

Z.T. XUDOYKULOV
SH.Z. ISLOMOV
U.R. MARDIYEV

KRIPTOGRAFIYA 1

O'quv qo'llanma



- Kriptografiya va uning fundamental tushunchalari
- Kriptografiyaning matematik asosi
- Klassik shifrlash algoritmlari
- Psevdotasodifiy sonlar generatori va oqimli simmetrik shifrlash algoritmlari
- Simmetrik blokli shifrlash algoritmlari
- Xesh funksiyalar va ma'lumotning yaxlitligi ta'minlash

ISBN 978-9943-7323-8-4



9 789943 732384

**O‘ZBEKISTON RESPUBLIKASI AXBOROT
TEKNOLOGIYALARI VA KOMMUNIKATSIYALARINI
RIVOJLANTIRISH VAZIRLIGI**

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

Z.T.XUDOYKULOV, SH.Z.ISLOMOV, U.R.MARDIYEV

KRIPTOGRAFIYA 1

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

**TOSHKENT
“IQTISOD-MOLIYA”
2021**

UDK: 004.056.5(075.8)

KBK: 32.81

Taqrizchilar:

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

O.P.Axmedova – texnika fanlari nomzodi, “UNICON.UZ” DUK – Fan-texnika va marketing tadqiqotlari markazi “Axborot xavfsizligi va kriptologiya ilmiy tadqiqot bo'limi” boshlig'i.

X 78 Kriptografiya 1: O'quv qo'llanma / Z.T.Xudoykulov, Sh.k.Z.Islomov, U.R.Mardiyev; – T.: “Iqtisod-Moliya”, 2021. – 204 b.

O'quv qo'llanmada kriptografiya fan sohasi va uning axborot xavfsizligini ta'minlashdagi o'rni, kriptografiyaning matematik asosi, klassik shifrlar va ularning tahlili, psevdotasodifiy sonlar generatori va ularga asoslangan simmetrik oqimli shifrlash algoritmlari, simmetrik blokli shifrlash algoritmlari, xesh funksiyalarni yaratish asosi va zamonaviy xesh funksiyalarning nazariy va amaliy asoslari muhokama etilgan.

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

UDK: 004.056.5(075.8)

KBK: 32.81

ISBN 978-9943-7323-8-4

**© Z.T.Xudoykulov, Sh.k.Z.Islomov,
U.R.Mardiyev, 2021**

© “IQTISOD-MOLIYA”, 2021

MUQADDIMA

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

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

Keyingi yillarda kriptologiya yo‘nalishini rivojlantirishga davlatimiz tomonidan katta ahamiyat berilmoqda. 2017–2021-yillarda O‘zbekiston Respublikasini yanada rivojlantirish bo‘yicha Harakatlar strategiyasida vazifalar belgilab olindi, shular qatorida «...axborot xavfsizligini ta‘minlash va axborotni himoya qilish tizimini takomillashtirish, axborot sohasidagi tahdidlarga o‘z vaqtida va munosib qarshilik ko‘rsatish» va kiberjinoyatchilikni fosh etish masalalariga alohida e‘tibor qaratilgan. Bundan tashqari, O‘zbekiston Respublikasi Prezidentining 2007-yil 3-aprelda qabul qilingan «O‘zbekiston Respublikasida axborotning kriptografik himoyasini tashkil etish chora-tadbirlari to‘g‘risida»gi PQ-614-son Qarorida belgilangan asosiy vazifalardan biri axborotni muhofaza qilish sohasida yuqori malakali kadrlarni tayyorlashdan iborat bo‘lib, buning uchun axborot xavfsizligi va kriptografiya yo‘nalishlarida davlat tilida ta‘lim olayotgan talabalar, tadqiqotchilar va ilmiy xodimlar uchun mo‘ljallangan o‘quv qo‘llanmalar, darsliklar, uslubiy qo‘llanmalar va kitoblar chop etish muhim ahamiyat kasb etadi. Mazkur o‘quv qo‘llanma ana shu sohada bajarilgan ishlardan biri hisoblanadi.

Qo‘llanmaning birinchi bobida axborot xavfsizligini ta‘minlashda kriptografiyaning o‘rni, kriptografik funksiyalar, kriptografiyaning asosiy tushunchalari va atamalari, zamonaviy kriptografiyaning bo‘limlari haqida ma‘lumotlar keltirilgan.

Ikkinchi bob kriptografiyaning matematik asosiga bag'ishlangan hamda ehtimollar nazariyasi asoslari, axborot nazariyasi asoslari, murakkablik nazariyasi, sonlar nazariyasi va fundamental algebra asoslariga oid ma'lumotlar keltirilgan.

Uchinchi bobda klassik shifrlash algoritmlari, xususan, sodda o'rniga qo'yish va o'rin almashtirish shifrlari, Vernam shifri, Kodlar kitobi, Enigma mashinasi va ularning kriptotahliliga oid ma'lumotlar keltirilgan.

Qo'llanmaning to'rtinchi bobi oqimli shifrlash algoritmlariga bag'ishlangan bo'lib, tasodifiy ketma-ketliklarni hosil qilish usullari, chiziqli va chiziqsiz kongurent generatorlar, oqimli shifrlarni qurish usullari hamda qator zamonaviy oqimli shifrlash algoritmlari haqida ma'lumotlar keltirilgan.

Beshinchi bobda simmetrik blokli shifrlarni qurish usullari, zamonaviy simmetrik blokli shifrlar standartlari, algoritmlari va simmetrik blokli shifrlash rejimlari haqida batafsil ma'lumotlar keltirilgan.

Yettinchi bob axborotning yaxlitligini ta'minlashga bag'ishlangan bo'lib, unda xesh funksiyalar va ularni qurish usullari, zamonaviy xesh funksiya algoritmlari, ma'lumotlarni autentifikatsiyalash kodlari haqida ma'lumotlar keltirilgan.

1 BOB. KRIPTOGRAFIYA VA UNING FUNDAMENTAL TUSHUNCHALARI

1.1. Axborot xavfsizligi va kriptografiya

Axborot tushunchasi tushunilgan miqdorni anglatib, u turli ko‘rinishlarda bo‘lishi mumkin. Axborotni ishonchli himoyasini tashkil etishda kriptografiya muhim ahamiyat kasb etadi. Kriptografik himoyani joriy qilish uchun axborot xavfsizligi bilan bog‘liq umumiy masalalarni tushunish kerak. Axborot xavfsizligi vaziyat va talabga muvofiq ravishda turlicha namoyon bo‘ladi. Foydalanuvchining kimligidan va qanday darajada ishtirok etganidan qat‘iy nazar tomonlar axborot xavfsizligi bilan bog‘liq ba‘zi maqsadlarga erishadi. 1.1-jadvalda ushbu maqsadlarning ba‘zilari keltirilgan.

1.1-jadval

Axborot xavfsizligining maqsadlari

| № | Maqsad | Izoh |
|----------|---|---|
| 1 | 2 | 3 |
| 1. | Shaxsiylik yoki konfidensiallik | Axborotni ko‘rish huquqiga ega bo‘lganlardan tashqari barchadan sir tutish.k. |
| 2. | Ma‘lumot yaxlitligi | Axborotni ruxsatsiz yoki noma‘lum vositalar bilan o‘zgartirilmaganligini ta‘minlash |
| 3. | Subyekt autentifikatsiyasi yoki identifikatsiyasi | Subyektning shaxsini tasdiqlash (masalan, shaxs, kompyuter, kredit karta va h.k.k.) |
| 4. | Xabar autentifikatsiyasi | Ma‘lumot manbasini tasdiqlash; u ma‘lumot kelib chiqishi autentifikatsiyasi deb ham ataladi |
| 5. | Imzo | Subyektga axborotni tegishligini ko‘rsatadi |
| 6. | Avtorizatsiya | Bir narsani qilish uchun subyektga ruxsatni yetkazish |
| 7. | Tasdiqlash | Axborot yoki resursdan foydalanish yoki boshqarishda avtorizatsiyani o‘z vaqtida taqdim etish |

| 1 | 2 | 3 |
|-----|--------------------------|--|
| 8. | Foydalanishni boshqarish | Imtiyozli subyektlarga resurslardan foydalanishni cheklash |
| 9. | Sertifikatlash | Axborotni ishonchli tashkilot tomonidan tasdiqlash |
| 10. | Vaqt belgisi | Axborotni yaratish yoki mavjud bo'lish vaqtini qayd etish |
| 11. | Guvohlik berish | Yaratuvchidan boshqa subyekt tomonidan axborotni yaratilganligi yoki mavjudligini tekshirish |
| 12. | Qabul qilish tasdig'i | Axborotni qabul qilinganligini tasdiqlash |
| 13. | Isbotlash | Xizmatlar taqdim etilganligini tasdiqlash |
| 14. | Egalik qilish | Subyektga resurslardan foydalanish yoki boshqalarga o'tkazish uchun qonuniy huquqni taqdim etish |
| 15. | Anonimlik | Ba'zi jarayonlarda ishtirok etuvchining shaxsini yashirish |
| 16. | Rad eta olmaslik | Oldingi majburiyatlarni yoki harakatlarni rad etishni oldini olish |
| 17. | Bekor qilish | Sertifikat yoki avtorizatsiyani bekor qilish |

Asrlar davomida axborotni fizik ko'rinishdagi hujjatlarda uzatish uchun axborot xavfsizligi masalalarini hal qiluvchi protokol va mexanizmlar ishlab chiqilgan. Axborot xavfsizligini ta'minlashda qo'yilgan maqsadga erishish nafaqat protokol yoki algoritmlar asosida, balki muolajaviy usullar va ma'lum qonunlarga rioya qilish asosida ham amalga oshiriladi. Masalan, maktub va xatlarni yetkazib berishda maxfiylik pochta xizmati orqali taqdim etilgan muhrlangan konvert orqali ta'minlanadi. Bundan tashqari, konvertga jismoniy zarar yetkazish yoki ruxsatsiz ochish jinoyat sifatida baholanadi.

O'z navbatida hozirgi elektronlashgan jamiyatda axborot xavfsizligiga erishish uchun ham ko'plab texnik va huquqiy ko'nikmalar talab etiladi. Shunday bo'lsada, axborot xavfsizligining barcha yuqorida keltirilgan maqsadlariga yetarli darajada erishishning imkoni yo'q. Aksariyat hollarda, axborot xavfsizligini ta'minlashda zarur bo'lgan texnik ko'nikmalar kriptografiya orqali ta'minlanadi.

Kriptografiya axborot xavfsizligining maqsadlari: konfidensiallik, ma'lumot yaxlitligi, subyekt autentifikatsiyasi va xabar

autentifikatsiyasi, bilan bog‘liq matematik usullarni o‘rganadi. Kriptografiya nafaqat axborot xavfsizligini ta‘minlash vositasi, balki usullar to‘plami ham hisoblanadi. Kriptografiya 1.1-jadvalda keltirilgan axborot xavfsizligining quyidagi maqsadlariga erishishni kafolatlaydi:

1. *Konfidensiallik* – bu axborot mazmunini unga ega bo‘lishga vakolati bo‘lganlardan tashqari, barchadan saqlash xizmati hisoblanadi. Ko‘p hollarda maxfiylik tushunchasi konfidensiallik va shaxsiylikka sinonim sifatida ishlatiladi. Konfidensiallikni ta‘minlashda fizik himoyalashdan tortib axborotni tushunarsiz holatga keltiruvchi matematik algoritmlargacha bo‘lgan yondashuvlardan foydalaniladi.

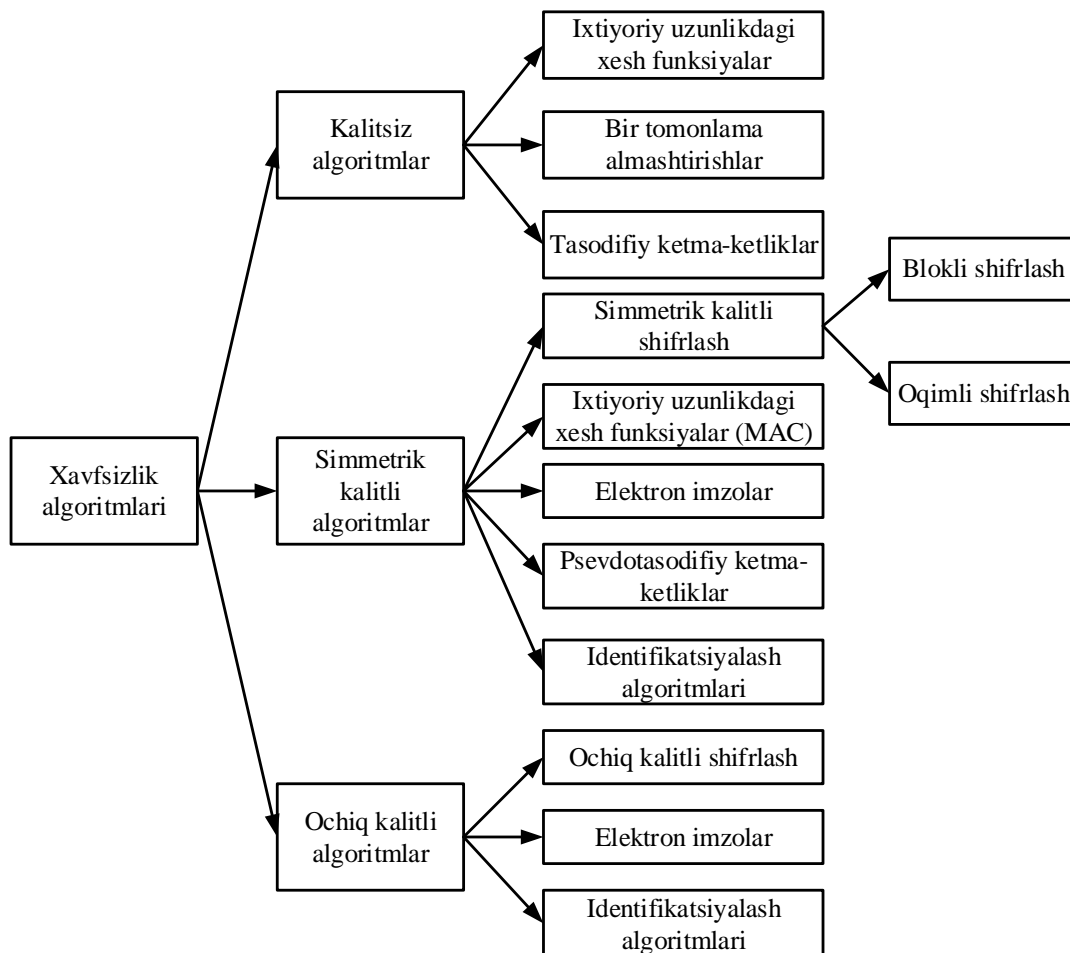
2. *Ma‘lumot yaxlitligi* - ma‘lumotlarni ruxsatsiz o‘zgartirishga qarshi qaratilgan xizmat bo‘lib, mazkur xizmatni kafolatlash uchun ruxsat etilmagan foydalanuvchilar tomonidan ma‘lumotlarni modifikatsiyalanishini aniqlash kerak bo‘ladi. Ma‘lumotlarni modifikatsiyalash o‘zida *qo‘shish, o‘chirish va almashtirish* kabi amallarni mujassamlashtiradi.

3. *Autentifikatsiyalash* xizmati identifikatsiyalashga aloqador bo‘lib, u ham subyekt ham ma‘lumotning o‘zi uchun amal qiladi. Ma‘lumot almashinuvchi ikki tomon bir-birini haqiqiylikni tasdiqlashi talab etilsa, aloqa kanalida uzatilayotgan axborotni uning manbasini, yaratilgan vaqti, ma‘lumot tarkibi, yuborilgan vaqti va h.k.k. bo‘yicha tasdiqlash kerak bo‘ladi. Shu sababli kriptografiyaning mazkur maqsadi ikki sinfga: subyektni autentifikatsiyalash va xabarni autentifikatsiyalashga ajratiladi.

4. *Rad eta olmaslik* xizmati avvalgi majburiyatlarni yoki harakatlarni rad etishga to‘sqinlik qiladi. Ko‘p holatlarda subyekt tomonidan muayyan harakatlarni amalga oshirilganligi inkor etilgani bois, nizolar kelib chiqadi. Mazkur muammolarni oldini olishda ishonchli uchinchi tomon ishtirokidagi biror muolaja talab etiladi.

Kriptografiyaning asosiy maqsadi ham nazariyada ham amaliyotda ushbu to‘rtta vazifani yetarli darajada amalga oshirishdan iborat. Shuning uchun kriptografiyani aldash va boshqa zararli harakatlarni aniqlash va ulardan himoyalash haqidagi fan sifatida ham qarash mumkin.

Mazkur o‘quv qo‘llanma axborot xavfsizligini ta‘minlashda foydalaniluvchi bir qancha asosiy kriptografik algoritmlarga bag‘ishlangan bo‘lib, 1.1-rasmda ularning umumiy holati aks ettirilgan. Ular haqida ushbu bobda qisqacha to‘xtilib o‘tilsa, keyingi boblarda ular haqida batafsil ma‘lumotlar keltiriladi.



1.1-rasm. Kriptografik algoritmlar tasnifi

Keltirilgan kriptografik algoritmlar quyidagi omillar bo‘yicha baholanishi kerak:

1. *Xavfsizlik darajasi.* Ushbu omilni miqdoriy qiymatini aniqlash murakkab bo‘lib, qo‘yilgan vazifani bajarish uchun zarur bo‘lgan amallar soni (joriy vaqtda mavjud bo‘lgan eng yaxshi usul va vositalardan foydalangan holda) bo‘yicha beriladi.

2. *Funksionallik.* Axborot xavfsizligini turli maqsadlariga erishishda kriptografik algoritmlarni birlashtirish kerak bo‘ladi. Berilgan maqsad uchun qaysi kriptografik algoritm eng samarali ekanligi uning xususiyati bilan belgilanadi.

3. *Ishlash usuli.* Kriptografik algoritmlar turli usul va ma’lumotlar bilan qo‘llanilganda, turli xususiyatlarni namoyish etadi. Shuning uchun, bitta kriptografik algoritm ishlash uslubi yoki ishlatilishiga qarab turli funksiyalarni taqdim etishi mumkin.

4. *Samaradorlik.* Bu omil ma’lum bir ishlash rejimi uchun kriptografik algoritmning samaradorligini ko‘rsatadi (masalan, shifrlash

algoritmining darajasi bir sekundda shifrlanuvchi ma'lumot hajmi bilan belgilanishi mumkin).

5. *Amalga oshirishning osonligi.* Bu omil amalda kriptografik algoritmi amalga oshirishning murakkabligini anglatadi. Bu kriptografik algoritmi dasturiy yoki apparat ko'rinishda amalga oshirishning murakkabligini o'z ichiga olishi mumkin.

1.2. Kriptografik funksiyalar

Kriptografiya fani matematik bilimlarga asoslangan bo'lib, uning fundamental tushunchalaridan biri – *funksiya* hisoblanadi. Shuningdek, kriptografiyada funksiya tushunchasiga analog bo'lgan *akslantirish* va *almashtirish* tushunchalari ham ishlatiladi.

Funksiyalar

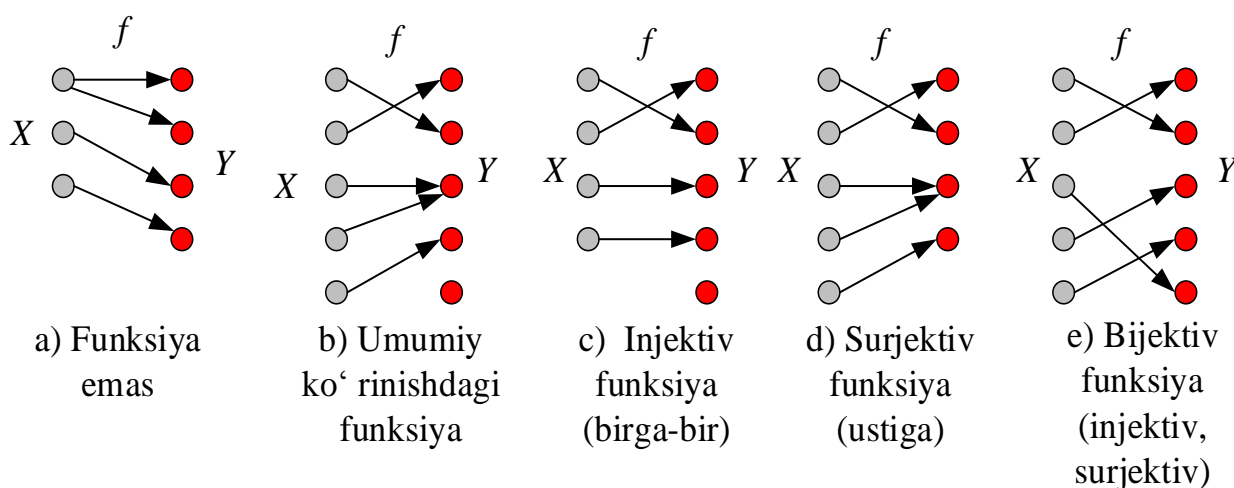
To'plam chekli sondagi obyektlardan iborat bo'lib, ular *elementlar* deb ataladi. Masalan, X to'plam a , b va c elementlardan iborat bo'lishi mumkin va shuning uchun $X = \{a, b, c\}$ shaklida belgilanadi.

Funksiya ikkita to'plam, X va Y hamda X to'plamdagi har bir elementni Y to'plamdagi bir elementga bog'lovchi f qoida bilan belgilanadi. X to'plam funksiyaning *aniqlanish sohasi* deb atalsa, Y to'plam funksiyaning *qiymatlar sohasi* deb ataladi. Agar X to'plamning elementi x bo'lsa (odatda $x \in X$ shaklida yoziladi) va unga mos qiymatlar sohasining elementi y bo'lsa, uni $y = f(x)$ shaklida ifodalash mumkin. X to'plamdan Y to'plamga akslantiruvchi f funksiyaning standart ifodasi $f: X \rightarrow Y$ shaklida ifodalanadi (1.2-rasm "b").

Ta'rif 1.2.1. Agar Y qiymatlar sohasining har bir elementi X aniqlanish sohasida eng ko'pi bilan bir elementga mos kelsa, u holda bu funksiya *1-1 (birga bir yoki injektiv) funksiya* deb ataladi (1.2-rasm "c").

Ta'rif 1.2.2. Agar Y qiymatlar sohasining har bir elementi X aniqlanish sohasida eng kamida bir elementiga mos kelsa, u holda bu funksiya *ustiga (ko'pga bir yoki surjektiv) funksiya* deb ataladi (1.2-rasm "d"). Agar $f: X \rightarrow Y$ funksiya surjektiv bo'lsa, $Im(f) = Y$ shaklida belgilanadi.

Ta'rif 1.2.3. Agar f funksiya ham injektiv ham surjektiv bo'lsa, u holda bu funksiya *bijektiv funksiya* deb ataladi (1.2-rasm "d").



1.2-rasm. **Funksiyalarning tasvirlanishi**

Ta'rif 1.2.4. Agar f funksiya X to'plamdan Y to'plamga akslantiruvchi bijektiv funksiya bo'lsa, u holda Y to'plamdan X to'plamga akslantiruvchi g bijektiv funksiyani olish mumkin: har bir $y \in Y$ uchun $g(y) = x$ aniqlanadi. Bu yerda, $x \in X$ va $f(x) = y$. Olingan g funksiya f funksiyaning *teskarisi* (yoki *inversi*) deb ataladi va $g = f^{-1}$ shaklida belgilanadi.

Bir tomonlama funksiyalar. Funksiyalarning shunday turlari mavjudki, ular kriptografiyada muhim o'rin tutadi. Ulardan biri *bir tomonlama* funksiya

Ta'rif 1.2.5. Agar f funksiya barcha $x \in X$ uchun oson hisoblanarli, biroq, barcha $y = Im(f)$ lar uchun $f(x) = y$ shartni qanoatlantiruvchi $x \in X$ larni topish imkonsiz bo'lsa, u holda f funksiya X to'plamdan Y to'plamga akslantiruvchi *bir tomonlama funksiya* deb ataladi.

Misol 1.2.1. $X = \{1,2,3, \dots, 16\}$ va barcha $x \in X$ lar uchun $f(x) = r_x$ o'rinli bo'lsin. Bu yerda, $r_x = 3^x \text{ mod } 17$ ga teng bo'lsin. U holda funksiya qiymatlari quyidagicha bo'ladi:

| | | | | | | | | | | | | | | | | |
|--------|---|---|----|----|---|----|----|----|----|----|----|----|----|----|----|----|
| x | 1 | 2 | 3 | 4 | 5 | 6 | 7 | 8 | 9 | 10 | 11 | 12 | 13 | 14 | 15 | 16 |
| $f(x)$ | 3 | 9 | 10 | 13 | 5 | 15 | 11 | 16 | 14 | 8 | 7 | 4 | 12 | 2 | 6 | 1 |

Yuqorida keltirilgani kabi 1 dan 16 gacha bo'lgan sonlar uchun f funksiya qiymatini hisoblash oson. Biroq, berilgan 7 uchun yuqoridagi jadvaldan foydalanmasdan $f(x) = 7$ shartni qanoatlantiruvchi x elementni topish imkonsiz hisoblanadi.

Misol 1.2.2. Tub sonlar birdan katta musbat butun sonlar bo'lib, faqat bir va o'ziga bo'linadi. Tub bo'lgan $p = 48611$ va $q = 53993$

sonlar bo'lsa, u holda $n = p * p = 2624653723$ ga teng. Shuningdek, $X = \{1,2,3, \dots, n - 1\}$ ga teng bo'lsin. Aniqlanish sohasi X bo'lgan f funksiya $f(x) = r_x$ ga teng bo'lib, bu yerda $r_x = x^3 \bmod n$ ga teng. Masalan, $2489991^3 = 5881949859 * n + 1981394214$ bo'lgani bois, $f(2489991) = 1981394214$ ga teng. $f(x)$ funksiyaning hisoblash juda oson bo'lib, uning teskarisini aniqlash juda murakkab. Ayniqsa, n noma'lum bo'lganda mazkur muammo yanada murakkablashadi.

Qopqonli bir tomonlama funksiyalar

Ta'rif 1.2.6. Berilgan ixtiyoriy $y \in Im(f)$ uchun $x \in X$ ni topishda ba'zi ortiqcha axborotni (tuzoqli axborot) taqdim qiluvchi qo'shimcha xususiyatga ega bir tomonlama $f: X \rightarrow Y$ funksiyaga qopqonli bir tomonlama funksiya deb ataladi.

1.2.2-misol qopqonli bir tomonlama funksiyaning aks ettiradi. Qo'shimcha axborot, $n = 2624653723$ (ya'ni, $p = 48611$ va $q = 53993$, har biri 5 xonali sondan iborat) ma'lum bo'lganda, funksiyaning invertini hisoblash oson. 2624653723 sonini hisoblash vositasidan foydalanmasdan faktorlash esa murakkab. Albatta, buni zamonaviy kompyuterlar yordamida osonlik bilan hisoblash mumkin. Boshqa tomondan, p va q sonlari yetarlicha katta tanlansa (masalan, har biri 100 xonadan iborat), hozirgi kundagi hisoblash kompyuterlari yordamida ham ushbu muammoni yechish murakkab hisoblanadi. Ushbu muammo *butun sonni faktorlash* deb nomlanadi.

Bir tomonlama va qopqonli bir tomonlama funksiyalar ochiq kalitli kriptografiyaning asosi hisoblanadi. Ushbu funksiyalarni kriptografik himoyada qo'llanilishini ko'rib chiqqanda ularning ahamiyati yanada aniq bo'ladi.

O'rin almashtirish funksiyalari

O'rin almashtirishlar turli kriptografik tuzilmalarda keng qo'llaniluvchi funksiya hisoblanadi.

Ta'rif 1.2.7. S chekli sondagi elementlar to'plami berilgan bo'lsin. U holda p o'rin almashtirish funksiyasi S to'plamdan o'ziga akslantiruvchi, $p: S \rightarrow S$ (boshqacha aytganda, aniqlanish va qiymatlar sohasi teng) bijektiv funksiyaadir.

Misol 1.2.3. Faraz qilaylik $S = \{1,2,3,4,5\}$ va o'rin almashtirish funksiyasi $p: S \rightarrow S$ quyidagicha bo'lsin:

$$p(1) = 3, p(2) = 5, p(3) = 4, p(4) = 2, p(5) = 1.$$

O‘rin almashtirish funksiyasi yuqoridagi kabi yoki quyida keltirilgan massiv kabi akslantirilishi mumkin:

$$p = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 3 & 5 & 4 & 2 & 1 \end{pmatrix}.$$

Bu yerda, massivning yuqori qatori o‘rin almashtirishning aniqlanishi sohasini ko‘rsatsa, pastki qatori qiymatlar sohasini ko‘rsatadi.

O‘rin almashtirish funksiyasi bijektiv bo‘lgani bois, unga teskari bo‘lgan funksiya mavjud. Agar o‘rin almashtirish funksiyasi p yuqoridagi kabi berilgan bo‘lsa, massiv qatorlari o‘rnini almashtirish va birinchi qatorni tartiblash orqali p ning teskarisini hosil qilish mumkin:

$$p^{-1} = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 5 & 4 & 1 & 3 & 2 \end{pmatrix}.$$

Involyutiv funksiyalar

Kriptografiyada keng qo‘llaniluvchi funksiyalardan yana biri *involyutiv* funksiyalar bo‘lib, o‘zining teskarisiga teng bo‘ladi.

Ta’rif 1.2.8. Agar S chekli elementdan iborat to‘plam va f esa S dan S ga akslantiruvchi bijektiv funksiya bo‘lsin. $f = f^{-1}$ shart bo‘lsa, f funksiya *involyutiv* deb ataladi. Ushbu tenglikni barcha $x \in S$ lar uchun $f(f(x)) = x$ shaklida ham yozish mumkin.

Misol 1.2.4. Faraz qilaylik $S = \{1,2,3,4,5\}$ ga teng bo‘lsin. U holda quyidagi f funksiyani $f: S \rightarrow S$ involyutiv deb aytish mumkin:

$$f(1) = 4, f(2) = 2, f(3) = 5, f(4) = 1, f(5) = 3.$$

1.3. Kriptografiyaning asosiy tushunchalari va atamalari

Har bir fanni o‘rganishdan oldin uning asosiy tushunchalarini bilish talab qilinadi. Quyida keyingi bayonlarda ishlatiluvchi asosiy atamalarga oydinlik kiritiladi.

Alfavit deganda axborotni ifodalashda ishlatiluvchi belgilarning chekli to‘plami tushuniladi. Zamonaviy kriptotizimlarda ko‘pincha atigi ikkita simvoldan $(0, 1)$ iborat ikkilik alfavit, $A = \{0,1\}$, ishlatiladi. Shuningdek, o‘ttiz oltita belgidan (harfdan) iborat o‘zbek tili alfavitini, o‘ttiz ikkita belgidan (harfdan) iborat rus tili alfavitini, yigirma sakkizta belgidan (harfdan) iborat lotin alfavitini, ikki yuzi ellik oltita belgidan

iborat ASCII kompyuter belgilarining alfavitini ham misol sifatida keltirish mumkin.

Matn yoki *xabar* – alfavit elementlaridan tartiblangan nabor. *Ochiq matn* (plaintext, P) – shifrlashga atalgan dastlabki xabar. *Shifrmatn* (cipher text, C) – ochiq matnni shifrlash natijasi.

Kalit (key, K), yoki kriptoo‘zgaruvchi (cryptovvariable) – o‘zgartirishlar oilasidan birini tanlashni ta‘minlovchi kriptografik algoritmning qandaydir parametrlarining muayyan qiymati.

Shifrlash (encryption, enciphering) – ochiq matnni shifrmatnga o‘zgartirish jarayoni, ya‘ni, $E_K: P \rightarrow C$ kabi belgilanib, u bijektiv funksiya hisoblanadi.

Rasshifrovkalash (decryption, deciphering) – shifrmatnni ochiq matnga o‘zgartiruvchi teskari jarayon, ya‘ni, $D_K: C \rightarrow P$ kabi belgilanib, u ham bijektiv funksiya hisoblanadi. Shifrlash va rasshifrovkalash bir – biriga teskari tushunchalar bo‘lgani bois, $D_K = E_K^{-1}$ tenglikni yozish mumkin. Shifrlash algoritmi turiga qarab shifrlash va rasshifrovkalash jarayonida foydalanilgan kalitlar o‘zaro teng yoki turlicha bo‘lishi mumkin.

Deshifrlash (breaking) – kalitni bilmasdan turib shifrmatn bo‘yicha ochiq matnni tiklash jarayoni.

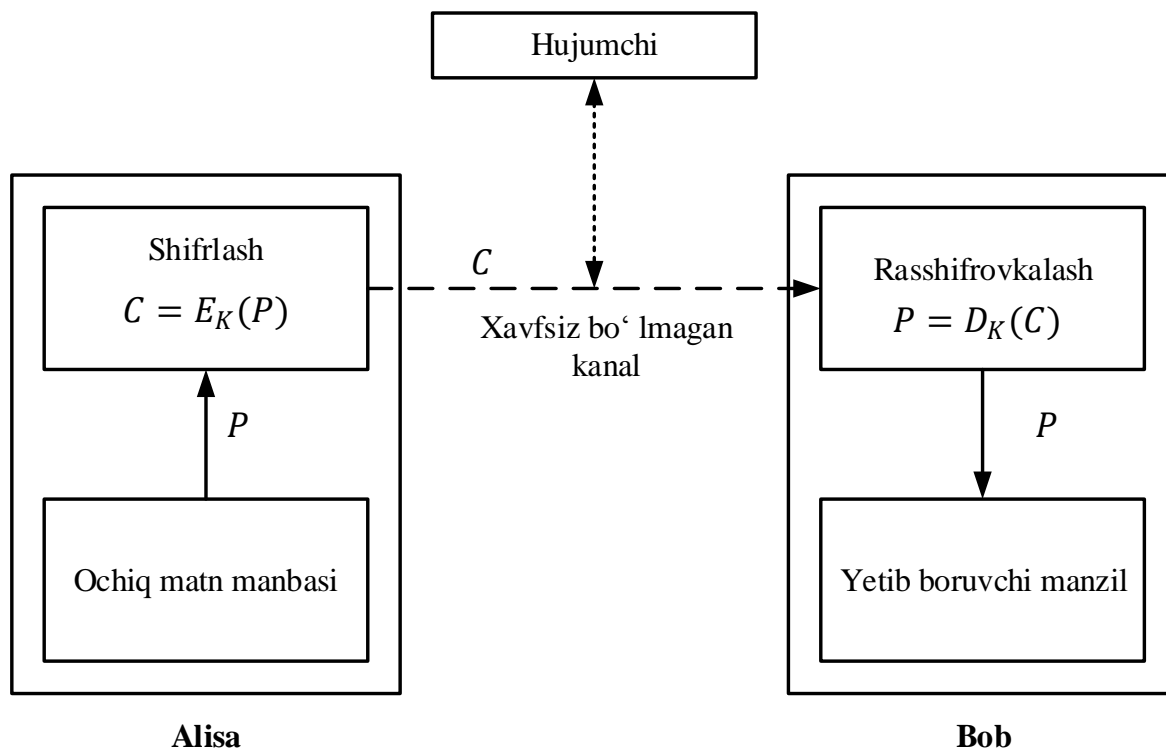
Rasshifrovkalash bilan deshifrlash orasidagi tafovutga e‘tibor qarataylik: agar rasshifrovkalash kriptografik algoritmdan foydalanilganda standart shtatli muolaja hisoblansa, deshifrlash, ko‘proq kriptotahlilga taalluqli, kriptotizimni buzishdir. “Shifrlash” umumiy atamasi shifrlash va rasshifrovkalash jarayonini bildiradi.

Shifrlash jarayonidan axborotni konfidensialligini ta‘minlash maqsadida foydalanilish mumkin. Ikki tomon, Alisa va Bob, o‘rtasida dastlab kalit K (faraz qilinsin, shifrlash va rasshifrovkalash uchun bir xil kalitdan foydalanilgan bo‘lsin) maxfiy tarzda yetkazilgan bo‘lsin. Agar Alisa P ochiq matnni yubormoqchi bo‘lsa, u holda $C = E_K(P)$ qiymatni hisoblaydi va Bobga yuboradi. Bob C ni qabul qilishi bilan $P = D_K(C)$ ni hisoblaydi va haqiqiy ochiq matn P ni tiklaydi.

Shifrlash va rasshifrovkalash jarayonida kalitdan foydalanilganiga e‘tibor qarataylik. Nima uchun shunchaki biror shifrlash funksiyasi va unga mos rasshifrovkalash funksiyasidan foydalanish mumkin emas? Shifrlash va rasshifrovkalash funksiyasida kalitdan foydalanishdan asosiy maqsad har bir ma‘lumot uchun ularni qayta loyihalashdan

qochishdir. Ya'ni, faqat shifrlash va unga mos rasshifrovkalash funksiyasidan foydalanilganda agar buzg'unchi ularni aniqlasa, yangi shifrlash/ rasshifrovkalash funksiyasini loyihalash talab etiladi. Agar kalitdan foylanilgan bo'lsa, unda faqat kalitni almashtirishning o'zi yetarli bo'ladi.

Umumiy holda shifrlashga asoslangan ikki tomon orasida tashkil qilingan aloqaning umumiy ko'rinishi 1.3-rasmda keltirilgan.



1.3-rasm. Shifrlashga asoslangan ikki tomon o'rtasida tashkil etilgan aloqa sxemasi

Yuqorida keltirilgan shifrlashga asoslangan aloqa sxemasida quyidagi ishtirokchilar mavjud:

- *subyekt* yoki *tomon* axborotni jo'natuvchi, qabul qiluvchi va o'zgartiruvchi foydalanuvchi yoki uning nomidan ishlovchi elektron qurilma. 1.3-rasmdagi Alisa va Bob keltirilgan aloqa sxemasi uchun subyekt sifatida xizmat qiladi. Subyekt sifatida shaxs, hisoblash mashinasi va h.k. xizmat qilishi mumkin.

- *jo'natuvchi* ikki tomon o'rtasida tashkil qilingan aloqa sxemasida axborotni qonuniy uzatuvchi subyekt hisoblanib, 1.3-rasmda Alisa sifatida aks ettirilgan.

- *qabul qiluvchi* ikki tomon o'rtasida tashkil qilingan aloqa sxemasida axborotni qonuniy qabul qiluvchi subyekt hisoblanib, 1.3-rasmda Bob sifatida aks ettirilgan.

- *hujumchi* ikki tomon o'rtasida tashkil qilingan aloqa sxemasida jo'natuvchi ham, qabul qiluvchi ham bo'lmagan, biroq, jo'natuvchi va qabul qiluvchi o'rtasida ta'minlangan axborot xavfsizligini buzishga harakat qiluvchi ikki tomonlama aloqada bo'lgan subyekt. Ushbu subyektning hujumchidan tashqari ko'plab nomlari, xakker, buzg'unchi, g'araz niyatli va h.k. mavjud. Ikki tomon o'rtasida tashkil qilingan aloqa sxemasida hujumchi ham jo'natuvchi ham qabul qiluvchi rolda bo'lishi mumkin.

Bundan tashqari, tomonlar o'rtasida o'rnatilgan aloqa kanali ham kriptografiya muhim ahamiyatga ega. Aloqa kanallariga oid quyidagi tushunchalar mavjud:

- *kanal* – axborotni boshqa tomonga yetkazish vositasi;
- *fizik xavfsiz kanal* yoki *xavfsiz kanal* – hujumchi fizik kira olmaydigan kanal;

- *himoyalangan kanal* – axborot nisbatan qonuniy foydalanish huquqiga ega tomonlardan tashqari tomonlar ham axborotni o'zgartirishi, o'qishi, o'chirishi va kiritishi mumkin bo'lgan kanal;

- *himoyalangan kanal* – hujumchiga axborotni o'zgartirish, o'qish, o'chirish va kiritish imkoniyatini taqdim etmagan kanal.

Kriptotizimni ikki tarkibli algoritm va kalitdan iborat ekanligiga asoslangan holda *Kerkhoff prinsipini* eslatib o'tish lozim. Ushbu prinsipga binoan faqat kalit sir saqlanishi, shifrlash algoritmi esa ochiq bo'lishi lozim. Bu degani, agar niyati buzuq algoritmni bilgan taqdirda ham tizim obro'sizlanmaydi. Kalitni esa almashtirish mumkin. Klod Shennon ushbu prinsipni “Dushman tizimni biladi”, deb ta'riflagan.

Ta'rif 1.3.1. Belgilangan vaqt ichida hujumchi rasshifrovkalash kalitini bilmasdan shifratmdan ochiq matnni tiklay olmasa bunday shifrlash sxemasi *bardoshli* deb aytiladi.

Kriptotizimlarni buzish usullari *kriptotahlil* (cryptoanalysis)ni o'rganish predmeti hisoblanadi. Kriptografiya va kriptotahlil uzviy bog'langanliklari sababli, ularni ko'pincha birgalikda yagona fan – *kriptologiya* (cryptology) (*kryptos* - mahfiy, *logos*- ilm) sifatida qabul qilinadi.

Kriptotizim (cryptosystem) – ochiq matnni, har biri mos algoritm va kalit orqali aniqlanuvchi, shifratnga qaytariluvchan o'zgartirishlar oilasi.

Kriptografik usullar umumiy xususiyatlari bo'yicha ikki turga, *simmetrik* va *ochiq kalitliga* bo'linadi. Ular bilan keyingi bo'limlarda tanishib chiqiladi.

1.4. Simmetrik kalitli shifrlash algoritmlari va xesh funksiyalar

Ushbu bo'limda simmetrik kalitli shifrlash algoritmlari va xesh funksiyalarga oid umumiy ma'lumotlar bilan tanishib chiqiladi.

Ta'rif 1.4.1. Ma'lumotni shifrlash va rasshifrovkalash uchun yagona kalitdan foydalanuvchi shifrlash – *simmetrik kalitli shifrlash* usuli (ba'zi adabiyotlarda *yagona kalitli*, *bir kalitli*, *shaxsiy kalitli shifrlash* deb ham yuritiladi) deb atiladi.

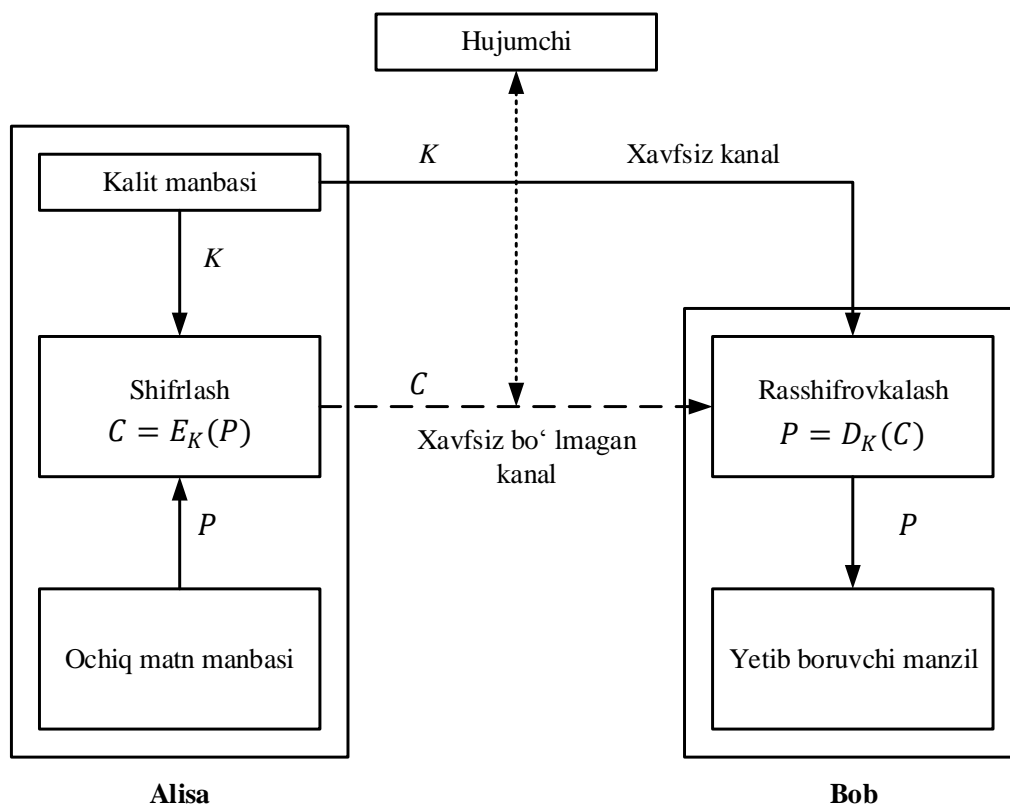
Misol 1.4.1. Faraz qilaylik $A = \{a, b, c, \dots, x, y, z\}$ Ingliz harflaridan iborat alfavit bo'lsin. Kalit K sifatida esa A alfavitni almashtirish (har bir elementini o'ngga siljitish) soni qaralsin va $K = 3$ ga teng bo'lsin. U holda yangi alfavitni $B = \{d, e, f, \dots, a, b, c\}$ ga tengligini bilish oson. Umumiy holda ikki alfavit quyidagiga teng bo'ladi:

| | | | | | | | | | | | | | | | | | | | | | | | | | | | |
|----------|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| A | = | a | b | c | d | e | f | g | h | i | j | k | l | m | n | o | p | q | r | s | t | u | v | w | x | y | z |
| B | = | d | e | f | g | h | i | j | k | l | m | n | o | p | q | r | s | t | u | v | w | x | y | z | a | b | c |

Shifrlash usuli sifatida esa ochiq matn belgilarini A alfavitdan topib, unga mos shifrmavn belgisini B alfavitdan topish qaralgan bo'lsin. Agar ochiq matn $P = "bu\ sodda\ shifrlash\ usuli"$ ga teng bo'lsa, u holda shifrmavn $C = "ex\ vrggd\ vkliuodvk\ xv\ xol"$ ga tengligini bilish oson.

Rasshifrovkalashda shifrmavn belgilari B alfavitdan olinib, unga mos ochiq matn belgilari A alfavitdan olinadi. Keltirilgan misolda kalit sifatida ochiq matn belgilari olingan A alfavitdan mos bo'lgan shifrmavn belgilari olinuvchi B alfavitni hosil qiluvchi o'ngga siljitishlar soni olingan.

Umumiy holda ikki tomon o'rtasida simmetrik kalitli shifrlashdan foydalanib tashkil qilingan aloqa sxemasini quyidagicha tasvirlash mumkin (1.4-rasm). Ko'rish mumkinki, ma'lumotni shifrlash kalitini Bobga yetkazish uchun xavfsiz aloqa kanali talab qilinmoqda. Bu esa, simmetrik kalitli shifrlarda *kalitlarni xavfsiz taqsimlash* muammosi mavjudligini ko'rsatadi.



1.4-rasm. Simmetrik kalitli shifrlashga asoslangan ikki tomon o'rtasidagi aloqa sxemasi

Simmetrik kalitli shifrlash sxemalari ikkita sinfga: *blokli shifrlar* va *oqimli shifrlarga* ajratiladi.

Ta'rif 1.4.2. Blokli shifrlar A alfavitda ochiq matni o'zgarmas t uzunlikdagi qismlarga (*bloklar* deb ataladi) bo'luvchi shifrlash sxemasi bo'lib, bir vaqtning o'zida bitta blokni shifrlaydi.

Blokli shifrlar keng tarqalgan shifrlash sxemalaridan bo'lib, uning *o'rniga qo'yishga asoslangan* va *o'rin almashtirishga asoslangan* ikki muhim sinfi mavjud.

O'rniga qo'yishga asoslangan shifrlarda ochiq matn belgilarining o'rniga boshqa belgilar yoki belgilar guruhini qo'yish bilan shifrmavn hosil qilinadi. Qabul qiluvchi esa rasshifrovkalash uchun teskari o'rniga qo'yishni amalga oshirish bilan haqiqiy matnni tiklaydi.

An'anaviy kriptografiyada o'rniga qo'yish shifrlarining to'rt turi mavjud:

Ta'rif 1.4.3. Sodda o'rniga qo'yishli shifrlash yoki *monoalfavitli shifrlashda* ochiq matndagi har bir belgi shifrmavnndagi mos belgiga almashtiriladi. 1.4.1-misolni sodda o'rniga qo'yish shifriga misol keltirish mumkin.

Ta'rif 1.4.4. Omofonik o'rniga qo'yish shifrlari sodda o'rniga qo'yishli shifrlashga o'xshash bo'lib, ochiq matndagi har bir belgi shifratmada bir nechta belgiga almashtirilishi bilan farq qiladi. Masalan, *A* belgi 5, 13, 25 yoki 56 ga mos bo'lishi yoki *B* belgi 7, 19, 31 yoki 42 ga mos bo'lishi va h.k.

Ta'rif 1.4.5. Poligram o'rniga qo'yish shifrida belgilar bloki guruhlar shaklida shifrlanadi. Masalan, ochiq matndagi “ABA” blokiga “RTQ” yoki “ABB” blokiga “SLL” mos kelishini olish mumkin.

Ta'rif 1.4.6. Polialfavitli o'rniga qo'yish shifri ko'p sonli sodda o'rniga qo'yish shifrlari yordamida quriladi. Masalan, 5 ta turli sodda o'rniga qo'yish shifrlari foydalanilishi mumkin. 3.1-paragrafda keltirilgan Vijiner shifri polialfavitli o'rniga qo'yishga misol bo'ladi.

O'rin almashtirish shifrlari ochiq matn blokidagi belgilarni o'rnini almashtirishga asoslanadi. Boshqacha aytganda, ochiq matndagi belgilarning tarkibi o'zgarmas saqlanib, tartibi o'zgaradi. Bunga ochiq matnni jadvalga ustun bo'yicha yozib, satr bo'yicha o'qib olishni misol keltirish mumkin.

Misol 1.4.2.

Ochiq matn: “sodda_o'rin_almashtirish_funksiyasi”

| | | | |
|----|----|----|---|
| s | i | t | n |
| o | n | i | k |
| d | | r | s |
| d | a | i | i |
| a | l | sh | y |
| | m | | a |
| o' | a | f | s |
| r | sh | u | i |

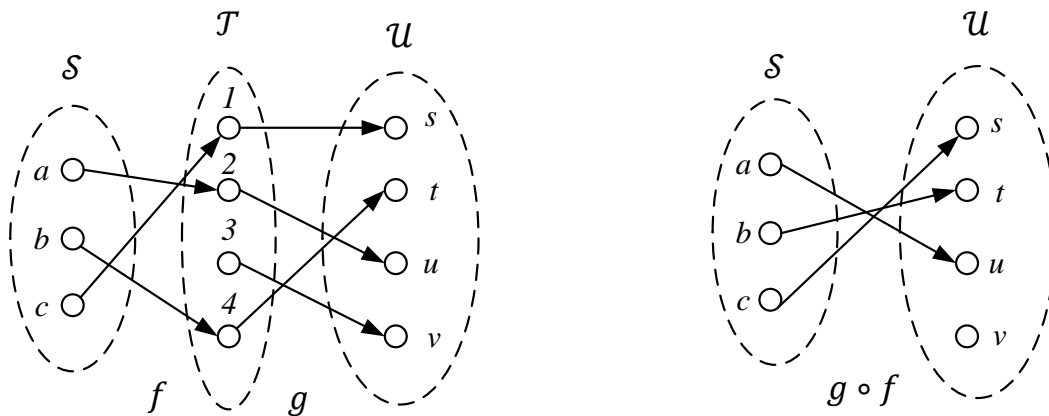
Shifr matn: “sitnonikd_rsdaiialshy_m_ao'afsrshui”.

Hozirda zamonaviy shifrlarni qurishda bir qancha sodda funksiyalarning majmuasidan iborat bo'lgan *funksiyalar birlashmasidan* foydalaniladi.

Ta'rif 1.4.7. Faraz qilaylik \mathcal{S}, \mathcal{T} va \mathcal{U} – chekli to'plamlar hamda $f: \mathcal{S} \rightarrow \mathcal{T}$ va $g: \mathcal{T} \rightarrow \mathcal{U}$ – funksiyalar bo'lsin. f ning g bilan birlashmasi $g \circ f$ (yoki shunchaki fg) kabi belgilanib, funksiya \mathcal{S} dan \mathcal{U} to'plamga

almashtirishni amalga oshiradi (1.5-rasm) va barcha $x \in \mathcal{S}$ uchun $(g \circ f)(x) = g(f(x))$ kabi belgilanadi.

Keltirilgandan xulosa qilgan holda, birlashma funksiyani 2 dan ortiq funksiyalardan ham hosil qilish mumkin. Masalan, f_1, f_2, \dots, f_t funksiyalar uchun birlashma funksiyani $f_t \circ \dots \circ f_2 \circ f_1$ kabi ifodalash mumkin. O‘rin almashtirish va o‘rniga qo‘yish akslantirishlaridan alohida foydalanish bilan yuqori bardoshli shifrlarni qurishning imkoniyati yo‘qligi bois, amalda ularning birlashmasidan keng foydalaniladi.



1.5-rasm. g va f funksiyalarning $g \circ f$ birlashmasi

Simmetrik kalitli shifrlarning yana bir keng tarqalgan ko‘rinishi bu – *oqimli shifrlar*. Tarmoq bo‘ylab uzatiladigan axborot tashqi xalallar tufayli o‘zgarishi kuzatiladigan muhitlarda oqimli shifrlardan keng foydalaniladi.

Ta’rif 1.4.8. Faraz qilaylik \mathcal{K} shifrlash akslantirishlari to‘plami uchun kalit maydoni bo‘lsin. U holda, $e_1 e_2 e_3 \dots e_i \in \mathcal{K}$ belgilar ketma-ketligi *kalit oqimi* deb ataladi.

Ta’rif 1.4.9. Faraz qilaylik \mathcal{A} alfavit q belgidan iborat va $e \in \mathcal{K}$ uchun E_e blok uzunligi birga teng bo‘lgan sodda o‘rniga qo‘yish shifri bo‘lsin. Shuningdek, ochiq matn qatori $m_1 m_2 m_3 \dots$ va \mathcal{K} dan olingan kalit oqimi $e_1 e_2 e_3 \dots$ ga teng bo‘lsin. U holda *oqimli shifr* ochiq matn qatorini qabul qilib, shifrmatn qatori $c_1 c_2 c_3 \dots$ ni $c_i = E_{e_i}(m_i)$ tenglik orqali hosil qilinadi. Agar d_i qiymat e_i ning teskarisi bo‘lsa, u holda ochiq matn $D_{d_i}(c_i) = m_i$ ga ega bo‘linadi.

Oqimli shifrlarda foydalanilgan kalit oqimiga asoslangan holda sodda akslantirishlar qo‘llaniladi. Kalit oqimi tasodifiy tarzda yoki kichik

uzunlikdagi boshlang'ich kalitdan *kalit oqimi generatori* deb nomlanuvchi biror algoritm asosida hosil qilinadi.

Misol 1.4.3. Vernam shifri $\mathcal{A} = \{0,1\}$ alfavit uchun aniqlangan oqimli shifr hisoblanadi. t bit uzunlikdagi binar xabar $m_1m_2m_3 \dots m_t$ uzunligiga teng bo'lgan binar kalit $k_1k_2k_3 \dots k_t$ bilan XOR amalida $c_1c_2c_3 \dots c_t$ shifratni hosil qiladi:

$$c_i = m_i \oplus k_i, 1 \leq i \leq t.$$

Agar kalit qatori tasodifiy tanlansa va takrorlanmasa, Vernam shifri *bir martali tizim* yoki *bir martali bloknot* deb ataladi.

Kalit maydonining o'lchami shifr tizim uchun mavjud bo'lgan shifrlash/rasshifrovkalash kalitlari juftlarining soni bilan xarakterlanadi. Masalan, 1.4.1-misolda keltirilgan sodda o'rniga qo'yish akslantirish uchun kalit maydonining o'lchami $26! \approx 4 \times 10^{26}$ ga teng bo'ladi.

Zamonaviy kriptografiyaning yana bir simmetrik akslantirishlaridan biri – *kriptografik xesh funksiyalar* hisoblanadi.

Ta'rif 1.4.10. Xesh funksiya deb o'zgaruvchan uzunlikdagi binar qatorlarni *xesh qiymat* deb ataluvchi biror o'zgarmas uzunlikdagi qiymatga samarali hisoblashlar orqali aks ettiruvchi bir tomonlama funksiyaga aytiladi.

n bitli xesh qiymatlarni (masalan, $n = 128$ yoki 160) qaytaruvchi va talab etilgan xususiyatlarga ega xesh funksiya uchun tasodifiy kiruvchi satrning ma'lum bir xesh qiymatga bog'lanish ehtimoli 2^{-n} ga teng bo'ladi. Buning uchun, biror h kriptografik xesh funksiyani loyihalashda ikkita turli kirish qiymatlari uchun bir xil xesh qiymatni hosil bo'lishini imkonsizligiga e'tibor qaratiladi (ya'ni, $x \neq y$ kiruvchi qatorlar uchun $h(x) = h(y)$ holat kuzatilmasligi shart).

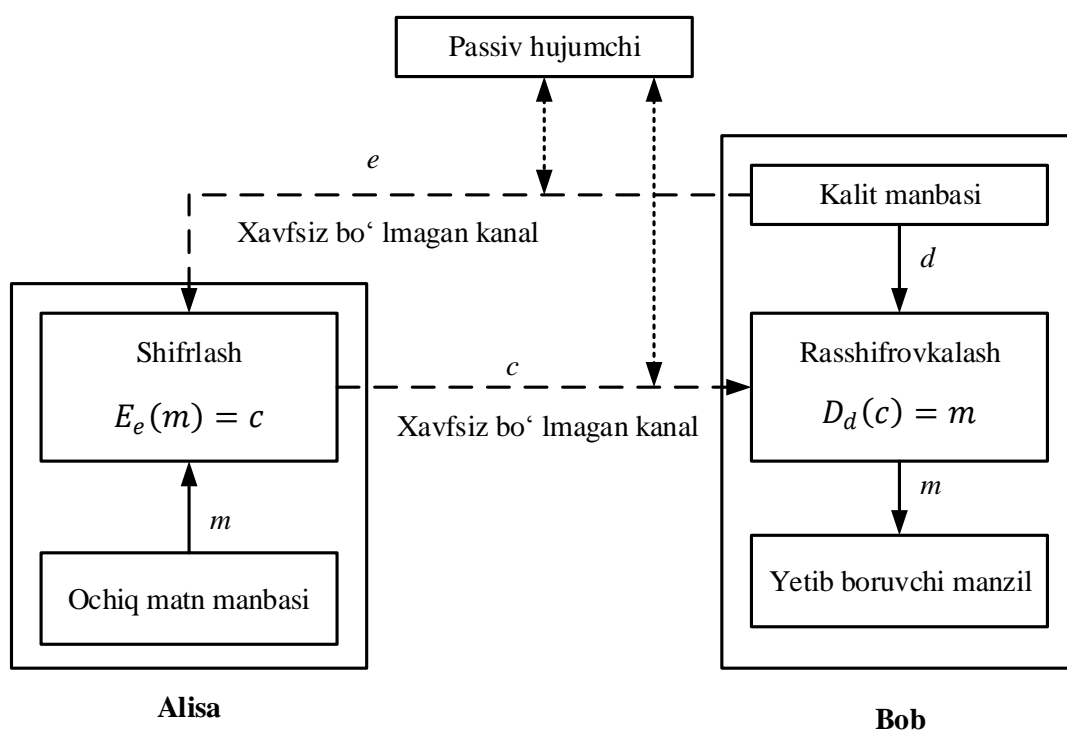
Kriptografik xesh funksiyalar axborot xavfsizligida elektron raqamli imzo algoritmlarini yaratishda va ma'lumotlar yaxlitligini ta'minlashda foydalaniladi.

1.5. Ochiq kalitli kriptografik algoritmlar va elektron raqamli imzo

Kriptografiyada keng qo'llaniluvchi shifrlash usullaridan yana biri *ochiq kalitli* deb (yoki ikki kalitli deb ham ataladi) nomlanib, ma'lumotni shifrlashda va rasshifrovkalashda turli kalitlardan foydalanadi.

Faraz qilaylik, \mathcal{K} kalit maydonida $\{E_e: e \in \mathcal{K}\}$ shifrlash funksiyasi va $\{D_d: d \in \mathcal{K}\}$ unga mos rasshifrovkalash funksiyasi bo'lsin. Shuningdek, barcha shifrlash/rasshifrovkalash funksiyalari jufti (E_e, D_d) uchun berilgan shifrmata $c \in \mathcal{C}$ uchun E_e funksiya yordamida ochiq matn $m \in M$ ni ($E_e(m) = c$ shartni qanoatlantiruvchi) hisoblashning imkoni mavjud bo'lmasin. Bu xususiyat, berilgan shifrlash kaliti e dan foydalanib, rasshifrovkalash kaliti d ni topishning imkonsizligini ko'rsatadi. Bu yerda, E_e – qopqonli bir tomonlama funksiya hisoblanib, uni teskarisini topish uchun faqat d parametr talab etiladi. Shu sababli, ochiq kalitli shifrlash algoritmlari shifrlash va rasshifrovkalash kalitlari bir xil bo'lgan, simmetrik shifrlardan farqlanadi.

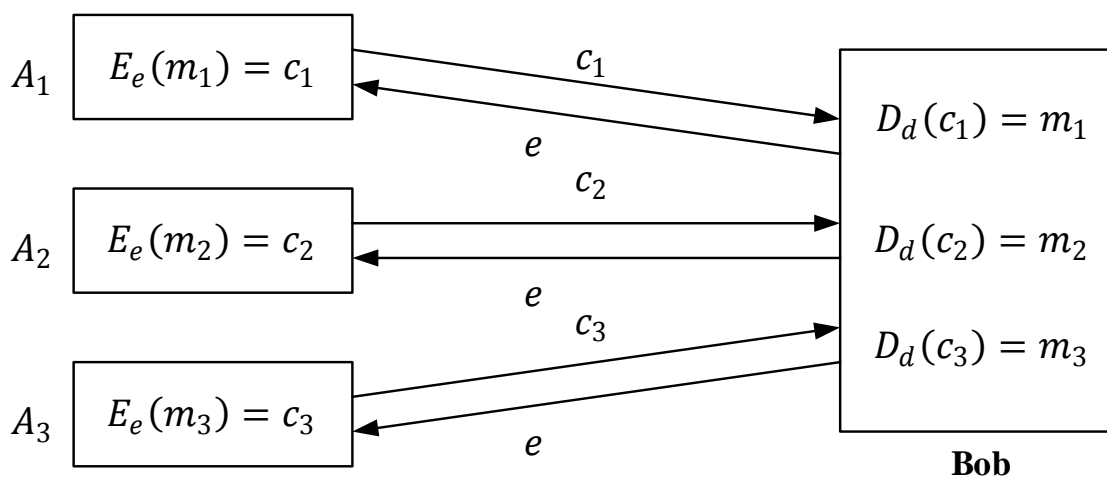
Ochiq kalitli shifrlash algoritmi yordamida hosil qilingan ikki tomon o'rtasidagi aloqa kanalining umumiy ko'rinishi 1.6-rasmda keltirilgan. Bunga ko'ra, Bob (e, d) kalit juftlarini tanlaydi. Shifrlash kaliti e (*ochiq kalit* deb ataladi)ni Alisaga ochiq tarmoq orqali yuboradi va rasshifrovkalash kaliti d (*shaxsiy kalit* deb ataladi)ni o'zida maxfiy saqlaydi. Shundan so'ng, Alisa ochiq matn m ni Bobning ochiq kaliti yordamida shifrlaydi: $c = E_e(m)$ va uni ochiq tarmoq orqali yuboradi. Bob esa qabul qilingan shifrmata c ni d kalit bilan D_d funksiya yordamida rasshifrovkalaydi.



1.6-rasm. Ochiq kalitli shifrlash usuli yordamida shifrlash

Ochiq kalitli shifrlash algoritmlari yordamida shifrlash jarayoni shifrlash kalitini ochiq yuborilishi bilan simmetrik kalitli shifrlardan farq qiladi. Bundan tashqari, ochiq kalitli shifrlash algoritmlari yordamida ma'lumot uzatishda simmetrik kriptotizimlar kabi har bir ma'lumot uzatuvchi va qabul qiluvchi orasida alohida – alohida kalitdan foydalanishni talab etmaydi. Bobning ochiq kaliti e ni bilgan har bir ishtirokchi ma'lumotni shifrlab unga yuborishi mumkin. Shifrlangan ma'lumotni rasshifrovkalash esa faqat d kalitni bilgan Bob uchun joiz bo'ladi. Mazkur holat 1.7-rasmda keltirilgan. Bu yerda A_1 , A_2 va A_3 turli tomonlar bo'lib, Bobning yagona kaliti e bilan m_1 , m_2 va m_3 ma'lumotlarni shifrlashi mumkin bo'ladi. Hosil bo'lgan barcha shifrlarni esa Bob yagona shaxsiy kalit d bilan rasshifrovkalashi mumkin bo'ladi.

Ochiq kalitli shifrlash algoritmlari shifrlash kalitini uzatish uchun xavfsiz kanalni talab etmasligi bilan ajralib tursada, bu amalda to'liq xavfsizlikni ta'minlash uchun yetarli hisoblanmaydi. 1.8-rasmda buzg'unchi tomonidan ochiq kalitli shifrlash algoritmini buzmasdan ma'lumotni qo'lga kiritish jarayoni keltirilgan. Mazkur holat *obro'sizlantirish* deb ataladi.



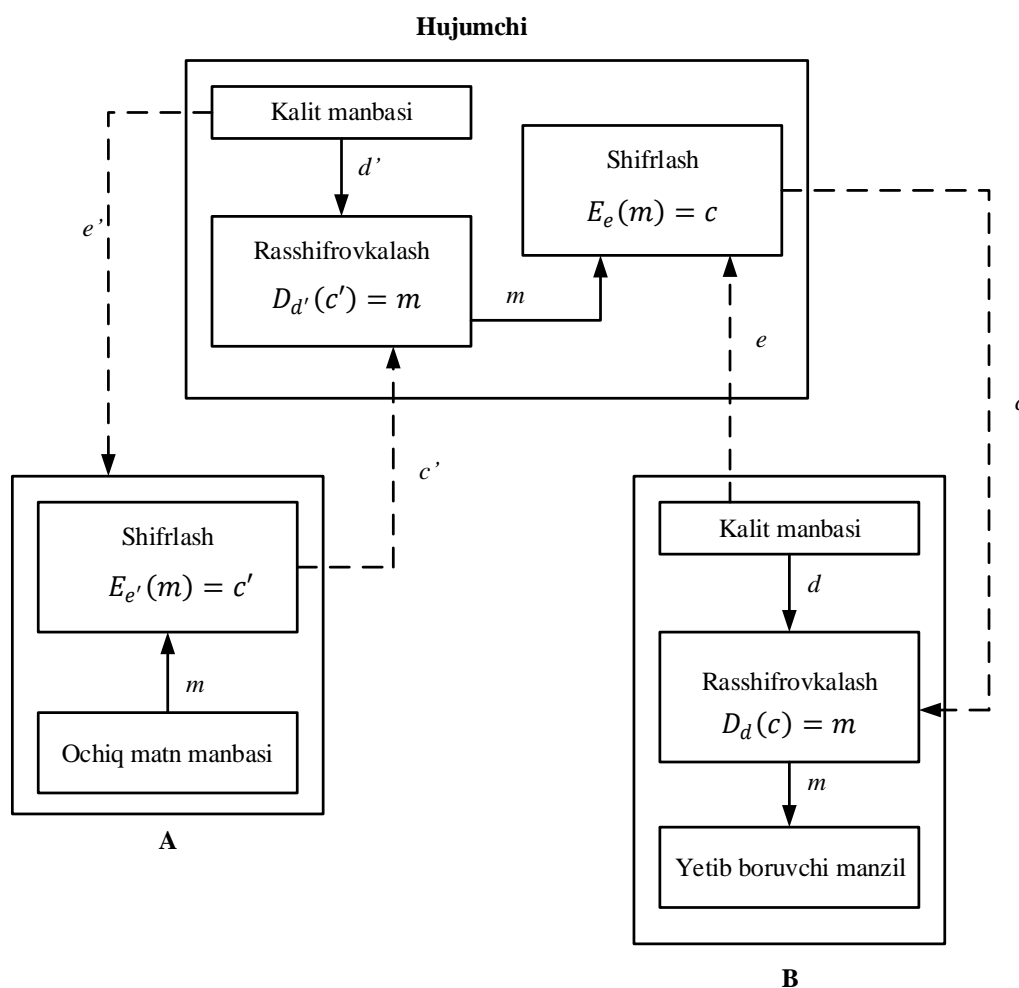
1.7-rasm. Ochiq kalitli shifrlashdan foydalanish sxemasi

Yuqoridagi ssenariyda, obro'sizlantirish holati hujumchi e' kalitni B tomonning ochiq kaliti deb A tomonni ishontirishi natijasida yuzaga kelmoqda. Bunda, hujumchi A dan B tomon uzatilgan shifrlarni o'zining d' shaxsiy kaliti bilan rasshifrovkalaydi hamda B tomonning ochiq kaliti e bilan qayta shifrlab unga yuboradi. Mazkur holda muammo A tomon ochiq kalitni B tomonga tegishli ekanligini tekshira olmasligi natijasida yuzaga kelmoqda.

Amalda ochiq kalitli shifrlash algoritmlaridan elektron raqamli imzo deb ataluvchi tizimni qurish uchun foydalaniladi. Elektron raqamli imzo algoritmlari ochiq kalitli kriptotizimlarning bir turi hisoblanadi. Faraz qilaylik, E_e ochiq matn maydoni \mathcal{M} dan shifrmtn maydoni \mathcal{C} ga akslantiruvchi shifrlash funksiyasi va bunda $\mathcal{M} = \mathcal{C}$ bo'lsin. Agar E_e ga mos bo'lgan rasshifrovkalash funksiyasi D_d bo'lsa, u holda E_e va D_d lar uchun o'rin almashtirish mumkin:

$$\text{barcha } m \in \mathcal{M} \text{ lar uchun, } D_d(E_e(m)) = E_e(D_d(m)) = m.$$

Ochiq kalitli shifrlashning mazkur ko'rinishi *qaytariladigan* deb ataladi. Bunda, faqat $m \in \mathcal{M}$ holat uchun $\mathcal{M} = \mathcal{C}$ o'rinli bo'lishini inobatga olish kerak. Qolgan holatlarda esa ($m \notin \mathcal{C}$), $D_d(m)$ akslantirish ma'noga ega bo'lmaydi.

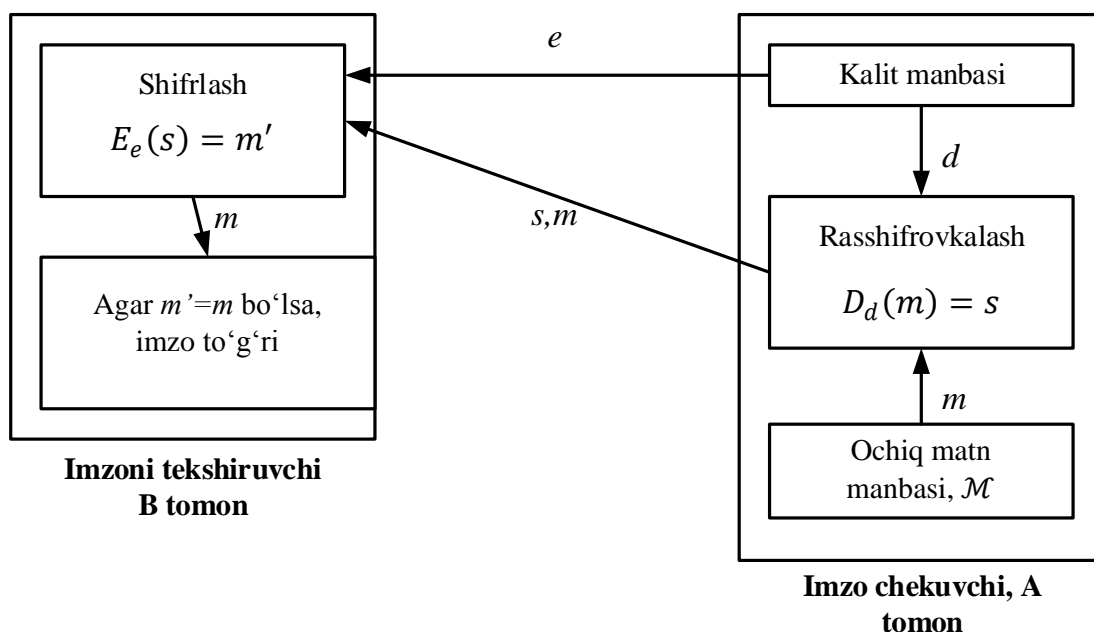


1.8-rasm. Ikki tomon orasidagi aloqaning obro'sizlantirilishi

Elektron raqamli imzo tizimlarini qurish quyidagi tartibda amalga oshiriladi (1.9-rasm):

1. Faraz qilaylik imzolash sxemasi uchun \mathcal{M} ochiq matn maydoni bo'lsin.
2. Faraz qilaylik imzo maydoni \mathcal{S} uchun $\mathcal{M} = \mathcal{C}$ o'rinli bo'lsin.
3. Faraz qilaylik (e, d) – ochiq kalitli shifrlash sxemasi uchun kalit jufti bo'lsin.
4. Imzolash funksiyasi S_A ni D_d ga teng deb olsak, u holda $m \in \mathcal{M}$ xabarlar uchun imzo $s = D_d(m)$ ga teng bo'ladi.
5. Imzoni tekshirish funksiyasi V_A esa quyidagiga teng bo'ladi:

$$V_A(m, s) = \begin{cases} true, & \text{agar } E_e(s) = m \\ false, & \text{qolgan hollarda.} \end{cases}$$



1.9-rasm. Elektron raqamli imzoning soddaxemasi

Simmetrik kalitli kriptotizimlar kabi ochiq kalitli shifrlash orqali ma'lumotni konfidensialligini ta'minlash amalga oshiriladi. Biroq, elektron raqamli imzo tizimlari ma'lumotni yaxlitligini va rad etishdan himoyasini ta'minlashni maqsad qiladi.

Yuqorida ko'rib o'tilgan simmetrik va ochiq kalitli kriptotizimlar o'ziga xos qator afzallik va kamchiliklarga ega. Xususan, ularga quyidagilarni keltirish mumkin (1.2-jadval).

Simmetrik va ochiq kalitli kriptotizimlarning afzalliklari va kamchiliklari

| Xususiyat Kriptotizim | Afzallik | Kamchilik |
|-------------------------------------|---|--|
| Simmetrik kriptotizimlar | 1. Simmetrik kalitli shifrlar ma'lumotni shifrlashda yuqori tezkorlik taqdim etadi. 2. Simmetrik kriptotizim kalitining uzunligi nisbatan qisqa. | 1. Simmetrik kriptotizimdan foydalanish uchun ikki tomonda ham yagona kalit bo'lishi shart. 2. Simmetrik kalitlardan foydalanish davri kam. |
| Ochiq kalitli kriptotizimlar | 1. Faqat shaxsiy kalitni maxfiy saqlash talab etiladi. 2. Shaxsiy va ochiq kalitlar juftida yetarlicha uzoq vaqt foydalanish mumkin. | 1. Ochiq kalitli shifrlar ma'lumotlarni shifrlashda past tezkorlik qayd etadi. 2. Ochiq kalitli kriptotizimlarda kalit uzunligi nisbatan katta. |

1.6. Kriptografik protokollar va kalitlarni boshqarish

Bir nechta kriptografik algoritmlar yagona maqsad yo'lida *kriptografik protokol* sifatida birlashtiriladi. Shifrlash algoritmlari, elektron raqamli imzo va tasodifiy sonlar generatori kriptografik protokolni qurishda ishlatilishi mumkin.

