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

**MIRZO ULUG‘BEK NOMIDAGI
O‘ZBEKISTON MILLIY UNIVERSITETI**

**M. Aripov, A.S. Matyakubov**

# AXBOROTLARNI HIMOYALASH USULLARI

**Toshkent
“Universitet”
2014**

**M. Aripov, A.S. Matyakubov. Axborotlarni himoyalash usullari. Toshkent: Universitet, 2014. 96 bet.**

O‘quv-uslubiy qo‘llanma “Amaliy matematika va informatika”, “Informatika va axborot texnologiyalari”, “Axborot xavfsizligi”, “Axborot tizimlarining matematik va dasturiy ta’minoti” yo‘nalishlarida ta’lim olayotgan oliy o‘quv yurtlari talabalari uchun mo‘ljallangan.

T a q r i z c h i l a r :

| | |
|---|---|
| R.D. Aloyev | fizika-matematika fanlari doktori |
| M.S. Xodjayeva | fizika-matematika fanlari nomzodi |

*Mazkur o‘quv-uslubiy qo‘llanma Mirzo Ulug‘bek nomidagi O‘zbekiston Milliy universiteti Mexanika-matemetika fakulteti Ilmiy kengashida ko‘rib chiqilgan va chop etishga tavsiya etilgan. 2011 yil 31 yanvar 7-sonli bayonnoma.*

*Mazkur o‘quv-uslubiy qo‘llanma Mirzo Ulug‘bek nomidagi O‘zbekiston Milliy universiteti O‘quv-uslubiy kengashida ko‘rib chiqilgan va chop etishga tavsiya etilgan. 2012 yil 9 mart 6-sonli bayonnoma .*

ISBN-978-9943-305-66-3

# 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'l-lanilishi 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 muammo-larini dolzarb qilib qo'ydi.

Respublikamizda aholiga axborot xizmati koʻrsatish sifatini oshirish, axborot xavfsizligini ta’minlashda axborotlashtirish sohasi mutaxassislari tomonidan yaratilayotgan ixtirolarining oʻrni beqiyos. Oʻzbekiston Respublikasining milliy kriptografik algoritmlarini yaratish, ularni takomillashtirish va axborotni kriptografik muhofazalashning milliy dasturiy va apparat-dasturiy vositalarini ishlab chiqish Oʻzbekiston Respublikasi Prezidentining 2007 yil 3-apreldagi «Oʻzbekiston Respublikasida axborotning kriptografik muhofazasini tashkil etishga oid chora-tadbirlar toʻgʻrisidagi» 614-sonli qarorida birinchi galdagi vazifa qilib qoʻyilgan.

Kriptografiya (kriptografiya - *kryptos* – maxfiy, *grapho* – yozish kabi grekcha soʻzlardan olingan) shifrlash usullari haqidagi fan sifatida paydo boʻldi va uzoq vaqt mobaynida shifrlash ya’ni, uzatiladigan va saqlanadigan axborotlarni ruxsat berilmagan foydalanuvchilardan himoyalashni oʻrganadigan fan sifatida shakllandi. Lekin, keyingi yillarda axborot texnologiyalarning gurkirab rivojlanishi maxfiy axborotlarni yashirish bilan toʻgʻridan–toʻgʻri bogʻliq boʻlmagan koʻpgina yangi kriptografiya masalalarini keltirib chiqardi.

Shifrlashning oddiy metodlaridan qadimgi davrlarda ham foydalanilgan. Lekin kriptografik metodlarni tadqiq etish va ishlab chiqishga ilmiy yondashish oʻtgan asrdagina (XX asr) paydo boʻldi. Ayni vaqtda kriptografiya ham fundamental, ham amaliy natijalar (teoremalar, aksiomalar) toʻplamiga ega. Jiddiy matematik tayyorgarlikka ega boʻlmasdan turib kriptografiya bilan shugʻullanib boʻlmaydi. Xususan, diskret matematika, sonlar nazariyasi, abstrakt algebra va algoritmlar nazariyasi sohasidagi bilimlarni egallash muhimdir. Shu bilan birgalikda, kriptografik metodlar birinchi navbatda amaliy qoʻllanilishini esdan chiqarmaslik lozim. Chunki, nazariy jihatdan turgʻun hisoblangan algoritmlar, matematik modelda koʻzda tutilmagan hujumlarga nisbatan himoyasiz boʻlib qolishi mumkin. Shuning uchun, abstrakt matematik model tahlilidan soʻng, albatta olingan algoritmni amaliyotda qoʻllanilishidagi 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‘illanadi. 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 shifirlash va deshifirlash 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 matinni 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

Axborot xavfsizligi 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

Kriptografik tizim, yoki qisqacha, kriptotizim shifrlash ham shifrni ochish algoritmlari, bu algoritmlarda ishlatiladigan kalitlar, shu kalitlarni boshqaruv tizimi hamda shifrlanadigan va shifrlangan matnlarning o‘zaro bog‘langan majmuasidir.

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 shifr ochish 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‘lsa-da, 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 5-6 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 larning paydo bo‘lishi bilan muvaffaqqiyatli kriptografik hujum qilish imkoni paydo bo‘ldi.

*Ilmiy kriptografiya*ning (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-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 |

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-13 | s-18 | v-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 |

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?

## Mustaqil ish uchun misollar.

1. Kalit so‘z “pelikan”: C=”ioijryx oiollgf kyfa aui tttiea laaa lbr lad qqiti” M=?
2. Kalit so‘z “flashki”: C=”rxjyioilflgoioai aukyf eliatttb llraa aiiqt adq” M=?
3. Kalit so‘z “uylandi”: C=” iiyrjxo oogllfi fkuaaiy ttaeilt aarblla qati qid” M=?
4. Kalit so‘z “uylandi”: C=” hulsyb elmezidu nono xhmr onas alct aehin” M=?
5. Kalit so‘z “flashki”: C=” sbylue hzdie mulo hxno mnaa snolre ihatnc” M=?
6. Kalit so‘z “pelikan”: C=” uehysl bmu lized omnxo nholrs anatn cheai” M=?

7. Kalit so‘z “pelikan”: C=”sensaomceunftmros aneili absed eithntd eilva rrfinioy siuecddoetkeopefhsoettnaeardwlefutlgiuctnof” M=?
8. Kalit so‘z “pelikan”: C=” utnoegolbrnuihsesenacbalailv” M=?
9. Kalit so‘z “pelikan”: C=” eielvtrteofrhtrrcoedenrsuike” M=?
10. Kalit so‘z “pelikan”: C=”wrorrhealreedienthgfislsyetiumtrsce” M=?
11. Kalit so‘z “pelikan”: C=”arrcourcebydosfrptuirteysselcsruttm” M=?
12. Kalit so‘z “pelikan”: C=” arrcour sebydus npyilgppr ngoaweaetm rre t th ofs” M=?
13. Kalit so‘z “pelikan”: C=” yoanmlofcsoktoeeilfshbsemtuy” M=?
14. Kalit so‘z “pelikan”: C=”fnotni acdhetonors penriigfnlde sstym ednhet eottnaiis” M=?
15. Kalit so‘z “pelikan”: C=” fcupkia teoncelfti fdenmsroftrde arhdha iedvtr” M=?
16. Kalit so‘z “pelikan”: C=” fcupkiateo ncalcninsoihrctea rvdrid ermn orfai” M=?

## 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 |

2.2. 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 |

2.3. 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 |

2.4. 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?

**Mustaqil ish uchun misollar.**

1. Kalit so‘z “7253416, 31425”: C=” muli zed olrsa naueh yslbom nxonh tncheai” M=?
2. Kalit so‘z “3724156, 43125”: C=” xohn onm saaronliz dlme uysbh ulehe ictan” M=?

## 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 yig‘indisi 15 soniga teng chiqadi.

| | | |
|---|---|---|
| 8 | 1 | 6 |
| 3 | 5 | 7 |
| 4 | 9 | 2 |

Yig‘indi quyidagi formula orqali topiladi: $S = \frac{1+n^2}{2} \cdot n$, bu yerda 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<br>i | 1<br>s | 6<br>n |
| 3<br>i | 5<br>e | 7<br>d |
| 4<br>p | 9<br>a | 2<br>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?

## Mustaqil ish uchun misollar.

1. C=gaaf i qidlenr inatti riilabat lrhrlzi ouvtiib kgalg rana, M=?
2. C=hvab onni lmneis aauril vvaahn oqrlsao hsyxtb shaaoa razg, M=?
3. C=alsian nlbtiy mfaia enuan xgstimi lriiivel admetarlnaak, M=?
4. C=udtboo nlaoilbd lakanru arsyovulmd boindbhol krooubva diilaiaarlrud balyarjb xasaruuma rbgaimxhuxr ndoread moiafoaav raliiinmmfnsh vibmldlibsixaialo vailsoitrbd rfsaryom eabaixqu htyziav, M=?
5. C=tiih m omn daisma idgn iattaiq bxssdra aooqdvgs yqain raan, M=?
6. C=hscqibt hackaiquihs godsdhtmcambd aara alu erhm aiqamin uankli aqrozibm nrdiinlst ymlhodaauiaqao iuaibivnsnkidmbnnyarou hsalgo idoztjzmnom gankor oeikadaxaq dkimlthe qironaan nadiacsradtt, M=?
7. C=ilrrtaa ilimlsdkagk iryslloanabosi biahagnugnixhob mqlranzablsirs aiainhlnia hyahlnriio umrnaudaamao blkaosbliqshqsadsqq hsdh qag sioz isboouarta abzid aeskzlb ondoyntg lhinairs gtotoiam, M=?

## 2.5. Sezar shifri

Almashtirish usullari sifatida quyidagi usullarni 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?

## Mustaqil ish uchun misollar.

1. k=5, n=26: C=jsyjw, M=?
2. k=5, n=26: C=rtsnytw, M=?
3. k=5, n=26: C=xuehj, M=?
4. k=5, n=26: C=wzhmpe, M=?
5. k=5, n=26: C=vfqfr, M=?

