O’ZBEKISTON RESPUBLIKASI OLIY
VA O’RTA MAXSUS TA’LIM VAZIRLIGI

MIRZO ULUG’BEK NOMIDAGI
O’ZBEKISTON MILLIY UNIVERSITETI

M.M.Aripov, B.F.Abdurahimov, A.S.Matyakubov

KRIPTOGRAFIK USULLAR

Toshkent 2020

M.M. Aripov, B.F. Abdurahimov, A.S. Matyakubov. Kriptografik usullar. Toshkent. 2020 yil. 213 bet.

O‘quv qo‘llanmada axborotlarni himoyalashning kriptografik usullari ko‘rib chiqilgan. Simmetrik va nosimmetrik shifrlash tizimlari, elektron raqamli imzo, kalitlarni boshqarish, identifikatsiya sxemalari, kvant kriptografiyasi bo‘yicha ma’lumotlar taqdim etilgan.

O‘quv qo‘llanma 5113200-Amaliy matematika va informatika, 5330200-Informatika va axborot texnologiyalari (dasturiy ta’minot), 5330300-Axborot xavfsizligi (kompyuter tizimlari xavfsizligi) bakalavriat ta’lim yo‘nalishlari hamda mustaqil o‘rganuvchilar uchun mo‘ljallangan.

Taqrizchilar: **Kabulov A.** O’zbekiston Milliy universiteti, Axborot xavfsizligi kafedrasi professori

Xudoyqulov Z. Toshkent axborot texnologiyalari universiteti, Kriptologiya kafedrasi mudiri

Mazkur o‘quv qo‘llanma Mirzo Ulug’bek nomidagi O‘zbekiston Milliy universiteti Matematika fakulteti o‘quv-uslubiy kengashida ko‘rib chiqilgan va nashrga tavsiya etilgan.

Mazkur o‘quv qo‘llanma Mirzo Ulug’bek nomidagi O‘zbekiston Milliy universiteti o‘quv-uslubiy kengashida ko‘rib chiqilgan va nashrga tavsiya etilgan.

KIRISH

Axborot texnologiyalari bugungi kunda hayotimizning hamma sohalarini qamrab olgan. Axborot atrof-muhit ob'ektlari va hodisalari, ularning o'lchamlari, xususiyat va holatlari to'g'risidagi ma'lumotlardir. Keng ma'noda axborot insonlar o'rtasida ma'lumotlar ayirboshlash, odamlar va qurilmalar o'rtasida signallar ayriboshlashni ifoda etadigan umummilliy tushunchadir.

Bugungi kunda axborotning narxi ko'pincha u joylashgan kompyuter tizimi narxidan bir necha baravar yuqori turadi. Demak, axborotni ruxsatsiz foydalanishdan, atayin o'zgartirishdan, yo'q qilishdan va boshqa buzg'unchi harakatlardan himoyalash zaruriyati tug'iladi.

Axborot-kommunikatsiya tarmoqlarida Internet paydo bo'lganidan boshlab, axborot o'g'irlash, axborot mazmunini egasidan iznsiz o'zgartirib va buzib qo'yish, tarmoq va serverlardan beruxsat foydalanish, tarmoqqa tajovuz qilish, avval qo'lga kiritilgan uzatmalarni qayta uzatish, xizmatdan yoki axborotga daxldorlikdan bo'yin tovlash, jo'natmalarni ruxsat etilmagan yo'l orqali jo'natish hollari jahon miqyosida ko'paydi.

Axborot texnologiyalarni turli sohalarda qo'llash uchun ularning ishonchliligini va xafvsizligini ta'minlash kerak. Xavfsizlik deganda ko'zda tutilmagan vaziyatlarda bo'ladigan tashqi harakatlarda axborot tizimi o'zining yaxlitligini, ishlay olish imkoniyatini saqlab qolish xususiyati tushuniladi. Axborot texnologiyalarni keng miqyosda qo'llanilishi axborotlar xavfsizligini ta'minlovchi turli metodlarni, asosan kriptografiyaning gurkirab rivojlanishiga olib keldi. Rivojlangan davlatlar axborot-telekommunikatsiya tarmoqlarida maxfiy axborotlarni xavfsiz uzatish va elektron raqamli imzo yaratishda o'z milliy algoritmlaridan foydalanishmoqda. Shuni alohida ta'kidlash lozimki, bir davlat boshqa bir davlatga axborot-telekommunikatsiya texnologiyalarini eksport qilar ekan, ularning axborot muhofazasi tizimi yetarli darajada puxtalikka ega bo'lishiga kafolat berishi mushkul. Chunki, xorijga eksport qilinadigan dasturiy mahsulotlarda milliy standartlar qo'llanilmaydi. Bu hozirga kelib, O'zbekiston Respublikasida milliy kriptografik algoritmlarni yaratish va ularni

takomillashtirish muammolarini dolzarb qilib qo‘ydi.

Kriptografiya (kriptografiya – *kryptos* – maxfiy, *grapho* – yozish kabi grekcha so‘zlardan olingan) shifrlash usullari haqidagi fan sifatida paydo bo‘ldi va uzoq vaqt mobaynida shifrlash ya’ni, uzatiladigan va saqlanadigan axborotlarni ruxsat berilmagan foydalanuvchilardan himoyalashni o‘rganadigan fan sifatida shakllandi. Lekin, keyingi yillarda axborot texnologiyalarning gurkirab rivojlanishi maxfiy axborotlarni yashirish bilan to‘g‘ridan – to‘g‘ri bog‘liq bo‘lmagan ko‘pgina yangi kriptografiya masalalarini keltirib chiqardi.

Shifrlashning oddiy metodlaridan qadimgi davrlarda ham foydalanilgan. Lekin kriptografik metodlarni tadqiq etish va ishlab chiqishga ilmiy yondashish o‘tgan asrdagina (XX asr) paydo bo‘ldi. Ayni vaqtda kriptografiya ham fundamental, ham amaliy natijalar (teoremalar, aksiomalar) to‘plamiga ega. Jiddiy matematik tayyorgarlikka ega bo‘lmasdan turib kriptografiya bilan shug‘ullanib bo‘lmaydi. Xususan, diskret matematika, sonlar nazariyasi, abstrakt algebra va algoritmlar nazariyasi sohasidagi bilimlarni egallash muhimdir. Shu bilan birgalikda, kriptografik metodlar birinchi navbatda amaliy qo‘llanilishini esdan chiqarmaslik lozim. Chunki, nazariy jihatdan turg‘un hisoblangan algoritmlar, matematik modelda ko‘zda tutilmagan hujumlarga nisbatan himoyasiz bo‘lib qolishi mumkin. Shuning uchun, abstrakt matematik model tahlilidan so‘ng, albatta olingan algoritmni amaliyotda qo‘llanilishidagi holatlarini hisobga olgan holda uni yana tadqiq etish zarur.

I BOB. KRIPTOLOGIYA ASOSLARI

Shifrlash yordamida ma’lumotlarni himoyalash – xavfsizlik muammolarining muhim yechimlaridan biri. Shifrlangan ma’lumotga faqatgina uni ochish usulini biladigan kishigina murojaat qilish imkoniga ega bo‘ladi. Ruxsat etilmagan foydalanuvchi ma’lumotni o‘g‘irlashi hech qanday ma’noga ega emas.

Kriptografik uslublarning axborotlar tizimi muhofazasida qo‘llanishi ayniqsa hozirgi kunda faollashib bormoqda. Haqiqatan ham, bir tomondan kompyuter tizimlarida internet tarmoqlaridan foydalangan holda katta hajmdagi davlat va harbiy ahamiyatga ega bo‘lgan hamda iqtisodiy, shaxsiy, shuningdek boshqa turdagi axborotlarni tez va sifatli uzatish va qabul qilish kengayib bormoqda. Ikkinchi tomondan esa bunday axborotlarning muhofazasini ta’minlash masalalari muhimlashib bormoqda.

1.1. Asosiy tushunchalar

Axborotni himoyalashning matematik metodlarini o‘rganuvchi fan kriptologiya deb aytiladi.

Axborotlarning muhofazasi masalalari bilan *kriptologiya* (cryptos – mahfiy, logos – ilm) fani shug‘ullanadi. Kriptologiya maqsadlari o‘zaro qarama – qarshi bo‘lgan ikki yo‘nalishga ega:

- *Kriptografiya* va *kriptotahlil.*

Kriptografiya – axborotlarni aslidan o‘zgartirilgan holatga akslantirish uslublarini topish va takomillashtirish bilan shug‘illanadi.

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

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

1) Simmetrik kriptotizimlar.

2) Nosimmetrik, yoki yana boshqacha aytganda, ochiq kalit algoritmiga asoslangan kriptotizimlar.

3) Elektron raqamli imzo kriptotizimlari.

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

Kriptografik uslublardan foydalanishning asosiy yo‘nalishlari quyidagilar:

• mahfiy ma’lumotlarni ochiq aloqa kanali bo‘yicha muhofazalangan holda uzatish;

• uzatilgan ma’lumotlarning xaqiqiyligini ta’minlash;

• axborotlarni (elektron hujjatlarni, elektron ma’lumotlar jamg‘armasini) kompyuterlar tizimi xotiralarida shifrlangan holda saqlash va shular kabi masalalarning yechimlarini o‘z ichiga oladi.

Axborotlar muhofazasining kriptografik uslublari ochiq ma’lumotlarni asl holidan o‘zgartirib, faqat kalit ma’lum bo‘lgandagina uning asl holatiga ega bo‘lish imkoniyatini beradi.

Shifrlash va deshifirlash masalalariga tegishli bo‘lgan, ma’lum bir *alfavitda* tuzilgan ma’lumotlar *matnlarni* tashkil etadi.

Alfavit - axborotlarni kodlashtirish uchun foydalaniladigan chekli sondagi belgilar to‘plami. Misollar sifatida:

- ✓ o‘ttiz oltita belgidan (harfdan) iborat o‘zbek tili (kirill) alfaviti;
- ✓ o‘ttiz ikkita belgidan (harfdan) iborat rus tili alfaviti;
- ✓ yigirma sakkizta belgidan (harfdan) iborat lotin alfaviti;
- ✓ ikki yuzi ellik oltita belgidan iborat ASCII va KOI-8 standart kompyuter kodlarining alfaviti;
- ✓ binar alfavit, yani 0 va 1 belgilardan iborat bo‘lgan alfavit;
- ✓ sakkizlik va o‘n oltilik sanoq tizimlari belgilaridan iborat bo‘lgan alfavitlarni keltirish mumkin.

Matn – alfavitning elementlaridan (belgilaridan) tashkil topgan tartiblangan tuzilma.

Shifr deganda ochiq ma’lumotlar to‘plamini berilgan kriptografik almashtirishlar orqali shifrlangan ma’lumotlar to‘plamiga akslantiruvchi teskarisi mavjud bo‘lgan akslantirishlar majmuiga aytiladi.

Kriptografik tizim yoki shifr o‘zida ochiq matnni shifrlangan matnga akslantiruvchi teskarisi mavjud teskarilanuvchi akslantirishlar oilasiga aytiladi. Bu oilaning azolarini kalit deb nomlanuvchi songa o‘zaro bir qiymatli mos qo‘yish mumkin.

Shifrlash – ochiq matn, deb ataluvchi dastlabki ma’lumotni shifrlangan ma’lumot (kriptogramma) holatiga o‘tkazish jarayoni.

Deshifrlash - shifrlashga teskari bo‘lgan jarayon, ya’ni kalit yordamida shifrlangan ma’lumotni dastlabki ma’lumot holatiga o‘tkazish.

Kalit – bevosita dastlabki ma’lumotni shifrlash va deshifrlash uchun zarur bo‘lgan manba. U ma’lumotlarni kriptografik qayta o‘zgartirish algoritmi ayrim parametrlarining aniq maxfiy holati bo‘lib, bu algoritm uchun turli – tuman to‘plamdan bitta variantni tanlashini ta’minlaydi. Kalitning maxfiyligi shifrlangan matndan berilgan matnni tiklash mumkin bo‘lmasligini ta’minlaydi. K – kalitlar fazosi, bu mumkin bo‘lgan kalit qiymatlari to‘plamidir. Odatda kalit o‘zida alfavit harflari qatorini ifodalaydi. «Kalit» va «Parol» tushunchalarini farqlash lozim. Parol ham maxfiy alfavit harflari ketma – ketligi bo‘lib, u faqatgina shifrlash uchun emas, balki subyektni autentifikatsiya qilish uchun ham ishlatiladi.

Kriptotizimlar simmetrik va nosimmetrik (ochiq kalitli) kriptotizimlarga ajratiladi. Simmetrik kriptotizimlarda shifrlash va shifrni ochish uchun bitta va faqat bitta kalit qo‘llaniladi. Ochiq kalitli tizimlarda o‘zaro matematik bog‘langan ikkita kalit, ochiq va yopiq kalitlar qo‘llaniladi.

Axborot hamma uchun foydalanish mumkin bo‘lgan ochiq kalit yordamida shifrlanadi va faqatgina qabul qiluvchiga ma’lum bo‘lgan yopiq kalit orqali ochiladi. Kalitlarni taqsimlash va kalitlarni boshqarish terminlari kalitlarni ishlab chiqish va ularni foydalanuvchilar o‘rtasida taqsimlashdagi axborotlarga ishlov berish jarayonlariga tegishli.

Kalitlarni taqsimlash va *boshqarish* – kriptobardoshli kalitlarni ishlab chiqish (yoki yaratish), ularni muhofazali saqlash va kalitlarni foydalanuvchilar orasida muhofazalangan holda taqsimlash jarayonlarini o‘z ichiga oladi.

Elektron raqamli imzo – elektron matnga ilova qilinadigan kriptografik almashtirishdan iborat bo‘lib, shu elektron matn jo‘natilgan shaxsga qabul qilingan elektron matnning va matnni raqamli imzolovchining haqiqiy yoki soxta ekanligini aniqlash imkonini beradi.

Kriptobardoshlilik – shifrlash kaliti noma’lum bo‘lgan holda shifrlangan ma’lumotni deshifrlashning qiyinlik darajasini belgilaydi. Kriptobardoshlilikni belgilovchi bir nechta ko‘rsatkichlar mavjud, bulardan:

- deshifrlash uchun qidirilayotgan kalitlarning mumkin bo‘lgan barcha imkoniyatlari soni;
- deshifrlash uchun zarur bo‘lgan o‘rtacha vaqt.

Axborotlarni muhofazalash maqsadida shifrlashning sifati kalitning maxfiy saqlanishi va shifrlashning kriptobardoshlilik darajasiga bog‘liq.

Axborotlar tizimi muhofazasining zamonaviy kriptografik uslublariga quyidagi umumiy talablar qo‘yiladi:

- shifrlangan ma’lumotni asl nusxasiga ega bo‘lish imkoniyati faqat deshifrlash kaliti ma’lum bo‘lgandagina mumkin bo‘lsin;

foydalanilgan shifrlash kalitini shifrmatnning biror ma’lum qismi bo‘yicha yoki unga mos keluvchi ochiq qismi bo‘yicha aniqlash uchun bajarilishi zarur bo‘lgan amallar soni kalitni aniq topish uchun bajarilishi kerak bo‘lgan barcha amallar sonidan kam bo‘lmasligi, ya’ni kalitni tanlab olinishi kerak bo‘lgan to‘plam elementlarining sonidan kam bo‘lmasligi;

- shifrlash algoritmining ma’lumligi uning bardoshliligiga salbiy ta’sir ko‘rsatmasligi;
- kalitning har qanday darajadagi o‘zgarishi shifrlangan ma’lumotning jiddiy o‘zgarishiga olib kelishi;
- shifrlash algoritmining tarkibidagi elementlar o‘zgarmas bo‘lishi;
- shifirlash jarayoni davomida ma’lumotlarga kiritiladigan qo‘shimcha bitlar (elementlar) shifrlangan tekstda (ma’lumotda) to‘la va ishonchli holda qo‘llanilgan bo‘lishi;
- shifrlash jarayonida qo‘llaniladigan kalitlar orasida sodda va osonlik

bilan o‘rnatiladigan bog‘liqliklar bo‘lmasligi;

- kalitlar tarkibi to‘plamidan olingan ixtiyoriy kalit axborotlarning ishonchli muhofazasini ta’minlashi; kriptoalgoritm dasturiy hamda texnik jihatdan amaliy qo‘llanishga qulay bo‘lib, kalit uzunligining o‘zgarishi shifrlash algoritmining sifatsizligiga olib kelmasligi kerak.

Axborot – kommunikatsiya tarmoqlarida axborotlarni muhofazasini ta’minlashning kriptografik vositalari kriptografik algoritmlarning dasturiy taminoti va apparat-dasturiy qurilmalaridan iborat bo‘ladi. Nisbatan sodda, ammo kriptobardoshli bo‘lgan algoritmlarning apparat-texnik qurilmalari samarali qo‘llaniladi.

1.2. Axborot xavfsizligi kategoriyalari

Axborotxavfsizligi nuqtai nazaridan olib qaraganda axborotlarni quyidagi kategoriyalarga ajratish mumkin:

1. maxfiylik (konfidensiallik) - bu axborotlarning mo‘ljallangan

shaxslardan boshqasidan himoyalanganlik kafolati. Bu kategoriyaning buzulishi, axborotning o‘g‘irlanishi yoki fosh etilishi deyiladi;

2. butunlik – axborot uzatilganda yoki saqlanganda ko‘rinishining o‘zgarmaganlik kafolati. Bu kategoriyaning buzulishi soxtalashtirish deyiladi;

3. autentifikatsiya – foydalanuvchilarning haqiqiyligini aniqlash.

4. mualliflik – axborotda ko‘rsatilgan muallifning aynan o‘zi bo‘lishi kafolati;

5. qayta tekshirish – tekshirish natijasida muallifning aynan o‘zi bo‘lishini isbotlash.

Axborot xavfsizligi nuqtai nazaridan olib qaraganda axborot tizimlarini quyidagi kategoriyalarga ajratish mumkin:

1. ishonchlilik – tizim turlicha holatlar sodir bo‘lganda o‘zini qanday rejalashtirilgan bo‘lsa shunday tutishi kafolati;

2. aniqlik – barcha buyruqlarning aniq va to‘liq bajarilishi kafolati;

3. tizimga kirish nazorati – har xil guruhga mansub foydalanuvchilar

axborot obyektlariga kirish ruxsati turlicha bo‘lishi va bu cheklashlar har doim bajarilishi kafolati;

4. dastur nazorati – ixtiyoriy paytda dasturlar majmuasining ixtiyoriy komponentlari to‘laligicha tekshirilishi mumkinligi kafolati;

5. identifikatsiya nazorati – tizimga ayni paytda kirgan foydalanuvchining aynan o‘zi bo‘lishi kafolati;

6. atayin qilingan xatolarga nisbatan turg‘unligi – oldindan kelishilgan qoidalar chegarasida atayin qilingan xatolarga tizim o‘zini kelishilganidek tutishi kafolati.

Ushbu axborot xavfsizligi kategoriyalari kriptografiyaning asosiy yechilishi lozim bo‘lgan masalalaridir.

1.3. Simmetrik va ochiq kalitli (nosimmetrik) kriptotizimlar

Kriptotizimdan foydalanishda matn egasi shifrlash algoritmi va shifrlash kaliti vositasida avvalo dastlabki matnni shifrlangan matnga o‘giradi. Matn egasi uni o‘zi foydalanishi uchun shifrlagan bo‘lsa (bunda kalitlarni boshqaruv tizimiga hojat ham bo‘lmaydi) saqlab qo‘yadi va kerakli vaqtda shifrlangan matnni ochadi. Ochilgan matn asliga (dastlabki matn) aynan bo‘lsa, saqlab qo‘yilgan axborotning butunligiga ishonch hosil bo‘ladi. Aks holda axborot butunligi buzilgan bo‘lib chiqadi. Agar shifrlangan matn undan qonuniy foydalanuvchiga (oluvchiga) mo‘ljallangan bo‘lsa, u tegishli manzilga jo‘natiladi. So‘ngra shifrlangan matn oluvchi tomonidan unga avvaldan ma'lum bo‘lgan shifrochish kaliti va algoritmi vositasida dastlabki matnga aylantiriladi. Bunda kalitni qanday hosil qilish, aloqa qatnashchilariga bu kalitni maxfiyligi saqlangan holda yetkazish, va umuman, ishtirokchilar orasida kalit uzatilgunga qadar xavfsiz aloqa kanalini hosil qilish asosiy muammo bo‘lib turadi. Undan tashqari yana boshqa bir muammo – autentifikatsiya muammosi ham ko‘ndalang bo‘ladi. Chunki, dastlabki matn (xabar) shifrlash kalitiga ega bo‘lgan kimsa tomonidan shifrlanadi. Bu kimsa kalitning haqiqiy egasi bo‘lishi ham, begona (mabodo kriptotizimning siri ochilgan bo‘lsa) bo‘lishi ham mumkin. Aloqa

ishtirokchilari shifrlash kalitini olishganda u chindan ham shu kalitni yaratishga vakolatli kimsa tomonidan yoki tajovuzkor tomonidan yuborilgan bo‘lishi ham mumkin. Bu muammolarni turli kriptotizimlar turlicha hal qilib beradi.

Simmetrik kriptotizimda kalit aloqaning ikkala tomoni uchun bir xil maxfiy va ikkovlaridan boshqa hech kimga oshkor bo‘lmasligi shart. Bunday tizimning xavfsizligi asosan yagona maxfiy kalitning himoya xossalariga bog‘liq. Simmetrik kriptotizimlar uzoq o‘tmishga ega bo‘lsada, ular asosida olingan algoritmlar kompyuterlardagi axborotlarni himoyalash zarurati tufayli ba'zi davlatlarda standart maqomiga ko‘tarildilar. Masalan, AQShda ma'lumotlarni shifrlash standarti sifatida AES (Advanced Encryption Standart) algoritmi 2000 yilda qabul qilingan. Rossiyada unga o‘xshash standart GOST 28147-89 sifatida 128 bitli kalit bilan ishlaydigan algoritm 1989 yilda tasdiqlangan. Bular dastlabki axborotni 64 bitli bloklarga bo‘lib alohida yoki bir – biriga bog‘liq holda shifrlashga asoslanganlar. Algoritmlarning matematikaviy asosida axborot bitlarini aralashtirish, o‘rniga qo‘yish, o‘rin almashtirish va modul bo‘yicha qo‘shish amallari yotadi. Unda kirish va chiqishdagi matnlarning axborot miqdorlari deyarli bir xil bo‘ladi. Bunday tizimning xavfsizligi asosan maxfiy kalitning himoya xossalariga bog‘liq.

Simmetrik kriptotizimdan foydalanib elektron yozishmalar boshlash uchun avvalo maxfiy kalitni yoki parolni ikki aloqa ishtirokchisidan biri ikkinchisiga maxfiy holda yetkazishi kerak. Maxfiy kalitni yetkazish uchun maxfiy aloqa kanali(shaxsan uchrashish, himoyalangan aloqa kanali va sh.o‘.) kerak. Shunday qilib yopiq davra hosil bo‘ladi: maxfiy kalitni topshirish uchun maxfiy kanal kerak, maxfiy kanalni hosil qilish uchun maxfiy kalit kerak. Maxfiy kalit tez – tez o‘zgartirilib turilsa (aslida, har bir yozishmaga alohida maxfiy kalit ishlatilganda eng yuqori maxfiylikka erishiladi) bu muammo doimo ko‘ndalang bo‘laveradi.

Shifrlash va shifr ochish kalitlari o‘zaro funktsional bog‘langan bo‘lib ulardan biri asosida ikkinchisi amaliy jihatdan (mavjud hisoblash vositalari taraqqiyoti darajasida) hisoblab topilishi mumkin bo‘lmagan va ulardan biri

faqat bitta aloqa ishtirokchisiga ma’lum bo‘lib boshqalardan maxfiy tutiladigan, ikkinchisi esa aloqa ishtirokchilarining hammasiga oshkor bo‘lgan kriptotizim nosimmetrik (sinonimlari: ochiq kalitli, ikki kalitli) kriptotizim deb ataladi.

Nosimmetrik kriptotizim ikki kalitli tizim bo‘lib, unda aloqa ishtirokchilarining har biri o‘zining shaxsiy maxfiy va ochiq kalitlari juftiga ega bo‘lib o‘z ochiq kalitini boshqa aloqa ishtirokchilariga e’lon qiladi. Shaxsiy yopiq kalit qabul qilinadigan axborot pinhonligini ta’minlash uchun yaratilganda shifrni ochish kaliti bo‘lib xizmat qiladi. Bunda kimga pinhona axborot jo‘natiladigan bo‘lsa shuning ochiq kalitidan foydalanib shifrlangan axborot jo‘natiladi. Bunday axborotning shifrini faqat yagona yopiq kalit egasigina ocha oladi. Agar maxfiy kalit autentifikatsiya maqsadida jo‘natmalarga raqamli imzo bosish uchun hosil qilingan bo‘lsa, u shifrlash kaliti sifatida foydalaniladi. Ochiq kalit esa yuqoridagi birinchi holda shifrlash kaliti bo‘lib, ikkinchi holda shifrni ochish (tekshirib ko‘rish) kaliti bo‘lib xizmat qiladi.

Nosimmetrik kriptotizimlar asoslari simmetrik tizimlarda yechilmay qolgan kalit tarqatish va raqamli imzo muammolarining yechimini izlash yo‘llarida Massachuset texnologiya institutida U.Diffi (W.Diffie) va uning ilmiy rahbari M.Xellman (M.E.Hellman) tomonidan 1975 yilda taklif etilgan. 1977 yili shu tamoyil asosida o‘sha institutda R.Rivest, A.Shamir, L.Adlman (R.Rivest, A.Shamir, L.Adleman) tomonidan RSA algoritmi ishlab chiqildi. Keyinchalik elliptik va sh.o‘. bir tomonlama oson hisoblanadigan funksiyalar asosiga qurilgan boshqa algoritmlar yaratildi.

Nosimmetrik kriptotizimlar simmetrik kriptotizimlarga nisbatan o‘nlab marta ko‘proq axborot miqdoriga ega (512, 1024, 2048, 4096 bitli) kalitlardan foydalanadi va shunga ko‘ra yuzlab marta sekinroq ishlaydi. Nosimmetrik kriptotizimlarning matematik asosida bir tomonlama oson hisoblanadigan funksiyalar (darajaga oshirish, elliptik funksiya, rekursiya va sh.o‘.) yotadi.

Yashirin yo‘lli birtomonlama funksiyalardan foydalanilganda almashiladigan axborotlarni uzatish va raqamli imzo asosida autentifikatsiya muammosini yechish ham oson hal bo‘ladi. Bunday qulay funksiya turini

birinchi bo‘lib RSA algoritmining mualliflari taklif etishgan. Unda oshkora modul ikki tub sonning ko‘paytmasi bo‘lib, ko‘paytuvchilar sir tutiladi. Ko‘paytuvchilardan bitta kam sonlar ko‘paytmasi ikkinchi (mahfiy) modul bo‘lib, u ham sir tutiladi. Mahfiy modulga nisbatan o‘zaro teskari ikki sondan biri shaxsiy ochiq kalit, ikkinchisi shaxsiy yopiq kalit deb qabul qilinadi. Shu shaxsga yo‘llaniladigan axborot bloklari uning ochiq kalitida shifrlanib (modul bo‘yicha ochiq kalitga teng darajaga oshirib) jo‘natiladi. Qabul qilib olingan axborot bloklari shifri shu shaxsning shaxsiy yopiq kalitida ochiladi (modul bo‘yicha yopiq kalitga teng darajaga oshirib).

II BOB. AXBOROTLARNI HIMOYALASHNING KLASSIK USULLARI

Jamiyatda yozuvning ommalashuvi natijasida xat va xabarlarni almashishiga talab paydo bo‘lishi yozma ma’lumotlar mazmunini begona kishilardan yashirish zaruriyatini keltirib chiqardi. Yozma ma’lumotlar mazmunini yashirish uslubi uch guruhga bo‘linadi:

1. mavjud axborotni o‘zida yashirishni ta’minlovchi maskirovka yoki steganografiya metodlari;
2. maxfiy belgilar bilan xat yozish yoki kriptografiyaning turli metodlari;
3. axborotni maxfiylashtiruvchi maxsus texnik qurilmalarni tuzishga mo‘ljallangan metodlar.

2.1. Kriptografiya tarixi

Kriptografiya tarixi – insonlar tili tarixi bilan tengdoshdir. Bundan tashqari, dastlabki yozuvning o‘zi qadimgi jamiyatdan faqatgina tanlab olingan kishilargina foydalanishni bilgan o‘ziga xos kriptografik tizimdir. Maxfiy belgilar bilan xat yozishni rivojlanishiga urushlar katta turtki berdi. Yozma buyruqlar va xabarlar kur’er asirga olinsada dushman muhim axborotni qo‘lga kirita olmasligini ta’minlash uchun albatta shifrlangan. Tarixiy manbalarda keltirilishicha qadimgi sivilizatsiya bo‘lmish Misr, Hindiston va Mesopotamiyada so‘zlarni shifrlash va shifrlangan ma’lumotni o‘qish tizimlarining 64 turi mavjud bo‘lganligi aniqlangan. Manbalarda keltirilishicha maxfiy ma’lumot almashish erkak va ayol bilishi lozim bo‘lgan 64 san’atning biri bo‘lgan.

Axborotni shifrlashga doir yana ham aniq ma’lumotlar qadimgi Gretsiyaning paydo bo‘lish davrlariga borib taqaladi. Eramizdan oldingi 56 asrlarda Sparta davlatida yaxshi rivojlangan kriptografiya mavjud bo‘lgan. Ushbu davrlarga oid ikkita mashhur asbob, Sitala va Eniya jadvali mavjud bo‘lgan. Ular yordamida ochiq tekstdagi ma’lumot harflarini jadvaldagi harflarga maxsus qoidalarga binoan almashtirilar edi. Eniy o‘zining “Mudofaa

haqida” nomli asarida “Kitobli shifr” bobini yozgan, Polibiy esa “Polibiy kvadrati” nomli shifrlash metodini yozgan. Bu metod maxfiy ma’lumotdagi har bir harfni ikkita raqam bilan almashtirishni, bu raqamlar o‘z navbatida 5x5 kvadrat ichiga yozilgan mos harflar alfavit koordinatalari edi. Yuliy Sezar o‘zining “Gall urushi haqida qo‘lyozmalar” asarida, maxfiy ma’lumot harflarini uchta pozitsiya o‘ngga surish orqali shifrlash metodini keltirgan.

Shu davrda matematikaning asosi bo‘lgan manbalar, geometrik va algebraik hisob-kitob paydo bo‘lgan edi. Uchburchak va trapetsiyalarning yuzasini topish, kvadrat asosli piramidaning hajmini topish, oddiy tenglamalarni yechish usullari, Pifagor teoremasi va oddiy arifmetik progressiyaning yig‘indisini topish metodlari kashf qilingan. O‘sha davrlar kriptgografiyaning talabgorlari boshqaruv va diniy hokimiyat vakillari hisoblanar edi.

Arab davlatlarining uyg‘onish davrida (8 asr) kriptografiya yangi rivojlanish bosqichiga o‘tdi. 855 yilda “Qadimgi yozuv sirlarini ochishga insonning harakati haqidagi kitob” nomli qo‘llanma yaratildi. Bu qo‘llanmada shifr tizimlarning tariflari va bir qancha shifr alfavitlarning namunalari keltirilgan. 1412 yili “Shauba Al-Asha” nomli 14 tomdan iborat bo‘lgan ilmiy ensiklopediya yaratiladi. Bu ensiklopediyani tuzgan shaxs Shixob Al Kashkandi edi. “Shauba Al-Asha” da kriptografiyaga oid bo‘lim bo‘lib, unda barcha mashhur shifrlash usullariga ta’riflar keltirilgan. Ushbu bo‘limda kriptotahlil tizimining ochiq tekst va yopiq tekstlarning o‘zaro shifrlashga oid ma’lumotlari ham kiritilgan. O‘sha davr sharq matematikasi haqida gap ketganda, albatta bu o‘rinda yurtdoshimiz Al Xorazmiyning sonlar ustida arifmetik amallar haqidagi asari “Al-jabr val- muqobala”ni keltirishimiz mumkin. “Algebra” so‘zi ushbu asarning nomidan kelib chiqqan. Olimning nomi esa fanda “Algoritm” shaklida fanda abadiy o‘rnashgan.

Kriptografiya tarixini shartli ravishda to‘rtta bosqichga ajratish mumkin: sodda, formal (rasmiy), ilmiy, kompyuterli.

Sodda kriptografiya (XV asr boshlarigacha) uchun shifrlangan matn mazmuniga nisbatan dushmanni chalkashtiruvchi ixtiyoriy, odatda sodda

usullarning qo‘llanilishi xosdir. Dastlabki bosqichda axborotni himoyalash uchun kodlashtirish va steganografiya usullari qo‘llanildi. Qo‘llaniladigan shifrlarning aksariyati joyini o‘zgartirish va bir alfavitli o‘rin almashtirishga kelar edi. Birinchi bo‘lib qayd qilingan shifrlardan biri berilgan matndagi har bir harfni alfavit bo‘yicha aniqlangan sondagi o‘ringa siljitish asosida ishlovchi almashtirish Sezar shifridir. Boshqa shifr, grek yozuvchisi Polibian muallifligiga tegishli Polibian kvadratidir. Bu usulda alfavitning kvadrat jadvali (grek alfaviti 5x5 o‘lchamda bo‘ladi) yordamida tasodifiy ravishda to‘ldirilgan. Joriy tekstdagi har bir harf kvadratda undan pastda turgan harf bilan almashtiriladi.

Rasmiy kriptografiya (XV asr oxiridan XX asr boshlarigacha) bosqichi rasmiylashgan va qo‘lda bajariluvchi shifr kriptotahlilini paydo bo‘lishi bilan bog‘liq. Yevropa davlatlarida bu Tiklanish davriga to‘g‘ri keldi. Bunda fan va savdoni rivojlanishi axborotni himoyalashni ishonchli usuliga bo‘lgan talabni oshirdi. Bu bosqichdagi muhim rol birinchilardan bo‘lib, ko‘p alfavitli almashtirishni taklif etgan italiyalik arxitektor Leon Batista Albertiga tegishlidir. XVI asr diplomati Blez Vijiner nomidan olingan joriy shifr joriy matn harflarini kalit (bu protsedurani maxsus jadvallar yordamida osonlashtirish mumkin) bilan ketma-ket «qo‘shish» dan tashkil topgan. Uning «Shifr haqida traktat» nomli ishi kriptologiyada birinchi ilmiy ish hisoblanadi. Dastlabki chop etilgan ishlardan biri o‘sha vaqtda taniqli bo‘lgan shifrlash algoritmini umumlashtirgan va ta’riflagan nemis abbati Iogann Trisemusga tegishlidir. U ikkita uncha katta bo‘lmagan, lekin juda muhim bo‘lgan polibian kvadratini to‘ldirish usuli (kvadratning birinchi pozitsiyalari kalit so‘zlar, qolganlari esa alfavitning boshqa harflari bilan to‘ldiriladi) va hafrlar juftligi (bigramma) orqali shifrlash usullarini yaratdi. Ko‘p alfavitli almashtirishni oddiy, lekin chidamli bo‘lgan usuli bo‘lgan Pleyfer shifri XIX asr boshlarida Charlz Uitston tomonidan yaratildi. Uistonga yana «Ikkilik kvadrat» nomli takomillashgan shifrlash usuli ham tegishlidir. Pleyfer va Uiston shifrlari birinchi jahon urushiga qadar ishlatildi. Chunki ular qo‘l orqali bajariladigan kriptotahlilga yetarlicha qiyinchilik tug‘dirar edi.

XIX asrda gollandiyalik Kerkxoff kriptografik tizimlar uchun hozirgacha

dolzarb bo‘lgan, «shifrlarning maxfiyligi algoritmlarning maxfiyligiga emas, balki kalitning maxfiyligiga asoslanishi kerak» degan bosh talabni shakllantirdi. Natijada yaratilgan usullar nisbatan yuqori kriptobardoshlilikni ta’minladi va shifrlash jarayonini avtomatlashtiruvchi (mexanizatsiyalash ma’nosida) rotorli kriptotizimlarni yaratilishiga olib keldi. Yana shunga o‘xshash tizimlardan biri 1790 yilda AQSh ning bo‘lg‘usi prezidenti Tomas Jeferson tomonidan yaratildi. Bunda rotorli mashina yordamida ko‘p alfavitli almashtirish amalga oshirilar edi. Rotorli mashinalar XX asrning boshlaridagina amaliyotga keng tarqaldi. Dastlabki amaliyotda qo‘llanilgan mashinalardan biri nemis «Enigma»si bo‘lib, u 1917 yilda Edvard Xebern tomonidan ishlab chiqilgan va Artur Kirx tomonidan takomillashtirilgan. Tuzilishiga ko‘ra “Enigma” oddiy avtomobil odometrini eslatardi: uchta rotordan (shifrdisk) iborat bo‘lib, elektr moslamalar yordamida oldinma keyin joylashgan edi. Operator ochiq tekstdagi biror bir harfni qurilmaga yozmoqchi bo‘lsa, qurilmadagi mos klavishani bosishi kerak bo‘lar edi. Klavisha bosilganidan so‘ng signal uchta shifrdiskda joylashgan aloqa tugmalaridan o‘tadi. Shundan so‘ng hosil bo‘lgan ma’lumot reflektor bo‘limiga o‘tar, undan esa boshqa yo‘l “elekt yo‘l” orqali ortga qaytar edi. Shundan so‘ng birinchi disk bir pozitsiyaga o‘zgarar edi. Shu sababdan kiritilayotgan keyingi harfning shifri butunlay boshqa qoidaga asosan hosil bo‘lar edi. Operator 26 ta harfni kiritganidan so‘ng birinchi disk o‘zining boshlang‘ich holiga qaytar, ammo ikkinchi disk bir pozitsiya o‘zgarar edi. “Enigma” qurilmasi yordamida ma’lumotni tezda shifrlash uchun to‘rt kishidan iborat brigada guruhi zarur edi: birinchisi ochiq tekstni o‘qib turgan, ikkinchisi tekstni klaviatura yordamida terib turgan, uchinchisi indikatordan chiqqan shifrlangan ma’lumotni o‘qib turgan, to‘rtinchisi esa o‘qilayotgan shifrtekstni telefon yoki boshqa qurilmalar orqali uzatib turgan. “Enigma” shifr tekstlarining kalitlari bo‘lib rotorlarning boshlang‘ich holi va elektron kommutatsiya zanjirlari keltirilar edi. Kalitlarni topish kombinatsiyasining ehtimoli 92 ta nollardan iborat bo‘lgan raqam edi.

Rotor mashinalar ikkinchi jahon urushi vaqtida faol ishlatildi. Enigma nemis mashinasidan tashqari Sigaba (AQSh), Typex (Buyuk Britaniya), Red,

Orangle va Purple (Yaponiya) kabi qurilmalar ham amaliyotda keng qo‘llanildi. Rotorli tizimlar - formal kriptografiyaning cho‘qqisi edi. Bunda juda chidamli shifrlar oson amalga oshirilgan edi. Rotorli tizimlarga 40-yillarda EHM laming paydo bo‘lishi bilan muvaffaqqiyatli kriptografik hujum qilish imkoni paydo bo‘ldi.

Ilmiy kriptografiyaning (1930-60 yillar) boshqalardan ajralib turadigan tomoni - kriptobardoshliligi qat’iy tarzda matematik formulalar orqali asoslangan kriptografik tizimlarning paydo bo‘lishidir. 30-yillarning oxirlarida kriptologiyaning ilmiy asoslari bo‘lgan matematikaning alohida bo‘limlari: ehtimollar nazariyasi va matematik statistika, umumiy algebra, sonlar nazariyasi, axborotlar nazariyasi, kibernetika shakllandi. Algoritmlar nazariyasi aktiv tarzda rivojlandi. Klod Shennonning «Maxfiy tizimlarda aloqa nazariyasi» (1949) ishi o‘ziga xos chegara bo‘lib, kriptografiya va kriptotahlilning ilmiy asoslariga zamin yaratdi. Shu vaqtdan boshlab, kriptologiya - axborot maxfiyligini ta’minlash uchun qayta o‘zgartirish haqidagi fan to‘g‘risida so‘z yuritila boshlandi. Kriptografiya va kriptotahlilni 1949 yilgacha rivojlanish bosqichini ilmiy kriptologiyagacha bo‘lgan davr deb atash mumkin. Shennon «sochilish» va «aralashtirish» kabi tushunchalarni kiritdi va yetarlicha mustahkam kriptotizimlarni tuzish imkonini asosladi.

1960 yillardan boshlab, yetakchi kriptografik maktablar, rotorli kriptotizimlar bilan taqqoslaganda ancha mustahkam bo‘lgan, lekin amaliyotda faqatgina raqamli elektron qurimalardagina bajariladigan blokli shifrlarni tuza boshladilar.

Kompyuter kriptografiyasiga (1970-yillardan boshlab) «qo‘lda bajariladigan» va «mexanik» shifrlardan bir necha barobar katta kriptobardoshlilikka ega bo‘lgan shifrlashni katta tezlik bilan bajarilishini ta’minlovchi samarali hisoblash vositalarini paydo bo‘lishi bilan asos solindi.

Blokli shifrlar qudratli va kompakt hisoblash vositalari paydo bo‘lishi bilan amaliyotda qo‘llanilgan dastlabki kriptotizimlar sinfidir. 1970 yilda DES Amerika Qo‘shma Shtatlari shifrlash standarti ishlab chiqildi (1978 yilda qabul

qilindi). Uning mualliflaridan biri Xorst Feystel (IBM xodimi) boshqa simmetrik kriptografik tizimlar uchun ham asos bo‘ladigan blokli shifrlash modelini tavsifladi. Xuddi shu model asosida boshqa shifrlash modellariga nisbatan mustahkamroq bo‘lgan GOST 28147-89 simmetrik kriptotizimi yaratilgan.

DES ning paydo bo‘lishi bilan kriptotahlil ham ancha boyidi, amerika algoritmiga hujum qilish kriptotahlilning bir nechta ko‘rinishlari (chiziqli, differentsial va boshqalar) tuzildi. Ularning amaliyotda qo‘llanilishi faqatgina qudratli hisoblash tizimlarini paydo bo‘lishi bilan amalga oshishi mumkin. XX asrning 70 - yillarining o‘rtalariga kelib maxfiy kalitni tomonlarga uzatishni talab qilmaydigan nosimmetrik kriptotizimlarning paydo bo‘lishi bilan zamonaviy kriptografiyada haqiqiy burilish yuz berdi. Bunda 1976 yilda Uitfild Diffi va Martin Xellman tomonidan nashr qilingan «Zamonaviy kriptografiyaning yangi yo‘nalishlari» nomli ishi asosiy hisoblanadi. Bu ishda birinchi bo‘lib, shifrlangan axborotni maxfiy kalitni o‘zaro almashmasdan uzatish tamoyillari shakllantirilgan. Ularga bog‘liq bo‘lmagan holda Ralf Merkl ham nosimmetrik kriptotizimlar g‘oyasini ishlab chiqdi. Bir necha yillardan keyin Ron Rivest, Adi Shamir va Leonard Adlemanlar birinchi amaliy nosimmetrik kriptografik tizim bo‘lgan, katta tub sonlarni faktorizatsiyasi muammosiga asoslangan RSA tizimini ixtiro qilishdi. Nosimmetrik kriptografiyada darhol bir nechta yangi amaliy yo‘nalishlar, xususan elektron raqamli imzo (ERI) va elektron pul to‘lovi yo‘nalishlari ochildi.

1980-90 yillarda kriptografiyaning mutlaqo yangi yo‘nalishlari: ehtimolli shifrlash, kvant kriptografiyasi va boshqalar paydo bo‘ldi. Ularning amaliy qiymatini tushinish hali oldinda. Simmetrik kriptotizimlarni takomillashtirish ham haligacha dolzarb masala bo‘lib qolmoqda. Bu davr ichida feystel to‘riga ega bo‘lmagan shifrlar (SAFER, RC6 va boshqalar) yaratildi. 2005 yildan boshlab O‘zbekistonda ham yangi milliy shifrlash va raqamli imzo standartlari qabul qilindi.

Kriptografiya axborot konfidentsialligi va yaxlitligini nazorat qilishni ta’minlovchi hamma narsadan ko‘ra qudratli vositadir. Ko‘pgina munosabatlarda

u xavfsizlikning dasturiy – texnik boshqaruvchilari o‘rtasida markaziy o‘rin egallaydi. Masalan, portativ kompyuterlarda, ma’lumotlarni jismoniy himoyalash juda qiyin, faqatgina kriptografiya hatto axborot o‘g‘irlanganda ham uning konfidentsialligini kafolatlash imkonini beradi.

2.2. Kalit so’zli jadval almashtirishlar

O‘rin almashtirish shifrlari tanlangan o‘rin almashtirish kaliti (qoidasi)ga mos holda matndagi harflar guruhini qayta tartiblaydi. Buning uchun oddiy shifrlash protsedura (kalit)larini beruvchi maxsus jadvallardan foydalaniladi. Unga ko‘ra xabardagi harflar o‘rnini almashtirish amalga oshirilgan. Bunday jadvaldagi kalit sifatida jadval o‘lchamlari hamda almashtirish yoki jadvalning boshqa maxsus xususiyatlarini beruvchi iboralar xizmat qiladi.

Kalit so‘zi oltita harfdan kam bo‘lmasligi va bu so‘zda har bir harf faqat bir marotaba ishtirok etishi kerak. Masalan, kalit so‘z – sevinch, shifrlanadigan matn “O‘zbekiston kelajagi buyuk davlatdir” bo‘lsin.

Matnni shifrlash:

1.1. Jadvalning birinchi satriga kalit so‘z yoziladi;

1.2. Ikkinchi satridan boshlab matn yozib chiqiladi;

1.3. Jadvalning bo‘sh qolgan qismini bir xil belgi bilan to‘ldirib chiqiladi (bu holda x harfi bilan);

s	e	v	i	N	c	h
o	.	z	b	E	k	i
s	t	o	n	K	e	l
a	j	a	g	I	b	u
y	u	k	d	A	v	l
a	t	d	i	r	x	x

1.4. Kalitdagi harflarning alfavitdagi tartib raqamlari yozib chiqiladi;

s-	e-4	v-	i-8	n-	c-2	h-7
o	*C.*	z	b	e	k	i
s	T	o	n	k	e	l
a	j	a	g	i	b	u
y	U	k	d	a	v	l
a	T	d	i	r	x	x

1.5. Kalit harflarining tartib raqamlari bo‘yicha o‘sish taribida ustunlar tartiblanadi;

2	4	7	8	13	18	21
k	.	i	b	e	o	z
e	t	l	n	t	s	o
b	j	u	g	i	a	a
v	u	l	d	a	y	k
x	t	x	i	r	a	d

1.6. Ushbu jadvaldagi harflar gorizontal ketma-ketlikda yoziladi va matnning shifri hosil bo‘ladi. C - “k’ibeozetlntsobjugiaavuldaykxtxirad”.

Shifrlangan matnni ochish:

2.1. Shifrlangan matn gorizontal ketma-ketlikda jadvalga yoziladi;

k	‘	i	b	e	o	z
e	t	l	n	t	s	o
b	j	u	g	i	a	a
v	u	l	d	a	y	k
x	t	x	i	r	a	d

2.2. Kalitdagi harflarning harfini tartib raqamini yozib s-18, e-4, v-21, i-8, n-13, c-2, h-7 jadvalning 1 satriga o‘sish tartibida yoziladi;

c-2	e-4	h-7	i-8	n-	s-18	v-
k	‘	i	b	e	o	z
e	t	l	n	t	s	o
b	j	u	g	i	a	a
v	u	l	d	a	y	k
x	t	x	i	r	a	d

2.3. Kalit harflariga mos ravishda ustunlar tartiblanadi;

s-18	e-4	v-21	i-8	n-13	c-2	h-7
o	‘	z	b	e	k	i
s	T	o	n	k	e	l
a	J	a	g	i	b	u
y	U	k	d	a	v	l
a	T	d	i	r	x	x

2.4. Ushbu jadvaldagi harflar gorizontal ketma-ketlikda yoziladi va ochiq matn hosil bo‘ladi: “O‘zbekiston kelajagi buyuk davlatdir”

Nazorat uchun savollar:

1. Kalit so‘zga qanday shartlar qo‘yiladi?
2. Kalit so‘z jadvalning qaysi qismiga yoziladi?
3. Shifrlanadigan matn jadvalga qaysi tartib bilan yoziladi?
4. Shifrlanadigan matn jadvalning barcha kataklarini to‘ldirmasa nima qilinadi?
5. Jadval kataklari qaysi qoidaga asosan almashtiriladi?
6. Kalit so‘z har ikkala tomonda ham bo‘lishi shartmi?

2.3. Kalit sonli jadval almashtirishlar

Kalit sifatida 2 ta son olinadi. Har bir sonda raqamlar takrorlanmasligi

kerak. 1- yozilgan son gorizontal kalit, 2-yozilgan son vertikal kalit sifatida ishlatiladi. Birinchi son birinchi satrga yoziladi, ikkinchi son birinchi ustunga yoziladi. Ochiq matn shu jadval o‘lchamiga mos qilib tuziladi. Agar matn katta bo‘lsa, bloklarga ajratiladi.

Shifrlash: Masalan, kalit ”364512, 76815”, ochiq matn ”Axborotni himoyalash usullari fan” bo‘lsin. 6x7 jadval chiziladi, gorizontal kalit birinchi satrga yoziladi, vertikal kalit birinchi ustunga yoziladi, matn gorizontal tarzda jadval ichiga yozib chiqiladi.

	3	6	4	5	1	2
7	A	x	b	o	r	o
6	T	n	i	h	i	m
8	O	y	a	l	a	s
1	H	u	s	u	l	l
5	A	r	i	f	a	n

1.1. Gorizontal kalit bo‘yicha ustunlarni o‘sish tartibida joylashtiriladi;

	1	2	3	4	5	6
7	r	o	a	b	o	x
6	I	m	t	I	h	n
8	a	s	o	a	l	y
1	l	l	h	s	u	u
5	a	n	a	i	f	r

1.2 . Vertikal kalit bo‘yicha satrlarni o‘sish tartibida joylashtiriladi;

1	L	l	h	s	u	u
5	A	n	a	i	f	r
6	L	m	t	l	h	n
7	R	o	a	b	o	x
8	A	s	o	a	l	y

1.3. Ushbu jadvaldagi harflar gorizontal ketma-ketlikda yoziladi va

shifrlangan matn hosil bo‘ladi. Shifrlangan matn - ”llhsuuan aifr lmtl hnroab oxasoaly” .

Shifrlangan matnni ochish:

2.1. 6x7 jadval chiziladi, gorizontal kalit birinchi satrga raqamlarining o‘sish tartibida yoziladi, vertikal kalit birinchi ustunga raqamlarining o‘sish tartibida yoziladi, shifrlangan matn gorizontal tarzda jadval ichiga yozib chiqiladi;

	1	2	3	4	5	6
1	L	l	h	s	u	u
5	A	n	a	i	f	r
6	L	m	t	l	h	n
7	R	o	a	b	o	x
8	A	s	o	a	l	y

2.1. Vertikal kalit o‘z holiga keltiriladi, shu bilan satrlar o‘rni almashadi.

7	R	o	a	b	o	x
6	I	m	t	I	h	n
8	A	s	o	a	l	Y
1	L	l	h	s	u	u
5	A	n	a	i	f	r

2.2. Gorizontal kalit o‘z holiga keltiriladi, shu bilan ustunlar o‘rni almashadi;

3	6	4	5	1	2
A	x	b	o	r	o
T	n	i	h	i	m
O	y	a	l	a	s
H	u	s	u	l	l
A	r	i	f	a	n

2.3. Hosil bo‘lgan jadvaldagi harflar gorizontal ketma-ketlikda yoziladi va ochiq matn hosil bo‘ladi. Ochiq matn: ”Axborotni himoyalash usullari fan”.

Nazorat uchun savollar:

1. Kalit sonlarga qanday shartlar qo‘yiladi?
2. Kalit sonlar jadvalning qaysi qismiga yoziladi?
3. Shifrlanadigan matn jadvalga qaysi tartib bilan yoziladi?
4. Shifrlanadigan matn jadvalning barcha kataklarini to‘ldirmasa nima qilinadi?
5. Jadval kataklari qaysi qoidaga asosan almashtiriladi?
6. Kalit sonlar har ikkala tomonda ham bo‘lishi shartmi?

2.4. Sehrli kvadrat usuli

Satr va ustun sonlari teng bo‘lgan jadval chiziladi. Jadval kataklari 1 sonidan boshlab ketma-ket natural sonlar bilan to‘ldiriladi. Bunda agar kataklar ichidagi sonlarni gorizontal, vertikal va diagonal yig‘indisi hisoblanganda bir xil son chiqsa sehrli kvadrat deyiladi.

Masalan, 3X3 jadval olaylik. Bunda gorizontal, vertikal va diagonal kataklar ichidagi sonlarni gorizontal, vertikal va diagonal yig‘indisi hisoblanganda bir xil son chiqsa sehrli kvadrat deyiladi.

8	1	6
3	5	7
4	9	2

Yig‘indi quyidagi formula orqali topiladi: n, bu yerda $S = \frac{1+n^2}{2} \cdot n$, n – jadval o‘lchami.

Shifrlash: Sehrli kvadratlar usulida M=“s t i p e n d i a” so‘zini shifrlaymiz. Bunda harflarning matnda kelish tartibini sonlar bilan yozamiz: s-1, t-2, i-3, p-4, e-5, n-6, d-7, i-8, a-9. Jadvaldagi sonlar o‘rniga mos keluvchi harflarni yoziladi:

i	s	n
i	e	d
P	a	t

Gorizontal tarzda matnni yozib chiqamiz: “isniedpat” - shifrtekst hosil bo‘ladi.

Shifrni ochish: Jadval ichiga shifrtekst gorizontal tarzda yozib chiqiladi.

8 i	1 s	6 n
3 i	5 e	7 d
4 p	9 a	2 t

Sonlarni o‘sish tartibida yozib chiqib, shunga mos harflar yozib chiqiladi, “stipendia” so‘zi hosil bo‘ladi.

Bu usullarning asosiy kamchiliklaridan biri tekstni jadvallarga karrali qilib tanlash kerak bo‘ladi.

Nazorat uchun savollar:

1. Sehrli kvadratlar usulida kalit nimadan iborat?
2. Sehrli kvadrat qurishning qanday usullarini bilasiz?
3. Shifrlanadigan matn jadvalga qaysi tartib bilan yoziladi?
4. Shifrlanadigan matn jadvalning barcha kataklarini to‘ldirmasa nima qilinadi?
5. Kalit har ikkala tomonda ham bo‘lishi shartmi?

2.5. Sezar shifri

Almashtirish usullari sifatida quyidagi usullami keltirish mumkin: Sezar usuli, Affin tizimidagi Sezar usuli, tayanch so‘zli Sezar usuli va boshqalar.

Sezar usulida almashtiriluvchi harflar k soniga siljishi bilan aniqlanadi. Yuliy Sezar bevosita k=3 bo‘lganda ushbu usuldan foydalangan.

k = 3 bo‘lganda va alfavitdagi harflar m = 26 ta bo‘lganda quyidagi jadval hosil qilinadi:

Siljimagan alfavit	Siljigan alfavit	Siljimagan alfavit	Siljigan alfavit	Siljimagan alfavit	Siljigan alfavit
A	*D*	J	*M*	S	*V*
V	*E*	K	*N*	T	*W*
C	*F*	L	*O*	U	*X*
D	*G*	M	*P*	V	*Y*
E	*H*	N	*Q*	W	*Z*
F	*I*	O	*R*	X	*A*
G	*J*	P	*S*	Y	*B*
H	*K*	Q	*T*	Z	*C*
I	*L*	R	*U*		

Masalan, matn sifatida KOMPYUTER so‘zini oladigan bo‘lsak, Sezar usuli natijasida quyidagi shifrlangan yozuv hosil bo‘ladi:

C = NRPSBXWHU.

Sezar usulining kamchiligi bu bir xil harflarning o‘z navbatida, bir xil harflarga almashishidir.

Misol.

Bizga k-kalit, m-harflar soni, t-harflarning alfavitdagi tartib raqami, x-shifrlangan harf, M-shifrlanuvchi so‘z berilgan bo‘lsin.

(t+k) mod m = x ^shifrlash formulasi; (x-k) mod m = t ^shifrni ochish formulasi; Shifrlash:

M-’doska”;

K=3;

M=26;

d: (3+3) mod 26=6 ^g o: (14+3) mod 26=17 ^r s: (18+3) mod 26=21 ^v k: (10+3) mod 26=13 ^n a: (0+3) mod 26=3 ^d

c=”grvnd”;

Shifrni ochish:

g: (6-3) mod 26=3 ^d r: (17-3) mod 26=14 ^o v: (21-3) mod 26=17 ^s n: (13-3) mod 26=10 ^k d: (3-3) mod 26=0 ^a

M=”doska”

Nazorat uchun savollar:

1. Sezar usulida kalit nimadan iborat?
2. Kalit qaysi sondan qaysi songacha oraliqda bo‘ladi?
3. Shifrlanadigan matn harflari qaysi tartib bilan nomerlanadi?
4. Shifrlangan matnni ochishda modulda manfiy son chiqsa nima qilinadi?
5. Kalit har ikkala tomonda ham bo‘lishi shartmi?
6. Kalitsiz qanday ochish mumkin?

2.6. Affin tizimi

Affin tizimidagi Sezar usulida har bir harfga almashtiriluvchi harflar maxsus formula bo‘yicha aniqlanadi: (at+b) mod m, bu yerda a, b - butun sonlar, 0<a, b<m, a va m o‘zaro tub sonlar. t - harflarning alfavitda joylashgan tartibi (0 dan boshlab tartiblanadi), m - alfavitdagi harflar soni.

m=26, a=3, b=5 bo‘lganda, Shunga mos ravishda harflar quyidagi jadval hosil qilinadi: quyidagicha almashadi:

A	F
B	J
C	N
D	R
E	S
F	V
G	Z
H	D

t	3t+5
0	5
1	8
2	11
3	14
4	17
5	20
6	23
7	26
8	29
9	32
10	35
11	38
12	41
13	44
14	47
15	50
16	53
17	56
18	59
19	62
20	65
21	68
22	71
23	74
24	77
25	80
26	83

I	H
J	L
K	P
L	T
M	X
N	B
O	F
P	J
Q	N
R	R
S	V
T	Z
U	D
V	H
W	L
X	P
Y	T
Z	X

Natijada yuqorida keltirilgan matn quyidagicha shifrlanadi: C=PFXJDZSR

Shifrni ochish formulasi quyidagicha: $M = (a\sim^{1}(C — b))mod\ m.$ Bu yerda a^{-1} qiymat a sonining mod m bo‘yicha teskarisi, C - shifrtekst.

Nazorat uchun savollar:

1. Affin usulida kalit nimadan iborat?
2. Kalit qaysi sondan qaysi songacha oraliqda bo‘ladi?
3. Shifrlanadigan matn harflari nomerlanish tartibi qanday?
4. Shifrlangan matnni ochishda modulda manfiy son chiqsa nima qilinadi?
5. Kalit har ikkala tomonda ham bo‘lishi shartmi?
6. Kalitsiz qanday ochish mumkin?

2.7. Steganografiya

Steganografiya (grekcha axsyavoa – yashirin va $\gamma\rho\alpha\varphi\omega$ – yozayapman, sirli yozuv degan manoni anglatadi) – bu ochiq ma’lumotni uzatilayotgan vaqtda shifrni yoki sirni ichiga joylashtirib uzatishni o‘rganuvchi fan hisoblanadi.

Kriptografiyada shifr yoki sirli xabarning ko‘rinishi mavjud bo‘ladi, steganografiyada esa u ham sir saqlanadi. Steganografiyani, odatda, kriptografiya metodlari bilan birgalikda qo‘llaniladi va ular bir birini to‘ldiradi deyish mumkin.

90-yillar oxirida steganografiyaning bir nechta yo‘nalishlari qayd etildi:

- Klassik steganografiya
- Kompyuter steganografiyasi
- Raqamli steganografiya

Klassik steganografiya

Qadimgi dunyo steganografiyasi

Yunon tarixchisi Gerodotning keltirishicha, axborotni yashirishning bir necha xil usullari mavjud bo‘lgan. Misol uchun, ular qullarning boshiga kerakli axborotni yozishgan, qulning sochi o‘sgach esa u manzilga jo‘natilgan. Manzilga yetgach uning sochi olinib, ma’lumot yetib borgan deya hisoblangan.

Maxsus (ko‘rinmas) siyoh usuli

Klassik steganografiyaning keng tarqalgan usullaridan biri bu maxsus(ko‘rinmas) siyoh usulidir. Bunday siyohlarda yozilgan matn faqatgina maxsus sharoitlarda qog‘ozda paydo bo‘lgan (isitish, yoritish va kimyoviy qorishma qo‘shish kabi). Bu usul I asrda Aleksandr Felono tomonidan kashf etilgan bo‘lib, o‘rta asrlarda ham ishlatilgan. Qog‘ozga qatorlar orasiga sut bilan yozilsa, sut esa qog‘oz olovda qizdirilganda ko‘rinishi haqidagi usul ham mavjud.

Boshqa steganografik usullar

Ikkinchi jahon urushi paytida *mikronuqta* usuli keng qo‘llanilgan, bu mikronuqtalar mikroskopik fotosuratlar bo‘lib, ular telegramma va xatlarning matnlariga joylashtirilgan.

Bundan tashqari yana quyidagi axborotni himoyalash usullari mavjud bo‘lgan:

- Xaritaning orqa qismiga uning tartibi bo‘yicha xabar yozish;
- Qaynatilgan tuxum ichiga matn yozish va h.k ;

Hozirgi kunda steganografiyani axborotni matnli, grafik yoki audio ko‘rinishda yashirishning maxsus dasturiy ta’minotini ishlatish usuli deya tushunish mumkin.

Kompyuter steganografiyasi

Kompyuter steganografiyasi - bu klassik steganografiyaning yo‘nalishi bo‘lib, kompyuter platformasi uchun asoslangan. Masalan, Linux uchun, steganografik fayl tizimsi StegFS, ma’lumotlarni ishlatish mumkin bo‘lmagan joylarda ularni ma’lum fayl formati ko‘rinishida saqlash, belgilarni fayllar nomiga almashtirish, matnli steganografiya va h.k. Bir necha misollar keltiramiz:

- Zahiralangan formatli fayllarni kompyuterda qo‘llash – bu usulda to‘lmagan axborotning kengaytma maydoni nollar bilan to‘ldiriladi. Mos ravishda biz bu nolli qismni o‘zimizning ma’lumotlarimiz bilan to‘ldirishimiz mumkin. Bu usulning kamchiligi ma’lumotlar yashirish hajmining kamligidir.
- Egiluvchan diskning ishlatilmaydigan qismiga xabar yashirish usuli –

bunda xabar diskning ishlatilmagan bo‘sh qismiga yoziladi. Kamchiligi – kam hajmdagi axborotni uzatish mumkin.

• Faylli tizimning xususiyatidan foydalanish – qattiq diskka fayl saqlanganda u har doim klasterlarda joy egallaydi. Masalan, ilgari keng qo‘llanilgan fayl tizimsi FAT 32 (Windows 98, 2000, ME larda qo‘llanilgan) da klasterlarning standart o‘lchami – 4kb. Mos ravishda 1 kb ma’lumotni saqlash uchun xotiradan 4 kb joy ajratiladi, shundan 1 kb ma’lumot uchun ketsa, qolgan 3 kb hech narsa uchun ishlatilmaydi, bundan esa, bu joyni axborot yashirish uchun qo‘llash mumkin. Bu usulning kamchiligi – xabarni ochishning osonligi.

Raqamli steganografiya

Raqamli steganografiya – klassik steganografiyaning yo‘nalishi bo‘lib, raqamli obyektlarga axborotlarni yashirish yoki zarar yetishdan asrash asosida yaratilgan. Bu obyektlar multimedia obyektlari bo‘lib (tasvir, video, audio, 3D – obyektlar teksturasi) hisoblanadi.

Raqamli steganografiya doirasida eng ko‘p talabga mos yo‘nalish – raqamli, suvli, belgi qurilishi (RSB) (watermarking) va DRM (Digital rights management) tizimlarini himoya qilish usuli hisoblanadi.

Barcha yashirin axborot asosida qurilgan algoritmlarni bir necha bo‘limlarga bo‘lish mumkin:

• Raqamli signallar bilan ishlovchi usullar.

• Yashirin xabarni «Ichib qo‘yish». Bunda yashirin rasm (ovoz, ba’zida matn) originalining orasiga joylashtiriladi. Ko‘pincha RSB usulida qo‘llaniladi.

• Fayl formatlari xususiyatlaridan foydalanish, bu yerda faylning zaxiralangan qismiga yashirin axborot yozish mumkin bo‘ladi.

2.8. Bir martalik bloknot usuli

Bir martalik bloknot usuli Onetimepad deb ham yuritiladi. Kalit sifatida esa uzunligi juda katta bo‘lgan belgilar ketma – ketligi olinadi.

Masalan, biror yozuvchining asarini olishimiz mumkin. Misol sifatida Pirimqul Qodirovning “Yulduzli tunlar” asarini olamiz. Bunda shifirlanuvchi

matn kalitdagi mos belgilar bilan qo‘shiladi va modul olinadi. Modul olinayotgan son tanlanayotgan alfavit uzunligiga teng bo‘lishi shart. Kalitning ishlatilgan qismi o‘chirib tashlanadi. Bu jarayon to shifrlanayotgan matn tamom bo‘lguncha davom ettiriladi. Ushbu Onetimepad usuli shifrni ochishdagi qiyinchiligi bilan (axborotlarni himoyalash borasida) ancha mustahkam shifrlash usuli hisoblangan. Yana bir jihati kalitning uzunligida bo‘lgan.

Misol: K - kalit, M - shifrlanuvchi so‘z yoki matn, m - alfavit uzunligi, C - shifrlangan so‘z yoki matn. Alfavit oldindan kelishuv asosida belgilangan bo‘lishi kerak. Alfavitga turli belgilarni (tire, qo‘shtirnoq, ikki nuqta, vergul) kabi belgilarni ham qo‘shish mumkin. Ushbu biz ko‘rayotgan misolda ingliz alfaviti tanlab olingan. Har bir harf ketma-ket tarzda raqamlangan:

a	b	c	d	e	f	g	h	i	j	K	l	m	n	o	P	q	r
0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17

s	t	u	v	w	x	y	z
18	19	20	21	22	23	24	25

K= “shifrlangan”, m=26, M=“kompyuter”, C=?

s	h	i	f	r	l	a	n	g	a	n
18	7	8	5	17	11	0	13	6	0	13

k	o	m	P	y	u	t	e	r
10	14	12	15	24	20	19	4	17

Shifrlash: C = (M + *K)mod m* formuladan foydalaniladi.

C_1=(10+18) mod 26 = 2 - c

C_2=(14+7) mod 26 = 21 - v

C_3=(12+8) mod 26 = 20 - u

C_4=(15+5) mod 26 = 20 - u

Cs=(24+17) mod 26 = 15 - p

C_6= (20+11) mod 26 = 5 - f

C_7= (19+0) mod 26 = 19 - t

C_8= (4+13) mod 26 = 17 - r

C_9= (17+6) mod 26 = 23 - x

Shifrlangan so‘z: C = “ c v u u p f t r x”

Shifrni ochish: M = (C — *K)mod m* formuladan foydalaniladi.

M_1 = (2-18) mod 26 =10 - k

M_2 = (21-7) mod 26 = 14 - o

M_3 = (20-8) mod 26 = 12 - m

M_4 = (20-5) mod 26 = 15 - p

M_5 = (15-17) mod 26 = 24 - y

M_6 = (5-11) mod 26 = 20 - u

M_7 = (19-0) mod 26 = 19 - t

M_8 = (17-13) mod 26 = 4 - e

M_9 = (23-6) mod 26 = 17 - r

M = ” kompyuter” so‘zi paydo bo‘ldi.

