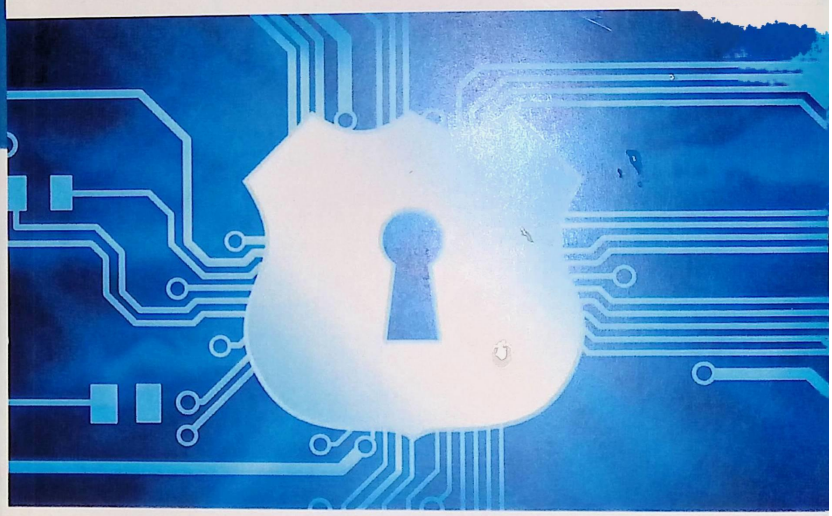
M.M. Aripov, B.F. Abdurahimov,
A.S. Matyakubov

KRIPTOGRAFIK USULLAR



O‘QUV QO‘LLANMA

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

MIRZO ULUG‘BEK NOMIDAGI
O‘ZBEKISTON MILLIY UNIVERSITETI

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

KRIPTOGRAFIK USULLAR

(O‘R OO‘MT vazirligining 2020 yil 14 avgustdagi 418-sonli buyrug‘iga asosan 5113200-Amaliy matematika va informatika, 5330200-Informatika va axborot texnologiyalari, 5330300-Axborot xavfsizligi bakalavriat ta’lim yo‘nalishlari uchun o‘quv qo‘llanma sifatida nashrga tavsiya etilgan)

Toshkent
«Tafakkur avlodi»
2023

UO'K: 003.26(075.8)
KBK: 73ya73
A 75

Aripov, M.M.
Kriptografik usullar [Matn]: o'quv qo'llanma / M.M. Aripov, B.F. Abdurahimov, A.S. Matyakubov. – Toshkent: «Tafakkur avlodi», 2023. – 188 b.

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

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

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

Xudoyqulov Z. Toshkent axborot texnologiyalari universiteti, Kriptologiya kafedrasi mudiri

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

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

ISBN 978-9943-8638-9-7

KIRISH

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

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

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

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

Kriptografiya (kriptografiya – *kryptos* – maxfiy, *grapho* – yozish kabi grekcha so'zlardan olingan) shifrlash usullari haqidagi fan sifatida paydo bo'ldi va uzoq vaqt mobaynida shifrlash ya'ni, uzatiladigan va

saqlanadigan axborotlarni ruxsat berilmagan foydalanuvchilardan himoyalashni o‘rganadigan fan sifatida shakllandi. Lekin, keyingi yillarda axborot texnologiyalarning gurkirab rivojlanishi maxfiy axborotlarni yashirish bilan to‘g‘ridan – to‘g‘ri bog‘liq bo‘lmagan ko‘pgina yangi kriptografiya masalalarini keltirib chiqardi.

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

I BOB. KRIPTOLOGIYA ASOSLARI

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

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

1.1. Asosiy tushunchalar

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

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

- *Kriptografiya* va *kriptotahlil.*

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

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

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

1) Simmetrik kriptotizimlar.

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

3) Elektron raqamli imzo kriptotizimlari.