6. k=6, n=26: C= ygrus, M=?
7. k=6, n=26: C= jkqgt, M=?
8. k=7, n=26: C= wypualy, M=?
9. k=7, n=26: C= uvrph, M=?
10. k=7, n=26: C= alslmvu, M=?
11. n=26: C=mjnad afxmds mjgvgyzuz smeaeukwadu zuetxmdu M=?
12. n=26: C=nkobebgk nisfvmyvt vfbknfvqntvk bmvetvkbyng M=?
13. n=26: C=olpcfchlojtgwnzwuwyohucfwmozofw M=?
14. n=26: C=pmqdgdiapgmxbdnphxpqhigpzibdsaapgx M=?
15. n=26: C= rkpyixdydwudwaefjqhgqbwqdkikbbqhy M=?
16. n=26: C=bizgkfcfxzprrjfjcrizrjfjzpkljyletyrcri M=?
17. n=26: C=sdygjalenscsdaldsjcjahlglarae M=?
18. n=26: C=lbffmk bdtezhkbmf etkhvabjdteb mebtezh kbmfetk M=?
19. n=26: C=elcjninurfcfufailcngrupzmctfcac M=?

## 2.6. Affin tizimi

Affin tizimidagi Sezar usulida har bir harfga almashtiriluvchi harflar maxsus formula bo‘yicha aniqlanadi: (a·t+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, quyidagi jadval hosil qilinadi:

| t | 3t+5 |
|---|---|
| 0 | 5 |
| 1 | 8 |
| 2 | 11 |
| 3 | 14 |
| 4 | 17 |
| 5 | 20 |
| 6 | 23 |
| 7 | 26 |

Shunga mos ravishda harflar quyidagicha almashadi:

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

| | |
|---|---|
| 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 |

| | |
|---|---|
| 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: $M = \left(a^{-1}(C - b)\right) mod\ m.$ 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?

## Mustaqil ish uchun misollar.

1. a=5, b=11, n=26:  C= zxuyzyptlnxlaz,  M=?
2. a=5, b=12, n=26: C= jakdeqtmuumeczm,  M=?
3. a=7, b=12, n=26: C= smimlmlmbnmzolq,  M=?
4. a=9, b=11, n=26: C= frwrahgfthigfz,  M=?
5. a=11, b=11, n=26: C= clcflulgabuly,  M=?
6. a=17, b=11, n=26: C= rfayryjhluhnyr,  M=?
7. a=19, b=11, n=26: C= mlerwlirwhzl,  M=?
8. a=21, b=11, n=26: C= olonlctzxijxixzc,  M=?
9. a=23, b=11, n=26: C= plrglgnheljq,  M=?
10. a=3, b=11, n=26: C= zjyubznvtgjqjul,  M=?
11. a=3, b=14, n=26: C= ehanoqmebtmlmygo,  M=?
12. a=5, b=17, n=26: C= wjdatryfdaoreluf,  M=?
13. a=7, b=19, n=26: C= otpwdistijtlxixpq,  M=?
14. a=19, b=17, n=26: C= rlrssrcnenkrgrcnvu, M=?
15. a=25, b=11, n=26: C= slqtdnlhsdalid,  M=?
16. a=23, b=12, n=26: C= swpcmrokwjwh,  M=?
17. a=15, b=14, n=26: C= wijobwxwmwbnxoje,  M=?
18. a=17, b=8, n=26: C= zyliamtgivwmlciteinil,  M=?
19. a=19, b=17, n=26: C= krgrcnvuzrknsrc,  M=?

## 2.7. Steganografiya

Steganografiya (grekcha στεγανοσ — yashirin va γραφω — 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
$C_5$=(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?

## Mustaqil ish uchun misollar.

K=bmgnkjkljklpqweygwygfcsbcsvctysafascdabvudfhtyhptyojulksnxvfczdaxasawqeswdvgcbdfhvbdhjvbedvafszxaqeweretbcnv:

1. C=qowyrkkafnszmmhstjsyxirndrtcciwxbwpcxkobgt, M=?
2. C=uazydwkmfhfouhwepszlnnkguspqbtatvnurgdn, M=?

K=werrtgfbvfgbvfjszdgfhfdvbxvdfidrjmfcgibugtosieewqwswerdswaskxdpflhptukjkhfmns:

1. C=bskwupbsjavrnkzasfaf, M=?
2. C=xsidnartyodkjcrteufnb, M=?
3. C=fugtpfouywthmjwia, M=?

# III BOB. KRIPTOGRAFIK PROTOKOLLAR

## 3.1. 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.

## 3.2. 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.

## 3.3. 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.

### 3.4. 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.

### 3.5. 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.

# IV BOB. KALITLARNI BOSHQARISH

## 4.1. 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.

## 4.2. 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.

## 4.3. 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 yashirish

lozim. 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.

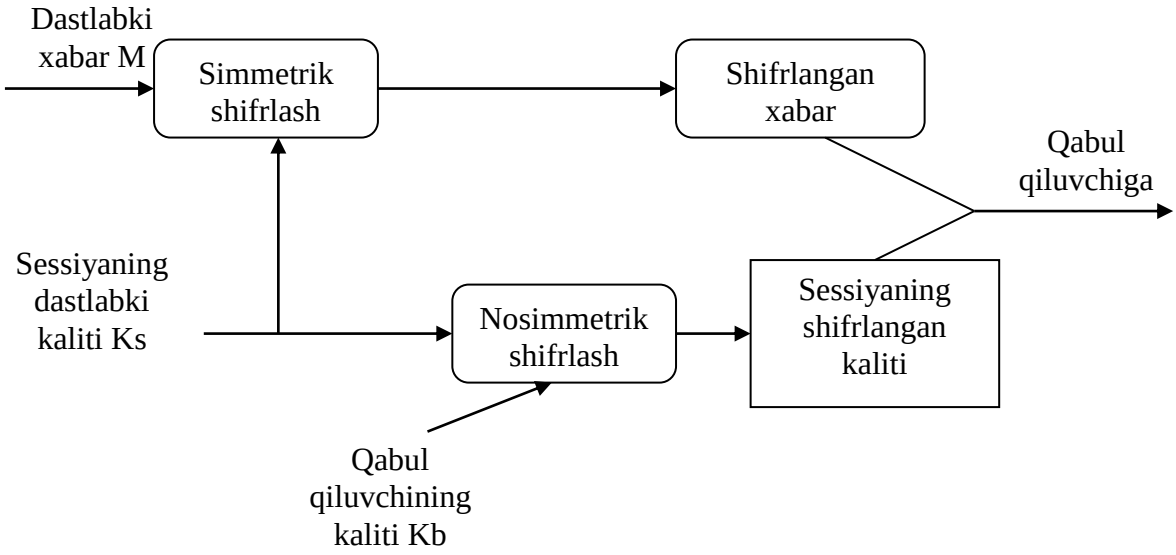
**Kombinatsiyalangan usul bo‘yicha xabarni shifrlash sxemasi**

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:

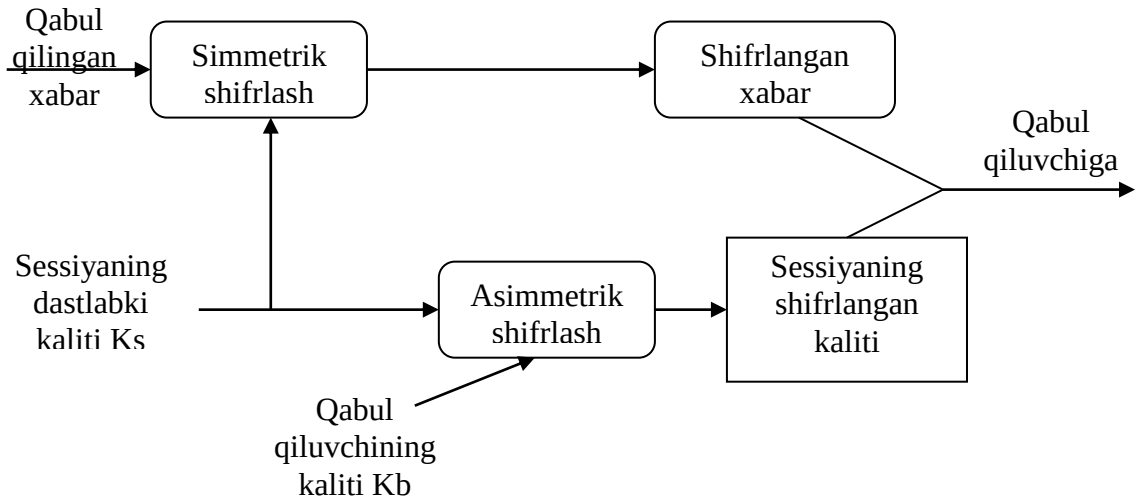


### Kombinatsiyalangan usul bo‘yicha xabarni ochish

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.

## 4.4. 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.;
- 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.

# V BOB. NOSIMMETRIK ALGORITMLAR

## 5.1. 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 $a,b \in Z$ bo‘lib, $a \neq 0$ 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 $0 \leq r_1 < r$, $r_1=0$ 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 $0 \leq r_2 < r_1$, $r_2=0$ 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,

$$a \equiv b \bmod n$$

deb yoziladi. Bundan esa, *a* va *b* sonlar ayirmasining *n* ga qoldiqsiz bo‘linishi kelib chiqadi.

Qoldiqni ifodalash uchun ushbu

$$b = a \bmod n$$

tenglikdan foydalaniladi hamda $b=a \bmod n$ tenglikni qanoatlantiruvchi *b* sonini topish *a sonini modul n bo‘yicha keltirish* deyiladi. Ixtiyoriy butun *b* soni uchun ushbu

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

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

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

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

$$(a+b)\bmod n=((a \bmod n)+(b \bmod n))\bmod n,$$

$$(a-b)\bmod n=((a \bmod n)-(b \bmod n))\bmod n,$$

$$(ab)\bmod n=((a \bmod n)\cdot(b \bmod n))\bmod n,$$

$$(a(b+c))\bmod n=((ab) \bmod n+(ac) \bmod n)\bmod n.$$

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, $b = a^{-1}$ 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. $F(n)=n(1-1/p_1)(1-1/p_2)\ldots(1-1/p_k)$,

agar $n=\prod_{i=1}^{k} p_i^{t_i},\ k, t_i \in N,\ p_i\ (i=1,..,k)-$ 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 $x^2 \bmod p = a$ 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 $g^a \bmod p = b$ 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,

$$a^x \bmod \mathrm{n} = \mathrm{b}$$

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: $T=f(n)$ 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 $T=f(n)=5n^2+6n+11$ bo'lsa, u holda uning $n^2$ tartibli hisoblash murakkabligi $O(n^2)$ 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 $O(1)$;
2. Algoritm ***chiziqli*** deyiladi, agarda uning murakkabligi qiymatining tartibi $O(n)$ bo‘lsa;
3. Algoritm ***polinomial*** deyiladi, agarda uning murakkabligi qiymatining tartibi $O(n^m)$ (bu yerda $m>1$) bo‘lsa;
4. Algoritm ***eksponensial*** deyiladi, agarda uning murakkabligi qiymatining tartibi $O(t^{f(n)})$ (bu yerda $const=t>1$ va $f(n)$ – boshlang‘ich qiymat o‘lchovi $n$ ga nisbatan polinomial funksiya) bo‘lsa;
5. Murakkabligi qiymatining tartibi $O(t^{f(n)})$ bo‘lgan *eksponensial* algoritmlar to‘plamiga qism to‘plam bo‘ladigan algoritmlar ***superpolinomial*** deyiladi, agarda $f(n)$ – 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 бўлса, $a^{-1} \bmod n=?$

