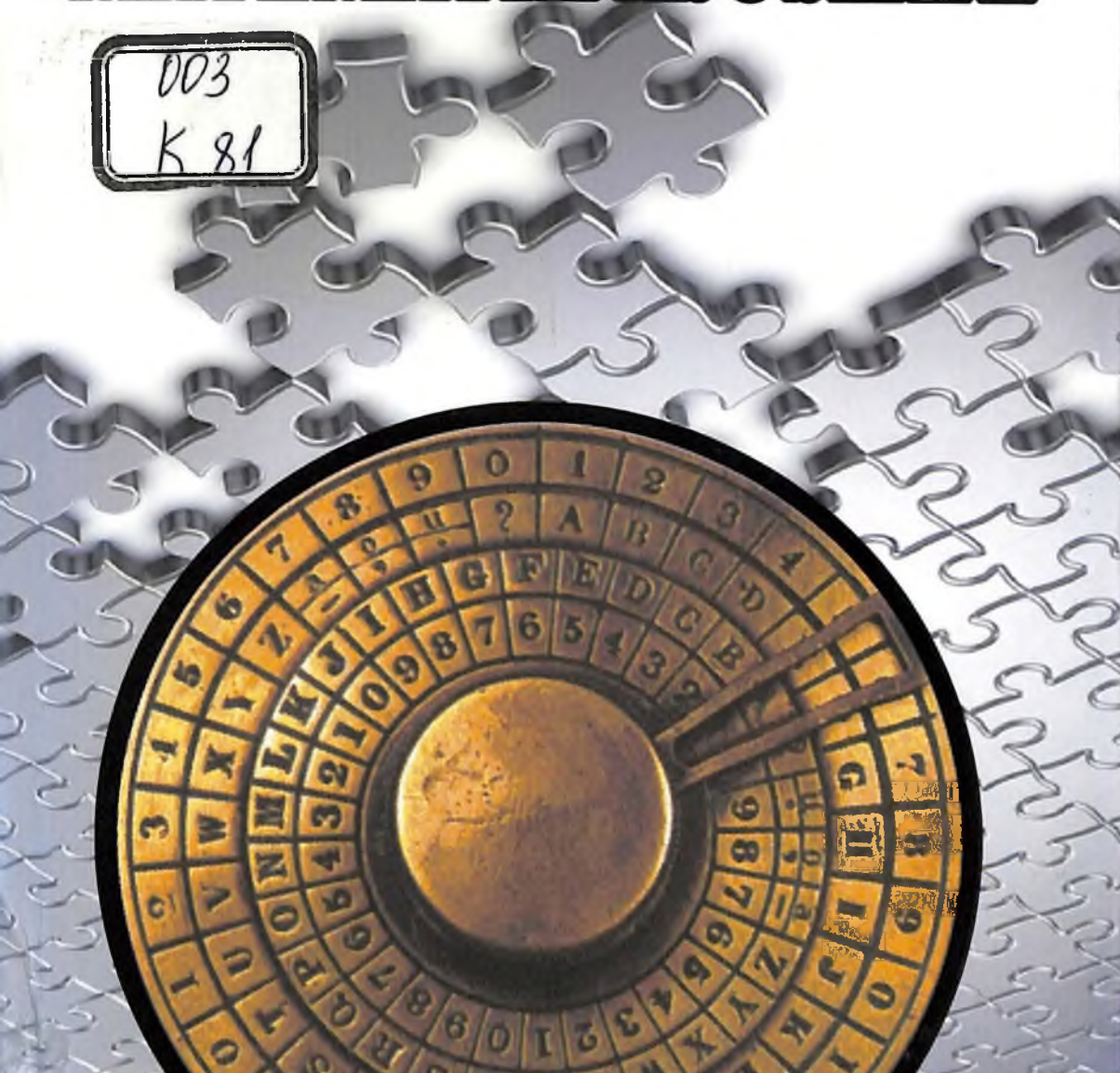
D.Y.Akbarov, P.F.Xasanov, X.P.Xasanov,
O.P.Axmedova, I.U.Xolimtayeva

KRIPTOGRAFIYANING MATEMATIK ASOSLARI



O‘ZBEKISTON RESPUBLIKASI AXBOROT
TEXNOLOGIYALARI
VA KOMMUNIKASIYALARINI RIVOJLANTIRISH VAZIRLIGI

MUHAMMAD AL-XORAZMIY NOMIDAGI TOSHKENT
AXBOROT TEXNOLOGIYALARI UNIVERSITETI

D.Y.Akbarov, P.F.Xasanov, X.P.Xasanov,
O.P.Ahmedova, I.U.Xolimtayeva

KRIPTOGRAFIYANING MATEMATIK ASOSLARI

(O‘quv qo‘llanma)

Toshkent – 2019

UO'K: 512.624.95
BBK 32.973.202-018.2
A 81
D.Y.Akbarov, P.F.Xasanov, X.P.Xasanov, O.P.Axmedova, I.U.Xolimtayeva. Kriptografiyaning matematik asoslari. O'quv qo'llanma. T.: «Aloqachi», 2019, 192 bet.

ISBN 978–9943–5570–3–1

Ushbu o'quv qo'llanmada kriptografiya tarixi, kriptografiyaning asosiy matematik tushunchalari, ta'riflari, teoremalari hamda simmetrik va nosimmetrik kriptografik algoritmlarning matematik asoslari bayon etilgan.

O'quv qo'llanmada parametrli funksiyalar va ularning asosiy xossalari, diamatrisalar algebrasi va parametrli elliptik egri chiziqli funksiyalar hamda ular asosida ishlab chiqilgan kriptoalgoritmlar keltirilgan.

Ushbu o'quv qo'llanma Muhammad al-Xorazmiy nomidagi TATU axborot xavfsizligi va kriptografiya yo'nalishida ta'lim olayotgan magistrlar uchun mo'ljallangan. Shuningdek ushbu o'quv qo'llanmadan axborot xavfsizligi yo'nalishida bakalavrlar tayyorlash jarayonida hamda kriptografiya yo'nalishida ilmiy-tadqiqot olib borayotgan tadqiqotchilar, ilmiy xodimlar va soha mutaxassislari foydalanishlari mumkin.

O'quv qo'llanma Muhammad al-Xorazmiy nomidagi Toshkent axborot texnologiyalari universiteti ilmiy-uslubiy kengashining qarori bilan chop etildi.

UO'K: 512.624.95
BBK 32.973.202-018.2

Taqrizchilar:
M.M.Karimov;
D.YA.Irgasheva.

ISBN 978–9943–5570–3–1

QISQARTMALAR

1.	AES (Advanced Encryption Standard) –	AQShning ma’lumotlarni shifrlash standarti.
2.	AQSh –	Amerika Qo‘shma shtatlari.
3.	GOST 28147-89 –	Rossiya Federasiyasining ma’lumotlar-ni shifrlash standarti.
4.	GOST R 34.10–94 –	Rossiya Federasiyasining diskret logarifmlashga asoslangan elektron raqamli imzo standarti.
5.	GOST R 34.10-2001 –	Rossiya Federasiyasining elliptik egri chiziqda diskret logarifmlashga asoslangan elektron raqamli imzo standarti.
6.	DES (Data Encryption Standard) –	AQShning ma’lumotlarni shifrlash standarti.
7.	DSA (Digital Signature Algorithm) –	AQShning diskret logarifmlashga asoslangan elektron raqamli imzo algoritmi.
8.	EC-DSA-2000 (Elliptic Curve Digital Signature Algorithm) –	AQShning elliptik egri chiziqda diskret logarifmlashga asoslangan elektron raqamli imzo algoritmi.
9.	EC-KCDSA –	Koreyaning elliptik egri chiziqda diskret logarifmlashga asoslangan elektron raqamli imzo algoritmi.
10.	EC-GDSA –	Germaniya Federativ Respublikasining elliptik egri chiziqda diskret logarifmlashga asoslangan elektron raqamli imzo algoritmi.
11.	EKUB –	Eng katta umumiy bo‘luvchi.
12.	FEAL (Fast Data Encryption Algorithm) –	Yaponiya ma’lumotlarni shifrlash algoritmi.
13.	IDEA (International Data Encryption Algorithm) –	Xalqaro ma’lumotlarni shifrlash algoritmi.
14.	KROM –	Kalitlarni ro‘yxatga olish markazi.
15.	NIST (National Institute of Standards and Technology) –	Standartlar va texnologiyalar milliy instituti
16.	MShA –	Ma’lumotlarni shifrlash algoritmi.
17.	PTKK –	Psevdotasodifiy ketma-ketlik.
18.	RSA –	Rayvest-Shamir-Adleman algoritmi.
19.	XOR –	2 modul bo‘yicha qo‘shish.
20.	O‘z DSt 1092:2005, O‘z DSt 1092:2009 –	O‘zbekistonning daraja parametri muammolarining murakkabligiga asoslangan elektron raqamli imzo bo‘yicha davlat standartlari.
21.	ERI –	Elektron raqamli imzo.
22.	ERIA –	Elektron raqamli imzo algoritmi.
23.	EECh –	Elliptik egri chiziq.

KIRISH

Axborot va telekommunikasiya texnologiyalarining jadal sur’atlar bilan rivojlanib borishi turli manbalardan tez va oson yo‘l bilan axborot olish imkoniyatlarini oshirdi. Davlat muassasalari, tijorat korxonalari va alohida shaxslar axborotni elektron shaklda yaratib saqlay boshladilar. Tarmoq orqali axborot uzatish bir onda yuz berishi, uni saqlash esa ixcham joy egallashi, boy ma’lumotlar bazalaridan samarali foydalanish imkoniyatlari kengaya borishi axborot miqdorining jadal sur’atlar bilan o‘sishiga olib keldi. Ilm-fan, ta’lim, ishlab chiqarish, boshqaruv, tijorat va ko‘pgina boshqa sohalar uchun yaxlit axborot eng qimmatli mulkdir [1-2].

Yigirma birinchi asr axborotlashtirish asri ekaniga tobora ko‘pchilik ishonch hosil qilmoqda. Bu albatta ommaviy axborot va hamma bilishi mumkin va zarur bo‘lgan axborot haqida gap borganda o‘ta ijobiy hodisa. Lekin konfidensial va o‘ta maxfiy axborot oqimlari uchun zamonaviy axborot-kommunikasiya texnologiyalari qulayliklar bilan bir qatorda yangi muammolarni o‘rtaga qo‘ymoqda. Axborot bazalarida saqlanadigan va telekommunikasiya tizimlarida aylanayotgan axborot xavfsizligiga tahdid keskin oshdi. Keyingi vaqtda, ayniqsa, Internet paydo bo‘lgandan boshlab, axborot o‘g‘irlash, axborot mazmunini buzib qo‘yish, egasidan iznsiz o‘zgartirib qo‘yish, tarmoq va serverlardan beruxsat foydalanish, tarmoqqa tajovuz qilish, avval qo‘lga kiritilgan uzatmalarni qayta uzatish, xizmatdan yoki axborotga daxldorlikdan bo‘yin tovlash, jo‘natmalarni ruxsat etilmagan yo‘l orqali jo‘natish hollari ko‘paydi.

Natijada axborot xavfsizligi muammosi O‘zbekiston Respublikasi uchun ham dolzarb muammoga aylandi. Bu o‘z navbatida kriptologiya fanini rivojlantirish vazifalarini dolzarb muammolar qatoriga qo‘ydi, chunki hozirgi kunda bu yo‘l axborot xavfsizligini ta’minlash sohasida asosiy yo‘ldir.

Axborotni muhofaza qilish masalalari bilan *kriptologiya* fani shug‘ullanadi. Keyingi oxirigi yillarda kriptologiya yo‘nalishini rivojlantirishga davlatimiz tomonidan katta ahamiyat berilmoqda. O‘zbekiston Respublikasi Prezidentining 2007 yil 3 aprelda qabul qilgan “O‘zbekiston Respublikasida axborotning kriptografik himoyasini tashkil etish chora-tadbirlari to‘g‘risida” gi PQ-614–son

qarorida hamda O‘zbekiston Respublikasi Prezidentining 2017 yil 7 fevraldagi “O‘zbekiston Respublikasini yanada rivojlantirish bo‘yicha Harakatlar strategiyasi to‘g‘risida” gi PF-4947-son farmoyishida beshta ustuvor yo‘nalishdan biri sifatida axborotni muhofaza qilish tizimini takomillashtirish, axborot sohasidagi tahdidlarga o‘z vaqtida va munosib qarshilik ko‘rsatish kabilar ko‘zda tutilgan. Mazkur qaror va farmoyishning asosiy vazifalaridan biri axborotni muhofaza qilish sohasida yuqori malakali kadrlarni tayyorlashdan iborat bo‘lib, buning uchun axborot xavfsizligi va kriptografiya yo‘nalishida davlat tilida ta’lim olayotgan talabalar, tadqiqotchilar va ilmiy xodimlar uchun mo‘ljallangan o‘quv qo‘llanmalar, darsliklar, uslubiy qo‘llanmalar va kitoblar ishlab chiqish muhim ahamiyat kasb etadi.

Taqdim etilayotgan o‘quv qo‘llanma ana shu sohada bajarilgan ishlardan biri hisoblanadi. Ushbu o‘quv qo‘llanma axborot xavfsizligi va kriptografiya yo‘nalishida ta’lim olayotgan magistrlar uchun mo‘ljallangan. Shuningdek ushbu o‘quv qo‘llanmadan axborot xavfsizligi yo‘nalishida bakalavrlar tayyorlash jarayonida hamda kriptografiya yo‘nalishida ilmiy-tadqiqot olib borayotgan tadqiqotchilar, ilmiy xodimlar va soha mutaxassislari foydalanishlari mumkin.

1. KLASSIK SHIFRLAR VA ASOSIY TUSHUNCHALAR

1.1. Ta’riflar va atamalar

Qadim zamonlardan beri inson mo‘jizalar, sirli voqyea va hodisalar sababi hamda mohiyati haqida axborot olishga intilgan. Axborot inson tili va yozuvida o‘z aksini topadi. Dastlabki yozuvlar o‘ziga xos bo‘lgan kriptografik tizim bo‘lib, qadimgi jamoalarda ularni faqat nufuzli shaxslargina tushunishgan. Qadimiy Misr va Hindistonda mavjud bo‘lgan ilohiy kitoblar bunga misol bo‘la oladi. Bundan 4000 yil avvalgi davrga oid eng qadimiy shifrmatn Messopatamiya qazilmalarida topilgan. Unda loydan ishlangan taxtachada o‘ymakor yozuvda tijorat siri – kulolchilik buyumlarini glazurlash resepti yozilgan. Qadimiy Misrda shifrlangan diniy matnlar va tibbiy reseptlar ham mavjud bo‘lgan.

Kriptologiya (grekchada *kryptos* - “sirli” va *logos* -“xabar”) deganda aloqa xavfsizligi haqidagi fan tushuniladi. U aloqa kanallari orqali axborotning xavfsizligini ta’minlab saqlash hamda uzatish tizimlarini yaratish va tahlillash to‘g‘risidagi fandir. Kriptologiya ikki ilmiy irmoqqa ajraladi. Bular kriptografiya va kriptotahlildir [1-10].

Kriptografiya axborot almashtirish tamoyillari, vosita va usullari bilan shug‘ullanadigan fan sohasi bo‘lib, uning maqsadi axborot mazmunidan beruxsat erkin foydalanishdan muhofazalash va axborotni buzishning oldini olish hisoblanadi.

Kriptotahlil shifrni yoki har qanday boshqa shakldagi kriptografiya obyektining sirini ochish san’ati va ilmi bo‘lib, kalitni bilmasdan turib shifrlangan matndan dastlabki matnni olish yoki dastlabki matn va shifrlangan matn bo‘yicha kalitni hisoblash jarayonidir.

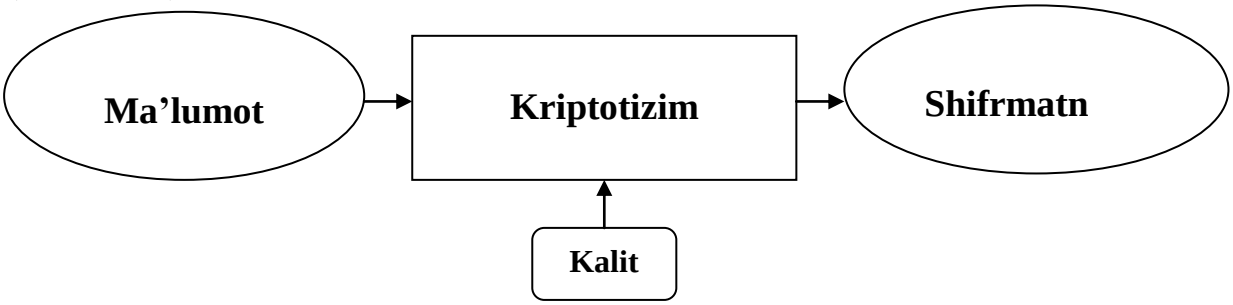
Kriptotahlil usullari tarixi kriptografiya tarixi bilan egizdir.

Kalitdan foydalangan holda alohida qoidalar bo‘yicha ochiq (dastlabki) ma’lumotlar to‘plamini shifrlangan ma’lumotlar to‘plamiga almashtirish uchun amalga oshiriladigan qaytar almashtirishlar majmui *shifr* deb ataladi.

Dastlabki ochiq matnni uning ma’nosini berkitish maqsadida shifrlangan ma’lumotga o‘girish natijasi *shifrmatn* (shifrma’lumot) deb ataladi.

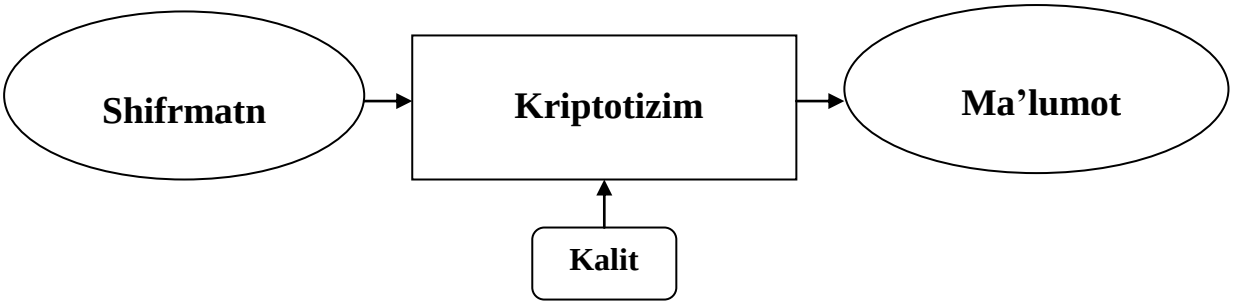
Keng ma’noda *axborotni shifrlash* deganda shifrmatnga o‘girish jarayoni tushuniladi.

Dastlabki ma’lumotlar (axborotlar)ni shifr (kalit) yordamida shifrlangan ma’lumotlarga almashtirish jarayoni *ma’lumotlarni shifrmatnga o‘girish (yoki tor ma’noda shifrlash) jarayoni* deyiladi (1.1-rasm).



1.1- rasm. Ma’lumotlarni shifrmatnga o‘girish jarayoni

Shifrmatnga o‘girilgan ma’lumotlarni shifr (kalit) yordamida dastlabkisiga almashtirish *ma’lumotlarni dastlabki matnga o‘girish* (yoki tor ma’noda deshifrlash) jarayoni deyiladi (1.2- rasm).



1.2- rasm. Ma’lumotlarni dastlabki matnga o‘girish jarayoni

Parametrlarning bir qismi maxfiy holda bo‘lgan kriptografik algoritm bo‘yicha ma’lumotlarni almashtirish *kriptografik o‘zgartirish* deyiladi.

Kriptologiya biror chekli sondagi alifbo belgilarining ketma-ketligi orqali ifodalangan ma’lumotni va uning o‘zgarishlari (akslantirishlari) bilan bog‘liq jarayonlarni tadqiq qiladi. Kriptografik tizimlar matematikaning: to‘plamlar va funksiyalar nazariyasi, algebra, diskret matematika, sonlar nazariyasi, ehtimollar nazariyasi, haqiqiy va kompleks o‘zgaruvchi funksiyalar nazariyasi, murakkablik nazariyasi, axborotlar nazariyasi va shu kabi bo‘limlarga tegishli

bo‘lgan matematik modellar asosida yaratiladi va tadqiq etiladi. Alohida olingan kriptografik modellarning matematik asoslari bilan chuqurroq tanishishni istaganlar kriptografiyaga oid adabiyotlar ro‘yxatida keltirilgan manbalardan foydalanishlari mumkin.

Matematik model boshlang‘ich kuzatuv, fikr va mulohazalar asosida o‘tkazilgan tajribalar natijalarini solishtirish hamda tadqiq qilinayotgan obyekt xususiyatlarini belgilovchi parametrlarning bog‘liqligi qonuniyatlarini ifodalovchi tenglik, tengsizlik va tegishlilik munosabatlari bilan aniqlanadi. Ilmiy tadqiq qilinayotgan obyektlar matematik modellarining moslik darajasi - adekvatligi ular bilan bog‘liq bo‘lgan jarayonlarni qanchalik to‘liq va aniq ifodalanishi bilan belgilanadi. Kriptografik algoritmlar asosini tashkil etuvchi akslantirishlarning modellari asosan xususiyatlari va xossalari jihatidan bir-biriga bog‘liq bo‘lmagan ko‘p o‘zgaruvchili diskret funksiyalarning chekli sondagi ketma-ketligidan iborat majmuani tashkil etadi. Bu funksiyalar parametrlari ochiq ma’lumot, kalit va akslantirishlar oraliq natijalari bloklarini o‘z ichiga oladi.

Ochiq ma’lumotlar *alifbo* deb ataluvchi chekli sondagi belgilar to‘plami elementlarining ma’no beruvchi tartibli ketma-ketligidan iborat [11-13]. Ochiq ma’lumotni tashkil etuvchi alifbo belgilari yoki belgilar birikmalarini akslantirishlar natijasida hosil qilingan shifrmatn ham o‘z navbatida biror chekli sondagi belgilar to‘plamidan iborat bo‘lib, bu belgilar to‘plami *shifrmatn alifbosini* tashkil etadi. Shifrlash jarayonida bajariladigan akslantirishlar ochiq ma’lumot alifbosi belgilari to‘plami elementlarini shifrmatn alifbosi belgilari to‘plami elementlariga biror amal bajarish orqali almashtiriladi, ya’ni to‘plamlar va ularning elementlari ustida amallar bajariladi. Shuning uchun ham berilgan to‘plamda aniqlangan amal va to‘plamning bu amal bilan bog‘liq xossalarini o‘rganish matematikaning asoslarini tashkil etgani kabi kriptologiya fanining matematik asoslariga ham poydevor bo‘lishiga shubha yo‘q. To‘plam elementlari ustida biror amal aniqlash bilan bu to‘plamda shu amal bilan bog‘liq tizim yoki tuzilma aniqlanadi. To‘plamda aniqlangan amallar soni va ularning xossalariga ko‘ra to‘plam elementlari *gruppa*, *halqa*, *maydon* va shu kabi *algebraik tizim (tuzilma, struktura)lar* deb ataluvchi tizimlarni tashkil etadi. Bu algebraik tizimlar bugungi kunda matematikaning turli bo‘limlarida atroflicha o‘rganilgan bo‘lib, bu o‘rganishlarning

ilmiy natijalari kriptologiya masalalari tadqiqini, yechish usullarini va tadbiqini ilmiy asoslash vositasining matematik modellari negizini tashkil etadi.

Kriptografik algoritmlar akslantirishlarining matematik modellari asoslarini chuqur va keng ilmiy o‘rganish mavjud algoritmlarni tahlil qilish va maqsadli takomillashtirishni, kriptobardoshli va amaliy qo‘llanishi samarali bo‘lgan yangi algoritmlar yaratish kabi imkoniyatlarni vujudga keltiradi.

1.2. Kriptografiya tarixi

Ming yilliklar davomida kriptografiyadan davlat qurilishida, harbiy va diplomatiya aloqasini muhofazalashda foydalanib kelingan bo‘lsa, axborot asrining boshlanishi bilan kriptologiya jamiyatda, xususiy sektorda foydalanish uchun ham zarur bo‘lib qoldi [14-15]. Qariyb 35 yildan buyon kriptologiyada keng miqyosda ochiq tadqiqotlar olib borilmoqda. Hozirgi kunda konfidensial axborot (masalan, yuridik hujjatlar, moliyaviy, kredit stavkalari to‘g‘risidagi axborotlar, kasallik tarixi va shunga o‘xshash)larning talay qismi kompyuterlararo odatdagi aloqa kanallari orqali uzatilmoqda. Jamiyat uchun bunday axborotning konfidensialligi va asl holda saqlanishi zaruratga aylangan.

Kriptografiya tarixini shartli ravishda 4 bosqichga bo‘lish mumkin [1, 3-6]:

1. Dastlabki kriptografiya.
2. Formal kriptografiya.
3. Ilmiy kriptografiya.
4. Kompyuter kriptografiyasi, bu bosqich kriptografiyada simmetrik va nosimmetrik kriptotizimlar bo‘yicha ikki ilmiy yo‘nalish yuzaga kelishi bilan xarakterlanadi.

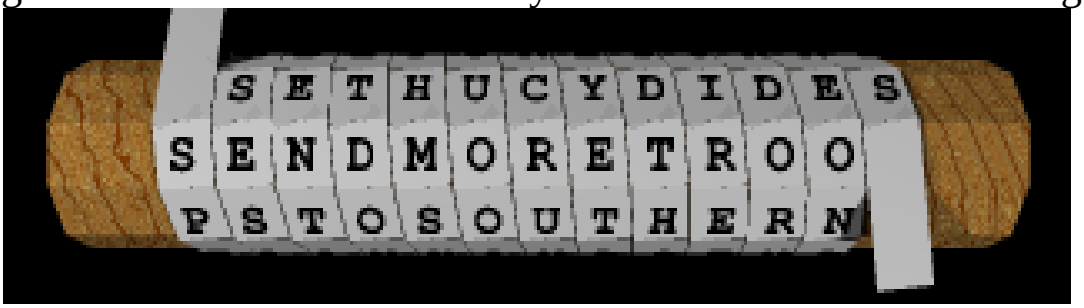
1.2.1. Dastlabki kriptografiya davri

Dastlabki kriptografiya (XVI asr boshigacha) bosqichi uchun sodda usullardan foydalanib, shifrlangan matn mazmunidan begonalarni chalg‘itish xosdir. Bu bosqichda axborotni muhofaza qilish uchun kriptografiya oilasiga mansub, ammo aynan bo‘lmagan

kodlash usullaridan foydalanilgan. Foydalanilgan shifrlarning koʻpchiligi bir alifboli oʻrniga qoʻyish yoki koʻp alifboli oʻrniga qoʻyishga asoslangan.

Dastlabki kriptografiya davriga oid shifrlar haqida gap borganda Yevropa fani tarixidan oʻrin olgan Plutarx, Aristotel (miloddan avvalgi IV asr), Yuliy Sezar (miloddan avvalgi 100-44 yy.), R. Bekon (1214-1294 yy.) shifrlarini aytib oʻtish joiz [1-10].

Dastlabki shifrlash moslamalaridan biri sifatida gʻaltak (skitala)dan foydalanilgan (1.3-rasm). Silindrsimon gʻaltakka zich bir qavat oʻralgan ensiz papirus lentasiga dastlabki matn harflari silindr oʻqi boʻylab yozilib shifrmatn shakllantirilgan. Lenta gʻaltakdan yechib olinib qabul qiluvchiga joʻnatilgan. Qabul qiluvchi shifrmatnli lentani shifrlash gʻaltagi bilan bir xil gʻaltakka oʻrab dastlabki matnni oʻqigan. Gʻaltak oʻlchamlari maxfiy shifrlash kaliti vazifasini oʻtagan.



1.3- rasm. Skitala

Bunday shifr moslamasidan eramizgacha V asrda boʻlib oʻtgan Spartaning Afinaga qarshi urushi davrida foydalanilgan. Shifrlash gʻaltagi oʻlchamlarini topish gʻoyasi Aristotelga tegishlidir. U buning uchun uzun konus olib, unga asosidan boshlab konus uchigacha shifrmatnli lenta oʻralganda konusning biror qismida oʻqiladigan matn hosil boʻlishiga qarab gʻaltak oʻzagi diametrini aniqlagan [1-10].

Qadim zamonlarda atbash deb atalgan shifr ma’lum boʻlgan, undan ba’zan muqaddas iudey matnlarini shifrlashda foydalanilgan (1.4-rasm). Shifrmatn yaratishda dastlabki matnga tegishli alifboning birinchi harfi oxirgisiga, ikkinchi harfi undan avvalgisiga va h.k. almashtirilgan.

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

1.4- rasm. Atbash usuli

To‘la bayoni saqlangan shifrlardan yana biri Sezar shifri bo‘lib, u ham atbash shifri oilasiga mansubdir. Yuliy Sezar o‘z shifridan Siseron (miloddan avvalgi 106-43 yy.) bilan axborot almashishda foydalangani ma’lum [1, 5]. Turli davrlarda bu tizimning turli rusumlaridan foydalanib kelingan. Dastlabki matnning qanday berilishi ahamiyatga ega emas. Sezar usulida shifrlash dastlabki matnga tegishli alifbo harfi o‘rniga shifrlash kaliti *k* qadamga surilgan o‘rinda joylashgan alifbo harfini qo‘yish asosida amalga oshiriladi (1.5-rasm). Bunda surish alifbo harflari soni *26* ga teng bo‘lgan modul bo‘yicha bajariladi. Alifbo harflari boshidan oxiri tomon, oxiridan qayta bosh tomondan boshlab davriy ravishda surib boriladi.

Masalan, *k=3* hol uchun quyidagi ko‘rinishga ega bo‘lamiz:

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**
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**

1.5- rasm. Sezar usulida shifrlash

Bu holda dastlabki matn ODAMni shifrlash natijasi RGDP bo‘ladi.

Sezar tizimining kalit maydoni *26* ta son: *0,1,2,...,25* dan iborat. *k* kalitli E_k shifrlash algoritmi alifbodagi harflarni *k* qadam bilan o‘ngga siljitishni o‘z ichiga oladi. Mos ravishda shifrmatn D_k ni ochish algoritmi alifbodagi harflarni *k* qadam bilan chapga siljitish natijasini beradi.

Sezar tizimi va unga o‘xshash tizimlarni hozirgi zamon o‘quvchisi uchun harflarni alifbodagi tartib raqami bilan almashtirib sonlar ustida modul bo‘yicha qo‘shish amali $\oplus$ yordamida tushuntirish oson. Sezar tizimiga muvofiq, shifrmatn hosil qilishda dastlabki matnning har bir α harfi shifrmatnda $sh\alpha \equiv \alpha \oplus k (mod 26)$ga aylanadi. Dastlabki matn harfi $\alpha \equiv sh\alpha \oplus k (mod 26)$ ko‘rinishda tiklanadi. Ta’kidlash joizki, modul arifmetikasida mazkur qo‘shish amali zamonaviy shifrlarda ham eng ko‘p foydalaniladigan amaldir.

Miloddan avvalgi II asrda qadimgi Gresiyada “Polibiy kvadrati” (1.6-rasm) deb atalmish shifr mashhur bo‘lgan. Shifrlash jadvali *5* ta satr va *5* ta ustundan tuzilgan bo‘lib, ular *1* dan *5* gacha raqamlar bilan belgilangan va jadval xonalarida *25* ta harf joylashgan.

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

1.6- rasm. Polibiy kvadrati

Shifrmatn dastlabki matnga tegishli jadval xonasidagi harflarni satr va ustun raqamlari juftligi bilan almashtirish natijasida hosil etilgan. Shifrlash jadvalida harflarning joylashish tartibi shifrlash kaliti vazifasini o‘tagan. Masalan, yuqorida keltirilgan jadval bo‘yicha I, R va M harflar ifodasi mos ravishda BD, DB va CB bo‘ladi. Kirish xabari ODAM ga mos shifrmatn CDADAACB ko‘rinishda bo‘ladi.

Shifrmatnni dastlabki matnga o‘girish satr va ustun raqamlari juftligini shifrlash jadvali harfiga almashtirishdan iborat bo‘lgan.

1.2.2. Formal kriptografiya davri

Formal kriptografiya (XV asr oxiri – XX asr boshlari) bosqichi qo‘lda kriptotahlillashga bardoshli va formallashtirilgan shifrlar paydo bo‘lishi bilan xarakterlanadi. Kriptografiya tarixining bu davrida Leon Batista Alberti (1404-1472 yy.), Iogann Trisemus (1462-1516 yy.), Djirolano Kardono, Kardinal Rishelye, Djovanni Batista Port, Blez de Vijener (1523-1596 yy.), Fransua Viyet (1540-1603 yy.), Frensis Bekon (1562-1626 yy.), Karl Fridrix Gauss (1777-1855 yy.), Ogyust Kerkxoff (1835-1903 yy.) va G.S.Vernamlar [1, 3, 8, 16-17] ijodiyoti alohida chuqur iz qoldirgan.

Italyan arxitektori Leon Batista Alberti muhim hissa qo‘shganlardan biri hisoblanadi. U ko‘p alifboli o‘rniga qo‘yish usulini birinchilardan bo‘lib taklif etgan. Bu shifr XVI asr diplomati Bleyz de Vijener nomi bilan atalgan. Uning 1466 yildagi «Shifrlar haqida traktat» asari kriptologiyaga oid dastlabki ilmiy asar hisoblanadi [1, 3-8].

Nemis abbati Iogann Trisemus tomonidan 1508 yilda nashr qilingan «Poligrafiya» risolasi o‘sha vaqtda ma’lum bo‘lgan shifrlash algoritmlari umumlashtirilgan va to‘plangan dastlabki asar hisoblanadi. Iogann Trisemus muhim ikkita yangi shifrlash usulini taklif etgan: bular Polibiy kvadratini to‘ldirish usuli (dastlabki kataklar oson esda qoladigan kalit so‘zi yordamida, boshqalari esa alifboning qolgan harflari bilan to‘ldiriladi) va bigramma, ya’ni harflarni juftlab shifrlash usulidir.