Ta'rif 1.6.1. Kriptografik protokol – aniq xavfsizlik maqsadiga erishish uchun ikki yoki undan ortiq subyektlardan talab qilinadigan harakatlarni izchil ko'rsatib beradigan bosqichlar ketma-ketligi bilan taqsimlangan algoritm.

Kriptografik protokoldan farqli o'laroq mexanizm tushunchasi ham mavjud. *Mexanizm* – muayyan xavfsizlik maqsadlariga erishish uchun protokollarni, algoritmlarni va kriptografik bo'lmagan usullarni o'z ichiga olgan umumiy atama.

Misol 1.6.1. (Sodda kalit almashinish protokoli). Alisa va Bob xavfsiz bo'lmagan kanal orqali aloqa o'rnatish uchun simmetrik shifrlash tizimini tanladilar. Bu o'rinda, ma'lumotni shifrlash uchun ularga kalit

zarur bo‘ladi. Mazkur holda tomonlar o‘rtasida aloqa o‘rnatish protokoli quyidagicha bo‘ladi:

1. Bob ochiq kalitni shifrlash algoritmini tanlaydi va o‘zining ochiq kalitini kanal orqali Alisaga yuboradi.

2. Alisa ma’lumotlarni shifrlash uchun simmetrik kriptotizim kalitini generatsiya qiladi.

3. Alisa simmetrik kriptotizim kalitini Bobning ochiq kaliti bilan shifrlagan holda uni Bobga yuboradi.

4. Bob o‘zining shaxsiy kaliti yordamida simmetrik kriptotizim kalitini qayta tiklaydi.

5. Shundan so‘ng, Alisa va Bob umumiy simmetrik kalitga va uning yordamida ma’lumotlarni shifrlab uzatish imkoniyatiga ega bo‘ladilar.

Mazkur protokolning maqsadi xavfsiz bo‘lmagan tarmoqda xavfsiz aloqani qurish hisoblanadi va buning uchun ochiq kalitli va simmetrik shifrlash tizimlaridan foydalanilgan.

Amalda kriptografik funksiyalar alohida-alohida tarzda emas, balki kriptografik protokol sifatida keng qo‘llaniladi. Bu esa qurilayotgan kriptografik protokolning xavfsizligi nafaqat unda foydalanilgan algoritmlarga, shuningdek, ularning birgalikda qanday loyihalanganligiga ham bog‘liq bo‘ladi.

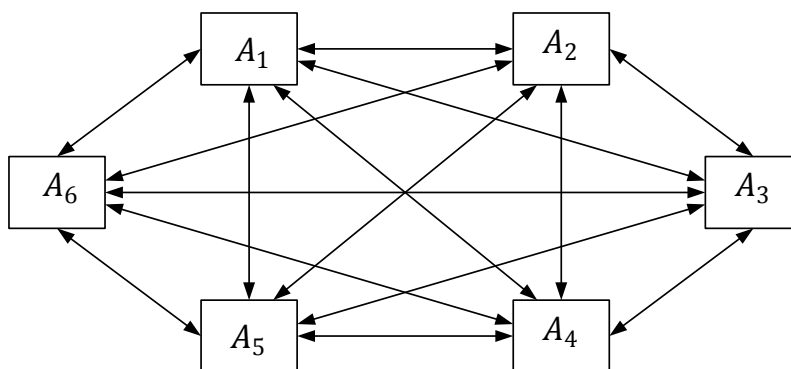
Yuqorida simmetrik, ochiq kalitli va elektron raqamli imzo kabi kriptotizimlar bilan tanishib o‘tildi. Xususan, ularning har biri uchun kalitlarni generatsiyalash jarayoni mavjudligini ko‘rishimiz mumkin. Kriptografik kalitlarni generatsiyalash va kalitni o‘rnatish kabi vazifalar bilan kriptografiyaning *kalitlarni boshqarish* deb nomlangan bo‘limi shug‘ullanadi.

Ta’rif 1.6.2. Kalitni o‘rnatish – ikki yoki undan ortiq tomonlarga keyingi kriptografik algoritmlar foydalanishi uchun kerak bo‘lgan kalitni taqsimlash jarayoni.

Ta’rif 1.6.3. Kalitni boshqarish – kalitlarni o‘rnatishni madadlovchi, tomonlar o‘rtasida doimiy aloqani saqlab turuvchi hamda kalitlar eskirganda ularni yangilovchi jarayon va mexanizmlarning to‘plami.

Kalitlarni o‘rnatish jarayoni o‘zida *kalitlarni kelishish* va *kalitlarni uzatish* qism jarayonlarini mujassamlashtirgan. Kalitlarni o‘rnatish jarayoni ko‘plab protokollar tomonidan amalga oshirilgan.

Kalitlarni o‘rnatish simmetrik kriptotizimlar uchun jiddiy muammolardan hisoblanadi. Xususan, 6 ta ishtirokchi o‘rtasida kalitni o‘rnatish holatining ko‘rinishi 1.10-rasmda keltirilgan.



1.10-rasm. Olti tomon o‘rtasidagi kalitlarning bog‘lanishi

Ma’lumot almashmoqchi bo‘lgan har bir tomon o‘rtasida alohida-alohida simmetrik kalitlar talab qilingani bois, tomonlar o‘rtasidagi jami simmetrik kalitlar soni $\binom{n}{2} = \frac{n(n-1)}{2}$ tenglik bilan aniqlanadi. Bu yerda, n – tomonlar soni bo‘lib, 6 ta tomon uchun umumiy simmetrik kalitlar soni 15 ga teng bo‘ladi.

Kalitlarni boshqarishning yana bir asosiy jarayoni – *kalitlarni generatsiyalash* hisoblanadi. Masalan, shifrlash jarayoni uchun hujumchi noma’lum bo‘lgan va uni bashorat qilish ehtimoli kam bo‘lgan tasodifiy kalitlarni generatsiyalash talab etiladi. Tasodifiy kalitlarni generatsiyalash tasodifiy sonlarni yoki bitlar ketma-ketligini tanlashdan iborat bo‘lib, amalga oshirishda yetarlicha murakkabliklarni taqdim etadi.

Misol 1.6.1. 0 va 1 lardan iborat bo‘lgan tasodifiy ketma-ketlikni generatsiyalash uchun tangani to‘g‘ri tushgan holatini 1 deb, teskari holatini esa 0 deb olish mumkin. Agar tanga xolis deb hisoblanilsa, u holda tangani to‘g‘ri tushish ehtimoli $\frac{1}{2}$ ga teng bo‘ladi. Bu holat tangani qanday yasalganiga va tangani tashlash qanday amalga oshirilganiga bog‘liq bo‘ladi. Mazkur usul katta uzunlikdagi tasodifiy bitlar ketma-ketligini talab qiluvchi muhit uchun o‘rinli hisoblanmaydi. Ushbu misol tasodifiylikka misol bo‘la olsada, amaliy tomondan ahamiyatga ega hisoblanmaydi.

Tasodifiy ketma-ketliklarning haqiqiy manbasi fizik jihozlar bo‘lgani bois, amalda ulardan foydalanish yuqori narx talab etishi yoki jarayon sekin amalga oshirilishi mumkin. Ushbu muammoni yechishda, amalda dastlabki kichik uzunlikdagi qiymatdan (*seed* deb nomlanadi) hisoblash asosida *pseudotasodifiy ketma-ketliklarni* generatsiyalash usulidan foydalaniladi. Agar pseudotasodifiy ketma-ketliklarni generatsiyalash usuli noma’lum bo‘lganda, u to‘liq tasodifiy ketma-

ketliklarni generatsiyalashga imkon beradi. Biroq, kriptografik algoritmlarni yaratishda *Kerkgoff prinsiga* asoslanilgani bois, amalda bardoshli psevdotasodifiy ketma-ketliklarni generatsiyalash usullarini yaratish murakkab masalalardan hisoblanadi.

1.7. Kriptografik algoritmlarga qaratilgan hujumlar

Yuqorida simmetrik va ochiq kalitli kriptografik tizimlardan foydalanish sxemalarida hujumchi yoki passiv hujumchi atamalari keltirildi. Bundan tashqari, deshifrlash tushunchasi haqida ma'lumotlar keltirildi. Ushbu tushunchalar kriptotahlil deb nomlanuvchi fan sohasiga tegishli bo'lib, ushbu bo'limda ularga qisqacha to'xtalib o'tiladi.

Ta'rif 1.7.1. Kriptoanaliz – qanday ishlashini tushunish, ularni buzish yoki obro'sizlantirish usullarini topish hamda takomillashtirish maqsadida shifratn, shifrlash algoritmi yoki kriptotizimni o'rganish jarayoni.

Odatda kriptoanalizda asosiy maqsad sifatida shifrlash kalitini topish qaraladi. Hujumchilarning darajasiga ko'ra kriptografik hujumlar quyidagi turlarga ajratiladi:

1. *Passiv hujumda* hujumchiga faqat aloqa kanalini kuzatish imkoniyati beriladi va u asosan ma'lumotning konfidensialligini buzishga qaratiladi.

2. *Aktiv hujumda* hujumchi kanal orqali uzatilgan ma'lumotlarni o'chirishi, modifikatsiyalashi yoki almashtirishning boshqa usullaridan foydalanishi mumkin bo'ladi. Aktiv hujum ma'lumot yaxlitligi, konfidensialini va autentifikatsiyasini buzishga qaratilgan bo'ladi.

Shifrlash sxemalari uchun shifratndan ochiq matnni olishni yoki shifrlash kalitini topishni maqsad qilgan quyidagi hujum usullari mavjud:

1. *Faqat shifratnga asoslangan hujum* faqat bir yoki bir nechta shifratnlar asosida ochiq matnni yoki shifrlash kalitini topishni maqsad qiladi. Ushbu hujumga bardoshsiz bo'lgan shifrlash algoritmi to'liq xavfsiz emas deb qaraladi.

2. *Ma'lum ochiq matnlarga asoslangan hujum* ma'lum sondagi ochiq matnlar va ularga mos bo'lgan shifratnlar asosida shifrlash kalitini topishni maqsad qiladi. Biroq, ko'p sonli ochiq matn va shifratn juftliklari kerak bo'lgani bois, ushbu hujumni amalga oshirish murakkab vazifa hisoblanadi.

3. *Tanlangan ochiq matnga asoslangan hujum* buzg'unchi tomonidan tanlangan ochiq matn va unga mos shifratn berilganda

shifrlash kalitini topishni maqsad qiladi. Shundan so‘ng, berilgan shifratmlar uchun ochiq matnni topish imkoniyati tug‘iladi.

4. *Adaptiv tanlangan ochiq matnga asoslangan hujum* ham tanlangan ochiq matnga asoslangan hujum kabi bo‘lib, ochiq matnni tanlanishi oldingi shifratmga bog‘liq bo‘lishi bilan farqlanadi.

5. *Tanlangan shifratmga asoslangan hujum* hujumchi tomonidan tanlangan shifratmga mos bo‘lgan ochiq matn berilishi bilan xarakterlanadi.

6. *Adaptiv tanlangan shifratmga asoslangan hujum* ham tanlangan shifratmga asoslangan hujum kabi bo‘lib, shifratmni tanlanishi oldingi ochiqmatnga bog‘liq bo‘lishi bilan farqlanadi.

Kriptografik algoritmlardan protokol ko‘rinishida foydalanilgani bois, protokollarga qaratilgan hujumlarning ayrimlari quyida keltirilgan:

1. *Ma‘lum kalit bo‘yicha hujum*. Ushbu hujumda hujumchi oldin foydalanilgan kalitlar haqidagi ma‘lumot asosida yangi kalitlarni hisoblaydi.

2. *Takrorlash hujumi*. Ushbu hujumda hujumchi o‘rnatilgan aloqa seansini to‘liq ko‘chirib oladi va keyinchalik uni to‘liqligicha yoki qisman takrorlaydi.

3. *Obro‘sizlantirish hujumi*. Ushbu hujumda hujumchi tarmoqdagi qonuniy tomonlarning biri nomidan amallarni bajaradi.

4. *Lug‘atga asoslangan hujum*. Ushbu hujum parolga qaratilgan bo‘lib, bunda parollar faylida saqlangan parollarning xesh qiymatlariga mos haqiqiy parolni topishda keng tarqalgan parollar lug‘atidan foydalanadi. Keng tarqalgan parollar lug‘ati Internet tarmog‘idagi ko‘p sonli foydalanuvchilar tomonidan foydalanilgan eng ommabob parollardan tashkil topgan.

Nazorat savollari

1. Axborot xavfsizligi va uning asosiy tushunchalari.
2. Kriptografik funksiyalar va ularning turlari.
3. Kriptografiyaning asosiy tushunchalari.
4. Simmetrik kalitli shifrlash algoritmlari va xesh funksiyalarga oid asosiy tushunchalar.
5. Ochiq kalitli kriptotizimlar va ularning vazifalari.
6. Zamonaviy kriptografiyaning bo‘limlari.
7. Simmetrik kalitli shifrlarda foydalanilgan akslantirishlar.
8. Kriptografik protokol va uning vazifasi.

9. Kriptografik kalitlarni boshqarish bo‘limi va unga oid asosiy muolajalar.
10. Kriptografik algoritmlarga qaratilgan hujum turlari.
11. Kriptotahlil fan sohasi va uning maqsadi.
12. Axborotni himoyalashda kriptografiyaning o‘rnini asoslang.
13. Bir tomonlama funksiya va uning xususiyatlari.

2 BOB. KRIPTOGRAFIYANING MATEMATIK ASOSI

Ushbu bo‘lim kriptografiyaning matematik asosiga bag‘ishlanadi. Shu sababli ularni boshlashdan oldin umumiy standart ko‘rinishdagi belgilanishlarni keltirish maqsadga muvofiq:

- \mathbb{Z} – butun sonlar to‘plamini ifodalaydi: $\{\dots, -2, -1, 0, 1, 2, \dots\}$.
- \mathbb{Q} – ratsional sonlar to‘plamini ifodalaydi: $\left(\frac{a}{b} \mid a, b \in \mathbb{Z}, b \neq 0\right)$.
- \mathbb{R} – real sonlar to‘plamini ifodalaydi.
- π – matematik o‘zgarmas, $\pi \approx 3.14159$.
- e – natural logarifm asosi, $e \approx 2.71828$.
- $[a, b]$ – belgilanish $a \leq x \leq b$ shartni qanoatlantiruvchi x butun sonni ifodalaydi;
- $\lfloor x \rfloor$ – belgilanish x ga teng yoki undan kichik eng katta butun sonni ko‘rsatadi. Masalan, $\lfloor 5.2 \rfloor = 5$ va $\lfloor -5.2 \rfloor = -6$.
- $\lceil x \rceil$ – belgilanish x ga teng yoki undan katta eng kichik butun sonni ko‘rsatadi. Masalan, $\lceil 5.2 \rceil = 6$ va $\lceil -5.2 \rceil = -5$.
- $\{x\}$ – belgilanish x ning butun qismini ko‘rsatadi. Masalan, $\{5.2\} = 0.2$, va $\{5.8\} = 0.8$.
- Agar A chekli to‘plam bo‘lsa, A dagi elementlar soni $|A|$ bilan belgilanadi.
- $a \in A$ – element a ning to‘plam A ga tegishligini anglatadi.
- $A \subseteq B$ – to‘plam A to‘plam B ning qism to‘plami ekanligini anglatadi.
- $A \subset B$ – to‘plam A to‘plam B ning mos qism to‘plami, ya’ni: $A \subseteq B$ va $A \neq B$.
- A va B to‘plamlarning *kesishmasi* bo‘lgan to‘plam $A \cap B = \{x \mid x \in A \text{ va } x \in B\}$ bilan belgilanadi.
- A va B to‘plamlarning *birlashmasi* bo‘lgan to‘plam $A \cup B = \{x \mid x \in A \text{ yoki } x \in B\}$ bilan belgilanadi.
- A va B to‘plamlarning *farqi* bo‘lgan to‘plam $A - B = \{x \mid x \in A \text{ va } x \notin B\}$ bilan belgilanadi.
- A va B to‘plamlarning Dekart ko‘paytmasi $A \times B = \{(a, b) \mid a \in A \text{ va } b \in B\}$ bilan belgilanadi. Masalan, $\{a_1, a_2\} \times \{b_1, b_2, b_3\} = \{(a_1, b_1), (a_1, b_2), (a_1, b_3), (a_2, b_1), (a_2, b_2), (a_2, b_3)\}$.
- *Funksiya* yoki *akslantirish* $f: A \rightarrow B$ – A to‘plamning har bir a elementini B to‘plamning aniq bir b elementiga o‘zlashtiruvchi qoida. Agar $a \in A$ element $b \in B$ elementga akslantirilsa, b element a elementning *aksi*, a element esa b elementning *asli* deb ataladi va

$f(a) = b$ shaklida ifodalanadi. A to'plam f funksiyaning *aniqlanish sohasi*, B to'plam esa f funksiyaning *qiymatlar sohasi* deb ataladi.

- Agar B to'plamdagi har bir element A to'plamda ko'pi bilan bir elementning aksi bo'lsa, $f: A \rightarrow B$ funksiya *birga-bir (1-1 yoki injektiv)* funksiya deb aytiladi. Shuning uchun $f(a_1) = f(a_2)$ deyilganda $a_1 = a_2$ nazarda tutiladi.

- Agar har bir $b \in B$ kamida bitta $a \in A$ ning aksi bo'lsa, u holda $f: A \rightarrow B$ - *ustiga (yoki surjektiv)* funksiya deyiladi.

- Agar $f: A \rightarrow B$ funksiya ham birga-bir ham ustiga funksiya bo'lsa, u holda *bijektiv* funksiya funksiya deb ataladi. Agar f funksiya A va B to'plamlar orasida bijektiv bo'lsa, u holda $|A| = |B|$ tenglik o'rinli. Agar f funksiya A va B o'zining o'rtasida bijektiv bo'lsa, f funksiya A to'plamda *o'rin almashtirish funksiyasi* deb aytiladi.

- $\ln x$ - x ning natural logarifmi, ya'ni, e asosga ko'ra x ning logarifmi.

- $\lg x$ - 2 asosga ko'ra x ning logarifmi.

- $\exp(x) = e^x$ eksponent funksiya.

- $\sum_{i=1}^n a_i$ ifoda $a_1 + a_2 + \dots + a_n$ yig'indini ifodalaydi.

- $\prod_{i=1}^n a_i$ ifoda $a_1 \cdot a_2 \cdot \dots \cdot a_n$ ko'paytmanni ifodalaydi.

- Musbat n soni uchun $n! = n(n-1)(n-2) \dots 1$ - faktorial funksiyasini ifodalaydi. Shartli holatda, $0! = 1$ ga teng.

2.1. Ehtimollar nazariyasi asoslari

Ta'rif 2.1.1. Tajriba – bu ma'lum natijalar to'plamidan birini beruvchi protsedura bo'lib, mumkin bo'lgan individual natijalar *oddiy hodisalar* deb ataladi. Barcha mumkin bo'lgan natijalar to'plami esa *na'munalar maydoni* deb ataladi.

Mazkur bo'limda faqat chekli sondagi natijalarga ega bo'lgan – *diskret* na'munalar maydoni ko'rib chiqiladi. Faraz qilaylik, S na'munalar maydonidagi oddiy hodisalar s_1, s_2, \dots, s_n kabi belgilansin.

Ta'rif 2.1.2. S maydonda P ehtimollik taqsimoti – manfiy bo'lmagan va yig'indisi 1 ga teng bo'lgan p_1, p_2, \dots, p_n sonlar ketma – ketligi bo'lib, p_i kattalik tajriba natijasini s_i hodisa bo'lish ehtimolini ko'rsatadi.

Ta'rif 2.1.3. Hodisa E na'munalar maydoni S ning qism to'plami bo'lsin. E hodisaning paydo bo'lish ehtimoli – $P(E)$ kabi belgilanib, E hodisaga tegishli bo'lgan barcha s_i sodda hodisalarning p_i

ehtimolliklarining yig'indisi hisoblanadi. Agar $s_i \in S$ bo'lsa, $P(\{s_i\})$ ehtimollikni $P(s_i)$ kabi belgilash mumkin.

Ta'rif 2.1.4. Agar E hodisa bo'lsa, unga *teskari hodisa* \bar{E} kabi belgilanadi va E ga tegishli bo'lmagan sodda hodisalar to'plamini ifodalaydi.

Faraz qilaylik, $E \subseteq S$ hodisa bo'lsin.

I. $0 \leq P(E) \leq 1$. Bundan tashqari, $P(S) = 1$ va $P(\emptyset) = 0$ (bu yerda, \emptyset - bo'sh to'plam).

II. $P(\bar{E}) = 1 - P(E)$.

III. Agar S maydondagi natijalar teng darajada bo'lsa, u holda $P(E) = \frac{|E|}{|S|}$ o'rinli.

Ta'rif 2.1.5. Agar $P(E_1 \cap E_2) = 0$ o'rinli bo'lsa, u holda ikki E_1 va E_2 hodisalar bir-birini inkor etuvchi deb ataladi. Ya'ni, ikkita hodisadan birining sodir bo'lishi, boshqasining sodir bo'lish ehtimolini inkor qiladi.

Faraz qilaylik, E_1 va E_2 ikki turli hodisa bo'lsin. U holda quyidagilar o'rinli:

I. Agar $E_1 \subseteq E_2$ bo'lsa, u holda $P(E_1) \leq P(E_2)$ o'rinli bo'ladi.

II. $P(E_1 \cup E_2) + P(E_1 \cap E_2) = P(E_1) + P(E_2)$. Shu sababli, agar E_1 va E_2 lar bir-birini inkor etuvchi bo'lsa, u holda $P(E_1 \cup E_2) = P(E_1) + P(E_2)$ o'rinli bo'ladi.

Shartli ehtimollik

Ta'rif 2.1.6. Faraz qilaylik, E_1 va E_2 lar $P(E_2) > 0$ ehtimolikka ega bo'lgan ikki turli hodisa bo'lsin. Berilgan E_2 hodisa paydo bo'lganda E_1 hodisaning paydo bo'lishining *shartli ehtimoli* $P(E_1|E_2)$ kabi belgilanadi va u quyidagiga teng:

$$P(E_1|E_2) = \frac{P(E_1 \cap E_2)}{P(E_2)}$$

Ta'rif 2.1.7. Agar $P(E_1 \cap E_2) = P(E_1)P(E_2)$ bo'lsa, E_1 va E_2 hodisalar *mustaqil* deb aytiladi.

Yuqoridagi ta'rifdan kelib chiqib, agar E_1 va E_2 hodisalar mustaqil bo'lsa, u holda $P(E_1|E_2) = P(E_1)$ va $P(E_2|E_1) = P(E_2)$ o'rinli bo'ladi.

Bayes teoremasi. Agar E_1 va E_2 lar $P(E_2) > 0$ ehtimolikka ega ikki turli hodisa bo'lsa, u holda quyidagi tenglik o'rinli:

$$P(E_1|E_2) = \frac{P(E_1)P(E_2|E_1)}{P(E_2)}$$

Binomial taqsimot

Binomial koefitsient xususiyatlari. Faraz qilaylik, n va k manfiy bo‘lmagan butun sonlar bo‘lsin. U holda quyidagilar o‘rinli bo‘ladi:

- I. $\binom{n}{k} = \frac{n!}{k!(n-k)!}$.
- II. $\binom{n}{k} = \binom{n}{n-k}$.
- III. $\binom{n+1}{k+1} = \binom{n}{k} + \binom{n}{k+1}$.

Tug‘ilgan kun muammosi

Musbat m , n ($m \geq n$) butun sonlar uchun, $m^{(n)}$ butun son quyidagicha hisoblanadi:

$$m^{(n)} = m(m-1)(m-2) \cdots (m-n+1).$$

m , n ($m \geq n$) manfiy bo‘lmagan butun sonlar bo‘lsin. *Ikkinchi turdagi Stirling raqami* - $\left\{ \begin{matrix} m \\ n \end{matrix} \right\}$ kabi belgilanib, quyidagiga teng:

$$\left\{ \begin{matrix} m \\ n \end{matrix} \right\} = \frac{1}{n!} \sum_{k=0}^n (-1)^{n-k} \binom{n}{k} k^m,$$

Bu yerda, $\left\{ \begin{matrix} 0 \\ 0 \end{matrix} \right\} = 1$ holat bundan mustasno.

$\left\{ \begin{matrix} m \\ n \end{matrix} \right\}$ belgilanish m obyektlar to‘plamini n bo‘sh bo‘lmagan qismto‘plamlarga bo‘lish yo‘llari sonini ifodalaydi.

Klassik bandlik muammosi. Ko‘zda 1 dan m gacha raqamlangan m ta sharcha mavjud. Faraz qilaylik, ko‘zadan aralashtirish yo‘li bilan birin-ketin n ta sharcha tortib olindi va ularning raqamlari qayd etildi. Bu holda, turli t sharning tanlanish ehtimoli quyidagiga teng:

$$P_1(m, n, t) = \left\{ \begin{matrix} n \\ t \end{matrix} \right\} \frac{m^{(t)}}{m^n}, \quad 1 \leq t \leq n.$$

Tug‘ilgan kun muammosi ham klassik muammoning bir xususiy holati hisoblanadi.

Tug‘ilgan kun muammosi. Ko‘zada 1 dan m gacha raqamlangan m ta sharcha mavjud. Faraz qilaylik, ko‘zadan birin-ketin aralashtirish yo‘li bilan n ta sharcha tortib olindi va ularning raqamlari qayd etildi.

I. Tanlashdagi kamida bir marta takrorlanish ehtimoli (ya’ni, kamida ikkita sharcha tanlanganda) quyidagiga teng:

$$P_2(m, n) = 1 - P_1(m, n, n) = 1 - \frac{m^{(n)}}{m^n}, \quad 1 \leq n \leq m. \quad (2.1)$$

Agar $n = O(\sqrt{m})$ (2.3-bo‘limga qarang) va $m \rightarrow \infty$, u holda:

$$P_2(m, n) \rightarrow 1 - \exp\left(-\frac{n(n-1)}{2m} + O\left(\frac{1}{\sqrt{m}}\right)\right) \approx 1 - \exp\left(-\frac{n^2}{2m}\right)$$

II. $m \rightarrow \infty$ ni inobatga olib, bir xil sharcha takrorlanishidan oldingi kutiladigan tanlashlar soni $\sqrt{\frac{\pi m}{2}}$ ga teng bo‘ladi.

Yuqoridagi holatni nima uchun *tug‘ilgan kun muammosi* deb atalishiga qisqacha izoh bersak. 23 kishilik xonada kamida 2 kishining tug‘ilgan kuni bir xil bo‘lish ehtimoli $P_2(365, 23) \approx 0.507$ ga teng bo‘lib, u yetarlicha katta hisoblanadi. Bundan tashqari, $P_2(365, n)$ miqdor n ning ortishi bilan tez ko‘payadi; masalan, $P_2(365, 30) \approx 0.706$.

2.2. Axborot nazariyasi asoslari

Faraz qilaylik, X tasodifiy o‘zgaruvchi bo‘lib, $P(X = x_i) = p_i$ ehtimollikga ega x_1, x_2, \dots, x_n chekli sondagi qiymatlar to‘plamidan iborat bo‘lsin. Bu yerda, har bir i ($1 \leq i \leq n$) uchun $0 \leq p_i \leq 1$ o‘rinli va $\sum_{i=1}^n p_i = 1$ ga teng. Shuningdek, Y va Z lar ham tasodifiy o‘zgaruvchi bo‘lib, chekli sondagi qiymatlar to‘plamidan iborat.

Informatsiyaning statistik nazariyasi K.Shennon tomonidan batafsil o‘rganilgan.

Yuz berish ehtimolligi birga yaqin bo‘lgan tez-tez uchraydigan hodisa xususida xabar paydo bo‘lsa, bunday xabarning qabul qiluvchi uchun informativligi kam bo‘ladi. Xuddi shunday yuz berish ehtimolligi nolga yaqin bo‘lgan xabarning ham informativligi kam bo‘ladi.

Hodisalarga qandaydir tajribaning natijasi sifatida qarash mumkinki, bunday tajribaning barcha natijalari ansamblni, ya’ni hodisalarning to‘liq guruhini tashkil etadi. K.Shennon tajriba jarayonida

paydo bo'luvchi hodisaning *noaniqligi* tushunchasini kiritdi va uni *entropiya* deb atadi.

Ansambl entropiyasi uning noaniqligining va demak informativligining miqdoriy o'lchovi bo'lib, tajribaning har bir mumkin bo'lgan natijalari ehtimolligi to'plamining o'rtacha funksiyasi sifatida ifodalanadi.

Ta'rif 2.2.1. X o'zgaruvchining *noaniqligi* yoki *entropiyasi* $H(X) = -\sum_{i=1}^n p_i \lg p_i = \sum_{i=1}^n p_i \lg\left(\frac{1}{p_i}\right)$ kabi belgilanib, shartli ravishda, agar $p_i = 0$ bo'lsa, $p_i \lg p_i = p_i \lg\left(\frac{1}{p_i}\right) = 0$ tenglik o'rinli.

Entropiyaning xususiyatlari. Faraz qilaylik, X kattalik n ta qiymatdan iborat o'zgaruvchi bo'lsin. U holda quyidagilar o'rinli:

I. $0 \leq H(X) \leq \lg n$;

II. Faqat i ning biror qiymati uchun $p_i = 1$ va qolgan barcha $i \neq j$ uchun $p_j = 0$ bo'lsa, $H(X) = 0$ ga teng bo'ladi (ya'ni, natijaning noaniqligi yo'q).

III. Faqat i ning ($1 \leq i \leq n$) har bir qiymati uchun $p_i = 1/n$ o'rinli bo'lsa, $H(X) = \lg n$ ga teng bo'ladi.

Birlashma entropiya statistik bog'langan xabarlarining birgalikda paydo bo'lish entropiyasini hisoblashda ishlatiladi.

Ta'rif 2.2.2. X va Y larning *birlashma entropiyasi* quyidagiga teng:

$$H(X, Y) = - \sum_{x, y} P(X = x, Y = y) \lg(P(X = x, Y = y)),$$

bu yerda, yig'indi x va y larni mos holda X va Y larning qiymatlari sohasida tegishligini bildiradi. Ifodani ixtiyoriy sondagi tasodifiy o'zgaruvchilar uchun ham ifodalash mumkin.

Agar X va Y lar tasodifiy o'zgaruvchilar bo'lsa, u holda $H(X, Y) \leq H(X) + H(Y)$ shart faqat va faqat X va Y lar mustaqil bo'lganda o'rinli bo'ladi.

Entropiyalarni jamlash qoidasiga muvofiq ikkita mazmun jihatidan turli (mustaqil) kitoblardagi informatsiya miqdori – alohida kitoblardagi informatsiya miqdorlarining yig'indisiga teng. Agar bir kitob ikkinchi kitobning qismini o'z ichiga olsa, ushbu ikki kitobdagi informatsiya miqdori alohida kitoblardagi informatsiya miqdorlarining yig'indisiga teng bo'lmaydi, balki undan kam bo'ladi. Bu holda informatsiya miqdorini o'lchashda *shartli entropiya* tushunchasidan foydalaniladi.

Shartli entropiyani hisoblashda shartli ehtimolliklar u yoki bu ko‘rinishda ishlatiladi.

Ta’rif 2.2.3. Agar X va Y lar tasodifiy o‘zgaruvchilar bo‘lsa, berilgan $Y = y$ uchun X ning shartli entropiyasi quyidagicha ifodalanadi:

$$H(X|Y = y) = - \sum_x P(X = x|Y = y) \lg(P(X = x|Y = y)),$$

bu yerda, yig‘indi x qiymat X ning qiymatlari sohasida tegishligini bildiradi.

Shartli entropiya quyidagi xususiyatlarga ega:

I. $H(X|Y)$ miqdor Y hodisa kuzatilganidan so‘ng X ning noma’lumlik darajasi miqdorini o‘lchaydi.

II. $H(X|Y) \geq 0$ va $H(X|X) = 0$.

III. $H(X, Y) = H(X) + H(Y|X) = H(Y) + H(X|Y)$.

$H(X|Y) \leq H(X)$ shart faqat va faqat X va Y lar mustaqil bo‘lganda o‘rinli bo‘ladi.

2.3. Murakkablik nazariyasi

Murakkablik nazariyasining *asosiy maqsadi* hisoblash muammolarini ularni yechish uchun zarur bo‘lgan resurslarga qarab tasniflash mexanizmlari bilan ta’minlashdir. Bunda, tasniflash biror hisoblash modeliga bog‘liq bo‘lmasdan, muammoni ichki farqini o‘lchashi kerak bo‘ladi. O‘lchashdagi resurslar sifatida vaqt, saqlash uchun xotira hajmi, tasodifiy bitlar, protsessorlar soni va h.k. bo‘lishi mumkin. Biroq, aksariyat holda vaqtga yoki ba’zida xotira hajmiga asosiy e’tibor beriladi.

Ta’rif 2.3.1. Algoritm – bu o‘zgaruvchan kirishni qabul qiluvchi va chiqish bilan to‘xtovchi yaxshi ishlab chiqilgan hisoblash muolajasi.

Yuqoridagi ta’rifda keltirilgan “yaxshi ishlab chiqilgan hisoblash muolajasi” tushunchasi matematik jihatdan aniq emas. Hisoblashlarni Turing mashinasi (Turing machine), xotiradan ixtiyoriy foydalanishli mashina (Random-access machine) yoki mantiqiy sxema (Boolean circuits) yordamida amalga oshirish mumkin bo‘lsada, biror dasturlash tilida yozilgan ixtiyoriy kirishni qabul qiluvchi va chiqish qiymati bilan to‘xtovchi kompyuter dasturi ko‘rinishida yozilgan algoritm sifatida qarash bir muncha qulay hisoblanadi. Mazkur holda, qo‘yilgan

muammoni yechuvchi eng samarali (tezkor) algoritmni topish muhimdir. Mazkur muammoni yechish uchun algoritm sarflagan vaqti qo'yilgan muammoning "o'lchamiga" bog'liq bo'ladi. Bundan tashqari, algoritmlarni solishtirish jarayonida bir xil vaqt birliklaridan foydalanish ham talab etiladi.

Ta'rif 2.3.2. Kirish o'lchami – kirish qiymatini biror kodlash sxemasi yordamida ikkilik ko'rinishda aks ettirishda zarur bo'lgan bitlarning umumiy soni. Ba'zida, kirish o'lchami kirishdagi elementlar soniga teng bo'ladi.

Masalan:

- musbat n sonini ikkilik ko'rinishda taqdim etishdagi bitlar soni $1 + \lfloor \lg n \rfloor$ ga teng. Ya'ni, $n = 7$ bo'lsa, $1 + \lfloor \lg 7 \rfloor = 1 + \lfloor 2.807 \rfloor = 1 + 2 = 3$ ga teng bo'ladi.

- agar f eng katta darajasi k bo'lgan ko'phad bo'lsa va uning koeffitsientlari musbat, n dan katta bo'lmagan butun sonlar bo'lsa, u holda f ning o'lchami $(k + 1) \lg n$ ga teng bo'ladi.

- agar A matritsa r qator va s ustundan iborat bo'lsa va elementlari n dan katta bo'lmagan musbat butun sonlar bo'lsa, u holda A ning bitdagi uzunligi $rs \lg n$ ga teng bo'ladi.

Ta'rif 2.3.3. Algoritmning biror kirish qiymati uchun *ishlash vaqti* - bajariluvchi bazaviy amallar yoki "qadam" lar soniga teng.

Bu yerda, odatda "qadam" sifatida katta bo'lmagan amallar qaralsa, ba'zida esa taqqoslash, mashina komandalari (Machine Instructions), mashina takti (Machine clock cycle), modul bo'yicha ko'paytirish va h.k. olinishi mumkin.

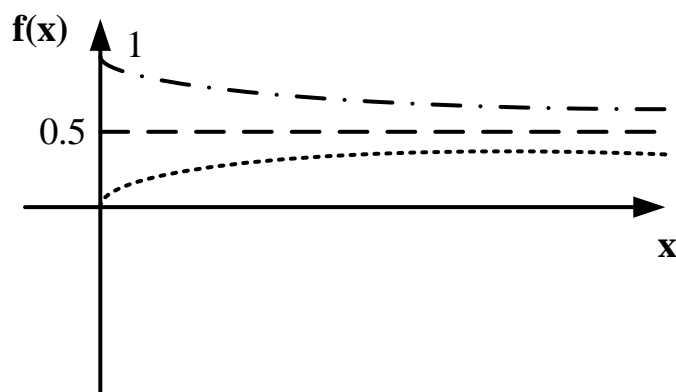
Ta'rif 2.3.4. Algoritm *ishlashining eng yomon vaqti* – funksiyani ixtiyoriy kirish qiymatida ishlash vaqtining eng yuqori chegarasi bilan belgilanadi.

Ta'rif 2.3.5. Algoritm *ishlashining o'rtacha vaqti* – funksiyani ixtiyoriy kirish qiymatida ishlash vaqtining o'rtacha qiymati bilan belgilanadi.

Asimptotik belgilanishlar

Algoritmning ishlash vaqtini aniqlash aksariyat hollarda murakkab hisoblanadi. Bunday vaziyatda, ishlash vaqtini taxminiy qiymat bilan hisoblashga to'g'ri keladi. Mazkur holda qurilmaga, amalga oshirilgan algoritmgaga bog'liqsiz holda algoritmning samaradorligini baholash zarur bo'ladi. *Asimptotik tahlil* ushbu imkoniyatni taqdim etib, algoritmning ishlash vaqtini ifodalovchi matematik vosita hisoblanadi.

Norasmiy ravishda *asimptotik* atamasi qiymatga yoki egri chiziqqa ixtiyoriy yaqinlashishni anglatadi (ya'ni, biror chegara olinganligi sababli). Berilgan E egri chiziqqa asimptotik bo'lgan chiziq yoki A egri chiziq – E ning *asimptotasi* deyiladi. Masalan, 2.1-rasmda $y = 0.5$ chiziqqa asimptotik bo'lgan ikkita egri chiziq aks ettirilgan. Birinchisi $[0,1]$ kamayish tartibida bo'lsa, ikkinchisi $[0,0]$ dan o'sish tartibida.

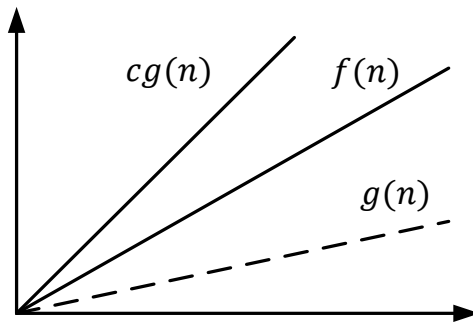


2.1-rasm. Asimptotik egri chiziqlar

Asimptotik tahlil cheklangan xatti harakatlarni tavsiflash usuli. Masalan, n ning qiymati juda katta bo'lgan holat uchun $f(n)$ funksiya xususiyatlarini olaylik. Agar $f(n) = n^2 + 3n$ shaklida bo'lsa va n ning qiymati juda katta bo'lganda, ifodadagi $3n$ had n^2 hadga nisbatan ahamiyatini yo'qotadi. Yoki, $n \rightarrow \infty$ uchun $f(n)$ funksiya n^2 ga asimptotik ekvivalent deb aytish mumkin va bu odatda $f(n) \sim n^2$ shaklida belgilanadi.

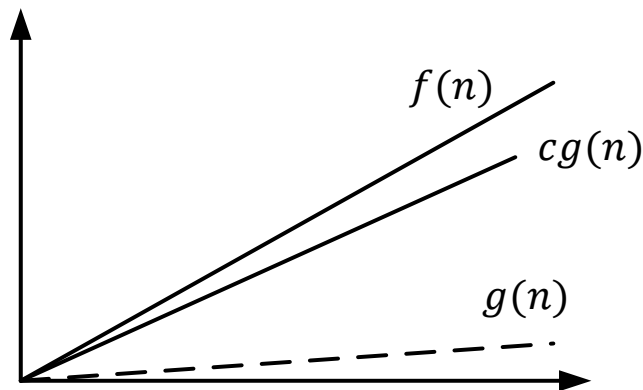
Keyinchalik foydalanish uchun faqat butun musbat sonlar uchun aniqlangan va manfiy bo'lmagan qiymatlarni qaytaruvchi funksiyalar (f va g) qaraladi.

Asimptotik yuqori chegara (katta O belgilanishi). Agar barcha $n \geq n_0$ lar uchun $0 \leq f(n) \leq cg(n)$ shartni qanoatlantiruvchi musbat o'zgarmas c va musbat butun son n_0 mavjud bo'lsa, $f(n) = O(g(n))$ o'rinli. Bu yerda, $f(n) = O(g(n))$ ning ma'nosi o'zgarmasga ko'paytirilgan hol uchun f funksiya $g(n)$ ga nisbatan tezkor asimptotik emas. Algoritm ishlashining eng yomon vaqtini hisoblashda asimptotik yuqori chegaradan foydalaniladi (2.2-rasm).



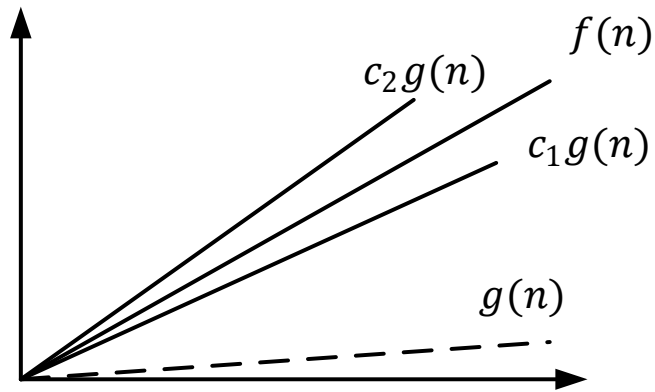
2.2-rasm. **Katta O belgilanishi**

Asimptotik quyi chegara (Ω belgilanish). Agar barcha $n \geq n_0$ lar uchun $0 \leq cg(n) \leq f(n)$ shartni qanoatlantiruvchi musbat o'zgarmas c va musbat butun son n_0 mavjud bo'lsa, $f(n) = \Omega(g(n))$ o'rinli. Bu yerda, $f(n) = \Omega(g(n))$ ning ma'nosi $f(n)$ funksiya o'zgarishga ko'paytirilgan hol uchun kamida $g(n)$ kabi tez o'sishini anglatadi. Algoritm ishlashining eng yaxshi vaqtini hisoblashda asimptotik quyi chegaradan foydalaniladi (2.3-rasm).



2.3-rasm. **Ω belgilanish**

Asimptotik qat'iy chegara (Θ belgilanish). Agar barcha $n \geq n_0$ lar uchun $c_1g(n) \leq f(n) \leq c_2g(n)$ shartni qanoatlantiruvchi musbat o'zgarmas c_1, c_2 va musbat butun son n_0 mavjud bo'lsa, $f(n) = \Theta(g(n))$ o'rinli (2.4-rasm).



2.4-rasm. Θ belgilanish

Kichik o belgilanishi. Agar barcha $n \geq n_0$ larda $0 \leq f(n) < cg(n)$ shartni qanoatlantiruvchi musbat o'zgarimas $c > 0$ uchun musbat $n_0 > 0$ o'zgarimas mavjud bo'lsa, $f(n) = o(g(n))$ o'rinli. Bu yerda, $f(n) = o(g(n))$ ning ma'nosi $g(n)$ funksiya $g(n)$ uchun asimptotik qat'iy bo'lmagan yuqori chegara. Ya'ni, n ning qiymati ortishi bilan $f(n)$ funksiyaning $g(n)$ ga bog'liqligi kamayib boradi.

Yuqoridagi belgilanishlar qator xususiyatlarga ega. Ixtiyoriy $f(n)$, $g(n)$, $h(n)$ va $l(n)$ funksiyalar uchun quyidagilar o'rinli:

1. Agar faqat va faqat $g(n) = \Omega(f(n))$ o'rinli bo'lsa, $f(n) = O(g(n))$ o'rinli bo'ladi.

2. Agar faqat va faqat $f(n) = O(g(n))$ va $f(n) = \Omega(g(n))$ o'rinli bo'lsa, $f(n) = \Theta(g(n))$ o'rinli bo'ladi.

3. Agar $f(n) = O(h(n))$ va $g(n) = O(h(n))$ bo'lsa, u holda $(f + g)(n) = O(h(n))$ o'rinli bo'ladi.

4. Agar $f(n) = O(h(n))$ va $g(n) = O(l(n))$ bo'lsa, u holda $(f \cdot g)(n) = O(h(n)l(n))$ o'rinli bo'ladi.

5. (*Reflektivlik*) $f(n) = O(f(n))$.

6. (*Tranzitivlik*) Agar $f(n) = O(g(n))$ va $g(n) = O(h(n))$ bo'lsa, $f(n) = O(h(n))$ o'rinli bo'ladi.

Asimptotik tahlil algoritmlarning ishlash vaqtlarini hisoblashda foydalanilib, quyida misol sifatida "Chiziqli qidirish (Linear Search)" algoritmi uchun qo'llanilgan. Algoritmni baholashni quyidagi holatlarda ko'rib chiqamiz:

- 1) Algoritm ishlashining eng yomon vaqti.
- 2) Algoritm ishlashining o'rtacha vaqti.
- 3) Algoritm ishlashining eng yaxshi vaqti.

“Chiziqli qidirish” algoritmi C dasturlash tilida quyidagicha amalga oshirilgan bo‘lsin:

```
#include <bits/stdc++.h>
using namespace std;
// arr[] ichidan x ni chiziqli qidirish.k.
// Agar x bor bo'lsa, uning joylashgan o'rni
qaytariladi,
// aks holda -1 qaytariladi.
int search(int arr[], int n, int x)
{
    int i;
    for (i = 0; i < n; i++) {
        if (arr[i] == x)
            return i;
    }
    return -1;
}

// Foydalanish kodi
int main()
{
    int arr[] = { 1, 10, 30, 15 };
    int x = 30;
    int n = sizeof(arr) / sizeof(arr[0]);
    cout << x << " element "
        << search(arr, n, x) << " o'rinda
joylashgan";
    getchar();
    return 0;
}
```

Algoritm ishlashining eng yomon vaqti. Algoritm ishlash vaqtining eng yomon vaqtini bilish uchun asimptotik yuqori chegarani hisoblash zarur bo‘ladi. Chiziqli qidiruvda algoritm ishlashining eng yomon vaqti izlanayotgan x element to‘plamda mavjud bo‘lmaganida yuz beradi. Boshqacha aytganda, x element to‘plamda mavjud bo‘lmaganida algoritm barcha elementlar bilan taqqoslashni amalga oshiradi. Shuning uchun chiziqli qidiruv algoritmining eng yomon ishlash vaqti $O(n)$ ga teng bo‘ladi.

Algoritm ishlashining o'rtacha vaqti. Algoritm ishlashining o'rtacha vaqtini hisoblash uchun, barcha kirishlar uchun vaqtlarni aniqlash va ularni o'rtachasini hisoblash talab etiladi. Buning uchun esa, qidirilayotgan elementlarning taqsimlanishini bilish shart. Agar chiziqli qidirishda izlanuvchi barcha elementlarni tekis taqsimot qonuniga bo'ysinadi deb faraz qilsak, barcha holatlarni yig'ish va uni $(n + 1)$ ga bo'lishning o'zi yetarli bo'ladi:

$$T = \frac{\sum_{i=1}^{n+1} \theta(i)}{n+1} = \frac{\theta((n+1)*(n+2)/2)}{n+1} = O(n).$$

Algoritm ishlashining eng yaxshi vaqti. Algoritm ishlash vaqtining eng yomon vaqtini bilish uchun asimptotik quyi chegarani hisoblash zarur bo'ladi. Ya'ni, amalga oshiriluvchi minimal amallar sonini bilish talab etiladi. Chiziqli qidirishda mazkur holat izlanayotgan element birinchi o'rinda joylashganda yuzaga keladi. Mazkur holatda, amallar soni o'zgarmas bo'ladi (n ga bog'liq bo'lmaydi) hamda $\Omega(1)$ ga teng bo'ladi.

2.4. Sonlar nazariyasi

Mazkur bo'limda ko'rib o'tiladigan amallar butun sonlar (butun sonlar to'plami \mathbb{Z} bilan belgilanib, $\{\dots, -3, -2, -1, 0, 1, 2, 3, \dots\}$ sonlardan iborat) ustida amalga oshiriladi.

Ta'rif 2.4.1. Faraz qilaylik, a, b butun sonlar bo'lsin. U holda, agar $b = ac$ shartni qanoatlantiruvchi biror c soni mavjud bo'lsa, a soni b ni bo'luvchisi (bo'ladi) deb aytiladi va u $a|b$ kabi belgilanadi.

Masalan, $18 = (-3)(-6)$ ekanligidan $-3|18$ deb yozish mumkin.

Qoida 2.4.1. Sonlarni bo'lishda, $a, b, c \in \mathbb{Z}$ lar uchun quyidagi xususiyatlar o'rinli:

1. $a|a$.
2. Agar $a|b$ va $b|c$ bo'lsa, u holda $a|c$ o'rinli.
3. Agar $a|b$ va $a|c$ bo'lsa, u holda $x, y \in \mathbb{Z}$ lar uchun $a|(bx + cy)$ o'rinli.
4. Agar $a|b$ va $b|a$ bo'lsa, u holda $a = \pm b$.

Ta'rif 2.4.2. Agar a, b ($b \geq 1$) butun sonlar bo'lsa, u holda a ni b ga bo'lganda bo'linma q ga va qoldiq r ga teng:

$$a = qb + r, \quad 0 \leq r < b.$$

Bundan tashqari, q va r lar unikal. Bo‘linmadagi qoldiq $a \bmod b$ shaklida, bo‘linma esa $a \operatorname{div} b$ shaklida belgilanadi.

Qoida 2.4.2. Faraz qilaylik, $a, b \in \mathbb{Z}$ va $b \neq 0$. U holda $a \operatorname{div} b = \lfloor a/b \rfloor$ va $a \bmod b = a - b\lfloor a/b \rfloor$.

Masalan, agar $a = 73$, $b = 17$ bo‘lsa, u holda $q = 4$ va $r = 5$ ga teng. Shuning uchun, $73 \bmod 17 = 5$ va $73 \operatorname{div} 17 = 4$.

Ta’rif 2.4.3. Agar $c|a$ va $c|b$ bo‘lsa, u holda c soni a va b sonlarining *umumiy bo‘luvchisi* deb aytiladi.

Ta’rif 2.4.4. Agar quyidagi shartlar o‘rinli bo‘lsa, manfiy bo‘lmagan d soni a va b butun sonlarining *eng katta umumiy bo‘luvchi* (*EKUB*, *greatest common divisor* - \gcd) deb aytiladi va $d = \gcd(a, b)$ kabi belgilanadi:

- 1) d soni a va b sonlarining umumiy bo‘luvchisi;
- 2) har doim $c|a$ va $c|b$ bo‘lsa, u holda $c|d$ bo‘ladi.

Boshqacha aytganda, $\gcd(a, b)$ soni a va b ni bo‘luvchi eng katta musbat butun son. Xususiyl holda, $\gcd(0, 0) = 0$ ga teng.

Masalan, 12 va 18 sonlarining umumiy bo‘luvchilari $\{\pm 1, \pm 2, \pm 3, \pm 6\}$ va $\gcd(12, 18) = 6$ ga teng.

Ta’rif 2.4.5. Agar quyidagi shartlar o‘rinli bo‘lsa, manfiy bo‘lmagan d soni a va b butun sonlarining *eng kichik umumiy karralisi* (*EKUK*, *least common multiple* - lcm) deb aytiladi va $d = \operatorname{lcm}(a, b)$ kabi belgilanadi.

- 1) $a|d$ va $b|d$;
- 2) har doim $a|c$ va $b|c$ bo‘lsa, u holda $d|c$ bo‘ladi.

Boshqacha aytganda, $\operatorname{lcm}(a, b)$ soni a va b ga bo‘linuvchi eng kichik qiymatni ko‘rsatadi.

Qoida 2.4.3. Agar a va b lar musbat butun sonlar bo‘lsa, u holda $\operatorname{lcm}(a, b) = a \cdot b / \gcd(a, b)$ ga teng bo‘ladi.

Masalan, $\gcd(12, 18) = 6$ bo‘lgani bois, $\operatorname{lcm}(12, 18) = 12 \cdot \frac{18}{6} = 36$ ga teng bo‘ladi.

Ta’rif 2.4.6. Agar $\gcd(a, b) = 1$ shart o‘rinli bo‘lsa, u holda ikki a va b sonlar *o‘zaro tub sonlar* deb ataladi.

Ta’rif 2.4.7. $p \geq 2$ butun son *tub* deyiladi, agar uning bo‘luvchilari faqat 1 va p bo‘lsa. Aks holda, p soni *murakkab son* deb aytiladi.

Qoida 2.4.4. Agar p tub son bo‘lsa va $p|ab$ o‘rinli bo‘lsa, u holda $p|a$ yoki $p|b$ (yoki har ikkalasi) o‘rinli bo‘ladi.

Qoida 2.4.5. Tub sonlar soni cheksiz.

Qoida 2.4.6. Faraz qilaylik, x dan kichik tub sonlar soni $\pi(x)$ ga teng bo'lsin. U holda quyidagi tenglik o'rinli:

$$\lim_{x \rightarrow \infty} \frac{\pi(x)}{x/\ln x} = 1.$$

Masalan, $x = 10^{10}$ uchun $\pi(x) = 455\,052\,511$ ga tengligi bois, $[x/\ln x] = 434\,294\,481$ o'rinli bo'ladi.

Qoida 2.4.7. x dan kichik tub sonlar soni $\pi(x)$ ga teng bo'lsin. U holda $x \geq 17$ uchun $\pi(x) > \frac{x}{\ln x}$ shart va $x > 1$ uchun $\pi(x) < 1.25506 \frac{x}{\ln x}$ shart o'rinli bo'ladi.

Qoida 2.4.8. Har bir $n \geq 2$ butun sonni tub sonlarning daraja ko'rinishidagi ko'paytmasi shaklida ifodalash mumkin:

$$n = p_1^{e_1} p_2^{e_2} \dots p_k^{e_k}$$

Bu yerda, p_i – bir biridan farqli tub sonlar va e_i – musbat butun sonlar.

Qoida 2.4.9. Agar har bir $e_i \geq 0$ va $f_i \geq 0$ uchun $a = p_1^{e_1} p_2^{e_2} \dots p_k^{e_k}$, $b = p_1^{f_1} p_2^{f_2} \dots p_k^{f_k}$ o'rinli bo'lsa, u holda quyidagilarlar o'rinli bo'ladi:

$$\begin{aligned} \gcd(a, b) &= p_1^{\min(e_1, f_1)} p_2^{\min(e_2, f_2)} \dots p_k^{\min(e_k, f_k)} \text{ va} \\ \text{lcm}(a, b) &= p_1^{\max(e_1, f_1)} p_2^{\max(e_2, f_2)} \dots p_k^{\max(e_k, f_k)}. \end{aligned}$$

Masalan, $a = 4864 = 2^8 \cdot 19$, $b = 3458 = 2 \cdot 7 \cdot 13 \cdot 19$. U holda $\gcd(4864, 3458) = 2 \cdot 19 = 38$ va $\text{lcm}(4864, 3458) = 2^8 \cdot 7 \cdot 13 \cdot 19 = 442624$.

Ta'rif 2.4.8. Faraz qilaylik, $n \geq 1$ uchun $[1, n]$ oraliqda n bilan o'zaro tub bo'lgan sonlar miqdori $\phi(n)$ kabi belgilansin. ϕ funksiya Eylerning *fi* (*phi*) funksiyasi deb ataladi.

Qoida 2.4.10. Eylerning *fi* funksiya quyidagi xususiyatlar o'rinli:

- 1) Agar p tub son bo'lsa, u holda $\phi(p) = p - 1$ ga teng.
- 2) Eylerning *fi* funksiyasi multiplikativ. Ya'ni, agar $\gcd(m, n) = 1$ bo'lsa, u holda $\phi(mn) = \phi(m) \cdot \phi(n)$ o'rinli.

3) Agar $n = p_1^{e_1} p_2^{e_2} \dots p_k^{e_k}$ bo'lsa, u holda $\phi(n) = n(1 - \frac{1}{p_1})(1 - \frac{1}{p_2}) \dots (1 - \frac{1}{p_k})$ ga teng bo'ladi.

Qoida 2.4.11. $n \geq 5$ bo'lgan barcha butun sonlar uchun $\phi(n) > \frac{n}{6 \ln \ln n}$ shart o'rinli bo'lib, $\phi(n)$ funksiya uchun quyi chegarani aniqlaydi.

Qoida 2.4.12. Faraz qilaylik, a va b manfiy bo'lmagan sonlar n dan kichik yoki unga teng bo'lsin. n son b ni ikkilik ko'rinishda taqdim etish uchun kerak bo'lgan bitlar soni $\lfloor \lg n \rfloor + 1$ ga teng bo'ladi va bu son $\lg n$ yaqin. Butun sonlar ustida bajariluvchi to'rt asosiy amallar: qo'shish, ayirish, ko'paytirish va bo'lish, uchun bit amallarining soni quyidagi jadvalda keltirilgan.

2.1-jadval

Amallar va ularning bitlar soni

| Amallar | Bit amallari soni |
|---------------------------|---|
| Qo'shish: $a + b$ | $O(\lg a + \lg b) = O(\lg n)$ |
| Ayirish: $a - b$ | $O(\lg a + \lg b) = O(\lg n)$ |
| Ko'paytirish: $a \cdot b$ | $O((\lg a) \cdot (\lg b)) = O((\lg n)^2)$ |
| Bo'lish: $a = qb + r$ | $O((\lg q) \cdot (\lg b)) = O((\lg n)^2)$ |

Qoida 2.4.13. Agar a va b musbat butun sonlar $a > b$ shartni qanoatlantirsa, u holda $\gcd(a, b) = \gcd(b, a \bmod b)$ o'rinli.

Algoritm 2.4.1. (Ikki butun son uchun EKUBni hisoblashning Evklid algoritmi)

KIRISH: $a \geq b$ shartni qanoatlantiruvchi a va b musbat butun sonlar

ChIQISH: a va b ning EKUBi

1. $b \neq 0$ holat uchun quyidagilar bajarilsin:

1.1. $r \leftarrow a \bmod b, a \leftarrow b, b \leftarrow r.$

2. a ni qaytarish.k.

Qoida 2.4.14. EKUBni hisoblashning Evklid algoritmining ishlash vaqti $O((\lg n)^2)$ bit amallari sonini tashkil qiladi.

Masalan, Algoritm 2.4.1 algoritm asosida $\gcd(4864, 3458) = 38$ tengligini ko'rish mumkin:

$$4864 = 1 \cdot 3458 + 1406$$

$$3458 = 2 \cdot 1406 + 646$$

$$1406 = 2 \cdot 646 + 114$$

$$646 = 5 \cdot 114 + 76$$

$$114 = 1 \cdot 76 + 38$$

$$76 = 2 \cdot 38 + 0$$

Shuningdek, yuqorida keltirilgan Evklid algoritmini ikki butun son a va b ni EKUBi bo'lgan d ni va $ax + by = d$ tenglikni qanoatlantiruvchi x va y butun sonlarini topish uchun “kengaytirish” mumkin.

Algoritm 2.4.2. (Kengaytirilgan Evklid algoritmi)

KIRISH: $a \geq b$ shartni qanoatlantiruvchi a va b musbat butun sonlar

CHIQUISH: $d = \gcd(a, b)$ va $ax + by = d$ tenglikni qanoatlantiruvchi x va y butun sonlari

1. Agar $b = 0$ bo'lsa, u holda $d \leftarrow a$, $x \leftarrow 1$, $y \leftarrow 0$ va (d, x, y) qaytarilsin.

2. Quyidagilar o'rnatilsin: $x_2 \leftarrow 1$, $x_1 \leftarrow 0$, $y_2 \leftarrow 0$, $y_1 \leftarrow 1$.

3. $b > 0$ uchun quyidagilar bajarilsin:

3.1. $q \leftarrow \lfloor a/b \rfloor$, $r \leftarrow a - qb$, $x \leftarrow x_2 - qx_1$, $y \leftarrow y_2 - qy_1$.

3.2. $a \leftarrow b$, $b \leftarrow r$, $x_2 \leftarrow x_1$, $x_1 \leftarrow x$, $y_2 \leftarrow y_1$ va $y_1 \leftarrow y$.

2. Quyidagilar o'rnatilsin: $d \leftarrow a$, $x \leftarrow x_2$, $y \leftarrow y_2$ va (d, x, y) ni qaytarilsin.

Qoida 2.4.15. Kengaytirilgan Evklid algoritmining ishlash vaqti $O((\lg n)^2)$ bit amallari sonini tashkil qiladi.

Masalan, 2.4.2 algoritm yordamida $a = 4864$ va $b = 3458$ sonlari uchun $\gcd(4864, 3458) = 38$ va $(4864)(32) + (3458)(-45) = 38$ ni hisoblash mumkin:

| q | r | x | y | a | b | x_2 | x_1 | y_2 | y_1 |
|-----|------|-----|-----|------|------|-------|-------|-------|-------|
| - | - | - | - | 4864 | 3458 | 1 | 0 | 0 | 1 |
| 1 | 1406 | 1 | -1 | 3458 | 1406 | 0 | 1 | 1 | -1 |
| 2 | 646 | -2 | 3 | 1406 | 646 | 1 | -2 | -1 | 3 |
| 2 | 114 | 5 | -7 | 646 | 114 | -2 | 5 | 3 | -7 |
| 5 | 76 | -27 | 38 | 114 | 76 | 5 | -27 | -7 | 38 |
| 1 | 38 | 32 | -45 | 76 | 38 | -27 | 32 | 38 | -45 |
| 2 | 0 | -91 | 128 | 38 | 0 | 32 | -91 | -45 | 128 |

n butun son bo'yicha modul ($\text{mod } n$). Faraz qilaylik n musbat butun son bo'lsin.

Ta'rif 2.4.9. Agar a va b lar butun sonlar bo'lsa, u holda a soni $b \text{ mod } n$ soniga kongurent deb aytiladi hamda agar $(a - b)$ soni n ga bo'linsa, $a \equiv b(\text{mod } n)$ shaklida belgilanadi.

Masalan, $24 - 9 = 3 \cdot 5$ bo'lgani bois $24 \equiv 9 \pmod{5}$ o'rinli. Yoki, $-11 - 17 = -4 \cdot 7$ bo'lgani bois $-11 \equiv 17 \pmod{7}$ o'rinli bo'ladi.

Kongurentlik xususiyatlari. Barcha $a, a_1, b, b_1, c \in \mathbb{Z}$ lar uchun quyidagilar o'rinli:

1) Agar faqat va faqat a hamda b sonlarini n ga bo'lganda bir xil qoldiq qolsa $a \equiv b \pmod{n}$ tenglik o'rinli bo'ladi.

2) (*akslantirish xususiyati*) $a \equiv a \pmod{n}$.

3) (*simmetriklik xususiyati*) Agar $a \equiv b \pmod{n}$ bo'lsa, u holda $b \equiv a \pmod{n}$ o'rinli bo'ladi.

4) (*tranzitivlik xususiyati*) Agar $a \equiv b \pmod{n}$ va $b \equiv c \pmod{n}$ bo'lsa, u holda $a \equiv c \pmod{n}$ o'rinli bo'ladi.

5) Agar $a \equiv a_1 \pmod{n}$ va $b \equiv b_1 \pmod{n}$ bo'lsa, u holda $a + b \equiv a_1 + b_1 \pmod{n}$ va $ab \equiv a_1 b_1 \pmod{n}$ o'rinli.

Ta'rif 2.4.10. n butun son bo'yicha modul \mathbb{Z}_n kabi belgilanib, $\{0, 1, 2, \dots, n-1\}$ sonlar to'plamidan iborat bo'ladi. \mathbb{Z}_n da qo'shish, ayirish va ko'paytirish \pmod{n} bo'yicha amalga oshiriladi.

Masalan, $\mathbb{Z}_{25} = \{0, 1, 2, \dots, 24\}$ bo'lsin. U holda, \mathbb{Z}_{25} da $13 + 16 = 29 \equiv 4 \pmod{25}$ bo'lgani bois, $13 + 16 = 4$ bo'ladi.

Ta'rif 2.4.11. Faraz qilaylik $a \in \mathbb{Z}_n$ bo'lsin. \pmod{n} bo'yicha a sonining *multiplikativ teskarisi* $x \in \mathbb{Z}_n$ bo'lib, $ax \equiv 1 \pmod{n}$ shart o'rinli bo'ladi. Agar x mavjud bo'lsa, u holda u unikal va a ning teskarisi mavjud deyiladi. a ning teskarisi a^{-1} kabi belgilanadi.

Ta'rif 2.4.12. Faraz qilaylik $a, b \in \mathbb{Z}_n$ bo'lsin. \pmod{n} bo'yicha a ni b ga bo'lish a va b^{-1} ni \pmod{n} bo'yicha ko'paytirishga teng bo'lib, faqat b soni \pmod{n} bo'yicha teskarisiga ega bo'lsa joiz bo'ladi.

Qoida 2.4.16. Faraz qilaylik $a \in \mathbb{Z}_n$ bo'lsin. U holda, faqat va faqat $\gcd(a, n) = 1$ bo'lsa, a ning teskarisi mavjud deyiladi.

Masalan, \mathbb{Z}_9 uchun 1, 2, 4, 5, 7 va 8 sonlarining teskarisi mavjud. Xususan, $4 \cdot 7 \equiv 1 \pmod{9}$ sababli $4^{-1} = 7$ ga teng.

Qoida 2.4.17. Faraz qilaylik $d = \gcd(a, n)$ bo'lsin. Faqat va faqat b soni d ga bo'linsa, $ax \equiv b \pmod{n}$ tenglik x yechimga ega bo'ladi. Bu yerda, d ning qiymati $[0, n-1]$ oraliqda yotadi.

Qoida 2.4.18. (*Qoldiqlar haqida Xitoy teoremasi, (Chinese remainder theorem, CRT)*). Agar n_1, n_2, \dots, n_k butun sonlari juftlikka nisbatan o'zaro tub bo'lsa, u holda quyidagi tengliklar:

$$x \equiv a_1 \pmod{n_1}$$

$$\begin{aligned} x &\equiv a_2 \pmod{n_2} \\ &\vdots \\ x &\equiv a_k \pmod{n_k} \end{aligned}$$

yagona $n = n_1 n_2 \cdots n_k$ modul yechimiga ega bo'ladi.

Qoida 2.4.19. (Gauss algoritmi). Qoldiqlar haqida Xitoy teoremasidagi $x = \sum_{i=1}^k a_i N_i M_i \pmod{n}$ teng. Bu yerda, $N_i = n/n_i$ va $M_i = N_i^{-1} \pmod{n_i}$ ga teng. Ushbu hisoblashda $O((\lg n)^2)$ bit amali talab etiladi.

Masalan, 5, 7, 9 va 11 ga bo'lganda qoldiq 1, 2, 3 va 4 bo'ladigan x sonni toping. Mazkur holda quyidagi tenglamalar sistemasini yechish talab qilinmoqda:

$$\begin{aligned} x &\equiv 1 \pmod{5} \\ x &\equiv 2 \pmod{7} \\ x &\equiv 3 \pmod{9} \\ x &\equiv 4 \pmod{11} \end{aligned}$$

5, 7, 9 va 11 sonlari juftlikka nisbatan o'zaro tub bo'lgani bois, $n = 5 \cdot 7 \cdot 9 \cdot 11 = 3465$ ga teng. $N_1 = \frac{n}{5} = 693$, $N_2 = \frac{n}{7} = 495$, $N_3 = \frac{n}{9} = 385$ va $N_4 = \frac{n}{11} = 315$. Kichik hisoblashlar orqali $M_1 = 2$, $M_2 = 3$, $M_3 = 4$ va $M_4 = 8$ ga tengligini bilish mumkin. Shuning uchun, $x = (1 \cdot 693 \cdot 2 + 2 \cdot 495 \cdot 3 + 3 \cdot 385 \cdot 4 + 4 \cdot 315 \cdot 8) \pmod{3465} = 19056 \pmod{3465} = 1731$ ga teng bo'ladi. Bu esa, 1731 ni eng kichik yechim ekanligini ko'rsatadi.

Qoida 2.4.20. Agar $\gcd(n_1, n_2) = 1$ bo'lsa, u holda $x \equiv a \pmod{n_1}$ va $x \equiv a \pmod{n_2}$ juftlik unikal echim $x \equiv a \pmod{n_1 n_2}$ ga ega.

Ta'rif 2.4.13. \mathbb{Z}_n maydonning multiplikativ guruhi $\mathbb{Z}_n^* = \{a \in \mathbb{Z}_n \mid \gcd(a, n) = 1\}$. Xususan, agar n tub bo'lsa, u holda $\mathbb{Z}_n^* = \{a \mid 1 \leq a \leq n - 1\}$ ga teng bo'ladi.

Ta'rif 2.4.14. \mathbb{Z}_n^* tartibi undagi elementlar soni bilan aniqlanib, $|\mathbb{Z}_n^*|$ kabi belgilanadi.

Eylerning ϕ funksiyasiga ko'ra $|\mathbb{Z}_n^*| = \phi(n)$ ga teng bo'ladi. Bundan tashqari, agar $a \in \mathbb{Z}_n^*$ va $b \in \mathbb{Z}_n^*$ bo'lsa, $a \cdot b \in \mathbb{Z}_n^*$ o'rinli.

Qoida 2.4.21. Faraz qilaylik $n \geq 2$ bo'lsin.

1)(Eylar teoremasi) Agar $a \in \mathbb{Z}_n^*$ bo'lsa, u holda $a^{\phi(n)} \equiv 1 \pmod{n}$ ga teng.

2) Agar n turli tub sonlarning ko'paytmasi va $r \equiv s \pmod{\phi(n)}$ bo'lsa, u holda barcha a butun sonlar uchun $a^r \equiv a^s \pmod{n}$ o'rinli bo'ladi. Boshqacha aytganda, modul bilan ishlaganda (masalan, n) daraja $\pmod{\phi(n)}$ gacha kamayishi kerak.

Masalan, $\phi(12) = 4$ ga teng. Agar $\gcd(a, 12) = 1$ bo'lsa, u holda $a^4 \equiv 1 \pmod{12}$ o'rinli bo'ladi.

Eylar funksiyasining xususiy ko'rinishi Fermaning (kichik) teoremasi hisoblanadi.

Qoida 2.4.22. Faraz qilaylik p soni tub bo'lsin.

1)(Ferma teoremasi) Agar $\gcd(a, p) = 1$ bo'lsa, u holda $a^{p-1} \equiv 1 \pmod{p}$ o'rinli bo'ladi.

2) Agar $r \equiv s \pmod{p-1}$ o'rinli bo'lsa, u holda barcha a butun sonlar uchun $a^r \equiv a^s \pmod{p}$ tenglik o'rinli. Boshqacha aytganda, tub qiymatli modul bilan ishlaganda (masalan, p) daraja $\pmod{p-1}$ gacha kamayishi kerak.

3) Xususan, barcha butun son a uchun $a^p \equiv a \pmod{p}$ tenglik o'rinli.

Ta'rif 2.4.15. Faraz qilaylik $a \in \mathbb{Z}_n^*$ bo'lsin. a ning tartibi (order) $ord(a)$ deb belgilanib, $a^t \equiv 1 \pmod{n}$ shartni qanoatlantiruvchi eng kichik musbat t songa teng.

Qoida 2.4.23. Agar $a \in \mathbb{Z}_n^*$ ning tartibi t bo'lsa va $a^s \equiv 1 \pmod{n}$ ga teng bo'lsa, u holda s soni t ga bo'linadi. Xususan, $t | \phi(n)$.

Masalan, faraz qilaylik $n = 21$ ga teng. U holda $\mathbb{Z}_{21}^* = \{1, 2, 4, 5, 8, 10, 11, 13, 16, 17, 19, 20\}$. Bundan tashqari, $\phi(21) = \phi(7)\phi(3) = 12 = |\mathbb{Z}_{21}^*|$. U holda \mathbb{Z}_{21}^* dagi elementlarning tartiblari quyidagicha bo'ladi:

| | | | | | | | | | | | | |
|---------------------------|---|---|---|---|---|----|----|----|----|----|----|----|
| $a \in \mathbb{Z}_{21}^*$ | 1 | 2 | 4 | 5 | 8 | 10 | 11 | 13 | 16 | 17 | 19 | 20 |
| a ning tartibi | 1 | 6 | 3 | 6 | 2 | 6 | 6 | 2 | 3 | 6 | 6 | 2 |

Ta'rif 2.4.16. Faraz qilaylik $\alpha \in \mathbb{Z}_n^*$ bo'lsin. Agar α ning tartibi $\phi(n)$ ga teng bo'lsa, u holda α – generator yoki \mathbb{Z}_n^* ning primitiv elementi deyiladi. Agar \mathbb{Z}_n^* generator bo'lsa, u holda \mathbb{Z}_n^* ga nisbatan siklik deb aytiladi.

\mathbb{Z}_n^* generatorning xususiyatlari:

1) Faqat va faqat $n = 2, 4, p^k$ yoki $2p^k$ ga teng bo'lsa, u holda \mathbb{Z}_n^* uchun generator mavjud deyiladi. Bu yerda, p toq tub son (2 dan tashqari barcha tub sonlar toq tub sonlar deyiladi) va $k \geq 1$. Xususiyligida agar p tub son bo'lsa, u holda \mathbb{Z}_n^* uchun generator mavjud.

2) Agar \mathbb{Z}_n^* ning generatori α bo'lsa, u holda $\mathbb{Z}_n^* = \{\alpha^i \bmod n \mid 0 \leq i \leq \phi(n) - 1\}$ ga teng.

3) Faraz qilaylik \mathbb{Z}_n^* ning generatori α bo'lsin. U holda, faqat va faqat $\gcd(i, \phi(n)) = 1$ bo'lganida, $b = \alpha^i \bmod n$ ham \mathbb{Z}_n^* ning generatori bo'ladi. Bundan kelib chiqadiki, agar \mathbb{Z}_n^* siklik bo'lsa, u holda generatorlar soni $\phi(\phi(n))$ ga teng bo'ladi.

4) Faqat va faqat $\phi(n)$ ning har bir tub bo'luvchisi p uchun $\alpha^{\phi(n)/2} \not\equiv 1 \pmod{n}$ o'rinli bo'lsa, \mathbb{Z}_n^* ning generatori $\alpha \in \mathbb{Z}_n^*$ bo'ladi.

Masalan, yuqorida keltirilgan \mathbb{Z}_{21}^* siklik bo'lmagani bois ($\phi(21) = 12$ tartibga ega elementi mavjud emasligi uchun), \mathbb{Z}_n^* generatorning 1-xususiyatini qanoatlantirmaydi. Boshqa tomondan, \mathbb{Z}_{25}^* siklik hisoblanadi va unda $\alpha = 2$ generator mavjud (ya'ni, $\phi(25) = 20$ va $2^{20} \bmod 25 = 1$ bo'lgani bois).