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:

$$21^{-1} \bmod 41 = 21^{40-1} \bmod 41 = 21^{39} \bmod 41 = \left(21^3 \bmod 41\right)^{13} \bmod 41 = \left(9261 \bmod 41\right)^{13} \bmod 41 =$$

$$= 36^{13} \bmod 41 = \left(36 \cdot 36^{12}\right) \bmod 41 = \left(36 \cdot \left(36^3 \bmod 41\right)^4\right) \bmod 41 = \left(36 \cdot \left(46656 \bmod 41\right)^4\right) \bmod 41 =$$

$$= \left(36 \cdot 39^4\right) \bmod 41 = \left(36 \cdot 2313441\right) \bmod 41 = \left(36 \cdot 16\right) \bmod 41 = 576 \bmod 41 = 2$$

**Tekshirish:** $(2 \cdot 21) mod 41 = 42 mod 41 = 1$. 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?

**Mustaqil ish uchun misollar.**

Quyida keltirilgan sonlarning teskarisi topilsin:

1. a=21, n=1763 bo‘lsa, $a^{-1}$mod n=?
2. a=22, n=41 bo‘lsa, $a^{-1}$mod n=?
3. a=22, n=1517 bo‘lsa, $a^{-1}$mod n=?
4. a=23, n=41 bo‘lsa, $a^{-1}$mod n=?
5. a=23, n=2911 bo‘lsa, $a^{-1}$mod n=?
6. a=24, n=41 bo‘lsa, $a^{-1}$mod n=?
7. a=24, n=4171 bo‘lsa, $a^{-1}$mod n=?
8. a=25, n=41 bo‘lsa, $a^{-1}$mod n=?
9. a=25, n=4897 bo‘lsa, $a^{-1}$mod n=?
10. a=26, n=41 bo‘lsa, $a^{-1}$mod n=?
11. a=26, n=3403 bo‘lsa, $a^{-1}$mod n=?
12. a=27, n=41 bo‘lsa, $a^{-1}$mod n=?
13. a=27, n=4687 bo‘lsa, $a^{-1}$mod n=?
14. a=28, n=41 bo‘lsa, $a^{-1}$mod n=?
15. a=28, n=9047 bo‘lsa, $a^{-1}$mod n=?
16. a=29, n=41 bo‘lsa, $a^{-1}$mod n=?
17. a=29, n=7739 bo‘lsa, $a^{-1}$mod n=?
18. a=30, n=41 bo‘lsa, $a^{-1}$mod n=?
19. a=30, n=11639 bo‘lsa, $a^{-1}$mod n=?
20. a=11, n=41 bo‘lsa, $a^{-1}$mod n=?
21. a=11, n=1763 bo‘lsa, $a^{-1}$mod n=?
22. a=12, n=41 bo‘lsa, $a^{-1}$mod n=?
23. a=22, n=1517 bo‘lsa, $a^{-1}$mod n=?
24. a=13, n=41 bo‘lsa, $a^{-1}$mod n=?

25. a=13, n=2911 bo‘lsa, $a^{-1}$mod n=?
26. a=14, n=41 bo‘lsa, $a^{-1}$mod n=?
27. a=14, n=4171 bo‘lsa, $a^{-1}$mod n=?
28. a=15, n=41 bo‘lsa, $a^{-1}$mod n=?
29. a=15, n=4897 bo‘lsa, $a^{-1}$mod n=?
30. a=16, n=41 bo‘lsa, $a^{-1}$mod n=?
31. a=16, n=3403 bo‘lsa, $a^{-1}$mod n=?
32. a=17, n=41 bo‘lsa, $a^{-1}$mod n=?
33. a=17, n=4687 bo‘lsa, $a^{-1}$mod n=?
34. a=18, n=41 bo‘lsa, $a^{-1}$mod n=?
35. a=18, n=9047 bo‘lsa, $a^{-1}$mod n=?
36. a=19, n=41 bo‘lsa, $a^{-1}$mod n=?
37. a=19, n=7739 bo‘lsa, $a^{-1}$mod n=?
38. a=20, n=41 bo‘lsa, $a^{-1}$mod n=?
39. a=20, n=11639 bo‘lsa, $a^{-1}$mod n=?
40. a=31, n=41 bo‘lsa, $a^{-1}$mod n=?
41. a=31, n=1763 bo‘lsa, $a^{-1}$mod n=?
42. a=32, n=41 bo‘lsa, $a^{-1}$mod n=?
43. a=32, n=1517 bo‘lsa, $a^{-1}$mod n=?

## 5.2. 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* ish-latiladi. 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-хеш, 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.

## 5.3. 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

$$w=(w_1, w_2, \dots w_n)$$

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

$$x_i \in [0,1].$$

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.

$$w_{k+1} > \sum_{i=1}^{k} w_i$$

*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 $b_i$ ketma-ketlik *normal ketma-ketlik* deyiladi.

$b_i = (w_i * r) \bmod q$ – normal ketma-ketlik. Bu yerda normal ketma-ketlik ($b_1, b_2, \ldots b_n$) ochiq kalit hisoblanadi. O‘suvchi ketma-ketlik ($w_1, w_2, \ldots w_n$) 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 ($m_1, m_2, \ldots, m_n$):

$$\left( \sum_{i=1}^{n} b_i m_i \right) \bmod q = c_i$$

formula yordamida shifrlanadi. Shifrtekst $C = \{c_1, c_2, \ldots\}$ ko‘rinishida hosil bo‘ladi.

**Shifrni ochish.**

$C = \{c_1, c_2, \ldots\}$ ko‘rinishidagi shifrtekstni

$$(r^{-1} c_i) \bmod q = m_i$$

formula yordamida ochiladi. Ochilgan $m_i$ 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 shifrlarni 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. $b_i = (w_i * r) \bmod q$ formula orqali normal ketma-ketlik hosil qilamiz:

   $b_1=(w_1 \cdot r) \bmod q= (2 \cdot 11) \bmod 28=22$

   $b_2=(w_2 \cdot r) \bmod q= (3 \cdot 11) \bmod 28=5$

   $b_3=(w_3 \cdot r) \bmod q= (7 \cdot 11) \bmod 28=21$

   $b_4=(w_4 \cdot r) \bmod q= (15 \cdot 11) \bmod 28=25$
3. Ketma-ketlik hadlari 4 ta bo‘lgani uchun matnni 4 bitdan bloklarga ajratamiz: $M_1=\{m_1,m_2,m_3,m_4\}=0100,\ M_2=\{m_1,m_2,m_3,m_4\}=1000,$ $M_3=\{m_1,m_2,m_3,m_4\}=0100,\ M_4=\{m_1,m_2,m_3,m_4\}=0001.$
4. $\left(\sum_{i=1}^{4} b_i m_i\right) \bmod q = c_i$ formula yordamida shifrlaymiz:

   $$c_1=\left(\sum_{i=1}^{4} b_i m_i\right) \bmod q=(22\cdot 0+5\cdot 1+21\cdot 0+25\cdot 0) \bmod 28=5$$

   $$c_2=\left(\sum_{i=1}^{4} b_i m_i\right) \bmod q=(22\cdot 1+5\cdot 0+21\cdot 0+25\cdot 0) \bmod 28=22$$

   $$c_3=\left(\sum_{i=1}^{4} b_i m_i\right) \bmod q=(22\cdot 0+5\cdot 1+21\cdot 0+25\cdot 0) \bmod 28=5$$

   $$c_4=\left(\sum_{i=1}^{4} b_i m_i\right) \bmod q=(22\cdot 0+5\cdot 0+21\cdot 0+25\cdot 1) \bmod 28=25$$
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: $11^{-1} \bmod 28 = 11^{11} \bmod 28 = (11(11^2 \bmod 28)^5) \bmod 28 = (11*9^5) \bmod 28 = (11*9(9^2 \bmod 28)^2) \bmod 28 = (11 * 9 * 25^2) \bmod 28 = 23$

2. $(r^{-1}c_i) \bmod q = m_i$ formuladan matnni topamiz:

$M_1 = (23 \cdot 5) \bmod 28 = 3 = 2 \cdot 0 + 3 \cdot 1 + 7 \cdot 0 + 15 \cdot 0$, bundan $M_1 = 0100$ ekanligini aniqlaymiz.

3. $M_2 = (23 \cdot 22) \bmod 28 = 2 = 2 \cdot 1 + 3 \cdot 0 + 7 \cdot 0 + 15 \cdot 0$, bundan $M_2 = 1000$ ekanligini aniqlaymiz.

4. $M_3 = (23 \cdot 5) \bmod 28 = 3 = 2 \cdot 0 + 3 \cdot 1 + 7 \cdot 0 + 15 \cdot 0$, bundan $M_3 = 0100$ ekanligini aniqlaymiz.

5. $M_4 = (23 \cdot 25) \bmod 28 = 15 = 2 \cdot 0 + 3 \cdot 0 + 7 \cdot 0 + 15 \cdot 1$, bundan $M_4 = 0001$ ekanligini aniqlaymiz.

6. Barcha $M_i$ larni ketma-ket yozib harflarga o‘tiladi:

M=0100100001000001

$0100\ 1000_{\ 2} = 48_{\ 16} = H$

$0100\ 0001_{\ 2} = 41_{\ 16} = A$

M = “HA”

**Mustaqil ish uchun misollar**.

1. m=397, n=17, a={2,3,6,12,24,49,100,200}, C={163, 314, 591, 62}, M=?
2. m=397, n=17, a={2,3,6,12,24,49,100,200}, C={437, 101, 294, 286}, M=?
3. m=397, n=17, a={2,3,6,12,24,49,100,200}, C={275, 213, 90, 490 }, M=?

4. m=397, n=17, a={2,3,6,12,24,49,100,200}, C={ 90, 286, 325, 275 }, M=?