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

Kriptografik uslublardan foydalanishning asosiy yo'nalishlari quyidagilar:

- mahfiy ma'lumotlarni ochiq aloqa kanali bo'yicha muhofazalangan holda uzatish;

• uzatilgan ma'lumotlarning xaqiqiyligini ta'minlash;

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

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

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

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

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

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

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

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

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

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

Kalit – bevosita dastlabki ma'lumotni shifrlash va deshifrlash uchun zarur bo'lgan manba. U ma'lumotlarni kriptografik qayta o'zgartirish algoritmi ayrim parametrlarining aniq maxfiy holati bo'lib, bu algoritm uchun turli – tuman to'plamdan bitta variantni tanlashini ta'minlaydi. Kalitning maxfiyligi shifrlangan matndan berilgan matnni

tiklash mumkin bo'lmasligini ta'minlaydi. K – kalitlar fazosi, bu mumkin bo'lgan kalit qiymatlari to'plamidir. Odatda kalit o'zida alfavit harflari qatorini ifodalaydi. «Kalit» va «Parol» tushunchalarini farqlash lozim. Parol ham maxfiy alfavit harflari ketma – ketligi bo'lib, u faqatgina shifrlash uchun emas, balki subyektni autentifikatsiya qilish uchun ham ishlatiladi.

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

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

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

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

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

– deshifrlash uchun qidirilayotgan kalitlarning mumkin bo'lgan barcha imkoniyatlari soni;

– deshifrlash uchun zarur bo'lgan o'rtacha vaqt.

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

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

– shifrlangan ma'lumotni asl nusxasiga ega bo'lish imkoniyati faqat deshifrlash kaliti ma'lum bo'lgandagina mumkin bo'lsin;

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

– shifrlash algoritmining ma'lumligi uning bardoshliligiga salbiy ta'sir ko'rsatmasligi;

– kalitning har qanday darajadagi o'zgarishi shifrlangan ma'lumotning jiddiy o'zgarishiga olib kelishi;

– shifrlash algoritmining tarkibidagi elementlar o'zgarmas bo'lishi;

– shifirlash jarayoni davomida ma'lumotlarga kiritiladigan qo'shimcha bitlar (elementlar) shifrlangan tekstda (ma'lumotda) to'la va ishonchli holda qo'llanilgan bo'lishi;

– shifrlash jarayonida qo'llaniladigan kalitlar orasida sodda va osonlik bilan o'rnatiladigan bog'liqliklar bo'lmasligi;

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

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

1.2. Axborot xavfsizligi kategoriyalari

Axborotxavfsizligi nuqtai nazaridan olib qaraganda axborotlarni quyidagi kategoriyalarga ajratish mumkin:

1. maxfiylik (konfidensiallik) - bu axborotlarning mo'ljallangan shaxslardan boshqasidan himoyalanganlik kafolati. Bu kategoriyaning buzulishi, axborotning o'g'irlanishi yoki fosh etilishi deyiladi;
2. butunlik – axborot uzatilganda yoki saqlanganda ko'rinishining o'zgarmaganlik kafolati. Bu kategoriyaning buzulishi soxtalashtirish deyiladi;
3. autentifikatsiya – foydalanuvchilarning haqiqiyligini aniqlash.
4. mualliflik – axborotda ko'rsatilgan muallifning aynan o'zi bo'lishi kafolati;

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

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

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

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

3. tizimga kirish nazorati – har xil guruhga mansub foydalanuvchilar axborot obyektlariga kirish ruxsati turlicha bo‘lishi va bu cheklashlar har doim bajarilishi kafolati;

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

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

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

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

1.3. Simmetrik va ochiq kalitli (nosimmetrik) kriptotizimlar

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

mumkin. Aloqa ishtirokchilari shifrlash kalitini olishganda u chinda ham shu kalitni yaratishga vakolatli kimsa tomonidan yoki tajovuzko tomonidan yuborilgan bo'lishi ham mumkin. Bu muammolarni tur kriptotizimlar turlicha hal qilib beradi.