Ta'rif 2.4.17. Faraz qilaylik $a \in \mathbb{Z}_n^*$ bo'lsin. Agar $x^2 \equiv a \pmod{n}$ shartni qanoatlantiruvchi $x \in \mathbb{Z}_n^*$ mavjud bo'lsa, u holda a element $\bmod n$ bo'yicha kvadratik qoldiq deb ataladi. Agar bunday x mavjud bo'lmasa, a element $\bmod n$ bo'yicha kvadratik bo'lmagan qoldiq deyiladi. $\bmod n$ bo'yicha barcha kvadratik qoldiqlar to'plami Q_n kabi, barcha kvadratik bo'lmagan qoldiqlar to'plamini esa $\overline{Q_n}$ kabi belgilaylik.

Izoh: $0 \notin \mathbb{Z}_n^*$ bo'lgani bois, $0 \notin Q_n$ va $0 \notin \overline{Q_n}$ o'rinli.

Qoida 2.4.24. Faraz qilaylik p soni toq tub son va \mathbb{Z}_p^* ning generatori α ga teng bo'lsin. U holda, faqat va faqat $a = \alpha^i \bmod p$ (bu yerda, i – juft butun son) bo'lsa, u holda $a \in \mathbb{Z}_p^*$ element $\bmod p$ bo'yicha kvadratik qoldiq bo'ladi. Bundan, $|Q_n| = (p - 1)/2$ va $|\overline{Q_n}| = (p - 1)/2$ ligini bilish mumkin. Boshqacha aytganda, \mathbb{Z}_p^* ning yarim elementi kvadratik qoldiqlar va yarmi esa kvadratik bo'lmagan qoldiqlar.

Masalan, \mathbb{Z}_{13}^* ning generatori $\alpha = 6$ ga teng. α ning darajalari quyidagi jadvalda keltirilgan:

| | | | | | | | | | | | | |
|---------------------|---|---|----|---|---|---|----|---|---|---|----|----|
| i | 0 | 1 | 2 | 3 | 4 | 5 | 6 | 7 | 8 | 9 | 10 | 11 |
| $\alpha^i \bmod 13$ | 1 | 6 | 10 | 8 | 9 | 2 | 12 | 7 | 3 | 5 | 4 | 11 |

Bundan, $Q_{13} = \{1, 3, 4, 9, 10, 12\}$ va $\overline{Q_{13}} = \{2, 5, 6, 7, 8, 11\}$ ga tengligini ko'rish mumkin.

Qoida 2.4.25. Faraz qilaylik, $n = pq$ soni ikkita toq tub sonlar, p va q larning ko'paytmasi bo'lsin. U holda, faqat va faqat $a \in Q_p$ va $a \in Q_q$ bo'lganida, $a \in \mathbb{Z}_n^*$ soni *mod* n bo'yicha kvadratik qoldiq bo'ladi. Bundan kelib chiqib, $|Q_n| = |Q_p| \cdot |Q_q| = (p - 1)(q - 1)/4$ va $|\overline{Q_n}| = 3(p - 1)(q - 1)/4$ tengliklarni yozish mumkin.

Masalan, faraz qilaylik $n = 21$. U holda, $Q_{21} = \{1, 4, 16\}$ va $\overline{Q_n} = \{2, 5, 8, 10, 11, 13, 17, 19, 20\}$ teng bo'ladi.

Ta'rif 2.4.18. Faraz qilaylik, $a \in Q_n$. Agar $x \in \mathbb{Z}_n^*$ son $x^2 \equiv a \pmod{n}$ shartni qanoatlantirsa, u holda x soni *mod* n bo'yicha kvadrat ildiz deb aytiladi.

Qoida 2.4.26. (kvadrat ildizlar soniga oid)

1) Agar p soni toq tub son va $a \in Q_p$ bo'lsa, u holda a soni *mod* p bo'yicha ikkita kvadrat ildizga ega bo'ladi.

2) Umumiy holda, faraz qilaylik $n = p_1^{e_1} p_2^{e_2} \dots p_k^{e_k}$. Bu yerda, p_i lar turli tub toq sonlar va $e_1 \geq 1$. Agar $a \in Q_n$ bo'lsa, u holda a soni *mod* n bo'yicha 2^k ta kvadrat ildizga ega bo'ladi.

Masalan, 12 ning *mod* 37 bo'yicha, kvadrat ildizlari 7 va 30 ga teng. Yoki, 121 ning *mod* 315 bo'yicha, kvadrat ildizlari 11, 74, 101, 151, 164, 214, 241 va 304 ga teng.

Modul bo'yicha amallar. Faraz qilaylik, n musbat butun son bo'lsin. Yuqorida aytilgani kabi, \mathbb{Z}_n ning elementlari $\{0, 1, 2, \dots, n - 1\}$ butun sonlaridan iborat bo'ladi.

Agar $a, b \in \mathbb{Z}_n$ bo'lsa, u holda

$$(a + b) \bmod n = \begin{cases} a + b, & \text{agar } a + b < n, \\ a + b - n, & \text{agar } a + b \geq n. \end{cases}$$

Modul bo'yicha qo'shish (yoki ayirish) amali yuqorida keltirilgan kabi ko'p hisoblashlarni talab etmaydi. Xuddi shunga o'xshash, modul bo'yicha a, b sonlarini ko'paytirish mumkin. Ya'ni, ikki son dastlab ko'paytiriladi va uni n ga bo'lishdan olingan qoldiq aniqlanadi. $a \in \mathbb{Z}_n$ sonning teskarisini hisoblashda esa, Evklidning kengaytirilgan algoritmidan foydalaniladi.

Algoritm 2.4.3. (\mathbb{Z}_n da sonni multiplikativ teskarisini hisoblash algoritmi).

KIRISH: $a \in \mathbb{Z}_n$.

CHIQUISH: mavjud bo'lish sharti bilan $a^{-1} \bmod n$.

1. Evklidning kengaytirilgan algoritmidan foydalanib, $ax + ny = d$ shartni qanoatlantiruvchi (bu yerda, $d = \gcd(a, n)$) x va y sonlar topilsin.
 2. Agar $d > 1$ bo'lsa, u holda $a^{-1} \bmod n$ mavjud emas. Aks holda x qaytarilsin.
-

Modul bo'yicha darajaga ko'tarishda quyida keltirilgan takroriy kvadratga oshirish va ko'paytirish algoritmidan foydalaniladi. Faraz qilaylik, k sonining binar ko'rinishi har bir $k_i \in \{0, 1\}$ uchun $\sum_{i=0}^t k_i 2^i$ ga teng bo'lsin. U holda,

$$a^k = \prod_{i=0}^t a^{k_i 2^i} = (a^{2^0})^{k_0} (a^{2^1})^{k_1} \dots (a^{2^t})^{k_t} \text{ ga teng bo'ladi.}$$

Algoritm 2.4.4. (\mathbb{Z}_n da takroriy kvadratga oshirish va ko'paytirishni hisoblash algoritmi).

KIRISH: $a \in \mathbb{Z}_n$ va butun $0 \leq k < n$ sonning binar ko'rinishi $k = \sum_{i=0}^t k_i 2^i$.

CHIQUISH: $a^k \bmod n$.

1. $b \leftarrow 1$ o'rnatilsin. Agar $k = 0$ bo'lsa, b qaytarilsin.
 2. $A \leftarrow a$ o'rnatilsin.
 3. Agar $k_0 = 1$ bo'lsa, $b \leftarrow a$ o'rnatilsin.
 4. $1 \leq i < t$ uchun quyidagilar bajarilsin:
 - 4.1. $A \leftarrow A^2 \bmod n$ o'rnatilsin.
 - 4.2. Agar $k_i = 1$ bo'lsa, u holda $b \leftarrow A \cdot b \bmod n$ o'rnatilsin.
 5. b qaytarilsin.
-

Masalan, quyida $5^{596} \bmod 1234 = 1013$ tenglikni batafsil yechimi keltirilgan.

| | | | | | | | | | | |
|-------|---|----|-----|-----|------|-----|------|------|------|------|
| i | 0 | 1 | 2 | 3 | 4 | 5 | 6 | 7 | 8 | 9 |
| k_i | 0 | 0 | 1 | 0 | 1 | 0 | 1 | 0 | 0 | 1 |
| A | 5 | 25 | 625 | 681 | 1011 | 369 | 421 | 779 | 947 | 925 |
| b | 1 | 1 | 625 | 625 | 67 | 67 | 1059 | 1059 | 1059 | 1013 |

\mathbb{Z}_n da fundamental amallar uchun bit sathidagi amallar soni 2.2-jadvalda aks ettirilgan.

2.2-jadval

\mathbb{Z}_n da fundamental amallar va ularning bitlar soni

| Amallar | Bit amallari soni |
|--|-------------------|
| Modul bo'yicha qo'shish: $(a + b) \bmod n$ | $O(\lg n)$ |
| Modul bo'yicha ayirish: $(a - b) \bmod n$ | $O(\lg n)$ |
| Modul bo'yicha ko'paytirish: $(a \cdot b) \bmod n$ | $O((\lg n)^2)$ |
| Modul bo'yicha teskarilash: $a^{-1} \bmod n$ | $O((\lg n)^2)$ |
| Modul bo'yicha darajaga oshirish: $a^k \bmod n, k < n$ | $O((\lg n)^3)$ |

Lejandr va Yakobi belgilari. Lejandr belgisi tub bo'lgan p soni bo'yicha modulda a sonini kvadratik qoldiq ekanligini aniqlashda foydalaniladi.

Ta'rif 2.4.19. Faraz qilaylik p toq tub son va a soni butun son bo'lsin. U holda Lejandr belgisi $\left(\frac{a}{p}\right)$ quyidagicha aniqlanadi:

$$\left(\frac{a}{p}\right) = \begin{cases} 0, & \text{agar } p|a \text{ bo'lsa,} \\ 1, & \text{agar } a \in Q_p \text{ bo'lsa,} \\ -1, & \text{agar } a \in \overline{Q}_p \text{ bo'lsa.} \end{cases}$$

Qoida 2.4.27. (Lejandr belgisining xususiyatlari). Faraz qilaylik, p toq tub son va $a, b \in \mathbb{Z}$ bo'lsin. U holda Lejandr belgisi quyidagi xususiyatlarga ega:

1) $\left(\frac{a}{p}\right) \equiv a^{\frac{p-1}{2}} \pmod{p}$. Xususan, $\left(\frac{1}{p}\right) = 1$ va $\left(\frac{-1}{p}\right) = (-1)^{(p-1)/2}$.
Shu sababli, agar $p \equiv 1 \pmod{4}$ bo'lsa, $-1 \in Q_p$ va agar $p \equiv 3 \pmod{4}$ bo'lsa, $-1 \in \overline{Q}_p$ bo'ladi.

2) $\left(\frac{ab}{p}\right) = \left(\frac{a}{p}\right) \left(\frac{b}{p}\right)$. Shu sababli, agar $a \in \mathbb{Z}_p^*$ bo'lsa, u holda $\left(\frac{a^2}{p}\right) = 1$ o'rinli.

3) Agar $a \equiv b \pmod{p}$ bo'lsa, u holda $\left(\frac{a}{p}\right) = \left(\frac{b}{p}\right)$ o'rinli bo'ladi.

4) $\left(\frac{2}{p}\right) = (-1)^{(p^2-1)/8}$. Shu sababli, agar $p \equiv 1$ yoki $7 \pmod{8}$ bo'lsa, $\left(\frac{2}{p}\right) = 1$ va agar $p \equiv 3$ yoki $5 \pmod{8}$ bo'lsa, $\left(\frac{2}{p}\right) = -1$ ga teng bo'ladi.

5) (kvadratik qoldiqlarning o'zaro bog'liqlik qonuni). Agar q soni p dan farqli toq tub son bo'lsa, u holda quyidagi o'rinli:

$$\left(\frac{p}{q}\right) = \left(\frac{q}{p}\right) (-1)^{(p-1)(q-1)/4}.$$

Boshqacha aytganda, p va q lar $3 \pmod{4}$ ga kongurent bo'lsa, $\left(\frac{p}{q}\right) = -\left(\frac{q}{p}\right)$, aks holda $\left(\frac{p}{q}\right) = \left(\frac{q}{p}\right)$ o'rinli bo'ladi.

Yakobi belgisi n butun son bo'lgandagi (ya'ni, n soni toq, biroq tub bo'lishi shart emas) Lejandr belgisining umumiy ko'rinishi hisoblanadi.

Ta'rif 2.4.20. Faraz qilaylik, $n \geq 3$ soni toq va asosi tub bo'lgan faktorlash $n = p_1^{e_1} p_2^{e_2} \dots p_k^{e_k}$ ko'rinishga ega bo'lsin. U holda Yakobi belgisi $\left(\frac{a}{n}\right) = \left(\frac{a}{p_1}\right)^{e_1} \left(\frac{a}{p_2}\right)^{e_2} \dots \left(\frac{a}{p_k}\right)^{e_k}$ ga teng bo'ladi. Agar n soni tub bo'lganida, Yakobi belgisi Lejandr belgisiga teng bo'ladi.

Qoida 2.4.28. (Yakobi belgisining xususiyatlari) Faraz qilaylik $m \geq 3$, $n \geq 3$ bo'lgan toq sonlar va $a, b \in \mathbb{Z}$ bo'lsin. U holda Yakobi belgisi quyidagi xususiyatlarga ega:

1) $\left(\frac{a}{n}\right) = 0, 1, \text{ yoki } -1$. Xususan, faqat va faqat $\gcd(a, n) \neq 1$ bo'lsa, $\left(\frac{a}{n}\right) = 0$ bo'ladi.

2) $\left(\frac{ab}{n}\right) = \left(\frac{a}{n}\right) \left(\frac{b}{n}\right)$. Shu sababli, agar $a \in \mathbb{Z}_n^*$ bo'lsa, u holda $\left(\frac{a^2}{n}\right) = 1$.

3) $\left(\frac{a}{mn}\right) = \left(\frac{a}{m}\right) \left(\frac{a}{n}\right)$.

4) Agar $a \equiv b \pmod{n}$ bo'lsa, u holda $\left(\frac{a}{n}\right) = \left(\frac{b}{n}\right)$.

5) $\left(\frac{1}{n}\right) = 1$.

6) $\left(\frac{-1}{n}\right) = (-1)^{(n-1)/2}$. Shu sababli, agar $n \equiv 1 \pmod{4}$ bo'lsa, $\left(\frac{-1}{n}\right) = 1$ va agar $n \equiv 3 \pmod{4}$ bo'lsa, $\left(\frac{-1}{n}\right) = -1$ ga teng.

7) $\left(\frac{2}{n}\right) = (-1)^{(n^2-1)/8}$. Shu sababli, agar $n \equiv 1$ yoki $7 \pmod{8}$ bo'lsa, $\left(\frac{2}{n}\right) = 1$ va agar $n \equiv 3$ yoki $5 \pmod{8}$ bo'lsa, $\left(\frac{2}{n}\right) = -1$ ga teng.

8) $\left(\frac{m}{n}\right) = \left(\frac{n}{m}\right) (-1)^{(m-1)(n-1)/4}$. Boshqacha aytganda, m va n lar $3 \pmod{4}$ ga kongurent bo'lsa, $\left(\frac{m}{n}\right) = -\left(\frac{n}{m}\right)$, aks holda $\left(\frac{m}{n}\right) = \left(\frac{n}{m}\right)$ o'rinli bo'ladi.

Yakobi belgisining xususiyatidan kelib chiqqan holda, agar n toq va $a = 2^e a_1$ bo'lsa (bu yerda, a_1 toq), u holda $\left(\frac{a}{n}\right) = \left(\frac{2^e}{n}\right) \left(\frac{a_1}{n}\right) = \left(\frac{2}{n}\right)^e \left(\frac{n \bmod a_1}{a_1}\right) (-1)^{(a_1-1)(n-1)/4}$ ga teng bo'ladi.

$\left(\frac{a}{n}\right)$ hisoblashning n sonini tub sonning darajasi shaklida ifodalamasdan, quyida keltirilgan rekursiv algoritm yordamida hisoblash mumkin.

Algoritm 2.4.5. (Yakobi (yoki Lejandr) belgisini hisoblash algoritmi).

$JACOBI(a, n)$

KIRISH: toq $n \geq 3$ butun son va a butun son ($0 \leq a < n$).

CHIQISH: Yakobi belgisi $\left(\frac{a}{n}\right)$ (agar n soni tub bo'lsa, Lejandr belgisi bo'ladi)

1. Agar $a = 0$ bo'lsa, 0 qaytarilsin.
2. Agar $a = 1$ bo'lsa, 1 qaytarilsin.
3. Tub bo'lgan a_1 uchun, $a = 2^e a_1$ shaklida yozilsin.
4. Agar e juft bo'lsa, u holda $s \leftarrow 1$ o'rnatilsin. Aks holda, agar $n \equiv 1$ yoki $7 \pmod{8}$ bo'lsa, $s \leftarrow 1$ yoki agar $n \equiv 3$ yoki $5 \pmod{8}$ bo'lsa, $s \leftarrow -1$ o'rnatilsin.
5. Agar $n \equiv 3 \pmod{4}$ va $a_1 \equiv 3 \pmod{4}$ bo'lsa, u holda $s \leftarrow -s$ o'rnatilsin.
6. $n_1 \leftarrow n \bmod a_1$.
7. Agar $a_1 = 2$ bo'lsa, u holda s qaytarilsin. Aks holda, $(s \cdot JACOBI(n_1, a_1))$ qaytarilsin.

Yuqorida keltirilgan algoritmning ishlash vaqti $O((\lg n)^2)$ bit amallari soniga teng.

Masalan, $a = 158$ va $n = 235$ uchun, 2.4.5-algoritm yordamida Yakobi belgisi $\left(\frac{158}{235}\right)$ ni hisoblash quyidagicha bo‘ladi:

$$\begin{aligned} \left(\frac{158}{235}\right) &= \left(\frac{2}{235}\right) \left(\frac{79}{235}\right) = (-1) \left(\frac{235}{79}\right) (-1)^{78 \cdot \frac{234}{4}} = \left(\frac{77}{79}\right) = \\ &= \left(\frac{79}{77}\right) (-1)^{76 \cdot 78/4} = \left(\frac{2}{77}\right) = -1. \end{aligned}$$

Lejandr belgisidan farqli ravishda Yakobi belgisi $\left(\frac{a}{n}\right)$ son a ni $\text{mod } n$ uchun kvadratik qoldiqligi yoki emasligini ko‘rsatmaydi.

Biroq, quyidagi jadvalda \mathbb{Z}_{21}^* maydon elementlari va ularning Yakobi belgilari keltirilgan. Yuqorida keltirilgan misolga keltirilgani kabi, $Q_{21} = \{1, 4, 16\}$ ga teng bo‘ladi. Kuzatish natijasida, $\left(\frac{5}{21}\right) = 1$, biroq $5 \notin Q_{21}$ ligini bilish mumkin.

| | | | | | | | | | | | | |
|-----------------------------|---|----|----|----|----|----|----|----|----|----|----|----|
| $a \in \mathbb{Z}_{21}^*$ | 1 | 2 | 4 | 5 | 8 | 10 | 11 | 13 | 16 | 17 | 19 | 20 |
| $a^2 \text{ mod } n$ | 1 | 4 | 16 | 4 | 1 | 16 | 16 | 1 | 4 | 16 | 4 | 1 |
| $\left(\frac{a}{3}\right)$ | 1 | -1 | 1 | -1 | -1 | 1 | -1 | 1 | 1 | -1 | 1 | -1 |
| $\left(\frac{a}{7}\right)$ | 1 | 1 | 1 | -1 | 1 | -1 | 1 | -1 | 1 | -1 | -1 | -1 |
| $\left(\frac{a}{21}\right)$ | 1 | -1 | 1 | 1 | -1 | -1 | -1 | -1 | 1 | 1 | -1 | 1 |

Blum butun sonlari. Blum soni har biri $3 \text{ mod } 4$ ga kongruent bo‘lgan turli p va q sonlarning ko‘paytmasi $n = pq$ ga teng.

Qoida 2.4.29. Faraz qilaylik $n = pq$ Blum soni va $a \in Q_n$ butun bo‘lsin. U holda a uchun aniq 4 ta son $\text{mod } n$ bo‘yicha kvadratik ildiz mavjud bo‘ladi va ulardan faqat bittasi Q_n ga tegishli bo‘ladi. Q_n dagi a ning kvadratik ildizi, *asosiy kvadratik ildiz* deb ataladi.

Masalan, $n = 21$ ga teng bo‘lgan Blum soni uchun, $J_n = \{1, 4, 5, 16, 17, 20\}$ va $\bar{Q}_n = \{5, 17, 20\}$. Bunda, a ning to‘rt kvadratik ildizi 2, 5, 16 va 19 bo‘lib, ulardan faqat 16 ga teng element Q_{21} ga tegishli. Shuning uchun, 16 ga teng bo‘lgan element $4 \text{ mod } 21$ ga asosiy kvadratik ildiz deb ataladi.

Qoida 2.4.30. Agar $n = pq$ Blum soni bo‘lsa, u holda $f(x) = x^2 \text{ mod } n$ ko‘rinishidagi $f: Q_n \rightarrow Q_n$ funksiya o‘rin almashtirishni

amalga oshiradi. f funksiyaning teskarisi $f^{-1}(x) = x^{((p-1)(q-1)+4)/8} \pmod n$ ga teng bo'ladi.

2.5. Fundamental algebra asoslari

Ta'rif 2.5.1. S to'plamda $*$ binar amali $S \times S$ dan S ga akslantirishni amalga oshiradi. Ya'ni, $*$ amali S dan elementlarning har bir talab qilingan jufti uchun S dan biror elementni belgilaydigan qoida.

Ta'rif 2.5.2. Guruh $(G, *)$ to'plam G bilan $*$ binar amaldan iborat bo'lib, G quyidagi 3 ta aksiomaga ega:

1) Guruh amali assotsiativ. Ya'ni, barcha $a, b, c \in G$ uchun $a * (b * c) = (a * b) * c$ tenglik o'rinli.

2) $1 \in G$ element mavjud bo'lib, u *birlik element* deb ataladi. Ya'ni, barcha $a \in G$ uchun $a * 1 = 1 * a = a$ tenglik o'rinli.

3) Har bir $a \in G$ element uchun a ning *teskarisi* deb ataluvchi $a^{-1} \in G$ element mavjud. Ya'ni, $a * a^{-1} = a^{-1} * a = 1$ tenglik o'rinli.

4) Agar guruh G barcha $a, b \in G$ lar uchun $a * b = b * a$ tenglikni qanoatlantirsa, u holda *kommunikativ* (yoki *abelev*) guruh deb ataladi.

Izoh.k. Izoh o'rnida shuni aytish lozimki, multiplikativ guruh belgisi faqat guruh amali sifatida foydalaniladi. Agar guruh amali qo'shish bo'lsa, u holda guruh qo'shishga asoslangan guruh deyiladi hamda birlik element 0 ga teng bo'lib, a ning teskarisi $-a$ kabi belgilanadi.

Ta'rif 2.5.3. Agar $|G|$ chekli bo'lsa, G to'plam *chekli* deb ataladi. Chekli guruhdagi elementlar soni uning *tartibi* deb ataladi.

Masalan, qo'shish amaliga ega butun sonlar to'plami \mathbb{Z} dan iborat guruh bo'lsin. Bunda, birlik element 0 ga va a elementning teskarisi $-a$ ga teng bo'ladi.

Bundan tashqari, $\pmod n$ bo'yicha qo'shish amaliga ega butun sonlar to'plami \mathbb{Z}_n dan iborat guruh bo'lsa, uning tartibi n ga teng bo'ladi. Yoki, $\pmod n$ bo'yicha ko'paytirish amali va butun sonlar to'plami \mathbb{Z}_n dan iborat guruh bo'la olmaydi. Buning sababi, har bir element uchun teskari elementni mavjud emasligi hisoblanadi. Biroq, \mathbb{Z}_n^* guruh bo'lib, multiplikativ $\pmod n$ uchun $\phi(n)$ tartibga ega va birlik elementi 1 ga teng.

Ta'rif 2.5.4. Agar H guruh bo'lib, G guruh amaliga bo'ysunsa, G guruhning bo'sh bo'lmagan qismto'plami H guruh G ning *qismguruhi* deb ataladi. Agar, H guruh G ning qismguruhi va $H \neq G$ bo'lsa, u holda H guruh G ning *xususiy qismguruhi* deb ataladi.

Ta'rif 2.5.5. Agar har bir $b \in G$ uchun butun son i bilan $b = \alpha^i$ shartni qanoatlantiruvchi $\alpha \in G$ element mavjud bo'lsa, u holda G guruh siklik deb ataladi. α element esa G guruhning *generatori* deb ataladi.

Qoida 2.5.1. Agar G guruh va $\alpha \in G$ bo'lsa, u holda a ning barcha darajalari to'plami G ning siklik qismguruhlarini shakllantiradi va ular a tomonidan generatsiya qilingan qismguruhlar deb atalib, $\langle a \rangle$ shaklida belgilanadi.

Ta'rif 2.5.6. G guruh va $a \in G$ bo'lsin. α ning tartibi $a^t = 1$ shartni qanoatlantiruvchi eng kichik musbat t bilan belgilanadi. Agar bunday t mavjud bo'lmasa, α ning tartibi ∞ kabi belgilanadi.

Qoida 2.5.2. G guruh va $a \in G$ element chekli t tartibga ega bo'lsin. U holda $|\langle a \rangle|$, a tomonidan generatsiya qilingan qismguruhlarini sonini ko'rsatib, t ga teng bo'ladi.

Qoida 2.5.3. (Lagranj teoremasi) Agar G chekli guruh va H uning qism guruhi bo'lsa, u holda $|H|$ qiymat $|G|$ qiymatni bo'luvchisi bo'ladi. Shu sababli, agar $a \in G$ bo'lsa, a ning tartibi $|G|$ qiymatni bo'luvchisi bo'ladi.

Qoida 2.5.4. Siklik guruh G ning har bir qism guruhi ham siklik bo'ladi. Agar G siklik guruh n tartibga ega bo'lsa, u holda n ning har bir musbat bo'luvchi d uchun, G guruh d tartibga ega bo'lgan aniq bir qismguruhdan tashkil topgan.

Qoida 2.5.5. Faraz qilaylik G guruh bo'lsin.

1) Agar $a \in G$ ning tartibi t ga teng bo'lsa, u holda a^k ning tartibi $\frac{t}{\gcd(t,k)}$ ga teng bo'ladi.

2) Agar G guruh n tartibga ega va $d|n$ bo'lsa, u holda G da d tartibli $\phi(d)$ ta elementlar mavjud.

Masalan, $\mathbb{Z}_{19}^* = \{1, 2, \dots, 18\}$ tartibi 18 ga teng bo'lgan multiplikativ guruh bo'lsin. Guruh siklik va $\alpha = 2$ generatorga ega. \mathbb{Z}_{19}^* ning qismguruhlari va uning generatorlari quyidagi jadvalda keltirilgan:

| Qism guruh | Generatorlar | Tartibi |
|--------------------------------|----------------------|---------|
| {1} | 1 | 1 |
| {1, 18} | 18 | 2 |
| {1, 7, 11} | 7, 11 | 3 |
| {1, 7, 8, 11, 12, 18} | 8, 12 | 6 |
| {1, 4, 5, 6, 7, 9, 11, 16, 17} | 4, 5, 6, 9, 16, 17 | 9 |
| {1, 2, 3, ..., 18} | 2, 3, 10, 13, 14, 15 | 18 |

Halqa

Ta'rif 2.5.7. Halqa $(R, +, \times)$ to'plam R va ikkita, qo'shish (+), ko'paytirish (\times) kabi binar amallardan iborat bo'lib, quyidagi aksiomalar o'rinli:

1. $(R, +, \times)$ – birlik elementi 0 ga teng bo'lgan kommutativ guruh.k.
2. \times - amali assotsiativ. Ya'ni, barcha $a, b, c \in R$ uchun $a \times (b \times c) = (a \times b) \times c$ tenglik o'rinli.
3. Multiplikativ 1 ga teng bo'lgan birlik element mavjud, ya'ni, barcha $a \in R$ uchun $1 \times a = a \times 1 = a$.
4. + amali uchun \times amali taqsimot qonuniyatiga ega, ya'ni, $a, b, c \in R$ uchun $a \times (b + c) = (a \times b) + (a \times c)$ va $(b + c) \times a = (b \times a) + (c \times a)$ tenglik o'rinli.

Agar halqada barcha $a, b \in R$ lar uchun $a \times b = b \times a$ tenglik o'rinli bo'lsa, u holda halqaga *kommutativ halqa* deb aytiladi.

Ta'rif 2.5.8. Agar $a \times b = 1$ shartni qanoatlantiruvchi $b \in R$ mavjud bo'lsa, u holda R xalqaning elementi a *birlik* yoki *teskarisi mavjud element* deb ataladi.

Qoida 2.5.6. R halqadagi birliklar to'plami multiplikativ guruhni tashkil qilib, R halqaning *birliklar guruhi* deb nomlanadi.

Masalan, \mathbb{Z}_n halqaning birliklar guruhi \mathbb{Z}_n^* ga teng.

Maydon

Ta'rif 2.5.9. Barcha noldan farqli elementlari multiplikativ teskrisiga ega bo'lgan kommutativ halqa *maydon* deyiladi.

Ta'rif 2.5.10. Agar ixtiyoriy $m \geq 1$ uchun $\overbrace{1 + 1 + \dots + 1}^{m \text{ marta}}$ tenglik hech qachon 0 ga teng bo'lmasa, u holda maydonning *xarakteristikasi* nol deyiladi. Aks holda, maydonning *xarakteristikasi* $\sum_{i=1}^m 1$ yig'indini nolga teng qiluvchi eng kichik musbat son m ga teng bo'ladi.

Masalan, odatiy qo'shish va ko'paytirish amallari uchun butun sonlar to'plami maydon bo'la olmaydi. Bu yerda, faqat, multiplikativ teskrisiga ega yagona noldan farqli sonlar 1 va -1 ga teng. Biroq, ratsional sonlar \mathbb{Q} , real sonlar \mathbb{R} va kompleks sonlar \mathbb{C} odatiy amallar uchun nol xarakteristikali maydonni shakllantiradi.

Qoida 2.5.7. Faqat va faqat n tub son bo'lsa, \mathbb{Z}_n (*mod n bo'yicha* qo'shish va ko'paytirish amallari uchun) maydon bo'ladi. Agar n tub bo'lsa, u holda \mathbb{Z}_n maydon n xarakteristikali maydon deyiladi.

Qoida 2.5.8. Agar maydonning m xarakteristikasi nolga teng bo'lmasa, u holda m – tub son.

Ta'rif 2.5.11. Agar E maydon amallari uchun F ham maydon bo'lsa, E maydonning qism to'plami bo'lgan F uning *qismto'plami* deb ataladi. Boshqacha aytganda, E maydon F maydonning *kengaytirilgani* deb ataladi.

Polinom halqalar

Ta'rif 2.5.12. Agar R halqa kommutativ bo'lsa, u holda R halqa ustida aniqlanmagan x tarkibli *polinom (ko'phad)* quyidagi shaklda ifodalanadi:

$$f(x) = a_n x^n + \dots + a_2 x^2 + a_1 x + a_0$$

Bu yerda, har bir $a_i \in R$ va $n \geq 0$. a_i element $f(x)$ dagi x^i ning koeffitsienti deyiladi. $a_m \neq 0$ shartdagi eng katta m butun soni $f(x)$ ning *darajasi* deyiladi va $\deg f(x)$ kabi belgilanadi; a_m ning o'zi esa $f(x)$ ning *yetakchi koeffitsienti* deyiladi. Agar $f(x) = a_0$ (o'zgarmas polinom) va $a_0 \neq 0$ bo'lsa, $f(x)$ polinom 0 darajaga ega deyiladi. Agar $f(x)$ ning barcha koeffitsientlari nolga teng bo'lsa, u holda *nol polinom* deyiladi va uning darajasi $-\infty$ kabi belgilanadi. Agar $f(x)$ polinomning yetakchi koeffitsienti birga teng bo'lsa, u *birlik (yoki monik) polinom* deyiladi.

Ta'rif 2.5.13. Agar R halqa kommutativ bo'lsa, $R[x]$ *polinom halqa* R dan olingan koeffitsientlarga ega aniqlanmagan x tarkibli barcha polinomlar to'plami orqali ifodalanuvchi halqadir. Polinom ustida bajariluvchi ikki amal esa standart qo'shish va ko'paytirish amali bo'lib, R halqada koeffitsientlar bilan bajariladi.

Masalan, faraz qilaylik, $f(x) = x^3 + x + 1$ va $g(x) = x^2 + x$ lar $\mathbb{Z}_2[x]$ polinom halqa elementlari bo'lsin. U holda, ularning yig'indisi va ko'paytmasi quyidagilarga teng bo'ladi:

$$\begin{aligned} f(x) + g(x) &= x^3 + x^2 + 1 \text{ va} \\ f(x) \cdot g(x) &= x^5 + x^4 + x^3 + x \end{aligned}$$

Mazkur bo'limning qolgan qismi uchun, F ni o'zgaruvchan maydon sifatida qaraymiz. $F[x]$ polinom xalqa butun sonlar bilan umumiy bo'lgan ko'plab xususiyatlarga ega.

Ta'rif 2.5.14. Faraz qilaylik, $f(x) \in F[x]$ darajasi kamida 1 bo'lgan polinom bo'lsin. U holda $f(x)$ polinom F bo'ylab *qisqartirilmaydigan*

deyiladi, agar uni har birining darajasi musbat bo'lgan $F[x]$ dagi ikki polinomlarning ko'paytmasi shaklida ifodalashning imkoni bo'lmasa.

Ta'rif 2.5.15. (Polinomlar uchun bo'lish algoritmi) Agar $g(x)$, $h(x) \in F[x]$ va $h(x) \neq 0$ bo'lsa, u holda $g(x)$ ni $h(x)$ ga bo'lish natijasida bir-biriga teng bo'lmagan $F[x]$ dagi $q(x)$ va $r(x)$ polinomlar paydo bo'ladi:

$$g(x) = q(x)h(x) + r(x)$$

Bu yerda, $\deg r(x) < \deg h(x)$ shart o'rinli. Bu yerda, $q(x)$ polinom *bo'linma* va $r(x)$ polinom *qoldiq* deb ataladi. Qoldiq odatda $g(x) \bmod h(x)$ kabi belgilansa, bo'linma esa $g(x) \operatorname{div} h(x)$ kabi belgilanadi.

Masalan, $\mathbb{Z}_2[x]$ maydonda $g(x) = x^6 + x^5 + x^3 + x^2 + x + 1$ va $h(x) = x^4 + x^3 + 1$ polinomlar bo'lsin. $g(x)$ polinomni $h(x)$ ga bo'lish quyidagicha amalga oshiriladi:

$$g(x) = x^2h(x) + (x^3 + x + 1).$$

Shuning uchun, $g(x) \bmod h(x) = x^3 + x + 1$ va $g(x) \operatorname{div} h(x) = x^2$ ga teng.

Ta'rif 2.5.16. Agar $g(x)$, $h(x) \in F[x]$ va $g(x) \bmod h(x) = 0$ bo'lsa, u holda $h(x)$ polinom $g(x)$ ni bo'ladi va $h(x) | g(x)$ kabi yoziladi.

Faraz qilaylik, $f(x)$ polinom $F[x]$ dagi o'zgarmas polinom bo'lsin.

Ta'rif 2.5.17. Agar $g(x)$, $h(x) \in F[x]$ va $f(x)$ polinom $g(x) - h(x)$ ning bo'luvchisi bo'lsa, u holda $g(x)$ polinom $h(x) \bmod f(x)$ ga *kongurent* deb ataladi hamda $g(x) \equiv h(x) \bmod f(x)$ shaklida ifodalanadi.

Qoida 2.5.9. (Kongurentlik xususiyatlari) Barcha $g(x)$, $h(x)$, $g_1(x)$, $h_1(x)$, $s(x) \in F[x]$ lar uchun quyidagilar o'rinli:

1) Agar, faqat va faqat $g(x)$ va $h(x)$ larni $f(x)$ ga bo'lganda, bir xil qoldiq bo'lsa, $g(x) \equiv h(x) \bmod f(x)$ o'rinli bo'ladi.

2) (*refleksivlik*) $g(x) \equiv g(x) \bmod f(x)$.

3) (*simmetriklik*) Agar $g(x) \equiv h(x) \bmod f(x)$ bo'lsa, u holda $h(x) \equiv g(x) \bmod f(x)$.

4) (*tranzitivlik*) Agar $g(x) \equiv h(x) \bmod f(x)$ va $h(x) \equiv s(x) \bmod f(x)$ bo'lsa, u holda $g(x) \equiv s(x) \bmod f(x)$ o'rinli bo'ladi.

5) Agar $g(x) \equiv g_1(x) \pmod{f(x)}$ va $h(x) \equiv h_1(x) \pmod{f(x)}$ bo'lsa, u holda $g(x) + h(x) \equiv g_1(x) + h_1(x) \pmod{f(x)}$ va $g(x)h(x) \equiv g_1(x)h_1(x) \pmod{f(x)}$ o'rinli bo'ladi.

Ta'rif 2.5.18. $F[x]$ dagi $n = \deg f(x)$ dan kichik darajali polinomlar to'plami $F[x]/(f(x))$ kabi belgilanadi. Qo'shish va ko'paytirish $f(x)$ polinom bo'yicha amalga oshiriladi.

Qoida 2.5.10. $F[x]/(f(x))$ – kommutativ halqa.

Qoida 2.5.11. F bo'ylab $f(x)$ qisqarmas bo'lsa, u holda $F[x]/(f(x))$ maydon.

Vektor fazosi

Ta'rif 2.5.19. F maydoni bo'ylab *vektor fazosi* V kommunikativ guruh $(V, +)$ bo'lib, ko'paytirish amalini madadlaydi: $F \times V \rightarrow V$ hamda $a, b \in F$ va $v, w \in V$ uchun quyidagi aksiomalar o'rinli:

$$1) a(v + w) = av + aw.$$

$$2) (a + b)v = av + bv.$$

$$3) (ab)v = a(bv).$$

$$4) iv = v.$$

V ning elementlari *chektorlar*, F ning elementlari skalyarlar deyiladi. Guruh amali $+$ *vektorli qo'shish*, ko'paytirish amali *skalyarga ko'paytirish* deb ataladi.

Ta'rif 2.5.20. Faraz qilaylik V maydon F bo'ylab vektor fazosi bo'lsin. V ning *qism fazosi* qo'shish amali uchun qism gruppaga U ga teng bo'lib, skalyar ko'paytirishga yaqin, ya'ni: barcha $a \in F$ va $v \in U$ uchun $av \in U$.

Qoida 2.5.12. Vektor fazosining qism fazosi ham vektor fazosi bo'ladi.

Ta'rif 2.5.21. Faraz qilaylik F maydon bo'ylab vektor fazosi V ning chekli qism to'plami $S = \{v_1, v_2, \dots, v_n\}$ bo'lsin.

1) Har bir $a_i \in F$ uchun S ning *chiziqli kombinatsiyasi* quyidagicha ifodalanadi: $a_1v_1 + a_2v_2 + \dots + a_nv_n$.

2) S ning *qobig'i* (*span, оболочка*) $\langle S \rangle$ kabi belgilanib, S ning barcha chiziqli kombinatsiyalari to'plami hisoblanadi. S ning *qobig'i* V ning qism fazosi bo'ladi.

3) Agar V ning qism fazosi U bo'lsa, u holda agar $\langle S \rangle = U$ bo'lsa, S to'plam U ni qamrab oladi deyiladi.

4) Agar $a_1v_1 + a_2v_2 + \dots + a_nv_n = 0$ shartni qanoatlantiruvchi, barchasi nol bo'lmagan a_1, a_2, \dots, a_n skalyarlar mavjud bo'lsa, u holda S to'plam F bo'ylab *chiziqli bog'liq* deb ataladi.

Agar bunday skalyarlar mavjud bo'lsa, u holda holda S to'plam F bo'ylab *chiziqli bog'liq emas* deb ataladi.

5) Chiziqli bog'liq bo'lmagan vektorlar to'plami, ya'ni, V ning qobig'i V uchun *asos (basis)* deb ataladi.

Qoida 2.5.13. Faraz qilaylik, V vektor fazosi bo'lsin.

1) Agar V da chekli qobiq to'plam mavjud bo'lsa, u holda unda *basis* mavjud bo'ladi.

2) Agar V da *basis* mavjud bo'lsa, u holda barcha *basis*lar teng sonli elementlarga ega bo'ladi.

Ta'rif 2.5.22. Agar V vektor fazosida *basis* mavjud bo'lsa, u holda *basis*dagi elementlar soni V ning *o'lchovi* deyiladi va $\dim V$ kabi belgilanadi.

Ta'rif 2.5.23. Faraz qilaylik, F ning kengaytirilgan maydoni E bo'lsin. U holda E qism maydon F bo'ylab, vektor fazosi sifatida ko'rinadi. Bu yerda vektorni qo'shish va skalyarga ko'paytirish E dagi sodda maydon amallari, qo'shish va ko'paytirishdir. Vektor fazosining o'lchami F bo'ylab E ning *darajasi* deb ataladi va $[E:F]$ kabi belgilanadi. Agar daraja chekli bo'lsa, u holda E maydon F ning *chekli kengaytirilgani* deb ataladi.

Qoida 2.5.14. Faraz qilaylik, F , E va L maydonlar bo'lsin. Agar E ning chekli kengaytirilgani L va F ning chekli kengaytirilgani E bo'lsa, u holda L maydon F ning ham chekli kengaytirilgani bo'ladi:

$$[L:F] = [L:E][E:F].$$

Chekli maydon

Ta'rif 2.5.24. Chekli sondagi elementlardan iborat F maydonga *chekli maydon* deb aytiladi. F maydonning *tartibi* undagi elementlar soni bilan belgilanadi.

Qoida 2.5.15. (chekli maydonning mavjudligi va unikalligi haqida)

1) Agar F chekli maydon bo'lsa, u holda biror p tub va $m \geq 1$ butun son uchun F maydon p^m elementdan iborat.

2) Har bir p^m uchun, tartibi p^m bo'lgan unikal chekli maydon mavjud. Bu maydon F_{p^m} kabi yoki ba'zida $GF(p^m)$ kabi belgilanadi.

Boshqacha aytganda, ikki maydon bir xil tuzilishga ega bo'lsa (biroq, maydon elementlarini taqdim etilishi turlicha), ular *izomorfik* deb ataladi. Masalan, agar p soni tub bo'lsa, \mathbb{Z}_p maydon bo'ladi va shuning uchun p tartibdagi har bir maydon \mathbb{Z}_p ga izomorf bo'ladi. Boshqa shartlar

mavjud bo'lmaganda, F_p chekli maydonni \mathbb{Z}_p orqali anglash ham mumkin.

Qoida 2.5.16. Agar F_q chekli maydon tartibi $q = p^m$ ga teng va p tub bo'lsa, u holda F_q ning xarakteristikasi p ga teng bo'ladi. Bundan tashqari, F_q qism maydon sifatida \mathbb{Z}_p nusxasidan tashkil topgan. Shuning uchun, F_q chekli maydonga darajasi m bo'lgan \mathbb{Z}_p maydonning kengaytirilgani kabi qarash mumkin.

Qoida 2.5.17. (chekli maydonning qism maydonlari) Faraz qilaylik, F_q chekli maydon tartibi $q = p^m$ ga teng bo'lsin. U holda F_q ning har bir qism maydoni p^n tartibga ega (bu yerda, n soni m ning musbat bo'luvchisi). Aksincha, agar n soni m ning musbat bo'luvchisi bo'lsa, u holda aniq p^n tartibga ega F_q ning qism maydoni mavjud; faqat va faqat $a^{p^n} = a$ bo'lsa, $a \in F_q$ element F_{p^n} qism maydonda ham mavjud bo'ladi.

Ta'rif 2.5.25. F_q ning noldan farqli elementlari ko'paytirish amali bilan F_q ning *multiplikativ guruhini* shakllantiradi va F_q^* kabi belgilanadi.

Qoida 2.5.18. F_q^* tartibi $q - 1$ ga teng bo'lgan siklik guruh.k. Shuning uchun barcha $a \in F_q$ lar uchun $a^q = a$ o'rinli.

Ta'rif 2.5.26. Siklik guruh F_q^* ning generatori *asos element* yoki F_q ning generatori deb ataladi.

Qoida 2.5.19. Agar $a, b \in F_q$ bo'lsa, p esa chekli maydon xarakteristikasi bo'lsa, u holda barcha $t \geq 0$ lar uchun quyidagi o'rinli bo'ladi:

$$(a + b)^{p^t} = a^{p^t} + b^{p^t}.$$

Nazorat savollari

1. Funksiyaning aniqlanish va qiymatlar sohasiga ta'rif bering.
2. Injektiv, surjektiv, bijektiv funksiyalarga ta'rif bering.
3. Ehtimollik tushunchasi va uning turlari.
4. Shartli ehtimollik uchun Bayes teoremasi.
5. Binomial taqsimot va uning mohiyati.
6. Tug'ilgan kun muammosini tushuntiring.
7. Entropiyaga ta'rif bering. Entropiyaning turlari.
8. Algoritm ishlashining eng yomon vaqti tushunchasiga ta'rif bering.

9. Katta O belgilanishi va uning mohiyati.
10. Ω belgilanish va uning mohiyati.
11. Θ belgilanish va uning mohiyati.
12. EKUBga ta'rif bering. Uni hisoblash usullarini ayting.
13. EKUKga ta'rif bering. Uni hisoblash usullarini ayting.
14. Tub son, murakkab son va o'zaro tub soni tushunchalariga ta'rif bering.
15. Eylerning φ (phi) funksiyasi va uning matematik ma'nosi.
16. Kengaytirilgan Evklid algoritmini tushuntiring.
17. Modul arifmetikasi va uning xususiyatlari.
18. Qoldiqlar haqida Xitoy teoremasining mohiyatini tushuntiring.
19. Eyer teoremasi mohiyatini tushuntiring.
20. Lejandr va Yakobi belgilarini ma'nosini tushuntiring.

3 BOB. KLASSIK SHIFRLASH ALGORITMLARI

Mazkur bo‘limda hozirgi zamonaviy kriptotizimlarga aloqador bo‘lgan turli klassik shifrlar bilan tanishib chiqiladi.

3.1. Sodda o‘rniga qo‘yish va o‘rin almashtirish shifrlari

O‘rniga qo‘yishga asoslangan ko‘plab shifrlar mavjud bo‘lib, oddiy holda ochiq matn belgisini uning alfavitdagi o‘rnini n taga siljitishdan hosil bo‘lgan belgiga almashtirish orqali xabarni shifrlash usulini qarab chiqsak. Masalan, $n = 3$, o‘rniga qo‘yish akslantirishi kalit sifatida xizmat qiladi:

Ochiq matn: a b c d e f g h i j k l m n o p q r s t u v w x y z
Shifrmtn: D E F G H I J K L M N O P Q R S T U V W X Y Z A B C

Shartli holatda, ochiq matnni kichik harflarda va shifrmtnni katta harflarda ifodalandi. Bu yerda, kalitni “3” ga teng qarash mumkin. Chunki, mazkur holda siljish soni aslida kalit hisoblanadi.

“3” ga teng bo‘lgan kalit bilan quyidagi ochiq matnni shifrlash uchun yuqoridagi jadvaldan foydalaniladi.

“simple substitution cipher”

Ochiq matn belgilari jadvaldagi birinchi satrdan topilib, unga mos shifr matn belgilari pastki satrdan olinadi. Boshqacha aytganda, shifrmtn belgilarini hosil qilish uchun ochiq matn belgilari o‘nga 3 belgiga siljiriladi. Natijaviy shifr matn ko‘rinishi esa quyidagicha bo‘ladi:

“VLPSOHVXE VWLWXWXL RQFLSKHU”

Rasshivrovkalashda, shifrmtn belgilari yuqoridagi jadvalning ikkinchi satridan olinib, unga mos ochiq matn belgilari esa birinchi satrdan olinadi. Boshqacha aytganda, rasshivrovkalash uchun shifrmtn belgilari chapga uch belgiga siljiriladi. Ushbu siljitishga asoslangan sodda o‘rniga qo‘yish usuli Sezar shifri deb ataladi.

Kalit sifatida faqat 3 emas, ixtiyoriy musbat butun son bo‘lishi mumkin. Alfavitning uzunligini 25 ga tengligini inobatga olib, bo‘lishi mumkin bo‘lgan kalitlarni $n \in \{0, 1, 2, \dots, 25\}$ ligini bilish qiyin emas.

Faraz qilaylik, buzgʻunchi shifratn, “amkzmbumaaiom”ni, tutib oldi. Shundan soʻng, agar sodda oʻrniga qoʻyish usulidan foydalanilganini bilsa, u holda 26 ta kalitlarni barchasini sinab koʻradi va ochiq matnni biror maʼnoli soʻzni anglatishini tekshirib koʻradi. Agar shifr haqiqatda siljitishga asoslangan boʻlsa, ochiq matnni topish uchun oʻrtacha 13 ta urinishni amalga oshirishi talab etiladi.

Buzgʻunchi tomonidan koʻrsatilgan sondagi urinishlarni amalga oshirish “qoʻpol kuch hujumi” (Brute force attack) deb ataladi. Mazkur hujum mos kalitni topish va xabarni aniqlash uchun yetarlicha koʻp vaqt va hisoblash resursini talab qiladi. Boshqacha aytganda, mazkur hujumda kalitning boʻlishi mumkin boʻlgan barcha variantlari tekshirib chiqiladi.

Mazkur hujumga qarshi bardoshlilikni taʼminlashda kalitni uzunligini toʻgʻri tanlash muhim hisoblanadi. Faraz qilaylik, buzgʻunchida sekundiga 2^{40} ta kalitni testdan oʻtkazuvchi kompyuter (yoki kompyuterlar guruhi) mavjud boʻlsin. U holda 2^{56} (yoki 56 bitli kalitning barcha variantlari) ga teng kalit sohasini testlashda 2^{16} sekund yoki 18 soatga yaqin vaqt talab etilsa, 2^{64} ga teng kalit sohasi uchun yarim yildan koʻproq vaqt va 2^{128} ga teng kalit sohasi uchun $9 * 10^{30}$ dan ortiq yil talab etiladi. Shuning uchun hozirgi zamonaviy simmetrik kriptografik tizimlarda kalit uzunligi kamida 128 bit boʻlishi talab etiladi.

Yuqoridagi misolda kalit sifatida siljishlar soni olingani va alfavit uzunligining kichikligi bois kalit qisqa vaqtda aniqlangan. Mazkur holda kalit sifatida siljishlar sonining oʻrniga 26 ta belgilarning ixtiyoriy almashinishini olish mumkin. Masalan, quyida keltirilgan alfavitni siljitishga asoslanmagan, almashtirish tartibi kalit sifatida xizmat qilishi mumkin:

Ochiq matn: a b c d e f g h i j k l m n o p q r s t u v w x y z
Shifratn: Z P B Y J R G K F L X Q N W V D H M S U T O I A E C

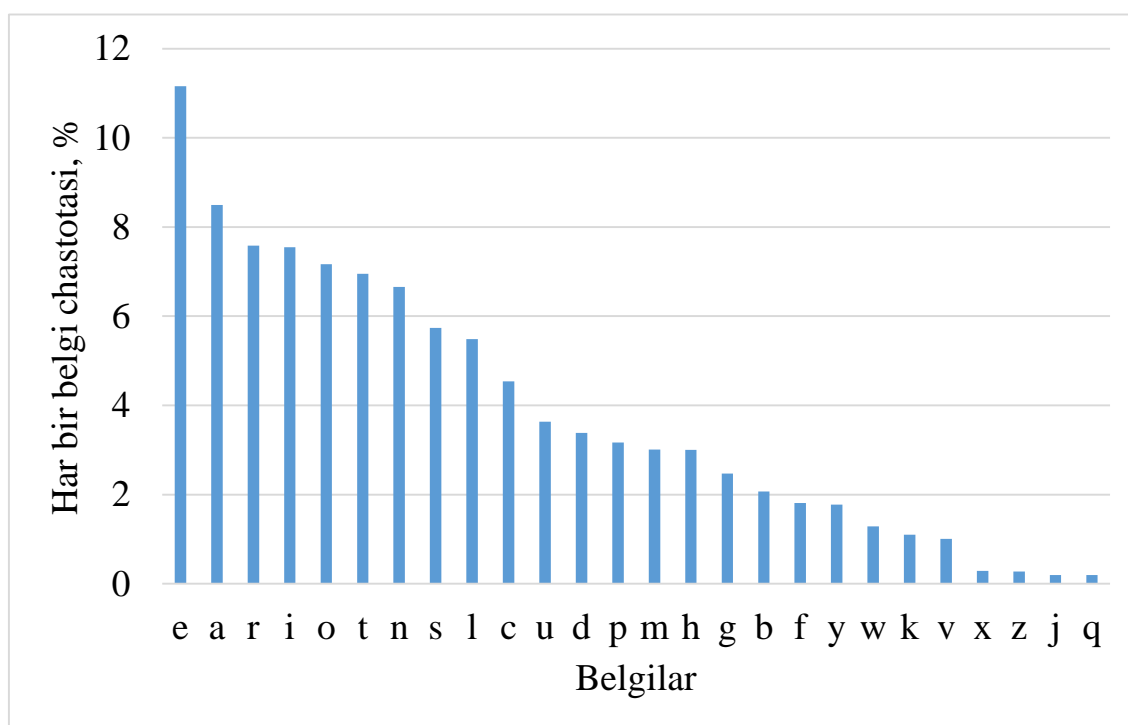
Umumiy holda alfavitni ixtiyoriy almashtirish kalit sifatida xizmat qilishi mumkin va bunda $26! \approx 2^{88}$ ta turli kalitlar boʻlishi mumkin. Mazkur kalit sohasini barcha variantlarini aniqlash uchun yuqorida keltirilgan buzgʻunchi kompyuteri 8,9 million yildan ortiq vaqt talab qiladi.

Sodda o‘rniga qo‘yish shifrlarining kriptotahlili

Faraz qilaylik, buzg‘unchi tomonidan quyidagi shifrmtn tutib olingan. Bundan tashqari, buzg‘unchi shifrmtnni sodda o‘rniga qo‘yish usuli asosida hosil qilinganini va kalit sifatida alfavitning ixtiyoriy o‘rin almashtirish holati bo‘lishi mumkinligini biladi.

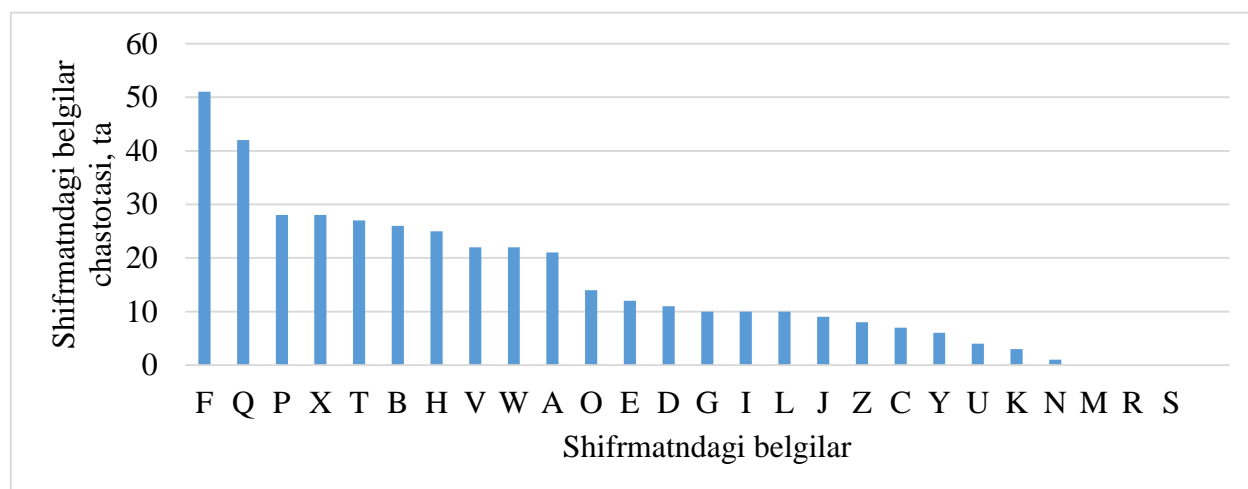
PBFPVYFBQXZTYFPBFEQJHDXXQVAPTPQJKTOYQWIPBWLXTOXBTFXCQWA
XBVCXQWAXFQJWLEQNTQZQGGQLFXQWAKVWLXQWAEBIPBFXFQVXGTVJV
WLBTPQWAEFBFBFHCVLXBQUFEWLXGDPEQVPQGVPPBFTIXPFHXZHVFAG
FOTHFEFBQUFTDHZBQPOTHXTYFTODXQHFTDPTOGHFQPBQWAQJJTODXQH
FOQPWTBDHHIXQVAPBFZQHCFWPFHPBFIPBQWKFABVYYDZBOTHBPBQPQT
QOTOGHFQAPBFEQJHDXXQVAVXEBQPEFZBVFOJIWFFACCFCHQWAUVWFL
QHGFVAVFXQHUFHILTTAVWAFFAWTEVDITDHFHFQAITIXPFHXAFQHEFZ
QWGFLVWPTOFFA

Mazkur holda bo‘lishi mumkin bo‘lgan 2^{88} kalitlarni tekshirib ko‘rish usuli samarasiz hisoblanadi. Faraz qilaylik, Ingliz alfavitidan foydalanilgan bo‘lsin. Boshqa tomondan tajriba o‘tkazish orqali Ingliz tili uchun harflarni so‘zlarda paydo bo‘lish chastotasini aniqlash mumkin (buni Internet tarmog‘i orqali osonlik bilan topish ham mumkin). Quyidagi 3.1-rasmda Concise Oxford Dictionary (9-nashr, 1995 yil) manbasida Ingliz alfavitidagi belgilarning takrorlanish chastotalari keltirilgan.



3.1-rasm. Ingliz alfavitidagi belgilarning takrorlanish chastotalari

Shunga o‘xshash yuqorida keltirilgan shifratndagi belgilarning chastotalarini ham osonlik bilan hisoblash mumkin. Hisoblashdan olingan natijalar 3.2-rasmda keltirilgan.



3.2-rasm. Shifratndagi belgilar va ularning chastotasi

3.2-rasmda keltirilgan shifratndagi belgilar chastotasidan ko‘rish mumkinki, “F” harfi shifratnda eng ko‘p qatnashgan va u 3.1-rasmda keltirilgan Ingliz alfavitida eng yuqori chastotaga ega bo‘lgan “E” harfiga mos keladi. Shu sababli, buzg‘unchi shifratndagi “F” harfining o‘rniga “E” harfini qo‘yadi. Shu tartibda, biror ma’noli so‘z hosil bo‘lgunga qadar almashtirish amalga oshiriladi. Mazkur kriptotahlil usuli kalitning barcha variantlarini sinab ko‘rishga qaraganda samarali hisoblanadi.

Sodda o‘rin almashtirish shifri

Mazkur qismda sodda o‘rin almashtirish akslantirishi hisoblangan – klassik ikki tomonlama o‘rin almashtirish usuli bilan tanishib chiqiladi. Ushbu shifrlash usulida ochiq matn dastlab berilgan o‘lchamdagi ikki o‘lchovli massivga yoziladi. Shifrlash uchun satrlar va ustunlarning o‘rni biror kalitga ko‘ra almashtiriladi. Masalan, “ochiqmatnlar” ochiq matnini 3×4 o‘lchamli massivga quyidagicha yozaylik:

$$\begin{bmatrix} o & c & h & i \\ q & m & a & t \\ n & l & a & r \end{bmatrix}$$

Shundan so‘ng, satrlarni $(1,2,3) \rightarrow (3,2,1)$ tartibda va ustunlarni esa $(1,2,3,4) \rightarrow (4,2,1,3)$ tartibda almashtirish natijasida quyidagilarni olish mumkin:

$$\begin{bmatrix} o & c & h & i \\ q & m & a & t \\ n & l & a & r \end{bmatrix} \rightarrow \begin{bmatrix} n & l & a & r \\ q & m & a & t \\ o & c & h & i \end{bmatrix} \rightarrow \begin{bmatrix} r & l & n & a \\ t & m & q & a \\ i & c & o & h \end{bmatrix}$$

Yuqoridagilardan kelib chiqib, shifmatni “RLNATMQAICOH” ga tengligini bilish mumkin. Mazkur holda shifrlash kaliti sifatida massivning o‘lchami hamda satrlar va ustunlarni almashtirish tartibi xizmat qiladi.

Rasshifrovkalash uchun esa shifmatn dastlab 3×4 massiv shaklida ifodalanadi. Shundan so‘ng, ustunlar (4,2,1,3) tarzida raqamlanib, (1,2,3,4) tartibida qaytadan tartiblanadi. Xuddi shunga o‘xshash, satrlar (3,2,1) tarzida raqamlanib, (1,2,3) tartibida qaytadan tartiblanadi:

$$\begin{bmatrix} R & L & N & A \\ T & M & Q & A \\ I & C & O & H \end{bmatrix} \rightarrow \begin{bmatrix} N & L & A & R \\ Q & M & A & T \\ O & C & H & I \end{bmatrix} \rightarrow \begin{bmatrix} O & C & H & I \\ Q & M & A & T \\ N & L & A & R \end{bmatrix}$$

Oxirgi massiv ko‘rinishidan esa, ochiq matnni “ochiqmatnlar” ga tengligini bilish mumkin. Mazkur shifrlash usuli o‘rniga qo‘yishga asoslangan usullarga nisbatan afzallik va kamchiliklarga ega. Masalan, ochiq matn va shifmatnda bir xil belgilarning bo‘lishi uning kamchiligi hisoblansa, ochiq matnga oid statistik ma’lumotlarga asoslangan kriptotahlil usullariga (masalan, chastotalar bo‘yicha tahlil) bardoshligi uning afzalligi hisoblanadi.

3.2. Vernam shifri

Bir martali bloknot (one time pad) yoki “Vernam shifri” nomi bilan tanilgan kriptotizim *bardoshli* shifrlash algoritmi hisoblanib, tarixda keng foydalanilgan bo‘lsada, ko‘p hollarda amalga oshirishning imkoniyati mavjud bo‘lmagan. Uning bir martali deb atalishiga asosiy sabab, undagi *kalitning (bloknotning)* bir marta foydalanilishi bo‘lib, uni aksariyat hollarda amalga oshirishning imkoni bo‘lmaydi. Masalan, ushbu shifrlash algoritmini tushuntirish uchun 8 ta simvoldan iborat bo‘lgan alfavitni olaylik. Olingan alfavit simvollarini va unga mos bo‘lgan binar qiymatlar 3.1 - jadvalda keltirilgan. Alifbo simvollarini va ularga mos

bit qiymatlari barcha uchun ochiq va sir saqlanmaydi (ASCII jadvali kabi).

3.1-jadval

Alfavit simvollari va unga mos bo‘lgan binar qiymatlar

| Belgilar | B | E | I | L | O | P | S | T |
|--------------|-----|-----|-----|-----|-----|-----|-----|-----|
| Binar qiymat | 000 | 001 | 010 | 011 | 100 | 101 | 110 | 111 |

Faraz qilaylik, biror qonuniy foydalanuvchi A bir martali bloknotdan foydalangan holda “POSSIBLE” matnini shifrlab, o‘z sherigi B tomonga jo‘natishi talab etilsin. Ushbu ochiq matnni binar qiymatdagi ko‘rinishi quyidagicha bo‘ladi:

| | | | | | | | |
|-----|-----|-----|-----|-----|-----|-----|-----|
| P | O | S | S | I | B | L | E |
| 101 | 100 | 110 | 110 | 010 | 000 | 011 | 001 |

Bir martali bloknot usulida shifrlashda ochiq matn uzunligiga teng bo‘lgan tasodifiy tanlangan kalitdan foydalaniladi. Ochiq matnga kalitni XOR amali orqali shifrmatn hosil qilinadi (R – ochiq matn, K – kalit va C – shifrmatn deb belgilansa): $C = P \oplus K$. XOR amali (\oplus) binar amal hisoblanib, quyida keltirilgan:

| |
|------------------|
| $0 \oplus 0 = 0$ |
| $0 \oplus 1 = 1$ |
| $1 \oplus 0 = 1$ |
| $1 \oplus 1 = 0$ |

Jadvaldan, $x \oplus y \oplus y = x$ tenglik o‘rinligini ko‘ramiz. Shuning uchun bir martali parol bilan rasshifrovkalash uchun shifrmatnga kalitni XOR amalida bajarilishining o‘zi yetarli hisoblanadi: $P = C \oplus K$.

Faraz qilaylik, A tomon jadvaldagi ochiq matn uzunligiga teng bo‘lgan quyidagi kalitga ega bo‘lsin:

111 101 110 101 111 100 000 101

A tomon ushbu kalit asosida shifrmatnni quyidagicha hisoblaydi:

| | | | | | | | | |
|-------------|-----|-----|-----|-----|-----|-----|-----|-----|
| | P | O | S | S | I | B | L | E |
| Ochiq matn: | 101 | 100 | 110 | 110 | 010 | 000 | 011 | 001 |
| Kalit: | 111 | 101 | 110 | 101 | 111 | 100 | 000 | 101 |
| Shifrmavn: | 010 | 001 | 000 | 011 | 101 | 100 | 011 | 100 |
| | I | E | B | L | P | O | L | O |

A tomonidan jo‘natilgan shifrmavn B tomonda bir xil kalitdan foydalanib osongina rasshifrovkalanadi:

| | | | | | | | | |
|-------------|-----|-----|-----|-----|-----|-----|-----|-----|
| | I | E | B | L | P | O | L | O |
| Shifrmavn: | 010 | 001 | 000 | 011 | 101 | 100 | 011 | 100 |
| Kalit: | 111 | 101 | 110 | 101 | 111 | 100 | 000 | 101 |
| Ochiq matn: | 101 | 100 | 110 | 110 | 010 | 000 | 011 | 001 |
| | P | O | S | S | I | B | L | E |

Ushbu shifrlash algoritmi uchun quyidagi ikki holatni qarab chiqish muhim: faraz qilaylik, A tomonning dushmani *M*, A tomon quyidagi kalitdan foydalangan deb biladi:

101 111 000 101 111 100 000 101 110 000

Agar *M* dushman ushbu kalitni *B* tomonga uzata olsa, u holda *B* tomon shifrmavnni quyidagicha rasshifrovkalaydi:

| | | | | | | | | | | |
|---------------|-----|-----|-----|-----|-----|-----|-----|-----|-----|-----|
| | S | R | L | H | H | H | T | H | S | R |
| Shifrmavn: | 110 | 101 | 100 | 001 | 110 | 110 | 111 | 001 | 110 | 101 |
| “Kalit”: | 101 | 111 | 000 | 101 | 111 | 100 | 000 | 101 | 110 | 000 |
| “Ochiq matn”: | 011 | 010 | 100 | 100 | 001 | 010 | 111 | 100 | 000 | 101 |
| | K | I | L | L | H | I | T | L | E | R |

Agar *B* tomon kriptografiyadan xabari bo‘lmasa, u holda *A* tomonning qarori muhokamaga sabab bo‘ladi.

Ikkinchi holat: faraz qilamiz *A* foydalanuvchi dushmani *M* tomonidan qo‘lga olindi va shifrmavnnga ega bo‘ldi. Dushman shifrmavnni o‘qiy olmaydi va shuning uchun *A* tomondan uning kalitini talab etadi. *A* tomon o‘zini har ikkala tomonga “o‘ynashini” aytib, shifrmavnni rasshifrovkalanish kaliti deb quyidagini aytadi:

111 101 000 011 101 110 001 011 101 101

Ushbu kalit orqali dushman M shifratni rasshifrovkalaganda quyidagi ochiq matn hosil bo‘ladi:

| | | | | | | | | | | |
|---------------|-----|-----|-----|-----|-----|-----|-----|-----|-----|-----|
| | S | R | L | H | H | H | T | H | S | R |
| Shifratn: | 110 | 101 | 100 | 001 | 110 | 110 | 111 | 001 | 110 | 101 |
| “Kalit”: | 111 | 101 | 000 | 011 | 101 | 110 | 001 | 011 | 101 | 101 |
| “Ochiq matn”: | 001 | 000 | 100 | 010 | 011 | 000 | 110 | 010 | 011 | 000 |
| | H | E | L | I | K | E | S | I | K | E |

Agar dushman kriptografiya haqida ma’lumotga ega bo‘lmasa, ushbu ochiq matnga ishonadi va A tomonni qo‘yib yuboradi.

Yuqorida keltirilgan misollar bir martali bloknot shifrini *bardoshli* ekanini ko‘rsatadi. Bir martali bloknotda agar kalit tasodifiy tanlansa va bir marta foydalanilgan taqdirda hujumchi shifratndan ochiq matn haqida biror axborotga ega bo‘la olmaydi (albatta ma’lumotning uzunligidan tashqari). Ya’ni, berilgan shifratn uchun mos “kalit” yordamida shifratn uzunligidagi ixtiyoriy “ochiq matnlar”ni generatsiyalash mumkin va bunda barcha ochiq matnlar bir xil o‘xshashlikka ega bo‘ladi. Shuning uchun shifratndan ochiq matn haqida biror foydali axborotni olishning imkoni yo‘q. Kriptografik nuqtai nazardan shifratnlar o‘zidan ma’lumotni oshkor qilmaydi.

Buning uchun albatta, bir martali bloknotdan to‘g‘ri foydalanish, kalitni tasodifiy tanlash, undan bir marta foydalanilish hamda faqat A va B tomonlarga ma’lum bo‘lishi talab etiladi.

Bir martali bloknot yuqori bardoshlikni ta’minlashiga qaramasdan, har doim undan foydalanilmaydi. Sababi, har bir ochiq matn uchun uning uzunligiga teng bo‘lgan tasodifiy kalitni (bloknotni) generatsiyalash va uni qabul qiluvchiga xavfsiz uzatishning kafolati yo‘q. Agar ochiq matn uzunligidagi kalitni (bloknotni) xavfsiz uzatishning imkoniyati mavjud bo‘lsa, u holda kalitning o‘rniga ochiq matnni uzatish foydali emasmi? Uni shifrlashdan nima ma’no?

Bir martali bloknot usulidan tarixda cheklangan uzunlikdagi ma’lumotlarni shifrlashda qisman foydalanilgan bo‘lsada, hozirgi kundagi katta hajmli ma’lumotlarni uzatishda bir martali bloknotni to‘liq amaliy tomondan qo‘llab bo‘lmaydi.

Bir martali bloknotda kalitlardan faqat bir marta foydalanishdan maqsad nima? Faraz qilaylik, quyidagi ikki ochiq matn P_1 va P_2 bitta kalit

K dan foydalanib shifrlangan: $C_1 = P_1 \oplus K$ va $C_2 = P_2 \oplus K$. Kriptografiyada ushbu holatni “xavflilik” deb ataladi va bir martali bloknot xavfli holatda deb tushuniladi. Ya’ni, foydalanilgan kalit ortiq muammo tug’dirmaydi:

$$C_1 \oplus C_2 = P_1 \oplus K \oplus P_2 \oplus K = P_1 \oplus P_2.$$

Mazkur holda shifratn haqiqiy ochiq matn xususida ba’zi axborotni oshkor qiladi. Agar bir kalitdan foydalanib ko‘p marta shifrlash amalga oshirilsa, bu katta xavfga olib kelishi mumkin. Mazkur holat quyidagi misolda ko‘rib chiqilgan. Faraz qilaylik, quyidagi ikkita ochiq matn berilgan bo‘lsin (belgilarning binar kodi yuqoridagi jadvaldagi kabi):

$$P_1 = \text{LIKE} = 100\ 010\ 011\ 000 \text{ va } P_2 = \text{KITE} = 011\ 010\ 111\ 000.$$

Har ikkala ochiq matn yagona kalit $K = 110\ 011\ 101\ 111$ yordamida shifrlangan va shifratnlar quyidagiga teng bo‘lgan:

| | | | | |
|---------|-----|-----|-----|-----|
| | L | I | K | E |
| P_1 : | 100 | 010 | 011 | 000 |
| K : | 110 | 011 | 101 | 111 |
| C_1 : | 010 | 001 | 110 | 111 |
| | I | H | S | T |

va

| | | | | |
|---------|-----|-----|-----|-----|
| | K | I | T | E |
| P_2 : | 011 | 010 | 111 | 000 |
| K : | 110 | 011 | 101 | 111 |
| C_2 : | 101 | 001 | 010 | 111 |
| | R | H | I | T |

Agar hujumchi kriptotahlil bilan yaqindan tanish bo‘lsa va har ikkala ochiq matn bir xil kalit yordamida shifrlanganini bilsa, mos o‘rindagi shifratn simvollarini bir xilligi bo‘is ochiq matnlardagi 2- va 4-simvollarining bir xilligini osongina aniqlaydi. Bundan tashqari, hujumchi taxminiy P_1 ochiq matn oladi va uni to‘g‘riligini P_2 ochiq matn bilan tekshirib ko‘radi. Faraz qilaylik, hujumchi birinchi ochiq matn sifatida $P_1 = \text{KILL} = 011\ 010\ 100\ 100$ ni olgan bo‘lsin. Bu holda u ochiq matnga mos taxminiy kalitni quyidagicha hisoblaydi:

| | K | I | L | L |
|------------------|-----|-----|-----|-----|
| Taxminiy P_1 : | 011 | 010 | 100 | 100 |
| C_1 : | 010 | 001 | 110 | 111 |
| Taxminiy K : | 001 | 011 | 010 | 011 |

Olingan kalit K yordamida esa ikkinchi shifratmdan ochiq matnni hisoblaydi:

| | | | | |
|------------------|-----|-----|-----|-----|
| C_2 : | 101 | 001 | 010 | 111 |
| Taxminiy K : | 001 | 011 | 010 | 111 |
| Taxminiy P_2 : | 100 | 010 | 000 | 100 |
| | L | I | E | L |

Hisoblangan kalit K ikkinchi ochiq matn P_2 uchun mos bo‘lmagani sababli, hujumchi taxmin qilgan birinchi ochiq matn P_1 ni noto‘g‘riligini biladi. Shu tarzda davom etib, hujumchi qachonki birinchi ochiq matn $P_1 = LIKE$ tarzida taxmin qila olsa, ikkinchi ochiq matnni to‘g‘ri, $P_2 = KITE$, topa oladi.

Venona loyihasi

Venona loyihasi bir martalik bloknot bilan bog‘liq real hayotiy misolni o‘zida aks ettiradi. 1930 va 1940-yillarda Sovet ittifoqi josuslari AQShga bir martalik bloknot bilan “tashrif buyurishgan”. Josuslar xabarlarini bir martalik bloknotdan foydalanib, shifrlangan ko‘rinishda Moskvaga yuborishgan. Josuslar juda muvaffaqiyatli faoliyat yuritgan, ularning xabarlarini o‘sha paytda AQShdagi yuqori tashkilotlar tomonidan o‘rganilgan. Josuslarning asosiy e‘tibor markazida birinchi atom bombasining yaratilish rejasi bo‘lgan. Rozenberglar, Aljer Xiss va boshqa ko‘plab taniqli va hech kim bilmagan josuslar Venona xabarlarini jo‘natishda ishtirok etishgan.