5. m=397, n=17, a={2,3,6,12,24,49,100,200}, C={398, 518, 163, 275 }, M=?

6. m=397, n=17, a={2,3,6,12,24,49,100,200}, C={163, 275, 398, 518 }, M=?

7. m=397, n=17, a={2,3,6,12,24,49,100,200}, C={479, 437, 367, 286 }, M=?

8. m=397, n=17, a={2,3,6,12,24,49,100,200}, C={367, 437, 325, 275 }, M=?

9. m=397, n=17, a={2,3,6,12,24,49,100,200}, C={101, 286, 437, 213 }, M=?

10. m=397, n=17, a={2,3,6,12,24,49,100,200}, C={398, 437, 367, 294 }, M=?

11. m=397, n=17, a={2,3,6,12,24,49,100,200}, C={426, 437, 591, 294 }, M=?

12. m=397, n=17, a={2,3,6,12,24,49,100,200}, C={591, 437, 367, 294 }, M=?

13. m=397, n=17, a={2,3,6,12,24,49,100,200}, C={518, 314, 202, 275 }, M=?

14. m=397, n=17, a={2,3,6,12,24,49,100,200}, C={426, 437, 101, 202 }, M=?

15. m=397, n=17, a={2,3,6,12,24,49,100,200}, C={90, 437, 266, 275 }, M=?

16. m=397, n=17, a={2,3,6,12,24,49,100,200}, C={101, 286, 325, 275 }, M=?

17. m=397, n=17, a={2,3,6,12,24,49,100,200}, C={294, 286, 367, 314 }, M=?

18. m=397, n=17, a={2,3,6,12,24,49,100,200}, C={591, 62, 314, 367 }, M=?

19. m=397, n=17, a={2,3,6,12,24,49,100,200}, C={591, 275, 90, 437 }, M=?

20. m=397, n=17, a={2,3,6,12,24,49,100,200}, C={398, 437, 101, 275 }, M=?

21. m=397, n=17, a={2,3,6,12,24,49,100,200}, C={163, 314, 591, 62}, M=?

22. m=397, n=17, a={2,3,6,12,24,49,100,200}, C={437, 101, 294, 286}, M=?

23. m=397, n=17, a={2,3,6,12,24,49,100,200}, C={275, 213, 90, 490 }, M=?

24. m=397, n=17, a={2,3,6,12,24,49,100,200}, C={90, 286, 325, 275 }, M=?

25. m=397, n=17, a={2,3,6,12,24,49,100,200}, C={398, 518, 163, 275 }, M=?

26. m=727, n=111, a={2,3,6,12,24,49,100,200}, C={540,662,378,662, 296}, M=?

27. m=727, n=111, a={2,3,6,12,24,49,100,200}, C={613,285,378, 418,573}, M=?

28. m=727, n=111, a={2,3,6,12,24,49,100,200}, C={8,662,378,236,41}, M=?

29. m=397, n=17, a={2,3,6,12,24,49,100,200}, C={296,142,30,296, 377}, M=?

30. m=397, n=17, a={2,3,6,12,24,49,100,200}, C={378,377,72, 223, 367}, M=?

31. m=397, n=17, a={2,3,6,12,24,49,100,200}, C={82,40, 101, 142, 184}, M=?

32. m=397, n=17, a={2,3,6,12,24,49,100,200}, C={ 30, 19, 396, 367, 40}, M=?

## 5.4. RSA algoritmi

Ochiq kalitli kriptotizimlarni bir tomonli funksiyalar koʻrinishi boʻyicha farqlash mumkin. Bularning ichida RSA, El-Gamal va Mak-Elis tizimlarini alohida tilga olish oʻrinli. Hozirda eng samarali va keng tarqalgan ochiq kalitli shifrlash algoritmi sifatida RSA algoritmini koʻrsatish mumkin.

1976 yilda Uitfild Diffi va Martin Xellmanlar tomonidan chop etilgan “Kriptografiyada yangi yoʻnalish” deb nomlangan maqola kriptografik tizimlar haqidagi tasavvurlarni oʻzgartirib yubordi, ochiq kalitli kriptografiya paydo boʻlishiga zamin yaratdi. Bu maqolani oʻrganib 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 koʻtarish amalidan foydalanishga asoslangan. 1977 yil avgust oyida **Scientific American** jurnalida RSA kriptotizimini yoritib berishdi va shu algoritm bilan shifrlangan quyidagi iborani ochishni oʻquvchilarga taklif etishdi:

C=

| | | | |
|---|---|---|---|
| 9686 | 9613 | 7546 | 2206 |
| 1477 | 1409 | 2225 | 4355 |
| 8829 | 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 SQUEAMISH OSSIFRAGE.

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; RFC 3447 — 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 $M_i$, $i=\overline{1,I}$ sonlarning ketma-ketligi orqali ifodalanadi. I ning qiymati shifrlanuvchi ketma-ketlikning uzunligi orqali aniqlanadi.

7. Shifrlangan axborot quyidagi formula bo'yicha aniqlanuvchi $C_i$ sonlarning ketma-ketligi ko'rinishida olinadi:

$$C_i = M_i^e \bmod n.$$

Axborotni ochishda quyidagi munosabatdan foydalaniladi:

$$M_i = C_i^d \bmod n.$$

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 $n = p \cdot q = 1517$, $(p-1)\cdot(q-1)$ 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: 01000010 01000101 01010011 01001000.
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. $C_i = M_i^e \bmod n$ formula yordamida shifrlanadi:

$$C_1 = M_1^e \bmod n = 66^{11} \bmod 1517 = \left(66 \cdot \left(66^5 \bmod 1517\right)^2\right) \bmod 1517 =$$

$$= \left(66 \cdot 532^2 \bmod 1517\right) \bmod 1517 = \left(66 \cdot 862\right) \bmod 1517 = 763,$$

$$C_2 = M_2^e \bmod n = 69^{11} \bmod 1517 = 1441,\ C_3 = M_3^e \bmod n = 83^{11} \bmod 1517 = 821,$$

$$C_4 = M_4^e \bmod n = 72^{11} \bmod 1517 = 1097.$$

Hosil bo‘lgan shifrtekst quyidagicha: $C = \{763,1441,821,1097\}$.

**Shifrni ochish:**

Modul son $n = p \cdot q = 1517$, $(p-1)\cdot(q-1)$ 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 $(p-1)\cdot(q-1)$ modul bo‘yicha teskarisini topamiz:

$$d = e^{-1} \bmod\big((p-1)\cdot(q-1)\big) = 11^{-1} \bmod 1440 = 11^{383} \bmod 1440 = 131$$

2. $M_i = C_i^d \bmod n$ formula yordamida shifrni ochamiz:

$$M_1 = C_1^d \bmod n = 763^{131} \bmod 1517 = 66,\ M_2 = C_2^d \bmod n = 1441^{131} \bmod 1517 = 69,$$

$$M_3 = C_3^d \bmod n = 821^{131} \bmod 1517 = 83,\ M_4 = C_4^d \bmod n = 1097^{131} \bmod 1517 = 72,$$

3. $M_i$ larni o‘nlikdan ikkilikka o‘tkazib, ASCII jadval yordamida harflarga o‘tamiz va natijada M=BESH so‘zi paydo bo‘ladi.

## Mustaqil ish uchun misollar.

1. n=1517, e=11, C={ 413, 665, 620, 30 }, L=8 bit, M=?
2. n=1517, e=11, C={ 593, 27, 763, 30 } L=8 bit, M=?
3. n=1517, e=11, C={ 763, 30, 593, 27 }, L=8 bit, M=?
4. n=1517, e=11, C={ 1270, 1408, 902, 665 }, L=8 bit, M=?
5. n=1517, e=11, C={ 902, 1408, 620, 30 }, L=8 bit, M=?
6. n=1517, e=11, C={ 13, 665, 1408, 1390 }, L=8 bit, M=?
7. n=1517, e=11, C={ 1437, 1408, 902, 285 }, L=8 bit, M=?
8. n=1147, e=11, C={162,881,767,753,162,516,881,753,139,881,894, 162,1109,894,229,881,162,894,890,162,1109}, L=8 bit, M=?
9. n=1147, e=11, C={778,890,753,890,946,778,881,946,1109,139,881, 231,881,778,516,162,881,778}, L=8 bit, M=?
10. n=1189, e=11,C={1071,416,529,50,368,1096,801,55,368,368,1096, 148,55,575,646,628,1096,495,50,529,352}, L=8 bit, M=?
11. n=1189, e=11,C={220,1096,451,416,529,352,416,801,449,86,1096, 575,416,628,575,50,801,220,1096,451,368,50}, L=8 bit, M=?
12. n=341, e=13, L=6 bit, C={ 335, 161, 130, 276} M=?
13. n=407, e=13, L=6 bit, C={ 280, 334, 235, 315} M=?
14. n=341, e=13, L=6 bit, C={ 335, 232, 282, 226} M=?
15. n=407, e=13, L=6 bit, C={ 280, 165, 261, 348} M=?
16. n=341, e=13, L=6 bit, C={ 246, 112, 1, 293} M=?
17. n=407, e=13, L=6 bit, C={ 280, 23, 185, 94} M=?
18. n=341, e=13, L=6 bit, C={ 246, 198, 1, 226} M=?
19. n=407, e=13, L=6 bit, C={ 288, 334, 235, 310} M=?
20. n=341, e=13, L=6 bit, C={ 246, 161, 168, 130} M=?
21. n=407, e=13, L=6 bit, C={ 280, 165, 312, 310} M=?

22. n=341, e=13, L=6 bit, C={ 178, 161, 191, 151 } M=?
23. n=407, e=13, L=6 bit, C={ 174, 23, 258, 382 } M=?
24. n=341, e=13, L=6 bit, C={ 208, 208, 80, 132 } M=?
25. n=187, e=13, L=6 bit, C={ 21, 21, 25, 33 } M=?
26. n=209, e=13, L=6 bit, C={ 98, 98, 25, 154 } M=?
27. n=209, e=7, L=6 bit, C={ 36, 19, 4, 2 } M=?
28. n=209, e=13, L=6 bit, C={ 81, 98, 25, 204 } M=?
29. n=187, e=13, L=6 bit, C={ 169, 21, 25, 6 } M=?
30. n=341, e=7, L=6 bit, C={ 181, 145, 192, 271 } M=?
31. n=187, e=7, L=6 bit, C={ 104, 47, 181, 7 } M=?