Shifr mualliflari orasida davlat boshliqlari ham bo‘lganligi e’tiborga loyiq. Miloddan avvalgi birinchi asrda Yuliy Sezar shifri mashhur bo‘lgan bo‘lsa, XIX asr boshlarida AQSh davlat sekretari, keyinchalik prezident Tomas Jefferson o‘z diskli shifratori bilan tanilgan (1.7-rasm). Jefferson shifratori yog‘och silindrdan kesib tayyorlangan bir-biridan mustaqil ravishda umumiy o‘qda aylanuvchan 36ta diskdan tarkib topgan bo‘lib, har bir diskning yon sirtida ingliz alifbosi harflari ixtiyoriy va turli tartibda o‘yib yozilgan. Silindr yon sirtida o‘qqa parallel bo‘lgan chiziq ajratilgan. Shifrmatn shakllantirishda dastlabki matn 36 simvolli guruhlarga bo‘linib, guruhning 1-harfi birinchi diskning ajratilgan chiziqda birinchi disk holati bilan, ikkinchisi – ikkinchi disk holati bilan va h.k. belgilangan. Shifrmatn ajratilgan chiziqqa parallel bo‘lgan ixtiyoriy chiziqda yotgan harflar ketma-ketligi sifatida shakllantirilgan. Dastlabki matnni tiklash bunga teskari tartibda bajarilgan: disklarni aylantirish natijasida shifrmatn harflari ajratilgan chiziq bo‘ylab joylashtirilgan. Dastlabki matn o‘zaro parallel chiziqlar orasidan ma’noga ega matn hosil qiluvchi chiziqda joylashgan.

Avval ma’lum bo‘lgan ko‘p alifboli almashtirishga asoslangan Jefferson shifrator kalitining qismlari sifatida harflarning har bir diskda va disklarning umumiy o‘qda joylashish tartiblaridan foydalanilgan. Foydalanilishi mumkin bo‘lgan kalitlarning umumiy soni $(26!)^{36}$ga teng. Shifrning bunday yuksak kriptobardoshlilikka ega ekanligi XX asrga kelib tan olingan va AQSh armiyasida foydalanish uchun qabul qilingan [1, 10, 12].

1.7- rasm. Jefferson shifratori

T. Jefferson o‘z shifriga yuqori darajada ehtiyotkorlik bilan yondashib, uni chuqur tahlil etish lozim deb hisoblagan va o‘z amaliyotida an’anaviy kodlardan va Vijener tipidagi shifrlardan foydalanishda davom etgan. Uning shifri XX asrning 20-yillarida to‘rtinchi bor qayta kashf etilgan. T. Jefferson ixtirosining asosiy natijasi bo‘lib, XX asrda dastlabki murakkab elektromexanik shifratorlar yuzaga kelishi uchun zamin yaratdi. U amerika shifr maktabining otasi deb bejiz tan olinmagan.

XIX asr kriptografiyasi taraqqiyotiga sezilarli hissa qo‘shganlardan biri Prussiya armiyasi ofiseri Fridrix Kazisskiydir [1-6]. U 1863 yilda 100 betli “Maxfiy yozuv va shifrni kalitsiz ochish san’ati” kitobini chop etgan. Kriptografiya sohasida mashhur tarixchi D. Kan “Kazisskiy kriptografiyada inqilob qilgan” deb yozgan [1-10]. Asosan mazkur kitob Vijener shifri sinfiga oid qisqa davriy gammalash shifrlarini kalitsiz ochish usullariga bag‘ishlangan. Bunday shifrdan foydalanilganda dastlabki matnda davriy takrorlanuvchi harfiy birikma kalitga oid dastlabki gammaning davriy davomlari bilan mos kelib, shifrmatnda shunga mos harfiy birikmalar hosil etadi. Bunday takrorlanishlar shifrni kalitsiz ochishda juda qo‘l kelgan.

XIX asr oxiriga kelib kriptografiya aniq fan sifatlariga ega bo‘la boshladi va u harbiy akademiyalarda o‘rganila boshlandi.

XIX asrda yaratilgan shifrlar orasida Vijener shifri oilasiga oid Sen-Sir Fransiya harbiy-dala akademiyasi shifri - “Sen-Sir chizg‘ichi” mashhur bo‘lgan. Bunday shifrator logarifmik chizg‘ichga o‘xshash tuzilgan bo‘lib, alifbo harflari bosmalangan uzun karton bo‘lagi shaklidagi qo‘zg‘almas shkala qismdan va alifbo harflari ikki qayta bosmalangan tor karton bo‘lagi shaklidagi qo‘zg‘aluvchan qismdan

iborat. Shifrlash jarayoni qo‘zg‘aluvchan qismni kalitning 1-harfi shkalaning «A» harfi ostida joylashuv holatiga mos bo‘lguncha siljitishdan iborat. Bunda dastlabki matnning 1-harfini kalitning shu harfi bilan almashtiriladi. Shu zaylda dastlabki matnning 2-harfi qo‘zg‘aluvchan qismni kalitning 2-harfi shkalaning «A» harfi ostida joylashuv holatiga mos bo‘lguncha siljitib u bilan almashtiriladi va h.k. “Sen-Sir chizg‘ichi” Vijener shifrining sodda mexanik qurilmasi bo‘lgani uchun shifrlovchilar mehnatini osonlashtirgan. Bu g‘oya qo‘zg‘aluvchan qismda alifbo harflarini ixtiyoriy joylashtirish orqali o‘z rivojini topgan va kriptobardoshlilikning yanada oshishiga olib kelgan. “Sen-Sir chizg‘ichi”dan Germaniyada ham takomillashtirilgan shaklda foydalanilgan [1].

XIX asr oxirida Fransiya bosh vaziri Leon Gambetta shifr asboblaridan foydalanishning o‘rniga oddiy algebraik amallardan foydalanishni taklif etgan. Bunda matn harflari sonlar bilan almashtirilib, alifbo hajmiga teng modul bo‘yicha qo‘shish amalidan foydalaniladi. Zamonaviy Gamma shifri atamasi Gambetta nomidan kelib chiqqanligi e’tiborga loyiq.

Shu munosabat bilan, shifrlar nazariyasida buyuk vatandoshimiz Muhammad al-Xorazmiyning algebra fani va algoritm tushunchasi mustahkam o‘rin olganini ta’kidlash o‘rinlidir [1].

Elektrotexnika sohasida fundamental ilmiy asarlari bilan mashhur bo‘lgan Gollandiyalik yirik alloma Ogyust Kerxgoff XIX asr kriptografiyasi tarixida o‘z nomini abadiylashtirgan. U kriptografiya bilan boshlang‘ich tanishuvni harbiy–dala telegraf shifrlaridan boshlab, 1880-yillarda 64 betli “Harbiy kriptografiya” kitobini bosmadan chiqargan. Kitobda shifrga qo‘yiladigan quyidagi umumiy talablar shakllantirib berilgan:

- foydalanish osonligi;
- ishonchlilik (yuqori kriptobardoshlilik);
- tezkorlik (shifrmatnni shakllantirishda va dastlabki manni tiklashda kriptografik almashtirishlar uchun oz vaqt sarf bo‘lishi);
- kriptobardoshlilik faqat shifrlash kalitiga bog‘liq bo‘lishi.

Shifr, ya’ni kriptografik almashtirishlar algoritmi raqib tomonga ma’lum bo‘lganda ham yuqori kriptobardoshlilikning ta’minlanishi talab etilgan. Shifr qurilmasi bitta foydalanuvchi uchun

oson va qulay bo‘lishga mo‘ljallanishi talab etilgan. Lekin ikkinchi jahon urushi yillarida Germaniya qo‘shinlarida tezkorlikni ta’minlash maqsadida har bir shifratorda uchta foydalanuvchi xizmat ko‘rsatgan edi. Mazkur talablar bugungi kunda ham yaratiladigan shifrlar uchun majburiy talablar to‘plamining asosini tashkil etadi.

Noyob iste’dod egasi Kerxgoff ikki soha - adabiyot va fan bo‘yicha ilmiy darajalarga ega bo‘lgan, Gollandiya va Fransiya o‘quv yurtlarida ta’lim bergan. Uning kriptotahlil sohasidagi faoliyati Fransiyada yuksak qadrlangan. D. Kanning fikricha, birinchi jahon urushi arafasida Fransiya kriptografiya dunyosida ilg‘or o‘rinlardan birini egallashida Kerxgoffning hissasi bor [1, 16]. Germaniya o‘z navbatida asosiy e’tiborni asosan harbiy qurollarga qaratgan va bu bundan keyingi urushlarda Germaniya uchun qimmatga tushgan.

XIX asr kriptografiyasida ingliz allomasi, kompyuter kashfiyotchisi Charlz Bebbidj yorqin siymolardan biri bo‘lgan. Ingliz olimi Charlz Bebbidj mexanik kalkulyatorni ishlab chiqqan va 1823 yilda uni qurgan. Mexanik kalkulyator bug‘ yordamida harakatga keltirilgan va to‘la avtomatik bo‘lgan hamda ichiga o‘rnatilgan dastur orqali boshqarilgan. Shunisi e’tiborga loyiqki, uning sxemasi asosida qurilgan ilk kompyuter “Enigma” (1.8-rasm) ikkinchi jahon urushi davrida nemislar foydalangan shifratorni neytrallash uchun yaratilib, bu vazifani a’lo darajada hal etib bergan edi. Ch. Bebbidj o‘zining asosiy e’tiborini Vijener shifriga, gamma-davrasiga qaratgan va XIX asr o‘rtalarida o‘z shifrini yaratgan. Biroq arxiv ma’lumotlari tadqiqotlari shuni ko‘rsatadiki, Kazisskiy 1863 yilda Ch. Bebbidj shifrini qayta kashf etib, tarixda shifr uning nomida qolgan. Ch. Bebbidj birinchi bo‘lib shifrga oid asosiy tushunchalarni jiddiy matematik tarzda shakllantirgan, ko‘p alifboli shifrlarni yechish algoritmini bergan va birinchilardan bo‘lib algebradan foydalangan. Dastlabki matnga bog‘liq kalit – «xos kalit»ga asoslangan shifrlarni ochish g‘oyasi ham unga tegishlidir.

1.8- rasm. Enigma shifratori

XIX asr boshlarida Charlz Uitston tomonidan kashf qilingan Pleyfer shifri ko‘p alifboli o‘rniga qo‘yishning sodda, lekin kriptotahlilga bardoshli usullaridan hisoblanadi. Takomillashtirilgan shifrlash usullaridan biri bo‘lgan «qo‘sha kvadrat» usuli ham Uitstonga tegishli. Pleyfer va Uitston shifridan birinchi jahon urushi boshlangunga qadar foydalanilgan, uning kriptotahlili qo‘lda bajarilishi qiyin edi.

XX asr boshlarida amerikalik mashhur kriptograf Uilyam Fridman tomonidan 1918 yilda tayyorlangan 8 ta ma’ruzadan iborat «Riverben nashrlari» asari nazariy kriptografiyaga muhim hissa bo‘lib qo‘shilgan. «Riverben nashrlari» birinchi jahon urushi davrida kriptografiya va kriptotahlil xizmatida to‘plangan katta tajribaga asoslangan edi. U o‘z asarida kriptografiya masalalarini yechishda ehtimollar nazariyasidan foydalanish samarali ekanligini namoyish qilgan [1, 18-19].

Kommunikasiya sohasida yuzaga kelgan ixtirolar o‘z davrida yaratilgan shifrlar mohiyati o‘zgarishi bilan uzviy bog‘langan. Bunga amerikalik Gilbert Vernamning kriptografiyani rivojlanishiga qo‘shgan muhim hissasi misol bo‘ladi. Telegraf kompaniyasining bo‘lg‘usi xodimi 1917 yilda telegraf xabarlarini avtomatik shifrlash g‘oyasini taklif etgan. Uning mohiyati shundaki, dastalabki matn Bodo kodi (besh belgili «impuls birikmalari») ko‘rinishida tasvirlanadi. Bu kodda masalan, «A» harfi (++---) uchun qog‘oz lentada teshikchalar qatori quyidagicha ko‘rinish oladi:

● ● · · ·

(+) (+) (-) (-) (-)

«+» teshikcha borligini, «-» uning yo‘qligini bildiradi. Uni o‘qishda besh tishli elektromagnit o‘qish qurilmasidan foydalanilgan. To‘g‘ri chiziq bo‘ylab (aylanma) harakat qiluvchi lenta teshikchalari ketma-ketligi tok impulslari ketma-ketligiga aylantirilgan.

Vernam shifrlashda elektromexanik koordinatalar bo‘ylab dastlabki matn belgilariga oid impulslarni maxfiy kalit - gamma impulslari bilan 2 moduli bo‘yicha qo‘shishni (zamonaviy matematika tilida) taklif etgan. Shifrmatnni dastlabki matngga o‘girishda yana shu amaldan foydalanilgan. Vernam bu amallarni operatorsiz avtomatik tarzda amalga oshirish qurilmasini ham yaratgan. Shunday qilib, shifrmatn hosil qilish va uzatish jarayoni bir paytda bajariladigan «chiziqli shifrlash»ga, zamonaviy oqimli shifrlarga asos solgan. Bu aloqa tezkorligini keskin oshirgan. Vernam shifri amerikalik mumtoz kriptograf Klod Shennon tomonidan mukammal shifr nazariyasini asoslash uchun baza bo‘lib xizmat qilganini eslab o‘tish o‘rinlidir. Vernam shifri haddan tashqari bardoshli shifr hisoblanadi. Vernam o‘zi matematik-kriptograf bo‘lmasa ham, shifr gammasi shifrlashda qaytarilmasligini talab qilib to‘g‘ri yo‘l tutganligi o‘z isbotini topgan. Uning g‘oyalari katta hajmli xabarlarni uzatishda axborotni ishonchli muhofazalashga oid yangicha yondashuvlarning yuzaga kelishiga sabab bo‘lgan.

O‘rta Osiyo respublikalarining kriptografiya tarixi formal kriptografiyaning oxirigi yillari (1900-1929 yillar) va ilmiy kriptografiya davri (1930-1960 yillar)da Rossiya kriptografiya tarixining tarkibiy qismi bo‘lganligini e’tiborga olmoq lozim [1, 3].

Kriptografiya asosan urushlar zamonida va terrorizm avjiga chiqqan davrlarda hal qiluvchi ahamiyatga ega bo‘lgan. Bu kriptografiyani rivojlantirish borasida keng miqyosli tadbirlar amalga oshirilishiga turtki bo‘lgan. Masalan, 1866 yil 4 aprelda D.V. Karakozov tomonidan rus podshohi Aleksandr II ga qarata o‘q otilgandan so‘ng chor Rossiyasi kriptografiya xizmatining faoliyatida yangi davr boshlangan [1, 3].

XX asr boshlarida yuzaga kelgan radioaloqa armiya qismlarida foydalaniladigan shifrlar bardoshliligiga bo‘lgan talabni oshirib yubordi, bu davrda rus kriptografiya maktabi jahonda ilg‘or maktablar

qatoriga koʻtarilgan. Bir tomondan inqilobchilar, ikkinchi tomondan chor jandarmchilari orasida murosasiz tarafkashlik kurashi avj olgan. Bunda axborot xavfsizligi vositalari hal qiluvchilardan biri boʻlib, ustunlik to XX asrning 30 yiligacha chor Rossiyasi tarafdorlarida boʻlgan.

Kriptografiya tarixi boʻyicha birinchi asar [16] muallifi Devid Kanning yozishicha, Birinchi jahon urushi (1914-1917 yillar)da rus armiyasining magʻlub boʻlishiga armiyada foydalanilgan shifrlash vositalarining zaifligi sabab boʻlgan. Rus armiyasida foydalanilgan shifr tizimi koʻp alifboli shifr almashtirishlarga asoslangan boʻlsa-da, shifrtelegrammalar aslida bitta alifbo bilan shifrlangan harflar guruhidan iborat boʻlib, kriptobardoshliligi past boʻlgan.

Birinchi jahon urushi boshida rus armiyasi uchun kalitlarni bot-bot yangilashga moʻljallangan ikki karra oʻrin almashtirishga asoslangan murakkab shifr yaratildi. Ammo, eski shifrdan ham bir vaqtda foydalanish tartibsizliklarni vujudga keltirib, ochiq matndan foydalanishgacha borib yetgan, bunda shifr operatorlarining yaxshi tayyorgarlikdan oʻtmagani pand bergan.

1916 yilga kelib yangi shifr bilan barcha harbiy qismlarni ta’minlash imkoniyati tugʻildi. Lekin, 1917 yil oktyabr inqilobi Rossiya kriptografiya xizmatining batamom izdan chiqishiga olib keldi. Koʻpchilik yuqori ixtisosli kriptograflar va kriptotahlilchilar «oqlar» tarafida boʻlgan. Ba’zilari xorijga qochib ketganlar va ular oʻz xizmatlarini xorijiy davlatlarga taklif etganlar va u yerda Sovetlarga qarshi ishlaganlar. Masalan, kod va shifrlar boʻyicha ingliz hukumati maktabining rus seksiyasi rahbari Ernest Fetterleyn revolyusiyaga qadar chor Rossiyasida yetakchi kriptotahlichilardan boʻlgan va Angliyada sovet diplomatik shifrlarini buzib ochish boʻyicha ixtisoslashtirilgan. U Sovetlar Rossiyasining har qanday shifrini hyech qanday qiyinchiliksiz ocha olar edi. Bu Sovet Rossiyasi xalqaro munosabatlarida yoʻqsillar diktaturasi rahbarlarining gʻirrom hatti-harakatlarini oʻz vaqtida fosh boʻlishiga, xalqaro munosabatlarning keskinlashuviga olib kelgan. Bolsheviklar tarafida boʻlgan kam sonli kriptologlar yagona rahbariyatga ham ega boʻlmagan. Shunday qilib, 1920 yillarda Rossiyada axborot muhofazasini ta’minlashga qodir kriptologik markaz boʻlmagan.

Formal kriptografiyaning, umuman butun kriptografiya taraqqiyotining yuksak cho‘qqisi bo‘lib ilk bora amaliyotda foydalanila boshlangan 1917 yilda Edvard Xebern tomonidan ishlab chiqilgan va Artur Kirx tomonidan takomillashtirilgan nemis «Enigma» rotor shifrlash mashinasi tan olingan. Edvard Xebernning kriptografik jarayonlarni mexanizasiyalash borasida inqilobiy tamoyili rotor qurilmalar uchun asos sifatida qabul qilingan. Nemis Enigmasidan boshqa yana AQShning SIGABA, Buyuk Britaniyaning TYPEX, Yaponiyaning RED, ORANGE va PURPLE qurilmalaridan ham foydalanganlar.

AQShda kriptotahlil bo‘yicha mutaxassislar tayyorlash Birinchi jahon urushi boshlanishidan bir necha yil avval boshlangan. Ular dastlab aloqa qo‘shinlari maktabida, keyinchalik harbiy razvedka boshqarmasi qoshida tashkil etilgan armiya kriptologiya maktabida tayyorlandi.

XX asrning 1917 yil boshlarida kriptotahlil sohasidagi eng katta yutuqlardan biri Germaniyaning sobiq tashqi ishlar vaziri Simmerman maktubi sifatida mashhur. Britaniya dengiz razvedkasi tomonidan transatlantik kabeldan tutib olingan maxfiy telegramma matni AQSh hukumatiga topshirilgan. Unda Amerika shtatlari bo‘lgan Texas, Nyu-Mexiko va Arizonani Meksikaga qo‘shib olish haqida Meksikadagi nemis elchisiga Meksika hukumati bilan ittifoq tuzish taklif etilgan. Tarixchilarning ta’kidlashicha, telegramma shunday portlash sodir etganki, buning natijasida 1917 yil 6 aprelda Amerika kongressi Germaniyaga qarshi urush e’lon qilgan. Shunday qilib, kriptografiya *birinchi marta* o‘zining ahamiyati qanchalar muhimligini namoyish etgan.

Nemis harbiy kodlarini va shifrlarini kriptotahlil etish maqsadida bu ishga armiya kriptologiya maktabi sobiq bitiruvchilari va o‘qituvchilari jalb etilgan. Ular qatoridan XX asr AQSh kriptografiya tarixida yorqin siymolardan biri Uilyam Fridman ham o‘rin olgan edi. Uning rafiqasi ham kriptograf edi. Er-xotin Fridmanlar o‘zlarining faoliyatlarini «Enigmatologiya» («sirlarni o‘rganish»)ni o‘rganishdan boshlaganlar. Uilyam Fridman AQSh radiorazvedka xizmatining boshlig‘i sifatida faoliyat ko‘rsatib, armiya kodlari va shifrlarini ishlab chiqish, dushmanning radio va aloqa kanallaridan uzatilayotgan xabarlarini tutib olish, kod va shifrlarni

kriptotahlil etish, sirli yozuv sohasida laboratoriya tadqiqotlarini o‘tkazish bilan shug‘ullangan [10].

1919 yilda taniqli ingliz kriptografi, «Amerika qora kabineti» kitobi muallifi Gerbert Yardli vertikal o‘rniga qo‘yishga asoslangan katta hajmdagi ingliz agentligi shifrini ochishga muvaffaq (musharraf) bo‘ldi. Bu shifrxabar sobiq Sovet Ittifoqi havo yo‘li bo‘ylab Latviyaga qo‘nayotgan nemis aeroplanidan qo‘lga kiritilgan. Shifrlangan xatdan uning muallifi - G‘arbiy Yevropaning katta agentlik tarmog‘i ishiga rahbarlik qiluvchi shaxs ekani aniqlangan. Hujjatlar ichida «Diplomatik missiyalarda josuslikka jalb etilgan agentlar uchun yo‘riqnoma» ham bo‘lgan. Diplomatik yoki harbiy shifrlardan farqli ravishda sovet agentlik shifrlarini ochish hollari ham ba’zida sodir bo‘lib turgan [10].

«Qora kabinet» 1917 yildan 1929 yilgacha faoliyati davrida Yevropa va Janubiy Amerika davlatlarining 10 000 dan ortiq telegrammalari fosh etilgan. Yapon diplomatik kod va shifrlarini fosh etish «Qora kabinet» faoliyatining eng yirik muvaffaqiyati hisoblanadi [10].

Rossiya kriptografiya tarixida asosiy tashkiliy ishlar 1921 yil may oyidan boshlangan. Shu oyda Butunrossiya Favqulodda Komissiyasining kriptografiya bo‘limi bazasida kriptografiya maxsus bo‘limi (8-maxsus bo‘lim) tashkil topgan. Maxsus bo‘lim doirasida mehnat taqsimoti aniq belgilab qo‘yilgan, masalan, ikkinchi bo‘linma - kriptologiyaning nazariy muammolari va yangi shifrlar yaratish, uchinchi bo‘linma turli sovet idoralari (vedomstvo)da shifraloqani tashkil etish, to‘rtinchi bo‘linma - tutib olingan shifrxabarni kriptotahlillash bilan shug‘ullangan.

1921-22 yilllarda dastlabki diplomatik va harbiy Turkiya shifrlarini deshifrlash (shifrni kalitsiz ochish), 1925 yilga kelib o‘n beshta Yevropa davlatlari shifrlari bilan ishlash, 1927 yil Yaponiya xabarlarini o‘qish, 1930 yilda AQShning ba’zi shifrlarini buzib ochish mumkin bo‘lgan [1, 10].

1.2.3. Ilmiy kriptografiya davri

Kriptografiya tarixining navbatdagi bosqichi ***ilmiy kriptografiya davri*** XX asrning 30-60 yillarini o‘z ichiga oladi. Bu

davrning farqli tomoni kriptobardoshliligi jiddiy matematik asoslangan kriptotizimlarning yuzaga kelishidir. XX asrning 30 yillari boshlarida kriptologiyaning ilmiy asosi bo‘lgan matematikaning bo‘limlari batamom shakllanib bo‘ldi. Bularga *ehtimollar nazariyasi va matematik statistika, umumiy algebra, sonlar nazariyasi* kiradi. Ular bilan birgalikda *algoritmlar nazariyasi, axborot nazariyasi va kibernetika* faol rivojlana boshladi [20].

1930 yil boshida armiya kriptograflarini tayyorlashning keng miqyosli dasturi amalga oshirildi va Sovet Ittifoqida kriptografik xizmat xodimlari soni 500 nafarga ortdi. Bu Ikkinchi jahon urushi davrida muhim rol o‘ynadi. Lekin sovet shifrlari darajasi Enigmaga nisbatan ancha past bo‘lgan. Enigmadan Ikkinchi jahon urushining oxirigacha katta muvaffaqiyat bilan foydalanildi. U Ikkinchi jahon urushi davrida ittifoqchilar uchun katta to‘siqqa aylangan edi. Enigma shifrlarini samarali deshifrlash uchun har bir baraban ichidagi simlarning ulanishini bilish talab etilardi. Uning birinchi namunasi chizmalari bilan birgalikda Polsha razvedkasi tomonidan, ikkinchisi Norvegiya nemis bombardimonchi samolyotidan qo‘lga kiritilgan [10, 20].

1942 yilda Angliyada nemislarning shifrini deshifrlash maqsadida yaratilgan birinchi EHM «Koloss» Enigma shifrini 1.5 soat mobaynida deshifrlashning uddasidan chiqqan.

1941 yil dekabr oyida AQShning ikkinchi jahon urushiga qo‘shilishi munosabati bilan AQSh radiorazvedka va kriptotahlil xizmatining ish ko‘lami ortib ketdi. Ular tomonidan dushmanning oshkora va shifrlangan radioxabarlari tutib olinib, ularni baholash va ulardan foydalanish uchun harbiy razvedka boshqarmalariga yuborilar edi. Ikkinchi jahon urushi yillarida amerikalik kriptotahlilchilar tomonidan dushman tomonining bir qator kod va shifrlari deshifrlangan. 1942 yilda Yaponiyaning Harbiy Dengiz Kuchlari shifri deshifrlangan, 1943 yilda esa yapon armiyasi shifrlari fosh etilgan. Amerikada tezkorligi bo‘yicha inglizlar foydalangan EHMdan ustun RAM yuzaga kelgach, Arlington-Xoll va Bletchli-Park orasida maxsus aloqa kanali o‘rnatildi. Bu kanal orqali Buyuk Britaniyadan ingliz radiorazvedkasi tomonidan tutib olingan Enigma shifrmatnlari uzatilar edi. 1943 yil iyuldan 1945 yil yanvarigicha Arlington-Xollga

1357 nemis shifrlari kelib tushgan, ulardan 413 tasi muvaffaqiyatli deshifrlangan.

Amerikalik kriptologlar 1943 yilda «odamxo‘r-qo‘mondon» deb nom qozongan admiral Yamomatoning (Yamomato shaxsan o‘zi Perl Xarboredagi operasiyaga boshchilik qilgan) yagona samolyotini qo‘lga tushirib yo‘q qilganliklarini o‘zlarining eng katta yutuqlari deb biladilar [10, 20].

Ikkinchi jahon urushida Devid Kan yozishicha I jahon urushi davridagi «Sovet shifrlash xizmati ko‘z yoshlari to‘la tajribasini asosan hisobga oldi». Bu haqida 22 iyun 1941 yilda harbiy qismlararo kriptogrammalar almashishi tarixi guvohlik beradi [20-21]. Sovet Ittifoqiga Germaniyaning qo‘qqisdan hujumidan so‘ng bir zumda Qizil Armiyaning yetakchi postlaridan biri ochiq matnda «Bizni otmoqdalar. Nima qilaylik?» deb mamlakat ichkarisiga qilgan murojaatiga «Sizlar aqldan ozibsiz! Nega xabaringiz shifrlanmagan» degan javob qaytarilgan. Ikkinchi jahon urushi davrida Qizil Armiya shifrlash xizmati asosan «qayta shifrlash kodlari»dan foydalangan. Qayta shifrlash maxsus kod kitobidan foydalanishga asoslangan bo‘lib, unda har bir so‘z raqamlar kombinasiyasi bilan almashtirilgan. Masalan, «Batariya - o‘t och!» buyrug‘i va shunga o‘xshash buyruqlar uchun bu qulay, «ataka», «diviziya» so‘zlari 032, 1458 kodlari bilan almashtirilgach, kodga biror gamma qo‘shish (XOR amali asosida) orqali u qayta shifrlanib rasiya orqali uzatilgan. Agar rasiya orqali kod to‘g‘ridan-to‘g‘ri uzatilsa, 1914 yildagi hol yuz bergan bo‘lar edi, chunki kod kitobi matn statistikasini yashira olmaydi.

Sovet Ittifoqiga qarshi nemis razvedkasi samaradorligi past bo‘lgan. Ular strategik nuqtai nazardan arzigulik muvaffaqiyatga erishmaganlar. Nemislar Oliy Sovet Harbiy Qo‘mondonligining yozishmalarida foydalanilgan shifr tizimlarini buzib ochishga qodir bo‘lmaganlar. Bejiz nemis kriptograflaridan biri «Rossiya efirda Birinchi jahon urushida mag‘lub bo‘lgan bo‘lsa-da, Ikkinchi jahon urushi davrida revansh olishga muvaffaq bo‘ldi, deb tan olmagan. Ayniqsa, Sovet razvedkachilarining shifr yozishmalarini deshifrlash mumkin bo‘lmagan. Ularning ko‘pchiligi u davr uchun standart sanalgan shifr san’atining cho‘qqisi bo‘lgan. Foydalanilgan shifr rus inqilobchilari ishlatgan eski shifr tizimida qo‘shimcha bir marotabalik

gammalash amalini qo‘llash orqali takomillashtirilgan. Uni Moskvada absolyut bardoshli shifr bo‘lgan deb hisoblashadi.

Ikkinchi jahon urushi tugagach Sovet Ittifoqi G‘arb bilan jiddiy muholifatga yuz tutdi. Bu o‘z navbatida Sovet Ittifoqi kriptologiyasining rivojlanishiga katta hissa qo‘shib yangi zamonaviy kriptografiya fanining rivojlanish bosqichini boshlab berdi.

Ilmiy kriptografiya davrining muhim muvaffaqiyatlari ro‘yxati boshida Klod Elvud Shennonning *«Maxfiy tizimlarda aloqa nazariyasi»* (1949) asari turadi [15, 20]. Unda axborot muhofazasining nazariy tamoillari shakllantirib berilgan.

K.E. Shennon tomonidan qilingan bunday kashfiyot, albatta, uning elektrotexnika va matematika bo‘yicha chuqur bilimlari va bundan bir yil oldin u yaratgan axborot nazariyasi fani tufayli yuzaga kelgan edi. U nafaqat Vernamning tasodifiy shifrini buzib ochib bo‘lmasligini, balki himoyalangan kanal orqali uzatiladigan maxfiy kalit miqdori (bitlar soni) chegaralarini ham aniq ko‘rsatib berdi. U cheklanmagan resurslarga ega bo‘lgan kriptotahlilchi biror «tasodifiy shifr»ni ochishida maxfiy kalitni topishi uchun zarur bo‘lgan shifrlangan matndagi simvollar soni *s* quyidagicha ifodalanishini ko‘rsatdi:

$$S = H(k)/(r*Log\ n)$$

bu yerda: *H(k)* - kalit entropiyasi, ya’ni kalitning har bitta simvoliga to‘g‘ri keladigan axborot miqdori, *r* - ochiq matnning seriboraligi (ruscha, izbitochnost), *n* - alifbo hajmi.

Keltirilgan ifoda umumiy holda isbotlanmagan bo‘lsa-da ma’lum xususiy hollar uchun to‘g‘ri. Bundan quyidagi muhim xulosa kelib chiqadi: kriptotahlilchining ishini nafaqat kriptotizimni mukammallashtirish orqali, balki shifrlanadigan matnning seriboraligi nolgacha pasaytirilsa, kriptotahlilchi kichik kalit bilan shifrlangan matnni ham ocha olmaydi. Demak, shifrlash oldidan axborotni statistik kodlash (zichlashtirish, arxivlash) lozim. Bunda axborotning hajmi va seriboraligi kamayadi, entropiyasi oshadi. Chunki, ixchamlashgan matnda qaytariluvchi so‘zlar va harflar kamayib shifrni buzib ochish qiyinlashadi.

K. Shennon kriptotizimlar bardoshliligini *nazariy* va *amaliy* turlarga ajratadi. Nazariy bardoshlilik deganda raqib tomonning tahlilchisi u qo‘lga tushirgan kriptogrammalarni tahlillashda

cheklanmagan vaqtga va barcha zarur vositalarga ega bo‘lgan holda kriptotizimning bardoshliligi tushuniladi. Amaliy bardoshlilik deganda kriptotahlilchining vaqti va hisoblash imkoniyatlari cheklangan holga oid bardoshlilik tushuniladi. K. Shennon amaliy shifrlarda ishlatiladigan ikki tamoyilni ajratadi. Bular *yoyish va aralashtirishdir*. Yoyish deganda, ochiq matnning bitta simvolini shifrlangan matnning ko‘p simvollariga ta’sir etishi tushuniladi. Bu ochiq matnning statistik xossalarini yashirishga imkon beradi. Bu tamoyil kalit simvollariga nisbatan ham qo‘llaniladi. Aralashtirish deganda, K. Shennon shifrlanadigan va shifrlangan matnlar statistik xossalarining bir-biriga bog‘lanishini tiklashni qiyinlashtiruvchi shifrlashga oid o‘zgartirishlarni nazarda tutgan.