Nazorat uchun savollar:

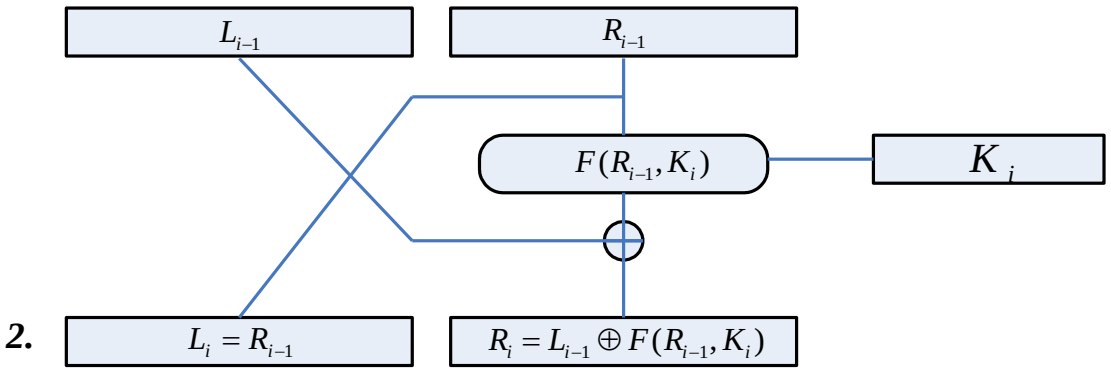
1. Onetimepad usulida kalit nimadan iborat?
2. Shifrlanadigan matn harflari qaysi tartib bilan nomerlanadi?
3. Shifrlangan matnni ochishda modulda manfiy son chiqsa nima qilinadi?
4. Kalit har ikkala tomonda ham bo‘lishi shartmi?
5. Kalit foydalanilganda bitta harfga surilib ketsa nima o‘zgaradi?
6. Kalitsiz qanday ochish mumkin?

III BOB. SIMMETRIK ALGORITMLAR

3.1. Feystel tarmog‘i va uning xususiyatlari

Feystel tarmog‘ining qo‘llanishi ko‘pgina simmetrik blokli shifrlash algoritmlarida uchraydi. Bu kriptoalgoritmlarga misol qilib FEAL, LOCI, Khufu, Khafre Blowfish, Lucifer, CAST, shuningdek, DES, GOST 28147-89 kabi standart algoritmlarni keltirish mumkin.

Feystel tarmog‘i g‘oyasi quyidagicha ifodalanadi. Shifrlanadigan blok ikkita L_0, R_0 qismlarga ajratiladi. Feystel tarmog‘i $i-$raundi iterativ blokli shifrlash almashtirishi quyidagi sxema bo‘yicha aniqlanadi:



1-rasm. Feystel tarmog‘i $i-$raundi.

Bu yerda $X_i = (L_{i-1}, R_{i-1}) - i$ -raund uchun L_{i-1} va R_{i-1} qismlarga ajratilgan kiruvchi ma’lumot, $Y_i = (L_i, R_i)$ esa X_i ni $i-$raund kaliti K_i bilan F akslantirish natijasida hosil bo‘lgan shifrma’alumot.

Feystel tarmog‘i $i-$raundining matematik modeli quyidagicha ifodalanadi:

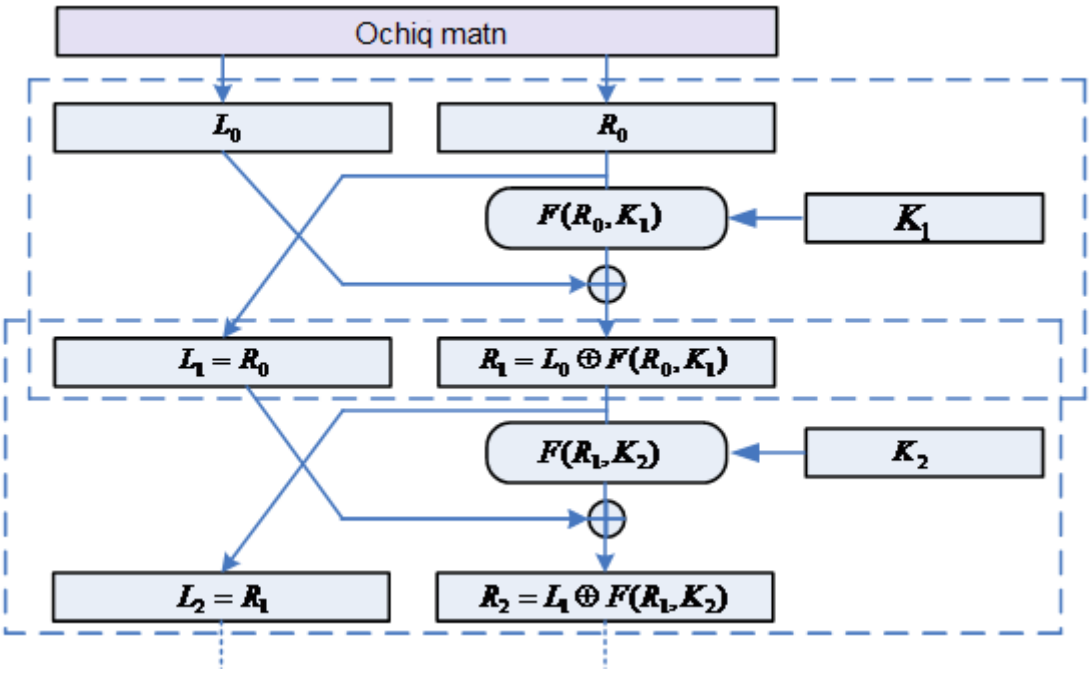
$$\begin{cases} L_i = R_{i-1}, \\ R_i = L_{i-1} \oplus F(R_{i-1}, K_i). \end{cases}$$

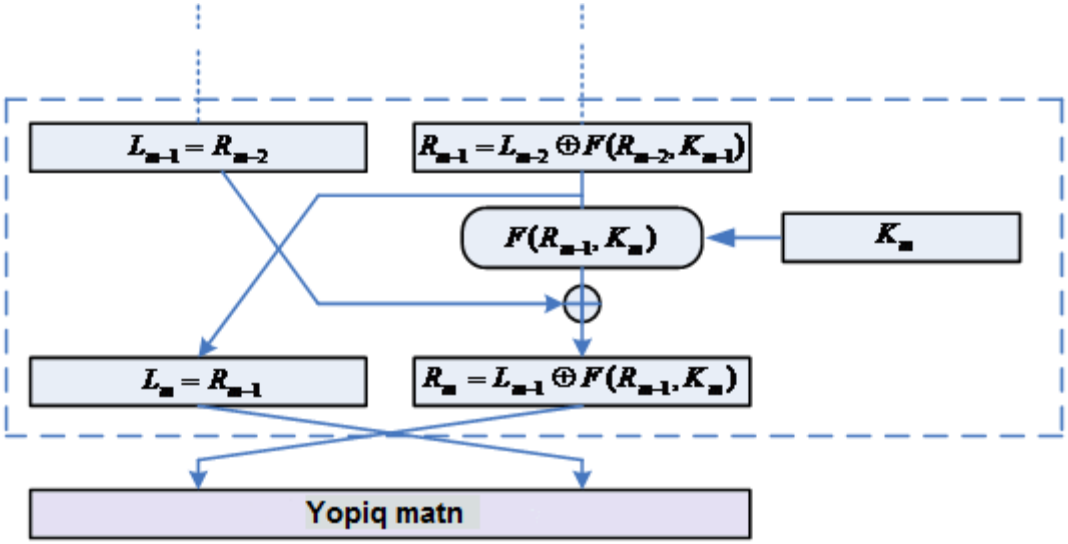
Feystel tarmog‘iga asoslangan algoritmlar bir necha iteratsiyadan tashkil topgan K_i kalitlarda shifrlanadigan funksiyadan tashkil topadi. Har bir $i-$ raunddagi shifrma’lumot $i+1-$ raund uchun kiruvchi (ochiq) ma’lumot hisoblanadi yoki $i-$ raunddagi kiruvchi ma’lumot $i-1-$raund uchun shifrma’lumot hisoblanadi. K_i raund kalitlari dastlabki K -kalitdan algoritmda ko‘rsatilgan qoida bilan hosil kilinadi.

Feystel tarmog‘i akslantirishlarining asosiy xossasi shundan iboratki, F -raund funksiyasi qaytmas bo‘lsa ham, Feystel tarmog‘i bu akslantirishlarini qaytarib beradi. Haqiqatan ham, yuqoridagi ifodada keltirilgan i – raund matematik modelida $\oplus$ - ikkilik sanok tizimida qo‘shish amali xossasidan foydalangan holda quyidagi tenglikni olish mumkin:

$$\begin{cases} R_{i-1} = L_i, \\ L_{i-1} = R_i \oplus F(L_i, K_i). \end{cases}$$

Bu oxirgi tengliklar tizimi Feystel tarmog‘i asosida qurilgan shifrlash algoritmlarini deshifrlashining matematik modelini ifodalaydi. Umumiy holatda m – raundli Feystel tarmog‘ining funksional sxemasi quyidagicha ifodalanadi:





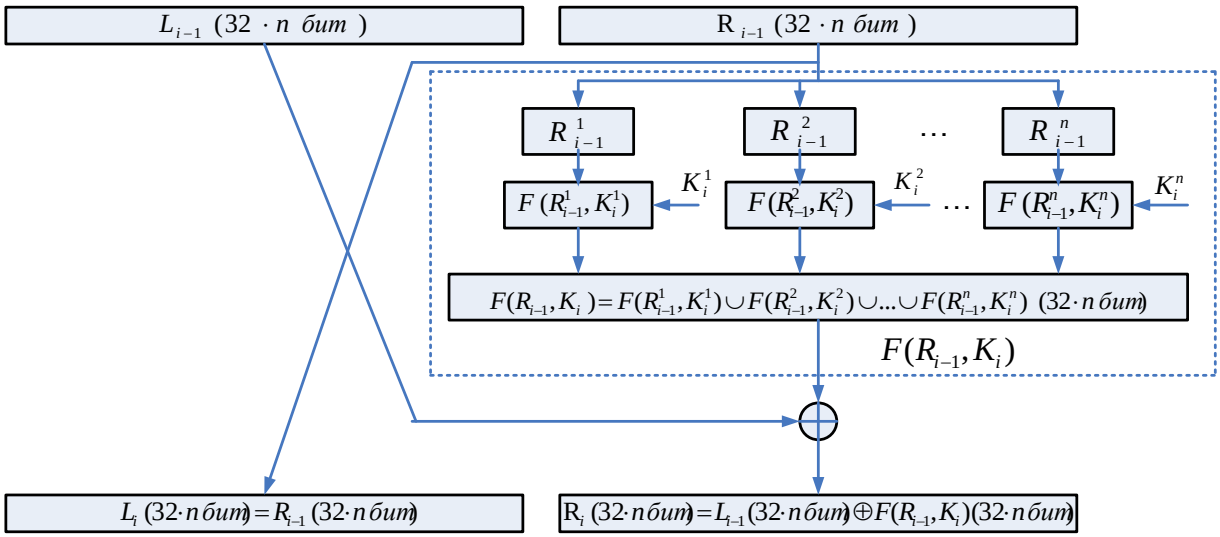
2.2 -rasm. m-raundli Feystel tarmog‘i.

Feystel tarmog‘i asosida qurilgan shifrlash algoritmlarida shifrlash va deshifrlash uchun bir xil algoritmdan foydalanilib, faqat raund kalitlarining qo‘llanilishi teskarisiga o‘zgaradi, ya’ni deshifrlashda 1-raundda K_m, 2 – raundda K_{m-1} va hakozo oxirgi raundda K_1 ishlatiladi. $F(R_{i-1}, K_i)$ funksiya bir tomonlama bo‘lsa ham, deshifrlash natijasida bu funksiya qaytadi.

Hisoblash texnikalari qurilmalarining takomillashuvi natijasida, bugungi kunda standart sifatida qo‘llanilib kelinayotgan shifrlash algoritmlarining bardoshliligi, ularda qo‘llanilaligan akslantirishlarga bog‘liq bo‘lmagan holda, ular kalitlarining uzunliklariga nisbatan kamayadi. Yuqorida sanab o‘tilgan Feystel tarmog‘iga asoslangan shifrlash algoritmlari bugungi kunda ham standat sifatida benuqson qo‘llanilib kelinayotganligi, bunday algoritmlar akslantirishlarini saqlab qolgan holda, ularning kalitlarini uzaytirish masalasining dolzarbligi kelib chiqadi. Quyida Feystel tarmog‘iga asoslangan barcha shifrlash algoritmlarini takomillashtirish uchun umumiy bo‘lgan qoida keltiriladi.

Bugungi kunda ko‘plab amalda qo‘llanilib kelinayotgan kompьyuterlardagi arifmetik amallarni bajaruvchi qurilma ikkilik sanok tizimida 32 razryad bilan ifodalanuvchi sonlar uchun mo‘ljallangan. Kelajakda kompьyuter foydalanuvchilari uchun bundan ham katta 64, 128 va xokazo razryadli sonlar ustida arifmetik amallar bajarish imkoniyatini beruvchi tezkor qurilmalar yaratilishi tabiiy hol. Shularni hisobga olib, Feystel tarmog‘iga asoslangan

shifrlash algoritmlarini akslantirish asoslarini saqlab qolgan holda, *K*-kalit uzunliklarini oshirish masalasi echiladi. Mana shunday masalani echish uchun Feystel tarmog‘i quyidagicha takomillashtiriladi:



2.3 – rasm . Takomillashgan Feystel tarmog‘i i ***– raundi.***

Bu yerda:

1. Shifrlanishi kerak bo‘lgan ochiq ma’lumot bloklari uzunligi $64m$ *bit*ga teng.

2. Kalit uzunligi $|K| \cdot n$ *bit*ga teng.

3. $K_i = K_i^1 K_i^2 ... K_i^n - i$ -raund qism kalitlari birlashmasi.

4. Feystel tarmog‘i R – o‘ng va L – chap qismlari uzunliklari: $|L| = |R| = 32 \cdot n$ *bit*ga teng.

5. $L_{i-1}(32 \cdot n\, bit) - i$ -raund chap qismi.

6. $R_{i-1}(32 \cdot n\, bit) - i$ -raund o‘ng qismi.

7. $L^1_{i-1}(32\, bit)$, $L^2_{i-1}(32\, bit)$,..., $L^n_{i-1}(32\, bit) - i$ -raund chap qismning 32 *bit*lik bo‘laklari.

8. $R^1_{i-1}(32\, bit)$, $R^2_{i-1}(32\, bit)$,..., $R^n_{i-1}(32\, bit) - i$ -raund o‘ng qismning 32 *bit*lik bo‘laklari.

9. $F(R^1_{i-1}, K^1_i)$, $F(R^2_{i-1}, K^2_i)$,..., $F(R^n_{i-1}, K^n_i) - i$ -raund Feystel funksiyasining mos akslantirishlari.

Takomillashgan Feystel tarmog‘i $i-$raundi matematik modeli quyidagicha ifodalanadi:

$$\begin{cases} L_i(32\cdot n bit) = R_{i-1}(32\cdot n bit) \\ R_i(32\cdot n bit) = L_{i-1}(32\cdot n bit) \oplus F(R_{i-1}, K_i)(32\cdot n bit) \end{cases}$$

Yuqorida takomillashgan va asosiy Feystel tarmog‘i sxemasidan ko‘rinib turibdiki, takomillashgan Feystel tarmog‘ida takomillashtirish parametri n ga bog‘liq bo‘lgan holda bir nechta $F(R_{i-1}^1, K_i^1)$, $F(R_{i-1}^2, K_i^2)$,..., $F(R_{i-1}^n, K_i^n)$ Feystel funksiyalari uchraydi. Bu esa n ga bog‘liq holda bir necha Feystel tarmog‘iga asoslangan algoritmlar funksiyalaridan yoki bir necha **S**-bloklardan foydalanish imkonini beradi. Shuningdek, n ga bog‘liq ravishda kalit uzunliklari ham ortib boradi, ya’ni $n=1$ da kalit uzunligi 256 bit bo‘lsa, $n=2$ da kalit uzunligi 512 va hakazo bo‘ladi. Kalit uzunligi va takomillashtirish parametri n orasida quyidagicha bog‘liqlik o‘rnatish mumkin:

$$l_1 = l \cdot n$$

bu erda $l-$ asosiy algoritm kaliti uzunligi, l_1-takomillashgan algoritm kaliti uzunligi.

Feystel tarmog‘iga asoslangan takomillashgan va asosiy algoritmlarning shifrlash va deshifrlash tezligi teng, chunki $n=1$ da algoritm blok uzunligi 64 ga teng bo‘lib, algoritm tezligi 20 taktdan iborat bo‘lsa, $n=2$ da takomillashgan algoritm blok uzunligi 128 bit bo‘lib, tezligi 40 taktdan iborat bo‘ladi.

Demak, takomillashgan Feystel tarmog‘i quyidagi afzalliklarga ega:

1) Takomillashtirish parametri n ga bog‘liq holda shifrlash algoritmi xossalari va bardoshliligini saqlab qolgan holda algoritm kaliti uzunligini oshirib borish imkoniyati mavjud. Bu esa, o‘z navbatida, hisoblash texnikasi qurilmalarining takomillashuvi natijasida algoritm kaliti uzunligi to‘liq tanlash usuliga bardoshsiz bo‘lib qolishining oldini oladi.

2) Algorim tezligi takomillashtirish parametri n ga bog‘liq emas, ya’ni Feystel tarmog‘iga asoslangan takomillashgan va asosiy algoritm tezliklari teng. Bu xossa o‘z navbatida algoritm tezligini saqlab qolgan holda takomillashtirish imkoniyatini beradi.

Quyida Feystel tarmog‘iga asoslangan simmetrik blokli shifrlash algoritmlariga misollar ko‘rib o‘tiladi.

3.2. GOST 28147-89 standart simmetrik blokli shifrlash algoritmi

GOST 28147-89 kriptoalgoritmi hozirda Rossiya Federatsiyasi davlat standart shifrlash algoritmi hisoblanadi. Bu algoritm apparat va dasturiy ta’minot uchun mo‘ljallangan bo‘lib, himoyalanadigan ma’lumotning maxfiylik darajasiga chegaralash yo‘q. Algoritmning kalit uzunligi 256 bitga shifrlashni 64 bit uzunlikdagi bloklarda amalga oshiradi va raundlar soni 32 ga teng. Biror ma’lumotni GOST 28147-89 kriptoalgoritmi bilan shifrlash uchun dastlab 256 bitli kalitdan 32 ta 32 bitli rund kalitlari K_i generatsiya qilinadi va ochiq ma’lumot 64 bitli $X_i, i = 1,2,...$ bloklarga bo‘linadi. Bu 64 bitli X_i blok 32 bitli chap L_i va o‘ng R_i qismlarga bo‘linadi $X_i = L_i \| R_i$ va yuqoridagi formula yordamida almashtiriladi, ya’ni shifrlanadi.

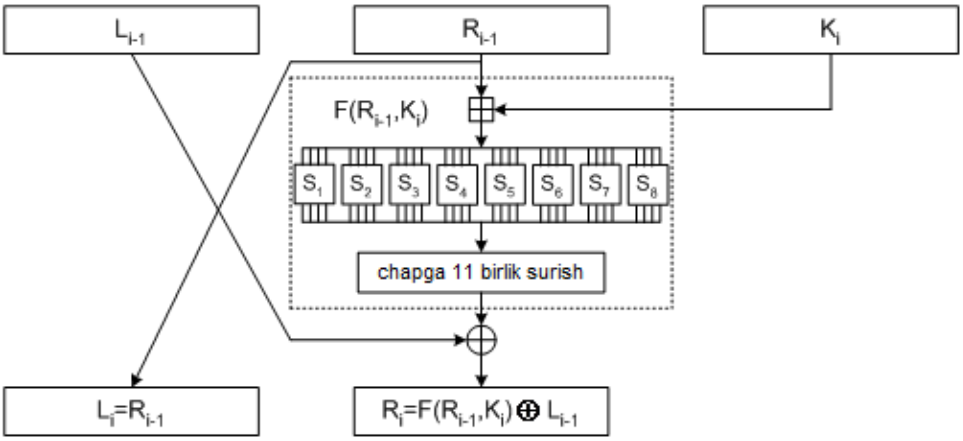
Kriptoalgoritmning *F* funksiyasi quyidagi amal va almashtirishlardan tashkil topgan:

1) blokni 32 bitli o‘ng qismi va 32 bitli raund kalitini $\bmod 2^{32}$ bo‘yicha qo‘shish: $C_i = (R_{i-1} + K_i) \bmod 2^{32}$;

2) 32 bitli C_i natija sakkizta maxfiy S-bloklarda o‘rniga qo‘yish akslantirishi orqali akslanadi ;

3) S-bloklarda chiquvchi 32 bitli blok chapga 11 birlikssiklik suriladi;

Ochiq ma’lumot 32 raund iterativ shifrlashdan so‘ng, chap L_{32} va o‘ng R_{32} qismlar birlashtiriladi va $Y_i = R_{32} \| L_{32}$ shifrma’lumot, ya’ni Y_i shifrma’lumot hosil qilinadi.



2.4-rasm. GOST 28147-89 kriptoalgoritmining i-raundi

GOST 28147-89 kriptoalgoritmida 8 ta S-bloklar qo‘llaniladi, S-bloklar maxfiy va bu algoritmdagi yagona chiziqli bo‘lmagan akslantirishdir. Bu S-bloklarning kirish va chiqish bitlari to‘rtga teng bo‘lib, noldan o‘n beshgacha bo‘lgan sonlar qatnashadi. Masalan, birinchi S-blok quyidagicha bo‘lishi mumkin:

0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15
11	7	13	0	7	9	14	1	6	15	3	4	10	2	5	12

Birinchi S-blokka kiruvchi qiymat 4 ga teng bo‘lsa, S-blokdan chiquvchi qiymat 7 ga teng. 4 va 7 sonlari orasida chiziqli bog‘lanish mavjud emas.

GOST 28147-89 kriptoalgoritmida blokning 32 bitli o‘ng qismi R_i 32 bitli raund kaliti K_{i+1} ga $\bmod 2^{32}$ amali bo‘yicha qo‘shiladi. Kriptoalgoritm K_{i+1} raund kaliti maxfiyligini hisobga olganda, R_i yoki K_{i+1} ni bitta biti o‘zgarishi natijaning kamida bitta bitini o‘zgarishiga olib keladi, shuningdek bu amal umumlashgan to‘ldirish xususiyatiga ega. Buning uchun kalit bilan qo‘shishda hosil bo‘ladigan kolliziyani ko‘rsatish etarli. φ_x -32 bitli blokni shifrlash akslantirishi, φ_k - kalit akslantirishi, F -shifrlash raund funksiyasi, L -chap blok, R -o‘ng blok bo‘lsin. To‘ldirish xususiyati quyidagi tenglik bo‘yicha aniqlanadi:

$$\varphi_x(L \oplus F(R+k)) = \varphi_x(L \oplus F(\varphi_x(R) + \varphi_k(k))) .$$

φ_x va F akslantirishlar teskarisi ham o‘ziga tengligi xossasidan foydalansak, quyidagi shifr avtomorfizmlik sharti hosil bo‘ladi:

$$R + k = \varphi_x(R) + \varphi_k(k) (\text{mod } 2^{32})$$

Xususan bu shartni $\varphi_x(X) = X + 2^{31} (\text{mod } 2^{32})$ va $\varphi_k(k) = k + 2^{31} (\text{mod } 2^{32})$ operatorlari ham qanoatlantiradi. Bu esa katta bitning inversiyasi raund kaliti yoki 32 bitli blokda paydo bo‘lishini bildiradi.

Kriptoalgoritmning S-bloklari maxfiyligi algoritm bardoshliligini yanada oshiradi. Har bir S-blokda 16 ta bir xil bo‘lmagan sonlar qatnashadi va bu sonlarni to‘liq tanlash 16! ni va sakkizta S-bloklarni tanlash $C_{16!}^{8} = \frac{(16!)!}{8!(16!-8)!}$ ni tashkil etadi. Kriptoalgoritm differensial va chiziqli kriptotahlil usullariga ham bardoshli bo‘lib, bu kriptotahlil usullarini algoritmga qo‘llash uchun 2^{64}, ya’ni mumkin bo‘lgan barcha bloklar sonidan ham ko‘p ochiq ma’lumot talab etiladi. Algoritmda S-bloklardan so‘ng 11 bit chapgassiklik surish akslantirishi qo‘llanilagan. 11 soni 33 ga karrali, 32 ga karrali emas va algoritmga kiruvchi blokdagi har bir element to‘liq aralashishini ta’minlaydi, ya’ni algoritmga kiruvchi blokning biror x_i elementi, masalan 4- o‘rinda x_4 bo‘lsa, 1 -raunddan so‘ng 30 -o‘rinda x_{30} bo‘lib, 2 -raunddan so‘ng 17 -o‘rinda x_{17} bo‘lib va hokazo o‘rinlarda uchraydi. Hech qachon biror raunddan so‘ng joylashgan o‘rni qaytarilmaydi, ya’ni $x_i \neq x_j, i \neq j$, $1 \leq i, j \leq 32$. Bu standart shifrlash algoritmi hozirgi kunda ham ko‘p jihatdan boshqa algoritmlarga nisbatan o‘zining kiriptografik samaradorligini saqlab kelmoqda.

Misol tariqasida bugungi kunda ham o‘zining samaradorligi va bardoshliligi bilan ishonchli kriptografik xususiyatlarga ega bo‘lgan Feystel tarmog‘iga asoslangan GOST 28147-89 standart simmetrik blokli shifrlash algoritmi takomillashgan variantini keltiramiz.

1. Kalit uzunligi: $|k| = 256 \cdot n\, bit = 32 \cdot n\, bayt.$
2. Blok uzunligi: $|B| = 64 \cdot n\, bit = 8 \cdot n\, bayt.$

3. R – o‘ng va L – chap qismlari uzunliklari: $|L| = |R| = 32 \cdot n\, bit = 4 \cdot n\, bayt$.

4. Takomillashgan algoritm kaliti: $k(256 \cdot n) = k_1 ... k_{8 \cdot 32 \cdot n} = k_1 ... k_{32 \cdot n}\, k_{32 \cdot n+1} ... k_{2 \cdot 32 \cdot n}$ $k_{2 \cdot 32 \cdot n+1} ... k_{3 \cdot 32 \cdot n}\, k_{3 \cdot 32 \cdot n+1} ... k_{4 \cdot 32 \cdot n}\, k_{4 \cdot 32 \cdot n+1} ... k_{5 \cdot 32 \cdot n}\, k_{5 \cdot 32 \cdot n+1} ... k_{6 \cdot 32 \cdot n}\, k_{6 \cdot 32 \cdot n+1} ... k_{7 \cdot 32 \cdot n}\, k_{7 \cdot 32 \cdot n+1} ... k_{8 \cdot 32 \cdot n}$.

5. Raund kalitlari: $k(i) = k_{(i-1) \cdot 32 \cdot n+1} ... k_{i \cdot 32 \cdot n}$, i=1,…8.

6. S-bloklar soni: $8 \cdot n$ (dona.)

7. Raund kalitlari uzunligi: $|k_{raund}(i)| = 32 \cdot n\, bit$.

Ma’lumki GOST 28147-89 da 8 ta S-bloklar ishlatilgan. Keltirilgan dasturiy ta’minotda $n = 1$ dan $n = 10$ gacha takomillashtirish imkoniyati yaratilgan. Keltirilgan takomillashtirilgan shifrlash algoritmi uchun S-bloklar standart shifrlash algoritmi S-bloklarini $n = 1$ da chapga 1ssiklik surishdan, $n = 2$ da esa chapga 2 xonagassiklik surishdan va hakozo $n = 10$ da chapga 10 xonaga surish bilan hosil qilingan.

Yuqorida takomillashgan va takomillashmagan Feystel tarmog‘i funksional sxemasidan ko‘rinib turibdiki, takomillashgan Feystel tarmog‘ida takomillashtirish parametri n ga bog‘liq bo‘lgan holda bir nechta $F(R_{i-1}^1, K_i^1)$, $F(R_{i-1}^2, K_i^2)$,..., $F(R_{i-1}^n, K_i^n)$ Feystel funksiyalari uchraydi. Bu esa n ga bog‘liq holda bir nechta Feystel tarmog‘iga asoslangan algoritmlar funksiyalaridan yoki bir nechta S-bloklardan foydalanish imkonini beradi. SHuningdek, n ga bog‘liq ravishda kalit uzunliklari ham ortib boradi, ya’ni $n = 1$ da kalit uzunligi 256 bit bo‘lsa, $n = 2$ da kalit uzunligi 512 va hokazo bo‘ladi. Kalit uzunligi va takomillashtirish parametri n orasida quyidagicha bog‘liqlik o‘rnatish mumkin:

$$l_1 = l \cdot n$$

bu erda l – takomillashmagan algoritm kalit uzunligi, l_1 – takomillashgan algoritm kalit uzunligi.

Feystel tarmog‘iga asoslangan takomillashgan va takomillashmagan algoritmlarning shifrlash va deshifrlash tezligi teng, chunki $n = 1$ da algoritm blok uzunligi 64 ga teng bo‘lib, algoritm tezligi 20 taktdan iborat bo‘lsa, $n = 2$ da

takomillashgan algoritm blok uzunligi 128 bit bo‘lib, tezligi 40 taktdan iborat bo‘ladi.

Demak, takomillashgan Feystel tarmog‘i quyidagi afzalliklarga ega:

1) Takomillashtirish parametri n ga bog‘liq bo‘lgan holda shifrlash algoritmi xossalari va bardoshliligini saqlab qolgan holda algoritm kalit uzunligini oshirib borish imkoniyati mavjud. Bu esa o‘z navbatida hisoblash texnikasi qurilmalarining takomillashuvi natijasida algoritm kalit uzunligi to‘liq tanlash usuliga bardoshsiz bo‘lib qolishini oldini oladi.

2) Algorim tezligi takomillashtirish parametri n ga bog‘liq emas, ya’ni Feystel tarmog‘iga asoslangan takomillashgan va takomillashmagan algoritm tezliklari teng. Bu xossa, o‘z navbatida, algoritm tezligini saqlab qolgan holda takomillashtirish imkoniyatini beradi.

3.3. S –blok va shifrlash algoritmi

Yuqrida o‘rganilgan blokli shifrlash algoritmlarining eng asosiy farqlari raundlar iteratsiyasida qo‘llanilgan asosiy akslantirishlar tuzilishlarining (konstruksiyalarining) har-xilligidadir. Bu akslantirishlar, elektron elementlar bazasida qulay amalga oshirilishi, kriptobardoshlilik xususiyatlarni ta’minlashi va apparat-texnik qurilmalar modifikatsiyalari uchun qulay va samarali bo‘lishi lozim.

E’tiboringizga havola etilayotgan algoritmda ma’lumot bloklari mos bitlarini raund kalitlari mos bitlariga mod 2 bo‘yicha – XOR amali bo‘yicha qo‘shish, hamda, bu algoritm muallifi tomonidan taklif etilgan 4 baytli (32-bitli) ma’lumot blokining xarakteristikasi 256 bo‘lgan chekli maydonda aniqlangan to‘g‘ri to‘rtburchakli matritsa orqali kengaytirish, baytlarni 256 baytli S–blokdan foydalanib almashtirish va kengaytirilgan blokni siqish jadvali asosida dastlabki o‘lchamiga keltirish akslantirishlari qo‘llanilgan.

Algoritm sanab o‘tilgan akslantirishlar kombinatsiyasi asosida 64-bitli ma’lumotni 256-bitli kalit orqali sakkiz raundli iteratsiya bilan shifrlash jarayonini amalga oshiradi.

Shifrlash va deshifrlash jaryonlarini yoritish uchun quyidagi belgilashlar kiritiladi:

- T_0 – 64-bitli ochiq ma’lumot bloki;

- T_{sh} – 64-bitli shifrlangan ma’lumot bloki;

- t_i – 64-bitli ochiq ma’lumot blokining i - biti, bu erda $i = 1,\ldots,64;$ $i = 0,1,2,\ldots,8$;

- L_i va R_i – 64-bitliblokning mos ravishda 32-bitli chap va o‘ng qismlari bo‘lib, bu erda $i = 0,1,2,\ldots,8$;

- $(a_1(i), a_2(i),\ldots, a_{32}(i))$ - i – raund akslantirishining chap qismi, ya’ni

$L_i = (a_1(i), a_2(i),\ldots, a_{32}(i))$;

- $(b_1(i), b_2(i),\ldots, b_{32}(i))$ - i – raund akslantirishining o‘ng qismi, ya’ni

$R_i = (b_1(i), b_2(i),\ldots, b_{32}(i))$;

- $x_{4\times1} = (x_1, x_2, x_3, x_4)$ – matritsali akslantirishga kiruvchi 4-baytli (32-bitli) vektor,bu erda x_i - baytlar qiymatlari ushbuoraliqdan olinadi $0 \le x_i \le 255,\ i = 1,2,3,4;$

- $A_{n\times4}$ – to‘g‘ri to‘rtburchakli matritsa (oldindan aniqlangan qoida bo‘yicha kalit ketma-ketligidan generatsiya qilinib, maxfiy hisoblanadi yoki alohida generatsiya qilinib, ochiq bo‘lishi ham mumkin), bunda $n = 2^m,\ m = 2,\ldots,M,\ M < \infty,$ matritsa elementlari $a_{ij}\ (i = 1,\ldots, n;\ j = 1,2,3,4;)$ bir bayt bilan ifodalanib, ushbu $0 \le a_{ij} \le 255$ tengsizlikni qanoatlantiradi;

- $y_{n\times1} = (y_1, y_2,\ldots, y_n)$ – xarakteristikasi 256 bo‘lgan chekli maydonda matritsali $A_{n\times4}x_{4\times1}$ akslantirish natijasini ifodalovchi vektor, ya’ni $y_{n\times4} = A_{n\times4}x_{4\times1} (\text{mod } 256)$, bu erda y_i – baytlar, $0 \le y_i \le 255, i=1,2,\ldots,n$;

- $k = k_1k_2\ldots k_8$ – sakizta k_i, $i = 1,\ldots,8;$ 32-bitli qismkalitlardan iborat bo‘lgan 256-bitli kalit;

- S – blok (oldindan aniqlangan qoida bo‘yicha kalitdan generatsiya qilinuvchi 256-baytli blok, maxfiy) akslantirish, 256 ta $S_0, S_1,\ldots, S_{255}$ -baytlardan iborat bo‘lgan:

S_0	S_1	S_2	…	S_{255}

jadval, bu erda $0 \le S_1, S_2, ..., S_{256} \le 255$, $S_i \ne S_j$, ya'ni $0 \le S_i \le 255$ shartni qanoatlantiruvchi S_i – sonlarning tasodifiy joylashuvidan iborat;

- $\oplus$ – bloklar vektorlarining mos bitlarini $\bmod 2$ bo'yicha – XOR amali bilan qo'shish;

- $z_{n\times 1} = (z_1, z_2, ..., z_n)$ – matritsali kengaytirish akslantirishi natijasi bo'lgan $y_{n\times 1} = (y_1, y_2, ..., y_n)$ –vektorni S – blok akslantirishlari natijasi, ya'ni $z_{n\times 1} = S(y_{n\times 1})$, bu erda z_i – baytlar, $0 \le z_i \le 255$, $i = 1,2,\ldots,n$;

- $k_i = k_1(i)k_2(i)..k_{32}(i)$ – 32-bitli i-qismkalit;

- $k_i^1 = k_1(i)k_2(i)..k_8(i), ..., k_i^4 = k_{25}(i)k_{26}(i)..k_{32}(i)$ –32-bitli i-qismkalitning to'rtta bayti;

- $k_{pi} = (k_1(pi)k_2(pi)..k_{32}(pi))$ – 32-bitli i-raund kaliti, bu erda $pi = 1,...,8$;

- $k_н$ –64-bitli boshlang'ich kalit;

- $k_к$ –64-bitli oxirgi kalit;

- f – shifrlash funksiyasi;

- SJ –siqish jadvali, o'lchovi 16x16 (maxfiy, kalit bilan birgalikda uzatiladi yoki oldindan aniqlangan qoida bo'yicha kalitdan generatsiya qilinadi), q_{ij} - elementlari $0 \le q_{ij} \le 15$, $i = 0,...,15$, $j = 0,...,15$ va teng taqsimlangan:

q_{00}	q_{01}	…	$q_{0,15}$
q_{10}	q_{11}	…	$q_{1,15}$
…	…	…	…
$q_{15,0}$	$q_{15,1}$	…	$q_{15,15}$

- $w_{4\times 1} = (w_1, w_2, w_3, w_4)$ – 32-bitli (4-baytli) vektor, SJ natijasi.

Shifrlashda kalitlarni saqlash qurilmasiga (massiviga) 32-bitli bo‘lgan sakkizta k_i-qismkalitlardan tashkil topgan 256-bitli $k = k_1 k_2 ... k_8$ -kalit bloki kiritiladi, ochiq ma’lumot 64-bitli bloklarga ajratilib, har bir T_0-blok 8-raundli akslantirishlar jarayonidan o‘tkaziladi. Har bir $i-$raund kaliti k_{pi} 32-bitli $k_i = k_1(i)k_2(i)...k_{32}(i)$-qismkalitni to‘rtta $k_i = (k_i^1, k_i^2, k_i^3, k_i^4) = (k_1(i)k_2(i)...k_8(i), ..., k_{25}(i)k_{26}(i)...k_{32}(i))$ baytlarga ajratilib, hosil bo‘lgan $k_i^1, \ldots, k_i^4$ baytlarni o‘nlik sanoq tizimidagi $(k_i^1)_{10}, \ldots, (k_i^4)_{10}$-qiymatlari bo‘yicha *S*-blok yacheykalari tartib soni (nomeri) aniqlanadi, hamda, har bir k_i^l-bayt *S*-blokning $(k_i^l)_{10}$-tartib sonli yacheykasida turgan $S_{k_i^l}$ soniga almashtirish bilan aniqlanadi, ya’ni

$$k_{pi} = S(k_i^1, ..., k_i^4) = (S(k_i^1), ..., S(k_i^4)) = ((S_{k_i^1})_2, ..., (S_{k_i^4})_2) = (k_{pi}^1, ..., k_{pi}^4) .$$

Dastlabki 256-bitli $k = k_1 k_2 ... k_8$-kalit ikki marta SJ akslantirishidan o‘tkazilib, 64-bitli boshlang‘ich kalit $k_н$ hosil qilinadi.

Dastlabki 256-bitli $k = k_1 k_2 ... k_8$-kalit *S*-blok akslantirishlaridan o‘tkazilib, hosil bo‘lgan 256-bitli natija ikki marta SJ akslantirishlaridan o‘tkazilib, 64-bitli oxirgi kalit $k_к$ olinadi.

Ochiq ma’lumot bloki T_0 mos bitlari boshlang‘ich kalit $k_н$ mos bitlari bilan XOR amali bo‘yicha qo‘shilib, ya’ni $T_0 \oplus k_н = T_0'$, hosil bo‘lgan natija T_0', yana T_0 o‘zgaruvchiga berilib $T_0 = T_0'$, T_0 ikkita 32-bitli qismlarga ajratiladi:

$$T_0 = (t_1(0), t_2(0), ..., t_{32}(0), t_{33}(0), ..., t_{64}(0)) = (a_1(0), a_2(0), ..., a_{32}(0), b_1(0), b_2(0), ..., b_{32}(0)) = (L_0, R_0)$$

Birinchi raundda *f*-funksiya qiymatini hisoblash quyidagicha amalga oshiriladi:

1. Blok R_0 mos bitlari raund kaliti $k_{p1} = k_1(p1)k_2(p1)...k_{32}(p1)$ mos bitlari bilan XOR amali bo‘yicha qo‘shiladi, ya’ni

$$b_1(0)b_2(0)...b_{32}(0) \oplus k_1(p1)k_2(p1)...k_{32}(p1) =$$

$$(b_1(0) \oplus k_1(p1))(b_2(0) \oplus k_2(p1))...(b_{32}(0) \oplus k_{32}(p1)) =$$

$$= x_1(1)x_2(1)...x_8(1)\ x_1(1)x_2(1)...x_8(1)\ x_1(3)x_2(3)...x_8(3)\ x_1(4)x_2(4)...x_8(4) =$$

$= (x_1, x_2, x_3, x_4) = x_{4\times1}$;

2. Oldingi bosqich natijasi $x_{4\times1}$ xarakteristikasi 256 bo‘lgan chekli maydonda aniqlangan to‘g‘ri to‘rtburchakli matritsa $A_{n\times4}$ orqali akslantiriladi:

$y_{n\times1} = (A_{n\times4} x_{4\times1}) \bmod 256$;

3. Baytlari soni n ta bo‘lgan $y_{n\times1}$ -vektorning har bir i - bayti y_i, $i=1,...n$, S - blok akslantirishlaridan o‘tkaziladi, bunda $i-$baytning $(y_1(i)y_2(i)...y_8(i))_2 = y_i$ o‘nlik sanoq tizimidagi ifodasi $(y_1(i)y_2(i)...y_8(i))_2 = (y_i)_{10}$ bo‘yicha S –blok yacheykalari tartib soni aniqlanib, $(y_1(i)y_2(i)...y_8(i))_2 = y_i$ bayt S-blokning $(y_i)_{10}$-tartib sonli yacheykasida turgan $S_{(y_i)}$ soniga almashtirish bilan aniqlanadi, ya’ni:

$z_i = S(y_i) = S(y_1(i)y_2(i)...y_8(i)) = (S_{y_i})_2$;

4. Siqish jadvali SJ bo‘yicha $8\times n-$bitli ($n-$baytli) vektor $z_{n\times1}$ 32 -bitli (4-baytli) vektorga $w_{4\times1} = (w_1, w_2, w_3, w_4)$ akslantiriladi:

- $z_{n\times1}$-vektorning har bir z_i baytiyarim baytli qismlarga ajratiladi, ya’ni $z_{n\times1} = (z_1,..., z_n) = (z'_1,..., z'_{2n}) = z'_{2n\times1}$;

- yarim baytli z'_1 va z'_{2n} bloklarning o‘nlik sanoq tizimidagi qiymatlari $(z'_1)_{10}$ va $(z'_{2n})_{10}$ bo‘yicha mos ravishda SJ satr va ustun tartib sonlari aniqlanib, ularning kesishgan joyidagi yarim bayt $q_{(z'_1)_{10}(z'_{2n})_{10}}$ yarim baytli z'_1 va z'_{2n} iborat bo‘lgan baytni $q_{(z'_1)_{10}(z'_{2n})_{10}}$ - yarim baytga SJ akslantirishi natijasi hisoblanadi. So‘ngra, bu jarayon barcha (z'_2, z'_{2n-1}), (z'_3, z'_{2n-2}), …, (z'_n, z'_{n+1}), ya’ni (z'_i, $z'_{2n-(i-1)}$), bu erda $i=1,\ldots, n$; juftliklar uchun qo‘llaniladi;

-oldingi qadamdagi SJ akslantirishi (m-2) marta qo‘llanilib, natijada 32-bitli (4-baytli) $w_{4\times1} = (w_1, w_2, w_3, w_4)$ blok olinadi;

5. To‘la siqish natijasi bo‘lgan $w_{4\times1} = (w_1, w_2, w_3, w_4)$ - 32-bitli (4-baytli) vektorning bitlari XOR amali bo‘yicha L_0-blokning mos bitlariga qo‘shiladi:

$$L_0 \oplus w_{4\times1} = t_1(0)t_2(0)..t_{32}(0) \oplus w_1(1)w_2(1)...w_8(1)w_1(2)...w_8(2)w_1(3)...w_8(3)w_1(4)...w_8(4) =$$
$$= L_0 \oplus f(R_0, k_{p1}) = R_1$$

bu erdafunksiya $f(R_0, k_{p1})$orqali 1-4 –bosqichlar akslantirishlari belgilangan;

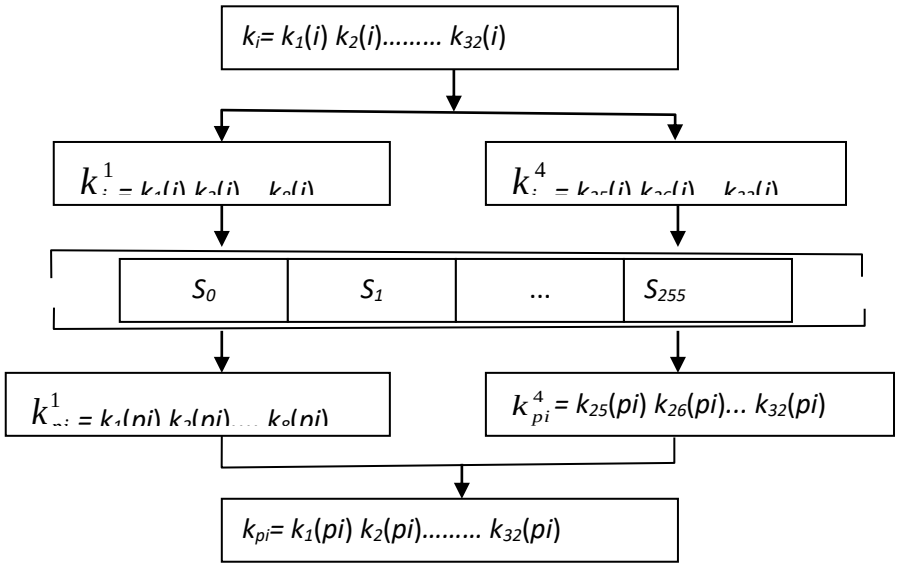
6. R_0 –blokning qiymati o‘zgarishsiz L_1-blokga beriladi: $L_1 = R_0$.

Yuqorida keltirilgan 1-6 –bosqich akslantirishlari e’tiboringizga havola etilayotgan shifrlash algoritmining 1-raund akslantirishlarini ifodalaydi.

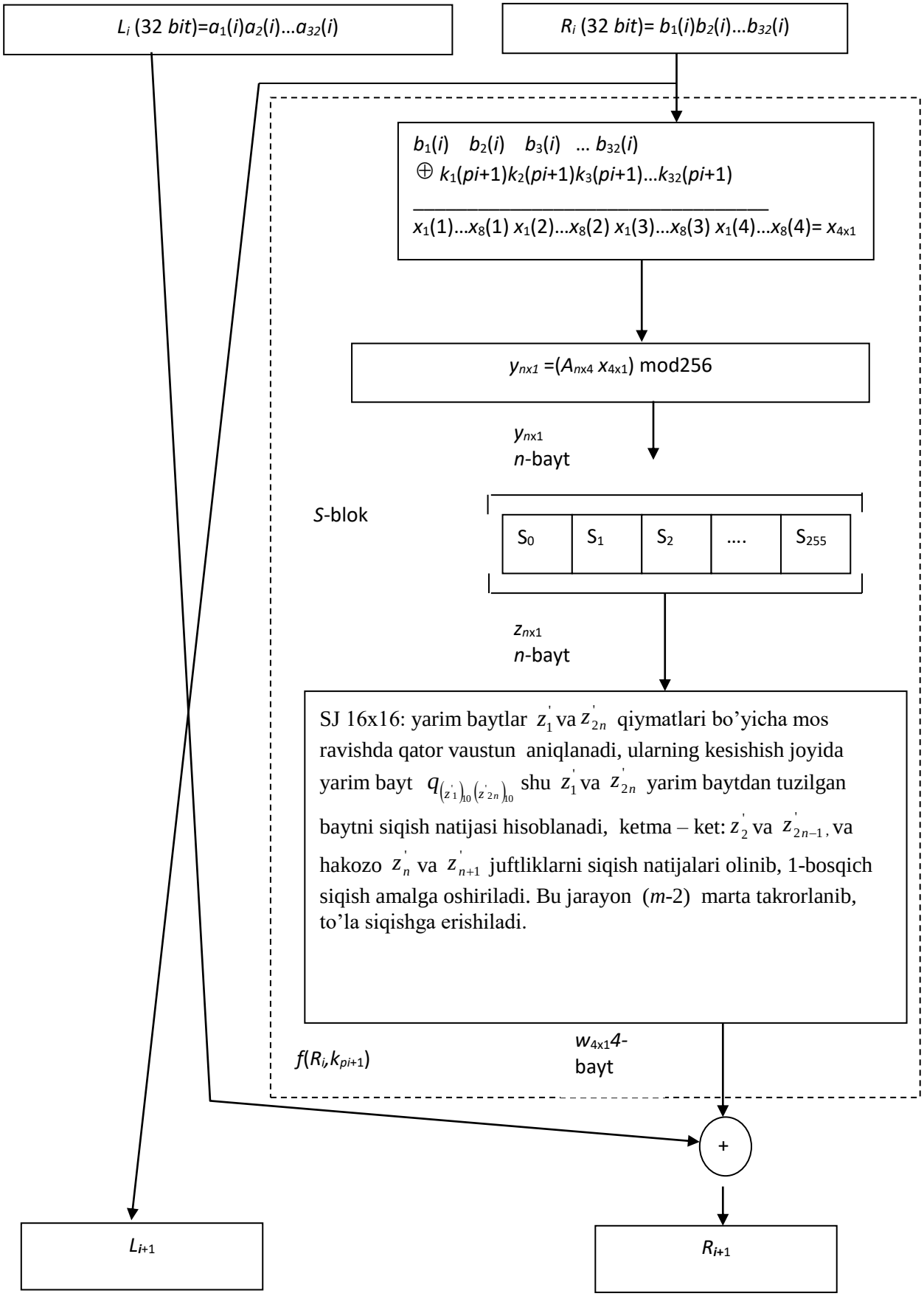
Birinchi raund akslantirishlari natijalarini ifodalovchi L_1 va R_1 o‘zgaruvchilar qiymatlarini mos ravishda L_0 va R_0 o‘zgaruvchilarga berilib, ya’ni $L_0 = L_1$, $R_0 = R_1$, hamda, birinchi raund kaliti massiviga ikkinchi raund kaliti massivi qiymatini berib $k_{p1} = k_{p2}$, so‘ngra, 1-6 –bosqichlar akslantirishlarini qo‘llab, 2-raund akslantirishlari amalga oshiriladi. SHunday qilib, agarda $(i-1)$ – raund akslantirish natijalari ma’lum bo‘lsa, ushbu $L_0 = L_{i-1}$, $R_0 = R_{i-1}$ va $k_{p1} = k_{pi-1}$ amallar bajarilib, so‘ngra 1-6 –bosqichlar akslantirishlarini qo‘llab, *i*-raund akslantirishlari amalga oshiriladi. Havola etilayotgan algoritmning raundlari soni 8 ta, ya’ni *i*=1,2,…,8.

L_8 va R_8-bloklarning birlashmasidan tuzilgan $T_к = R_8 L_8$-blokning bitlari $k_к$-blokning mos bitlariga XOR amali bilan qo‘shiladi, ya’ni $T_к \oplus k_k = T_ш$, ochiq ma’lumotning bitta 64-bitli blokini shifrlash jarayoni tamomlanadi.

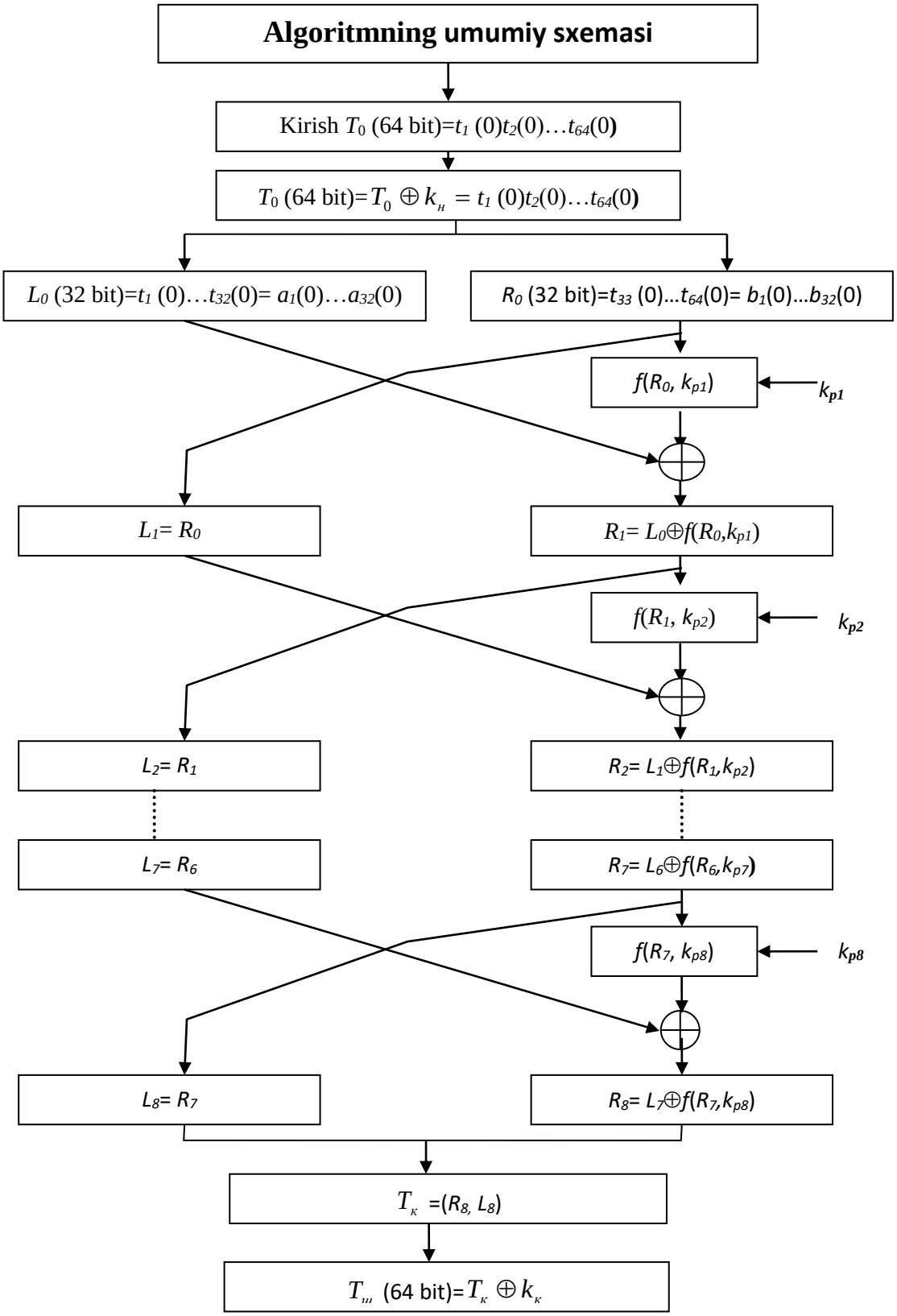
Quyida, dastlabki kalitdan raund kalitlarini generatsiya qilish, algoritm shifrlash jarayonining i – raundi, hamda, algoritmning umumiy blok sxemasi keltirilgan:



i – raund kaliti generatsiyasining blok sxemasi



Algoritm *i*-raundining blok sxemasi


Algoritmning umumiy sxemasi
Kirish T_0 (64 bit)=t_1 (0)t_2(0)…t_{64}(0)
T_0 (64 bit)=$T_0 \oplus k_н = t_1$ (0)t_2(0)…t_{64}(0)
L_0 (32 bit)=t_1 (0)…t_{32}(0)= a_1(0)…a_{32}(0)
R_0 (32 bit)=t_{33} (0)…t_{64}(0)= b_1(0)…b_{32}(0)
$f(R_0, k_{p1})$
k_{p1}
$L_1= R_0$
$R_1= L_0 \oplus f(R_0,k_{p1})$
$f(R_1, k_{p2})$
k_{p2}
$L_2= R_1$
$R_2= L_1 \oplus f(R_1,k_{p2})$
$L_7= R_6$
$R_7= L_6 \oplus f(R_6,k_{p7})$
$f(R_7, k_{p8})$
k_{p8}
$L_8= R_7$
$R_8= L_7 \oplus f(R_7,k_{p8})$
$T_к$ =(R_8, L_8)
$T_ш$ (64 bit)=$T_к \oplus k_к$

Algoritm shifrlash jarayonining keltirilgan umumiy sxemasida $T_к = (R_8, L_8)$ va 64-bitli T_{sh} - blok ifodasi $T_ш = T_к \oplus k_k = (R_8, L_8) \oplus k_k$ aniqlangan. Bunday aniqlanishlar apparat-dasturiy qurilmalardan foydalanib shifrlash va deshifrlash jarayonlarini amalga oshirishning qulayligini ta'minlash bilan bog'liq. Haqiqatan ham, kiruvchi blok sifatida $T_ш$-blok va boshlang'ich kalit sifatida k_k olinib, raund kalitlari teskarisiga qo'llanilib: 1-raundda k_{p8}, 2-raundda k_{p7}, …, 8-raundda k_{p1} hamda oxirgi kalit sifatida $k_и$-kalit ishlatilib, deshifrlash jarayoni xuddi shifrlash jarayoni kabi amalga oshiriladi.

Kriptobardoshlilikni oshirish maqsadida, har bir blokni shifrlashdan oldin 256-bitli k-kalitni, bitlari sonini saqlagan holda, λ-bitga (bu erda $3 \le \lambda \prec 255$) surish mumkin. Bunday surish ochiq ma'lumot bloklarini har-xil kalitlar bilan shifrlash imkoniyatini beradi.

Taklif etilgan algoritm Feystel tarmog'i funksiyasining asosiy akslantirishlari ochiq ma'lumot va uning akslantirishlarining bloki oraliq qiymatlari bitlarini raund kalitlarining mos bitlari bilan mod 2 bo'yicha qo'shish kabi amallarga qo'shimcha tarzda xarakteristikasi 256 bo'lgan chekli maydonda aniqlangan matritsali akslantirish, S-blok hamda SJ akslantirishlari amaliy jihatdan bir tomonlama akslantirishlar hisoblanadi. Bundan tashqari S-blok va SJ yuqori chiziqsizlikni ta'minlovchi akslantirishlardir, hamda, XOR amali akslantirishi yuqori korrelyasiya immunitetini ta'minlaydi, matritsali akslantirish yuqori bo'lmagan chiziqsizlik va korrelyasiya immunitetlarini ta'minlab, ko'proq tarqalish tamoilini ta'minlaydi.

Yuqorida ta'kidlaganidek, to'g'ri to'rtburchakli $A_{n\times 4}$-matritsa (bu erda $n = 2^m$, $m = 2,...,M$, $M < \infty$), S – blok va SJ dastlabki kalitdan generatsiya qilinishi ta'kidlagan edi. Quyida ularni generatsiya qilish qoidalari keltiriladi.

To'g'ri to'rtburchakli $A_{n\times 4}$ matritsa elementlari a_{ij} $(i = 1,..., n;\ j = 1,2,3,4;)$ baytlardan iborat bo'lib, ularning soni $4n$ ta :

1) m=3 bo'lganda n=2^3 =8 bo'lib, matritsa elementlari soni 32 tadan iborat, ularni 256-bitli dastlabki kalitni 32 ta baytga ajratib, juft-jufti bilan har-xil

bo‘laklaridan, har bir satrda kamida bitta toq qiymatli element bo‘ladigan qilib olinadi;

2) m=4 bo‘lganda n=2^4 =16 bo‘lib, matritsa elementlari soni 64 tadan iborat, ularni 256-bitli dastlabki kalitni biror λ-bitga bitlari sonini yo‘qotmasdan (siklik) surib, so‘ngra baytlarga ajratib, juft-jufti bilan har-xil bo‘lganlaridan oldingi 32 tagacha bo‘lgan elementlarini, oldin λ-bitga surilgan 256-bitli blokni yana λ-bitga surib, baytlarga ajratib, juft-jufti bilan har-xil bo‘laklaridan keyingi 32 tagacha bo‘lgan elementlarni har bir satrda kamida bitta toq qiymatli element hamda matritsaning hamma elementlari har-xil bo‘ladigan qilib olinadi va hokazo.

Shu keltirilgan qoida bo‘yicha $A_{n\times 4}$ ($n=2^m$, $m=2,...,M$, $M \prec \infty$) matritsaning barcha elementlarii hosil qilinadi.

Endi S-blok generatsiyasiga o‘tamiz. Dastlabki 256-bitli kalitni baytlarga ajratib, hosil bo‘lgan baytlar qiymatlarini juft-jufti bilan solishtirib, soni 32 tadan ortiq bo‘lmagan har-xil baytlar bilan S-blok yacheykalari to‘ldiriladi. So‘ngra, dastlabki kalit bitlari sonini yo‘qotmagan holda λ=1 bitga surilib, hosil bo‘lgan blokni baytlarga ajratib, hosil bo‘lgan baytlar qiymatlarini S – blokning to‘ldirilgan yacheykalaridagi qiymatlarga solishtirib, ulardan farqli bo‘lgan baytlar bilan bo‘sh yacheykalarni ketma-ket to‘ldiriladi. Bu jarayonni dastlabki kalit blokining bitlari sonini yo‘qotmagan holda λ=2, λ=3, ..., λ=255 bitlarga surish bilan S-blok yacheykalarini hammasi to‘lgunicha davom ettiriladi. Agar shunda ham S-blok yacheykalari oxirigacha to‘lmasa, u holda qolgan yacheykalar S-blokning to‘ldirilgan yacheykalarida uchramagan baytlar bilan oxirigacha to‘ldiriladi. Buning uchun, ushbu $y = x^z \bmod 257$ formula bo‘yicha $\{0 \le y \le 256 : y = x^z \bmod 257,\ z = const,\ 0 \le x \le 256\}$ -to‘plam elementlari ketma-ket hisoblanadi, bu erda $0 \le x \le 256$, $z = const$ bo‘lib, u kalit bilan birgalikda uzatiladi. So‘ngra, $\{0 \le \gamma \le 255 : \gamma = y \bmod 256,\ 0 \le y \le 256\}$ -to‘plamning γ -elementlari S – blokning to‘lgan yacheykalaridagi baytlar qiymatlari bilan solishtirilib, ulardan farqli bo‘lgan baytlar bilan ketma-ket to‘ldiriladi.

SJ generatsiyasi 256-bitli dastlabki kalitni 64 ta yarim baytli bloklarga ajratib, juft-jufti bilan har-xil bo‘lgan 16 ta yarim bayt bilan 1-satr, keyingi juft-jufti bilan har-xil bo‘lgan 16 ta yarim bayt bilan 2-satr va hokazo 16-satr to‘ldiriladi. Bunda, SJ satr va ustunlarida, hamda, bosh diagonallar elmentlarida bir xildagi yarim baytlarning takrorlanmasligi hisobga olinadi.

Ta’kidlash joizki, to‘g‘ri to‘rtburchakli matritsa $A_{n\times 4}$ (bu erda: $n = 2^m$, $m = 2,...,M,\ M < \infty$) , S – blok va SJ dastlabki kalitdan oldindan hisoblangan holda shu kalit bilan birgalikda uzatilishi mumkin yoki dastlabki kalitga bog‘liq bo‘lmagan holda ularning yuqorida keltirilgan xossalarini ta’minlash orqali generatsiya qilinishi mumkin.

Yuqoridagi paragraflarda Feystel tarmog‘iga asoslangan simmetrik blokli shifrlash algoritmlari va ularning asosiy akslantirishlari ko‘rib o‘tildi. Keyingi paragrafda Feystel tarmog‘iga asoslanmagan AES-FIPS 197 va boshqa algoritmlar keltirilgan.

3.4. AES-FIPS 197 standart simmetrik blokli shifrlash algoritmi

DES blokli shifrlash algoritmi 1999 yilgacha AQSHda standart shifrlash algoritmlari sifatida ishlatib kelingan.

1974 yildan Amerika qo‘shma shtatlarining standart shifrlash algoritmi sifatida qabul qilingan DES shifrlash algoritmi quyidagi :

- kalit uzunligining kichigligi, ya’ni 56 bit bo‘lib, uning 128 bitdan kichikligi;

- S-blok akslantirishlarining differensial kriptotahlil usuliga bardoshsizligi va boshqa sabablarga ko‘ra eskirgan deb sanaladi. Ayniqsa 1999 yilda DES shifrlash algoritmi yordamida shifrlangan maьlumotning Internet tarmog‘iga ulangan 300 ta paralel kompyuter tomonidan 24 soat davomida ochilishi haqidagi ma’lumotning tasdiqlanishi bundan keyin mazkur standart algoritmi yordamida ma’lumotlarni kriptografik muhofaza qilish masalasini qaytadan ko‘rib chiqish va yangi standart qabul qilish zaruratini keltirib chiqardi.

Amerika qo‘shma shtatlarining “Standartlar va texnologiyalar Milliy Instituti

(NIST)” tomonidan 1997 yilda XXI asrning ma’lumotlarni kriptografik muhofazalovchi yangi shifrlash algoritmi standartini qabul qilish maqsadida tanlov e’lon qilindi. 2000 yilda standart shifrlash algoritmi qilib RIJNDAEL shifrlash algoritmi asos qilib olingan AES (Advanced Encryption Standard) (FIPS 197) qabul qilindi. Algoritmning yaratuvchilari Belgiyalik mutaxassislar Yon Demen (Joan Daemen) va Vinsent Ryumen (Vincent Rijmen)larning familiyalaridan RIJNDAEL nomi olingan.

AES FIPS 197 blokli shifrlash algoritmida 8 va 32-bitli (1-baytli va 4-baytli) vektorlar ustida amallar bajariladi. AES FIPS 197 shifrlash algoritmi XXI asrning eng barqaror shifrlash algoritmi deb hisoblanadi. Bu algoritm boshqa mavjud standart simmetrik shifrlash algoritmlaridan farqli o‘laroq, Feystel tarmog‘iga asoslanmagan blokli shifrlash algoritmlari qatoriga kiradi.

3.5. AES kriptoalgoritmining matematik asosi

AES algoritmida baytlar ustida amallar bajariladi. Baytlar $GF(2^8)$ chekli maydon elementlari sifatida qaraladi. $GF(2^8)$ maydon elementlarini darajasi 7 dan katta bo‘lmagan ko‘phad sifatida tasvirlash mumkin. Agarda baytlar

$$\{a_7a_6a_5a_4a_3a_2a_1a_0\}, a_i \in \{0,1\}, i = \overline{0...7},$$

ko‘rinishda tasvirlangan bo‘lsa, u holda maydon elementlari quyidagicha ko‘phad ko‘rinishda yoziladi:

$$a_7 \cdot x^7 + a_6 \cdot x^6 + a_5 \cdot x^5 + a_4 \cdot x^4 + a_3 \cdot x^3 + a_2 \cdot x^2 + a_1 \cdot x + a_0 .$$

Misol uchun $\{11010101\}$ baytga $x^7 + x^6 + x^4 + x^2 + a_0$ ko‘rinishdagi ko‘phad mos keladi.

CHekli $GF(2^8)$ maydon elementlari uchun additivlik va mulьtiplikativlik xossalariga ega bo‘lgan qo‘shish va ko‘paytirish amallari aniqlangan.

Ko‘phadlarni qo‘shish

AES algoritmida ko‘phadlarni qo‘shish $\oplus$ **(XOR)** (berilgan ko‘phadlarga mos keluvchi ikkilik sanoq tizimidagi sonlarning mos bitlarini mod 2 bo‘yicha

qo‘shish) amali orqali bajariladi. Masalan, $x^7 + x^6 + x^4 + x^2 + x$ va $x^7 + x^5 + x^3 + x + 1$ ko‘phadlar natijasi quyidagicha hisoblanadi:

$$(x^7 + x^6 + x^4 + x^2 + x) \oplus (x^7 + x^5 + x^3 + x + 1) = (x^6 + x^5 + x^4 + x^3 + x^2 + 1)$$

Bu amal ikkilik va o‘n oltilik sanoq sistemalarida quyidagicha ifodalanadi:

$\{11010110\}_2 \oplus \{10101011\}_2 = \{01111101\}_2$ va $D6_{16} \oplus AB_{16} = 7D_{16}$.

CHekli maydonda istalgan nolga teng bo‘lmagan a element uchun unga teskari bo‘lgan $-a$ element mavjud va $a + (-a) = 0$ tenglik o‘rinli, bu erda nolь elementi sifatida $\{00\}_{16}$ qaraladi. $GF(2^8)$ maydonda $a \oplus a = 0$ tenglik o‘rinli.

Ko‘phadlarni ko‘paytirish

AES algoritmida ko‘phadlarni ko‘paytirish quyidagicha amalga oshiriladi:

–ikkita ko‘phad o‘nlik sanoq tizimida ko‘paytiriladi;

– ettinchi darajadan katta bo‘lgan har qanday ko‘phadni sakkizinchi darajali $\varphi(x) = x^8 + x^4 + x^3 + x + 1$ keltirilmaydigan ko‘phadga bo‘lganda qoldiqda etti va undan kichik bo‘lgan darajadagi ko‘phadlar hosil bo‘lib, ular natija sifatida olinadi, bunda bo‘lish jarayonida bajariladigan ayirish amali ikkilik sanoq tizimida, yuqorida keltirilgani kabi, $\oplus$ amali asosida bajariladi.