Simmetrik kriptotizimda kalit aloqaning ikkala tomoni uchun bi xil maxfiy va ikkovlaridan boshqa hech kimga oshkor bo'lmaslig shart. Bunday tizimning xavfsizligi asosan yagona maxfiy kalitning himoya xossalariga bog'liq. Simmetrik kriptotizimlar uzoq o'tmishg ega bo'lsada, ular asosida olingan algoritmlar kompyuterlardag axborotlarni himoyalash zarurati tufayli ba'zi davlatlarda standar maqomiga ko'tarildilar. Masalan, AQShda ma'lumotlarni shifrlash standarti sifatida AES (Advanced Encryption Standart) algoritmi 200 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 funksional 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 kalitlar

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 onmalashuvi natijasida xat va xabarlarni almashishiga talab paydo bo'lishi yozma ma'lumotlar mazmunini begona kishilardan yashirish zaruriyatini keltirib chiqardi. Yozma ma'lumotlar mazmunini yashirish uslubi uch guruhga bo'linadi:

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

2.1. Kriptografiya tarixi

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

Axborotni shifrlashga doir yana ham aniq ma'lumotlar qadimgi Gretsiyaning paydo bo'lish davrlariga borib taqaladi. Eramizdan oldingi 56 asrlarda Sparta davlatida yaxshi rivojlangan kriptografiya mavjud bo'lgan. Ushbu davrlarga oid ikkita mashhur asbob, Sitala va Eniya jadvali mavjud bo'lgan. Ular yordamida ochiq tekstdagi ma'lumot harflarini jadvaldagi harflarga maxsus qoidalarga binoan almashtirilar edi. Eniy o'zining "Mudofaa haqida" nomli asarida "Kitobli shifr" bobini yozgan, Polibiy esa "Polibiy kvadrati" nomli shifrlash metodini yozgan. Bu metod maxfiy ma'lumotdagi har bir harfni ikkita raqam bilan almashtirishni, bu raqamlar o'z navbatida 5x5 kvadrat ichiga yozilgan mos harflar alfavit koordinatalari edi. Yuliy Sezar o'zining "Gall urushi haqida qo'lyozmalar" asarida, maxfiy ma'lumot harflarini uchta pozitsiya o'ngga surish orqali shifrlash metodini keltirgan.

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

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

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

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

Rasmiy kriptografiya (XV asr oxiridan XX asr boshlarigacha) bosqichi rasmiylashgan va qo'lda bajariluvchi shifr kriptotahlilini

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

XIX asrda gollandiyalik Kerkxoff kriptografik tizimlar uchun hozirgacha dolzarb bo'lgan, «shifrlarning maxfiyligi algoritmlarning maxfiyligiga emas, balki kalitning maxfiyligiga asoslanishi kerak» degan bosh talabni shakllantirdi. Natijada yaratilgan usullar nisbatan yuqori kriptobardoshlilikni ta'minladi va shifrlash jarayonini avtomatlashtiruvchi (mexanizatsiyalash ma'nosida) rotorli kriptotizimlarni yaratilishiga olib keldi. Yana shunga o'xshash tizimlardan biri 1790 yilda AQSh ning bo'lg'usi prezidenti Tomas Jeferson tomonidan yaratildi. Bunda rotorli mashina yordamida ko'p alfavitli almashtirish amalga oshirilar edi. Rotorli mashinalar XX asrning boshlaridagina amaliyotga keng tarqaldi. Dastlabki amaliyotda qo'llanilgan mashinalardan biri nemis «Enigma»si bo'lib, u 1917 yilda Edvard Xebern tomonidan ishlab chiqilgan va Artur Kirx tomonidan takomillashtirilgan. Tuzilishiga ko'ra "Enigma" oddiy avtomobil odometrini eslatardi: uchta rotordan (shifrdisk) iborat bo'lib, elektr moslamalar yordamida oldinma keyin joylashgan edi. Operator ochiq tekstdagi biror bir harfni qurilmaga yozmoqchi bo'lsa, qurilmadagi mos klavishani bosishi kerak bo'lar edi. Klavisha bosilganidan so'ng signal uchta shifrdiskda joylashgan aloqa tugmalaridan o'tadi. Shundan so'ng