K. Shennonning ilmiy kriptologiya asoslarini o‘zida mujassamlashtirgan maqolasi bu sohada ochiq tadqiqotlarning sezilarli o‘sishiga turtki bo‘la olmadi. Chunki, birinchidan, maxfiy aloqa tizimlarining nazariy bardoshlilik nazariyasi o‘z mohiyatiga ko‘ra to‘la edi. Unga ko‘ra nazariy jihatdan bardoshli maxfiy tizimlarni hosil qilish uchun himoyalangan kanallar bo‘ylab haddan tashqari katta hajmdagi kalitlarni uzatish lozim bo‘lardi. Ikkinchidan, amaliy bardoshlilik masalalarini yechish mavjud kriptografiya usullarini takomillashtirish bilangina cheklanib qoldi.

K. Shennonning «yaxshi» shifr yaratish muammosi ma’lum shartlarni qondiruvchi eng murakkab masalalarni topishga keltiriladi. «Bizning shifrimizni shunday tuzish mumkinki, uni buzib ochish yechilishi katta hajmdagi ishlarni talab qilishi ma’lum bo‘lgan muammoni o‘z ichiga olsin yoki unga ekvivalent bo‘lsin» luqmasi yana chorak asr e’tiborsiz qoldi.

Devid Kanning «Kriptograflar» asari kriptografiya tarixi bo‘yicha mumtoz asar bo‘lib qolgan. Bu asar XX asrning 70 yillari oxirigacha ham Davlat Xavfsizligi Nazoratining maxsus kutubxonasida saqlanib undan foydalanishga ruxsati bo‘lgan kimsalar davrasi «ideologik mulohazalar asosida» jiddiy cheklangan. Unda Rossiya haqidagi bo‘limda «Maxfiy polisiyaning vazifalaridan biri bo‘lib yo‘qsillar diktaturasini yo‘qsillarning o‘zidan muhofaza qilish bo‘lgan» deyiladi. Bu XX asrning 70 yillarida ham qo‘rqinchli sir bo‘lgan [16, 20].

Ikkinchi jahon urushi tugagach, sovet kriptograflaridan undan kam bo‘lmagan kuchlarni sarflashni talab etgan «sovuq urush» davri boshlandi.

Bu davrda harbiy kriptografik xizmatning ko‘plab ilmiy xodimlari harbiy xizmatdan bo‘shatilgan edi. Bu sharoitlarda harbiy chaqiriq yoshida bo‘lgan yuqori malakali kriptograflar «xalqlar otasi»ga to‘g‘ridan-to‘g‘ri murojaat etishga o‘zlarida jasurlik topdilar va ularning murojaatiga e’tibor berildi.

1949 yil kuzida Sovet kriptografiyasi uchun katta ahamiyatga ega bo‘lgan Butunittifoq kommunistik bolsheviklar partiyasi qarorlari qabul qilindi. Qarorga muvofiq, bir-biriga bog‘lanmagan bo‘linmalar asosida Butunittifoq kommunistik bolsheviklar partiyasi Markaziy komiteti Maxsus xizmat bosh boshqarmasi tashkil etildi va uning oyoqqa turishi va rivojlanishi uchun vosita va katta mablag‘lar ajratildi; kriptografiya xizmati tezkor vazifalarni bajarish, hamda yangi yuqori malakali kadrlarni tayyorlash uchun eng kuchli olimlarni jalb etish choralari ko‘rildi, bu maqsadga erishish uchun kriptograflar oliy maktabi va Moskva Davlat Universiteti mexanika-matematika fakultetining yopiq bo‘linmasi tashkil etildi.

Bu qarorlar amalga oshirila borilib, 3 yil ichida Sovet kriptografiyasining siymosi batamom yangilandi.

Shu o‘rinda kriptografiyaga Sovet rahbariyati munosabatini tasavvur etish uchun Mixail Maslennikov [21] xotiralaridan parcha keltirish o‘rinli. U 1949 yil Moskva aviasiya institutini tamomlagandan so‘ng Ilyushin konstruktorlik byurosiga ishga jo‘natilgach, bir yildan so‘ng kriptografiya bo‘yicha o‘qishga tanlangan va 1800 rubl stipendiya bilan ta’minlangan. Uning podpolkovnik D. SHukin bilan bo‘lib o‘tgan suhbati alohida e’tiborga loyiq. «Biz kriptograflarmiz, shifrlar bilan maxfiy aloqa sohasida ishlaymiz. Lekin, o‘rtoq Stalin bizga ham «Hammani o‘qish, lekin bizning suhbatlar va yozishmalarni hyech kim o‘qiy olmasligi zarur»ligi vazifasini qo‘ydi. D. SHukin suhbatdoshiga telegraf aloqasini maxfiylashtirish uchun maxsus texnika yaratish bilan shug‘ullanishini, lekin bu haqda hyech kim na onasi, na yaqin do‘stlaridan birortasi bilmasligi zarurligini uqtirgan. Bundan bu davrlarda kriptografiya bilan shug‘ullanganlar ham maxfiy sir

saqlanishi va ular yetarli darajada iqtisodiy himoyalanganligi koʻrinib turibdi.

XX asrning 60 yillariga kelib kriptografik maktablar rotor kriptotizimlarga nisbatan bardoshliligi yuksak boʻlgan blokli shifrlar yaratishgacha yetib keldilar.

Kriptografiya tarixi boʻyicha birinchi asar Devid Kannning «Kod buzuvchilar» monografiyasi boʻldi. AQShda XX asrning 60 yil oxirlarida yuzaga kelgan bu asar kriptologiya sohasidagi birinchi fundamental ish boʻlib, u uzoq vaqt davomida kriptologiyaga bagʻishlangan umumiy tadqiqot yoʻnalishlarini aniqlab berdi. Ammo bu ish har tomonlama kriptologiyani qamrab olgan deyish qiyin, chunki u kriptologiyaning bir yoʻnalishi boʻlgan kriptotahlilni asos qilib olgan. Kanning bu asarida kriptotahlilning nazariy asoslari va uni amaliyotda qoʻllash koʻrib oʻtilgan. Lekin bu asarning ahamiyati shundaki, muallif oʻquvchilarni kriptologiyaning asosiy tushunchalari bilan tanishtirib oʻtgan. Kanning bu asari faqat tadqiqotchilar uchun emas, balki keng kitobxonlar ommasi uchun moʻljallangan ilmiy asar hisoblanadi.

1.2.4. Kompyuter kriptografiyasi davri

Kompyuter kriptografiyasi davri XX asrning 70 yillarida avvallari qoʻlda bajarib kelingan, undan soʻng mexanik va elektromexanik qurilmalar yordamida amalga oshirilgan shifrlar oʻrniga ulardan haddan ziyod yuqori kritobardoshlilikka va tezkorlikka ega kriptotizimlar yaratishga yangicha yondashuvlarni amalga oshirishga qodir boʻlgan elektron hisoblash mashina (kompyuter)larning yuzaga kelishi bilan xarakterlanadi. Yuqori quvvatli va ixcham kompyuterlarning paydo boʻlishi axborot texnologiyalarining misli koʻrilmagan rivojiga, kompyuter va kommunikasiya tarmoqlarining, Internet tarmogʻining keng quloch yoyishiga, aloqa vositalarining raqamlashishiga olib keldi va axborot xavfsizligi muammosi yanada dolzarb muammolar qatoridan joy oldi. Natijada kriptologiyada ikkita *muhim voqyea* sodir boʻldi [22].

Kompyuter kriptografiyasi davrining *birinchi muhim voqyeasi* simmetrik kriptotizimlarning birinchi sinfi boʻlgan blokli shifrlar yuzaga kelib, ular tarixda birinchi marta Davlat standarti maqomiga

ega bo‘lishi bo‘lsa, davrning ahamiyatga molik *ikkinchi tamoyilli muhim kashfiyoti* kriptologiyaga yangicha yondashuvlarni boshlab bergan oshkora kriptografiyaning yuzaga kelishidir.

Bu davrdan boshlab kriptografik tizimlar ikkita sinfga bo‘lina boshladi: *simmetrik (maxfiy kalitli, bir kalitli)* va *nosimmetrik (oshkora (ochiq) kalitli, ikki kalitli) kriptotizimlar.* O‘z navbatida simmetrik kriptotizimlar miloddan avvalgi davrlardan ma’lum bo‘lib, ular oqimli va blokli shifr turlariga bo‘linadi.

1.2.4.1. Simmetrik kriptotizimlar

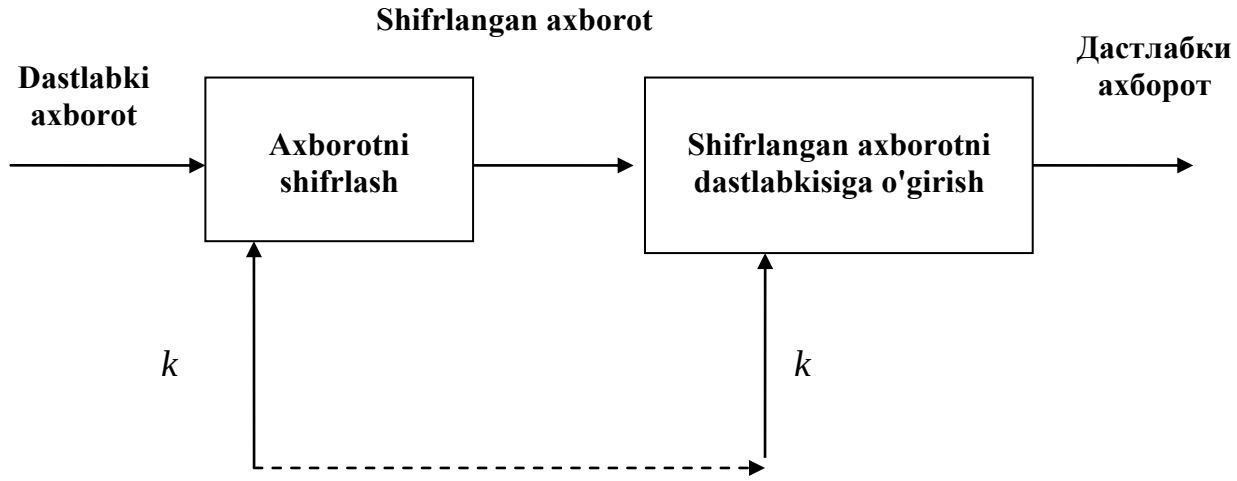
Simmetrik kriptotizimlarning ilmiy nazariyasi yaratilishi va amaliyoti rivojiga ilmiy kriptografiya asoschisi K. Shennon, A.N. Kolmogorov va formal kriptografiya namoyandalari O. Kerxgoff, Ch. Bebbidj, U. Fridman, G. Vernam, E. Xebern va boshqalar katta hissa qo‘shgan [23].

Axborot uzatish va saqlash jarayonlarining raqamlashtirilishi uzlukli (nutq) va uzluksiz (matn, faks, teleks, tasvir, animasiya) axborotlarni muhofazalash uchun yagona algoritmlardan foydalanish imkonini beradi. Shifrlash algoritmlariga quyidagicha asosiy talablar qo‘yiladi:

- shifrlangan axborotni o‘zgartirib qo‘yish yoki uning shifrini buzib – ochishga yo‘l qoldirmaslik;
- axborot muhofazasi faqat kalitning ma’lumligiga bog‘liq bo‘lib, algoritmning ma’lum yo noma’lumligiga bog‘liq emas (O.Kerkgoff qoidasi);
- dastlabki axborot (ma’lumot)ni yoki kalitni biroz o‘zgartirish shifrlangan matnning butunlay o‘zgartirib yuborishi lozim (K. Shennon tamoyili, “o‘pirilish” hodisasi);
- kalit qiymatlari sohasi shunday katta bo‘lishi kerakki, undan kalit qiymatlarini bir boshdan ko‘rib chiqish asosida shifrni buzib ochish imkoni bo‘lmasligi lozim;
- algoritm iqtisodiy jihatdan tejamli va yetarli tezkorlikka ega bo‘lishi lozim;
- shifrmatnni buzib ochishga ketadigan sarf-xarajatlar axborot bahosidan yuqori bo‘lishi lozim [23-24].

Kriptografik tizim, yo qisqacha, kriptotizim, shifrlash hamda shifrni ochish algoritmlari, bu algoritmlarda ishlatiladigan kalitlar, shifrlanadigan hamda shifrlangan matnlar va bularning o‘zaro moslashish qoidalarini o‘zida mujassamlantirgan protokol (bayonnoma)dan iborat majmuadir.

Kriptotizimdan foydalanishda matn muallifi shifrlash algoritmi va shifrlash kaliti vositasida avvalo dastlabki matnni shifrlangan matnga o‘giradi (1.9-rasm). Matn muallifi uni o‘zi foydalanishi uchun shifrlagan bo‘lsa (bunda kalitlarni boshqaruv tizimiga hojat ham bo‘lmaydi) uni saqlab qo‘yadi va kerakli vaqtda shifrlangan matnni ochadi.



1.9- rasm. Simmetrik kriptotizimlarda axborot almashish

Ochilgan matn asli (dastlabki matn)ga aynan bo‘lsa, saqlab qo‘yilgan axborotning yaxlitligiga ishonch hosil bo‘ladi. Aks holda axborot butunligi buzilgan bo‘lib chiqadi Bu yerda *k* – yuboruvchi va qabul qiluvchining simmetrik maxfiy kaliti.

Agar shifrlangan matn uni yaratgan kimsadan o‘zga qonuniy foydalanuvchiga (oluvchiga) mo‘ljallangan bo‘lsa, u tegishli manzilga jo‘natiladi. So‘ngra shifrlangan matn oluvchi tomonidan unga avvaldan ma’lum bo‘lgan shifrni ochish kaliti va algoritmi vositasida dastlabki matnga o‘giriladi.

Kriptograflar orasida mashhur bo‘lgan ma’lumotlarni shifrlash algoritmlari guruhiga AQSh davlat standartlari – DES [11, 25], AES [26], Rossiya Federasiyasi davlat standarti GOST 28147-89 [27], IDEA [11, 25], FEAL [11, 25] kiradi.

DES IBM firmasining butun bir kriptograflari guruhi tomonidan ishlab chiqilgan [11, 25]. Ma’lumotlarni shifrlash standarti 1976 yil 23 noyabrda Milliy Standartlar Byurosi tomonidan AQShning davlat standarti sifatida qabul qilingan va u 1977 yil iyul oyidan 2000 yil oktyabr oyigacha raqamli ma’lumotlarni shifrlash uchun standart bo‘lib xizmat qilgan. Hozirgi vaqtda u faqat nazariy ahamiyatga ega. DES zanjirsimon tuzilmali muvozanatlangan Feystal tarmog‘i arxitekturasiga ega. Mutaxassislarning fikriga ko‘ra bu standart yoyish va aralashtirish tamoyillariga asoslangan eng yaxshi kriptoalgoritmlardan biridir. Shifrlash algoritmida shifrmatnning har bir biti dastlabki matn va kalit barcha bitlarining funksiyasi bo‘ladi. Standartda o‘rniga qo‘yish, o‘rin almashtirish va 2 modul bo‘yicha qo‘shish amallarining kombinasiyasidan foydalaniladi.

GOST 28147-89 - sobiq Sovet Ittifoqida ishlab chiqilgan DES kabi muvozanatlangan Feystal tarmog‘i [27] arxitekturali *64*-bit blokli va kalit uzunligi *256* bit bo‘lgan kriptografik o‘zgartirish algoritmidir [27]. Algoritm bosqichlari soni *32* ga teng bo‘lsa-da, u DESga nisbatan tezkordir.

Shifrmatnni dastlabki matnga o‘girish ham xuddi dastlabki matnni shifrmatnga o‘girish kabi bajariladi, faqat bunda kalitlar ketma-ketligi o‘zgartiriladi.

GOST 28147-89da DES, AYeSga xos elektron kod kitobi rejimiga juda o‘xshash oddiy almashtirish rejimi, DES, AYeSga xos rejimlardan biroz farqli bo‘lgan gammalashtirish, teskari bog‘lanishli gammalashtirish rejimlari va ulardan tamoyilli farqli imitoqistirma ishlab berish rejimidan foydalanadi.

GOST 28147-89 algoritmi DESga nisbatan ancha yuqori kriptobardoshlilikni ta’minlaydi. Bu kungacha u eng samarali hisoblangan differensial va chiziqli kriptotahlil usullariga nisbatan yetarli darajada kriptobardoshli sanaladigan algoritmlardan biridir. Bu asosan, DESga nisbatan uzun, ya’ni 256 bitli kalitdan va S-bloklarga tegishli deyarli 354 bit (S-blok generasiyalovchilar va foydalanuvchilar guruhidan o‘zgalar uchun) maxfiy ma’lumotdan foydalanilishi bilan izohlanadi.

AES algoritmida kirish va chiqish bloklari uzunligi *128* bit shifrlash kalitining uzunligi *128*, *192* yoki *256* bit etib belgilandi.

Shifrlashda qo‘llaniladigan barcha almashtirishlar yoyilish va tarqalish tamoyillarini amalga oshirishga qaratilgan. Standartda blok va kalitning uzunligiga bog‘liq ravishda bosqich (raund)lar soni 10 dan 14 gacha belgilab qo‘yildi.

Shifrlash prosedurasi bosqich kalitlarini generasiyalash prosedurasini ham, bosqichlar soniga mos uzunlikdagi shifrmatnga o‘girish (dastlabki matnga o‘girish) uchun bosqich kalitlarini yuklashni ham o‘z ichiga oladi.

Shifrmatnni dastlabki matnga o‘girish amallarni inversiya (teskari) tarzida bajarish orqali amalga oshiriladi.

Hozirgi kungacha AES yuqori kriptobardoshlilikka ega bo‘lgan shifrlar qatoriga kiradi.

IDEA – yana bir *64*-bitli blokli shifrlash algoritmi bo‘lib, kalitining uzunligi *128* bitga teng [11, 25]. IDEA shifrining birinchi varianti Ksuyedji Lay va Djeyms Massi tomonidan *1990* yilda taklif etilgan. U tezligi bo‘yicha DES algoritmidan qolishmaydi, kriptotahlilga bardoshliligi jihatidan esa undan ham ustun.

IDEAda dastlabki matnni shifrmatnga o‘girish va shifrmatnni dastlabki matnga o‘girishda yagona algoritmdan foydalaniladi.

IDEA algoritmida ham boshqa blokli shifrlash algoritmlaridagi kabi aralashtirish va yoyish tamoyillari yetarli darajada amalga oshirilgan. Uning asosida “turli algebraik gruppalarning amallarini birlashtirish” falsafasi yotadi. Unda uch algebraik gruppa aralashtirilgan va ularning barchasi ham qurilma, ham dastur ko‘rinishida oson amalga oshiriladi.

Shifrni ochish amali ham xuddi shifrlash amali kabi bajariladi, bunda faqat qism kalitlar biroz o‘zgartiriladi.

FEAL algoritmi yapon mutaxassislari Akixiro Shimuzu va Shodji Miyaguchi tomonidan taklif etilgan bo‘lib, unda kirish va chiqishda *64*-bitli bloklardan va *64*-bitli kalitdan foydalaniladi [11, 25]. Uning maqsadi DESga nisbatan kuchli algoritm yaratishdan iborat bo‘lgan, lekin pirovardida bu algoritm boshlang‘ich maqsaddan uzoqlashib ketgan.

FEAL algoritmi differensial va chiziqli kriptotahlilga nisbatan yetarli kriptobardoshlilikni ta’minlay olmaganligi ma’lum [11, 25]. Shu bois, u asosan kriptotahlilchilar orasida mashhur, chunki kimda-

kim yangi kriptotahlil usulini yaratsa, uni avvalo **FEAL** algoritmi uchun sinab koʻrishi odat tusiga kirgan.

Oʻz DSt 1105:2005 va **Oʻz DSt 1105:2009** «Axborot texnologiyasi. Axborotning kriptografik muhofazasi. Maʼlumotlarni shifrlash algoritmi» (MShA)da modul arifmetikasining diamatrisalar algebrasidan foydalaniladi, bunda hisoblashning qiyinlik darajasi matrisalar algebrasidagi singari bajariladi [23, 28].

Shifrmatnga oʻgirish va dastlabki matnga oʻgirish proseduralarida foydalaniladigan diamatrisalar algebrasining asosiy amali diamatrisani *p* modul boʻyicha diamatrisaga teskarilash amali hisoblanadi. Bu amallarda ikki oʻlchamli seans kaliti massivining maxsus tuzilmali *4x4* tartibli kvadrat diamatrisa bilan aks ettiriluvchi qismlari ishtirok etadi. Maxsus tuzilmali diamatrisaning muhim xossasi diamatrisaning diaaniqlovchisini hisoblash formulasining soddaligidir, bu esa diamatrisani teskarilash shartlarini tekshirish ishlarini soddalashtiradi.

Maxsus tuzilmali diamatrisani teskarilash shartlarini tekshirish MShA parametrlariga qoʻyiladigan asosiy talab hisoblanadi. MShAda shuningdek butun sonlarni parametrli koʻpaytirish, teskarilash va darajaga oshirish deb atalgan parametrli gruppa amallaridan ham foydalaniladi. MShA belgilab qoʻyilgan ikki xil - *256* va *512* bit uzunlikdagi kalitlar yordamida amalga oshiriladi.

Barcha yuqorida bayon etilgan GOST 28147-89dan boshqa algoritmlar boʻyicha maʼlumotlarni shifrlashda 5 xil ish rejimini qoʻllash mumkin [27]: elektron kod kitobi; shifr bloklarning ilashishi; chiqish orqali teskari bogʻlanish; shifrmatn orqali teskari bogʻlanish (teskari bogʻlanishli gammalashtirish); sanoqchi. Tabiiyki, har bir ish rejimining oʻziga xos afzalligi va kamchiligi boʻladi. Masalan, kalitlarni shifrlashda elektron kod kitobi ish rejimini, alohida belgilar uchun shifr matn orqali teskari bogʻlanish ish rejimini, aloqa tizimida (odatda, biror shifrmatnni takror uzatish imkoniyati boʻlmaganda) chiqish orqali teskari bogʻlanish ish rejimini qoʻllash qulay hisoblanadi.

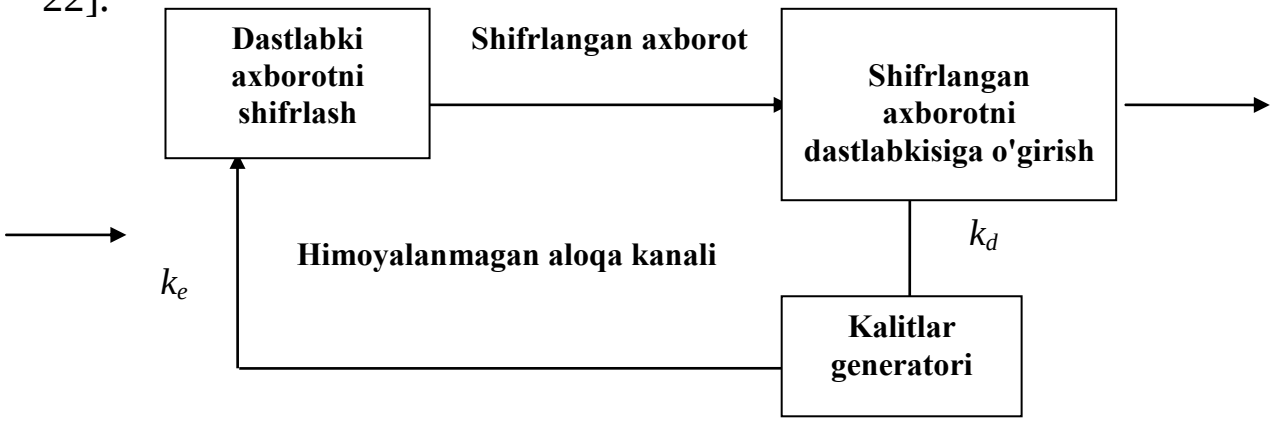
1.2.4.2. Nosimmetrik kriptotizimlar

Nosimmetrik kriptografik tizimlar yaratish tamoyili jahon kriptografiya tarixida ilk bor bundan 35 yil muqaddam amerikalik

olimlar Uitfild Diffi va Martin Xellman [29-30] tomonidan taklif etilgan bo‘lib, ular katta sonli chekli to‘plamlarda bir tomonlama funksiyalardan foydalanishga asoslangan. U. Diffi va M. Xellmanning 1976 yilda bosilib chiqqan “Kriptologiyada yangi yo‘nalishlar” maqolasida ilgari surilgan ”maxfiy kalitni uzatishni talab etmaydigan amaliy bardoshli maxfiy tizimlarni tuzish mumkin” degan fikri kriptologiyada nosimmetrik kriptotizimlarning yuzaga kelishi hamda ularning rivojlanish davrining boshlanishiga sabab bo‘ldi. U. Diffi va M. Xellman maqolasining hal qiluvchi hissasi ikkita ta’rifda mujassamlangan. Bular «bir tomonlama funksiya» va «yashirin yo‘lli bir tomonlama funksiya «tushunchalaridir.

Nosimmetrik kriptotizimlar nazariyasi va amaliyoti rivojiga U. Diffi va M. Xellman [29-30] bilan bir qatorda R. Rayvest, A. Shamir, L. Adleman [31-36], El Gamal [37-38], K. Shnorr [39-41], N. Koblis [42-44], A. Menezes [45-46], B. Shnayer [11, 25, 47] va boshqalar katta hissa qo‘shgan.

Shifrlash va shifr ochish kalitlari o‘zaro funksional bog‘langan bo‘lib, ulardan biri asosida ikkinchisi amaliy jihatdan (mavjud hisoblash vositalari taraqqiyoti darajasida) hisoblab topilishi mumkin bo‘lmagan va ulardan biri faqat aloqa ishtirokchisiga ma’lum bo‘lib, boshqalardan maxfiy tutiladigan, ikkinchisi esa aloqa ishtirokchilarining hammasiga oshkora bo‘lgan kriptotizim *nosimmetrik (oshkora kalitli) kriptotizim* deb ataladi (1.10-rasm) [2, 22].



1.10- rasm. Nosimmetrik kriptografik tizimda axborot uzatish jarayoni

Ushbu 1.10-rasmda nosimmetrik kriptografik tizimda axborot uzatish jarayoni aks etgan. Bu yerda k_e – qabul qiluvchining oshkora kaliti, k_d – qabul qiluvchining maxfiy kaliti.

Nosimmetrik kriptotizimda aloqa ishtirokchilarining har biri o‘zining shaxsiy maxfiy va oshkora kalitlari juftiga ega bo‘lib o‘z oshkora kalitini boshqa aloqa ishtirokchilariga e’lon qiladi. Shaxsiy maxfiy kalit qabul qilinadigan axborot konfidensialligini ta’minlash uchun yaratilganda shifrni ochish kaliti bo‘lib xizmat qiladi. Bunda kimga konfidensial axborot jo‘natiladigan bo‘lsa uning oshkora kalitidan foydalanib shifrlangan axborot jo‘natiladi. Bunday axborotning shifrini faqat yagona maxfiy kalit egasigina ocha oladi. Agar maxfiy kalit autentifikasiya maqsadida xabarlarga elektron raqamli imzo bosish uchun hosil qilingan bo‘lsa, u shifrlash kaliti sifatida foydalaniladi. Oshkora kalit esa yuqoridagi birinchi holda shifrlash kaliti bo‘lib, ikkinchi holda shifrni ochish (tekshirish) kaliti bo‘lib xizmat qiladi.

Nosimmetrik kriptotizimlar asosida simmetrik tizimlarda yechilmay qolgan kalit tarqatish va elektron raqamli imzo masalalarining yechimini izlash yo‘llarida U. Diffi va M. Xellman ko‘pgina takliflarni ilgari surganlar.

Oshkora kalitli kriptografiya asosida rivojlangan mamlakatlar orasida birinchi bo‘lib AQSh elektron raqamli imzo bo‘yicha milliy standart yaratishga kirishgan. Avvallari Milliy Xavfsizlik Agentligida ishlagan Devid Kravis DSA patenti egasi hisoblanadi. 1993 yil iyunda texnologiyalar va standartlar milliy instituti (NIST) DSA uchun patent lisenziyasini berishni taklif etgan. Aslida AQSh standarti DSAda 1985 yilda Toxir El Gamal tomonidan ishlab chiqilgan algoritm xususiyatlaridan va K. Shnorr g‘oyasi asosida imzo uzunligini qisqartirishga qaratilgan ikkinchi tub moduldan foydalanilgan. DSAning kriptobardoshliligi chekli maydonlarda butun sonlarni logarifmlash muammosi matematikada amaliy hisoblash nuqtai nazaridan hanuz yechilmaganligiga asoslanadi.

AQShdan keyin Yevropa davlatlari va Yaponiyada elektron raqamli imzo bo‘yicha qonun va dastlabki davlat standartlari qabul etildi. Boshqa oshkora kalitli kriptografiyaga asoslangan vositalar yaratildi, eksportga mo‘ljallangan axborot-kommunikasiya tizimlarida joriy etildi. Ko‘pchilik davlatlar, shu jumladan Hamdo‘stlik davlatlari ham oshkora kalitli kriptografiya vositalarini yaratishda AQShga ergashdilar. Bu oshkora kalitli kriptografiyaning dastlab AQShda yuzaga kelganligi bilan bog‘liq albatta. Ular axborot–

telekommunikasiya tarmoqlarida maxfiy axborotlarni xavfsiz uzatish va elektron raqamli imzo yaratishda o‘z milliy algoritmlaridan foydalanmoqdalar.

Ochiq kalitli kriptotizimlar axborot xavfsizligining ko‘plab muammolarini yechib berishga qodir bo‘lib, ularning muhim qo‘llanish sohalaridan biri *elektron raqamli imzo* (ERI) hisoblanadi.

Yuqorida keltirilgan kriptotizimlarning asosiy kamchiliklaridan biri, buzg‘unchi kriptotizim asosiga olingan muammoni yetarlicha aniq qo‘ya olganda va uning bu muammoni hal qilishga resurslari yetarlicha bo‘lganda, qabul qiluvchiga kelib tushgan raqamli imzo soxta bo‘lsa, imzolovchi shaxsda imzoning soxtaligini isbotlovchi dalillar va ma’lumotlarning yo‘qligidir. O‘zbekiston milliy standartlarini yaratishda bu kamchiliklarni bartaraf etishga e’tibor berildi va 2005-2009 yilllarda O‘zbekiston aloqa va axborotlashtirish agentligining «UNICON.UZ» - Fan-texnika va marketing tadqiqotlari markazi davlat unitan korxonasi O‘z DSt 1092:2005, O‘z DSt 1092:2009 «Axborot texnologiyasi. Axborotning kriptografik muhofazasi. Elektron raqamli imzoni shakllantirish va tekshirish jarayonlari» [48], O‘z DSt 1106:2009 Axborot texnologiyasi. Axborotning kriptografik muhofazasi. Xeshlash funksiyasi» [49] davlat standartlari ishlab chiqildi va O‘zbekiston standartlashtirish, metrologiya va sertifikatlashtirish agentligi tomonidan tasdiqlandi.

Ishlab chiqilgan elektron raqamli imzo algoritmi (ERIA)da ERIni shakllantirish jarayoniga ERIning haqiqiyligini tasdiqlash jarayonida qo‘llaniladigan seans kaliti prosedurasini kiritish bilan ERI soxtaligini aniqlashning zahiraviy yo‘li ham nazarda tutilgan.

Elektron raqamli imzo mexanizmi quyidagi jarayonlarni amalga oshirish orqali aniqlanadi:

- ERI va seans kalitini shakllantirish;
- ERI haqiqiyligini tasdiqlash.

Ishlab chiqilgan ERIA ikki asosiy rejim - seans kalitsiz va seans kalitli qo‘llaniladi:

Seans kalitli rejimda ERIAning kriptografik bardoshliligi ERIning ochiq kalitini generasiyalash jarayonida qo‘llaniladigan, darajaga ko‘tarish asosining maxfiyligiga asoslanadi. Bu elektron raqamli imzoni soxtalashtirish uchun diskret logarifmlash masalasining qo‘yilish imkoniyatini istisno etadi, chunki seans

kalitidan foydalanish, agar soxtalashtirish yuz bergan bo‘lsa, ERI soxtalashtirilganligini aniqlash imkonini beradi. Natijada ERIAning kriptobardoshliligi yetarli darajada yuqori bo‘ladi. Seans kalitisiz rejimda ERIAning kriptografik bardoshliligi diskret logarifmlash masalasi yechimining murakkabligiga, shuningdek boshqa unga o‘xshash algoritmlar kabi qo‘llaniladigan xesh-funksiyaning bardoshliligiga asoslanadi.

O‘z DSt 1092:2005, O‘z DSt 1092:2009da P.F. va X.P. Xasanovlar tomonidan taklif etilgan modul arifmetikasining ***yangi bir tomonlama funksiyasi*** qo‘llaniladi, bunda hisoblashlar qiyinlik darajasi bo‘yicha darajaga ko‘tarish amallari kabi yengil amalga oshiriladi, funksiyani teskarilash esa diskret logarifm muammosini yechish jarayonidagidan kam bo‘lmagan hisoblash sarflari va vaqt talab qiladi [48]. An’anaviy (klassik) bir tomonlama darajaga ko‘tarish funksiyasi ushbu bir tomonlama funksiyaning xususiy holidir.

Nazorat savollari

1. Kriptologiyaga ta’rif bering?
2. Kriptografiyaning kriptotahlildan farqi nima?
3. Axborotni shifrlash deganda nima tushuniladi?
4. Shifr va shifrmatn deb nimaga aytiladi?
5. Kriptografik o‘zgartirish deb nimaga aytiladi?
6. Alifbo deganda nimani tushunasiz?
7. Kriptografiya tarixi qanday davrlarga bo‘linadi?
8. Dastlabki kriptografiya davrining muhim jihatlari nimalardan iborat?
9. Formal kriptografiya davrining asosiy voqyealari nimalardan iborat?
10. Ilmiy kriptografiyaning rivojlanishida Klod Elvud Shennonning o‘rni qanday?
11. Kompyuter kriptografiyasi davrining muhim voqyealari nimalardan iborat?
12. Simmetrik kriptotizimlarning ilmiy nazariyasi asoschilaridan kimlarni bilasiz?
13. Oshkora kriptotizimlarning asosiy jihatlari nimalardan iborat?
14. Bir tomonlama funksiyalar haqida ma’lumot bering?

