или злонамеренного контроля вычислительной среды/инфраструктуры.

Kiber-hujum – hisoblash muhiti/ infrastrukturasini, o‘chirish, buzish yoki g‘arazli nazoratlash yoki ma’lumot yaxlitligini buzish yoki nazoratlanuvchi axborotni o‘g‘irlash maqsadida kiberfazodan foydalanuvchi tashkilotga atalgan kiberfazo orqali amalga oshiriluvchi hujum.
Cyber-attack – an attack, via cyberspace, targeting an enterprise’s use of cyberspace for the purpose of disabling, destroying, or maliciously controlling a computing environment/infrastructure.

Кибербезопасность - возможность охранять или защитить использование киберпространства кибератаками.
Kiberxavfsizlik – kiberfazoning kiberhujumlardan foydalanishidan qo‘riqlash yoki himoyalash imkoniyati.
Cybersecurity – the ability to protect or defend the use of cyberspace from cyber-attacks.

Киберпреступность — действия отдельных лиц или групп, направленные на взлом систем компьютерной защиты, на хищение или разрушение информатsии в корыстных или хулиганских целях.
Kiberjinoyatchilik - g‘arazli yoki xuliganlik maqsadlarida himoyalashning kompyuter tizimlarini buzib ochishga, axborotni o‘g‘irlashga yoki buzishga yo‘naltirilgan alohida shaxslarning yoki guruhlarning harakatlari.
Cyber cryme — the actions of individuals or groups aimed at cracking computer security systems, theft or destruction of information for selfish or destructive purposes.

Киберпространство - глобальный домен в информатsионной среде, состоящий из взаимозависимой сети инфраструктур информатsионных систем включая Интернет, сети телекоммуникатsии, компьютерные системы, и встроенные процессоры и контроллеры.
Kiberfazo – Internet, telekommunikatsiya tarmoqlari, kompyuter tizimlari va o‘rnatilgan prosessorlar va kontrollerlarni o‘z ichiga olgan, o‘zaro bog‘langan axborot tizimlari infrastrukturalar tarmog‘idan tashkil topgan axborot muhitidagi global domen.

Cyberspace – a global domain within the information environment consisting of the interdependent network of information systems infrastructures including the Internet, telecommunications networks, computer systems, and embedded processors and controllers.

Кибертерроризм — действия по дезорганизatsii компьютерных систем, создающие опасность гибели людей, значительного имущественного ущерба либо иных общественно опасных последствий.
Kiberterrorizm - insonlar halokati, aytarlicha moddiy zarar xavfini yoki boshqa jamiyatga xavfli oqibatlarni tug'diruvchi kompyuter tizimlarini izdan chiqarish bo'yicha harakatlar.
Cyber terrorism — action disruption of computer systems, creating a danger of loss of life, significant property damage or other socially dangerous consequences.

Привилегии - права пользователя или программы, состоящие в доступности определенных объектов и действий в вычислительной системе.
Imtiyozlar - hisoblash tizimida ma'lum obyektlardan foydalanish va ularda ishlashdan iborat foydalanuvchilarning yoki dasturning huquqlari.
Privilege - rights of the user or a program, consisting in the availability of certain objects and actions in a computing system.

Приложение – программное обеспечение (программа) информatsionной системы, выполняющая определенную функцию непосредственно для пользователя без доступа к системе управления, мониторинга или административным привилегиям.
Ilova – bevosita foydalanuvchi uchun boshqarish, monitoringlash tizimlaridan yoki ma'muriy imtiyozlardan foydalanmay aniq funksiyani bajaruvchi axborot tizimining dasturiy ta'minoti (dasturi).
Application – a software (program) hosted by an information system. In addition, software program that performs a specific function directly for a user and can be executed without access to system control, monitoring, or administrative privileges.

Программа антивирусная — программа компьютерная, предназначенная для защиты от вирусов компьютерных. Осуществляет обнаружение, восстановление, блокирование и/или удаление зараженных программных модулей и системных областей.
Virusga qarshi dastur - kompyuter viruslaridan himoyalashga mo'ljallangan kompyuter dasturi. Zaharlangan dasturiy modullarni va tizim sohalarini aniqlashni, tiklashni, blokirovka qilishni va/yoki yo'q qilishni amalga oshiradi.
Antivirus program - a computer program designed to protect the viruses from the computer. Detection, recovery, blocking and/or deleting infected software modules and system areas.

Виртуальная частная сеть - виртуальная сеть, построенная на основе существующих физических сетей, обеспечивающая безопасный туннель коммуникатsii для передачи данных или другой информатsii, передаваемой между сетями.
Virtual shaxsiy tarmoq - tarmoqlar orasida almashiniluvchi ma'lumotlar yoki boshqa axborotni uzatish uchun xavfsiz kommunikatsiya tunnelini ta'minlovchi, mavjud fizik tarmoqlar asosida qurilgan virtual tarmoq.
Virtual private network – a virtual network, built on top of existing physical networks that provides a secure communications tunnel for data and other information transmitted between networks.