SHunday qilib kiritilgan ko‘paytirish amali $\bullet$ bilan belgilanadi.

Masalan, $(x^6 + x^4 + x^2 + x + 1)$ va $(x^7 + x + 1)$ ko‘phadlar quyidagicha ko‘paytiriladi:

- bu ko‘phadlar o‘nlik sanoq tizimida ko‘paytiriladi

$$(x^6 + x^4 + x^2 + x + 1) \bullet (x^7 + x + 1) = (x^{13} + x^{11} + x^9 + x^8 + x^6 + x^5 + x^4 + x^3 + 1);$$

- natija $\varphi(x) = x^8 + x^4 + x^3 + x + 1$ keltirilmaydigan ko‘phadga bo‘linadi va qoldiq olinadi

$$(x^{13} + x^{11} + x^9 + x^8 + x^6 + x^5 + x^4 + x^3 + 1) \bmod (x^8 + x^4 + x^3 + x + 1) = (x^7 + x^6 + 1).$$

Haqiqatan ham $(x^{13} + x^{11} + x^9 + x^8 + x^6 + x^5 + x^4 + x^3 + 1) = (x^5 + x^3) \bullet$

$$\bullet (x^8 + x^4 + x^3 + x + 1) \oplus (x^7 + x^6 + 1).$$

Har qanday nolga teng bo‘lmagan element uchun $a \bullet 1 = a$, tenglik o‘rinli. $GF(2^8)$ maydonda bir element sifatida $\{01\}_{16}$ tushuniladi.

Kiritilgan ko‘paytirish amali umumiy holda quyidagicha bajariladi. Ixtiyoriyettinchidarajali

$$a_7x^7+a_6\,x^6+\,a_5\,x^5+\,a_4\,x^4+\,a_3\,x^3+\,a_2\,x^{\,2}+a_1x+\,a_0$$

ko‘phadni x ga ko‘paytirib, quyidagiga ega bo‘lamiz

$$a_7x^8+a_6\,x^7+\,a_5\,x^6+\,a_4\,x^5+\,a_3\,x^4+\,a_2\,x^3+\,a_1x^2+\,a_0\,x.$$

Bu ko‘phadni $\varphi(x)= x^8+x^4+x^3+x+1=1\{1b\}$ modul bo‘yicha hisoblab, chekli $GF(2^8)$ maydonga tegishli elementni hosil qilamiz. Buning uchun $a_7=1$ bo‘lganda $\varphi(x)= x^8+x^4+x^3+x+1$ ko‘phadni yuqorida olingan sakkizinchi darajali ko‘phaddan *XOR* amali bilan ayirishkifoya, ya’ni :

$$(a_7\oplus1)x^8+(a_6\oplus0)\,x^7+(a_5\oplus0)\,x^6+(a_{\,4}\oplus0)\,x^5+(a_3\oplus1)\,x^{\,4}\,+(a_2\oplus1)\,x^3+$$

$$+\,(\,a_1\oplus0)x^2+\,(a_0\oplus1)x+1=(a_6\oplus0)\,x^7+(a_5\oplus0)\,x^6+(a_{\,4}\oplus0)\,x^5+$$

$$+(a_3\oplus1)\,x^{\,4}\,+(a_2\oplus1)\,x^3+\,(\,a_1\oplus0)x^2+\,(a_0\oplus1)x+1,$$

bu erda $a_7=1$ bo‘lgani uchun

$$(a_7\oplus1)x^8=(1\oplus1)x^8=0.$$

Agarda $a_7=0$ bo‘lsa, u holda natija: $a_6\,x^7+\ldots+a_1x^2+\,a_0\,x$ ko‘phadning o‘zi bo‘ladi.

Ushbu *x time*() funksiya yuqorida kiritilgan ko‘paytirish amaliga nisbatan berilgan ko‘phadni x ga ko‘paytirishni ifodalasin. Shu funksiyani n marta qo‘llab x^n ga ko‘paytirish amali aniqlanadi. Bevosita hisoblash bilan quyidagilarning o‘rinli ekanligiga ishonch hosil qilish mumkin:

$$\{57\}\bullet\{13\}=\{fe\},$$

chunki

$$\{57\}\bullet\{02\}=x\ time\ (\{57\})=\{ae\}$$
$$\{57\}\bullet\{04\}=x\ time\ (\{ae\})=\{47\}$$

$$\{57\}\bullet\{08\}=x\ time\ (\{47\})=\{8e\}$$

$$\{57\}\bullet\{10\}=x\ time\ (\{8e\})=\{07\},$$

bundan

$$\{57\}\bullet\{13\}=\{57\}\bullet(\{01\}\oplus\{02\}\oplus\{10\})=\{57\}\oplus\{ae\}\oplus\{07\}=\{fe\}.$$

Yuqorida ta'kidlanganidek algoritm akslantirishlari baytlar va to'rt baytli so'zlar ustida bajariladi. To'rt baytli so'zlarni koeffitsientlari $GF(2^8)$ chekli maydondan olingan darajasi uchdan katta bo'lmagan ko'phadlar ko'rinishida ifodalash mumkin:

$a(x) = a_3 x^3 + a_2 x^2 + a_1 x + a_0$,

buerda $a_i = (a_7^i a_6^i a_5^i a_4^i a_3^i a_2^i a_1^i a_0^i)$, $a_j^i \in \{0;1\}$, $i=0,1,2,3$; $j=0, 1, \ldots,7$.

Bunday ikkita ko'phadlarni qo'shish o'xshash hadlar oldidagi koeffitsientlarni $\oplus$ amali bilan qo'shish orqaliamalga oshiriladi, ya'ni:

$$a(x)+b(x)=(a_3\oplus b_3)x^3+(a_2\oplus b_2)x^2+(a_1\oplus b_1)x+(a_0\oplus b_0).$$

Ko'paytirish amali quyidagicha amalga oshiriladi. Ikkita to'rt baytli so'zlar mos ko'phadlar bilan ifodalangan bo'lsin:

$a(x) = a_3 x^3 + a_2 x^2 + a_1 x + a_0$ i$b(x) = b_3 x^3 + b_2 x^2 + b_1 x + b_0$.

Ko'paytirish natijasi oltinchi darajadan katta bo'lmagan ko'phad

$$a(x)\,b(x) = s(x) = c_6 x^6 + c_5 x^5 + c_4 x^4 + c_3 x^3 + c_2 x^2 + c_1 x + c_0,$$

bo'lib, bu yerda $c_0 = a_0 \bullet b_0$, $c_1 = a_1 \bullet b_0 \oplus a_0 \bullet b_1$, $c_2 = a_2 \bullet b_0 \oplus a_1 \bullet b_1 \oplus a_0 \bullet b_2$, $c_3 = a_3 \bullet b_0 \oplus a_2 \bullet b_1 \oplus a_1 \bullet b_2 \oplus a_0 \bullet b_3$, $c_4 = a_3 \bullet b_1 \oplus a_2 \bullet b_2 \oplus a_1 \bullet b_3$, $c_5 = a_3 \bullet b_2 \oplus a_2 \bullet b_3$, $c_6 = a_3 \bullet b_3$.

Ko'paytirish natijasi to'rt baytli so'zdan iborat bo'lishi uchun, uchinchi darajadan katta bo'lgan har qanday ko'phadni to'rtinchi darajali $\varphi(x) = x^4+1$ keltirilmaydigan ko'phadga bo'lganda qoldiqda uchinchi va undan kichik bo'lgan darajadagi ko'phadlar hosil bo'lishini hisobga olgan holda, ular natija sifatida

olinadi, bunda bo‘lish jarayonida bajariladigan ayirish amali ikkilik sanoq tizimida, yuqorida keltirilgani kabi, $\oplus$ amali asosida bajariladi.

Quyidagi ifoda o‘rinli:

$$x^{i} \bmod (x^4+1) = x^{i \bmod 4}.$$

Shunday qilib, $a(x)$ va $b(x)$ ko‘phadlarni $\otimes$-kupaytmasini ifodalovchi

$a(x) \otimes b(x) = d(x) = d_3 x^3 + d_2 x^2 + d_1 x + d_0$,

natijaviy $d(x)$ –ko‘phadkoeffitsientlariquyidagichaaniqlanadi:

$d_0 = a_0 \bullet b_0 \oplus a_3 \bullet b_1 \oplus a_2 \bullet b_2 \oplus a_1 \bullet b_3$, $d_1 = a_1 \bullet b_0 \oplus a_0 \bullet b_1 \oplus a_3 \bullet b_2 \oplus a_2 \bullet b_3$, $d_2 = a_2 \bullet b_0 \oplus a_1 \bullet b_1 \oplus a_0 \bullet b_2 \oplus a_3 \bullet b_3$, $d_3 = a_3 \bullet b_0 \oplus a_2 \bullet b_1 \oplus a_1 \bullet b_2 \oplus a_0 \bullet b_3$.

Yuqorida keltirilgan amallarni matritsa ko‘rinishida quyidagicha ifodalash mumkin:

$$\begin{bmatrix} d_0 \\ d_1 \\ d_2 \\ d_3 \end{bmatrix} = \begin{bmatrix} a_0 & a_3 & a_2 & a_1 \\ a_1 & a_0 & a_3 & a_2 \\ a_2 & a_1 & a_0 & a_3 \\ a_3 & a_2 & a_1 & a_0 \end{bmatrix} \bullet \begin{bmatrix} b_0 \\ b_1 \\ b_2 \\ b_3 \end{bmatrix}$$

Kvadrat arxitekturaga ega AES blokli shifrlash algoritmi o‘zgaruvchan uzunlikdagi kalitlar orqali shifrlanadi. Kalit va blok uzunliklari bir-biriga bog‘liq bo‘lmagan holda 128, 192 yoki 256 bit bo‘ladi. Biz AES shifrlash algoritmini bloklar uzunligi 128 bit bo‘lgan hol uchun ko‘rib chiqamiz.

Blok o‘lchami 128 bitga teng kirish bu 16 baytli massiv 4 ta qator va 4 ta ustundan iboratdir (har bir satr va har bir ustun bu holda 32 bitli so‘z deb qaraladi).

Shifrlash uchun kirayotgan ma’lumot baytlari:

$$s_{00}, s_{10}, s_{20}, s_{30}, s_{01}, s_{11}, s_{21}, s_{31}, s_{02}, s_{12}, s_{22}, s_{32}, s_{03}, s_{13}, s_{23}, s_{33},$$

ko‘rinishida belgilanadi.

Kirayotgan ma’lumot quyidagi *1 – jadval* kvadrat massiv ko‘rinishida kiritiladi. Ya’ni, baytlarni tartib bilan ustun bo‘yicha to‘ldirib boriladi. Birinchi to‘rtta bayt (s_{00} , s_{10} , s_{20} , s_{30}) birinchi ustunga mos tushadi, ikkinchi to‘rtta bayt (s_{01} , s_{11}, s_{21}, s_{31}) ikkinchi ustunga mos tushadi, uchinchi to‘rtta bayt (s_{02} , s_{12} , s_{22} ,

s_{32}) uchinchi ustunga mos tushadi, to‘rtinchi to‘rtta bayt (s_{03} , s_{13} , s_{23} , s_{33}) to‘rtinchi ustunga mos tushadi.

s_{00}	s_{01}	s_{02}	s_{03}
s_{10}	s_{11}	s_{12}	S_{13}
s_{20}	s_{21}	s_{22}	s_{23}
s_{30}	s_{31}	s_{32}	s_{33}

1 – jadval. Kirayotgan ma’lumotlarning holat jadvali.

Xuddi shunday tartibda shifrlash kaliti ham kvadrat jadval shaklida kiritiladi. Ular 128 bit = 16 bayt = 4 so‘z (to‘rtta 32 bitlik blok) dan iborat:

k_{00} ,k_{10} , k_{20} , k_{30} , k_{01} , k_{11}, k_{21}, k_{31}, k_{02} , k_{12} , k_{22} , k_{32} , k_{03} , k_{13} , k_{23} , k_{33} .

K_{00}	k_{01}	k_{02}	k_{03}
K_{10}	k_{11}	k_{12}	k_{13}
K_{20}	k_{21}	k_{22}	k_{23}
K_{30}	k_{31}	k_{32}	k_{33}

2 – jadval. Shifrlash kaliti holat jadvali.

Shuningdek, AES shifrlash algoritmining raundlar soni N_r , kirish bloklar o‘lchami $N_b$va kalit uzunligi $N_k$ga bog‘liq holda quyidagi 3-jadvalga mos holda qo‘llaniladi.

N_r	N_b=4 128 bit	N_b=6 192 bit	N_b=8 256 bit
N_k=4 128 bit	10	12	14
N_k=6 192 bit	12	12	14

N_k=8 256 bit	14	14	14

3 – jadval. **Raund akslantirishlari**

Har bir raund shifrlash jarayonlari quyida keltirilgan to‘rtta akslantirishlardan foydalanilgan holda amalga oshiriladi:

1) ***SubBytes*** – algoritmda qayd etilgan 16x16 o‘lchamli jadval asosida baytlarni almashtirish, ya’ni S -blok akslantirishlarini amalga oshirish;

2) ***ShiftRows*** – algoritmda berilgan jadvalga ko‘ra holat baytlarini siklik surish;

3) ***MixColumns*** – ustun elementlarini aralashtirish, ya’ni algoritmda berilgan matritsa bo‘yicha akslantirishni amalga oshirish;

4) ***AddRoundKey –*** raund kalitlarini qo‘shish, ya’ni bloklar mos bitlarni ***XOR*** amali bilan qo‘shish.

Quyida keltirilgan akslantirishlarning matematik modellari va ularning umumiy qo‘llanilish sxemalari ko‘rib chiqiladi.

SubBytes **(S -blok akslantirishlari jadvali) –** akslantirishi har bir holat baytlariga bog‘liqsiz holda baytlarni chiziqli bo‘lmagan amallar asosida o‘rin almashtirishlarni amalga oshiradi. Bu jarayon ikki bosqichdan iborat bo‘lib:

a) har bir s_{ij}holat baytining mod $(x^8+x^4+x^3+x+1)$ bo‘yicha s_{ij}^{-1} teskarisi topiladi

$s_{ij}\, s_{ij}^{-1} \equiv 1 \bmod (x^8+x^4+x^3+x+1)$;

b) har bir s_{ij} ni teskarisi bo‘lgan s_{ij}^{-1} ni $b = s_{ij}^{-1}$ deb belgilab olib, bir baytdan iborat bo‘lgan b sonini uning bitlari orqali $b = (b_0, b_1, \ldots, b_7)$ ko‘rinishda tasvirlab, uning ustida quyidagi affin akslatirishibajariladi

$Cb + c (\bmod x^8 + 1) = b'$

Bu erda $C = \begin{bmatrix} 1&0&0&0&1&1&1&1 \\ 1&1&0&0&0&1&1&1 \\ 1&1&1&0&0&0&1&1 \\ 1&1&1&1&0&0&0&1 \\ 1&1&1&1&1&0&0&0 \\ 0&1&1&1&1&1&0&0 \\ 0&0&1&1&1&1&1&0 \\ 0&0&0&1&1&1&1&1 \end{bmatrix}$ -matritsa va $c = (c_0, c_1, \ldots, c_7) = (1,1,0,0,0,1,1,0)$ – vektor algoritmda berilgan o‘zgarmas ifodaga ega bo‘lib, keltirilgan afin akslantirishi

$$\begin{bmatrix} 1&0&0&0&1&1&1&1 \\ 1&1&0&0&0&1&1&1 \\ 1&1&1&0&0&0&1&1 \\ 1&1&1&1&0&0&0&1 \\ 1&1&1&1&1&0&0&0 \\ 0&1&1&1&1&1&0&0 \\ 0&0&1&1&1&1&1&0 \\ 0&0&0&1&1&1&1&1 \end{bmatrix} \begin{bmatrix} b_0 \\ b_1 \\ b_2 \\ b_3 \\ b_4 \\ b_5 \\ b_6 \\ b_7 \end{bmatrix} + \begin{bmatrix} 1 \\ 1 \\ 0 \\ 0 \\ 0 \\ 1 \\ 1 \\ 0 \end{bmatrix} (\text{mod } 257) = \begin{bmatrix} b_0' \\ b_1' \\ b_2' \\ b_3' \\ b_4' \\ b_5' \\ b_6' \\ b_7' \end{bmatrix}$$

ko‘rinishda amalga oshiriladi.

Natijaviy $b' = (b_0', b_1', \ldots, b_7')$ vektorning koordinatalari

$$b_i' = b_i \oplus b_{(i+4) \bmod 8} \oplus b_{(i+5) \bmod 8} \oplus b_{(i+6) \bmod 8} \oplus b_{(i+7) \bmod 8} \oplus c_i, \qquad i=0,1,2,\ldots,7;$$

ifoda bilan ratsional hisoblanadi.

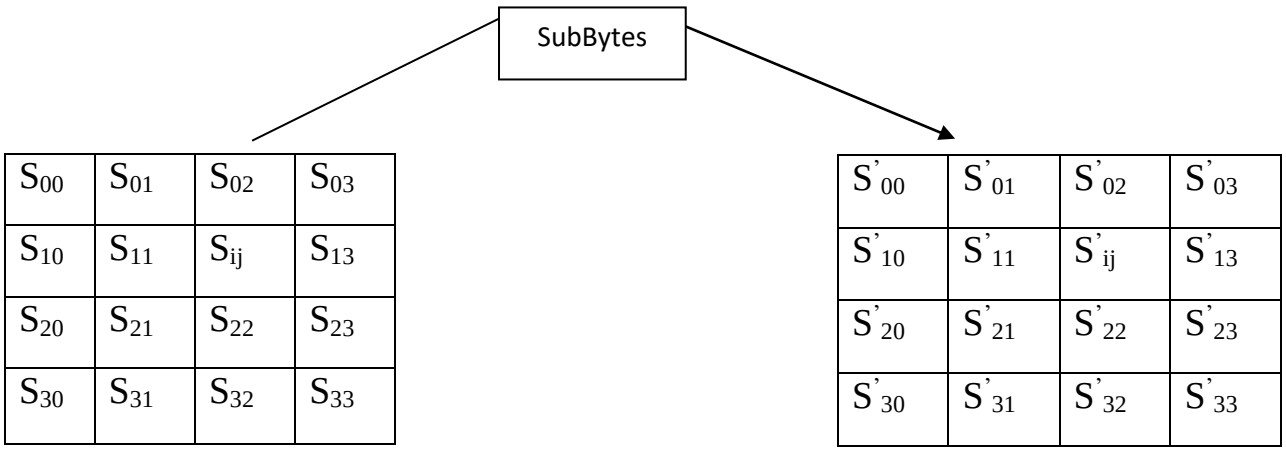
Yuqoridagi a) va b) qismlarda berilgan barcha mantiqiy va arifmetik amallarni bajarish bilan amalga oshiriladigan o‘rniga qo‘yish akslantirishi 4 - jadvaldagi*S* -blok akslantirishlariga (almashtirishlariga) keltirilgan. Bu esa algoritmning dasturiy ta’minoti va apparat qurilmasini yaratishda qulaylik tug‘diradi.

S -blok akslantirishlaridan foydalanib berilgan s –baytni 16-lik sanoq tizimida $s=(s_0 s_1 s_2 s_3 s_4 s_5 s_6 s_7) = \{s_0 s_1 s_2 s_3, s_4 s_5 s_6 s_7\} = \{xy\}$ kabi ifodalab *x*-satr va *y*-ustunlar kesishmasidagi baytlar almashtirish natijasi sifatida olinadi. Misol uchun *{62}* - ni *{aa}* ga ga almashtiriladi.

X	Y															
	0	**1**	**2**	**3**	**4**	**5**	**6**	**7**	**8**	**9**	**A**	**b**	**c**	**d**	**e**	**F**
0	63	7c	77	7b	12	6b	6f	C5	30	01	67	2b	fe	d7	ab	76
1	Ca	82	c9	7d	Fa	59	47	F0	ad	d4	a2	af	9c	a4	72	c0
2	b7	Fd	93	26	36	3f	F7	Cc	34	a5	e5	f1	71	d8	31	15
3	04	c7	23	c3	18	96	05	9a	07	12	80	e2	eb	27	b2	75
4	09	83	2c	1a	1b	62	5a	a0	52	3b	d6	b3	29	e3	2f	84
5	53	d1	00	ed	20	Fc	b1	5b	6a	Cb	Be	39	4a	4c	58	cf
6	d0	Ef	aa	fb	43	4d	33	85	45	f9	02	7f	50	3c	9f	a8
7	51	a3	40	8f	92	9d	38	f5	bc	b6	Da	21	10	ff	f3	d2
8	Cd	0c	13	ec	5f	97	44	17	c4	a7	7e	3d	64	5d	18	73
9	60	81	4f	dc	22	2a	90	88	46	Ee	b8	14	de	5e	0b	db
a	e0	32	3a	0a	49	06	24	5c	c2	d3	Ac	62	91	95	e4	79
b	e7	c8	37	6d	8d	D5	4e	a9	6c	56	f4	ea	65	7a	ae	08
c	Ba	78	25	2e	1c	A6	b4	c6	e8	Dd	74	1f	4d	bd	8b	8a
d	70	3e	b5	66	48	03	F6	0e	61	35	57	b9	86	c1	1d	9e
e	e1	f8	98	11	69	D9	8e	94	9b	1e	87	e9	ce	55	28	df
f	8c	a1	89	0d	Bf	E6	42	68	41	99	2d	0f	b0	54	bb	16

4 – jadval. S - blok almashtirish jadvali.

SubBytes **(S -blok akslantirishlari jadvali)** baytlarni almashtirish jarayonining umumiy sxemasini quyidagicha tasvirlash mumkin



***ShiftRows* (Holat baytlarinissiklik surish)** akslantirishining qo‘llanilishi quyidagicha amalga oshiriladi. Holat baytlarinissiklik surishda holat jadvali satrlari quyidagicha belgilab olinadi.

C_0-satr	S'_{00}	S'_{01}	S'_{02}	S'_{03}
C_1-satr	S'_{10}	S'_{11}	S'_{12}	S'_{13}
C_2-satr	S'_{20}	S'_{21}	S'_{22}	S'_{23}
C_3-satr	S'_{30}	S'_{31}	S'_{32}	S'_{33}

5 – jadval.

***ShiftRows* (Holat baytlarinissiklik surish)** akslantirishida jadvaldagi oxirgi uchta satr har bir baytlari chapgassiklik , ya’ni 1- satr C_1 baytga, 2- satr C_2 baytga, 3- satr C_3 baytga suriladi. C_1 , C_2 , C_3 surilish qiymati N_b blok uzunligiga bog‘liq. bo‘lib, ular algoritmda ko‘rsatilganidek, quyidagi 6-jadvalda aniqlangan:

l	N_b	C_0	C_1	C_2	C_3
128	4	0	1	2	3
192	6	0	1	2	3
256	8	0	1	3	4

6 – jadval.

Keltirilgan jadvalga ko‘ra $l = 128$ *bitli* shifrlash uchun $N_b=4$ ga teng bo‘lib, birinchi satr bo‘yicha holat baytlarinissiklik surish bajarilmaydi, ikkinchi satr bo‘yicha 1 baytga, uchinchi satr bo‘yicha 2 baytga, to‘rtinchi satr bo‘yicha 3 baytga ssiklik surish amalga oshiriladi.

l = 192 bitli shifrlash uchun $N_b=6$ ga teng bo‘lib, birinchi satr bo‘yicha holat baytlarinissiklik surish bajarilmaydi, ikkinchi satr bo‘yicha 1 baytga, uchinchi satr bo‘yicha 2 baytga, to‘rtinchi satr bo‘yicha 3 baytga ssiklik surish bajariladi.

l = 256 bitli shifrlash uchun $N_b=8$ ga teng bo‘lib birinchi satr bo‘yicha holat baytlarinissiklik surish bajarilmaydi, ikkinchi qator bo‘yicha 1 baytga, uchinchi satr bo‘yicha 3 baytga, to‘rtinchi satr bo‘yicha 4 baytga ssiklik surish amalga oshiriladi.

4.7 – jadvaldaesa *l = 128 bitli* shifrlash uchun $N_b=4$ ga teng bo‘lganda, satrlarni ssiklik surish bajarilgandan keyingi baytlarning o‘rni qay tarzda o‘zgarishi keltirilgan

S'_{00}	S'_{01}	S'_{02}	S'_{03}
S'_{10}	S'_{11}	S'_{12}	S'_{13}
S'_{20}	S'_{21}	S'_{22}	S'_{23}
S'_{30}	S'_{31}	S'_{32}	S'_{33}

ShiftRows →

S'_{00}	S'_{01}	S'_{02}	S'_{03}
S'_{11}	S'_{12}	S'_{13}	S'_{10}
S'_{22}	S'_{23}	S'_{20}	S'_{21}
S'_{33}	S'_{30}	S'_{31}	S'_{32}

7 – jadval.

MixColumns **(Ustun elementlarini aralashtirish) akslantirish**da holat ustunlari elementlari uchinchi darajadan katta bo‘lmagan ko‘phadning koeffitsientlari sifatida ifodalanib, ana shu ko‘phad algoritmda berilgan:

$g(x) = \{03\}x^3 + \{01\}x^2 + \{01\}x + \{02\}$

ko‘phadga x^4+1 moduль bo‘yicha ko‘paytiriladi.

Quyidagicha belgilash kiritilib:

$$s_{00} = s'_{00},\ s_{10} = s'_{11},\ s_{20} = s'_{22},\ s_{30} = s'_{33},$$

$$s_{01} = s'_{01},\ s_{11} = s'_{12},\ s_{21} = s'_{23},\ s_{31} = s'_{30},$$

$$s_{02} = s'_{02},\ s_{12} = s'_{13},\ s_{22} = s'_{20},\ s_{32} = s'_{31},$$

$$s_{03} = s'_{03},\ s_{13} = s'_{10},\ s_{23} = s'_{21},\ s_{33} = s'_{32},$$

ta’kidlangan ko‘phadlar ko‘paytmasining matritsa ko‘rinishidagi ifodasi:

$$\begin{bmatrix} s'_{0j} \\ s'_{1j} \\ s'_{2j} \\ s'_{3j} \end{bmatrix} = \begin{bmatrix} \{02\} & \{03\} & \{01\} & \{01\} \\ \{01\} & \{02\} & \{03\} & \{01\} \\ \{01\} & \{01\} & \{02\} & \{03\} \\ \{03\} & \{01\} & \{01\} & \{02\} \end{bmatrix} \bullet \begin{bmatrix} s_{0j} \\ s_{1j} \\ s_{2j} \\ s_{3j} \end{bmatrix}, 0 \le c \le 3,$$

bo‘ladi, bu erda *s*- ustun nomeri.

Oxirgi tenglik

$$s'_{0c} = (\{02\} \bullet s_{0c}) \oplus (\{03\} \bullet s_{1c}) \oplus s_{2c} \oplus s_{3c},$$
$$s'_{1c} = s_{0c} \oplus (\{02\} \bullet s_{1c}) \oplus (\{03\} \bullet s_{2c}) \oplus s_{3c},$$
$$s'_{2c} = s_{0c} \oplus s_{1c} \oplus (\{02\} \bullet s_{2c}) \oplus (\{03\} \bullet s_{3c}),$$
$$s'_{3c} = (\{03\} \bullet s_{0c}) \oplus s_{1c} \oplus s_{2c} \oplus (\{02\} \bullet s_{3c},$$

tengliklarga ekvivalent.

***AddRoundKey* (Raund kalitlarini qo‘shish) akslantirish**daholat blokining bitlari kalit bloki mos bitlari bilan xarakteristikasi ikki bo‘lgan chekli maydonda qo‘shiladi, ya’ni, massivning har bir ustuni va shu ustunning elementlari kalit massivining mos ustun va elementlariga XOR amali bilan qo‘shiladi.

3.6. Kalitlar generatsiyasi algoritmi (*KeySchedule*)

Raund kalitlari daslabki kalitdan, algoritmda ko‘zda tutilgan hamma raundlar uchun yaratib olinadi. Bu jarayon:

-kalitni kengaytirish(**KeyExpansion**);

-raund kalitlarini tanlash (**RoundKeySelection**);

bosqichlaridan iborat.

Raund kalitlarining umumiy bitlari soni kirish ma’lumotining bitlari sonining raund soniga ko‘paytmasiga va yana bitta kirish ma’lumoti bitlari sonini yig‘indisiga teng (misol uchun 128 bitli shifrlash uchun 128*10+128=1408 bit raund kaliti kerak bo‘ladi), ya’ni N_b (N_r+*1*) va $l(N_r+1)=128 \cdot 11=1408$ bit.

Demak, 128 bit uzunlikdagi blok va 10 raund uchun 1408 bit raund kalitlari talab qilinadi.

Dastlabki kalitni kengaytirishda, avval 128 bitli (16 bayt, simvol) boshlang‘ich kiruvchi kalit kiritib olinadi va to‘rtta (w_1, w_2, w_3, w_4) 32 bitdan iborat bo‘lakka bo‘linadi. Qolgan kengaytirilgan kalitlar mana shu to‘rtta (w_1, w_2, w_3, w_4) kengaytirilgan kalitlar yordamida topiladi. Kengaytirilgan kalitlar soni

$$N[w(i)] = N_b(N_r + 1);$$

Biz ko‘rayotgan holatda N_b= 4, N_r= 10 ga teng ya’ni, bayt uzunligi 4 ga, raundlar soni 10 ga teng. SHularni bilgan holda $N[w(i)]$ ni topiladi:

$$N[w(i)] = 4*(10+1) = 44$$

Demak, 128 bitli kirish blokiga va 10 ta raundga ega bo‘lgan shifrlash uchun 44 ta kengaytirilgan kalitlar kerak bo‘lar ekan.

Raund kalitlari kengaytirilgan kalitlardan quyida bayon qilingan qoida asosida yaratiladi. Kalitlar generatsiyasining formulalari quyidagi ko‘rinishlarga ega:

$$w[i] = w[i-1] \oplus w[i-N_k] \qquad (2.6)$$

$$w[i] = SubWord\,(RotWord\,(w[i-1]\,)) \oplus Rcon[\,i/N_k] \oplus w[i-N_k] \qquad (2.7)$$

Bizning holatda N_k = 4 bo‘lganligi sababli i=4,8,12,16,20,… qiymatlar uchun (4.2) formuladan foydalanib, kengaytirilgan kalitlar topiladi. YA’ni, i ning 4 ga karrali, 4 ga qoldiqsiz bo‘linadigan qiymatlarida (2.5) formuladan foydalaniladi. Qolgan barcha i=5,6,7,9,10,11,13,... qiymatlarida (2.6) formuladan foydalaniladi. Bu erda $w(i)$ – 32 bit – so‘zlardan iborat.

Masalan, biz ko‘rayotgan holatda raund kalitining uzunligi 128 bit teng bo‘lib, u to‘rtta kengaytirilgan kalitga teng bo‘ladi, ya’ni,

$$128 : 32 = 4 \text{ demak, } w(i) = 1,2,3,4$$

$w_1 = W_1, W_2, W_3, W_4, W_5, W_6, W_7, W_8, W_9, W_{10}, W_{11}, W_{12}, W_{13}, W_{14}, W_{15}, W_{16}, W_{17}, W_{18}, W_{19}, W_{20}, W_{21}, W_{22}, W_{23}, W_{24}, W_{25}, W_{26}, W_{27}, W_{28}, W_{29}, W_{30}, W_{31}, W_{32};$

$w_2 = W_{33}, W_{34}, W_{35}, W_{36}, W_{37}, W_{38}, W_{39}, W_{40}, W_{41}, W_{42}, W_{43}, W_{44}, W_{45}, W_{46}, W_{47}, W_{48}, W_{49}, W_{50}, W_{51}, W_{52}, W_{53}, W_{54}, W_{55}, W_{56}, W_{57}, W_{58}, W_{59}, W_{60}, W_{61}, W_{62}, W_{63}, W_{64};$

$w_3 = W_{65}, W_{66}, W_{67}, W_{68}, W_{69}, W_7, W_{71}, W_{72}, W_{73}, W_{74}, W_{75}, W_{76}, W_{77}, W_{78}, W_{79}, W_8, W_{81}, W_{82}, W_{83}, W_{84}, W_{85}, W_{86}, W_{87}, W_{88}, W_{89}, W_9, W_{91}, W_{92}, W_{93}, W_{94}, W_{95}, W_{96};$

$w_4 = W_{97}, W_{98}, W_{99}, W_{100}, W_{101}, W_{102}, W_{103}, W_{104}, W_{105}, W_{106}, W_{107}, W_{108}, W_{109}, W_{110}, W_{111}, W_{112}, W_{113}, W_{114}, W_{115}, W_{116}, W_{117}, W_{118}, W_{119}, W_{120}, W_{121}, W_{122}, W_{123}, W_{124}, W_{125}, W_{126}, W_{127}, W_{128};$

0 – raund kaliti kirish kaliti	$w_0, w_1, w_2, w_3.$
1 – raund kaliti	$\boldsymbol{w_4}, w_5, w_6, w_7.$
2 – raund kaliti	$\boldsymbol{w_8}, w_9, w_{10}, w_{11}.$
3 – raund kaliti	$\boldsymbol{w_{12}}, w_{13}, w_{14}, w_{15}.$
4 – raund kaliti	$\boldsymbol{w_{16}}, w_{17}, w_{18}, w_{19}.$
5 – raund kaliti	$\boldsymbol{w_{20}}, w_{21}, w_{22}, w_{23}.$
6 – raund kaliti	$\boldsymbol{w_{24}}, w_{25}, w_{26}, w_{27}.$
7 – raund kaliti	$\boldsymbol{w_{28}}, w_{29}, w_{30}, w_{31}.$
8 – raund kaliti	$\boldsymbol{w_{32}}, w_{33}, w_{34}, w_{35}.$
9 – raund kaliti	$\boldsymbol{w_{36}}, w_{37}, w_{38}, w_{39}.$
10 – raund kaliti	$\boldsymbol{w_{40}}, w_{41}, w_{42}, w_{43}.$

8-jadval. Algoritm barcha raundi kalitlari

8-jadvaldaraund kalitlari keltirilgan bo‘lib, 0-raund kaliti boshlang‘ich kirish kaliti hisoblanadi, to‘q qora rang bilan berilgan kengaytirilgan kalitlar (2.7) formuladan, qolgan kalitlar esa (2.6) formuladan hisoblab topiladi.

(2.7) formuladagi akslantirishlar quyidagi funksiyalar asosida amalga oshiriladi:

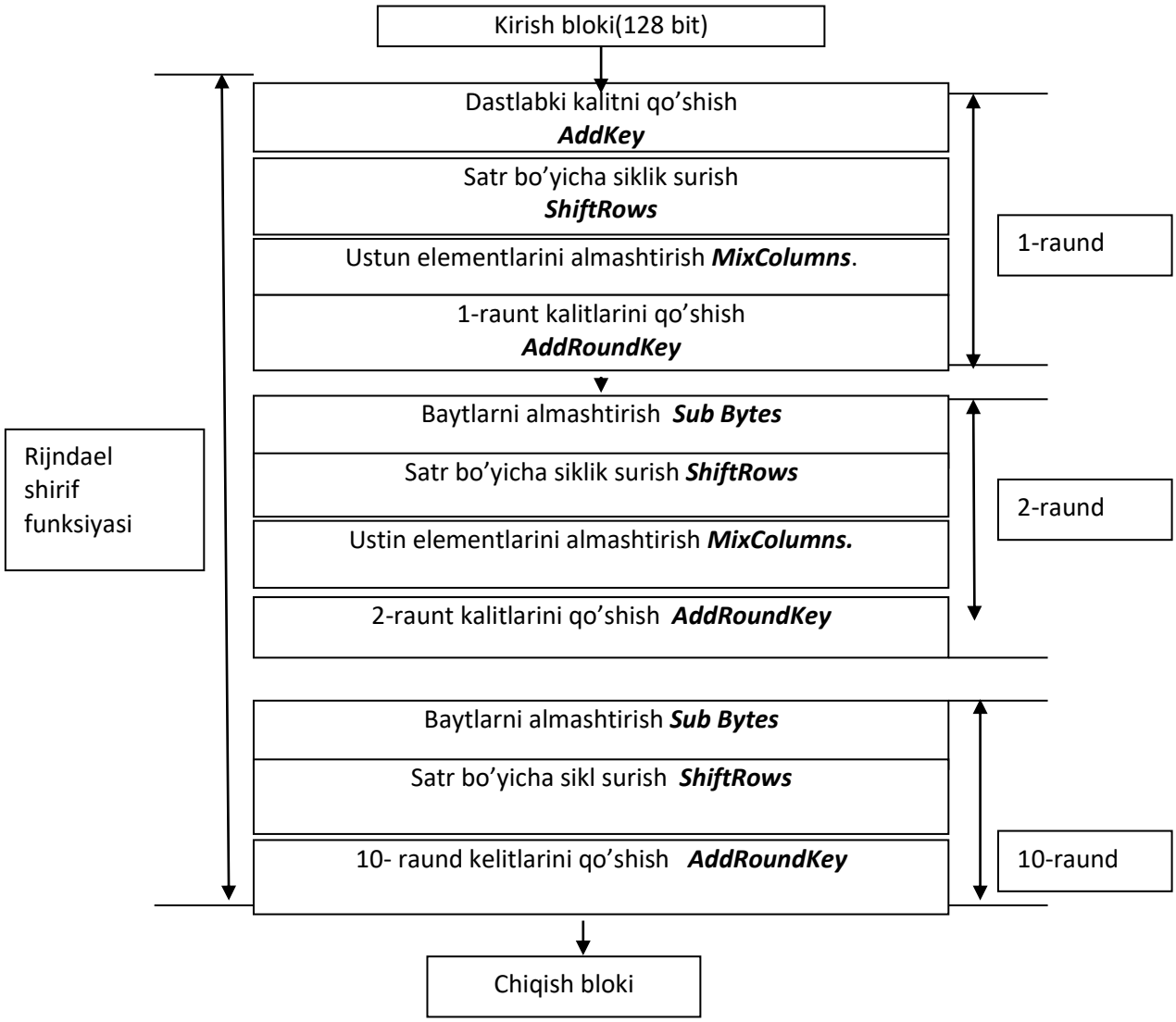
- ***RotWord*** — 32 bitli so‘zni bayt bo‘yicha quyidagi ko‘rinishda surish bajariladi $\{a_0\, a_1\, a_2\, a_3\} \to \{a_1\, a_2\, a_3\, a_0\}$;

- ***SubWord***— S blokdan va ***SubBytes***( ) funksiyasidan foydalangan holda bayt bo‘yicha akslantirish bajariladi.

- ***Rcon*** *[j]* = 2^{j-1}, bu erda j =(i / N_k) , i / N_k – bo‘lish natijasi butun son chiqadi, chunki N_k =const bo‘lib, i ning N_k ga karrali qiymatlari uchun bo‘lish amali bajariladi.

3.7. AES kriptoalgoritmi shifrlash va deshifrlash jarayonlarining blok sxemasi

Shifrlash jarayoni:



Deshifrlash jarayoni:

Shifrlash jarayonida foydalanilgan ***Sub Bytes***( ), ***ShiftRows***( ), ***MixColumns***( ) va ***AddRoundKey***( ) almashtirishlariga mos ravishda teskari:

- ***invSub Bytes*****( ),**
- ***in*****v*****ShiftRows*****( ),**
- **inv*****MixColumns*** **( ),**
- ***AddRoundKey*****( ) ,**

almashtirishlar mavjud bo‘lib, bunday holat qaralayotgan simmetrik shifrlash algritmining apparat-texnik qurilmasini yaratishda muhim omillardan hisoblanadi.

Quyida mazkur teskari almashtirishlarni batafsil ko‘rib chiqamiz:

1. ***AddRoundKey*****( )** –almashtrishida ishlatilayotgan XOR amalining xossasiga muvofiq, ushbu funksiya o‘z-o‘ziga teskari hisoblanadi.

2. ***invSub Bytes*****( )**-almashtirishi shifrlash jarayonida foydalaniladigan S-blokka (**4-jadval**) teskari amal bajarishga asoslangan. Masalan {a5} bayt uchun teskari bayt almashtirishi amalining natijasi S-blokda 2-satr va 9-ustun elementlarining kesishgan erida joylashgani uchun javob: ***invSub Bytes***({a5})= {29}.

3. **inv*****ShiftRows*****( )** –almashtirishi oxirgi holat matritsasining 3-ta satri berilgan jadval asosida o‘nggassiklik surish orqali amalga oshiriladi.

4. **inv*****MixColumns*** **( )** –almashtirishida holat matritsasi ustunlari $GF(2^8)$ maydonda uchinchi darajali ko‘phad ko‘rinishida qaralib,

$$g^{-1}(x) = \{0b\}x^3 + \{0d\}x^2 + \{09\}x + \{0e\}$$

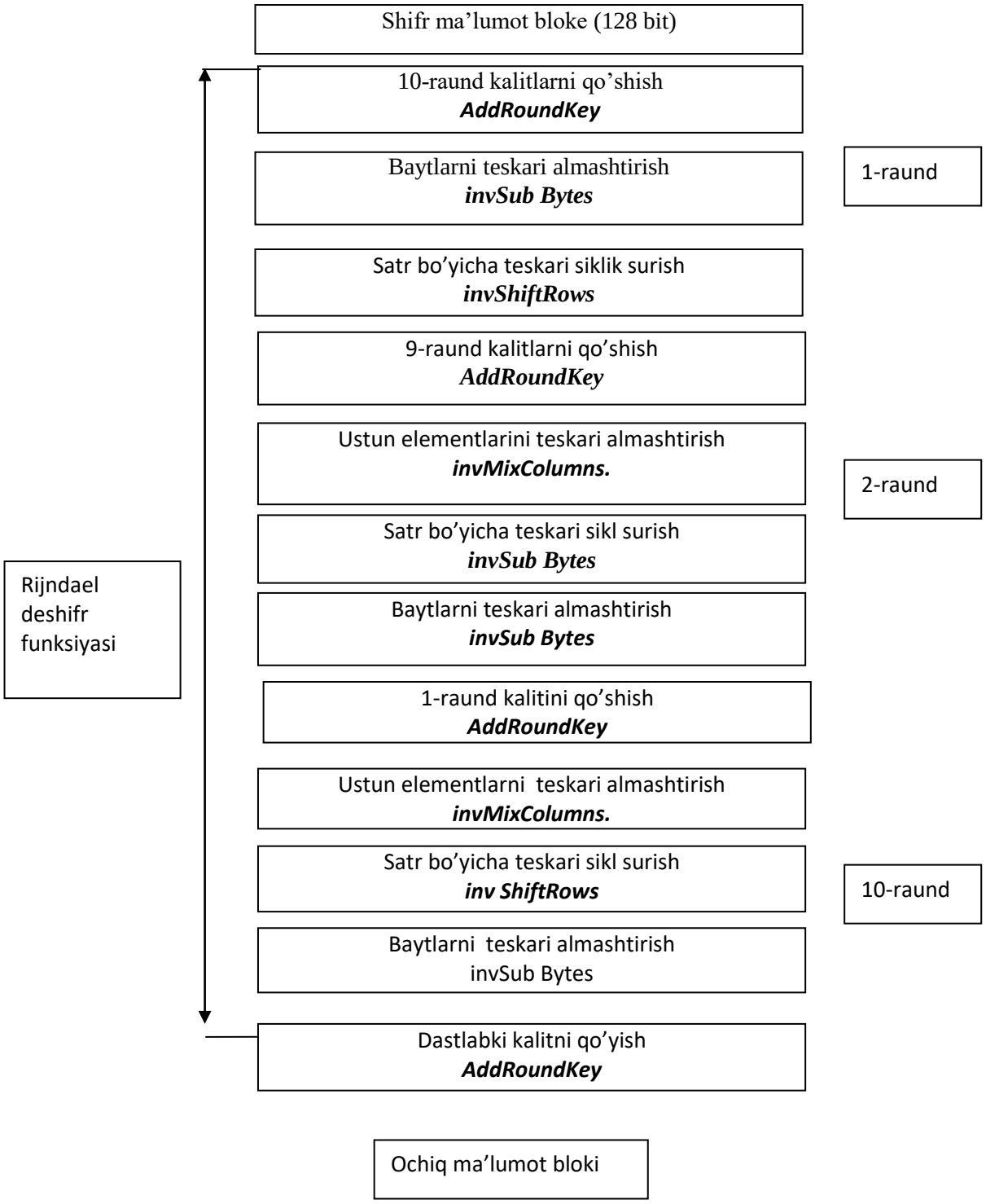
ko‘phadga moduль $x^4 + 1$ ko‘phad bo‘yicha ko‘paytiriladi. Mazkur fikrlarning matematik ifodasini quyidagicha tasvirlash mumkin:

$$\begin{bmatrix} s_{0j} \\ s_{1j} \\ s_{2j} \\ s_{3j} \end{bmatrix} = \begin{bmatrix} \{0e\} & \{0b\} & \{0d\} & \{09\} \\ \{09\} & \{0e\} & \{0b\} & \{0d\} \\ \{0d\} & \{09\} & \{0e\} & \{0b\} \\ \{0b\} & \{0d\} & \{09\} & \{0e\} \end{bmatrix} \bullet \begin{bmatrix} s'_{0j} \\ s'_{1j} \\ s'_{2j} \\ s'_{3j} \end{bmatrix} =$$

$$= \begin{bmatrix} (\{0e\} \bullet s'_{0j}) \oplus (\{0b\} \bullet s'_{1j}) \oplus (\{0d\} \bullet s'_{2j}) \oplus (\{09\} \bullet s'_{3j}) \\ (\{09\} \bullet s'_{0j}) \oplus (\{0e\} \bullet s'_{1j}) \oplus (\{0b\} \bullet s'_{2j}) \oplus (\{0d\} \bullet s'_{3j}) \\ ((0d) \bullet s'_{0j}) \oplus (\{09\} \bullet s'_{1j}) \oplus (\{0e\} \bullet s'_{2j}) \oplus (\{0b\} \bullet s'_{3j}) \\ (\{0b\} \bullet s'_{0j}) \oplus (\{0d\} \bullet s'_{1j}) \oplus (\{09\} \bullet s'_{2j}) \oplus (\{0e\} \bullet s'_{3j}) \end{bmatrix}$$

Ushbu teskari almashtirishlardan foydalanib, deshifrlash jarayonida generatsiya qilingan raund kalitlari oxirgidan boshlab bittadan kamaytirib qo‘shib boriladi, ya’ni deshifrlash jarayonining 1-raundida shifrma’lumot blokiga 10-raund kaliti, 2 – raundida 9-raund kaliti va hokazo, 10-raundida 1-raund kaliti va oxirida esa dastlabki kalit qo‘shiladi. Yuqorida ta’kidlangan jarayonni boshqa teskari akslantirishlar bilan birgalikda amalga oshirishning umumiy blok sxemasi quyida keltirilgan.

Deshifrlash jarayonining umumiy blok sxemasi



IV BOB. KRIPTOGRAFIK PROTOKOLLAR

4.1. SSL/TLS protokollari

Himoyalangan ulanishlar protokoli - Secure Sockets Layer (SSL) Internet brauzerlarining xavfsizligi muammosini yechish uchun yaratilgan. SSL taklif etgan birinchi brauzer - Netscape Navigator tijorat tranzaksiyalari uchun Internet tarmog‘ini xavfsiz qildi, natijada ma’lumotlarni uzatish uchun xavfsiz kanal paydo bo‘ldi. SSL protokoli shaffof, ya’ni ma’lumotlar tayinlangan joyga shifrlash va shifrni ochish jarayonida o‘zgarmasdan keladi. Shu sababli, SSL ko‘pgina ilovalar uchun ishlatilishi mumkin.

SSL o‘zidan keyingi TLS (Transport Layer Security - transport sathi himoyasi protokoli) bilan Internetda keng tarqalgan xavfsizlik protokolidir. Netscape kompaniyasi tomonidan 1994 yili tatbiq etilgan SSL/TLS hozirda har bir brauzerga va elektron pochtaning ko‘pgina dasturlariga o‘rnatiladi. SSL/TLS xavfsizlikning boshqa protokollari, masalan, Private Communication Technology (PCT - xususiy kommunikatsiya texnologiyasi), Secure Transport Layer Protocol (STLP - xavfsiz sathning transport protokoli) va Wireless Transport Layer Security (WTLS - simsiz muhitda transport sathini himoyalash protokoli) uchun asos vazifasini o‘tadi.

SSL/TLS ning asosiy vazifasi tarmoq trafigini yoki gipermatnni uzatish protokoli HTTP ni himoyalashdir. SSL/TLS aloqa jarayonining asosida yotadi. Oddiy HTTP kommunikatsiyalarda TCP ulanish o‘rnatiladi, hujjat xususida so‘rov yuboriladi, so‘ngra hujjatning o‘zi yuboriladi. SSL/TLS ulanishlarni autentifikatsiyalash va shifrlash uchun ishlatiladi. Bu jarayonlarda simmetrik va nosimmetrik algoritmlarga asoslangan turli texnologiyalar kombinatsiyalari ishtirok etadi. SSL/TLS da mijozni va serverni identifikatsiyalash mavjud, ammo aksariyat hollarda server autentifikatsiyalanadi.

SSL/TLS turli tarmoq kommunikatsiyalar xavfsizligini ta’minlashi mumkin. Protokolning juda keng tarqalishi elektron pochta, yangiliklar, Telnet va FTP (File Transfer Protocol - fayllarni uzatish protokoli) kabi mashhur TCP

kommunikatsiyalar bilan bog‘liq. Aksariyat hollarda SSL/TLS yordamida kommunikatsiya uchun alohida portlar ishlatiladi.

4.2. SSH protokoli

Secure Shell protokoli, SSL/TLS kabi kommunikatsiyalarni himoyalash uchun 1995 yili yaratilgan. O‘zining moslanuvchanligi va ishlatilishining soddaligi tufayli SSH ommaviy xavfsizlik protokoliga aylandi va hozirda aksariyat operatsion tizimlarda standart ilova hisoblanadi.

SSH da aloqa seansi jarayonida ma’lumotlarni uzatish uchun simmetrik kalitdan foydalaniladi. Serverni, ham mijozni autentifikatsiyalash uchun SSH ni osongina qayta konfiguratsiyalash mumkin. Ko‘pincha SSH tarmoq xostlarini boshqarishda ishlatiladigan, ko‘p tarqalgan ilova - telnet ni almashtirish uchun ishlatiladi. Ba’zida ishlab chiqaruvchilar SSH ni telnet yoki FTP ni almashtiruvchi sifatida ishlatmaydilar. Bunday hollarda SSH ni telnet, FTP, POP (Post Office Protocol - pochta xabarlari protokoli) yoki hatto HTTP kabi xavfsiz bo‘lmagan ilovalar xavfsizligini ta’minlash uchun ishlatish mumkin.

Xavfsiz bo‘lmagan tarmoqdan SSH serverga va aksincha hech qanday trafik o‘tkazilmaydi. SSH serverning SSH dan terminal foydalanishidan tashqari, portning qayta yo‘naltirilishi elektron pochta trafigini SSH serverga xavfsiz tarmoq bo‘yicha uzatilishini ta’minlashi mumkin. So‘ngra SSH server paketlarni elektron pochta serveriga qayta yo‘naltiradi. Elektron pochta serveriga trafik SSH-serverdan kelganidek tuyuladi va paketlar SSH serverga, foydalanuvchiga tunnellash uchun yuboriladi.

4.3. WLTS protokoli

SSL/TLS ga asoslangan WLTS protokoli WAP (Wireless Application Protocol - simsiz ilovalar protokoli) qurilmalarida, masalan, uyali telefonlarda va cho‘ntak kompyuterlarida ishlatiladi. SSL va WLTS bir-biridan transport sathi bilan farqlanadi. SSL yo‘qolgan paketlarni qayta uzatishda yoki nostandart paketlarni uzatishda TCP ishiga ishonadi. WLTS dan foydalanuvchi WAP

qurilmalari o‘z funksiyalarini bajarishida TCP ni qo‘llay olmaydilar, chunki faqat UDP (User Datagram Protocol) bo‘yicha ishlaydilar. UDP protokoli esa ulanishga mo‘ljallanmagan, shu sababli bu funksiyalar WLTS ga kiritilishi lozim.

"Qo‘l berib ko‘rishish" jarayonida quyidagi uchta sinf faollashishi mumkin:

- WLTS — 1-sinf. Sertifikatsiz;
- WLTS — 2-sinf. Sertifkatlar serverda;
- WLTS — 3-sinf. Sertifkatlar serverda va mijozda.

1-sinfda autentifikatsiyalash bajarilmaydi, protokol esa shifrlangan kanalni tashkil etishda ishlatiladi. 2-sinfda mijoz (odatda foydalanuvchi terminal) serverni autentifikatsiyalaydi, aksariyat hollarda sertifikatlar terminalning dasturiy ta’minotiga kiritiladi. 3-sinfda mijoz va server autentifikatsiyalanadi.

4.4. 802.1x protokoli

Bu protokolning asosiy vazifasi - autentifikatsiyalash; ba’zi hollarda protokoldan shifrlovchi kalitlarni o‘rnatishda foydalanish mumkin. Ulanish o‘rnatilganidan so‘ng undan faqat 802.1x. trafigi o‘tadi, ya’ni DHCP (Dynamic Host Configuration Protocol - xostlarni dinamik konfiguratsiyalash protokoli), IP va h. kabi protokollarga ruxsat berilmaydi. Extensible Authentification Protocol (EAP) (RFC 2284) foydalanuvchilarni autentifikatsiyalashda ishlatiladi. Boshlanishida EAP "nuqta-nuqta" (PPP, Point-to-Point Protocol) prtokoli yordamida autentifikatsiyalashning ba’zi muammolarini hal etish uchun ishlab chiqilgan edi, ammo uning asosiy vazifasi simsiz aloqa muammolarini hal etishga qaratilishi lozim. EAP ning autentifkatsiyalash paketlari foydalanuvchi ma’lumotlarini kiritgan foydalanish nuqtasiga yuboriladi, aksariyat hollarda bu ma’lumotlar foydalanuvchi ismi (login) va parolidan iborat bo‘ladi. Foydalanish nuqtasi tarmoq yaratuvchisi tanlagan vositalarning biri bilan foydalanuvchini identifikatsiyalashi mumkin. Foydalanuvchi identifikatsiyalanganidan va shifrlash uchun kanal o‘rnatilganidan so‘ng aloqa mumkin bo‘ladi va DHCP kabi

protokollarning o‘tishiga ruxsat beriladi.

4.5. IPSec protokoli

Protokollar stekida IPSec protokoli SSL/TLS, SSH yoki WLTS protokollaridan pastda joylashgan. Xavfsizlikni ta’minlash IP-sathida va Internet-modelda amalga oshiriladi. IPSec ni tatbiq qilish usullaridan ko‘p tarqalgani tunnellash bo‘lib, u bitta sessiyada IP-trafikni shifrlash va autentifikatsiyalash imkonini beradi. IPSec hozirda Internetda ishlatiluvchi aksariyat virtual xususiy tarmoqlardagi (VPN-Virtual Private Network) asosiy texnologiya hisoblanadi. IPSec ning moslashuvchanligi va ilovalar tanlanishining kengligi sababli, ko‘pchilik aynan bu sxemadan simsiz ilovalar xavfsizligini ta’minlashda foydalanadi. IPSecni ilovalarga asoslangan qo‘llanishining juda ko‘p imkoniyatlari mavjud. Xavfsiz kommunikatsiyalar uchun IPSec ning qo‘llanishi ko‘pincha Internet orqali masofadan foydalanish virtual xususiy tarmog‘i VPN bilan bog‘liq. Qachonki umumfoydalanuvchi tarmoq xususiy tarmoq funksiyalarini amalga oshirish uchun ishlatilsa, uni VPN deb atash mumkin. Bunday tarifga ATM (Asynchronous Transfer Mode - uzatishning asinxron usuli), Frame Relay va X.25 kabi tarmoq texnologiyalari ham tushadi, ammo aksariyat odamlar Internet bo‘yicha shifrlangan kanalni tashkil etish xususida gap ketganida VPN atamasini ishlatishadi.

V BOB. KALITLARNI BOSHQARISH

5.1. Simmetrik kalit uzunligi

Simmetrik kriptotizimlarda xavfsizlik ikkita omilga asoslanadi: algoritm ishonchliligi va kalit uzunligi. Kalit uzunligi 8 bitga teng bo‘lsa, 256 xil kalit bo‘lishi mumkin. Agar kalit uzunligi 128 bit bo‘lsa, 2^{128} xil kalit bo‘lishi mumkin. Agarda kompyuter 1 soniyada 10 000 000 ta kalitni tekshira olsa, barcha hollarni tekshirib chiqish uchun kompyuter taxminan 1 079 028 307 080 601 418 897 052 yil sarflaydi. Bu esa o‘z-o‘zidan kalitni topish qiyinligini ko‘rsatadi.

Quyidagi jadvalda kalit uzunligi va qurilma qiymatining bog‘liqligi keltirilgan (masalan, 100$ lik kompyuter 40 bitlik kalitni 1.5 soatda topadi):

Qurilma narxi, $	**40 bitlik kalit**	**56 bitlik kalit**	**64 bitlik kalit**	**80 bitlik kalit**	**112 bitlik kalit**	**128 bitlik kalit**
100	1.5 soat	11 yil	$3*10^3$ yil	$2*10^8$ yil	$8*10^{17}$ yil	$5*10^{22}$ yil
1000	1 minut	37 kun	30 yil	$2*10^6$ yil	$8*10^{15}$ yil	$5*10^{20}$ yil
10000	5 soniya	4 kun	3 yil	$2*10^5$ yil	$8*10^{14}$ yil	$5*10^{19}$ yil
100000	0.5 soniya	10 soat	100 kun	$2*10^4$ yil	$8*10^{13}$ yil	$5*10^{18}$ yil
1000000	0.05 soniya	1 soat	10 kun	$2*10^3$ yil	$8*10^{12}$ yil	$5*10^{17}$ yil
10000000	$5*10^{-3}$ soniya	6 daqiqa	1 kun	200 yil	$8*10^{11}$ yil	$5*10^{16}$ yil
100000000	$0.5*10^{-3}$ soniya	36 soniya	2.5 soat	20 yil	$8*10^{10}$ yil	$5*10^{15}$ yil
1000000000	$0.05*10^{-3}$ soniya	4 soniya	15 daqiqa	2 yil	$8*10^9$ yil	$5*10^{14}$ yil

10 milliard	$5*10^{-6}$ soniya	0.4 Soniya	1.5 daqiqa	70 kun	$8*10^{8}$ yil	$5*10^{13}$ yil

Agar buzg‘unchi kalitni topishni juda ham hohlasa, bu albatta mablag‘ sarflashga olib keladi. Ochiladigan xabar narxi 1 000 000 so‘m bo‘lib, uni ochish uchun 1 milliard so‘m sarflanishi lozim bo‘lsa, kalitni topishdan hech qanday ma’no yo‘q. Bundan tashqari xabarlarning narxlari vaqt o‘tgan sari tushib boradi, ma’lum vaqtdan keyin ahamiyatini butunlay yo‘qotadi.

5.2. Ochiq kalit uzunligi

Ochiq kalitli kriptotizimlar xavfsizligi ikkita katta tub sonning ko‘paytmasidan tashkil topgan sonni tub ko‘paytuvchilarga ajratish qiyinligiga asoslangan. Bunda kalit barcha imkoniyatlarni hisoblab topilmaydi, balki berilgan sonni tub ko‘paytuvchilarga ajratish orqali topiladi. Agar son kichikroq bo‘lsa, uni darrov topish mumkin, lekin katta son bo‘lsa, uni topish uchun faqat kompyuter resurslari yetarli bo‘lmaydi, balki samarali matematik usullarni topish ko‘proq foyda beradi. Kriptografiya sohasida taniqli olimlardan biri Ron Rivest 1977 yilda 125 razryadli sonni topishga 40 kvadrillion yil ketadi degan fikrni ilgari surgan, ammo 17 yildan keyin 129 razryadli sonlar ham tub ko‘paytuvchilarga ajratildi. Bundan kelib chiqadiki, ochiq kalitli kriptotizimlarda kalit xavfsizligi haqida oldindan bashorat qilish qiyin. Bugungi kunda asosan 1024 - 2048 bitli sonlardan foydalanilmoqda.

5.3. Kalitlarni boshqarish

Har qanday kriptografik tizim kriptografik kalitlardan foydalanishga asoslangan. Kalit axboroti deganda axborot tarmoqlari va tizimlarida ishlatiluvchi barcha kalitlar majmui tushuniladi. Agar kalit axborotlarining yetarlicha ishonchli boshqarilishi ta’minlanmasa, buzg‘unchi odam unga ega bo‘lib olib, tarmoq va tizimdagi barcha axborotdan hohlaganicha foydalanishi mumkin. Kalitlarni boshqarish kalitlarni generatsiyalash, saqlash va taqsimlash kabi vazifalarni bajaradi. Kalitlarni taqsimlash kalitlarni boshqarish jarayonidagi

eng ma’suliyatli jarayon hisoblanadi.

Simmetrik kriptotizimdan foydalanilganda axborot almashinuvida ishtirok etuvchi ikkala tomon avval maxfiy sessiya kaliti, ya’ni almashinuv jarayonida uzatiladigan barcha xabarlarni shifrlash kaliti bo‘yicha kelishishlari lozim. Bu kalitni boshqa hech kim bilmasligi va uni vaqti- vaqti bilan jo‘natuvchi va qabul qiluvchida bir vaqtda almashtirib turish lozim. Sessiya kaliti bo‘yicha kelishish jarayonini kalitlarni almashtirish yoki taqsimlash deb ham yuritiladi.

Nosimmetrik kriptotizimda ikkita kalit - ochiq va yopiq (maxfiy) kalit ishlatiladi. Ochiq kalitni oshkor etish mumkin, yopiq kalitni yashirishlozim. Xabar almashinuvida faqat ochiq kalitni uning haqiqiyligini ta’minlagan holda jo‘natish lozim.

Kalitlarni taqsimlashga quyidagi talablar qo‘yiladi:

- taqsimlashning operativligi va aniqligi;
- taqsimlanuvchi kalitlarning konfidensialligi va yaxlitligi.

Kompyuter tarmoqlaridan foydalanuvchilar o‘rtasida kalitlarni taqsimlashning quyidagi asosiy usullaridan foydalaniladi.

1. Kalitlarni taqsimlovchi bitta yoki bir nechta markazlardan foydalanish.
2. Tarmoq foydalanuvchilari o‘rtasida kalitlarni to‘g‘ridan-to‘g‘ri almashish.

Birinchi usulning muammosi shundaki, kalitlarni taqsimlash markaziga kimga qaysi kalitlar taqsimlanganligi ma’lum. Bu esa tarmoq bo‘yicha uzatilayotgan barcha xabarlarni o‘qishga imkon beradi. Bo‘lishi mumkin bo‘lgan suiste’mollar tarmoq xavfsizligining jiddiy buzilishiga olib kelishi mumkin.

Ikkinchi usuldagi muammo - tarmoq subyektlarining haqiqiy ekanligiga ishonch hosil qilishdir.

Kalitlarni taqsimlash masalasi quyidagilarni ta’minlovchi kalitlarni taqsimlash protokolini qurishga keltiriladi:

1. seans qatnashchilarining haqiqiyligiga ikkala tomonning tasdig‘i;
2. seans haqiqiyligining tasdig‘i;
3. kalitlar almashinuvida xabarlarning eng kam sonidan foydalanish.

Birinchi usulga misol tariqasida Kerberos deb ataluvchi kalitlarni

autentifikatsiyalash va taqsimlash tizimini ko‘rsatish mumkin.

Ikkinchi usulga - tarmoq foydalanuvchilari o‘rtasida kalitlarni to‘g‘ridan-to‘g‘ri almashishga batafsil to‘xtalamiz.

Simmetrik kalitli kriptotizimdan foydalanilganda kriptografik himoyalangan axborot almashinuvini istagan ikkala foydalanuvchi umumiy maxfiy kalitga ega bo‘lishlari lozim. Bu foydalanuvchilar umumiy kalitni aloqa kanali bo‘yicha xavfsiz almashishlari lozim. Agar foydalanuvchilar kalitni tez-tez o‘zgartirib tursalar, kalitni yetkazish jiddiy muammoga aylanadi. Bu muammoni yechish uchun quyidagi ikkita asosiy usul qo‘llaniladi:

1. Simmetrik kriptotizimning maxfiy kalitini himoyalash uchun ochiq kalitli nosimmetrik kriptotizimdan foydalanish;
2. Diffi-Xellmanning kalitlarni ochiq taqsimlash tizimidan foydalanish.

Birinchi usul simmetrik va nosimmetrik kalitli kombinatsiyalangan kriptotizim doirasida amalga oshiriladi. Bunday yondashishda simmetrik kriptotizim dastlabki ochiq matnni shifrlash va uzatishda ishlatilsa, ochiq kalitli kriptotizim faqat simmetrik kriptotizimning maxfiy kalitini shifrlash, uzatish va ochishda ishlatiladi. Shifrlashning bunday kombinatsiyalangan (gibrid) usuli ochiq kalitli kriptotizimning yuqori maxfiyligi bilan maxfiy kalitli simmetrik kriptotizimning yuqori tezkorligining uyg‘unlashishiga olib keladi.

Kombinatsiyalangan usul bo’yicha xabarni shifrlash sxemasi

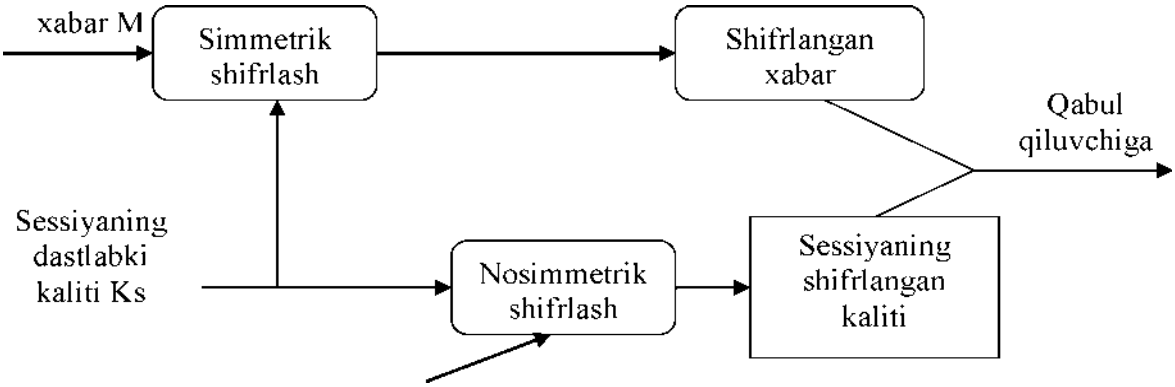
Faraz qilaylik, *A* foydalanuvchi *M* xabarni *V* foydalanuvchiga himoyalangan tarzda uzatish uchun shifrlashning kombinatsiyalangan usulidan foydalanmoqchi. Unda foydalanuvchilarning harakatlari quyidagicha bo‘ladi.

Foydalanuvchi *A* ning harakatlari:

1. Simmetrik seans maxfiy kalit K_S ni yaratadi (masalan, tasodifiy tarzda generatsiyalaydi).
2. Xabar *M* ni simmetrik seans maxfiy kalit K_S da shifrlaydi.
3. Maxfiy seans kalit K_S ni foydalanuvchi (xabar qabul qiluvchi) ning ochiq kaliti K_V da shifrlaydi.

4. Foydalanuvchi *V* adresiga aloqaning ochiq kanali bo‘yicha shifrlangan xabar *M* ni shifrlangan seans kaliti K_S bilan birgalikda uzatadi.