2. TO‘PLAM VA AKSLANTIRISHLAR

2.1. To‘plamlar

To‘plam matematikaning ko‘plab sohalarida boshlang‘ich - fundamental tushuncha hisoblanib, belgisi, xususiyati yoki xossalari bir xil narsalarning majmui tushuniladi [12-13, 50]. To‘plamni tashkil etuvchi narsalar to‘plamning elementlari deb yuritiladi.

Ushbu $x \in X$ ifoda x elementning X to‘plamga tegishli ekanligini bildiradi, aks holda $x \notin X$ ifoda bilan belgilanadi. To‘plam odatda biror alifboning bosh harfi bilan, uning elementlari figurali qavslar ichiga olingan yoki talqini berilgan kichik harflar bilan belgilanadi. Muhim ahamiyatga molik to‘plamlar uchun standart belgilardan foydalaniladi. **N, Z, Q, R** belgilari mos tarzda natural, butun, rasional va haqiqiy sonlar to‘plamlarini belgilashda foydalaniladi.

N – natural sonlar to‘plami: *1,2,…* ko‘rinishidagi butun musbat sonlar.

Z – butun sonlar to‘plami: *n, -n* va *0* ko‘rinishidagi sonlar, bu yerda *n* – natural son.

Q - rasional sonlar to‘plami: *p/q* ko‘rinishidagi sonlar, bu yerda *p* va *q* - butun sonlar va $0 \neq q$. Rasional sonlar sinfi barcha **Z** butun sonlar to‘plamini, shu bilan birga o‘z navbatida barcha **N** natural sonlarni ham o‘z ichiga oladi.

R – haqiqiy sonlar to‘plami: ushbu sinf rasional va barcha irrasional sonlarni o‘z ichiga oladi.

Agar har ikkala to‘plam ham bir xil elementlardan tashkil topgan bo‘lsa, berilgan X va Y to‘plamlar teng deyiladi, aks holda teng emas deyiladi.

Misol uchun:

$X = \{0;0;0;0\} = \{0;0;0;0\} = Y$, $X = \{0;0;0;0\} \neq \{0;0;0\} = Y$, ya’ni to‘plamlar elementlari soni teng emas.

Elementlari soni chekli (cheksiz) bo‘lgan to‘plam chekli (cheksiz) to‘plam deyiladi.

Har bir olingan $x \in X$ elementga bitta $\varphi(x) \in Y$ element mos kelib, har bir olingan $y \in Y$ elementga $\varphi(x) = y$ tenglikni qanoatlantiruvchi $x \in X$ element mos kelsa, unda berilgan X va Y

to‘plamlar o‘zaro bir qiymatli (biyektiv) φ - moslikka ega deyiladi, Bunday biyektiv moslik $\varphi: X \leftrightarrow Y$ ko‘rinishda ifodalanadi. Umuman olganda “φ- akslantirish X - to‘plam elementlarini Y - to‘plam elementlariga akslantiradi” iborasi: $\varphi: X \to Y$ ko‘rinishda ifodalanadi.

To‘plamlar bilan bog‘liq bo‘lgan tushunchalar, ta’rif va tasdiqlar juda keng tarqalgan bo‘lib, fan va texnikaning ko‘plab sohalariga tegishli bo‘lgan adabiyotlarda turli shakllarda keltirilganligi uchun, quyida ularni tartib raqamlarisiz keltiriladi.

Agar berilgan X - cheksiz to‘plamning elementlarini nomerlab chiqish mumkin bo‘lsa, ya’ni X - to‘plam bilan N - natural sonlar to‘plami o‘zaro bir qiymatli moslikka ega bo‘lsa, bu cheksiz to‘plam sanoqli deyiladi. Boshqa cheksiz to‘plamlar sanoqsiz deyiladi. Misol uchun, isbot qilish mumkinki, barcha rasional sonlar to‘plami sanoqli, $[0;1]$ - kesmadagi barcha haqiqiy sonlar to‘plami esa sanoqsizdir.

Berilgan chekli to‘plam elementlari soni uning quvvatini aniqlaydi. Elementlari soni n ta bo‘lgan X -to‘plamning quvvati n ga teng bo‘lib, $|X| = n$, deb ifodalanadi. Sanoqsiz to‘plamlar “kontinium” quvvatga ega deb ham yuritiladi.

To‘plamni aniqlash uning elementlarini bevosita ko‘rsatish bilan amalga oshiriladi. Bundan tashqari, to‘plamni, uning elementlari xususiyatlarini so‘zlar orqali yoritish:

M={i∈N: I –naturol son bo‘lib, 2 ga qoldiqsiz bo‘linadi}

yoki formulalar bilan ifodalash (rekursiv usul):

$$M = \{i \in N : i = 2k;\ k = 1,2,...\}$$

orqali aniqlash mumkin.

Agarda Y - to‘plamning har bir elementi X - to‘plamning ham elementi bo‘lsa, u holda Y - to‘plam X -to‘plamga qism to‘plam bo‘ladi va $Y \subseteq X$ ko‘rinishda ifodalanadi.

Agarda $Y \subseteq X$ bo‘lib, $Y \neq X$ bo‘lsa, u holda $Y \subset X$ ko‘rinishda ifodalanadi va Y -to‘plam X -to‘plamning xos qism to‘plami deyiladi.

Agar $Y \subseteq X$ va $X \subseteq Y$ bo‘lsa, u holda $Y = X$ bo‘ladi.

Birorta ham elementga ega bo‘lmagan to‘plam bo‘sh to‘plam deyiladi va $\varnothing$ belgi bilan ifodalanadi. Bo‘sh to‘plam $\varnothing$ ixtiyoriy to‘plamga qism to‘plam bo‘ladi va uning quvvati nolga teng, ya’ni $|\varnothing| = 0$.

Har qanday X va Y - to‘plamlar juftligi uchun quyidagi amallar aniqlangan:

1) yig‘indi $X \cup Y = \{x : x \in X \text{ ёки } x \in Y\}$;

2) kesishma (ko‘paytma) $X \cap Y = \{x : x \in X \text{ ва } x \in Y\}$;

3) ayirma $X \setminus Y = \{x : x \in X \text{ ва } x \notin Y\}$.

Bu amallar quyidagi xossalarga ega:

1) kommutativlik: $X \cup Y = Y \cup X$ va $X \cap Y = Y \cap X$;

2) assosiativlik: $(X \cup Y) \cup Z = X \cup (Y \cup Z)$ va $(X \cap Y) \cap Z = X \cap (Y \cap Z)$;

3) distributivlik: $X \cap (Y \cup Z) = (X \cap Y) \cup (X \cap Z)$

va $X \cup (Y \cap Z) = (X \cup Y) \cap (X \cup Z)$;

4) $(X \setminus Y) \cup (X \cap Y) = X$.

Agar $X \subseteq U$ bo‘lsa, u holda X - to‘plamning U - to‘plamga nisbatan to‘ldiruvchisi deb

$$\overline{X} = U \setminus X = \{x \in U : x \notin X \subseteq U\}$$

to‘plamga aytiladi.

Quyidagi munosabatlar o‘rinli:

$$\overline{X \cap Y} = \overline{X} \cup \overline{Y} \text{ i } \overline{X \cap Y} = \overline{X} \cap \overline{Y}.$$

Berilgan $X_1, X_2, \ldots, X_m$ - to‘plamlarning Dekart ko‘paytmasi deb, ushbu $X = X_1 \times X_2 \times \ldots \times X_m = \{(x_1, x_2, \ldots, x_m) = x \in X : x_i \in X_i\}$ - to‘plamga aytiladi. Matematik induksiya usulidan foydalanib $X_1, X_2, \ldots, X_m$ - to‘plamlar Dekart ko‘paytmasini tashkil etuvchi to‘plamning quvvati ushbu

$$|X_1 \times X_2 \times \ldots \times X_m| = \prod_{i=1}^{m} |X_i|$$

tenglik bilan aniqlanishini isbot qilish mumkin, ya’ni berilgan to‘plamlar Dekart ko‘paytmasini tashkil etuvchi to‘plamning quvvati ko‘paytuvchilar quvvatlarining ko‘paytmasidan iborat.

Berilgan X - to‘plam $\leq$ - munosabat bilan tartiblangan (chiziqli tartiblangan, to‘la tartiblangan) deyiladi, agarda $\forall a,b,c \in X$ - elementlar uchun quyidagi xossalar bajarilsa:

1) refleksivlik $a \leq a$;

2) antisimmetriklik – agar $a \leq b$ va $b \leq a$ bo‘lsa, u holda $a = b$;

3) tranzitivlik – agar $a \leq b$ va $b \leq c$ bo‘lsa, u holda $a \leq c$;

4) chiziqlilik – yoki $a \leq b$, yoki $b \leq a$.

Agar $\forall a,b,c \in X$ - elementlar uchun (1)-(3) xossalar bajarilsa, berilgan X - to‘plam qisman tartiblangan to‘plam deyiladi.

X - qisman tartiblangan to‘plamning *diagrammasi* (*Xaas diagrammasi*) deb, shu to‘plam elementlari juftliklarining $(a,b) \in X$ yoy (yo‘naltirilgan kesma) bilan bog‘langan ifodasini tekislikdagi tasviriga aytiladi. Graflar ta’rifida, X - qisman tartiblangan to‘plam – bu yo‘nalishga ega bo‘lgan graf bo‘lib, uning uchlari X - to‘plamdan iborat ekanligi, (a,b) - juftlik faqat va faqat ushbu $a \le b$ va $a \ne b$ - shartlar bilan birgalikda a va b elementlardan farqli bo‘lgan $a \le c \le b$ shartni qanoatlantiruvchi $c \in X$ element mavjud bo‘lmagandagina yoy tashkil etishi ta’kidlanadi.

Y - to‘plam berilgan X - qisman tartiblangan to‘plamning qism to‘plami bo‘lib, $a \in X$ bo‘lsin. U holda $a \in X$ bo‘lgan element Y - qism to‘plamning yuqori (quyi) chegarasi deyiladi, agarda barcha $b \in Y$ elementlar uchun $b \le a$ $(a \le b)$ shart bajarilsa. Y - to‘plamning yuqori chegarasi a uning aniq yuqori (quyi) chegarasi deyiladi, agarda Y - to‘plamning barcha *s*-yuqori (quyi) chegaralari uchun $a \le c$ $(c \le a)$ shart bajarilsa, $a = \sup Y$ $(a = \inf Y)$ deb belgilanadi.

Agar $\forall a,b \in X$ elementlar uchun $\sup(a,b) \in X$ hamda $\inf(a,b) \in X$ bo‘lsa, qisman tartiblangan to‘plam X *panjara* deyiladi.

To‘plamlarning xossalari bilan bog‘liq bo‘lgan kriptologiya masalalarini tahlil qilishda qo‘llaniladigan tushuncha va tasdiqlarni to‘plamlar nazariyasining amaliy tadbiqlari yoritilgan o‘quv qo‘llanmalaridan topish mumkin.

2.2. Akslantirishlar

Akslantirishlar berilgan to‘plamlar ustida amallar bajarish bilan ularning elementlari orasida moslik o‘rnatish jarayonini ifodalaydi. Akslantirishlarning xossalarini tahlil qilish bilan bog‘liq bo‘lgan ayrim tushuncha va ta’riflarni keltiramiz.

Berilgan φ-akslantirish (funksiya) X - to‘plamni Y - to‘plamga *bir qiymatli* akslantiradi deyiladi (va $\varphi : X \to Y$ ko‘rinishda belgilanadi), agarda har bir $x \in X$ elementga faqat bitta $y = \varphi(x) \in Y$ element mos qo‘yilsa. Bu yerda X - to‘plam φ-akslantirishning *aniqlanish sohasi*, *Y*

- to‘plam esa *qiymatlar sohasi*, *y*-element x-elementning *aksi*, *x*-element *y*-elementning *asli* deyiladi.

Agarda berilgan φ va ψ akslantirishlarning aniqlanish va qiymatlar sohalari to‘la ustma-ust tushib, $\forall x \in X$ element uchun $\varphi(x) = \psi(x)$ tenglik bajarilsa, bunday akslantirishlar *teng* deyiladi.

Ushbu $\varphi : X \to Y$ akslantirish berilgan bo‘lsin, u holda $\psi : X' \to Y$ akslantirish φ akslantirishning $X' \subseteq X$ to‘plamdagi *izi* deyiladi, agarda $\forall x \in X'$ uchun $\varphi(x) = \psi(x)$ tenglik o‘rinli bo‘lsa.

Berilgan $\varphi : X \to Y$ akslantirish uchun:

1) ixtiyoriy $x \in X$ uchun $\varphi(x) = y \in Y$ element mavjud bo‘lib, ba’zi $y \in Y$ elementlar uchun $\varphi^{-1}(y) = x$ tenglikni qanoatlantiruvchi $x \in X$ elementlar mavjud bo‘lmasa, bunday akslantirish *syuryektiv* yoki ustiga akslantirish deyiladi;

2) $x_1 \neq x_2$ bo‘lgan $\forall x_1, x_2 \in X$ elementlar uchun $y_1 = \varphi(x_1) \neq \varphi(x_2) = y_2$ shu kabi bo‘lsa, bunday akslantirish *inyektiv* akslantirish deyiladi.

3) bir paytning o‘zida ham *syuryektivlik* ham *inyektivlik* shartlari bajarilsa, bunday akslantirish *biyektiv* yoki *o‘zaro bir qiymatli* akslantirish deyiladi.

Ushbu $\varphi : X \to Y$ va $\psi : Y \to Z$ akslantirishlarning *ko‘paytmasi* (*kompozisiyasi*, *superpozisiyasi*) deb, $\sigma(x) = \psi(\varphi(x))$ tenglikni qanoatlantiruvchi $\sigma : X \to Z$ akslantirishga aytiladi hamda $\sigma = \psi \cdot \varphi$ ko‘rinishda ifodalanadi.

$\varphi : X \to X$ akslantirish X - to‘plamni *o‘zini-o‘ziga* akslantirish deyiladi.

$\forall x \in X$ element uchun $I(x) = x$ tenglikni qanoatlantiruvchi X - to‘plamni o‘zini-o‘ziga akslantiruvchi I - akslantirish *birlik* (*aynan*) akslantirish deyiladi.

Agar $\psi \cdot \varphi = \varphi \cdot \psi = I$ shart bajarilsa, berilgan $\varphi : X \to Y$ va $\psi : Y \to X$ -akslantirishlar *o‘zaro teskari* akslantirishlar deyiladi hamda $\psi^{-1} = \varphi, \ \varphi^{-1} = \psi$ deb yoziladi.

Teskarisi mavjud bo‘lmagan akslantirishlar *bir tomonlama* akslantirishlar deyiladi.

Biror $x \in X$ element uchun $\varphi(x) = x$ tenglik bajarilsa, bu element φ akslantirishning qo‘zg‘almas elementi deyiladi.

Elementlari soni *n* ta bo‘lgan X - to‘plamni o‘zini-o‘ziga biyektiv akslantiruvchi φ - akslantirish X - to‘plamda *n-darajali*

o‘rniga qo‘yish deyiladi. Agarda to‘plam $X=\{x_1,\ldots,x_n\}$ bo‘lsa, u holda φ- akslantirish quyidagicha:

$$\varphi=\begin{pmatrix} x_1,\ldots, & x_n \\ \varphi(x_1),\ldots,\varphi(x_n)\end{pmatrix}=\begin{pmatrix} x_1,\ldots,x_n \\ x_{i_1},\ldots,x_{i_n}\end{pmatrix},$$

yoziladi, bu yerda $(i_1,\ldots,i_n)$ - indekslar $(1,2,\ldots,n)$- sonlarning o‘rin almashtirishlaridan iborat.

Agarda o‘rniga qo‘yish akslantirishi φ ushbu $\varphi^{-1}=\varphi$ tenglikni qanoatlantirsa, u holda bu akslantirish *involyusiya* deyiladi.

X-to‘plamni o‘zini-o‘ziga akslantiruvchi φ- o‘rniga qo‘yish akslantirishi $x_i,x_j\in X$ elementlar uchun $\varphi(x_i)=x_j$ va $\varphi(x_j)=x_i$ tengliklarni qanoatlantirib, X-to‘plamning boshqa elementlari bu akslantirishga nisbatan qo‘zg‘almas elementlar bo‘lsa, bunday φ-akslantirish x_i va x_j elementlarning X-to‘plamdagi *transpozisiyasi* deyiladi.

2.3. Binar munosabatlar

Istalgan ikkita X va Y to‘plam uchun barcha $O\subset X\times Y$ qism to‘plamlar X va Y to‘plam o‘rtasidagi binar munosabat deb aytiladi [12].

X ga nisbatan ~ binar munosabat ekvivelentlik munosabati deyiladi, agarda barcha $x,x_1,x_2\in X$ uchun quyidagi shartlar bajarilsa:

1. $x\sim x$ (refleksivlik);
2. $x\sim x_1\Rightarrow x_1\sim x$ (simmetriklik);
3. $x\sim x_1$, $x_1\sim x_2\Rightarrow x_2\sim x$ (tranzitivlik).

Berilgan x ga ekvivalent bo‘lgan barcha elementlar qism to‘plami $H=\{x'\in X|x'\sim x\}\subset X$ x ni o‘z ichiga olgan ekvivalentlik sinfi deyiladi.

$x\sim x$ (1-shart) bajarilsa, u holda $x'\in H$ bo‘ladi. $x'\in H$ ning istalgan elementi H sinfining vakili deyiladi.

Teorema. X kesishmaydigan qismto‘plamlar birlashmasi bo‘lib, ~ munosabat bo‘yicha ekvivalentlik sinfi to‘plami uning tarkibiy qismi hisoblanadi.

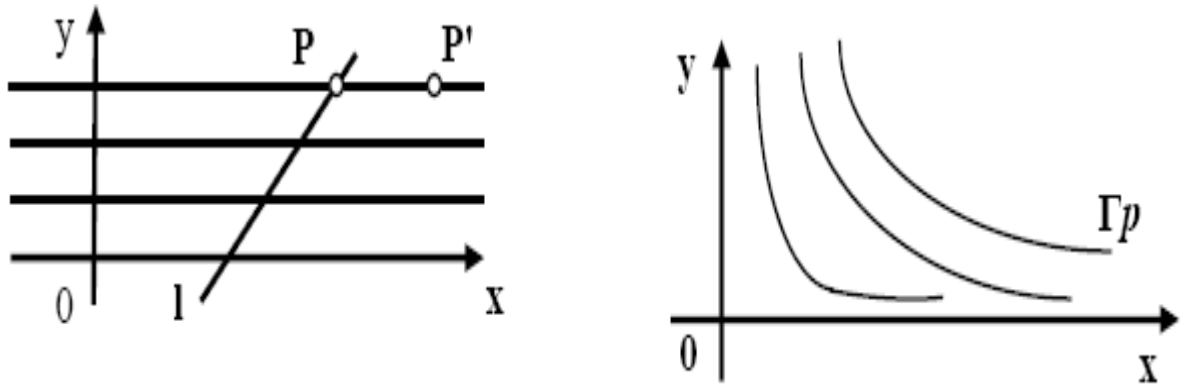
Isbot. $x\in H$ dan $X=\cup H_i$ kelib chiqadi. So‘ngra ixtiyoriy vakili orqali H aniqlab olinadi, ya’ni $H_i=H_j\Leftrightarrow x_i\sim x_j$. Bir tomonga: $x_i\sim x_j$ va

$x \in H_i \Rightarrow x \sim x_i \Rightarrow x \sim x_j \Rightarrow x \in H_j \Rightarrow H_i \subset H_j$ bajariladi. Ammo $x_i \sim x_j \Rightarrow x_j \sim x_i$ (2-shart). bo‘lgani uchun $H_j \subset H_i$ bajariladi. Demak $H_j = H_i$ ya’ni $x \in H$ bo‘lsa, u holda $H_i = H \Rightarrow x \in H_i \Rightarrow x \sim x_i$.

Agar $H_j \cap H_i \neq \varnothing$ va $x \in H_j \cap H_i$ bo‘lsa, u holda $x \sim x_i$ va $x \sim x_j$ bo‘ladi, tranzitivlik shartidan $x_i \sim x_j$ va $H_j = H_i$ ga ega bo‘linadi.. Demak turli sinflar kesishmaydi. Teorema isbotlandi.

Misol. To‘g‘riburchakli koordinatalar tizimida $V = R^2$ – tekislik berilgan bo‘lsin. U holda ~ xossasidan kelib chiqib P, $P' \in V$ nuqtalarning biror gorizontal to‘g‘ri chiziqqa tegishliligidan gorizontal to‘g‘ri chiziqlar sinfi bilan ekvivalentlik munosabati kelib chiqadi (2.1 a)-rasm).

$xy = p > 0$ shakldagi Gp giperbola $V_+ \subset V$ sohada $x > 0$, $y > 0$ koordinatali $P(x, y)$ nuqta bilan ekvivalentlik munosabatini aniqlaydi. (2.1 b)-rasm)



a) b)

2.1- rasm. Ekvivalentlik munosabati

2.4. Arifmetikaning asosiy teoremasi

Arifmetika natural sonlar xossalari bilan shug‘ullanuvchi fan bo‘lib, unda qadimdan asosiy e’tibor tub sonlarga qaratilib kelingan. Tub sonlarning fundamental xossasini *arifmetikaning asosiy teoremasi ochib beradi* [12].

Asosiy teorema. Birdan boshqa ixtiyoriy natural son tub son yoki tub sonlar ko‘paytmasi shaklida yoziladi, agar bu ko‘paytmada ko‘paytuvchilarning o‘rni e’tiborga olinmasa, u holda bu ko‘paytma yagona bo‘ladi.

Bu teorema birinchi qismining sodda isboti Yevklidning VII “Boshlang‘ich” kitobida keltirilgan va uning to‘la shakli (ko‘paytmaning yagonaligi bilan birgalikda) K.F. Gauss tomonidan berilgan.

Mazkur teoremadan birdan boshqa ixtiyoriy natural son a ning kanonik yoyilmasi

$$a=p_1^{\alpha 1}\, p_2^{\alpha 2} \ldots\, p_n^{\alpha n}$$

shaklida ifodalanishi ayon bo‘ladi. Bu yerda p_1, $p_2, \ldots,$ p_n har xil tub sonlar, α_1, α_2, … , , α_n - birga teng yoki undan katta daraja ko‘rsatkichlari, $n \geq 1$.

Nazorat savollari

1. To‘plam deb nimaga aytiladi ?
2. Qanday to‘plamlarni bilasiz?
3. To‘plamlar juftligi uchun qanday amallar aniqlangan?
4. Amallarning asosiy xossalari nimalardan iborat?
5. To‘plamning asosiy xossalari nimalardan iborat?
6. To‘plamlarni akslantirish deganda nimani tushunasiz?
7. Binar munosabatlar deganda nimani tushunasiz?
8. Arifmetikaning asosiy teoremasiga ta’rif bering?

3. TO‘PLAMLAR USTIDA ALGEBRAIK AMALLAR

3.1. Binar amallar

Faraz qilinsinki, ixtiyoriy X to‘plam berilgan bo‘lsin. Dekart kvadrat $X^2=X\text{x}X$ ni X ga ixtiyoriy (fiksirlangan) akslantirish φ: $X\text{x}X\to X$ shu to‘plam X da berilgan *binar algebraik amal* deb ataladi [12-13].

Shunday qilib, X ning har qanday tartiblangan elementlari jufti (a, b) ga $\varphi(a, b)$ mos qo‘yiladi. Ba’zida $\varphi(a, b)$ o‘rniga $a\varphi b$ yoziladi, ko‘pincha φ o‘rnida maxsus simvollar “*” yoki “+” ishlatiladi.

3.1-ta’rif. Binar amal:

1) komutativ deyiladi, agarda amal natijasi uning operand(element)lari o‘rnini almashtirishga bog‘liq bo‘lmasa, ya’ni

$a*b=b*a,\ \forall a,b\in X$;

2) assosiativ deyiladi, agarda $(a*b)*c=a*(b*c),\quad \forall a,b,c\in X$ tenglikni qanoatlantirsa;

3) alternativ deyiladi, agarda $(a*a)*b=a(a*b)$ va $y*(x*x)=(y*x),\ \forall a,b,c\in X$ tengliklarni qanoatlantirsa.

3.2. Yarimgruppalar va monoidlar

3.2-ta’rif. Bitta va undan ortiq amallar aniqlangan biror G-to‘plam *algebraik tizim* yoki *algebraik tuzilma (struktura)* deyiladi.

3.3-ta’rif. Biror G-to‘plamda “*” - binar amal (munosabat) aniqlangan bo‘lib, quyidagi:

1) *yopiqlilik* – ixtiyoriy elementlar $a, b\in G$ juftiga element $c\in G$ mos qo‘yilgan, bunda c-element a yoki b - element bilan mos tushishi ham mumkin;

2) “*”- amal *assosiativ*, ya’ni $\forall a, b, c\in G$ bo‘lgan elementlar uchun ushbu

$a*(b*c) = (a*b)*c$

munosabat o‘rinli;

3) G-to‘plamda ushbu $a*e = e*a = a$ shartni qanoatlantiruvchi e birlik element mavjud;

3.4-ta’rif. Yopiqlilik shartini qanoatlantiruvchi algebraik tuzilma $<G, *>$ *gruppoid* deyiladi.

3.5-ta'rif. Yopiqlilik va *assosiativlik* shartlarini qanoatlantiruvchi algebraik tuzilma <*G*, *> *yarimguppa* deyiladi.

3.6-ta'rif. Yopiqlilik va *assosiativlik* shartlarini qanoatlantiruvchi hamda birlik elementga ega bo‘lgan algebraik tuzilma <*G*, *> *monoid* deyiladi.

3.3. Gruppalar. Asosiy tushunchalar va ta'riflar

Elementar arifmetikada assosiativlik xossasiga ega bo‘lgan qo‘shish va ko‘paytirish amallaridan foydalaniladi. *Assosiativlik xossasiga ega bo‘lgan bitta amal aniqlangan algebraik tuzilma gruppa hisoblanadi*.

Agar $\forall a \in G$ element uchun $a*a^{-1}=a^{-1}*a=e$ munosabatni qanoatlantiruvchi teskari element $a^{-1} \in G$ mavjud shartlari bajarilgan bo‘lsa, bu <*G*, *> - algebraik tuzilma *gruppa* tashkil etadi deyiladi.

3.7-ta'rif. Gruppada aniqlangan amal "+" - qo‘shish amali xususiyatlariga ega bo‘lib, *a*-elementga qarama-qarshi ishorali *-a* – elementdan iborat hamda shunga mos ravishda birlik element *0* (nol) bo‘lsa, bunday gruppa *additiv gruppa* deyiladi.

3.8-ta'rif. Gruppada aniqlangan amal "*"- ko‘paytirish amali xususiyatlariga ega bo‘lib, *a*-elementga teskari element $a^{-1}=\frac{1}{a}$ hamda shunga mos ravishda birlik element 1 (bir) bo‘lsa, bunday gruppa *multiplikativ gruppa* deyiladi.

3.9-ta'rif. Multiplikativ gruppa <*G*, *> *siklik* deyiladi, agarda shunday element $a \in G$ mavjud bo‘lsaki, har bir element $b \in G$ uchun shunday natural son *k* majud bo‘lib, $b=a^k$ tenglik o‘rinli bo‘lsa. Bu son *a* multiplikativ gruppaning *yasovchisi* (*tuzuvchisi*) deyiladi. Keltirilgan ta'rifdan ixtiyoriy siklik gruppaning kommutativ ekanligi kelib chiqadi.

3.10-ta'rif. Gruppa *chekli* deyiladi, agarda u chekli sondagi elementlardan iborat bo‘lsa. Bunda chekli gruppa elementlarining soni uning *tartibi* deyiladi hamda $|G|$ yoki $\#G$ ko‘rinishida belgilanadi.

3.11-ta'rif. Agarda <*G*, *> - algebraik tuzilma *gruppa* tashkil etib, $\forall a, b \in G$ uchun ushbu $a*b = b*a$ tenglik o‘rinli bo‘lsa, bunday gruppa *kommutativ* yoki *Abel* gruppasi deyiladi.

3.12-ta'rif. Gruppada aniqlangan amal "+" - qo‘shish amali xususiyatlariga ega bo‘lib, *a*-elementga qarama-qarshi ishorali *-a* –

elementdan iborat hamda shunga mos ravishda birlik element *0* (nol) bo‘lsa, bunday gruppa *additiv gruppa* deyiladi.

3.13-ta’rif. Gruppada aniqlangan amal “*”- ko‘paytirish amali xususiyatlariga ega bo‘lib, *a*-elementga teskari element $a^{-1}=\frac{1}{a}$ hamda shunga mos ravishda birlik element 1 (bir) bo‘lsa, bunday gruppa *multiplikativ gruppa* deyiladi.

3.14-ta’rif. Multiplikativ gruppa <*G*, *> *siklik* deyiladi, agarda shunday element $a \in G$ mavjud bo‘lsaki, har bir element $b \in G$ uchun shunday natural son *k* majud bo‘lib, $b=a^k$ tenglik o‘rinli bo‘lsa. Bu son *a* multiplikativ gruppaning *yasovchisi* (*tuzuvchisi*) deyiladi. Keltirilgan ta’rifdan ixtiyoriy siklik gruppaning kommutativ ekanligi kelib chiqadi.

3.15-ta’rif. Gruppa *chekli* deyiladi, agarda u chekli sondagi elementlardan iborat bo‘lsa. Bunda chekli gruppa elementlarining soni uning *tartibi* deyiladi hamda $\left| G \right|$ yoki #*G* ko‘rinishida belgilanadi.

3.3.1. Parametrli multiplikativ gruppa

Parametrli gruppa quyidagicha ta’riflanadi [23].

3.16-ta’rif. F_n – chekli, ya’ni, *n* ta elementdan iborat butun sonlar to‘plami, ® – F_n ustida $a®b \equiv a + b + a*R*b \ (mod\ n)$ ko‘rinishidaaniqlangan algebraik amal bo‘lsa, (F_n; Ω) – juftlik parametrli multiplikativ gruppa deb ataladi; bu yerda *a, b,* $R \in F_n$, parametr $R>0$,+, * – butun sonlar ustida qo‘shish, ko‘paytirish amallarining va ® – parametrli ko‘paytirish amalining belgilari.

Parametrli ko‘paytirish amali o‘z mohiyati bo‘yicha ternar amaldir.

Noldan farqli to‘plam elementi *a* uchun teskari element $a^{\backslash -1}$ va qarama-qarshi element *n-a* mavjud. $a^{\backslash -1}$ parametrli teskari element deb ataladi va $a®a^{\backslash -1} \equiv 0 \ (mod\ n)$ shartini qanoatlantiradi. Bu yerda *0* – parametrli birlik elementi bo‘lib, $a®0 \equiv a$ aksiomani qanoatlantiradi.

Parametrli teskari element quyidagicha hisoblanadi:

$$a^{\backslash -1} \equiv -a(1+aR)^{-1} \ (mod\ n).$$

Bu yerda $^{-1}$ - *n* modul bo‘yicha teskarilash amalining belgisidir.

Izoh – Bu yerda va keyingi harfli ifodalarda (zarurat bo‘lmagan hollarda) ko‘paytirish belgisi “*” tushirib qoldirilgan.

Parametrli multiplikativ kommutativ gruppa quyidagi xossalarga ega.

1-xossa: agar parametrli multiplikativ kommutativ gruppaning parametri juft son va moduli $n=2k$ (k - ixtiyoriy natural son) ga teng bo‘lsa, uning tartibi (gruppa elementlari soni) $2k$ ga teng.

2-xossa: agar moduli n tub son bo‘lgan parametrli multiplikativ kommutativ gruppaning parametri ixtiyoriy natural son bo‘lsa, uning tartibi $\varphi(n)$ ga teng, bu yerda $\varphi(n)$ – Eyler pi-funksiyasi qiymati.

Misol:

1) $(F_8; ®)$, bu yerda $F_8=\{0,1,2,3,4,5,6,7\}$, $n=8$, $R=2$.

2) $(F_{\varphi(7)}; ®)$, bu yerda $F_7=\{0,1,2,3, 5,6\}$, $n=7$, $R=5$.

3-xossa: agar murakkab modulli parametrli multiplikativ kommutativ gruppaning parametri modul n bilan o‘zaro tub bo‘lsa, uning tartibi $\varphi(n)$ ga teng, bu yerda $\varphi(n)$ – Eyler pi-funksiyasi qiymati.

4-xossa: agar murakkab modul $n=pq$, bu yerda p, q – har xil tub sonlar, parametrli multiplikativ kommutativ gruppaning parametri R modul q bilan o‘zaro tub bo‘lib, p bilan o‘zaro tub bo‘lmasa, uning tartibi $p(q-1)$ ga teng.

Parametrli multiplikativ kommutativ gruppaning 1-, 2- , 4-xossalari an’anaviy multiplikativ gruppa $(F_n; *)$ xossalaridan o‘z tartibi bilan farq qiladi. Masalan, an’anaviy binar ko‘paytirish amali asosida shakllangan multiplikativ gruppa moduli $2k$ bo‘lganda, faqat toq elementlardan tashkil topgan chekli to‘plamda mavjud bo‘lsa, parametrli multiplikativ kommutativ gruppa butun sonlar to‘plamida mavjuddir. Murakkab modul $n=pq$ uchun parametrli multiplikativ kommutativ gruppaning parametri R modul p bilan o‘zaro tub bo‘lib, q bilan o‘zaro tub bo‘lmasa, uning tartibi an’anaviy multiplikativ gruppa $(F_n; *)$ tartibiga nisbatan yuqori bo‘ladi. Bular kriptotizim yaratish va ularni tahlillashning yangi imkoniyatlarini yuzaga chiqarishi mumkin.