Josuslar yaxshi o‘qitilgan va hech qachon kalitdan qayta foydalanmagan. Shunga qaramay tutib olingan ko‘plab shifratmlar oxir oqibat AQSh kriptanalitiklari tomonidan deshifrlangan. Agar bir martalik bloknot isbotlangan xavfsizlikka ega bo‘lsa, “qanday qilib bunday bo‘lishi mumkin?” degan savol tug‘ilishi aniq. Buning asosiy sababi kalitlarni generatsiyalash usulida kamchilik mavjudligi bo‘lgan. Boshqarcha aytganda, kalitlar ma’lum uzunlikdan so‘ng takrorlangan. Natijada, Venona shifratmlarini ochish imkoni yaratilgan.

3.3. Kodlar kitobi

Kodlar kitobi ko‘rinishidagi klassik shifrlash birinchi jahon urushi davrida ommalashgan. Kodlar kitobi lug‘atga o‘xshash bo‘lib, so‘zlar (ochiq matn so‘zlari)dan va unga mos bo‘lgan kod so‘zlar (shifrmavn)dan tashkil topgan. Shifrlash uchun ushbu kodlar kitobidan zarur bo‘lgan so‘z aniqlanadi va unga mos bo‘lgan kod so‘z shifrmavn sifatida olinadi. Rasshifrovkalashda esa ushbu jarayonning teskarisi amalga oshiriladi. Ya’ni, kodlar kitobidan shifrmavnndagi kod so‘z topiladi va ochiq matn sifatida unga mos bo‘lgan so‘z tanlanadi. Birinchi jahon urushi davrida Nemislar tomonidan foydalanilgan kodlar kitobi na‘munasi quyidagi jadvalda keltirilgan.

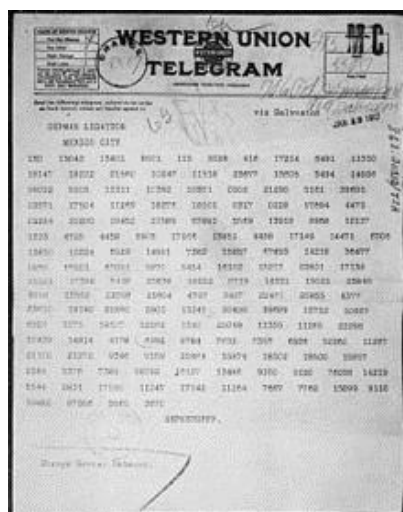
3.2-jadval

Kodlar kitobidan olingan namuna

| Ochiq matn | Shifrmavn |
|----------------|-----------|
| Februar | 13605 |
| fest | 13732 |
| finanzielle | 13850 |
| folgenger | 13918 |
| Frieden | 17142 |
| Friedenschluss | 17149 |
| ⋮ | ⋮ |

Masalan, “Februar” so‘zini shifrlash uchun butun so‘z 5 ta simvoldan iborat kod so‘z, 13605, bilan almashtirilgan. Kodlar kitobi shifrlash uchun, rasshifrovkalash uchun esa kod so‘zlar ustuni bo‘yicha tartiblangan kod so‘zlar kitobidan foydalanilgan. Kod so‘zlar kitobi o‘rniga qo‘yish akslantirishiga asoslangan bo‘lib, bunda bir simvol emas balki butun so‘z, ba’zida esa butun ibora o‘rniga kod so‘z qo‘yilgan.

3.2-jadvalda keltirilgan kod so‘zlar mashhur Zimmerman telegrammini shifrlash uchun foydalanilgan. 1917-yil birinchi jahon urushi davrida, Germaniya tashqi ishlar vaziri Artur Zimmerman Germaniyaning Meksikadagi elchisiga shifrlangan ko‘rinishdagi telegramma yuboradi. 3.3-rasmda keltirilgan shifrlangan xabar Britaniyaliklar tomonidan tutib olinadi. Bu vaqtda Britaniya va Fransiya Germaniya bilan urush va AQSh betaraf holatida edi.



3.3-rasm. Zimmerman telegrammasi

Ruslar Nemislarning kodlar kitobini to‘liq bo‘lmagan versiyasini tiklab, uni Britaniyaga yuboradi. Murakkab tahlillardan so‘ng, Britaniyaliklar Zimmerman telegrammasi yozilgan vaqtidagi kodlar kitobining bo‘shliqlarini to‘ldirishadi va uni deshifrlashadi. Telegrammada aytilishicha, Germaniya hukumati cheklanmagan suvosti urushi boshlashni rejalashtirayotgani va bu AQSh bilan urushga olib kelishi mumkinligi haqida mulohazalar borligi bayon etilgan. Shu sababli, Zimmerman o‘z elchisiga Meksikani AQShga nisbatan urushda Germaniya ittifoqchisi bo‘lishga undashi kerakligini aytadi. Xususan, Meksikani Texas, Yagni Meksika va Arizona shtatlaridagi hududlarini qaytarib olishga undagan. AQShda ushbu telegramma oshkor bo‘lgandan so‘ng, jamoatchilik Germaniyaga qarshi turadi. Shundan so‘ng, AQSh urushga kiradi. Zimmerman telegrammasini to‘liq deshifrlangan ko‘rinishi 3.4-rasmda keltirilgan.

We intend to begin on the first of February unrestricted submarine warfare. We shall endeavor in spite of this to keep the United States of America neutral. In the event of this not succeeding, we make Mexico a proposal of alliance on the following basis: make war together, make peace together, generous financial support and an understanding on our part that Mexico is to reconquer the lost territory in Texas, New Mexico, and Arizona. The settlement in detail is left to you. You will inform the President of the above most secretly as soon as the outbreak of war with the United States of America is certain, and add the suggestion that he should, on his own initiative, invite Japan to immediate adherence and at the same time mediate between Japan and ourselves. Please call the President's attention to the fact that the ruthless employment of our submarines now offers the prospect of compelling England in a few months to make peace.

Signed, ZIMMERMANN

3.4-rasm. Zimmerman telegrammasining deshifrlangan ko‘rinishi

3.4. Enigma mashinasi

Enigma mashinasi Natsislar Germaniyasi tomonidan ikkinchi jahon urushi davrida foydalanilgan. Enigma mashinasi dastlab tijorat maqsadida Artur Sherbius tomonidan yaratilgan. Enigma mashinasi 1920-yilda patentlangan bo'lsada, vaqt o'tishi bilan rivojlanishda davom etdi. Xususan, Germaniya hukumati tomonidan foydalanilgan versiya haqiqiy versiyadan katta farq qilgan.

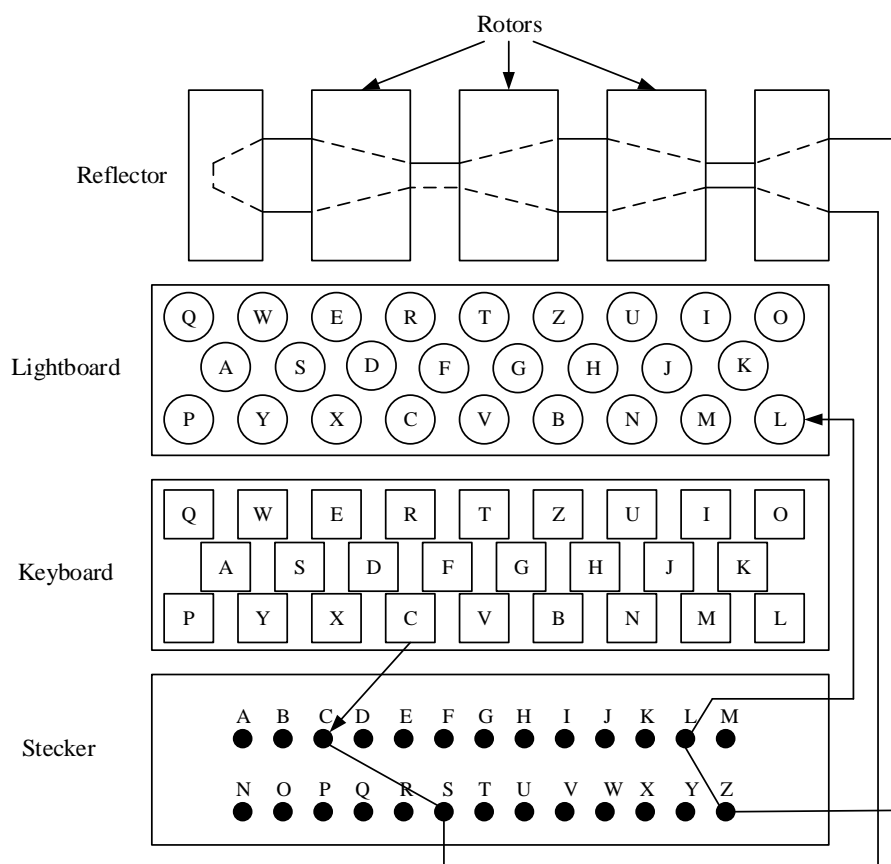
Umumiy miqdorda 100 000 dan ortiq Enigma mashinasi ishlab chiqilgan bo'lsa, shularning 40 000 dan ortig'i ikkinchi jahon urushi davrida to'g'ri keladi. Ushbu bo'limda nemis harbiylari tomonidan foydalanilgan Enigma mashinasining ishlash tartibi bilan tanishib chiqiladi.

Enigma mashinasi urush davrida ittifoqchilar tomonidan "buzilgan". Nemislar Enigmani buzilmas deb o'ylashgan. Biroq, uning buzilgani ma'lum bo'lganidan so'ng undan hayotiy masalalarni yechishda foydalanishda davom etganlar. Enigma mashinasining buzilishi ikkinchi jahon urushining natijasiga qanday ta'sir qilgani aniq bo'lmasada, Yevropada urushni bir yil oldin tugashiga va millionlab insonlarning hayotini saqlab qolishiga sabab bo'lgani haqiqat hisoblanadi.

Enigma mashinasining umumiy ko'rinishi va kriptografik tashkil etuvchilari 3.5-rasmda keltirilgan.



a) Enigma mashinasining ko'rinishi



b) Enigma mashinasi kriptografik tashkil etuvchilari
3.5-rasm. Enigma mashinasi

Rasmda ko‘rsatilgani kabi Enigma mashinasi klaviatura (keyboard) – mexanik tugmalar doskasi hamda shifrmtn belgisini ko‘rsatuvchi yorug‘lik doskasidan (lightboard) iborat. Bundan tashqari, eski telefon uzib-ulagichlariga o‘xshash, belgilar juftini bog‘lovchi kabel mavjud old panel (nimischada “stecker” deb atalgan), uchta rotordan (rotors) iborat.

Xabarni shifrlashdan oldin operator qurilmani ishga tayyorlashi zarur bo‘lgan. Bu jarayon rotorlarni dastlabki sozlanishlari va steckerni ulanishini o‘z ichiga olib, kalit sifatida xizmat qilgan.

Shundan so‘ng, xabar klaviatura orqali kiritilgan va unga mos shifmatn yorug‘lik doskasida paydo bo‘lgan. Hosil bo‘lgan shifrmtn radio orqali ovozda uzatilgan.

Rasshifrovkalash uchun qabul qiluvchi tomondan ham mashinani bir xil sozlashi talab etilgan. Shundan so‘ng, shifmatn klaviatura orqali kiritilgan va unga mos ochiq matn belgilari yorug‘liq doskasida paydo bo‘ladi.

Endi esa, 3.5b – rasmda keltirilgan tashkil etuvchilar bo‘yicha Enigma mashinasi ishlashini batafsil ko‘rib o‘tsak. Xabarni shifrlash uchun xabar belgilari klaviatura orqali kiritiladi. Dastlab belgi stecker

orqali o‘tib, navbati bilan 3 ta rotordan va undan so‘ng reflektordan o‘tadi. Shundan so‘ng, reflektordan qaytgan belgi uchta rotordan o‘tib, stecker orqali yorug‘lik doskasida shifratn sifatida taqdim etiladi. Har bir rotor va reflektor 26 ta belgini o‘rin almashinishini ta‘minlovchi qattiq-simlardan tashkil topgan. Rotorning tuzilishi bilan quyida tanishib chiqiladi.

Yuqorida keltirilgan rasmda stecker kabellari $C \rightarrow S$ shaklida ulangani bois, klaviatura yordamida kiritilgan C harfi S belgisiga almashadi. Shundan so‘ng, S harfi rotorlardan va reflektor orqali o‘tib, yana rotorlardan qaytadan o‘tadi. 3.5-rasmdagi holat uchun, S belgisi Z ga almashtiriladi. Steckerda L va Z belgilar o‘zaro bog‘langani bois, natijada L belgisi yoritish oynasida paydo bo‘ladi.

Keyingi tushuntirishlar uchun quyidagi belgilanishlarni qabul qilamiz:

- $R_r = o'ngda\ joylashgan\ rotor;$
- $R_m = o'rtada\ joylashgan\ rotor;$
- $R_l = chapda\ joylashgan\ rotor;$
- $T = reflektor;$
- $S = stecker.$

Keltirilgan belgilanishlar bilan 3.5-rasmdagi holat uchun x belgiga mos bo‘lgan y shifratn belgisini quyidagicha ifodalash mumkin:

$$y = S^{-1}R_r^{-1}R_m^{-1}R_l^{-1}R_lR_mR_rS(x) = (R_lR_mR_rS)^{-1}T(R_lR_mR_r)S(x) \quad (3.1)$$

Agar Enigma mashinasi yuqorida ifodalangani kabi bo‘lsa, u dastlabki sozlanishga bog‘liq holda oddiy o‘rniga qo‘yish akslantirishini amalga oshiradi. Biroq, har bir ochiq matn belgisi bosilganda o‘ngda joylashgan rotor qadami bittaga siljisa, qolgan rotorlar ham adometerga o‘xshash (o‘ngda joylashgan rotor har 26 ta siljiganda o‘rtadagisi bittaga, o‘rtadagi har 26 ta siljiganda chapdagisi bittaga) siljiydi. Reflektorni o‘zgarmas rotor kabi tasavvur etish mumkin. Ya‘ni, harflarni almashtiradi, biroq, siljimaydi. Xulosa qilib aytganda, uchta rotor qiymatlari turlicha bo‘ladi, reflektor va stecker qiymatlari esa o‘zgarmaydi.

Enigma o‘rniga qo‘yish shifri hisoblansada, Sesar kabi oddiy tuzilishga ega emas. Adometr ta‘siri sababli, o‘rniga qo‘yish holati

belgidan-belgiga almashib boradi. Shuning uchun uni ko‘p alfavitli o‘rniga qo‘yish shifri deb atash mumkin.

Enigma kalit maydon

Enigma shifrining kriptografik nuqtai-nazaridan muhim komponentlari: stecker, uchta rotor va reflektor. Biror xabarni shifrlash va rasshifrovkalashda ushbu komponentlarning dastlabki sozlanishi Enigma kalitini tashkil qiladi. Kalitni tashkil qilgan o‘zgaruvchan sozlanishlar quyidagilar:

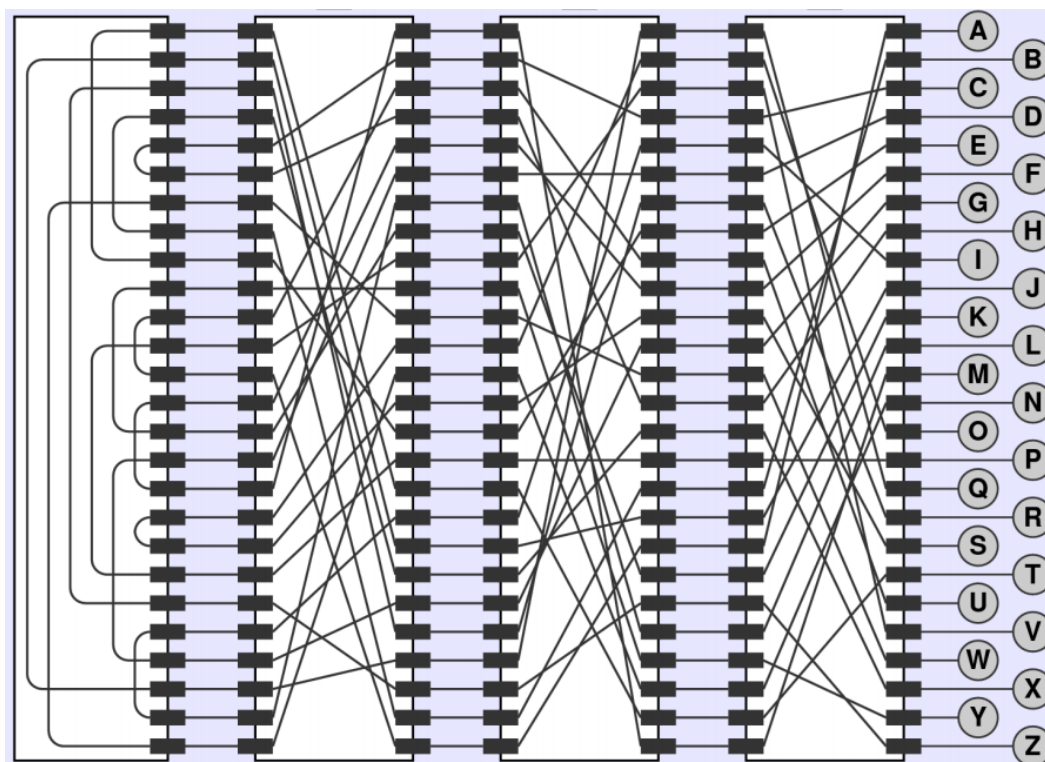
1. Rotorlarni tanlash.k.

2. O‘ng tomonda joylashgan ikki rotordagi harakatlanuvchi xalqaning holati. Bu xalqa rotorning tashqi tomonini (26 ta belgi bilan belgilangan) xalqaning ichki tomoniga (simli almashtirish amalga oshirilgan) moslab aylantirishga imkon beradi. Bu xalqalarni siljishi adometr hodisasini yuzaga kelishiga sabab bo‘ladi (3.6-rasm).

3. Har bir rotorning dastlabki holati.

4. Steckerda bog‘lanishlar soni va holati.

5. Reflektorni tanlash.k.



3.6-rasm. Rotorlar va reflektorning bog‘lanishi

Yuqorida aytilganidek, har bir rotor 26 belgidan iborat alfavitni o‘rnini almashtirishni amalga oshiradi. Harakatlanuvchi xalqalar ushbu 26 ta belgiga mos bo‘lgan biror holatda o‘rnatiladi.

Har bir rotor undagi A dan Z gacha belgilangan 26 ta holatdan biriga oʻrnatiladi. Stecker eski koʻrinishdagi telefonga oʻxshash boʻlib, har biri alfavit belgilari bilan belgilangan 26 ta “chuqur”chadan iborat. Stecker 0-13 oraliqdagi kabellardan iborat boʻlishi mumkin va ularning har biri bir juft chuqurlarni bogʻlaydi. Reflektor 26 ta belgining almashinishini taʼminlaydi va bunda biror belgi oʻziga almashmaydi. Shuning uchun, reflektorni 13 ta kabeldan iborat boʻlgan stecker sifatida qarash mumkin.

Enigma mashinasi 3 ta rotordan iboratligi va ularning har biri 26 ta belgidan iboratligi uchun, rotorlarni joylashtirish va tanlash holatlarining umumiy soni quyidagiga teng:

$$26! \cdot 26! \cdot 26! \approx 2^{265}.$$

Bundan tashqari, ikki harakatlanuvchi xalqalarning oʻrnatish holati – adometr holatini qachon yuz berishini aniqlovchi - $26 \cdot 26 \approx 2^{9.4}$ ga teng boʻladi.

Har bir rotor dastlabki holat sifatida 26 ta belgidan biriga oʻrnatilishi mumkinligi bois, rotorlarni sozlashning $26 \cdot 26 \cdot 26 = 2^{14.1}$ turli varianti mavjud boʻladi. Biroq, ushbu raqam yuqorida hisoblangan 2^{265} qiymat ichida boʻlgani bois, inobatga olinmaydi.

Eng soʻngi muhim tashkil etuvchi hisoblangan steckerni qarajak. Faraz qilaylik, $F(p)$ kattalik steckerdagi p ta kabellarni ulashning turli yoʻllari sonini ifodalasin. U holda quyidagi tenglikni yozish mumkin:

$$F(p) = \binom{26}{2p} (2p - 1)(2p - 3) \cdots 1.$$

Bu yerda, $\binom{n}{k} = \frac{n!}{k!(n-k)!}$ ga teng.

p ning turli qiymatlari uchun $F(p)$ kattalik qiymatlari quyidagi jadvalda keltirilgan (3.3-jadval).

3.3-jadval

Steckerdagi kombinatsiyalar soni

| | |
|-------------------------|-------------------------|
| $F(0) = 2^0$ | $F(1) \approx 2^{8.3}$ |
| $F(2) \approx 2^{15.5}$ | $F(3) \approx 2^{21.7}$ |
| $F(4) \approx 2^{27.3}$ | $F(5) \approx 2^{32.2}$ |
| $F(6) \approx 2^{36.5}$ | $F(7) \approx 2^{40.2}$ |
| $F(8) \approx 2^{43.3}$ | $F(9) \approx 2^{45.6}$ |

$$\begin{array}{l} F(10) \approx 2^{47.1} \quad F(11) \approx 2^{47.5} \\ F(12) \approx 2^{46.5} \quad F(13) \approx 2^{42.8} \end{array}$$

Yuqoridagi jadvaldan ko‘ringani kabi, eng ko‘p kombinatsiya 11 ta kabel holati uchun bo‘ladi. Yuqorida aytilgani kabi, 13 ta kabel mavjud stecker reflektorga ekvivalent hisoblanadi. Natijada, $F(13) \approx 2^{42.8}$ turli reflektor mavjud bo‘ladi.

Barcha olingan natijalarni birlashtirishdan Enigma mashinasi uchun kalit maydonini hisoblash mumkin:

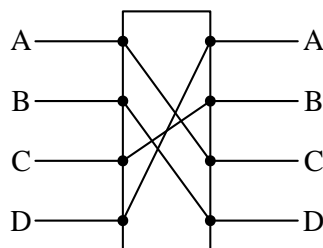
$$2^{265} \cdot 2^{9.4} \cdot 2^{48.9} \cdot 2^{42.8} \approx 2^{366}.$$

Boshqacha aytganda, Enigma shifrining kalit maydoni 366 bitli kalitga ekvivalent. Zamonaviy simmetrik shifrlash uchun kamida 128 bitli kalit uzunligini yetarli bo‘lishidan, Enigma shifrini yetarlicha bardoshlikka egaligini ko‘rish mumkin.

Rotorlar

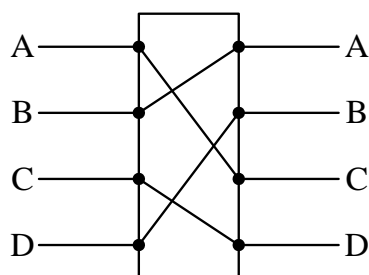
Rotorga asoslangan shifrlash mashinalari XX asrning birinchi yarmida juda ko‘p foydalanilgan bo‘lib, Enigma ular orasida eng mashhuridir. Shunga o‘xshash mashinaga Amerikaliklar tomonidan foydalanilgan Sigaba shifrini ham misol keltirish mumkin.

Soddalik uchun rotorni *A* dan *D* gacha belgilangan 4 ta belgidan iborat deb qaraylik. Agar signalni chapdan o‘nga harakatlanadi deb qarajak, 3.7-rasmda keltirilgan rotor *ABCD* dan *CDBA* ga almashtirishni amalga oshiradi. Ya’ni, $A \rightarrow C$, $B \rightarrow D$, $C \rightarrow B$ va $D \rightarrow A$ ga almashadi. Teskari almashtirish esa mazkur holat uchun *DCAB* ga teng bo‘ladi. Boshqacha aytganda, rotordan signalni o‘ngdan chapga o‘tkazish orqali amalga oshiriladi. Bu ajoyib xususiyat bo‘lib, shifrlashda foydalanilgan qurilma yordamida rasshifrovkalash amalga oshiriladi. Ya’ni, Enigma mashinasi o‘zining teskarisiga ega bo‘lib, faqat bir xil dastlabki sozlanishlarni talab qiladi.



3.7-rasm. Rotor

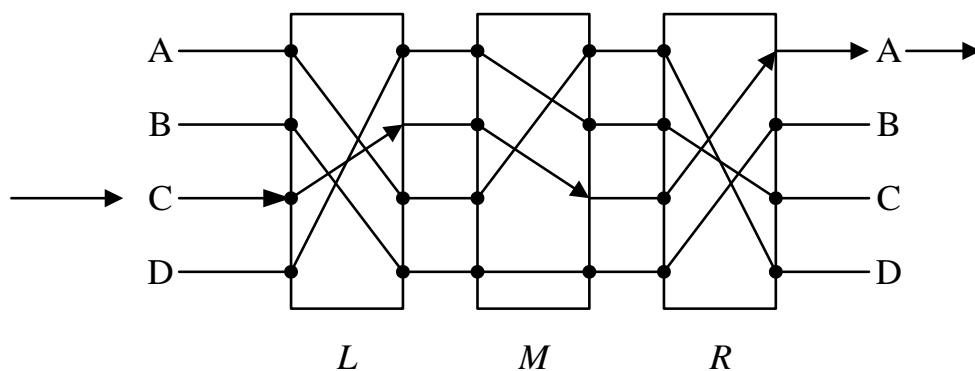
Faraz qilaylik, rotor 3.7-rasmda keltirilgani kabi bir qadamga siljigan bo'lsin. Shuni eslatib o'tish kerakki, tasvirdagi to'rtburchak shaklining o'zi rotor bo'lib, u aylanadi. Ichidagi kabel bilan bog'langan qism esa aylanmaydi. Ushbu misolda, faraz qilaylik rotor yuqoriga siljigan bo'lsin. Ya'ni, B belgisining yangi holati A , va h.k. A belgisining yangi holati esa D bo'ladi. 3.7-rasmda keltirilgan rotorning yuqorida bir qadamga siljishidan hosil bo'lgan holati 3.8-rasmda keltirilgan. Siljishdan keyingi natijaviy holat $CADB$ ga teng va bu 3.7-rasmdagi kabi $CDBA$ ga teng emas.



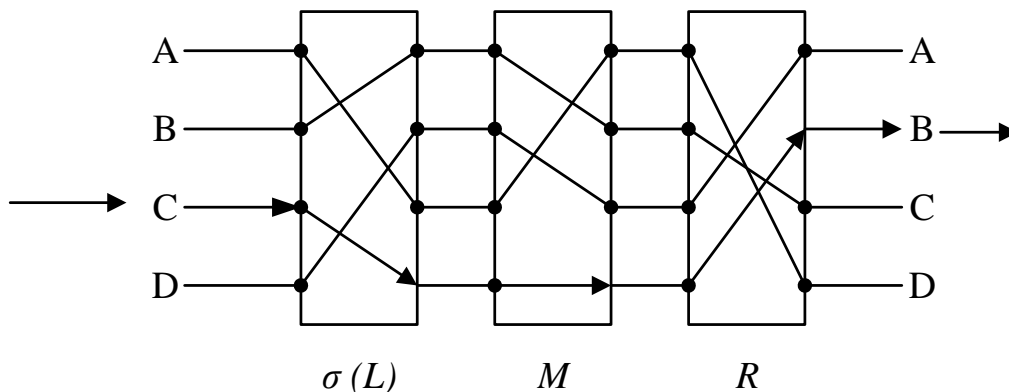
3.8-rasm. Siljigan rotor

Umuman olganda, almashtirishda rotorning siljishini aniqlash murakkab emas. Bu yerda muhimi, belgini qancha qadam bilan siljiganidir. Masalan, $CDBA$ almashtirishda, qadamlar quyidagiga teng: A belgisi C ga almashgani bois, qadam 2 ga, B esa D ga almashgani bois qadam 2 ga, C belgisi B ga almashgani bois qadam 3 ga va D belgisi A ga almashgani bois qadam 1 ga teng. Umumiy qilib aytganda, $CDBA$ holatga almashinish qadamlari $(2, 2, 3, 1)$ ga teng. 3.8-rasmda keltirilgan siklik siljishdan keyin hosil bo'lgan almashinish qadamlari esa $(2, 3, 1, 2)$ ga teng.

Yuqorida aytilgani kabi rotorlardan foydalanishning asosiy afzalligi soddalik bilan turli almashtirishlarni amalga oshirishdan iborat. Ko'p sonli rotorlardan foydalanish bilan esa ko'p sonli almashtirishlarni hosil qilish mumkin. Masalan, 3.9-rasmda C belgisi A ga almashgan. L rotorning siljishi, $\sigma(L)$ orqali belgilanib, natijasida C belgisi B ga almashadi (3.10-rasm). Ya'ni, bir rotorning o'zgarishi butun almashtirishga ta'sir qiladi.



3.9-rasm. Uchta rotor



3.10-rasm. *L* rotorning siljishi

Uchta rotordan iborat sxemada, *ABCD* belgilarni siklik ravishda jami 64 ta almashtirish holati mavjud. Mazkur holda, takrorlanishlar kuzatiladi. Unikal almashtirishlar soni esa 24 ga teng bo‘ladi.

Enigma mashinasiga hujum. Enigma mashinasiga nisbatan amalga oshirilgan birinchi samarali kriptotahlil Marian Reevskiy boshchiligidagi polshalik kriptotahlilchilar tomonidan amalga oshirilgan. Biroq, ular duch kelgan asosiy muammo bu - qaysi rotordan foydalanilganini bilishmagan. Biroq, yuqori matematik bilim va ba’zi josuslik ma’lumotlari yordamida shifratndan rotorlar almashinish tartibini aniqlashgan.

1939-yilda fashistlar Polshani bosib olganidan so‘ng, Marian Reevskiy boshchiligidagi kriptotahlilchilar guruhi Fransiyaga ko‘chib o‘tishadi. Fransiya ham fashistlar tomonidan bosib olinganidan so‘ng, o‘z tadqiqotlarini Vichi Fransiyada davom ettiradilar. Marian Reevskiy boshchiligidagi kriptotahlilchilar tomonidan erishilgan yutuqlar, britaniyalik kriptotahlilchilarga yetib boradi. Shundan so‘ng, tarkibida Gordon Velchman va kompyuter kashfiyotchisi Alan Turing bo‘lgan kriptotahlilchilar guruhi Enigma mashinasini tahlil qilishni boshlaydilar.

Ushbu bo‘limda keltirilgan Enigma mashinasining tahlili Alan Turing tomonidan amalga oshirilgan versiyaga o‘xshash, biroq, soddalashgan ko‘rinishidir. Ushbu hujumda ma’lum ochiq matnlar (o‘sha davrda “crib” deb atalgan) talab qilingan.

Amalga oshirilgan tahlilning asosiy g‘oyasi dastlab stekerni inobatga olmagan holatda, kalitni bashorat qilishdan iborat. Mazkur holatda, mavjud variantlar soni 2^{30} dan kichik bo‘ladi. Ularning har biri uchun cribdan ochiq ma’lumot tiklanib, noto‘g‘ri bo‘lgan variantlar tashlab yuboriladi. Ushbu hisoblashni amalga oshirish hozirgi zamondagi EHM uchun oson bo‘lsada, ikkinchi jahon urushi davridagi texnologiyalar uchun imkonsiz bo‘lgan. Faraz qilaylik, ochiq matn va unga mos shifratn quyidagicha bo‘lsin (3.4-jadval). Ushbu ma’lumotdan quyidagi keltiriladigan hujumni tushuntirishda foydalaniladi.

3.4-jadval

Enigma shifri uchun ma’lum ochiq matnga misol

| | | | | | | | | | | | | | | | | | | | | | | | | |
|------------|---|---|---|---|---|---|---|---|---|---|----|----|----|----|----|----|----|----|----|----|----|----|----|----|
| <i>i</i> | 0 | 1 | 2 | 3 | 4 | 5 | 6 | 7 | 8 | 9 | 10 | 11 | 12 | 13 | 14 | 15 | 16 | 17 | 18 | 19 | 20 | 21 | 22 | 23 |
| Ochiq matn | O | B | E | R | K | O | M | M | A | N | D | O | D | E | R | W | E | H | R | M | A | C | H | T |
| Shifratn | Z | M | G | E | R | F | E | W | M | L | K | M | T | A | W | X | T | S | W | V | U | I | N | Z |

x belgining stekerdan o‘tganidan keyingi natijasi $S(x)$ ga teng bo‘lsin. U holda, x ning stekerdan teskari yo‘nalishga o‘tishi $S^{-1}(x)$ ga teng bo‘ladi. Berilgan dastlabki sozlanish uchun, faraz qilaylik i -bosqich uchun almashtirish P_i ga teng bo‘lsin. Ya’ni, bu yerda P_i almashtirish uchta rotordan va reflektordan o‘tish, rotorlardan teskari yo‘nalishda qayta o‘tishni o‘z ichiga oladi. U holda (3.1) tenglikdan foydalangan holda, umumiy almashtirishni quyidagicha yozish mumkin (bu yerda, soddalik uchun R_l, R_m, R_r larning i qadamdagi bog‘lanishlari inobatga olinmadi):

$$P_i = S^{-1}R_r^{-1}R_m^{-1}R_l^{-1}TR_lR_mR_rS$$

P_i almashtirish uchun teskari P_i^{-1} almashtirish ham mavjud. Bundan tashqari, har bir belgi bosilganidan so‘ng almashtirish o‘zgarib turadi. Ya’ni, P_i almashtirish bosqich i ga bog‘liq bo‘ladi.

Taqdim etilayotgan hujumda ma'lum ochiqmatn va unga mos shifratndagi "siklni" aniqlash mumkin. Faraz qilaylik, 3.4-jadvaldagi 8-ustunni olaylik. Ochiq matn belgisi A steker orqali, so'ng P_8 almashtirish va so'ngra S^{-1} orqali o'tib, shifratn belgisi M ni hosil qiladi. Ya'ni, $S^{-1}P_8S(A) = M$. Ushbu tenglikdan esa $P_8S(A) = S(M)$ tenglikni yozish mumkin.

3.4-jadvalda keltirilgan ma'lum ochiq matnlar yordamida quyidagiga ega bo'lamiz:

$$\begin{aligned} P_8S(A) &= S(M) \\ P_6S(M) &= S(E) \\ P_{13}S(E) &= S(A) \end{aligned}$$

Ushbu sikllarni birlashtirish orqali esa siklni aniqlash mumkin:

$$S(E) = P_6P_8P_{13}S(E) \quad (3.2)$$

Faraz qilaylik, stekerni inobatga olmagan holda biror dastlabki sozlanishni tanlaylik. U holda, ushbu sozlanishga tegishli barcha P_i va P_i^{-1} lar ma'lum bo'ladi. Shundan so'ng, faraz qilaylik, stekerda E va G belgilar o'zaro ulangan bo'lsin, $S(E) = G$. Agar mashinaning sozlanishi faraz qilinganidek va steker yuqorida keltirilgani kabi bo'lsa, (3.2) tenglikdan quyidagiga ega bo'linadi:

$$G = P_6P_8P_{13}(G) \quad (3.3)$$

Agar $S(E)$ uchun barcha 26 ta holat sinab ko'rilsa va (3.3) tenglik hech qachon o'rinli bo'lmasa, u holda rotor sozlanishlari noto'g'ri bo'ladi va tanlov qisqartiriladi. Bu bilan rotorning sozlanishlar variantini kamaytirish va bittaga tushirish mumkin. Biroq, agar (3.2) tenglikni qanoatlantiruvchi $S(E)$ topilgan taqdirda ham, rotorlarning joriy sozlanishini bilib bo'lmaydi. Bundan tashqari, $S(E)$ ni aniqlashdagi barcha variantlar 26 ga tengligi bois, ularning har biri uchun, tasodifiy bo'lganda (3.2) tenglikni qanoatlantiruvchi holatni aniqlash ehtimoli $1/26$ ga teng bo'ladi. Natija esa, bir siklda kalitni topishdagi hisoblashlar soni kamaymaganini ko'rsatadi.

Biroq, hisoblash jarayonida $S(E)$ bilan bog'liq qo'shimcha sikl qo'shilsa, uning (3.2) tenglik bilan kombinatsiyasi yordamida bo'lishi

mumkin bo'lgan rotorlar sozlanishi sonini kamaytirish mumkin. Faraz qilaylik, quyidagi 4 ta tenglikdan, $S(E) = P_3P_{14}^{-1}P_7P_6^{-1}S(E)$ ni hosil qilish mumkin:

$$S(E) = P_3S(R)$$

$$S(W) = P_{14}S(R)$$

$$S(W) = P_7S(M)$$

$$S(E) = P_6S(M)$$

Agar, aytaylik $S(E) = G$ deb faraz qilsak, u holda ikkita tenglik o'rinli bo'lishi kerak. $S(E)$ uchun hanuz 26 ta tanlov mavjud, biroq, 2 ta sikl bilan. Shu sababli, har ikkalasining tasodifiy bo'lish ehtimoli $(1/26)^2$ ga teng bo'ladi. Shuning uchun, $S(E)$ da 2 ta sikl bilan, mashinani sozlanishlar sonini (ya'ni, kalitlar sonini) 26 marta kamaytirish mumkin. Ushbu kuzatishlar asosida Enigma mashinasiga hujumni osonlik bilan amalga oshirish mumkin.

Shuni alohida ta'kidlash lozimki, agar rotor sozlanishlari kuzatishlar natijasida aniqlansa, barcha P_0, P_1, P_2, \dots va $P_0^{-1}, P_2^{-1}, P_2^{-1}, \dots$ almashtirishlar ma'lum bo'ladi. Shundan so'ng, agar $S(E)$ uchun taxminiy qiymatlar aniqlansa, barcha sikl tenglamalarini to'g'riligini tekshirish mumkin bo'ladi. $S(E)$ noto'g'ri faraz qilinganida esa, sikl tenglamasini qanoqlantirish ehtimoli $1/26$ ga teng bo'ladi. Biroq, sikllar soni n ga teng bo'lganda, sikl tenglamalarini qanoqlantirish ehtimoli $(1/26)^n$ ga teng bo'ladi. Shu sababli, n siklga ega $S(E)$ bilan, bo'lishi mumkin bo'lgan rotor sozlanishlari sonini 26^{n-1} marta kamaytirish mumkin. Rotor sozlanishlarining umumiy soni 2^{30} ga tengligini inobatga olib, yetarli sondagi sikl bilan rotor sozlanishlarining bo'lishi mumkin bo'lgan sonini birga tushirish, ya'ni kalitni topish mumkin.

Nazorat savollari

1. Klassik shifrlarda foydalanilgan asosiy akslantirishlarni ayting.
2. Chastotalar bo'yicha tahlil qaysi akslantirishga qaratilgan.
3. Vernam shifri va uning bardoshligi haqida gapiring.
4. Venona loyihasi haqida ayting.
5. Kodlar kitobi asosida ma'lumotlarni shifrlash tartibini tushuntiring.

6. Zimmerman telegrami va u bilan bogʻliq hodisalar toʻgʻrisidan ayting.
7. Enigma mashinasi va uning tuzilishini tushuntiring.
8. Enigma shifrining kalit maydoni haqida gapiring.
9. Rotor nima va uning Enigma mashinasidagi ahamiyati.
10. Enigma mashinasiga qarshi amalga oshirilgan hujumlar haqida gapiring.

4 BOB. PSEVDOTASODIFIY SONLAR GENERATORI VA OQIMLI SIMMETRIK SHIFRLASH ALGORITMLARI

4.1. Tasodifiy ketma-ketliklarni hosil qilish usullari

Tasodifiy ketma-ketliklarni ishlab chiqarishda ko‘plab usullar va vositalar mavjud bo‘lib, ular turli maqsadlarda foydalaniladi. Tasodifiy ketma – ketliklarni shakllantiruvchi generatorlarni uch turkumga ajratish mumkin.

Xavfsiz bo‘lmagan tasodifiy sonlar generatori. Ushbu generatorlar kriptografik kalit generatorlariga qo‘yilgan talablarga javob bermaydi va shuning uchun hujumchi generator chiqishini taxmin qilishi mumkin.

Kriptografik psevdotasodifiy sonlar generatori (Cryptographic pseudorandom number generators, PRNGs). Bu turdagi generatorlar «hisoblanuvchi» generatorlar ham deb atalib, ular kirishda boshlang‘ich qiymatni (seed) talab etadi va bu boshlang‘ich qiymatdan kutilmagan tasodifiy sonlarni ishlab chiqaradi. Shuning uchun bu turdagi generatorlar tasodifiy emas psevdotasodifiy sonlar generatori va hosil qilgan qiymatlarini esa tasodifiy emas psevdotasodifiy sonlar deb ham ataladi. Ushbu generatorlar xavfsiz kirish qiymati amalga oshirilganda yuqori xavfsizlikni ta‘minlab beradi. Bu turdagi generatorlar odatda dasturiy shaklda ko‘proq amalga oshiriladi.

Entropiya to‘plovchilar. Bu turdagi generatorlar odatda «haqiqiy» tasodifiy sonlar generatori deb ham atalib, ular turli manbalardan entropiyalarni to‘playdi va ularni bevosita taqdim etadi. Ular ko‘p hollarda xavfsiz deb qaralsada, ma‘lumotlarni taqdim etishda juda ko‘p vaqt talab etadi. Shuning uchun bu turdagi generatorlar odatda apparat ko‘rinishda amalga oshiriladi. Ammo, ko‘plab entropiya to‘plovchilar operatsion tizimdagi turli tasodifiy hodisalardan entropiya to‘plashga asoslangan (masalan, /dev/random).

Birinchi toifadagi generatorlar odatda kriptografiyadan boshqa sohalarda foydalanishga tavsiya etilib, statistik tomondan tasodifiy bo‘lmagan sonlarni generatsiya qiladi. Bu turdagi generatorlar o‘zini ichki holatini oshkor etib qo‘yishi mumkinligi bois, xavfsiz sanalmaydi. Ushbu generatorlarga aksariyat kutubxonalarda mavjud bo‘lgan *rand()* va *random()* funksiyalarini keltirish mumkin (odatda chiziqli kongurent generatorlarga asoslangan). Bundan tashqari, eng keng tarqalgan kriptografik bo‘lmagan generatorlarga Microsoft Excel, GAUSS, Glib,

GNU Octave, MATLAB, Free Pascal, PHP, Python, Ruby, C++ (S++11 dan boshlab) va boshqa ko'plab kutubxona va dasturiy vositalarda tasodifiy sonlarni generatsiya qilish uchun foydalanilayotgan «Mersenn Tvister» generatorini misol keltirish mumkin.

Umumiy kriptografik maqsadda foydalanish uchun, ikkinchi usul maqul sanaladi. Buning uchun xavfsiz entropiya (ya'ni, haqiqiy tasodifiy ma'lumot) olinib, kriptografik psevdotasodifiy sonlar generatoriga kiritiladi va u ma'lum vaqt davomida psevdotasodifiy sonlarni generatsiya qiladi. Ushbu generatorlar ham ichki holati namayon bo'lganda kutuluvchi sonlarni taqdim etishi mumkin. Shuning uchun ushbu generatorlardan foydalanishda uni to'g'ri boshlang'ich qiymatni qabul qilishini ta'minlash lozim.

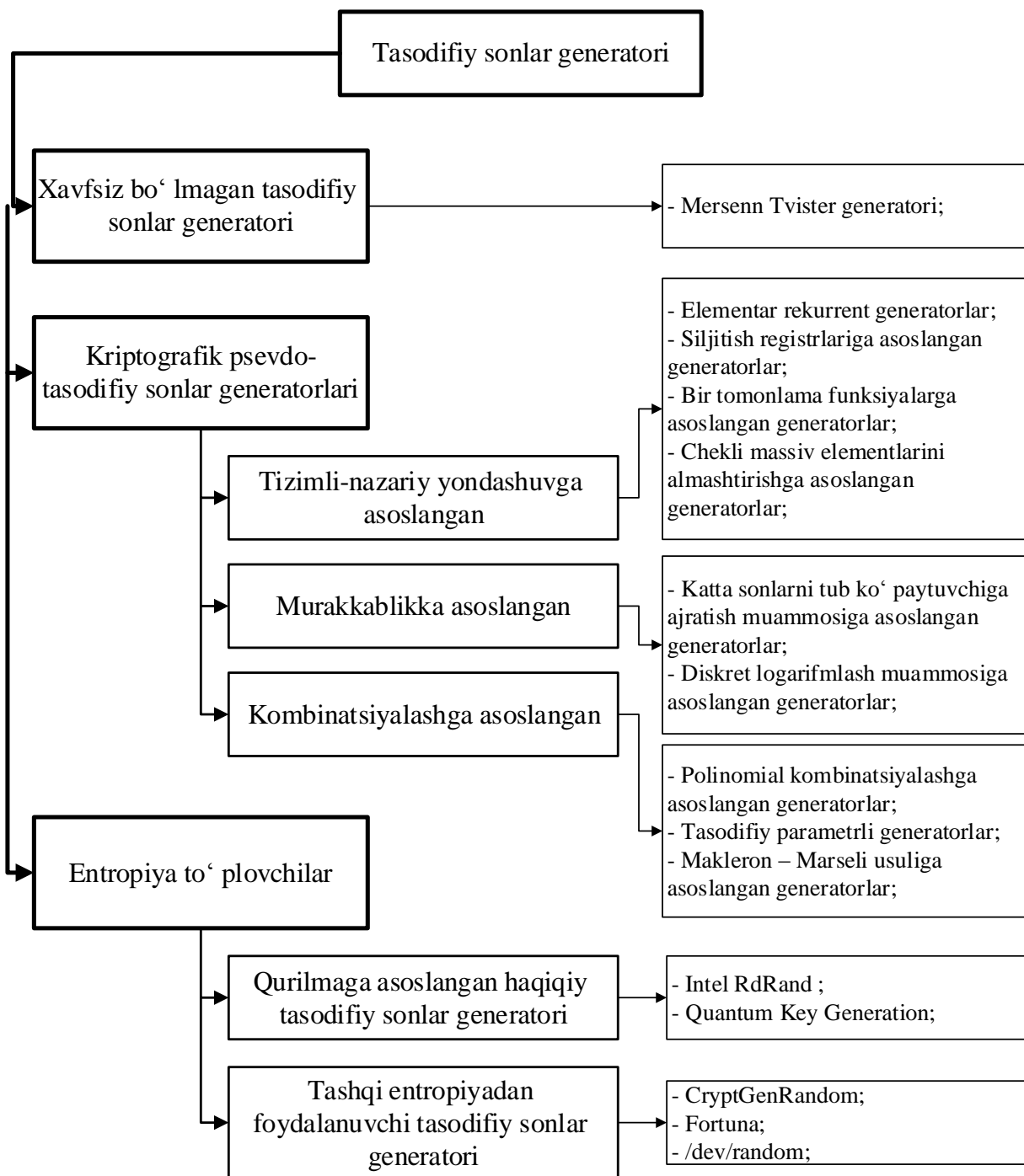
Ikkinchi usul qisqa vaqtda foydalaniluvchi kalit ma'lumotlarni ishlab chiqarish uchun qulay sanalsada, uzoq vaqt davomida foydalaniluvchi kalitlarni generatsiyalash uchun tavfsiya etilmaydi. Bu holda haqiqiy tasodifiy bo'lgan kalitlardan foydalanish talab etiladi.

Agar bir bayt ma'lumot haqiqiy tasodifiy sanalsa, unda har bir 2^8 (256) ta bo'lishi mumkin bo'lgan holatlar o'xshash bo'lishi va uni topish uchun hujumchidan 2^7 ta urinishni talab etishi kerak. Faqat shu holdagina ushbu baytni 8 bit entropiyaga ega deb qarash mumkin.

4.1-rasmda tasodifiy sonlar generatorlarining umumiy tasnifi keltirilgan. Haqiqiy tasodifiy generatorlarni yetarli entropiyani to'plash uchun ko'p vaqt talab etishi sababli, amalda ikkinchi va uchinchi usullarning kombinatsiyasidan foydalaniladi. Shu sababli, quyida keng foydalanilayotgan tashqi entropiyadan foydalanuvchi tasodifiy sonlar generatori va kriptografik psevdotasodifiy sonlar generatoriga ta'luqli ba'zi generatorlar tahlili keltirilgan.

Tasodifiylik darajasi yuqori bo'lgan psevdotasodifiy ketma-ketlikni ishlab chiqaruvchi generatorlar zamonaviy kriptotizimlarning ajralmas qismi hisoblanadi. Tasodifiy ketma-ketliklar kriptografiyada quyidagi maqsadlarda qo'llaniladi:

- simmetrik kriptotizimlar uchun tasodifiylik darajasi yuqori bo'lgan seans kalitlari va boshqa kalitlarni generatsiya qilishda;
- ochiq kalitli kriptotizimlarda qo'llaniladigan katta qiymatlar qabul qiluvchi parametrlarning tasodifiy boshlang'ich qiymatlari generatsiyasida;



4.1 – rasm. Tasodifiy sonlar generatorlarining tasnifi

- blokli shifrlash algoritmlarining boshlangʻich tasodifiy qiymat talab qiluvchi CBC, OFB va boshqa rejimlar uchun tasodifiylik darajasi yuqori boʻlgan boshlangʻich vektorlar hosil qilishda;
- elektron raqamli imzo tizimlarida katta qiymatga ega parametrlar uchun dastlabki tasodifiy qiymatlarni generatsiyasida;
- bitta protokol orqali bir xil maʼlumotlarni har-xil kalitlar qoʻllash bilan shifrlab turli koʻrinishda uzatish uchun talab qilinadigan holatlarda

kalit uchun yetarli uzunlikdagi tasodifiy ketma-ketlik hosil qilishda, masalan SSL va SET protokollarida.

4.2. Chiziqli va chiziqsiz kongruent generatorlar

Elementar rekurent hisoblashlarga asoslangan psevdotasodifiy ketma-ketlik generatorlari ularda qo'llanilgan akslantirishlarga ko'ra *chiziqli, multiplikativ, chiziqsiz* turkumlarga bo'linadi.

Chiziqli va multiplikativ kongruent generatorlar. Chiziqli kongruent generatorlar umumiy holatda $x_{i+1} = (ax_i + c) \bmod N$ formula bilan aniqlanuvchi rekurent hisoblashga asoslangan. Dastlabki berilgan kirish parametrlari asosida ketma-ketliklar hosil qilinadi.

Kirish parametrlari:

N – chekli maydon xarakteristikasini ifodalovchi son, a va c - o'zgarmas musbat butun sonlar, x_0 – boshlang'ich butun qiymatli son;

Ketma-ketlikni tashkil etuvchi chiqish qiymatlari:

$$x_{i+1} = (ax_i + c) \bmod N, i = 0, 1, 2, 3, \dots$$

Chiziqli kongruent generatorning kirish parametri $c = 0$ bo'lsa, ya'ni

$$x_{i+1} = (ax_i) \bmod N, i = 0, 1, 2, 3, \dots$$

bo'lsa, bu generator chiziqli multiplikativ generator deyiladi.

Qoida 4.2.1. Ushbu $x_{i+1} = (ax_i + c) \bmod N, i = 0, 1, 2, 3, \dots$ rekurent formula bilan aniqlangan psevdotasodifiy ketma-ketlik maksimal N davrga ega bo'lishi uchun quyidagi:

- 1) c va N -o'zaro tub sonlar, ya'ni $\gcd(c, N) = 1$;
- 2) r soni N sonining bo'luvchisi va $a - 1$ soni r soniga karrali;
- 3) N soni 4 karrali bo'lsa, $a - 1$ soni ham 4 ga karrali;
- 4) shartlarning bajarilishi zarur va yetarli.

Chiziqsiz kongruent generatorlar. Kirish parametrlari:

N – chekli maydon xarakteristikasini ifodalovchi son;

d, a va c - o'zgarmas musbat butun sonlar, x_0 – boshlang'ich qiymat;

Ketma-ketlikni tashkil etuvchi chiqish qiymatlari :

$$x_{i+1} = (dx_i^2 + ax_i + c) \bmod N, \text{ bu yerda } i = 0, 1, 2, \dots$$

Bu generator kvadratik generator deb ham ataladi.

Qoida 4.2.1. Kvadratik generatorlar hosil qilgan generator o'zining $T_{max} = N$ maksimal davriga ega bo'lishi uchun quyidagi shartlarning:

1) c va N o'zaro tub sonlar;

2) $d, a - 1$ -sonlari biror p -tub songa karrali bo'lib, bu p - soni N ning bo'luvchisi;

3) d - juft son bo'lib,

$$d = \begin{cases} (a - 1) \bmod 4, & \text{agar } N \text{ soni } 4 \text{ ga karrali bo'lsa;} \\ (a - 1) \bmod 2, & \text{agar } N \text{ soni } 2 \text{ ga karrali bo'lsa.} \end{cases}$$

4) agarda N soni 9 ga karrali bo'lsa, u holda $d \bmod 9 = 0$ yoki $d \bmod 9 = 1$ va $cd \bmod 9 = 6$;

bajarilishi zarur va yetarli.

Shuningdek, $N = 2^q$ bo'lsa, maksimal davrni ta'minlash uchun d -toq bo'lishi va $a = (d + 1) \bmod 4$ bo'lishi yetarlidir.

Kvadratik kongruent generator $x_{i+1} = (x_i^2) \bmod p$, ($i \geq 0$) uchun 512 bit uzunlikka ega bo'lgan p va x_0 parametrlar quyidagicha olinishi tavsiya etiladi:

$p = 987b6a6bf2c56a97291c445409920032499f9ee7ad128301b5d$
 $0254aa1a9633f$
 $dbd378d40149f1e23a13849f3d45992f5c4c6b7104099bc301f600$
 $5f9d8115e1$;

$x_0 = 3844506a9456c564b8b8538e0cc15aff46c95e69600f084f0657c2401$
 $b3c244734b62$
 $ea9bb95be4923b9b7e84eeaf1a224894ef0328d44bc3eb3e983644da3f5$.

Kirish bit uzunligi 512 bit bo'lgan kubik kongruent generator $x_{i+1} = x_0^3 \bmod 2^{512}$ uchun esa kirish parametrini $x_0 = 7844506a9456c564b8b8538e0cc15aff46c95e69600f084f0657c2401b3c244734b62ea9bb95be4923b9b7e84eeaf1a224894ef0328d44bc3eb3e983644da3f5$ ko'rinishda tanlash maqsadga muvofiqdir.

Chiziqli va multiplikativ kongruent generatorlar kabi chiziqsiz generatorlar ham kriptotahlil usuliga bardoshsiz.

4.3. Oqimli shifrlarni qurish asoslari

Oqimli shifrlash algoritmlarini qurilmalarda amalga oshirish yuqori samaradorlikka ega bo'lgani bois, ko'plab real vaqt ilovalarida (masalan, telefon orqali so'zlashuvda) keng qo'llanilmoqda. Oqimli shifrlash algoritmlari simmetrik kriptotizim hisoblanib, blokli shifrlash algoritmlariga alternativ tur hisoblanadi. Simmetrik oqimli shifrlash algoritmlarini ishlash g'oyasi bir martali bloknotga (yoki Vernam shifri deb ataluvchi) asoslangan bo'lib, unga ko'ra ochiq matn uzunligiga teng bo'lgan bir martali kalit ketma-ketligi hosil qilinadi va u ochiq matn bilan XOR amalida qo'shiladi. Mazkur holda agar kalit ketma-ketligi to'liq tasodifiy va bir marta foydalanilsa, mazkur shifrlash usuli to'liq bardoshlikni ta'minlaydi. Biroq, ochiq matn uzunligiga mos bo'lgan kalitlarni generatsiya qilish va uni qabul qiluvchiga xavfsiz etkazish zaruriyati, Vernam shifrini to'liq amaliyotga tatbiq etish imkoniyatini bermaydi.

Oqimli shifrlash algoritmlarida ushbu muammo xavfsizlik darajasini pasaytirish orqali bartaraf etilgan, ya'ni, tomonlar o'rtasida ma'lum uzunlikdagi maxfiy kalit taqsimlanadi va u kalit ketma-ketligini hosil qilish uchun ishlatiladi. Maxfiy kalit simmetrik kalit bo'lib, psevdotasodifiy sonlar generatoriga (PTSG) kiritiladi va natijada undan ochiq matn uzunligiga teng bo'lgan kalit ketma-ketligi hosil qilinadi. Biroq, foydalanilgan PTSG to'liq tasodifiy va xavfsiz bo'lmagani bois, yaratilgan shifrlash algoritmi ham Vernam shifridek to'liq xavfsizlikni ta'minlamaydi. Shuning uchun odatda PTSGga buzg'unchi kalit ketma-ketligini bilgan taqdirda ham maxfiy kalitni bilmaslik talabi qo'yiladi.

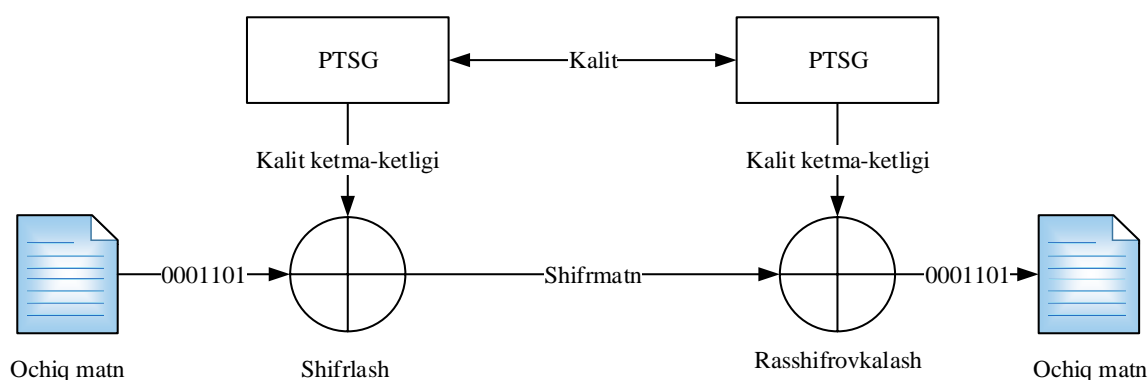
PTSGlaridan hosil bo'lgan ketma-ketliklar uchun takrorlanish oralig'i yetarlicha katta bo'lishi talab etiladi va u aynan xavfsizlik uchun muhim faktor hisoblanadi. Agar buzg'unchi takrorlanish oralig'ini bilish imkoniyatiga ega bo'lsa, u holda osonlik bilan shifratni rasshifrovkalaydi. Shuning uchun takrorlanish davri shifrlanuvchi ma'lumotning uzunligidan yetarlicha katta bo'lishi talab etiladi. Agar oqimli shifrlash algoritmida takrorlanish davri aniqlansa, maxfiy kalitni almashtirish yoki tasodifiy parametr (nonce) kiritish zaruriyati tug'iladi.

Oqimli shifrlash algoritmi to'liq sozlangandan so'ng, dastlabki hosil bo'lgan ma'lum uzunlikdagi ketma-ketliklardan foydalanish tavsiya etilmaydi. Buning asosiy sababi, kiritilgan maxfiy kalit asosida ketma-

ketliklarni hosil qilishda to‘liq “yaxshi aralashtirish” amalga oshirilmagani hisoblanadi.

Sinxronlashgan va o‘zi mustaqil sinxronlashuvchi shifrlar. Oqimli shifrlar ketma-ketlikni o‘zlarining ichki holatiga asosan hosil qilishadi. O‘z ichki holatini yangilash usuliga ko‘ra oqimli shifrlarni ikkiga ajratish mumkin.

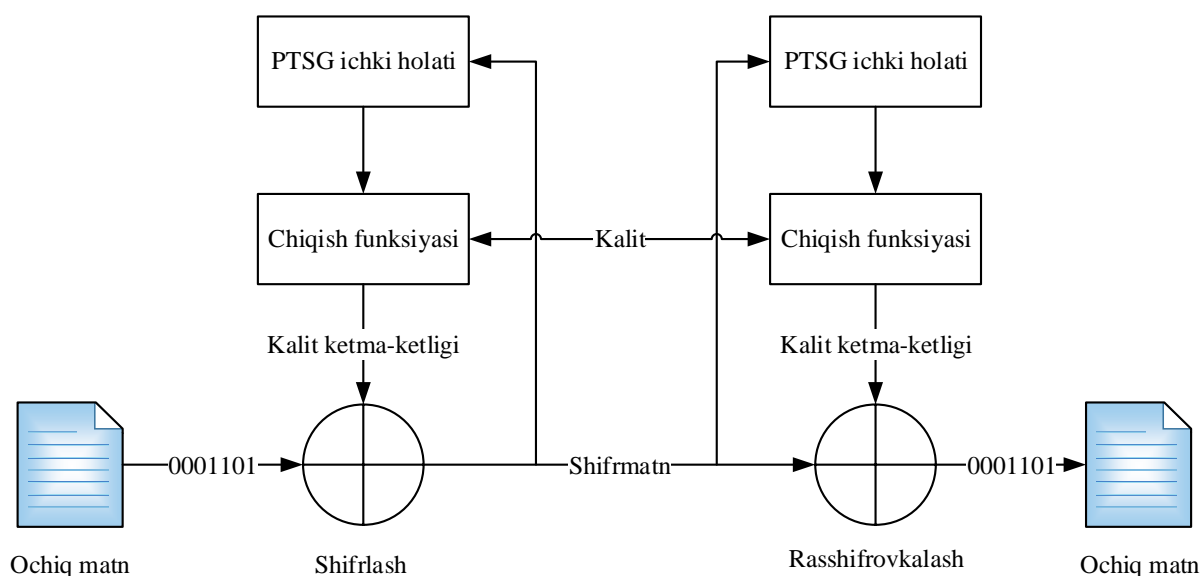
Sinxronlashgan oqimli shifrlash o‘z ichki holatini ochiq matn yoki shifrmatndan mustaqil ravishda yangilaydi. Shifrlash jarayoni boshlanishidan oldin tomonlardagi PTSGlari o‘z ichki holatlarini sinxronlashni amalga oshiradi. Agar shifrmatndagi yoki ochiq matndagi biror qism ma’lumotlar olib tashlansa yoki qo‘shilsa, sinxronlash buziladi. Bunda aloqani tiklash uchun qayta sinxronlash mexanizmi, yuqori hisoblash va murakkablikni talab etadi. Boshqa tomondan, shifrmatnning bir bitining o‘zgarishi ochiqmatnning ham bir bitini o‘zgarishiga sabab bo‘ladi va bu kam yo‘qotishni talab qiluvchi ilovalar (masalan, ovozli so‘zlashish yoki simsiz tarmoqlarda) uchun juda ham o‘rinlidir. 4.2-rasmda sinxron ravishda ishlovchi oqimli shifrlash algoritmlarining umumiy ko‘rinishi keltirilgan. Sinxronlashgan oqimli shifrlash aktiv hujumlarga (hujumchi aloqani uzishi va o‘zgartirilgan shifrmatn va unga mos ochiq matn orasidagi bog‘liqlikni topishi mumkin) zaif hisoblanadi. Ushbu turdagi shifrlarni tahlil qilishda ma’lum ochiqmatnga asoslangan usullardan keng foydalaniladi.



4.2-rasm. Sinxronlashgan oqimli shifrlash algoritmlari

O‘zi sinxronlashuvchi oqimli shifrlar ichki holatini shifrmatnning N bitiga ko‘ra yangilaydi va ushbu usulda shifrlashning umumiy ko‘rinishi 4.3-rasmda keltirilgan. O‘zi sinxronlashuvchi oqimli shifrlar yordamida qabul qiluvchi avtomatik ravishda N shifrmatn bitini qabul qilgandan so‘ng sinxronlash amalga oshiriladi. Bu imkoniyat shifrmatnga ba’zi bitlar qo‘shilganda yoki olib tashlanganda uni osonlik bilan tiklash

imkoniyatini taqdim qiladi. Agar shifrmtnning bir biti o'zgarishga uchrasa, ko'pi bilan N bit ochiq matn o'zgarishga uchrashi mumkin. Shuning uchun bu turdagi shifrlarga aktiv hujumni amalga oshirish murakkab hisoblanadi. Biroq, kriptografik nuqta nazaridan har bir o'zgargan bit ochiqmatning N bitiga ta'sir qilishi katta noqulaylikni olib keladi.

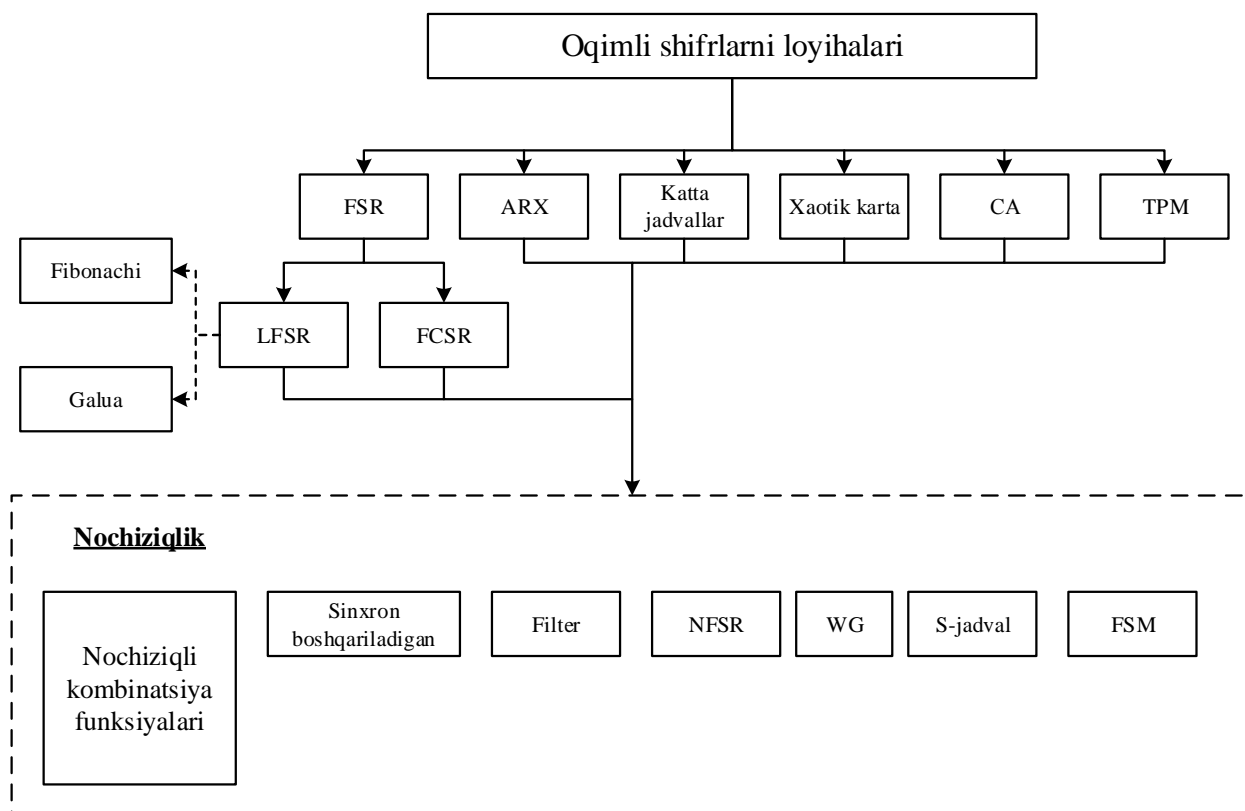


4.3-rasm. O'zi sinxronlashuvchi oqimli shifrlash usuli

Bundan tashqari, o'zi sinxronlashgan oqimli shifrlash usullari jiddiy xavfsizlik muammosiga ega. Kalit oldingi bitlar asosida yangilanganligi sabab, kalit ketma-ketligida statistik qonuniyat oshkor bo'lishi mumkin. O'zi sinxronlashuvchi oqimli shifrlar tanlangan shifrmtn bo'yicha hujumlarga bardoshsiz bo'lib, agar hujumchi shifrmtnning bir qismini deshifrlay olsa, u holda qolgan qismini ham deshifrlash imkoniyatiga ega bo'ladi. Bu esa o'zi sinxronlashuvchi oqimli shifrlarni xavfsiz tarzda loyihalash murakkab vazifa ekanligini anglatadi.

Har ikkala, sinxronlashgan va o'zi sinxronlashuvchi oqimli shifrlar ma'lumotlarni shifrlash/ rasshifrovkalash uchun foydalanilishi va balki, faqat noldan iborat ketma-ketlikni shifrlash orqali psevdotasodifiy sonlar generatori sifatida ham ishlatilishi mumkin.

Asosiy loyihalash usullari. Oqimli shifrlarni loyihalashga oid ma'lumotlar ko'plab manbalarda keltirilgan bo'lib, kam hisoblash imkoniyatiga ega qurilma va muhitlar uchun oqimli shifrlarni loyihalashning umumiy ko'rinishi 4.4-rasmda keltirilgan.



4.4-rasm. Oqimli shifrlarni loyihalashning tasnifi

Oqimli shifrlarni yaratishda asosan qayta aloqali siljitish registrlaridan (Feedback shift registers, FSR) foydalaniladi. Har bir siklda FSR kirish sifatida bir bitni qabul qiladi va chiqishda bir bitni taqdim qiladi. Kiruvchi bit oldingi holat funksiyasi hisoblanib, FSR funksiyasiga ko‘ra ikki turdagi FSR bo‘lishi mumkin: chiziqli qayta aloqali siljitish registri (Linear Feedback shift registers, LFSR) va qayta aloqali olib yuriluvchi siljitish registri (Feedback with carry shift registers, FCSR).

LFSR sxemasi oqimli shifrlar uchun keng tarqalgan usul hisoblanadi. Ular qurilmada amalga oshirishga qulay va tezkor hisoblanib, ularning xususiyatlari matematik tahlil qilinadi. Biroq, ular chiziqli tabiatga egaligi sababli, biror nochiziqli funksiya bilan ishlatilmasa xavfsiz emas. Siljitish amallariga ko‘ra ikki turdagi LFSR mavjud. Fibonachi LFSR usuli odatiydand bo‘lib, unda har bir bit o‘nga ko‘chiriladi va bitlar o‘nga siljiydi. O‘ng tomondagi eng chetki bit bu chiqish biti hisoblanadi. Chap tomon bitlari esa ba’zi maxsus bitlar asosida hisoblanadi. Galua LFSR usuli unga alternativ usuli bo‘lib, bitlar o‘nga siljiydi va bunda tanlangan bitlar o‘zgarishsiz qoladi. Nusxa olishdan oldin maxsus bitlarning eng o‘ngdagi oldingi chiqish biti bilan XOR amalida qo‘shiladi. Galua LFSR asosida yaratilgan shifrlar

Fibonachi LFSR asosida ishlab chiqilgan shifrlarga qaraganda qurilmalar uchun ko‘proq mos hisoblanadi.

FCSR oqimli shifrlarni yaratish yondashuvi LFSR ning arifmatik analogi hisoblanadi. Ular LFSR ga o‘xshash bo‘lib, faqat bir bosqichdan ikkinchi bochqichga o‘tishga ko‘mak berish uchun qo‘shimcha xotiradan iborat. Ushbu yondashuvni parallel arxitekturaga samarali amalga oshirish mumkin. Biroq, *FCSR* yondashuvi tabiiy holda takrorlanish davriga ega bo‘lgani bois, to‘g‘ridan-to‘g‘ri foydalanilmaydi.

FCSR ga asoslangan oqimli shifrlardan tashqari amalda qator alternativ variantlar ham mavjud. Masalan, modul bo‘yicha *qo‘shish*, *aylantirish* va *XOR* (add, rotate and XOR, ARX) amallariga asoslangan usullar juda ham mashhur bo‘lib, ular juda tezkor va amalga oshirish juda ham arzon. Ushbu amallar o‘zgarimas vaqtda yuklanadi va vaqt bo‘yicha hujumlarni yuzaga kelishini kamaytiradi. ARX amallariga asoslangan shifrlar tezkor va amalga oshirish uchun ancha ixcham hisoblansada, xavfsizlik nuqtai nazaridan mos emas.

Sodda amallarga asoslangan ARX yondashuvidan ko‘ra, dasturiy ta‘minot ko‘rinishida amalga oshirganda yuqori tezlikni taqdim qiluvchi *katta jadvallar* usuli mavjud. Katta jadvalda holat muhim ahamiyatga ega va uning kontenti nochiqli funksiyalar yordamida har bir raunda almashib boradi. Ushbu yondashuv ham dasturiy va ham apparat ta‘minotda katta xotira hajmini sarfi tufayli o‘ziga xos ahamiyatga ega.

Uyali avtomatika (Cellular automata, CA) bu – uyaning doimiy tarmog‘i bo‘lib, ularning har birida chekli sondagi holatlar mavjud. Har bir uya o‘z holatini belgilangan qonuniyatga ko‘ra yangilaydi. Har bir uyani holatini yangilash qonuniyati esa uyaning holati va uning qo‘shnisi holati asosida hisoblanadi. Berilgan qonuniyat bo‘yicha, keyingi holatlarni bilish oson bo‘lsada, oldingi holatlarni bilishni imkoni yo‘q. Kriptografiyada CAlar bir tomonlama funksiyalar kabi bo‘lib, unga teskari bo‘lgan funksiyani topish murakkab. Ularni apparat ko‘rinishida amalga oshirish qulay va dasturiy ko‘rinishda bosqichma-bosqich amalga oshirish ham samarali bo‘lishi mumkin. Bundan tashqari, parallel akslantirishlardan foydalanish ham mumkin bo‘lib, bu o‘tkazuvchanlik qobiliyatini yanada oshiradi.

Xaotik karta (Chaotic map) xaotik xususiyatga ega bo‘lgan taqdimotni amalga oshiruvchi karta. Ular iterativ funksiyalarga o‘xshash diskret vaqtli parametr orqali xarakterlanadi. Kriptografiyada ularning odatiy sozlanishi ochiq matn bilan kalit ketma-ketligini bitlararo amal yordamida aralashtirish hisoblanadi. Bunda PTSGidan hosil bo‘lgan

ketma-ketliklarni yaxshi tasodifiylik darajasiga egaligi muhim hisoblanadi. Bundan tashqari, bu turdagi shifrlash algoritmlarini apparat ko‘rinishda amalga oshirish yuqori samarali hisoblanadi.

Daraxt shoxli mashina (Tree Party Machine, TPM) ko‘p qatlamli oldinga siljuvchi neyron tarmoq hisoblanib, ular kriptografiyada keng tarqalgan tanlov hisoblanmasada, yuqori tasodifiylik darajasiga egaligi sababli oqimli shifrlarni yaratishda keng qo‘llaniladi.

Chiziqsizlik. LFSR loyihalashning xavfsizligini oshirish uchun ko‘plab sxemalar taklif etilgan va ularda nochiziqli funksiyalardan foydalanish tavsiya etilgan. Masalan, ular o‘z ichiga nochiziqli kombinatsiya funksiyalarini, vaqtga asosan boshqariluvchi generatorlarni va filter generatorlarini oladi. Nochiziqli kombinatsiya funksiyalari bilan, bir qancha parallel LFSRlarning chiqishlari nochiziqli bul funksiyasiga kiritiladi. Odatiy sozlanishda, LFSR doimiy holatda siljiydi. Generator ta’sir qiluvchi LFSR esa boshqa LFSRning chiqishiga ko‘ra siljishni amalga oshiradi. Agar filter funksiyalari foydalanilganda, LFSRning butun holati nochiziqli funksiyaga kiritiladi. Ushbu funksiyalarning birlashgan holatda foydalanilgan ko‘rinishlari ham mavjud.