Foydalanuvchi *A* ning harakatlarini rasmda keltirilgan xabarlarni kombinatsiyalangan usul bo‘yicha shifrlash sxemasi orqali tushunish mumkin:



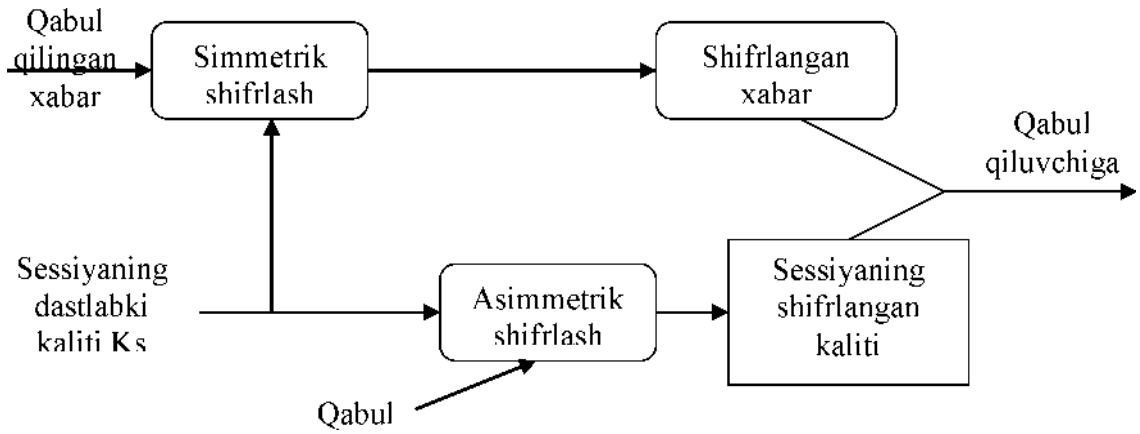
Qabul qiluvchining kaliti Kb

Konihinatsiyalangan usul bo’yicha xabarni ochish

Foydalanuvchi *V* ning harakatlari (shifrlangan xabar *M* ni va shifrlangan seans kaliti K_S ni olganidan so‘ng) quyidagicha:

1. O‘zining maxfiy kaliti K_V bo‘yicha seans kaliti K_S ni ochadi.
2. Olingan seans kaliti K_S bo‘yicha olingan xabar *M* ni ochadi.

Foydlanuvchi *V* ning harakatlarini quyidagi rasmda keltirilgan xabarlarni kombinatsiyalangan usul bo‘yicha ochish sxemasi orqali tushunish mumkin:



Olingan xabarni faqat foydalanuvchi *V* ochishi mumkin. Faqat maxfiy

kalit K_v egasi bo‘lgan foydalanuvchi V maxfiy seans kaliti K_S ni to‘g‘ri ochish va so‘ngra bu kalit yordamida olingan xabar M ni ochishi va o‘qishi mumkin.

5.4. Ochiq kalitlarni boshqarish infratuzilmasi

Tarixan axborot xavfsizligini boshqaruvchi har qanday markazning vazifalari doirasiga axborot xavfsizligining turli vositalari tomonidan ishlatiluvchi kalitlarni boshqarish kirgan. Bu - kalitlarni berish, yangilash, bekor qilish va tarqatish.

Simmetrik kriptografiyadan foydalanilganda kalitlarni tarqatish masalasi eng murakkab muammoga aylangan, chunki:

- N ta foydalanuvchi uchun himoyalangan N(N-1)/2 kalitni tarqatish lozim edi. N bir necha yuzga teng bo‘lganida, bu sermashaqqat vazifaga aylanishi mumkin;

- bunday tizimning murakkabligi (kalitlarning ko‘pligi va tarqatish kanalining maxfiyligi) xavfsizlik tizimini qurish qoidalarining biri - tizim oddiyligiga to‘gri kelmaydi, natijada zaif joylarning paydo bo‘lishiga olib keladi.

Nosimmetrik kriptografiya faqat N maxfiy kalitni tavsiya etib, bu muammoni chetlab o‘tishga imkon yaratadi. Bunda har bir foydalanuvchida faqat bitta maxfiy kalit va maxsus algoritm bo‘yicha maxfiy kalitdan olingan ochiq kalit bo‘ladi.

Ochiq kalitdan maxfiy kalitni olib bo‘lmasligi sababli ochiq kalitni himoyalanmagan holda barcha o‘zaro aloqa qatnashchilariga tarqatish mumkin. O‘zining maxfiy kaliti va o‘zaro aloqadagi sherigining ochiq kaliti yordamida har bir foydalanuvchi har qanday kriptoamallarni bajarishi mumkin: bo‘linuvchi sirni hisoblash, axborotning konfidensialligi va yaxlitligini himoyalash, elektron raqamli imzoni yaratish.

Ochiq kalitlarni boshqarish infratuzilmasining asosiy vazifalari quyidagilar:

- kalitlarni generatsiyalash, sertifikatlarni yaratish va imzolash, ularni taqsimlash va h.k;

- obro‘sizlantirish faktlarini qaydlash va chaqirib olingan sertifikatlarning "qora" ro‘yxatini chop etish;

- foydalanuvchining tizimdan foydalanish vaqtini imkoni boricha kamaytiruvchi identifikatsiyalash va autentifikatsiyalash jarayonlarini yaratish;

- mavjud ilovalar va xavfsizlik qism tizimining barcha komponentlarini integratsiyalash mexanizmini amalga oshirish;

- barcha foydalanuvchilar va ilovalar uchun bir xil va tarkibida barcha zaruriy kalit komponentlari va sertifikatlar bo‘lgan xavfsizlikning yagona dasturidan foydalanish imkoniyatini taqdim etish.

Xavfsizlik dasturi — foydalanuvchining tizimdagi barcha huquqlari va qurshovini aniqlovchi xavfsizlikning shaxsiy vositasi, masalan smart- karta.

VI BOB. NOSIMMETRIK ALGORITMLAR

6.1. Kriptografiyaning matematik asoslari

Natural sonlar to‘plamini N ={1, 2,3, ... } va butun sonlar to‘plamini Z={0, ± 1, ± 2, ±3, ... } ko‘rinishda belgilaymiz. Noldan farqli bo‘lgan *a* soni va *v* sonlar *Z* to‘plamga tegishli, ya’ni *a,b eZ* bo‘lib, *a*± 0 bo‘lsin. *v* soni *a* soniga butun bo‘linadi deyiladi, agarda shunday s soni mavjud bo‘lib, *v=as* tenglik bajarilsa. Berilgan *a* va *v* sonlarni bo‘luchi butun son, ularning *umumiy bo‘luvchisi* deyiladi. Umumiy bo‘luvchilar ichida eng kattasi *eng katta umumiy* bo‘luvchi (EKUB) deyiladi va (a,v) ko‘rinishda belgilanadi. Agarda *a* va *v* sonlarning eng katta umumiy bo‘luchisi 1, yani *(a,v)=1* bo‘lsa, *a* va *v* sonlar *O’zaro tub* deyiladi. Eng katta umumiy bo‘luvchilarni topishga oid bo‘lgan tasdiqlarni keltiramiz.

Agar *v* soni *a* soniga bo‘linsa, u holda bu sonlarnining eng katta umumiy bo‘luvchisi *(a,v)=a.*

Evklid algoritmi

Bu - ikkita sonning eng katta umumiy bo‘luvchisini topish algoritmi. Evklid bu usulni eramizdan avvalgi 300-yildagi kitobida keltirgan. Algoritm qadamlari quyidagilardan iborat:

1. a=b bo‘lsa, (a,b)=a yoki (a,b)=b.
2. a>b bo‘lsa, a=bq+r, bu yerda 0< r <b. Agar r=0 bo‘lsa, (a,b)=b bo‘lib algoritm to‘xtaydi, aks holda algoritm davom etadi.
3. $b=rq_1+r_1$ bajarilib, bu yerda $0< r_1<r$, $r_1=0$ bo‘lsa, (a,b)=r bo‘lib algoritm to‘xtaydi, aks holda algoritm davom etadi.
4. $r=r_1q_2+r_2$ bajarilib, bu yerda $0< r_2<r_1$, $r_2=0$ bo‘lsa, (a,b)=r_2 bo‘lib algoritm to‘xtaydi, aks holda algoritm davom etadi. Ushbu jarayon chekli qadamdan so‘ng tugaydi.

Nazorat uchun savollar:

1. Evklid usuli qayerda qo‘llaniladi?
2. Bu usul nima uchun Evklid algoritmi deyiladi?

3. Qanday sonlarning EKUB i birga teng?
4. Qanday sonlarning EKUB i ulardan biriga teng?

Mustaqil ish uchun misollar.

Quyida keltirilgan sonlarning EKUB i topilsin:

1. (21,35)=?
2. (42,180) =?
3. (258,312) =?
4. (1024,512) =?
5. (83,279) =?
6. (191,1021) =?
7. (415,747) =?

Agar n > 1 natural son bo‘lsa, quyidagilarni isbot qiling:

1. (n,2n+1)=1
2. (2n+1,3n+1)=1

Berilgan natural son *p>1* tub deyiladi, agarda bu son o‘zi *p* va 1 dan boshqa natural songa bo‘linmasa. Misol uchun: 2,3,5,7,11,13,17,19,23,29, tub sonlar, ularning soni cheksiz davom etadi.

Barcha butun sonlarni *modul* deb ataluvchi - biror fiksirlangan natural *n* soniga bo‘lganda qoladigan qoldiqlar bilan bog‘liq holda o‘rganamiz. Bunda elementlari soni cheksiz bo‘lgan barcha butun sonlar to‘plamiga, 0 dan *n-i* gacha bo‘lgan butun sonlarni o‘z ichiga oladigan chekli, quvvati *n* ga teng bo‘lgan {0;1;2;3;...;n-l} - to‘plam mos qo‘yiladi. Bu quyidagicha amalga oshiriladi: *a* va *n* -natural sonlar bo‘lsa, "a sonini *n* soniga qoldiq bilan bo‘lish", deganda ushbu

$$a = q\,n + r$$

tenglik tushuniladi. Bu yerda 0 <*r*< n, shartni qanoatlantiruvchi natural *q* va *r* sonlarini topish tushuniladi. Bu oxirgi tenglikda qoldiq deb ataluvchi *r* soni nolga teng bo‘lsa r=0, natural *a* soni *n* soniga butun bo‘linadi yoki *n* soni *a* sonining bo‘luvchisi deyiladi.

Butun *a* va *b* sonlari *modul n bo’yicha taqqoslanadigan* deyiladi, agarda

ularni *n* ga bo‘lganda qoladigan qoldiqlari teng bo‘lsa, a = *b mod n* deb yoziladi. Bundan esa, *a* va *b* sonlar ayirmasining *n* ga qoldiqsiz bo‘linishi kelib chiqadi.

Qoldiqni ifodalash uchun ushbu *b=a* mod *n* tenglikdan foydalaniladi hamda *b=a* mod *n* tenglikni qanoatlantiruvchi *b* sonini topish *a sonini modul n bo’yicha keltirish* deyiladi. Ixtiyoriy butun *b* soni uchun ushbu

$M=\{a_0,a_1...,a_{n-1} : 0<a_k<n-1;\ k=0,1,...,n-1\}$

to‘plamga tegishli $a_k=b$ mod n munosabatni qanoatlantiruvchi son a_k, $k = \{0,1,..., n-l\}$, mavjud bo‘lsa, *M* to‘plam modul *n* bo‘yicha *to‘liq chegirmalar tizimi* deyiladi. Ko‘rinib turibdiki, to‘liq chegirmalar tizimi $M=\{a_0,a_i,...,a_{n4}: 0<a_k<n-1;\ k=0,1,...,n-1\}$.

Biror *n* modul bo‘yicha qo‘shish, ayirish va ko‘paytirish amallariga nisbatan quyidagi kommutativlik, assotsiativlik va distributivlik munosabatlari o’rinli:

(a+b)mod n=((a mod n)+(b mod n))mod n,

(a-b)mod n=((a mod n)-(b mod n))mod n,

(ab)mod n=((a mod n)·(b mod n))mod n,

(a(b+c))mod n=((ab) mod n+(ac) mod n)mod n.

Butun *a* va *b* sonlari o‘zaro tub bo‘ladi faqat va faqat shundaki, qachonki shunday butun *u* va *v* sonlari topilsaki, ular uchun *au+bv=1* tenglik o‘rinli bo‘lsa.

Agarda butun *a* va *v* sonlari o‘zaro tub bo‘lsa, ya’ni *(a,n)=1* bo‘lsa, u holda ushbu (ab)mod *n=1* munosabatni qanoatlantiruvchi butun *b* soni mavjud bo‘lib, bu *b son a soniga modul n bo’yicha teskari* deyiladi, hamda, $b = a^4$ mod n deb belgilanadi.

Teskari elementni hisoblashning yana bir usulini keltiramiz. Berilgan *n* soni bilan o‘zaro tub bo‘lgan (1;n) oraliqdagi barcha elementlarning soni bilan aniqlanuvchi *F(n)* funksiyaga *Eyler funksiyasi* deyiladi va u quyidagicha aniqlanadi:

1. F (n)=n-1, agar n tub bo‘ lsa;
2. F(n)=(p-1)(q-1), agar n=pq bo‘lib, p va q sonlar tub bo‘lsa;

3. F(n)=n(1-1/p1)(1-1/p2)... .(1-1/p_k),

agar $\prod_{i=1}^{k} P_i^{t_i} \quad i, t_i \in N,\ p_i \ \ (i = 1, \dots, k)$ -tub sonlar.

Eyler teoremasi. a<n va n tub bo‘lsa, $a^{n-1} mod\ n = 1$ tenglik o‘rinli. *Demak, (a,n)=1 bo’lsa,* $a^{-1}=a^{F(n)-1} mod\ n$ *tenglik o’rinli.*

Fermaning kichik teoremasi. *n* - tub son bo‘lib, a<n bo‘lsa, a^{n-1} mod n=1 tenglik o‘rinli.

Agar *a* va *n* sonlari o‘zaro tub bo‘lsa, $a^{-1} = x$ mod *n* tenglama yagona yechimga ega bo‘ladi;

Agar *a* va *n* sonlari o‘zaro tub bo‘lmasa, $a^{-1} = x$ mod *n* tenglama yechimga ega emas.

Bevosita hisoblashlar asosida, ushbu (a* x) mod *n* = *b* tenglama *a,n,b* - sonlarining qanday qiymatlar qabul qilishiga qarab, yoki bir nechta yechimlarga ega bo‘lishi mumkinligiga, yoinki bitta ham yechimga ega bo‘lmasligiga ishonch hosil qilish mumkin.

Kvadratik ayirmalar. Agar *p* - tub son va 0<*a*< *p* bo‘lib, ushbu *x* mod *p* = *a* munosabatni qanoatlantiruvchi x - noma’lumning qiymatlari mavjud bo‘lsa, u holda *a* soni modul *p* bo‘yicha kvadratik ayirma deyiladi.

Agarda *a* soni modul *p* bo‘yicha kvadratik ayirma bo‘lsa, u holda *a* uchun ikkita kvadrat ildiz mavjud bo‘lib, ulardan biri [0; (p-1)/2] oraliqda, ikkinchisi [(p-1)/2 ; *p*-1] oraliqda, shu bilan birga ulardan biri modul *p* bo‘yicha kvadratik ayirma bo‘ladi va u *bosh kvadratik ildiz* deyiladi.

Yasovchi (Tuzuvchi). Berilgan *r* -tub son va *g*<*p* uchun, *g* -yasovchi *(tuzuvchi)* yoki modul *p* bo‘yicha *primitiv ildiz* deyiladi, agarda 1 <*b* < *p* -1 shartni qanoatlantiruvchi har bir *b* soni uchun, ushbu g^a modp = b tenglikni qanoatlantiruvchi *a* soni mavjud bo‘lsa.

Tub ko’paytuvchilarga ajratish. Berilgan sonni ko‘paytuvchilarga ajratish deganda, uning tub ko‘paytuvchilarini topish tushuniladi. Berilgan sonni ko‘paytuvchilarga ajratish sonlar nazariyasining eng dastlabki masalalaridan biri hisoblanadi. Berilgan sonni (yoki to‘plamni) biror amal yoki xususiyatga ko‘ra uning tashkil etuvchilari orqali ifodalanishi, shu sonni (yoki to‘plamni) faktorlash

(ajratish) deyiladi. Sonni ko‘paytuvchilarga ajratish qiyin jarayon emas, ammo ko‘paytuvchilarga ajratilishi kerak bo‘lgan sonning qiymati kattalashib borishi bilan, uni ko‘paytuvchilarga ajratish jaryoniga sarflanadigan vaqt ham ko‘payib boradi. Shunday bo‘lsada, ko‘paytuvchilarga ajratish jarayonini tezlashtiruvchi quyidagi algoritmlar mavjud:

1. *sonli maydon umumiy G’alviri usuli* - o‘nlik sanoq tizimida 110 ta va undan ko‘p razryadli (raqamli) sonlarni ko‘paytuvchilarga ajratishning ma’lum bo‘lgan eng samarali (tez, kam vaqt sarflanadigan) algoritmi;

2. *kvadratik G’alvir usuli* - o‘nlik sanoq tizimida 110 tadan kam bo‘lmagan razryadli (raqamli) sonlarni ko‘paytuvchilarga ajratishning ma’lum bo‘lgan eng samarali (tez, kam vaqt sariflanadigan) algoritmi;

3. *elliptik egri chiziq usuli* - o‘nlik sanoq tizimida tub ko‘paytuvchilarining razryadi (raqamlari soni) 43 tadan ko‘p bo‘lmagan sonlarni ko‘paytuvchilarga ajratishda foydalanilgan;

4. Pollardning Monte-Karlo usuli - amalda kam ishlatiladi;

5. *uzuliksiz kasrlar usuli* - qo‘llashga ko‘p vaqt sarflanadi;

6. *tanlab bO’lish usuli* - eng dastlabki usullardan bo‘lib, ko‘paytuvchilarga ajratilishi kerak bo‘lgan (berilgan) sonning kvadrat ildiziga teng va undan kichik bo‘lgan har bir tub sonni berilgan sonni qoldiqsiz bo‘lishi yoki bo‘lmasligi tekshirib chiqilishi natijasida, berilgan sonni tub ko‘paytuvchilari aniqlanadi.

Tub sonlar generatsiyasi (ishlab chiqarish). Ochiq kalitli kriptoalgoritmlar asoslari yaratilishida tub sonlarning xossalaridan foydalaniladi. Biror berilgan sonni tub ko‘paytuvchilarga ajratish, uni tub yoki tub emasligini aniqlashga nisbatan murakkab bo‘lgan masala. Yetarli katta razryaddagi toq sonni tasodifiy tanlab olib, uni ko‘paytuvchilarga ajratish bilan tub yoki tub emasligini aniqlashdan ko‘ra, uning tubligini biror mavjud usul bilan tekshirish osonroq. Buning uchun turli ehtimollik testlari mavjud bo‘lib, sonning tubligini berilgan darajadagi ishonch bilan aniqlab beradi. Kriptobardoshliligi yetarli darajada katta razryadli sonni tub ko‘paytuvchilarga ajratish masalasining murakkabligiga

asoslangan ochiq kalitli kriptoalgoritmlar mavjud.

Chekli maydonlarda diskret logarifmlash. Kriptografiyada birtomonli (teskarisi yo‘q) funksiya sifatida biror modul *n* bo‘yicha darajaga ko‘tarish amalini bajarishni hisoblashdan foydlalaniladi:

$y = a^x \bmod n$.

Bu funksiyaning *y* qiymatini x argumentning berilgan qiymati bo‘yicha hisoblash qiyinchilik tug‘dirmaydi. Ammo, *y* ning qiymatini bilgan holda, x ning qiymatini topish murakkab masala hisoblanadi. Umuman olganda,

$a^x \bmod n = b$

munosabatni qanoatlantiruvchi x noma’lumning butun qiymatlari har qanday *n* lar uchun ham mavjud bo‘lavermaydi. *a, b, n* -parametrlarning yetarli katta qiymatlarida bu yuqorida keltirilgan masalaning yechimi yana ham murakkablashadi.

Kriptografiyada nosimmetrik shifrlash algoritmlari asoslari bilan bog‘liq bo‘lgan quyidagi:

- tub sonlar maydonida *GF(p)* diskret logarifimlash;
- moduli asosi 2 bo‘lgan $GF(2^n)$ maydonda diskret logarifimlash;
- elliptik egri chiziq nuqtalari ustida bajariladigan amallarni biror chekli *F* maydonda amalga oshirish kabi masalalarni yechishning murakkabligi bilan bog‘liq bo‘lgan muammolalar asosida ish ko‘riladi.

Kriptobardoshliligi diskret logarifimlash masalasining murakkabligiga asoslangan ko‘plab ochiq kalitli kriptoalgoritmlar mavjud.

Ilmiy tadqiq qilinayotgan obyektlar matematik modellarining sifati darajasi (adekvatligi) ular bilan bog‘liq bo‘lgan jarayonlarni qanchalik to‘liq va aniq ifodalashi bilan belgilanadi. Matematik model boshlang‘ich fikr va mulohazalar asosida o‘tkazilgan tajribalar natijalarini solishtirish hamda tadqiq qilinayotgan obyektning xususiyatlarini belgilovchi parametrlarning tabiiy bog‘liqligi, qonuniyatlarini ifodalovchi tenglik, tengsizlik va tegishlilik munosabatlari bilan aniqlanadi. Kriptologiya biror chekli sondagi alfavit belgilarining ketma-ketligi

bilan ifodalangan ma’lumotni va uning o‘zgarishlari (akslantirilishlari) bilan bog‘liq bo‘lgan jarayonlarni tadqiq qiladi. Kriptografik akslantirishlar matematikaning: to‘plamlar va funksiyalar nazariyasi, algebra, diskret matematika, sonlar nazariyasi, ehtimollar nazariyasi, haqiqiy va kompleks o‘zgaruvchili funksiyalar nazariyasi, murakkablik nazariyasi, axborotlar nazariyasi kabi bo‘limlariga tegishli bo‘lgan matematik modellardan iborat. Murakkablik nazariyasi kriptografik algoritmlarning hisoblash murakkabliklarini tahlil qilish uslubini beradi. Har xil kriptografik algoritmlarning hisoblash murakkabliklarini solishtirib, ularning ishonchlilik - bardoshlilik darajasi aniqlanadi.

Algoritmning murakkabligi. Algoritmning murakkabligi, shu algoritmni to‘la amalga oshirish uchun bajarilishi nazarda tutilgan barcha amallar soni bilan aniqlanadi. Algoritmning hisoblash murakkabligi odatda ikkita parametr bilan aniqlanadi: algoritmda ko‘rsatilgan amallarni bajarishga sarflanadigan *vaqt bilan aniqlanadigan murakkablik* T va hisoblash qurilmasida algoritm parametlari ustida amallar bajarishda kerak bo‘ladigan registrlarning soni bilan aniqlanadigan - *hisoblash qurilmasi xotirasi hajmi bilan bog’liq bo’lgan murakkablik* S. Bu T va S parametrlar algoritm xususiyatlaridan kelib chiqib, boshlang‘ich qiymatlarning *n* o‘lchoviga bog‘liq holda aniqlanadi, ya’ni biror: *T=fn)* va *S* funksiyalar bilan.

Algoritmning hisoblash murakkabligi odatda hisoblash murakkabligi qiymatini tartibini ko‘rsatuvchi “O katta” deb ataluvchi belgi bilan ifodalanadi hamda bu belgi *n* - parametr qiymatining ortishi bilan murakablik funksiyasi ifodasi hadlari ichida qiymati eng tez o‘sadigan hadni ifodalab, boshqa hadlarni hisobga olmaydi. Masalan, algoritmning vaqt bilan aniqlanadigan murakkabligi $T=fn)=5n+6n+11$ bo‘lsa, u holda uning *n* tartibli hisoblash murakkabligi $O(n$) ko‘rinishda ifodalanadi. Hisoblash murakkabligi baholari boshlang‘ich qiymatlarni, algoritmning xususiyatlaridan kelib chiqqan holda, algoritmni amalga oshirish uchun sarflanadigan vaqt va hisoblash qurilmasi xotirasiga qo‘yadigan talablarini yaqqol namoyon etadi. Masalan, $T=O(n)$bo‘lsa, boshlang‘ich qiymat o‘lchovining ikki marta o‘sishi vaqtning ham ikki marta o‘sishiga olib keladi; agarda $T=O(2^n)$ bo‘lsa, boshlang‘ich qiymat o‘lchoviga bitta bitning qo‘shilishi

algoritmni amalga oshirish uchun sarflanadigan vaqtni ikki baravar oshishini bildiradi. Algoritmlar vaqt va hisoblash murakkabliklariga ko‘ra quyidagicha klassifikatsiyalanadi (sinflarga ajratiladi):

1. Algoritm *doimiy* deyiladi, agarda uning murakkabligi qiymati boshlang‘ich qiymat o‘lchoviga bog‘liq bo‘lmasa, ya’ni 0(1);
2. Algoritm *chiziqli* deyiladi, agarda uning murakkabligi qiymatining tartibi *0(n)* bo‘lsa;
3. Algoritm *polinomial* deyiladi, agarda uning murakkabligi qiymatining tartibi $0(n^m)$ (bu yerda m>1) bo‘lsa;
4. Algoritm *eksponensial* deyiladi, agarda uning murakkabligi qiymatining tartibi $0(^{fn)})$ (bu yerda *const*=*t*>1 va fn) - boshlang‘ich qiymat o‘lchovi *n* ga nisbatan polinomial funksiya) bo‘lsa;
5. Murakkabligi qiymatining tartibi $0(^{fn)})$ bo‘lgan *eksponensial* algoritmlar to‘plamiga qism to‘plam bo‘ladigan algoritmlar *superpolinomial* deyiladi, agarda *fn)* - polinomial funksiya *t* o‘zgarmasga nisbatan tezroq, lekin chiziqli funksiyaga nisbatan sekinroq o‘ssa.

Shu yerda ta’kidlash joizki, kriptoalgoritmlarning natijasiga ko‘ra uning noma’lum parametrlarini topishning mavjud algoritmlari superpolinomial murakkablikka ega bo‘lib, noma’lum parametrlarini topishning polinomial murakkablikka ega bo‘lgan algoritmlarini topish mumkin emasligi isbot qilinmagan. Ya’ni biror algoritmning noma’lum parametrini polinomial murakkablikka ega bo‘lgan algoritmlarini topish mumkinligi uning kriptobardoshsiz bo‘lib qolganligini bildiradi.

Sonning teskarisini topishga oid misol: a=21, n=41 6y^ca, a^{-1}mod n=?

Avvalo, 21 va 41 sonlari o‘zaro tubligini tekshiramiz: (21,41)=1, demak teskarisi mavjud. n=41 - tub son. Eyler funksiyasi F(n) 1-formulaga asosan n-1 ga teng, F(n)=40. Eyler teoremasiga asosan 21 sonining teskarisini topamiz:

$21\sim^{1} \bmod 41 = 21^{401} \bmod 41 = 21^{39} \bmod 41 = \wedge 21^{3} \bmod 41\wedge \bmod 41 = (9261\bmod 4l)^{13} \bmod 41 =$

$= 36^{13} \bmod 41 = (36 \bullet 36^{12}) \bmod 41 = \wedge 36 - (36^{3} \bmod 41)^{4}$ j mod 41 = ^36 •(46656

mod 41)^4) mod 41 = = (36 • 39^4) mod 41 = (36 • 2313441) mod41 = (36 16) mod41 = 576mod41 = 2

Tekshirish: (2 • 2 1)*mod4* 1 = 4 2*mod4* 1 = 1. Demak, 21 sonining 41 modul bo‘yicha teskarisi 2 ga teng.

Nazorat uchun savollar:

1. Sonning teskarisi deganda qanday son tushuniladi?
2. Sonning teskarisi yagonami?
3. Qanday sonlarning teskarisi mavjud emas?

6.2. Xesh-funksiyalar

Xesh-funksiya - bir taraflama, ya’ni qandaydir axborot bloki yoki xabarni, “barmoq izlari” fayli yoki daydjestni olishga mo‘ljallangan funksiya. Xesh-qiymat H funksiyasi orqali hisoblanadi: h=H(M). Bu yerda M - ixtiyoriy uzunlikdagi xabar va h - fiksirlangan uzunlikdagi xesh- qiymat.

1. Xesh-funksiya ixtiyoriy uzunlikdagi xabar uchun hisoblanishi mumkin.
2. Xesh-funksiyaning natijaviy xesh-qiymati fiksirlangan qiymat uzunlikda bo‘ladi.
3. Ixtiyoriy ma’lumotlar bloki (x,y) uchun x^y munosabat o‘rinli bo‘lganda H(x)^H(y) tengsizlik bajariladi.
4. Ixtiyoriy uzunlikdagi ma’lumotlar bloki uchun xesh-funksiyani hisoblash muddati uzoq bo‘lmasligi lozim.
5. Xesh-qiymatlar ma’lum bo‘lganda ham xabarni topa olmasligi lozim.
6. Ixtiyoriy uzunlikdagi ma’lumotlar juftligi uchun (x,y) quyidagi H(x)^H(y) o‘rinli bo‘ladi.

1 - 5 shartlarni bajaruvchi funksiyalar oddiy xesh-funksiyalar deyiladi. 1 - 6 shartlarni bajaruvchi funksiyalar kuchli xesh-funksiyalar deyiladi.

Shunday qilib, xeshlash funksiyasidan xabar o‘zgarishini payqashda foydalanish mumkin, ya’ni u *kriptografik nazorat yig‘indisini* (o‘zgarishlarni payqash kodi yoki *xabarni autentifikatsiyalash kodi* deb ham yuritiladi) shakllantirishga xizmat qilishi mumkin. Bu sifatda xesh- funksiya xabarning yaxlitligini nazoratlashda, elektron raqamli imzoni shakllantarishda va tekshirishda

ishlatiladi.

Xesh-funksiya foydalanuvchini autentifikatsiyalashda ham keng qo‘llaniladi. Axborot xavfsizligining qator texnologiyalarida shifrlashning o‘ziga xos usuli *bir tomonlama xesh-funksiya yordamida shifrlash* ishlatiladi. Bu shifrlashning o‘ziga xosligi shundan iboratki, u mohiyati bo‘yicha bir tomonlamadir, ya’ni xesh-qiymatdan hech qachon xabarni keltirib chiqarib bo‘lmaydi. Qabul qiluvchi tomon shifrni ochish bilan shug‘ullanmaydi, faqat to‘g‘ri yoki noto‘g‘riligini tekshira oladi.

Eng ommabop xesh-funksiyalar - JH, HAVAL, Keccak (SHA- 3), LM-xern, MD2, MD4, MD5, MD6, N-Hash, RIPEMD-128, RIPEMD- 160, RIPEMD-256, RIPEMD-320, SHA-1, SHA-2, Skein, Snefru, Tiger, Whirlpool, GOST R 34.11-94, GOST R 34.11-2012.

MD2, MD4, MD5 va MD6 - R.Rivest tomonidan ishlab chiqilgan axborot daydjestini hisoblovchi algoritm. Ularning har biri 128 bitli xesh- kodni tuzadi. MD2 algoritmi eng sekin ishlasa, MD4 algoritmi tezkor ishlaydi. MD5 algoritmi MD4 algoritmining modifikatsiyasi bo‘lib, MD4 algoritmida xavfsizlikning oshirilishi evaziga tezlikdan yutqazilgan. SHA (Secure Hash Algorithm) - 160 bitli *xesh-kodni* tuzuvchi axborot daydjestini hisoblovchi algoritm. Bu algoritm MD4 va MD5 algoritmlariga nisbatan ishonchliroq.

6.3. Kalitli xesh funksiyalar va ularning xossalari

Kalitli xesh funksiyalarni qo‘llashda ularga quyidagi asosiy talablar qo‘yiladi:

- fabrikatsiya imkoniyatining mavjud emasligi;
- modifikatsiyaning imkoniyati yo‘qligi.

Birinchi talab xesh qiymat berilganda unga mos bo‘lgan ma’lumotni tanlashning murakkab bo‘lishini bildiradi. Ikkinchi talab ma’lumot va uning xesh qiymati berilganda, xesh qiymati shunga teng bo‘ladigan boshqa ma’lumotni tanlash murakkab bo‘lishini bildiradi.

Ba’zan, bu ikkita xossani bitta kuchliroq xossaga – *hisoblash bardoshliligi* xossasiga birlashtiriladi. Bu talab xesh qiymatlari ma’lum bo‘lgan berilgan $\{x_1, x_2, \ldots, x_l\}$ ma’lumotlar uchun xesh qiymatlari shulardan biriga teng bo‘ladigan boshqa $x, \quad x \neq x_i, \quad i = 1, l$ ma’lumotni tanlashning murakkabligini bildiradi.

Murakkab deganda, masalani real vaqt davomida zamonaviy hisoblash qurilmalaridan foydalanib hal qilish imkoniyati bo‘lmaydigan hisoblash murakkabligi tushuniladi.

Kalitli xesh funksiyalar bir-biriga ishonuvchi tomonlar o‘rtasida ishlatiladi va ular umumiy maxfiy kalitga ega bo‘ladilar. Odatda bu sharoitda ikkinchi tomon ma’lumotni qabul qilib olganligini tan olmaslik yoki uni o‘zgartirish holatidan axborot-kommunikatsiya tizimini himoya qilish talab qilinmaydi. SHuning uchun kalitli xesh funksiyalardan kolliziyalarga bardoshlilik talab qilinmaydi.

Kalitli xesh funksiyalarga “imitatsiya” qilish, ya’ni bo‘sh kanalda qalbaki ma’lumotni uzatish hamda uzatilayotgan ma’lumotni qalbaki ma’lumotga almashtirish kabi hujumlar bo‘lishi mumkin.

Hisoblash bardoshliligi xossasidan xesh funksiyada qo‘llanilayotgan kalitni aniqlash imkoniyati yo‘qligi kelib chiqadi, kalitni bilish esa ixtiyoriy ma’lumotning xesh qiymatini hisoblash imkoniyatini beradi. Teskari tasdiq esa o‘rinli emas, chunki ba’zi bir hollarda kalitni oldindan bilmasdan turib, xesh qiymatni tanlash mumkin.

Misol uchun, keng tarqalgan, bir qadamli siqish funksiyasi yordamida qurilgan quyidagi ko‘rinishdagi xesh funksiyani ko‘rish mumkin:

$$f_k(x, H) = E_k(x \oplus H),$$

bu erda E_k –bloklab shifrlash algoritmi.

M -ma’lumotning $h(M)$ qiymatini hisoblash uchun ma’lumot ketma-ket kelgan m bitli $M_1, M_2, \ldots, M_N$ -bloklar ko‘rinishida ifodalanadi. Agar ma’lumot uzunligi blokning uzunligiga karrali bo‘lmasa, oxirgi blok biror maxsus shaklda to‘liq blokkacha to‘ldiriladi. Xesh qiymatni hisoblash algoritmi quyidagi ko‘rinishda bo‘ladi:

$$
\begin{aligned}
&H_0 = 0,\\
&H_i = E_k(M_i \oplus H_{i-1}), \quad i = 1,\ldots,N, \qquad (6.1)\\
&h(M) = H_N.
\end{aligned}
$$

Kalitli xesh funksiyalarni qurishning yana bir usuli kalitsiz xesh funksiyalardan foydalanishdir. Bunda xesh qiymatni hisoblash uchun kalit berilgan ma’lumotga qo‘shib yozib qo‘yiladi.

Agar kalit berilgan ma’lumotning boshiga yoki oxiriga to‘g‘ridan-to‘g‘ri qo‘shib qo‘yilsa, ba’zi hollarda ma’lumotni modifikatsiya qilishga imkon berishi mumkin.

Masalan, k kalit ma’lumotning boshiga $h_k(x) = h(k,x)$ formulaga asosan qo‘shib qo‘yilgan bo‘lsin. Agar h funksiya (6.1) formulaga asosan bir qadamli siquvchi funksiyalar yordamida qurilgan bo‘lsa, u holda M va $H = h(k,M)$ larning ma’lum qiymatlari bo‘yicha biror M' qo‘shib yozilgan (M,M') ko‘rinishdagi ixtiyoriy ma’lumot uchun bu funksiyaning qiymatlarini hisoblash mumkin. Bu xesh funksiyani hisoblashning iterativligi bilan izohlanadi, chunki $H' = h(k,M,M')$ qiymatni topish uchun k kalitning qiymatini bilish shart emas, H qiymatning hisoblangan oraliq qiymatlaridan foydalanish etarli. SHuning uchun bunday funksiya modifikatsiyaga bardoshli emas.

Agar kalit ma’lumotning oxiriga $H = h_k(M) = h(M,k)$ formulaga asosan qo‘shilgan bo‘lsa, h funksiya uchun kolliziyani, ya’ni $h(x_1) = h(x_2)$ bo‘ladigan $x_1, x_2, x_1 \neq x_2$ juftlikni bilish ixtiyoriy k kalit uchun $h(x_1,k) = h(x_2,k)$ qiymatni hisoblash imkonini beradi. SHuning uchun $M = x_1$ ma’lumotni modifikatsiya qilish murakkabligi $O(2^n)$ kattalik bilan emas, balki kolliziyalarni qidirish murakkabligi bilan taqqoslanadi va $O(2^{n/2})$ bilan baholanadi, chunki bu holda *“tug‘ilgan kun” paradoksi*ga asoslangan hujum o‘rinli bo‘ladi.

SHularni e’tiborga olib, kalitni ma’lumotga bir marta emas, bir necha marta qo‘yadigan usullar ishlatiladi. Bunga quyidagi ikkita usulni misol qilib keltirish mumkin:

$$
\begin{aligned}
&H = h(k,y,M,k),\\
&H = h(k,y_1,h(k,y_2,M)),
\end{aligned}
$$

bu erda y, y_1 va y_2 lar k kalitning n uzunlikdagi blokning karralisigacha o‘lchovga to‘ldirilganidir. Kalitsiz xesh funksiyalar uchun bunday usul effektiv hisoblanadigan va hujumlarga bardoshli kalitli xesh funksiyalarni qurish imkonini beradi. Bunday usulning kamchilik tomoni shundaki, xesh qiymatning n uzunligi juda katta bo‘ladi. Odatda, to‘lalikni tekshirish uchun xesh qiymat uzunligi 32 dan 64 bitgacha bo‘lishi, $2^{32} \le n \le 2^{64}$ bajarilishi kerak, autentifikatsiya uchun esa $n \ge 2^{128}$ shartning bajarilishi zarur.

Yuqorida aytib o‘tilgan bloklab shifrlash algoritmiga asoslangan yoki kalitsiz xesh funksiyani hisoblashga asoslangan algoritmlardan tashqari zamonaviy EHMlarda qo‘llash samaradorligini hisobga olib tuzilgan algoritmlar ham mavjud. Bunga MAA (Message Authenticator Algorithm) kalitli xesh funksiya algoritmini misol qilib keltirishimiz mumkin.

O‘zbekiston Respublikasining xesh funksiya davlat standarti O‘zDSt1106:2006 da kalitli xesh funksiya keltirilgan bo‘lib, kalit uzunligi 128 bit yoki 256 bit bo‘lishi mumkin. Evropa Hamjamiyatining RACE dasturi doirasida ishlab chiqilgan RIPE-MAC1 va RIPE-MAC3 xesh funksiya algoritmlari, Nippon Telephone and Telegraph kompaniyasi tomonidan ishlab chiqilgan N-xesh xesh funksiya algoritmi, shuningdek CBC-MAC va CRC-MAC xesh funksiyalarini kalitli xesh funksiya algoritmlariga misol qilib keltirishimiz mumkin.

6.4. Kalitsiz xesh funksiyalar va ularning xossalari

Kalitsiz xesh funksiyalar *xatolarni aniqlash kodlari* (modification detection code (MDC) yoki manipulation detection code, message integrity code (MIC)) deb ham yuritiladi. Kalitsiz xesh funksiya – qo‘shimcha vositalar (shifrlash yoki raqamli imzo) yordamida ma’lumotning to‘laligini kafolatlaydi. Bu xesh funksiyalar bir-biriga ishonuvchi hamda bir-biriga ishonmaydigan foydalanuvchilar tizimlarida ishlatiladi.

Odatda kalitsiz xesh funksiyalardan quyidagi xossalarni qanoatlantirishi talab qilinadi:

1) bir tomonlamalik;

2) kolliziyaga bardoshlilik;
3) xesh qiymatlari teng bo‘lgan ikkita ma’lumotni topishga bardoshlilik.

Birinchi shart berilgan xesh qiymatga ega bo‘lgan ma’lumotni, ikkinchi shart bir xil xesh qiymatga ega bo‘lgan ma’lumotlar juftini, uchinchi shart xesh qiymati ma’lum bo‘lgan berilgan ma’lumot uchun xesh qiymati shunga teng bo‘lgan ikkinchi ma’lumotni topishning murakkab ekanligini bildiradi.

Masalan, nazorat yig‘indini topuvchi SRC xesh funksiyasi chiziqli akslantirish bo‘ladi va shuning uchun ham bu uchta shartdan birontasini ham qanoatlantirmaydi.

Kalitsiz xesh funksiya sifatida yuqorida qaralgan “imitovstavka”ni ishlab chiqish rejimidagi bloklab shifrlash algoritmi asosida qurilgan (5.1) ko‘rinishdagi xesh funksiyadan foydalanish ham maqsadga muvofiq emas. CHunki, bloklab shifrlash algoritmining teskarilanuvchanligi ixtiyoriy xesh qiymat uchun fiksirlangan va hammaga ma’lum bo‘lgan kalitda kiruvchi ma’lumotni tanlash imkonini beradi.

Birinchi shartni qanoatlantiruvchi xesh funksiyaga misol qurish uchun

$$g_k(x) = E_k(x) \oplus x$$

formula bilan berilgan funksiyani qaraylik. Bu erda E_k -bloklab shifrlash algoritmi, ya’ni kriptografik funksiyasi. Bunday funksiyalar ikkala argumenti bo‘yicha ham bir tomonlama bo‘ladi. Shuning uchun, (6.1) qoidaga asosan bir qadamli siquvchi funksiyani

$$H=f(x,H)=E_H(x)\oplus x \qquad (6.2)$$

yoki

$$H=f(x,H)=E_x(H)\oplus H \qquad (6.3)$$

funksiyalardan biri deb olinib, uning asosida xesh funksiyani qurish mumkin.

Rossiyaning xesh funksiya standarti GOST P 34.11-94 asosida (6.3) formula, AQSHning xesh funksiya standarti SHA asosida (6.2) formula yotadi.

Quyidagi tasdiq o‘rinli:

6.1-tasdiq. Agar *h* xesh funksiya (6.1) qoidaga ko‘ra bir qadamli siquvchi *f* funksiyaga asosan qurilgan bo‘lsa, u holda *f* funksiyaning kolliziyaga bardoshliligidan *h* funksiyaning ham kolliziyaga bardoshliligi kelib chiqadi.

Haqiqatan ham, agarda *h* funksiya kolliziyaga ega bo‘lsa, u holda biror *i*-qadamda *f* funksiya ham kolliziyaga ega bo‘lishi kerak. Bu erda kolliziyani aniqlashda $f(x_1, x_2)$ funksiya x_1 va x_2 o‘zgaruvchilarni bitta kirish vektoriga konkatenatsiya qilishdan hosil qilingan bir o‘zgaruvchili funksiya deb qaralishi kerak.

Quyida 1) va 2) xossalar orasida o‘zaro bog‘liqlik mavjudligini ko‘rsatiladi:

6.2-tasdiq. Agar xesh funksiya kolliziyaga bardoshli bo‘lsa, u holda u o‘zining xesh qiymatlari teng bo‘lgan ikkita ma’lumotni topishga ham bardoshli bo‘ladi.

Haqiqatan ham, agar berilgan ma’lumotning xesh qiymati bo‘yicha shu xesh qiymatga ega bo‘lgan boshqa ma’lumotni tanlash mumkin bo‘lsa, u holda hosil qilingan ma’lumotlar jufti kolliziyani tashkil qiladi.

6.3 - tasdiq. Kolliziyaga bardoshli xesh funksiya bir tomonlama bo‘lishi shart emas.

Bu tasdiqqa misol sifatida siquvchi bo‘lmagan $f(x) = x$ funksiyani keltirish mumkin. Ravshanki bu funksiya kolliziyaga bardoshli, lekin bir tomonlama funksiya emas.

Siquvchi xesh funksiyaga misol sifatida quyidagi shartlar bilan aniqlangan *h* funksiya ko‘rilishi mumkin:

- $h(x) = (1, x)$, *agar x ning uzunligi nbitga teng bo‘lsa;*
- $h(x) = (0, g(x))$, *agar x ning uzunligi nbitdan katta bo‘lsa.*

Bu erda $g(x)$ kolliziyaga bardoshli bo‘lgan, siquvchi *n* bitlik funksiya.

h funksiya kolliziyalarga hamda xesh qiymatlari teng bo‘lgan ikkita ma’lumotni topishga bardoshli funksiya, lekin u bir tomonlama funksiya emas.

6.4-tasdiq. $h: X \to Y$ xesh funksiya berilgan bo‘lib, $|X| > 2|Y|$ bo‘lsin. Agarda *h* funksiyaning teskarisini topishning samarali algoritmi mavjud bo‘lsa, u

holda h funksiyaning kolliziyalarini muvaffaqiyatli topishning ehtimoli $\frac{1}{2}$ dan katta bo‘lgan ehtimoliy algoritmi mavjud bo‘ladi.

Bir tomonlama funksiya uchun xesh qiymatlari teng bo‘lgan ikkita ma’lumotni tanlash yoki xesh qiymatlari teng bo‘lgan ikkita ma’lumotni qidirish murakkablik darajasi $O(2^n)$ bilan baholanadi. SHu bilan birga kolliziyani qidirish murakkablik darajasi $O(2^{n/2})$ bilan baholanadi, chunki bu holatda “tug‘ilgan kun” paradoksiga asoslangan hujumni qo‘llash mumkin.

Quyida bloklab shifrlash algoritmlari asosida qurilgan xesh funksiyalarga misollar ko‘rib o‘tiladi.

E_k -bloklab shifrlash algoritmi, n -blokning uzunligi, l -kalit uzunligi va G uzunligi n bo‘lgan vektorga l uzunlikdagi vektorni mos qo‘yuvchi biror akslantirish bo‘lsin. E_k -bloklab shifrlash algoritmi asosida qurilgan quyidagi bir qadamli siquvchi funksiyalar ko‘riladi:

a) $f(x,H) = E_x(H) \oplus H$ (Devis-Meyer);

b) $f(x,H) = E_{G(x)}(x) \oplus x$ (Matias-Meyer-Oseas);

v) $f(x,H) = E_{G(x)}(x) \oplus x \oplus H$ (Miaguchi-Prinel).

Bu keltirilgan bir qadamli siquvchi funksiyalardan foydalanib qurilgan ixtiyoriy xesh funksiya qiymatining uzunligi o‘lchami n bo‘lgan blok uzunligiga teng vektor bo‘ladi. Agar bu uzunlik etarli bo‘lmasa, u holda bir qadamli f funksiyani uzunligining o‘lchami undan ikki marta katta bo‘lgan f' funksiya bilan almashtirish mumkin. Buni masalan, f funksiyani ikki marta qo‘llash va undan keyin yarim bloklarni aralashtirish bilan quyidagi formula asosida amalga oshirish mumkin:

$$f'(x,H_1,H_2) = \pi(f(x,H_1), f(x,H_2)),$$

bu erdagi π funksiya ixtiyoriy a,b,c,d -yarim bloklarni $\pi((a,b),(c,d)) = (a,d,c,b)$ qoida bo‘yicha almashtiradi. Bunday usul Matias-Meyer-Oseas sxemasidan foydalanib, MDC-2 bir qadamli funksiyasini qurishda qo‘llanilgan.

Umuman olganda bloklab shifrlash algoritmlaridan foydalanilib quriladigan kalitsiz xesh funksiyalarda blok uzunligi xesh qiymat uzunligiga teng bo‘ladigan sxemalar mavjud. Quyida ushbu tipdagi algoritmlarning umumiy sxemasi keltirilgan:

$H_0 = I_H$,

$H_i = E_A(B) \oplus C$.

Bu erda I_H -boshlang‘ich tasodifiy qiymat, *A*, *B* va *C* lar $M_i, H_{i-1}, (M_i \oplus H_{i-1})$ ga teng bo‘lishi mumkin, M_i -kiruvchi blok, H_i -iteratsiyaning *i* – qadami. Ushbu algoritmlarning ko‘rinishi quyidagicha:

1. $H_i = E_{Hi-1}(M_i) \square\square M_i$
2. $H_i = E_{Hi-1}(M_i \oplus H_{i-1}) \oplus M_i \square\square H_{i-1}$
3. $H_i = E_{Hi-1}(M_i) \square\square H_{i-1} \square\square M_i$
4. $H_i = E_{Hi-1}(M_i \square\square E_{Hi-1}) \square\square M_i$
5. $H_i = E_{Mi}(H_{i-1}) \square\square H_{i-1}$
6. $H_i = E_{Mi}(M_i \oplus H_{i-1})\ M_i \oplus H_{i-1}$
7. $H_i = E_{Mi}(H_{i-1}) \oplus M_i \square\square H_{i-1}$
8. $H_i = E_{Mi}(M_i \square\square H_{i-1}) \square\square H_{i-1}$
9. $H_i = E_{Mi \square Hi-1}(M_i) \square\square M_i$
10. $H_i = E_{Mi \square Hi-1}(H_{i-1}) \square\square H_{i-1}$
11. $H_i = E_{Mi \square Hi-1}(M_i) \square\square H_{i-1}$
12. $H_i = E_{Mi \square Hi-1}(H_{i-1}) \square\square M_i$

Boshqa kalitsiz xesh funksiyalarga MD4, MD5 va SHA xesh funksiyalari misol bo‘la oladi. Bu algoritmlar 32 razryadli EHMlarda samarali qo‘llanilishga mo‘ljallanib, maxsus loyihalashtirilgan algoritmlardir.

Bu algoritmlardan foydalanilganda berilgan *M* ma’lumot uzunligi $m = 512$ bit bo‘lgan bloklarga ajratiladi. Oxirgi blok ma’lumot oxiriga blokning uzunligi 448 bit bo‘lguncha 1000....000 kombinatsiyani qo‘shish bilan hosil qilinadi, undan

keyin ma’lumot uzunligini ifodalovchi 64 bitli kombinatsiya qo‘shiladi. Keyin $f(x,H) = E_H(H) \oplus H$ formula bilan berilgan bir qadamli siquvchi funksiyadan foydalanib, (5.1) tartibotga (protseduraga) asosan xesh qiymat hisoblanadi. Bu erda x – uzunligi $m = 512$ bit bo‘lgan ma’lumot bloki, N – n bitlik blok, E_x -bloklar to‘plamidagi biror akslantirish. Boshlang‘ich vektorning qiymati E_x akslantirishni aniqlashda beriladi.

GOST R 34.11-94 xesh funksiya standartida $n = m = 512$ qiymatlar qabul qilingan. $H_i = f(x_i, H_{i-1})$ qiymatlarni ketma-ket hisoblashda foydalaniladigan bir qadamli $f(x,H)$ siquvchi funksiya har biri 256 bit kalitga ega bo‘lgan va 64 bit uzunlikdagi bloklar bilan amallar bajaruvchi to‘rtta parallel ishlovchi bloklab shifrlash sxemasi (GOST 28147-89) negizida qurilgan. Har bir kalit mos ravishda kiruvchi x_i ma’lumot bloki va H_{i-1} qiymatning biror chiziqli funksiyasi ko‘rinishida hisoblanadi. H_i qiymat kiruvchi x_i ma’lumot bloki va H_{i-1} qiymat shifrlanishi natijasining chiziqli funksiyasi bo‘ladi. H_N qiymatni $M_1, M_2, \ldots, M_N$ bloklar ketma-ketligi uchun hisoblagandan keyin

$$H = h(M) = f(Z \oplus M_N, f(L, H_N))$$

formulaga asosan yana ikki qadam hisoblash bajariladi. Bu erda Z – ma’lumot barcha bloklarining modulь ikki bo‘yicha yig‘indisi, L – ma’lumot uzunligi.

Hozirgi kunda ko‘plab davlat standartlari xesh funksiyalarining algoritmlari kalitsiz xesh funksiya algoritmlaridir. Bunga misol qilib Rossiyaning GOST P 34.11-94 xesh funksiya davlat standartini, AQSHning federal standarti FIPS PUB 180 da keltirilgan SHA-0, FIPS PUB 180-1 da keltirilgan SHA-1, FIPS PUB 180-2 da keltirilgan SHA-256, SHA-384, SHA-512 xesh funksiyalarini, Belarusь Respublikasining xesh funksiya davlat standarti STB 1176.1 – 99 ni, AQSHning federal standarti SHA turidagi xesh funksiyalarni yaratishga asos bo‘lgan MD turidagi xesh funksiyalar va ularning modifikatsiyalari MD2, MD4 va MD5 xesh funksiyalarini (AQSHning federal standarti aynan MD5 xesh funksiyasi asosida ishlab chiqilgan), Evropa Hamjamiyatining RACE dasturi doirasida MD4 asosida ishlab chiqilgan RIPE-MD va uning modifikatsiyalari RIPEMD-160, RIPEMD-

256 va RIPEMD-320 xesh funksiyalarini, MD5 asosida ishlab chiqilgan HAVAL xesh funksiyasini va yuqoridagi xesh funksiyalar algoritmlaridan farq qiluvchi algoritmga ega bo‘lgan TIGER xesh funksiyasini keltirish mumkin [14, 29, 30, 31, 34-37].

Autentifikatsiya atamasi axborot-kommunikatsiya tarmoqlarida ma’lumotlar almashinuvi sub’ektlarining haqiqiylikni aniqlashini bildiradi. Bu ma’lumot almashishdagi barcha aspektlarga ta’lluqli bo‘lib, aloqa seansining, tomonlarning, ma’lumotning haqiqiyligini bildiradi. Bu aloqa tarmog‘i orqali uzatilgan ma’lumot manbai va mazmuni jihatidan, ma’lumotning yaratilgan vaqti hamda jo‘natilgan vaqti jihatidan tekshirganda haqiqiy bo‘lishini anglatadi.

Ma’lumot to‘laligi – ma’lumot yaratilgandan keyin uni saqlashda va uzatishda uning begonalar tomonidan o‘zgartirilmaganligiga ishonch hosil qilishni bildiradi. Ma’lumotni o‘zgartirish deganda odatda unga qo‘shimchalar qo‘shish, tushirib qoldirish, o‘zgartirish va ma’lumot qismlarining o‘rnini almashtirish tushuniladi.

Ma’lumotning manbaini autentifikatsiya qilish – qabul qilingan elektron hujjat haqiyqiy manba tomonidan yaratilganining tasdig‘ini olishdir. Bunda hujjat yaratilgan vaqt va elektron hujjatning yagonaligini tekshirish talab qilinmaydi. Hujjat yagonaligining buzilishi deganda, uni qaytadan uzatish yoki undan qaytadan foydalanish tushuniladi.

Ma’lumotning haqiqiyligi va ma’lumot manbaini autentifikatsiya qilish tushunchalari bir-biri bilan chambarchas bog‘liqdir. Haqiqatan ham, agar ma’lumot modifikatsiya qilingan bo‘lsa, uning manbai ham o‘zgaradi. Agar manba aniqlanmagan bo‘lsa, to‘lalik masalasini hal qilib bo‘lmaydi.

Endi xesh funksiyani axborot-kommunikatsiya tizimlarida qo‘llash sxemalari qarab chiqiladi:

a) $A \rightarrow V: E_K[M||H(M)]$ (5.1 a) – rasm)

-maxfiylikni ta’minlaydi (K kalit faqat A va V tomonlarga ma’lum).

-to‘lalikni ta’minlaydi (N(M) kriptografik himoyalangan).

b) $A \rightarrow V: M|| E_K[H(M)]$ (5.1 b) – rasm)

-to‘lalikni ta’minlaydi (N(M) kriptografik himoyalangan).

v) A→V:M||E_Y[H(M)] (5.1 v) – rasm)

-to‘lalikva raqamli imzoni ta’minlaydi (N(M) kriptografik himoyalangan hamda E_Y[H(M)] ni faqat A tomon hosil qilishi mumkin).

g) A→V: E_K[M||E_Y[H(M)]] (5.1 g) – rasm)

-to‘lalikva raqamli imzoni ta’minlaydi.

-maxfiylikni ta’minlaydi (K kalit faqat A va V tomonlarga ma’lum).

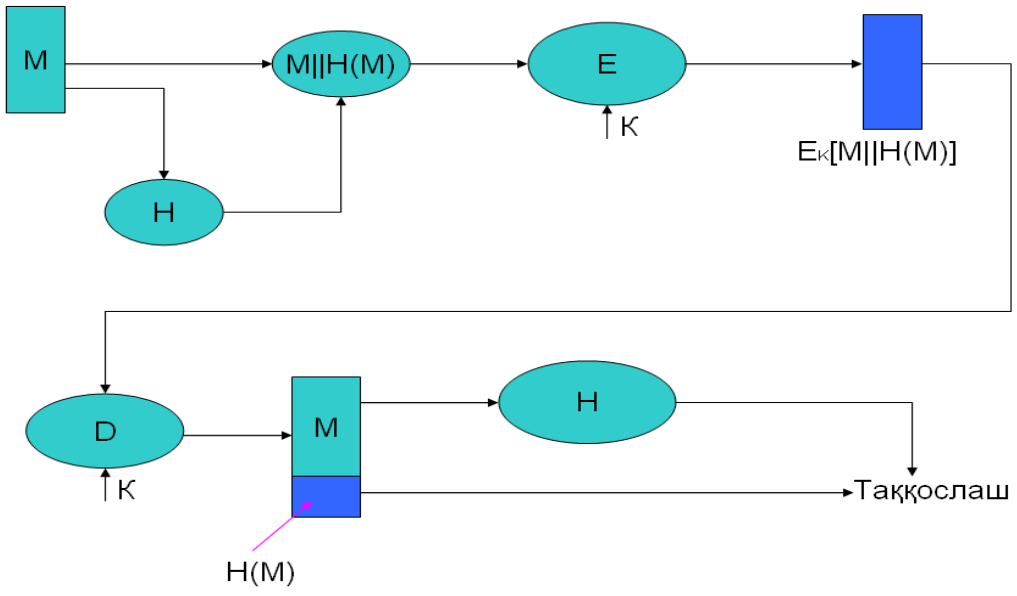
d) A→V: M||H(M||S) (5.1 d) – rasm)

- to‘lalikni ta’minlaydi (S faqat A va V tomonlarga ma’lum).

e) A→V: E_K[M||H(M||S)] (5.1 e) – rasm)

-maxfiylikni ta’minlaydi (K kalit faqat A va V tomonlarga ma’lum).

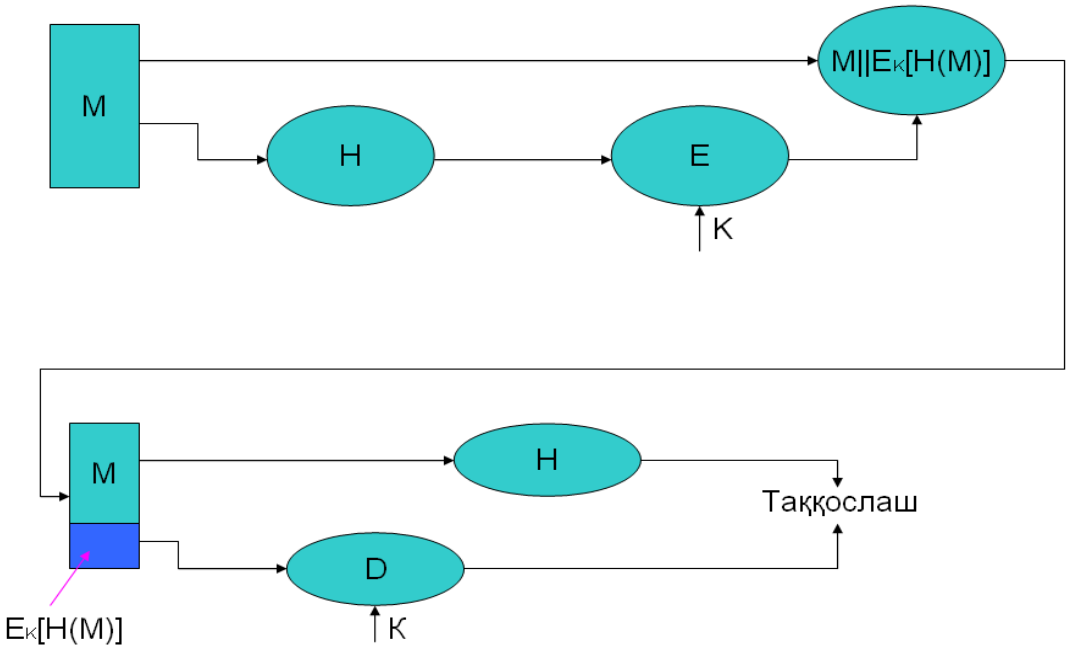
-to‘lalikni ta’minlaydi (S faqat A va V tomonlarga ma’lum).



(a)

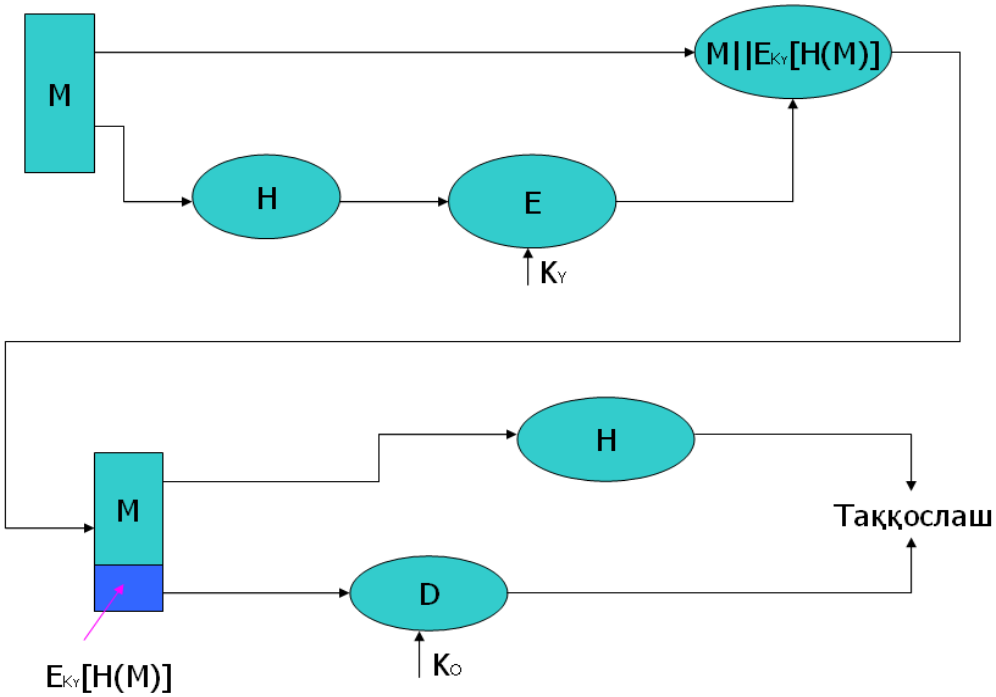
Axborot-kommunikatsiya tizimlarida xesh funksiyalarni qo‘llash sxemalari:

5.1 a) – rasm.



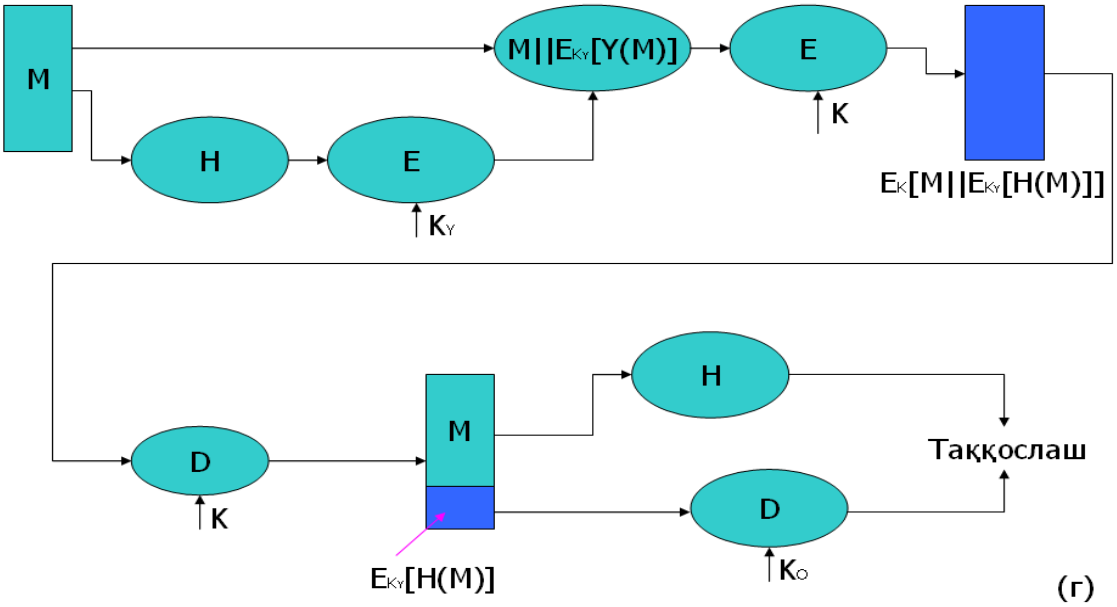
(б)

5.1 b) –rasm.

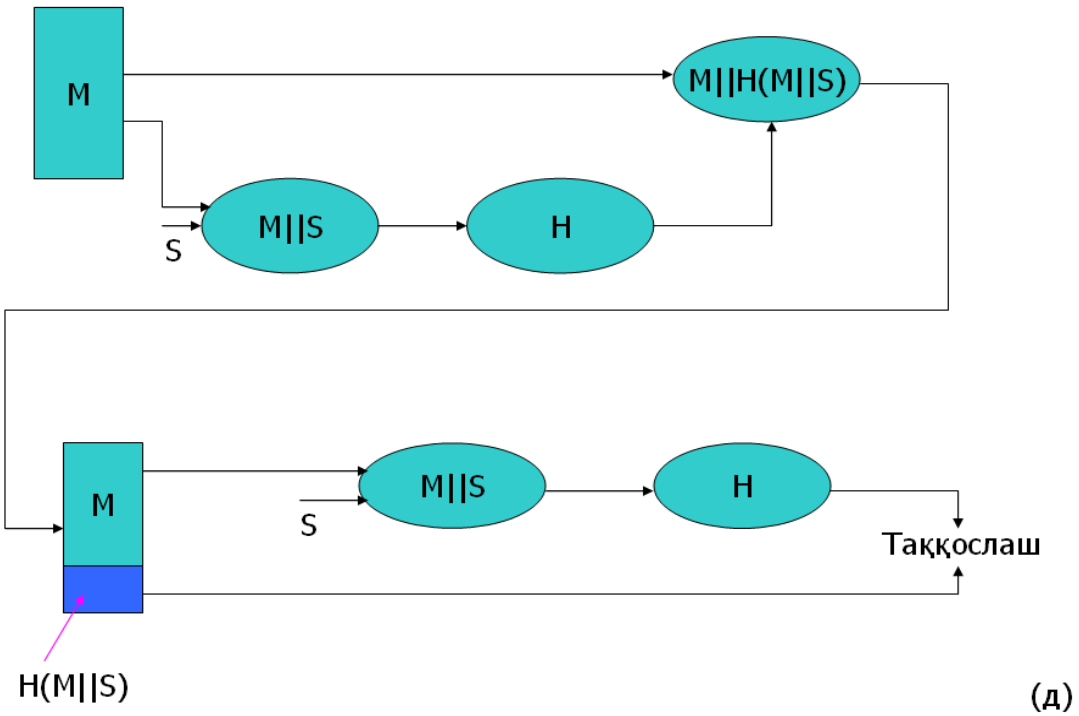


(в)

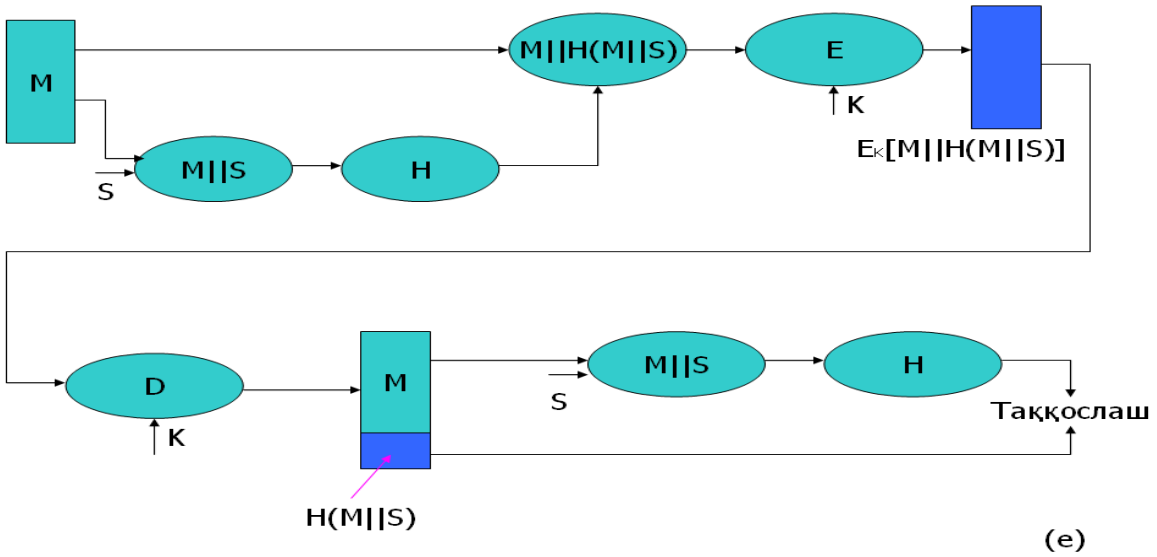
5.1 v) – rasm.