3.3.2. Parametrli funksiyalarning diskret darajaga oshirish funksiyasi xossalariga o‘xshash xossalari

Oshkora kriptografiyaga [2, 23, 50] oid nosimmetrik kriptotizimlarni yaratish bitta maxfiylikka ega bo‘lgan bir tomonlama funksiyalardan foydalanishga asoslanadi. Eng mashhur nosimmetrik

kriptotizimlarning kriptobardoshliligi diskret logarifm, elliptik egri chiziqda diskret logarifm va faktorlash masalalarini yechish asosida maxfiylikni topishning murakkabligiga asoslanadi. Bunda murakkablik darajasi kriptotizimdan noqonuniy (xaker) va qonuniy foydalanuvchilar uchun bir xil bo‘lib, katta hisoblash resursiga ega bo‘lgan tashqi noqonuniy buzg‘unchilar uchun kriptotizimni qo‘porish xavfiga o‘rin qoldiradi. Quyida noqonuniy buzg‘unchilarning qo‘poruvchilik imkoniyatlarini yo‘qqa chiqarishga imkon beruvchi, faqat qonuniy foydalanuvchilar uchungina ma’lum bo‘lgan an’anaviy maxfiylik(daraja ko‘rsatkichi – diskret logarifm uchun, Eyler pi-funksiyasi – faktorlash uchun)ka qo‘shimcha *R* parametrli bir tomonlama funksiyaning modul $n \in \{p, p_1p_2\}$ hollari uchun an’anaviy darajaga oshirish funksiyasi xossalariga o‘xshash xossalari bayon qilingan [23, 51-54]. Bu yerda *p* – tub son, p_1, p_2 – har xil tub sonlar, *R* – parametr.

Xossalar ta’riflarida modul *n* bo‘yicha asos *a* ni *R* parametrli *x* darajaga oshirish natijasi $a^{\backslash x} (mod\ n)$ shaklida ifodalangan, bu yerda $x \in \{0,1,-1,e, d, z\}$, $^{\backslash}$ – *R* parametrli darajaga oshirish belgisidir**.**

3.17-ta’rif. Modul arifmetikasida parametr $R \geq 1$ bilan darajaga oshirish funksiyasi parametrli funksiya deb ataladi.

Parametrli funksiyalarning chekli gruppa va halqada diskret darajaga oshirish funksiyasi xossalariga o‘xshash xossalariga *quyidagilar kiradi:*

1-xossa. $a^{\backslash z+d} \equiv a^{\backslash z}$ ® $a^{\backslash d}$ $(mod\ n)$, $a^{\backslash z} \equiv a^{\backslash z}$®$0\ (mod\ n)$, bu yerda ® – modul *n* bo‘yicha *R* parametrli ko‘paytirish amalining belgisi, *0* – birlik elementi, $^{\backslash}$ – parametr *R* bilan darajaga oshirish belgisi, *a, z, d* $\in \{1,2,.\ ..,\ n-1\}$; an’anaviy (parametrsiz) darajaga oshirish funksiyasida $a^{z+d} \equiv a^z a^d\ (mod\ n)$, $a^z \equiv a^z\ 1\ (mod\ n)$.

2-xossa. $a^{\backslash zd} \equiv (a^{\backslash z})^{\backslash d} \equiv (a^{\backslash d})^{\backslash z} (mod\ n)$, bu yerda $a \in \{1,2,.\ ..,\ n-1\}$, $^{\backslash}$ – parametr *R* bilan darajaga oshirish belgisi, $z,\ d \in \{1,2,.\ ..,\ \varphi(n)\ -1\}$; an’anaviy (parametrsiz) darajaga oshirish funksiyasida $a^{zd} \equiv (a^z)^d \equiv (a^d)^z\ (mod\ n)$.

Yuqorida keltirilgan xossalar parametrli funksiya qiymatini istalgan daraja ko‘rsatkichi uchun samarali hisoblash uchun yetarlidir. Bu yerda katta darajaga oshirish jarayoni, eksponensial funksiyani hisoblash jarayoni kabi kechib, davriy tarzda $x=2$ (kvadratlash)

darajaga oshirish va hosil bo‘lgan avvalgi natijani asosga parametrli ko‘paytirish amallaridan foydalanishdan iborat bo‘ladi.

3-xossa. $a^{\backslash\varphi(n)+1} \equiv a(mod\ n)$, $a^{\backslash 0} = 0$, $a^{\backslash 1} = a$, bu yerda $\varphi(n)$ – Eyler pi-funksiyasi, $a \in \{1,2,..,n-1\}$; an’anaviy (parametrsiz) darajaga oshirish funksiyasida $a^{\varphi(n)+1} \equiv a\ (mod\ n)$, $a^0 = 1$, $a^1 = a$.

4-xossa. Agar d , e $\varphi(n)$ bilan o‘zaro tub bo‘lib, $\varphi(n)$ moduli bo‘yicha o‘zaro teskari juftlik bo‘lsa, unda $(a^{\backslash d})^{\backslash e} \equiv a\ (mod\ n)$, bu yerda $a \in \{1,2,..,n-1\}$, $^{\backslash}$ – parametr R bilan darajaga oshirish belgisi; an’anaviy (parametrsiz) darajaga oshirish funksiyasida $(a^d)^e \equiv a\ (mod\ n)$.

Misol:

n	$\varphi(n)$	e	d	R	a	$a^{\backslash d}$	$a = (a^{\backslash d})^{\backslash e}$
107	106	37	43	7	4	19	4
299	264	161	41	7	4	55	4

5-xossa (yechim mavjudligi sharti). Agar $a \ ® \ x \equiv b\ (mod\ n)$ bo‘lsa, unda yechim x mavjud bo‘lishi uchun $a^{\backslash -1}(mod\ n)$ mavjud bo‘lishi shart, bu yerda $a, b \in \{1,2,..,n-1\}$, ® – modul n bo‘yicha R parametrli ko‘paytirish amalining belgisi, $x \equiv b\ ®a^{\backslash -1}(mod\ n)$; an’anaviy (parametrsiz) taqqoslama $ax \equiv b\ (mod\ n)$ uchun $x \equiv ba^{-1}\ (mod\ n)$.

Misol:

n	a	b	R	$a^{\backslash -1}$	$x = b® a^{\backslash -1}$
7	4	3	5	me	me
107	58	15	53	25	13
77	58	15	3	me	me
77	21	17	3	49	24

6-xossa (parametrli kvadratik chegirma). Parametrli Z^*_n gruppaning elementi bo‘lgan a soni uchun, bu yerda $n>1$, parametrli Z_n gruppada $b^{\backslash 2} \equiv a\ (mod\ n)$ shartni qanoatlantiruvchi b soni mavjud bo‘lsa, unda a soni modul n bo‘yicha R parametrli kvadratik chegirma, aks holda R parametrli kvadratik chegirma emas;

an’anaviy kvadratik chegirma a uchun $b^2 \equiv a\ (mod\ p)$ shartni qanoatlantiruvchi b son mavjudligi nazarda tutiladi.

7-xossa (parametrli Lejandr simvoli). Agar *a* soni p toq tub modul parametrli kvadratik chegirma bo‘lsa, unda parametrli Lejandr simvoli *(a/p)=0*, aks holda $(a/p)= (-2)R^{-1}(mod\ p);$

a soni p toq tub modul kvadratik chegirma bo‘lsa, unda an’anaviy (parametrsiz) Lejandr simvoli *(a/p)=1*, aks holda *(a/p)= -1*.

8-xossa (Qulay hisoblanadigan kvadratik ildiz). 1) Agar tub modul $p \equiv 3,7\ (mod\ 8),\ 4 \mid (p+1)$ shartni qanoatlantirsa va *a* parametrli kvadratik chegirma bo‘lsa, unda kvadratik ildiz $x=a^{(p+1)/4}\ (mod\ p);$

2) Agar tub modul $p \equiv 5\ (mod\ 8),\ 8 \mid (p+3)$ shartni qanoatlantirsa va *a* parametrli kvadratik chegirma bo‘lsa, unda kvadratik ildiz $x=a^{(p+3)/8}\ (mod\ p);$

an’anaviy ifodalarda darajaga oshirish belgisi qatnashmaydi.

9-xossa (Qoldiqlar haqida parametrli xitoycha teorema). Agar $i=1,2,\dots,k$ uchun berilgan tenglamalar sistemasi $x \equiv c_i\ (mod\ p_i)$ bo‘lsa, $1 \le p_i < p_j \le k$ bo‘lganda $EKUB(p_i, p_j) = 1$ bo‘lsa, unda

$\underline{I_{pi}} \equiv 0\ (mod\ p_j),\ i=1,2,\dots,k,$

taqqoslamalar sistemasini qanoatlantiruvchi parametrli chegirmalar sinfi $\underline{I_{pi}}$ va yagona yechim mavjud:

$x \equiv \underline{I_{p1}}\ c_1 \circledR \underline{I_{p2}}\ c_2 \circledR \dots \circledR \underline{I_{pk}}\ c_k\ (mod\ n),$

bu yerda $\underline{I_{pi}}=((n/p_i)^{-1}(mod\ p_i))\ n/p_i,$

modul $n=p_1\ p_{2***}\ p_k,$ ® – modul *n* bo‘yicha *R* parametrli ko‘paytirish amalining belgisi, EKUB - eng katta umumiy bo‘luvchi funksiyasining nomi, c_i - parametrli algebra amallari asosida aniqlangan kattalik, masalan, p_i modul bo‘yicha *R* parametr bilan berilgan kattalikni ildizdan chiqarish natijasi;

an’anaviy (parametrsiz) *qoldiqlar haqida* xitoycha teoremada

$x \equiv \sum_i^k \underline{I_{pi}}\ c_i\ (mod\ n),$ bu yerda $\underline{I_{pi}}=((n/p_i)^{-1}(mod\ p_i))n/p_i.$

Quyida qoldiqlar haqida an’anaviy va parametrli xitoycha teoremalarni *a=9* va *a=48* sonlarining *n=7*11=77* bo‘yicha kvadrat ildizlaridan birini topishga misol keltirilgan.

Misol:

a	*R*	*a(mod7)*	*a(mod11)*	$c_1=\sqrt{a(mod7)}$	$c_2=\sqrt{a(mod11)}$	$7^{-1}(mod11)$	$11^{-1}(mod7)$
9		*2*	*9*	*3*	*3*	*2*	*8*
48	*13*	*6*	*4*	*4*	*1*	*2*	*8*

$\underline{I_7}$=2*11	$\underline{I_{11}}$ =8*7	Kvadratik ildiz	Ildiz^2 (tekshirish)
22	56	$\underline{I_7}\, c_1 + \underline{I_{11}}\, c_2 = 3$	9
22	56	$\underline{I_7}\, c_1$® $\underline{I_{11}}\, c_2 = 67$	48

3.4. Gruppalar morfizmi

Izomorfizm

Agar $f: G \to G'$ akslantirish mavjud bo‘lib, f biyektiv bo‘lsa (1-shart), barcha $a, b \in G$ uchun $f(a*b) = f(a) \circ f(b)$ (2-shart) o‘rinli bo‘lsa, unda $<G,*>$ va $<G,\circ>$ gruppalar *izomorf* deyiladi,

Gruppalarning izomorfligi $\cong$ kabi belgilanadi, ya’ni $G \cong G'$.

Izomorfizmlarning eng sodda xossalari quyidagilardan iborat:

1. Birlik element birlik elementga o‘tadi.

Haqiqatan, agar e – G ning birlik elementi bo‘lsa, u holda $e*a=a*e=a$ va demak $f(e) \circ f(a) = f(a) \circ f(e) = f(a)$, bundan kelib chiqadiki $f(e) = e' - G'$ gruppaning birlik elementi. Bunda qisman bo‘lsa ham f – izomorfizmning ikkala xususiyatidan ham foydalaniladi.

2. $f(a^{-1}) = f(a)^{-1}$.

Haqiqatan ham $f(a) \circ f(a^{-1}) = f(a*a^{-1}) = f(e) = e'$. $e' - G'$ gruppaning birlik elementi. Demak, $f(a)^{-1} = f(a)^{-1} \circ e' = f(a)^{-1} \circ (f(a) \circ f(a^{-1})) = (f(a)^{-1} \circ f(a)) \circ f(a)^{-1} = e' \circ f(a)^{-1} = f(a)^{-1}$.

3. Teskari akslantirish $f^{-1}: G \to G'$ ham izomorfizm bo‘ladi. Buning uchun f^{-1} da ham 2- shart to‘g‘riligini tekshirish yetarli.

Faraz qilaylik, $a', b' \in G'$. U holda f ning biyektivligiga ko‘ra $a' = f(a), b' = f(b)$ qandaydir $a, b \in G$ uchun o‘rinli. f – izomorfizm bo‘lgani uchun $a' \circ b' = f(a) \circ f(b) = f(a*b)$. Bundan esa $a*b = f^{-1}(a' \circ b')$ ekanligi kelib chiqadi. $a = f^{-1}(a')$ va $b = f^{-1}(b')$ ekanligini e’tiborga olsak, $f^{-1}(a' \circ b') = f^{-1}(a') * f^{-1}(b')$. Demak bu xossa ham isbotlandi.

Misol. $(R_+, *, 1)$ musbat sonlarning multiplikativ gruppasini barcha haqiqiy sonlarning additiv gruppasi $(R, +, 0)$ga izomorf akslantirish deb $f = ln$ ni olish mumkin. Logarifmning $ln\, ab = ln\, a + ln\, b$ xossasi ta’rifidagi 2-shartni qanoatlantiradi. f ga teskari akslantirish $f^{-1}: x \to e^x$ bo‘ladi. Izomorfizm ta’rifida $G = \cong G'$ deb $\varphi: G \to G$ izomorf

akslantirishni hosil qilamiz. Bu akslantirish G gruppaning avtomorfizmi deyiladi.

Misol. $e_g: g \to g$ birlik akslantirish avtomorfizmdir.

Odatda G trivial bo‘lmagan avtomorfizmlarga ham ega.

Izomorf akslantirishlarning 3-xossasi avtomorfizmga teskari bo‘lgan akslantirish ham avtomorfizm bo‘lishini ko‘rsatadi.

Agar $\varphi, \psi \in G$ gruppaning avtomorfizmlari bo‘lsa, u holda $\forall a,b \in G$ uchun $(\varphi \circ \psi)(ab) = \varphi(\psi(ab)) = \varphi(\psi(a)\psi(b)) = (\varphi \circ \psi)(a) * (\varphi \circ \psi)(b)$ o‘rinli.

Demak, G gruppaning barcha avtomorfizmlari to‘plami $G \to G$ akslantiruvchi barcha biyeksiyalar to‘plami $S(G)$ ning qism gruppasi bo‘lgan $Aut(G)$ gruppani hosil qiladi.

Gomomorfizmlar

G gruppaning avtomorfizmlari gruppasi $Aut(G)$da bitta maxsus qism gruppa bor. Uni $Inn(G)$ bilan belgilanadi va ichki avtomorfizmlar gruppasi deb ataladi. Quyidagi akslantirishlar bu gruppaning elementlari bo‘ladi:

$I_a: g \to aga^{-1}$. Bu yerda $I_a^{-1} = I_{a-1}$, I_e – birlik avtomorfizm, $I_a \circ I_b = I_{ab}$, chunki $(I_a \circ I_b)(g) = I_a(I_b(g)) = I_a(bgb^{-1}) = abgb^{-1}a^{-1} = abg(ba)^{-1} = I_{ab}(g)$.

So‘nggi tenglik G gruppani uning ichki avtomorfizmlar gruppasi $Inn(G)$ ga akslantiruvchi $f(a) = I_a$, $a \in G$ formula bilan aniqlangan akslantirish izomorf akslantirishning $f(a) \circ f(b) = f(a*b)$ shartini qanoatlantiradi, biroq bunda biyektivlik sharti bajarilmaydi.

Agar G Abel gruppasi bo‘lsa, u holda barcha $a \in G$ uchun $aga^{-1} = g$ o‘rinli va demak, $I_a = I_e$, ya’ni butun $Inn(G)$ gruppa faqat bitta I_e elementdan iborat.

Agar barcha $a, b \in G$ uchun $f(a*b) = f(a) \circ f(b)$ o‘rinli bo‘lsa, unda $<G,*>$ gruppani $<G,\circ>$ gruppaga akslantiruvchi $f: G \to G'$ akslantirish gomomorfizm deb ataladi.

$Ker\ f = \{g \in G \mid f(g) = e' - G'$ gruppaning birlik elementi$\}$ to‘plam f gomomorfizmning yadrosi deb ataladi.

Gruppani o‘z-o‘ziga gomomorf akslantirish endomorfizm deb ataladi. Gomomorfizmning ta’rifida f akslantirishdan biyektivlik talab qilinmaydi. Lekin shunga qaramay f gomomorfizmning

izomorfizmdan asosiy farqi, unda trivial bo‘lmagan *Ker f* yadroning mavjudligidir.

Agar *Ker f={e}* bo‘lsa, u holda $f: G \to Inn\, f$ – izomorfizm bo‘ladi.

$\forall\ a,b \in Ker\ f$ uchun $f(a)=e'$, $f(b)=e' \Rightarrow f(a*b)= f(a) o\ f(b) =e' o e' =e'$ va $f(a^{-1})= f(a)^{-1} =(e)^{-1} =e'$.

Demak, *Ker f* yadro *G* gruppaning qism gruppasi ekan.

Faraz qilaylik, $N= Ker\ f \subset G$ bo‘lsin. U holda $\forall h \in H$, $g \in G$ uchun $f(ghg^{-1})=f(g)f(h)f(g^{-1})=f(g)e'\ f(g^{-1})= e'$, *ya’ni* $ghg^{-1} \in H$ bo‘ladi. Bu degani $ghg^{-1} \subset H$ bunda *g ni* g^{-1} bilan, g^{-1} ni *g* bilan almashtirib, $g^{-1} hg \subset H$ *ya’ni,* $H \subset ghg^{-1}$ ekanini aniqlaymiz. Demak, $\forall\, g \in G$ uchun $H= ghg^{-1}$. Bu xossa ega bo‘lgan qism gruppa normal qism gruppa deb ataladi.

3.5. Halqa. Ta’rif va umumiy xossalar

3.18-ta’rif. Biror *G*-to‘plamda ikkita “+” - qo‘shish va “*” - ko‘paytirish binar amallar (munosabatlar) aniqlangan bo‘lib, quyidagi:

1) *G*-to‘plam additiv Abel gruppasini tashkil etadi;

2) ko‘paytirish amali assosiativ, ya’ni $\forall\, a, b, c \in G$ bo‘lgan elementlar uchun ushbu

$a(bc) = (ab)c$

munosabat o‘rinli;

3) distributivlik qonuni o‘rinli, ya’ni $\forall\, a, b, c \in G$ bo‘lgan elementlar uchun ushbu

$a\,(b+c) = ab+ac$ va $(a+b)\,c = ac+bc$

munosabatlar o‘rinli shartlari bajarilgan bo‘lsa, bu <*G*, +, *> - algebraik tuzilma *halqa* tashkil etadi deyiladi.

Bitta (tegishli xossalarga ega bo‘lgan) amal aniqlangan gruppa tashkil etuvchi to‘plamdan farqli ravishda halqa tashkil etuvchi to‘plamda uning ta’rifida keltirilgan xossalarga ega bo‘lgan ikkita amal aniqlangan.

3.19-ta’rif. Halqa *birlik elementli* deyiladi, agarda multiplikativ birlik elementga ega bo‘lsa, ya’ni shunday element $1 \in G$ majud bo‘lsaki, uning uchun ushbu $a1=1a=a$ munosabat $\forall\, a \in G$ elementda bajariladi.

3.20-ta’rif. Halqa *kommutativ* deyiladi, agarda ko‘paytirish amali kommutativlik xossasiga ega bo‘lsa.

3.21-ta'rif. Halqa *butun* yoki *butun sohali* deyiladi, agarda u $e \neq 0$-birlik elementli kommutativ halqa tashkil etib, $a, b \in G$ elementlar uchun $ab=0$ munosabatdan $a=0$ yoki $b=0$ kelib chiqsa.

3.22-ta'rif. G – ixtiyoriy halqa bo‘lsin. Shunday natural son $p \in \{1,2,3,\ldots\}$ mavjud bo‘lsaki, har bir element $g \in G$ uchun $pg = 0$ bajarilsa, u holda eng kichik shunday p-son G-halqaning *xarakteristikasi* deyiladi. Agarda shunday natural son mavjud bo‘lmasa, u holda halqa *0* (nol) xarakteristikaga ega deyiladi. Halqaning *tartibi* shu halqaning additiv gruppasi tartibi bilan aniqlanib, halqaning elementlari soniga teng.

3.6. Maydonlar

3.23-ta'rif. Biror G-to‘plamda ikkita “+” - qo‘shish va “*” - ko‘paytirish binar amallar (munosabatlar) aniqlangan bo‘lib, quyidagi:

1) G-to‘plam *0* (nol) birlik elementli additiv Abel gruppasini tashkil etadi;

2) G-to‘plamning noldan farqli elementlari *1*(bir) birlik elementli multiplikativ Abel gruppasini tashkil etadi; ko‘paytirish amali assosiativ, ya'ni $\forall a, b, c \in G$ bo‘lgan elementlar uchun ushbu

$$a(bc) = (ab)c$$

munosabat o‘rinli;

3) qo‘shish va ko‘paytirish amallari distributivlik qonuni bilan bog‘langan;

4) qo‘shish va ko‘paytirish amallari uchun teskari amallar mavjud: ayirish va bo‘lish (nolga bo‘lishdan tashqari) shartlari bajarilgan bo‘lsa bu $<G, +, *>$ - algebraik tuzilma *maydon* tashkil etadi deyiladi.

3.24-ta'rif. Agar maydon tashkil etuvchi to‘plam q-chekli sondagi elementlardan iborat bo‘lsa, u holda maydon *chekli maydon* yoki *Galua maydoni* deyiladi va $GF(q)$ yoki F_q deb belgilanadi.

1-tasdiq. Chekli maydon mavjud bo‘lishi uchun maydonning elementlari sonini ifodalovchi q-tub son bo‘lishi yoki tub sonning darajasi $q=p^m$, bu yerda p - tub son, m - natural son ko‘rinishida ifodalanashi zarur va yetarli. Bunda p - tub son $GF(q)$ - chekli maydonning *xarakteristikasi*, m soni $GF(q)$ maydonning $GF(p)$ qism maydonga nisbatan *darajasi* deyiladi hamda $m=1$ bo‘lsa, *oddiy*, aks

holda *kengaytirilgan* maydon deyiladi. Agar *p* - tub son bo‘lmasa, u holda <*G*, +, *> - algebraik tuzilmada aniqlangan qo‘shish va ko‘paytirish amallari biror *n*-asosli modul (mod *n*) bo‘yicha aniqlangan bo‘lsa, hatto noldan farqli elementga bo‘lish har doim ham mumkin bo‘lavermaydi va bu tuzilma maydon tashkil etmay halqa tashkil etadi.

Har qanday maydonning barcha elementlari to‘plami qo‘shish amaliga ko‘ra additiv Abel gruppasini va noldan farqli barcha elementlari to‘plami ko‘paytirish amaliga nisbatan multiplikativ siklik gruppa tashkil etadi.

Mumkin bo‘lgan har bir *q* – tartib uchun faqat bitta maydon mavjud, ya’ni barcha *q* – tartibli chekli maydonlar izomorfdir. Misol uchun, agarda *q=p* – tub son bo‘lsa, u holda maydonning elementlari *0, 1, ..., (p-1)* – sonlar bo‘lib, qo‘shish va ko‘paytirish amallari mod *p* qo‘shish va ko‘paytirish amallaridan iborat, ya’ni *GF*(*p*)=*Z/p*. Shunday qilib, tub sonli modul bo‘yicha chegirmalar halqasi oddiy maydon tashkil etadi.

2-tasdiq. Ixtiyoriy *GF*(*q*) - chekli maydonning noldan farqli elementlari multiplikativ siklik gruppa tashkil etadi.

3.20-ta’rif. Siklik gruppaning α- *yasovchisi* (*tuzuvchisi*, *generatori*) chekli maydonning primitiv elementi deyiladi hamda bu maydonning barcha elementlarini quyidagicha ifodalash mumkin:

$GF(q)=\{0, \alpha, \alpha^2, \ldots, \alpha^{q-2}, \alpha^{q-1}, \alpha^0=1\}$.

3.6.1. Maydon ustida berilgan diamatrisalar algebrasi

3.21-ta’rif. Ď – chekli, ya’ni *n* ta elementdan iborat butun sonlar maydoni ustida aniqlangan kvadrat diamatrisalar chekli to‘plami, *Ω = {+, ®’}* – *Ď* ustida aniqlangan algebraik amallar to‘plami bo‘lsa, *<Ď; Ω>* – juftlik diamatrisalar algebrasi deb ataladi; bu yerda o‘zaro mos tarzda + – qo‘shish, ®’ – diamatrisaviy ko‘paytirish amallarining belgilaridir.

Mazkur takomillashgan diamatrisalar algebrasi [23] da keltirilgan algebradan amallar chekli to‘plam ustida berilgan diamatrisalar to‘plami ustida aniqlanishi, barcha amallar diamatrisalar to‘plami ustida aniqlanib diamatrisa hosil etilishi bilan farqlanadi.

Natijaviy diamatrisa $C \equiv A®'B \ (mod\ n)$ elementlari diagonal hamda nodiagonal elementlar uchun turlicha ifodalar asosida hisoblanadi.

$$c[u,u] \equiv a[u,u]*\Sigma^{m-1}_{i=0}\, b[i,u] - \Sigma^{m-1}_{i=0,\ i\neq c}\, a[i,i]*b[i,u] \ (mod\ n),$$

$$c[c,u]_{c\neq u} \equiv a[c,u]*\Sigma^{m-1}_{i=0}\, b[i,u] + b[c,u]*\Sigma^{m-1}_{i=0}\, a[i,u] - \Sigma^{m-1}_{i=0;\ i\neq c,u}\, a[c,i]*b[i,u] \ (mod\ n).$$

Diamatrisaviy ko‘paytirish amali matrisaviy ko‘paytirish amaliga nisbatan mukammal shifrlar yaratish muammosi nuqtai nazaridan qulay ekanligini ilmiy kriptologiya asoschisi Klod Shennonning [24] mukammal shifr yaratishda ishlatiladigan almashtirishlari yaxshi aralashish va keng yoyilishga olib kelishi lozimligi haqidagi tavsiyalari ko‘proq mos kelishi sababli O‘z DSt 1105:2006, O‘z DSt 1105:2009 - Ma’lumotlarni shifrlash algoritmlariga asos etib olingan. Buni quyidagi misollardan ko‘rish mumkin.

3.1- va 3.2-misollarda modul $n=256$ bo‘lganda 4-tartibli diamatrisalarning va matrisalarning 1 tadan elementlari o‘zgarganda natijaviy matrisalarda o‘zgargan sohalar aks etgan:

3.1-misol: d matrisaviy ko‘paytma

$$\underset{A}{\begin{vmatrix} 1 & 2 & 3 & 4 \\ 12 & 9 & 21 & 0 \\ 13 & 17 & 6 & 31 \\ 14 & 18 & 29 & 9 \end{vmatrix}} ®' \underset{V}{\begin{vmatrix} 17 & 1 & 2 & 3 \\ 4 & 5 & 7 & 8 \\ 9 & 10 & 11 & 12 \\ 13 & 14 & 15 & 16 \end{vmatrix}} \equiv \underset{C}{\begin{vmatrix} 92 & 14 & 111 & 224 \\ 255 & 83 & 9 & 80 \\ 107 & 141 & 10 & 206 \\ 73 & 84 & 241 & 204 \end{vmatrix}}$$

$$\underset{A'}{\begin{vmatrix} 1 & 2 & 3 & 4 \\ 12 & 10 & 21 & 0 \\ 13 & 17 & 6 & 31 \\ 14 & 18 & 29 & 9 \end{vmatrix}} ®' \underset{V}{\begin{vmatrix} 17 & 1 & 2 & 3 \\ 4 & 5 & 7 & 8 \\ 9 & 10 & 11 & 12 \\ 13 & 14 & 15 & 16 \end{vmatrix}} \equiv \underset{C'}{\begin{vmatrix} 88 & 14 & 111 & 224 \\ 3 & 113 & 16 & 88 \\ 107 & 141 & 3 & 206 \\ 73 & 84 & 241 & 196 \end{vmatrix}}$$

3.2-misol: Matrisaviy ko‘paytma

$$\begin{array}{ccccc} A & & B & & C \\ \begin{vmatrix} 1 & 2 & 3 & 4 \\ 12 & 9 & 21 & 0 \\ 13 & 17 & 6 & 31 \\ 14 & 18 & 29 & 9 \end{vmatrix} & \text{x} & \begin{vmatrix} 17 & 1 & 2 & 3 \\ 4 & 5 & 7 & 8 \\ 9 & 10 & 11 & 12 \\ 13 & 14 & 15 & 16 \end{vmatrix} & \equiv & \begin{vmatrix} 104 & 97 & 109 & 119 \\ 173 & 11 & 62 & 104 \\ 234 & 80 & 164 & 231 \\ 176 & 8 & 96 & 166 \end{vmatrix} \end{array}$$

$$\begin{array}{ccccc} A' & & B & & C' \\ \begin{vmatrix} 1 & 2 & 3 & 4 \\ 12 & 10 & 21 & 0 \\ 13 & 17 & 6 & 31 \\ 14 & 18 & 29 & 9 \end{vmatrix} & \text{x} & \begin{vmatrix} 17 & 1 & 2 & 3 \\ 4 & 5 & 7 & 8 \\ 9 & 10 & 11 & 12 \\ 13 & 14 & 15 & 16 \end{vmatrix} & \equiv & \begin{vmatrix} 104 & 97 & 109 & 119 \\ 177 & 16 & 69 & 112 \\ 234 & 80 & 164 & 231 \\ 176 & 8 & 96 & 166 \end{vmatrix} \end{array}$$

Misollardan ko‘rinib turibdiki, diamatrisaviy ko‘paytma natijasida *A* ning *1* ta elementi o‘zgarganda *C* da *7* ta element o‘zgargan; matrisaviy ko‘paytmada esa, *1* ta ustun yoki satr elementlari, ya’ni *4* ta element o‘zgargan.

3.6.2. Maydon ustida berilgan elliptik egri chiziq nuqtalari gruppasi

Elliptik egri chiziq

Ko‘plab oshkora kalitli kriptografik mahsulotlar va standartlar deyarli an’anaviy mavqyega erishgan RSA va El Gamal algoritmlariga asoslangan. So‘nggi vaqtlarda kriptotahlil usullarining va hisoblash texnikasining keskin rivojlanishi tizimlarning ishonchli himoyasi uchun kalit bitlari sonining ham katta bo‘lishiga olib keldi, bu esa an’anaviy tizimlarni qo‘llovchi tizimlar ilovasini yuklanish vaqtining ortishiga olib keldi. Bu o‘z navbatida katta tranzaksiyalarni himoyalash talab etiladigan, elektron tijoratga ixtisoslashgan aloqa tugunlarida ko‘plab muammolarni keltirib chiqardi. Shu bois an’anaviy mavqyega erishgan tizimlarga raqib - elliptik egri chiziqlarga asoslangan kriptografiya vujudga keldi.

Elliptik egri chiziqlarga asoslangan kriptografik tizimlarning an’anaviy tizimlarga nisbatan afzalligi, ularda foydalaniladigan kalit uzunligi razryadi kichik bo‘lganda ham, ekvivalent himoya bilan

ta’minlashidadir. Bu esa qabul qiluvchi va uzatuvchi moslama prosessorlarining yuklanish vaqtini kamaytiradi.

Hozirda elliptik egri chiziqlarning kriptografiya sohasiga tatbiqi keng qo‘llanilmoqda. Ushbu paragrafda elliptik egri chiziq va uning nuqtalari haqida umumiy tushunchalar hamda ularga bog‘liq bo‘lgan amallar bilan tanishish mumkin.

3.22-ta’rif. Biror *K*-maydonda olingan elliptik egri chiziq deb, quyidagi Veyershtrass tenglamasi deb ataluvchi tenglik orqali aniqlanuvchi

$$y^2 + a_1xy + a_3y = x^3 + a_2x^2 + a_4x + a_6 \quad (1)$$

egri chiziqqa aytiladi, bu yerda $a_1, a_2, a_3, a_4, a_6 \in K$.

Elliptik egri chiziq odatda E yoki E/K bilan belgilanadi va elliptik egri chiziqqa tegishli nuqtalar, yani (1) tenglama yechimlari shu elliptik egri chiziqning *affin nuqtalari* deyiladi.

3.23-ta’rif. $P(x_0, y_0) \in E$ nuqta elliptik egri chiziqning silliq nuqtasi deyiladi, agar

$$f(x_0, y_0) = y_0^2 + a_1x_0y_0 + a_3y_0 - x_0^3 - a_2x_0^2 - a_4x_0 - a_6$$

bo‘lib, quyidagi shartlardan bittasi o‘rinli bo‘lsa:

$$f_x`(x_0, y_0) \neq 0 \text{ yoki } f_y`(x_0, y_0) \neq 0 \quad (2)$$

3.24-ta’rif. E/K – elliptik egri chizik silliq deb ataladi, agar uning har bir affin nuqtasi silliq bo‘lsa.

1-misol. $y^2 = x^3$ elliptik egri chiziq uchun *(0;0)* nuqta silliq nuqta emasligi ko‘rsatilsin.

Yechish.