Nochiziqli qayta aloqali siljitivchi registorlar (Non-linear feedback shift registers, NFSR) usuli ham oqimli shifrlarni nochiziqligini ta’minlash uchun foydalaniluvchi o‘zak komponentlardan biri hisoblanadi. Bundan tashqari, u kriptotahlil usullariga ham bardoshli hisoblanadi va ularga oid kam sonli nazariy tahlil natijalari mavjud. NFSR usulidagi shifrlarni kriptotahlilga bardoshligi, uning murakkabligi bilan belgilanadi. Ularni apparat ko‘rinishda amalga oshirish LFSR va FCSR larga qaraganda murakkab hisoblanadi. Bundan tashqari, NFSR ko‘rinishidagi shifrlarni yaratishning o‘zi ham qiyin vazifa hisoblanadi.

Welch-Gong (WG) funksiyalari NFSR ga o‘xshamagan boshqa oilaga tegishli struktura bo‘lib, ularni matematik tahlil qilish mumkin. Ular turli darajadagi tasodifiylik darajasini qayd qilishi tasdiqlangan bo‘lib, ular shifrlash va autentifikatsiyalash uchun muhim ahamiyat kasb etadi.

S-jadvallar (Substitution-boxes, S-box) o‘zida almashtirishni amalga oshiradi va kirishdagi m bitni chiqishda n bitga akslantiradi. Ular blokli shifrlar uchun muhim komponent bo‘lib, kalit va ochiq matn o‘rtasidagi bog‘liqlikni kamaytirishga xizmat qiladi. Bundan tashqari S-jadvallar oqimli shifrlarda nochiziqlikni ta’minlash uchun ham keng qo‘llaniladi.

Chekli holatli mashinalar (Finite state machine, FSM) hisoblash ketma-ketligi mantiq'i uchun matematik model hisoblanadi. Har bir vaqtda FSM ko'p sonli holatlarning birida bo'ladi. Yangi holatga o'tish harakatlantiruvchi hodisa yoki shart natijasida amalga oshiriladi. Oqimli shifrlarni yaratishda FSMlar dasturiy ta'minot ko'rinishida yaxshi ishlaydi va turli tahdidlarni oldini oladi.

4.4. A5/1 oqimli shifrlash algoritmi

Ushbu oqimli shifrlash algoritmidan GSM mobil aloqa tizimlarida ma'lumotlarni konfidensialligini ta'minlashda foydalaniladi. Mazkur algoritm algebraik tuzilishga ega bo'lsada, uni sodda diagramma ko'rinishda ham tasvirlash imkoniyati mavjud.

A5/1 shifrlash algoritmi uchta *chiziqli siljitish registrlaridan* iborat, ular mos holda X, Y va Z kabi belgilanadi. X registr o'zida 19 bit $(x_0, x_1, \dots, x_{18})$, Y registr 22 bit $(y_0, y_1, \dots, y_{21})$ va Z registr 23 bit $(z_0, z_1, \dots, z_{22})$ ma'lumotni saqlaydi. Uchta registrning bunday o'lchamdagi bitlarni saqlashi bejiz emas. Sababi, chiziqli siljitish registrlari o'zida jami 64 bitni saqlaydi. A5/1 shifrlash algoritmidan foydalaniluvchi kalit K ning uzunligi 64 bitga teng va ushbu kalitdan registrlarni dastlabki to'ldirish uchun foydalaniladi. So'ngra oqimli shifrlash algoritmi asosida talab etilgan uzunlikdagi (ochiq matn uzunligiga teng bo'lgan) ketma-ketliklar generatsiyalanadi. Ketma-ketliklarni generatsiyalash tartibini o'rganishdan oldin, registrlar xususidagi ba'zi ma'lumotlarni bilish talab etiladi.

X siljitish registrida quyidagi amallar ketma-ketligi bajariladi:

$$t = x_{13} \oplus x_{16} \oplus x_{17} \oplus x_{18}$$

$$i = 18, 17, 16, \dots, 1 \text{ uchun } x_i = x_{i-1}, x_0 = t$$

Shunga o'xshash, Y va Z registrlar uchun ham quyidagilarni yozish mumkin:

$$t = y_{20} \oplus y_{21}$$

$$i = 21, 20, 19, \dots, 1 \text{ uchun } y_i = y_{i-1}, y_0 = t$$

va

$$t = z_7 \oplus z_{20} \oplus z_{21} \oplus z_{22}$$

$$i = 22, 21, 20, \dots, 1 \text{ uchun } z_i = z_{i-1}, z_0 = t$$

Berilgan uchta bit x, y va z uchun $maj(x, y, z)$ funksiya qiymati eng ko‘p bitga teng bo‘ladi. Masalan, agar x, y va z bitlar 0 ga teng bo‘lsa, u holda funksiyaning qiymati 0 ga teng bo‘ladi. Funksiyaga kiruvchi bitlar toq bo‘lgani uchun, funksiya har doim 0 ni yoki 1 ni qaytaradi. Boshqa holatlar bo‘lmaydi.

A5/1 shifrida, ketma-ketlikning har bir bitini generatsiyalash uchun quyidagilar bajariladi. Dastlab, $m = maj(x_8, y_{10}, z_{10})$ funksiya qiymati hisoblanadi. So‘ngra X, Y va Z registrlar quyidagicha sijitiladi (yoki siljiti olmaydi):

- agar $x_8 = m$ ga teng bo‘lsa, X siljiriladi;
- agar $y_{10} = m$ ga teng bo‘lsa, Y siljiriladi;
- agar $z_{10} = m$ ga teng bo‘lsa, Z siljiriladi.

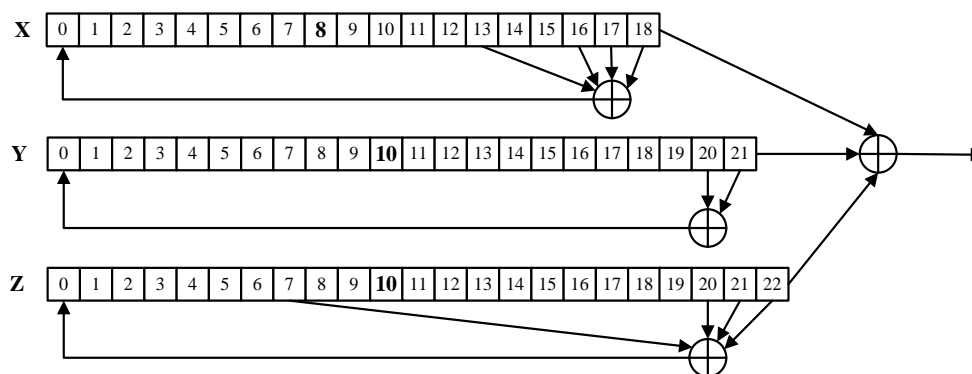
Ketma-ketlikning bir biti s quyidagicha generatsiyalanadi:

$$s = x_{18} \oplus y_{21} \oplus z_{22}$$

Yuqorida keltirilgan ketma-ketlik amallari talab etilguncha takrorlanadi (ochiq matn yoki shifratn uzunligiga teng).

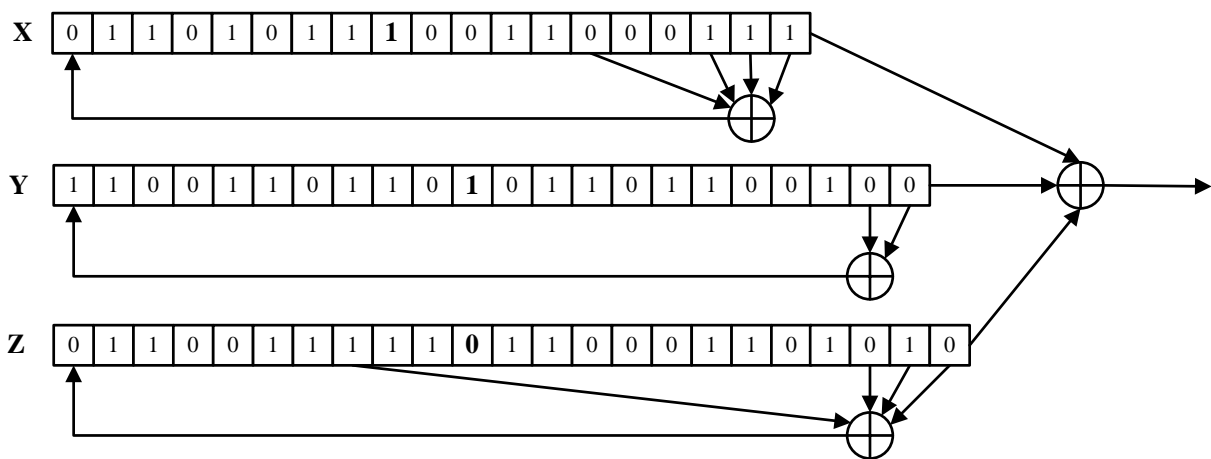
Agar biror registr siljirilsa, uning to‘liq holati o‘zgaradi. Ketma-ketlikning bir bitini hosil qilishda uchta registrdan kamida ikkitasi siljiydi va shuning uchun yuqoridagi ketma-ketlikni davom ettirgan holda yangi bitlar ketma-ketligini hosil qilish mumkin.

A5/1 oqimli shifrlash algoritmi murakkab ko‘rinsada, qurilmada amalga oshirilganida yuqori tezlik qayd etiladi. Umumiy holda A5/1 oqimli shifrni 4.5-rasmdagi kabi ifodalash mumkin.



4.5-rasm. A5/1 ketma-ketlik generatorining umumiy ko‘rinishi

Misol. Faraz qilaylik, 64 bitli kalit K ni X, Y va Z registrlariga bo‘lib yozish natijasi quyidagicha bo‘lsin (4.6-rasm).



4.6-rasm. X, Y va Z registrlarining dastlabki holati

Mazkur holda $maj(x_8, y_{10}, z_{10}) = maj(1, 1, 0) = 1$ va bu X va Y registrlar siljishini ko'rsatadi. Shuning uchun,

$$t = x_{13} \oplus x_{16} \oplus x_{17} \oplus x_{18} = 0 \oplus 1 \oplus 1 \oplus 1 = 1$$

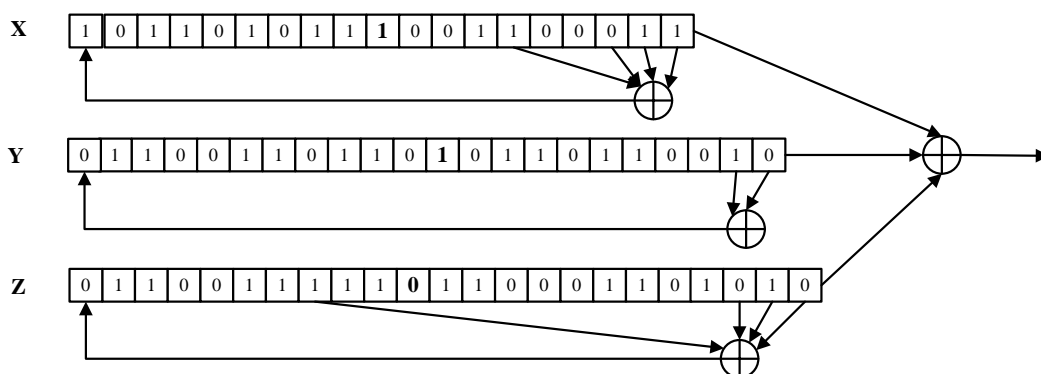
$$i = 18, 17, 16, \dots, 1 \text{ uchun } x_i = x_{i-1}, x_0 = 1$$

Shunga o'xshash, Y registr uchun ham quyidagilarni yozish mumkin:

$$t = y_{20} \oplus y_{21} = 0 \oplus 0 = 0$$

$$i = 21, 20, 19, \dots, 1 \text{ uchun } y_i = y_{i-1}, y_0 = 0$$

X va Y registrlar siljiganidan keyingi holat quyidagicha (4.7-rasm):



4.7-rasm. X, Y va Z registrlarining siljiganidan keyingi holati

Siljigan holatdan so'nggi registrlar holatidan generatsiyalangan bir bit $s = x_{18} \oplus y_{21} \oplus z_{22} = 1 \oplus 0 \oplus 0 = 1$. Shu tartibda talab etilgan bitlar ketma-ketligi generatsiyalanadi.

4.5. RC4 oqimli shifrlash algoritmi

Rivest Cipher 4 yoki RC4 oqimli shifrlash algoritmlari dasturiy vosita ko‘rinishida amalga oshirishga qulay bo‘lgan eng mashhur algoritmlardan biri bo‘lib, Wired Equivalent Privacy (WEP), Wi-Fi Protected Access (WPA) va Transport Layer Security (TLS) kabi protokollarda keng qo‘llanilmoqda. Ushbu shifrlash algoritmi sodda tuzilishga ega va shuning uchun katta tezkorlik qayd etadi. U LFSR yondashuviga asoslangan bo‘lib, undan farqli ravishda bit emas, balki bayt ko‘rinishdadir.

RC4 shifrini ishga tushirish ikki qismdan iborat:

1. S blokni shakllantirish;
2. Pseudotasodifiy ketma-ketlik K ni generatsiyalash.k.

S blokni shakllantirish.k. Algoritm kirishda foydalanuvchidan L bayt uzunlikdagi kalit Key ni talab etadi. Ushbu bosqich S massivni to‘ldirish bilan boshlanib, uning elementlari keyinchalik kalitga bog‘liq holda almashtiriladi. Ushbu bosqichning psevdokodi quyida keltirilgan:

```
for i from 0 to 255
    S[i] := i
endfor
j := 0
for i from 0 to 255
    j := ( j + S[i] + Key[ i mod L ] ) mod 256
    Swap(S[i],S[j]) // elementlar o‘rnini
almashtirish
endfor
```

Pseudotasodifiy ketma-ketlik K ni generatsiyalash.k. Algoritmning ushbu qismi generator deb nomlanadi. Generator har bir qadamda S blokdagi bir baytni pseudotasodifiy bayt sifatida taqdim etadi. Har bir bosqich uchun mos elementlar o‘rni almashtiriladi. Ushbu bosqichning psevdokodi quyida keltirilgan:

```
i := 0
j := 0
while generatsiyalash sharti:
    i := (i + 1) mod 256
```

```

    j := (j + S[i]) mod 256
    Swap(S[i], S[j])
    t := (S[i] + S[j]) mod 256
    K := S[t]
endwhile

```

Psevdokodda keltirilgan siklning har bir bosqichida bir bayt psevdotasodifiy qiymat hosil bo‘ladi va uni ochiq matnning bir baytiga qo‘shish orqali shifrlash amalga oshiriladi. Shu sababli, siklni ochiq matnning baytdagi uzunligicha davom etishini bilish mumkin.

RC4 shifrlash algoritmi ham dasturiy ham apparat ko‘rinishlarda amalga oshirish uchun qulay hisoblanadi. Biroq, ishlab chiqilganiga ancha muddat bo‘lgani va kalitni almashtirishda muammolar mavjudligi sababli, xavfsiz emas deb topilgan, xususan, protokollarda *nonce* va kalitning alohida-alohida yuborilmasligi va ular asosida kalit ketma-ketligini yaratish jarayoni. Bu holda bo‘lishi mumkin bo‘lgan yechimlardan biri bu – kalit va *nonce* kattaliklarini bardoshli MAC algoritmlari asosida xeshlash hisoblanadi. Hosil bo‘lgan kalit ketma-ketliklari asosiy kalitga bog‘liq bo‘lgani bois, WEP protokolini buzishga asos bo‘lgan. RC4 algoritmiga amalga oshirilgan oxirgi hujumlardan biri 224 ta ulanishni talab qilgan. Shifrnı o‘ziga amaliy tomondan hujumlar bo‘lmagan bo‘lsada, eng so‘ngi hisoblash imkoniyatlari va ilmiy ishlar buni amalga oshirish imkoniyatlari mavjudligini ko‘rsatmoqda.

4.6. SEAL oqimli shifrlash algoritmi

SEAL (Software-Optimized Encryption Algorithm) algoritmi dasturiy ko‘rinishda amalga oshirish uchun mo‘ljallangan bo‘lib, IBM tashkilotida Phil Rogaway va Don Coppersmith tomonidan ishlab chiqilgan. Algoritm 32 bitli protsessorlar uchun optimallashtirilgan bo‘lib, amalga oshirish uchun 8 ta 32 bitli register va bir necha kilobaytlar talab etiladi. Nisbatan sekinroq operatsiyalarnı qo‘llagan holda SEAL algoritmi jadvallar to‘plamida muhim amallarnı oldindan amalga oshiradi. Ushbu jadvallar keyinchalik kalit sifatida foydalanilib, shifrlash va rasshifrovkalashda tezkorlikni oshirishga xizmat qiladi.

SEAL algoritmining yuqorida keltirilgan ananaviy oqimli shifrlardan farqi, u psevdotasodifiy funksiyalar oilasiga tegishligi hisoblanadi. Berilgan 160 bitli kalit k va 32 bitli n uchun SEAL algoritmi n ni L bitli $k(n)$ ga kengaytiradi. Bu yerda, L kattalik 64 kilobaytdan

kichik ixtiyoriy qiymatni olishi mumkin. Ushbu bosqich natijasida 3 ta jadval, R , S va T hosil qilinadi.

Ushbu jadvallarni hosil qilishda $SHA1$ xesh funksiyasida foydalanilgan muolajalardan foydalanilgan. Umumiy holda jadvallarni hosil qilish funksiyasini 160 bit qiymat qaytaruvchi $G_k(n)$ ko‘rinishida ifodalash mumkin.

Quyidagi funksiya va o‘zgaruvchilar indeks t ga bog‘liq bo‘ladi:

– $0 \leq t \leq 19$ uchun $K_t = 0x5a827999$ va $f_t(B, C, D) = (B \wedge C) \vee (B \wedge D)$;

– $20 \leq t \leq 39$ uchun $K_t = 0x6ed9eba1$ va $f_t(B, C, D) = B \oplus C \oplus D$;

– $40 \leq t \leq 59$ uchun $K_t = 0x8f1bbcdc$ va $f_t(B, C, D) = (B \wedge C) \vee (B \wedge D) \vee (C \wedge D)$;

– $60 \leq t \leq 79$ uchun $K_t = 0xca62c1d6$ va $f_t(B, C, D) = B \oplus C \oplus D$.

Shundan so‘ng, 160 bitli k kalit 5 ta 32 bitli qismga ajratiladi: $k = H_0 \parallel H_1 \parallel H_2 \parallel H_3 \parallel H_4$.

Shuningdek, 16 ta 32 bitli so‘zlar quyidagicha hosil qilinadi: $W_0 = n$, $W_1 = W_2 = \dots = W_{15} = 0^{32}$.

Shundan so‘ng quyidagi hisoblashlar amalga oshiriladi:

1. $16 \leq t \leq 79$ uchun $W_t = (W_{t-3} \oplus W_{t-8} \oplus W_{t-14} \oplus W_{t-16}) \lll 1$;

2. $A = H_0, B = H_1, C = H_2, D = H_3, E = H_4$;

3. $0 \leq t \leq 79$ uchun:

$$TEMP = A \lll 5 + f_t(B, C, D) + E + W_t + K_t;$$

$$E = D, D = C, C = B \lll 30, B = A, A = TEMP;$$

4. $H_0 = H_0 + A, H_1 = H_1 + B, H_2 = H_2 + C, H_3 = H_3 + D, H_4 = H_4 + E$.

5. $G_k(n) = H_0 \parallel H_1 \parallel H_2 \parallel H_3 \parallel H_4$.

$$j = \lfloor i/5 \rfloor \text{ uchun } H_0^{5j} \parallel H_1^{5j+1} \parallel H_2^{5j+2} \parallel H_3^{5j+3} \parallel H_4^{5j+4} = G_k(j)$$

bo‘lgan $\Gamma_k(i) = H_{i \bmod 5}^i$ funksiyani kiritamiz. Ushbu funksiya 160 bitli $G_k(j)$ dan 32 bitli $\Gamma_k(i)$ ni olishga imkon beradi.

Shundan so‘ng, quyidagi uchta jadvalni hosil qilinadi:

$$T[i] = \Gamma_k(i), 0 \leq i < 512;$$

$$S[j] = \Gamma_k(0x1000 + j), 0 \leq j < 256;$$

$$R[k] = \Gamma_k(0x2000 + k), 0 \leq k < 256.$$

Shundan so‘ng, kalit k foydalanilmaydi.

Xizmat registrlarini qiymatlash.k. Pseudotasodifiy ketma-ketliklarni generatsiyalashdan oldin 4 ta 32 bitli xizmat registrlari (A, B, C va D) va 4 ta 32 bitli soʻzlarni (n_1, n_2, n_3 va n_4) hosil qilish kerak boʻladi. Ularning qiymatlari R va T jadvallarning qiymatlari, 32 bitli son n va l butun sonlari asosida quyidagicha hosil qilinadi:

Initialize($n, l, A, B, C, D, n_1, n_2, n_3, n_4$)

$A \leftarrow n \oplus R[4l];$

$B \leftarrow (n \ggg 8) \oplus R[4l + 1];$

$C \leftarrow (n \ggg 16) \oplus R[4l + 2];$

$D \leftarrow (n \ggg 24) \oplus R[4l + 3].$

for $j \leftarrow 1$ *to* 2 *do*

$P \leftarrow A \wedge 0x7fc; B \leftarrow B + T[P/4]; A \leftarrow A \ggg 9;$

$P \leftarrow B \wedge 0x7fc; C \leftarrow C + T[P/4]; B \leftarrow B \ggg 9;$

$P \leftarrow C \wedge 0x7fc; D \leftarrow D + T[P/4]; C \leftarrow C \ggg 9;$

$P \leftarrow D \wedge 0x7fc; A \leftarrow A + T[P/4]; D \leftarrow D \ggg 9;$

$(n_1, n_2, n_3, n_4) \leftarrow (D, B, A, C).$

$P \leftarrow A \wedge 0x7fc; B \leftarrow B + T[P/4]; A \leftarrow A \ggg 9;$

$P \leftarrow B \wedge 0x7fc; C \leftarrow C + T[P/4]; B \leftarrow B \ggg 9;$

$P \leftarrow C \wedge 0x7fc; D \leftarrow D + T[P/4]; C \leftarrow C \ggg 9;$

$P \leftarrow D \wedge 0x7fc; A \leftarrow A + T[P/4]; D \leftarrow D \ggg 9.$

Pseudotasodifiy ketma-ketliklarni generatsiyalash.k. SEAL algoritmidagi pseudotasodifiy ketma-ketliklarni generatsiyalashning asosiy funksiyasi $SEAL(k, n, L)$ quyidagicha amalga oshiriladi:

SEAL(k, n, L):

$y = 0^L;$

for $l \leftarrow 0$ *to* ∞ *do*

Initialize($n, l, A, B, C, D, n_1, n_2, n_3, n_4$)

for $i \leftarrow 1$ *to* 64 *do*

$P \leftarrow A \wedge 0x7fc; B \leftarrow B + T[P/4]; A \leftarrow A \ggg 9; B \leftarrow B \oplus A;$

$Q \leftarrow B \wedge 0x7fc; C \leftarrow C \oplus T[Q/4]; B \leftarrow B \ggg 9; C \leftarrow C + B;$

$P \leftarrow (P + C) \wedge 0x7fc; D \leftarrow D + T[P/4]; C \leftarrow C \ggg 9; D \leftarrow D \oplus C;$

$Q \leftarrow (Q + D) \wedge 0x7fc; A \leftarrow A \oplus T[Q/4]; D \leftarrow D \ggg 9;$

$A \leftarrow A + D;$

$P \leftarrow (P + A) \wedge 0x7fc; B \leftarrow B \oplus T[P/4]; A \leftarrow A \ggg 9;$

$Q \leftarrow (Q + B) \wedge 0x7fc; C \leftarrow C + T[Q/4]; B \leftarrow B \ggg 9;$

$$\begin{aligned}
P &\leftarrow (P + C) \wedge 0x7fc; D \leftarrow D \oplus T[P/4]; C \leftarrow C \ggg 9; \\
Q &\leftarrow (Q + D) \wedge 0x7fc; A \leftarrow A + T[Q/4]; D \leftarrow D \ggg 9; \\
y &\leftarrow y \parallel B + S[4i - 4] \parallel C \oplus S[4i - 3] \parallel D + S[4i - 2] \parallel \\
&A \oplus S[4i] - 1;
\end{aligned}$$

agar $|y| \geq L$ bo'lsa, u holda $y_0 y_1 \dots y_{L-1}$ qaytarish;

agar $odd(i)$ bo'lsa, u holda $(A, B, C, D) \leftarrow (A + n_1, B + n_2, C \oplus n_1, D \oplus n_2)$;

aks holda $(A, B, C, D) \leftarrow (A + n_3, B + n_4, C \oplus n_3, D \oplus n_4)$.

SEAL algoritmi ochiq matnning bir baytini shifrlash uchun 5 ta elementar mashina amalini talab qiladi. Ushbu algoritm 50 MHz chastotali Intel 80486 mashinasida sekundiga 58 Mbit ma'lumotni shifrlash imkonini beradi.

4.7. WAKE oqimli shifrlash algoritmi

WAKE (Word Auto Key Encryption, avtomatik kalitda so'zlarni shifrlash) algoritmi David Wheeler tomonidan 1993 yilda yaratilgan. Ushbu algoritm 32 bitli so'zlar ketma-ketligini generatsiyalab, ularni ochiq matn belgilariga XOR amalida qo'shish bilan shifratni hosil qiladi.

Ushbu algoritm CFB (Cipher Feedback Mode) rejimida ishlaydi. Ya'ni, oldingi shifratni keyingisi uchun xizmat qiladi. Shifrlash algoritmidan 32 bit so'zlar ustida amallar bajariladi va dastlabki kalitning uzunligi 128 bitga teng bo'ladi. Ushbu algoritmda ham S blokdan foydalanilgan bo'lib, har biri 32 bit bo'lgan 256 ta elementdan iborat. Algoritm yetarlicha tezkor bo'lib, bir bayt uchun 6.38 ta siklni talab etadi. Bu ko'rsatkich SEAL algoritmiga nisbatan yomon ko'rsatkich bo'lsada, RC4 algoritmiga qaraganda yaxshi ko'rsatkich hisoblanadi (mos holda 3.5 ga 10.6 ta sikl).

Shifrlash jarayoni uchta bosqichdan iborat:

1. S blokni generatsiyalash.k.
2. Avtomatik kalitni generatsiyalash.k.
3. Shifrlash va rasshifrovkalash jarayoni.

S blokni generatsiyalash.k. Dastlabki kalitdan S blokning birinchi elementlari generatsiya qilinib, qolganlari quyidagicha hosil qilinadi:

1. S blokni shakllantirishda quyidagi 8 ta 32 bitli so'zlardan foydalaniladi:

$s[0]: 0x726a8f3b;$

$s[1]: 0xe69a3b5c;$

$s[2]: 0xd3c71fe5;$

$s[3]: 0xab3c73d2;$

$s[4]: 0x4d3a8eb3;$

$s[5]: 0x0396d6e8;$

$s[6]: 0x3d4c2f7a;$

$s[7]: 0x9ee27cf3.$

2. S ning dastlabki 4 elementi kalitdan quyidagicha hosil qilinadi:

$S[0] \dots S[3]: S[0] = K[0]; S[1] = K[1]; S[2] = K[2]; S[3] = K[3].$

Bu yerda, $K[0]$, $K[1]$, $K[2]$ va $K[3]$ lar dastlabki kalitning 4 ta teng qismi.

3. S blokning qolgan elementlari quyidagicha hisoblanadi:

for $n = 4$ to 255:

$$x = S[n - 1] + S[n - 4]$$

$$S[n] = x \gg 3 \oplus s[x \wedge 7].$$

4. Shundan soʻng, quyidagi yigʻindi hisoblanadi:

for $n = 0$ to 22:

$$S[n] += S[n + 89];$$

Yigʻindini hisoblash, kalitning barcha bitini bir qancha S blok elementlariga bogʻlashga xizmat qiladi.

5. Quyidagi yordamchi oʻzgaruvchilar aniqlanadi:

$$X = S[33];$$

$$Z = S[59] \vee 0x01000001;$$

$$Z = Z \wedge 0xFF7FFFFFFF;$$

$$X = (X \wedge 0xFF7FFFFFFF) + Z.$$

6. S jadvaldagi soʻzlarning birinchi bayti quyidagicha almashtiriladi:

for $n = 0$ to 255:

$$X = (X \wedge 0xFF7FFFFFFF) + Z;$$

$$S[n] = S[n] \wedge 0x00FFFFFF \oplus X.$$

7. Quyidagi oʻzgaruvchini shakllantirish:

$$S[256] = S[0];$$

$$X = X \wedge 255;$$

8. S blok elementlari oʻrnini almashtirish:

for $n = 0$ to 255:

$$Temp = (S[n \oplus X] \oplus X) \wedge 255;$$

$$S[n] = S[Temp];$$

$$S[X] = S[n + 1].$$

Avtomatik kalitni generatsiyalash.k. Ushbu jarayon quyidagicha amalga oshiriladi:

1. Dastlab kalit K (balki boshqa kalit ham bo‘lishi mumkin) dan $R3$, $R4$, $R5$, $R6$ registor qiymatlari quyidagicha o‘zlashtiriladi:

$$R3[0] = K[0]; R4[0] = K[1];$$

$$R5[0] = K[2]; R6[0] = K[3].$$

Bu yerda, $K[0]$, $K[1]$, $K[2]$ va $K[3]$ lar dastlabki kalitning (yoki boshqa kiritilganning) 4 ta teng qismi.

2. Avtomatik kalitlar ketma-ketligi quyidagicha hisoblanadi:

$$R3[i + 1] = M(R3[i], R6[i], S);$$

$$R4[i + 1] = M(R4[i], R3[i], S);$$

$$R5[i + 1] = M(R5[i], R4[i], S);$$

$$R6[i + 1] = M(R6[i], R5[i], S).$$

3. Pseudotasodifik ketma-ketlikning navbatdagi so‘zi chetki registr qiymatiga teng bo‘ladi:

$$K_{i+1} = R6[i + 1].$$

Bu yerda, $M(x, y, S) = (x + y) \gg 8 \oplus S[(x + y) \wedge 255]$ ga teng.

Nazorat savollari

1. Tasodifiy ketma – ketliklarni shakllantiruvchi generatorlar va ularning turlari.

2. Entropiya to‘plovchilar va ularning afzalliklari, kamchiliklari.

3. Pseudotasodifiy sonlar generatori va uning kriptografik algoritmlardagi ahamiyati.

4. Chiziqli va chiziqsiz kongurent generatorlarni tushuntiring.

5. Simmetrik oqimli shifrlar va ularni ma’lumotni shifrlashdagi o‘ziga xos xususiyatlarini ayting.

6. Oqimli shifrlarni qurish usullari haqida ayting.

7. A5/1 oqimli shifrlash algoritmi va uning matematik asosi.

8. RC4 oqimli shifrlash algoritmi va uning matematik asosi.

9. SEAL oqimli shifrlash algoritmi va uning matematik asosi.

10. WEAK oqimli shifrlash algoritmi va uning matematik asosi.

11. Oqimli shifrlarning kelajagi haqida gapiring.

5 BOB. SIMMETRIK BLOKLI SHIFRLASH ALGORITMLARI

5.1. Simmetrik blokli shifrlar va ularni qurish usullari

Simmetrik blokli shifrlash algoritmlari barcha kriptografik tizimlarning muhim tashkil etuvchisi sanaladi. Simmetrik blokli shifrlash algoritmlari ma'lumot maxfiylikini ta'minlab, ma'lumotlarni ma'lum uzunlikdagi bloklarga bo'lgan holda ular ustida takroriy holatda amallarni bajarish orqali amalga oshiriladi.

Simmetrik blokli shifrlash algoritmlariga tegishli bo'lgan asosiy tushunchalar quyidagilar:

Blok uzunligi. Kiruvchi ma'lumotlarning bo'linishi kerak bo'lgan uzunligi bo'lib, odatda Feystel tarmog'iga asoslangan tizimlar uchun 64-bitni tashkil etadi.

Kalit uzunligi. Ma'lumotni shifrlashda va rasshifrovkalashda foydalanilgan kalitlarning uzunligi.

Raundlar soni. Blokli shifrlash algoritmlariga xos bo'lgan xususiyat bo'lib, bir ma'lumot bloki ustida turli kalitlardan foydalangan holda bajariladigan bir xil funksiyani bajaralish sonini ko'rsatadi. Masalan, DES shifrlash algoritmida raundlar soni 16 tani tashkil etadi.

Raund funksiyasi. Shifrlash va rasshifrovkalash algoritmlarining muhim qismi sanalib, har bir raundda bajariladigan ishlar ketma-ketligidan iborat bo'ladi. Ushbu funksiyada odatda ikkita kiruvchi qiymat, ma'lumot qismi va kalit bo'ladi.

Raund kaliti. Shifrlashda va rasshifrovkalashda foydalaniladigan kalit sanalib, dastlabki kalit asosida ma'lum algoritm yordamida hosil qilinadi.

Shifrlash rejimlari. Simmetrik blokli shifrlash algoritmlariga xos bo'lgan xususiyat bo'lib, blokli shifrlash algoritmlaridan ma'lum usullar asosida foydalanishga asoslanadi. Bunda shifrlash algoritmi o'zgartirilmay, balki ushbu algoritm asosida tizim quriladi.

Boshlang'ich vektor (initialization vector, IV). Blokli shifrlash algoritmlari rejimlaridan foydalanishda kerakli bo'lgan kattalik bo'lib, maxfiy tutilmaydi.

Shifrlash funksiyasi. Ochiq ma'lumot bloklarini yashiringan holda o'tkazish uchun foydalaniladigan funksiya.

Rasshifrovkalash funksiyasi. Shifrlangan matn bloklarini ochiq matnga aylantirish uchun foydalanilgan funksiya.

Zamonaviy simmetrik shifrlash algoritmlarida umumiy holda quyidagi matematik amallardan foydalaniladi:

- XOR amali;
- $\text{mod}2^{32}$ bo'yicha qo'shish amali;
- chapga yoki o'nga siklik surish amallari;
- jadvallar asosida o'rin almashtirish;
- mantiqiy amallar, VA, YOKI, INKOR;
- va h.k.

Zamonaviy blokli shifrlash algoritmlari yaratilish asosiga ko'ra quyidagi uchta asosiy yo'nalishga bo'linadi:

- Feystel tarmog'iga asoslangan;
- SPN (Substitution-permutation networks) asoslangan;
- Lai-Massey arxitekturasida asoslangan.

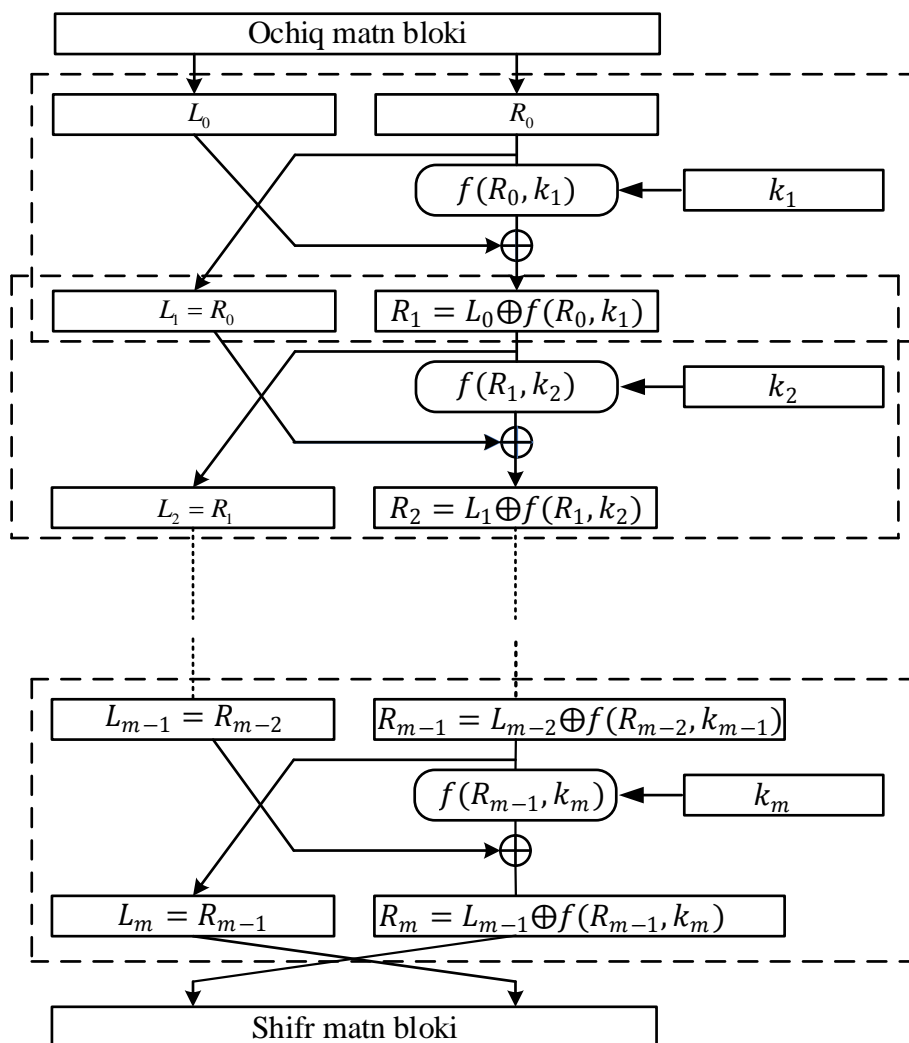
Feystel tarmog'iga asoslangan simmetrik blokli shifrlash algoritmlari. Ushbu yo'nalishga ko'ra ochiq matn bloklari teng ikki qismga ajratilib, biror yarim qism ustida (odatda o'ng qism ustida) kalit bilan amallar bajariladi va ikkinchi qism tomon bilan XOR amalida qo'shiladi. Shundan so'ng, ikki qism tomon o'rinlari almashtiriladi. Algoritmida berilgan raundlar soniga ko'ra $(0, 1, \dots, n)$ raund kalitlari hosil qilinadi (k_0, k_1, \dots, k_n) . Raund funksiyasi sifatida esa ikkita parametрни qabul qiluvchi f funksiyasidan foydalaniladi (5.1-rasm).

Feystel tarmog'ining asosiy amallari quyidagilar:

- ochiq matn bloki teng ikki qismga bo'linadi (L_0, R_0) ;
- har bir raund uchun quyidagilar bajariladi: $L_{i+1} = R_i, R_{i+1} = L_i \oplus f(R_i, k_i)$;
- shundan so'ng shifrmtn olinadi : (R_{n+1}, L_{n+1}) .

Rasshifrovkashda esa (R_{n+1}, L_{n+1}) shifrmtn blokidan kalitlarni teskari tartibda $(i = n, n - 1, \dots, 0)$ foydalanib, quyidagi amallar bajariladi: $R_i = L_{i+1}, L_i = R_{i+1} \oplus f(L_{i+1}, k_i)$. Shundan so'ng, ochiq matn jufti (L_0, R_0) olinadi. Ushbu arxitekturani boshqalaridan farqi shundaki, ma'lumotni rasshifrovkashda shifrlash funksiyasiga teskari bo'lgan funksiya ta'lab etilmaydi, kalitlarni teskari tartibda foydalanish bilan chegaralanadi.

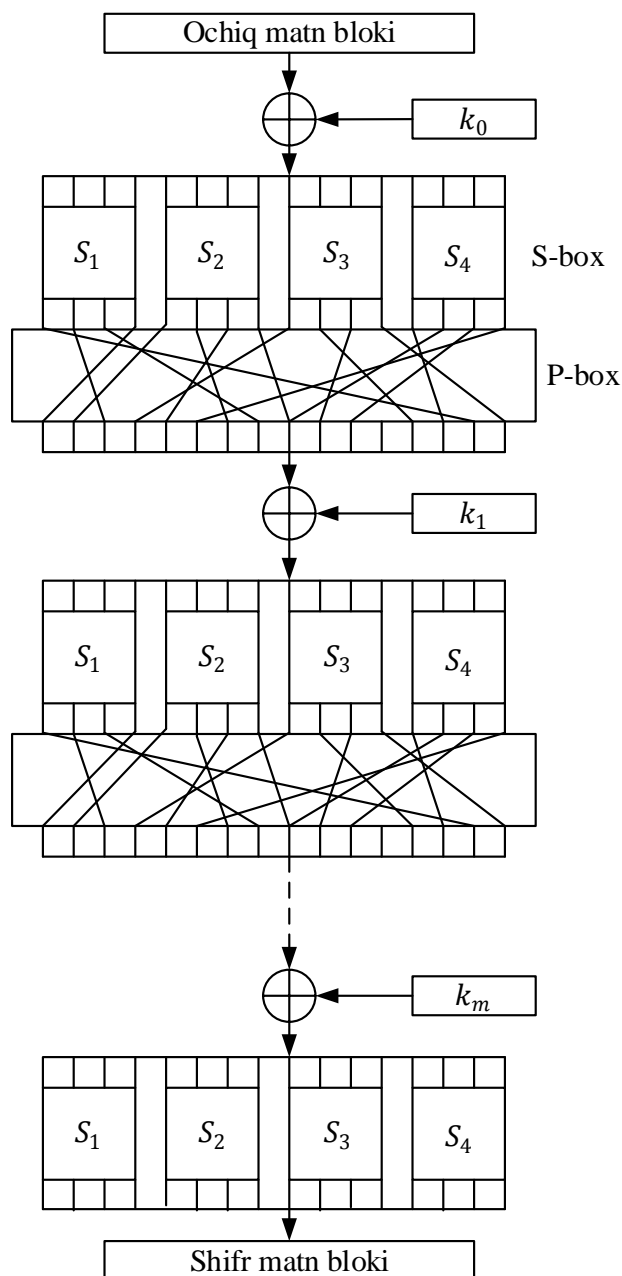
Umumiy holatda m -raundli Feystel tarmog'ining funksional sxemasi quyidagicha ifodalanadi:



5.1-rasm. m – raundli Feistel tarmog‘i arxitekturasi

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

SPN (Substitution-permutation networks)ga asoslangan blokli simmetrik shifrlash algoritmlari. Ushbu arxitekturaga ko‘ra kiruvchi parametrlar sifatida ochiq matn bloki va kalitlar olinib, almashtirish va o‘rniga qo‘yish amallaridan foydalangan holda shifrmtn olinadi. Bunda, ikki turdagi jadvallardan, o‘rniga qo‘yish - *substitution box* (S-box) va o‘rin almashtirish - *permutation box* (P-box) jadvallardan foydalaniladi (5.2-rasm).



5.2-rasm. SPN tarmoq arxitekturası

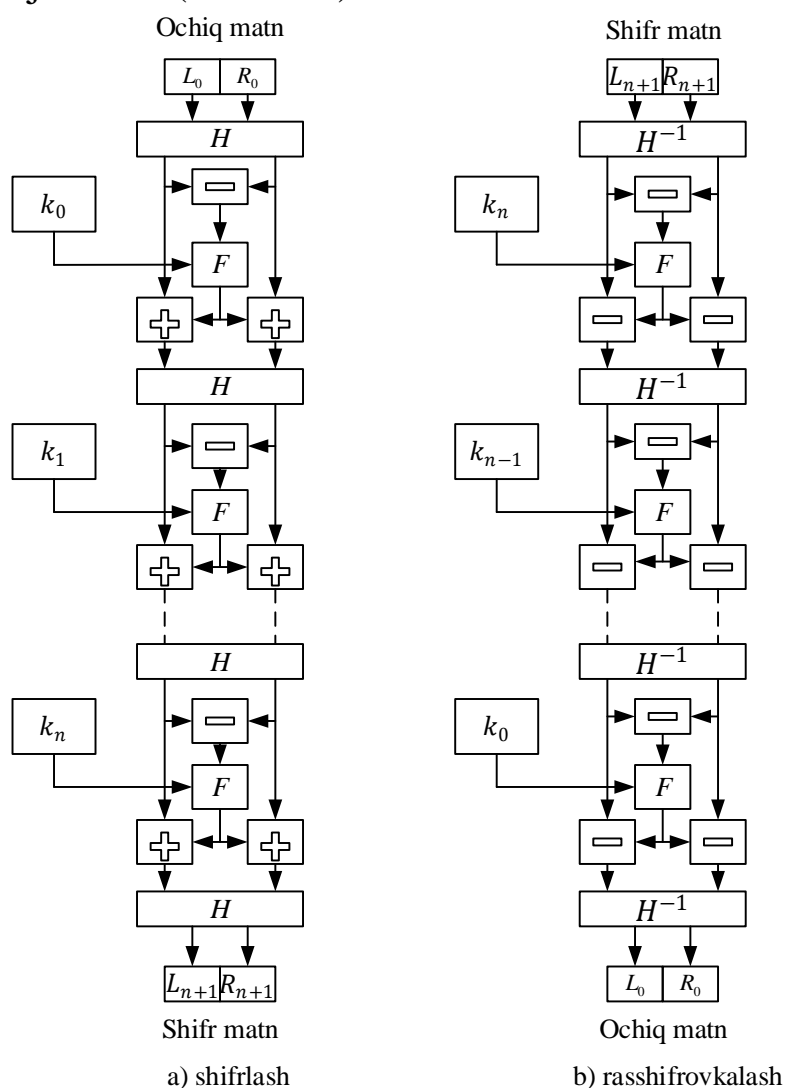
Har bir raunda alohida kalitlardan foydalanilib, almashtirish va oʻrniga qoʻyish amallari bajariladi.

Rasshifrovkalash esa Feystel tarmogʻidan farqli ravishda ham kalitlarning tartibi, ham jadvallarga invert boʻlgan jadvallardan foydalanish orqali amal oshiriladi.

Ushbu arxitekturaga asoslangan algoritmlarga misol sifatida Rijndael, Kuznechik, Serpent, SQUARE, Oʻz Dst 1105:2009, Kalyna, CRYPTON va h.k. keltirish mumkin.

Lai-Massey shifrlari (Lai-Massey ciphers). Ushbu usulda asoslangan kriptografiy tizimlar Feystel tarmogʻiga oʻxshash boʻlib,

farqli tomoni raund funksiyasi qaytmasdir. Bu usulda ham kirish bloki ikki qismga ajratiladi (5.3-rasm).



5.3-rasm. Lai-Massey sxemasining ko‘rinishi

Bunda, F - raund funksiyasi, H - esa yarim-raund funksiyasi. k_0, k_1, \dots, k_n lar esa $0, 1, \dots, n$ ga mos raund kalitlari.

Ushbu usulda asoslangan shifrlarga IDEA, MESH, RIDEA, WIDEA- n , FOX/IDEA-NXT, REESSE3+, BelT va h.k. larni misol keltirish.k.

Simmetrik blokli shifrlar turli akslantirishlardan iborat bo‘lib, umumiy holda ularni *chiziqli* va *nochiziqli* turlarga ajratish mumkin.

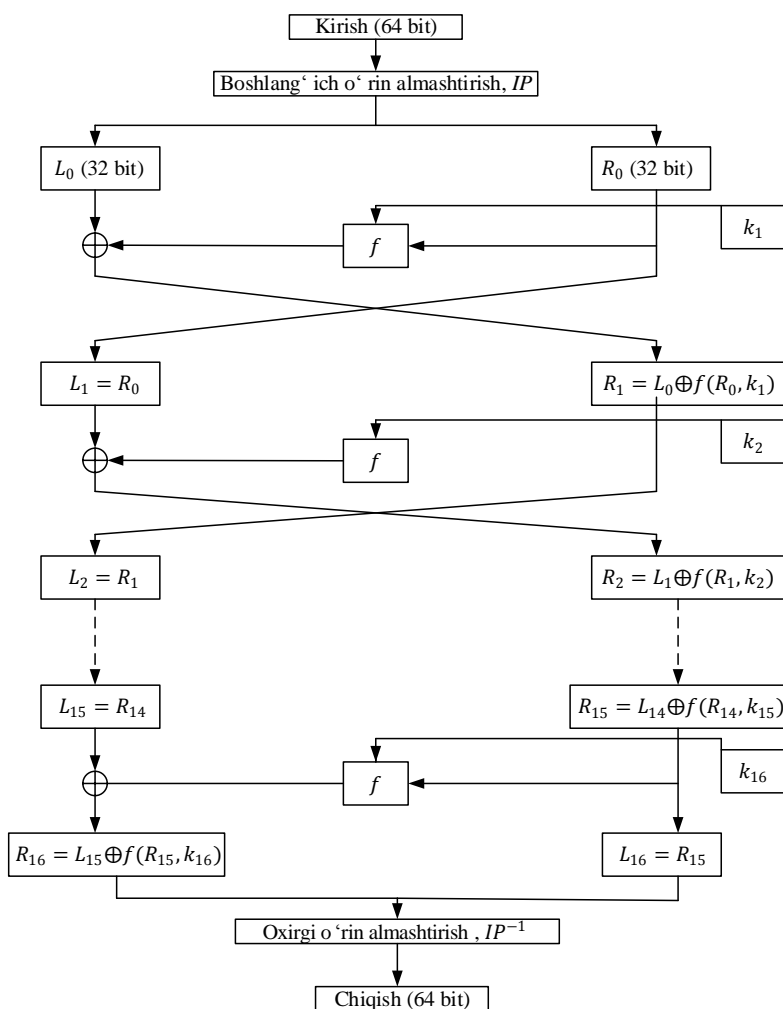
5.2. DES simmetrik blokli shifrlash algoritmi

DES standart shifrlash algoritmi Amerika Qo‘shma Shtatlari (AQSh) “Milliy Standartlar Byurosi” tomonidan 1977 yilda e‘lon qilingan. 1980 yilda AQShning “Standartlar va Texnologiyalar Milliy

Instituti” bu algoritmni davlat va savdo-sotiq moliyasi sohasidagi maxfiy bo‘lmagan, ammo muhim bo‘lgan ma’lumotlarni ruxsat etilmagan jismoniy va yuridik shaxslardan muhofaza qilishda shifrlash algoritmi sifatida qo‘llash standarti deb qabul qildi.

DES algoritmidagi dastlabki 56 bitli kalitdan raund kalitlarini hosil qilishning murakkab emasligi, raund asosiy akslantirishlarining apparat-texnik va dasturiy ta’minot ko‘rinishlarida qo‘llanilishini ta’minlashning qulayligi, hamda, ular kriptografik xossalarning samaradorligi – kriptobardoshligining yuqoriligi, bu algoritmning asosiy xususiyatlarini belgilaydi.

DES algoritmi, 64-bitli ma’lumotlar blokini turli o‘rin almashtirishlar va akslantirishlar kombinatsiyasiga asoslanib 56 bitli K kalit bilan shifrlashni amalga oshiradi. DES shifrlash algoritmining sxemasi 5.4-rasmda keltirilgan. Shifrlash jarayoni, kiruvchi blokni boshlang‘ich o‘rin almashtirish, o‘n olti marta shifrlash siklini takrorlanishi hamda oxirgi bitlarni o‘rin almashtirishdan iborat.



5.4-rasm. DES shifrlash algoritmining blok sxemasi

Algoritmda keltirilgan barcha o‘rin almashtirish va akslantirishlar jadvallari standart qabul qilingan, algoritm bajarilishida bular hech qanday o‘zgartirishlarsiz o‘z holicha saqlanadi.

Foydalanilgan belgilanishlar:

L_i va R_i – 64 bitli blokning chap va o‘ng qismlari;

\oplus - ikkilik modul bo‘yicha qo‘shish amali, XOR;

k_i – 48 bitli i -raund kaliti;

f – shifrlash funksiyasi;

IP – boshlang‘ich o‘rin almashtirish funksiyasi.

Shifrlash jarayoni. Ma’lumotning T blokini shifrlashda uning barcha bitlari 5.1-jadval bo‘yicha (IP -jadval) boshlang‘ich o‘rin almashtiriladi.

5.1-jadval

IP -jadval

| | | | | | | | |
|----|----|----|----|----|----|----|---|
| 58 | 50 | 42 | 34 | 26 | 18 | 10 | 2 |
| 60 | 52 | 44 | 36 | 28 | 20 | 12 | 4 |
| 62 | 54 | 46 | 38 | 30 | 22 | 14 | 6 |
| 64 | 56 | 48 | 40 | 32 | 24 | 16 | 8 |
| 57 | 49 | 41 | 33 | 25 | 17 | 9 | 1 |
| 59 | 51 | 43 | 35 | 27 | 19 | 11 | 3 |
| 61 | 53 | 45 | 37 | 29 | 21 | 13 | 5 |
| 63 | 55 | 47 | 39 | 31 | 23 | 15 | 7 |

Bunda, 58-bit T blokning 1-biti, 50-bit 2-biti va h.k., ko‘rinishda o‘rin almashtirish bajariladi. O‘rin almashtirishdan keyin hosil bo‘lgan $IP(T)$ blok mos ravishda ikki: L_0 , 1-bitdan 32-bitgacha va R_0 , 33-bitdan 64-bitgacha bo‘lgan bloklarga ajraladi. Keyin, Feystel akslantirishlariga asoslangan 16 marta takrorlanuvchi iterativ shifrlash jarayoni bajariladi.

$T_{i-1} = L_{i-1}R_{i-1}$ - blok $(i - 1)$ – iteratsiya natijasi bo‘lsin. U holda, i – iteratsiya natijasi $T_i = L_iR_i$ quyidagi formuladan aniqlanadi:

$$\begin{aligned} L_i &= R_{i-1}; \\ R_i &= L_{i-1} \oplus f(R_{i-1}, k_i), \quad i = 1, \dots, 16 \end{aligned} \quad (5.1)$$

Bu yerda, f – shifrlash funksiyasi. Funksiya argumenti 32 bitli R_{i-1} vektor va 56 bitli shifrlash K kalitdan akslantirishlar asosida olingan 48

bitli k_i kalitdir. $T_{16} = R_{16}L_{16}$ oxirgi iteratsiya natijasi. Shifrlash tugashi bilan bitlarning o‘z joylarini qayta tiklash maqsadida T_{16} ga IP^{-1} qayta o‘rin almashtirishlar qilinadi.

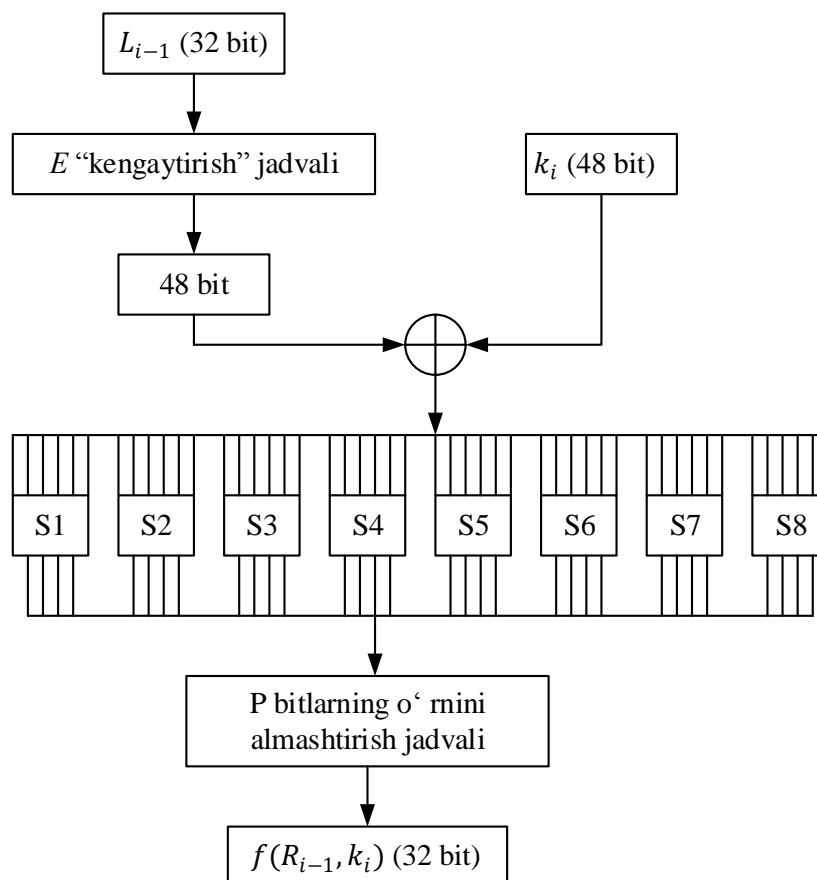
Ma’lumotni qayta shifrlash uchun yuqoridagi qilingan ishlar teskari tartibda bajariladi, shunga ko‘ra (5.1) munosabat o‘rniga quyidagi munosabatni qo‘llashga to‘g‘ri keladi:

$$\begin{aligned} R_{i-1} &= L_i; \\ L_{i-1} &= R_i \oplus f(L_i, k_i), \quad i = 1, \dots, 16. \end{aligned}$$

$f(R_{i-1}, k_i)$ shifrlash funksiyasi qiymatini hisoblash sxemasi 5.5-rasmda tasvirlangan.

f shifrlash funksiyasining qiymatini hisoblashda E “kengaytirish” jadvalidan, S_1, S_2, \dots, S_8 bloklaridan iborat S va R o‘rin almashtirishlardan foydalaniladi. R_{i-1} (32 bit) vektor va k_i (48 bit) kalitlar f funksiya argumenti hisoblanadi.

E “kengaytirish” jadvali 32 bitli R_{i-1} vektorni 5.2-jadvalga ko‘ra bir xil bitlarni takrorlash yo‘li bilan $E(R_{i-1})$ 48 bitli vektor hosil qiladi.



5.5-rasm. $f(R_{i-1}, k_i)$ shifrlash funksiyasi

E “kengaytirish” jadvali

| | | | | | |
|----|----|----|----|----|----|
| 32 | 1 | 2 | 3 | 4 | 5 |
| 4 | 5 | 6 | 7 | 8 | 9 |
| 8 | 9 | 10 | 11 | 12 | 13 |
| 12 | 13 | 14 | 15 | 16 | 17 |
| 16 | 17 | 18 | 19 | 20 | 21 |
| 20 | 21 | 22 | 23 | 24 | 25 |
| 24 | 25 | 26 | 27 | 28 | 29 |
| 28 | 29 | 30 | 31 | 32 | 1 |

$E(R_{i-1})$ vektorning birinchi uchta biti mos ravshida R_{i-1} vektorni 32, 1 va 2-bitlari, oxirgi uchta biti esa R_{i-1} vektorni 31, 32, 1-bitlaridir.

Hosil bo‘lgan natija mavjud k_i kalitga 2 moduli bo‘yicha bitma-bit qo‘shiladi va 6 bitlik 8 ta V_1, V_1, \dots, V_8 bloklar ketma-ketligi hosil qilinadi.

$$E(R_{i-1}) \oplus k_i = V_1, V_1, \dots, V_8.$$

So‘ngra har bir V_j blok 4-bitli V'_j blokka mos kelgan S_j jadvali yordamida o‘zgartiriladi, S -bloklar ro‘yxati 5.3-jadvalda keltirilgan.

S-bloklar ro‘yxati S_1

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

 S_2

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

S_3

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

 S_4

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

 S_5

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

 S_6

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

 S_7

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

 S_8

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

V_j blokning V'_j ga o'zgartirilishini ushbu misolda keltiramiz. Masalan, V_2 blok 111010 dan iborat bo'lsin. V_2 blokni birinchi razryadi $a_1 = 1$ va oxirgi razryadi $a_6 = 0$ dan tashkil topgan $a = a_1 a_6$ sonining ikkilik sanoq sistemasidagi yozuvi bo'lsa, bu sonning o'nlik sanoq sistemasidagi qiymati 4 dan katta bo'lmaydi, ya'ni, $0 \leq a < 4$. Oradagi 4 ta $b = a_2 a_3 a_4 a_5 = 1101$ dan tashkil topgan b soni esa $0 \leq b < 16$ munosabatni qanoatlantiradi. Olingan holda $a = 2, b = 13$. S_2 blokning satrlari 0 dan a gacha bo'lgan sonlar bilan ustunlari esa 0 dan b gacha bo'lgan sonlarda raqamlab chiqilgan. Shunday qilib, (a, b) sonlar juftligi jadvaldagi a -satr va b -ustunning kesishmasidagi biror sonni aniqlaydi. Ushbu holatda kesishmada turgan son 3. Bu sonni ikkilik sanoq sistemasiga o'tkazib V'_2 ni hosil qilinadi: 0011.

$f(R_{i-1}, k_i)$ ni qiymati, P bitli o'rin almashtirishlarni 5.4-jadvaldan foydalanib hosil qiladi.

5.4-jadval

P bitli o'rin almashtirish jadvali

| | | | |
|----|----|----|----|
| 16 | 7 | 20 | 21 |
| 29 | 12 | 28 | 17 |
| 1 | 15 | 23 | 26 |
| 5 | 18 | 31 | 10 |
| 2 | 8 | 24 | 14 |
| 32 | 27 | 3 | 9 |
| 19 | 13 | 30 | 6 |
| 22 | 11 | 4 | 25 |

Raund kalitlarini hosil qilish.k. Har bir iteratsiyada k_i (48 bit) kalitning ayni paytdagi qiymati foydalaniladi. Ushbu qiymatlar dastlabki K kalitdan quyidagicha olinadi.

Dastlab foydalanuvchi 56 ta ixtoriy bitli kalitni tanlaydi. 8, 16, ..., 64 -o'rinlarda turgan 8 ta bit kalitga shunday qo'shiladiki undagi har bir bayt toq sondagi birlik raqamlarini o'z ichiga olsin. Lekin, bu bitlar shifrlash jarayonlarida qatnashmaydi.

Bu kalitlarni uzatish va saqlashda uchraydigan ayrim xatoliklarni topishda juda qo'l keladi. 56 bit kalit 5.5-jadvalga ko'ra o'rin almashtirishlar asosida olinadi.

64 bitdan 56 bitga o'tkazish jadvali

| | | | | | | |
|----|----|----|----|----|----|----|
| 57 | 49 | 41 | 33 | 25 | 17 | 9 |
| 1 | 58 | 50 | 42 | 34 | 26 | 18 |
| 10 | 2 | 59 | 51 | 43 | 35 | 27 |
| 19 | 11 | 3 | 60 | 52 | 44 | 36 |
| 63 | 55 | 47 | 39 | 31 | 23 | 15 |
| 7 | 62 | 54 | 46 | 38 | 30 | 22 |
| 14 | 6 | 61 | 53 | 45 | 37 | 29 |
| 21 | 13 | 5 | 28 | 20 | 12 | 4 |

Bu o'rin almashtirish har biri 28 bitdan iborat bo'lgan ikkita C_0 va D_0 bloklar bilan aniqlanadi (ular mos ravishda jadvalning yuqori va pastki qismlarini egallagan). C_0 ni uchta oldingi bitlari kalitning 57,49,41 - bitlariga mos keladi va jadval asosida davom ettiriladi. Keyin, induktiv yo'l bilan C_i va D_i ($i = 1, \dots, 16$) bloklar aniqlanadi. Agar C_{i-1} va D_{i-1} lar aniqlangan bo'lsa, u holda C_i va D_i lar ulardan 5.6-jadvalga asosan bir yoki ikkita chapga siklik surish bilan hosil qilinadi.

Raund kalitlarni generatsiyalash uchun siklik surishlar jadvali

| i | 1 | 2 | 3 | 4 | 5 | 6 | 7 | 8 | 9 | 10 | 11 | 12 | 13 | 14 | 15 | 16 |
|----------------|---|---|---|---|---|---|---|---|---|----|----|----|----|----|----|----|
| Surishlar soni | 1 | 1 | 2 | 2 | 2 | 2 | 2 | 2 | 1 | 2 | 2 | 2 | 2 | 2 | 2 | 1 |

Endi, k_i ($1 \leq i \leq 16$) kalitlarni aniqlaymiz. k_i kalit 48 bitdan tashkil topgan bo'lib, ular 5.7-jadvalga asosan $C_i D_i$ blok bitlaridan tanlab olingan. Takidlash joizki, $C_i D_i$ dagi 56 bitdan 8 tasi (9, 18, 22, 25, 35, 38, 43, 54 raqamli) k_i da yo'q.

56 bitdan 48 bitga tushirish qoidasi

| | | | | | |
|----|----|----|----|----|----|
| 14 | 17 | 11 | 24 | 1 | 5 |
| 3 | 28 | 15 | 6 | 21 | 10 |
| 23 | 19 | 12 | 4 | 26 | 8 |
| 16 | 7 | 27 | 20 | 13 | 2 |
| 41 | 52 | 31 | 37 | 47 | 55 |
| 30 | 40 | 51 | 45 | 33 | 48 |
| 44 | 49 | 39 | 56 | 34 | 53 |
| 46 | 42 | 50 | 36 | 29 | 32 |

5.3. AES simmetrik blokli shifrlash standarti

Amerika qo'shma shtatlarining Standartlar va Texnologiyalar Milliy Instituti (NIST) 1997 yilda XXI asrning ma'lumotlarni kriptografik muhofazalovchi yangi shifrlash algoritmi standartini qabul qilish maqsadida tanlov e'lon qildi. 2001 yilda standart shifrlash algoritmi qilib, RIJNDAEL shifrlash algoritmi asos qilib olingan AES (Advanced Encryption Standard) (FIPS 197) qabul qilindi. Algoritmning yaratuvchilari Belgiyalik mutaxassislar Yon Demen (Joan Daemen) va Vinsent Ryumen (Vincent Rijmen)larning familiyalaridan RIJNDAEL nomi olingan.

RIJNDAEL algoritmi 128, 192 va 256 bitli ma'lumotlar bloklarini shifrlashga mo'ljallangan bo'lib, buning uchun 128, 192 va 256 bitli kalitlardan foydalaniladi. AES standartida esa ochiq matn blokining faqat 128 bitga teng holati olingan. Raundlar soni esa kalit uzunligiga bog'liq bo'ladi. Xususan, AES shifrlash algoritmi raundlar soni N_r , kirish bloklar o'lchami N_b (32 bitli so'zlarda) va kalit uzunligi N_k (32 bitli so'zlarda)larga bog'liq holda 5.8-jadvalga mos holda qo'llaniladi.

5.8-jadval

Rijndael algoritmidagi sozlanishlar parametri

| N_r | $N_b = 4,$ 128 bit | $N_b = 6,$ 192 bit | $N_b = 8,$ 256 bit |
|--------------------|-----------------------|-----------------------|-----------------------|
| $N_k = 4, 128$ bit | 10 | 12 | 14 |
| $N_k = 6, 192$ bit | 12 | 12 | 14 |
| $N_k = 8, 256$ bit | 14 | 14 | 14 |

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

$$\{a_7 a_6 a_5 a_4 a_3 a_2 a_1 a_0\}, a_i \in \{0, 1\}, i = \overline{0 \dots 7},$$

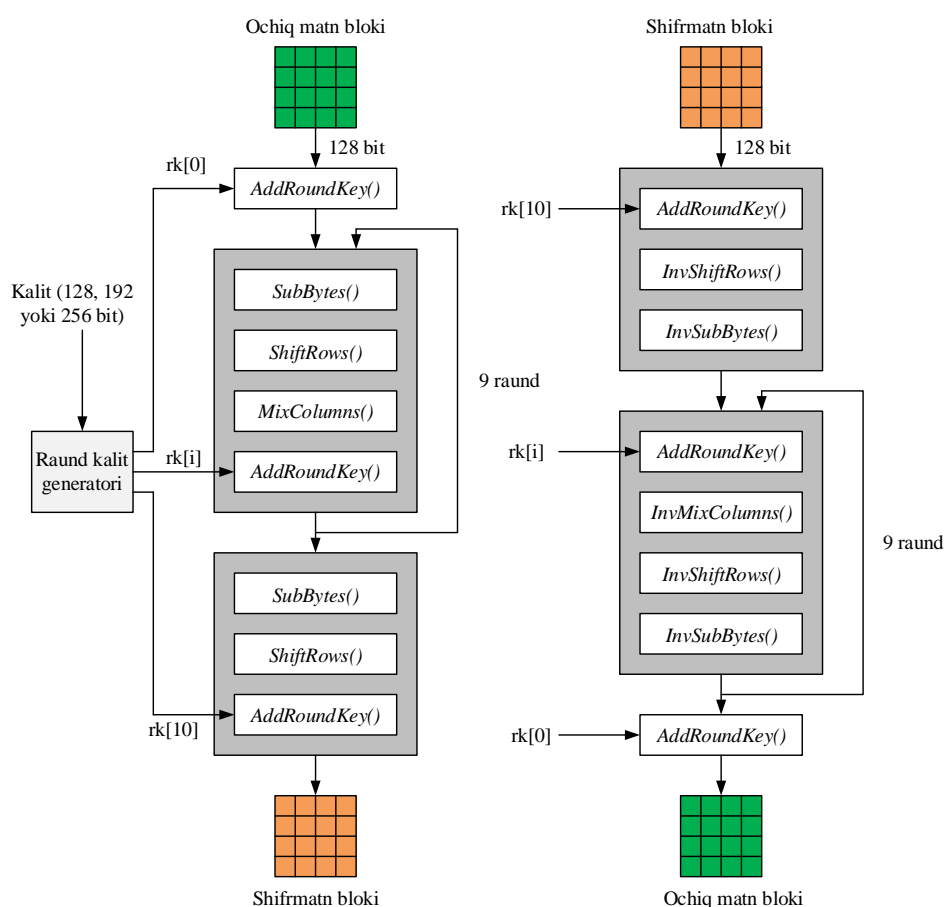
ko'rinishda tasvirlangan bo'lsa, u holda maydon elementlari ko'phad ko'rinishda quyidagicha yoziladi:

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

Misol uchun $\{11010101\}$ baytga $x^7 + x^6 + x^4 + x^2 + 1$ ko‘rinishdagi ko‘phad mos keladi.

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

Shifrlash va rasshifrovkalash jarayoni. AES standartida ma‘lumotlarni shifrlash va rasshifrovkalashning umumiy ko‘rinishi 5.6-rasmda keltirilgan.



5.6-rasm. AES standartida ma‘lumotni shifrlash va rasshifrovkalash (128 bitli kalit uchun)

Shifrlash algoritmidagi quyidagi akslantirishlardan foydalaniladi:

- *AddRoundKey()* – raund kalitlarini qo‘shish;
- *SubBytes()* - jadval asosida baytlarni almashtirish;
- *ShiftRows()* – satr bo‘yicha siljitish;
- *MixColumns()* – ustunlar bo‘yicha aralashtirish.k.

Rasshifrovkalashda esa shifrlashda foydalanilgan akslantirishlarga teskari akslantirishlardan foydalaniladi:

- *InvSubBytes()* - jadval asosida baytlarni almashtirish;
- *InvShiftRows()* – satr bo‘yicha siljitish;
- *InvMixColumns()* – ustunlar bo‘yicha aralashtirish.k.

SubBytes() *akslantirishi*. *SubBytes()* algoritmda qayd etilgan 16×16 o‘lchamli jadval asosida baytlarni almashtirish, ya’ni S-blok akslantirishlarini amalga oshiradi. Shifrlash jarayonida foydalanilgan S-blok 5.8-jadvalda, unga teskari bo‘lgan va rasshifrovkalashda jarayonida foydalanilgan S-blok esa 5.9-jadvalda keltirilgan.

5.8-jadval

S-blok (16 sanoq tizimida ifodalangan)

| | 00 | 01 | 02 | 03 | 04 | 05 | 06 | 07 | 08 | 09 | 0a | 0b | 0c | 0d | 0e | 0f |
|----|----|----|----|----|----|----|----|----|----|----|----|----|----|----|----|----|
| 00 | 63 | 7c | 77 | 7b | f2 | 6b | 6f | c5 | 30 | 01 | 67 | 2b | fe | d7 | ab | 76 |
| 10 | ca | 82 | c9 | 7d | fa | 59 | 47 | f0 | ad | d4 | a2 | af | 9c | a4 | 72 | c0 |
| 20 | b7 | fd | 93 | 26 | 36 | 3f | f7 | cc | 34 | a5 | e5 | f1 | 71 | d8 | 31 | 15 |
| 30 | 04 | c7 | 23 | c3 | 18 | 96 | 05 | 9a | 07 | 12 | 80 | e2 | eb | 27 | b2 | 75 |
| 40 | 09 | 83 | 2c | 1a | 1b | 6e | 5a | a0 | 52 | 3b | d6 | b3 | 29 | e3 | 2f | 84 |
| 50 | 53 | d1 | 00 | ed | 20 | fc | b1 | 5b | 6a | cb | be | 39 | 4a | 4c | 58 | cf |
| 60 | d0 | ef | aa | fb | 43 | 4d | 33 | 85 | 45 | f9 | 02 | 7f | 50 | 3c | 9f | a8 |
| 70 | 51 | a3 | 40 | 8f | 92 | 9d | 38 | f5 | bc | b6 | da | 21 | 10 | ff | f3 | d2 |
| 80 | cd | 0c | 13 | ec | 5f | 97 | 44 | 17 | c4 | a7 | 7e | 3d | 64 | 5d | 19 | 73 |
| 90 | 60 | 81 | 4f | dc | 22 | 2a | 90 | 88 | 46 | ee | b8 | 14 | de | 5e | 0b | db |
| a0 | e0 | 32 | 3a | 0a | 49 | 06 | 24 | 5c | c2 | d3 | ac | 62 | 91 | 95 | e4 | 79 |
| b0 | e7 | c8 | 37 | 6d | 8d | d5 | 4e | a9 | 6c | 56 | f4 | ea | 65 | 7a | ae | 08 |
| c0 | ba | 78 | 25 | 2e | 1c | a6 | b4 | c6 | e8 | dd | 74 | 1f | 4b | bd | 8b | 8a |
| d0 | 70 | 3e | b5 | 66 | 48 | 03 | f6 | 0e | 61 | 35 | 57 | b9 | 86 | c1 | 1d | 9e |
| e0 | e1 | f8 | 98 | 11 | 69 | d9 | 8e | 94 | 9b | 1e | 87 | e9 | ce | 55 | 28 | df |
| f0 | 8c | a1 | 89 | 0d | bf | e6 | 42 | 68 | 41 | 99 | 2d | 0f | b0 | 54 | bb | 16 |

Teskari S-blok (16 sanoq tizimida ifodalangan)

| | 00 | 01 | 02 | 03 | 04 | 05 | 06 | 07 | 08 | 09 | 0a | 0b | 0c | 0d | 0e | 0f |
|----|----|----|----|----|----|----|----|----|----|----|----|----|----|----|----|----|
| 00 | 52 | 09 | 6a | d5 | 30 | 36 | a5 | 38 | bf | 40 | a3 | 9e | 81 | f3 | d7 | fb |
| 10 | 7c | e3 | 39 | 82 | 9b | 2f | ff | 87 | 34 | 8e | 43 | 44 | c4 | de | e9 | cb |
| 20 | 54 | 7b | 94 | 32 | a6 | c2 | 23 | 3d | ee | 4c | 95 | 0b | 42 | fa | c3 | 4e |
| 30 | 08 | 2e | a1 | 66 | 28 | d9 | 24 | b2 | 76 | 5b | a2 | 49 | 6d | 8b | d1 | 25 |
| 40 | 72 | f8 | f6 | 64 | 86 | 68 | 98 | 16 | d4 | a4 | 5c | cc | 5d | 65 | b6 | 92 |
| 50 | 6c | 70 | 48 | 50 | fd | ed | b9 | da | 5e | 15 | 46 | 57 | a7 | 8d | 9d | 84 |
| 60 | 90 | d8 | ab | 00 | 8c | bc | d3 | 0a | f7 | e4 | 58 | 05 | b8 | b3 | 45 | 06 |
| 70 | d0 | 2c | 1e | 8f | ca | 3f | 0f | 02 | c1 | af | bd | 03 | 01 | 13 | 8a | 6b |
| 80 | 3a | 91 | 11 | 41 | 4f | 67 | dc | ea | 97 | f2 | cf | ce | f0 | b4 | e6 | 73 |
| 90 | 96 | ac | 74 | 22 | e7 | ad | 35 | 85 | e2 | f9 | 37 | e8 | 1c | 75 | df | 6e |
| a0 | 47 | f1 | 1a | 71 | 1d | 29 | c5 | 89 | 6f | b7 | 62 | 0e | aa | 18 | be | 1b |
| b0 | fc | 56 | 3e | 4b | c6 | d2 | 79 | 20 | 9a | db | c0 | fe | 78 | cd | 5a | f4 |
| c0 | 1f | dd | a8 | 33 | 88 | 07 | c7 | 31 | b1 | 12 | 10 | 59 | 27 | 80 | ec | 5f |
| d0 | 60 | 51 | 7f | a9 | 19 | b5 | 4a | 0d | 2d | e5 | 7a | 9f | 93 | c9 | 9c | ef |
| e0 | a0 | e0 | 3b | 4d | ae | 2a | f5 | b0 | c8 | eb | bb | 3c | 83 | 53 | 99 | 61 |
| f0 | 17 | 2b | 04 | 7e | ba | 77 | d6 | 26 | e1 | 69 | 14 | 63 | 55 | 21 | 0c | 7d |

Masalan, kiruvchi bayt $0x68$ ga teng bo'lsa, S-blok natijasiga ko'ra $0x45$ ga almashadi, ya'ni, $SubBytes(0x68)=0x45$. Teskari S-blokdan foydalangan holda esa, $InvSubBytes(0x45)=0x68$ tengligini bilish oson.