5.1 g) – rasm.



5.1 d) – rasm.



5.1 e) – rasm.

Quyida mavjud standart xesh funksiyalarining kriptografik xossalari jadvali keltiriladi:

1-jadval

	Xeshlanadigan matn uzunligi	Kirish blokining uzunligi	Xesh qiymat uzunligi	Har bir blokni xeshlash qadamlari soni
GOST R 34.11-94	Ixtiyoriy	256	256	19
MD 2	Ixtiyoriy	512	128	1598
MD 4	Ixtiyoriy	512	128	72
MD 5	Ixtiyoriy	512	128	88
SHA-1	$<2^{64}$	512	160	80
SHA-256	$<2^{64}$	512	256	64
SHA-384	$<2^{128}$	1024	384	80
SHA-512	$<2^{128}$	1024	512	80
STB 1176.1 – 99	Ixtiyoriy	256	$142 \leq L \leq 256$	77
O‘zDSt 1106 : 2006	Ixtiyoriy	128, 256	128, 256	16b+74, 16b+46, Bu erda b-bloklar

				soni

6.5. GOST R 34.11-94 xesh funksiyasi algoritmi

Rossiyaning GOST R 34.11-94 xesh funksiya standarti axborotni kriptografik usulda muhofaza qilish uchun, xususan GOST R 34.10-94 va GOST R 34.10-2001 elektron raqamli imzo algoritmlarida ishlatish uchun mo‘ljallangan [35]. Xesh funksiyaning qiymatini hisoblash jarayonida GOST 28147-89 shifrlash standartidan foydalaniladi.

GOST R 34.11-94 xesh funksiya standartida chiqish uzunligi belgilangan qadamli xeshlash funksiyasidan foydalanuvchi ketma-ket xeshlash usulidan foydalaniladi. Xesh funksiya argumentining uzunligi 256 bit bo‘lgan funksiya bo‘lib, xesh qiymat uzunligi 256 bit bo‘ladi. Xeshlanadigan ma’lumot uzunligi ixtiyoriy bo‘lib, ma’lumot uzunligi 256 bit bo‘lgan bloklarga ajratiladi. Oxirgi blok uzunligi 256 bitdan kichik bo‘lsa, 256 bitgacha nol bilan to‘ldiriladi. Undan tashqari, bu bloklarning oxiriga ma’lumot uzunligining kodini bildiruvchi va nazorat yig‘indisini bildiruvchi yana ikkita 256 bitlik bloklar qo‘shiladi. Ma’lumot uzunligining kodini blok xeshlanadigan ma’lumotning bit uzunligi mod 2^{256} bo‘yicha hisoblanib (bu protsedura MD kuchaytirish deyiladi) hosil qilinadi. Nazorat yig‘indisining kodini bildiruvchi blok esa, oxirgi to‘liqmas blok nolь bilan to‘ldirilgandan keyin barcha bloklarning yig‘indisi mod 2^{256} bo‘yicha hisoblanib hosil qilinadi.

GOST R 34.11-94 xesh funksiyasini hisoblashda quyidagi belgilashlardan foydalaniladi:

M – xeshlanishi kerak bo‘lgan ma’lumot,

h – M ma’lumotni $h(\mathrm{M}) \in V_{256}(2)$ ga akslantiruvchi xesh funksiya, bu erda $V_{256}(2)$ – uzunligi 256 bit bo‘lgan barcha ikkilik so‘zlar to‘plami,

$E_K(A)$ - A ni GOST 28147-89 shifrlash algoritmidan foydalanib K kalitda shifrlash natijasi,

$\mathrm{N} \in V_{256}(2)$ – berilgan boshlang‘ich vektor.

GOST R 34.11-94 xesh funksiyasini hisoblash uchun quyidagilar zarur:

- qadamli xeshlash funksiyasi $\chi : V_{256}(2) \times V_{256}(2) \to V_{256}(2)$ ni hisoblash algoritmi;

- xesh qiymatni iterativ hisoblash jarayoni.

Qadamli xeshlash funksiyasi uch bosqichda hisoblanadi. Birinchi bosqichda uzunliklari 256 bit bo‘lgan to‘rtta K_1, K_2,K_3,K_4 kalit generatsiya qilinadi. Ikkinchi bosqichda boshlang‘ich N vektor har birining uzunligi 64 bit bo‘lgan to‘rtta blokka ajratiladi va bu bloklar mos K_1, K_2, K_3, K_4 kalitlar bilan GOST 28147-89 algoritmi yordamida shifrlanadi. Uchinchi bosqichda shifrlash natijasini aralashtiruvchi akslantirish bajariladi.

Quyida xesh funksiya standartidagi akslantirish jarayonlarining har bir qadami ko‘rib chiqiladi:

1. **Kalitlar generatsiyasi.**

$X=(b_{256}, b_{255}, \ldots, b_1) \in V_{256}(2)$ berilgan bo‘lsin.

$X=x_4||x_3||x_2||x_1=\eta_{16}||\eta_{15}||\ldots||\eta_1=\xi_{32}||\xi_{31}||\ldots||\xi_1$ deb olamiz, bu erda $x_i \in V_{64}(2)$, i=1,2,3,4, $\eta_j \in V_{16}(2)$, j=1, …,16, $\xi_k \in V_8(2)$, k=1,…,32 bo‘ladi.

$A(X)=(x_1 \oplus x_2)||x_4||x_3||x_2$, deb belgilanadi.

P: $V_{256}(2) \to V_{256}(2)$ akslantirish $\xi_{32}||\xi_{31}||\ldots||\xi_1$ ni $\xi_{\varphi(32)}||\xi_{\varphi(31)}||\ldots||\xi_{\varphi(1)}$ ga akslantirsin, bu erda $\varphi(i+1+4(k-1))=8i+k$, i=0,1,2,3; k=1, 2, …,8.

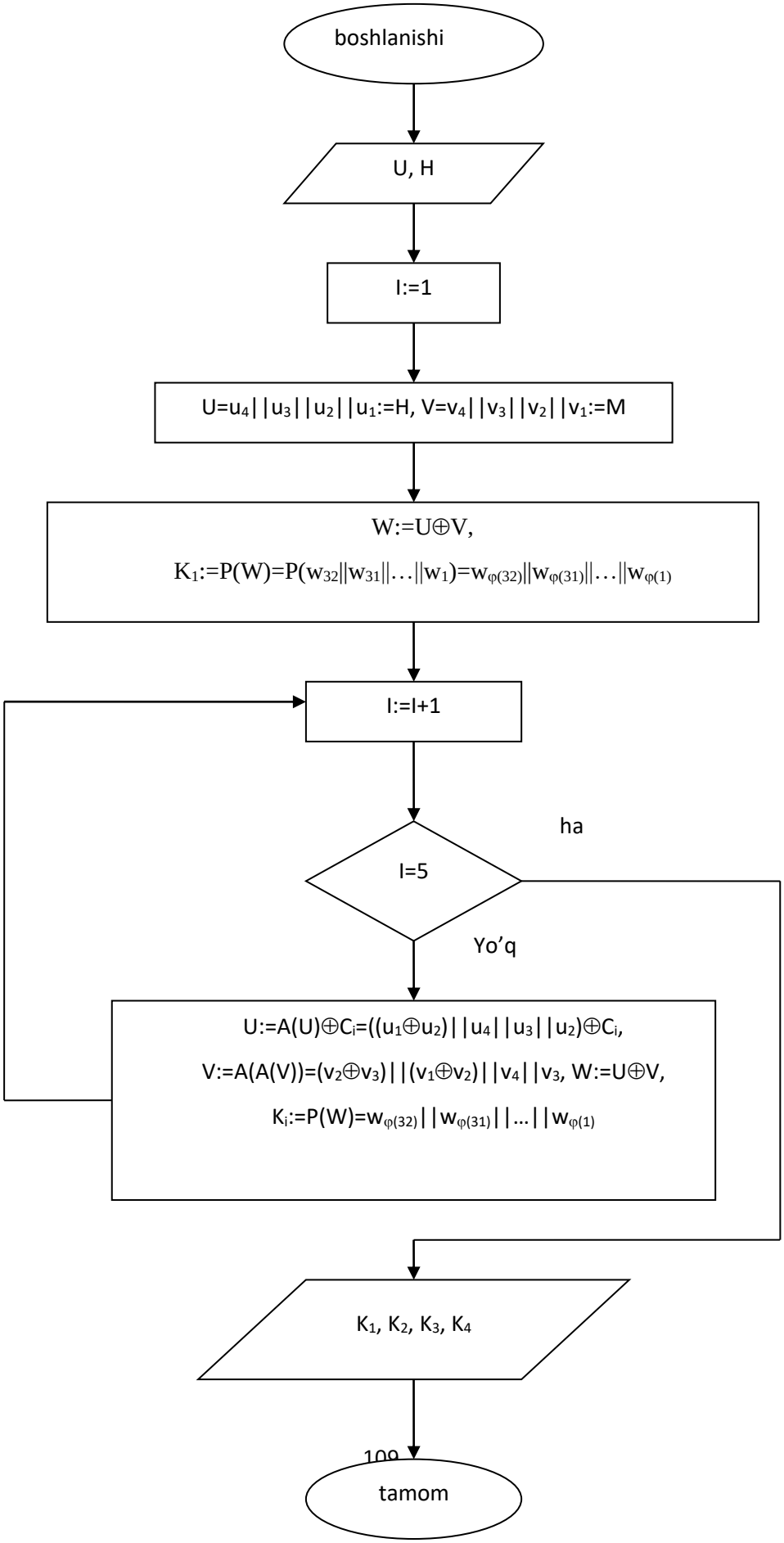
K_1, K_2,K_3,K_4 kalitlarni generatsiya qilish uchun N, M $\in V_{256}(2)$ berilganlar hamda $S_2=S_4=0^{256}$ va $S_3=1^80^81^{16}0^{24}1^{16}0^8(0^81^8)^21^80^8(0^81^8)^4(1^80^8)^4$ –o‘zgarmaslardan foydalaniladi.

Maxfiy kalitlarni generatsiya qilish algoritmi quyidagi qadamlar asosida amalga oshiriladi: i=1, U=H, V=M.

1. $W=U \oplus V$, $K_1=P(W)$.
2. i=i+1. i=5 shartni tekshiramiz, agar bu shart bajarilsa 7-qadamga o‘tiladi, aks holda 5-qadamga o‘tiladi.
3. $U=A(U) \oplus C_i$, $V=A(A(V))$, $W=U \oplus V$, $K_i=P(W)$.
4. 3-qadamga o‘tiladi.

5. Algoritm ishini tugatadi.

Quyida ushbu algoritmning blok-sxemasi keltirilgan:



2. Shifrlovchi akslantirish.

Bu bosqichda N ni to‘rtta 64 bitlik qismlarga ajratamiz va ularni K_1, K_2,K_3,K_4 –kalitlar yordamida shifrlaymiz.

SHifrlovchi akslantirishda $H=h_4||h_3||h_2||h_1$, $h_i \in V_{64}(2)$, i=1,2,3,4 berilganlar va K_1, K_2,K_3,K_4 -kalitlardan foydalaniladi.

SHifrlagandan keyin $s_i=E_{Ki}(h_i)$, i=1,2,3,4 ni hosil qilamiz. Natijada

$S=s_4||s_3||s_2||s_1$

vektor hosil bo‘ladi.

3. Aralashtiruvchi akslantirish.

Bu bosqichda berilgan 256 bitlik ketma-ketlik 16 bitlik so‘zlarga ajratilib, ularni aralashtiruvchi akslantirish bajariladi. Buning uchun bizga N, M, $S \in V_{256}(2)$ lar berilgan bo‘ladi.

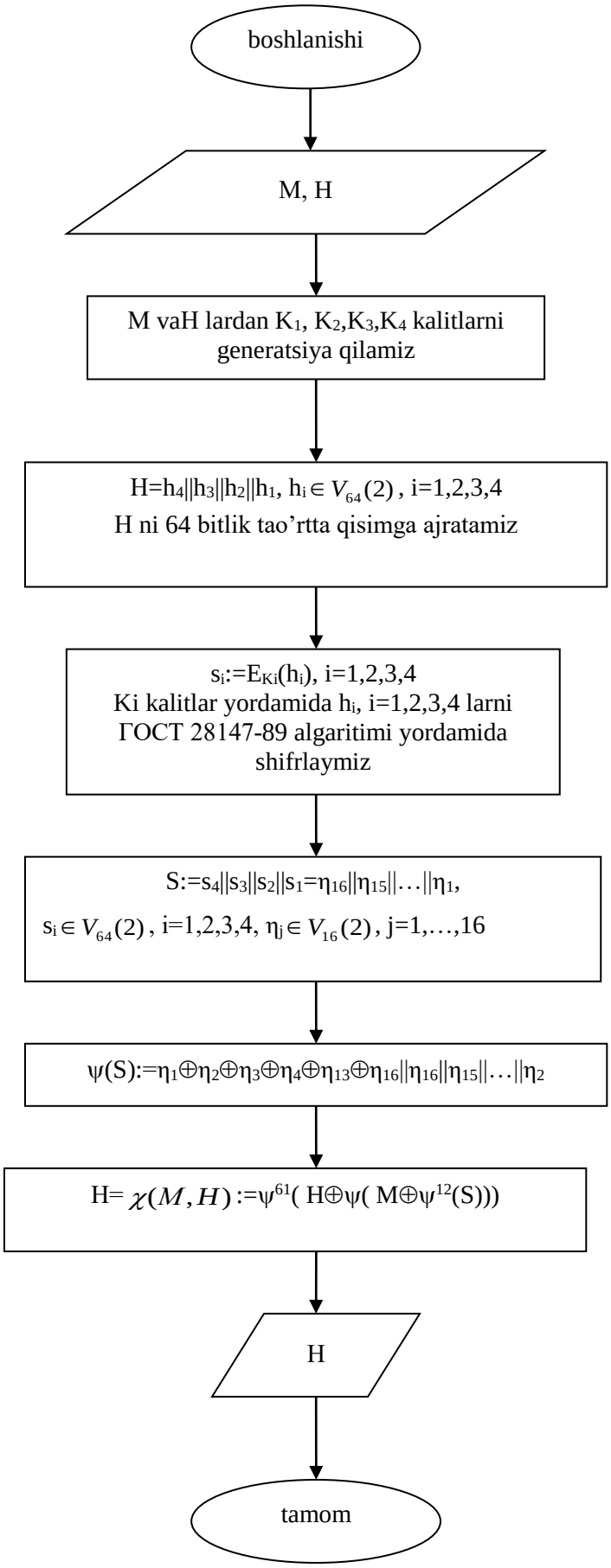
$\psi : V_{256}(2) \to V_{256}(2)$ akslantirish $\eta_{16}||\eta_{15}||\ldots||\eta_1$, $\eta_j \in V_{16}(2)$, j=1,…,16 so‘zni $\eta_1 \oplus \eta_2 \oplus \eta_3 \oplus \eta_4 \oplus \eta_{13} \oplus \eta_{16}||\eta_{16}||\eta_{15}||\ldots||\eta_2$ co‘zga akslantirsin.

U holda qadamli xeshlash (iteratsiya) funksiyasi quyidagicha aniqlanadi:

$$\chi(M,H) = \psi^{61}(H \oplus \psi(M \oplus \psi^{12}(S))).$$

Bu erda ψ^i - ψ akslantirishning i - darajasi.

Quyida qadamli xeshlash funksiyasini hisoblash algoritmining blok-sxemasi keltirilgan:


boshlanishi
M, H
M vaH lardan K1, K2,K3,K4 kalitlarni generatsiya qilamiz
H=h4||h3||h2||h1, hi ∈ V64(2) , i=1,2,3,4
H ni 64 bitlik tao'rtta qisimga ajratamiz
si:=EKi(hi), i=1,2,3,4
Ki kalitlar yordamida hi, i=1,2,3,4 larni ГОСТ 28147-89 algaritimi yordamida shifrlaymiz
S:=s4||s3||s2||s1=η16||η15||…||η1,
si ∈ V64(2) , i=1,2,3,4, ηj ∈ V16(2) , j=1,…,16
ψ(S):=η1⊕η2⊕η3⊕η4⊕η13⊕η16||η16||η15||…||η2
H= χ(M,H) :=ψ61(H⊕ψ(M⊕ψ12(S)))
H
tamom

Xesh funksiyani hisoblash tartiboti (protsedurasi).

M – xeshlanishi kerak bo‘lgan ma’lumot berilgan bo‘lsin. *h* xesh qiymatni hisoblash uchun parametr sifatida $N \in V_{256}(2)$ boshlang‘ich vektor berilgan bo‘lsin.

h xesh qiymatni hisoblash jarayonining har bir iteratsiyasida quyidagi miqdorlardan foydalaniladi:

M –berilgan xeshlanishi kerak bo‘lgan ma’lumotning oldingi iteratsiyalarda xeshlash jarayonidan o‘tmagan qismi;

$N \in V_{256}(2)$ – xesh funksiyaning joriy qiymati;

$Sum \in V_{256}(2)$ – nazorat yig‘indisining joriy qiymati;

$L \in V_{256}(2)$ – berilgan ma’lumotning oldingi iteratsiyalardan o‘tgan qismi uzunligining joriy qiymati.

Xesh qiymatni hisoblash jarayoni quyidagi uchta bosqichdan iborat:

1-bosqich.

Joriy miqdorlarga boshlang‘ich qiymatlar beriladi:

1.1 M:=M;

1.2. H:=H;

1.3. Sum:=0^{256};

1.4. L:=0^{256}.

2-bosqich.

2.1. |M|>256 shart tekshiriladi;

Agar bu shart bajarilsa 3-bosqichga o‘tiladi, aks holda quyidagi hisoblashlar ketma-ketligi bajariladi:

2.2. L=(L + |M|) mod 2^{256};

2.3. T=$0^{256-|M|}$||M;

2.4. Sum=(Sum + T) mod 2^{256};

2.5.H= $\chi(T,H)$;

2.6.H= $\chi(L,H)$;

2.7.H= $\chi(Sum,H)$;

2.8. Algoritm o‘z ishini tugallaydi.

3-bosqich.

3.1. Berilgan M ma’lumotning $M_S \in V_{256}(2)$ qismi ajratib olinadi ($M=M_P||M_S$); keyin quyidagi hisoblashlar ketma-ketligi bajariladi:

3.2. H= $\chi(M_S, H)$;

3.3. L=(L+256) mod 2^{256};

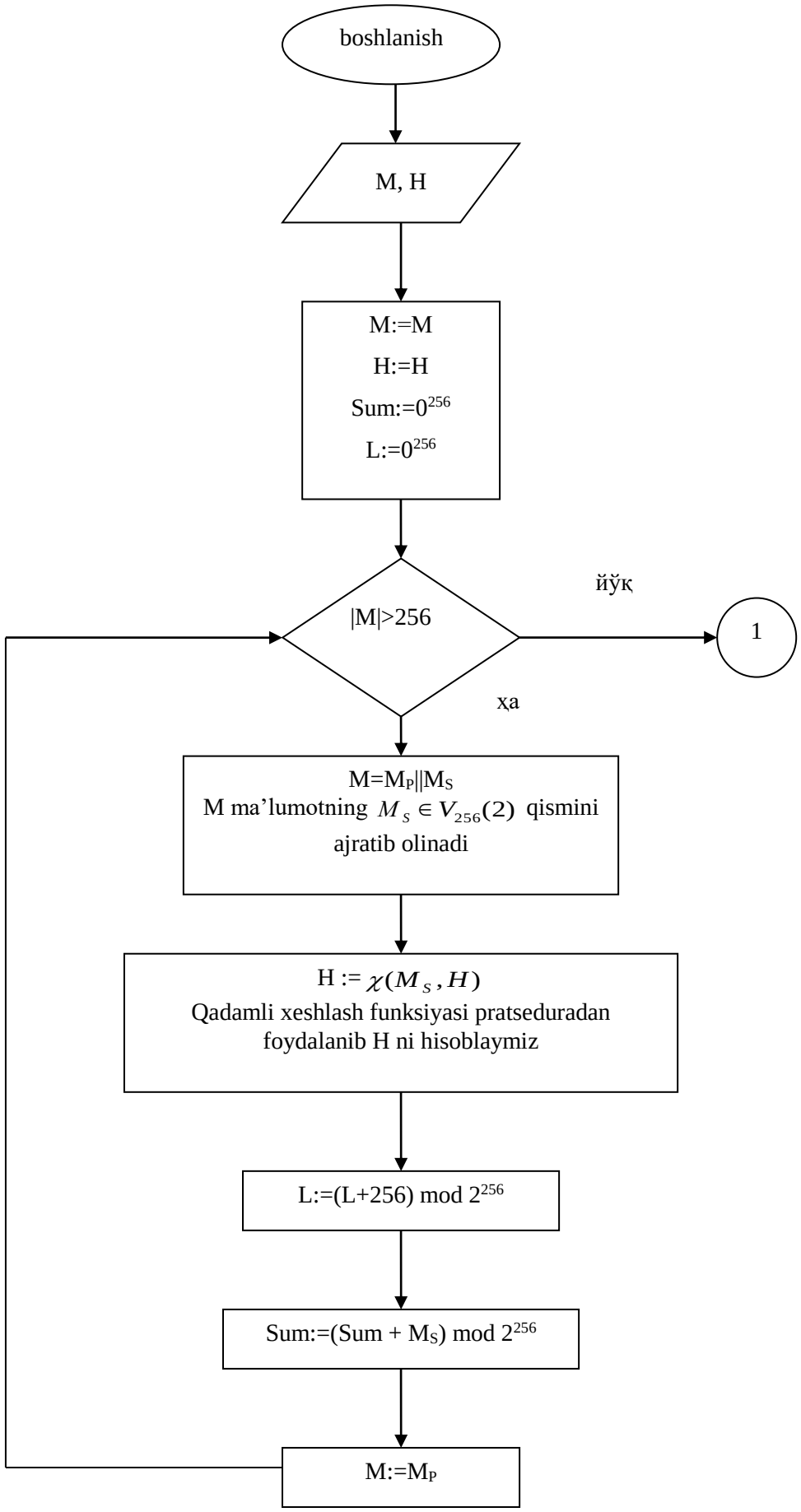
3.4. Sum=(Sum + M_S) mod 2^{256};

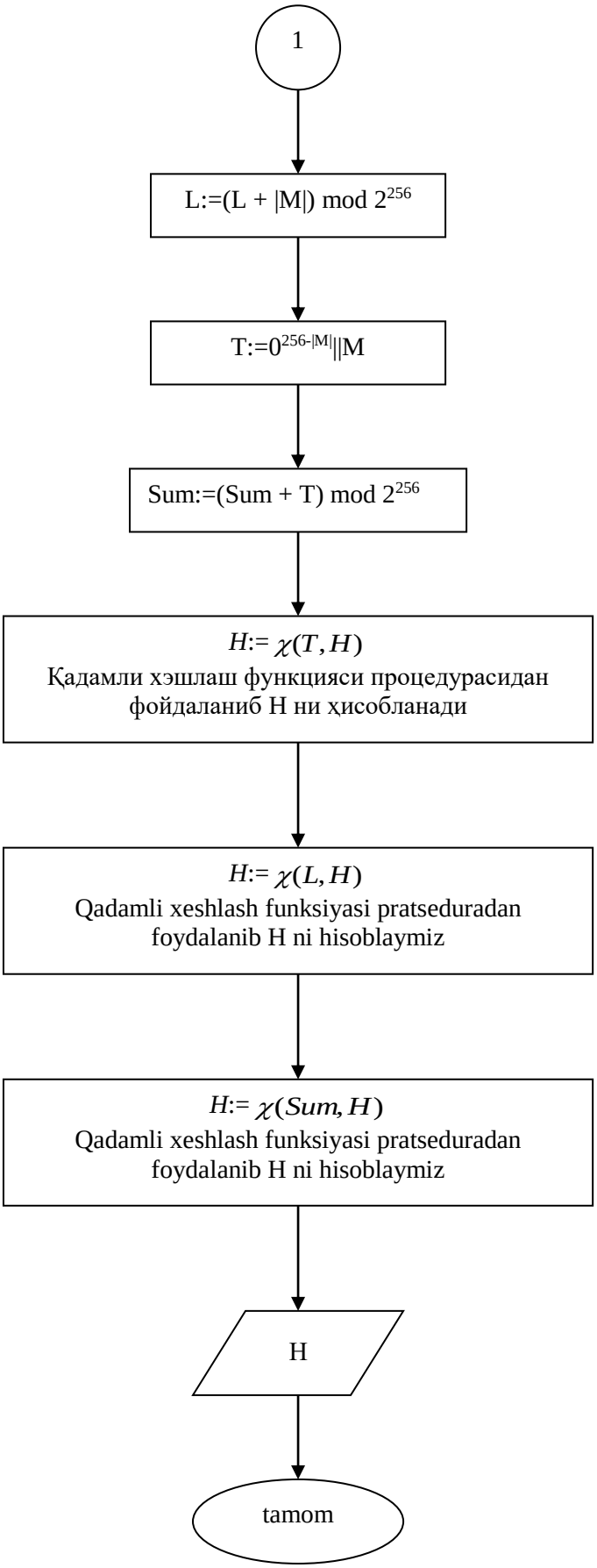
3.5. M= M_P;

3.6. Ikkinchi bosqichga o‘tiladi.

2.7 - qadamda olingan N ning qiymati 3.2- qadamda M ma’lumotning xesh qiymati bo‘ladi.

Quyida GOST 34.11-94 xesh funksiya algoritmining blok-sxemasi keltirilgan:


boshlanish
M, H
M:=M
H:=H
Sum:=0^256
L:=0^256
|M|>256
йўқ
1
ҳа
M=MP||MS
M ma'lumotning M_S ∈ V_256(2) qismini ajratib olinadi
H := χ(M_S, H)
Qadamli xeshlash funksiyasi pratseduradan foydalanib H ni hisoblaymiz
L:=(L+256) mod 2^256
Sum:=(Sum + MS) mod 2^256
M:=MP


1
L:=(L + |M|) mod 2^256
T:=0^256-|M||M
Sum:=(Sum + T) mod 2^256
H:= χ(T, H)
Қадамли хэшлаш функцияси процедурасидан фойдаланиб H ни ҳисобланади
H:= χ(L, H)
Qadamli xeshlash funksiyasi pratseduradan foydalanib H ni hisoblaymiz
H:= χ(Sum, H)
Qadamli xeshlash funksiyasi pratseduradan foydalanib H ni hisoblaymiz
H
tamom

6.6. SHA-1 xesh funksiyasi algoritmi

Kafolatlangan bardoshlilikka ega bo‘lgan xeshlash algoritmi SHA (Secure Hash Algorithm) AQSHning standartlar va texnologiyalar Milliy instituti (NIST) tomonidan ishlab chiqilgan bo‘lib, 1992 yilda axborotni qayta ishlash federal standarti (RUB FIPS 180) ko‘rinishida nashr qilindi [36]. 1995 yilda bu standart qaytadan ko‘rib chiqildi va SHA-1 deb nomlandi (RUB FIPS 180-1). SHA algoritmi MD4 algoritmiga asoslanadi va uning tuzilishi MD4 algoritmining tuzilishiga juda yaqin. Bu algoritm DSS standarti asosidagi elektron raqamli imzo algoritmlarida ishlatish uchun mo‘ljallangan.

Bu algoritmda kiruvchi ma’lumot uzunligi 2^{64} bitdan kichik, xesh qiymat uzunligi 160 bit bo‘ladi. Kiritilayotgan ma’lumot 512 bitlik bloklarga ajratilib qayta ishlanadi.

Xesh qiymatni hisoblash jarayoni quyidagi bosqichlardan iborat:

1-bosqich.To‘ldirish bitlarini qo‘shish.

Berilgan ma’lumot uzunligi 512 modulь bo‘yicha 448 bilan taqqoslanadigan (ma’lumot uzunligi ≡ 448 mod 512) qilib to‘ldiriladi. To‘ldirish hamma vaqt, hattoki ma’lumot uzunligi 512 modulь bo‘yicha 448 bilan taqqoslanadigan bo‘lsa ham bajariladi.

To‘ldirish quyidagi tartibda amalga oshiriladi: ma’lumotga 1 ga teng bo‘lgan bitta bit qo‘shiladi, qolgan bitlar esa nolь bilan to‘ldiriladi. SHuning uchun qo‘shilgan bitlar soni 1 dan 512 tagacha bo‘ladi.

2- bosqich. Ma’lumotning uzunligini qo‘shish.

1-bosqich natijasiga berilgan ma’lumot uzunligining 64 bitlik qiymati qo‘shiladi.

3- bosqich. Xesh qiymat uchun bufer initsializatsiya qilish.

Xesh funksiyaning oraliq va oxirgi natijalarini saqlash uchun 160 bitlik buferdan foydalaniladi. Bu buferni beshta 32 bitlik A, B, C, D, E registrlar ko‘rinishida tasvirlash mumkin. Bu registrlarga 16 lik sanoq tizimida quyidagi boshlang‘ich qiymatlar beriladi:

A=0x67452301,

B=0xEFCDAB89,

C=0x98BADCFE,

D=0x10325476,

E=0xC3D2E1F0.

Keyinchalik bu o‘zgaruvchilar mos ravishda yangi *a, b, c, d* va *e* o‘zgaruvchilarga yozib olinadi.

4- bosqich. Ma’lumotni 512 bitlik bloklarga ajratib qayta ishlash.

Bu xesh funksiyaning asosiyssikli quyidagicha bo‘ladi:

for (t = 0; t< 80; t++){

$temp = (a <<< 5) + f_t(b, c, d) + e + W_t + K_t$;

$e = d$; $d = c$; $c = b <<< 30$; $b = a$; $a = temp$;

},

Bu erda <<<–chapgassiklik surish amali. K_t lar 16 lik sanoq tizimida yozilgan quyidagi sonlardan iborat:

$$\mathbf{K}_t = \begin{cases} \mathbf{5A827999}, & t = 0,...,19, \\ \mathbf{6ED9EBA1}, & t = 20,...,39, \\ \mathbf{8F1BBCDC}, & t = 40,...,59, \\ \mathbf{CA62C1D6}, & t = 60,...,79. \end{cases}$$

$f_t(x, y, z)$ funksiyalar esa quyidagi ifodalar orqali aniqlanadi:

$$f_t(\mathbf{x,y,z}) = \begin{cases} \mathbf{X} \wedge \mathbf{Y} \vee \neg\mathbf{X} \wedge \mathbf{Z}, & \mathbf{t} = 0,...,19, \\ \mathbf{X} \oplus \mathbf{Y} \oplus \mathbf{Z}, & \mathbf{t} = 20,...,39,\ 60,...,79, \\ \mathbf{X} \wedge \mathbf{Y} \vee \mathbf{X} \wedge \mathbf{Z} \vee \mathbf{Y} \wedge \mathbf{Z}, & \mathbf{t} = 40,...,59. \end{cases}$$

$W_t$lar kengaytirilgan ma’lumotning 512 bitlik blokining 32 bitlik qism bloklaridan quyidagi qoida bo‘yicha hosil qilinadi:

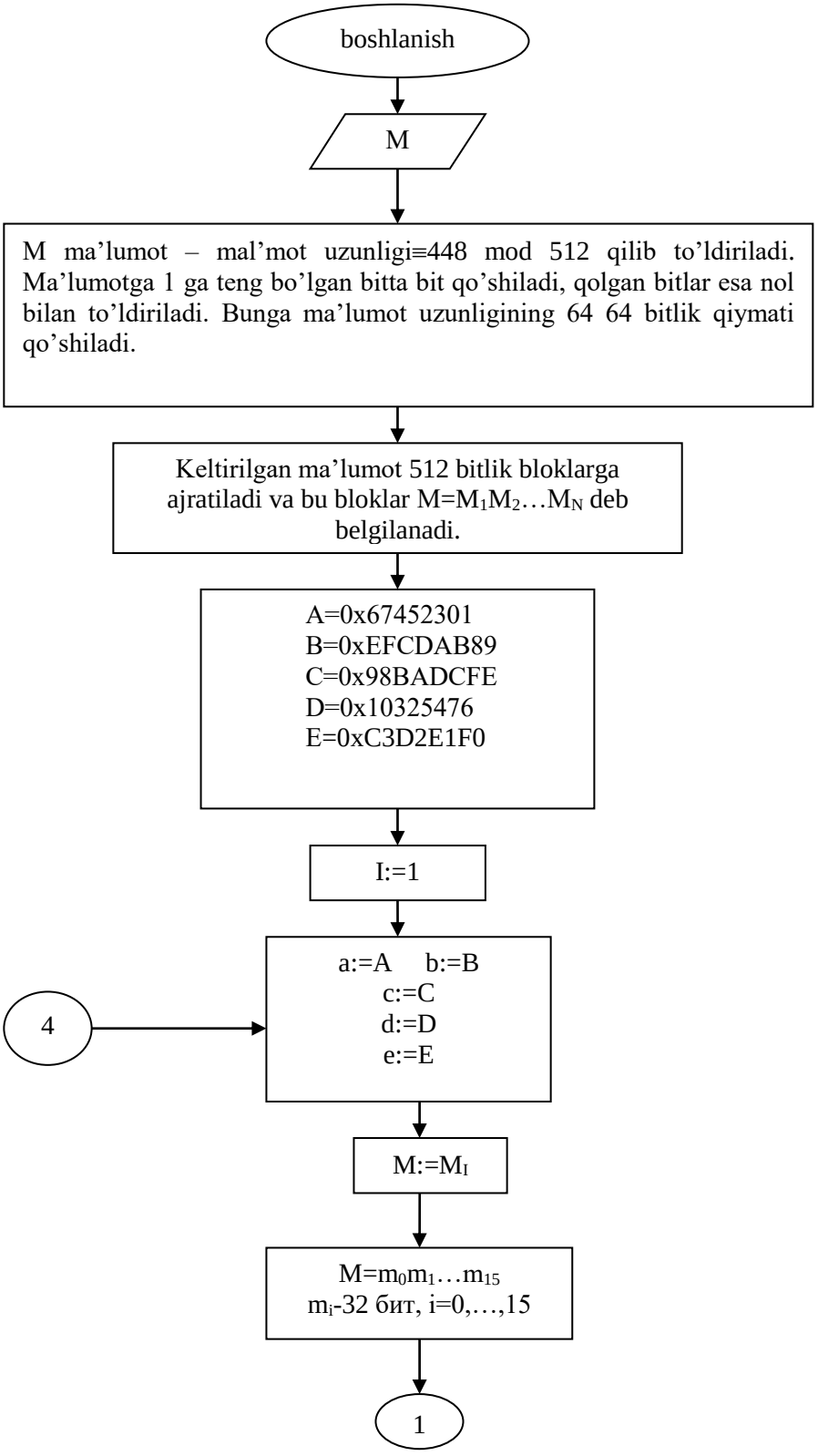
$$W_t = \begin{cases} M_t, & t = 0,...,15, \\ (W_{t-3} \oplus W_{t-8} \oplus W_{t-14} \oplus W_{t-16}) <<< 1, & t = 16,...,79. \end{cases}$$

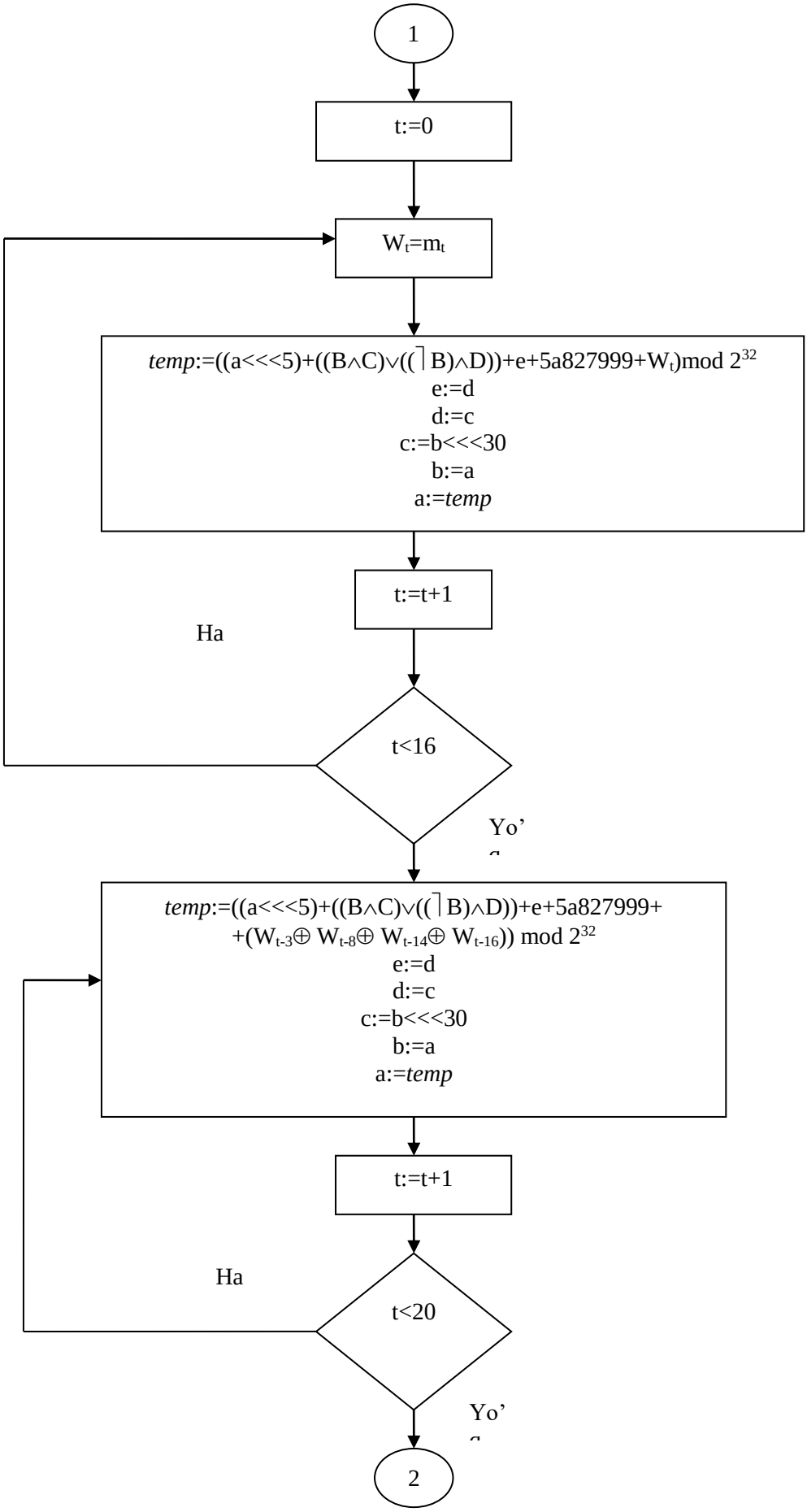
Asosiyssikl tugagandan keyin, *a, b, c, d* va *e* larning qiymatlari mos ravishda A, B, C, D va E registrlardagi qiymatlarga qo‘shiladi hamda shu registrlarga yozib qo‘yiladi va kengaytirilgan ma’lumot keyingi 512 bitlik blokini qayta ishlashga o‘tiladi.

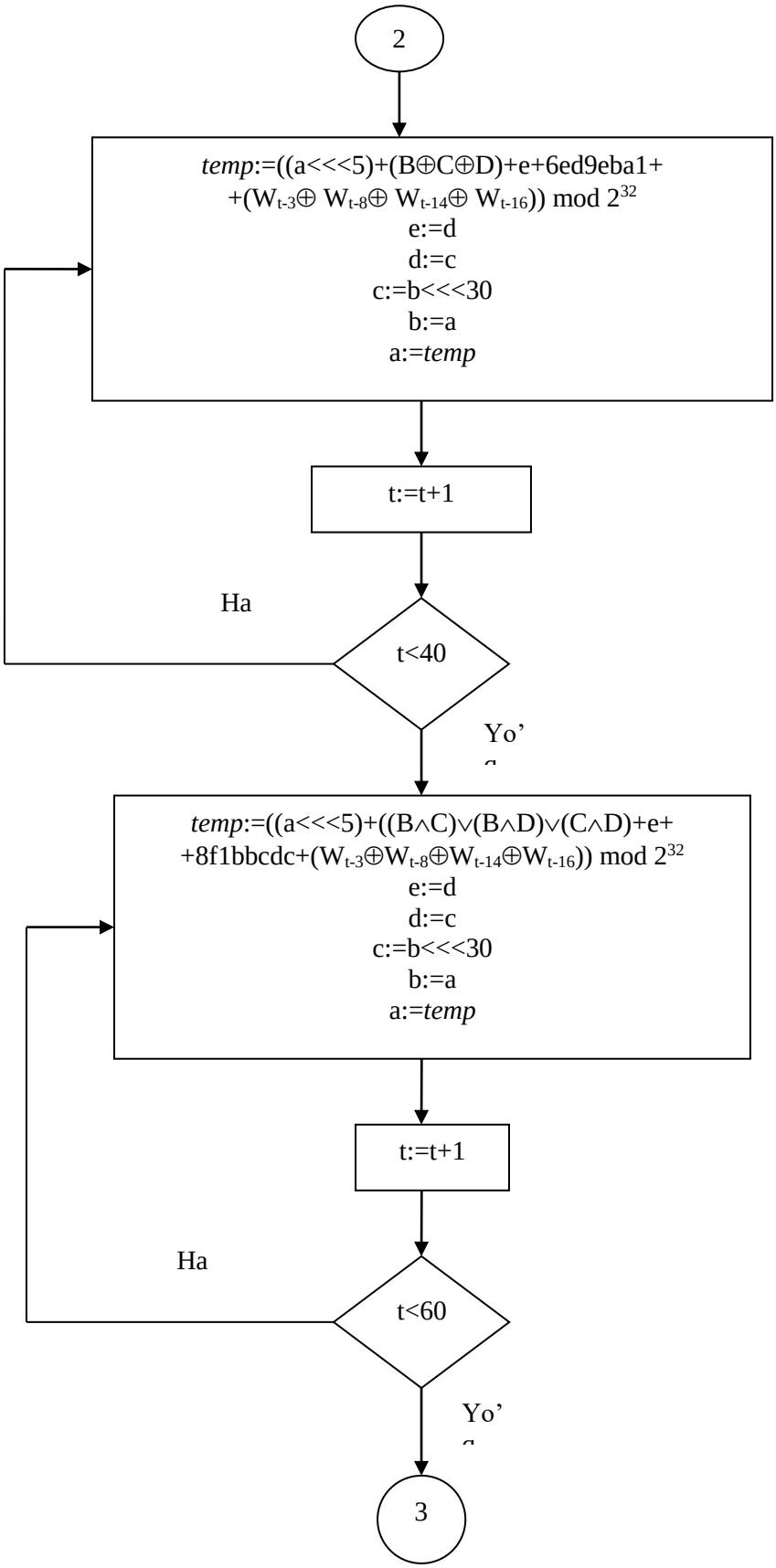
5- bosqich. Natija.

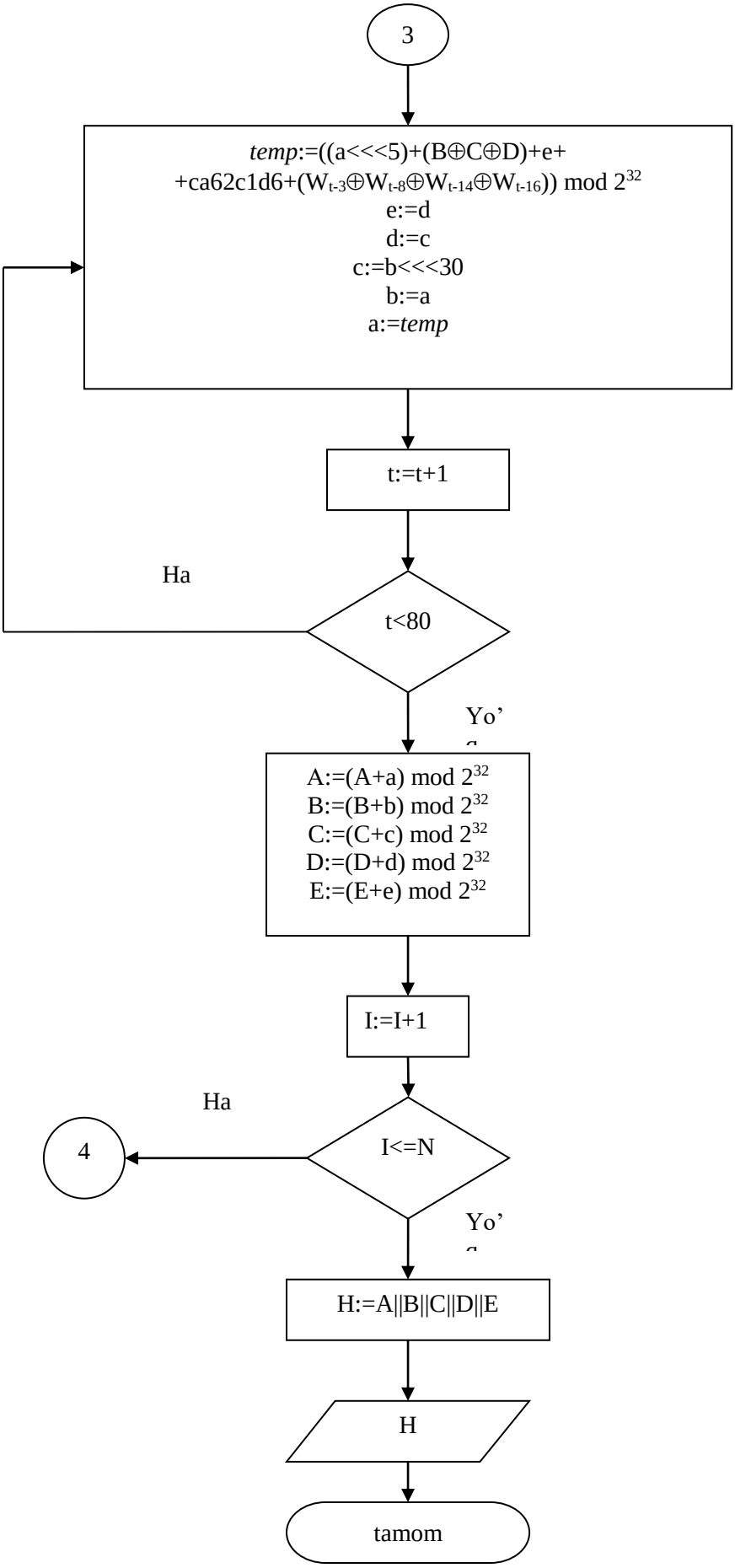
Ma’lumotning xesh qiymati A, B, C, D va E registrlardagi qiymatlarni birlashtirish natijasida hosil qilinadi.

Quyida SHA-1 xesh funksiyaci algoritmining blok sxemasi keltirilgan:




1
t:=0
$W_t=m_t$
temp:=((a<<<5)+((B∧C)∨((¬B)∧D))+e+5a827999+W_t)mod 2^{32}
e:=d
d:=c
c:=b<<<30
b:=a
a:=*temp*
t:=t+1
Ha
t<16
Yo’
temp:=((a<<<5)+((B∧C)∨((¬B)∧D))+e+5a827999+
+(W_{t-3}⊕ W_{t-8}⊕ W_{t-14}⊕ W_{t-16})) mod 2^{32}
e:=d
d:=c
c:=b<<<30
b:=a
a:=*temp*
t:=t+1
Ha
t<20
Yo’
2


2
temp:=((a<<<5)+(B⊕C⊕D)+e+6ed9eba1+
+(Wt-3⊕ Wt-8⊕ Wt-14⊕ Wt-16)) mod 232
e:=d
d:=c
c:=b<<<30
b:=a
a:=temp
t:=t+1
Ha
t<40
Yo’
temp:=((a<<<5)+((B∧C)∨(B∧D)∨(C∧D)+e+
+8f1bbcdc+(Wt-3⊕Wt-8⊕Wt-14⊕Wt-16)) mod 232
e:=d
d:=c
c:=b<<<30
b:=a
a:=temp
t:=t+1
Ha
t<60
Yo’
3


3
temp:=((a<<<5)+(B⊕C⊕D)+e+
+ca62c1d6+(Wt-3⊕Wt-8⊕Wt-14⊕Wt-16)) mod 2^32
e:=d
d:=c
c:=b<<<30
b:=a
a:=temp
t:=t+1
Ha
t<80
Yo'
A:=(A+a) mod 2^32
B:=(B+b) mod 2^32
C:=(C+c) mod 2^32
D:=(D+d) mod 2^32
E:=(E+e) mod 2^32
I:=I+1
Ha
4
I<=N
Yo'
H:=A||B||C||D||E
H
tamom

Xeshlashfunksiyasiningmatnlar to‘qnashuvini topishga nisbatan bardoshliligi $2^{n/2}$ ga teng. AQSHda kalit uzunligi 128, 192 va 256 bit bo‘lgan yangi shifrlash standarti ishlab chiqilganligi munosabati bilan shu darajadagi bardoshlilikka ega bo‘lgan yangi xesh funksiyalar algoritmlarini yaratishga ehtiyoj paydo bo‘ldi. SHu sababli 2002 yilda AQSHning yangi xesh funksiya standarti RUB FIPS 180-2 qabul qilindi. Bu standartda to‘rtta xesh funksiya – SHA-1, SHA-256, SHA-384 va SHA-512 algoritmlari keltirilgan.

Quyida SHA-256 xesh funksiyasi algoritmi ko‘rib o‘tiladi. Bu algoritmda kiruvchi ma’lumot uzunligi 2^{64} bitdan kichik, xesh qiymat uzunligi 256 bit bo‘ladi. Ushbu algoritmni ikki qismga – siqish funksiyasi va ma’lumotni qayta ishlash algoritmiga bo‘lish mumkin. Siqish funksiyasi uzunligi 256 bit bo‘ladigan oraliq xesh qiymatni matnning navbatdagi blokini kalit sifatida olib shifrlash algoritmidan iborat. Siqish funksiyasida oldingi belgilashlardan tashqari quyidagi belgilashlar ham ishlatiladi: R^n – so‘zni n bit o‘ngga surish, S^n – so‘zni n bit o‘nggassiklik surish. So‘zning o‘lchami 32 bitga teng deb, qo‘shish esa mod 2^{32} bo‘yicha olinadi. Boshlang‘ich xeshlash vektori $H^{(0)}$ 8 ta 32 razryadlik so‘zlardan iborat bo‘lib, u quyidagi tub sonlardan olingan kvadrat ildizlarning kasr qismlariga teng qilib olinadi:

$H^{(0)}$={6a09e667, bb67ae85, 3c6ef372, a54ff53a, 510e527f, 9b05688c, 1f83d9ab, 5be0cd19}.

Keyingi hisoblashlar quyidagi sxema bo‘yicha olib boriladi:

1. Boshlang‘ich qayta ishlash. Xeshlanuvchi ma’lumot SHA-1 ga o‘xshab uzunligi 512 ga karrali bo‘lguncha to‘ldiriladi. To‘ldirishda ma’lumotdan keyin 1 yoziladi va qolgan bitlar nolь bilan to‘ldiriladi. Bunda ma’lumot uzunligi 512 modulь bo‘yicha 448 bilan taqqoslanadigan qilib to‘ldiriladi. Keyin berilgan ma’lumotning 64 bitlik uzunligi yoziladi.

2. Ma’lumotni 512 bitlik bloklarga ajratish. Kengaytirilgan ma’lumot 512 bitlik $M^{(1)}, M^{(2)}, ..., M^{(N)}$ bloklarga ajratiladi.

3. Asosiy sikl. Bussiklni yozish uchun argumenti va qiymatlari 32 bit bo‘lgan oltita mantiqiy funksiyadan foydalaniladi:

Ch (x,y,z)=(x∧y)⊕(¬x∧z),

Maj (x,y,z)=(x∧y)⊕(x∧z)⊕(y∧z),

$\Sigma_0(x)=S^2(x)\oplus S^{13}(x)\oplus S^{22}(x)$,

$\Sigma_1(x)=S^6(x)\oplus S^{11}(x)\oplus S^{25}(x)$,

$\sigma_0(x)=S^7(x)\oplus S^{18}(x)\oplus R^3(x)$,

$\sigma_1(x)=S^{17}(x)\oplus S^{19}(x)\oplus R^{10}(x)$.

$M^{(i)}$ blokni $M^{(i)} = M_0^{(i)} M_1^{(i)} ... M_{15}^{(i)}$ 16 ta 32 bitlik so‘zlarga ajratiladi va $W_0,...,W_{63}$ lar quyidagicha aniqlanadi:

$W_j = M_j^{(i)}, \quad j = 0,...,15,$

for j=16 to 63 {

$W_j = \sigma_1(W_{j-2}) + W_{j-7} + \sigma_0(W_{j-15}) + W_{j-16}$

}

$K_0,...,K_{63}$ o‘zgarmaslar sifatida esa quyidagi 64 ta 16 lik ko‘rinishda tasvirlangan tub sonlardan chiqarilgan kub ildizlar kasr qismlarining birinchi 32 biti olinadi:

428a2f98 71374491 b5c0fbcf e9b5dba5 3956c25b 59f111f1 923f82a4 ab1c5ed5
d807aa98 12835b01 243185be 550c7dc3 72be5d74 80deb1fe 9bdc06a7 c19bf174
e49b69c1 efbe4786 0fc19dc6 240ca1cc2de92c6f 4a7484aa 5cb0a9dc 76f988da
983e5152 a831c66d b00327c8 bf597fc7 c6e00bf3 d5a79147 06ca6351 14292967
27b70a85 2e1b2138 4d2c6dfc 53380d13 650a7354766a0abb 81c2c92e 92722c85
a2bfe8a1 a81a664b c24b8b70 c76c51a3 d192e819 d6990624 f40e3585 106aa070
19a4c116 1e376c08 2748774c 34b0bcb5 391c0cb3 4ed8aa4a 5b9cca4f 682e6ff3
748f82ee 78a5636f 84c87814 8cc70208 90befffa a4506ceb bef9a3f7 c67178f2

Asosiy sikl quyidagicha bo‘ladi:

for i=0 to N { // N – kengaytirilgan ma’lumotning bloklari soni.

// a, b, c, d, e, f, g, h registrlarni xesh funksiyaning (i-1) oraliq qiymati bilan // initsializatsiya qilish.

$a = H_1^{(i-1)};\ b = H_2^{(i-1)};\ c = H_3^{(i-1)};\ d = H_4^{(i-1)};\ e = H_5^{(i-1)};\ f = H_6^{(i-1)};\ g = H_7^{(i-1)};\ h = H_8^{(i-1)};$

// a, b, c, d, e, f, g, h registrlarga siqish funksiyasini qo‘llaymiz.

for i=0 to 63 {// *Ch* (e,f,g), *Maj* (a,b,c), Σ_0(a), Σ_1(e) va W_j larni hisoblaymiz.

$$T_1 = h + \Sigma_1(e) + Ch(e, f, g) + K_j + W_j$$

$$T_2 = \Sigma_0(a) + Maj(a, b, c)$$

$$h = g;\ g = f;\ f = e;\ e = d + T_1;\ d = c;\ c = b;\ b = a;\ a = T_1 + T_2$$

}

// i – oraliq xesh qiymat $H^{(i)}$ ni hisoblash.

$$H_1^{(i)} = a + H_1^{(i-1)};\ H_2^{(i)} = b + H_2^{(i-1)};\ H_3^{(i)} = c + H_3^{(i-1)};\ H_4^{(i)} = d + H_4^{(i-1)};$$

$$H_5^{(i)} = e + H_5^{(i-1)};\ H_6^{(i)} = f + H_6^{(i-1)};\ H_7^{(i)} = g + H_7^{(i-1)};\ H_8^{(i)} = h + H_7^{(i-1)}$$

}

// i – bo‘yichassikl.

Natijada $H^{(N)} = H_1^{(N)} \| H_2^{(N)} \| H_3^{(N)} \| H_4^{(N)} \| H_5^{(N)} \| H_6^{(N)} \| H_7^{(N)} \| H_8^{(N)}$ ifoda M ma’lumotning xesh qiymatini beradi.

SHA-512 xesh funksiyasi o‘zining tuzilishiga ko‘ra, SHA-256 xesh funksiyasiga o‘xshaydi, lekin unda uzunligi 64 bit bo‘lgan so‘zlar ustida amallar bajariladi. Bu algoritmda kiruvchi ma’lumotning uzunligi 2^{128} bitdan kichik, xesh qiymat uzunligi 512 bit bo‘ladi. Ma’lumotning uzunligi 1024 ga karrali qilib to‘ldiriladi. To‘ldirishda ma’lumot oxiriga 1 yozilib, qolgan qismi nolь bilan shunday to‘ldiriladiki, ma’lumot uzunligi 1024 ga karrali condan 128 bit kam bo‘lishi kerak. Oxiriga berilgan ma’lumotning 128 bit uzunligi qo‘shiladi. SHunday qilib, kengaytirilgan ma’lumot uzunligi 1024 ga karrali bo‘ladi. Boshlang‘ich vektor $H^{(0)}$ 8 ta 64 razryadli so‘zlardan iborat bo‘lib, u quyidagi tub sonlar kvadrat ildizlarining kasr qismlariga teng qilib olinadi:

$H^{(0)}$={6a09e667f3bcc908, bb67ae8584caa73b, 3c6ef372fe94f82b, a54ff53a5f1d36f1, 510e527fade682d1, 9b05688c2b3e6c1f, 1f83d9abfb41bd6b, 5be0cd19137e2179}.

Ma’lumot 1024 bitlik $M^{(1)}, M^{(2)}, ..., M^{(N)}$ bloklarga ajratiladi va ular ketma-ket qayta ishlanadi.

Asosiy sikl xuddi SHA-256 algoritmidagidek bo‘lib, faqat SHA-512 algoritmidagi funksiyalar va bajariladigan amallar 64 bitlik so‘zlarda aniqlangan

hamda qo‘shish mod 2^{64} bo‘yicha olinadi. Siqish funksiyasi esa faqatssikldagi iteratsiyalar soni bilan farq qiladi:

for i=0 to 79 { // *Ch* (e,f,g), *Maj* (a,b,c), Σ_0(a), Σ_1(e) va W_j larni hisoblanadi.

$$T_1 = h + \Sigma_1(e) + Ch(e, f, g) + K_j + W_j$$

$$T_2 = \Sigma_0(a) + Maj(a, b, c)$$

$$h = g;\ g = f;\ f = e;\ e = d + T_1;\ d = c;\ c = b;\ b = a;\ a = T_1 + T_2$$

}

Natijada $H^{(N)} = H_1^{(N)} \| H_2^{(N)} \| H_3^{(N)} \| H_4^{(N)} \| H_5^{(N)} \| H_6^{(N)} \| H_7^{(N)} \| H_8^{(N)}$ ifoda M ma’lumotning xesh qiymatini beradi.

Mantiqiy funksiyalar esa SHA-256 algoritmidagi mantiqiy funksiyalardan quyidagicha farq qiladi:

$\Sigma_0(x)=S^{28}(x)\oplus S^{34}(x)\oplus S^{39}(x)$,

$\Sigma_1(x)=S^{14}(x)\oplus S^{18}(x)\oplus S^{41}(x)$,

$\sigma_0(x)=S^{1}(x)\oplus S^{8}(x)\oplus R^{7}(x)$,

$\sigma_1(x)=S^{19}(x)\oplus S^{61}(x)\oplus R^{6}(x)$.

$M^{(i)}$ blokni $M^{(i)} = M_0^{(i)} M_1^{(i)} ... M_{15}^{(i)}$ 16 ta 64 bitlik bloklarga ajratiladi va $W_0,...,W_{79}$ larni quyidagicha aniqlanadi:

$$W_j = M_j^{(i)}, \quad j = 0,...,15,$$

for j=16 to 79 {

$$W_j = \sigma_1(W_{j-2}) + W_{j-7} + \sigma_0(W_{j-15}) + W_{j-16}$$

}

$K_0,...,K_{79}$ o‘zgarmaslar sifatida esa quyidagi 80 ta 16 lik ko‘rinishda tasvirlangan tub sonlardan chiqarilgan kub ildizlar kasr qismlarining birinchi 64 biti olinadi:

428a2f98d728ae22 7137449123ef65cd b5c0fbcfec4d3b2f e9b5dba58189dbbc
3956c25bf348b538 59f111f1b605d019 923f82a4af194f9b ab1c5ed5da6d8118
d807aa98a3030242 12835b0145706fbe 243185be4ee4b28c 550c7dc3d5ffb4e2

72be5d74f27b896f 80deb1fe3b1696b1 9bdc06a725c71235 c19bf174cf692694
e49b69c19ef14ad2 efbe4786384f25e3 0fc19dc68b8cd5b5 240ca1cc77ac9c65
2de92c6f592b0275 4a7484aa6ea6e483 5cb0a9dcbd41fbd4 76f988da831153b5
983e5152ee66dfab a831c66d2db43210 b00327c898fb213f bf597fc7beef0ee4
c6e00bf33da88fc2 d5a79147930aa725 06ca6351e003826f 142929670a0e6e70
27b70a8546d22ffc 2e1b21385c26c926 4d2c6dfc5ac42aed 53380d139d95b3df
650a73548baf63de 766a0abb3c77b2a8 81c2c92e47edaee6 92722c851482353b
a2bfe8a14cf10364 a81a664bbc423001 c24b8b70d0f89791 c76c51a30654be30
d192e819d6ef5218 d69906245565a910 f40e35855771202a 106aa07032bbd1b8
19a4c116b8d2d0c8 1e376c085141ab53 2748774cdf8eeb99 34b0bcb5e19b48a8
391c0cb3c5c95a63 4ed8aa4ae3418acb 5b9cca4f7763e373 682e6ff3d6b2b8a3
748f82ee5defb2fc 78a5636f43172f60 84c87814a1f0ab72 8cc702081a6439ec
90befffa23631e28 a4506cebde82bde9 bef9a3f7b2c67915 c67178f2e372532b
ca273eceea26619c d186b8c721c0c207 eada7dd6cde0eb1e f57d4f7fee6ed178
06f067aa72176fba 0a637dc5a2c898a6 113f9804bef90dae 1b710b35131c471b
28db77f523047d84 32caab7b40c72493 3c9ebe0a15c9bebc 431d67c49c100d4c
4cc5d4becb3e42b6 597f299cfc657e2a 5fcb6fab3ad6faec 6c44198c4a475817.

SHA-384 xesh funksiyasi algoritmi SHA-512 algoritmidan faqat boshlang‘ich vektori:

$H^{(0)}$ = {cbbb9d5dc1059ed8, 629a292a367cd507, 9159015a3070dd17, 152fecd8f70e5939, 67332667ffc00b31, 8eb44a8768581511, db0c2e0d64f98fa7, 47b5481dbefa4fa4} bilan farq qiladi. Bu algoritmda kiruvchi ma’lumotning uzunligi 2^{128} bitdan kichik bo‘lib, xesh qiymat uzunligi 384 bit bo‘ladi. Boshqa hamma hisoblashlar SHA-512 algoritmi bilan bir xil bo‘ladi. Natijada, chiquvchi xesh qiymat sifatida:

$H^{(N)} = H_1^{(N)} \| H_2^{(N)} \| H_3^{(N)} \| H_4^{(N)} \| H_5^{(N)} \| H_6^{(N)} \| H_7^{(N)} \| H_8^{(N)}$ ning chap tomondan 384 biti, ya’ni $H^{(N)} = H_1^{(N)} \| H_2^{(N)} \| H_3^{(N)} \| H_4^{(N)} \| H_5^{(N)} \| H_6^{(N)}$ olinadi.

6.7. O‘z DSt 1106 : 2006 shifrlash standarti

O‘zbekiston Respublikasining O‘z DSt 1106 : 2006 xesh funksiyasi 2006 yilda bir yil sinov muddati bilan qabul qilingan kalitli xesh-funksiya bo‘lib, unda kalit uzunligi 128 bit yoki 256 bit bo‘lishi nazarda tutilgan. Chiquvchi xesh qiymat uzunligi ham mos ravishda 128 bit yoki 256 bit bo‘ladi.

Ushbu standart ixtiyoriy uzunlikdagi matn uchun xesh-funksiyani hisoblash algoritmi va ketma-ketligini aniqlab, axborotlarni kriptografik usullar asosida qayta ishlash va himoyalashda, shu bilan birga axborot-kommunikatsiya tizimlarida ma’lumotlarni uzatish, qayta ishlash va saqlashda, ERI jarayonini ta’minlashda qo‘llashga mo‘ljallangan.

O‘z DSt 1106 : 2006 xesh-funksiya standarti parametrlar algebrasi asosida qurilgan bo‘lib, parametrlar algebrasining ko‘paytirish, darajaga ko‘tarish, teskarilash amallaridan foydalaniladi:

1) a va b sonlarni *R*-koeffitsient asosida moduly *p*-bo‘yicha ko‘paytirish formulasi:

$$a \otimes b = a + (1 + R * a)(\mathrm{mod}\ p).$$

2) a sonini R- koeffitsent bo‘yicha biror x darajaga ko‘tarish formulasi(R va n lar o‘zaro tub):

$$a^{\backslash x} = ((1 + R * a)^{\backslash x} - 1) * R^{-1} (\mathrm{mod}\ n).$$

3) a sonini *R* - koeffitsent asosida modulьn -bo‘yicha teskarisini topish formulasi:

$$a^{\backslash -1} = a * (1 + R * a)^{-1} (\mathrm{mod}\ n)$$

Shuningdek, mazkur standartdassiklik siljitishlardan ham keng foydalanilgan.

Xesh-funksiya algoritmida 128 bit uzunlikdagi bloklar ustida amal bajarilganda bazaviy birlik sifatida yarim bayt (“polubayt”) – 4 bitlik ketma-ketlikdan foydalanilgan, 256 bit uzunlikdagi bloklar ustida amal bajarilganda baytlar ustida amallar bajariladi.

Algoritmda 128 bitlik bloklar uchun bosqichlar soni b+10, 256 bitlik bloklar uchun esa bosqichlar soni b+6 qilib belgilangan, bu erda, b – bloklar soni.

Xesh-funksiya algoritmi ketma-ket bajariluvchi 3 ta qismdan iborat bo‘lib, birinchi qismda, faqat kiruvchi bloklar ustida amallar bajariladi, ikkinchi qismda

birinchi qismning oxirgi blok natijasi ustida 10(6) bosqich davomida akslantirishlar amalga oshiriladi, uchinchi qism esa, ikkita akslantirishdan iborat.

Algoritm ikkita rejimda ishlashga mo‘ljallangan bo‘lib, 0-rejimda birinchi qismning har bir bosqichi Aralash( ), Daraja(holat,R), SurKalit( ), SurHolat( ), Teskari(k_e,R), Qo’shBosqichKalit( ), TuzilmaKalit(k_e,R) akslantirishlar ketma-ketligidan, 1-rejimda esa, birinchi qismning har bir bosqichi Aralash( ), Daraja(holat,R), Daraja(k_e,R), SurKalit( ), SurHolat( ), Teskari(holat,R), Teskari(k_e,R), Qo’shBosqichKalit( ), TuzilmaKalit(k_e,R) akslantirishlar ketma-ketligidan iborat.