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

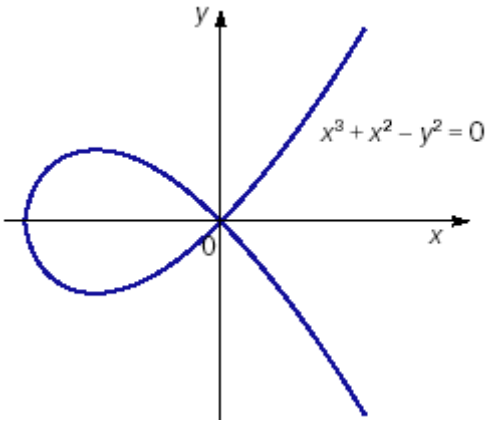
bo‘lib, (2) shartga nisbatan ziddiyatga kelinadi. Natijada, *(0;0)* nuqtaning haqiqatan ham silliq nuqta bo‘la olmasligi kelib chiqadi.

2-misol. $y^2 = x^3 + x^2$ elliptik egri chiziq uchun *(0;0)* nuqta silliq nuqta emasligi ko‘rsatilsin.

Yechish. Haqiqatan ham,

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

bo‘lib, (2) shartga nisbatan ziddiyatga kelinadi. Natijada, *(0;0)* nuqtaning haqiqatan ham silliq nuqta bo‘la olmasligi kelib chiqadi:



Quyida elliptik egri chiziqlarning umumiy kanonik ko‘rinishi hisoblangan ushbu

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

tenglama bilan ish ko‘ramiz, bu yerda $a,b,c \in Z$ (a,b,c - butun sonlar) va ko‘phad $p(x) = x^3 + ax^2 + bx + c$ karrali ildizga ega emas deb qaraladi.

Elliptik egri chiziqlarning grafiklari

Yuqorida keltirilgan (3) ko‘rinishdagi egri chiziq grafigini chizish uchun

$$y = \sqrt{x^3 + ax^2 + bx + c}\ ,\ (4)$$

chizish va Ox – o‘qiga nisbatan simmetrik akslantirish lozim. Bu (4) berilgan funksiya grafigini chizish uchun esa kvadratsiz holidagi funksiya

$$z = x^3 + ax^2 + bx + c$$

grafigini chizib olish kerak bo‘ladi. Funksiya grafigining *Ox*-o‘qi bilan kesishish nuqtalari

$$x^3 + ax^2 + bx + c = 0$$

tenglamaning yechimlarini topish orqali aniqlanadi. Bu tenglamadan,

$$v = x + \frac{a}{3}\ \left(x = v - \frac{a}{3}\right)$$

almashtirishdan foydalanib,

$$v^3 + pv + q = 0$$

keltirilgan tenglama olinadi, bu yerda $p = \frac{3b - a^2}{3}$, $q = \frac{2a^3}{27} - \frac{ab}{3} + c$. $D = \left(p/3\right)^3 + \left(q/2\right)^2$ ifoda diskriminant deb atalib,

keltirilgan tenglamaning ildizlari soni diskriminant qiymatining ishorasiga bog‘liq:

a) $D>0$ bo‘lsa, bitta haqiqiy ildizga ega, ya’ni funksiya grafigi *Ox*-o‘qi bilan bitta nuqtada kesishadi;

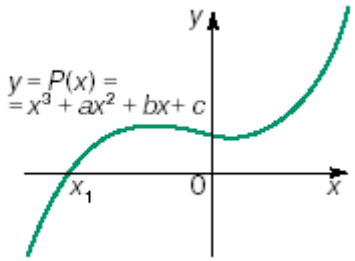
b) $D<0$ bo‘lsa, uchta haqiqiy ildizga ega, ya’ni funksiya grafigi *Ox*-o‘qi bilan uchta nuqtada kesishadi;

s) $D=0$ bo‘lsa, uchta haqiqiy ildizga ega bo‘lib, ularning ikkitasi teng (karrali), ya’ni funksiya grafigi *Ox*-o‘qi bilan ikkita nuqtada kesishadi.

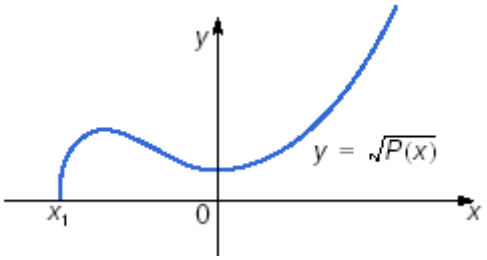
Keltirilgan hol uchun

$$z=x^3+ax^2+bx+c\ ,$$

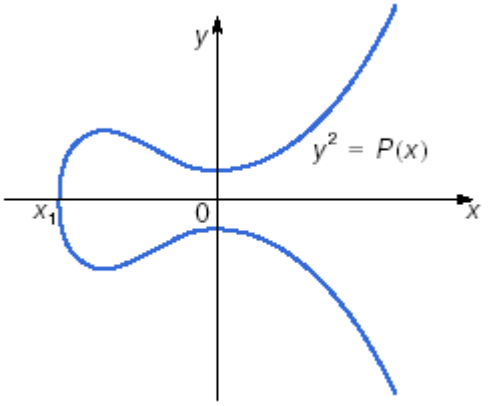
funksiya grafigi quyidagi ko‘rinishga ega:



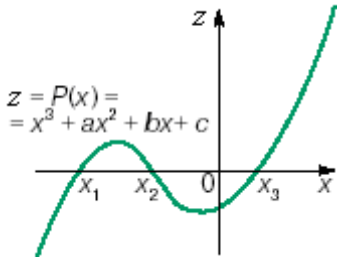
Bu grafikdan (4) funksiya grafigini olish uchun, kvadrat ildiz ostidagi ifodaning manfiy bo‘lmagan qiymatlar sohasiga mos keluvchi - aniqlanish sohasining qismi



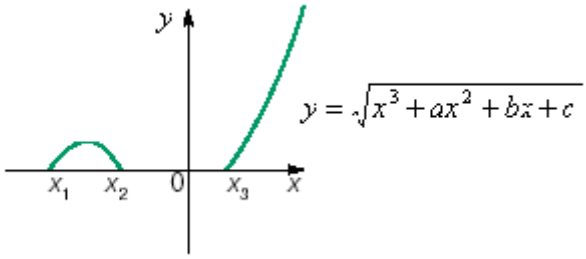
Ox - o‘qiga nisbatan simmetrik ko‘chiriladi, ya’ni:



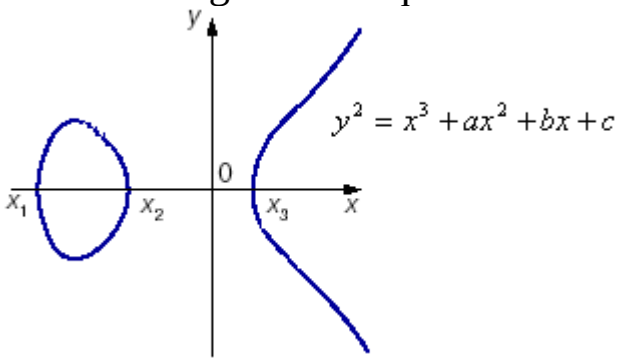
Uchta haqiqiy ildizga ega bo‘lgan b) hol uchun $z = x^3 + ax^2 + bx + c$,
funksiya grafigi quyidagi ko‘rinishga ega:



Xuddi yuqoridagi fikr va mulohazalarga ko‘ra, bu grafikdan (4) funksiya grafigini olish uchun, kvadrat ildiz ostidagi ifodaning manfiy bo‘lmagan qiymatlar sohasiga mos keluvchi - aniqlanish sohasining qismi



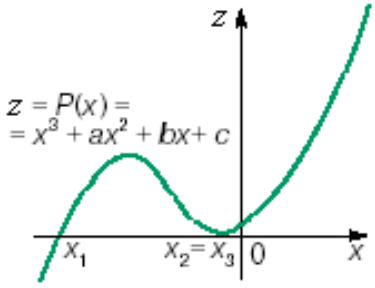
Ox - o‘qiga nisbatan simmetrik ko‘chiriladi, natijada grafik ellips va giperboladan iborat bo‘lgan ikkita qismlar bilan ifodalanadi:



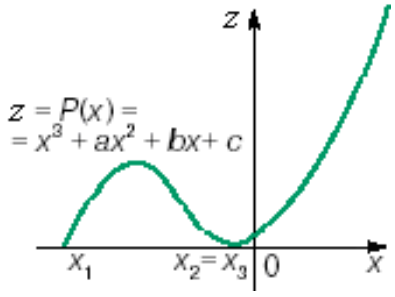
Uchta haqiqiy ildizga ega bo‘lib, ularning ikkitasi teng (karrali) bo‘lgan *s*) hol uchun

$$z = x^3 + ax^2 + bx + c \ ,$$

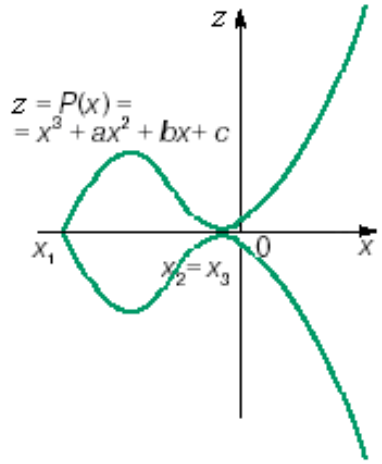
funksiya grafigi quyidagi ko‘rinishga ega:



Bu grafikdan (4) funksiya grafigini olish uchun, kvadrat ildiz ostidagi ifodaning manfiy bo‘lmagan qiymatlar sohasiga mos keluvchi - aniqlanish sohasinin qismi



Ox- o‘qiga nisbatan simmetrik ko‘chiriladi, natijada grafik umumiy nuqtaga ega bo‘lgan ellips va giperboladan iborat bo‘lgan ikkita qismlar bilan ifodalanadi:



Amalda, $y^2 = x^3 + ax^2 + bx + c$ - elliptik egri chiziq koeffisiyenti $a = 0$ bo‘lgan $y^2 = x^3 + bx + c$ - elliptik egri chiziqning keltirilgan ko‘rinishidagi ifodasidan hamda uning diskriminanti $D < 0$ bo‘lib, uchta haqiqiy ildizga ega, ya’ni funksiya grafigi O*x*-o‘qi bilan uchta nuqtada kesishadigan holatidan foydalanish qulay va samarali tatbiqqa ega.

Elliptik egri chiziqqa tegishli rasional nuqtalarni aniqlash usullari

Oldindan shuni aytish lozimki, hozirgi kunda

$$y^2 = x^3 + ax^2 + bx + c,$$

tenglamaning barcha rasional yechimlarini topish matematikada nomalumligicha qolib kelmokda. Lekin, quyidagi ikkita usuldan foydalanib, rasional yechimlarni topish mumkin.

1-usul. Tanlangan $y^2=x^3+ax+b$ tenglamaga x_i qiymatlarni berib, tenglamaning o‘ng tomoni to‘la kvadrat tashkil qilish tekshiriladi. Agar biror x_k qiymatda tenglikni o‘ng tomonidagi ifodaning qiymati to‘la kvadrat tashkil qilsa, u holda tenglamaga tegishli nuqta koordinatalarini

$$(x_k ; y_k = \pm\sqrt{x_k^3 + ax_k + b}\ ) \quad (5)$$

juftliklar bilan fiksirlanadi.

2- usul. Bu usulda nuqta koordinatalari (x; y) va tenglamaning bitta a –koeffisiyentini fiksirlab: (a; x; $y \in R$) ,

$$b=y^2-x^3-ax \quad (6)$$

formula orqali b–koeffisiyent hisoblab topiladi va uning asosida tenglama quriladi. Elliptik egri chiziq koeffisiyentlarini olingan rasional koordinatali nuqta orqali aniqlashning bunday usuli samarali hisoblanadi.

Elliptik egri chiziqlarning rasional nuqtalarini qo‘shish

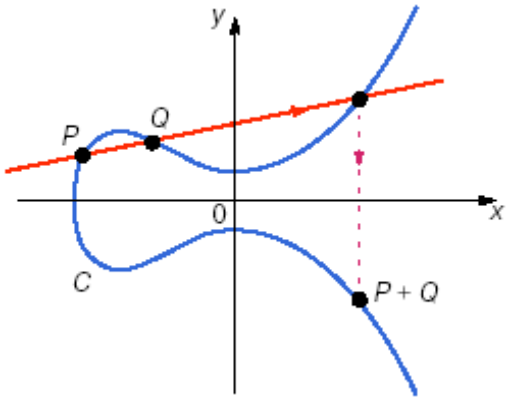
Ushbu

$$E: y^2 = x^3 + ax^2 + bx + c,$$

elliptik egri chiziqda $P(x_1, y_1)$, $Q(x_2, y_2)$ nuqtalar berilgan bo‘lsin. Bu nuqtalar orqali to‘g‘ri chiziq o‘tkaziladi. U holda o‘tkazilgan chiziq, Ye - egri chiziqni uchinchi nuqtada kesib o‘tadi. Bu $B(x_3, y_3)$ nuqtani Ox - o‘qiga simmetrik ko‘chiriladi va hosil bo‘lgan:

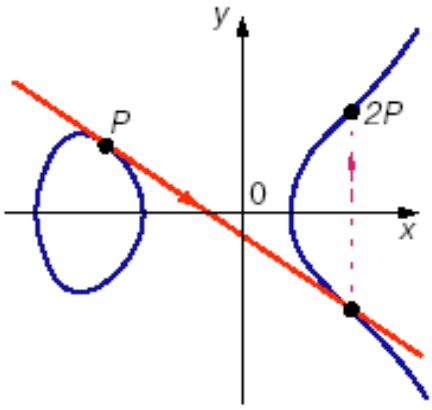
$$B`(x_3, -y_3) = P(x_1, y_1) + Q(x_2, y_2)$$

nuqta $P(x_1, y_1)$ va $Q(x_2, y_2)$ nuqtalarning elliptik egri chiziq ustida yig‘indisi deb elon qilinadi:



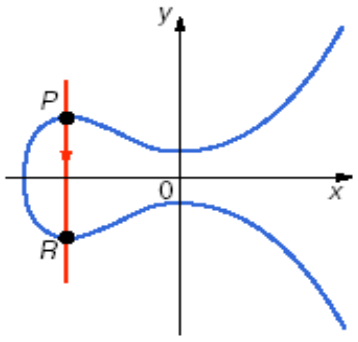
Bu grafik $x^3+ax^2+bx+c=0$ tenglama bitta yechimga ega bo‘lgan hol uchun keltirildi.

Yuqorida elliptik egri chiziqda koordinatalari har xil bo‘lgan, ya’ni $P(x_1,y_1)\neq Q(x_2,y_2)\neq 0$ bo‘lgan nuqtalar yig‘indisini $P(x_1,y_1)+Q(x_2,y_2)$ topish ko‘rib chiqildi. Endi $P+P=?$ qanday amalga oshirilishi haqida to‘xtab o‘tiladi. Buning uchun elliptik egri chiziqdagi P-nuqta orqali urinma to‘g‘ri chiziq o‘tkaziladi. Bu urinma elliptik egri chiziq grafigidagi ikkinchi qismni (giperbola qismida) biror nuqtada kesib o‘tadi. Ana shu kesib o‘tgan nuqta Ox-o‘qiga nisbatan simmetrik ko‘chiriladi va bu nuqta *[2]P* deb elon qilinadi:



So‘ngra, *[3]P* ni topish uchun, *[3]P=[2]P+P*, shu kabi *[4]P=[3]P+P, [5]P=[4]P+P* va hokazolar amalga oshiriladi.

Har doim ham $P(x_1,y_1)$ va $Q(x_2,y_2)$ nuqtalar orqali o‘tuvchi to‘g‘ri chiziq elliptik egri chiziqni uchinchi nuqtada kesib o‘tavermaydi. Masalan, $P(x_1,y_1)$ va $Q(x_1,-y_1)$ nuqtalardan o‘tuvchi to‘g‘ri chiziq Ox-o‘qiga perpendikulyar bo‘lib, u elliptik egri chiziqni uchinchi nuqtada kesib o‘tmaydi:



Bunday holda o‘tkazilgan to‘g‘ri chiziq elliptik egri chiziqni cheksizlikda kesib o‘tadi deb qabul qilinib, cheksizlikdagi barcha nuqtalar bitta nol nuqtaga birlashtirilgan deb hisoblanadi, ya’ni cheksizlikdagi barcha nuqtalar, elliptik egri chiziq nuqtalari ustida aniqlangan qo‘shish amaliga nisbatan, haqiqiy sonlarni qo‘shishdagi nol qiymati kabi xossaga ega. Haqiqatan ham, $P(x_1, y_1)$ va $Q(x_1, -y_1)$ nuqtalardan o‘tuvchi to‘g‘ri chiziq Ox-o‘qiga perpendikulyar bo‘lib, u elliptik egri chiziqni uchinchi nuqtada kesib o‘tmay, cheksizlikdagi 0_E nuqtaga yo‘naladi. Cheksizlikdagi 0_E nuqta bilan $P(x_1, y_1)$-nuqtani qo‘shishni $0_E + P(x_1, y_1)$ shaklida ko‘rib chiqadigan bo‘lsak, bu nuqtalardan o‘tuvchi to‘g‘ri chiziq Ox-o‘qiga perpendikulyar bo‘lib, elliptik egri chiziqni $Q(x_1, -y_1)$- nuqtada kesib o‘tadi, so‘ngra $0_E + P(x_1, y_1)$ -yig‘indini ifodalovchi nuqtani topish uchun bu $Q(x_1, -y_1)$-nuqta Ox- o‘qiga simmetrik akslantirilsa, $P(x_1, y_1)$- nuqta bilan ustma-ust tushadi, ya’ni kiritilgan qo‘shish amali qoidasiga ko‘ra $0_E + P(x_1, y_1) = P(x_1, y_1)$ tenglik o‘rinli bo‘ladi. Bu 0_E nuqta Ox- o‘qiga nisbatan akslantirilsa, yana qarama-qarshi tomon cheksizligidagi (-0_E) - nuqtaga yo‘naladi. Ammo, cheksizlikdagi barcha nuqtalar bitta nol nuqtaga birlashtirilganda $(-0_E) + P(x_1, y_1) = P(x_1, y_1)$ tenglikning o‘rinli bo‘lishiga keltirilgan fikr-mulohozalar asosida ham ishonch hosil qilish mumkin.

Bevosita hisoblashlar bilan ko‘rsatish mumkinki, elliptik egri chiziq nuqtalarini qo‘shish amali Abel gruppasini tashkil etadi, yani elliptik egri chiziqqa tegishli bo‘lgan a, b, c - nuqtalar uchun:

1) kommutativlik $a + b = b + a$;

2) assosiativlik $(a + b) + c = (b + c) + a$;

3) nol elementining mavjudligi $a + 0_E = a$;

4) teskari (qarama-qarshi ishorali) elementning mavjudligi $a + (-a) = 0_E$ kabi Abel gruppasining aksiomalari o‘rinlidir.

Elliptik egri chiziqning nuqtalarini qo‘shish formulalari uning geometrik ma’nosidan kelib chiqqan holda keltirib chiqariladi. Ko‘rib o‘tilganlarga muvofiq, agar $P(x_1, y_1)$ va $Q(x_2, y_2)$- nuqtalar E-elliptik egri chiziqda yotsa, ya’ni $P(x_1, y_1)$, $Q(x_2, y_2) \in E$ nuqtalar bo‘lsa, unda ular orqali kesuvchi to‘g‘ri chiziq o‘tkazilib, bu kesuvchi to‘g‘ri chiziq E-elliptik egri chiziqni biror uchinchi $R(x_3, y_3)$ nuqtada kesib

o‘tadi.

3-tasdiq. Agar $P(x_1, y_1)$, $Q(x_2, y_2) \in E$ nuqtalar rasional koordinatali bo‘lsa, u holda $R(x_3, y_3)$ nuqta koordinatalari ham rasional bo‘ladi.

Isboti. $P(x_1, y_1)$, $Q(x_2, y_2) \in E$ nuqtalar orqali o‘tuvchi to‘g‘ri chiziqning umumiy ko‘rinishi:

$$y = kx + d$$

ifodaga ega bo‘lib, bu yerda k, d – koeffisiyentlar $P(x_1, y_1)$ va $Q(x_2, y_2)$ nuqtalarning koordinatalari orqali ifodalanadi. $P(x_1, y_1)$, $Q(x_2, y_2)$ - nuqtalar $y = kx + d$ chiziqqa tegishli. Bundan esa:

$$\begin{cases} y_1 = kx_1 + d, \\ y_2 = kx_2 + d, \end{cases}$$

ekanligi kelib chiqadi. $y_1 - y_2 = k(x_1 - x_2)$ ва $k = \dfrac{y_1 - y_2}{x_1 - x_2}$,

Shuningdek,

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

Shunday qilib, $u = k\,x + d$ to‘g‘ri chizig‘i tiklab olindi. Keyingi qadamda

$u = kx + d$ – ifoda $y^2 = x^3 + ax^2 + bx + c$,

elliptik egri chiziqning tenglamasiga qo‘yiladi, yani

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

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

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

tenglik o‘rinli bo‘lib, bu oxirgi tenglikda x_1, x_2 - rasional sonlar bo‘lgani uchun, x_3 ham rasional son bo‘ladi. Xuddi shuningdek,

$$y_3 = kx_3 + d$$

ifodaga ko‘ra y_3 - sonining ham rasional ekanligi kelib chiqadi.

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

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

chunki $u = x_3,\quad v = -y_3.$ Bu formulada k-koeffisiyenti qiymatining o‘rniga $\frac{y_1 - y_2}{x_1 - x_2}$ qo‘yilsa, quyidagi tengliklar hosil bo‘ladi:

$$\begin{cases} v = \frac{y_1 - y_2}{x_1 - x_2}(-u + x_1) - y_1, \\ u = \frac{(y_1 - y_2)^2}{(x_1 - x_2)^2} - (a + x_1 + x_2) \end{cases} \quad (7)$$

Bu yerda, $x_1 \neq x_2$.

Agar $x_1 = x_2$ bo‘lsa, u holda kesuvchi to‘g‘ri chiziq o‘rniga urinma o‘tkazilib, quyidagi formulalar keltirib chiqariladi:

$$\begin{cases} u = -2x_1 - a + \frac{(3x_1^2 + 2ax_1 + b)^2}{4y_1^2}, \\ v = -y_1 - \frac{3x_1^2 + 2ax_1 + b}{2y_1}(u - x_1). \end{cases} \quad (8)$$

Shunday qilib, hyech bo‘lmasa bitta P- rasional nuqta elliptik egri chiziqdagi nuqta bo‘lsa, u holda (7), (8) - formulalar orqali *[2]P*-ni topish uchun, *[2]P=P+P*, *[3]P*-ni topish uchun, *[3]P=[2]P+P*, shu kabi *[4]P=[3]P+P*, *[5]P=[4]P+P* va hokazolarni topishimiz mumkin bo‘ladi.

Shuni alohida ta’kidlash kerakki, keltirilgan (7) va (8) formulalar (3) tenglamaga nisbatan keltirib chiqarildi. Endi elliptik egri chiziqning kriptografiyada keng qo‘llaniladigan

$$y = x^3 + ax + b$$

tenglamasi uchun rasional nuqtalarini qo‘shish formulalari keltirib o‘tiladi:

$$\begin{cases} u = \frac{(y_1 - y_2)^2}{(x_1 - x_2)^2} - x_1 - x_2, \\ v = -y_1 + \frac{y_1 - y_2}{x_1 - x_2}(x_1 - u). \end{cases} \quad (9)$$

bu yerda, $x_1 \neq x_2$.

Agar $x_1 = x_2$ bo‘lsa, u holda

$$\begin{cases} u = \dfrac{(3x_1^2 + a)^2}{4y_1^2} - 2x_1, \\ v = -y_1 - \dfrac{3x_1^2 + a}{2y_1}(x_1 - u). \end{cases} \qquad (10)$$

Oldindan berilgan $y^2 = x^3 + ax^2 + bx + c$ - EECh rasional nuqtalarini topishning samarali usulini aniqlash hozirgi kunda sonlar nazariyasining muammolaridan biri hisoblansada, egri chiziqqa tegishli bitta nuqta topilsa, qolganlari (7), (8) formulalar orqali aniqlanadi.

EECh nuqtalarini qo‘shish jarayonida quyidagi ikkita holat bo‘lishi mumkin:

1. Biror *n* –qadamda $[n]P = 0_E$ tenglik bajarilishi mumkin;
2. *[2]P, [3]P, [4]P* va hokazo *[n]P* – nuqtalar har xil qiymatga ega bo‘lishi mumkin.

3.25-ta’rif. Agar barcha $m < n$ holatlarda $[m]P \neq 0_E$ bajarilib, $[n]P = 0_E$ bo‘lsa, u holda P – nuqta n – chekli tartibga ega deyiladi.

3.6.3. Maydon ustida berilgan parametrli elliptik egri chiziq nuqtalari gruppasi

3.6.3.1. Parametrli elliptik egri chiziq nuqtalari gruppasi

Oshkora kriptografiyaning an’anaviy elliptik egri chiziq (EECh)li nosimmetrik kriptotizimlaridan qo‘shimcha maxfiylikka ega bo‘lgan yangi kriptotizimlarga o‘tish dolzarb muammo hisoblanadi.

Quyida an’anaviy EEChlar asosida shakllantirilgan parametrli algebraik gruppa haqida so‘z boradi [55].

Ma’lumki, foydalanish uchun qulay bo‘lgan EECh tenglamalarining ko‘pchiligi Veyershtrass [56-58] tenglamasini umumlashgan shaklining xususiy hollaridir. Shu jumladan, GOST R 34.10-2001ga asos qilib olingan Veyershtrass tenglamasi umumlashgan shaklining xususiy holi

$$y_0^2 \equiv x_0^3 + ax_0 + b$$

ko‘rinishga ega bo‘lib, o‘zgaruvchilarni va koeffisiyentlarni almashtirish, parametr *R* ni kiritish orqali quyidagi modulyar ko‘rinishga keltiriladi:

$$y^{\backslash 2} \equiv x^{\backslash 3} + ax + B \ (mod\ p),$$

bu yerda:

$B \equiv (a+b)\ R^{-1} (mod\ p)$,

$y^{\backslash 2} \equiv (y_0^2-1)\ R^{-1} (mod\ p)$,

$y \equiv (y_0-1)\ R^{-1} (mod\ p)$,

$y \equiv (x^{\backslash 3}+ax+B)^{\backslash 0.5} (mod\ p)$,

$y^{-} \equiv -(y+2\ R^{-1})\ (mod\ p)$,

$x^{\backslash 3} \equiv (x_0^3-1)\ R^{-1} (mod\ p)$,

$x \equiv (x_0-1)\ R^{-1}\ (mod\ p)$,

y_0, x_0, y, y^{-}, x - o‘zgaruvchilar,

a, B - butun sonli koeffisiyentlar,

R – parametr, $0<R< n$, $(R; n)=1$ shartlarini qanoatlantiradi**.**

$Q_1=(x_1, y_1)$ va $Q_2=(x_2, y_2)$ nuqtalar ustida ***parametrli qo‘shish*** amali “$+^{\backslash}$ **“** bilan belgilanadi va $Q_3 = Q_1 +^{\backslash} Q_2$ ko‘rinishida ifodalanadi. (x_1, y_1) va (x_2, y_2) nuqtalar ustida ***parametrli qo‘shish*** quyidagi taqqoslamalar asosida amalga oshiriladi:

1) $x_1 \neq x_2$ hol uchun $Q_3=(x_3, y_3)$**:**

$x_3 \equiv (L^2-3)R^{-1}-x_1- x_2)\ (mod\ p)$, (11)

$y_3 \equiv L(x_1- x_3)+ y_1^{-}\ (mod\ p)$, (11’)

bu yerda:

$L \equiv (y_2- y_1)\ (x_2- x_1)^{-1}\ (mod\ p)$;

2) $x_1=x_2$, $y_1= y_2 \neq 0$ hol uchun $Q_3=(x_3, y_3)$:

$x_3 \equiv (L^2-3)R^{-1}-2x_1\ (mod\ p)$, (12)

$y_3 \equiv L(x_1- x_3) + y_1^{-}\ (mod\ p)$, (12’)

bu yerda: $L \equiv (3(R\ x_1^{\backslash 2}+1)+a)(2(R\ y_1+1))^{-1}\ (mod\ p)$;

3) $x_1=x_2$, $y_2= y_1^{-}$ hol uchun $Q_1=(x_1, x_2)$ va $Q_2=(x_2, y_1^{-})$ nuqtalarning ***parametrli*** yig‘indisi nollik (cheksizlikdagi) nuqta 0_E ga teng.

Nollik nuqta uchun $Q+^{\backslash} 0_E = 0_E +^{\backslash} Q = Q$ (13)
tenglik o‘rinlidir.

EECh nuqtasini o‘ziga o‘zini d marta parametrli qo‘shish natijasi nuqtani skalyar son d ga ko‘paytirish amalini beradi. EECh nuqtasini skalyar son d ga ko‘paytirish amali “ $*^{\backslash}$ “ belgisi bilan ifodalanadi.

Shuni ta’kidlash kerakki, Veyershtrass [56-58] umumiy ko‘rinishdagi tenglamasining qolgan barcha xususiy hollari bo‘lgan EECh tenglamalari uchun ham yuqorida keltirilgan EECh nuqtalari ustida parametrli qo‘shish $+^{\backslash}$ va EECh nuqtasini skalyar son d ga

ko‘paytirish amali $*^{\backslash}$ ni aniqlash hyech qanday qiyinchilik tug‘dirmaydi.

EECh barcha nuqtalari ustida parametr $R \geq 1$ bilan qo‘shish amali chekli additiv kommutativ gruppani tashkil etadi.

3.26-ta’rif. $PE(F_n) = \{$parametrli EECh nuqtalari$\} U\{0_E\}$, ya’ni parametrli EECh barcha nuqtalari to‘plami va nollik nuqta, parametr $0 < R \in F_n$ bo‘lsa, $+^{\backslash}$ – $PE(F_n)$ ustida aniqlangan parametrli qo‘shish amali bo‘lsa, $(PE(F_n); +^{\backslash})$ – juftlik parametrli EECh nuqtalari gruppasi deb ataladi.

An’anaviy EECh va parametrli EECh nuqtalari to‘plamlari o‘zaro izomorfligi tufayli ***additiv kommutativ gruppaning*** barcha aksiomalari parametrli EECh nuqtalari gruppasini ham qanoatlantiradi.

Bu holat parametrli EECh nuqtalari gruppasi asosida qo‘shimcha maxfiylikka ega bo‘lgan bir tomonlama funksiyalar asosida mavjud kriptotizimlarga analog bo‘lgan yangi kriptotizimlarni va yangi kriptotahlillash usullarini yaratishga yo‘l ochadi.

3.6.3.2. Parametrli elliptik egri chiziq funksiyasi xossalarining elliptik egri chiziq funksiyasiga o‘xshash xossalari

Avvalgi bandda keltirilgan parametrli EECh nuqtalari gruppasi $(PE(F_p); +^{\backslash})$ dan foydalanish qo‘shimcha maxfiy parametr R tufayli hozircha ma’lum bo‘lmagan oshkormas EECh parametri muammosi yuzaga kelishi va buning oqibatida kriptobardoshlilik ortishi qayd etilgan edi.

Parametrli EEChlardan foydalanishga asoslangan algoritmlar bardoshliligi ular maxsus apparatli modul sifatida amalga oshirilganda eng yuqori darajada bo‘lishi [55] da izohlangan.

3.27-ta’rif. $y^{\backslash 2} \equiv x^{\backslash 3}+ax+B \pmod p$ taqqoslamani qanoatlantiruvchi EECh nuqtalari gruppasi $PE(F_p)$ da EECh nuqtasini parametrlar uchligi $<R, a, B>$ bilan skalyar songa ko‘paytirish $(*^{\backslash})$ funksiyasi parametrli EECh funksiyasi deb ataladi.

Bu yerda:

$y \equiv (x^{\backslash 3}+ax+B)^{\backslash 0.5} \pmod p$,

$y^{-} \equiv -(y+2R^{-1}) \pmod p$,

a, B – butun sonli koeffisiyentlar,

R – parametr, $0 < R < p$, $(R; p)=1$ shartlarini qanoatlantiradi**,**

q – parametrli EECh nuqtalari tartibi,

p – tub son.

G nuqtani skalyar son d ga parametrli ko‘paytirish natijasi $d*^{\backslash}G$ shaklida ifodalangan, $^{\backslash}$ – R parametrli darajaga oshirish belgisi, $*^{\backslash}$ – skalyar songa parametr R bilan ko‘paytirish belgisi**.**

Parametrli EECh funksiyasi xossalarining EECh funksiyasiga o‘xshash xossalariga ***quyidagilar kiradi:***

2.3.1-xossa. $(d_1+d_2 \bmod q)*^{\backslash}G = (d_2*^{\backslash}G)+^{\backslash}(d_1*^{\backslash}G)$, bu yerda d_1, $d_2 \in\{1,2,.\ ..,\ q-1\}$; an’anaviy (parametrsiz) nuqtani skalyar songa ko‘paytirish funksiyasida $(d_1 +d_2 \bmod q)”*” G = (d_2”*” G)\ “+”(\ d_1\ ”*”G)$.

Misol.

p	q	G		d_2	d_1	$d_2*^{\backslash}G$		$d_1*^{\backslash}G$		d_1+d_2	$(d_2+d_1)*^{\backslash}G$	
29	37	13	3	7	8	27	25	0	13	15	15	27

2.3.2-xossa. $(d_1d_2 \bmod q)*^{\backslash}G = d_2*^{\backslash}\ (d_1\ *^{\backslash}G)$, bu yerda d_1, $d_2 \in\{1,2,.\ ..,\ q-1\}$; an’anaviy (parametrsiz) nuqtani skalyar songa ko‘paytirish funksiyasida $(d_1d_2 \bmod q)\ ”*”G = d_2”*”(\ d_1\ ”*”G)$.