## 5.5. 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 quyidagilarni qanoatlantirishi kerak:

p mod4=3, q mod4=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:** $C=M^2 \bmod n$;

**Shifrni ochishda** quyidagilar hisoblanadi: $m_1 = C^{\frac{p+1}{4}} mod\ p$, $m_2 = \left(p - C^{\frac{p+1}{4}}\right) mod\ p$, $m_3 = C^{\frac{q+1}{4}} mod\ q$, $m_4 = \left(q - C^{\frac{q+1}{4}}\right) mod\ q$, $a = p(p^{-1} mod\ q)$, $b = q(q^{-1} mod\ p)$,

$$M_1 = (a \cdot m_3 + b \cdot m_1) mod\ n,$$
$$M_2 = (a \cdot m_3 + b \cdot m_2) mod\ n,$$
$$M_3 = (a \cdot m_4 + b \cdot m_1) mod\ n,$$
$$M_4 = (a \cdot m_4 + b \cdot m_2) mod\ n.$$

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·p=19·43=817
2. Matnni 10 lik sanoq sistemasida ifodalaymiz: $O \to 4F \to 79$,
$L \to 4C \to 76$, $T \to 54 \to 84$, $I \to 49 \to 73$.
M=79, 76, 84, 73.
2. $C_i = M_i^2 \bmod n$ formula yordamida shifrlash amalga oshiriladi:

$$C_1 = M_1^2 \bmod n = 79^2 \bmod 817 = 522,$$
$$C_2 = M_2^2 \bmod n = 76^2 \bmod 817 = 57,$$
$$C_3 = M_3^2 \bmod n = 84^2 \bmod 817 = 520,$$
$$C_4 = M_4^2 \bmod n = 73^2 \bmod 817 = 427.$$

$C = \{C_1, C_2, C_3, C_4\} = \{522,57,520,427\}$ shifrtekst hosil bo‘ldi.

**Shifrni ochish.**

Shifrni ochish jarayoniga ko‘proq vaqt sarflanadi. Shifrtekstdagi har bir son alohida ochiladi. $C = C_1 = 522$ ni ko‘rib chiqamiz.

1. $m_1 = C^{\frac{p+1}{4}} \bmod p = 522^{11} \bmod 43 = 36$
2. $m_2 = (p - C^{\frac{p+1}{4}}) \bmod p = (43-36) \bmod 43 = 7$
3. $m_3 = C^{\frac{q+1}{4}} \bmod q = 522^5 \bmod 19 = 16$
4. $m_4 = (q - C^{\frac{q+1}{4}}) \bmod q = (19-16) \bmod 19 = 3$
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 $M_1$, $M_2$, $M_3$, $M_4$ 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.

## Mustaqil ish uchun misollar.

1. n=989, C={ 400, 805, 955, 239 }, M=?
2. n=989, C={ 307, 831, 133, 384 }, M=?
3. n=989, C={ 269, 150, 668, 9 }, M=?
4. n=989, C={ 668, 384, 984, 269 }, M=?
5. n=989, C={ 680, 302, 400, 269 }, M=?
6. n=989, C={ 400, 269, 680, 302 }, M=?
7. n=989, C={ 627, 307, 790, 384 }, M=?
8. n=989, C={ 790, 307, 984, 269 }, M=?
9. n=989, C={ 831, 384, 307, 150 }, M=?
10. n=989, C={ 944, 307, 790, 133 }, M=?
11. n=989, C={ 96, 307, 955, 133 }, M=?
12. n=989, C={ 955, 307, 790, 133 }, M=?
13. n=989, C={ 302, 805, 944, 269 }, M=?
14. n=989, C={ 96, 307, 831, 944 }, M=?
15. n=989, C={ 668, 307, 821, 269 }, M=?
16. n=989, C={ 831, 384, 984, 269 }, M=?
17. n=989, C={ 133, 384, 790, 805 }, M=?
18. n=989, C={ 955, 239, 805, 790 }, M=?
19. n=989, C={ 955, 269, 668, 307 }, M=?
20. n=989, C={ 680, 307, 831, 269 }, M=?
21. n=989, C={ 269, 831, 384, 9 }, M=?
22. n=989, C={ 473, 269, 831, 384 }, M=?
23. n=437, C={ 119, 232, 308, 115, 95, 85, 187, 87}, M=?
24. n=437, C={ 282, 232, 142, 115, 150, 423, 323, 150, 232, 87, 150}, M=?
25. n=437, C={ 334, 187, 323, 85, 302, 302, 95, 85, 187, 87}, M=?
26. n=437, C={ 282, 232, 121, 150, 254, 85, 177, 301}, M=?
27. n=437, C={ 254, 150, 302, 150, 346, 150, 377, 85, 82, 150}, M=?
28. n=437, C={ 334, 328, 100, 353, 346, 391, 301, 386}, M=?
29. n=437, C={ 119, 346, 323, 302, 292, 302, 346, 254, 150, 302}, M=?
30. n=437, C={ 282, 323, 100, 301, 346, 391, 115, 187}, M=?
31. n=437, C={ 140, 100, 301, 386, 85, 177, 115, 248, 150}, M=?

32. n=437, C={ 64, 232, 427, 334, 187, 323, 150, 150, 301}, M=?
33. N=989, C={307,785,311}; N=209, C={130,4,163,157,80,4,163, 199,38}; N=473, C={170,232}, M=?
34. N=209, C={36,169,4,169}; N=253, C={110,48,133,93,133}; N=817, C={815,404}, M=?
35. N=473, C={102,23,56,422}; N=253, C={9,69}; N=817, C={427, 662,384,397,741}, M=?
36. N=209, C={133,199,58}; N=473, C={441,275,203,268,312, 268,454}; N=817, C={139,422,226}, M=?
37. N=253, C={55,48,93,69,81}; N=817, C={226,66,662,422}; N=473, C={170,232}. M=?
38. N=817, C={140,404};N=253, C={110,146,26,48,209}; N=209, C={158,157,187,187,169,38}, M=?
39. N=817, C={723,741,617,178,397,752,741,66}; N=253, C={210, 146,177,209}. M=?
40. N=473, C={99,268,275,471,146,97,422}; N=817, C={681,66, 741,384,66}, M=?

## 5.6. 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 = $\frac{b}{a^x}$ mod 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 sanoq tizimida ifodalaymiz: $\mathrm{B} \to 42_{16} \to 01000010_2, \mathrm{B} \to 42_{16} \to 01000010_2, C \to 43_{16} \to 01000011_2$. 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: $\mathrm{M}_1 = 010000_2 \to 16_{10}, \mathrm{M}_2 = 100100_2 \to 36_{10}, \mathrm{M}_3 = 001001_2 \to 9_{10}, \mathrm{M}_4 = 000011_2 \to 3_{10}$.
5. y = $\mathrm{g}^x$ mod p= $11^3 \mathrm{mod}\ 89 = 85$.
6. k=7.
7. $a = g^{\mathrm{k}} \mathrm{mod}\ \mathrm{p} = 11^7 \mathrm{mod}\ 89 = 87$.
8. $b_1 = (y^{\mathrm{k}} \cdot \mathrm{M}_1) \mathrm{mod}\ \mathrm{p} = (85^7 \cdot 16) \mathrm{mod}\ 89 = (81 \cdot 16) \mathrm{mod}\ 89 = 50,$
   $b_2 = (y^{\mathrm{k}} \cdot \mathrm{M}_2) \mathrm{mod}\ \mathrm{p} = (85^7 \cdot 36) \mathrm{mod}\ 89 = (81 \cdot 36) \mathrm{mod}\ 89 = 68,$
   $b_3 = (y^{\mathrm{k}} \cdot \mathrm{M}_3) \mathrm{mod}\ \mathrm{p} = (85^7 \cdot 9) \mathrm{mod}\ 89 = (81 \cdot 9) \mathrm{mod}\ 89 = 17,$
   $b_4 = (y^{\mathrm{k}} \cdot \mathrm{M}_4) \mathrm{mod}\ \mathrm{p} = (85^7 \cdot 3) \mathrm{mod}\ 89 = (81 \cdot 3) \mathrm{mod}\ 89 = 65.$

$\mathrm{C} = \{\mathrm{a}, \mathrm{b}_1, \mathrm{b}_2, \mathrm{b}_3, \mathrm{b}_4\} = \{87,50,68,17,65\}$ shifrtekst hosil bo‘ldi.

**Shifrni ochish.**

Shifrni ochish jarayoniga ko‘proq vaqt sarflanadi. Shifrtekstdagi har bir son alohida ochiladi.

$\mathrm{M} = (\mathrm{b} \cdot (\mathrm{a}^{-1})^{\mathrm{x}}) \mathrm{mod}\ \mathrm{p}$ formuladan foydalanamiz.

1. $\mathrm{M}_1 = (\mathrm{b}_1 \cdot (\mathrm{a}^{-1})^{\mathrm{x}}) \mathrm{mod}\ \mathrm{p} = (50 \cdot 44^3) \mathrm{mod}\ 89 = (50 \cdot 11) \mod 89 = 16.$
2. $\mathrm{M}_2 = (\mathrm{b}_2 \cdot (\mathrm{a}^{-1})^{\mathrm{x}}) \mathrm{mod}\ \mathrm{p} = (68 \cdot 44^3) \mathrm{mod}\ 89 = (68 \cdot 11) \mod 89 = 36.$
3. $\mathrm{M}_3 = (\mathrm{b}_3 \cdot (\mathrm{a}^{-1})^{\mathrm{x}}) \mathrm{mod}\ \mathrm{p} = (17 \cdot 44^3) \mathrm{mod}\ 89 = (17 \cdot 11) \mod 89 = 9.$

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.

$01000010010000100100000 11_2 \rightarrow (01000010,01000010,01000011)_2 \rightarrow (42,42,43)_{16} \rightarrow$ BBC. Ochiq matn hosil bo‘ldi.