6.8. Ryukzak algoritmi

Bizga ma’lumki ma’lumotlarni yoki axborotlarni sir saqlash yoki ikkinchi tomonga maxfiy axborotlarni yetkazish vazifasi yuklatiladigan bo‘lsa, hech qanday muammolarga uchramasdan bu masalani hal etishimiz.
mumkin. Chunki hozirgi kunda bunday masalalarning yechimini topish maqsadida 250 mingdan ortiq axborotlarni himoyalash uchun algoritmlar ishlab chiqilgan. Bu algoritmlarning har birining o‘z muallifi mavjud.

Ochiq kalitli shifrlash tizimlarida ikkita kalit ishlatiladi. Axborot ochiq kalit yordamida shifrlansa, maxfiy kalit yordamida deshifrlanadi.

Ochiq kalitli tizimlarini qo‘llash asosida qaytarilmas yoki bir tomonli funksiyalardan foydalanish yotadi. Bunday funksiyalar quyidagi xususiyatlarga ega. x ma’lum bo‘lsa, y=f(x) funksiyani aniqlash oson. Ammo uning ma’lum qiymati bo‘yicha x ni aniqlash amaliy jihatdan mumkin emas. Kriptografiyada yashirin deb ataluvchi yo‘lga ega bo‘lgan bir tomonli funksiyalar ishlatiladi. *z* parametrli bunday funksiyalar quyidagi xususiyatlarga ega. Ma’lum *z* uchun E_z va D_z algoritmlarini aniqlash mumkin. E_z algoritmi yordamida aniqlik sohasidagi barcha x uchun f_z (x) funksiyani osongina olish mumkin. Xuddi shu tariqa D_z algoritmi yordamida joiz qiymatlar sohasidagi barcha *y*lar uchun teskari funksiya $x=f^1(y)$ ham osongina aniqlanadi. Ayni vaqtda joiz qiymatlar sohasidagi barcha *z* va deyarli barcha, *y*uchun hatto E_z ma’lum bo‘lganida ham $f^{-1}(y)$ni hisoblashlar

yordamida topib bo‘lmaydi. Ochiq kalit sifatida *y*ishlatilsa, maxfiy kalit sifatida x ishlatiladi.

Ochiq kalitni ishlatib shifrlash amalga oshirilganda o‘zaro muloqotda bo‘lgan subyektlar o‘rtasida maxfiy kalitni almashish zaruriyati yo‘qoladi. Bu esa o‘z navbatida uzatiluvchi axborotning kriptohimoyasini soddalashtiradi.

Ryukzak masalasini ilk bor Ralf Merkel va Martin Xelman tomonlaridan bir biriga bog‘liqsiz ravishda 1978 yili yaratilgan. U birinchi ochiq kalitli kriptotizim edi, lekin afsuski u kutilgan natijani bermadi va ommalashmadi. Bu algoritmning 1997 yilda patent muddati tugagan.

Ryukzak masalasi: bu algoritmda S hajmli ryugzak bor. Bizga

$$\boldsymbol{w} = (\boldsymbol{w_1}, \boldsymbol{w_2}, \dots, \boldsymbol{w_n})$$

$$w=(w_u\ W2,\dots\ W_n)$$

n ta tosh berilgan. Bu toshlarni S ryukzakka solamiz.

Bizga

$$x = (x_1, x_2, \dots, x_n)$$

binar vektor ham beriladi, bu vektor elementlari 0 yoki 1 qiymatni qabul qiladi

$$x_1 \in [0,1]$$

Shunda ryukzak quyidagi ko‘rinishga keladi

$$S = \sum_{i=1}^{n} x_i w_i$$

Ta’rif: Berilgan ketma-ketlikni har bir hadi o‘zidan oldingi hadlar yig‘indisidan katta bo‘lsa, bu ketma-ketlikka *O’suvchi ketma-ketlik* deyiladi

$$w_{k+1} > \sum_{i=1}^{n} w_i$$

q modul son tanlanadi. Modul son sifatida o‘suvchi ketma-ketlik hadlari yig‘indisidan katta bo‘lgan ixtiyoriy natural son tanlanadi:

$$q > \sum_{i=1}^{n} w_i$$

q modul bilan o‘zaro tub bo‘lgan ixtiyoriy *r* natural sonni o‘suvchi ketma-

ketlikning har bir hadiga ko‘paytirib, *q* bo‘yicha modul olinib, hosil qilingan b_t ketma-ketlik *normal ketma-ketlik* deyiladi. *bi = (*w_i * r) mod *q* - normal ketma-ketlik. Bu yerda normal ketma-ketlik *(*b_j*,* b_2 *,...*b_n*)* ochiq kalit hisoblanadi. O‘suvchi ketma-ketlik *(wj,* w_2 *,...Wn)* va modul *q* va *r* sonlari yopiq kalit hisoblanadi. Xavfsizlik nuqtai nazaridan ketma-ketlik hadlari uzunligi uchun 200 bitdan 400 bitgacha bo‘lgan sonlar olinishi tavsiya etiladi.

Shifrlash.

Berilgan xabar *M* harfi bilan belgilanadi. Shifrtekst esa, *C* bilan belgilanadi. Xabar bit ko‘rinishida yozib olinadi (*m_j, m_2, ..., m_n):*

$$(\sum_{i=1}^{n} b_i m_i) \bmod q = c_1$$

formula yordamida shifrlanadi. Shifrtekst *C* = {c_1, c_2, ...} ko‘rinishida hosil bo‘ladi.

Shifrni ochish.

C = {c_j, c_2, ...} ko‘rinishidagi shifrtekstni

$(r^{-1} c_i) \bmod q = m_i$

formula yordamida ochiladi. Ochilgan m_t larni yig‘ib chiqib, *M* hosil qilinadi.

R.Merkl tizimni buzib ocha olgan odamga 100 AQSh dollari mukofoti berishini e’lon qildi. 1982 yilda Adi Shamir bu mukofotga sazovor bo‘ldi. U mahfiy kalitga teng bo‘lmagan kalit yasab shifrarni ocha oldi.

Misol.

O‘suvchi ketma-ketlik w = {2, 3, 7, 15}, modul son q=28, q modul bilan o‘zaro tub bo‘lgan r=11, shifrlanadigan matn M=HA so‘zi bo‘lsin.

Shifrlash:

1. HA so‘zini ASCII jadvali yordamida bit ko‘rinishga o‘tkazamiz:
   0100100001000001.
2. b_i*= (*w_i * r)* mod *q* formula orqali normal ketma-ketlik hosil qilamiz:

$b_1 = (w_1 \cdot r) \bmod q = (2 \cdot 11) \bmod 28 = 22$

$b_2 = (w_2 \cdot r) \bmod q = (3 \cdot 11) \bmod 28 = 5$

b=(w_3·r) mod q=(7·11) mod28=21

b_4=(w_4·r) mod q= (15·11) mod 28=25

3. Ketma-ketlik hadlari 4 ta bo‘lgani uchun matnni 4 bitdan bloklarga ajratamiz:

$M_1 = \{m_1, m_2, m_3, m_4\} = 0100$; $M_1 = \{m_1, m_2, m_3, m_4\} = 1000$

$M_1 = \{m_1, m_2, m_3, m_4\} = 0100$; $M_1 = \{m_1, m_2, m_3, m_4\} = 0001$

$(\sum_{i=1}^{n} b_i m_i)\ \mathrm{mod} q = c_1$formula yordamida shifrlaymiz:

$$c_1 = (\sum_{i=1}^{4} b_i m_i)\ \mathrm{mod}\ q = (22 \cdot 0 + 5 \cdot 1 + 21 \cdot 0 + 25 \cdot 0) \mathrm{mod}\ 8 = 5$$

$$c_2 = (\sum_{i=1}^{4} b_i m_i)\ \mathrm{mod}\ q = (22 \cdot 1 + 5 \cdot 0 + 21 \cdot 0 + 25 \cdot 0) \mathrm{mod}\ 8 = 5$$

$$c_3 = (\sum_{i=1}^{4} b_i m_i)\ \mathrm{mod}\ q = (22 \cdot 0 + 5 \cdot 1 + 21 \cdot 0 + 25 \cdot 0) \mathrm{mod}\ 8 = 5$$

$$c_4 = (\sum_{i=1}^{4} b_i m_i)\ \mathrm{mod}\ q = (22 \cdot 0 + 5 \cdot 0 + 21 \cdot 0 + 25 \cdot 1) \mathrm{mod}\ 8 = 5$$

5. Shifrtekst hosil bo‘ladi: $C = \{c_1, c_2, c_3, c_4\} = \{5,22,5,25\}$.

Shifrni ochish:

O‘suvchi ketma-ketlik w = {2, 3, 7, 15}, modul son q=28, q modul bilan o‘zaro tub bo‘lgan r=11, C={5, 22, 5, 25} bizga ma’lum.

1. r sonining q modul bo‘yicha teskarisini topamiz: $11^{-1} \mathrm{mod} 28 = 11^{11} \mathrm{mod} 28 = (11(11^2 \bmod 28)^5) \bmod 28 = (11 * 9^5) \bmod 28 = (11 * 9(9^2 \bmod 28)^2) \bmod 28 = (11 * 9 * 25^2) \bmod 28 = 23$

2. $(r^{-1}C) \mathrm{mod}\ q =$ formuladan matnni topamiz:

M = (23 • 5) mod 28 = 3=2 • 0 +3-1 + 7 • 0 + 15 • 0, bundan M_1 =0100 ekanligini aniqlaymiz.

3. M = (23 • 22) mod 28 = 2=2 -1 +3 • 0 + 7 • 0 + 15 • 0, bundan M_2=1000 ekanligini aniqlaymiz.

4. M = (23 • 5) mod 28 = 3=2 • 0 +3 4 + 7 • 0 + 15 • 0, bundan M_3 = 0100 ekanligini aniqlaymiz.

5. M4=(23 • 25) mod 28 = 15 = 2-0+3-0+7-0+15-1, bundan M_4=0001 ekanligini aniqlaymiz.

6. Barcha Mi larni ketma-ket yozib harflarga o‘tiladi: M=0100100001000001

100 0_2 = 48 $_{16}$ = H 0100 0001 2 = 41 16 = A M = “HA”

6.9. RSA algoritmi

Ochiq kalitli kriptotizimlarni bir tomonli funksiyalar ko‘rinishi bo‘yicha farqlash mumkin. Bularning ichida RSA, El-Gamal va Mak-Elis tizimlarini alohida tilga olish o‘rinli. Hozirda eng samarali va keng tarqalgan ochiq kalitli shifrlash algoritmi sifatida RSA algoritmini ko‘rsatish mumkin.

1976 yilda Uitfild Diffi va Martin Xellmanlar tomonidan chop etilgan “Kriptografiyada yangi yo‘nalish” deb nomlangan maqola kriptografik tizimlar haqidagi tasavvurlarni o‘zgartirib yubordi, ochiq kalitli kriptografiya paydo bo‘lishiga zamin yaratdi. Bu maqolani o‘rganib chiqqan Massachusets texnologiyalar instituti olimlari Ronald Rivest, Adi Shamir va Leonard Adleman 1977 yilda RSA algoritmini yaratdilar.

RSA nomi algoritmni yaratuvchilari familiyalarining birinchi harflaridan olingan. Algoritm modul arifmetikasining darajaga ko‘tarish amalidan foydalanishga asoslangan. 1977 yil avgust oyida ScientificAmerican jurnalida RSA kriptotizimini yoritib berishdi va shu algoritm bilan shifrlangan quyidagi iborani ochishni o‘quvchilarga taklif etishdi:

C=

9686	9613	7546	2206
1477	1409	2225	4355
SS29	0575	9991	1245
7431	9874	6951	2093
0816	2982	2514	5708
3569	3147	6622	8839
8962	8013	3919	9055
1829	9451	5781	5154

n=114381625757888867669235779976146612010218296721242362562561842935706935245733897830597123563958705058989075147599290026879543541, e=9007, M=?

Mukofot sifatida 100 AQSh dollari e'lon qilindi. Algoritm avtorlaridan biri Rivest bu shifrni ochishga 40 kvadrillion yil ketishini aytgan bo'lsa, 1993 yil 3 sentabrdan 1994 yil mart oyigacha 20 ta mamlakatdan 600 ta ko'ngilli shaxslar 1600 ta kompyuterda parallel ishlab bu shifrni ochishdi - THE MAGIC WORDS ARE SQUEAMISHOSSIFRAGE.

1982 yilda Ronald Rivest, Adi Shamir va Leonard Adleman RSA Data Security kompaniyasini tashkil etishdi. 1989 yildan boshlab RSA algoritmi Internetda foydalanila boshlandi. 1990 yildan boshlab AQSh mudofaa vazirligi foydalana boshladi.1993 yilda PKCS1 standartining 1.5 versiyasida RSA algoritmini shifrlash va elektron imzo yaratishda qo'llash keltirildi. Bu standartning oxirgi versiyalari RFC standartida keltirilgan (RFC 2313 — 1.5, 1993 yil; RFC 2437 — 2.0, 1998 yil; RFC3447— 2.1, 2002 yil).

Algoritmni quyidagi qadamlar ketma-ketligi ko'rinishida ifodalash mumkin:

1. Ikkita katta tub son p va q tanlanadi.
2. Kalitning ochiq tashkil etuvchisi n hosil qilinadi: $n=p\cdot q$
3. Quyidagi formula bo'yicha k (Eyler funksiyasi qiymati) hisoblanadi: $k=(p-1)(q-1)$.
4. k qiymati bilan o'zaro tub bo'lgan katta tub son e tanlab olinadi.
5. Quyidagi shartni qanoatlantiruvchi d soni aniqlanadi:

$d = e^{-1} \bmod k$.

Bu shartga binoan $e \cdot d$ ko'paytmaning k qiymatga bo'lishdan qolgan qoldiq 1 ga teng. e soni ochiq kalitning ikkinchi tashkil etuvchisi sifatida qabul qilinadi. Yopiq kalit sifatida d soni ishlatiladi.

6. Dastlabki axborot uning fizik tabiatidan qat'iy nazar raqamli ikkili ko'rinishda ifodalanadi. Bitlar ketma-ketligi L bit uzunlikdagi bloklarga ajratiladi, bu yerda blok sifatida $L < \log_2(n+1)$ shartini qanoatlantiruvchi eng katta butun sonni olish tavsiya etiladi. Har bir blok [0, n-1] oraliqqa taalluqli butun musbat son

kabi ko‘riladi. Shunday qilib, dastlabki axborot M_i, i=17 sonlarning ketma-ketligi orqali ifodalanadi. I ning qiymati shifrlanuvchi ketma-ketlikning uzunligi orqali aniqlanadi.

7. Shifrlangan axborot quyidagi formula bo‘yicha aniqlanuvchi Q sonlarning ketma-ketligi ko‘rinishida olinadi:

$C = M_i^e \bmod n$.

Axborotni ochishda quyidagi munosabatdan foydalaniladi:

$M = C \bmod n$.

Bugungi kunda RSA tizimi programma ta’minoti xavfsizligini ta’minlashda va elektron raqamli imzo sxemalarida foydalaniladi. Shifrlash tezligining pastligi sababli (2 GHz protsessorlarda 512 bitli kalit yordamida 30 kb/s tezlikda shifrlaydi) simmetrik algoritmlarning kalitlarini shifrlab uzatishda ko‘proq foydalaniladi.

Misol.

Modul son n = p - q = 1517, (p -1)-(q -1) ko‘paytma bilan o‘zaro tub bo‘lgan e=11 ochiq kalit, shifrlanadigan matn M=BESH so‘zi va matn uzunligi L=8 bit berilgan. Agar L berilmagan bo‘lsa, $L=[\log_2(n+1)]$ formula orqali topiladi.

Shifrlash:

1. BESH so‘zini ASCII jadvali yordamida bit ko‘rinishga o‘tkazamiz: 01000010010001010101001101001000.
2. Bitlardan iborat matnni 8 bitdan bloklarga ajratamiz va har bir blokni o‘nlik sanoq sistemasiga o‘tkazamiz: $M_1=66$, $M_2=69$, $M_3=83$, $M_4=72$.
3. $C = M^e_i \bmod n$ formula yordamida shifrlanadi:

$C_1 = M^e_1 \bmod n = 66^{11} \bmod 1517 = (66\cdot(66^5 \bmod 1517)^2) \bmod 1517 = (66\cdot 532^2 \bmod 1517) \bmod 1517 = (66\cdot 862) \bmod 517 = 763$,

$C_2 = M^e_2 \bmod n = 69^{11} \bmod 1517 = 821$,

$C_3 = M^e_3 \bmod n = 83^{11} \bmod 1517 = 812$,

$C_4 = M^e_4 \bmod n = 72^{11} \bmod 1517 = 1097$,

Hosil bo‘lgan shifrtekst quyidagicha: C = {763,1441,821,1097}.

Shifrni ochish:

Modul son n = p - q = 1517, (p -1)-(q -1) ko‘paytma bilan o‘zaro tub bo‘lgan e=11 ochiq kalit, matn uzunligi L=8 bit va C = {763,1441,821,1097} bizga ma’lum.

1. e sonining (p -1)·(q -1) modul bo‘yicha teskarisini topamiz: $d = e^{-1} \bmod ((p-1) \cdot (q-1)) = 11^{-1} \bmod 1440 = 11^{383} \bmod 1440 = 131$

2. $M_i = C_i^d$ modn formula yordamida shifrni ochamiz:

$M_1 = C^d_i \bmod n = 763^{131} \bmod 1517 = 66$; $M_2 = Cd \text{ modn} = 1441^{131} \bmod 1517 = 69$,

$M_3 = C_3^d \text{ modn} = 821^{131} \bmod 1517 = 83$, $M_4 = Cd \text{ modn} = 1097^{131} \bmod 1517 = 72$,

3. M_i larni o‘nlikdan ikkilikka o‘tkazib, ASCII jadval yordamida harflarga o‘tamiz va natijada M=BESH so‘zi paydo bo‘ladi.

6.10. Rabin algoritmi

Bu shifrlash usuli 1979 yilda Maykl Rabin tomonidan chop etilgan. Algoritmning xavfsizligi katta tub sonlarga va ko‘paytuvchilarga ajratish muammosiga asoslangan. Bunda ikkita katta tub son tanlanadi va ularning har birini to‘rt soniga bo‘lganda uch qoldiq chiqishi kerak. Bu sonlar yopiq kalit hisoblanadi. Ularning ko‘paytmasi ochiq kalit hisoblanadi. p, q tub sonlar tanlanadi.Yuqoridagi shartga ko‘ra ular quyidagilarniqanoatlantirishi kerak:

$$p \bmod 4 = 3, \quad q \bmod 4 = 3.$$

Ochiq kalit n=p-q. M ochiq xabar va M<n bo‘lishi kerak.Aks holda bo‘laklarga ajratiladi. Shifrlash va shifrni ochish uchun quyidagi formulalardan foydalaniladi:

Shifrlash: $C=M^2 \text{ modn};$

Shifrni ochishda quyidagilar hisoblanadi:

$$m_1 = C^{\frac{p+1}{4}} mod\ p,$$

$$m_2 = (p - C^{\frac{p+1}{4}}) mod\ p,$$

$$m_3 = C^{\frac{p+1}{4}} mod\ q,$$

$$m_4 = (p - C^{\frac{p+1}{4}} mod\ q,$$

$$a = p(p^{-1} mod\ q), \qquad b = q(q^{-1} mod\ p)$$

$M_1 = (a \cdot m_3 + b \cdot m_1) \bmod n,$

$M_2 = (a \cdot m_3 + b \cdot m_2) mod\ n,$

$M_3 = (a \cdot m_4 + b \cdot m_1)\bmod n$,

$M_4 = (a \cdot m_4 + b \cdot m_2)\bmod n$.

Hosil bo‘lgan M_1, M_2, M_3, M_4 lardan bittasi kerakli M xabarga teng bo‘ladi.

$M=\{ M_1, M_2, M_3, M_4\}$.

Qolgan uchta xabar yolg‘on bo‘ladi. Mana shu jihat bu algoritmning keng tarqalishiga to‘sqinlik qildi. Shifrlash tezligi jihatidan RSA algoritmidan ustun turadi, lekin shifrni ochishda tezlikdan ancha yutqazadi. Agar shifrlanayotgan xabar tasodifiy bitlardan iborat bo‘lsa, uni ochishda qiyinchiliklar tug‘diradi, chunki qaysi javob to‘g‘riligini aniqlash uchun ichiga ma’lum tekstlarni joylashtirishga to‘g‘ri keladi.

Misol.

Ikkita tub son p=43, q=19 va M=OLTI matn berilgan. Shu matnni Rabin algoritmidan foydalanib shifrlaymiz.

Shifrlash.

1. n ni hisoblab olamiz $n=q \cdot p=19\cdot 43=817$
2. Matnni 10 lik sanoq sistemasida ifodalaymiz: 0 → 4F →7 9 ,

L → 4 C → 76, T → 54 → 84, 1 → 49 → 73 .

M=79, 76, 84, 73.

2. $C_1=M_i^2 \bmod n$formula yordamida shifrlash amalga oshiriladi:

$$C_1 = M_i^2 \bmod n = 79^2 \bmod 817 = 522$$

$$C_2 = M_i^2 \bmod n = 76^2 \bmod 817 = 57,$$

$$C_3 = M_i^2 \bmod n = 84^2 \bmod 817 = 520,$$

$$C_4 = M_i^2 \bmod n = 73^2 \bmod 817 = 427.$$

$C = \{ C_1 , C_2 , C_3 , C_4\} = \{522, 57, 520, 427\}$ shifrtekst hosil bo‘ldi.

Shifrni ochish.

Shifrni ochish jarayoniga ko‘proq vaqt sarflanadi. Shifrtekstdagi har bir son alohida ochiladi. $C = C_1 = 5\ 2\ 2$ ni ko‘rib chiqamiz.

1. $m_1 = C^{\frac{p+1}{4}} \bmod p = 522 \bmod 43 = 36$

2. $m_2 = C^{\frac{p+1}{4}} mod\ p = (43 - 36) \bmod 43 = 7$
3. $m_3 = C^{\frac{q+1}{4}} mod\ p = 522 \bmod 19 = 16$
4. $m_4 = C^{\frac{q+1}{4}} mod\ p = (19 - 16) \bmod 19 = 3$

5. a va b larni hisoblash uchun p, q larning teskarisini topib olamiz:

   $p^{-1} \bmod q = 43^{-1} \bmod 19 = 5^{17} \bmod 19 = 4$

   $q^{-1} \bmod p = 19^{-1} \bmod 43 = 19^{41} \bmod 43 = 34$

6. $a = p(p^{-1} \bmod q) = 43 \cdot 4 = 172$

   $b = q(q^{-1} \bmod p) = 19 \cdot 34 = 646$

7. $M_1 = (a \cdot m_3 + b \cdot m_1) \bmod n = (172 \cdot 16 + 646 \cdot 36) \bmod 817 = 681$
8. $M_2 = (a \cdot m_4 + b \cdot m_1) \bmod n = (172 \cdot 3 + 646 \cdot 36) \bmod 817 = 79$
9. $M_3 = (a \cdot m_3 + b \cdot m_2) \bmod n = (172 \cdot 16 + 646 \cdot 7) \bmod 817 = 738$
10. $M_4 = (a \cdot m_4 + b \cdot m_2) \bmod n = (172 \cdot 3 + 646 \cdot 7) \bmod 817 = 136$

Olingan Mi, M_2, M_3, M_4 lardan 127 dan kichiklarini o‘n oltilik sanoq tizimiga o‘tkazamiz: $79_{10} => 4F_{16} =>$ O harfi paydo bo‘ldi.

1-10 qadamlar C_2 , C_3 , C_4 larning har biri uchun alohida hisoblanadi.

Shu orqali bizda M=OLTI ochiq matn hosil bo‘ladi.

6.11. ElGamal shifrlash algoritmi

Bu sxema 1984 yilda misrlik olim Taher El Gamal tomonidan taklif etilgan. ElGamal algoritmi shifrlash va raqamli imzo qo‘yishda foydalaniladi. Algoritm xavfsizligi chekli maydonda diskret logarifmlarni hisoblash qiyinligiga asoslangan. ElGamal sxemasi AQSh (DSA) va Rossiya (GOST R 34.10-94) elektron raqamli imzo standartlari asosini tashkil etadi.

Shifrlash.

1. p - katta tub son tanlanadi.
2. Foydalanuvchilar guruhi uchun umumiy g < p tanlanadi.
3. x < p-1 yopiq kalit tanlanadi.
4. M < p qilib bloklarga ajratiladi.
5. $y = g^x \bmod p$ hisoblanadi.

6. Tasodifiy sessiys kaliti 1< k < p-1 soni tanlanadi.
7. $a = g^k \bmod p$ hisoblanadi.
8. $b = (y^k * M) \bmod p$ hisoblanadi.

a va b juftlik shifr tekst deyiladi.

Shifrni ochish.

$M = {}^{b} \bmod p$ formula orqali shifr ochiladi.

Misol.

Tub son p=89, yopiq kalit x=3 va M=BBC matn berilgan. Shu matnni Elgamal algoritmidan foydalanib shifrlaymiz.

Shifrlash.

1. Foydalanuvchilar guruhi uchun umumiy g = 11 (g<p) tanlanadi.
2. x =3 yopiq kalit.
3. Matnni ikkilik sanoqtizimida ifodalaymiz:

$B \rightarrow 42_{16} \rightarrow 01000010_2$, $B \rightarrow 42_{16} \rightarrow 01000010_2$, $C \rightarrow 43_{16} \rightarrow 01000011_2$. Demak, BBC matn ikkilik sanoq tizimida quyidagicha ifodalanadi:

$$M=010000100100001001000011.$$

4. Matnni 6 bit ($l = [\log_2 p = [\log_2 89 = 6)$ uzunlikda bloklarga ajratamiz:

$M_1 = 010000_2 \rightarrow 16_{10}$, $M_2 = 100100_2 \rightarrow 36_{10}$, $M_3 = 1001_2 \rightarrow 9_{10}$,

$M_4 = 000011_2 \rightarrow 3_{10}$.

5. $y = g^x \bmod p = 11^3 \bmod 89 = 85$.
6. k=7.
7. $a = g^k \bmod p = 11^7 \bmod 89 = 87$
8. $b_1 = (y^k \cdot M_1) \bmod p = (85^7 \cdot 16) \bmod 89 = (81 \cdot 36) \bmod 89 = 50$,

   $b_2 = (y^k \cdot M_2) \bmod p = (85^7 \cdot 36) \bmod 89 = (81 \cdot 36) \bmod 89 = 68$,

   $b_3 = (y^k \cdot M_3) \bmod p = (85^7 \cdot 9) \bmod 89 = (81 \cdot 9) \bmod 89 = 11$,

   $b_4 = (y^k \cdot M_4) \bmod p = (85^7 \cdot 3) \bmod 89 = (81 \cdot 3) \bmod 89 = 65$.

   C = { a, b_1, b_2, b_3, b_4 }= {87, 50, 68, 11, 65} shifrtekst hosil bo‘ldi.

Shifrni ochish.

Shifrni ochish jarayoniga ko‘proq vaqt sarflanadi. Shifrtekstdagi har bir son

alohida ochiladi.

$M = (b \cdot (a^{-1})^x) \bmod p$ formuladan foydalanamiz.

1. $M_1 = (b_1 \cdot (a^{-1})^x) \bmod p = (50 \cdot 44^3) \bmod 89 = (50 \cdot 11) \bmod 89 = 16.$
2. $M_2 = (b_2 \cdot (a^{-1})^x) \bmod p = (68 \cdot 44^3) \bmod 89 = (68 \cdot 11) \bmod 89 = 36.$
3. $M_3 = (b_3 \cdot (a^{-1})^x) \bmod p = (17 \cdot 44^3) \bmod 89 = (17 \cdot 11) \bmod 89 = 9.$
4. $M_4 = (b_4 \cdot (a^{-1})^x) \bmod p = (65 \cdot 44^3) \bmod 89 = (65 \cdot 11) \bmod 89 = 3.$

Olingan M_1, M_2, M_3, M_4 larni ikkilik sanoq tizimiga o‘tkazamiz: $16_{10} => 010000_2$, $36_{10} => 100100_2$, $9_{10} => 001001_2$, $3_{10} => 000011_2$.

Ularni ketma-ket yozib, 8 bitdan bo‘laklarga ajratib, harflarga o‘tamiz. $01000010010000010010000011_2 \rightarrow (01000010,01000010,01000011)_2 \rightarrow (42,42,43)_{16} \rightarrow$ BBC

Ochiq matn hosil bo‘ldi.

Nosimmetrik kriptoalgoritmlarda simmetrik kriptoalgoritmlardagi quyidagi kamchiliklar bartaraf etilgan:

- kalitlarni maxfiy tarzda yetkazish zaruriyati yo‘q; nosimmetrik shifrlash ochiq kalitlarni dinamik tarzda yetkazishga imkon beradi, simmetrik shifrlashda esa himoyalangan aloqa seansi boshlanishidan avval maxfiy kalitlar almashinishi zarur edi;
- kalitlar sonining foydalanuvchilar soniga kvadratli bog‘lanishligi yo‘qoladi; RSA nosimmetrik kriptotizimda kalitlar sonining foydalanuvchilar soniga bog‘liqligi chiziqli ko‘rinishga ega (N foydalanuvchisi bo‘lgan tizimda *2N* kalit ishlatiladi).

Ammo nosimmetrik kriptotizimlar, xususan RSA kriptotizimi, kamchiliklardan xoli emas:

- hozirgacha nosimmetrik algoritmlarda ishlatiluvchi funksiyalarning qaytarilmasligining matematik isboti yo‘q;
- nosimmetrik shifrlash simmetrik shifrlashga nisbatan sekin amalga oshiriladi, chunki shifrlashda va shifrni ochishda katta resurs talab etiladigan amallar ishlatiladi (xususan, RSA da katta sonni katta sonli darajaga oshirish talab etiladi). Shu sababli nosimmetrik algoritmlarni qurilmalarda amalga oshirilishi simmetrik algoritmlardagiga nisbatan anchagina murakkab;

- ochiq kalitlarni almashtirib qo‘yilishidan himoyalash zarur. Faraz qilaylik "A" abonentning kompyuterida "V" abonentning ochiq kaliti *"K_V"* saqlanadi. "p" buzg‘unchi odam "A" abonentda saqlanayotgan ochiq kalitlardan foydalana oladi. U o‘zining juft (ochiq va maxfiy) *"K_p"* va *"k_p"* kalitlarini yaratadi va "A" abonentda saqlanayotgan "V" abonentning *"K_V"* kalitini o‘zining ochiq *"K_p"* kaliti bilan almashtiradi. "A" abonent qandaydir axborotni "V" abonentga jo‘natish uchun uni *"K_p"* kalitda (bu *"K_V"* kalit deb o‘ylagan holda) shifrlaydi. Natijada, bu xabarni "V" abonent o‘qiy olmaydi, " *p"* abonent osongina ochadi va o‘qiydi. Ochiq kalitlarni almashtirishning oldini olish uchun kalitlar sertifikatlaniladi.

VII. BOB. KVANT KRIPTOGRAFIYASI

7.1. Kvant axborotlari nazariyasining asosiy tushunchalari

Axborotning kvant nazariyasi XX asrning eng muhim ikki nazariyasining kesishmasidir: Bular kvantmexanikasi va axborot nazariyasi. Kvantmexanika axborotni uzatish va qayta ishlashda ishtirok etish imkoniyatlari va holatlari bilan shug'ullanadi va ko'rib chiqadi. Ushbu nazariya XX asrning 60-yillarda kompyuter texnologiyasini tezkor rivojlantirishda paydo bo‘ldi, natijada hisoblash qurilmalari hajmining doimiy ravishda pasayib borishi muqarrar ravishda vaqtni axborot resursi sifatida yagona kvant holatidan foydalanishga majbur bo‘ladi. Bu yangi qiyinchiliklarni, birinchi navbatda kvant shovqinining kuchli ta’sirini anglatadi, bu hal qiluvchi omil deb hisoblandi. Biroq, ushbu hodisani batafsil o'rganish natijasida, kvant shovqinlari axborotni uzatish va qayta ishlashda yordam berishi mumkinligi aniqlandi: shunday qilib, hodisa bir zarrachaning kvantli "tarqalishi", ammo bir nechta kosmik nuqtalar aralashuvlar xususiyatiga ega, bu esa juda ko‘p holatlarda ishlatilishi mumkin. Kvant axborot nazariyasi yangi fan sifatida kvant fenomenlari bilan ishlaydi, ularning xususiyatlarini belgilaydi va ularni qo‘llaydigan texnologiyalarni o‘rganadi. Ayniqsa, kvant holatini qo‘llash, kvant kompyuterning g‘oyasi hisobiga hisoblash tezligini yangi darajaga olib chiqishi mumkin, shuningdek, kvant kriptografiyasida kalitlarning taqsimlanishining mutlaq maxfiyligini kafolatlaydi.

Ushbu bobda kelajakda kvant kriptografiya protokollari xususiyatlarini taqdim etishda foydalaniladigan kvant axborot nazariyasining asosiy tushunchalari va faktlari ko`rib chiqiladi.

7.2. Kvant holatlar

Boshlang‘ich zarralar bo‘yicha dastlabki tajribalar paytida, ularning harakatlari ayni paytda mavjud bo‘lgan jismoniy hodisalar g‘oyalari bilan murosaga kelishi juda qiyin bo‘lgan. Bu elementar zarrachalarning xatti-harakatini tasvirlaydigan yangi qonunlar shakllangach, fizikaning bu qismi kvant nazariyasi deb atala boshlandi va o‘sha paytda dunyodagi jismoniy rasmi - klassik edi.

To‘lqin funksiyasi va sof holatlar

Kvant nazariyasi va klassikasi o‘rtasida bir-biridan muhim farqlar mavjud va uning bunday asosiy farqlardan biri kvant zarrachasining ta’rifi va uning holati. Bunday zarrachaning ma’lum koordinatalari, o‘lchamlari va massasiga ega bo'lgan qismi kabi g'oyasi aslida noto'g'ri bo'lib chiqdi, chunki ba'zi bir zarralar uchun, aslida qayerda bo'lishidan qat'iy nazar, ularni tushunish mumkin emas edi. Lekin bunday zarralarning xatti-harakatlarini oldindan aytish mumkin edi. Shu bilan birga, bu xatti-xarakatlarni faqat tizimning barcha "an'anaviy" jismoniy xususiyatlarini hisoblashga urinishdan voz kechganidan keyin tushuntirish mumkin edi.Bu esa, har qanday elementar zarracha (yoki zarracha tizimi bir necha bo'lsa) ning "to'lqin funktsiyasi" deb atalishi - dunyoning kvant rasmidagi tubdan yangi narsa bo'lganligiga olib keldi. Avvalo sof kvant holatining tushunchasini tanishtiramiz. Bunday holat Gilbert tipidagi $\mathcal{H}$ ning birligi normasi bilan vektordir. Vektorning normasi uning skalyar maydonining ildizidir:

$$|| \psi ||= \sqrt{(\psi, \psi)}, \ \psi \in \mathrm{H}$$

Ushbu ish doirasida faqat son o'lchamli Gilbert bo'shliqlari hisobga olinadi va skalyar mahsulotning mavjudligi ularning xususiyatlaridan eng muhimi bo'ladi. Shunday qilib, vektor uchun ψ, birlik normasining xususiyati shunga o'xshash tarzda yozilishi mumkin $\psi^* \psi = 1$.

Yuqoridagi ta’rifni to‘lqin funksiyalarining an’anaviy shakllanishiga osonlik bilan bog‘lash mumkin: har bir to‘lqin funksiyasiga ko‘ra vektorga to‘g‘ri keladi, bu i-koordinatasi fazoda ψ_i -nuqtada zarralarni topish ehtimoli amplitudasiga teng. Shunday qilib, muammoning shartlariga eng mos bo‘lgan joyni topish muhim ahamiyatga ega.

Shtatning normallashuvi talabi, zarrachani aniqlashning umumiy ehtimoli birligini anglatadi. Holatlar va operatorlar uchun kvant axborot nazariyasida Dirak tomonidan kiritilgan yozuvdan foydalanish odatiy holdir. Holat φ 'ψ), va skalyar mahsulotda $\langle\psi$ kabi ishlatiladigan holati ψ^*. Keyin vektorlar ($\langle\psi$) skalyar

mahsuloti ($\varphi \mid \psi$) sifatida yoziladi.Har bir sof kvant holatiga $\langle\psi$ muvofiq operatori $\langle\psi$ = zichlik operatori deb ataladi. Bu operator 1-darajaga ega, uning izi bir xil va u sof holatda proyektor vazifasini bajaradi $\langle\psi$).

Aralash holatlar

Zichlik operatorlari yordamida kvant holatining umumiy kontseptsiyasi kiritiladi. Qo'shma kvant holati bir nechta sof holatlarning statistik aralashmasidir (ya'ni, mos keladigan ehtimolliklarga ega sof holatlar to'plami): $p = \sum_i p_i \mid \psi_i >< \psi \mid$,

$p_i = 0 \ \forall_i \ \sum_i p_i = 1$

Aralash holatning izi birga teng. Uning ijobiy ta'rifini ko'rsatish osonroq:

$(\varphi \mid \rho \mid \varphi >= \sum_i p_i \mid < \varphi \mid \psi > \mid^2 \geq 0 \quad \forall \mid \varphi > \in \mathrm{H}$

Bundan tashqari, har qanday ermit A operatori siyrak holatga ega ekanligi

$$\text{ma'lum } A = \sum_i \lambda_i \mid \lambda_i >< \lambda_i \mid,$$

bu yerda λ_i o'zliklari haqiqiydir va o'z vektorlari $\mid \lambda_i$) normalizatsiya qilinadi va ortogonaldir. Bu operator bilan atalgan bo'lishi mumkin, iz bilan har qanday ijobiy ermit operatori bir kvant holati zichligi, degan ma'noni anglatadi: (ehtimol og'irligi sifatida qabul qilinadi) quyidagi ijobiy barcha vektorlar ijobiy ta`rifidir va bir iz holatidan - vektorlar yig'indisi birga teng deb. Shuning uchun ularning shunga o'xshash birikmasi statistik aralashma sifatida ko'rib chiqilishi mumkin. Bu kvant holatining umumiy ta'rifiga olib keladi:

Ta'rif: Kvant holati H -Gilbert tekisligidagi ijobiy operatori ya'ni bir izli.

Kvantli vaziyatlar H ustidan operatorlar bo'shlig'ida konveksni hosil qiladi. Kvant holatlarining to'plami odatda $\mathrm{S}(\mathrm{H})$ bilan belgilanadi. Ushbu to'siqning qirra nuqtalari 1-darajali operatorlar tomonidan baholangan sof kvant holatidir.

Vaqti-vaqti bilan holat o'zgarishlari

Kvant mexanikasining asosiy qonunlaridan biri - kvant holatini vaqtdagi

o‘zgarishlarni tavsiflovchi Shryodingger tenglamasi, kvant mexanikasining an’anaviy kurslarida

$$ih\frac{d|\psi>}{dt} = H|\psi>, \qquad (1)$$

bu yerda h-doimiy koeffitsienti va taxminan $1.054*10^{-34}$ ga teng

Ermitlik operator H sistemadagi Gamiltoni deb ataladi va uning evolyutsiyasiga ta’sir qiladi. Ermit va unitar operatorlar o‘rtasidagi yozishmalar tufayli

$$U = e^{i H}$$

Shryodinger tenglamasi shaklda qayta yozilishi mumkin

$$|\psi'>=U|\psi>. \qquad (2)$$

Keyingi hisob-kitoblar uchun bu Shryodinger tenglamasining eng qulay usuli hisoblanadi, chunki u kvant tizimining har qanday evolyutsiyasi unitar transformatsiyalarning harakati sifatida ifodalanishi mumkinligini anglatadi. Unitar operator operatorni qoniqtiruvchi holat deb hisoblaydi

$$UU^{\uparrow} = U*U = I$$

Kubitlar

Noyob kvant obyektining eng oddiy misoli – ikki asosiy holatga ega bo'lgan tizimdir. Bunday tizimlarning fizik misollari polyarizatsiya (vertikal | $\updownarrow$) va gorizontal | mos keladigan yo'nalishli fotonlar bo'lishi mumkin $\leftrightarrow$)) yoki elektronning yo'nalishi ($|\uparrow$ yuqoriga va pastga | $\downarrow$). Bu holatda tegishli Gilbert fazosi ikki o'lchamli bo'ladi va odatda "H^2" deb ataladi. Odatda, agar ikki darajali tizimning o'ziga xos jismoniy tabiati ahamiyatga ega bo‘lmasa, uning holatlari $|0\rangle$ va $|1\rangle$) deb ko'rsatilgan. Klassik bit bilan taqqoslaganda bunday tizim kubit, deyiladi, ya'ni "miqdoriy bit" degan ma’noni anglatadi.

Kubitningixtiyoriy sof holati quyidagicha yozilishi mumkin

$$|\psi>=\cos a|0>+\sin a|1>,$$

Zichlik operatorining p darajasi 1 ga teng bo'lishi mumkin (sof holda $|\psi><\psi|$) uchun) yoki 2 –L^2holatida har doim ikkita sof holatlarning statistik aralashmasi

sifatida ifodalanishi mumkin bo‘lgan aralash holat:

$$p = p\,|\psi><\psi\,| + (1-p)\,|\psi^{\perp}><\psi^{\perp}|,$$

7.3. O'lchovlar

Kvant holatini klassikadan tajribalar o'tkazishning kvant holatini ajratib turuvchi va kvant kriptografiya qo'llanilishiga imkon beradigan tartiblarni o'lchash usuli. Kvant mexanikasi va klassika o'rtasidagi eng muhim farq shundaki, umumiy holda kvant tizimini o'lchash dastlabki holatini o'zgartiradi.

Kvant kuzatilmalari

Birinchidan, muayyan jismoniy tizimda eksperimentlarni o'tkazishning umumiy tamoyillarini ko'rib chiqaylik.Shuning uchun har qanday tajribada ikkita bosqichni ajratish mumkin: p holatni tayyorlash va M uni o'lchash. M o'lchami aniq natijani berishi shart emas, umuman, o'lchov natijasi statistik natijalar to'plami {x} mos keladigan ehtimolliklar bilan $\mu_p(x)$. Bir nechta kvant holatlarining statistik ansambllari uchun ularning kuzatish natijalari ham statistik aralashmalar bo'lishini talab qilishi tabiiydir.

7.4. Kvant fizikasi asoslari

Kvant (lotin quantum – "qancha") fizikadagi har qanday miqdorning bo'linmas qismi. Plankning doimiysi (harakat kvantasi) elektromagnit nurlanish energiyasini uning chastotasi bilan bog'laydigan koeffitsientdir

$$h = \frac{E}{v} = 6{,}62606957(29) * 10^{-34}$$

bu yerda

E – elektromagnit nurlanishning energiyasi [J];

v – elektromagnit nurlanish chastotasi [1/sekund];

Hozirgi kunda ko'pgina olimlar klassik fizikaning qonunlari makroskopik darajada (yulduzlar, odamlar, molekulalar) amal qiladi, boshqalari, shu jumladan mikroskopik (elementar zarralar kvarklar, fotonlar, elektronlar). darajada amal qiladi deb o`ylashadi. Kvant fizikasi doirasida har qanday elementar zarracha, bu

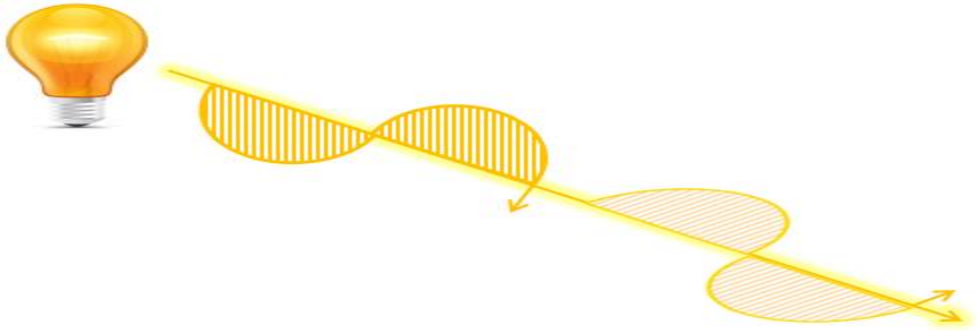
zarracha uchun xarakterli bo'lgan maydonning qo'zg'alishi kvanti deb hisoblanadi. Kvantli maydonlar bir-biri bilan o'zaro ta'sir qilishi mumkin, natijada kvantlar (zarralar) bir-biriga aylanishi mumkin.

Elementar zarrachalardan biri fotondir. Foton (yunoncha φῶς - "yorug'lik") – elektromagnit nur (elektromagnit to'lqin) kvanti bo'lib, Massa va zaryadi nolga teng bo'lgan elementar zarra. Zamonaviy g'oyalarga ko'ra, foton korpuskulyar to'lqinli dualizm bilan ajralib turadi. Bir tomondan, to'siqlarning o'lchamlari foton to'lqin uzunligi bilan taqqoslanadigan holatda foton difraksiya fenomenida to'lqin xususiyatlarini namoyon etadi. Boshqa tomondan, fotonlar bilan materiyaning o'zaro ta'siri jarayonlari (radiatsiya va absorbsiya) faqat bu haqida diskret g'oyalar asosida muvaffaqiyatli talqin qilinishi mumkin.

Yorqin jismning nurlanishini, har tomonga undan yo'naltirilgan foton oqimlari deb tasavvur qilish mumkin.

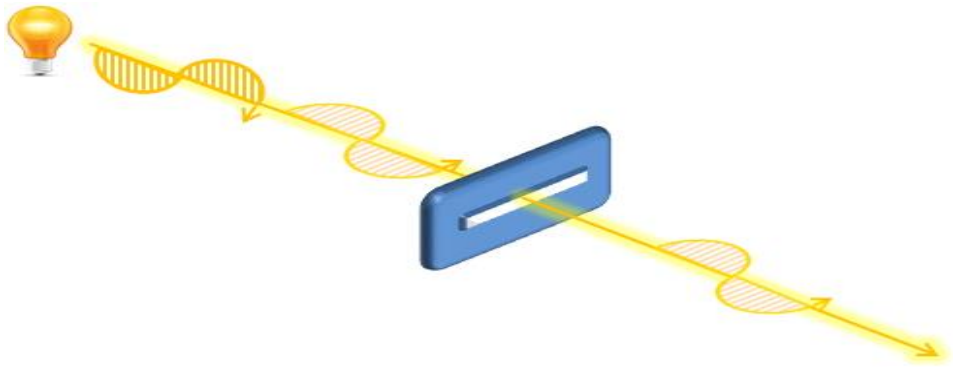
Yorqin jismning nurlanishi

Bu oqimlar odatda kichik to'siqlarni (diffraktsiyaga qarang) yoki massa jismlarga (sayyoralar, yulduzlar) yaqinlashmasidan tashqari, bir tekis nur bo'ylab tarqaladi. Shunday qilib, foton oqimi bir tekislikda osmon (qutblangan) elektromagnit to'lqinlarining to'plami sifatida ifodalanishi mumkin.



Ikki foton oqimi (elektromagnit to'lqinlar)

Optik nurlanish chiziqli polyarizator orqali (masalan, Glan prizmasi) o'tgach, kerakli polyarizatsiyaga ega foton chiqishida olinishi mumkin. Majoziy ma'noda, bu jarayon fotonlarning bir tekis diafragma bilan filtri orqali o'tishi mumkin, bu fotonlarning faqat bir qismidan o'tadi - polyarizatsiya tekisligi filtr teshiklarining yo'nalishiga mos tushadi.



Filtr orqali foton oqimining o'tishi

Agar kerakli polarizatsiyaga ega foton oqimini hosil qilish mumkin bo'lsa, ixtiyoriy ushlangan fotonlarning zamonaviy o'lchash asboblari bilan polyarizatsiyasini aniq aniqlash mumkin emas. Ushbu holat ma'lumotni shifrlash uchun kvant mexanikasidan foydalanish imkonini berdi.

Har xil polyarizatsiya tekisliklariga ega bo'lgan ikki yo'nalishli polyarizatorlar bit shaklida ko'rsatilgan ma'lumotlarni kodlash uchun yetarli. Bir tekislikka yo'naltirilgan fotonlar "1" ga, ikkinchisida "0" ga to'g'ri keladi. Ushbu tamoyil uzatish moslamasi (foton generatori) ishiga asoslangan.

Qabul qiluvchi qurilma chiziqli polyarizator yoki polyarizatsiya ajratish prizmasiga asoslangan holda yaratilishi mumkin.

Birinchi holda, olingan foton polyarizatordan o'tib, fotodetektor tomonidan ro'yxatga olingan bo'lsa, u holda "1", aks holda "0" deb belgilanadi.

Ikkinchi holda, optikasi orqali fotonlarning o'tish ikki o'zaro perpendikulyar polyarizatsiya tekisligi (asoslari) uchun tegishli.Qayta yo'riqnoma polyarizatsiya tekisligi olingan fotonning polyarizatsiya tekisligiga eng yaqin bo'lgan fotodetektorga o'tkaziladi. Agar jo'natuvchi va qabul qiluvchi tomonlar bir xil polyarizatsiya asosini (masalan, gorizontal-vertikal) ishlatsa, qabul qiluvchi tomon kiruvchi fotonlarni (masalan, gorizontal polyarizatsiya bilan "1", vertikal "0" deb

nomlanadi) identifikatsiyalashadi.Agar qabul qiluvchi tomon boshqa polyarizatsiya asosini qo'llasa, to'g'ri identifikatsiya qilish ehtimoli kamayadi. Xususan, bazaning qabul qiluvchi tomoni uzatish moslamasiga nisbatan 45% atrofida qaytarilsa, to'g'ri identifikatsiya qilish ehtimolligi taxminan 50% ni tashkil qiladi.

7.5. Kvant shifrlash asoslari

Qabul qiluvchi tomondan chiziqli polarizatorlar yordamida shifrlash

Fotonlarni yuborish va olish uchun tomonlar to'rtta filtrdan (polyarizator) foydalanishlari mumkin.

a) gorizontal | b) vertikal | c) chap-o`ng past-yuqori | d) chap-o`ng yuqori-past

Fotonlarni yuborish va qabul qilish uchun filtrlar

Agar bitta foton uchun (ma`lumotlar bitda) jo'natuvchi va qabul qiluvchi tomonlar bir xil filtrlardan foydalanadigan bo'lsa, u qabul qiluvchi tomonning fotodetektori tomonidan ro'yxatga olinadi va "1", aks holda - "0" deb belgilanadi.

Tomonlar maxfiy ma'lumotlarni almashtirish uchun ikkita filtrdan foydalanishlari kifoya. Buning uchun ular qabul qiluvchi tomondan foydalanish tartibini oldindan belgilab qo'yishadi, lekin bu mumkin bo'lgan raqib uchun tasodifiy bo'lishi kerak. Ushbu buyurtmani shifrlash / deshifrlash kaliti bo'ladi. Filtrni qabul qiluvchiga (kalit) qo'llash tartibini biluvchi jo'natuvchi, qabul qiluvchining olingan fotonni to'g'ri aniqlab berishi uchun, xabarni yuborish uchun tegishli filtrni qo'llashi kerak.

Quyidagi jadvalda qabul qiluvchi gorizontal va vertikal filtrlardan foydalanganida "00110101_2" xabarini yuborishning namunasi berilgan.

1-jadval. Xabar yuborish va qabul qilishga misoli

Xabar yuborish, bit	0	0	1	1	0	1	0	1
Qabul qiluvchilar tomonidan ishlatiladigan filtrlar (kalit)								
Yuboruvchi tomonidan tanlanadigan filtrlar								
Qabul qilinuvchi xabar, bit	0	0	1	1	0	1	0	1

Chunki dushman filtrlardan qanday foydalanishni bilmaydi, keyin fotonni to'sib qo'yganini to'g'ri izohlay olmaydi.

Ushbu shifrlash sxemasining mustahkamligini ta'minlash uchun gammani kodlashda kalit, albatta, tasodifiy va bir martalik bo'lishi kerak. Gamma generatorlari bunday kalitlarni ishlab chiqarish uchun ishlatilishi mumkin. Misol uchun, gamma keyingi bit "1" bo'lsa, qabul qiluvchi gorizontal filtrdan foydalanishi kerak, aks holda - vertikal. Kalitni (gamma) yaratish uchun siz kvant kalit almashinuvi protokollarini (masalan, BB84 protokoli) ishlatishingiz mumkin.

Shifrlashning barqarorligini oshirish uchun qabul qiluvchi tomondan filtr juftlarini almashtirish tavsiya etiladi. Bu shuningdek, aloqa kanalini tinglash faktini ham aniqlaydi. Foton ushlanganida, dushmanning nusxasini (klonini) yaratish va uni axborotni huquqiy oluvchisiga yuborish kerak. Agar dushman bir xil juftlik filtri yoki ajratuvchi prizmadan foydalanmasa, u holda fotonlarning bir qismini polyarizatsiyasini to'g'ri aniqlay olmaydi va shuning uchun kerakli nusxalarni yaratadi.Xabarni bekor qilishni tekshirish uchun jo'natuvchi va qabul qiluvchi jo'natilgan va qabul qilingan xabarlarning navbati bilan xesh ta’svirlarni (kontrol summa) hisoblab chiqishi mumkin. Ochiq kanal orqali ularni himoya

qilmasdan o'tkazilishi mumkin bo'lgan xesh – tasvirlarni taqqoslab, ular aloqa kanalini tinglayotgani yoki ma’lumotlar uzatilishi (yaxlitligi) to‘g‘ri ekanligini tasdiqlashi mumkin.

Qabul qiluvchi tarafdagi polyarizatsiya ajratish prizmasidan foydalanib shifrlash

Maxfiy ma'lumotlarni uzatish va qabul qilish uchun ikki asosdan: to'g'richiziqli va diagonaldan foydalaniladi. Bu holda, avvalgi sxemada ko'rsatilganidek, alohida fotonlar uchun ma'lumot almashinadigan bazalar ketma-ketligi taraflarga ma'lum va potentsial dushman uchun tasodifiy bo'lishi kerak. Ushbu buyruq gamma generatorlari yoki BB84 protokollaridan foydalanishingiz mumkin bo'lgan shifrlash / deshifrlash kalitidir. Bunday holatda, agar gamma keyingi bit "1" ga teng bo‘lsa, unda tomonlar to‘g‘ridan-to‘g‘ri chiziqli asosda, aks holda - diagonalli foydalanishi kerak.

Fotonlarni yuborish uchun yuboruvchi tomon to'rtta filtrni qo'llaydi.

Baza	Filtr turi	Bit qiymat
To`g`richiziqli 	Gorizontal 	1
	Vertikal 	0
Dioganalli 	Chap-o`ng past-yuqori 	1
	Chap-o`ng yuqori-past 	0

Fotonlarni jo'natish uchun filtrlar

Yagona fotonni uzatishga mo'ljallangan filtr turiga qarab foydalaniladigan bazalar tartibiga qarab tanlanadi. Qabul qiluvchi tomon xuddi shunday qo'llaydi - kalitga qarab polyarizatsiya bazasini ishlatadi.

Xabar yuborish, bit	0	0	1	1	0	1	0	1
Qabul qiluvchilar tomonidan ishlatiladigan bazalar (kalit)								
Yuboruvchi tomonidan tanlanadigan filtrlar								
Qabul qilinuvchi xabar, bit	0	0	1	1	0	1	0	1

Xabar yuborish va qabul qilish misoli

Raqib(dushman) tomon fotonni ushlab, mutlaq aniqlik bilan uning qutblashuvini aniqlay olmaydi: u amaliy bazani taxmin qildimi (yuborilgan bitni aniqlaganmi) yoki u qo‘llanilganiga 45° burchak ostida joylashganmi? Ikkinchidan, to‘g‘ri bit identifikatsiya qilish ehtimolligi 50% ni tashkil etadi.

Ushbu holat aloqa kanalini tinglash faktini aniqlashga imkon beradi. Qoplangan foton uchun bit qiymatini aniqlab, nusxa olish uchun ikki xil bazaga mos keladigan ikkita tenglashtiriladigan polyarizatsiya variantiga ega bo'ladi. Xabarning buzilganini tekshirish uchun jo'natuvchi va qabul qiluvchi taraflar yuborilgan va qabul qilingan xabarlarning navbati bilan xesh ko`rinishlarini (kontrol summa) hisoblab chiqishlari va ularni taqqoslashlari mumkin.

7.6. Kvant kalit tarqatish uchun BB84 protokoli

1984 yilga kelib yuqorida asosiy qism natijalari allaqachon ma'lum edi.Ular kvant kriptografiya tamoyillarini shakllantirish va kamida bir marta ta'minlash uchun maxfiylik tomonidan ishonchli emas lekin juda sezgirlik vajlari yetarli edi. So‘ngra u kvant kriptografiyasi to'g'ri rasmiyatchilikni rivojlantirish uchun vaqt

bo'ldi: muhim harakatlar qonuniy foydalanuvchilar, rasmiy harakat aralashishi, bayon qilingan. Shuningdek maxfiylik BB84 deb nomlangan birinchi asosiy kvant tarqatish protokoli isbotlangan.

Kvant kriptografiya asosidagi kvant axborot nazariyasining asosiy faktlari bilan kvant holatini nusxa ko‘chirish mumkin emasligi va izotropik holatlarni ishonchli farqlashning mumkin emasligi o'zaro bog'liqdir. Ushbu faktlar kvant holatini noturg'un bo'lmagan to'plamdan aralashuvga aralashtirishga urinishlar, ya’ni kvant harakatlarini aniqlash mumkin, ammo bu qabul qiluvchi tarafidagi xatoning kattaligidir.

Bu kvant kriptografiya yengillashtirish harakatlari tabiati va unga mavjud resurslar haqida, yashirincha quloq soluvchi barcha resurslarga ega va tabiat ayni paytda ma'lum qonun doirasida har bir narsani iloji boricha harakatlari, albatta, mumkin, deb taxmin qilinishini ta'kidlash muhimdir. Bu sezilarli, hisoblash quvvati chegarasi yengillashtirishda mumtoz kvant kriptografiya farqiga tayanadi. Ushbu bobda, asosiy kvant tarqatish BB84 bayonnomasi ko'rib chiqiladi va maxfiyligi uning sxemasida dalil sifatida berilgan, keyin Interseptor hujumlar turli sinflar uchun davom etadi.

7.7. Protokolning umumiy sxemasi

Norasmiy ravishda kvant kriptografiyasining barcha protokollarining ishlash printsipi quyidagicha ta'riflanishi mumkin: har bir bosqichda uzatuvchi tomon (Alisa) har bir bosqichda holatlardan birining ortik bo'lmagan to'plamlaridan birini yuboradi va qabul qiluvchi tomon (Bob) bunday o'lchovni amalga oshiradi, keyinchalik tomonlar o'rtasida klassik ma'lumot almashishdan so'ng, chiziqli, ideal kanalning holati va interseptorning yo'qligi bilan to'liq mos keladi. Ushbu chiziqlardagi xatolar ideal bo'lmagan ikkita kanalni va kollektorning harakatlarini ham gapirishga qodir.Xato muayyan cheklovdan oshib ketgan bo'lsa, protokolning ishlashi to'xtatiladi, aks holda qonuniy foydalanuvchilar barcha maxfiy kalitlarni (qisman mos keladigan) bittadan ajratib olishlari mumkin.

Ushbu bo'limda BB84 protokoli va kalitlarning kvant taqsimotida qonuniy

foydalanuvchilarning umumiy sxemasi tasvirlanadi.

Signal holatining uzatilishi

BB84 protokolida ikkita bazadan foydalaniladi:

$$+ : |x\rangle = |0\rangle,\ |y\rangle = |1\rangle,$$

$$x : |u\rangle = \frac{1}{\sqrt{2}}(|0\rangle + |1\rangle),\ |v\rangle = \frac{1}{\sqrt{2}}(|0\rangle - |1\rangle)$$

Ushbu bazalarning xolislik holatiga mos kelishini tekshirish oson

$$|\langle x|u\rangle|^2 = |\langle x|v\rangle^2 = \frac{1}{2},$$

$$|\langle y|u\rangle|^2 = |\langle y|v\rangle^2 = \frac{1}{2},$$

bu holatning asosiy nuqtai nazaridan simmetrik joylashuvga ega bo'lganligini norasmiy ravishda kamaytiradi.

Holatlarni tayyorlash bosqichida Alisa tasodifiy shu asoslardan birini tanlaydi va keyin tasodifiy bit qiymatini tanlaydi: 0 yoki 1 va bu tanlovga ko'ra to'rtta signaldan birini yuboradi:

- $|x\rangle$, agar asosi "+" bo`lsa bit qiymati 0 bo'ladi.
- $|y\rangle$ Xuddi shu bazis asosida bitning qiymati 1.
- $|u\rangle$ qachonki "x" yo`qolganda bit 0 bo'ladi.
- $|v\rangle$, agar 1 bit "x" asosida tushib qolsa.

Ushbu signallarning har birini yuborganida, Alisa o'zining tanlovi va bitning tanlovini eslab qoladi, bu esa uning yonida ikki tasodifiy bittasining paydo bo'lishiga olib keladi. Alisa tomonidan yuborilgan har bir signalni olgan Bob, har bir Alisa asosidagi holatlarning ortogonalligi tufayli ishonchli natija berishga qodir ikkita o'lchovlardan birini tasodifiy amalga oshiradi:

$$M_0^+ = |x\rangle\langle x|,\quad M_1^+ = |y\rangle\langle y|,$$

$$M_0^x = |u\rangle\langle u|,\quad M_1^x = |v\rangle\langle v|,$$

- Natijada, u ikkita qatorga ega bo`ladi: ularning qaysi biridir o'lchash uchun tanlangan va bu o'lchovlarning natijalari bilan.

· Shunday qilib, barcha holatlar va o'lchovlar o'tkazilgandan keyin, Alisa va Bobning ikki bosqichlari bor. Ochiq kanal lekin Alisa va Bob bazalarini tanlash bilan bir-biriga ularning qatorlari e'loni va ular asoslari mos emas bo'lganini xabar qilishadi: mos kelmagan bazislarni tashlab yuborishadi. E`tibor berish kerakki, asosiy ideal kanal va shunday taalluqli asoslarini mos tegishli holatda o'z bit chiziqlari bir aloqa kanali natijalarini aralash javob holida, Alisa bilan Bob bir vaqtga to'g'ri keladigan bit qatorni yuborib, ishlatilgan bo'lsa, har qanday Intereptor harakat bit satrlari bo'lishi kerak. Biroq, kanal xato yoki Interseptor ularning izchil bit satrlari taxminan yarmini oshkor qilib tekshirish uchun,

Alisa va Bobda mos bo`lishi mumkin emas ya`ni axborot bit satrlari ustida bildirmay harakat bo'lsa. Markaziy oraliq teoremasiga ko'ra, ochiq bit ketma-ketlikda xatto butun ketma-ketlikda bor ekanligi, to'g'ri taxminni beradi, hali u aniq qolgan holatlarda xato ehtimolini baholash mumkin. Xato qiymati ma'lum bir qiymat (protokol parametr) dan katta bo'lsa, ma'lumotlar uzatish Interseptor kaliti haqida juda ko'p ma'lumotlar bor, degan ma'noni anglatadi. Aks holda, Alisa va Bob oldidagi umumiy vazifa maxfiy kalitni olishdir. Bu vazifani ikki bosqichga bo'lish mumkin: birinchi navbatda, xato tuzatish amalga oshiriladi, natijada Alisa va Bob tasodifiy bit lentalariga ega. Ikkinchi bosqich, maxfiylik deb ataladigan, xatoliklarni tuzatishda yoki ishlatilgan kvant holatidagi xatti-harakatlar natijasida interseptorga kelishi mumkin bo'lgan kalit haqida ma'lumotni chiqarib tashlashga qaratilgan. Ushbu qadam natijasida Alisa va Bobning umumiy bit tasmasi haqida ma'lumot olmagan bo'lishi kerak.

Xatolarni tuzatish

Shunday qilib, xatolarni tuzatish amaliyotining maqsadi Alisa va Bobning bir xil bit lentalaridan butunlay bir xil bo'lishini ta'minlashdir. Bu klassik protsedura, chunki u faqat klassik bit va ochiq aloqa kanallari bilan ishlaydi.

Eng samarali xato tuzatish amaliyoti tasodifiy kodlardan foydalanishga qisqartirilgan. Q xatosi ehtimolligi bilan klassik kanalning o'tkazuvchanligi.

$$C_{clas}(Q) = 1 - h(Q),$$

bu yerda h(Q) - Shennonning binar entropiyasi. Kanaldagi xatolar ehtimolini

bilish va ketma-ket nomlar uzunligi n δ - parametr n katta qiymatlari uchun kichik amalga oshirilishi mumkin. $2^{n(C_{clas}-\delta)}$ tasodifiy so`z kodini hosil qilinadi va Alisa bir bit ketma-ketlikni qo'shadi, so'ngra Bob so'z kodi majmuyini ochadi (va shu sababli ular Yeva bilan ma'lum bo'ladi), so`z kodi natijasida ro'yxatdan Bob ehtimoli Alisaning bit satrni tanlaydi, so'zlar kodi bilan bu tanlov, kanal shovqini uchun teoremani kodlashtirishga ko'ra, Xemming metrikasi ketma-ketlikda yaqin tanlaydi. Shunga qaramasdan, amaliyotda to'liq tasodifiy kodlarni amalda bajarish oson emas, chunki ularni qo'llashda xotirada kattaroq (n qator uzunliklariga qarab) kod so'zlari soni saqlanishi kerak. Odatda real chizmalarda boshqa dizayn kodlari qo'llaniladi, ularning samaradorligi past bo'ladi.

Maxfiylikni oshirish

Ushbu bosqichda Alisa va Bob Yevaga loyiq ma'lumotlarning bit lentalariga va smetasiga ega. Ushbu taxmin "pishloq" kalitidagi xatoliklar sonidan berilgan (bu xatoliklar aloqa kanalida aralashuvlar bilan bog'liqligini va ularning hammasi Yevaning faoliyati bilan bog'liqligini eslang.) Uning ma'lumotlarini qanday baholaysiz, ammo xatolarning soni keyinroq ko'rsatiladi.

Maxfiylik bosqichining vazifasi qisman maxfiy bitdan olishdir. Alisa va Bobning Yeva sirli kalitiga mutlaqo noma'lum bo'lgan satrlari. Odatda, bunday operatsiya davomida kalit uzunligi sezilarli darajada kamayadi. Maxfiylikni oshirishga imkon beradigan asosiy usul - universal xesh funktsiyalarining klassi G[4]. Ushbu funktsiya shunday m-bit satrlari to'plamining m-bit satr A to`plamini ko'rsatadi, bir tasodifiy tanlangan hesh funktsiya $g \in G$ va $a_1, a_1 \in A$ har qanday tengsiz elementlar uchun, tasvirlar $g(a_1) = g(a_2)$ tasodifiy ehtimoli 1/2 B dan oshmasligi kerak. Bu vazifa B ning ikkita elementi prototiplarini topib, ro'yxatga olish yoki taxmin qilish orqali yanada samarali hal etilmaydi.Yevaning yakuniy kalit haqida qisman maxfiy kalit va dastlabki kalit uzunligi haqidagi dastlabki ma'lumotlari orqali taxmin qilinayotgan teorema mavjud:

Teorema. *X p(x)ning - tasodifiy o'zgaruvchisi bo'lsin va G - tasodifiy miqdori, ya'ni tenglashtiriladigan tasodifiy xesh funktsiyalariga mos keladigan xesh funktsiyalarining umumiy sinfi alifbosi X в* ***{0,1}m*** *Bunda*

$$H(G(X)\,|\,G) \geq H_c(G(X)\,|\,G) \geq M - 2^{m-H_c(X)}$$

$$bu\ yerda \qquad H_c(X) = -\log[\sum_x p(x)^2]$$

kollizion entropiya deb ataladi.

Uning ilovasi Yeva haqidagi ma'lumotni baholashni amalga oshiruvchi qonuniy foydalanuvchilar (bu $H_c(X)$ qiymati bilan berilgan) ga tushadi. (4) ning chap tomoni bilan berilgan oxirgi kalitga nisbatan Yeva noma'lumligi shubhali yakuniy kalitning uzunligini har doim tanlashi mumkin, bu umumiy sirga mos keladigan aniqlanmagan sodda taxminlarga yaqin bo'ladi.