Misol.

p	q	G		d_2	d_1	$d_2*(d_1*^{\backslash}G)$		$d_1*^{\backslash}G$		d_1*d_2	$(d_2*d_1)*^{\backslash}G$	
29	37	13	3	7	8	24	3	0	13	19	24	3

2.3.3-xossa. $q*^{\backslash}G = 0_E$, $(q+1)*^{\backslash}G = G$, $1*^{\backslash}G = G$, $1*^{\backslash}G = G$, $0_E*^{\backslash}G = 0_E$, $d_1*^{\backslash}(d_2\ *^{\backslash}G) = d_2\ *^{\backslash}(d_1*^{\backslash}G)$, bu yerda q **-** parametrli EECh nuqtalari tartibi; an’anaviy (parametrsiz) nuqtani skalyar songa ko‘paytirish funksiyasida $q”*^{”}G=0_E$, $(q+1)”*^{”}G=G$, $1”*^{”}G=G$, $0_E”*^{”}G=0$, $d_1”*^{”}(d_2”*^{”}G)=d_1”*^{”}(d_1”*^{”}G)$.

Misol.

p	q	R	G		d_1	d_2	$d_1*\backslash G$		$Y_2=d_2*^{\backslash}G$	
29	37	1	4	21	11	23	16	18	9	3

d_1	$d_1*^{\backslash}Y_2$		d_2	$d_2*^{\backslash}Y_1$	
11	12	5	23	12	5

2.3.4-xossa. Agar *d, e q* moduli bo‘yicha o‘zaro teskari juftlik bo‘lsa, unda $d *^{\backslash} G = S$, $e *^{\backslash} S = G$, $e *^{\backslash} (d *^{\backslash} G) = G$,

bu yerda *G* - dastlabki matnga tegishli *S* - shifrlangan matnga tegishli parametrli EECh ning tartibi *q* bo‘lgan nuqtalari; an’anaviy (parametrsiz) nuqtani skalyar songa ko‘paytirish funksiyasida $d''*''G=S$, $e''*''S=G$, $e''*''(d''*''G)=G$.

Misol.

p	*q*	*R*	*G*		*d*	$S=d*^{\backslash} G$		d^{-1}	$G= d^{-1} *^{\backslash} S$	
29	*37*	*7*	*13*	*3*	*8*	*0*	*13*	*14*	*13*	*3*

Yuqorida keltirilgan 1-4 xossalar an’anaviy EECh funksiyasi xossalariga o‘xshash bo‘lib, ulardan birinchisi va ikkinchisi parametrli EECh funksiyasi qiymatini istalgan skalyar son uchun samarali hisoblash uchun yetarlidir. Bu yerda, katta skalyar songa parametrli ko‘paytirish jarayoni eksponensial funksiyani hisoblash jarayoni kabi kechib, *d* ni *2* ning darajalari yig‘indisi sifatida ifodalashga va davriy tarzda yig‘indini tashkil etuvchi *2* ning daraja ko‘rsatkichi, agar juft qiymatli bo‘lsa, *2* ga parametrli ko‘paytirish, aks holda joriy qiymatni berilgan nuqtaga parametrli ko‘paytirish amallaridan foydalanishdan iborat bo‘ladi.

1-4 xossalar an’anaviy EECh funksiyasi xossalaridan foydalanishga asoslangan kriptografik tizimlarga o‘xshash kriptotizimlar yaratishga imkon beradi.

3.7. Ko‘phadlar to‘plami. Algebraning asosiy teoremasi

Agar *q* son *p* tub sonning darajasi bo‘lsa $q=p^m$, u holda bunday maydonning elementlari koeffisiyentlari *GF*(*p*) - oddiy maydon elementlaridan iborat (*m*-1)-darajagacha *ko‘phadlar to‘plamini* o‘z ichiga oladi. Bunday ko‘phadlarni qo‘shish va ko‘paytirish ko‘phadlarni oddiy qo‘shish va ko‘paytirish qoidalari bo‘yicha bajarilib, hosil bo‘lgan ko‘phad asos sifatida olingan *m*-darajali $g_m(x)$-ko‘phadga bo‘lishdan hosil bo‘lgan qoldiq natija sifatida qabul qilinadi. Berilgan ko‘phadni biror asos sifatida olingan $g_m(x)$-ko‘phad bo‘yicha modulini $(mod g_m(x))$ hisoblash ushbu $a(x)=b(x)$ (mod g_m)(x) taqqoslama bilan bog‘liq: unda $a(x)$ va $b(x)$ ko‘phadlar $g_m(x)$-modul

bo‘yicha teng (yoki taqqoslanuvchi) deyiladi, agarda bu ko‘phadlarni $g_m(x)$-ko‘phadga bo‘linganda bir xil qoldiqqa ega bo‘lsa yoki $a(x)$-$b(x)$ – ko‘phad $g_m(x)$-ko‘phadga qoldiqsiz bo‘linsa. Shunday qilib, ko‘phadlarni taqqoslash butun sonlarni taqqoslash kabi tushuncha ekanligi kelib chiqadi. Asos sifatida olingan $g_m(x)$-ko‘phadni koeffisiyentlari $GF(p)$-oddiy maydon elementlaridan iborat bo‘lgan ko‘phadlarning ko‘paytmasi shaklida ifodalash imkoniyati yo‘qligi xususiyatiga ega. Bunday ko‘phad keltirilmaydigan deyiladi va mohiyatiga ko‘ra tub sonlarga o‘xshashdir. Misol uchun, koeffisiyentlari $GF(2)$-oddiy maydon elementlaridan *{0;1}* iborat bo‘lgan $g_3(x)=1+x+x^3$ – keltirilmaydigan ko‘phad bo‘lib, undan $GF(8)$-kengaytirilgan maydonni qurishda foydalanish mumkin. $GF(8)$-kengaytirilgan maydon elementlari: 1, x, x^2, $1+x$, $1+x^2$, $x+x^2$, $1+x+x^2$.

Algebraning asosiy teoremasi. Darajasi *1* dan kichik bo‘lmagan kompleks koeffisiyentli har qanday ko‘phad kamida bitta kompleks ildizga ega.

Toq darajali ko‘phad doimo ildizga ega ekanligi ma’lum. Bundan kompleks koeffisiyentli darajasi *1* dan kichik bo‘lmagan juft darajali ko‘phadlar kamida bitta kompleks ildizga ekanligi o‘z isbotini topadi.

Quyida algebra asosiy teoremasining ba’zi natijalarini keltiramiz.

1-natija. Kompleks sonlar maydonidagi n-darajali ko‘phadning n ta ildizi mavjud.

2-natija. n-darajali $f(x)$ ko‘phad x ning n tadan ortiq har xil qiymatlarida nolga teng bo‘lsa, unda $f(x)$ nol ko‘phad bo‘ladi.

3-natija. Darajalari n dan yuqori bo‘lmagan $f(x)$ va $\varphi(x)$ ko‘phadlar x ning n tadan ortiq har xil qiymatlarida bir-biriga teng bo‘lsa, unda $f(x)$ va $\varphi(x)$ ko‘phadlar o‘zaro teng ko‘phadlar bo‘ladi.

3.8. Sonlar nazariyasi elementlari

Sonlar nazariyasi kriptografik masalalarning tadqiq qilinishi hamda ularning yechimlarida muhim rol o‘ynaydi.

Natural sonlar to‘plamini $N=\{1, 2,3, \dots\}$ va butun sonlar to‘plamini $Z=\{0, \pm 1, \pm 2, \pm 3, \dots\}$ ko‘rinishda belgilaymiz.

Noldan farqli bo‘lgan a soni va b sonlar Z –to‘plamga tegishli, ya’ni

$a, b \in Z$ bo‘lib, $a \neq 0$ bo‘lsin, agarda shunday s soni mavjud bo‘lib, $b = as$ tenglik bajarilsa, u holda a soni b sonini bo‘ladi, deyiladi.

3.8.1. Eng katta umumiy bo‘luvchi

Berilgan a va v sonlarni bo‘luvchi butun son, ularning *umumiy bo‘luvchisi* deyiladi. Umumiy bo‘luvchilar ichida eng kattasi *eng katta umumiy bo‘luvchi* (EKUB) deyiladi va EKUB(a, b) ko‘rinishda belgilanadi. Agarda a va b sonlarning eng katta umumiy bo‘luvchisi 1, EKUB (a, b)=1 bo‘lsa, a va b sonlar *o‘zaro tub* deyiladi. Eng katta umumiy bo‘luvchilarni topishga oid tasdiqlarni keltiramiz.

1-lemma. Agar b soni a sonini bo‘lsa, u holda bu sonlarning eng katta umumiy bo‘luvchisi EKUB (a, b)= b, ya’ni a sonining umumiy bo‘luvchilari to‘plami b sonining umumiy bo‘luvchilari to‘plami bilan ustma-ust tushadi.

2-lemma. Agar $a=bq+c$ bo‘lsa, u holda a va b sonlarining eng katta umumiy bo‘luvchisi b va s sonlarining eng katta umumiy bo‘luvchisi bilan ustma-ust tushadi, ya’ni EKUB (a, b)= EKUB (b, c): a va b sonlarining umumiy bo‘luvchilari to‘plami b va s sonlarining umumiy bo‘luvchilari to‘plami bilan ustma-ust tushadi.

Yuqorida keltirilgan lemmalardan EKUBni topish – Yevklid algoritmi kelib chiqadi.

Haqiqatan ham quyidagi bo‘lish amallarini bajaramiz:

$$a=bq_1+r_1,\ 0 \le r_1<b,$$
$$b=r_1q_2+r_2,\ 0 \le r_2<r_1,$$

$$\dots\dots\dots,\ \dots\dots\dots,$$

$$r_{n-2}=r_{n-1}\,q_n+r_n,\ 0 \le r_n<r_{n-1},$$
$$r_{n-1}=r_nq_{n+1.}$$

U holda EKUB (a, b)= EKUB (b, r_1)=…=(r_{n-2}, r_{n-1})= r_n .

Berilgan natural son $p>1$ tub deyiladi, agarda bu son o‘zi p va 1 dan boshqa natural songa bo‘linmasa. Misol uchun: *2, 3, 5, 7, 11, 13, 17, 19, 23, 29,* ..., tub sonlar, ular sanoqli va cheksiz quvvatli to‘plamni tashkil etadi.

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

$$a=qn+r, \text{ bu yerda } 0\le r<n,$$

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

3.8.2. Taqqoslamalar

Butun *a* va *b* sonlari *modul n bo‘ycha taqqoslanadigan* deyiladi, agarda ularni *n* ga bo‘lganda qoladigan qoldiqlari teng bo‘lsa,

$$a\equiv b(mod\ n)$$

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

Qoldiqni ifodalash uchun ushbu

$$b=a\ (mod\ n)$$

tenglikdan foydalaniladi hamda $b=a\ (mod\ n)$ tenglikni qanoatlantiruvchi *b* sonini topish *a sonini modul n bo‘yicha keltirish* deyiladi.

Ixtiyoriy butun *b* soni uchun ushbu

$$M=\{a_0, a_1, \dots, a_{n-1}\in Z: 0\le a_k\le n-1;\ k=0,1,\dots,n-1\}$$

to‘plamga tegishli $a_k\equiv b\ (mod\ n)$ munosabatni qanoatlantiruvchi son a_k, $k\in\{0,1,\dots, n-1\}$ mavjud bo‘lsa, to‘plam *M* modul *n* bo‘yicha *to‘liq chegirmalar sinfi* deyiladi. Ko‘rinib turibdiki, to‘liq chegirmalar *sinfi*

$$M=\{a_0, a_1, \dots, a_{n-1}\in Z: 0\le a_k\le n-1;\ k=0,1,\dots,n-1\}=\{0,1,\dots,n-1\}.$$

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

$$(a+b)(\mathrm{mod}\ n)=((a \bmod n)+(b \bmod n))(\mathrm{mod}\ n),$$
$$(a-b)(\mathrm{mod}\ n)=((a \bmod n)-(b \bmod n))(\mathrm{mod}\ n),$$
$$(ab)(\mathrm{mod}\ n)=((a \bmod n)\,(b \bmod n))(\mathrm{mod}\ n),$$
$$a(b+c)(\mathrm{mod}\ n)=(((ab) \bmod n)+(ac) \bmod n))(\mathrm{mod}\ n).$$

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

Bu keltirilgan teoremani quyidagicha ham ifodalash mumkin: *butun a va b sonlari o‘zaro tub bo‘lishi uchun, butun bo‘lgan u va v sonlari topilib, ular uchun au+bv=1 tenglikning bajarilishi zarur va yetarli.*

Agarda butun *a* va *b* sonlari o‘zaro tub bo‘lsa, ya’ni EKUB (*a*, *n*)=*1* bo‘lsa, u holda ushbu $aa' \equiv 1(\mathrm{mod}\ n)$ munosabatni qanoatlantiruvchi butun a' soni mavjud bo‘lib, bu a' *son a soniga modul n bo‘yicha teskari* deyiladi hamda $a' \equiv a^{-1}(\mathrm{mod}\ n)$ deb belgilanadi. Teskari a' elementni *a* va *n* sonlarining chiziqli kombinasiyasidan iborat bo‘lgan ularning EKUB ifodasidan $au+bn=1$ foydalangan holda, bu tenglikning har ikkala tomonini modul *n* bo‘yicha keltirish (hisoblash) bilan $a' \equiv u\ (\mathrm{mod}\ n)$ ekanligi topiladi.

Quyida teskari elementni hisoblashning yana bir usuli keltiriladi.

Berilgan *n* soni bilan o‘zaro tub bo‘lgan *(1; n)* oraliqdagi barcha elementlarning soni bilan aniqlanuvchi $\varphi(n)$ funksiyaga *Eyler funksiyasi* deyiladi:

$\varphi(n)=|M|$, bu yerda $|M|$ M – to‘plamning quvvati, $M=\{m_i \in N : 1 \le m_i \le n;\ \ (m_i, n)=1\}$.

Agarda $n=p_1^{k_1} \cdot \ldots \cdot p_t^{k_t}$ bo‘lib, $p_1,\ldots,p_t$ - har xil tub sonlar bo‘lsa, u holda Eyler funksiyasining qiymati $\varphi(n)=\prod_{j=1}^{t}(p_j-1)\cdot p_j^{k_j-1}$ ifoda bilan hisoblanadi.

Fermaning kichik teoremasi deb ataluvchi ushbu tasdiq o‘rinli, agar *n* – tub son bo‘lsa, $a^{n-1} \equiv 1(\mathrm{mod}\ n)$ o‘rinli.

Eyler tomonidan olingan, *Ferma kichik teoremasining umumlashgani* deb ataluvchi ushbu tasdiq o‘rinli, agar *n* – tub son bo‘lsa, $a^{\varphi(n)} \equiv 1(\mathrm{mod}\ n)$ munosabat bajariladi.

Yuqoridagilardan kelib chiqqan holda, $a^{-1} \equiv a^{\varphi(n)-1}(\mathrm{mod}\ n)$ munosabatning o‘rinligiga ishonch hosil qilinadi.

Agar *n*–tub son bo‘lsa, u holda $\varphi(n)=n-1$. Agar *n=pq* bo‘lib, *p* va *q*–tub sonlar bo‘lsa, u holda $\varphi(n)=(p-1)(q-1)$. Bu kabi xossalardan ochiq kalitli kriptoalgoritmlar yaratishda foydalaniladi. Masalan, qanday son modul 7 bo‘yicha 5 soniga teskari ekanligini topaylik. Bu yerda, *7* soni tub bo‘lgani uchun, uning Eyler funksiyasi $\varphi(7)=7-1$ =6, modul *7* bo‘yicha *5* soniga teskari son esa $a^{-1} \equiv a^{\varphi(n)-1} (mod\ n)$ formulaga ko‘ra $5^{-1}=5^{6-1}\bmod 7=5^5\bmod 7=3125\bmod 7$.

Haqiqatan ham, $5\cdot 3\bmod 7=15\bmod 7=1\bmod 7=1$. Biror modul bo‘yicha berilgan songa teskari bo‘lgan son har doim ham mavjud bo‘lavermaydi. Misol uchun, *5* soniga modul *14* bo‘yicha teskari son *3*: $5\cdot 3\bmod 14=15\bmod 14=1\bmod 14=1$. Ammo, *2* sonining modul *14* bo‘yicha teskarisi mavjud emas, ya’ni $2x\equiv 1\ (mod\ 14)$ yoki $2x=14k+1$ tenglama *x* va *k* noma’lumlarning butun qiymatlarida yechimga ega emas, chunki *x* va *k* noma’lumlarning butun qiymatlarida har doim tenglikning chap tomonida juft son, o‘ng tomonida esa toq son hosil bo‘ladi.

Umumiy holda, agar *a* va *n* sonlari o‘zaro tub bo‘lsa, tenglama $a^{-1} \equiv x$ mod *n* yagona yechimga ega bo‘ladi; agar *a* va *n* sonlari o‘zaro tub bo‘lmasa, tenglama $a^{-1} \equiv x$ (mod *n)* yechimga ega emas. Bevosita hisoblashlar asosida, ushbu (*ax*) mod *n* = *b* tenglama *a, n, b* – sonlarining qanday qiymatlar qabul qilishiga qarab yoki bir nechta yechimlarga ega bo‘lishi mumkinligiga yoki bitta ham yechimga ega bo‘lmasligiga ishonch hosil qilish mumkin.

Quyidagilarni ta’kidlash joiz: agar *a* soni *M* sonini bo‘lsa va *b* soni ham *M* sonini bo‘lsa, u holda bu $M \in N$ soni $a,b \in Z$ sonlarning *umumiy bo‘linuvchisi* (*karralisi*) deyiladi. Umumiy bo‘linuvchilar ichida eng kichigi *eng kichik umumiy bo‘linuvchi* deyiladi hamda [*a, b*] deb belgilanadi.

2-teorema. Agar $M \in N$ son $a,b \in Z$ sonlarning umumiy bo‘linuvchisi bo‘lsa, u holda *M* soni bu sonlarning eng kichik bo‘linuvchisi [*a, b*] ga ham bo‘linadi.

3-teorema. Ushbu [*a, b*] = *ab/ EKUB* (*a, b*) munosabat o‘rinli.

3.8.3 Kvadratik chegirmalar

Agar *p* – tub son va *0< a< p* bo‘lib, ushbu

$$x^2 \equiv a(mod\ r)$$

munosabatni qanoatlantiruvchi x – noma'lumning qiymatlari mavjud bo‘lsa, u holda a soni modul p bo‘yicha kvadratik chegirma hisoblanadi.

Misol uchun, $r=7$ bo‘lsa, kvadratik chegirma tashkil etuvchilar: *1, 2* va *4* sonlaridan iborat, ya'ni $a=1$, $a=2$ va $a=4$ qiymatlarda, ushbu taqqoslamalar

$$1^2=1\equiv 1(mod\ 7);\ 2^2=4\equiv 4(mod\ 7);\ 3^2=9\equiv 2(mod\ 7);\ 4^2=16\equiv 2(mod\ 7);$$

$$5^2=25\equiv 4(mod\ 7);\ 6^2=36\equiv 1(mod\ 7);$$

o‘rinli.

Noma'lum x ning quyidagi munosabatlarni:

$$x^2\equiv 3(mod\ 7);\ x^2\equiv 5(mod\ 7);\ x^2\equiv 6(mod\ 7),$$

qanoatlantiruvchi qiymatlari mavjud emas, shuning uchun $a=3$, $a=5$ va $a=6$ sonlari modul *7* bo‘yicha kvadratik chegirma emas, ya'ni berilgan kvadratik taqqoslamalar yechimga ega emas.

Modul p juft bo‘lsa, u holda $(p-1)/2$ ta kvadratik chegirma mavjud va shuncha kvadratik chegirma mavjud emas, ya'ni ushbu

$$x^2\equiv a(mod\ r)$$

munosabatni qanoatlantiruvchi x –noma'lum mavjud bo‘ladigan a parametrning mumkin bo‘lgan qiymatlari soni $(p-1)/2$ ta, bu munosabatni qanoatlantiruvchi x –noma'lum mavjud bo‘lmaydigan a parametrning mumkin bo‘lgan qiymatlari soni ham $(p-1)/2$ ta. Bundan tashqari, agarda a soni modul p bo‘yicha kvadratik chegirma bo‘lsa, u holda a uchun ikkita kvadrat ildiz mavjud bo‘lib, ulardan biri $[0;\ (p-1)/2]$ oraliqda, ikkinchisi $[(p-1)/2;\ p-1]$ oraliqda, shu bilan birga ulardan biri modul p bo‘yicha kvadratik chegirma bo‘ladi va u *bosh kvadratik ildiz* deyiladi.

3.8.4. Murakkab masalalar

Quyida nosimmetrik kriptotizimlar bardoshliligini ta'minlovchi murakkab masalalar (muammolar)ga to‘xtalib o‘tiladi.

Tub ko‘paytuvchilarga ajratish (faktorlash)

Berilgan sonni ko‘paytuvchilarga ajratish deganda, uning tub ko‘paytuvchilarini topish tushuniladi.

Misol uchun:

1) 100 soni *2, 2, 5* va *5* tub sonlaridan iborat koʻpaytuvchilarga ega, ya’ni *100=2·2·5·5;*

2) *6279* soni *3, 7, 13* va *23* tub sonlaridan iborat koʻpaytuvchilarga ega, ya’ni *6279=3·7·13·23.*

Berilgan sonni koʻpaytuvchilarga ajratish sonlar nazariyasining eng dastlabki masalalaridan biri hisoblanadi. Berilgan sonni (yoki toʻplamni) biror amal yoki xususiyatga koʻra uning tashkil etuvchilari orqali ifodalanishi shu sonni (yoki toʻplamni) faktorlash (ajratish) deyiladi. Sonni koʻpaytuvchilarga ajratish qiyin jarayon emas, ammo koʻpaytuvchilarga ajratilishi kerak boʻlgan sonning qiymati kattalashib borishi bilan uni koʻpaytuvchilarga ajratish jarayoniga sarflanadigan vaqt ham koʻpayib boradi. Shunday boʻlsada, koʻpaytuvchilarga ajratish jarayonini tezlashtiruvchi quyidagi algoritmlar mavjud [12-13]:

1. *Sonli maydon umumiy gʻalvir usuli* – oʻnlik sanoq tizimida 110 ta va undan koʻp razryadli (raqamli) sonlarni koʻpaytuvchilarga ajratishning ma’lum boʻlgan eng samarali (tez, kam vaqt sarflanadigan) algoritmi;

2. *Kvadratik gʻalvir usuli* – oʻnlik sanoq tizimida 110 tadan kam boʻlmagan razryadli (raqamli) sonlarni koʻpaytuvchilarga ajratishning ma’lum boʻlgan eng samarali (tez va kam vaqt sarflanadigan) algoritmi;

3. *EEChusuli* – oʻnlik sanoq tizimida tub koʻpaytuvchilarning razryadi (raqamlari soni) 43 tadan koʻp boʻlmagan sonlarni koʻpaytuvchilarga ajratishda foydalanilgan;

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

5. *Uzuluksiz kasrlar usuli* – qoʻllashga koʻp vaqt sarflanadi;

6. *Tanlab boʻlish usuli* – eng dastlabki usullardan boʻlib, koʻpaytuvchilarga ajratilishi kerak boʻlgan (berilgan) sonning kvadrat ildiziga teng va undan kichik boʻlgan har bir tub sonni berilgan sonni qoldiqsiz boʻlishi yoki boʻlmasligi tekshirib chiqilishi natijasida, berilgan sonning tub koʻpaytuvchilari aniqlanadi.

Modul n boʻyicha kvadrat ildiz. Agarda maydon xarakteristikasini ifodalovchi *n* soni ikkita tub sonning koʻpaytmasidan iborat boʻlsa, u holda sonning kvadrat ildizini modul *n* boʻyicha topish masalasini yechish *n* sonini koʻpaytuvchilarga ajratish masalasini yechish hisoblash nuqtai nazaridan teng kuchli

masalalar hisoblanadi. Ya'ni maydon xarakteristikasini ifodalovchi *n* sonining ko‘paytuvchilari ma'lum bo‘lsa, berilgan ixtiyoriy sonning kvadrat ildizini modul *n* bo‘yicha hisoblash qiyinchilik tug‘dirmaydi, aks holda hisoblashlar *n* sonining tub ko‘paytuvchilarini topish masalasi kabi murakkabliklarni o‘z ichiga oladi. Maydon xarakteristikasi yetarlicha katta bo‘lganda kriptobardoshliligi kvadrat ildizni hisoblash masalasining murakkabligiga asoslangan ochiq kalitli kriptoalgoritmlar mavjud.

Tub sonlar generasiyasi (ishlab chiqarish). Ochiq kalitli kriptoalgoritmlar asoslari yaratilishida tub sonlarning xossalaridan foydalaniladi. Biror berilgan sonni tub ko‘paytuvchilarga ajratish, uni tub yoki tub emasligini aniqlashga nisbatan murakkab bo‘lgan masala. Yetarli katta razryaddagi toq sonni tasodifiy tanlab olib, uni ko‘paytuvchilarga ajratish bilan tub yoki tub emasligini aniqlashdan ko‘ra, uni tubligini biror mavjud usul bilan tekshirish osonroq. Buning uchun turli ehtimollik testlari mavjud bo‘lib [12-13], sonning tubligini berilgan darajadagi ishonch bilan aniqlab beradi. Kriptobardoshliligi yetarli darajada katta razryadli sonni tub ko‘paytuvchilarga ajratish masalasining murakkabligiga asoslangan ochiq kalitli kriptoalgoritmlar mavjud.

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

$$y = a^x \bmod n.$$

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

$$a^x \equiv b(\bmod n)$$

munosabatni qanoatlantiruvchi *x* noma'lumning butun qiymatlari har qanday *n* lar uchun ham mavjud bo‘lavermaydi. Misol uchun, ushbu

$$3^x \equiv 7(\bmod 13)$$

munosabat *x* ning hyech bir butun qiymatida bajarilmaydi. *a*, *b*, *n* – parametrlarning yetarli katta qiymatlarida yuqorida keltirilgan masalaning yechimi yana ham murakkablashadi.

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

- tub sonlar maydonida $GF(p)$ diskret logarifmlash;

- xarakteristikasi asosi 2 bo‘lgan $GF(2^n)$ maydonda diskret logarifmlash;

- EEChnuqtalari ustida bajariladigan amallarni biror chekli F maydonda amalga oshirish masalalarini yechishning murakkabligi bilan bog‘liq bo‘lgan muammolar asosida ish ko‘riladi.

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

Nazorat savollari

1. Binar amal deb nimaga aytiladi?
2. Algebraik tuzilma deganda nimani tushunasiz?
3. Gruppa deb nimaga aytiladi va u qanday shartlarni bajarishi kerak?
4. Kommutativ gruppaga ta’rif bering?
5. Gruppoidga ta’rif bering?
6. Yarimguppa qanday gruppa?
7. Monoidga ta’rif bering?
8. Additiv gruppa deb nimaga aytiladi ?
9. Qanday gruppa multiplikativ gruppa deyiladi?
10. Qanday multiplikativ gruppa siklik deyiladi?
11. Parametrli gruppaga ta’rif bering?
12. Parametrli multiplikativ kommutativ gruppa qanday xossalarga ega?
13. Parametrli funksiyalarning diskret darajaga oshirish funksiyasi xossalariga o‘xshash xossalarini tushuntiring?
14. Halqaning ta’rifi va umumiy xossalari haqida ma’lumot bering?
15. Maydon deb nimaga aytiladi va u qanday shartlarni bajarishi kerak?
16. Gruppalar morfizmi deganda nimani tushunasiz?
17. Ko‘phadlar to‘plami deganda nimani tushunasiz?
18. Algebraning asosiy teoremasiga ta’rif bering?
19. Diamatrisalar algebrasiga ta’rif bering?

20. Diamatrisalar algebrasinng afzalligini qanday misollar bilan isbotlash mumkin?

21. EECh deb qanday chiziqqa aytiladi?

22. EECh qachon silliq deb ataladi va uni misollar bilan tushuntiring?

23. EEChga tegishli rasional nuqtalarni aniqlashning qanday usullarini bilasiz?

24. EEChlarning rasional nuqtalarini qo‘shish qanday amalga oshiriladi?

25. EEChga tegishli bo‘lgan nuqtalar uchun qanday aksiomalar o‘rinli?

26. EECh nuqtalarini qo‘shish formulalari qanday keltirib chiqariladi?

27. Parametrli EECh nuqtalari gruppasiga ta’rif bering?

28. Parametrli EECh funksiyasiga ta’rif bering?

29. Parametrli EECh funksiyasining xossalarini anxanaviy EECh funksiyasi xossalariga o‘xshash xossalarini tushuntiring?

30. Sonlar nazariyasining kriptografiya uchun ahamiyati nimada?

31. Eng katta umumiy bo‘luvchi deb nimaga aytiladi?

32. Taqqoslamalar haqida ma’lumot bering?

33. Kvadratik chegirma deganda nimani tushunasiz?

34. Nosimmetrik kriptotizimlar bardoshliligini ta’minlovchi qanday murakkab masalalar (muammolar)ni bilasiz?

35. Tub ko‘paytuvchilarga ajratish jarayonini tezlashtiruvchi qanday algoritmlar mavjud?

4. SIMMETRIK KRIPTOTIZIMLAR

Shifrlash algoritmlarining tasniflanishi [13] da atroflicha yoritilgan. Unda kalitlardan foydalanish qoidasiga koʻra shifrlar simmetrik va nosimmetrik sinflarga boʻlinishi taʼkidlanib, agar shifrlash va deshifrlash jarayonlari mos ravishda maxfiy maʼlumotni joʻnatuvchi va qabul qilib oluvchi tomonidan bitta kalit bilan amalga oshirilsa, bunday algoritm simmetrik shifrlash sinfiga kirishi taʼriflangan. Agar shifrlash jarayonida biror akslantirish orqali ochiq maʼlumot alifbosi belgilari shifrmaʼlumot alifbosi belgilariga almashtirilsa, bunday akslantirishga asoslangan shifrlash algoritmi *oʻrniga qoʻyishga asoslangan shifrlash* sinfiga kiradi. Agar shifrlash jarayonida biror akslantirish orqali ochiq maʼlumot alifbosi belgilarining oʻrinlari almashtirilsa, bunday shifrlash algoritmi *oʻrin almashtirishga asoslangan shifrlash* sinfiga kiradi. Oʻrin almashtirishga asoslangan shifrlash algoritmlarida ochiq maʼlumotni tashkil etuvchi alifbo belgilarining maʼnosi shifrmaʼlumotda ham oʻzgarmasdan qoladi. Oʻrniga qoʻyishga asoslangan shifrlash algoritmlarida shifrmaʼlumotni tashkil etuvchi alifbo belgilari maʼnosi ochiq maʼlumotni tashkil etuvchi alifbo belgilarining maʼnosi bilan bir xil boʻlmaydi. Shifrlash jarayonida oʻrniga qoʻyish va oʻrin almashtirish akslantirishlarining kombinasiyalaridan birgalikda foydalanilsa, bunday shifrlash algoritmi *kompozision shifrlash* sinfiga kiradi. Umuman olganda, oʻrniga qoʻyishga asoslangan shifrlash algoritmlari akslantirishlarining matematik modellari koʻp qiymatli funksiyalar bilan ifodalansada, amalda bir qiymatli (teskarisi mavjud boʻlgan, qaytar) funksiyalar bilan ifodalanuvchi akslantirishlarni qoʻllash qulaylik tugʻdiradi. Umumiy holda, oʻrniga qoʻyishga asoslangan shifrlash algoritmlari *bir qiymatli* va *koʻp qiymatli shifrlash* sinfiga boʻlinadi. Bir qiymatli shifrlash algoritmlarida ochiq maʼlumot alifbosi belgilarining har biriga shifrmaʼlumot alifbosining bitta belgisi mos qoʻyiladi. Koʻp qiymatli shifrlash algoritmlarida ochiq maʼlumot alifbosi belgilarining har biriga shifrmaʼlumot alifbosining ikkita yoki undan ortiq chekli sondagi belgilari mos qoʻyiladi, yaʼni ochiq maʼlumot alifbosining biror x_i belgisiga shifrmaʼlumot alifbosining chekli $\{y_{i1}, y_{i2}, ..., y_{it}\}$ toʻplamdan olingan biror y_{ij} , $(1 \le j \le t)$ belgisi mos qoʻyiladi.

Shifrlash algoritmlari, kalitlardan foydalanish turlariga koʻra, *simmetrik* va *nosimmetrik* sinflarga boʻlinadi. Agar shifrlash va

deshifrlash jarayonlari bir xil kalit bilan amalga oshirilsa, bunday shifrlash algoritmi simmetrik shifrlash algoritmi sinfiga kiradi. Agar shifrlash jarayoni biror k_1 kalit bilan amalga oshirilib, deshifrlash jarayoni $k_2 \neq k_1$ bo‘lgan k_2 kalit bilan amalga oshirilib, k_1 kalitni bilgan holda k_2 kalitni topish yechilishi murakkab bo‘lgan masala bilan bog‘liq bo‘lsa, bunday shifrlash algoritmi nosimmetrik shifrlash algoritmi sinfiga taalluqli bo‘ladi.

Shifrlash jarayoni ochiq ma’lumotni ifodalovchi elementar (masalan: bit, yarim bayt, besh bit, bayt) belgilarni shifrma’lumotni ifodalovchi elementar belgilarga akslantirish asosida amalga oshirilsa, bunday shifrlash algoritmi *oqimli (uzluksiz) shifrlash* sinfiga kiradi.

Shifrlash jarayoni ochiq ma’lumot alifbosi belgilarining ikki va undan ortiq chekli sondagi birikmalarini shifrma’lumot alifbosi belgilarining birikmalariga akslantirishga asoslangan bo‘lsa, bunday shifrlash algoritmi *blokli shifrlash* sinfiga kiradi.