## Mustaqil ish uchun misollar.

1. p=83, x=3, a=34, b=32,32,73,74 bo‘lsa, M=?
2. p=83, x=3, a=39, b=71,8,34,49 bo‘lsa, M=?
3. p=83, x=3, a=34, b=56,32,73,19 bo‘lsa, M=?
4. p=89, x=3, a=61, b=67,14,28,60 bo‘lsa, M=?
5. p=89, x=3, a=61, b=51,48,12,4 bo‘lsa, M=?
6. p=97, x=3, a=21, b=93,93,26,63 bo‘lsa, M=?
7. p=79, x=4, a=32, b=76,26,17,19 bo‘lsa, M=?
8. p=83, x=3, a=42, b=2,13,53,57 bo‘lsa, M=?
9. p=103, x=3, a=35, b=49,19,11,53 bo‘lsa, M=?
10. p=107, x=3, a=22, b=24,54,67,58 bo‘lsa, M=?
11. p=97, x=3, a=49, b=39,39,86,89 bo‘lsa, M=?
12. p=79, x=3, a=32, b=32,65,3,8 bo‘lsa, M=?
13. p=83, x=3, a=3, b=17,69,77,28 bo‘lsa, M=?
14. p=103, x=3, a=51, b=48,6,36,33 bo‘lsa, M=?
15. p=107, x=3, a=5, b=74,6,55,54 bo‘lsa, M=?
16. p=97, x=3, a=21, b=93,93,26,63 bo‘lsa, M=?
17. p=79, x=3, a=59, b=7,71,13,61 bo‘lsa, M=?
18. p=83, x=4, a=3, b=51,41,65,1 bo‘lsa, M=?
19. p=103, x=3, a=30, b=83,49,88,12 bo‘lsa, M=?
20. p=107, x=3, a=57, b=44,99,105,35 bo‘lsa, M=?

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.

# VI 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.

## 6.1. Diffi-Xelman algoritmi

Bu algoritm 1976 yilda Whitfield Diffie va Martin Hellmanlar tomonidan taklif etilgan. 2002 yilda Xelman bu algoritmni yaratishda Ralf Merklning hissasi kata 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:** $\forall$ x < n bo‘lgan katta son tanlaydi va hisoblaydi: $A=g^x \bmod n$ va natijani B tomonga jo‘natadi. B tomon uni qabul qilib oladi.
2. **B tomon:** $\forall$ y < n bo‘lgan katta son tanlaydi va quyidagi formula bo‘yicha $B=g^y \bmod n$ 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: $B^x \bmod n = g^{xy} \bmod n$ – kalit.
4. **B tomon:** A tomon jo‘natgan ma’lumotni o‘zining tanlagan soni y darajaga oshirib hisoblaydi va kalitni hosil qiladi: $A^y \bmod n = g^{xy} \bmod n$ – kalit.

Topilgan $g^{xy} \bmod n$ qiymatdan kalit sifatida foydalaniladi. Algoritmdan tomonlar uchta va undan ko‘p bo‘lganda ham foydalanish mumkin.

## 6.2. 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: $\forall$ 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:** $\forall$ x <n bo‘lgan katta son tanlaydi va hisoblaydi: $A=g^x \bmod n$ va hech kimga jo‘natmaydi.

2. **B tomon:** $\forall$ y <n bo‘lgan katta son tanlaydi va hisoblaydi: $B=g^y \bmod n$ va natijani A tomonga jo‘natadi.

3. **A tomon:** $B^x \bmod n = A_1$ hisoblaydi va $A_1$ ni B tomonga jo‘natadi.

4. **B tomon**: $z=y^{-1} \bmod n$ ni hisoblaydi.

$A_1^z \bmod n = B^{xz} \bmod n = g^{xyz} \bmod n = g^x \bmod n$ – 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.

# VII 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.

Hozirda ERI Internet orqali axborot almashishning qonuniy rasmiylashtirilgan jarayoni hisoblanadi. Jumladan, 2003 yil 11 dekabrda 562-II-son Ozbekiston Respublikasi “Elektron raqamli imzo to‘g‘risida” va 2004 yil 29 aprelda 611-II-son “Elektron hujjat aylanishi to‘g‘risida” qonuni qabul qilindi. Bundan maqsad elektron raqamli imzodan foydalanish va elektron hujjat aylanishi sohasidagi munosabatlarini tartibga solishdir. Qonunga ko‘ra elektron raqamli imzodan foydalanish sohasini davlat tomonidan tartibga solishni O‘zbekiston Respublikasi Vazirlar Mahkamasi va u vakolat bergan maxsus organ amalga oshiradi. Bularga muhim komponent sifatida bir qator normativ hujjatlar, davlat standartlari va O‘zbekiston Respublikasi Prezidenti va Vazirlar Mahkamasi qarorlari qabul qilindi.

2005 yil 8 iyulda O‘zbekiston aloqa va axborotlashtirish agentligi ERI dan foydalanish sohasi bo‘yicha maxsus vakolatli organ, deb e’lon qilindi va 2006 yilning 15 martida O‘zbekiston Respublikasida internet-banking, himoyalangan hujjat aylanishi, elektron tijorat rivojlanishida muhim o‘rin egallaydigan ochiq kalitli infratuzilma texnologiyalaridan foydalanuvchi ERI kalitlarini ro‘yxatdan o‘tkazuvchi markaz ochildi.

Fan-texnika va marketing tadqiqotlari markazi (FTMTM) qoshidagi ERI kalitlarini ro‘yxatga olish markazi tomonidan ERI va milliy standartlar asosidagi shifrlashdan foydalanadigan himoyalangan E-XAT elektron pochta tizimining dasturiy ta’minoti ishlab chiqildi. Berilgan xizmatdan ommaviy foydalanish maqsadida himoyalangan E-XAT elektron pochta tizimi “UzNet” filialining ma’lumotlar uzatish tarmog‘iga o‘rnatildi va hozirda bu xizmatdan internetning ixtiyoriy foydalanuvchisi foydalanishi mumkin.

Foydalanuvchilarga ochiq kalitlar infratuzilmasi, undagi huquqiy va texnologik tartibga solishni takomillashtirish masalasini ko‘rib chiqish, axborot xavfsizligi sohasida texnologik yechimlar va yangi yutuqlar, mahsulotlardan boxabar etuvchi www.pki.uz sayti ham ishlab chiqildi.

Yuqorida aytib o‘tilgan ma’lumotlarga asoslanib shuni aytish mumkinki, 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.

## 7.1. 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:

$$h < q, \quad h^{p-1/q} \bmod p > 1.$$

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. $U1=(H(m) \cdot W) \bmod q$ hisoblanadi.

13. $U2=(a \cdot W) \bmod q$ hisoblanadi.

14. $v=(g^{u1} \cdot y^{u2} \bmod p) \bmod q$ hisoblanadi. Agar v = a bo‘lsa imzo to‘gri qo‘yilgan bo‘ladi.

## Mustaqil ish uchun misollar.

1. p=83, q=41, h=13, x=12, k=5, H(m)=7 bo‘lsa, (r,s)=?

2. p=83, q=41, h=12, x=7, k=6, H(m)=5 bo‘lsa, (r,s)=?

3. p=83, q=41, h=10, x=21, k=7, H(m)=17 bo‘lsa, (r,s)=?

4. p=83, q=41, h=20, x=31, k=8, H(m)=11 bo‘lsa, (r,s)=?

5. p=83, q=41, h=8, x=3, k=9, H(m)=9 bo‘lsa, (r,s)=?

6. p=83, q=41, h=14, x=12, k=15, H(m)=7 bo‘lsa, (r,s)=?

7. p=83, q=41, h=15, x=7, k=16, H(m)=5 bo‘lsa, (r,s)=?

8. p=83, q=41, h=16, x=21, k=17, H(m)=17 bo‘lsa, (r,s)=?

9. p=83, q=41, h=17, x=31, k=18, H(m)=11 bo‘lsa, (r,s)=?

10. p=83, q=41, h=18, x=3, k=19, H(m)=9 bo‘lsa, (r,s)=?

11. Imzo tekshirish: p=83, q=41, g=38, y=48, H(m)=7, r={11,3,9} va s={12,31,11} bo‘lsa, haqiqiy (r,s)=?

12. Imzo tekshirish: p=83, q=41, g=38, y=9, H(m)=7, r={7,9,25} va s={21,25,3} bo‘lsa, haqiqiy (r,s)=?

13. Imzo tekshirish: p=83, q=41, g=38, y=48, H(m)=9, r={5,9,27} va s={9,18,40} bo‘lsa, haqiqiy (r,s)=?

14. Imzo tekshirish: p=83, q=41, g=38, y=48, H(m)=14, r={3,7,9} va s={11,6,8} bo‘lsa, haqiqiy (r,s)=?

15. Imzo tekshirish: p=83, q=41, g=18, y=48, H(m)=15, r={7,9,11} va s={4,19,20} bo‘lsa, haqiqiy (r,s)=?

## 7.2. 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. $a^q$ modp=l shartni qanoatlantiruvchi 0<a<p-1 oraliqdagi a son tanlanadi.

4. $y=a^x$ modp 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. $1 \le k \le q$ intervaldan tasodifiy k soni olinadi, u maxfiy saqlanadi va imzo qo‘yilgandan keyin darhol yo‘qotiladi.

7. $r=( a^k \text{ modp}) \text{ mod } q$ 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. $s=(x \cdot r+k \cdot H(M)) \text{modq}$ 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 $1 \le r,s \le n-1$ shart bajarilmasa, u holda imzo qalbaki va imzoni tekshirish to‘xtatiladi. Bu shartlar bajarilsa keyingi qadamga o‘tiladi.

10. $w = H^{q-2}(M) \text{ modq}$ hisoblanadi.

11. $u1= (s \cdot w) \text{ modq}$ hisoblanadi.

12. $u2 = ((q-r) \cdot w) \text{ modq}$ hisoblanadi.

13. $u = (a^{u1} y^{u2} \text{modp}) \text{modq}$ hisoblanadi. Agar u=r shart bajarilsa, u holda imzo haqiqiy, aks holda imzo qalbaki va imzoni tekshirish to‘xtatiladi.

## Mustaqil ish uchun misollar.

1. Imzoni tekshirish: p=83, q=41, a=3, y=77, H(m)=7, r={7,27,31} va s={5,17,33} bo‘lsa, haqiqiy (r,s)=?
2. Imzoni tekshirish: p=83, q=41, a=3, y=81, H(m)=6, r={14,21,36} va s={10,15,17} bo‘lsa, haqiqiy (r,s)=?
3. Imzoni tekshirish: p=83, q=41, a=3, y=77, H(m)=8, r={7,25,29} va s={31,37,39} bo‘lsa, haqiqiy (r,s)=?
4. Imzoni tekshirish: p=83, q=41, a=3, y=27, H(m)=10, r={12,15,17} va s={3,9,12} bo‘lsa, haqiqiy (r,s)=?