Контроль доступа на основе ролей - модель для управления доступом к ресурсам, когда разрешенные действия на ресурсы идентифицированы с ролями, а не с личными идентификаторами субъекта.
Rollarga asoslangan ruxsatni nazoratlash - resurslardan foydalanishni boshqarish modeli bo'lib, resurslarda ruxsat berilgan harakatlar shaxsiy subyekt identifikatorining o'rniga rollar bilan identifikatsiyalanadi.
Role-based access control – a model for controlling access to resources where permitted actions on resources are identified with roles rather than with individual subject identities.

Конфиденциальность – 1. Некоторый класс данных, получение либо использование которых неавторизованными для этого лица не

может стать причиной серьезного ущерба для организатсии. 2. Свойство информатсии, состоящее в том, что она не может быть обнаружена и сделана доступной без разрешения отдельным лицам, модулям или процессам.

Konfidensiallik – 1. Avtorizatsiyalanmagan shaxs tomonidan olinishi yoki foydalanishi tashkilot uchun jiddiy zarar sababi bo'la olmaydigan ma'lumotlarning qandaydir sinfi. 2. Alohida shaxslar, modullar, jarayonlar ruxsatisiz aniqlanishi, va foydalanishi mumkin bo'lmagan axborot xususiyati.

Confidentiality – 1. Some class data, obtaining or the use of which by unauthorized persons could not cause serious damage to the organization. 2. The quality of information, consisting in that it cannot be detected and made available without the permission of individuals, modules or processes.

Менеджмент риска — полный процесс идентификатсии, контроля, устранения или уменьшения последствий опасных событий, которые могут оказать влияние на ресурсы информатсионно-телекоммуникатсионных технологий.

Risk menejmenti — axborot-telekommunikatsiya texnologiya resurslariga ta'sir etishi mumkin bo'lgan xavfli xodisalar oqibatlarini identifikatsiyalashning, nazoratlashning, bartaraf etishning yoki kamaytirishning to'liq jarayoni.

Risk management — the complete process of identification, control, eliminate or mitigate the consequences of hazardous events that may affect resources of information and telecommunication technologies.

Целостность - свойство информатсии, заключающееся в её существовании в неискаженном виде (неизменном по отношению к некоторому физическому её состоянию).

Yaxlitlik - axborotning buzilmagan ko'rinishda (axborotning qandaydir fizik holatiga nisbatan o'zgarmagan shaklda) mavjud bo'lishida ifodalangan xususiyati.

Integrity - the property of information, namely, its existence in an undistorted view (unchanged with respect to some physical condition).

MUNDARIJA

"Kriptografiya 2"

5330300 – Axborot xavfsizligi
yo'nalishi talabalari uchun o'quv qo'llanma.

Kriptologiya kafedrasi majlisida
ko'rib chiqildi va nashr etishga ruxsat etildi.
20__ yil __ _____
__ - sonli bayonnoma

"Kiberxavfsizlik" fakulteti UK majlisida
ko'rib chiqildi va nashr etishga ruxsat etildi.
20__ yil __ _____
___ - sonli bayonnoma

Muhammad al-Xorazmiy nomidagi
TATU O'UK majlisida
ko'rib chiqildi, nashr etishga va nashr
guvohnomasini olishga ruxsat etildi
20__ yil ___ _____
____ - sonli bayonnoma

Tuzuvchilar: Z.T.Xudoykulov, O.M.Allanov,
I.M.Boyquziyev, I.S.Olimov,
O.O.Tursunov, U.U.Tojiakbarova

Taqrizchilar: K.A.Tashev
M.M.Kadirov

Mas'ul muharrir: _____

Z.T.XUDOYKULOV, O.M.ALLANOV, I.M.BOYQUZIYEV, I.S.OLIMOV,
O.O.TURSUNOV, U.U.TOJIAKBAROVA

KRIPTOGRAFIYA 2

Muharrir: I. Tursunova
Badiiy muharrir: B. Haydarov
Kompyuter sahifalovchi: N. Fayziyeva
Korrektor: Sh. Hikmatova

Nashr. lits. AI № 276 15.06.2015.
Bosishga ruxsat etildi. 29.08.2023.
Bichimi 60x84 1/16 Offset qog'ozi.
Times New Roman garniturasi.
Shartli bosma tabog'i 11,75. Nashr hisob tabog'i 7,3.
Adadi 100 nusxada. Buyurtma № 13-11.

"LESSON PRESS" MCHJ nashriyoti.
100071. Toshkent, Komolon ko'chasi 13.

«ZUXRA BARAKA BIZNES» MChJ bosmaxonasida chop etildi.
Toshkent shahri Bunyodkor shoh ko'chasi 27 A–uy.