Shunday qilib, Alisa va Bobning o'zaro axborotlari Alisa va Yevaning o'zaro axborotidan ustun bo'lgan holatda, asl qisman maxfiy kalitdan butunlay maxfiy kalitni universal xesh funktsiyasi yordamida siqib chiqarib olishi mumkin.

7.8. Protokolning qat'iyligi

BB84 protokoli taklif etilganda uning qarshiligi faqat intuitiv darajada namoyon bo'ldi: tashabbus Yeva orqali yuborilgan holatlarni o'lchash ularning halokatiga olib keladi, bu esa qabul qiluvchi tomonidan qo'shimcha xatoliklarga olib keladi. Ammo, faqat yuborilgan signallarni o'lchash orqali Yeva harakatlari cheklangan emas. Bundan tashqari, uning doirasida barcha mumkin bo'lgan harakatlari uchun Yevaga olish mumkin ma'lumotlarni hisoblash mumkin. Biroq, u BB84 protokoliga qarshiligini isbotladi va barcha mumkin bo'lgan hujumlar bilan Yeva uchun taxmin qiymati ma'lumotlarga murojaat mumkin emas deb paydo bo`ldi. Shunday qilib, 2000 yilda, u [15] kvant aloqa kanali xatolarini ishonchli tuzatadi, agar kvant kriptografiya yashirinligi kvant xato tuzatish kodlari xususiyatlariga kamaytirish mumkin, erishish va nozik ma'lumotlar ko'rsatilishi mumkin etildi. Bu maxfiy kalitni taqsimlash mumkin bo'lgan juda muhim xatolarni beradi.

Protokolning barqarorligini isbotlashning eng oson usuli bir nechta qo'shimcha protokollarni joriy qilishdir. Shunday qilib, dastlab taqdim etilgan

birinchi EPR protokoli dastlab kvant o'lchovlar nazariyasidan osonlik bilan chiqadi va qonuniy foydalanuvchilarning ayrim harakatlarining o'zgarishi oqibatida, bu haqiqiy sirni buzmasdan, yanada aniq ta'riflangan BB84 protokoliga tushirilishi mumkin.

Yordamchi EPR protokoli

Ilgari EPR holati joriy etildi

$$|\psi_{EPR}\rangle = \frac{1}{\sqrt{2}}(|00\rangle + |11\rangle),$$

eng muhim xususiyati har qanday darajada o'lchanadigan bo'lsa, ikkala quyi tizimga olib keladigan holatlar bir xil bo'ladi. Shunday qilib Bobning o'lchovlari "+" va "x" bazislarida kuzatilgan

$$\frac{\sqrt{M_0^+}\,|\psi_{EPR}>}{<\psi_{EPR}|\sqrt{M_0^+}\,|\psi_{EPR}} = |00> = |xx>, \qquad \frac{\sqrt{M_1^+}\,|\psi_{EPR}>}{<\psi_{EPR}|\sqrt{M_1^+}\,|\psi_{EPR}} = |00> = |yy>,$$

$$\frac{\sqrt{M_0^x}\,|\psi_{EPR}>}{<\psi_{EPR}|\sqrt{M_0^x}\,|\psi_{EPR}} = \frac{(|0>+|1>)\otimes(|1>+|1>)}{2} = |uu>,$$

$$\frac{\sqrt{M_1^x}\,|\psi_{EPR}>}{<\psi_{EPR}|\sqrt{M_1^x}\,|\psi_{EPR}} = \frac{(|0>-|1>)\otimes(|1>-|1>)}{2} = |vv>,$$

Ushbu printsip EPR protokoli tamoyiliga asoslanadi: EPR holatini o'lchashda ikki qatnashchining natijalari bir xil bo'lganda, uni tasodifiy maxfiy kalit yaratish uchun foydalanishingiz mumkin. Buning uchun Alisa va Bob muvofiqlashtirilgan o'lchov asoslarini ishlatish bilan shunchaki kelishib olishlari kerak: ideal EPR juftlari uchun ularning natijalari bir xil bo'ladi va interseptor kalit haqida hech qanday ma'lumotga ega bo'lmaydi (bu ideal EPR juftligining sofligi bilan kafolatlanadi).

Shunga qaramay, agar Alisa va Bob orasida sof EPR holatlari bo'lmasa ham, ularning holatlarini ideal holatda tasodif darajasiga qarab, ular har doim Yeva uchun mavjud bo'lgan ma'lumotlarni taxmin qila olishadi:

Teorema. $^{\otimes n}\langle\psi_{EPR}|\rho|\psi_{EPR}\rangle^{\otimes n} > 1-2^{-s}$, unda ρ entropiya yuqoridan miqdor bilan chegaralangan bo’ladi.

$$H(\rho) < \left(2n + s + \frac{1}{\ln 2}\right)2^{-s} + O\left(2^{-2s}\right)$$

Shmidt teoremasi yordamida tizimning qisman zichlikli operatorlari va atrof-muhitning o'zliklari mos keladi va shuning uchun Yevaning entropiyasi yuqoridan yuqoriroq miqdorda (5) chegaralanadi. Xolev qiymati o'z navbatida H (p) entropiyasidan yuqoriroq baholagani bois, yuqoridagi teoremani to'xtatuvchiga mavjud bo'lgan ma'lumotlarni baholash uchun muvaffaqiyatli ishlatilishi mumkin. Bu Alisa va Bob Yevaning boshqalaridan keyin ko'proq ma'lumotga ega emasligiga har doim amin bo'lishi mumkin. Aks holda (Alisa va Bobning ideal holatiga ega bo'lgan FERV umumiy holatining past darajadagi darajasi bilan) (FERV \) protokol bekor qilingan. Agar axborotni Yevaga tashqaridagi xabarlar kichkina bo'lsa, klassik xatolarni tuzatish protseduralari va maxfiylikning yaxshilanishi yordamida to'liq maxfiy kalitni olish mumkin.

Lo-Chu Protokoli

Lo-Chu protokoli EPR va BB84 protokollarining oraliq aloqasi sifatida ishlab chiqilgan ESR protokoli kabi, ESR juftlarini dastlabki holatlarda ishlatadi, lekin endi bu hollar Alisa tomonida ochiq ko'rinib turadi va Bobga kvant kanal orqali yuboriladi (BB84 protokoli kabi ixtiyoriy kodlash)

Yuqorida ko'rsatilgandek, Yevaning axboroti ideal holatda bo'lgan Alisa va Bob o'rtasidagi dastlabki holatlarning tasodif yuqoridan kiritishi mumkin sof EPR iborat | Parom) - bu baholash orqali, Alisa va Bob xato tuzatish va ortish maxfiyligi parametrlarini qanday tushunish mumkin, ularga murojaat qilish kerak. Fikr bayonnomasi Lo-Chu o'rniga bu ikki klassik tartiblarini Alisa va Bob ularga maxfiy kalitlari to'liq teng imkoniyatiga ega bo'ladi aniq EPR juft, tozalashingiz, murojaat qilishingiz mumkin, deb hisoblanadi.Shunday qilib, tozalash tartibi klassik xatolarni tuzatish protseduralarining kvant analogi va maxfiylikni oshirish kabi qabul qilinishi mumkin.

Yaroqsiz bo'linish tegishli kvantli xato tuzatish kodi yordamida amalga oshirilishi mumkin ekan, uzatilgan holatdagi o'zgarishlar va bit xatolar sonini o'z ichiga oladi. Agar xatolar q kubitdan ko'p bo'lsa, u holda dastlabki n kubitlardan q

xatlarni boshqaruvchi [n,k] – kod orqali EPR juftlarini olish mumkin.

Yana aniqki, Lo-Chu protokoli shunga o'xshash:

1. Alisa 2n EPR juftini $|\psi_{\mathrm{EPR}}\rangle^{\otimes 2n}$ da hosil qiladi.

2. Alisa tasodifiy 2n EPR juftidan n ni tanlaydi, keyinchalik o`zi va Bob bilan vaziyatlarning tasodifan darajasini tekshirish, ularni nazorat qilish uchun ishlatadi.

3. Alisa tasodifiy bitli qatorni s_A uzunligi 2n hosil qiladi va Adamar konvertatsiyasini har bir juftning ikkinchi kubitiga to'g'ri keladi, buning uchun s_A=1 ga teng.

4. Alisa kvant kanalidagi har bir juftning ikkinchi kubitini Bobga yuboradi.

5. Bob kubitlarni oladi va uni omma e'tiboriga havola qiladi.

6. Alisa s_A nazorat kubitlari va qator simvolining pozitsiyalarini oshkor e'lon qiladi.

7. Bob, Adamar konvertatsiyasini s_A=1ga teng kubatlarga qo'llaydi.

8. Alisa va Bob nazorat kubitlarini "+" asosida o'lchaydi va natijalarni omma e'tiboriga havola qiladi. Agar q bitdan ko'p bo'lsa, protokolni bajarish to'xtatiladi.

9. Alisa va Bob qolgan n kubitlarni [n,k] kodining tekshiruv matritsasi bo'yicha q xatoligacha tuzatadi. Xato sindromini hisoblash natijalarini baham ko'rgach, ular EPR juftiga kirishlari mumkin.

10. Alisa va Bob "umumiy" maxfiy kalitni olish uchun "+" asosida EPR juftliklari bilan o'lchanadi.

Bu yerda, 3 va 7 bosqichlarda tasodifiy kubitlar to'plamining Adamar kontseptsiyasi, Yeva tomonidan amalga oshirilgan har qanday hujumni, faza va bit xatolar ehtimoli iloji boricha yaqinroq bo'lishini ta'minlash uchun kerak va bu kvant tuzatish kodlarini qo'llash uchun eng qulay sharoitlarni yaratadi.

CSS-kodlar protokoli

EPR protokoliga asoslangan Lo-Chu protokoli EPR juftlarini olish uchun kvantli xato tuzatish kodidan foydalanadi va ayni paytda kvant xatolarining nazorat qilinmasligi umumiy holatda uni amalga oshirish uchun kvant kompyuterni talab qiladigan murakkab texnik muammo hisoblanadi. CSS-kodlari protokoli faqat bu klassik xatolikni tuzatish kodlaridan foydalanib, bu ehtiyojni qondiradi. Buning

butun jarayon ishonchliligini buzmasdan bajarishi mumkin.

Alisa tomonidan 8-bosqichda o'tkazilgan o'lchovlar dastlabki holatlarning to'siqligini buzganligi sababli, APR juftlarining qismlarini aniq qilib yuborish kerak emas: biz ma'lum kvant holatini (0) yoki [1] ni oddiygina tayyorlab, Adamar konvertatsiyasini ixtiyoriy holat ravishida ifodalanadi.

Xuddi shunday, 9 va 10 bosqichlarida foydalanuvchi o'lchovlari asl EPR juftlarini yo'q qilib, tasodifiy kvant xato tuzatish kodi bilan kodlangan tasodifiy kubitlarga aylantiradi. Shuning uchun, EPR juftlarini olish uchun kodni ishlatish o'rniga Aliksa shunchaki tasodifiy kalitni bit kodlaridan CSS-kod yordamida C1, C2 tasodifiy x va z parametrlari bilan Bob kodli kubits yuborish mumkin. Keyinchalik, 6 da Alisa AT-ning faqatgina "SA" va "bit" pozitsiyalarini emas, balki x va z kodlarining parametrlarini ham e'lon qiladi, shuning uchun Bob uzunlikdagi yashirin kalitni ochib bera olmaydi.

Shunday qilib, yuqorida keltirilgan o'zgarishlarni hisobga olgan holda CSS kod protokoli quyidagicha ko'rinadi:

1. Alisa tasodifiy nazorat bitlarini, tasodifiy k uzunlik k ni va ikkita tasodifiy bitli x va z ni hosil qiladi. Bu asosiy kodlash uchun CSS kodni 2 (C'1, C2) qo'llaniladi va holat n nazorat kubits tayyorlaydi (0) va (1) nazorat qilish bitga muvofiq.

2. Alisa tasodifiy kubits xabar kodlangan joy qolgan holatlarda kubits nazorat qilishga qo'yib, 2n holatda n tanlaydi.

3. Alisa tasodifiy bit satrni $s_A$uzunligi 2n chiqaradi va Adamard kabi tegishli holatda s_A=1 ikkinchi kubit uchun har bir qatorni o'zgartiradi, lekin Alisa Bob kvant kanaliga olingan kubatlarni yuboradi.

4. Alisa kvant kanalidagi har bir juftning ikkinchi kubitini Bobga yuboradi.

5. Bob kubit oladi va uni ochiqchasiga e'lon qiladi.

6. Alisa nazorat kubitlarini s_A liniyasining pozitsiyalarini ommaviy ravishda e'lon qiladi x va z.

7.Bob, Adamard konvertatsiyasini ushbu kubatlarga nisbatan ishlatadi, ular uchun s_A=1.

8. Bob, nazorat kubitlarini "+" asosida o'lchaydi va natijalarni jamoatchilikka e'lon qiladi. Agar q bitdan ko'p bo'lsa, protokolni bajarish to'xtatiladi.

9. Bob, qolgan n-kubitlarni CSS kodi bo'yicha (C'1, C'2) kodi bilan kodlaydi. "

10. Bob, Alisa bilan birgalikda yashirin kalitni olish uchun kubitlarni o'lchaydi.

BB84 protokoli ma`lumoti

Texnik jihatdan Lo-Chu protokolidan oddiyroq bo'lishiga qaramasdan, CSS kodlari protokoli hali juda murakkabdir, chunki u kvant holatini kodlash va dekodlash uchun kvant hisoblashni talab qiladi, shuningdek ularni kvant xotirasida xabar qabul qilinmaguncha saqlaydi Alicedan, ushbu protokolning qisqartirilishini bildiradigan BB84 protokolining ishonchli versiyasi bunday texnologiyani talab qilmaydi.

CSS-kod ikki klassik C1 va C2 koddan foydalanadi, aslida kvant kod hal qilish jarayoni yanada holat klassik hal qilish bilan almashtirilishi mumkin (aniq sabablarini ko'rib [20]), endi faqat tanlanadi, bu o'tish mohiyati kodi C 2 sinf va siri bilan bog'liq - kodi Ci va xato tuzatish jarayoni va ikkinchi mos keladi. Endi maxfiylik amplifikatsion, keyin oddiygina yetarlicha C1 kodi so'zini e'lon qiladi va kodlash va signal o'girishga ishlab chiqariladi, protokol ketidan osonlashtiriladi.

Nihoyat, Alisaning kubitlarini kvant xotirasida saqlab qolish uchun, kodlar Bobga mos kelmasligi uchun, Bobdan tasodifiy tanlab olingan "+" yoki "x" asosida foydalanib, har bir signalni darhol o'lchab olishlari mumkin. Alisa, navbatda, bu bazislardan birida signal yuboradi. Bazislarning taxminan yarmida Alisa va Bobning asoslari mos kelmaydi va ularning o'lchov qiymatini yo'qotish kerak bo'ladi, chunki chiziqning umumiy uzunligi 2n dan 4n (1 + δ) ga oshishi kerak.

Shunday qilib, BB84 protokolining yakuniy ishonchli versiyasi quyidagicha:

1. Alisa, $4n(1+\delta)$ tasodifiy bitni tanlaydi
2. bit har biri uchun Alice Tasodifiy mag'lubiyatga muvofiq asos "+" va

"x" tanlab, Bob signal yuboradi

3. Alisa tasodifiy codeword $v_k \in C_1$ tanlaydi.

4. Bob Tasodifiy mag'lubiyatga muvofiq ravishda "+" va "x" bilan qubits va chora-tadbirlar ularning har biri qabul s_b

5. Alisa va Bob aks holda protokoli bekor qilinadi, faqat nashrni natijasida o'rinlarni katta ehtimollik 2n bitni qolmoqda bilan bit tegishli qadriyatlar, nishonlamoqchi bo'lgan satr kubits tark satr va s_b, oshkor.

6. Alisa tasodifiy qolgan 2n n bit nazorat dan tanlaydi.

7. Alisa va Bob ularning nazorat bitlarining qiymatlarini ochiqchasiga solishtirishadi. Turli xil bitlarning soni qning kritik qiymatidan katta bo'lsa, protokol bekor qilinadi.

8. Alisa $x - v_k$ e'lon qiladi; Bob ushbu natija natijasidan chiqarib, xatolarni bartaraf etish uchun "C" ni ishlatadi, v_k - aniqlanmaydigan mag'lubiyatga ega, ammo qisman Yevaga ma'lum bo'lishi mumkin.

9. Alisa va Bob bir-biriga yaqinlik sinfini hisoblab chiqadi, ($v_k + C_2$ uchun umumiy maxfiy kalitni olish uchun.

Ushbu protokol sxemasi xatoliklarni tuzatish va maxfiylikni CSS-kodlar xususiyatlarini on-line rejimida rivojlantirish uchun foydalanadi. Kvant kanalida tuzilishi mumkin bo'lgan xato q ning kattaligi uchun nazariy taxmin Shennon chegarasi tomonidan beriladi: 1 - 2h (q)> 0, bu chegara yaxshiroqdirVarshamova-G Nilbert CSS-kodlarining mavjudligini kafolatlaydi.Shannon chegarasi (tasodifiy klassik kodlardan foydalanishga) kamaytirilsa, maxfiy ma'lumotlarni tarqatish mumkin bo'lgan xatoning nazariy chegarasi taxminan 11% ni tashkil etadi, ya'ni 1 - 2h(q) = 0 tenglamaning ildizi.

7.9. Tinglovchilar strategiyalari

BB84 protokoli maxfiyligining yuqorida keltirilgan dalili, qabul qiluvchi tomondan xatolikni 11% dan kam bo'lgan holda, maxfiy axborotni uzatish mumkinligini ta'kidlaydi. Shu bilan birga, protokolning maxfiyligini qanday katta

xato qiymati bilan yo'qotgani haqida gapirilmaydi. Bu qismda qabul qiluvchi tomonning nazariy xato chegarasi 11% ga yetkazilgan hujum sxemasi aniq ko'rsatilgan.

Boshqa nodalistik strategiyalar ham ko'rib chiqiladi va ularning har biri uchun muhim xato qiymati topiladi. Muhim natija: tinglashning eng keng tarqalgan usuli kollektiv hujum hisoblanadi: protokol sxemasida yengil o'zgarish bilan umumiy izga tushish interseptorga qo'shimcha qiymat bermaydi.

Qabul rejasini o'zgartirish

Yevaning xatti-harakatlari uchun eng sodda ssenariy - bu kvant kanaliga yuborilgan holatning o'lchovidir va undan keyin to'liq natijaga javob bermaslik. Shunday qilib, klassik kanallarni tinglash mumkin. Biz kvant holatida bunday strategiya ishlamayotganligini ko'rsatamiz. Ushbu bo'lim, Yeva ma'lumotlarini kelajakda amalga oshiriladiganidan ko'ra kamroq rasmiy tilda baholaydi, ammo u kvant kriptografiya protokollari barqarorligini tahlil qilishning asosiy g'oyalarini ko'rsatadi.Agar Yeva o'zining Bob ishlab chiqaradigan xuddi shunday harakatlarga erishmoqchi bo'lsa, unda dastlabki holatni bilmagan holda, u muqarrar ravishda holatlarni inertsional to`plamiga ajratib bo'lmaydigan muammosiga duchor qiladi. Shunday qilib, o'lchovlarning tasodifiy birida qo'llash mumkin

+ : $M_x = \{x\} M_y = \{y\}$,

x : $M_u = \{u\} M_v = |г>(и|$

yuborilgan ahvolga, taxminan yarim soatgaYeva noto'g'ri tasavvur qila oladi: «x» o'lchamini yuborilgan holatga (x) yoki | y) qo'llang yoki {+ rn), | z) holatiga nisbatan o'lchovni qo'llang ". Ko'rinib turibdiki, usul noto'g'ri taxmin qilingan asosga ega bo'lsa, Yeva xatosining ehtimoli 50% ni tashkil qiladi, ya'ni Yeva signal haqida foydali ma'lumot olmadi.

Shu bilan birga, bu Yevaning muammolari emas, chunki o'lchov uchun asosni noto'g'ri tasavvur qilgan Yeva, to'lqin funksiyasining qisqarishi xususiyati tufayli muqarrar ravishda Bobga noto'g'ri holat yuboradi.Shunday qilib, boshlang'ich holatdan qat'iy nazar, o'lchov yordamida "+" o'lchovidan foydalanib,), | y)} va "x" o'lchami shtatlarning biri | r}).

Bu hollarni ular uchun "to'g'ri" tarzda o'lchab, Bob xato qiladi, lekin Yevaning xatti-harakatlari aniqlanishi mumkin.

Sichqonning qabul qiluvchi tomonidagi xato qiymati quyidagicha hisoblanishi mumkin: Masalan, Yeva barcha holatlarga hujum qilmadi, biroq ulardan ba'zilari har bir signalga ehtimollik p bilan hujum qildi. Keyinchalik 1-p signallarining fraktsiyasi hech qanday xatosiz Bobga keladi (Yeva faqat har bir bunday binoning bit qiymatini bilishi kerak, shuning uchun uning xatosida (1-p) / 2 ga teng hissa beriladi, keyin Yeva tomonidan hujumga uchragan signallar uchun bir vaqtning o'zida ikkita teng imkoniyatga ega hodisalar mavjud:

• Yeva o'lchov asosini to'g'ri taxmin qildi va shuning uchun, bir tomondan, uzatilgan signal haqida aniq ma'lumot olgani va boshqa tomondan, hech qanday noqulaylikni keltirmadi.

• Yeva o'lchovlarni tanlash uchun xato tanladi. Keyin, 1/2 ehtimoli bilan, u noto'g'ri natijaga erishdi va juda aniq, u Bobning xato holatini uzatdi, bu uning tarafida xatolikka olib keladi, ehtimolligi ham 1/2. Ushbu ssenariylarning har birining ehtimoli p/2 va bu strategiya bilan qabul qiluvchi tomondagi xato darajasi p/4 bo'ladi va Yeva uchun xato darajasi

$$\frac{1-p}{2}+\frac{p}{2}=\frac{1}{2}-\frac{p}{4}$$

Bu parametr P ning barcha qiymatlari birlikdan kamligini bildiradi. Yeva Bobga qaraganda ko'proq xatoga yo'l qo'ydi, demak uning uzatilgan kalit haqidagi ma'lumoti juda kam. Shu bilan birga, p=1 bilan, Bob va Yeva xatoliklar ulushi to'g'ri keladi va 25% ga teng. Bobning xatosi parametr p bilan bevosita bog'liqligi sababli, 25% bunday maxfiy kalitni taqsimlash mumkin bo'lgan bunday hujum uchun chegara qiymati deb hisoblashimiz mumkin.

Shuni ta'kidlash kerakki, o'ng tomonda xatolik faqatgina Yevaning xatti-harakatlari bilan emas, balki kanal yoki detektorlarning g'oyaviyligi kabi sabablarga ham sabab bo'lishi mumkin. Biroq, protokolning barqarorligini baholashda, barcha xatolar to'xtatuvchi tomonidan yuzaga kelgan deb taxmin qilinadi: bu, albatta, eng yaxshi scenariydir.

Shunday qilib, qabul qiluvchi tomonidan bir muhim xato, mumkin bo'lgan maxfiy kalit tarqatishni - kvant protokollari kriptografiyasini asosiy xususiyati, umuman, u faqat protokolning o'zi bog'liq, lekin ayrim maxsus hollarda, hujumlar muayyan sinflar kodi ular uchun muhim xato hisoblashi mumkin. Protokol kvant kriptografik, yana muhim bir xato hisoblanadi: bu holatda aloqa kanali yaxshiroq mustahkam shovqinga va katta tezlik, katta masofalarga maxfiy kalit ishlash ega.

Shaffof individual tinglash

Shubhasiz, qabul qilish-o'tkazish strategiyasi Yeva nuqtai nazaridan maqbul emas – agar uning tanqidiy xato qiymati 11% nazariy chegaradan ancha katta bo'lsa. Ushbu bo'limda taklif etilgan shaffof hujum yaxshi natijalarga erishishga qodir.

Shaffof tinglashning mohiyati shundan iboratki, Yeva har posilkalardagi holatni to'g'ridan-to'g'ri efirga uzatish vaqtida emas, balki kanalda o'lchashga majbur emas, chunki o'sha paytda foydalanilgan asos hali ma'lum emas, chunki Yeva uchun har bir uzatish evolyutsiyasini o'z holati bilan oxirigacha tark etishi uchun foydalidir o'z-o'zidan umumiy, bog'langan, holatning bir qismi, qolganlari esa Bobga yuboriladi.Shuni eslatib o'tish joizki, umumiy ahvolda Bobning o'lchovi Yevaning qisman holatini aniqlaydi va uning asosini bilib olishi mumkin (u haqda ma'lumot ochiq kanalga uzatiladi), uning kichik tizimida o'lchashni amalga oshirishi mumkin. Natijada, Yeva uzatilgan holatlar haqida ko'proq ma'lumotga ega bo'ladi va kritik xato qiymati qabul-uzatish strategiyasidan kam bo'ladi.

VIII BOB. KALITLARNI ALMASHISH ALGORITMLARI

Kalitlarni almashish algoritmlari asosan ikki va undan ortiq tomonlarning himoyalanmagan kanalda ma’lumotlarni bir-biriga uzatishdan oldin simmetrik algoritmlar uchun shifrlash kalitlarini hosil qilish uchun ishlatiladi. Algoritmlar shifrlash va elektron raqamli imzo shakllantirish uchun qo‘llanilmaydi.

8.1. Diffi-Xelman algoritmi

Bu algoritm 1976-yilda Whitfield Diffie va Martin Hellmanlar tomonidan taklif etilgan. 2002-yilda Xelman bu algoritmni yaratishda Ralf Merklning hissasi katta ekanligini va nomlash lozim bo‘lsa Diffi-Xelman-Merkl deb nomlanishi kerakligini aytgan.

Algoritmni ikkita tomon uchun ko‘rib chiqaylik. 1-tomon A, 2-tomon B bo‘lsin. Himoyalanmagan kanal orqali ma’lumotlarni almashishdan oldin quyidagilar bajariladi: n - katta tub son tanlanadi, g - natural son tanlanadi, u n dan kichik va darajalari n moduli bo‘yicha qoldig‘i takrorlanuvchi siklga tushmaydigan son bo‘lishi kerak.

1. A tomon: v x < n bo‘lgan katta son tanlaydi va hisoblaydi: $A=g^x$ mod n va natijani B tomonga jo‘natadi. B tomon uni qabul qilib oladi.
2. B tomon: v y < n bo‘lgan katta son tanlaydi va quyidagi formula bo‘yicha $B=g^J$ mod n natijani hisoblab A tomonga jo‘natadi. A tomon uni qabul qilib oladi.
3. A tomon: B tomon jo‘natgan ma’lumotni o‘zining tanlagan soni x darajaga oshirib hisoblaydi va kalitni hosil qiladi: B^x mod n = g^ mod n - kalit.
4. B tomon: A tomon jo‘natgan ma’lumotni o‘zining tanlagan soni y darajaga oshirib hisoblaydi va kalitni hosil qiladi: A^y mod n = g m o d n - kalit.

Topilgan g m o d n qiymatdan kalit sifatida foydalaniladi. Algoritmdan tomonlar uchta va undan ko‘p bo‘lganda ham foydalanish mumkin.

8.2. Hughes algoritmi

Ikkita tomon uchun ko‘rib chiqaylik. 1-tomon A, 2-tomon B bo‘lsin. Himoyalanmagan kanal orqali ma’lumotlarni almashishdan oldin quyidagilar bajariladi: v n katta tub son tanlanadi. g soni g<n tengsizlikni qanoatlantiruvchi, darajalari modul n bo‘yicha siklga tushmaydigan qoldiqlar beruvchi qilib tanlab olinadi.

1. A tomon: v x <n bo‘lgan katta son tanlaydi va hisoblaydi: $A=g^x$ mod n va hech kimga jo‘natmaydi.
2. B tomon: v y <n bo‘lgan katta son tanlaydi va hisoblaydi: B=g * mod n va natijani A tomonga jo‘natadi.
3. A tomon: B^x mod n = A_x hisoblaydi va A_x ni B tomonga jo‘natadi.
4. B tomon: $z=y^1$ mod n ni hisoblaydi.

   A ^ mod n = B^{Iz} mod n = g mod n=g^x mod n - ushbu almashinuvchi kalit hisoblanadi.

   Ushbu algoritmdan foydalanib, tomonlar soni uchta yoki undan ko‘p bo‘lgan hollarda ham amalga oshirish mumkin.

Bu algoritmning Diffi-Xelman algoritmiga nisbatan qulaylik tomonlari maxfiylikning yanada ortishida va bajariladigan amallar sonnining kamayganida ham ko‘rish mumkin. Bundan tashqari kalitlarni almashish algoritmi tomonlar sonining qanchalik ortishi bilan kalitning maxfiylik darajasi ham shunchaga ortishi ko‘plab tizimlardagilarga ma’qul tushgan. Ushbu algoritmdan hozirda ko‘plab soha tizimlarida foydalanib kelinmoqda.

IX BOB. ELEKTRON RAQAMLI IMZO

Keyingi yillarda elektron tijorat jahon bo‘ylab jadal rivojlanmoqda. Tabiiyki, bu jarayon moliya-kredit tashkilotlari a’zoligida amalga oshiriladi. Savdoning bu turi ommalashib bormoqda. Xorijlik yetakchi mutaxassislar fikriga ko‘ra elektron tijorat jarayonining rivojlanishi asosan axborot xavfsizligi sohasidagi taraqqiyot bilan belgilanadi. Axborot xavfsizligi - axborot egasi va undan foydalanuvchining moddiy va ma’naviy zarar ko‘rishiga sabab bo‘luvchi ma’lumotning yo‘qotilishini, buzilishini, ochilish imkoniyatini yo‘q qiluvchi, tasodifiy va atayin uyushtirilgan ta’sirlarga axborotning bardoshliligidir. Axborot xavfsizligiga erishishda bazis vazifalar - axborotni konfedensialligi, to‘liqligi, unga erkin kirish yo‘li va huquqiy ahamiyatini ta’minlashdir.

Huquqiy ahamiyatga ega bo‘lgan elektron hujjat almashinuvi (EHA) bugungi kunda munozarali mavzu darajasidan real xizmat turiga aylandi. Bu xizmatga talab fond bozorida elektron savdoning rivojlanishi bilan kundan-kunga oshib bormoqda.

“Internet orqali savdo”ni amalga oshirish avval amal qilgan tizimdan butunlay farq qiladi. Avvaldagi kabi maxsus aloqa kanali orqali savdo tizimiga kirish huquqiga xuddi o‘sha savdo qatnashchisining o‘zi javob beradi. Biroq treyder mijozning “qog‘oz” talabnomalarini savdo terminaliga o‘z qo‘li bilan kiritish imkoniyatidan tashqari, mijozlarda “shlyuz” dasturi orqali talabnomalarni shaxsan o‘zlari to‘ldirgan elektron va kompyuter tizimlari orqali yo‘naltirgan shakllarini savdo tizimiga yuborish imkoniyati tug‘ildi. Elektron talabnomalarni qayta ishlash jadalligi ularni birma-bir qo‘lda tekshirishdan ming marotaba tezroq amalga oshadi. Bunday talabnomalar tayyorlanadi va kirish nazoratiga maxsus dasturiy ta’minot orqali o‘tkaziladi. Nazoratning muhim bosqichlaridan biri talabnomaning aslligi va muallifligini tekshirilishdadir. Ya’ni, talabnoma matni yuboruvchidan qabul qiluvchiga kompyuter tizimi orqali yetkazib berish jarayonida buzilmaganligini va aynan uni yuborgan shaxs (firma) nomidan kelganligi aniqlanadi. Endilikda hujjat kuryer tomonidan disketada yoki Internet tarmog‘ining ochiq kanallari orqali kelganmi - bu muhim rol o‘ynamaydi.

Tekshirish jarayoni shunday ishonchli bo‘lishi kerakki, sudda ishni ko‘rish holatida sudya bahsli masalani hal qilishda tekshiruv natijalaridan foydalanishga rozi bo‘lishi kerak.

An’anaviy imzodan farqli ravishda elektron raqamli imzo (ERI) shaxs bilan emas, hujjat va yopiq kalit bilan bog‘liq. Agar sizning ERI saqlagan disketangizni kimdir topib olsa, tabiiy u sizni o‘rningizga imzo qo‘yishi mumkin. Lekin imzoni oddiy imzo kabi bir hujjatdan ikkinchisiga o‘tkazish imkoniyati yo‘q. Har bir hujjat uchun u takrorlanmasdir. Shu yo‘l bilan ERI bilan imzolangan hujjatni qabul qiluvchi shaxs berilgan hujjatni matni va muallifligi o‘zgartirilmaganligi bilan kafolatlanadi.

Respublikamizda internet biznes rivojlanish bosqichidagi istiqbolli, yangi tijorat faoliyatidir. Bu yo‘nalishda biz ham birinchi qadamni tashladik va bizni ham jiddiy axborot xavfsizligi muammolari kutyapti. Tahlillarga ko‘ra O‘zbekistonda elektron tijoratning shiddat bilan o‘sishi ERI ning online operatsiyalarda rasmiy ravishda keng qo‘llanilishi bilan boshlanadi.

O‘zbekistonda elektron biznes uchun yetarli sharoitlar, imkoniyatlar bor, faqat ular ustida tadqiqotlar olib borib, kamchiliklar, muammolarni bartaraf etish bilan takomillashgan xavfsiz, ishonchli virtual savdo maydonini yaratish mumkin. ERI va axborot xavfsizligi sohasida xalqaro standartlarni ishlab chiqish va ularni tan olish yanada faol va raqobatbardosh, ishonchli ERI vositalarini xalqaro axborot hamkorlik sohalarida joriy etishga imkon tug‘diradi.

ERI dan foydalanishning afzalliklarini IT- kompaniyalariga, axborot almashinuv bilan shug‘ullanadigan tashkilot, davlat va nodavlat muassasalari mutasaddilariga tushuntirilib, targ‘ibot ishlarini olib borish kutilgan natijani beradi. Amaldagi qonunlar esa xavfsiz elektron hujjat almashinuvini ta’minlab, xalqaro doirada istiqbolli, o‘zaro manfaatli shartnomalarni tuzish, tovar va xizmatlarni virtual olamda ishonch bilan keng ko‘lamda taqdim etish imkoniyatini beradi.

Elektron raqamli imzo quyidagi hususiyatlarga ega:

1. Axborotni shifrlamasdan ochiq holatda qoldiradi.
2. Imzoni tekshirish imkoniyati kafolatlanadi.

3. Imzo sifatida sonlar juftligi keltiriladi.

9.1. DSA (Digital Signature Algorithm) elektron raqamli imzo algoritmi

Bu algoritm AQSHning standart algoritmi hisoblanadi. Bu algoritmni 1991 yili AQSHning NIST (National Institut Standart and Tekhnology) kompaniyasi U.S.Patent 5231668 patenti bilan ishlab chiqqan. Aslida NSA yaratuvchisi hisoblanadi. Ushbu algoritm ma'lumotni shifrlash uchun emas, balki elektron raqamli imzo yaratishda qo'llaniladi. Ushbu algoritm SHA-1 xesh funksiyasi bilan birgalikda DSS (Digital Signature Standard) ning qismi hisoblanadi. DSS versiyasida SHA-1 xesh funksiyasi 160 bitli uzunlik taklif etilgan. Lekin hozirgi kunda SHA-1 algoritmi yetarlicha mustahkam emas. Ushbu versiyada foydalanilayotgan tub sonlarning uzunliklari quyidagi L va N juftliklarida keltirilgan:

L = 1024, N = 160, L = 2048, N = 224,

L =2048, N = 256, L =3072, N =256.

Albatta bular bilan birgalikda SHA-2 xesh funksiyasi ham taklif etilgan. Yuqori tashkilotlar bulardan birini tanlashi lozim, lekin ular ixtiyoriy tanlashlari mumkin. Tizimni loyihalashda ixtiyoriy xesh-funksiyani tanlasa bo'ladi. DSA algoritmining mustahkamligi xesh- funksiyaning mustahkamligi va L,N juftliklarining mustahkamligini ta'minlab bermaydi. Avvalari L ning uzunligi 1024 bit bo'lgan bo'lsa, hozirgi kunda tizimlarning mustahkamligi uchun 2011 yildan 2030 yilgacha L ning uzunligi 2048-3072 bitgacha taklif etilmoqda.

DSA algoritmi:

1. p - katta tub son tanlanadi. Uzunligi 512-1024 bitgacha va uzunligi 64 ga karrali.
2. q-tub son tanlanadi, uzunligi 160 bit va (p-1) ning bo'luvchisi, ya'ni (p-1)/q € N.
3. Quyidagi tengsizlikni qanoatlantiruvchi h-natural son tanlanadi:
   $h < q$, $h^{p-1/q} \bmod p > 1$.
4. g-hisoblanadi: $g = h^{(p-1)/q} \bmod p$.
5. Uzunligi 160 bit bo'lgan q dan kichik ixtiyoriy natural son x tanlanadi va u yopiq

kalit hisoblanadi.

6. Ochiq kalit quyidagi formula yordamida hisoblanadi: $y = g^x \bmod p$, uning uzunligi 512-1024 bitgacha.

(p, q, g, y) - ochiq parametrlar hisoblanadi, faqatgina x yopiq parametr hisoblanadi. (p, q, g) barcha foydalanuvchi guruhlar uchun ochiq bo‘lishi mumkin, x va y esa yopiq bo‘ladi. Ma’lumotni imzolashda maxfiy son x va k dan foydalaniladi. Bu yerda k ixtiyoriy tanlanadi.

Imzo qo’yish:

7. $k < q$ - tasodifiy son tanlanadi.
8. $a=(g^k \bmod p) \bmod q$ - birinchi imzo
9. $b=(k^{-1}(H(m)+x \cdot a)) \bmod q$ - ikkinchi imzo, bu yerda H(m) – xesh qiymat.
10. (a,b) sonlar juftligi imzo hisoblanadi. M, (a,b) - ikkinchi tomonga yuboriladi.

Imzoni tekshirish:

11. $W=b^{-1} \bmod q$ hisoblanadi.
12. $U1=(H(m)W) \bmod q$ hisoblanadi.
13. $U2=(aW) \bmod q$ hisoblanadi.
14. $v=(g^{u1}y^{u2} \bmod p) \bmod q$ hisoblanadi. Agar v = a bo‘lsa imzo to‘gri qo‘yilgan bo‘ladi.

9.2. GOST R 34.10-94 elektron raqamli imzo algoritmi

2000 yilgacha Rossiya standarti hisoblangan GOST R 34.10-94 ERI algoritmi DSA algoritmiga o‘xshash va quyidagi boshlang‘ich ochiq parametrlardan foydalanadi:

1. Uzunligi L bo‘lgan katta p tub son tanlanadi, bu yerda L son 509 bitdan 512 bitgacha yoki 1020 bitdan 1024 bitgacha oraliqdan tanlanadi.

2. Uzunligi L1 bo‘lgan katta q tub son tanlanadi, bu yerda L1 son 254 bitdan 256 bitgacha oraliqdan tanlanadi.

3. $a^q \bmod p=1$ shartni qanoatlantiruvchi $0<a<p-1$ oraliqdagi a son tanlanadi.

4. $y=a^x \bmod p$ formuladan y ochiq kalit hisoblanadi, bu yerda $0<x<q$ oraliqdan olingan x - yopiq kalit.

5. H(M) - xesh-funksiya berilgan M ma’lumot bo‘yicha hisoblangan butun

son bo‘lib, 1 dan q gacha oraliqdagi qiymatlarni qabul qiladi, ya’ni 1 <H(M)<q.

Imzo qo’yish:

6. 1<k<q intervaldan tasodifiy k soni olinadi, u maxfiy saqlanadi va imzo qo‘yilgandan keyin darhol yo‘qotiladi.

7. r=(a^k modp) mod q hisoblanadi.

Jo‘natilayotgan M ma’lumotning H(M) - xesh qiymati hisoblanadi. Agar r=0 yoki H(M)modq=0 bo‘lsa, u holda 6- qadamga o‘tilib, boshqa k tanlanadi.

8. s=(x r+k H(M))modq hisoblanadi, bu yerda yopiq kalit x faqat imzo qo‘yuvchining o‘zigagina ma’lum. Agar s=0 bo‘lsa, u holda 6-qadamga boriladi. M xabar imzosi - (r,s) juftligidan iborat.

Imzoni tekshirish:

9. Agar 1<r,s<n-1 shart bajarilmasa, u holda imzo qalbaki va imzoni tekshirish to‘xtatiladi. Bu shartlar bajarilsa keyingi qadamga o‘tiladi.

10. w = H^{q-2}(M) modq hisoblanadi.

11. u1= (sw) modq hisoblanadi.

12. u2 = ((q-r)w) modq hisoblanadi.

13. u = ($a^{u1}y^{u2}$modp)modq hisoblanadi. Agar u=r shart bajarilsa, u holda imzo haqiqiy, aks holda imzo qalbaki va imzoni tekshirish to‘xtatiladi.

9.3. Elgamal elektron raqamli imzo algoritmi

1. p katta tub son tanlanadi. M xabarning o‘nlik formasi p dan kichik bo‘lishi kerak, aks holda M bloklarga ajratiladi.
2. g < p bo‘lgan tasodifiy son tanlanadi.
3. x < p bo‘lgan ixtiyoriy son tanlanadi, x - yopiq kalit.
4. Quyidagi tenglik hisoblanadi: y = g^x mod p.

Imzo qo’yish:

5. p – 1 dan kichik bo‘lgan va p – 1 bilan o‘zaro tub bo‘lgan k - tasodifiy son tanlanadi.
6. a = g^k mod p hisoblanadi.
7. b =((M - a·x) · k^{-1}) mod (p - 1) hisoblanadi.

(a ,b) sonlar juftligi raqamli imzo hisoblanadi.

Imzoni tekshirish:

8. $(y^a \cdot a^b) \bmod p = g^M \bmod p$ tenglik o‘rinli bo‘lsa, imzo to‘g‘ri bo‘ladi, aks holda soxtalashtirilgan hisoblanadi.

9.4. Feige-Fiat-Shamir identifikatsiya sxemasi

Kompyuter tizimida ro‘yxatga olingan har bir subyekt (foydalanuvchi yoki foydalanuvchi nomidan harakatlanuvchi jarayon) bilan uni bir ma’noda indentifikatsiyalovchi axborotga bog‘liq bo‘ladi.

Bu mazkur subyektga nom beruvchi son yoki simvollar satri bo‘lishi mumkin. Bu axborot subyekti *indentifikatori,* deb yuritiladi. Agar foydalanuvchi tarmoqda ro‘yxatga olingan indentifikatorga ega bo‘lsa u legal (qonuniy), aks holda nolegal (noqonuniy) foydalanuvchi hisoblanadi. Kompyuter resurslaridan foydalanishdan avval foydalanuvchi kompyuter tizimining identifikatsiya va autentifikatsiya jarayonidan o‘tishi lozim.

Identifikatsiya (Identification) - foydalanuvchini uning identifikatori (nomi) bo‘yicha aniqlash jarayoni. Bu foydalanuvchi tarmoqdan foydalanishga uringanida birinchi galda bajariladigan ishdir. Foydalanuvchi tizimga uning so‘rovi bo‘yicha o‘zining identifikatorini bildiradi, tizim esa o‘zining ma’lumotlar bazasida uning borligini tekshiradi.

Autentifikatsiya (Authentication) — ma’lum qilingan foydalanuvchi, jarayon yoki qurilmaning haqiqiy ekanligini tekshirish muolajasi. Bu tekshirish foydalanuvchi (jarayon yoki qurilma) haqiqatan aynan o‘zi ekanligiga ishonch hosil qilinishiga imkon beradi. Autentifikatsiya o‘tkazishda tekshiruvchi taraf tekshiriluvchi tarafning haqiqiy ekanligiga ishonch hosil qilishi bilan bir qatorda tekshiriluvchi taraf ham axborot almashinuv jarayonida faol qatnashadi. Odatda foydalanuvchi tizimga o‘z xususidagi noyob, boshqalarga ma’lum bo‘lmagan axborotni (masalan, parol yoki sertifikat) kiritishi orqali identifikatsiyani tasdiqlaydi.

Identifikatsiya va autentifikatsiya subyektlarning (foydalanuvchilarning)

haqiqiy ekanligini aniqlash va tekshirishning o‘zaro bog‘langan jarayonidir. Muayyan foydalanuvchi yoki jarayonning tizim resurslaridan foydalanishiga tizimning ruxsati aynan shularga bog‘liq. Subyektni identifikatsiyalash va autentifikatsiyalashdan so‘ng uni avtorizatsiyalash boshlanadi.

Avtorizatsiya (Authorization) - subyektga tizimda ma’lum vakolat va resurslarni berish muolajasi, ya’ni avtorizatsiya subyekt harakati doirasini va u foydalanadigan resurslarni belgilaydi. Agar tizim avtorizatsiyalangan shaxsni avtorizatsiyalanmagan shaxsdan ishonchli tarzda ajrata olmasa, bu tizimda axborotning konfidensialligi va yaxlitligi buzilishi mumkin. Autentifikatsiya va avtorizatsiya muolajalari bilan foydalanuvchi harakatini ma’murlash muolajasi uzviy bog‘langan.

Ma ’murlash (Accounting) - foydalanuvchining tarmoqdagi

harakatini, shu jumladan, uning resurslardan foydalanishga urinishini qayd etish. Ushbu hisobot axboroti xavfsizlik nuqtai nazaridan tarmoqdagi xavfsizlik hodisalarini oshkor qilish, taxlillash va ularga mos reaksiya ko‘rsatish uchun juda muhimdir.

Ma’lumotlarni uzatish kanallarini himoyalashda *subyektlarning O’zaro autentifikatsiyasi*, ya’ni aloqa kanallari orqali bog‘lanadigan subyektlar haqiqiyligining o‘zaro tasdig‘i bajarilishi shart. Haqiqiylikning tasdig‘i odatda seans boshida, abonentlarning bir-biriga ulanish jarayonida amalga oshiriladi. “Ulash” atamasi orqali tarmoqning ikkita subyekti o‘rtasida mantiqiy bog‘lanish tushuniladi. Ushbu muolajaning maqsadi ulash qonuniy subyekt bilan amalga oshirilganligiga va barcha axborot mo‘ljallangan manzilga borishligiga ishonchni ta’minlashdir.

O‘zining haqiqiyligining tasdiqlash uchun subyekt tizimga turli asoslarni ko‘rsatishi mumkin. Subyekt ko‘rsatadigan asoslarga bog‘liq holda autentifikatsiya jarayonlari quyidagi kategoriyalarga bo‘linishi mumkin:

- *biror narsani bilish asosida.* Misol sifatida parol, shaxsiy identifikatsiya kodi PIN (Personal Identification Number) hamda “so‘rov- javob” xilidagi protokollarda namoyish etiluvchi maxfiy va ochiq kalitlarni ko‘rsatish mumkin;

- *biror narsaga egaligi asosida.* Odatda bular magnit kartalar, smart-kartalar, sertifikatlar va xotira qurilmalari;

- *qandaydir daxlsiz tavsiflar asosida.* Ushbu kategoriya o‘z tarkibiga foydalanuvchining biometrik tavsiflariga (ovozlar, ko‘zining rangdor pardasi va to‘r pardasi, barmoq izlari, kaft geometriyasi va x.k.) asoslangan usullarni o‘z ichiga oladi. Bu kategoriyada kriptografik usullar va vositalar ishlatilmaydi. Biometrik tavsiflar binodan yoki qandaydir texnikadan foydalanishni nazoratlashda ishlatiladi.

Parol — foydalanuvchi hamda uning axborot almashinuvidagi sherigi biladigan narsa. O‘zaro autentifikatsiya uchun foydalanuvchi va uning sherigi o‘rtasida parol almashinishi mumkin. Plastik karta va smart - karta egasini autentifikatsiyasida shaxsiy identifikatsiya nomeri PIN sinalgan usul hisoblanadi. PIN — kodning maxfiy qiymati faqat karta egasiga ma’lum bo‘lishi shart.

Dinamik (bir martalik) parol - bir marta ishlatilganidan so‘ng boshqa umuman ishlatilmaydigan parol. Amalda odatda doimiy parolga yoki tayanch iboroga asoslanuvchi muntazam o‘zgarib turuvchi qiymat ishlatiladi.

“So‘rov-javob” tizimi - taraflarning biri noyob va oldindan bilib bo‘lmaydigan “so‘rov” qiymatini ikkinchi tarafga jo‘natish orqali. autentifikatsiyani boshlab beradi, ikkinchi taraf esa so‘rov va sir yordamida hisoblangan javobni jo‘natadi. Ikkala tarafga bitta sir ma’lum bo‘lgani sababli, birinchi taraf ikkinchi taraf javobini to‘g‘riligini tekshirishi mumkin.

Sertifikatlar va raqamli imzolar - agar autentifikatsiya uchun sertifikatlar ishlatilsa, bu sertifikatlarda raqamli imzoning ishlatilishi talab etiladi. Sertifikatlar foydalanuvchi tashkilotining mas’ul shaxsi, sertifikatlar serveri yoki tashqi ishonchli tashkilot tomonidan beriladi. Internet doirasida ochiq kalit sertifikatlarini tarqatish uchun ochiq kalitlarni boshqaruvchi qator tijorat infratuzilmalari PKI (Public Key Infrastrusture) paydo bo‘ldi. Foydalanuvchilar turli darajali sertifikatlarini olishlari mumkin. Autentifikatsiya jaryonlarini ta’minlanuvchi xavfsizlik darajasi bo‘yicha ham turkumlash mumkin. Ushbu yondashishga binoan autentifikatsiya jarayonlari quyidagi turlarga bo‘linadi:

- parollar va raqamli sertifikatlardan foydalanuvchi autentifikatsiya;
- kriptografik usullar va vositalar asosidagi qat’iy autentifikatsiya;
- foydalanuvchilarning biometrik autentifikatsiyasi.

Xavfsizlik nuqtai nazaridan yuqorida keltirilganlarning har biri o‘ziga xos masalalarni yechishga imkon beradi. Shu sababli autentifikatsiya jarayonlari va protokollari amalda faol ishlatiladi.

Feige-Fiat-Shamir identifikatsiya sxemasi 1986 yilda U.Feyge, A.Fiat va A.Shamirlar tomonidan taklif etilgan. Bu sxemada ikkita tomon ishtirok etadi. Tomonlarning har biri n=p*q, p va q lar katta tub sonlarni oldindan bilishi shart, boshqa hech kim p va q larni bilmasliklari kerak. Protokol boshlanishidan oldin quyidagilar hisoblanishi kerak: x modn=v tenglikdan barcha v lar topiladi. Bunda x natural son bo‘lib, 1 dan n/2 gacha o‘zgaradi. Topilgan v larning n bilan o‘zaro tub bo‘lganlari ajratib olinadi va v^{-1}modn hisoblanadi. s=sqrt(v^{-1})modn tenglik orqali ochiq kalit hisoblanadi va e’lon qilinadi.

1. A tomon: tasodifiy r < n-1 natural son tanlaydi va hisoblaydi: y=r modn va y qiymatni B tomonga jo‘natadi.
2. B tomon: ixtiyoriy b bit tanlaydi va uni A tomonga jo‘natadi.
3. A tomon: B tomon jo‘natgan bit 0 ga teng bo‘lsa, r qiymatni B tomonga jo‘natadi. Agar B tomon jo‘natgan bit 1 ga teng bo‘lsa, z=r*s modn qiymatni B tomonga jo‘natadi.
4. B tomon: A tomonga 0 ni jo‘natgan bo‘lsa, r^2modn=y tenglikni tekshiradi, aks holda (z *v) modn=y tenglikni tekshiradi. Tenglik bajarilsa B tomon A tomon ekanligiga ishonch hosil qilguncha shu 4 ta bosqichni bir necha marta takrorlaydi.

Bu 4 ta bosqich protokolning bitta sikli bo‘lib, akkreditatsiya deyiladi. Har bir siklda aldanish ehtimolligi 50% ni tashkil etadi. Sikl 10 marta takrorlansa, aldanish ehtimolligi 0,1% ni tashkil etadi.

Bu sxemani yanada umumiyroq qilib yozish mumkin:

1. A tomon: tasodifiy r < n-1 natural son tanlaydi va hisoblaydi: y=r modn va y qiymatni B tomonga jo‘natadi.
2. B tomon: ixtiyoriy b (i=1,..,k) bitlarni tanlaydi va ularni A tomonga jo‘natadi.
3. A tomon: z= $r \prod_{i=1}^{k} S_i^{b_i} modn$ qiymatni B tomonga jo‘natadi.

4. B tomon $z^2 \prod_{i=1}^{k} v_i^{b_i} modn = y$ tenglikni tekshiradi. Tenglik bajarilsa B tomon A tomon ekanligiga ishonch hosil qilguncha shu 4 ta bosqichni bir necha marta takrorlaydi.

Har bir siklda aldanish ehtimolligi $(1/2)^k$ ni tashkil etadi. k=10 bo‘lsa va sikl bir marta takrorlansa, aldanish ehtimolligi 0,1% ni tashkil etadi.

9.5. Bir nechta kalit algoritmlar

Bir necha kalitli algoritmlarning ishlash prinsiplari RSA algoritmiga o‘xshab ketadi. Ikkita katta tub sonlar ko‘paytuvchisi bo‘lgan n soni tanlanadi. RSA algoritmdagi e,d sonlari o‘rniga k_i (i=1,.., t, t € N) sonlar tanlanadi:

$(k_1 \cdot k_2 \cdot \ldots \cdot k_t)$ mod ((p-1)(q-1))=1.

Bu algoritmlardan shifrlashda va raqamli imzo qo‘yishda foydalanish mumkin. Masalan, t=7 bo‘lganda, k_1 , k_2 , k_3 kalitlar shifrlash uchun, k_4 , k_5 , k_6 , k_7 kalitlar shifrni ochish uchun ishlatilishi mumkin. Raqamli imzoda k_1, kalitni bir kishiga, k_2, k_3 kalitlarni boshqasiga, qolgan kalitlarni ochiq, deb e’lon qilish mumkin.

Shifrlash: $C = M^{k_1 \cdot k_2 \cdot k_3} \text{mod } n$ formula orqali bajariladi.

Shifrni ochish: $M = C^{k_4 \cdot k_5 \cdot k_6} \text{ mod } n$ formula orqali bajariladi.

Imzo qo’yish: M xabarga imzo qo‘yishdan oldin k_1, k_2 kalitlarning egasi o‘qib chiqadi va tasdiqlash uchun imzo qo‘yadi: C= $M^{k_1} modn$. Imzo qo‘yilgan xabar ikkinchi kishiga beriladi va u o‘z kalitlari, ochiq deb e’lon qilingan kalitlardan foydalanib, M xabarni ochadi va o‘qib ko‘radi: $C_1 = M^{k_1} modn$, hammasi to‘g‘ri bo‘lsa, tasdiqlash uchun imzo qo‘yadi: $M = C_1^{k_2 k_3 k_4 k_5 k_6 k_7} modn$ hammasi to’g’ri bo’lsa, tasdiqlash uchun imzo qo’yiladi: $C_2 = C_1^{k_2 k_3} modn$

Raqamli imzo ichiga yashirin xabarni joylashtirib jo‘natish usuli *yashirin kanal* deyiladi. Bu usulni 1984 yilda Gustavus Simmons taklif etgan. U bir nechta raqamli imzo algoritmlari ichiga yashirin xabarlarni joylashtirish mumkinligini ko‘rsatgan. Shulardan biri Elgamal algoritmidir:

1. p katta tub son tanlanadi.
2. p dan kichik bo‘lgan g va r tasodifiy sonlar tanlanadi.
3. $K = g^r \bmod p$ hisoblanadi.

Bu yerda K, g, p sonlar ochiq kalit, r yopiq kalit. Yopiq kalit ikkala tomonda ham bo‘lishi kerak. Bu kalit faqat imzo qo‘yish uchun emas, balki yashirin xabarni o‘qish uchun ham kerak bo‘ladi. M - yashirin xabar, M’ - ochiq xabar bo‘lsin. Bunda M, M’ lar p sonidan kichik bo‘lishi lozim, bundan tashqari M va p-1 o‘zaro tub bo‘lishi kerak.

4. $X = g^M \bmod p$, $Y = (M^{-1} (M'-rX)) \bmod (p-1)$ – birinchi tomon hisoblaydi.
5. (X,Y) imzo va M’ xabarni ikkinchi tomonga jo‘natadi.
   Nazoratchi imzoni tekshirib ko‘rishi mumkin: $(K^X X^Y) \bmod p = g^{M'} \bmod p$
   tenglik to‘g‘ri bo‘lsa, imzo to‘g‘ri va u o‘tkazib yuboradi.
6. Ikkinchi tomon ham (X,Y) imzo va M’ xabar yetib kelgandan keyin birinchi navbatda imzo to‘g‘riligini tekshiradi:
   $(K^X X^Y) \bmod p = g^{M'} \bmod p$.
7. Nazoratchi o’zgartirmaganligiga ishonch hosil qilgach M xabarni tiklaydi:
   $M=(Y^{-1}(M' - rX)) \bmod (p - 1)$

XULOSA

Axborot texnologiyalarining hozirgi zamon taraqqiyoti hamda yutuqlari fan va inson faoliyatining barcha sohalarini axborotlashtirish zarurligini taqozo etmoqda. Chunki aynan mana shu narsa butun jamiyatning axborotlashtirilishi uchun asos va muhim zamin bo‘ladi. Jamiyatni axborotlashtirish respublikamiz xalqi turmush darajasining yaxshilanishiga, ijtimoiy ehtiyojlarning qondirlishiga, iqtisodning o‘sishi hamda fan-texnika taraqqiyotining jadallashishiga xizmat qiladi.

Axborotlarni himoya qilish hozirgi davrning asosiy muammolaridan biri hisoblanadi. XX asrning oxirlaridan boshlab barcha turdagi axborotlar qog‘ozdan elektron ko‘rinishga o‘tkazildi. Hozirgi kunda elektron ko‘rinishdagi axborotlar har xil buzg‘unchilar, xakerlar tomonidan hujumga uchramoqda. Global kompyuter tarmoqlari paydo bo‘lgandan keyin axborotlarni himoya qilish yanada qiyinlashdi. Endilikda tarmoq orqali yuqori darajada himoyalanmagan tizimlarni buzib kirish yoki ishdan chiqarish ham mumkin bo‘lib qoldi. Tizim xavfsizligini ta’minlash uchun bu muammolarga kompleks tarzda yondashish kerak.

Hozirgi paytda kriptografik metod va vositalar nafaqat davlat, balki tashkilotlar va oddiy shaxslarning axborot xavfsizligini ta’minlash uchun qo‘llanilmoqda. Rivojlangan davlatlarda shu sohaga oid standartlar qabul qilingan. 2003 yil sentabr va dekabr oylarida respublikamizda elektron raqamli imzo haqida qonunlar qabul qilindi, 2005 yilda shifrlash algoritmi va 2009 yilda raqamli imzo algoritmi davlat standarti tasdiqlandi.

Ushbu o‘quv qo‘llanma “Amaliy matematika va informatika”, “Informatika va axborot texnologiyalari”, “Axborot xavfsizligi”, “Axborot tizimlarining matematik va dasturiy ta’minoti”, “Kriptografiya va kriptotahlil” yo‘nalishlarida ta’lim olayotgan oliy o‘quv yurtlari talabalari va kriptografiyaga qiziquvchilarga axborotlarni himoya qilish sohasi haqida tasavvur va bilim berishda yordam bersa, biz maqsadimizga yetgan bo‘lamiz.

GLOSSARIY

AddRoundKey – raund kalitlarini qo‘shish, ya’ni bloklar mos bitlarni XOR amali bilan qo‘shish.

AES – Advanced Encryption Standard – Shifrlashning yaxshilangan standarti. DES ni almashtirish uchun, AQSH hukumati tomonidan tasdiqlangan shifrlash standarti.

Affin tizimi – Affin tizimidagi Sezar usulida har bir harfga almashtiriluvchi harflar maxsus formula bo‘yicha aniqlanadi.

Alfavit – axborotlarni kodlashtirish uchun foydalaniladigan chekli sondagi belgilar to‘plami.

Autentifikatsiya – ingl.: authentication rus.: аутентификация 1. Obyektning e’lon qilingan bir xilligini tekshirish jarayoni. 2. Subyekt taqdim etgan aynanlovchi (identifikator) unga tegishliligini tekshirish; haqiqiyligini tekshirish. 3. Foydalanuvchining tizimdan erkin foydalanish uchun kiritgan qayd etilgan axborotining to‘g‘riligini tekshirish tartibi. Autentifikatsiya resurslardan erkin foydalanish huquqlari va tizimda amallarni bajarish huquqlarini majburan cheklash uchun qo‘llaniladi."

Avtorizatsiya – (Authorization) - subyektga tizimda ma’lum vakolat va resurslarni berish muolajasi, ya’ni avtorizatsiya subyekt harakati doirasini va u foydalanadigan resurslarni belgilaydi.

Axborot – axborot ingl.: information rus.: информация

Axborot butunligi – ingl.: information integrity rus.: целостность информации

1. Axborot va uni tashuvchining holati. Butunlay axborot va uning alohida tarkibiy qismlari bo‘linmasligini ta’minlash hamda ularni ruxsatsiz qasddan yo‘q qilish, buzib talqin qilish, sizib chiqib ketish, o‘g‘irlash, axborot butunligi qalbakilashtirish va almashtirib qo‘yishni, oldindan bartaraf qilishni nazarda tutiladi. 2. Hisoblash texnikasining yoki avtomatlashtirilgan tizimning tasodifiy va (yoki) qasddan qilingan g‘alati qilib qo‘yish (barbod qilish) sharoitida, axborotning o‘zgarmay qolishini ta’minlash qobiliyati. Axborot butunligini ta’minlash uchun uch uslubdan foydalaniladi: - yopiq kanallarni yaratish; - yo‘naltirilishni kuzatib

borish; ma’lumotlardan erkin foydalanishni boshqarish. Butunlik kriptografiya yordamida ham ta’minlanishi mumkin. Bundan tashqari boshqa usullar ham mavjud. Masalan, chop etilgan ma’lumotlarga elektron imzo qo‘shib qo‘yish, ma’lumotlarni takrorlash, nazorat qiymatini qo‘shib qo‘yish."

Axborot egasi – ingl.: information owner rus.: владелец информации 1. Qonun va/yoki axborot egasi tomonidan belgilangan huquqlar doirasida axborotga ega bo‘lgan va undan foydalanayotgan hamda foydalanish vakolatlarini amalga oshirayotgan subyekt. 2. Axborot uzatishni va tarqatishni, yaratilgan axborotni iste’molchiga eltib berishni ta’minlaydigan alohida huquqlarni qo‘lga kiritgan shaxs yoki shaxslar. 3. Axborot ishlab chiqaruvchilari va iste’molchilari orasidagi vositachi.

Axborot ishonchliligi – ingl.: information validity rus.: достоверность информации Axborotning to‘g‘ri qabul qilinish xususiyati. U quyidagilar yordamida ta’minlanadi: uzatilayotgan xabarlarda voqealar ro‘y berish vaqtining belgilanishi; turli manbalardan olingan ma’lumotlarning puxta o‘rganilishi va taqqoslanishi; soxta informatsiyaning vaqtida fosh etilishi; buzilgan axborotning o‘chirilishi va h.k.

Axborot iste’molchisi – ingl.: information consumer rus.: потребитель информации O‘z ehtiyojlarini qondirish (bilimlarni oshirish, ta’lim olish, qarorlarni qabul qilish va h.k.) maqsadida axborotga muhtoj, uni izlovchi va oluvchi shaxs yoki shaxslar.

Axborot izlash tizimi – ingl.: information retrieval system rus.: информационно-поисковая система Ma’lumotlar bazasi va jami axborot resurslarida axborot izlash uchun mo‘ljallangan tizim.

Axborot mazmuni – ingl.: information content rus.: содержание информации Ma’lum obyekt yoki hodisa to‘g‘risida jami elementlar, tomonlar, ular o‘rtasidagi aloqa va munosabatlarni belgilovchi aniq ma’lumotlar."

Axborot muhiti – ingl.: information environment rus.: информационная среда Kompyuterda saqlanuvchi, biroq axborot tizimi sifatida shakllantirilmagan,

ma’lum predmet sohasiga tegishli va bitta yoki bir necha foydalanuvchi tomonidan ishlatiladigan jami bilimlar, faktlar va ma’lumotlar.

Axborot o‘chirilishi – ingl.: information destruction rus.: разрушение информации Kompyuterning xotirasida saqlanayotgan axborotni o‘chirish.

Axborot olishning osonligi – ingl.: information accessibility rus.: доступность информации axborot muhofazasining. Axborotning (erkin) olinish xususiyati.

Axborot qadrsizlanishi – ingl.: discredit of information rus.: компрометация информации Pinhoniy axborotni chiqib ketishi yoki oshkor bo‘lishi, yo mualliflashtirilmagan subyektlar tomonidan olinishi.

Axborot resurslarining mulkdori – ingl.: owner of information resources rus.: собственник информационных ресурсов Axborot resurslariga egalik qiluvchi, ulardan foydalanuvchi va ularni tasarruf etuvchi yuridik yoki jismoniy shaxs. (qonun)

Axborot sifati – ingl.: information quality rus.: качество информации Obyektlar va ularni o‘zaro bog‘lanishlari haqidagi muayyan axborotni yaroqliligini ifodalovchi xossalar majmui. U foydalanuvchi u yoki bu turdagi faoliyatni amalga oshirishi, o‘z oldida turgan maqsadlarga erishishi uchun zarur. Eng umumiy parametrlar qatoriga ma’lumot ishonchliligi, mavridiyligi, yangiligi, qimmatliligi, foydaliligi, olish qulayliligi kiradi.

Axborot tahdidi – ingl.: information threat rus.: информационная угроза Jamiyat axborot sohasining faoliyatiga xavf tug‘dirayotgan jami omillar va omillar guruhlari."

Axborot tahlili – ingl.: information analysis rus.: информационный анализ Hujjatlarni o‘rganish va shakllanayotgan hamda foydalanilayotgan axborot hajmini aynanlash, shuningdek, hujjatlar aylanishi sxemasini va axborot aloqalari modelini ishlab chiqish."

Axborot tarmog‘i – ingl.: information network rus.: информационная сеть Aloqa kanallari bo‘yicha ma’lumotlarni uzatish va ularga ishlov berish uchun dasturlitexnikaviy vositalar majmui.

Axborot tashuvchisi – ingl.: information carrier rus.: носитель информации Jismoniy shaxs yoki moddiy obyekt. Moddiy obyekt jumlasiga axborot ramzi, timsol, signal, texnik yechimlar va jarayonlar shaklida aks ettirilgan moddiy obyekt, shu jumladan fizik maydonlar kiradi.

Axborot texnologiyalari – ingl.: information technologies rus.: технологии информационные qarang: axborot texnologiyasi.

Axborot texnologiyasining xavfsizligi – ingl.: information technology security rus.: безопасность информационной технологии Axborotni qayta ishlash texnologik jarayonining muhofazalanganligi.

Axborot urushi – ingl.: information war rus.: информационная война 1. Dushman axboroti, axborotga asoslangan jarayonlar va axborot tizimlariga zarar yetkazish harakatlari. Ayni paytda o‘z axboroti, axborotga asoslangan jarayonlari va axborot tizimlarini muhofaza qilish orqali axborot ustunligiga erishish ko‘zlanadi. 2. Tizimlarning moddiy, harbiy, siyosiy yoki mafkuraviy sohada ma’lum yutuqqa erishishga qaratilgan bir-biriga ochiqdan-ochiq yoki yashirincha qaratilgan axborot hujumlari.

Axborot xavfsizligi ko‘rsatgichi – ingl.: criteria of information security rus.: критерий безопасности информации Turli xavf-xatar faktorlari ta’siriga nisbatan axborot xavfsizligini tavsiflovchi ko‘rsatkich.

Axborot xavfsizligi obyekti – ingl.: information security object rus.: объект информационной безопасности Axborot sohasida amalga oshiriladigan axborot xavfsizligi subyektlarining huquq va erkinliklari; axborot resurslari; axborot infratuzilmasi.

Axborotni muhofaza qilishning kriptografik usuli – ingl.: cryptographic method of information protection rus.: криптографический метод защиты информации Axborotni shifrlash va kodlash tamoyiliga asoslangan, axborotni muhofazalash usuli. Kriptografik usul dasturiy vositalar bilan ham, apparat vositalar bilan ham amalga oshirilishi mumkin.