ShiftRows() akslantirishi. ShiftRows (holat baytlarini siklik surish) akslantirishining qo'llanishi quyidagicha amalga oshiriladi. Holat baytlarini siklik surishda holat jadvali satrlari quyidagicha belgilab olinadi.

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

ShiftRows akslantirishida jadvaldagi oxirgi uchta satr har bir baytlari chapga siklik, ya'ni 1-satr C_1 baytga, 2-satr C_2 baytga, 3-satr C_3 baytga suriladi. C_1, C_2, C_3 surilish qiymati N_b blok uzunligiga bog'liq bo'lib, ular algoritmda ko'rsatilganidek, quyidagi jadvalda keltirilgan:

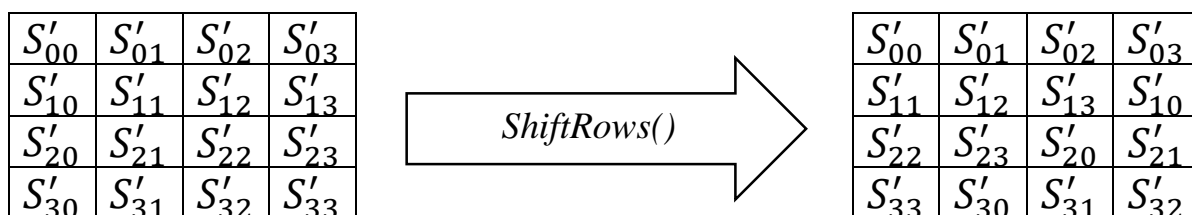
| l | N_b | C_0 | C_1 | C_2 | C_3 |
|-----|-------|-------|-------|-------|-------|
| 128 | 4 | 0 | 1 | 2 | 3 |
| 192 | 6 | 0 | 1 | 2 | 3 |
| 256 | 8 | 0 | 1 | 3 | 4 |

Keltirilgan jadvalga ko'ra $l = 128$ bitli blok uchun $N_b = 4$ ga teng bo'lib, birinchi satr bo'yicha holat baytlarini siklik surish bajarilmaydi, ikkinchi satr bo'yicha 1 baytga, uchinchi satr bo'yicha 2 baytga, to'rtinchi satr bo'yicha 3 baytga siklik surish amalga oshiriladi.

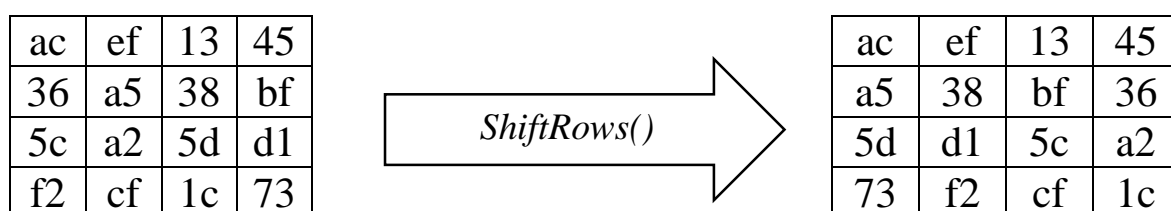
$l = 192$ bitli blok uchun $N_b = 6$ ga teng bo'lib, birinchi satr bo'yicha holat baytlarini siklik surish bajarilmaydi, ikkinchi satr bo'yicha 1 baytga, uchinchi satr bo'yicha 2 baytga, to'rtinchi satr bo'yicha 3 baytga siklik surish bajariladi.

$l = 256$ bitli blok uchun $N_b = 8$ ga teng bo'lib, birinchi satr bo'yicha holat baytlarini siklik surish bajarilmaydi, ikkinchi qator bo'yicha 1 baytga, uchinchi satr bo'yicha 3 baytga, to'rtinchi satr bo'yicha 4 baytga siklik surish amalga oshiriladi.

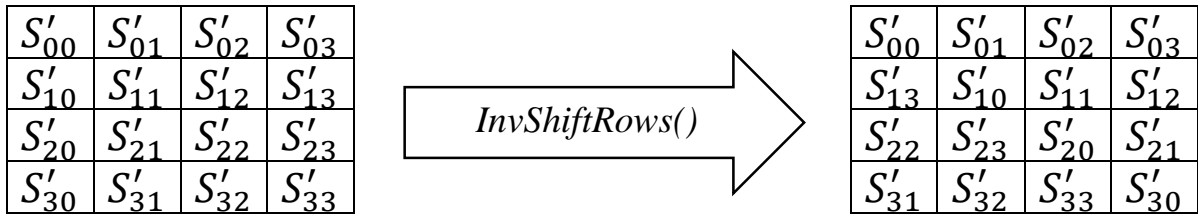
Quyidagi jadvalda esa $l = 128$ bitli shifrlash uchun $N_b = 4$ ga teng bo'lganda, satrlarni siklik surish bajarilgandan keyingi baytlarning o'rnini qay tarzda o'zgarishi ko'rsatilgan:



Quyida siklik surishga misol keltirilgan:



Rasshifrovkalash jarayoni uchun *InvShiftRows()* jarayoni quyidagicha amalga oshiriladi:



MixColumns() akslantirishi. *MixColumns()* (ustun elementlarini aralashtirish) akslantirishida holat ustunlari elementlari uchinchi darajadan katta bo'lmagan ko'phadning koeffitsientlari sifatida ifodalanib, ana shu ko'phad algoritmda berilgan: $g(x) = \{03\}x^3 + \{01\}x^2 + \{01\}x + \{02\}$ ko'phadga $x^4 + 1$ modul bo'yicha ko'paytiriladi.

Mazkur akslantirishni quyidagicha matritsa ko'rinishida tasvirlash mumkin:

$$\begin{bmatrix} s'_{0c} \\ s'_{1c} \\ s'_{2c} \\ s'_{3c} \end{bmatrix} = \begin{bmatrix} \{02\} & \{03\} & \{01\} & \{01\} \\ \{01\} & \{02\} & \{03\} & \{01\} \\ \{01\} & \{01\} & \{02\} & \{03\} \\ \{03\} & \{01\} & \{01\} & \{02\} \end{bmatrix} \cdot \begin{bmatrix} s_{0c} \\ s_{1c} \\ s_{2c} \\ s_{3c} \end{bmatrix}, \quad 0 \leq c \leq 3,$$

bu yerda, c – ustun nomeri.

Bunday ko'paytirish natijasida s_{0c} , s_{1c} , s_{2c} , s_{3c} ustun baytlari mos baytlarga o'zgaradi:

$$\begin{aligned} s'_{0c} &= (\{02\} \cdot s_{0c}) \oplus (\{03\} \cdot s_{1c}) \oplus s_{2c} \oplus s_{3c}, \\ s'_{1c} &= s_{0c} \oplus (\{02\} \cdot s_{1c}) \oplus (\{03\} \cdot s_{2c}) \oplus s_{3c}, \\ s'_{2c} &= s_{0c} \oplus s_{1c} \oplus (\{02\} \cdot s_{2c}) \oplus (\{03\} \cdot s_{3c}), \\ s'_{3c} &= (\{03\} \cdot s_{0c}) \oplus s_{1c} \oplus s_{2c} \oplus (\{02\} \cdot s_{3c}). \end{aligned}$$

Masalan, $\begin{bmatrix} s_{0c} \\ s_{1c} \\ s_{2c} \\ s_{3c} \end{bmatrix} = \begin{bmatrix} ac \\ c1 \\ d6 \\ b8 \end{bmatrix}$ ustunni *MixColumns()* akslantirishidagi natijasini hisoblaylik.

$$s_{0c} = ac_{16} = 10101100_2 = x^7 + x^5 + x^3 + x^2;$$

$$s_{1c} = c1_{16} = 11000001_2 = x^7 + x^6 + 1;$$

$$s_{2c} = d6_{16} = 11010110_2 = x^7 + x^6 + x^4 + x^2 + x;$$

$$s_{3c} = b8_{16} = 10111000_2 = x^7 + x^5 + x^4 + x^3.$$

$$\begin{bmatrix} s'_{0c} \\ s'_{1c} \\ s'_{2c} \\ s'_{3c} \end{bmatrix} = \begin{bmatrix} \{02\} & \{03\} & \{01\} & \{01\} \\ \{01\} & \{02\} & \{03\} & \{01\} \\ \{01\} & \{01\} & \{02\} & \{03\} \\ \{03\} & \{01\} & \{01\} & \{02\} \end{bmatrix} \cdot \begin{bmatrix} ac \\ c1 \\ d6 \\ b8 \end{bmatrix}.$$

$$s'_{0c} = (\{02\} \cdot ac) \oplus (\{03\} \cdot c1) \oplus d6 \oplus b8 = 75_{16}:$$

- $\{02\} \cdot ac = x \cdot (x^7 + x^5 + x^3 + x^2) \bmod (x^8 + x^4 + x^3 + x + 1) = (x^8 + x^6 + x^4 + x^3) \bmod (x^8 + x^4 + x^3 + x + 1) = x^6 + x + 1;$
- $\{03\} \cdot c1 = (x + 1) \cdot (x^7 + x^6 + 1) \bmod (x^8 + x^4 + x^3 + x + 1) = (x^8 + x^6 + x + 1) \bmod (x^8 + x^4 + x^3 + x + 1) = x^6 + x^4 + x^3;$
- $s'_{0c} = (x^6 + x + 1) \oplus (x^6 + x^4 + x^3) \oplus (x^7 + x^6 + x^4 + x^2 + x) \oplus (x^7 + x^5 + x^4 + x^3) = x^6 + x^5 + x^4 + x^2 + 1 = 01110101_2 = 75_{16}.$

$$s'_{1c} = ac \oplus (\{02\} \cdot c1) \oplus (\{03\} \cdot d6) \oplus b8 = ec_{16}:$$

- $\{02\} \cdot c1 = x \cdot (x^7 + x^6 + 1) \bmod (x^8 + x^4 + x^3 + x + 1) = (x^8 + x^7 + x) \bmod (x^8 + x^4 + x^3 + x + 1) = x^7 + x^4 + x^3 + 1;$
- $\{03\} \cdot d6 = (x + 1) \cdot (x^7 + x^6 + x^4 + x^2 + x) \bmod (x^8 + x^4 + x^3 + x + 1) = (x^8 + x^6 + x^5 + x^4 + x^3 + x) \bmod (x^8 + x^4 + x^3 + x + 1) = x^6 + x^5 + 1;$
- $s'_{1c} = (x^7 + x^5 + x^3 + x^2) \oplus (x^7 + x^4 + x^3 + 1) \oplus (x^6 + x^5 + 1) \oplus (x^7 + x^5 + x^4 + x^3) = x^7 + x^6 + x^5 + x^3 + x^2 = 11101100_2 = ec_{16}.$

$$s'_{2c} = ac \oplus c1 \oplus (\{02\} \cdot d6) \oplus (\{03\} \cdot b8) = 09_{16}:$$

- $\{02\} \cdot d6 = x \cdot (x^7 + x^6 + x^4 + x^2 + x) \bmod (x^8 + x^4 + x^3 + x + 1) = (x^8 + x^7 + x^5 + x^3 + x^2) \bmod (x^8 + x^4 + x^3 + x + 1) = x^7 + x^5 + x^4 + x^2 + x + 1;$
- $\{03\} \cdot b8 = (x + 1) \cdot (x^7 + x^5 + x^4 + x^3) \bmod (x^8 + x^4 + x^3 + x + 1) = (x^8 + x^7 + x^6 + x^3) \bmod (x^8 + x^4 + x^3 + x + 1) = x^7 + x^6 + x^4 + x + 1;$

$$- s'_{2c} = (x^7 + x^5 + x^3 + x^2) \oplus (x^7 + x^6 + 1) \oplus (x^7 + x^5 + x^4 + x^2 + x + 1) \oplus (x^7 + x^6 + x^4 + x + 1) = x^3 + 1 = 00001001_2 = 09_{16}.$$

$$s'_{3c} = (\{03\} \cdot ac) \oplus c1 \oplus d6 \oplus (\{02\} \cdot b8) = 93_{16}:$$

$$- \{03\} \cdot ac = (x + 1) \cdot (x^7 + x^5 + x^3 + x^2) \bmod (x^8 + x^4 + x^3 + x + 1) = (x^8 + x^7 + x^6 + x^5 + x^4 + x^2) \bmod (x^8 + x^4 + x^3 + x + 1) = x^7 + x^6 + x^5 + x^3 + x^2 + x + 1;$$

$$- \{02\} \cdot b8 = x \cdot (x^7 + x^5 + x^4 + x^3) \bmod (x^8 + x^4 + x^3 + x + 1) = (x^8 + x^6 + x^5 + x^4) \bmod (x^8 + x^4 + x^3 + x + 1) = x^6 + x^5 + x^3 + x + 1;$$

$$- s'_{3c} = (x^7 + x^6 + x^5 + x^3 + x^2 + x + 1) \oplus (x^7 + x^6 + 1) \oplus (x^7 + x^6 + x^4 + x^2 + x) \oplus (x^6 + x^5 + x^3 + x + 1) = x^7 + x^4 + x + 1 = 10010011_2 = 93_{16}.$$

Umumiy natija esa quyidagicha bo'ladi:

$$\begin{bmatrix} s'_{0c} \\ s'_{1c} \\ s'_{2c} \\ s'_{3c} \end{bmatrix} = \begin{bmatrix} \{02\} & \{03\} & \{01\} & \{01\} \\ \{01\} & \{02\} & \{03\} & \{01\} \\ \{01\} & \{01\} & \{02\} & \{03\} \\ \{03\} & \{01\} & \{01\} & \{02\} \end{bmatrix} \cdot \begin{bmatrix} ac \\ c1 \\ d6 \\ b8 \end{bmatrix} = \begin{bmatrix} 75 \\ ec \\ 09 \\ 93 \end{bmatrix}.$$

Rasshifrovkalash jarayonida esa *InvMixColumns()* akslantirishi quyidagicha bo'ladi:

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

Bu yerda, $\begin{bmatrix} \{0e\} & \{0b\} & \{0d\} & \{09\} \\ \{09\} & \{0e\} & \{0b\} & \{0d\} \\ \{0d\} & \{09\} & \{0e\} & \{0b\} \\ \{0b\} & \{0d\} & \{09\} & \{0e\} \end{bmatrix}$ matritsa

$\begin{bmatrix} \{02\} & \{03\} & \{01\} & \{01\} \\ \{01\} & \{02\} & \{03\} & \{01\} \\ \{01\} & \{01\} & \{02\} & \{03\} \\ \{03\} & \{01\} & \{01\} & \{02\} \end{bmatrix}$ matritsaga teskari, ya'ni, ularning

ko'paytmasi olingan maydon uchun birga teng.

AddRoundKey() *akslantirishi*. Ushbu akslantirishda holat bloking bitlari kalit bloki mos bitlari bilan xarakteristikasi ikki bo‘lgan chekli maydonda qo‘shiladi, ya’ni, massivning har bir ustuni va shu ustunning elementlari kalit massivining mos ustun va elementlariga XOR amali bilan qo‘shiladi. Masalan, dastlabki ochiq matn bloki quyidagicha bo‘lsin:

$$\begin{bmatrix} \{25\} & \{bd\} & \{b6\} & \{4c\} \\ \{d1\} & \{11\} & \{3a\} & \{4c\} \\ \{a9\} & \{d1\} & \{33\} & \{c0\} \\ \{ad\} & \{68\} & \{8e\} & \{b0\} \end{bmatrix}$$

Dastlabki raund kaliti esa quyidagiga teng bo‘lsin:

$$\begin{bmatrix} \{d4\} & \{7c\} & \{ca\} & \{11\} \\ \{d1\} & \{83\} & \{f2\} & \{f9\} \\ \{c6\} & \{9d\} & \{b8\} & \{15\} \\ \{f8\} & \{87\} & \{bc\} & \{bc\} \end{bmatrix}$$

U holda *AddRoundKey()* akslantirishining natijasi quyidagiga teng bo‘ladi:

$$\begin{bmatrix} \{25\} & \{bd\} & \{b6\} & \{4c\} \\ \{d1\} & \{11\} & \{3a\} & \{4c\} \\ \{a9\} & \{d1\} & \{33\} & \{c0\} \\ \{ad\} & \{68\} & \{8e\} & \{b0\} \end{bmatrix} \oplus \begin{bmatrix} \{d4\} & \{7c\} & \{ca\} & \{11\} \\ \{d1\} & \{83\} & \{f2\} & \{f9\} \\ \{c6\} & \{9d\} & \{b8\} & \{15\} \\ \{f8\} & \{87\} & \{bc\} & \{bc\} \end{bmatrix} =$$

$$\begin{bmatrix} \{25 \oplus d4\} & \{bd \oplus 7c\} & \{b6 \oplus ca\} & \{4c \oplus 11\} \\ \{d1 \oplus d1\} & \{11 \oplus 83\} & \{3a \oplus f2\} & \{4c \oplus f9\} \\ \{a9 \oplus c6\} & \{d1 \oplus 9d\} & \{33 \oplus b8\} & \{c0 \oplus 15\} \\ \{ad \oplus f8\} & \{68 \oplus 87\} & \{8e \oplus bc\} & \{b0 \oplus bc\} \end{bmatrix} =$$

$$\begin{bmatrix} \{f1\} & \{c1\} & \{7c\} & \{5d\} \\ \{00\} & \{92\} & \{c8\} & \{b5\} \\ \{6f\} & \{4c\} & \{8b\} & \{d5\} \\ \{55\} & \{ef\} & \{32\} & \{0c\} \end{bmatrix}$$

Raund kalitlarini generatsiyalash.k. AES shifrlash algoritmidan raund kalitlari dastlabki kiritilgan shifrlash kalitidan hosil qilinib, u quyidagi jarayonlardan iborat:

- kalitni kengaytirish (Key Expansion);
- raund kalitlarini tanlash (Round Key Selection).

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

Demak, 128 bit uzunlikdagi blok va 10 raund uchun 1408 bit raund kalitlari talab qilinadi. 128 bitli kalit uzunligi uchun raund kalitlarini generatsiyalash jarayonini ko'rib o'taylik.

Dastlabki kalitni kengaytirishda, dastlab 128 bitli (16 bayt) boshlang'ich kiruvchi kalit kiritiladi va to'rtta (w_0, w_1, w_2, w_3) 32 bitdan bo'lgan bo'lakka bo'linadi. Qolgan kengaytirilgan kalitlar mana shu to'rtta (w_0, w_1, w_2, w_3) kalitlar yordamida topiladi. Ya'ni, kengaytirilgan kalitlar quyida keltirilgan (5.2) va (5.3) formulalar asosida hisoblab topiladi. Kengaytirilgan kalitlar soni $N[w(i)] = N_b(N_r + 1)$ tenglik bilan hisoblanadi. Xususan, 128 bitli kalit uchun $N_b = 4$, $N_r = 10$ ga tengligi bois, $N[w(i)] = 4(10 + 1) = 44$ ga teng.

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

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

$$w[i] = w[i - 1] \oplus w[i - N_k], \quad (5.2)$$

va

$$w[i] = \text{SubWord}(\text{RotWord}(w[i - 1])) \oplus \text{Rcon}[i/N_k] \oplus w[i - N_k] \quad (5.3)$$

128 bitli kalit uchun raund kalitlarini generatsiyalashga oid misol 1-ilovaga keltirilgan.

5.4. ГОСТ 28147-89 simmetrik blokli shifrlash standarti

ГОСТ 28147-89 kriptotalgoritmi hozirda Rossiya Federatsiyasi davlat standart shifrlash algoritmi hisoblanadi. Bu algoritm apparat va dasturiy ta'minot uchun mo'ljallangan bo'lib, himoyalangan ma'lumotning maxfiylik darajasiga chegara yo'q. Algoritmning kalit uzunligi 256 bitga shifrlashni 64 bit uzunlikdagi bloklarda amalga oshiradi va raundlar soni 32 ga teng. Ushbu algoritm Feystel tarmog'iga asoslangan bo'lib, asosiy shifrlash rejimi oddiy almashtirishga asoslangan (bundan tashqari, murakkablikka asoslangan gammalishtirish rejimi, qayta aloqali gammalashtirish rejimi va xesh funksiya sifatida foydalanishga mo'ljallangan imitoqo'yish rejimi mavjud).

ГОСТ 28147-89 shifrlash algoritmining matematik asosi quyidagi amallarga asoslanadi:

- $mod2^{32}$ bo'yicha qo'shish amali. Ushbu jarayonda ma'lumot blokining o'ng qismi va 32 bitli raund kaliti $mod2^{32}$ amali asosida qo'shiladi. Ushbu amal XOR amaliga qaraganda kriptobardoshli sanaladi.

- Almashtirish jadvali orqali o'rin almashtirish.k. Ushbu amal ГОСТ 28147-89 algoritmidan foydalanilgan yagona chiziqsiz funksiya bo'lib, u maxfiylik darajasini yanada oshiradi.

- Siklik surish amali. Ushbu amal chiziqli funksiya hisoblanadi. 32 bitli ma'lumotni 11 bit siklik chapga surish orqali amalga oshiriladi.

- XOR amalida qo'shish.k. Ushbu amalda ma'lumotning chap tomoni va 11 bit siklik surilgan o'ng tomon qo'shiladi.

Ushbu kriptografik algoritm o'zida yuqorida ko'rsatilgan sodda matematik amallarni birlashtirgan bo'lib, bu imkoniyat shifrlash/rasshifrovkalashda katta tezlikni beradi.

ГОСТ 28147-89 algoritmidan kalit generatori. Kiritilgan 256 bitli K kalit 32 bitli 8 ta teng qismlarga ajratiladi: $K = K_0K_1K_2K_3K_4K_5K_6K_7$. Shundan so'ng, ushbu qismkalitlarni quyidagicha foydalanish orqali 32 raund uchun raund kalitlari shakllantiriladi:

| Raundlar soni | Kalitlar |
|---------------|----------------------------|
| 1-8 | $K_0K_1K_2K_3K_4K_5K_6K_7$ |
| 9-16 | $K_0K_1K_2K_3K_4K_5K_6K_7$ |
| 17-24 | $K_0K_1K_2K_3K_4K_5K_6K_7$ |
| 25-32 | $K_7K_6K_5K_4K_3K_2K_1K_0$ |

Biror ma'lumotni FOCT 28147-89 kript algoritmi bilan shifrlash uchun dastlab 256 bitli kalitdan 32 ta 32 bitli rund kalitlari K_i generatsiya qilinadi va ochiq ma'lumot 64 bitli $X_i, i = 1, 2, \dots$ bloklarga bo'linadi. Bu 64 bitli X_i blok 32 bitli chap L_i va o'ng R_i qismlarga bo'linadi $X_i = L_i \parallel R_i$ va $\begin{cases} L_i = R_{i-1} \\ R_i = L_{i-1} \oplus F(R_{i-1}, K_i) \end{cases}$ formula yordamida almashtiriladi, ya'ni shifrlanadi.

Kript algoritmnining F funksiyasi quyidagi amal va almashtirishlardan tashkil topgan:

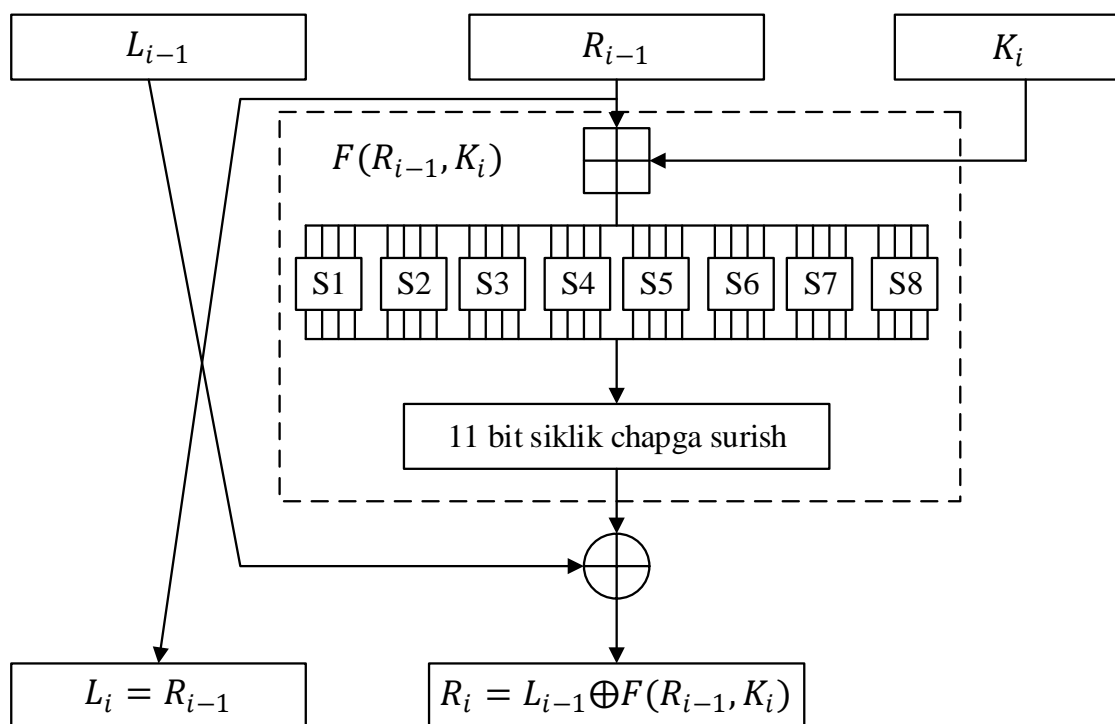
1) Blokning 32 bitli o'ng qismi va 32 bitli raund kalitini $\text{mod}2^{32}$ bo'yicha qo'shish: $C_i = (R_{i-1} + K_i) \text{mod}2^{32}$;

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

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

4) Ochik ma'lumot 32 raund iterativ shifrlashdan so'ng, chap L_{32} va o'ng R_{32} qismlar birlashtiriladi va $Y_i = R_{32} \parallel L_{32}$ shifirma'lumot, ya'ni Y_i shifirma'lumot hosil qilinadi.

FOCT 28147-89 kript algoritmining i -raundining funksional sxemasi quyida keltirilgan:



5.7-rasm. FOCT 28147-89 kript algoritmining i -raundi

Ushbu algoritm to‘rt xil rejimda ishlaydi:

- oddiy almashtirish;
- gammalashga asoslangan;
- teskari aloqali gammalashga asoslangan;
- imitoqo‘yish rejimi.

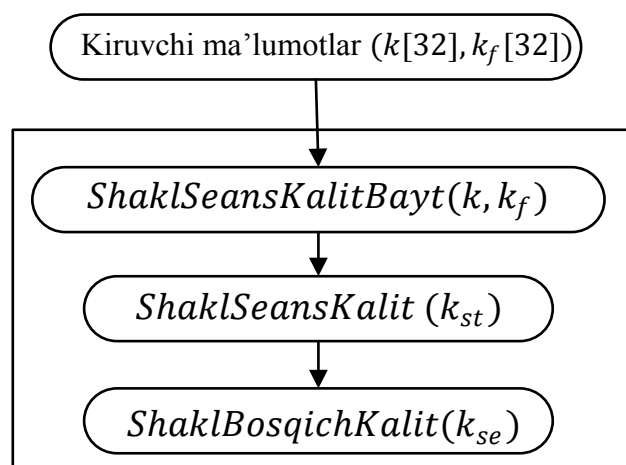
ГОСТ 28147-89 kriptooritmidan foydalanilgan S-bloklar statik emas. Turli tashkilotlar tomonidan turli S-bloklardan foydalanilgan. Quyida Rosstandartning “Axborotning kriptografiya himoyasi” bo‘yicha standartida keltirilgan S-blok keltirilgan.

| S-blok raqami | Qiymatlari | | | | | | | | | | | | | | | |
|---------------|------------|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| | 0 | 1 | 2 | 3 | 4 | 5 | 6 | 7 | 8 | 9 | A | B | C | D | E | F |
| 1 | C | 4 | 6 | 2 | A | 5 | B | 9 | E | 8 | D | 7 | 0 | 3 | F | 1 |
| 2 | 6 | 8 | 2 | 3 | 9 | A | 5 | C | 1 | E | 4 | 7 | B | D | 0 | F |
| 3 | B | 3 | 5 | 8 | 2 | F | A | D | E | 1 | 7 | 4 | C | 9 | 6 | 0 |
| 4 | C | 8 | 2 | 1 | D | 4 | F | 6 | 7 | 0 | A | 5 | 3 | E | 9 | B |
| 5 | 7 | F | 5 | A | 8 | 1 | 6 | D | 0 | 9 | 3 | E | B | 4 | 2 | C |
| 6 | 5 | D | F | 6 | 9 | 2 | C | A | B | 7 | 8 | 1 | 4 | 3 | E | 0 |
| 7 | 8 | E | 2 | 5 | 6 | 9 | 1 | C | F | 4 | B | 0 | D | A | 3 | 7 |
| 8 | 1 | 7 | E | D | 0 | 5 | 8 | 3 | 4 | F | A | 6 | 9 | C | B | 2 |

5.5. O‘z Dst 1105:2009 simmetrik blokli shifrlash standarti

O‘z DSt 1105:2009 algoritmi O‘zbekiston Respublikasining shifrlash standarti hisoblanadi. Ushbu “Ma’lumotlarni shifrlash algoritmi” (MSHA) standarti elektron ma’lumotlarni muhofaza qilish uchun mo‘ljallangan kriptografik algoritmni ifodalaydi. MSHA - simmetrik blokli shifr bo‘lib, 256 bit uzunlikdagi ma’lumotlar blokini shifratilgan o‘g‘irish va shifratilgan dastlabki matnga o‘g‘irish uchun 256 yoki 512 bit uzunlikdagi kriptografik kalitlardan foydalanadi.

Algoritm asosan ikki qismdan kalitlarni generatsiyalash va shifrlash/ rasshifrovkalash jarayonlaridan tashkil topgan. Kalitlarni generatsiyalash bosqichida shifrlash kaliti va funksional kalitdan foydalanib, raund kalitlarini va S bloklarni hosil qilish bosqichlari bajariladi. Bu bosqichlar quyidagi 5.8-rasmda keltirilgan *ShaklSeansKalitBayt()*, *ShaklSeansKalit()*, *ShaklBosqichKalit()* funksiyalarini ketma-ket bajarish orqali amalga oshiriladi.



5.8-rasm. Raund kalitlari va S bloklarni generatsiyalash tartibi

$ShaklSeansKalitBayt(k[32], k_f[32])$ almashtirish funksiyasining vazifasi seans kalitini hosil qilish va uning yordamida S bloklarni generatsiyalashdan iborat.

Seans kaliti

$$k_{se} = k + k' * (1 + k_f * k) \quad (5.4)$$

formula yordamida hosil qilingan qiymatning chapdan 672 bitini ajratib olish orqali hosil qilinadi.

Bu yerda, k va k_f - mos holda tanlangan shifrlash va funksional kalitlar, k' – k_f ning o'ngdan 192 bitli qismi hisoblanadi.

Hosil qilingan seans kaliti yordamida S – bloklarni generatsiyalash quyidagi tartibda amalga oshiriladi:

– k_{se} seans kalitining o'ngdan 256+64 bitli qismi ajratib olinadi va uning chapdan 256 bitli qismidan baytli elementlardan tarkib topgan chiziqli massiv $k_{st} = [0,1,2,3, \dots 31]$, qolgan 64 bitli qismidan – bayt sathida elementlardan tarkib topgan chiziqli massiv $B = [0,1,2,3,4,5,6,7]$ shakllantiriladi;

– chiziqli massiv B elementlari $B_1 = [0,1,2,3]$ va $B_2 = [4,5,6,7]$ massivlarga ajratiladi va ulardan ma'lum qoidalar asosida (d_1, R_1, L_1) va (d_2, R_2, L_2) parametrlar uchliklari shakllantiriladi.

Yuqoridagi uchlik parametrlardan foydalanib bayt sathida shifrlash uchun, toq va juft raundlarda ishlatiladigan chiziqli massivlar juftligidan iborat $(B_{1A} [256], B_{2A} [256])$ S-bloklar quyidagicha formula yordamida hosil qilinadi:

$$i = 0 \div 255 \text{ uchun}$$

$$b_{sA}[i] \equiv \left(((i + L) \bmod 256) + 1 \right) |^{ds} \pmod{257} \pmod{256} \quad (5.5)$$

bu yerda, butun sonlarni ko'paytirish, teskarilash va darajaga oshirish deb atalgan parametrli algebra amallaridan foydalaniladi.

X ni Y ga p modul bo'yicha R parametrli ko'paytirish quyidagicha bajariladi:

$$X \otimes Y \pmod{p} \equiv X + Y(1 + RX) \pmod{p} \quad (5.6)$$

X o'zgaruvchini p modul bo'yicha R parametrli teskarilash quyidagicha bajariladi:

$$X^{-1} \pmod{p} \equiv -X(1 + RX)^{-1} \pmod{p} \quad (5.7)$$

bu yerda $X^{-1} \otimes X \equiv 0 \pmod{p}$, 0 – parametrli gruppaning birlik asosidir.

Misol. X ni p modul bo'yicha R parametr d darajaga oshirish amali $X^d \pmod{p}$ ko'rinishida ifodalanadi:

Masalan $X = 3$, $R = 7$, $d = 35$, $p = 256$ bo'lganda X^{35} quyidagicha hisoblanadi:

$$X^{35} \equiv X^{32+2+1} \equiv (((X^2)^2)^2)^2 \otimes X^2 \otimes X \pmod{p}$$

$$\text{bu yerda: } X^2 \pmod{p} \equiv X(2 + XR) \pmod{p}$$

Qiymatlarni o'rniga qo'yib quyidagiga ega bo'linadi:

$$\begin{aligned} X^2 \pmod{p} &\equiv 3(2 + 3 * 7) \pmod{256} = 69 \\ X^{35} &\equiv (((69)^2)^2)^2 \otimes 3^2 \otimes 3 \pmod{256} \\ &\equiv (69 * (2 + 69 * 7) \pmod{256})^2 \otimes 3^2 \otimes 3 \pmod{256} \\ &\equiv ((185 \\ &* (2 + 185 * 7) \pmod{256})^2 \otimes 3^2 \otimes 3 \pmod{256} \\ &\equiv (73 * (2 + 73 * 7) \pmod{256})^2 \otimes 3^2 \otimes 3 \pmod{256} \\ &\equiv 73 * (2 + 73 * 7) \pmod{256} \otimes 3^2 \otimes 3 \pmod{256} \\ &\equiv 73 \otimes 69 \otimes 3 \equiv (73 + 69 * (1 + 7 * 73)) \pmod{256} \otimes 3 \\ &\equiv 73 \otimes 3 \equiv (73 + 3 * (1 + 7 * 73)) \pmod{256} \equiv 73 \end{aligned}$$

Keyingi qadamda *ShaklSeansKalit* (k_{st}) funksiyasi yordamida shifrlash va rasshifrovkalashda ishlatiladigan diamatritsalar quyidagicha generatsiya qilinadi:

– baytli elementlardan tarkib topgan chiziqli massiv $k_{st} = [0,1,2,3, \dots 31]$ ning chapdan 20 baytli elementlaridan tarkib topgan chiziqli massiv qismi $K_{ss} = [0,1,2,3, \dots 19]$ ajratib olinadi;

– $i = 0 - 19$ uchun, agar $K_{ss}[i] = 0$ bo'lsa, u holda $K_{ss}[i]$ ni $K_{ss}[i] - 1 \pmod{p}$ ga almashtiriladi.

Chiziqli massiv K_{ss} ning elementlaridan ikki o'lchamli $K_1[4,4]$ va $K_2[4,4]$ massivlari quyidagi tartibda shakllantiriladi:

chiziqli massiv $K_s = [0,1,2,3, \dots 19]$ ikkita chiziqli massivlar $k_{s1} = [0,1,2,3, \dots 9]$ va $k_{s2} = [10,11,12,13, \dots, 19]$ ga ajratiladi va ularning har biri mos tarzda tartiblangan to'plam $\{k_{s1}[0,1], k_{s1}[0,2], k_{s1}[0,3], k_{s1}[1,0], k_{s1}[2,0], k_{s1}[2,1], k_{s1}[2,2], k_{s1}[3,0], k_{s1}[3,1], k_{s1}[3,2]\}$ va $\{k_{s2}[0,1], k_{s2}[0,2], k_{s2}[0,3], k_{s2}[1,0], k_{s2}[2,0], k_{s2}[2,1], k_{s2}[2,2], k_{s2}[3,0], k_{s2}[3,1], k_{s2}[3,2]\}$ ga o'zaro – bir qiymatli akslantiriladi va ularning har biridan mos tarzda ikkita $K_1[4,4]$ va $K_2[4,4]$ massivlarining $k_1[i,j]$, $k_2[i,j]$ elementlari shakllantiriladi (bu yerda, $i, j \in \{0,1,2,3\}$).

$K_s[4,4]$, $s \in \{1,2\}$ massivlarining qolgan elementlari quyidagi qoida asosida shakllantiriladi:

– $j \in \{0,1,2,3\}$ uchun $i = j$ bo'lganda, elementlar aynan va qiymati bo'yicha $K_s[2,2]$ elementga teng;

– $i = 1, j = 0,2,3$ uchun elementlar aynan va qiymati bo'yicha $K_s[1,0]$ elementga teng;

– $i = 2, j = 0,3$ uchun elementlar aynan va qiymati bo'yicha $K_s[2,0]$ elementga teng.

Natijada, *sh*-shifrlash rejimida foydalanish uchun $K_s[8,4]$ sifatida quyidagi $K_1[4,4]$ va $K_2[4,4]$ ikkita maxsus tuzilmali diamatritsa shakllanadi.

Massiv K_1

| | | | |
|------------|------------|------------|------------|
| $k_1[0,0]$ | $k_1[0,1]$ | $k_1[0,2]$ | $k_1[0,3]$ |
| $k_1[1,0]$ | $k_1[1,1]$ | $k_1[1,2]$ | $k_1[1,3]$ |
| $k_1[2,0]$ | $k_1[2,1]$ | $k_1[2,2]$ | $k_1[2,3]$ |
| $k_1[3,0]$ | $k_1[3,1]$ | $k_1[3,2]$ | $k_1[3,3]$ |

Massiv K_2

| | | | |
|------------|------------|------------|------------|
| $k_2[0,0]$ | $k_2[0,1]$ | $k_2[0,2]$ | $k_2[0,3]$ |
| $k_2[1,0]$ | $k_2[1,1]$ | $k_2[1,2]$ | $k_2[1,3]$ |

| | | | |
|-------------|-------------|-------------|-------------|
| $k_2 [2,0]$ | $k_2 [2,1]$ | $k_2 [2,2]$ | $k_2 [2,3]$ |
| $k_2 [3,0]$ | $k_2 [3,1]$ | $k_2 [3,2]$ | $k_2 [3,3]$ |

sh - shifrlash rejimidan foydalanishda maxsus tuzilmali diamatritsa $K_1[4,4]$ uchun teskari maxsus tuzilmali diamatritsa $K_{1t}[4,4]$ hisoblanadi. Shuningdek, *dsh* - rasshifrovkalash rejimidan foydalanishda ham maxsus tuzilmali diamatritsa $K_2[4,4]$ uchun teskari maxsus tuzilmali diamatritsa $K_{2t}[4,4]$ hisoblanadi.

Diaaniqlovchisi noldan farqli maxsus tuzilmali diamatritsa $K_{1i}[4,4]$ ni (bu yerda, $i = \{1, 2\}$) teskarilash uning ustida diaalmashtirish natijasida hosil bo'lgan matritsaning teskari matritsasini hisoblash va hosil bo'lgan teskari matritsa ustida diaalmashtirish amalini bajarish natijasini olishdan iborat.

Teskarilash natijasida ikkala $K_{1t}[4,4]$ va $K_{2t}[4,4]$ ham maxsus tuzilmali diamatritsa ko'rinishiga ega bo'lgan quyidagi K_{1t} va K_{2t} massivlar hosil bo'ladi:

Massiv K_{1t}

| | | | |
|----------------|---------------|---------------|----------------|
| $k_{1t} [0,0]$ | $k_{1t}[0,1]$ | $k_{1t}[0,2]$ | $k_{1t} [0,3]$ |
| $k_{1t} [1,0]$ | $k_{1t}[1,1]$ | $k_{1t}[1,2]$ | $k_{1t} [1,3]$ |
| $k_{1t} [2,0]$ | $k_{1t}[2,1]$ | $k_{1t}[2,2]$ | $k_{1t} [2,3]$ |
| $k_{1t}[3,0]$ | $k_{1t}[3,1]$ | $k_{1t}[3,2]$ | $k_{1t} [3,3]$ |

Massiv K_{2t}

| | | | |
|----------------|----------------|----------------|----------------|
| $k_{2t} [0,0]$ | $k_{2t} [0,1]$ | $k_{2t} [0,2]$ | $k_{2t} [0,3]$ |
| $k_{2t} [1,0]$ | $k_{2t} [1,1]$ | $k_{2t} [1,2]$ | $k_{2t} [1,3]$ |
| $k_{2t} [2,0]$ | $k_{2t} [2,1]$ | $k_{2t} [2,2]$ | $k_{2t} [2,3]$ |
| $k_{2t}[3,0]$ | $k_{2t} [3,1]$ | $k_{2t} [3,2]$ | $k_{2t} [3,3]$ |

sh-shifrlash rejimidan foydalanishda (K_{1t}, K_2) juftlik, *dsh*-rejimidan foydalanishda esa (K_1, K_{2t}) juftlik ishlatiladi.

Keyingi bosqichda *ShaklBosqichKalit*(k_{se}) almashtirish funksiyasi (chizikli seans-bosqich kaliti massivini shakllantirish) yordamida raund kalitlari quyidagicha generatsiya qilinadi:

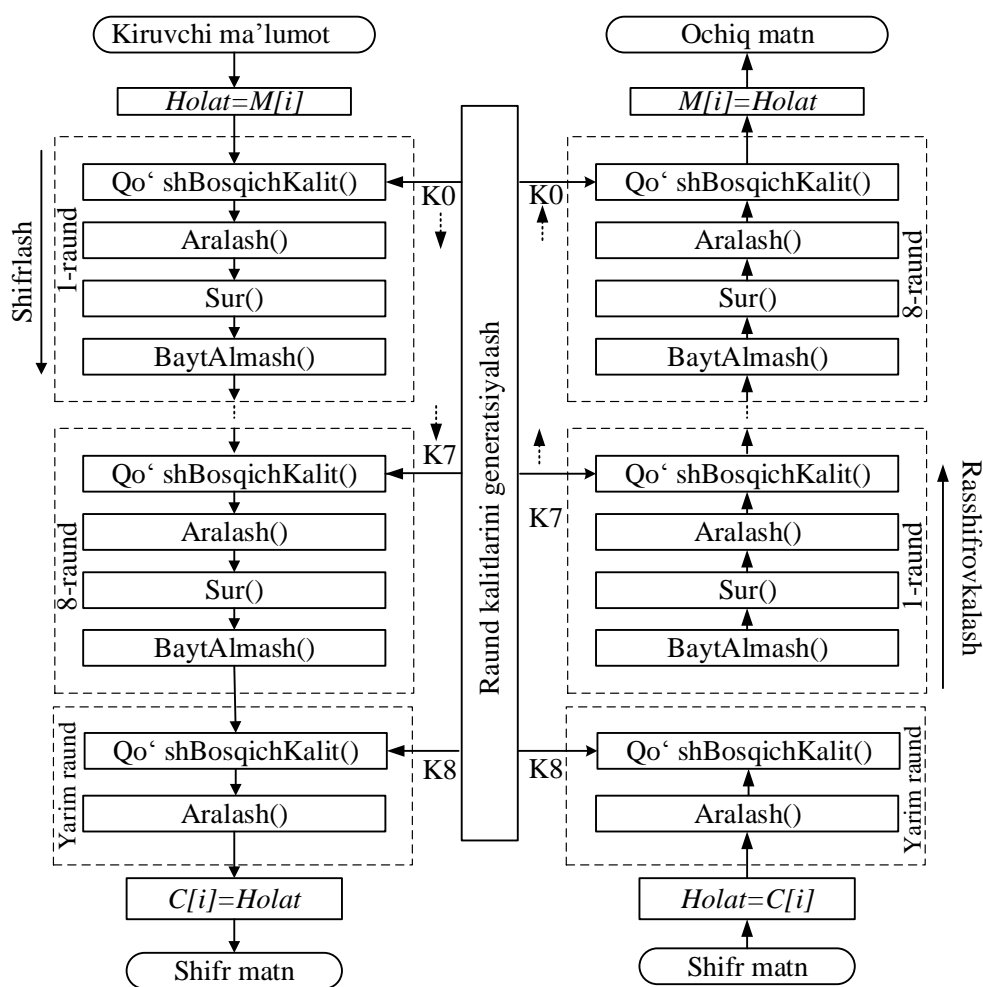
– *bosqich*=1 va $m=sh$ bo'lsa, u holda chizikli seans-bosqich kaliti massivi k_{se} o'zgarishsiz qoldiriladi, agar *bosqich*=0 va $m=dsh$ bo'lsa, u holda k_{se} massivi o'ngga $672-(e \times 83) \bmod 672$ bitga suriladi (e – raund tartibi);

– agar *bosqich*>1 va $m=sh$ bo'lsa, unda davriy tarzda o'ngga k_{se} massivi 83 bitga suriladi, agar *bosqich*≥1 va $m=dsh$ bo'lsa, unda davriy tarzda chapga k_{se} massivi 83 bitga suriladi.

Chizikli seans-bosqich kaliti massivining chap tomonidan 256 bitli qismini ajratib olib, undan elementlari bayt sathida berilgan $K_e[8,4]$ massivi shakllantiriladi. Bu almashtirish shifrlash jarayoni boshlangunga qadar hamma bosqichlar uchun amalga oshiriladi.

S bloklar generatsiya qilingandan so'ng shifrlash va rasshifrovkalash jarayoni quyidagi 5.9-rasmda ko'rsatilgan sxema asosida bajariladi.

Dastlab matnni shifratnga almashtirish rejimida ochiqmatn, shifratni dastlabki matnga almashtirish rejimida esa shifratni kriptografik modulning $Holat[8,4]$ massiviga yuklanadi. Keyin 8 ta raundning har birida $Qo'shBosqichKalit(Holat, K_e)$, $Aralash(Holat, K_s)$, $Sur(Holat)$, $BaytAlmash(Holat, B_a)$ funksiyalari bajariladi. 8-raund tugagandan so'ng esa faqat $Qo'shBosqichKalit(Holat, K_e)$, $Aralash(Holat, K_s)$ funksiyalari bajariladi. Shifrlash jarayoni 2 xil rejimda amalga oshiriladi. Bular shifratn bloklarini ilaktirish (Cipher block chaining, CBC) va elektron kod kitobi (Electronic code book, ECB) rejimlaridir.



5.9-rasm. Elektron kod kitobi rejimida shifrlash va rasshifrovkalash jarayoni blok sxemasi

Ochiqmatn $Holat[8,4]$ massiviga yuklangandan so‘ng $Qo'shBosqichKalit(Holat, K_e)$ funksiyasi yordamida $Holat$ massivi va $K_e[8,4]$ seans kaliti massivlarining har bir bayt sathidagi bir nomli elementlari ustida XOR amali quyidagi tartibda bajariladi:

$0 \leq c < 8$ uchun

$$\begin{aligned} & [h'[c, 0], h'[c, 1], h'[c, 2], h'[c, 3]] = \\ & [h[c, 0], h[c, 1], h[c, 2], h[c, 3]] \oplus [ke[c, 0], ke[c, 1], ke[c, 2], ke[c, 3]]. \end{aligned}$$

Natija $Holat$ massiviga ko‘chiriladi. Keyin $Sur (Holat)$ funksiyasi bajariladi. $Sur (Holat)$ almashtirishi agar $m = sh$ rejimida bo‘lsa, unda davriy tarzda $Holat$ massivining j –ustuni avvalo, pastga $(j + 1) \pmod{8}$ baytga suriladi, keyin hosil bo‘lgan massivning i –satri o‘ngga $(i + 1) \pmod{4}$ baytga suriladi, aks holda $m = dsh$ bo‘lsa, unda davriy tarzda $Holat$ massivining i –satri avvalo, chapga $(i + 1) \pmod{4}$ baytga suriladi, so‘ngra hosil bo‘lgan massivning j -ustuni yuqoriga $(j + 1) \pmod{8}$ baytga suriladi. Bu yerda, $0 \leq i < 4, 0 \leq j < 8$.

Keyingi amal $Aralash (Holat, K_s)$ quyidagi amallarni bajarishdan iborat:

– agar $m = sh$ bo‘lsa, unda $K_1 = K_{1t}, K_2 = K_2$ qabul qilinadi, $H_1 \otimes_2 K_1 \pmod{p}, H_2 \otimes_2 K_2 \pmod{p}$ hisoblanadi, natija H_1, H_2 massivlariga yozilib, $Holat$ massiviga ko‘chiriladi, aks holda, ya‘ni $m = dsh$ bo‘lsa, unda $K_1 = K_1, K_2 = K_{2t}$ qabul qilinadi, $H_1 \otimes_2 K_1 \pmod{p}, H_2 \otimes_2 K_2 \pmod{p}$ hisoblanadi, natija H_1, H_2 massivlariga yozilib, $Holat$ massiviga ko‘chiriladi. $H_1 \otimes_2 K_1 \pmod{p}, H_2 \otimes_2 K_2 \pmod{p}$ ochiq matn biti $H_i, i \in [1,2]$ ni maxsus tuzilmali diamatritsaga ko‘paytirish qo‘yidagi qoidalar asosida amalga oshiriladi:

| | |
|-----------|---|
| $h'[0,0]$ | $h'_0 = h_0(k_0 + k_4 + k_8 + k_{12}) - h_5k_4 - h_{10}k_8 - h_{15}k_{12} \pmod{p}$ |
| $h'[1,1]$ | $h'_5 = h_5(k_1 + k_5 + k_9 + k_{13}) - h_0k_1 - h_{10}k_9 - h_{15}k_{13} \pmod{p}$ |
| $h'[2,2]$ | $h'_{10} = h_{10}(k_2 + k_6 + k_{10} + k_{14}) - h_0k_2 - h_5k_6 - h_{15}k_{14} \pmod{p}$ |
| $h'[3,3]$ | $h'_{15} = h_{15}(k_3 + k_7 + k_{11} + k_{15}) - h_0k_3 - h_5k_7 - h_{10}k_{11} \pmod{p}$ |
| $h'[0,1]$ | $h'_1 = h_1(k_1 + k_5 + k_9 + k_{13}) + (h_0 + h_4 + h_8 + h_{12})k_1 - h_2k_9 - h_3k_{13} \pmod{p}$ |
| $h'[0,2]$ | $h'_2 = h_2(k_2 + k_6 + k_{10} + k_{14}) + (h_0 + h_4 + h_8 + h_{12})k_2 - h_1k_6 - h_3k_{14} \pmod{p}$ |
| $h'[0,3]$ | $h'_3 = h_3(k_3 + k_7 + k_{11} + k_{15}) + (h_0 + h_4 + h_8 + h_{12})k_3 - h_1k_7 - h_2k_{11} \pmod{p}$ |

| | |
|-----------|---|
| $h'[1,0]$ | $h'_4=h_4(k_0+k_4+k_8+k_{12})+(h_1+h_5+h_9+h_{13})k_4-h_6k_8-h_7k_{12}(modp)$ |
| $h'[1,2]$ | $h'_6=h_6(k_2+k_6+k_{10}+k_{14})+(h_1+h_5+h_9+h_{13})k_6-h_4k_2-h_7k_{14}(modp)$ |
| $h'[1,3]$ | $h'_7=h_7(k_3+k_7+k_{11}+k_{15})+(h_1+h_5+h_9+h_{13})k_7-h_4k_3-h_6k_{11}(modp)$ |
| $h'[2,0]$ | $h'_8=h_8(k_0+k_4+k_8+k_{12})+(h_2+h_6+h_{10}+h_{14})k_8-h_9k_4-h_{11}k_{12}(modp)$ |
| $h'[2,1]$ | $h'_9=h_9(k_1+k_5+k_9+k_{13})+(h_2+h_6+h_{10}+h_{14})k_9-h_8k_1-h_{11}k_{13}(modp)$ |
| $h'[2,3]$ | $h'_{11}=h_{11}(k_3+k_7+k_{11}+k_{15})+(h_2+h_6+h_{10}+h_{14})k_{11}-h_8k_3-h_9k_7(modp)$ |
| $h'[3,0]$ | $h'_{12}=h_{12}(k_0+k_4+k_8+k_{12})+(h_3+h_7+h_{11}+h_{15})k_{12}-h_{13}k_4-h_{14}k_8(modp)$ |
| $h'[3,1]$ | $h'_{13}=h_{13}(k_1+k_5+k_9+k_{13})+(h_3+h_7+h_{11}+h_{15})k_{13}-h_{12}k_1-h_{14}k_9(modp)$ |
| $h'[3,2]$ | $h'_{14}=h_{14}(k_2+k_6+k_{10}+k_{14})+(h_3+h_7+h_{11}+h_{15})k_{14}-h_{12}k_2-h_{13}k_6(modp)$ |

Misol. d_2 – diamatritsaviy ko‘paytirish:

$$\begin{array}{ccc}
 d_2H_1 & d_2K_1 & d_2C_1 \\
 \left| \begin{array}{cccc} 1 & 2 & 3 & 4 \\ 12 & 9 & 21 & 0 \\ 13 & 17 & 6 & 31 \\ 14 & 18 & 29 & 9 \end{array} \right| & \otimes_{\mathbb{R}_2} & \left| \begin{array}{cccc} 17 & 1 & 2 & 3 \\ 4 & 5 & 7 & 8 \\ 9 & 10 & 11 & 12 \\ 13 & 14 & 15 & 16 \end{array} \right| \equiv \\
 \left| \begin{array}{cccc} 92 & 14 & 111 & 224 \\ 255 & 83 & 9 & 80 \\ 107 & 141 & 10 & 206 \\ 73 & 84 & 241 & 204 \end{array} \right| & &
 \end{array}$$

Yuqoridagi diamatritsaga ko‘paytirish qoidalaridan foydalanib hisoblangan natijaviy matritsani hisoblashning bitta elementi quyidagicha:

$$\begin{aligned}
 h'[0,0] &= h'_0 = h_0(k_0+k_4+k_8+k_{12}) - h_5k_4 - h_{10}k_8 - \\
 & h_{15}k_{12} (modp) = 1*(17+4+9+13) - 9*4 - 6*9 - 9*13 = (43-36-54- \\
 & 117)(mod 256) = 92.
 \end{aligned}$$

Qolgan elementlar ham yuqoridagi jadvaldagi qoidalar asosida hisoblanadi.

So‘ngi funksiya $BaytAlmash(Holat, B_a)$ almashtirishi quyidagi amallarni bajarishdan iborat:

– elementlari bayt sathida berilgan $Holat[8,4]$ massivi elementlari bayt sathida berilgan $Holatb[8,4]$ massivi ko‘rinishida nomlanadi;

– agar $m=sh$ bo‘lsa, u holda $B_a[256] = B_{sA}[256]$ qabul qilinadi, $Holatb[8,4]$ massivining har bir elementi B_a massivining adresi

bo'yicha unga mos elementi bilan almashtiriladi va natijaviy $Holatb[8,4]$ massivi bayt sathida berilgan $Holat[8,4]$ massiviga almashtiriladi, aks holda, ya'ni $m=dsh$ bo'lsa, u holda $B_a[256] = B_{sAD}[256]$ qabul qilinadi, $Holatb[8,4]$ massivining har bir elementi B_a massivining addressi bo'yicha unga mos elementi bilan almashtiriladi va natijaviy $Holat[8,4]$ massivi bayt sathida berilgan $Holat[8,4]$ massiviga almashtiriladi (bu yerda, $s \in \{1,2\}$). Almashtirish natijasining nusxasi $Holat$ massiviga ko'chiriladi va shifratn sifatida qabul qilinadi.

5.6. IDEA simmetrik blokli shifrlash algoritmi

IDEA (ing. International Data Encryption Algorithm – ma'lumotni shifrlashning xalqaro algoritmi) – simmetrik blokli shifrlash algoritmi bo'lib, Shvetsariyaning Ascom firmasi tomonidan patenglangan. Ushbu algoritmning birinchi versiyasi 1990-yilda Lay Syueszya va Djejms Messi tomonidan PES (ing. Proposed Encryption Standard – taklif etilgan shifrlash standarti) nomi bilan yaratilgan. Ushbu algoritmi Lay-Messi arxitekturasi asoslangan.

IDEA algoritmi 128 bitli kalit va 64 bitli blokdan foydalanadi. Raundlar soni 8 ga teng. Ochiq matnlar 64 bitli bloklarga bo'linadi. Agar ochiq matnning bitdagi uzunligi 64 ga karrali bo'lmasa, oxirgi blok aniqlangan baytlar bilan to'ldiriladi. Kiritilgan har bir 64 bitli blok 4 ta teng qismga (16 bitdan) bo'linadi va 16 bitli sonlar ustida shifrlashda foydalanilgan algebraik amallar bajariladi. IDEA shifrlash va rasshifrovkalash uchun yagona algoritmdan foydalanadi.

Algoritmda turli maydonlarda amalga oshiriluvchi quyidagi algebraik amallardan foydalanilgan:

- 2^{16} bo'yicha qo'shish amali (\boxplus);
- $2^{16} + 1$ bo'yicha ko'paytirish amali (\odot);
- bitlar ustida bajariluvchi XOR amali (\oplus).

Ushbu amallar uchun distributivlik va assotsiativlik qonuni o'rinli emas, ya'ni:

- $a \odot (b \boxplus c) \neq (a \odot b) \boxplus (a \odot c)$;
- $a \boxplus (b \oplus c) \neq (a \boxplus b) \oplus c$.

Raund kalitlarini generatsiyalash. k. 128 bitli kalitdan 8 raundning har biri uchun 16 bitli 6 ta kalit generatsiya qilinadi. Bundan tashqari, 8-raundan so'ng yana 4 ta 16 bitli kalit asosida amallar bajariladi. Umumiy hisobda, $52=8 \times 6+4$, 16 bitli kalitlar quyidagicha generatsiya qilinadi:

- dastlab 128 bitli kalit 16 bitli qismlarga ajratilib, dastlabki 8 ta qismkalitlarni hosil qiladi: $K_1^{(1)}, K_2^{(1)}, K_3^{(1)}, K_4^{(1)}, K_5^{(1)}, K_6^{(1)}, K_1^{(2)}, K_2^{(2)}$;
- shundan so‘ng, 128 bitli kalit chapga 25 bit siklik siljutilib, hosil bo‘lgan 128 bitli kalit yuqoridagi kabi 8 ta 16 bitli qismkalitlarga bo‘linadi: $K_3^{(2)}, K_4^{(2)}, K_5^{(2)}, K_6^{(2)}, K_1^{(3)}, K_2^{(3)}, K_3^{(3)}, K_4^{(3)}$;
- mazkur ketma-ketlik 52 ta 16 bitli bloklar hosil qilingunga qadar davom ettiriladi.

Natijaviy raund kalitlari esa quyidagicha bo‘ladi:

| Raund tartibi | Raundda foydalaniladigan qism kalitlar |
|-----------------------------|--|
| 1 | $K_1^{(1)}, K_2^{(1)}, K_3^{(1)}, K_4^{(1)}, K_5^{(1)}, K_6^{(1)}$ |
| 2 | $K_1^{(2)}, K_2^{(2)}, K_3^{(2)}, K_4^{(2)}, K_5^{(2)}, K_6^{(2)}$ |
| 3 | $K_1^{(3)}, K_2^{(3)}, K_3^{(3)}, K_4^{(3)}, K_5^{(3)}, K_6^{(3)}$ |
| 4 | $K_1^{(4)}, K_2^{(4)}, K_3^{(4)}, K_4^{(4)}, K_5^{(4)}, K_6^{(4)}$ |
| 5 | $K_1^{(5)}, K_2^{(5)}, K_3^{(5)}, K_4^{(5)}, K_5^{(5)}, K_6^{(5)}$ |
| 6 | $K_1^{(6)}, K_2^{(6)}, K_3^{(6)}, K_4^{(6)}, K_5^{(6)}, K_6^{(6)}$ |
| 7 | $K_1^{(7)}, K_2^{(7)}, K_3^{(7)}, K_4^{(7)}, K_5^{(7)}, K_6^{(7)}$ |
| 8 | $K_1^{(8)}, K_2^{(8)}, K_3^{(8)}, K_4^{(8)}, K_5^{(8)}, K_6^{(8)}$ |
| Chiqish akslantirishi uchun | $K_1^{(9)}, K_2^{(9)}, K_3^{(9)}, K_4^{(9)}$ |

Shifrlash jarayoni. IDEA algoritmidagi ma’lumot blokining shifrlash jarayoni 5.10-rasmda keltirilgan. Shifrlash jarayoni 8 ta raund va chiqish akslantirishidan iborat. Kiritilgan ma’lumot bloki 16 bitli 4 ta qismga ajratiladi (P_1, P_2, P_3, P_4). Mazkur 16 bitli bloklar ustida yuqorida keltirilgan uchta amaldan foydalaniladi. Ko‘paytirish amalida 0 o‘rniga 2^{16} foydalaniladi.

Shifrlash algoritmining matematik ifodasi quyida keltirilgan:

- 64 bitli blok 16 bitli qismlarga ajratiladi ($P_1^{(0)}, P_2^{(0)}, P_3^{(0)}, P_4^{(0)}$);
- har bir raund uchun ($i = 1 \dots 8$) quyidagilar bajariladi:
 - $A^{(i)} = P_1^{(i-1)} \odot K_1^{(i)}$;
 - $B^{(i)} = P_2^{(i-1)} \boxplus K_2^{(i)}$;
 - $C^{(i)} = P_3^{(i-1)} \boxplus K_3^{(i)}$;

$$\begin{aligned}
& \circ D^{(i)} = P_4^{(i-1)} \odot K_4^{(i)}; \\
& \circ E^{(i)} = A^{(i)} \oplus C^{(i)}; \\
& \circ F^{(i)} = B^{(i)} \oplus D^{(i)}; \\
& \circ P_1^{(i)} = A^{(i)} \oplus ((F^{(i)} \boxplus E^{(i)} \odot K_5^{(i)}) \odot K_6^{(i)}); \\
& \circ P_2^{(i)} = C^{(i)} \oplus ((F^{(i)} \boxplus E^{(i)} \odot K_5^{(i)}) \odot K_6^{(i)}); \\
& \circ P_3^{(i)} = B^{(i)} \oplus (E^{(i)} \odot K_5^{(i)} \boxplus (F^{(i)} \boxplus E^{(i)} \odot K_5^{(i)}) \odot K_6^{(i)}); \\
& \circ P_4^{(i)} = D^{(i)} \oplus (E^{(i)} \odot K_5^{(i)} \boxplus (F^{(i)} \boxplus E^{(i)} \odot K_5^{(i)}) \odot K_6^{(i)}).
\end{aligned}$$

Yuqorida keltirilgan amallar 8 raund bajarilgandan so‘ng, natijaviy 4 ta 16 bitli bloklar $P_1^{(8)}, P_2^{(8)}, P_3^{(8)}, P_4^{(8)}$ ga teng bo‘ladi.

Shundan so‘ng, natijaviy akslantirish quyidagicha amalga oshiriladi ($i = 9$):

$$\begin{aligned}
- P_1^{(9)} &= P_1^{(8)} \odot K_1^{(9)}; \\
- P_2^{(9)} &= P_3^{(8)} \boxplus K_2^{(9)}; \\
- P_3^{(9)} &= P_2^{(8)} \boxplus K_3^{(9)}; \\
- P_4^{(9)} &= P_4^{(8)} \odot K_4^{(9)}.
\end{aligned}$$

Shundan so‘ng, $P_1^{(9)}, P_2^{(9)}, P_3^{(9)}, P_4^{(9)}$ qisimbloklar shifratni hosil qiladi.

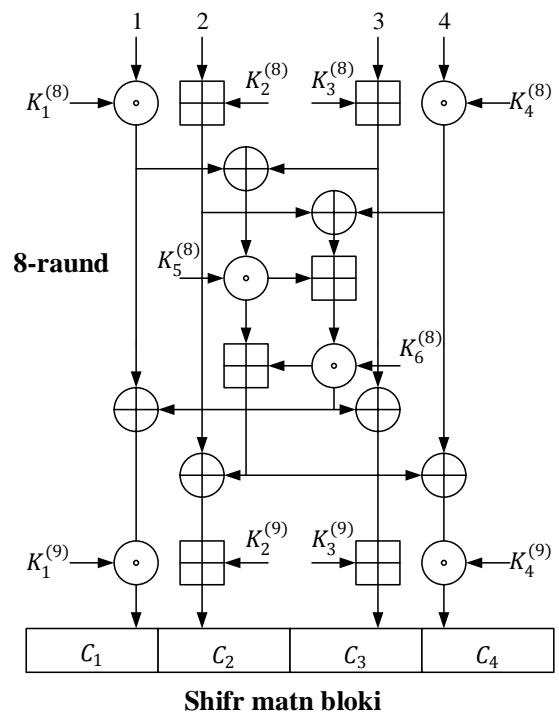
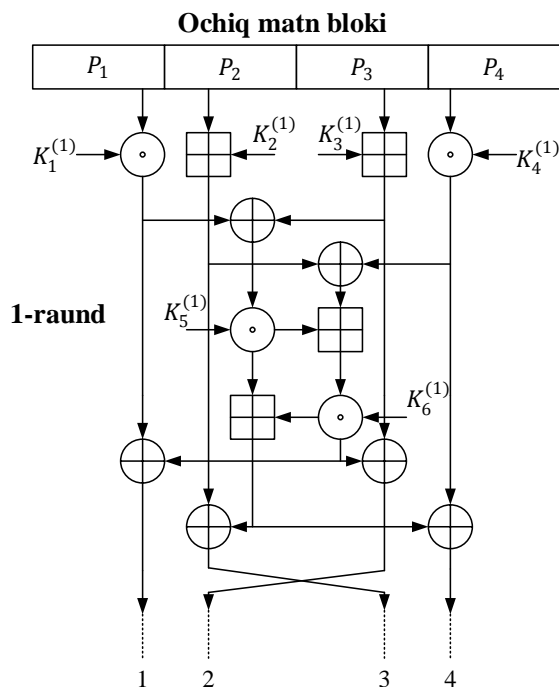
Rasshifrovkalash jarayoni. Rasshifrovkalash jarayoni ham 5.10-rasmda keltirilgan kabi amalga oshiriladi. Faqat, raund kalitlari teskari tartibda foydalaniladi. Rasshifrovkalash uchun raund kalitlarini teskari foydalanish tartibi 5.10-jadvalda keltirilgan.

5.10-jadval

Rasshifrovkalash uchun raund kalitlarining tartibi

| Raund tartibi | Raundda foydalaniladigan qism kalitlar |
|---------------|--|
| 1 | 2 |
| 1 | $1/K_1^{(9)}, -K_2^{(9)}, -K_3^{(9)}, 1/K_4^{(9)}, K_5^{(8)}, K_6^{(8)}$ |
| 2 | $1/K_1^{(8)}, -K_3^{(8)}, -K_2^{(8)}, 1/K_4^{(8)}, K_5^{(7)}, K_6^{(7)}$ |
| 3 | $1/K_1^{(7)}, -K_3^{(7)}, -K_2^{(7)}, 1/K_4^{(7)}, K_5^{(6)}, K_6^{(6)}$ |

| 1 | 2 |
|-----------------------------|--|
| 4 | $1/K_1^{(6)}, -K_3^{(6)}, -K_2^{(6)}, 1/K_4^{(6)}, K_5^{(5)}, K_6^{(5)}$ |
| 5 | $1/K_1^{(5)}, -K_3^{(5)}, -K_2^{(5)}, 1/K_4^{(5)}, K_5^{(4)}, K_6^{(4)}$ |
| 6 | $1/K_1^{(4)}, -K_3^{(4)}, -K_2^{(4)}, 1/K_4^{(4)}, K_5^{(3)}, K_6^{(3)}$ |
| 7 | $1/K_1^{(3)}, -K_3^{(3)}, -K_2^{(3)}, 1/K_4^{(3)}, K_5^{(2)}, K_6^{(2)}$ |
| 8 | $1/K_1^{(2)}, -K_3^{(2)}, -K_2^{(2)}, 1/K_4^{(2)}, K_5^{(1)}, K_6^{(1)}$ |
| Chiqish akslantirishi uchun | $1/K_1^{(1)}, -K_2^{(1)}, -K_3^{(1)}, 1/K_4^{(1)}$ |



5.10-rasm. IDEA algoritmining shifrlash jarayoni

Bu yerda, $1/K_j^{(i)}$ qism kalit $K_j^{(i)}$ kalitning $2^{16} + 1$ maydondagi multiplikativ teskarisi bo'lib, ular uchun $1/K_j^{(i)} * K_j^{(i)} = 1 \text{ mod}(2^{16} + 1)$ tenglik o'rinli bo'ladi. $-K_j^{(i)}$ qism kalit esa $K_j^{(i)}$ kalitning teskarisi bo'lib, ular uchun $-K_j^{(i)} + K_j^{(i)} = 0 \text{ mod}(2^{16})$ tenglik o'rinli. Masalan, $K_1^{(9)} = 0x0080$ ga teng bo'lsa, $1/K_1^{(9)} = 0xfe01$ ga teng bo'ladi, yoki $K_2^{(9)} = 0x00c0$ uchun $-K_2^{(9)} = 0xff40$ ga teng bo'ladi.

Ushbu algoritm shifrlash jarayonida yuqori tezlik qayd etib, apparat tarzda amalga oshirishga qulay hisoblanadi. Xususan, IDEA algoritmi

DES algoritmiga nisbatan 2 marta tezkor va xavfsizlik nuqtai nazaridan bardoshli hisoblanadi.

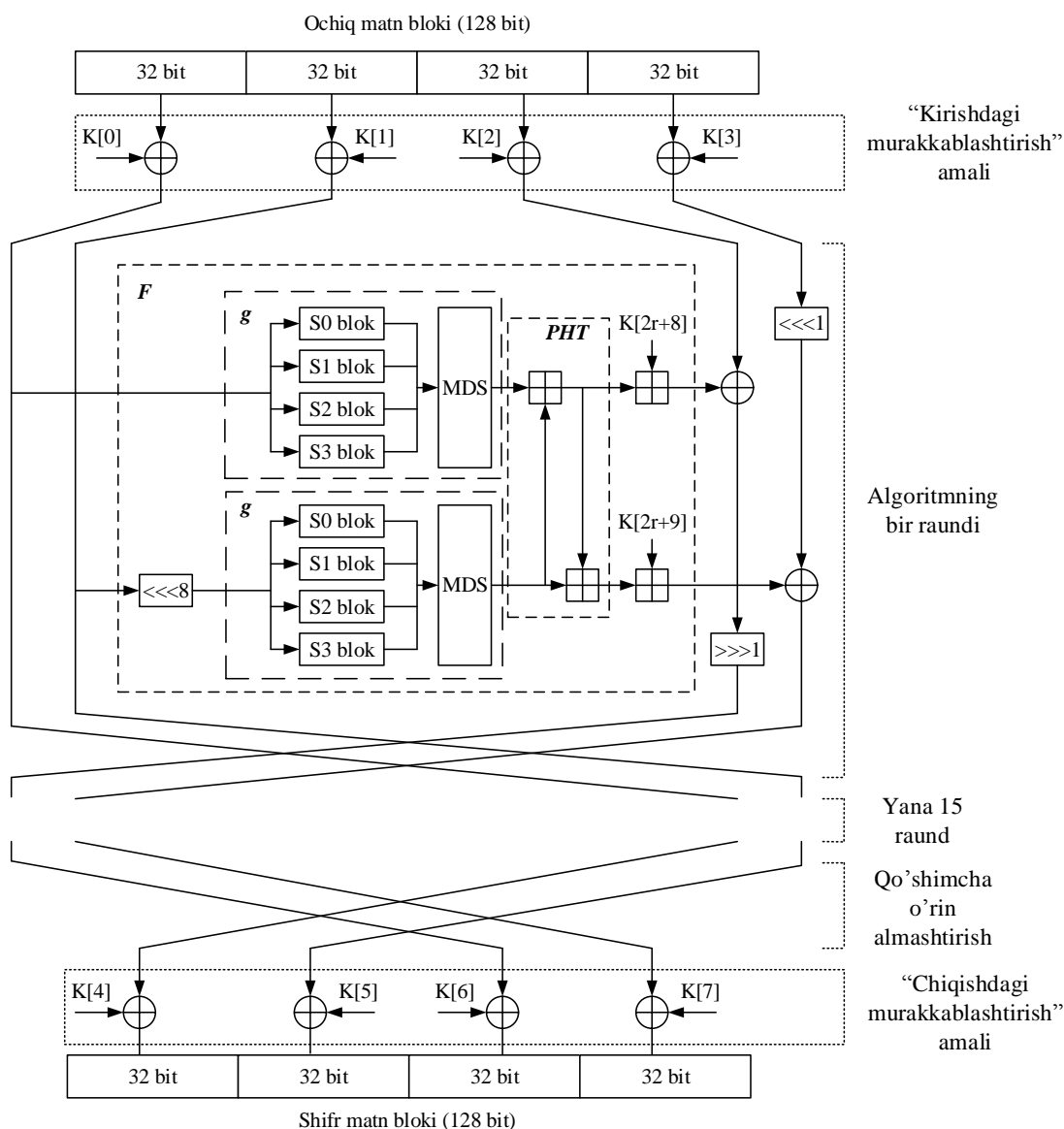
5.7. Twofish simmetrik blokli shifrlash algoritmi

Twofish algoritmi ma'lumotni shifrlashda 128 bitli ochiq matn bloki, 128, 192 va 256 bitli kalitlardan foydalanadi. Raundlar soni esa 16 ga teng bo'lib, Bryus Shnayer boshchiligidagi kriptografiklar tomonidan 1998-yilda ishlab chiqilgan. Ushbu algoritm AES konkursining 2 raundida ishtirok etgan 5 ta algoritmdan biri hisoblanadi. Ushbu algoritm Blowfish, SAFER va SQUARE algoritmlari asosida ishlab chiqilgan.