5. Imzoni tekshirish: p=83, q=41, a=3, y=77, H(m)=11, r={11,19,36} va s={21,29,30} bo‘lsa, haqiqiy (r,s)=?
6. Imzoni tekshirish: p=83, q=41, a=3, y=77, H(m)=5, r={12,15,21} va s={9,21,23} bo‘lsa, haqiqiy (r,s)=?
7. Imzoni tekshirish: p=83, q=41, a=3, y=77, H(m)=12, r={21,27,29} va s={14,19,24} bo‘lsa, haqiqiy (r,s)=?

## 7.3. 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: $y = g^x \bmod p$.

**Imzo qo‘yish:**

5. p – 1 dan kichik bo‘lgan va p – 1 bilan o‘zaro tub bo‘lgan k – tasodifiy son tanlanadi.
6. $a = g^k \bmod p$ hisoblanadi.
7. $b = ((M - a \cdot x) \cdot k^{-1}) \bmod (p - 1)$ 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.

## Mustaqil ish uchun misollar.

1. Imzo qo‘yish: p=83, g=3, x=7, k=9, M=12 bo‘lsa, imzo (a,b)=?
2. Imzo qo‘yish: p=83, g=5, x=9, k=11, M=13 bo‘lsa, imzo (a,b)=?
3. Imzo qo‘yish: p=83, g=11, x=29, k=15, M=15 bo‘lsa, imzo (a,b)=?
4. Imzo qo‘yish: p=83, g=19, x=17, k=13, M=18 bo‘lsa, imzo (a,b)=?
5. Imzo qo‘yish: p=83, g=23, x=13, k=17, M=55 bo‘lsa, imzo (a,b)=?
6. Imzo qo‘yish: p=83, g=3, x=7, k=9, M=12 bo‘lsa, imzo (a,b)=?
7. Imzo qo‘yish: p=83, g=5, x=9, k=11, M=13 bo‘lsa, imzo (a,b)=?
8. Imzo qo‘yish: p=83, g=11, x=29, k=15, M=15 bo‘lsa, imzo (a,b)=?
9. Imzo qo‘yish: p=83, g=19, x=17, k=13, M=18 bo‘lsa, imzo (a,b)=?
10. Imzoni tekshirish: M=65, p=83, g=4, y=28, a={22,29,64} va b={31,79,59} bo‘lsa, haqiqiy (a,b)=?
11. Imzoni tekshirish: M=66, p=83, g=4, y=28, a={39,41,64} va b={79,52,82} bo‘lsa, haqiqiy (a,b)=?

12. Imzoni tekshirish: M=67, p=83, g=4, y=28, a={11,19,64} va b={24,25,51} bo‘lsa, haqiqiy (a,b)=?
13. Imzoni tekshirish: M=68, p=83, g=4, y=33, a={59,64,69} va b={53,54,10} bo‘lsa, haqiqiy (a,b)=?
14. Imzoni tekshirish: M=69, p=83, g=5, y=22, a={7,42,79} va b={7,39,44} bo‘lsa, haqiqiy (a,b)=?

# VIII BOB. IDENTIFIKATSIYA SXEMALARI

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 koʻrsatish uchun juda muhimdir.

Ma'lumotlarni uzatish kanallarini himoyalashda *subyektlarning oʻzaro autentifikatsiyasi*, ya'ni aloqa kanallari orqali bogʻlanadigan subyektlar haqiqiyligining oʻzaro tasdigʻi bajarilishi shart. Haqiqiylikning tasdigʻi odatda seans boshida, abonentlarning bir-biriga ulanish jarayonida amalga oshiriladi. "Ulash" atamasi orqali tarmoqning ikkita subyekti oʻrtasida mantiqiy bogʻlanish tushuniladi. Ushbu muolajaning maqsadi ulash qonuniy subyekt bilan amalga oshirilganligiga va barcha axborot moʻljallangan manzilga borishligiga ishonchni ta'minlashdir.

Oʻzining haqiqiyligining tasdiqlash uchun subyekt tizimga turli asoslarni koʻrsatishi mumkin. Subyekt koʻrsatadigan asoslarga bogʻliq holda autentifikatsiya jarayonlari quyidagi kategoriyalarga boʻlinishi mumkin:

- *biror narsani bilish asosida.* Misol sifatida parol, shaxsiy identifikatsiya kodi PIN (Personal Identification Number) hamda "soʻrov-javob" xilidagi protokollarda namoyish etiluvchi maxfiy va ochiq kalitlarni koʻrsatish mumkin;

- *biror narsaga egaligi asosida.* Odatda bular magnit kartalar, smart-kartalar, sertifikatlar va xotira qurilmalari;

- *qandaydir daxlsiz tavsiflar asosida.* Ushbu kategoriya oʻz tarkibiga foydalanuvchining biometrik tavsiflariga (ovozlar, koʻzining rangdor pardasi va toʻr pardasi, barmoq izlari, kaft geometriyasi va x.k.) asoslangan usullarni oʻz 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. Oʻzaro autentifikatsiya uchun foydalanuvchi va uning sherigi oʻrtasida 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 boʻlishi shart.

*Dinamik (bir martalik) parol* – bir marta ishlatilganidan soʻng boshqa umuman ishlatilmaydigan parol. Amalda odatda doimiy parolga yoki tayanch iboroga asoslanuvchi muntazam oʻzgarib turuvchi qiymat ishlatiladi.

*"Soʻrov-javob" tizimi* - taraflarning biri noyob va oldindan bilib boʻlmaydigan "soʻrov" qiymatini ikkinchi tarafga joʻnatish 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.

## 8.1. Feige-Fiat-Shamir identifikatsiya sxemasi

Bu sxema 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: $x^2$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=$r^2$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, $r^2$modn=y tenglikni tekshiradi, aks holda ($z^2$*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: $y=r^2 \bmod n$ va y qiymatni B tomonga jo‘natadi.
2. **B tomon:** ixtiyoriy $b_i$ (i=1,..,k) bitlarni tanlaydi va ularni A tomonga jo‘natadi.
3. **A tomon:** $z = r\prod_{i=1}^{k} s_i^{b_i} \bmod n$ qiymatni B tomonga jo‘natadi.
4. **B tomon:** $z^2\prod_{i=1}^{k} v_i^{b_i} \bmod n = y$ 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.

## 8.2. Bir necha kalitli 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, $t \in N$) sonlar tanlanadi: $(k_1 \cdot k_2 \cdot .. \cdot k_t) \bmod ((p-1)(q-1))=1$.

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:** $C = M^{k_1 \cdot k_2 \cdot k_3} \bmod n$ formula orqali bajariladi.

**Shifrni ochish:** $M = C^{k_4 \cdot k_5 \cdot k_6} \bmod n$ 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: $C_1 = M^{k_1} \bmod n$. 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: $M = C_1^{k_2 \cdot k_3 \cdot k_4 \cdot k_5 \cdot k_6 \cdot k_7} \bmod n$, hammasi to‘g‘ri bo‘lsa, tasdiqlash uchun imzo qo‘yadi: $C_2 = C_1^{k_2 \cdot k_3} \bmod n$.

## 8.3. «Yashirin» kanal

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. $X = g^M \bmod p,\ Y = \left(M^{-1}\left(M' - rX\right)\right)\bmod(p-1)$ – birinchi tomon hisoblaydi.
5. (X,Y) imzo va M’ xabarni ikkinchi tomonga jo‘natadi.

Nazoratchi imzoni tekshirib ko‘rishi mumkin: $\left(K^X X^Y\right)\bmod p = g^{M'} \bmod p$ 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: $\left(K^X X^Y\right)\bmod p = g^{M'} \bmod p$.
7. Nazoratchi o‘zgartirmaganligiga ishonch hosil qilgach M xabarni tiklaydi: $M = \left(Y^{-1}\left(M' - rX\right)\right)\bmod(p-1)$.

### Mustaqil ish uchun misollar.

1. A (34,83), p=193, r=7 bo‘lsa, yashirin xabarni toping ?
2. A (78,53), p=193, r=7 bo‘lsa, yashirin xabarni toping ?
3. A (114,133), p=193, r=7 bo‘lsa, yashirin xabarni toping ?
4. A (148,13), p=193, r=7 bo‘lsa, yashirin xabarni toping ?
5. M (78,185), p=193, r=7 bo‘lsa, yashirin xabarni toping ?
6. O (114,71), p=193, r=7 bo‘lsa, yashirin xabarni toping ?
7. E (34,151), p=193, r=7 bo‘lsa, yashirin xabarni toping ?
8. G (148,163), p=193, r=7 bo‘lsa, yashirin xabarni toping ?
9. S (78,59), p=193, r=7 bo‘lsa, yashirin xabarni toping ?
10. G (78,119), p=193, r=7 bo‘lsa, yashirin xabarni toping ?

# 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.

## REFERAT VA MUSTAQIL ISH MAVZULARI

1. RSA algoritmi variantlari.
2. Pohlig-Hellman algoritmi.
3. Williams algoritmi.
4. Elektron raqamli imzo.
5. Kriptografik protokollar.
6. Kalit uzunligi.
7. Kalitlarni boshqarish.
8. Kriptografik rejimlar.
9. Kriptografiyaning matematik asoslari.
10. Sonlar nazariyasi.
11. AES algoritmidan foydalanib shifrlash.
12. Xesh-funksiyalar.
13. Ochik kalitli kriptotizimlar.
14. Algebraik tizimlar.
15. Bir yo‘nalishli (oneway) funksiyalar.
16. Nosimmetrik algoritmlar.
17. RSA algoritmi.
18. ELGAMAL algoritmidan foydalanib shifrlash.
19. DSA.
20. GOST elektron raqamli imzo.
21. Diskret logarifmlar.
22. ONG-SHNORR-SHAMIR elektron raqamli imzo
23. ESIGN elektron raqamli imzo
24. ELGAMAL elektron raqamli imzo.
25. Bir necha kalitli algoritmlar.
26. «Yashirin» kanal.
27. Inkor etib bo‘lmaydigan raqamli imzo.
28. Shifrlangan ma’lumotlar bilan hisoblanish.
29. «Hammasi yoki hech narsa» protokoli.
30. Identifikatsiya sxemalari.
31. Fiat-Shamir imzo sxemalari.
32. Guillou-Quisquater imzo sxemalari.
33. Polinomial algoritmlar.
34. Psevdotasodifiy generatorlar.
35. Elektron to‘lovlar.
36. Xabarlar anonimligi
37. O‘zDSt shifrlash va raqamli imzo algoritmlari