hosil bo'lgan ma'lumot reflektor bo'limiga o'tar, undan esa boshqa yo'l "elekt yo'l" orqali ortga qaytar edi. Shundan so'ng birinchi disk bir pozitsiyaga o'zgarar edi. Shu sababdan kiritilayotgan keyingi harfning shifri butunlay boshqa qoidaga asosan hosil bo'lar edi. Operator 26 ta harfni kiritganidan so'ng birinchi disk o'zining boshlang'ich holiga qaytar, ammo ikkinchi disk bir pozitsiya o'zgarar edi. "Enigma" qurilmasi yordamida ma'lumotni tezda shifrlash uchun to'rt kishidan iborat brigada guruhi zarur edi: birinchisi ochiq tekstni o'qib turgan, ikkinchisi tekstni klaviatura yordamida terib turgan, uchinchisi indikatordan chiqqan shifrlangan ma'lumotni o'qib turgan, to'rtinchisi esa o'qilayotgan shifrtekstni telefon yoki boshqa qurilmalar orqali uzatib turgan. "Enigma" shifr tekstlarining kalitlari bo'lib rotorlarning boshlang'ich holi va elektron kommutatsiya zanjirlari keltirilar edi. Kalitlarni topish kombinatsiyasining ehtimoli 92 ta nollardan iborat bo'lgan raqam edi.

Rotor mashinalar ikkinchi jahon urushi vaqtida faol ishlatildi. Enigma nemis mashinasidan tashqari Sigaba (AQSh), Typex (Buyuk Britaniya), Red, Orangle va Purple (Yaponiya) kabi qurilmalar ham amaliyotda keng qo'llanildi. Rotorli tizimlar - formal kriptografiyaning cho'qqisi edi. Bunda juda chidamli shifrlar oson amalga oshirilgan edi. Rotorli tizimlarga 40-yillarda EHM laming paydo bo'lishi bilan muvaffaqqiyatli kriptografik hujum qilish imkoni paydo bo'ldi.

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

1960 yillardan boshlab, yetakchi kriptografik maktablar, rotorli kriptotizimlar bilan taqqoslaganda ancha mustahkam bo'lgan, lekin

amaliyotda faqatgina raqamli elektron qurimalardagina bajariladigan blokli shifrlarni tuza boshladilar.

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

Blokli shifrlar qudratli va kompakt hisoblash vositalari paydo bo'lishi bilan amaliyotda qo'llanilgan dastlabki kriptotizimlar sinfidir. 1970 yilda DES Amerika Qo'shma Shtatlari shifrlash standarti ishlab chiqildi (1978 yilda qabul qilindi). Uning mualliflaridan biri Xorst Feystel (IBM xodimi) boshqa simmetrik kriptografik tizimlar uchun ham asos bo'ladigan blokli shifrlash modelini tavsifladi. Xuddi shu model asosida boshqa shifrlash modellariga nisbatan mustahkamroq bo'lgan GOST 28147-89 simmetrik kriptotizimi yaratilgan.

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

1980-90 yillarda kriptografiyaning mutlaqo yangi yo'nalishlari: ehtimolli shifrlash, kvant kriptografiyasi va boshqalar paydo bo'ldi. Ularning amaliy qiymatini tushinish hali oldinda. Simmetrik kriptotizimlarni takomillashtirish ham haligacha dolzarb masala bo'lib qolmoqda. Bu davr ichida feystel to'riga ega bo'lmagan shifrlar

(SAFER, RC6 va boshqalar) yaratildi. 2005 yildan boshlab O'zbekistonda ham yangi milliy shifrlash va raqamli imzo standartlari qabul qilindi.

Kriptografiya axborot konfidentsialligi va yaxlitligini nazorat qilishni ta'minlovchi hamma narsadan ko'ra qudratli vositadir. Ko'pgina munosabatlarda u xavfsizlikning dasturiy – texnik boshqaruvchilari o'rtasida markaziy o'rin egallaydi. Masalan, portativ kompyuterlarda, ma'lumotlarni jismoniy himoyalash juda qiyin, faqatgina kriptografiya hatto axborot o'g'irlanganda ham uning konfidentsialligini kafolatlash imkonini beradi.

2.2. Kalit so'zli jadval almashtirishlar

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

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

Matnni shifrlash:

1.1. Jadvalning birinchi satriga kalit so'z yoziladi;

1.2. Ikkinchi satridan boshlab matn yozib chiqiladi;

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

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

1.4. Kalitdagi harflarning alfavitdagi tartib raqamlari yozib chiqiladi;

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

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

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

1.6. Ushbu jadvaldagi harflar gorizontal ketma-ketlikda yoziladi va matnning shifri hosil bo'ladi.

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