Mazkur shifrlash algoritmi Feystel tarmog'iga asoslangan bo'lib, F funksiya yordamida kalitga bog'liq hosil bo'ladigan to'rtta 8×8 o'lchamdagi S jadvallar, $GF(2^8)$ maydonda hisoblanadigan 4×4 o'lchamdagi o'zgaras MDS matritsasi, PHT (pseuda-Hadamard transform) Adamar kriptoaqlantirishi, siklik surish orqali hosil bo'ladigan kalit jadvallaridan iborat. Raund funksiyalari, kalitlarni generatsiyalash vaqti, mantiqiy amallari soni va xotira sarfining kamligi bilan simmetik blokli shifrlar orasida eng tezkor algoritmlardan biri hisoblanadi.

Twofish algoritmining umumiy sxemasini quyida 5.11-rasmda keltirilgan. Raundlar soni 16 ga teng. Algoritmida $\text{mod } 2^{32}$ bo'yicha qo'shish, XOR, siklik surish, $GF(2^8)$ maydonida ko'paytirish, o'rin almashtirish va o'rniga qo'yish amallaridan foydalanilgan. Twofish algoritmida foydalanilgan akslantirishlar quyidagilar.

Murakkablashtirish.k. Ushbu amal birinchi raundan oldin va oxirgi raundan keyin amalga oshiriladi. Shifrlashda dastlab "kirishdagi murakkablashtirish" (input whitening) amali bajarilib, unda 128 bitli ochiq ma'lumot bloki 32 bitli qismlarga bo'linib, 4 ta 32 bitli qism kalitlarga (K_0, K_1, K_2, K_3) XOR amalida qo'shiladi. Hosil bo'lgan ma'lumot bloki esa, 16 raund davomida 32 ta qism kalitlar bilan shifrlanadi. 16-raunddan so'ng "chiqishdagi murakkablashtirish" (output whitening) amali bajariladi. Bunda, 16-raund natijasi 4 ta 32 bitli qismlarga ajratilib, 4 ta 32 bitli qism kalitlar (K_4, K_5, K_6, K_7) bilan XOR amalida qo'shiladi.



5.11-rasm. Twofish algoritmining shifrlash jarayoni sxemasi

g funksiya. *g* funksiya Twofish algoritmining asosi hisoblanadi. Ushbu funksiya kirishida 32 bitli maʼlumot X qabul qilinadi va u 4 baytga x_0, x_1, x_2, x_3 baytlarga ajratiladi. Har bir bayt oʻziga biriktirilgan S bloklardan (S bloklar statik emas, kalitga bogʻliq holda oʻzgaradi) oʻtkaziladi. S jadvaldan olingan 4 bayt vektor sifatida talqin qilinib, 4×4 oʻlchamli statik MDS (maximum distance separable) matritsaga $GF(2^8)$ maydonida $x^8 + x^6 + x^5 + x^3 + 1$ modul boʻyicha koʻpaytiriladi. Twofish algoritmidan foydalanilgan MDS matritsa quyida keltirilgan boʻlib, kirishda bir baytning oʻzgarishi chiqishdagi 4 baytning oʻzgarishini taʼminlaydi.

$$MDS = \begin{pmatrix} 01 & EF & 5B & 5B \\ 5B & EF & EF & 01 \\ EF & 5B & 01 & EF \\ EF & 01 & EF & 5B \end{pmatrix}$$

Adamar kriptoaqsantirishi. Ushbu akslantirish $2n$ uzunlikdagi bitlar qatorini qayta akslantirishni amalga oshiradi. Qator dastlab, n bitdan bo‘lgan ikkita a , b qismlarga ajratiladi. Akslantirish quyidagicha amalga oshiriladi:

$$\begin{aligned} a' &= a + b(\text{mod } 2^n); \\ b' &= a + 2b(\text{mod } 2^n). \end{aligned}$$

Mazkur akslantirish ko‘plab algoritmlarda foydalanilgan (masalan, SAFER) bo‘lib, Twofish algoritmi uchun $n = 32$ ga teng.

Siklik 1 bitga surish.k. Har bir raund uchun F funksiyaning natijasi o‘ng tomondagi ikki tashkil etuvchilar bilan XOR amalida qo‘shilgandan so‘ng (va oldin), qo‘shimcha tarzda bir bitga siklik siljtiladi. Xususan, uchinchi blok XOR amalidan so‘ng o‘nga bir bit, to‘rtinchi blok esa XOR amalidan oldin chapga bir bit siklik siljtiladi. Ushbu siljitishlar S jadvallar va MDS matritsaga xos bo‘lgan baytlar bo‘yicha nomutanosiblikni bartaraf etish uchun maxsus qo‘shilgan. Rasshifrovkalash jarayonida esa, siljitishlar qarama-qarshi yo‘nalishda amalga oshiriladi.

Raund kalitlari va S bloklarni generatsiyalash.k. Twofish algoritmidan $N=128$, $N=192$ va $N=256$ bitli kalitdan foydalanish mumkin. Kirish kalitining 256 bitdan kichik ixtiyoriy qiymatida 0 bilan to‘ldirilib, keyingi aniqlangan kalit uzunligiga yetkaziladi. Kiruvchi kalitdan 40 ta 32 bitli qism kalitlar generatsiya qilinadi: ularning dastlabki 8 tasi “kirishdagi murakkablashtirish” va “chiqishdagi murakkablashtirish” uchun, qolgan 32 tasi esa har bir raunda 2 tadan foydalaniladi. Twofish algoritmidan kiruvchi kalit nafaqat raund kalitlarini generatsiyalashda, balki S jadvallarni hosil qilishda ham ishlatiladi.

$k = N/64$ kabi belgilaylik. U holda M kirish kaliti $8k$ baytdan, m_0, \dots, m_{8k-1} , iborat bo‘ladi. Baytlar dastlab $2k$ ta 32 bitli so‘zlarga ajratiladi:

$$M_i = \sum_{j=0}^3 m_{(4i+j)} \cdot 2^{8j}, \quad i = 0, \dots, 2k - 1.$$

Shundan so‘ng ular, k uzunlikdagi ikkita vektorga ajratiladi:

$$\begin{aligned} M_e &= (M_0, M_2, \dots, M_{2k-2}); \\ M_o &= (M_1, M_3, \dots, M_{2k-1}). \end{aligned}$$

M_e va M_o asosida 40 ta qism kalitlar quyidagicha hosil qilinadi:

$$\begin{aligned} p &= 2^{24} + 2^{16} + 2^8 + 2^0; \\ A_i &= h(2ip, M_e); \\ B_i &= h((2i + 1)p, M_o) \lll 8; \\ K_{2i} &= (A_i + B_i) \bmod 2^{32}; \\ K_{2i+1} &= ((A_i + 2B_i) \bmod 2^{32}) \lll 9. \end{aligned}$$

Bu yerda, $i = 0, \dots, 19$ bo‘lib, umumiy 40 ta qism kalitlarni generatsiyalash imkonini beradi. $2ip$ – belgilanish esa, $2i$ qiymatni 4 marta takrorlanishini bildiradi, ya’ni, $2ip = 2i \parallel 2i \parallel 2i \parallel 2i$. h funksiyaning tavsifi esa quyida keltiriladi.

Uzunligi k ga teng S bloklarni generatsiyalash uchun kiruvchi kalitdan foydalaniladi. Buning uchun kiruvchi kalit uzunligi 8 ga teng baytdan tashkil topgan guruhlariga bo‘linadi. Masalan, 128 bitli kalit uchun birinchi guruh m_0, \dots, m_7 dan iborat bo‘lsa, ikkinchi guruh esa m_8, \dots, m_{15} elementlardan iborat bo‘ladi. Har bir guruh vektor shaklida ifodalanib, Reed Solomon kodida foydalanilgan 4×8 o‘lchamli matritsaga $GF(2^8)$ maydonida $x^8 + x^6 + x^3 + x^2 + 1$ modul bo‘yicha ko‘paytiriladi.

$$\begin{bmatrix} S_{i,0} \\ S_{i,1} \\ S_{i,2} \\ S_{i,3} \end{bmatrix} = \begin{bmatrix} 01 & A4 & 55 & 87 & 5A & 58 & DB & 9E \\ A4 & 56 & 82 & F3 & 1E & C6 & 68 & E5 \\ 02 & A1 & FC & C1 & 47 & AE & 3D & 19 \\ A4 & 55 & 87 & 5A & 58 & DB & 9E & 03 \end{bmatrix} \cdot \begin{bmatrix} m_{8i} \\ m_{8i+1} \\ m_{8i+2} \\ m_{8i+3} \\ m_{8i+4} \\ m_{8i+5} \\ m_{8i+6} \\ m_{8i+7} \end{bmatrix}$$

Bitta guruh uchun hosil qilingan $S_i = \sum_{j=0}^3 s_{i,j} \cdot 2^{8j}$ ga teng bo‘ladi. Shu tartibda, kalit uzunligiga bog‘liq holda S bloklar hosil qilinadi.

h funksiya. Raund kalitlarini hosil qilishda va g funksiyani shakllantirishda Twofish algoritmi $h(X, L_0, L_1, \dots, L_k)$ funksiyadan

foydalanilgan. Bu yerda, X, L_0, L_1, \dots, L_k larning har biri 32 bitdan iborat. Ushbu funksiya k bosqichda bajariladi. Ya'ni, 256 bitli kalit uchun 4 bosqichda, 192 bitli kalit uchun 3 bosqich va 128 bitli kalit uchun 2 bosqichda amalga oshiriladi (5.12-rasm).

Har bir bosqichda kiruvchi 32 bitli blok 4 baytga ajratilib, har bir bayt quyida keltirilgan q_0 va q_1 jadvallar asosida almashtiriladi.

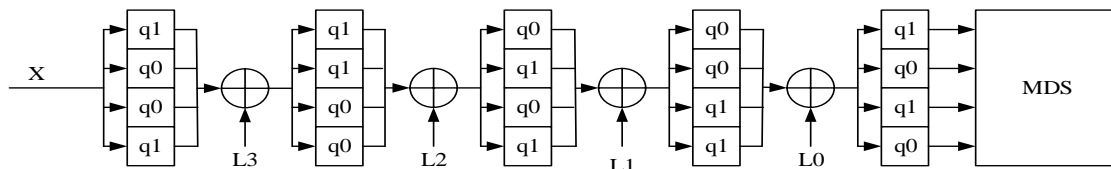
| q_0 | 0 | 1 | 2 | 3 | 4 | 5 | 6 | 7 | 8 | 9 | A | B | C | D | E | F |
|-------|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| t_0 | 8 | 1 | 7 | D | 6 | F | 3 | 2 | 0 | B | 5 | 9 | E | C | A | 4 |
| t_1 | E | C | B | 8 | 1 | 2 | 3 | 5 | F | 4 | A | 6 | 7 | 0 | 9 | D |
| t_2 | B | A | 5 | E | 6 | D | 9 | 0 | C | 8 | F | 3 | 2 | 4 | 7 | 1 |
| t_3 | D | 7 | F | 4 | 1 | 2 | 6 | E | 9 | B | 3 | 0 | 8 | 5 | C | A |

| q_1 | 0 | 1 | 2 | 3 | 4 | 5 | 6 | 7 | 8 | 9 | A | B | C | D | E | F |
|-------|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| t_0 | 2 | 8 | B | D | F | 7 | 6 | E | 3 | 1 | 9 | 4 | 0 | A | C | 5 |
| t_1 | 1 | E | 2 | B | 4 | C | 3 | 7 | 6 | D | A | 5 | F | 9 | 0 | 8 |
| t_2 | 4 | C | 7 | 5 | 1 | 6 | 9 | A | 0 | E | D | 8 | 2 | B | 3 | F |
| t_3 | 8 | 9 | 5 | 1 | C | 3 | D | E | 6 | 4 | 7 | F | 2 | 0 | 8 | A |

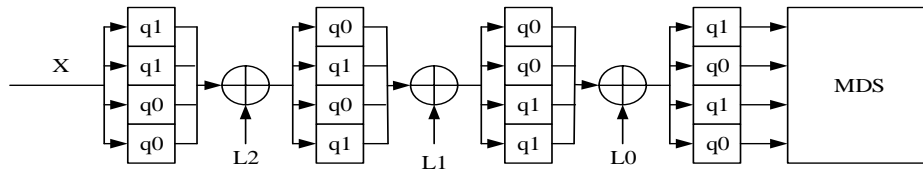
Buning uchun, kiruvchi bayt x ikkita 4 bitli $a_0 = \lfloor x/16 \rfloor$ va $b_0 = x \bmod 16$ qismlarga ajratiladi hamda ular ustida quyidagi amallar bajariladi:

$$\begin{aligned}
 a_1 &= a_0 \oplus b_0; \\
 b_1 &= a_0 \oplus (b_0 \ggg 4) \oplus ((8a_0) \bmod 16); \\
 a_2 &= t_0[a_1]; \\
 b_2 &= t_1[b_1]; \\
 a_3 &= a_2 \oplus b_2; \\
 b_3 &= a_1 \oplus (b_2 \ggg 2) \oplus ((8a_2) \bmod 16); \\
 a_4 &= t_2[a_3]; \\
 b_4 &= t_3[b_3]; \\
 y &= 16b_4 + a_4.
 \end{aligned}$$

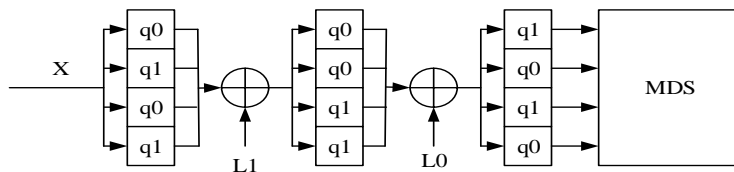
Shundan so'ng, y qiymatlar 4 baytli vektor sifatida akslantirilib, yuqorida keltirilgan MDS matritsaga ko'paytiriladi.



256 bitli kalit uchun, $k=4$



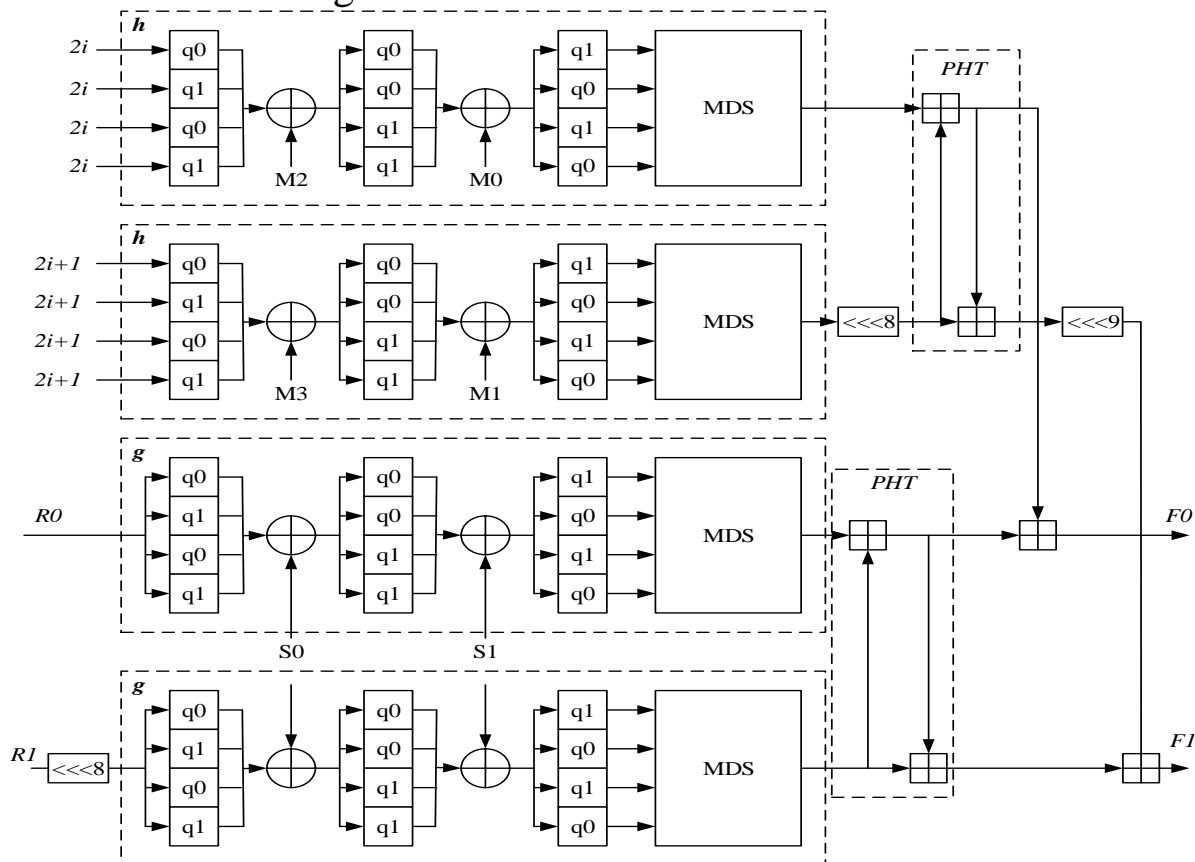
192 bitli kalit uchun, $k=3$



128 bitli kalit uchun, $k=2$

5.12-rasm. Turli kalit uzunliklari uchun h funksiyaning ko‘rinishi

Yuqorida keltirilgan akslantirishlardan kelib chiqib, Twofish algoritmda 128 bitli kalit asosida ma’lumotni shifrlashning bir raundi 5.13-rasmda keltirilgan.



5.13-rasm. Twofish algoritmda 128 bitli kalit asosida ma’lumotni shifrlashning bir raundi

Bu yerda, R_0, R_1 bloklar F raund funksiyasiga kiritiladi va mos F_0, F_1 qiymatlar olinadi.

5.8. Simmetrik blokli shifrlash rejimlari

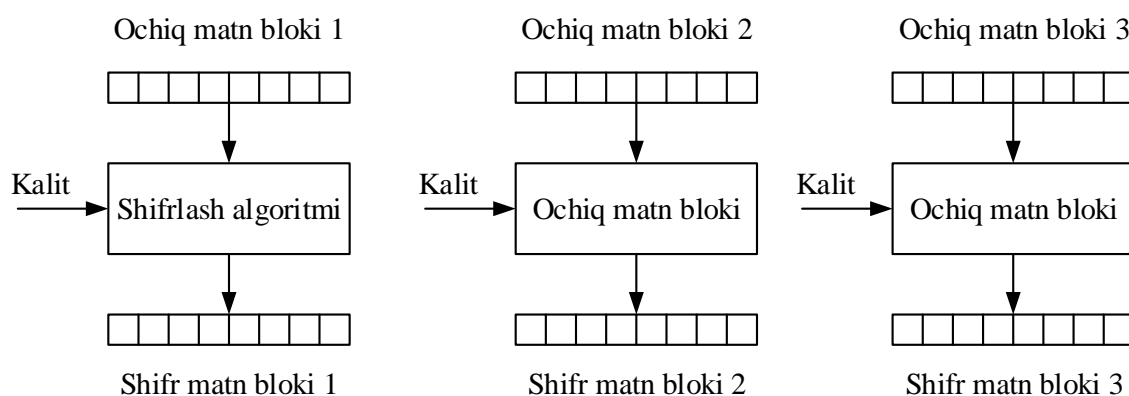
Oqimli shifrlardan foydalanish juda ham sodda – ochiq matn (yoki shifrmavn) uzunligiga teng bo‘lgan kalitlar ketma-ketligi generatsiya qilinadi va XOR amalida bajariladi. Blokli shifrlardan foydalanish faqat bir blokni shifrlashda oson. Biroq, bir nechta (ko‘plab) bloklarni shifrlash qanday amalga oshiriladi? Javob esa, bir qaraganda oson emas.

Shu sababli, simmetrik blokli shifrlardan turli ko‘rinishlarda (rejimlarda) foydalanishga harakat qilinadi. Aksariyat rejimlarda amalga boshlang‘ich vektor (initialization vector, IV) dan foydalaniladi. Boshlang‘ich vektor ma‘lum bitlar ketma-ketligidan iborat bo‘lib, ochiq matnga yoki kalitga ma‘lum algoritm bo‘yicha qo‘shiladi. Bu kattalik kalitdan farqli sanalib, odatda zarur bo‘lsa ham sir saqlanmaydi.

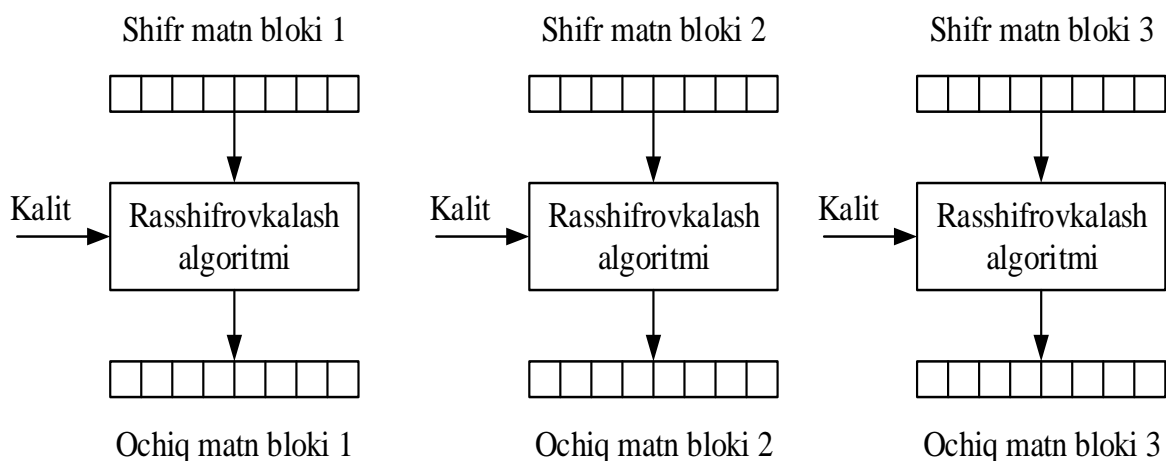
Hozirda quyidagi rejimlar keng qo‘llaniladi:

- elektronik codebook (ECB);
- cipher-block chaining (CBC);
- propagating cipher-block chaining (PCBC);
- cipher feedback (CFB);
- output feedback (OFB);
- counter (CTR).

Electronic codebook (ECB). Dastlabki sodda rejimlardan biri bo‘lib, ochiq matn bloklarga bo‘linadi va har bir blok ustida kalit bilan amallar bajariladi (5.14, 5.15-rasmlar).



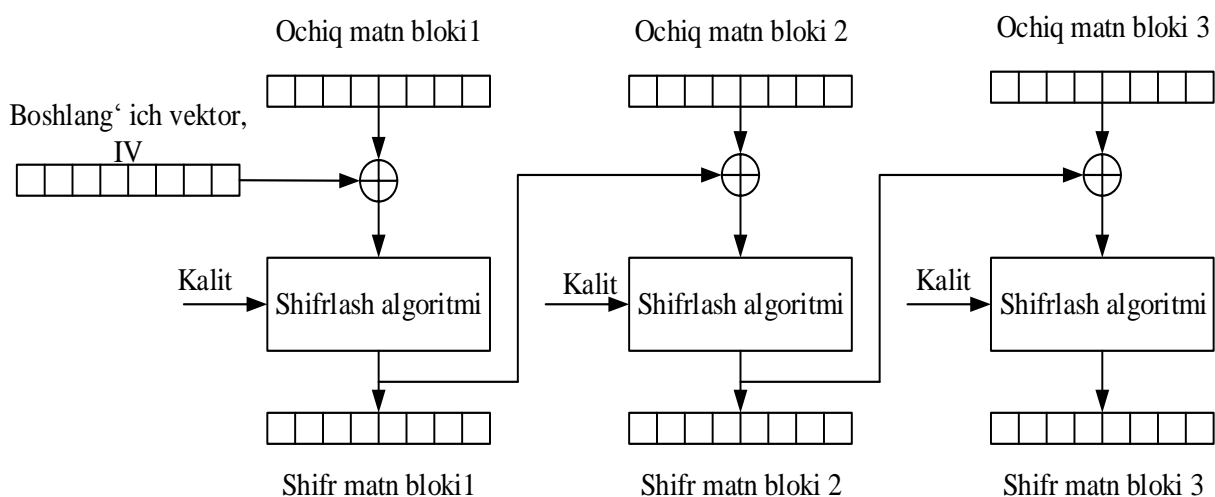
5.14-rasm. ECB rejimida shifrlash



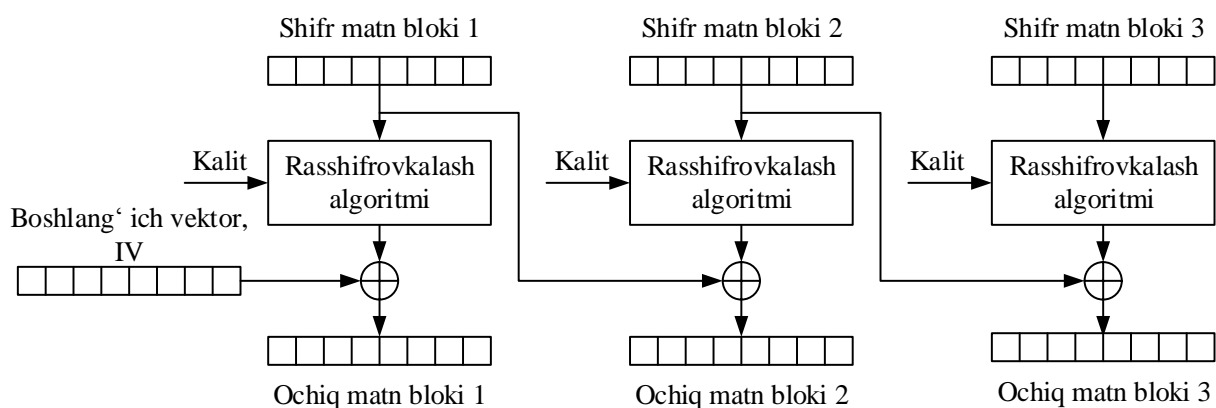
5.15-rasm. ECB rejimida rasshifrovkalash

Ushbu rejimning asosiy kamchiligi bir xil ochiq matn bir xil shifr matnga almashadi. Bundan tashqari, bu rejim matnni yashirish kabi vazifalarni bajarmaydi. Shularni hisobga olgan holda o‘ta maxfiy axborot bilan ishlashda ushbu rejimdan foydalanish tavsiya etilmaydi. Biroq, dasturiy ko‘rinishda parallel ravishda amalga oshirish imkoniyati mavjud.

Cipher-block chaining (CBC). Ushbu rejim 1976-yil IBM kompaniyasi tomonidan ishlab chiqilgan bo‘lib, dastlab ochiq matnga boshlang‘ich vektor qo‘shilib, natija kalit yordamida shifrlanadi (5.16, 5.17-rasmlar).



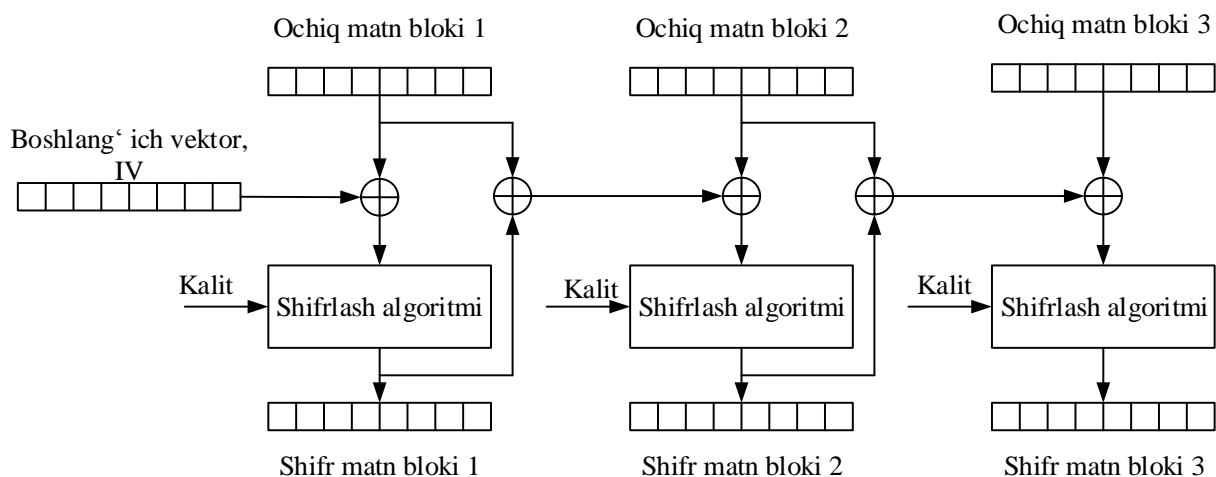
5.16-rasm. CBC rejimida shifrlash



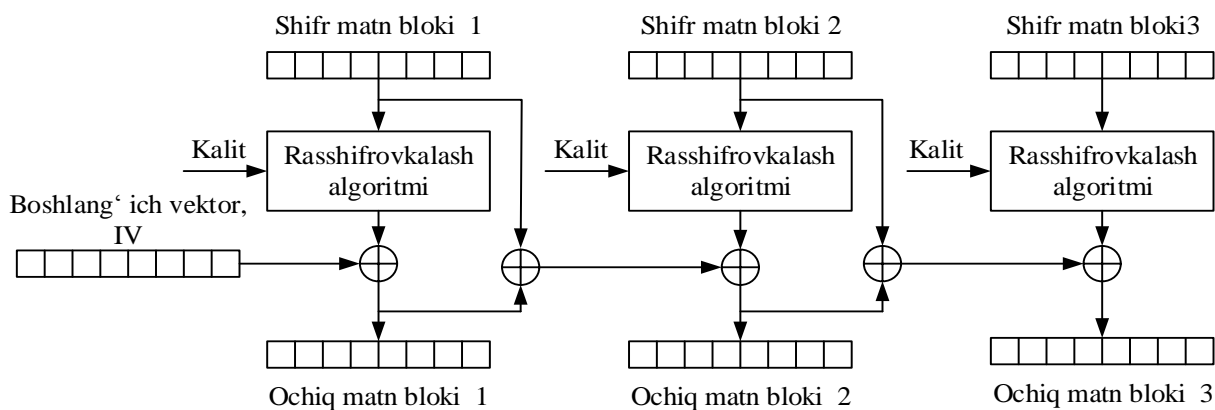
5.17-rasm. CBC rejimida rasshifrovkalash

Ushbu rejimda shifrlashda bir xil ma'lumot bloklari har xil shifratn bloklariga almashtiriladi. Bu esa shifratnnga qarab tahlil qilish usulini oldini olishga yordam beradi. Keyingi bosqich natijasi oldingi bosqich natijasiga bog'liq bo'lgani bois, algoritmni parallel tarzda amalga oshirish mumkin emas.

Propagating cipher-block chaining (PCBC). Ushbu rejim Kerberosv4 va WASTE protakollarida foydalanilgan bo'lsada, bardoshsizligi sababli amalda keng qo'llanilmaydi. Bundan tashqari, ushbu rejim parallel amalga oshirish imkoniyatini bermaydi (5.18, 1.19-rasmlar).

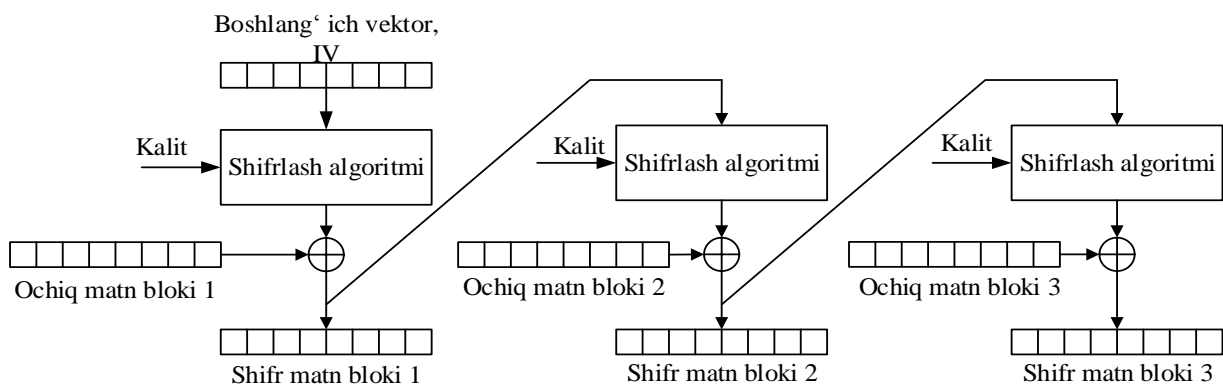


5.18-rasm. PCBC rejimida shifrlash

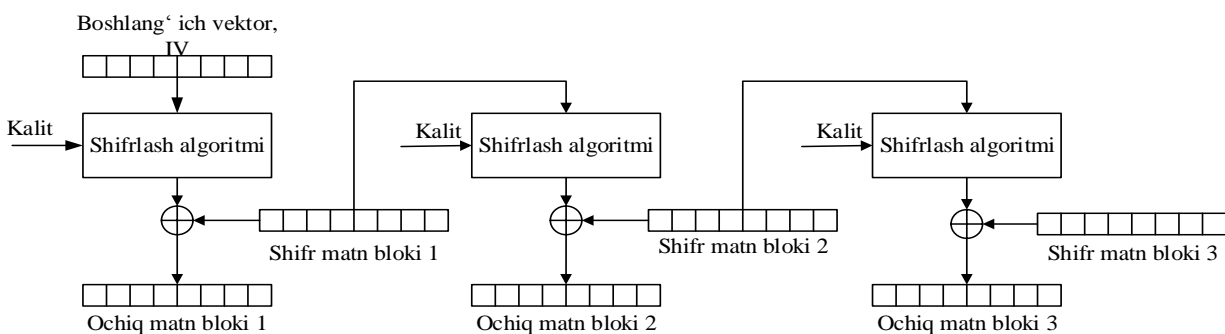


5.19-rasm. PCBC rejimida rasshifrovkalash

Cipher feedback (CFB). Ushbu rejim CBC rejimiga yaqin bo‘lib, ushbu modelda rasshifrovkalash CBC modelida shifrlash amaliga o‘xshaydi. Ushbu rejimda rasshifrovkalashda ham shifrlash amaldan foydalaniladi. Ushbu rejimni ham dasturiy tomondan parallel amalga oshirish imkoniyati mavjud emas (5.20, 5.21-rasmlar).

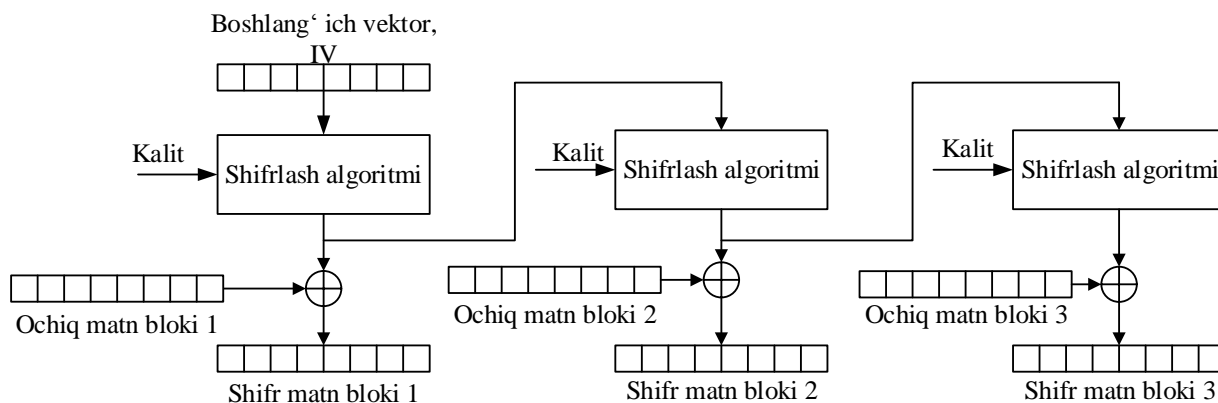


5.20-rasm. CFB rejimida shifrlash

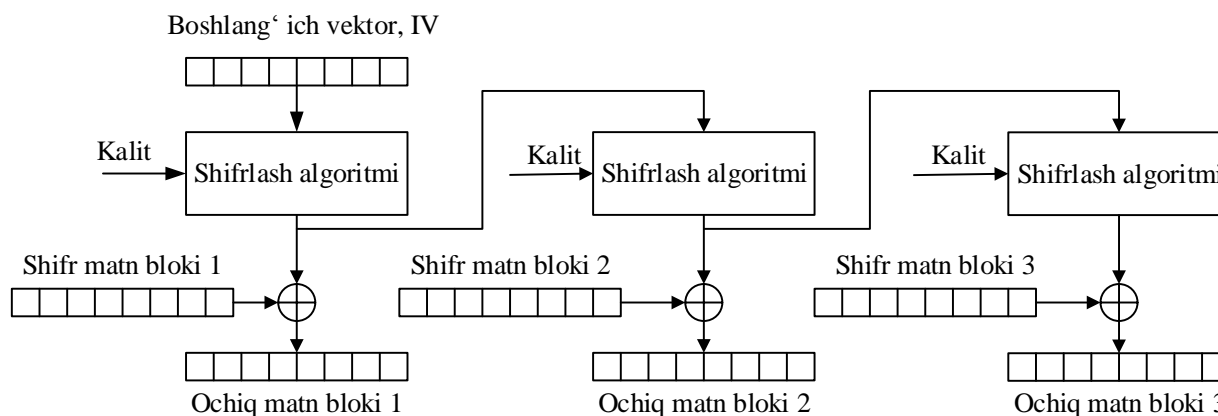


5.21-rasm. CFB rejimida rasshifrovkalash

Output feedback (OFB). Ushbu rejimda shifrlash amali sinxron oqimli shifrlash algoritmlarini qurishga imkon beradi. Ushbu rejimda shifrlashda keyingi blok oldingi blokga bog‘liq bo‘lganligi sababli, parallel ravishda amalga oshirish imkoniyati mavjud emas (5.22, 5.23-rasmlar).

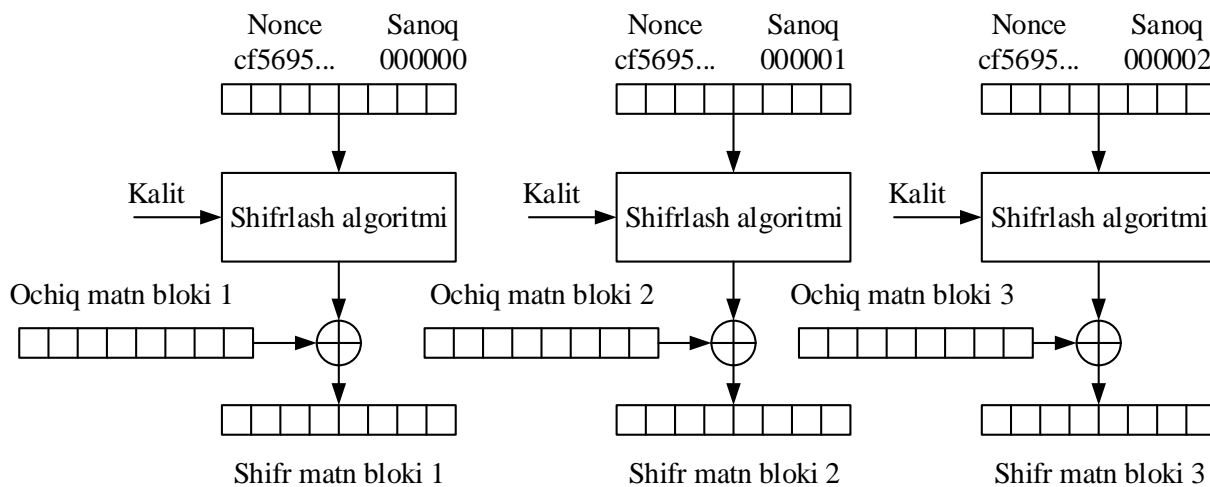


5.22-rasm. OFB rejimda shifrlash

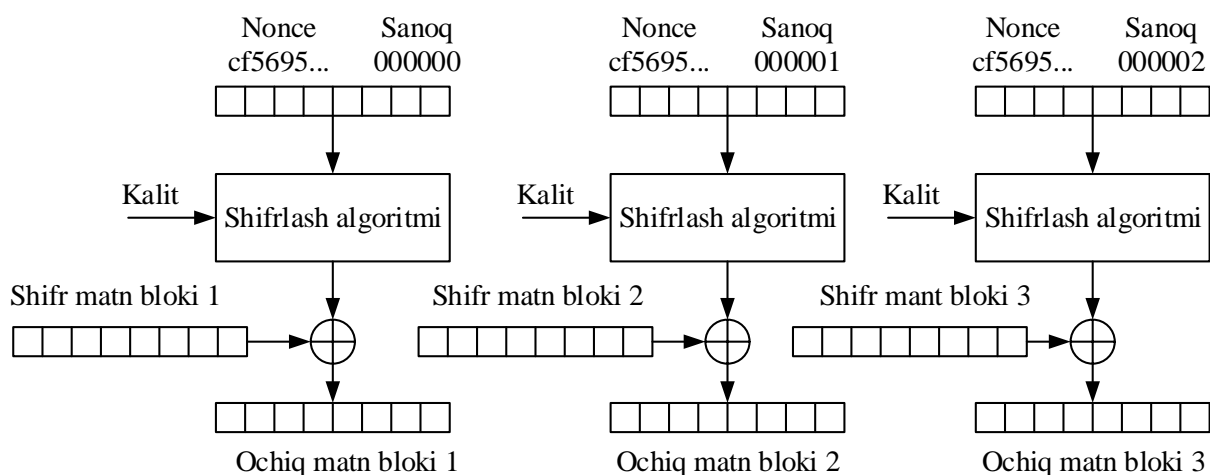


5.23-rasm. OFB rejimda rasshifrovkalash

Counter (CTR). OFB rejimi kabi ushbu rejimda ham oqimli shifrlashni amalga oshirish mumkin. Bunda keyingi kalit ketma-ketligi sanagich qiymatini shifrlash amali orqali amalga oshiriladi. Sanagich qiymati esa takrorlanmaydigan algoritm asosida hosil qilinadi. Ushbu usul amalda keng foydalanilib, kriptobardoshligi yuqori va parallel hisoblash imkonini beradi (5.24, 5.25-rasmlar).



5.24-rasm. CTR rejimida shifrlash



5.25-rasm. CTR rejimida rasshifrovkalash

Yuqoridagi rasmlardan ko‘rinib turibdiki, ba’zi shifrlash rejimlarida ham shifrlash ham rasshifrovkalash amallari birgalikda amalga oshirilsa, ba’zida faqat shifrlash amaldan foydalaniladi.

Navorat savollari

1. Simmetrik blokli shifrlarga oid asosiy tushunchalarni ayting.
2. Zamonaviy blokli shifrlash algoritmlari yaratilish asosiga ko‘ra qanday turlarga bo‘linadi.
3. Feystel tarmog‘i va uning xususiyatlari haqida gapiring.
4. SPN tarmoq va unda foydalanilgan akslantirishlar haqida ma’lumot bering.
5. Lai-Massey tarmog‘iga asoslangan shifrlarni o‘ziga xos xususiyatlarini ayting.
6. DES algoritmi va unda ma’lumotni shifrlash tartibini tushuntiring.
7. DES algoritmidan raund kalitlarini generatsiyalash tartibini ayting.
8. AES shifrlash algoritmi va uning matematik asosi haqida ayting.
9. AES shifrlash algoritmidan ma’lumotni shifrlash tartibini tushuntiring.
10. AES shifrlash algoritmidan raund kalitlarini generatsiyalash tartibini ayting.
11. GOST 28147-89 kriptotalgoritmi va unda foydalanilgan matematik amallar.

12. O'z Dst 1105:2009 simmetrik blokli shifrlash standarti va unda ma'lumotni shifrlash tartibi.
13. O'z Dst 1105:2009 simmetrik blokli shifrlash standartidagi Aralash() akslantirishini tushuntiring.
14. O'z Dst 1105:2009 simmetrik blokli shifrlash standartida raund kalitlarini generatsiyalash tartibini ayting.
15. IDEA simmetrik blokli shifrlash algoritmi va uning matematik asosi haqida ayting.
16. Twofish simmetrik blokli shifrlash algoritmi va uning matematik asosi.
17. Twofish simmetrik blokli shifrlash algoritmida raund kalitlari va S jadvallarni generatsiyalash tartibini tushuntiring.
18. Simmetrik blokli shifrlash rejimlari nima va ularning vazifasi.
19. CTR shifrlash rejimi va uning afzalliklari.
20. CBC shifrlash rejimi va uning afzalliklari.

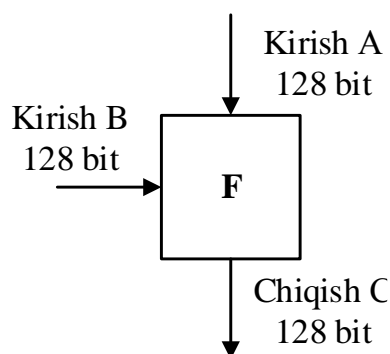
6 BOB. XESH FUNKSIYALAR VA MA'LUMOTNING YAXLITLIGI TA'MINLASH

6.1. Xesh funksiyalar va ularni qurish usullari

Xesh funksiya kirishdagi cheklanmagan uzunlikdagi ma'lumotni chiqishda qat'iy uzunlikdagi qiymatga akslantiruvchi funksiya. Kriptografik xesh funksiyaga quyidagi talablar qo'yiladi:

1. Ixtiyoriy uzunlikdagi matnga qo'llash.k.
2. Chiqishda tayinlangan uzunlikdagi qiymatni qaytarish.k.
3. Berilgan ixtiyoriy x bo'yicha $h(x)$ oson hisoblanishi.
4. Berilgan ixtiyoriy H bo'yicha $h(x) = N$ tenglikdan x ni hisoblab topib bo'lmaslik (bir tomonlilik xossasi).
5. Olingan x va $y \neq x$ matnlar uchun $h(x) \neq h(y)$ bajarilishi (kolliziyaga bardoshlilik xossasi).

Siqish funksiyasi. Xesh funksiyalarning asosiy xususiyatlaridan biri bu – siqish imkoniyati bo'lib, kriptografiyada bu – fiksirlangan ikkita kiruvchi bloklarni, chiqishda bitta fiksirlangan blokga aylantirib beruvchi bir tomonlama funksiyaga aytiladi (6.1-rasm).



6.1 – rasm. Bir tomonlama siqish funksiyasi

Bir tomonlama siqish funksiyalarni ishlab chiqishda ba'zida mavjud kriptografik algoritmlardan foydalanilsa, ba'zida biror matematik muammodan kelib chiqqan holda yondashiladi. Quyida keng tarqalgan bir tomonlama siqish funksiyalarini yaratish usullari keltirilgan:

1. Blokli shifrlarga asoslangan:
 - a) bitta blok uzunligiga siqish:
 - Davies-Meyer (Davies-Meyer);
 - Matias-Meyer-Oseas (Matyas-Meyer-Oseas);
 - Miaguchi-Prinel (Miyaguchi-Preneel).
 - b) ikkita blok uzunligiga siqish:

- MDC-2;
 - MDC-4;
 - Hirose.
2. Oqimli shifrlarga asoslangan;
 3. Maxsus siqishga asoslangan;
 4. Modul arifmetikasiga asoslangan.

Xesh funksiyalarga qaratilgan hujumlar. Xesh funksiyalarni xavfsizlik xususiyatlarini tahlil qilganda odatda *haqiqiy* ma'lumotni topish, *ikkilamchi haqiqiy* ma'lumotni topish va *kolliziyani* topishga qaratiladi. Agar haqiqiy ma'lumotni topish, ikkilamchi haqiqiy ma'lumotni topish va kolliziyani topish uchun mos ravishda 2^n , 2^n va $2^{n/2}$ dan kam bo'lgan urinishlar soni talab etilsa, bu xesh funksiya ko'rsatilgan turdagi hujumlarga bardoshsiz deb qaraladi. Xesh funksiyalarga qaratilgan hujumlarni maqsadiga ko'ra quyidagicha ifodalash mumkin (6.1 - jadval).

6.1 – jadval

Xesh funksiyalarga qaratilgan hujumlarning maqsad va uni amalga oshirish uchun hujumchi imkoniyatlari

| Hujum | Berilgan imkoniyat | Hujumdan maqsad |
|--------------------|---------------------------|--|
| Haqiqiy | $H(M)$ | M ni topish |
| Ikkilamchi haqiqiy | $M \& H(M)$ | $M' \neq M$ va $H(M') \neq H(M)$ ni topish |
| Kolliziya | - | $M' \neq M$ va $H(M') \neq H(M)$ ni topish |

Tug'ilgan kun hujumi. Ushbu hujum kolliziyani topishga qaratilgan bo'lib, *tug'ilgan kun muammosi* yoki *tug'ilgan kun paradoksiga* asoslanadi. Bu muammo minimal sondagi odamlar orasida kamida ikkita odamning tug'ilgan kunining bir xil bo'lish ehtimoli $\frac{1}{2}$ dan katta bo'lishi haqida bo'lib, buni xesh funksiyalarga qo'llaganda bir tug'ilgan kunga ega bo'lgan ikkita insonning mavjudligini bildiradi.

Ushbu hujumda hujumchi maxsus kolliziyani topishdan ko'ra ixtiyoriy kolliziyani topishga harakat qiladi. Agar hujumchi N ta odamlar orasidan biror maxsus kolliziyani, ya'ni bir odamning tug'ilgan kuni bilan bir xil bo'lgan kuni topayotgan bo'lsa, u holda bu ehtimol quyidagiga teng bo'ladi:

$$P_{kolliziya}(N) = 1 - \left(\frac{364}{365}\right)^N$$

Bu ehtimollik $\frac{1}{2}$ dan katta bo'lishi uchun N qiymat 254 dan katta bo'lishi talab etiladi. Ushbu g'oyani xesh funksiyaga tadbiiq etilsa, biror xabar va uning xesh qiymati berilganda xesh qiymatlari teng bo'lgan turli ma'lumotni topish masalasi qaraladi.

Biroq hujumchidan N tug'ilgan kunlar orasida ixtiyoriy kolliziyani topish ehtimoli quyidagiga teng bo'ladi:

$$P_{kolliziya}(N) = 1 - \left(\frac{365}{365}\right) \left(\frac{364}{365}\right) \left(\frac{363}{365}\right) \dots \left(\frac{365 - N + 1}{365}\right)$$

Ushbu holda ehtimollik $\frac{1}{2}$ dan katta bo'lishi uchun $N=23$ imkoniyatning o'zi yetarli bo'ladi.

Agar hujumchi n bitli xesh qiymat chiqaruvchi xesh funksiya uchun $\frac{1}{2}$ dan ko'p bo'lgan ehtimollik bilan ixtiyoriy kolliziyani topishi $2^{n/2}$ ga teng bo'ladi.

Agar xesh funksiya uchun xesh qiymatning uzunligi n bitga teng bo'lsa va u p ehtimollik bilan aniqlanishi uchun kerak bo'lgan hisoblashlar soni N ga teng bo'lsa, ular orasidagi bog'liqlikning mental ko'rinishi quyidagiga teng bo'ladi:

$$N \approx \sqrt{2 * 2^n * p}.$$

Xesh funksiyalarni qurish usullari. Yuqorida keltirilgan siqish usullari asosida turli konstruksiyalardan foydalanilgan holda xesh funksiyalarni qurish amalga oshiriladi. Takroriy xeshlashga asoslangan funksiyalar hozirda keng tarqalgan usullardan biri bo'lib, xesh funksiyalarni qurishda keng foydalaniladi. Quyida keng tarqalgan xesh funksiyalarni qurish usullari keltirilgan.

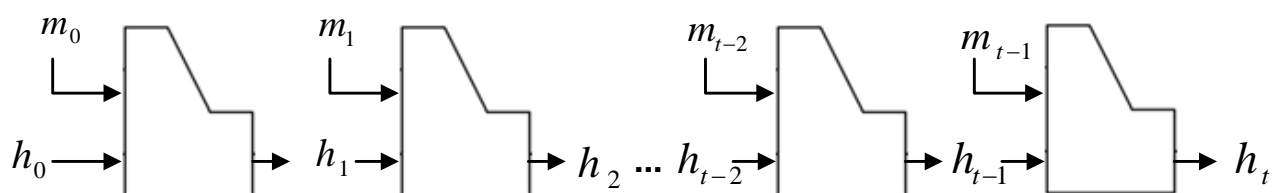
Merkle-Damgard (MD) usuli. Ushbu usul xesh funksiyalarni qurishda eng keng tarqalgan usul sanalib, 1989-yilda R.Merkl va I.Damgard tomonidan ishlab chiqilgan. Ushbu usul odatda uchta qadamdan iborat bo'ladi. Birinchi qadamda ma'lumotga qo'shimcha ma'lumot qo'shish orqali uni teng bloklarga ajratish.k. Bunda keng tarqalgan to'ldirish usuli bu – bitta bir va qolganlarini nol bilan to'ldirishdir. Ikkinchi bosqich bu – kiritilgan ma'lumot bloki m ni qism

bloklarga m_0, m_1, \dots, m_n ajratishdir. Shundan so‘ng ochiq tanlab olingan boshlang‘ich vektor va qism bloklardan foydalangan holda takroriy fiksirlangan qiymatlar hisoblanadi.

$$h_0 = IV,$$

$$h_i = f(h_{i-1}, m_{i-1}) \quad i = 1, 2, \dots, t.$$

Bu yerda, f -siqish funksiyasi. Ushbu konstruksiyaning umumiy ko‘rinish quyidagi 6.2 – rasmda keltirilgan.



6.2 – rasm. Merkle – Damgard konstruktori

Sxemaning zaif tomonlari:

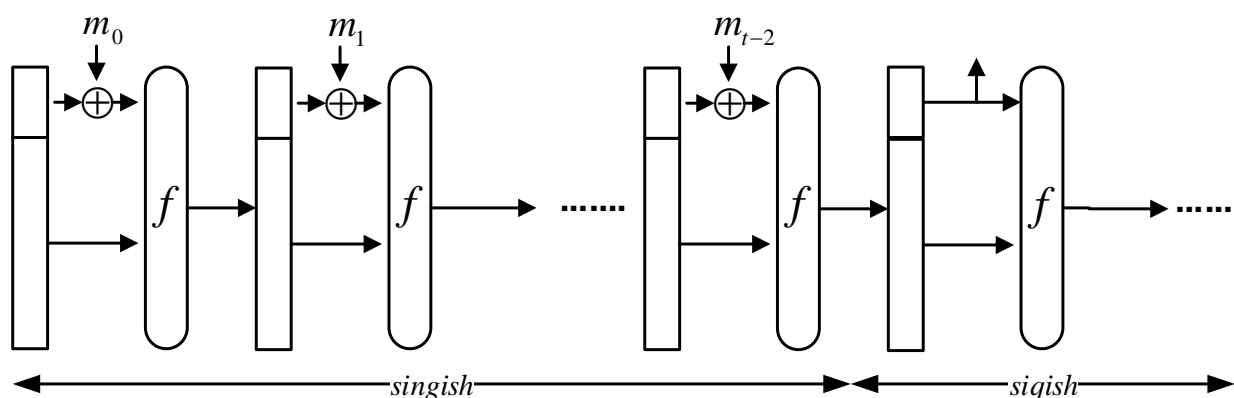
1. Ma‘lumotni kerakli uzunlikkacha to‘ldirish.k. Ya‘ni, agar kriptanalitik bitta kolliziya topsa, boshqalarini ham topish oson.
2. Xesh qiymatni beruvchi ikkinchi bir ma‘lumotni (ikkinchi haqiqiyini) topish uzun ma‘lumotlar uchun “to‘liq tanlash hujumiga”ga nisbatan effektiv hisoblanadi.
3. Ma‘lumotni to‘ldirishga qaratilgan hujum, ya‘ni, X ma‘lumotning xesh qiymati $H(X)$ ma‘lum bo‘lganida $H(pad(X)||Y)$ ning qiymatini topish oson bo‘ladi. Bu yerda, pad -to‘ldirish funksiyasi bo‘lib, u X ga bog‘liq bo‘lgan ma‘lumotning xesh qiymatini topish imkonini beradi.

HAIFA usuli. Merkle-Damgard usuli kolliziyaga bardoshli sanalib, yildan yil hisoblash qurilmalarining imkoniyatlari ortishi natijasida ko‘plab hujumlarga zaif bo‘lib bormoqda. Ushbu usuldagi kamchiliklar Biham va Dunkelmannlar tomonidan tuzatilib, yangi *HAIFA (HAsH Iterative FrAmework)* usulini taklif etilgan. HAIFA ham Merkle-Damgard usuli kabi takroriy sanalib, qo‘shimcha ravishda xavfsizlikni oshirish uchun vosita kiritilgan.

MD usulida siqish funksiyasida kiruvchi qiymat sifatida h_i va m_i qiymatlar olinsa, HAIFAda esa ularga qo‘shimcha ravishda b va s kattaliklar ham kiritiladi va umumiy ko‘rinish quyidagicha bo‘ladi: $h_i = f(h_{i-1}, m_{i-1}, b, s)$ ga teng bo‘ladi.

Sponge(gubka) usuli. Ushbu funksiya xesh funksiya va oqimli shifrlarni yaratish uchun yangi usul sanalib, u tasodifiy almashtirish yoki tasodifiy funksiyaga asoslanadi. Agar f funksiya tasodifiy almashtirish kabi tasvirlansa, unda P – *sponge*, aks holda T – *sponge* deb ataladi. Sponge usulida siqish va qolgan usullardagi siqish usullarining farqi, unda kirishdagi l bit qiymat chiqishda ham l bit shaklda ifodalanadi.

Ushbu usul ikkita bosqichdan iborat: *singish (absorbing)* va *siqish (squeezing)*. Birinchi bosqich takroriy holda bloklar ustida amalga oshiriladi. Bunda xabar bloki holat bilan takroriy holda XOR amalida qo‘shiladi. Ushbu amal barcha bloklar ustida amalga oshirilgandan so‘ng ikkinchi bosqich amalga oshiriladi. Bu bosqichda ba‘zi qiymatlar chiqariladi va kutilgan xesh qiymat olingunga qadar f funksiya qo‘llaniladi (6.3-rasm).



6.3 – rasm. **Sponge konstrukturi**

Bulardan tashqari, xesh funksiyalarni qurishda *keng kanalli va ikki kanalli (Wide Pipe and Double Pipe)*, *erkin old qo‘shiluvchili Merkle-Damgard (Prefix-Free Merkle-Damgård)*, *qobiqli Merkle-Damgard (Enveloped Merkle-Damgård)*, *RMX, 3C va 3C-X, dinamik xesh funksiya* konstruksiyalaridan keng foydalanilmoqda.

Xesh-funksiyalar ikki muhim turga, *kalitli* va *kalitsiz* xesh-funksiyalarga bo‘linadi. Kalitli xesh-funksiyalar simmetrik kriptotizimlarda foydalaniladi. Ularni ma‘lumotni autentifikatsiyalash kodlari deb ham atashadi. Ular bir-biriga ishonuvchi tomonlar uchun qo‘shimcha vositalarsiz manbaning haqiqiyliги va ma‘lumotning yaxlitligini kafolatlaydi. Kalitsiz xesh-funksiyalar xatolarni aniqlash kodlari deb ham yuritiladi. Kalitsiz xesh-funksiyalar qo‘shimcha vositalarsiz ma‘lumotning yaxlitligini kafolatlaydi. Bu xesh-funksiyalar bir-biriga ishonuvchi hamda bir-biriga ishonmaydigan tomonlar orasida

ishlatiladi. Odatda kalitsiz xesh-funksiyalar quyidagi xossalarni qanoatlantirishi shart:

- bir tomonlamalik;
- kolliziyaga bardoshlilik;
- xesh qiymatlari teng bo'lgan ikkita ma'lumotni topishga bardoshlilik.

Keng foydalaniluvchi xesh-funksiyalar sifatida MD5, SHA1, SHA2, SHA3, GOST R 34.11-94, O'z DSt 1106 : 2006 algoritmlarini misol keltirish mumkin.

6.2. MD5 xesh funksiyasi

MD5 xesh-funksiyasi kalitsiz xesh-funksiyalar turkumiga tegishli bo'lib, Massachusetts texnologiyalar instituti professori R.Rivest tomonidan 1992-yilda taqdim qilingan. MD5 xesh-funksiyasida xeshlanuvchi ma'lumot uzunligi ixtiyoriy bo'lib, xesh qiymat uzunligi 128 bit uzunlikda bo'ladi. MD5 xesh-funksiyasida xeshlanuvchi ma'lumot 512 bitlik bloklarga ajratiladi. Ular esa o'z o'rnida 16 ta 32 bitli qism bloklarga ajratiladi va ular ustida amallar bajariladi.

Masalan, uzunligi b bit bo'lgan (bu yerda, b ixtiyoriy manfiy bo'lmagan butun son) ma'lumot berilgan va bu ma'lumotning bitlari $m_0m_1 \dots m_{b-1}$ tartibda yozilgan. Xesh qiymatni hisoblash uchun quyidagi beshta bosqich bajariladi:

1-bochqich.k. To'ldirish bitlarini qo'shish.k.

Berilgan ma'lumot uzunligi L , 512 modul bo'yicha 448 bilan taqqoslanadigan ($L \equiv 448 \pmod{512}$) ko'rinishda to'ldiriladi, ya'ni, kengaytirilgan ma'lumotning uzunligi unga eng yaqin bo'lgan 512 ga karrali bo'lgan sonidan 64 bitga kichik bo'lishi kerak. To'ldirish bosqichi, hamma vaqt xattoki ma'lumot uzunligi 512 modul bo'yicha 448 bilan taqqoslanadigan bo'lsa ham bajariladi. To'ldirish quyidagi tartibda amalga oshiriladi: ma'lumotga qiymati 1 ga teng bo'lgan bitta bit qo'shiladi, qolgan bitlar esa 0 lar bilan to'ldiriladi. Shuning uchun qo'shilgan bitlar soni 1 dan 512 tagacha bo'ladi.

Masalan, xabar M ="message" ga teng bo'lsin. U holda xabarning ASCIIIdagi ko'rinishi quyidagicha bo'ladi:

01101101 01100101 01110011 01110011 01100001 01100111 01100101

Xabar uzunligi $L = 56$ ga tengligi bois, qo‘shiluvchi bitlar sonini 392 ga tengligini ko‘rish mumkin: $(56 + 392) \bmod 512 = 448$. Shu sababli, birinchi bosqich natijasi quyidagicha bo‘ladi:

```

01101101 01100101 01110011 01110011 01100001 01100111 01100101
10000000 00000000 00000000 00000000 00000000 00000000 00000000
00000000 00000000 00000000 00000000 00000000 00000000 00000000
00000000 00000000 00000000 00000000 00000000 00000000 00000000
00000000 00000000 00000000 00000000 00000000 00000000 00000000
00000000 00000000 00000000 00000000 00000000 00000000 00000000
00000000 00000000 00000000 00000000 00000000 00000000 00000000

```

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

1-bosqichning natijasiga berilgan ma’lumot uzunligining 64 bitlik qiymati qo‘shiladi. Agar ma’lumotning uzunligi 2^{64} bitdan katta bo‘lsa, uzunlik $\bmod 2^{64}$ bo‘yicha qo‘shiladi. Shunday qilib, birinchi ikkita bosqich bajarilgandan keyin uzunligi 512 bitga karrali bo‘lgan ma’lumot olinadi, ya’ni, kengaytirilgan ma’lumot uzunligi 16 ta 32 bitlik so‘zdan iborat blok uzunligiga karrali bo‘ladi. Natijada, hosil qilingan ma’lumot so‘zlarini $M[0, \dots, N - 1]$ orqali belgilaymiz. U holda N soni 16 ga karrali bo‘ladi. Shunday qilib, $N = T \times 16$ bo‘ladi.

Yuqoridagi misolda $L = 56$ bo‘lgani bois, uning 64 bitli razryaddagi ko‘rinishi quyidagicha bo‘ladi:

```

00000000 00000000 00000000 00000000 00000000 00000000 00000000
00111000

```

3-bosqich.k. Xesh qiymat uchun bufer initsializatsiya qilish.k.

Xesh funksiyaning oraliq va oxirgi natijalarini saqlash uchun 128 bitli buferdan foydalaniladi. Bu buferni to‘rtta 32 bitli A, B, C, D registrlar ko‘rinishida tasvirlash mumkin. Bu registrlarga 16 lik sanoq sistemasidagi quyidagi boshlang‘ich qiymatlar beriladi:

```

A = 0x01234567;
B = 0x89ABCDEF;
C = 0xFEDCBA98;
D = 0x76543210.

```

4-bosqich.k. 512 bitli ma’lumotni 32 bitlik bloklarga ajratib qayta ishlash.k.

MD5 algoritmidagi argumenti va qiymati 32 bitli soʻz boʻladigan toʻrtta funksiyadan foydalanilgan:

$$F(X, Y, Z) = (X \wedge Y) \vee (\neg X \wedge Z)$$

$$G(X, Y, Z) = (X \wedge Z) \vee (Y \wedge \neg Z)$$

$$H(X, Y, Z) = X \oplus Y \oplus Z$$

$$I(X, Y, Z) = Y \oplus (X \vee \neg Z)$$

Bu yerda, bitlar boʻyicha mantiqiy *AND*, *OR*, *NOT*, *XOR* amallari mos ravishda \wedge , \vee , \neg , \oplus belgilari bilan ifodalangan.

Shundan soʻng, 64 ta 32 bitli soʻzdan iborat $K[0, \dots, 63]$ massiv sinus funksiyasi asosida quyidagicha hosil qilinadi:

$$K[i] = [2^{32} \times \text{abs}(\sin(i))].$$

Bu yerda, $0 \leq i \leq 63$ ga teng. Ushbu tenglik natijasi quyida keltirilgan:

| | | | | | |
|-------------|----|---------------|--------------|-------------|-------------|
| $K[0..3]$ | := | {0xd76aa478, | 0xe8c7b756, | 0x242070db, | 0xc1bdceee} |
| $K[4..7]$ | := | {0xf57c0faf, | 0x4787c62a, | 0xa8304613, | 0xfd469501} |
| $K[8..11]$ | := | {0x698098d8, | 0x8b44f7af, | 0xffff5bb1, | 0x895cd7be} |
| $K[12..15]$ | := | {0x6b901122, | 0xfd987193, | 0xa679438e, | 0x49b40821} |
| $K[16..19]$ | := | {0xf61e2562, | 0xc040b340, | 0x265e5a51, | 0xe9b6c7aa} |
| $K[20..23]$ | := | {0xd62f105d, | 0x02441453, | 0xd8a1e681, | 0xe7d3fbc8} |
| $K[24..27]$ | := | {0x21e1cde6, | 0xc33707d6, | 0xf4d50d87, | 0x455a14ed} |
| $K[28..31]$ | := | {0xa9e3e905, | 0xfcefa3f8, | 0x676f02d9, | 0x8d2a4c8a} |
| $K[32..35]$ | := | {0xffffa3942, | 0x8771f681, | 0x6d9d6122, | 0xfde5380c} |
| $K[36..39]$ | := | {0xa4beea44, | 0x4bdecfa9, | 0xf6bb4b60, | 0xbebfb7c0} |
| $K[40..43]$ | := | {0x289b7ec6, | 0xeeaa127fa, | 0xd4ef3085, | 0x04881d05} |
| $K[44..47]$ | := | {0xd9d4d039, | 0xe6db99e5, | 0x1fa27cf8, | 0xc4ac5665} |
| $K[48..51]$ | := | {0xf4292244, | 0x432aff97, | 0xab9423a7, | 0xfc93a039} |
| $K[52..55]$ | := | {0x655b59c3, | 0x8f0ccc92, | 0xffeff47d, | 0x85845dd1} |
| $K[56..59]$ | := | {0x6fa87e4f, | 0xfe2ce6e0, | 0xa3014314, | 0x4e0811a1} |
| $K[60..63]$ | := | {0xf7537e82, | 0xbd3af235, | 0x2ad7d2bb, | 0xeb86d391} |

Bundan tashqari, 64 ta elementdan iborat s massivdan foydalanilib, u siljitishlar sonini ifodalaydi:

$$s[0..15] := \{7, 12, 17, 22, 7, 12, 17, 22, 7, 12, 17, 22, 7, 12, 17, 22\}$$

$$s[16..31] := \{5, 9, 14, 20, 5, 9, 14, 20, 5, 9, 14, 20, 5, 9, 14, 20\}$$

$s[32..47] := \{4, 11, 16, 23, 4, 11, 16, 23, 4, 11, 16, 23, 4, 11, 16, 23\}$
 $s[48..63] := \{6, 10, 15, 21, 6, 10, 15, 21, 6, 10, 15, 21, 6, 10, 15, 21\}$

MD5 xesh funksiyasida 64 raund davomida har bir 512 bitli blok ustida quyidagi amallar bajariladi:

4.1. 512 bitli blok M 16 ta 32 bitli qismlarga ajratiladi: $M[j]$, $0 \leq j \leq 15$.

4.2. Quyidagilar o'zlashtiriladi:

$a = A;$

$b = B;$

$c = C;$

$d = D.$

4.3. 64 raund quyidagichasi bajariladi:

```

for i from 0 to 63 do:
if 0 ≤ i ≤ 15 then:
    f = F(b, c, d);
    g = i;
if 16 ≤ i ≤ 31 then:
    f = G(b, c, d);
    g = (5 × i + 1) mod 16;
if 32 ≤ i ≤ 47 then:
    f = H(b, c, d);
    g = (3 × i + 5) mod 16;
if 48 ≤ i ≤ 63 then:
    f = I(b, c, d);
    g = (7 × i) mod 16;
    f = (f + a + K[i] + M[g]) mod 232;
A = D;
D = C;
C = B;
B = (B + leftrotate(f, s[i])) mod 232;
end for
A = (A + a) mod 232;
B = (B + b) mod 232;
C = (C + c) mod 232;
D = (D + d) mod 232.

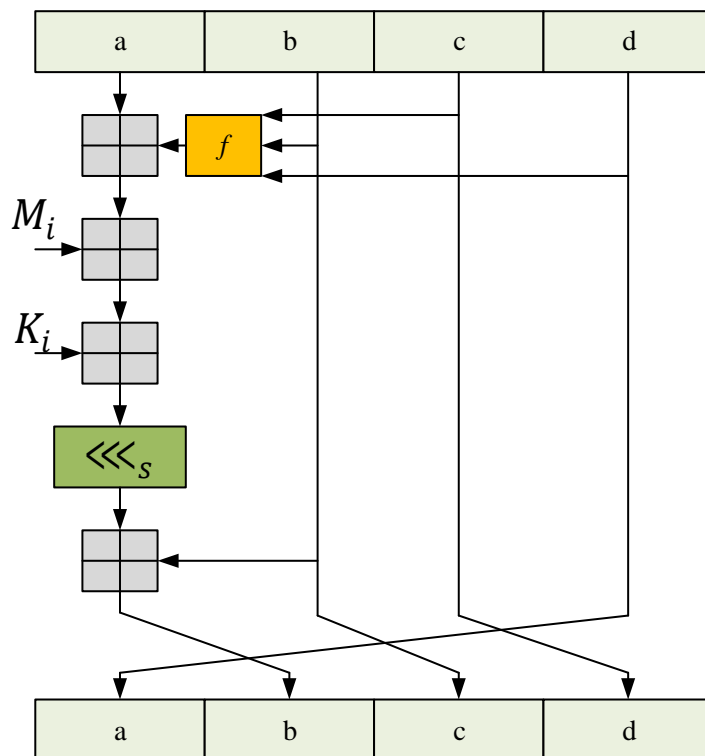
```

4.4. Barcha ma'lumot bloklari uchun 4.1 va 4.2-bosqichlar bajarilib bo'linganidan so'ng, yakuniy xesh qiymat quyidagicha hosil qilinadi:

$$h = A \parallel B \parallel C \parallel D.$$

Bu yerda, $\text{leftrotate}(x, c) = (x \ll c) \vee (x \gg (32 - c))$ ga teng.

Umumiy holda MD5 xesh funksiyasi bir raundining akslantirilishi 6.4-rasmda keltirilgan.



6.4-rasm. MD5 algoritmining *i*-raundi

MD5 funksiyasida kolliziya hodisasi aniqlangan bo'lib, quyida ushbu ikki bir-biridan farq qiluvchi ma'lumotlar keltirilgan.

M_1 :

d131dd02c5e6eec4 693d9a0698aff95c 2fcab58712467eab 4004583eb8fb7f89
 55ad340609f4b302 83e488832571415a 085125e8f7cdc99f d91dbdf280373c5b
 d8823e3156348f5b ae6dacd436c919c6 dd53e2b487da03fd 02396306d248cda0
 e99f33420f577ee8 ce54b67080a80d1e c69821bcb6a88393 96f9652b6ff72a70

M_2 :

d131dd02c5e6eec4 693d9a0698aff95c 2fcab50712467eab 4004583eb8fb7f89
 55ad340609f4b302 83e4888325f1415a 085125e8f7cdc99f d91dbd7280373c5b
 d8823e3156348f5b ae6dacd436c919c6 dd53e23487da03fd 02396306d248cda0
 e99f33420f577ee8 ce54b67080280d1e c69821bcb6a88393 96f965ab6ff72a70

Ushbu ikki ma'lumotning xesh qiymati "79054025255fb1a26e4bc422aef54eb4" ga teng. Shu sababli, yuqori darajadagi xavfsizlik talab etilgan tizimlarda ushbu algoritmdan foydalanish tavsiya etilmaydi.

6.3. SHA1 xesh funksiyasi

SHA (Secure Hash Algorithm) xeshlash algoritmi AQShning standartlar va texnologiyalar Milliy instituti (NIST) tomonidan ishlab chiqilgan bo'lib, 1992-yilda axborotni qayta ishlash federal standarti (PUB FIPS 180) sifatida nashr qilingan. Ushbu standart 1995-yilda qaytadan ko'rib chiqilib, SHA-1 deb nomlandi (PUB FIPS 180-1). SHA1 algoritmi MD4 algoritmiga asoslangan. Ushbu algoritm DSS (Digital Signature Standard) standartida elektron raqamli imzo algoritmlarini shakllantirishda foydalanish uchun mo'ljallangan.

SHA1 algoritmidagi kiruvchi ma'lumotning uzunligi 2^{64} bitdan kichik bo'lib, xesh qiymat uzunligi 160 bitga teng. Kiritilayotgan ma'lumot 512 bitli bloklarga ajratilib qayta ishlanadi.