## FOYDALANILGAN ADABIYOTLAR


1. Арипов М., Пудовченко Ю. Основы криптологии. Ташкент, 2003.
2. Гулямов С.С. Основы информационной безопасности. Ташкент, 2004.
3. Шнайер Б. Прикладная криптография. Протоколы, алгоритмы, исходные тексты на языке Си. Applied Cryptography. Protocols, Algorithms and Source Code in C. М.: Триумф, 2002.
4. Ғаниев С.К., Каримов М.М., Ташев К.А. Ахборот хавфсизлиги. Ахборот-коммуникацион тизимлар хавфсизлиги. Тошкент, 2009.
5. Аннин Б. Защита компьютерной информации. Москва, 2006.
6. Ященко В.В. Введение в криптографию. Москва, 1999.
7. Кузьминов В.П. Криптографические методы защиты информации. Новосибирск, 1998.
8. Menezes A., P. van Oorschot, Vanstone S. Handbook of Applied Cryptography. CRC Press, 1996. ISBN 0-8493-8523-7.
9. Gustavus J. Simmons. Contemporary Cryptology: The Science of Information Integrity (Wiley 1999). ISBN 0-7803-5352-8.
10. Gustavus J. Simmons. The subliminal channel and digital signatures. In Proc. of the EUROCRYPT 84 workshop on Advances in cryptology: theory and application of cryptographic techniques. New York, USA, 1985. Springer-Verlag New York, Inc.
11. Whitfield Diffie, Martin E. Hellman. New Directions in Cryptography. IEEE Transactions on Information Theory. — Nov. 1976. — T. IT-22.
12. Rivest R. L., Shamir A., Adleman L. A method for obtaining digital signatures and public-key cryptosystems. Communications of the ACM. - New York, NY, USA: ACM, 1978. - T. 21. - № 2, Feb. 1978.
13. Alfred J. Menezes, Paul C. van Oorschot, Scott A. Vanstone 11.5.2 The ElGamal signature scheme // Handbook of applied cryptography - http://www.cacr.math.uwaterloo.ca/hac/about/chap11.pdf
14. RFC 2631 – Diffie–Hellman Key Agreement Method E. Rescorla June 1999 - http://tools.ietf.org/html/rfc2631
15. Bakhtiari M., Maarof M. A. Serious Security Weakness in RSA Cryptosystem // IJCSI International Journal of Computer Science. — January 2012. — В. 1, № 3. — Т. 9. — ISSN1694-0814

16. Martin Gardner. Mathematical Games: A new kind of cipher that would take millions of years to break (англ.) // Scientific American. — 1977
17. Венбо Мао. Современная криптография. Теория и практика = Modern Cryptography: Theory and Practice. — М.: Вильямс, 2005. — 768 с.
18. Нильс Фергюсон, Брюс Шнайер. Практическая криптография = Practical Cryptography: Designing and Implementing Secure Cryptographic Systems. — М.: Диалектика, 2004
19. Б.А.Фороузан. Схема цифровой подписи Эль-Гамаля. Управление ключами шифрования и безопасность сети. Пер. А. Н. Берлин. — Курс лекций.
20. Саломаа А. Криптография с открытым ключом. — М.: Мир, 1995. — 318 с. — ISBN 5-03-001991-X
21. Pascal & Canteaut, Anne Advanced Linear Cryptanalysis of Block and Stream Ciphers. — IOS Press, 2011. — P. 2. — ISBN 9781607508441
22. Modeling Linear Characteristics of Substitution-Permutation Networks. Selected areas in cryptography: 6th annual international workshop, SAC'99, Kingston, Ontario, Canada, August 9-10, 1999 : proceedings. — Springer, 2000. — P. 79. — ISBN 9783540671855
23. Dial 'C' for Cipher // Selected areas in cryptography: 13th international workshop, SAC 2006, Montreal, Canada, August 17-18, 2006 : revised selected papers. — Springer, 2007. — P. 77. — ISBN 9783540744610
24. Cryptographic Boolean functions and applications. — Academic Press, 2009. — P. 164. — ISBN 9780123748904
25. Menezes, van Oorschot. Block Cipher Modes. NIST Computer Security Resource Center.
26. Morris Dworkin (December 2001), «Recommendation for Block Cipher Modes of Operation – Methods and Techniques», Special Publication 800-38A (National Institute of Standards and Technology (NIST))
27. «Kryptographische Verfahren: Empfehlungen und Schlüssellängen», BSI TR-02102 (no. Version 1.0), June 20, 2008
28. Martin, Keith M. Everyday Cryptography: Fundamental Principles and Applications. — Oxford University Press, 2012. — P. 114. — ISBN 9780199695591
29. Understanding Cryptography: A Textbook for Students and Practitioners. — Springer, 2010. — P. 30. — ISBN 9783642041006

30. James Nechvatal, Elaine Barker, Lawrence Bassham, William Burr, Morris Dworkin, James Foti, Edward Roback (October 2000), «Report on the Development of the Advanced Encryption Standard (AES)», National Institute of Standards and Technology (NIST)
31. Nicolas T. Courtois. Security Evaluation of GOST 28147-89. In View Of International Standardisation. Cryptology ePrint Archive: Report 2011/211
32. Лапонина О.Р. Криптографические основы безопасности. — М.: Интернет-университет информационных технологий - ИНТУИТ.ру, 2004. — С. 320. — ISBN 5-9556-00020-5
33. Гатчин Ю.А., Коробейников А.Г. Основы криптографических алгоритмов. Учебное пособие. - СПб.: СПбГИТМО(ТУ), 2002.
34. Кон П. Универсальная алгебра. - М.: Мир. - 1968.
35. Коробейников А. Г. Математические основы криптографии. Учебное пособие. СПб: СПб ГИТМО (ТУ), 2002.
36. Семаев И.А. Анализ и синтез криптографических протоколов. М.:, 2001
37. Pierre-Alain Fouque, Nick Howgrave-Graham, Gwenaelle Martinet, and Guillaume Poupard. The Insecurity of Esign in Practical Implementations. ASIACRYPT 2003, LNCS 2894, pp. 492-506, 2003.
38. Jean-Sebastien Coron, Marc Joye, David Naccache, and Pascal Paillier. Universal Padding Schemes for RSA. CRYPTO 2002, LNCS 2442, pp. 226-241, 2002.
39. А.В. Кобец (Komlin). Механизмы махинации с подписью в новом российском стандарте ЭЦП ГОСТ 34.19-2001. http://www.cryptography.ru/db/msg.html?mid=1169548
40. А.В. Кобец (Komlin). Подмена подписанного документа в новом американском стандарте ECDSA. http://www.cryptography.ru/db/msg.html?mid=1169548
41. Б.А. Погорелов, А.В. Черемушкин, С.И. Чечета. Об определении основных криптографических понятий. http://www.cryptography.ru/db/msg.html?mid=1169587
42. А. Винокуров. Стандарты аутентификации и ЭЦП России и США. http://www.bre.ru/security/19192.html
43. David Kahn. Remarks on the 50th Anniversary of the National Security Agency.
44. Alex Biryukov and Eyal Kushilevitz.: From Differential Cryptanalysis to Ciphertext-Only Attacks.

45. Yoshiharu Maeno. Node discovery in a networked organization. Proceedings of the IEEE International Conference on Systems, Man and Cybernetics. — San Antonio.
46. Дж. Л. Месси. Введение в современную криптологию. ТИИЭР, т.76, №5, Май 88 – М, Мир, 1988, с.24-42.
47. У. Диффи. Первые десять лет криптографии с открытым ключом. ТИИЭР, т.76, №5, Май 88 – М, Мир, 1988, с.54-74.
48. А. В. Спесивцев и др. Защита информации в персональных компьютерах. – М., Радио и связь. 1992, с.140-149.
49. В. Жельников. Криптография от папируса до компьютера. – М., ABF, 1996.
50. Hal Tipton and Micki Krause. Handbook of Information Security Management – CRC Press LLC, 1998.
51. Закон «Об информационно-библиотечной деятельности» от 13.04.2011г. №ЗРУ-280
52. Закон «О связи» от 13.01.1992 г. № 512-XII
53. Закон «О радиочастотном спектре» от 25.12.1998 г. № 725-I
54. Закон «О телекоммуникациях»
55. Закон «Об информатизации» от 11.12.2003 г. № 560-II
56. Закон «Об электронной цифровой подписи» от 11.12.2003 г № 562-II
57. Закон «Об электронном документообороте» от 29.04.2004 г. № 611-II
58. Закон «Об электронной коммерции» от 29.04.2004 г. № 613-II
59. Закон «О защите информации в автоматизированной банковской системе» от 04.04.2006 г. NЗРУ-30
60. Закон «О внесении изменений и дополнений в некоторые законодательные акты Республики Узбекистан в связи с усилением ответственности за совершение незаконных действий в области информатизации и передачи данных» от 25.12.2007г. №ЗРУ_137.

## VEB MANBALAR


1. www.intuit.ru
2. www.ziyonet.uz
3. www.nuu.uz
4. www.tuit.uz
5. www.rsa.com
6. Martin E. Hellman An overview of public key cryptography www.comsoc.org/livepub s/ci1/public/anniv/pdfs/hellman.pdf
7. www.williamspublishing.com/PDF/5-8459-0847-7/part.pdf
8. www.security.uz
9. www.cert.uz
10. www.unicon.uz
11. www.uzinfocom.uz
12. http://ccitt.uz/ru
13. www.securitylab.ru
14. www.wikipedia.org
15. www.cryptopro.ru
16. www.itsecurity.com
17. www.securityfocus.com
18. www.cert.org
19. www.infosyssec.com
20. www.securit.ru
21. www.leta.ru
22. www.cryptobook.rsu.ru
23. www.nasa.gov\statistics\

## MUNDARIJA

**ARIPOV MIRSAID MIRSIDIKOVICH**
**MATYAKUBOV ALISHER SAMANDAROVICH**

# AXBOROTLARNI HIMOYALASH USULLARI

(o‘quv-uslubiy qo‘llanma)

**Muharrir S.Qurbonov**

Bosishga ruxsat etildi 15.10.2012 y. Bichimi 60x84 $_{1/16}$.
Nashriyot hisob tabog‘i 7.0. Shartli bosma tabog‘i 10.0.
Adadi 100 nusxa. Bahosi shartnoma asosida.

“Universitet” nashriyoti. Toshkent – 100174.
Talabalar shaharchasi. Mirzo Ulug‘bek nomidagi
O‘zbekiston Milliy universiteti ma’muriy binosi.
O‘zMU bosmaxonasida bosildi.