Axborotni muhofaza qilishning kriptografik usuli – ingl.: cryptographic method of information protection rus.: криптографический метод защиты информации

Axborotni shifrlash va kodlash tamoyiliga asoslangan, axborotni muhofazalash usuli. Kriptografik usul dasturiy vositalar bilan ham, apparat vositalar bilan ham amalga oshirilishi mumkin.

Axborotning sizishi – ingl.: information leakage rus.: утечка информации Muhofaza qilinayotgan axborotning nazoratsiz tarqalishi. Bu axborotni oshkor qilish, uni ruxsatsiz olish va razvedka tomonidan axborotni olish natijasida sodir bo‘ladi.

Bir martalik bloknot usuli – Onetimepad deb ham yuritiladi. Kalit sifatida esa uzunligi juda katta bo‘lgan belgilar ketma – ketligi olinadi.

Birmarotabali raqamli imzo – ingl.: disposable digital signature rus.: одноразовая цифровая подпись Raqamli imzo ixtiyoriy xabar uchun faqat bir marta ishlatilishi mumkin bo‘lgan sxema, ya’ni, har qanday yangi xabarga yangi kalitlar jufti zarur bo‘ladi. Bunday sxemaning afzalligi tezkorlik bo‘lsa, kamchiligi – katta miqdordagi axborotni (oshkora kalitlarni) e’lon qilishdir, chunki, har bir imzo faqat bir marta ishlatiladi.

Birtomonlama funksiya – ingl.: one-way function rus.: односторонняя функция Berilgan X argument bo‘yicha F(X) funksiyaning qiymatini hisoblash yengil bo‘lsa, X ni F(X) dan aniqlash, hisoblashda qiyin bo‘lgan funksiya. Hozirgi kungacha birtomonlama funksiyalar mavjudligi qat’iy isbot qilinmagan. Axborotni shifrlash uchun birtomonlama funksiyalar yaramaydi, chunki, ular yordamida shiflangan matnni, uning shifrini egasi ham hatto ocha olmaydi. Birtomonlama funksiyalar asimmetrik kriptografiyada keng tatbiqini topdi.

Bod – ingl.: baud rus.: бод Ma’lumotlarni uzatish tezligining o‘lchov birligi. U bir sekundda uzatilgan ramzlar soni bilan aniqlanadi. Axborotni ikkilik kodida uzatadigan kanallar uchun 1 bod 1 bit/sekundga teng. Hozirgi zamonda bu tushuncha ishlatilmaydi.

Bul algebrasi – ingl.: boolean algebra rus.: булева алгебра 1. Har bir o‘zgaruvchisi ROST yoki YOLG‘ON qiymatlardan birini qabul qilishi mumkin bo‘lgan algebra. 2. Uch amaldan AND (VA), OR (YOKI), NOT (YO‘Q) iborat algebraik tuzulma. Bul algebrasi, mantiq qonuniyatlarini o‘rganib uni taklif etgan

irlandiyalik Jon Bul sha’niga uning nomi bilan atalgan. Bul algebrasida o‘zgaruvchilar ustida bajariladigan amallar bul amallari yoki mantiqiy amallar deb ataladi. Mantiqiy amallarni bajarish qoidalari mantiqiy sxemalarni o‘zgartirish uchun qulay. Shu sababli, bul algebrasi kompyuterni ishlab chiqishda asos bo‘lgan.

Butunlik – ingl.: integrity rus.: целостность Obyektning (axborotni, apparat yoki dasturiy ta’minotni) buzilmagan shaklda (uning qaydlangan biror bir holatiga nisbatan) mavjud bo‘lish xossasi.

Buzib erkin foydalanish – ingl.: hacking rus.: взлом Kompyuter muhofazasidagi ma’lum elementni chetlab o‘tish yoki ishdan chiqarish. Bu ma’lumotlarni qayta ishlash tizimidan erkin foydalanishga olib kelishi mumkin. Aniqlanadigan yoki aniqlanmaydigan bo‘lishi mumkin.

Buzib ochish – ingl.: disclosure rus.: раскрытие Kompyuter muhofazasi buzilishi. Buning oqibatida, ma’lumotlardan mualliflashmagan obyektlar erkin foydalanishi mumkin.

Dasturiy qaroqchilik – ingl.: software piracy rus.: программное пиратство 1.Dasturiy vositalardan ruxsatsiz foydalanish, ulardan nusxa ko‘chirish va ularni tarqatish. 2.Dasturiy mahsulotlardan noqonuniy ravishda foydalanish yoki ulardan nusxa ko‘chirish.

Dasturiy ta’minot umri – ingl.: software life cycle rus.: жизненный цикл программного обеспечения Kompyuter dasturiy ta’minotini loyihalashtirish boshlangan daqiqadan to uning ishlatilishi to‘xtashigacha o‘tgan vaqt.

Dasturiy xatcho‘p – ingl.: software bookmark rus.: программная закладка Axborotga tahdid tug‘diruvchi, ruxsatsiz o‘rnatilgan dastur.

Davlat sirini tashkil qiluvchi ma’lumotlarni olish – ingl.: access to state secrets rus.: доступ к сведениям, составляющим государственную тайну Ma’lum shaxsning vakolatli mansabdor shaxs ruxsati asosida davlat sirini tashkil qiluvchi ma’lumotlar bilan tanishib chiqishi.

DES – qisq.: Data Encryption Standard Ma’lumotlarni shifrlash standarti, DES shifrlash standarti. AQSH hukumatining davlat siri hamda tijoriy bo‘lmagan axborot uchun shifrlash standarti. Kalit uzunligi 56 bit bo‘lgan blokli shifr.

Kuchaytirilgan hili mavjud bo‘lib, u «uchlangan DES» (triple-DES, 3DES) deb ataladi, unda uchta turli kalit bilan DES standarti qo‘llaniladi.

Deshifrlash – shifrlashga teskari bo‘lgan jarayon, ya’ni kalit yordamida shifrlangan ma’lumotni dastlabki ma’lumot holatiga o‘tkazish.

Disk – ingl.: disk rus.: диск Bitta yoki ikkita tomonida ma’lumotlarni o‘qish yoki yozishni amalga oshirish uchun aylanuvchi yassi dumaloq plastinadan iborat ma’lumotlar tashuvchisi. qarang: Qattiq disk, Lazer disk.

Diskret – ingl.: discrete rus.: дискретный Ramzlar kabi alohida elementlardan iborat bo‘lgan ma’lumotlar yoki aniq ko‘rsatilgan qiymatlarning chekli soniga ega bo‘lgan fizik miqdorlarga, shuningdek, jarayonlar va ushbu ma’lumotlardan foydalanuvchi funksional moslamalarga tegishli ta’rif.

Doimiy algoritm – murakkabligi qiymati boshlang‘ich qiymat o‘lchoviga bog‘liq bo'lmasa.

Domen – ingl.: domain rus.: домен 1. Tarmoq ichida umumiy qoidalar va tartibotlar asosida yaxlit shaklda idora etiluvchi kompyuterlar va qurilmalar guruhi. Internet tarmog‘ida domen IP manzil bilan belgilanadi. 2. Ikki nuqta orasidagi domen manzili qismi. Chekka o‘ng tomondagi domen yuqori pog‘ona domeni bo‘ladi. Masalan, www.mves.gov.uz - 3-pog‘ona domeni; mves.gov.uz - 2-pog‘ona domeni; gov.uz - 1- pog‘ona domeni; uz - 0- pog‘ona domeni. Shunday qilib, yuqori pog‘ona domenlari shajarasi tashkil bo‘ladi: yuqori pog‘ona uz (O‘zbekiston) domeni, o‘z ichiga olgan gov (hukumat) domeni, uni o‘z ichiga olgan mves (Tashqi iqtisodiy aloqalar vazirligi) va uni o‘z ichiga olgan www (www serveri). Nolinchi pog‘ona domenlari har doim tarmoq nomlarini bildiradi. Nol pog‘ona domenlari – xalqaro shartnomalar predmeti. 1chi va undan yuqori pog‘ona domenlarini taqsimlash vakolatli tashkilotlar va provayderlar tomonidan amalga oshiriladi. 3. Ma’lumotlar bazalari texnologiyalarida domen atributning mumkin bo‘lgan qiymatlari tavsifidir.

Domen nomi – ingl.: domain name rus.: доменное имя Domen nomlar tizimiga binoan kompyuter tarmog‘i bog‘lamasiga berilgan noyob belgili nom. Internet tarmog‘ida bu doimiy IPmanzilga ega bo‘lgan qurilma nomidir. Odatda u

bog‘lamaning umumiy joylashishini belgilaydi. Har bir domen nomi tarmoqda ro‘yxatdan o‘tkazilib, alohida kompyuter yoki funksional guruh (domen)ga birlashtirilgan identifikator bo‘lib xizmat qiladi.

Elektromagnit spektr – ingl.: electromagnetic spectrum rus.: электромагнитный спектр Elektromagnit nurlanishlarning spektri.

Elektron armiya – ingl.: electronic army rus.: электронная армия Informatika va telekommunikatsiya tizimlaridan harbiy ishda foydalanish texnologiyasi.

Elektron arxiv – ingl.: electronic archive rus.: электронный архив Avtomatlashtirilgan axborot tizimlarida foydalanishga yaraydigan elektron shaklda taqdim qilingan hujjatlar arxivi.

Elektron hamyon – ingl.: electronic purse rus.: электронный кошелек 1. Xilma xil tovarlarni sotib olish va xizmatlar uchun to‘lovlarni amalga oshirishda foydalanish mumkin bo‘lgan naqd pulni o‘z mikrochipida raqamli shaklda saqlaydigan smart-karta. Smart-karta emitenti mablag‘larni turli elektron hamyonlar orasida xavfsiz ko‘chib yurishini ta’minlaydi. 2. Xotirasida pul mablag‘larini saqlaydigan, xarid qilish imkonini beradigan va offlayn texnologiyasini nazarda tutadigan elektron qurilma.

Elektron hujjatning asl nusxasi – ingl.: original of e-document rus.: оригинал электронного документа Elektron hujjatning har bir aynan bir xil nusxasi, basharti u belgilangan tartibda haqiqiy deb tasdiqlangan bo‘lsa, asl nusxadir.

Elektron kissa – ingl.: electronic wallet rus.: электронный бумажник Smart-karta egasiga, onlayn maromda tranzaksiyalarni amalga oshirishga, to‘lovlarni olishni boshqarishga va raqamli sertifikatlarni saqlashga imkon beradigan dasturiy ta’minot." **Elektron ochiqxat** – ingl.: virtual card (e-card) rus.: электронная открытка (sinonimi - virtual ochiqxat) O‘zining oshnasiga xushfe’l xabar (tabriknoma, taklifnoma va sh.k.) yubormoqchi bo‘lgan odam, veb-xizmatdan - elektron ochiqxatlar xizmatidan foydalanishi mumkin. Ochiqxatlar saytida mos keladigan rasmni tanlab unga matn qo‘shib, oluvchi manzilini (e-mail) ko‘rsatish kifoya. Goho, ochiqxatlar sayti topshirish vaqtini ham ko‘rsatishni taklif qiladilar. Ayrim hollarda, ochiqxat animatsiyali yoki musiqali bo‘lishi mumkin. Manzil

egasi «dalolatnoma» xat olgach, unda saytning sahifasiga murojaat bo‘lib, u o‘z ochiqxatini ko‘rib, o‘qishi mumkin.

Elektron raqamli imzo – elektron matnga ilova qilinadigan kriptografik almashtirishdan iborat bo‘lib, shu elektron matn jo‘natilgan shaxsga qabul qilingan elektron matnning va matinni raqamli imzolovchining haqiqiy yoki soxta ekanligini aniqlash imkonini beradi.

Elektron raqamli imzo – ingl.: electronic digital signature rus.: электронная цифровая подпись elektron pochta manzili Elektron hujjatdagi mazkur elektron hujjat axborotini elektron raqamli imzoning yopiq kalitidan foydalangan holda maxsus o‘zgartirish natijasida hosil qilingan hamda elektron raqamli imzoning ochiq kaliti yordamida elektron hujjatdagi axborotda xatolik yo‘qligini aniqlash va elektron raqamli imzo yopiq kalitining egasini identifikatsiya qilish imkoniyatini beradigan imzo. (qonun) Qonunda talab etilgan shartlarga rioya etilgan taqdirda elektron raqamli imzo qog‘oz hujjatga shaxsan qo‘yilgan imzo bilan bir xil ahamiyatga egadir.

Elektron raqamli imzo (ERI) – ingl.: electronic digital signature rus.: электронная цифровая подпись 1. Elektron hujjatdagi mazkur elektron hujjat axborotini elektron raqamli imzoning yopiq kalitidan foydalangan holda maxsus o‘zgartirish natijasida hosil qilingan hamda elektron raqamli imzoning ochiq kaliti yordamida elektron hujjatdagi axborotda xatolik yo‘qligini aniqlash va elektron raqamli imzo yopiq kalitining egasini identifikatsiya qilish imkoniyatini beradigan imzo. (qonun) Qonunda talab etilgan shartlarga rioya etilgan taqdirda elektron raqamli imzo qog‘oz hujjatga shaxsan qo‘yilgan imzo bilan bir xil ahamiyatga egadir. 2. Elektron ma’lumotlarni kriptografik o‘zgartirish natijasida hosil qilingan belgilar ketma-ketligi. Elektron raqamli imzo ma’lumotlar blokiga qo‘shib qo‘yiladi va blokni qabul qiluvchiga, manbani va ma’lumotlarning butunligini tekshirish hamda soxtalashtirishdan muhofazalanish imkonini beradi. Hozirgi kunga kelib, ayrim mamlakatlar qonunchilik yo‘li bilan raqamli imzodan foydalanishni layoqatliligini qonunlashtirib qo‘yganlar. Elektron raqamli imzo kalitlari sertifikatlari ro‘yxatga olish markazlari tomonidan beriladi.

Elektron raqamli imzoning ochiq kaliti – ingl.: public key of the EDS rus.: открытый ключ электронной цифровой подписи Elektron raqamli imzo vositalaridan foydalangan holda hosil qilingan, elektron raqamli imzoning yopiq kalitiga mos keluvchi, axborot tizimining har qanday foydalanuvchisi foydalana oladigan va elektron hujjatdagi elektron raqamli imzoning haqiqiyligini tasdiqlash uchun mo‘ljallangan belgilar ketmaketligi. (qonun).

Elektron raqamli imzoning yopiq kaliti – ingl.: private key of the EDS rus.: закрытый ключ электронной цифровой подписи Elektron raqamli imzo vositalaridan foydalangan holda hosil qilingan, faqat imzo qo‘yuvchi shaxsning o‘ziga ma’lum bo‘lgan va elektron hujjatda elektron raqamli imzoni yaratish uchun mo‘ljallangan belgilar ketmaketligi. (qonun).

Faol tahdid – ingl.: active threat rus.: активная угроза Ma’lumotlarga ishlov berish tizimi holatini ruxsatsiz ataylab o‘zgartirish tahdidi. Masalan, xabarlarni o‘zgartirish, qalbaki xabarlarni jo‘natish, maskarad yoki xizmat ko‘rsatishni rad etishga olib keluvchi tahdid.

FC – qisq.: Fibre Channel Optik-tola kanali, Fibre Channel standarti. Ma’lumotlarni optik tolasi orqali uzatish uchun ANSI standarti.

FCC – qisq.: Federal Communication Commission AQSH Federal aloqa hayati. AQSHning xohlagan elektron apparaturasini uning nurlanishining insonlarga va/yoki boshqa elektron texnikasiga xavflilik sinfi bo‘yicha sertifikatlashtiruvchi tashkiloti. Ushbu tashkilot tomonidan sertifikatlarning ikkita turi beriladi – FCC-Class A – faqat kasbiy foydalanish uchun ruxsat etilgan va FCC-Class B – xohlagan joyda foydalanilishi mumkin.

Feystel shifri – ingl.: Feistel’s cipher rus.: шифр Фейстеля Takrorlanadigan blokli shifrning maxsus sinfi. Unda shifr - matn ochiq matn asosida aylanib o‘tish vazifasini takror qo‘llash hisoblanadi. Ayrim hollarda Feystel shifrini DES kabi shifr deb atashadi. Ishlov berilayotgan matn ikki qismga bo‘linadi va aylanib o‘tish vazifasi qo‘shimcha kalitni birinchi qismga qo‘llanadi. Aylanib o‘tish vazifasini qo‘llashning natijasi ikkinchi qism bilan 2 moduli (XOR amali) bo‘yicha qo‘shiladi. So‘ngra, ikkala bo‘lak o‘zaro almashib jarayon takrorlanadi.

Filtr – ingl.: filter rus.: фильтр 1. Filtrlashni bajarish uchun ishlatiladigan qurilma (sodda elektrik sxema) yoki dastur. Filtr kirishdagi signallar yoki ma’lumotlar oqimini bir necha kerakli qismlarga bo‘ladi. 2. Muayyan turdagi erkin foydalanish ma’lumotlarini qabul qilib, unga ishlov berib, so‘ngra chiqarib beruvchi dastur. Masalan, saralash dasturi filtrdir. U saralanmagan shaklda so‘zlarni qabul qiladi, so‘ngra ularni saralaydi va foydalanuvchiga saralangan ko‘rinishda beradi. Gohida, filtr deganda, tashqi dasturlardan ma’lumotlarni import - eksport qilish vositalari ham tushuniladi. 3. Ma’lumotlarni tanlab olish sharti. Filtr faqat berilgan shartlarni qanoatlantiruvchi ma’lumotlarni chiqarib beradi. 4. Grafik muharrirlarda, tasvirga tatbiq qilish mumkin bo‘lgan zo‘r hodisa filtrdir. Ayrim shunday filtrlar, tasvirni tanib bo‘lmaydigan darajagacha o‘zgartirib yuborishi mumkin. 5. Pochta mijoziga ko‘rsatmalar. Ularning vazifasi – xabarlarni avtomatik tarzda saralash. Tarkibiga xabarlarni ajratish qoidalari va ajratilgan xabarlar bilan bajariladigan harakatlar kiradi. Gohida filtrlarni xabarlar uchun qoidalar deb ham ataladi."

Filtrlash – ingl.: filtering rus.: фильтрация Signallarni yoki ma’lumotlarni umumiy oqimidan kerakli mezonlarga ega bo‘lganlarini ajratib qo‘yish jarayoni. Filtrlash filtr yordamida amalga oshiriladi.

Foydalanuvchi – ingl.: user rus.: пользователь Ma’lumotlarga ishlov berish tizimiga buyruq yoki xabarlar beruvchi yoki axborotga ishlov berish tizimidan xabar qabul qiluvchi har qanday shaxs yoki obyekt.

Gammalash – ingl.: gamming rus.: гаммирование Dastlaki (ochiq) matnni ma’lum algoritm bo‘yicha shifr gammasi bilan qoplash. Xorijda «gammalash» atamasining sinonimi «oqim shifri» bo‘ladi.

Globallashuv – ingl.: globalization rus.: глобализация Axborot texnlogiyalari, mahsulotlari va tizimlarini butun dunyoga tarqalish jarayoni. U iqtisodiy va madaniy jihatlardan qaraganda uyg‘unlashuvga olib keladi. Bu jarayonning tarafdorlari bundan keyinggi taraqqiyot imkoniyatlarini faqat global axborot jamiyatini rivojlanish sharoitlarida ko‘rishadi. Opponentlar globallashuvni milliy madaniy qadriyatlarga keltiradigan xatarlari haqida ogohlantirishmoqda.

GOST 28147-89 – kriptoalgoritmi hozirda Rossiya Federatsiyasi davlat standart shifrlash algoritmi hisoblanadi. Bu algoritm apparat va dasturiy ta’minot uchun mo‘ljallangan bo‘lib, himoyalanadigan ma’lumotning maxfiylik darajasiga chegaralash yo‘q.

Grafik fayl – ingl.: graphic file rus.: графический файл Nuqtama-nuqta kodlangan tasvirni o‘z ichiga olgan fayl. Bundan tashqari, grafik faylga dasturlarda va qurilmalarda ishlatiladigan boshqaruvchi kodlar ham kiradi.

Guruh imzosi – ingl.: group signature rus.: групповая подпись Chom va Van Xeyst tomonidan 1991 yilda taklif qilingan raqamli imzo sxemasi. U guruhning ixtiyoriy a’zosiga xabarni shunday imzolash imkonini beradiki, imzo tekshirilganda habar guruhning biror bir a’zosi imzolaganda shaxsi aniqlanmaydi.

Guruh manzili – ingl.: group address rus.: групповой адрес Obyektlar to‘plamini aniqlaydigan manzil. Ma’lumotlar bloki shu manzilga atalgan.

Guruhiy kodlash – ingl.: group encoding rus.: групповое кодирование (кодирование группами отрезков) Rastrli ma’lumotlarni zichlashtirish usullaridan biri. U sodda va ommalashgan bo‘lib, ketmaketlikda takrorlanadigan ramzlar guruhini takrorlanishlar soni bilan ko‘rsatishga (masalan, 00000111107777 ketma-ketligini 50411047 guruh kodi shaklida) asoslanadi, o‘zgacha aytganda, rastrning nomdosh elementlaridan tashkil topgan kesmani, kesma uzunligi bilan almashtiradi.

Haqiqiylikni tekshirish – ingl.: authenticity checking rus.: проверка подлинности Shaxs yoki obyekt haqiqiyligini tekshirish jarayoni. Masalan, foydalanuvchi haqiqiyligini tekshirish uchun foydalanuvchining ismi va paroli kerak bo‘lishi mumkin.

Harfiy-raqamli kodlash – ingl.: alphanumeric coding rus.: буквенно-цифровое кодирование Harflar, sonlar va alfavitning boshqa ramzlaridan tashkil topgan koddan foydalanidigan kodlash.

ICC – qisq.: Integrated Circuit Card Mikrosxemali kartochka, smart-karta.

Identifikatsiya – ingl.: identification rus.: идентификация Erkin foydalanish subyekt yoki obyektlariga identifikator berish va (yoki) taqdim etilayotgan identifikatorni berilgan identifikatorlar ro‘yxati bilan taqqoslash.

Ilmiy kriptografiyaning – (1930-60 yillar) boshqalardan ajralib turadigan tomoni - kriptobardoshliligi qat’iy tarzda matematik formulalar orqali asoslangan kriptografik tizimlarning paydo bo‘lishidir.

Imzo – ingl.: signature rus.: подпись Familiya, ism, manzil va boshqa axborotdan iborat kichik matn. Uy katalogidagi maxsus fayldan olinadigan imzo avtomatik ravishda jo‘natilayotgan xat va teleanjumanda jo‘natilgan maqolalar oxiriga qo‘shiladi. **Raqamli imzo** – shaxsingizga guvoh bo‘luvchi maxfiy kod.

Internetning ichki tahdidlari – ingl.: internal Internet threats rus.: внутренние угрозы Интернет Tarmoq axborot makonining ahvoli va rivojlanishi uchun salbiy oqibatlarga ega bo‘lishi mumkin bo‘lgan tahdidlar. Bular: tarmoqning ortiqcha yuklanganligi tufayli axborot kollapsi (qulashi); xakerlarning ma’lumotlarni yo‘q qilish yoki o‘zgartirish, uzellar va trafikning «chetlab o‘tish» yo‘nalishlarini to‘sish maqsadida uyushtirgan hujumlari; kommunikatsion kanallarning tasodifiy yoki uyushtirilgan avariyalari; axborot-izlash tizimlarning mukammal emasligi; protokollarning «ma’naviy» eskirib qolishi va boshqalar.

Internetning tashqi tahdidlari – ingl.: external Internet threats rus.: внешние угрозы Интернет Foydalanuvchilar uchun salbiy oqibatlarga ega bo‘lishi mumkin bo‘lgan tahdidlar. Tashqi tahdidlar texnologik va ijtimoiy bo‘lishi mumkin. Texnologik: sekin kanallar; tarmoqqa ulanishning unumsiz uslublari; olib keltirilgan viruslar; axborot «toshqini» va h.k. Ijtimoiy: foydalanuvchilarning jismoniy va psixik sog‘lig‘iga bo‘lgan ta’sir; insonning shaxsiy ongiga bo‘lgan ta’sir; axborot terrori va jinoyati; resurslarni ingliz tilida chop etish tendensiyasi va boshqalar.

Ipsec – qisq.: Secure IP Xavfsiz IP, IPsec bayonnomasi

IS – qisq.: Information System Axborot tizimi.

Jug‘rofiy domen – ingl.: geographic domain rus.: географический домен Jug‘rofiy belgi bo‘yicha birlashtirilgan domen nomlari guruhi. Masalan, www.uza.uz, www.bilimdon.uz nomlari «uz» (O‘zbekiston) domeniga mansub.

Kalit – dastlabki matnni shifrmatnga o‘girish va unga teskari amalarini boshqarish uchun ishlatiladigan axborot majmui (bitlar ketma-ketligi).

Kalit generatsiyasi – ingl.: key generation rus.: генерация ключей Kriptografik kalitni generatsiyalash jarayoni. Bunda turli usullar, masalan tasodifiy sonlar va soxta tasodifiy sonlar ketma-ketligini generatsiyalash ishlatiladi.

Kalit sonli jadval – Kalit sifatida 2 ta son olinadi. Har bir sonda raqamlar takrorlanmasligi kerak. 1- yozilgan son gorizontal kalit, 2-yozilgan son vertikal kalit sifatida ishlatiladi.

Kalitlarni eksponensial tarqatish – ingl.: exponential distribution of keys rus.: экспоненциальное распределение ключей Kalitlarni ochiq taqsimlash algoritmi. U asimmetrik kriptotizimlarga xos bo‘lib, Diffi- Xellman algoritmi deb ham ataladi. Modul arifmetikasida birtomonlama ko‘rsatkichli funksiya f(x) = ax (mod n) dan foydalanishga asoslangan. Bu yerda x - daraja kursatkichi, a – asos, n – modul.

Kalitlarni taqsimlash va boshqarish – kriptobardoshli kalitlarni ishlab chiqish (yoki yaratish), ularni muhofazali saqlash va kalitlarni foydalanuvchilar orasida muhofazalangan holda taqsimlash jarayonlarini o‘z ichiga oladi.

Kanalli shifrlash – ingl.: channel level coding rus.: канальное шифрование Telekommunikatsiya vositalari bilan uzatilayotgan axborotni kriptografik usullar bilan muhofazalash. Shifrlash, aloqa kanalinig ikki bog‘lamasi (yuboruvchidan qabul qiluvchigacha yo‘lda oraliq shifrlash ham bo‘lishi mumkin) orasida amalga oshiriladi.

Kanalli shifrlash – ingl.: channel level coding rus.: канальное шифрование Telekommunikatsiya vositalari bilan uzatilayotgan axborotni kriptografik usullar bilan muhofazalash. Shifrlash, aloqa kanalinig ikki bog‘lamasi (yuboruvchidan qabul qiluvchigacha yo‘lda oraliq shifrlash ham bo‘lishi mumkin) orasida amalga oshiriladi.

Kbps – qisq.: KiloBits Per Second Kilobit soniyaga.

KLOC – qisq.: KiloLines Of Code Kodning ming qatori. Dasturlar murakkabligining o‘lchov birligi.

Ko‘p manzilli uzatish – ingl.: multiaddress trasmission rus.: многоадресная передача Maxsus manzilga («hammaga») ko‘ra har bir abonent tizimiga blok nusxalarini alohida, ketma-ket yo‘naltirish orqali keng tarqatish.

Ko‘p pog‘onali kriptografiya – ingl.: multilevel cryptography rus.: многоуровневая криптография R.Rayvest tomonidan taklif qilingan va simmetrik kriptotizimlar uchun kriptografik kalitlar tuzishning maxsus usulini ko‘zlovchi mexanizm. Ushbu mexanizmni amalga oshiruvchi kriptotizim shunday tuzilganki, birinchi kriptografik kalit ixtiyoriy ravishda tanlanishi mumkin, barcha keyingi kalitlarni tanlash esa muayyan qonunga mos kelishi lozim.

Kod – ingl.: code rus.: код 1. Shartli belgi, odatda raqamli. 2. Muayyan ma’no berilgan ramzlar majmui. Kod, inson, qurilmalar va dasturiy ta’minot idrok qila oladigan axborotning ramzlar to‘plami bilan tasviflash usulini belgilaydi. 3. Ochiq daslabki matn elementlarini (harflar, harflar birikmasi, so‘z, va h.k.) ramzlar guruhi (harflar, raqamlar yoki boshqa ishoralar) bilan almashtirishlar to‘plami. U shifrning maxsus turidir. 4. Xabarlarni bir (dastlabki) alifbodan boshqa (obyektli) alifboga, odatda axborot talofat ko‘rmagan holda, o‘zgartirish qoidasi.

Koder – ingl.: coder rus.: кодер Kodlashni amalga oshiruvchi qurilma yoki dastur.

Kodlash kaliti – ingl.: coding key rus.: ключ кодирования Kriptografiyada - kodlarni o‘zgartirishda, ularning o‘zaro mosligini tekshirish uchun ishlatiladigan kalit. Bu kalitning vazifasi, begona obyektlar tomonidan dasturlarni va ma’lumotlarni ishlatishdan muhofazalash.

Kommunikativistika – ingl.: communication science rus.: коммуникативистика Axborot kommunikatsiyalari (shu jumladan, tarmoqlar) muammolarini o‘rganadigan fan.

Kompyuter dasturlarini qo‘riqlash – ingl.: protection of computer software rus.: охрана компьютерных программ Ixtiyoriy tilda va ixtiyoriy shaklda, shu jumladan, dastlabki matn yoki obyektli kod ham, ifodalanishi mumkin bo‘lgan,

dasturlarni (shu qatori operatsion tizimlar ham) barchasiga tegishli bo‘lgan qo‘riqlash turi.

Kompyuter jinoyatlari – ingl.: computer crimes rus.: компьютерные преступления 1.Bevosita ma’lumotlarga ishlov berish tizimi yoki kompyuter tarmog‘i yordamida qilingan jinoyatlar. 2. Apparat, dasturiy vositalarni va ma’lumotlarni ishlatish, turlash yoki qo‘porish yo‘li bilan sodir etilgan jinoyat. 3. Kompyuter informatikasi sohasidagi jinoyatlarning qisqartirilgan nomi. 4. Axborot – telekommunikatsiya tarmoqlari orqali axborotdan erkin foydalanishning yangi imkoniyatlarini ishlatish, hamda kompyuter tizimlari foalitini buzish bilan bog‘liq huquqbuzarlik harakatlari.

Kompyuter kriptografiyasiga – (1970-yillardan boshlab) «qo‘lda bajariladigan» va «mexanik» shifrlardan bir necha barobar katta kriptobardoshlilikka ega bo‘lgan shifrlashni katta tezlik bilan bajarilishini ta’minlovchi samarali hisoblash vositalarini paydo bo‘lishi bilan asos solindi.

Kompyuter steganografiyasi – bu klassik steganografiyaning yo‘nalishi bo‘lib, kompyuter platformasi uchun asoslangan. Masalan, Linux uchun, steganografik fayl tizimsi StegFS, ma’lumotlarni ishlatish mumkin bo‘lmagan joylarda ularni ma’lum fayl formati ko‘rinishida saqlash, belgilarni fayllar nomiga almashtirish, matnli steganografiya va h.k.

Kompyuter tezligi – ingl.: computer speed rus.: быстродействие компьютера Mashinaning markaziy protsessorlari tomonidan bir sekundda bajarilayotgan elementar amallarsoni. Zamonaviy kompyuterlar tezligi sekundiga bir necha milliard amallarga yetadi.

Kompyuteramaniya – ingl.: computer-prone rus.: компьютеромания Insonning kompyuter tizimlarini muntazam ishlatishdagi patologik ehtiyoji. Bu inson ruhiyatiga kompyuter o‘yinlari va virtual borliq texnologiyalari ta’siriga ko‘nikib qolishi bilan yuzaga kelgan.

Kompyuterlar avlodi – ingl.: computers’ generation rus.: поколение компьютеров Asosan ishlab chiqarish jarayonida qo‘llaniluvchi texnologiyaga asoslangan kompyuterlarning tarixiy tasnifidagi toifa. Masalan, birinchi avlod

kompyuterlari rele yoki elektron lampalarga, ikkinchisi – tranzistorlarga, kompyuter xaritasi uchinchisi – integral mikrosxemalarga, to‘rtinchisi – katta va o‘ta katta integral sxemalarga asoslangan.

Kreker – ingl.: cracker rus.: крекер Xakerning Internetda qabul qilingan nomlanishi. Tarmoqda haqorat so‘zi hisoblanmaydigan «xaker» so‘zidan farqli, aynan qo‘poruvchi (sindiruvchi - «yomon odam»). Bu atama ko‘p ma’noli: sindiruvchi deb qarsillab sinadigan quruq pecheniyni ham, va shovqinsiz, muhofazani sindiradigan xakerlarning dasturlarini ham, atashadi.

Kriptobardoshlilik – shifrlash kaliti noma’lum bo‘lgan holda shifrlangan ma’lumotni deshifrlashning qiyinlik darajasini belgilaydi.

Kriptografik algoritm – ingl.: cryptographic algorithm rus.: криптографический алгоритм Axborotni (ma’lumotlarni) buzishga to‘sqinlik qilish va undan ruxsatsiz erkin foydalanish dan muhofazalash maqsadida uni o‘zgartirishning matematik algoritmi.

Kriptografik kalit – ingl.: cryptographic key rus.: ключ криптографический 1. Dastlabki matnni shifrmatnga va shifrmatnni dastlabki matnga o‘girish imkonini ta’minlaydigan, kriptografik algoritmning parametri bo‘lgan ramzlar ketma-ketligi. 2. Shifr o‘zgartirishlari to‘plamidan muayyan o‘zgartirishni aniqlaydigan ma’lumotlar majmui.

Kriptografik muhofaza – ingl.: cryptographic protection rus.: криптографическая защита Axborotni kriptografik o‘zgartirish bajarish yo‘li bilan muhofazalash."

Kriptografik muhofaza – ingl.: cryptographic protection rus.: криптографическая защита Axborotni kriptografik o‘zgartirish bajarish yo‘li bilan muhofazalash."

Kriptografiya – axborotlarni aslidan o‘zgartirilgan holatga akslantirish uslublarini topish va takomillashtirish bilan shug‘illanadi.

Kriptografiya tarixi – shartli ravishda to‘rtta bosqichga ajratish mumkin: sodda, formal (rasmiy), ilmiy, kompyuterli.

Kriptografiyada – dastlabki matnni shifrmatnga o‘girish va unga teskari amalarini boshqarish uchun ishlatiladigan axborot majmui (bitlar ketma-ketligi).

Kriptologiya – ingl.: cryptology rus.: криптология Aloqa kanallari orqali axborotning xavsizligini ta’minlab saqlash va uzatish tizimlarini yaratish va tahlil qilish to‘g‘risidagi fan. Kriptologiyani ikki qismga bo‘lishadi: kriptografiya va kriptotahlil."

Kriptosistema – algoritmlar va hamma mumkin bo’lgan ochiq matnlar, shifrli matnlar va kalitlar xisoblanadi.

Kriptotahlil – shifrlash uslubini (kalitini yoki algoritmini) bilmagan holda shifrlangan ma’lumotning asl holatini (mos keluvchi ochiq ma’lumotni) topish masalalarini yechish bilan shug‘ullanadi.

Kruk kriptotizimi – ingl.: Crook’s cryptosystem rus.: криптосистема Крука Xatolarni tuzatish kodlariga asoslangan kriptotizim. MakEllisning kriptotizimini kamchiliklarini yo‘qotish uchun YE.Kruk tomonidan taklif qilingan.

Kvadratik ayirma – Agar p - tub son va 0<a< p bo‘lib, ushbu x mod p = a munosabatni qanoatlantiruvchi x - noma’lumning qiymatlari mavjud bo‘lsa, u holda a soni modul p bo‘yicha kvadratik ayirma deyiladi.

Kvant – ingl.: quantum rus.: квант Diskret fizik kattalik, masalan, signal o‘zgarishi mumkin bo‘lgan eng kam kattalik.

Kvant axborot nazariyasi – ingl.: quantum theory of information rus.: квантовая теория информации Kvant axborotining vujudga kelishi, ishlov berish, uzatish va saqlash jarayonlarini ifodalovchi futuristik nazariya. Bu axborot ustidan amallar, bitlar sifatida elementar zarrachalar holatini ishlatish yo‘li bilan amalga oshiriladi. Kvant axborotini mumtoz shaklga aylantirish uchun maxsus dekoderlovchi qurilma ishlatiladi. Axborotning kvant nazariyasi sof nazariy fan bo‘lib, hozirgacha, u asosida qurilgan texnologiyalar amaliyotdan ancha uzoq.

Kvantlash – ingl.: quantization rus.: квантование 1. Biror bir uzluksiz kattalik qiymatlari kengligini chekli bir-biri bilan kesishmaydigan oraliqlarga bo‘lish. 2. Ma’lumotlarni uzluksiz shakldan diskret shaklga o‘tkazish amali. 3. Ma’lumotlarni nimguruhlarga (sinflarga) bo‘lish, masalan, tasvirlarga raqamli ishlov berilganda.

Kvantlash berilgan kattalikni kvantlarga bo‘lishga keltiriladi. Informatikada, birinchi navbatda kvantlashga vaqt va analogli signallar yo‘liqadi.

Liniyaga sust ulanish – ingl.: passive line connection rus.: пассивное подключение к линии Liniyaga ma’lumotlarni o‘qish uchun qo‘shilish.

Log – ingl.: log file rus.: лог Veb-saytning o‘ziga xos bortdagi jurnali. Server loglariga u yoki bu foydalanuvchi qayerdan va qachon kelgani, saytda qancha vaqt bo‘lgani va u yerda nimani ko‘rgani va yuklab olgani, uning brauzeri va uning kompyuterining IP manzili qandayligi haqidagi ma’lumot yoziladi. Logga har bir yozuv ma’lum xitga tegishli bo‘ladi, chunki server aynan sayt elementlaridan biriga murojaat qilishni qayd qilishi mumkin.

Log-fayl – ingl.: log-file rus.: лог-файл Resurslardan erkin foydalanish urinishlarini qayd qiluvchi fayl. Masalan, log-fayl vebsaytingizga kirganlar haqidagi ma’lumotlarni saqlashi mumkin: foydalanuvchi nomi, foydalanuvchi domeni, ma’lum sahifada o‘tkazilgan muddat, ochilgan gipermurojaatlar va h.k.

Login – ingl.: login rus.: логин 1. Foydalanuvchining kompyuter yoki tarmoqdan erkin foydalanish jarayoni. 2. Kompyuterdan erkin foydalanishga ega bo‘lish uchun foydalaniluvchi qayd yozuvi nomi. Maxfiy emas. 3. Kompyuterga aynanlash ma’lumotlarini (odatda qayd yozuvi nomi va parol) uzatayotganda u bilan bog‘lanish.

Ma’murlash – (Accounting) - foydalanuvchining tarmoqdagi harakatini, shu jumladan, uning resurslardan foydalanishga urinishini qayd etish.

Ma’lumotlar autentifikatsiyasi – ingl.: data authentication rus.: аутентификация данных Ma’lumotlar butunligini tekshirish uchun foydalaniladigan jarayon. Masalan, olingan ma’lumotlarning yuborilgan ma’lumotlar bilan bir xilligini tekshirish; dasturning virusdan zararlanmaganligini tekshirish.

Ma’lumotlar butunligi – ingl.: data integrity rus.: целостность данных qarang: axborot butunligi.

Ma’lumotlarni filtrlash – ingl.: data filtering rus.: фильтрация данных Ma’lumotlarni umumiy oqimidan kerakli mezonlarga ega bo‘lganlarini ajratib qo‘yish jarayoni. Ma’lumotlarni filtrlash jismoniy pog‘onadan tashqari barcha

pog‘onalarda amalga oshirilishi mumkin. Ular quyidagilar zarur bo‘lganda bajariladi: - ruxsatsiz erkin foydalanish ga urinishlar bilan bog‘liq ma’lumotlarning xavfsizligini ta’minlash; - yakkakanal yoki halqa tarmoqlarda ma’lumotlar bloklarining tanlanishi; - o‘rnatilgan standartlarga mos kelmagan, masalan MB ga yozishda, ma’lumotlarni chiqarib tashlash; - ma’lumotlarni zichlashtirish, masalan, bittasidan boshqa bir biri bilan ketma ket kelgan barcha ochiq joylarni yo‘q qilish va ularning o‘rniga ochiq joylar sonini yozib qo‘yish.

Ma’lumotlarni muvofiqlash – ingl.: data authentication rus.: аутентификация данных qarang: ma’lumotlar autentifikatsiyasi.

Mantiqiy bomba – ingl.: logic bomb rus.: логическая бомба Biror bir shart bajarilsa ishga tushib ketadigan va avtomatlashtirilgan tizim resurslarining (ma’lumotlar, dasturiy yoki apparat ta’minoti) shikastlanishiga olib keladigan kompyuter dasturi yoki dastur bo‘lagi.

Matn – alfavitning elementlaridan (belgilaridan) tashkil topgan tartiblangan tuzilma.

Matnli xabar – ingl.: message text rus.: текстовое сообщение Matndan iborat va tarmoq bo‘yicha uzatiladigan xabar.

Maxfiy savol – ingl.: secret question rus.: секретный вопрос «Maxfiy savol»+»Maxfiy javob» - bu qo‘shimcha parol. Siz asosiy parolingizni unutgan bo‘lsangiz, sizdan maxfiy savol so‘raladi, sizdan olingan javob esa maxfiy javob bilan solishtiriladi. Javoblar bir xil bo‘lsa, siz uchun fayllaringizga yo‘l ochiladi.

Maxfiylik kaliti – ingl.: privacy key rus.: ключ секретности Foydalanuvchining yoki dasturning resurslar va ma’lumotlar bilan ishlash huquqlarini aniqlaydigan kalit. Maxfiylik kaliti autentifikatsiyada ishlatilib, parol, ya’ni, maxfiy so‘z turlaridan biridir.

Maxsus (ko‘rinmas) siyoh usuli – Klassik steganografiyaning keng tarqalgan usullaridan biri bu maxsus(ko‘rinmas) siyoh usulidir. Bunday siyohlarda yozilgan matn faqatgina maxsus sharoitlarda qog‘ozda paydo bo‘lgan (isitish, yoritish va kimyoviy qorishma qo‘shish kabi). Bu usul I asrda Aleksandr Felono tomonidan kashf etilgan bo‘lib, o‘rta asrlarda ham ishlatilgan. Qog‘ozga qatorlar orasiga sut

bilan yozilsa, sut esa qog‘oz olovda qizdirilganda ko‘rinishi haqidagi usul ham mavjud.

MixColumns – ustun elementlarini aralashtirish, ya’ni algoritmda berilgan matritsa bo‘yicha akslantirishni amalga oshirish.

Mualliflash – ingl.: authorization rus.: авторизация 1. Huquqlarni berish. U erkin foydalanish huquqlari asosida erkin foydalanishga huquq berishni ham o‘z ichiga oladi. 2. Foydalanuvchining resursdan erkin foydalanish huquqlari va ruxsatlarini tekshirish jarayoni. 3. Foydalanuvchiga hisoblash tizimida ba’zi ishlarni bajarish uchun muayyan huquqlarni berish.

Muhofaza ma’muri – ingl.: protection administrator rus.: администратор защиты Avtomatlashtirilgan tizimni undagi axborotlardan ruxsatsiz erkin foydalanishdan muhofaza uchun javobgar subyekt.

Muhofazalangan muhit – ingl.: protected environemnt rus.: защищенная среда Ma’lumotlarni va resurslarni tasodifiy yoki qasddan qilingan harakatlardan muhofazalashga alohida e’tibor (mualliflash, erkin foydalanish, tarkibiy tuzilmani boshqarish va h.k shakllarda) beriladigan muhit.

Muhofazalanganlik – ingl.: security state rus.: защищенность Tizimning maxfiy axborotdan beruxsat erkin foydalanishga, uni soxtalashtirish yoki buzishga qarshi tura olish qobiliyati. Texnik muhofaza (yo‘latmaslik xossasi) nuqtai nazaridan ham, maxfiylik darajasiga qarab ijtimoiy-psixologik nuqtai nazardan ham qaraladi.

Muhofazalanmaganlik – ingl.: vulnerability rus.: незащищенность Ma’lumotlarni qayta ishlash tizimidagi muayyan zaiflikka aniq hujum uyushtirish mumkinligi.

Muvaqqat kriptotizim – ingl.: cryptosystem with temporarily disclosure rus.: криптосистема с временным раскрытием Muhofazalangan xabarni berilgan vaqt oralig‘i o‘tgandan so‘ng, shifrini ochishga imkon beradigan kriptografik tizim. Hozirgi kunda, bunday tizimlarni amalga oshirishning ikki turi mavjud: - vaqtincha qulfli Sharadalar; - o‘ziga, berilgan vaqt oralig‘ida axborotni ochmaslik majburiyatini oladigan ishonchli vakillarni ishlatish.

Muvofiqlash – ingl.: authentication rus.: аутентификация qarang: autentifikatsiya.

Niderraytera kriptotizimi – ingl.: Nideraiter’s cryptosystem rus.: криптосистема Нидеррайтера Xatolarni tuzatish kodlariga asoslangan kriptotizim. 1986 yili G. Niderrayter tomonidan taklif qilingan.

Niqoblash – ingl.: masking rus.: маскировка Obyektni jinoyatkorlar uchun kirib bo‘lmaydigan (ko‘rinmaydigan) yoki undan erkin foydalanishni murakkablashtiruvchi harakatlarni bajarishga asoslangan obyektlarni muhofaza qilish uslubi.

NIST – qisq.: National Institute of Standards and Technology Standartlar va texnologiyalar milliy instituti.

O’suvchi ketma-ketlik – Berilgan ketma-ketlikni har bir hadi o‘zidan oldingi hadlar yig‘indisidan katta bo‘lsa, bu ketma-ketlikka O’suvchi ketma-ketlik deyiladi.

Ochiq kalit – ingl.: public key rus.: открытый ключ Asimmetrik kriptotizimda ishlatiladigan va tizimning barcha foydalanuvchilari erkin foydalanishi mumkin bo‘lgan kalit. Yana qaralsin: elektron raqamli imzoning yopiq kaliti.

Ochiq kalitli kriptotizim – ingl.: cryptosystem with public key rus.: криптосистема с открытым ключом Ikkita, maxfiy va ochiq kalit ishlatadigan kriptografik tizim. Unda kalitlarning birortasi ham boshqasidan yetarli vaqt mobaynida hisoblab chiqarilishi mumkin emas. Maxfiy kalit sir saqlanadi, ochiq kalit esa, o‘zaro ishlovchi barcha abonentlarga yuborilishi mumkin. Ochiq kalitdan foydalanib ixtiyoriy abonent, ochiq kalitning muallifiga muhofazalangan xabarni jo‘natishi mumkin. Bunda, bu xabarni faqat ochiq kalitga mos keluvchi maxfiy kalitga ega bo‘lgan tomon dastlabki matnga o‘girishi mumkin. Bunday kriptotizimlar ikki kalitli, yoki asimmetrik deb nomlanadi. Ochiq kalitli kriptotizimlar, ham nazariy, ham amaliy kriptobardoshlikni ta’minlovchi simmetrik kriptotizimlardan farqli o‘laroq, faqatgina amaliy kriptobardoshlikni ta’minlaydilar.

Parol – ingl.: password rus.: пароль 1. Sir tutiladigan belgilar ketma-ketligi. Parol, uning egasi haqiqiymi yo yo‘qmi, shuni aniqlash jarayonida tekshiruv axboroti sifatida ishlatiladi. 2. Subyekt siri bo‘lmish erkin foydalanish subyekti identifikatori. 3. Erkin foydalanishni aynanlash vositasi. U kompyuter bilan muloqot boshlashdan oldin, unga terminal klaviaturasi orqali yoki identifikatsiya (kodli) kartasi yordamida kiritiladigan harfli, raqamli yoki harfli-raqamli kod shaklidagi maxfiy so‘zdan iborat.

PIN – qisq.: Personal Identification Number. Shaxsiy aynanlash tartib raqami.

Ping – ingl.: ping rus.: пинг (ingl. ping – “taqqillatmoq” so‘zidan) Boshqa kompyuterga tarmoq orqali signalni jo‘natish va javob signalini kutib olish. Odatda bu aloqani tekshirish uchun qilinadi.

Polinomial algoritm – murakkabligi qiymatining tartibi 0(nm) (bu yerda m>1) bo‘lsa.

Port tartib raqami – ingl.: port number rus.: номер порта Bitta kompyuterda tarmoq orqali aloqa qila oladigan bir necha dasturni yurgizish mumkin. Ushbu dasturlarni ajratish uchun ularga yurgizilish paytida shaxsiy port tartib raqami beriladi. Ba’zan port tartib raqami URLda kompyuter nomidan keyin yoziladi. Masalan, http://www.website.com:80/ URL tarkibida 80 soni bor. Bu port tartib raqami, u kompyuter nomidan ikki nuqta bilan ajratiladi.

Qadimgi dunyo steganografiyasi – Yunon tarixchisi Gerodotning keltirishicha, axborotni yashirishning bir necha xil usullari mavjud bo‘lgan. Misol uchun, ular qullarning boshiga kerakli axborotni yozishgan, qulning sochi o‘sgach esa u manzilga jo‘natilgan. Manzilga yetgach uning sochi olinib, ma’lumot yetib borgan deya hisoblangan.

Qo‘riqlanadigan axborot – ingl.: protected information rus.: охраняемая информация 1. Axborot mulkdori yoki mulkdor vakolat bergan shaxs tomonidan, kuchga ega qonunchilikka binoan muhofaza qilish maromi o‘rnatilgan axborot. 2. Erkin foydalanish va almashuv bilan bog‘liq jarayonlarda, ishlatilishi, qonunchilik bilan o‘rnatilgan qoidalarga mos bajariladigan axborot.

Rabin algoritmi – Bu shifrlash usuli 1979 yilda Maykl Rabin tomonidan chop etilgan. Algoritmning xavfsizligi katta tub sonlarga va ko‘paytuvchilarga ajratish muammosiga asoslangan.

Raqamli imzo – ingl.: digital signature rus.: цифровая подпись qarang: elektron raqamli imzo.

Raqamli steganografiya – – klassik steganografiyaning yo‘nalishi bo‘lib, raqamli obyektlarga axborotlarni yashirish yoki zarar yetishdan asrash asosida yaratilgan. Bu obyektlar multimedia obyektlari bo‘lib (tasvir, video, audio, 3D – obyektlar teksturasi) hisoblanadi.

Raqamli tarmoq – ingl.: digital network rus.: цифровая сеть Diskret signallar uzatadigan va ularga ishlov beradigan kommunikatsiya tarmog‘i. Raqamli tarmoqlar, avvalgi analogli tarmoqlarga nisbatan yetarlicha afzalliklarga ega. Ularga birinchi navbatda, shovqinga yuqori bardoshligi, mikroprotsessor va xotira qurilmalaridan keng foydalanish, kanal hosil qiluvchi apparatlarning oddiyligi kiradi. O‘lchamlariga qarab mahalliy, hududiy va global tarmoqlar faqlanadi.

Rasmiy kriptografiya – (XV asr oxiridan XX asr boshlarigacha) bosqichi rasmiylashgan va qo‘lda bajariluvchi shifr kriptotahlilini paydo bo‘lishi bilan bog‘liq. **RSA** – qisq.: Rivest-Shamir-Adleman RSA algoritmi. Ochiq kalit asosida shifrlash algoritmi, 1977 yilda ishlab chiqilgan. Algoritmning nomi uning mualliflari familiyalarining birinchi harflaridan hosil bo‘lgan: Ron Rivest, Adi Shamir, Leonard Adleman.

Sehrli kvadrat – Satr va ustun sonlari teng bo‘lgan jadval chiziladi. Jadval kataklari 1.sonidan boshlab ketma-ket natural sonlar bilan to‘ldiriladi. Bunda agar kataklar ichidagi sonlarni gorizontal, vertikal va diagonal yig‘indisi hisoblanganda bir xil son chiqsa sehrli kvadrat deyiladi.

SET – qisq.: Secure Electronic Transaction qarang: xavfsiz elektron kelishuv.

Shaxsiy identifikatsiya raqami – ingl.: personal ID rus.: персональный идентификационный номер Biror kimsaning shaxsiy kodi bo‘lib, undan erkin foydalanish boshqariladigan tizimdan erkin foydalanish uchun imkoniyat yaratishga xizmat qiladi.

Shaxsiy imzo kaliti – ingl.: private signature key rus.: личный ключ подписи Aniq shaxsga tegishli bo‘lgan va elektron raqamli imzoni yaratishda qo‘llaniladigan ramzlarning tartiblangan to‘plami.

Shaxsiy kalit – ingl.: private key rus.: личный ключ Shifrlangan matnni ochiq matnga o‘girish uchun mo‘ljallangan faqat uning egasi tomonidan qo‘llaniladigan va sir tutiladigan kalit.

Shifr – ingl.: cipher rus.: шифр Axborotni ko‘rib, uning ma’nosini anglashni muhofaza etish maqsadida qandaydir maxfiy elementdan foydalangan holda qayta o‘zgartirish usuli. Bu holda dastlabki axborot ochiq matn deb ataladi, unga shifrni tatbiq qilish natijasi esa, yopiq matn yoki shifrmatn deb ataladi.

Shifrlangan matnga hujum – ingl.: attack on encrypted text rus.: атака на зашифрованный текст Faqat shifrlangan matn asosida kriptoanalitik uyushtirayotgan tahliliy hujum.

Shifrlash – ochiq matn, deb ataluvchi dastlabki ma’lumotni shifrlangan ma’lumot (kriptogramma) holatiga o‘tkazish jarayoni.

Shifrlash algoritmi – ingl.: ciphering algorithm rus.: алгоритм шифрования Shifrning rasmiy tavsifi.

Shifrmatn – ingl.: cipher text rus.: шифртекст qarang: shifrlangan matn.

Shifrni kalitsiz ochish – ingl.: decryption rus.: дешифрование 1. Shifrlash kalitisiz ma’lumotlarni dastlabki, ya’ni shifrlashdan oldin bo‘lgan shaklga keltirish; 2.Shifrlashga teskari amal.

ShiftRows – algoritmda berilgan jadvalga ko‘ra holat baytlarini siklik surish;

Signal – ingl.: signal rus.: сигнал 1. Ma’lumotlarni aks ettirish uchun ishlatiladigan fizikaviy kattalikning o‘zgarishi. 2. Parametrlari xabarni mos ravishda aks ettiruvchi xohlagan fizikaviy jarayonni bildiruvchi moddiy axborot tashuvchisi. O‘zining fizikaviy tabiatiga ko‘ra signal elektr, akustik, optik, elektrmagnit va boshqa bo‘lishi mumkin.

Signallarni filtrlash – ingl.: signal filtering rus.: фильтрация сигналов Signallarni umumiy oqimidan kerakli mezonlarga ega bo‘lganlarini ajratib qo‘yish jarayoni. Signallarni filtrlash quyidagi zaruriyatlardan hosil qilingan sharoitlarda

ishlatiladi: - modulatsiyada tashuvchining ustiga qoplangan signalni ajratish; - yagona jismoniy kanal orqali uzatish uchun multiplekslashda birlashtirilgan signallarni ajratib olish; - signalga keyinchalik uning shaklini yoki tavsifnomalarini o‘zgartirish uchun lozim bo‘lgan ishlov berish; - kuchli shovqinlangan signaldan foydalisini ajratib olish. Signallarni filtrlash jismoniy pog‘onada bajariladi.

Simmetrik shifr – ingl.: symmetric code rus.: симметричный шифр Axborotni shifr-matnga o‘girish va dastlabki matnga o‘girish uchun bir xil kalit ishlatiluvchi shifr.

Sodda kriptografiya – (XV asr boshlarigacha) uchun shifrlangan matn mazmuniga nisbatan dushmanni chalkashtiruvchi ixtiyoriy, odatda sodda usullarning qo‘llanilishi xosdir. Dastlabki bosqichda axborotni himoyalash uchun kodlashtirish va steganografiya usullari qo‘llanildi.

SSH – qisq.: Secure Shell Kompyuterni masofadan boshqarish va fayllarni uzatish imkonini beruvchi tarmoq bayonnomasi. Funksionalligi bo‘yicha Telnet va rlogin bayonnomasiga o‘xshash, biroq kuchli kriptografiyadan foydalanadi. SSH bayonnomasining kriptografikaviy muhofazasi mustahkamlanmagan bo‘lib, turli shifrlash algoritmlarini tanlash imkoni mavjud. Ushbu bayonnomaning mijozlari va serverlari turli maslaklar uchun ochiq, u nafaqat mashinada xavfsiz uzoqlashgan shellga ega bo‘lishni, balki grafik interfeysini tunnellash (X Tunnelling) imkonini ham beradi (faqat Windows grafik interfeysidan foydalanuvchi UNIXga o‘xshash OT yoki qo‘llanmalar uchun).

SSL – qisq.: Secure Sockets Layer Muhofaza qilingan soketlar bayonnomasi, SSL bayonnomasi. Netscape Communications korporatsiyasi tomonidan axborotni shifrlash va uni Internet orqali xavfsiz uzatish uchun ishlab chiqilgan standart.

Steganografiya – (grekcha axsyavoa – yashirin – yozayapman, sirli yozuv degan manoni anglatadi) – bu ochiq ma’lumotni uzatilayotgan vaqtda shifrni yoki sirni ichiga joylashtirib uzatishni o‘rganuvchi fan hisoblanadi.

SubBytes – algoritmda qayd etilgan 16x16 o‘lchamli jadval asosida baytlarni almashtirish, ya’ni S -blok akslantirishlarini amalga oshirish.

SubBytes (S -blok akslantirishlari jadvali) – akslantirishi har bir holat baytlariga bog‘liqsiz holda baytlarni chiziqli bo‘lmagan amallar asosida o‘rin almashtirishlarni amalga oshiradi.

Tahliliy hujum – ingl.: analytic attack rus.: аналитическая атака Tahliliy uslublar yordamida kodni ochish yoki kalitni topishga urinish. Misollar – tasvirlarning statistik tahlili, shifrlash algoritmida kamchiliklarni topish.

Tizim – ingl.: system rus.: система Ma’lum natijaga erishish uchun birlashtiriluvchi bir butun yoki jami turli xil obyektlar sifatida o‘rganiluvchi ixtiyoriy obyekt.

TLS – 1. Thread Local Storage – Oqimning mahalliy xotirasi. 2. Transport Layer Security – Transport pog‘onasida xavfsizlik, TLS bayonnomasi.

Xabar autentifikatsiyasi – ingl.: message authentication rus.: аутентификация сообщения Xabarning mo‘ljallangan manba tomonidan oldindan belgilangan oluvchiga yuborilganligini va ushbu xabarning uzatish paytida o‘zgartirilmaganligini tekshirish.

Xabar jo‘natuvchisi – Xabarni jo‘natmoqchi yoki saqlashdan oldin xabar hosil qilmoqchi bo‘lgan (yoki uning nomidan harakat qilgan) shaxs, ammo, xabarga nisbatan vositachi shaxs bunga kirmaydi.

Xabar oluvchi – ingl.: message receiver rus.: адресат сообщения Xabarni jo‘natuvchi shaxs xabar oluvchi deb mo‘ljallayotgan shaxsni bildiradi, biroq xabarga vositachi bo‘lgan shaxs hisobga olinmaydi.

Xabar xesh-funksiyasi – ingl.: message hashing function rus.: хэш-функция сообщения Qiymati kirish ketma-ketligining, ya’ni, ikkilik sanoq tizimida berilgan xeshlantiriluvchi sonning har bir bitiga yoki xeshlantiriluvchi dastlabki matnni har bir ramziga bog‘liq bo‘lgan funksiya. Xeshlantirish algoritmi kirish matnidan birxil uzunlikda natija chiqaradi. Bunda uzunlik deganda, ikkilik sanoq tizimida berilgan ifodadagi bitlar soni nazarda tutiladi.

Xavfsizlik dasturi – foydalanuvchining tizimdagi barcha huquqlari va qurshovini aniqlovchi xavfsizlikning shaxsiy vositasi, masalan smart- karta.

Xavfsizlik tizimi – ingl.: security system rus.: система безопасности 1. Qonunga muvofiq xavfsizlikni ta’minlashda ishtirok etadigan qonunchilik, ijrochilik va sud hokimiyati organlari, ijtimoiy va boshqa tashkilot va uyushmalar, fuqarolar, shuningdek, xavfsizlik sohasidagi munosabatlarni tartibga soluvchi qonunlar. 2. Xavfsizlik siyosatini amalga oshirishga qaratilgan jami tashkiliy choralar, texnikaviy va dasturiy vositalar.

Xesh-funksiya – ingl.: hashing function rus.: хэш-функция qarang: xabar xesh-funksiyasi.

Yopiq kanal – ingl.: closed channel rus.: закрытый канал Ma’lumotlardan ruxsatsiz erkin foydalanishdan muhofazalangan mantiqiy kanal. Bunday mantiqiy kanallarning bayonnomalari transport pog‘onasidan yuqorida joylashgan bo‘ladi va o‘zaro aloqadagi foydalanuvchilar orasidagi uzatishni maxfiyligini kafolotlaydi.

Chiziqli algoritm – murakkabligi qiymatining tartibi 0(n) bo‘lsa.

Adabiyotlar ro’yxati

1. Акбаров Д. Е. Ахборот хавфсизлигини таъминлашнинг криптографик усуллари ва уларнинг қўлланилиши – Т 2008
2. Арипов М.М., Пудовченко Ю.Е. Основы криптологии – Ташкент: 2004.
3. Бабаш А.В., Гольев Ю.И., Ларин Д.А. Шанкин Г.П. Криптографические идеи XIX века. Защита информации. Конфидент. 2004 г
4. Шнайер Б. Прикладная криптография. Протоколы, алгоритмы, исходные тексты на языке Си. –М.: издательство ТРИУМФ, 2003

Жельников В. Криптография от папируса до компьютера. М. ABF, 1997. – 336 с.

5. Алферов А.П., Зубов А.Ю., Кузьмин А.С., Черемушкин А.В. Основы криптографии: Учебное пособие, 2-е изд. –М.: Гелиос АРВ, 2002.-480 с.
6. Vernam G.S. Cipher printing telegraph systems for secret wire and radio telegraphic communications, «J. Amer. Inst. Elec. Eng., vol. 55, pp. 109-115, 1926.
4. Шенон К. Э. Теория связи в секретных тизимх. В кн.: Шенон К.Э. Работы по теории информации и кибернетике. М.: ИЛ, 1963, том 1. - С. 333-402.
5. Шенон К.Э. Теория связи в секретных тизимх. В кн.: Шенон К.Э. Работы по теории информации и кибернетике. М.: ИЛ, 1963, том 2. -С. 243-332.
6. Diffie W. and HellmanM.E. «New directions in cryptography» IEEE Trans. Informat. Theory, vol. IT-22, pp. 644-654, Nov. 1976.
7. R. C. Merkle «Secure communication over insecure channels», Comm. ACM, pp. 294-299, Apr. 1978.
8. Дейтель Г. Введение в операционные системы. Том 2. М.: Мир, 1987, с. 357-371.
9. Феллер В. Введение в теорию вероятностей и ее приложения. Том 2. М.: Мир, 1984.
10. Кнут Д. Искусство программирования для ЭВМ. Том 1. Основные алгоритмы. М.: Мир, 1976.

11. Гэри М. , Джонсон Д. Вычислительные машины итруднорешаемые задачи. М.: Мир, 1982.

12. Simmons G. J. «Authentication theory/coding theory, in Advances in Cryptology, Proceedings of CRYPTO 84, G. R. Blakley and D. Chaum, Eds. Lecture Notes in Computer Sciense, No. 196. New York, NY: Springer, 1985, pp. 411-431

13. Бабаш А.В., Шанкин Г.П. Криптография. –Москва: Лори Гелиос АРВ, 2002. –512 с.

14. Шнайер Б. Прикладная криптография. Протоколы, алгоритмы, исходные тексты на языке Си. –М.: издательство ТРИУМФ, 2003 - 816 с.

15.Молдовян Н.А., Молдовян А. А., Еремеев М.А. Криптография: от примитивов к синтезу алгоритмов. –СПб.: БХВ-Петербург, 2004. - 448 с.

16.Новиков П.С. Элементы математической логики. - М. ИЛ, 1973.

17.Логачёв О. А., Сальников А.А., Ященко В.В. Булевы функции в теории кодирования и криптологии. – М. Изд. МЦНМО, 2004. – 470 с.

18.Фомичев В. М. Дискретная математика и криптология. – Москва, “ДИАЛОГ-МИФИ”, 2003. – 400 с.

19.Коблиц Н. Курс теории чисел и криптографии. – М. Научное изд-во ТВП, 2001г. – 261 стр.

20.Харин Ю.С., Берник В.И., Матвеев Г.В., Агиевич С.Г. «Математические и комьютерные основы криптологии» ООО «Новое знание» 2003 г. 381 стр.

21.Молдавян А.А., Молдавян Н.А., Гуц Н.Д., Изотов Б.В. «Криптография. Скоростные шифры» Санкт-Петербург. «БХВ-Петербург» 2002г. 439 стр.

22.Молдавян А.А., Молдавян Н.А.Введение в криптосистемы с открытым ключом. Санкт – Петербург «БХВ-Петербург» 2005г. 288с.

23.Ростовцев А. Г., Маховенко Е. Б., Теоретическая криптография. НПО «Профессионал», Санкт-Петербург. 2004г. - 478 стр.

24. Василенко О. Н. Теоретико-числовые алгоритмы в криптографии. – М., МЦНМО, 2003. – 328 с.

25. Зензин О.С., Иванов М.А.. Стандарт криптографической защиты – AES.

Конечные поля /Под ред. М.А. Иванова – М.: КУДИЦ-ОБРАЗ, 2002. -176 с.

26. Акбаров Д.Е. Криптография, Стандарты алгоритмов криптографической защиты информации и их приложения. –Ташкент, 2007. -188 с.

27. Венбо Мао. Современная криптография. Теория и практика. –Москва– Санкт-Петербург–Киев: Лори Вильямс, 2005. –768 с.

28. Иванов М. Криптографические методы защиты информации в компьютерных тизимх и сетях. – М., «Кудиц-Образ», 2001, –368с.

29. Столлингс В. Криптография и защита сетей: принципы и практика. – М. , Изд. дом «Вильямс», 2001. – 672 с.

30. Анохин М.И., Варновский Н.П., Сидельников В.М., Ященко В.В. Криптография в банковском деле. – М., Изд. МИФИ, 1997.

31. O‘zDSt 1106 : 2006. Государственный Стандарт Узбекистана. Информационная технология. Криптографическая защита информации. Функция хэширования. – Ташкент. Узбекское агентство стандартизации, метрологии и сертификации. 2006.

32.ShafiGoldwasser, MihirBellare. Lecture Notes on Cryptography. Cambridge, Massachusetts, August, 1999. – 268 p.

33. Menezes A., P. van Oorshot, Vanstone S. Handbook of Applied Cryptography. CRCPress, 1996. – 780 p.

34. Молдовян А.А., Молдовян Н.А., Советов Б.Я.. Криптография. – Санкт-Петербург, Изд. «Лань», 2001. – 224 с.

35. ГОСТ Р 34.11 – 94. Государственный Стандарт Российской Федерации. Информационная технология. Криптографическая защита информации. Функция хэширования. – Москва. Издательство стандартов, 1994.

36. Federal Information Processing Standards Publication 180-2. Secure Hash Standard. 2002 August 1.

37. Federal Information Processing Standards Publication 198. The Keyed-Hash Message Authentication Code (HMAC). 2002 March 6.

38. Ященко В.В. и др. Введение в криптографию. – М., МЦНМО, 2000. – 288 с.

39. Чмора А. Современная прикладная криптография. – М., Гелиос АРВ, 2002. – 256 с.
40. Аграновский А.В., Хади Р.А. «Практическая криптография» Москва. СОЛОН- Пресс.2002г. - 254 стр.
41. Ростовцев А., Михайлова М. Методы криптоанализа классических шифров.
42. Хасанов Х. П. Такомиллашган диаматрицалар алгебралари ва параметрли алгебра асосида криптотизимлар яратиш усуллари ва алгоритмлари. – Тошкент, 2008. -208 б.

MUNDARIJA