Xesh qiymatni hisoblash jarayoni quyidagi bosqichlardan iborat:

1-bosqich.k. To'ldirish bitlarini qo'shish.k. Mazkur bosqich MD5 algoritmidagi kabi amalga oshiriladi.

2- bosqich.k. Ma'lumotning uzunligini qo'shish.k. Ushbu bosqich ham MD5 algoritmidagi keltirilgani kabi amalga oshiriladi.

3- bosqich.k. Xesh qiymat uchun bufer initsializatsiya qilish.k.

SHA1 algoritmidagi oraliq va oxirgi natijalarini saqlash uchun 160 bitli buferdan foydalanilgan. Ushbu bufer beshta 32 bitli A, B, C, D, E registrlardan tashkil topgan. Ushbu registrlarning 16 lik sanoq tizimidagi boshlang'ich qiymatlari quyida berilgan:

$$A = 0x67452301;$$

$$B = 0xEFCDAB89;$$

$$C = 0x98BADCFE;$$

$$D = 0x10325476;$$

$$E = 0xC3D2E1F0.$$

Keyinchalik ushbu o'zgaruvchilar mos ravishda yangi a, b, c, d va e o'zgaruvchilarga o'zlashtiriladi.

4- bosqich.k. Ma'lumotni 512 bitli bloklarga ajratib qayta ishlash.k.

SHA1 algoritmda har bir 512 bitli blok ustida 80 raund davomida qayta ishlash amalga oshiriladi. Ushbu algoritmda quyidagi o‘zgarmlar va funksiyalardan foydalanilgan:

Barcha raundlar uchun 32 bitli K_t o‘zgarmlar qiymatlari:

$$K_t = \begin{cases} 0x5A827999, & 0 \leq t \leq 19 \\ 0x6ED9EBA1, & 20 \leq t \leq 39 \\ 0x8F1BBCDC, & 40 \leq t \leq 59 \\ 0xCA62C1D6, & 60 \leq t \leq 79 \end{cases}$$

$f_t(x, y, z)$ esa raundlar bo‘yicha quyidagicha ifodalanadi:

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

512 bitli blok (M) 16 ta 32 bitli qismlarga ajratiladi va undan 80 ta raund uchun W_t quyidagicha hosil qilinadi:

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

SHA1 xesh funksiyasining asosiy sikli esa quyidagicha:

```
for t from 0 to 79 do:
temp = ((a <<< 5) + f_t(b, c, d) + e + W_t + K_t) mod 232;
e = d; d = c; c = b <<< 30; b = a; a = temp;
end for
```

Asosiy sikl tugagandan keyin a, b, c, d va e larning qiymatlari mos ravishda A, B, C, D va E registrlardagi qiymatlariga qo‘shiladi va ma’lumotning keyingi 512 bitli blokini qayta ishlashga o‘tiladi.

```
A = (A + a) mod 232;
B = (B + b) mod 232;
C = (C + c) mod 232;
D = (D + d) mod 232;
```

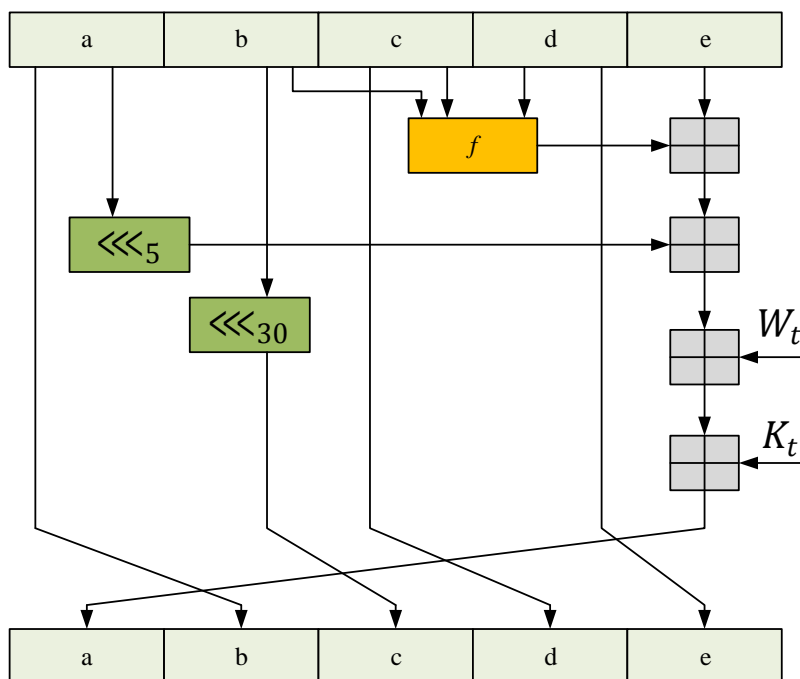
$$E = (E + e) \bmod 2^{32}.$$

5- bosqich.k. Yakuniy xesh qiymatni hosil qilish.k.

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

$$h = A \parallel B \parallel C \parallel D \parallel E.$$

6.5-rasmda SHA1 xesh funksiyasi algoritmining i -raund ko'rinishi keltirilgan.



6.5-rasm. SHA1 algoritmining i -raundi

MD5 algoritmi kabi, SHA1 algoritmi uchun ham kolliziya holati aniqlangan. 2017 yilda Google tashkiloti va CWI (Centrum Wiskunde & Informatica) markazi mutaxassislari tomonidan bir xil xesh qiymatni beruvchi ikkita turli PDF formatidagi fayllar generatsiya qilingan.

6.4. O'z DSt 1106 : 2006 xesh funksiyasi

Ushbu standart ikkita algoritmdan iborat ular 1-algoritm va 2-algoritm deb nomlangan. 1-algoritm kirish ketma-ketligining uzunligi 128 yoki 256 bitga karrali bo'lib, chiqish ketma-ketligi va xeshlash kaliti qayd etilgan 128 yoki 256 bit uzunlikka ega.

Birinchi algoritm parametrli algebraga muammosiga asoslangan bo'lsa, ikkinchi algoritm GOST 28147-89 blokli shifrlash algoritmiga asoslangan. Ushbu standartda quyidagi belgilanishlar va sozlanmalar mavjud:

O'z DSt 1106:2009 – birinchi algoritm. Ushbu algoritmning tavsifi quyida keltirilgan. Birinchi algoritm uchun quyidagi belgilanishlar qabul qilingan:

M - dastlabki ma'lumot (xabar);

h – xesh funksiya;

m – xesh funksiya qiymati, bunda $m = h(M)$;

k - xeshlash kaliti;

k_e - 4×8 tartibli ikki o'lchamli massiv ko'rinishidagi bosqich kaliti;

$holat$ - 4×8 tartibli ikki o'lchamli massiv ko'rinishidagi xeshlashning oraliq natijasi;

$holatn$ - 4×8 tartibli ikki o'lchamli massiv ko'rinishidagi kirish bloki;

r - modul, bunda $p \in \{16, 256\}$;

e - xeshlash protsedurasining bosqichlar soni;

b - dastlabki ma'lumotlardagi bloklar soni;

\oplus - XOR amalining simvoli (2-modul bo'yicha qo'shish amallari);

\otimes - diamatritsalarini r moduli bo'yicha ko'paytirish amalining simvoli;

\otimes_r - parametr bilan r moduli bo'yicha ko'paytirish amalining simvoli;

$^{-1}$ - r moduli bo'yicha teskarilash amalining simvoli;

\setminus^{-1} – parametr bilan r moduli bo'yicha teskarilash amalining simvoli;

\setminus^x - parametr bilan r moduli bo'yicha x darajaga ko'tarish amalining simvoli;

XF - xeshlash funksiyasi;

NY - nazorat summasi;

|| - konkatenatsiya simvoli.

XFda quyidagi parametr va funksiyalar foydalaniladi:

a) k – yarim bayt (bayt) darajasidagi chiziqli massivi ko'rinishidagi 128 yoki 256 bit uzunlikdagi xeshlash kaliti;

b) k_e - 4×8 tartibdagi ikki o'lchamli massiv ko'rinishidagi bosqich (raund) kaliti;

c) b – dastlabki ma'lumotlardagi bloklar soni;

d) *uzunlik* – dastlabki ma'lumotlarning bitlardagi uzunligini o'z ichiga oluvchi xeshlash funksiyasiga kiruvchi ma'lumotlarning oxirigidan oldingi bloki;

e) *NY* - o'nlik sanoq tizimida dastlabki ma'lumotlar qiymatlari summasini o'z ichiga oluvchi xeshlash funksiyasiga kiruvchi ma'lumotlarning oxirgi bloki;

f) *r* - modul, $r \in \{16, 256\}$;

g) $e_0 - 128$ va (256) bitli kirish bloklari uchun $(b + 2)10$ ga teng bo'lgan xeshlash protsedurasida bosqichlarining umumiy soni;

h) *Qo'sh (holat, holatn)* - *holat* massivi va *holatn* massivi joriy qiymatlarining yarim bayt (bayt) darajasidagi elementlari ustida *p* moduli bo'yicha (*A*, *B*, *R*) parametri bilan darajaga ko'tarish amali asosida xeshlash protsedurasida foydalaniladigan o'zgartirish;

i) *BaytZichlash (holat, holatn)* - *holat* massivi va *holatn* massivi joriy qiymatlarining yarim bayt (bayt) darajasidagi elementlari ustida, agar modul $p=16$ bo'lsa, *XOR* amalidan foydalanilgan holda yoki agar modul $p=256$ bo'lsa, bitta massivga zichlash chiziqli massivi asosida xeshlash protsedurasida foydalaniladigan o'zgartirish;

j) *Aralash(holat, k_e)* – diamatritsalarini ko'paytirish amali asosida xeshlash protsedurasida foydalaniladigan o'zgartirish. Bu yerda ko'paytiriladigan diamatritsalar, mos ravishda, *holat* va k_e bosqich kaliti ikki o'lchamli massivlarining kvadrat shaklidagi chap va o'ng yarimlariga o'zaro mos keladi;

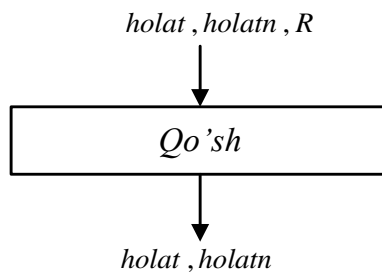
k) *SurHolat(holat)* - *holat* massivi ustida amalga oshiriladigan, xeshlash protsedurasida foydalaniladigan o'zgartirish, bu *holat* massivining barcha to'rtta satrini gorizontaal va vertikal bo'yicha surilishlarning turli qiymatlariga davriy surishlardan iborat;

l) *SurKalit(k_e)* - k_e massivi ustida amalga oshiriladigan xeshlash protsedurasida foydalaniladigan o'zgartirish, bu k_e massivining barcha to'rtta satrini gorizontaal va vertikal bo'yicha surilishlarning turli qiymatlariga davriy surishlardan iborat;

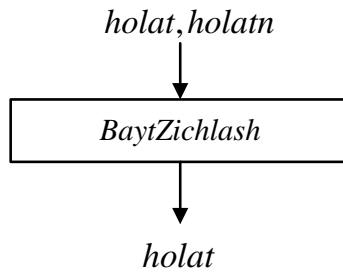
m) *TuzilmaKalit(k_e, k)* - xeshlash protsedurasining har bir bosqichi so'ngida foydalaniladigan o'zgartirish, bu uning strukturasi dastlabki xeshlash kaliti *k* strukturasi keltirish maqsadida k_e massivining har bir yarim bayti (bayti) ustida amalga oshiriladi; ushbu o'zgartirish natijasi k_e massivining kvadrat qismlaridan har birini teskarilash shartlarini qanoatlantiradi.

Keltirilgan almashtirishlarning umumiy ko'rinishi quyidagicha:

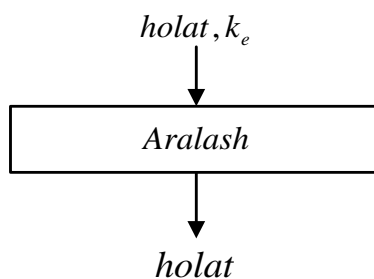
1. *Qo'sh(holat, holatn, R) o'zgartirish*



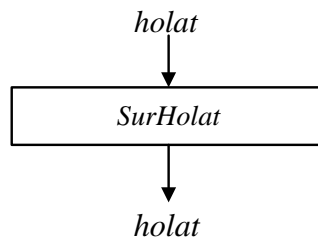
2. *BaytZichlash(holat, holatn) o'zgartirishi*



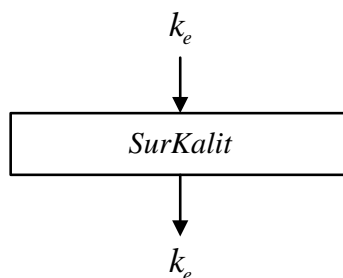
3. *Aralash(holat, k_e) o'zgartirishi*



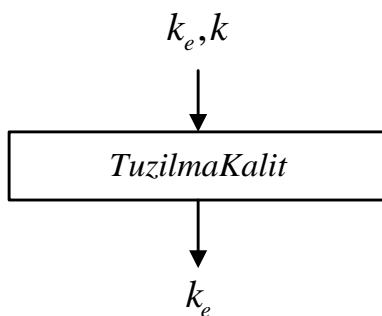
4. *SurHolat(holat) o'zgartirishi*



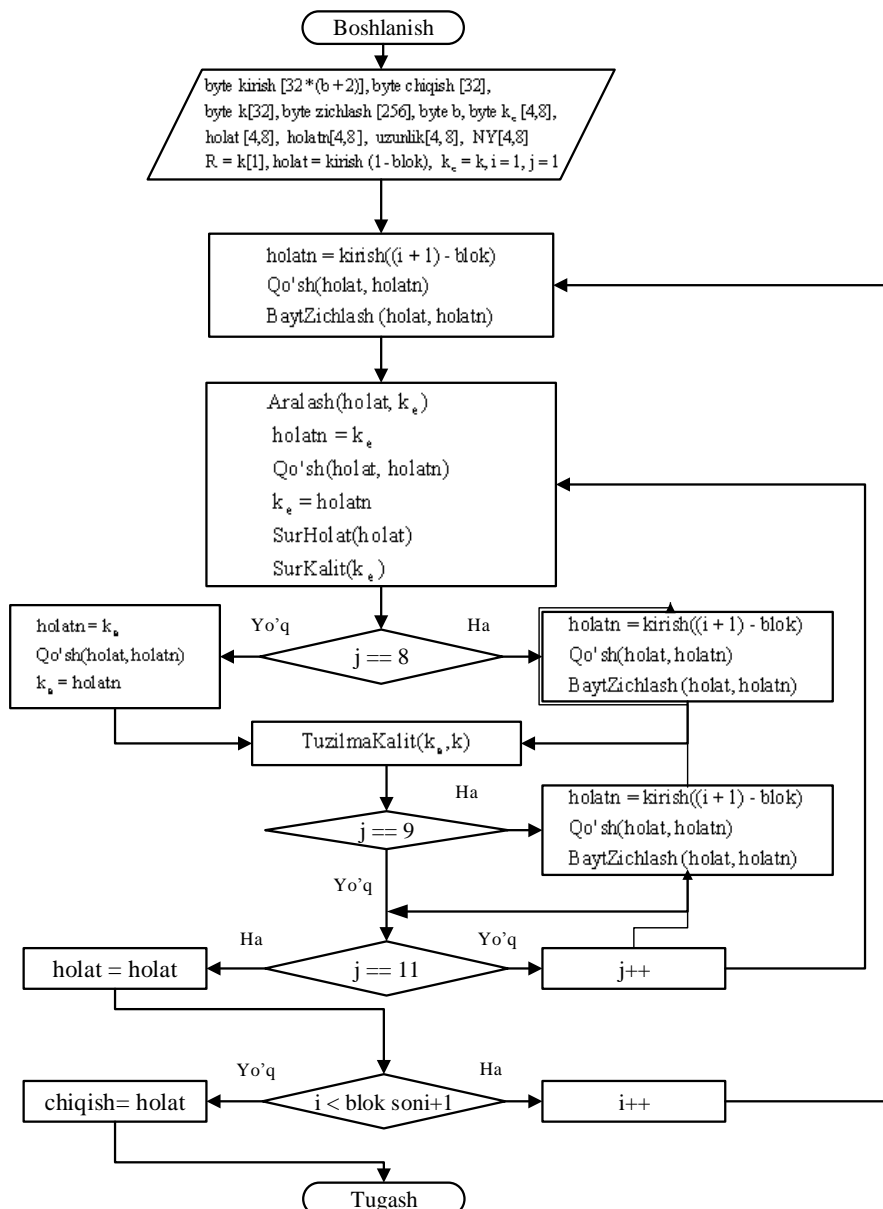
5. *SurKalit(k_e) o'zgartirishi*



6. *TuzilmaKalit(k_e, k) o'zgartirishi*



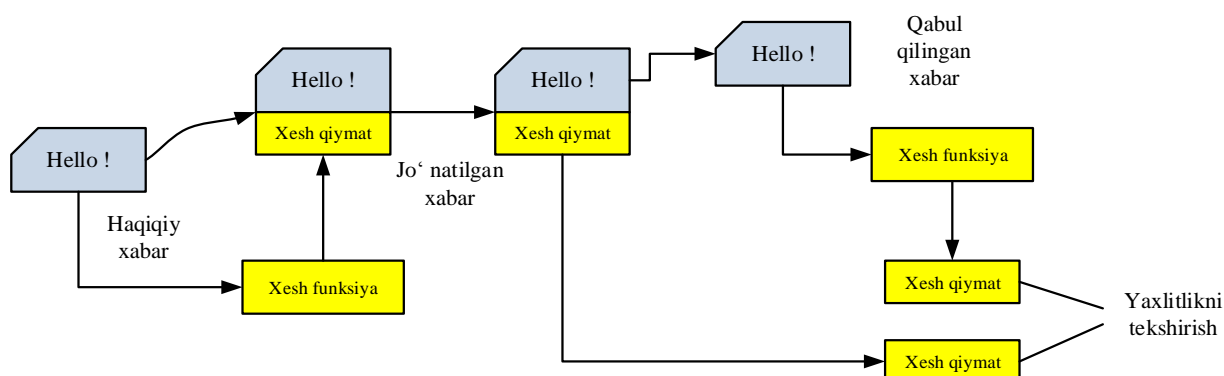
Keltirilgan akslantirishlar asosida O‘z DSt 1106:2009 standartining birinchi algoritmining blok sxemasi 6.6-rasmda keltirilgan.



6.6-rasm. O‘z DSt 1106:2009 standarti 1-algoritmining blok-sxemasi

6.5. Ma'lumotlarni autentifikatsiyalash kodlari. HMAC algoritmi

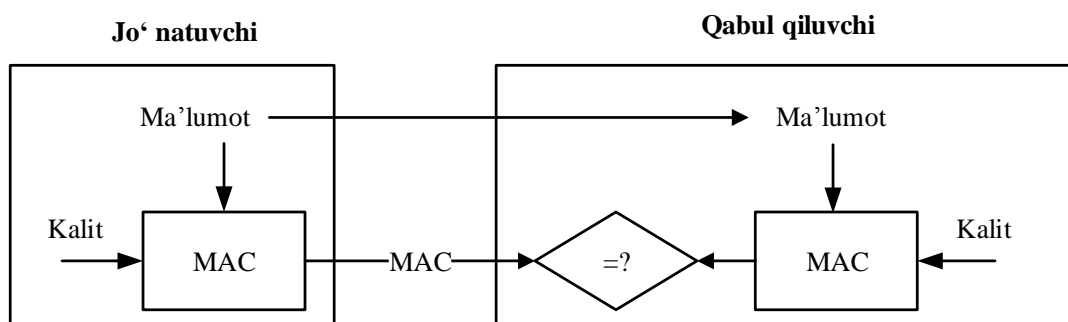
Xesh funksiya yordamida uzatilayotgan ma'lumotlar yaxlitligini tekshirishning sodda ko'rinishi 6.7-rasmda keltirilgan. Jo'natuvchi xabarning xesh qiymatini hisoblaydi va uni qabul qiluvchiga xabar bilan birgalikda yuboradi. Qabul qiluvchi dastlab xabarning xesh qiymatini hisoblaydi va qabul qilingan xesh qiymat bilan taqqoslaydi. Agar har ikkala xesh qiymat teng bo'lsa, ma'lumotning yaxlitligi o'zgarmagan, aks holda o'zgargan deb topiladi. Odatda xesh funksiya kirishda ma'lumotdan tashqari hech qanday qiymatni talab etmagani bois, *kalitsiz kriptografik funksiyalar* deb ham ataladi (kalit talab qiluvchi ma'lumotlarning yaxlitligini ta'minlash usullari ham mavjud).



6.7-rasm. Xesh funksiya asosida ma'lumotlar yaxlitligini tekshirish

Yuqorida keltirilgan usulda xavfsizlik muammosi jiddiy bo'lgani bois, undan amalda foydalanilmaydi. Ya'ni, hujumchi tomonidan faqat ma'lumot o'zgartirilgan holda yaxlitlikni tekshirish imkoniyati mavjud. Biroq, hujumchi ma'lumotning xesh qiymatini almashtirish orqali foydalanuvchini osonlik bilan ma'lumot yaxlitligiga ishontirishi mumkin. Buning asosiy sababi, ma'lumotning xesh qiymatini hosil qilishda hujumchiga noma'lum biror axborotdan foydalanilmaganligi.

Ushbu muammoni bartaraf etuvchi – *xabarlarni autentifikatsiyalash kodi (message authentication code, MAC)* tizimlari mavjud bo'lib, unga ko'ra biror maxfiy kalit asosida ma'lumotning xesh qiymati hisoblanadi (6.8-rasm).



6.8-rasm. MAC tizimi

MAC tizimlarini ishlab chiqishda blokli shifrlardan ham foydalanish mumkin. Buning uchun blokli shifrni CBC (Cipher Block Chaining – shifr bloklar zanjiri) rejimida foydalanish va eng oxirgi shifratn blokini olishning o‘zi yetarli (qolganlari tashlab yuboriladi). Ushbu oxirgi shifratn bloki *MAC* sifatida xizmat qiladi. Mazkur holda N blokdan iborat bo‘lgan ma’lumot bloklari, $P_0, P_1, P_2, \dots, P_{N-1}$ uchun *MAC* quyidagi formula orqali hisoblanadi:

$$C_0 = E(P_0 \oplus IV, K), C_1 = E(P_1 \oplus C_0, K), \dots, C_{N-1} = E(P_{N-1} \oplus C_{N-2}, K) = MAC.$$

Buning uchun har ikkala tomonda IV va K ni bo‘lishining o‘zi yetarli.

Faraz qilaylik, A va B tomonlardan uzatilayotgan ma’lumotlar yaxlitligini tekshirish talab etilgan bo‘lsin (bu yerda ma’lumot konfidensialligini ta’minlash masalasi qaralmagan). Bu holda A va B tomonlar orasida xavfsiz taqsimlangan K kalit yordamida A tomon *MAC* ni hisoblaydi va ma’lumotni IV ga qo‘shib B ga uzatadi. B tomon ma’lumot, K va IV yordamida *MAC* ni hisoblaydi. Agar hisoblangan *MAC* qabul qilingan *MAC'* ga teng bo‘lsa, ma’lumot o‘zgartirilmagan aks holda o‘zgartirilgan deb topiladi.

Qanday qilib, ikkita hisoblangan *MAC* qiymatlar turlicha bo‘lishi mumkin? Faraz qilaylik, A tomon quyidagilarni B ga yuborgan bo‘lsin:

$$IV, P_0, P_1, P_2, P_3, MAC.$$

Faraz qilaylik, hujumchi birinchi blok P_1 ni o‘zgartirdi (u Q deb belgilansin), bu holda B tomon *MAC* ni quyidagicha hisoblaydi:

$$C_0 = E(P_0 \oplus IV, K), \hat{C}_1 = E(Q \oplus C_0, K), \hat{C}_2 = E(P_2 \oplus \hat{C}_1, K), \hat{C}_3 = E(P_3 \oplus \hat{C}_2, K) = \text{"MAC"} \neq MAC.$$

Ya'ni, ochiq matndagi bir blokning o'zgarishi keyingi barcha bloklarga ta'sir qiladi va buning natijasida shifratn bloklari turlicha bo'ladi. Ma'lumki, CBC rejimida shifratndagi bir blok o'zgarishi rasshifrovkalanganda faqat 2 ta ochiq matn blokiga ta'sir qiladi. Biroq, ochiq matnning bir blokini o'zgarishi undan keyingi barcha shifratn bloklariga ta'sir qiladi va bu MAC tizimlari uchun juda muhim.

Albatta, mazkur usul MAC tizimlarini yaratishning yagona usuli emas. Quyida xesh funksiyalar asosida MAC tizimlarini yaratish bilan tanishib chiqiladi.

Xesh – funksiyalar asosida ma'lumot yaxlitligini tekshirish.k. Yuqorida M ma'lumot yaxlitligini tekshirishda $h(M)$ ni hisoblash va qabul qiluvchiga $M, h(M)$ ni yuborish orqali amalga oshirishning kamchiligi haqida aytib o'tilgan edi. Shuning uchun, amalda xesh funksiyalardan ma'lumot yaxlitligini ta'minlashda bevosita foydalanilmaydi. Boshqacha aytganda, xesh funksiyalar asosida ma'lumot yaxlitligini ta'minlashda hisoblangan xesh qiymatni o'zgartira olmaslikni kafolatlash zarur. Buni amalga oshirish uchun balki xesh qiymatni simmetrik kalitli shifrlar asosida shifrlash zarurdir (ya'ni, $E(h(M), K)$). Biroq, buni amalga oshirishning soddaroq usuli – *xeshlangan MAC* (hashed MAC yoki HMAC) usuli mavjud. Bu usulga ko'ra, xesh qiymatni shifrlashning o'rniga, xesh qiymatni hisoblash jarayonida kalitni bevosita ma'lumotga biriktirish amalga oshiriladi. HMAC tizimida kalitlar qanday biriktiriladi? Umumiy holda ikki usul: kalitni matnni oldidan qo'yish ($h(K, M)$) yoki kalitni matndan keyin qo'yish ($h(M, K)$) mavjud bo'lsada, ularning har ikkalasida jiddiy xavfsizlik muammosi mavjud.

Xesh funksiyalar ham simmetrik kriptotizim hisoblanadi va simmetrik blokli shifrlash kabi ma'lumotlarni xeshlashda bloklarga ajratiladi. Odatda aksariyat xesh funksiyalar uchun (masalan, MD5, SHA1, Tiger) blok uzunligi 64 baytga yoki 512 bitga teng.

HMAC tizimida kalit ma'lumotga quyidagicha biriktiriladi. Dastlab xesh funksiyadagi blokning uzunligi baytlarda aniqlanadi. Masalan. MD5 xesh funksiyasida blok uzunligi $B = 64$ baytga teng bo'lsin. Olingan kalit (K) uzunligi ham blok uzunligiga keltiriladi. Bunda 3 ta holat bo'lishi mumkin: (1) agar kalitning uzunligi 64 baytga teng bo'lsa, hech

qanday o'zgarish amalga oshirilmaydi, (2) agar kalitning uzunligi 64 dan kichik bo'lsa, u holda yetmagan baytlar o'rnini nollar bilan to'ldiriladi, (3) agar kalit uzunligi blok uzunligidan katta bo'lsa, kalit dastlab xeshlanadi va hosil bo'lgan xesh qiymatning o'ng tomoni blok uzunligiga yetguncha nollar bilan to'ldiriladi. Shu tariqa, kalit uzunligi blok uzunligiga moslashtiriladi.

Shunday qilib, ma'lumot va moslashtirilgan kalit asosida HMAC qiymati quyidagicha hisoblanadi:

$$HMAC(M, K) = H(K \oplus opad, H(K \oplus ipad, M)).$$

Bu yerda, *ipad* va *opad* o'zgaruvchilar quyidagicha hosil qilinadi:

$$\begin{aligned} ipad &= 0x36 \text{ ni } B \text{ marta takrorlash natijasida} \\ opad &= 0x5c \text{ ni } B \text{ marta takrorlash natijasida} \end{aligned}$$

Tenglikdan ko'rinib turibdiki, HMAC da ikki marta xeshlash amalga oshirilmoqda. Kalit K faqat ikki tomonga (jo'natuvchi va qabul qiluvchiga) ma'lum bo'lgani uchun, hujumchi mos xesh qiymatni qayta hisoblay olmaydi. A tomondan yuborilgan $(M, HMAC(M, K))$ ma'lumot juftlaridan hujumchi faqat ma'lumotni o'zgartirishi mumkin bo'ladi va bu holat qabul qiluvchi tomonidan osonlik bilan aniqlanadi.

GCM (Galois/Counter Mode) rejimi. GCM – simmetrik blokli shifrlash algoritmlari uchun amalga oshirish rejimi bo'lib, yuqori samaradorligi bois keng qo'llaniladi. Ushbu rejim ham konfidensiallik, ham yaxlitlikni ta'minlash maqsadida ishlab chiqilgan bo'lib, 128 bitli blok uzunligidagi blokli shifrlar uchun mo'ljallangan.

GCM rejimida ikkita amal: autentifikatsiyalangan shifrlash va autentifikatsiyalangan rasshifrovkalash, mavjud. Autentifikatsiyalangan shifrlash amali uchun 4 ta kirish parametrlari bo'lib, ular quyidagilar:

- maxfiy kalit K – tanlangan blokli shifrlash algoritmining kaliti;
- boshlang'ich vektor IV – 1 va 2^{64} oraliqdagi ixtiyoriy bitlar qatori.

Har bir kalit uchun IV ham turlicha bo'lishi shart va bunda ularning uzunligini bir xil bo'lishi talab qilinmaydi. 96 bitli IV amalga oshirishdagi eng samarali uzunlik hisoblanadi;

- ochiq matn P – 0 va 2^{39} -256 oraliqdagi bitlar qatori;
- qo'shimcha autentifikatsiyalanuvchi ma'lumot (Additional authenticated data) A – bo'lib, u autentifikatsiyalansada, shifrlanmaydi

va ushbu kattalik 0 va 2^{64} oraliqdagi ixtiyoriy bitlar qatori bo'lishi mumkin;

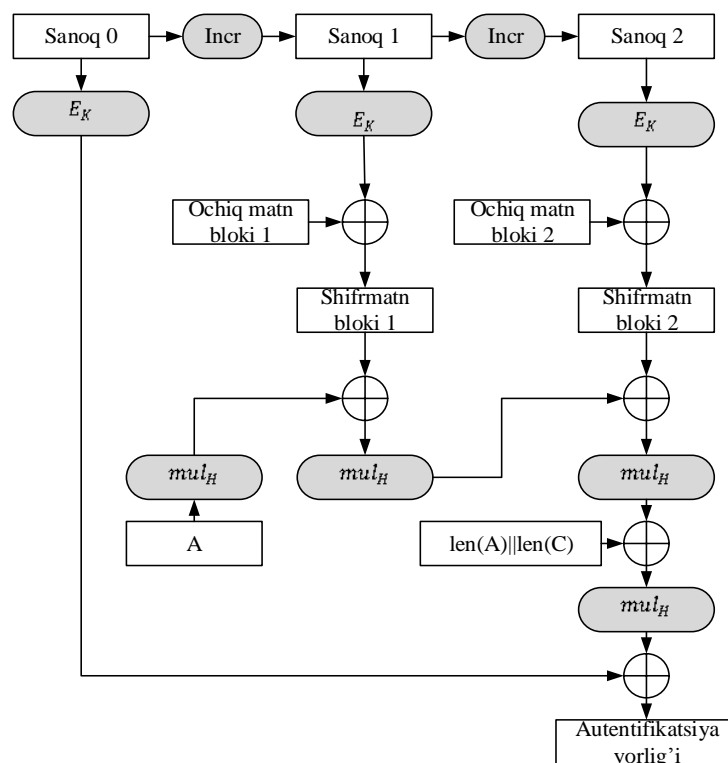
GCM amalida quyidagi 2 ta kattaliklar hosil qilinadi:

- shifrmavn C bo'lib, uning uzunligi ochiq matn uzunligiga teng bo'ladi;

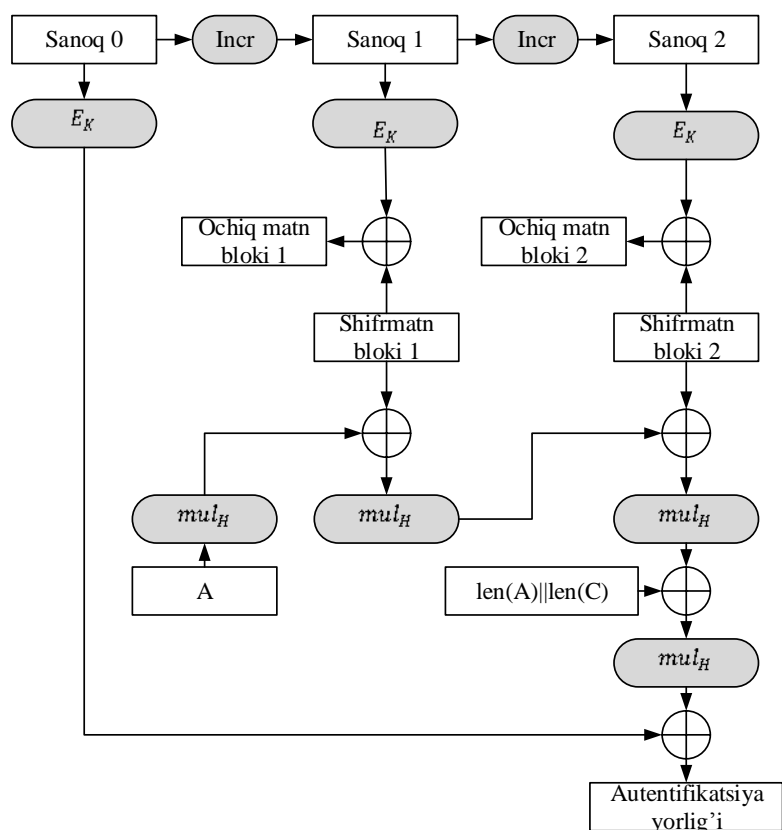
- autentifikatsiya yorlig'i T bo'lib, u 0 va 128 oraliqidagi bitlar qatoridir.

GCM rejimining autentifikatsiyalangan rasshifrovkalash amalida esa K, IV, C, A va T parametrlari kiritiladi hamda chiqishda ochiq matn P yoki autentifikatsiyadan o'ta olmaganlik holatini ko'rsatuvchi $FAIL$ belgisi hosil bo'ladi.

Umumiy holda autentifikatsiyalangan shifrlash va rasshifrovkalash amallarining 2 ta blok uchun ko'rinishi 6.9-rasmda keltirilgan. Bu yerda, *counter* – sanoq, dastlabki qiymati IV va u har bir blok uchun *incr* funksiyasi yordamida bittadan ortib boradi. E_K – kalit yordamida simmetrik blokli shifrlash funksiyasi, mul_H – xesh kalit H yordamida $GF(2^{128})$ maydonda ko'paytirishni anglatadi. Bu yerda, $H = E(K, 0^{128})$ ga teng. $len(A)$ va $len(C)$ – funksiyalar esa mos holda A va C kattaliklarni bitdagi uzunligini ko'rsatadi va u oxirgi shiflanuvchi/rasshifrovkalanuvchi blokdan so'ng amalga oshiriladi.



a) Autentifikatsiyalangan shifrlash amali



b) Autentifikatsiyalangan rasshifrovkalash amali
6.9-rasm. **GCM rejimi**

GCM rejimida ko‘plab standartlarda, IEEE 802.1AE, IEEE 802.11ad, ANSI (INCITS) Fibre Channel Security Protocols (FC-SP), IEEE P1619.1, IETF Ipsec, SSH, TLS 1.2 va 1.3, qo‘llanilgan.

Nazorat savollari

1. Xesh funksiyaga ta’rif bering.
2. Xesh funksiyalarga qo‘yilgan talablarni ayting.
3. Xesh funksiyalarni qurish usullari haqida ayting.
4. Xesh funksiyada kolliziya hodisasi nima?
5. MD5 xesh funksiyasi va uning matematik asosi haqida ayting.
6. MD5 xesh funksiyasiga ma’lumotga to‘ldirish bitlari qanday qo‘shiladi.
7. SHA1 xesh funksiyasi va uning matematik asosi haqida gapiring.
8. O‘z DSt 1106 : 2006 xesh funksiyasi va uning matematik asosi haqida ayting.
9. Xabarlarni autentifikatsiyalash kodi nima va uning asosiy vazifasini tushuntiring.

10. MAC tizimlarida kalitdan foydalanishdan asosiy maqsadni tushuntiring.
11. HMAC algoritmining ishlash tartibini tushuntiring.
12. GCM rejimi va uning asosiy vazifasini ayting.

FOYDALANILGAN ADABIYOTLAR

1. A.J.Menezes, P.C. van Oorschot, S.A.Vanstone. Handbook of Applied Cryptography. CRC Press, 2001, 816 p.
2. Шнайер Б. Прикладная криптография. Протоколы, алгоритмы, исходные тексты на языке Си. –М.: издательство ТРИУМФ, 2003 -816 стр.
3. С.К.Ганиев, М.М.Каримов, З.Т.Худойкулов, М.М.Кадиров. Толковый словарь терминов и понятий по безопасности информации на русском, узбекском и английском языках. –Т.: «Иқтисод-молия», - 2017, 480 с.
4. S.K.Ganiev, M.M.Karimov, K.A.Tashev. Axborot xavfsizligi. –Т.: «Fan va texnologiya», 2016, 372 bet.
5. S.K.Ganiev, M.M.Karimov, K.A.Tashev. Axborot xavfsizligi. Axborot-kommunikatsion tizimlar xavfsizligi. O‘quv qo‘llanma. –Т.: «Aloqachi», 2008, 382 bet.
6. Stamp M. Information security: principles and practice // John Wiley & Sons, 2011, -P. – 606.
7. S.K.Ganiev, A.A.Ganiev, Z.T.Xudoyqulov. Kiberxavfsizlik asoslari. O‘quv qo‘llanma. –Т.: «Iqtisod-moliya», - 2021, 228 bet.
8. D.Ya.Akbarov, P.F.Xasanov, X.P.Xasanov, O.P.Axmedova, I.U.Xolimtoeva. Kriptografiyaning matematik asoslari. O‘quv qo‘llanma. –Т.: «Aloqachi», 2019, 192 bet.
9. Akbarov D.Ye. Axborot xavfsizligini ta’minlashning kriptografik usullari va ularning qo‘llanilishi // Toshkent, 2008, -B. - 394.
10. А.П. Алферов, А.Ю. Зубов, А.С. Кузьмин, А.В. Черемушкин. Основы криптографии: Учебное пособие, 2-е изд. –М.: Гелиос АРВ, 2002.-480 с.
11. Xasanov X.P. Takomillashgan diamatritsalar algebra lari va parametrli algebra asosida kriptotizimlar yaratish usullari va algoritmlari. –Toshkent, 2008. - 208 bet.
12. O‘z DSt 1105:2009 Axborot texnologiyasi. Axborotning kriptografik muhofazasi. Ma’lumotlarni shifrlash algoritmi.
13. O‘z DSt 1106:2009 Axborot texnologiyasi. Axborotning kriptografik muhofazasi. Xeshlash funksiyasi.
14. David A. McGrew, John Viega. The Galois/Counter Mode of Operation (GCM), 2001. <https://csrc.nist.gov/groups/ST/toolkit/BCM/documents/proposedmodes/gcm/gcm-spec.pdf>

15. DES Modes of Operation. Federal Information Processing Standards Publication 81, December, 1980.

16. Federal Information, Processing Standards Publication 197. Announcing the Advanced Encryption Standard (AES). November 26, 2001.

17. Rogaway, P., Coppersmith, D. A Software-Optimized Encryption Algorithm. J.Cryptology 11, 273–287 (1998). <https://doi.org/10.1007/s001459900048>

Internet resurslari

1. Twofish: A 128-Bit Block Cipher [sayt]: <https://www.schneier.com/wp-content/uploads/2016/02/paper-twofish-paper.pdf> (murojaat vaqti: 26.04.2021).

2. MD5 [sayt]: <https://en.wikipedia.org/wiki/MD5> (murojaat vaqti: 26.04.2021).

3. SHA-1 [sayt]: <https://en.wikipedia.org/wiki/SHA-1> (murojaat vaqti: 26.04.2021).

4. HMAC [sayt]: <https://en.wikipedia.org/wiki/HMAC> (murojaat vaqti: 26.04.2021).

5. International Data Encryption Algorithm [sayt]: https://en.wikipedia.org/wiki/International_Data_Encryption_Algorithm (murojaat vaqti: 26.04.2021).

6. GOST 28147-89 [sayt]: https://ru.wikipedia.org/wiki/%D0%93%D0%9E%D0%A1%D0%A2_28147-89 (murojaat vaqti: 26.04.2021).

7. A5/1 [sayt]: <https://en.wikipedia.org/wiki/A5/1> (murojaat vaqti: 26.04.2021).

8. RC4 [sayt]: <https://en.wikipedia.org/wiki/RC4> (murojaat vaqti: 26.04.2021).

9. Enigma Machine Emulator [sayt]: <https://www.101computing.net/enigma-machine-emulator/> (murojaat vaqti: 26.04.2021).

10. WAKE [sayt]: <https://ru.wikipedia.org/wiki/WAKE> (murojaat vaqti: 26.04.2021).

ILOVALAR

1-ilova

128 bitli AES kalitini kengaytirish

$K = 2b\ 7e\ 15\ 16\ 28\ ae\ d2\ a6\ ab\ f7\ 15\ 88\ 09\ cf\ 4f\ 3c$

$N_k = 4$ bo'lgani bois quyidagi o'rinli:

$w_0 = 2b\ 7e\ 15\ 16,$

$w_1 = 28\ ae\ d2\ a6,$

$w_2 = ab\ f7\ 15\ 88,$

$w_3 = 09\ cf\ 4f\ 3c.$

| i (dec) | Temp | RotWord() dan s'ong | SubWord() dan s'ong | Rcon[i/Nk] | Rcon bilan XOR amalidan s'ong | w[i-Nk] | w[i]=temp XOR w[i- Nk] |
|------------|----------|------------------------|------------------------|------------|---|----------|------------------------------|
| 4 | 09cf4f3c | cf4f3c09 | 8a84eb01 | 01000000 | 8b84eb01 | 2b7e1516 | a0fafe17 |
| 5 | a0fafe17 | | | | | 28aed2a6 | 88542cb1 |
| 6 | 88542cb1 | | | | | abf71588 | 23a33939 |
| 7 | 23a33939 | | | | | 09cf4f3c | 2a6c7605 |
| 8 | 2a6c7605 | 6c76052a | 50386be5 | 02000000 | 52386be5 | a0fafe17 | f2c295f2 |
| 9 | f2c295f2 | | | | | 88542cb1 | 7a96b943 |
| 10 | 7a96b943 | | | | | 23a33939 | 5935807a |
| 11 | 5935807a | | | | | 2a6c7605 | 7359f67f |
| 12 | 7359f67f | 59f67f73 | cb42d28f | 04000000 | cf42d28f | f2c295f2 | 3d80477d |
| 13 | 3d80477d | | | | | 7a96b943 | 4716fe3e |
| 14 | 4716fe3e | | | | | 5935807a | 1e237e44 |
| 15 | 1e237e44 | | | | | 7359f67f | 6d7a883b |
| 16 | 6d7a883b | 7a883b6d | dac4e23c | 08000000 | d2c4e23c | 3d80477d | ef44a541 |
| 17 | ef44a541 | | | | | 4716fe3e | a8525b7f |
| 18 | a8525b7f | | | | | 1e237e44 | b671253b |
| 19 | b671253b | | | | | 6d7a883b | db0bad00 |
| 20 | db0bad00 | 0bad00db | 2b9563b9 | 10000000 | 3b9563b9 | ef44a541 | d4d1c6f8 |
| 21 | d4d1c6f8 | | | | | a8525b7f | 7c839d87 |
| 22 | 7c839d87 | | | | | b671253b | caf2b8bc |
| 23 | caf2b8bc | | | | | db0bad00 | 11f915bc |
| 24 | 11f915bc | f915bc11 | 99596582 | 20000000 | b9596582 | d4d1c6f8 | 6d88a37a |
| 25 | 6d88a37a | | | | | 7c839d87 | 110b3efd |
| 26 | 110b3efd | | | | | caf2b8bc | dbf98641 |
| 27 | dbf98641 | | | | | 11f915bc | ca0093fd |
| 28 | ca0093fd | 0093fdca | 63dc5474 | 40000000 | 23dc5474 | 6d88a37a | 4e54f70e |
| 29 | 4e54f70e | | | | | 110b3efd | 5f5fc9f3 |
| 30 | 5f5fc9f3 | | | | | dbf98641 | 84a64fb2 |
| 31 | 84a64fb2 | | | | | ca0093fd | 4ea6dc4f |
| 32 | 4ea6dc4f | a6dc4f4e | 2486842f | 80000000 | a486842f | 4e54f70e | ead27321 |
| 33 | ead27321 | | | | | 5f5fc9f3 | b58dbad2 |
| 34 | b58dbad2 | | | | | 84a64fb2 | 312bf560 |
| 35 | 312bf560 | | | | | 4ea6dc4f | 7f8d292f |
| 36 | 7f8d292f | 8d292f7f | 5da515d2 | 1b000000 | 46a515d2 | ead27321 | ac7766f3 |
| 37 | ac7766f3 | | | | | b58dbad2 | 19fadc21 |
| 38 | 19fadc21 | | | | | 312bf560 | 28d12941 |
| 39 | 28d12941 | | | | | 7f8d292f | 575c006e |
| 40 | 575c006e | 5c006e57 | 4a639f5b | 36000000 | 7c639f5b | ac7766f3 | d014f9a8 |
| 41 | d014f9a8 | | | | | 19fadc21 | c9ee2589 |
| 42 | c9ee2589 | | | | | 28d12941 | e13f0cc8 |
| 43 | e13f0cc8 | | | | | 575c006e | b6630ca6 |

ATAMALARNING RUS, O‘ZBEK VA INGLIZ TILLARIDAGI IZOHLI LUG‘ATI

Алгоритм - упорядоченный конечный набор четко определенных правил для решения задач за конечное количество шагов.

Algoritm – amallarning cheklangan soni yordamida masala yechimini belgilovchi buyruqlarning cheklangan to‘plami.

Algorithm - an ordered finite set of clearly defined rules for solving problems in a finite number of steps.

Алгоритм Rijndael - криптографический алгоритм, указанный в Advanced Encryption Standard.

Rijndael algoritmi - Advanced Encryption Standardda ko‘rsatilgan kriptografik algoritmi.

Rijndael – cryptographic algorithm specified in the Advanced Encryption Standard.

Алгоритм SHA - хэш-алгоритм со свойствами, которые в вычислительном отношении неосуществимы: 1) чтобы найти сообщение, которое соответствует данному дайджесту сообщения или 2) найти два различных сообщения, которые производят тот же самый дайджест сообщения.

SHA algoritmi - 1) berilgan xabar daydjestiga mos xabarni topish yoki 2) bir xil xabar daydjestini hosil qiluvchi ikkita turli xabarlarni hisoblash orqali topish imkonsiz bo‘lgan xususiyatlarga ega xesh - algoritmi.

Secure hash algorithm (SHA) – a hash algorithm with the property that is computationally infeasible 1) to find a message that corresponds to a given message digest, or 2) to find two different messages that produce the same message digest.

Алгоритм шифрования блочный базовый - алгоритм шифрования, реализующий при каждом фиксированном значении ключа одно обратимое отображение множества блоков текста открытого, имеющих фиксированную длину. Представляет собой алгоритм простой замены блоков текста фиксированной длины.

Shifrlashning bazaviy blokli algoritmi - kalitning har bir muayyan qiymatida belgilangan uzunlikdagi ochiq matn bloklari to‘plami ustida bitta qaytariluvchi akslantirishni amalga oshiruvchi shifrlash algoritmi.

Belgilangan uzunlikdagi matn bloklarini oddiy almashtirish algoritmi hisoblanadi.

Basic block encryption algorithm – the encoding algorithm that implements each fixed key value one reversible mapping from a set of plaintext blocks, having a fixed length. k . The algorithm is a simple replacement of blocks of text of fixed length. k .

Алгоритм шифрования поточный - алгоритм шифрования, реализующий при каждом фиксированном значении ключа последовательность обратимых отображений, действующую на последовательность блоков текста открытого.

Oqimli shifrlash algoritmi - kalitning har bir muayyan qiymatida ochiq matn bloklari ketma-ketligiga ta'sir etuvchi qaytariluvchi akslantirish ketma-ketligini amalga oshiruvchi shifrlash algoritmi.

Stream encryption algorithm - an encryption algorithm that implements, for each fixed value of key, sequence of reversible mapping that acting on a sequence of blocks of plaintext.

Алгоритм шифрования - алгоритм криптографический, реализующий функцию шифрования. В случае шифрсистем блочных получается использованием алгоритма шифрования блочного базового в конкретном режиме шифрования.

Shifrlash algoritmi - shifrlash funksiyasini amalga oshiruvchi kriptografik algoritm. Blokli shifrtizim holda shifrlashning muayyan rejimida shifrlashning bazaviy blokli algoritmidan foydalanib hosil qilinadi.

Encryption algorithm - a cryptographic algorithm that implements the function of encryption. In the case of block cipher system is obtained using the algorithm of the base block encryption in a particular mode of encryption.

Алгоритм кодирования имитозащитающего - алгоритм криптографического преобразования информации, обеспечивающий контроль ее целостности (как правило за счет внесения избыточности). В отличие от алгоритма формирования подписи цифровой использует криптосистемы симметричные. Примерами а. к. и. являются код аутентификации, некоторые автоматные преобразования и алгоритмы шифрования.

Imitohimoyalovchi kodlash algoritmi – axborot yaxlitligini (odatda, ortiqchalikni kiritish evaziga) nazoratlashni ta'minlovchi axborotni kriptografik o'zgartirish algoritmi. Raqamli imzoni shakllantirish algoritmidan farqli holda simmetrik kriptotizim ishlatiladi. Misol sifatida autentifikatsiyalash kodini, ba'zi avtomatik o'zgartirishlarni va shifrlash algoritmlarini ko'rsatish mumkin.

Integrity protection coding algorithm - the algorithm of cryptographic transformation of information, providing control its integrity (usually by introducing redundancy). In contrast to the algorithm for generating the digital signature uses a symmetric cryptosystem. Examples of the integrity protection coding algorithm are authentication code, some automatic conversion and encryption algorithms.

Алгоритм криптографический - алгоритм, реализующий вычисление одной из функций криптографических.

Kriptografik algoritmi – kriptografik funksiyalardan birini hisoblashni amalga oshiruvchi algoritmi.

Cryptographic algorithm - the algorithm that implements the calculation of one cryptographic functions.

Алгоритм расшифрования - алгоритм криптографический, обратный к алгоритму шифрования и реализующий функцию расшифрования.

Deshifrlash algoritmi – deshifrlash funksiyasini amalga oshiruvchi va shifrlash algoritmiga teskari algoritmi.

Decryption algorithm – the cryptographic algorithm which is inverse to the encryption algorithm that implements the decryption function.

Алгоритм формирования подписи цифровой - составная часть схемы подписи цифровой. Алгоритм (вообще говоря, рандомизированный), на вход которого подаются подписываемое сообщение, ключ секретный, а также открытые параметры схемы подписи цифровой. Результатом работы алгоритма является подпись цифровая. В некоторых разновидностях схемы подписи цифровой при формировании подписи используется протокол.

Raqamli imzoni shakllantirish algoritmi – raqamli imzo sxemasining tarkibiy qismi. Kirish yo'liga imzolanuvchi xabar, maxfiy kalit, hamda raqamli imzo sxemasining ochiq parametrlari beriluvchi algoritmi (umuman randomizatsiyalangan algoritmi). Algoritmi ishining natijasi

raqamli imzo hisoblanadi. Raqamli imzo sxemasining ba'zi turlarida imzoni shakllantirishda protokol ishlatiladi.

The algorithm for generating a digital signature - an integral part of the digital signature scheme. The algorithm (generally randomized), the input of which serves a signed message, secret key and public parameters of the signature scheme digital. The result of the algorithm is the digital signature. In some versions of this signature scheme in the formation of the digital signature protocol is used.

Алгоритм хеширования - в криптографии - алгоритм, реализующий хеш-функцию криптографическую. В математике и программировании - алгоритм преобразования строк символов, как правило, уменьшающий длину строки и такой, что значение каждого символа выходной строки зависит сложным образом от большого количества входных символов (в идеале - от всех). Обычно, алгоритм хеширования преобразует строки произвольной длины в строки фиксированной длины.

Xeshlash algoritmi – kriptografiyada kriptografik xesh-funksiyani amalga oshiruvchi algoritm. Matematika va dasturlashda – odatda, satr uzunligini kamaytiruvchi simvollar satrini o'zgartiruvchi algoritm. Chiqish yo'li satrining har bir simvolining qiymati kirish yo'li simvollarining katta soniga (idealda – barchasiga) murakkab tarzda bog'liq. Odatda xeshlash algoritmi ixtiyoriy uzunlikdagi satrni belgilangan uzunlikdagi satrga o'zgartiradi.

Hashing algorithm – in cryptography, an algorithm that implements the cryptographic hash function. In mathematics and computer programming - algorithm for converting strings of characters, generally reducing the length of the string and such that the value of each symbol of the output string depends in a complex way from a large number of input characters (ideally all). Usually, hashing algorithm converts strings of arbitrary length to strings of fixed length.k.

Алгоритм цифровой подписи - асимметричный алгоритм, используемый для цифровой подписи данных.

Raqamli imzo algoritmi - ma'lumotlarni raqamli imzolah uchun foydalaniluvchi asimmetrik algoritm.

Digital signature algorithm – asymmetric algorithm used for digitally signing data.

Алгоритм шифрования RSA - алгоритм шифрования, предложенный в 1978 г. Р. Райвестом, А. Шамиром и Л. Адлеманом и предназначенный для построения шифрсистем асимметричных.

RSA shifrlash algoritmi – 1978 yili R. Rayvest, A Shamir va L.Adleman tomonidan taklif etilgan va asimetrik shifr tizimlarini qurishga mo'ljallangan shifrlash algoritmi.

RSA encryption algorithm - the encryption algorithm proposed in 1978 by R. Rivest, A. Shamir and L. Adleman and is designed to build asymmetric ciphers.

Алгоритм шифрования инволютивный - алгоритм шифрования, для которого алгоритмы шифрования и расшифрования совпадают. Другими словами, если к тексту открытому дважды применить алгоритм шифрования, то получится тот же самый открытый текст. Исторически для таких алгоритмов употребляется название «обратимый», но правильно называть их именно «инволютивными», в соответствии с общим пониманием инволюции в математике.

Involutiv shifrlash algoritmi – shifrlash va deshifrlash algoritmlari bir xil bo'lgan shifrlash algoritmi. Boshqacha aytganda, agar ochiq matnga shifrlash algoritmi ikki marta qo'llanilsa, dastlabki ochik matn olinadi. Tarixan bunday algoritmlarga “qaytalanuvchi“ iborasi ishlatiladi, ammo matematikadagi involyutsiya tushunchasiga mos holda aynan “involutiv“ iborasi ishlatilgani to'g'ri bo'ladi.

Involutive encryption algorithm - the encryption algorithm for which the encryption and decryption algorithms are the same. In other words, if the encoding algorithm is applied to the plaintext twice, we get the same plaintext. Historically, such algorithms used the name “reversible”, but the correct name for them is “involutive”, in accordance with the common understanding of involution in mathematics.

Алгоритм шифрования итеративный - алгоритм шифрования, для которого соответствующие алгоритм шифрования и алгоритм расшифрования состоят из последовательных однотипных циклов шифрования.

Iterativ shifrlash algoritmi – mos shifrlash algoritmi va deshifrlash algoritmi shifrlashning ketma-ket bir xil sikllardan tashkil topgan shifrlash algoritmi.

Iterative encryption algorithm - the encryption algorithm for which the corresponding encoding algorithm and the decryption algorithm consist of sequential identical cycles of encryption.

Атака на криптосистему - попытка противника и/или нарушителя понизить уровень безопасности конкретной системы криптографической на основе определенных методов криптоанализа и при некоторых предположениях криптоанализа. Совокупность различных атак постоянно расширяется за счет развития теоретических методов и возможностей техники.

Kriptotizimga hujum – dushmanning va/yoki buzg'unchining kriptotahlilning ma'lum usullari asosida va kriptotahlilning ba'zi taxminlarida muayyan kriptografik tizim xavfsizligi darajasini pasaytirishga urinishi. Turli hujumlar majmui nazariy usullar va texnika imkoniyatlarining rivoji evaziga doimo kengaya boradi.

The attack on the cryptosystem - attempt of the opponent and/or the offender to decrease the level of security of specific cryptographic systems based on specific methods of cryptanalysis under certain assumptions cryptanalysis. The combination of different attacks is constantly expanding due to the development of theoretical methods and the potential of technology.

Бит (двоичный код) - минимальная единица количества информации в компьютере, равная одному двоичному разряду.

Bit (ikkili kod) – kompyuterdagi bitta ikkili xonaga teng axborot miqdorining minimal birligi.

Bit (binary) - the minimum unit of the amount of information in a computer, equal to one binary digit.

Бит достоверности - бит, добавляемый к слову в памяти компьютера для указания достоверности информации.

Haqiqiylik biti – axborot haqiqiyligini ko'rsatish maqsadida kompyuter хотirasidagi so'zga qo'shiladigan bit.

Validity bit - the bit added to the word in the computer memory to indicate the reliability of the information.

Бит защиты - двоичный разряд в ключе памяти, устанавливающий защиту соответствующего блока памяти от записи либо от выборки и записи.

Himoya biti – xotiraning mos blokiga yozish yoki undan tanlash va unga yozishdan himoyalash uchun o'rnatiladigan xotira kalitidagi ikkili xona.
Protection bit - binary digit in the memory key setting protection of a corresponding memory block from write or from select and write.

Бит контроля на четность - контрольный бит, добавляемый к данным для контроля их верности таким образом, чтобы сумма двоичных единиц, составляющих данное, включая и единицу контрольного бита, всегда была четной (либо всегда нечетной).

Juftlikka tekshirish biti – ma'lumotlarga, ularning to'g'riligini nazorat qilish uchun ma'lumotni tashkil etuvchi ikkili birliklarning, jumladan, nazorat biti birligining yig'indigi doimo juft (yoki doimo toq) bo'lishligini ta'minlash maqsadida qo'shiladigan nazorat biti.

Parity bit - control bits added to the data to control their loyalty so that the sum of binary units, the components of this, including the unit control a bit, was always even (or always odd).

Бит маски - сочетание битов, устанавливаемых в нулевое или единичное значение для разрешения или запрета определенных операций либо для проверки или изменения содержимого поля.

Niqob biti – ma'lum amallar bajarilishiga ruxsat berish yoki rad etish yoki hoshiya tarkibini tekshirish yoki o'zgartirish uchun nol yoki bir qiymatiga o'rnatiluvchi bitlar birikmasi.

Mask bit - the combination of bits set to zero or a single value to allow or prevent certain operations or to verify or modify the field contents.

Блок – последовательность бинарных битов, которые включают ввод, вывод, состояние и раунд ключа. Длина последовательности - число битов, которые он содержит. Блоки также интерпретируются как массивы байтов.

Blok – kalitning kirish, chiqish, holat va raundini o'z ichiga oluvchi binar bitlar ketma – ketligi. Ketma – ketlik uzunligi - u tashkil topgan bitlar soni. Bloklar baytlar massivlari shaklida ham izohlanadi.

Block – sequence of binary bits that comprise the input, output, state, and round key. The length of a sequence is the number of bits it contains. Blocks are also interpreted as arrays of bytes.

Блок текста — мультиграмма текста (текста открытого, текста шифрованного или промежуточного), составленная из подряд

идуших знаков. Обычно текст разбивается на блоки одинаковой длины.

Matn bloki - ketma-ket keluvchi belgilardan tuzilgan matn multigrammasi (ochiq matn, shifrlangan matn, oraliq matn). Odatda matn uzunligi bir xil bloklarga ajratiladi.

Text block - multigram text (plaintext, ciphertext, or intermediate text), made up of consecutive digits. Usually the text is divided into blocks of equal length.k.

Блокнот одноразовый — записанный на некотором материальном носителе (например, в специальных бумажных блокнотах) набор данных, используемых для получения последовательностей, управляющих для однократного шифрования. Этот набор данных, обладающий определенными свойствами, должен обеспечивать стойкость (шифрсистемы) совершенную при однократном применении.

Bir martali bloknot - bir martali shifrlash uchun boshqaruvchi ketma-ketlikni olish maqsadida ishlatiluvchi qandaydir moddiy eltuvchida (masalan, maxsus qog'oz bloknotlarda) yozilgan ma'lumotlar nabori. Ma'lum xususiyatlarga ega bo'lgan ushbu ma'lumotlar nabori bir martali ishlatilishida mutlaqo bardoshlikni (kriptotizim bardoshligini) ta'minlashi lozim.

One-time pad - recorded on some tangible medium (e.g., special paper, notebooks) data set used to obtain the sequences of governors for a one-time encryption. This dataset, have certain properties that must ensure stability (cipher system) perfect after a single use.

Блочный алгоритм шифрования - алгоритм шифрования, осуществляющий криптографическое преобразование исходной информации путем выполнения криптографических операций над n -битными блоками открытого текста.

Shifrlashning blokli algoritmi – ochiq matnning n -bitli bloklari ustida kriptografik amallarni bajarish yo'li bilan dastlabki axborotning kriptografik o'zgartirishni amalga oshiruvchi shifrlash algoritmi.

Block encryption algorithm - the encryption algorithm performing a cryptographic transformation of the original information by performing cryptographic operations on n -bit blocks of plain text.

Гамма шифра - псевдослучайная двоичная последовательность, вырабатываемая по заданному алгоритму для шифрования открытой информации и расшифрования шифрованной.

Shifr gammasi – ochiq axborotni shifrlash va deshifrlash uchun berilgan algoritm bo'yicha ishlab chiqiladigan psevdotasodifiy ikkili ketma-ketlik.

Gamma cipher - pseudorandom binary sequence generated by a given algorithm for encoding public information and decrypt the encrypted.

Гаммирование - процесс наложения по определенному закону гаммы шифра на открытые данные.

Gammalash – ochiq ma'lumotlarga ma'lum qonuniyat bo'yicha gamma shifrini qo'yish jarayoni.

Gaming - the overlay process under the particular law of gamma cipher on the open data.

Генератор ключей - техническое устройство или программа, предназначенные для выработки массивов чисел или других данных, используемых в качестве ключей (криптосистемы), последовательности ключевой, векторов инициализации и т. п.

Kalitlar generatori - kalit (kriptotizim kaliti), kalit ketma-ketligi, inisilizatsiya vektorlari va h.k. sifatida ishlatiluvchi son massivlari yoki boshqa ma'lumotlarni ishlab chiqarishga mo'ljallangan texnik qurilma yoki dastur.

Key generator - a technical device or program that is designed to generate arrays of numbers or other data used as a key (cryptosystem), the sequence of key, initialization vectors, etc.

Генератор последовательностей псевдослучайных — техническое устройство или программа для выработки последовательностей псевдослучайных.

Psevdotasodifiy ketma-ketliklar generatori - psevdotasodifiy ketma-ketliklarni ishlab chiqaruvchi texnik qurilma yoki dastur.

Pseudorandom sequences generator - a technical device or program to generate pseudorandom sequences.

Дешифрование - операция, обратная шифрованию и связанная с восстановлением исходного текста из шифрованного.

Deshifrlash – shifrlangan matnni dastlabki matnga tiklash bilan bog'liq shifrlashga teskari amal.

Decryption - the inverse operation of encryption and associated with the restoration of the original text from the encrypted.

Ключ бинарный — ключ, заданный вектором с двоичными координатами.

Ikkili kalit – ikkili koordinatali vektor ko'rinishida berilgan kalit.

Binary key — the key specified by the vector with integer coordinates.

Ключ главный — элемент ключа составного, который используется для шифрования ключей, предназначенных для шифрования ключей разовых или для генерации других видов ключей посредством шифрования определённых данных.

Bosh kalit - bir martali kalitlarni shifrlashga yoki ma'lum ma'lumotlarni shifrlash orqali kalitlarning boshqa turini generatsiyalash uchun mo'ljallangan kalitlarni shifrlashda ishlatiluvchi tarkibiy kalit elementi.

Master key — item composite key, used to encrypt keys for a single encryption key or to generate other types of keys through encryption of certain data.

Ключ долговременный — элемент ключей составных, действующий в неизменном виде длительное время.

Davomli kalit - uzoq vaqt davomida o'zgarmagan holda ishlatiluvchi tarkibiy kalit elementi.

Long-term key — item composite key, valid unchanged for a long time.

Ключ шифрования — ключ, используемый при шифровании.

Shifrlash kaliti - shifrlashda ishlatiluvchi kalit.

Encryption key — the key used in the encoding.

Ключ шифрованный - криптографический ключ, который был шифрован с помощью аттестованной функции безопасности с ключом ключа шифрования, ПИН-кода или пароля для того, чтобы скрыть значение базового ключа открытого текста.

Shifrlangan kalit - ochiq matnning bazaviy kaliti qiymatini yashirish maqsadida attestatsiyadan o'tgan xavfsizlik funksiyasi bilan kalitni shifrlash kaliti, PIN kod yoki parol yordamida shifrlangan kriptografik kalit.

Encrypted key – a cryptographic key that has been encrypted using an approved security function with a key encrypting key, a PIN, or a password in order to disguise the value of the underlying plaintext key.

Ключ симметричный - криптографический ключ, использующийся для выполнения как криптографической операции и её инверсии, например, для шифрования и дешифрования, или создать код аутентификации сообщения и проверки кода.

Simmetrik kalit - har ikkala, kriptografik amal va uning inversiyasini, masalan, shifrlash va deshifrlashni yoki xabarni autentifikatsiyalash kodini hosil qilish va kodni tekshirishni amalga oshirish uchun foydalaniluvchi kriptografik kalit.

Symmetric key – a cryptographic key that is used to perform both the cryptographic operation and its inverse, for example to encrypt and decrypt, or create a message authentication code and to verify the code.

Ключ слабый — ключ криптосистемы, при котором заметно ухудшаются характеристики стойкости криптографической криптосистемы по сравнению со средними значениями тех же характеристик при ключе, случайно равномерно выбранном из множества ключевого криптосистемы.

Zaif kalit - kriptotizim kaliti bo'lib, unda kriptotizimning kriptobardoshlik xarakteristikalari, kriptotizim kalitlari to'plamidan tasodifan, teng ehtimollik tarzda tanlangan kalitning o'sha xarakteristikalarining o'rtacha qiymatlariga nisbatan sezilarli darajada yomonlashadi.

Weak key — key cryptosystem, which significantly degraded the strength of cryptographic cryptosystem in comparison with the average values of the same characteristics when key randomly uniformly chosen from the set key of the cryptosystem.

Код аутентификации — вид алгоритма кодирования имитозащищающей информации. Как правило, код аутентификации сопоставляет сообщение с его кодом аутентичности. Алгоритм принятия решения о подлинности информации основан на проверке значения кода аутентичности сообщения.

Autentifikatsiya kodi – axborotni imitohimoyalovchi kodlash algoritmining turi. Odatda, autentifikatsiya kodi xabarni uning haqiqiylik

kodi bilan taqqoslaydi. Axborotning haqiqiyligi xususida qaror qabul qilish algoritmi xabar haqiqiyligi kodi qiymatini tekshirishga asoslangan. **Authentication code** — the type of encoding algorithm mitsamiouli information. Typically, the authentication code matches the message code authenticity of the message. The decision algorithm on the authentication information based on the verification code value to the authenticity of the message.

Код аутентификации сообщений на основе хэш - код аутентификации сообщения, использующий криптографический ключ в сочетании с хэш-функцией.

Xeshga asoslangan xabarlarni autentifikatsiyalash kodi - xesh funksiya bilan birgalikda kriptografik kalitdan foydalanuvchi, xabarlarni autentifikatsiyalash kodi.

Hash-based message authentication code – a message authentication code that uses a cryptographic key in conjunction with a hash function.

Коды Рида Соломона - важное семейство линейных блочных кодов с исправлением ошибок, особенно удобных для исправления пакетов ошибок. Они могут рассматриваться и как обобщение кодов Боуза Чоудхури Хокенгема, и как особый случай кодов Гоппы, могут быть отнесены к циклическим кодам.

Rid Solomon kodlari – xatoliklarni tuzatuvchi, ayniqsa, xatoliklar paketini tuzatishga qulay chiziqli blokli kodlarning muhim oilasi. Ushbu kodlarni Bouz Choudxuri Hokengem kodlarining umumlashtirilgani sifatida va Goppa kodlarining maxsus holi sifatida, siklik kodlar sifatida ko'rish mumkin.

Reed - Solomon codes - an important family of linear block codes with error correction particularly useful for correcting error bursts. They can be considered as a generalization of codes Bose Chowdhury of Hockenheim, and as a special case codes happy, can be related to cyclic codes.

Коллизия – два или больше разных типов ввода, которые осуществляют одинаковый вывод.

Kolliziya – ikki yoki undan ortiq turli kirishlarni bir xil chiqish hosil qilishi.

Collision – two or more distinct inputs produce the same output.

MUNDARIJA

| | |
|--|-----------|
| MUQADDIMA | 3 |
| 1 BOB. KRIPTOGRAFIYA VA UNING FUNDAMENTAL TUSHUNCHALARI | 5 |
| 1.1. Axborot xavfsizligi va kriptografiya..... | 5 |
| 1.2. Kriptografik funksiyalar..... | 9 |
| 1.3. Kriptografiyaning asosiy tushunchalari va atamalari | 12 |
| 1.4. Simmetrik kalitli shifrlash algoritmlari va xesh funksiyalar | 16 |
| 1.5. Ochiq kalitli kriptografik algoritmlar va elektron raqamli imzo . | 20 |
| 1.6. Kriptografik protokollar va kalitlarni boshqarish | 25 |
| 1.7. Kriptografik algoritmlarga qaratilgan hujumlar | 28 |
| Nazorat savollari..... | 29 |
| 2 BOB. KRIPTOGRAFIYANING MATEMATIK ASOSI..... | 31 |
| 2.1. Ehtimollar nazariyasi asoslari | 32 |
| 2.2. Axborot nazariyasi asoslari | 35 |
| 2.3. Murakkablik nazariyasi | 37 |
| 2.4. Sonlar nazariyasi | 43 |
| 2.5. Fundamental algebra asoslari | 58 |
| Nazorat savollari..... | 65 |
| 3 BOB. KLASSIK SHIFRLASH ALGORITMLARI | 67 |
| 3.1. Sodda o‘rniga qo‘yish va o‘rin almashtirish shifrlari | 67 |
| 3.2. Vernam shifri..... | 71 |
| 3.3. Kodlar kitobi..... | 77 |
| 3.4. Enigma mashinasi | 79 |
| Nazorat savollari..... | 89 |
| 4 BOB. PSEVDOTASODIFIY SONLAR GENERATORI VA OQIMLI SIMMETRIK SHIFRLASH ALGORITMLARI | 91 |
| 4.1. Tasodifiy ketma-ketliklarni hosil qilish usullari..... | 91 |
| 4.2. Chiziqli va chiziqsiz kongruent generatorlar | 94 |
| 4.3. Oqimli shifrlarni qurish asoslari | 96 |
| 4.4. A5/1 oqimli shifrlash algoritmi..... | 102 |

| | |
|--|------------|
| 4.5. RC4 oqimli shifrlash algoritmi | 105 |
| 4.6. SEAL oqimli shifrlash algoritmi..... | 106 |
| 4.7. WAKE oqimli shifrlash algoritmi..... | 109 |
| Nazorat savollari..... | 111 |
| 5 BOB. SIMMETRIK BLOKLI SHIFRLASH ALGORITMLARI | 112 |
| 5.1. Simmetrik blokli shifrlar va ularni qurish usullari..... | 112 |
| 5.2. DES simmetrik blokli shifrlash algoritmi | 116 |
| 5.3. AES simmetrik blokli shifrlash standarti | 124 |
| 5.4. ГОСТ 28147-89 simmetrik blokli shifrlash standarti..... | 134 |
| 5.5. O‘z Dst 1105:2009 simmetrik blokli shifrlash standarti..... | 136 |
| 5.6. IDEA simmetrik blokli shifrlash algoritmi | 144 |
| 5.7. Twofish simmetrik blokli shifrlash algoritmi | 148 |
| 5.8. Simmetrik blokli shifrlash rejimlari | 154 |
| Nazorat savollari | 159 |
| 6 BOB. XESH FUNKSIYALAR VA MA’LUMOTNING YAXLITLIGI TA’MINLASH | 161 |
| 6.1. Xesh funksiyalar va ularni qurish usullari | 161 |
| 6.2. MD5 xesh funksiyasi..... | 166 |
| 6.3. SHA1 xesh funksiyasi | 171 |
| 6.4. O‘z DSt 1106 : 2006 xesh funksiyasi | 173 |
| 6.5. Ma’lumotlarni autentifikatsiyalash kodlari. HMAC algoritmi.. | 178 |
| Nazorat savollari..... | 183 |
| FOYDALANILGAN ADABIYOTLAR..... | 185 |
| ILOVALAR | 187 |
| ATAMALARNING RUS, O‘ZBEK VA INGLIZ TILLARIDAGI IZOHLI LUG‘ATI..... | 188 |

“Kriptografiya 1”

5330300 – Axborot xavfsizligi
yo‘nalishi talabalari uchun o‘quv qo‘llanma.

Kriptologiya kafedراسi majlisida
ko‘rib chiqildi va nashr etishga ruxsat etildi.

2021 yil 20 aprel
35 - sonli bayonnoma

“AX” fakulteti UK majlisida
ko‘rib chiqildi va nashr etishga ruxsat etildi.

2021 yil 28 aprel
9 - sonli bayonnoma

Muhammad al-Xorazmiy nomidagi
TATU Kengashi majlisida
ko‘rib chiqildi, nashr etishga va nashr
guvohnomasini olishga ruxsat etildi

2021 yil 27 may
10(712) - sonli bayonnoma

Tuzuvchilar:

Z.T.Xudoykulov
Sh.k.Z.Islomov
U.R.Mardiyev

Taqrizchilar:

K.A.Tashev
O.P.Axmedova

Mas’ul muharrir:

A.A.Ganiev

Z.T.XUDOYKULOV, SH.Z.ISLOMOV, U.R.MARDIYEV

KRIPTOGRAFIYA 1

O'quv qo'llanma

Muharrir **Sh. Bazarova**

Badiiy muharrir **K. Boyxo'jayev**

Kompyuterda sahifalovchi **K. Boyxo'jayev**

Nashr lits. AI¹ 305. Bosishga ruxsat etildi 12.10.2021.
Qog'oz bichimi 60x84 1/16. Shartli bosma tabog'i 11,7.
Hisob-nashr tabog'i 12,2. Adadi 50.
55-buyurtma.

«IQTISOD-MOLIYA» nashriyotida tayyorlandi.
100000, Toshkent, Amir Temur ko'chasi, 60^A.

«DAVR MATBUOT SAVDO» MChJ
bosmaxonasida chop etildi.
100198, Toshkent, Qo‘yliq, 4-mavze, 46.