Shifrlash jarayonida ochiq ma’lumot alifbosining biror alohida olingan a_i belgisi har doim shifrma’lumot alifbosining biror fiksirlangan b_j belgisiga almashtirilsa, bunday shifrlash algoritmi *bir alifboli shifrlash* sinfiga kiradi. Agar shifrlash jarayonining har xil bosqichlarida ochiq ma’lumot alifbosining biror alohida olingan a_i belgisi shifrma’lumot alifbosining har xil b_j, b_l, ..., b_t belgilariga almashtirilsa, bunday shifrlash algoritmi *ko‘p alifboli shifrlash* sinfiga kiradi.

Shifrlash jarayonida ochiq ma’lumot alifbosi belgilari yoki alifbo belgilari birikmalari biror amal bajarish bilan shifrma’lumot alifbosi belgilari yoki ularning birikmalariga almashtirilsa, bunday shifrlash algoritmi *gammalashtirilgan shifrlash* sinfiga kiradi.

Quyida o‘rniga qo‘yish va o‘rin almashtirishga asoslangan shifrlash algoritmlarining turkumlarining matematik asoslari alohida-alohida ko‘rib chiqiladi.

4.1. Bir alifboli va ko‘p alifboli o‘rniga qo‘yishlar

4.1.1. Oddiy o‘rniga qo‘yishga asoslangan shifrlash algoritmlarining jadvalli va analitik matematik modellari

Shifrlash algoritmlari ochiq ma’lumot alifbosi belgilarini shifrma’lumot belgilariga akslantirishdan iborat ekanligi yuqorida

ta’kidlangan edi. Akslantirishlar funksiyalari (kalit deb ataluvchi noma’lum) parametrga bog‘liq holda: jadval va analitik (formulali) ifoda ko‘rinishlarida berilishi mumkin. O‘rniga qo‘yishga asoslangan shifrlash algoritmlarining dastlabki namunalari bo‘lgan tarixiy shifrlash algoritmlarining deyarli hammasi jadval ko‘rinishida ifodalanadi. Ular haqidagi to‘liq ma’lumotlar [13] da mavjud. O‘rniga qo‘yishga asoslangan shifrlash algoritmlarining umumiy xususiyatini hisobga olib, bu sinfdagi algoritmlarni 4.1- jadval ko‘rinishida quyidagicha ifodalash mumkin.

4.1- jadval

O‘rniga qo‘yishga asoslangan shifrlash algoritmlari

Ochiq ma’lumot alifbosi (kirillcha belgilar)	A	B	...	...	Ya
Shifrma’lumot alifbosi (ikkilik sanoq tizimi belgilari)	$x_0^0 x_1^0 x_2^0 x_3^0 x_4^0$	$x_0^1 x_1^1 x_2^1 x_3^1 x_4^1$	...	...	$x_0^{31} x_1^{31} x_2^{31} x_3^{31} x_4^{31}$

Kirillcha alifbo belgilari soni *32* ta, shu *32* ta har xil belgilarni bitlar bilan ifodalash uchun besh bit kifoya, ya’ni $2^5 = 32$. Keltirilgan 4.1- jadvaldan foydalanib, kirillcha alifboda ifodalangan ochiq malumot belgilarini ularga mos keluvchi ikkilik sanoq tizimidagi besh bitlik belgilarga almashtirib shifrma’lumot hosil qilinadi, ya’ni $x_i^j \in \{0;1\}$. Agarda, keltirilgan jadvalda ochiq ma’lumot alifbosi belgilariga shifrma’lumot alifbosining qanday besh bitlik belgilari mos qo‘yilganligi noma’lum bo‘lsa, bu jadval kalit bo‘lib, shifrma’lumotdan ochiq ma’lumotni tiklash masalasi murakkablashadi. Bunday shifrlash jarayonini ifodalovchi algoritm kalitlarining umumiy soni $32!$ bo‘lib, ushbu $n! \approx \left(\frac{n}{e}\right)^n \sqrt{2\pi n}$ - Stirling formulasiga ko‘ra quyidagicha $32! = \left(\frac{32}{2{,}7}\right)^{32} \sqrt{2 \cdot 3{,}14 \cdot 32} > \left(\frac{32}{4}\right)^{32} \sqrt{2 \cdot 2 \cdot 32} > \left(\frac{32}{4}\right)^{32} \sqrt{2 \cdot 2 \cdot 32} = 2^{96} \cdot 2^3 \cdot \sqrt{2} > 2^{99}$ hisoblanadi. Bunday holat esa kalitni bilmagan holda deshiflash jarayonini amalga oshirishni jiddiy murakkablashtiradi.

Agarda ochiq ma’lumot kompyuterdan foydalanilgan holda tuzilib, standart ASCII kodi alifbosi belgilaridan iborat bo‘lib, shifrma’lumot standart ASCII kodi alifbosi belgilarini birini boshqasi bilan almashtirishdan iborat bo‘lgan o‘rniga qo‘yishga asoslangan shifrlash algoritmini qo‘llash natijasida hosil qilingan bo‘lsa, u holda shifrlash jarayoni asosini quyidagi o‘rniga qo‘yish almashtirish 4.2-jadvali tashkil etadi.

4.2- jadval

O‘rniga qo‘yish almashtirish (ASCII kodi alifbosi belgilari asosida) jadvali

Ochiq ma’lumot alifbosi (standart ASCII kodi belgilari)	$ASCII_0$	$ASCII_1$	…	…	$ASCII_{255}$
Shifrma’lumot alifbosi (ikkilik sanoq tizimi belgilari)	$x_0^0 x_1^0 ... x_7^0$	$x_0^1 x_1^1 ... x_7^1$			$x_0^{255} x_1^{255} ... x_7^{255}$

bu yerda $x_i^j \in \{0;1\}$ bo‘lib, standart ASCII kodi alifbosi *256* ta har xil belgilarini bitlar bilan ifodalash uchun sakkiz bit kifoya, ya’ni $2^8 = 256$.

Bu shifrlash jarayonini ifodalovchi algoritm kalitlarining umumiy soni $256!$ bo‘lib, ushbu $n! \approx \left(\frac{n}{e}\right)^n \sqrt{2\pi n}$ - Stirling formulasiga ko‘ra quyidagicha

$$256! = \left(\frac{256}{2,7}\right)^{256} \sqrt{2 \cdot 3,14 \cdot 256} > \left(\frac{256}{4}\right)^{256} \sqrt{2 \cdot 2 \cdot 256} > \left(\frac{4 \cdot 2^6}{4}\right)^{256} \sqrt{2 \cdot 2 \cdot 2^8} = 2^{6 \cdot 256} \cdot 2^5 = 2^{1541}$$

hisoblanadi. Bunday holat esa kalitni bilmagan holda deshifrlash jarayonini amalga oshirishni yetarli darajada murakkablashtiradi.

Yuqorida keltirilgan jadvallar o‘rniga qo‘yishga asoslangan shifrlash algoritmlarining eng oddiy ko‘rinishlari modelini ifodalaydi. Ya’ni shifrlash jarayonida shifr qiymatlar deb ataluvchi ochiq ma’lumot alifbosi belgilariga mos keluvchi shifrbelgilar deb ataluvchi shifrma’lumot alifbosi belgilari o‘zgarmaydi.

Agarda ochiq ma’lumot kompyuterdan foydalanilgan holda tuzilib, standart ASCII kodi alifbosi belgilarini kengaytirilgan kompyuter standart ANSI kodi alifbosi belgilaridan iborat bo‘lib,

shifrma’lumot standart ANSI kodi alifbosi belgilarini birini boshqasi bilan almashtirishdan iborat bo‘lgan o‘rniga qo‘yishga asoslangan shifrlash algoritmini qo‘llash natijasida hosil qilingan bo‘lsa, u holda shifrlash jarayoni asosini quyidagi o‘rniga qo‘yish almashtirish 4.3-jadvali tashkil etadi.

4.3- jadval

O‘rniga qo‘yish almashtirish (ANSI kodi alifbosi belgilari asosida) jadvali

Ochiq ma’lumot alifbosi (standart ANSI kodi belgilari)	ANSI $_0$	ANSI $_1$	…	…	ANSI $_{2^{32}-1}$
Shifrma’lumot alifbosi (ikkilik sanoq tizimi belgilari)	$x_0^0 x_1^0 ... x_{31}^0$	$x_0^1 x_1^1 ... x_{31}^1$	…	…	$x_0^{2^{32}-1} x_1^{2^{32}-1} ... x_{31}^{2^{32}-1}$

Oddiy o‘rniga qo‘yishga asoslangan shifrlash algoritmlarining analitik (formulali) ifodasini ikkita teng kuchli to‘plamlar, ya’ni elementlari soni teng bo‘lgan to‘plamlar, elementlari ustida o‘rnatilgan o‘zaro bir qiymatli akslantirishlardan (funksiyalardan) iborat deb tushunish mumkin. Bunday akslantirishlar har doim teskarisiga ega bo‘ladi, ya’ni o‘zaro bir qiymatlilik xossasi akslantirishning teskarisi mavjudligining yetarlilik shartini ta’minlaydi. O‘zaro bir qiymatli funksiya odatda chiziqlilik xossasiga ega. Masalan, yuqorida keltirilgan jadvalli oddiy o‘rniga qo‘yishga asoslangan shifrlash algoritmlarining modellarini mos ravishda ularning ushbu ko‘rinishdagi: $f(x_i) = kx_i + b(\mathrm{mod}\,32),\ i = 0,1,...,31;$ $f(x_j) = kx_j + b(\mathrm{mod}\,256),\quad j = 0,1,...,255;\quad f(x_l) = kx_l + b(\mathrm{mod}\,2^{32}),\quad l = 0,1,...,2^{32}-1;$ analitik (formulali) ifodalari bilan almashtirish mumkin, bu yerda k va b o‘zgarmas sonlar. $f(x_i)$-funksiya chiziqsiz bo‘lsa, u ko‘p qiymatli bo‘lib, uning teskarisini har doim ham analitik (formulali) ko‘rinishda ifodalash imkoni mavjud bo‘lavermay, umumiy ko‘rinishda to‘plamga tegishlilik ifodasiga ega bo‘ladi: $f^{-1}(y_i) \in \{x_{i_1}, x_{i_2}, ..., x_{i_t}\}$.

4.1.2. Bir qiymatli va ko‘p qiymatli o‘rniga qo‘yishga asoslangan shifrlash algoritmlarining matematik modellari

O‘rniga qo‘yishga asoslangan shifrlash algoritmlari, ularning asosini tashkil etuvchi akslantirishning bir qiymatli yoki ko‘p qiymatligiga ko‘ra, bir qiymatli va ko‘p qiymatli sinflarga bo‘linadi.

Agar o‘rniga qo‘yishga asoslangan shifrlash algoritmida ochiq ma’lumot alifbosi belgilarining har biriga shifrma’lumot alifbosining bitta belgisi mos qo‘yilsa, bunday algoritm bir qiymatli o‘rniga qo‘yishga asoslangan shifrlash algoritmi sinfiga kiradi. Ochiq ma’lumot alifbosi belgilari $x_1, x_2, \ldots, x_N$ deb belgilansa, masalan, lotin alifbosi belgilari uchun $N = 26$, kirill alifbosi belgilari uchun $N = 32$, standart ASCII kodi alifbosi belgilari uchun $N = 256$ va hokazo. Shifrma’lumot alifbosi belgilari $y_1, y_2, \ldots, y_M$ deb belgilansa, u holda bir qiymatli o‘rniga qo‘yishga asoslangan shifrlash algoritmining umumiy holdagi modeli 4.4- jadval ko‘rinishda quyidagicha ifodalanadi:

4.4- jadval

O‘rniga qo‘yishga asoslangan shifrlash algoritmining umumiy modeli

Ochiq ma’lumot alifbosi belgilari	x_1	x_2	...	...	x_N
Shifrma’lumot alifbosi belgilari	y_{i_1}	y_{i_2}	...	...	y_{i_N}

bu yerda $y_{i_j} \in \{y_1, y_2, ..., y_M\}$. Bu yerda *M* soni *N* sonidan qancha katta bo‘lsa, ya’ni shifrbelgilar to‘plamining quvvati shifr qiymatlar to‘plamining quvvatidan qancha katta bo‘lsa, kalitlarni ifodalovchi mumkin bo‘lgan barcha jadvallar soni shuncha ko‘p bo‘lib, bunday shifrlash algoritmining kriptobardoshliligi ortadi. Analitik ifodasining umumiy ko‘rinishi ushbu chiziqli funksiyadan iborat: $y_{i_j} = kx_j + b (\mathrm{mod}\, N)$ bo‘lib, bu yerda $j = 0,1,..., M-1;\ i = 0,1,..., N-1.$

Misol sifatida quyidagi *(2*x*26)*-o‘lchamli 4.5- jadvalni keltirish mumkin.

4.5- jadval

(2x26) - o‘lchamli jadval

Ochiq ma’lumot alifbosi (lotincha belgilar 26 ta)	A	B	..	...	Z
Shifrma’lumot alifbosi (kirillcha belgilar 32 ta)	I	L	..	...	U

Ko‘p qiymatli shifrlash algoritmlarida ochiq ma’lumot alifbosi belgilarining har biriga shifrma’lumot alifbosining ikki yoki undan ortiq chekli sondagi belgilari mos qo‘yiladi, ya’ni ochiq ma’lumot alifbosining biror x_i belgisiga shifrma’lumot alifbosining chekli $\{y_{i1}, y_{i2},..., y_{it}\} \subset \{y_1, y_2,..., y_M\}$ to‘plamidan olingan biror y_{ij} , $(1 \le j \le t)$, belgisi mos qo‘yiladi. Ko‘p qiymatli o‘rniga qo‘yishga asoslangan shifrlash algoritmining umumiy holdagi modeli 4.6- jadval ko‘rinishida quyidagicha ifodalanadi.

4.6- jadval

Ko‘p qiymatli o‘rniga qo‘yishga asoslangan shifrlash algoritmining umumiy modeli

Ochiq ma’lumot alifbosi belgi-lari	x_1	x_2	…	x_N
Shifrma’lumot alifbosi belgilari	$\{y_{i_1^1}, y_{i_2^1},..., y_{i_t^1}\} = sh1$	$\{y_{i_1^2}, y_{i_2^2},..., y_{i_r^2}\} = sh2$	…	$\{y_{i_1^N}, y_{i_2^N},..., y_{i_p^N}\} = shN$

bu yerda: $y_{i_l^d} \in \{y_1, y_2,..., y_M\}$. 4.6- jadvaldagi $sh1, sh2,..., shN$ - to‘plamlar teng quvvatli bo‘lsa, ya’ni elementlari soni teng bo‘lsa, algoritm teng qiymatli o‘rniga qo‘yishga asoslangan shifrlash algoritmi bo‘ladi, aks holda har xil qiymatli shifrlash algoritmi bo‘ladi.

Agar $\max\{y_1, y_2,..., y_M\} + 1 = D$ bo‘lsa, bu jadvalning analitik ifodasi: $y_{i_l^d} = f(x_d) (\mathrm{mod}\, D) \in shd$ bo‘ladi, bu yerda $f(\cdot)$ - iror o‘zgaruvchan parametrga bog‘liq yoki chiziqsizlik kabi ko‘p qiymatlilik xossasiga ega bo‘lgan funksiya, $1 \le i_l \le M$, $1 \le d \le N$.

Misol sifatida quyidagi *(2x32)*-o‘lchamli 4.7- jadvalni keltirish mumkin.

4.7- jadval

(2x32)-o‘lchamli jadval

Ochiq ma’lumot alifbosi (kirillcha belgilar)	A	B	...	...	Ya
Shifrma’lumot alifbosi (standart ASCII kodi belgilari)	*, d, n	W, &, s, g	...	...	14, !, /, j, a

Ko‘p qiymatli shifrlash algoritmlarining apparat-texnik va apparat-dasturiy ta’minotlari nisbatan samarasiz bo‘lganligi sababli amalda kam qo‘llaniladi.

O‘rniga qo‘yishga asoslangan shifrlash algoritmlari, ularning asosidagi akslantirishni shifrlash jarayonida bosqichma-bosqich o‘zgarib turishiga ko‘ra bir alifboli va ko‘p alifboli shifrlash sinflariga bo‘linadi.

4.1.3. Bir alifboli va ko‘p alifboli o‘rniga qo‘yishga asoslangan shifrlash algoritmlari akslantirishlarining matematik asoslari va xususiyatlari

Oldingi paragraflarda bir qiymatli va ko‘p qiymatli o‘rniga qo‘yishga asoslangan shifrlash algoritmlarining umumiy modelini mos ravishda satrlari soni ikkiga va ustunlari soni ochiq ma’lumot alifbosi belgilari soniga teng bo‘lgan *(2xN)* – o‘lchamli jadvallar va ularga mos keluvchi analitik formulalar bilan ifodalandi. Bu jadvallar o‘rniga qo‘yish akslantirishni ifodalaydi va shifrlash jarayonida faqat bitta jadvaldan foydalaniladi, ya’ni ochiq ma’lumot alifbosining biror alohida olingan belgisi, shifrlash jarayonida uning necha marta takrorlanishidan qat’iy nazar, har doim jadvalning shifrma’lumot alifbosi belgilari satridagi mos belgiga almashtiriladi. Shifrma’lumot alifbosi o‘zgarmaydi. Agarda o‘rniga qo‘yishga asoslangan shifrlash algoritmi akslantirishining asosini tashkil etuvchi jadvalning shifrma’lumot alifbosi belgilari satridagi mos belgilarining joylashish tartibi shifrlash jarayoni bosqichlarida o‘zgarib turmasa, bunday algoritm bir alifboli o‘rniga qo‘yishga asoslangan shifrlash algoritmi

sinfiga kiradi. Aksincha bo‘lsa, ya’ni shifrma’lumot alifbosi belgilari satridagi mos belgilarning joylashish tartibi shifrlash jarayoni bosqichlarida o‘zgarib tursa, bunday algoritm ko‘p alifboli o‘rniga qo‘yishga asoslangan shifrlash algoritmi sinfiga kiradi. Bundan kelib chiqadiki, ko‘p alifboli o‘rniga qo‘yishga asoslangan shifrlash algoritmining modelini ifodalovchi akslantirish jadvalining satrlari soni uchta va undan ortiq bo‘ladi, ularning soni qancha ko‘p bo‘lsa, mos algoritmning bardoshliligi shuncha yuqori bo‘ladi. Shunday qilib, ko‘p alifboli o‘rniga qo‘yishga asoslangan shifrlash algoritmining umumiy holdagi modeli 4.8- jadval ko‘rinishida quyidagicha ifodalanadi.

4.8- jadval

Ko‘p alifboli o‘rniga qo‘yishga asoslangan shifrlash algoritmining umumiy modeli

Ochiq ma’lumot alifbosi belgilari	x_1	x_2	...	...	x_N
Shifrma’lumot alifbosi belgilari	$y_{i_1}^1$	$y_{i_2}^1$	...	...	$y_{i_N}^1$
Shifrma’lumot alifbosi belgilari	$y_{i_1}^2$	$y_{i_2}^2$	...	...	$y_{i_N}^2$
...	...	...	...	...	...
...	...	...	...	...	...
Shifrma’lumot alifbosi belgilari	$y_{i_1}^w$	$y_{i_2}^w$	...	...	$y_{i_N}^w$

Bu yerda $y_l^d \in \{y_1, y_2, ..., y_M\}$. Bu jadvalga mos keluvchi ko‘p alifboli shifrlash jarayonining analitik ifodasi: $y_{i_j}^d = f(x_j)$, d – bosqich tartibi, $1 \le d \le w$, $f(\cdot)$-akslantirish d-parametrga bog‘liq bo‘lgan chiziqli funksiya, ya’ni $f(x_j) = k_d x_j + b_d (\mathrm{mod}\, D)$, bu yerda $D = \max\{y_1, y_2, ..., y_M\} + 1$, k_d va b_d -bosqichlarga mos keluvchi natural sonli koeffisiyentlar.

Misol sifatida quyidagi 4.9- va 4.10- jadvallar bilan ifodalanuvchi ko‘p alifboli o‘rniga qo‘yishga asoslangan shifrlash algoritmlarining modellarini keltirish mumkin:

4.9- jadval

Ochiq ma’lumot alifbosi (lotincha belgilar)	A	B	...	...	Z
Shifrma’lumot alifbosi (kirillcha belgilar)	I	L	...	...	U
...	...	...	...	...	...
Shifrma’lumot alifbosi (kirillcha belgilar)	D	Ya	...	...	Z

hamda

4.10- jadval

Ochiq ma’lumot alifbosi (lotincha belgilar)	A	B	...	...	Z
Shifrma’lumot alifbosi (kirillcha belgilar)	I	L	...	...	U
Shifrma’lumot alifbosi (standart ASCII kodi belgilari)	*	G	…	…	&
...	...	...	...	...	...
Shifrma’lumot alifbosi (kirillcha belgilar)	D	Ya	...	...	Z

Yuqorida o‘rniga qo‘yishga asoslangan shifrlash jarayoni modeli jadvallari va ularga mos kelishi mumkin bo‘lgan analitik ifodalar haqida so‘z yuritildi. O‘rniga qo‘yishga asoslangan shifrlash jarayonlarini ifodalovchi akslantirishlar funksiyalarini har doim ham apparatli qo‘llanishi amaliy jihatdan qulay bo‘lgan jadval ko‘rinishda ifodalash imkoni bo‘lavermaydi. Xususan, quyida o‘rniga qo‘yishga asoslangan shifrlash jarayoni shifr qiymat va maxfiy kalit ustida biror amalni qo‘llash bilan amalga oshiriladigan algoritmlar modelining matematik ifodalari haqida so‘z yuritiladi.

4.2. Vijener shifrlash tizimi

Fransuz kriptografi Bleyz de Vijener qadimda eng mashhur bo‘lgan ko‘p alifboli tizimlarga asos solgan. Bu tizim uning sharafiga

Vijener tizimi deb atalgan. Vijener tizimi ham Sezar tizimiga o‘xshash bo‘lib, unda kalit qadam-baqadam o‘zgaradi. Shifrmatn hosil qilish va uni dastlabki matnga o‘girishda Vijener kvadratidan foydalaniladi [4.1-rasm]. Har bir ustun *0,1,2,..,25* kalitli Sezar tizimi kabi qaralishi mumkin. Shifrlash uchun dastlabki matn harflari kvadrat jadval satridan Sezar tizimi kalitini esa kvadrat jadval ustunidan o‘qiladi.

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

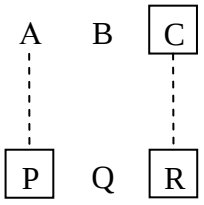
4.1- rasm. Vijener kvadrati

Kalitlar odatda kalit so‘zi atamasi bilan ifodalanadi. Masalan, dastlabki matnda ODAMGA so‘zi kalit so‘z CRYPTO yordamida shifrmatn birinchi harfi O–satr va C-ustunga tegishli katakda joylashgan Q harfi bo‘ladi. Shunday qilib, shifrmatn bo‘lagi QUYBZO shaklini oladi. Bu yerda kalit so‘zining davri 6 ga teng bo‘lib, odatda ko‘p harfli xabarlarni shifrlashda davriy ravishda takrorlanadi. Masalan, agar xabar 15 harfdan iborat bo‘lsa, kalit so‘zi CRYPTOCRYPTOCRY ko‘rinishida bo‘ladi. Shifrmatnni dastlabki matnga o‘girishda satr va ustunlarning o‘rni o‘zaro almashtirilgan kvadratdan foydalanish kifoyadir [17].

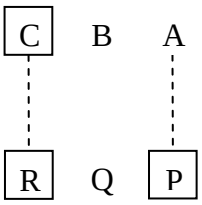
Vijener kvadratini to‘ldirish tartibi ham aslida kalitning bir qismi bo‘lib xizmat qiladi. Shuning uchun Vijener kvadrati sifatida oson eslab qolinadigan kvadratlardan foydalanilgan. Bular orasida admiral Frensis Byufort kvadrati mashhurdir [17].

Uning satrlari bo‘lib teskari tartibda yozilgan Vijener kvadrati satrlari xizmat qiladi. Bu tizim shamol tezligini aniqlovchi shkalani yaratgan admiral Frensis Byufort sharafiga nomlangan.

Agar Vijener kvadratida birinchi ustun va birinchi satr, satr va ustunlarni ko‘rsatsa, Byufort kvadratida esa bu vazifani birinchi satr va oxirgi ustun bajaradi. Shunday qilib, CRYPTO xabarini shifrlashda kriptotizimning birinchi harfi ikki kvadratdan quyidagicha hosil bo‘ladi:



Виженер



Бьюфорт

XVI asrda Djirolano Kardano Vijener tizimining navbatdagi modifikasiyasi AUTOCLAVEni yaratdi. U matematiklar orasida

uchinchi va to‘rtinchi darajali tenglamalar tizimini yechishga bag‘ishlangan formulalari bilan mashhurdir. AUTOCLAVE tizimida shifrlanadigan xabar ma’lum qadamga surilgan holda shifrmatn kaliti vazifasini ham o‘taydi, ya’ni xabar o‘zi-o‘ziga kalit bo‘lib xizmat qiladi. Kalit bosh qismi sifatida kalit so‘zidan yoki xabarning davriy oxiridan foydalanilgan.

4.3. O‘rin almashtirishga asoslangan shifrlash algoritmlarining xususiyatlari va matematik modeli

O‘rin almashtirishga asoslangan shifrlash algoritmlarining asosiy xususiyati ochiq ma’lumot va shifrma’lumot alifbosi belgilarining bir xilligidadir, ya’ni shifrma’lumotni tashkil etuvchi belgilarning ma’nosi mos keluvchi ochiq ma’lumotdagi belgilarning ma’nosi bilan bir xil bo‘ladi. Haqiqatan ham, o‘rin almashtirishga asoslangan shifrlash jarayonida ochiq ma’lumot alifbosi belgilari o‘rinlari almashtirilishi natijasida shifrma’lumot hosil qilinadi. Misol uchun, shartli ravishda, biror alifboda tuzilgan ushbu “$x_1x_2...x_N$” – ochiq ma’lumotdan, uni tashkil etuvchi shifr qiymatlar o‘rinlarini almatirish natijasida “$x_{i_1}x_{i_2}...x_{i_N}$” –shifrma’lumot hosil qilingan bo‘lsa, u holda kalitni ifodalovchi $1\to i_1, 2\to i_2, ..., N\to i_N$ - o‘rin almashtirishlar soni ochiq ma’lumotni tashkil etuvchi alifbo belgilarining soni bilan teng. Kalitni ifodalovchi funksiyani ushbu 4.11- jadval ko‘rinishida berish mumkin.

4.11- jadval

Tartib sonlar	1	2	3	...	*N*-2	*N*-1	*N*
Shifr qiymatlarining ochiq ma’lumotdagi o‘rni	x_1	x_2	x_3		x_{N-2}	x_{N-1}	x_N
Shifr qiymatlarining shifrma’lumotdagi o‘rni	x_{i_1}	x_{i_2}	x_{i_3}		$x_{i_{N-2}}$	$x_{i_{N-1}}$	x_{i_N}

bu yerda $1\le i_j \le N$. Umumiy holda o‘rin almashtirishga asoslangan shifrlash algoritmlari akslantirishlari ochiq ma’lumot shifr

qiymatlarining shifrlanuvchi ma’lumot matnida joylashgan o‘rnini belgilovchi indekslar ustida amalga oshirilib, shifr qiymatlarning shifrma’lumotda joylashish o‘rnini belgilovchi indekslarini aniqlaydi, ya’ni o‘rin almashtirish qoidasini – funksiyasini aniqlaydi. Keltirilgan jadvalli funksiyaga mos analitik formula ko‘rinishidagi funksiya: $f(i) \bmod (N+1) = j_i$ yoki $x_i = x_{f(i) \bmod (N+1)} = x_{i_j}$ bo‘lishi mumkin. Bu yerda $f(\cdot)$ - indekslar o‘rin almashtirish qoidasini aniqlovchi funksiya.

O‘rin almashtirishga asoslangan shifrlash algoritmlarining kaliti uzunligi, umuman olganda, shifrlanishi kerak bo‘lgan ma’lumot uzunligiga, ya’ni ochiq ma’lumotni tashkil etuvchi alifbo belgilarining soniga teng. Bundan tashqari, ochiq ma’lumotni tashkil etuvchi alifbo belgilarining chastotaviy xususiyatlari to‘laligicha shifrma’lumotga o‘tadi. Bunday holatlar amaliy tatbiq imkoniyatlarini cheklaydi. Shunday bo‘lsada ularning samarali tatbiqlarini ta’minlashga qaratilgan sinflari mavjud. *Yo‘nalishli o‘rin almashtirish* sinfidagi shifrlarning qo‘llanilishi amalda ko‘p tarqalgan. Bunday shifrlash algoritmlari biror geometrik shaklga asoslangan bo‘ladi. Ochiq ma’lumot bloklari geometrik shaklga biror trayektoriya (uzluksiz iz) bo‘yicha joylashtiriladi. Shifrma’lumot esa boshqa trayektoriya bo‘yicha hosil qilinadi. Geometrik shakl sifatida (*n*x*m*) o‘lchamli jadval olib, uning birinchi satri boshidan boshlab ochiq ma’lumot belgilarini chapdan o‘ngga ketma-ket joylashtirib, satr tugagach ikkinchi satrga, ochiq ma’lumot belgilarini o‘ngdan chapga ketma-ket joylashtirib, bu satr tamom bo‘lgach, keyingi satrga oldingisiga teskari yo‘nalishda joylashtiriladi va hokazo. Oxirida to‘lmay qolgan satr yacheykalari ochiq ma’lumot alifbosidan farqli bo‘lgan belgilar bilan to‘ldiriladi. So‘ngra ochiq ma’lumotni joylashtirish tartibidan farqli bo‘lgan biror yo‘nalish tanlab olinib, shu yo‘nalish asosida shifrma’lumot hosil qilinadi. Shifrma’lumot hosil qilish yo‘nalishi kalit vazifasini bajaradi. Misol sifatida “*yo‘nalishli o‘rin almashtirishga asoslangan shifrlash algoritmi*” jumlasini shifrlashni *(4*x*10)*–o‘lchamli jadval asosida quyidagicha amalga oshirish mumkin (amalda jadvalning o‘lchami kalit sifatida maxfiy hisoblanadi):

1	2	3	4	5	6	7	8	9	10
y	*o‘*	*n*	*a*	*l*	*i*	*sh*	*l*	*i*	*o‘*
i	*t*	*sh*	*a*	*m*	*l*	*a*	*n*	*i*	*r*
r	*i*	*sh*	*sh*	*i*	*f*	*r*	*l*	*a*	*sh*
...	*i*	*m*	*t*	*i*	*r*	*o*	*g*	*l*	*a*

Bu jadval ustunlari ketma-ketliklarini aralashtirgan holda (bunday aralashtirishlarning umumiy soni *10!=3628800* ta bo‘ladi), masalan, *72968411035* tartib (kalit) bilan

“*sharoo‘tiiiialilfrlnlgaashtyiro‘rshanshshmlmii*”

shifrma’lumotni hosil qilamiz. Shifrma’lumotni hosil qilish jarayonini jadvalning satrlari o‘rinlarini yoki har bir ustunlari satrlarini alohida almashtirishlar bilan yana ham murakkablashtirish mumkin. Satrlar, ustunlar va alohida olingan satr ustunlarini yoki alohida olingan ustun satrlarini shifrlash jarayoni bosqichlarida o‘zgartirib turish bilan yana ham murakkab bo‘lgan shifrlash algoritmlarini hosil qilish mumkin.

Berilgan *4*x*10* o‘lchamli jadval *4*x*10* o‘lchamli $A_{4\times10}$ - matrisa ko‘rinishida ifodalansa, uning elementlari a_{ij}, $i=1,2,3,4;\ j=1,2,...,8;$ satr va ustunlari ustida akslantirishlarni bajarish qulay bo‘lib, matrisalar nazariyasining ayrim xossalaridan foydalanib, kriptografik samaradorlikni oshirishning ilmiy asoslangan usullari kelib chiqadi. Bu fikrlarning isboti hozirgi kunda matrisalarni kriptologiya sohasida keng va samarali qo‘llanilayotgani hamda yangi ilmiy izlanish g‘oyalari natijalari bilan tasdiqlanadi.

O‘rin almashtirishga asoslangan shifrlash algoritmlari haqida to‘laroq ma’lumotlarni [12-13, 59-60] dan topish mumkin.

4.4. Gammalashtirishga asoslangan shifrlash algoritmlarining matematik asoslari

Shifrlash jarayonida ochiq ma’lumotni tashkil etuvchi mos alifbo belgilari bilan “kalit” deb ataluvchi parametrning mos elementlari ustida biror amal bajarish natijasida shifrma’lumotni tashkil etuvchi

alifbo begilariga akslantirish amalga oshirilsa, bunday shifrlash algoritmi gammalashtirish shifrlash algoritmi turkumiga kiradi.

Gammalashtirish bilan shifrlash uslubining mohiyati ochiq ma’lumotni (yoki shifrma’lumotni) tashkil etuvchi alifbo belgilari bilan, shifrlash kalitini ifodalovchi psevdotasodifiy ketma-ketlikning mos elementlari gammasini tashkil etuvchi elementlar ustida biror amal bajarish bilan shifrma’lumot hosil qilishdan iborat. Bunda ochiq, shifrlangan va kalitni ifodalovchi gamma ma’lumotlarning alifbo belgilari bitta to‘plamdan olingan bo‘lishi zarur. Misol uchun *2* modul bo‘yicha qo‘shish amalidan foydalanib, ikkilik sanoq tizimi alifbosida raqamli ko‘rinishda berilgan ma’lumotni quyidagicha shifrlash va deshifrlash mumkin:

Ochiq matn: 0110011100100011...

Kalitni ifodalovchi gamma: 110110010110101...

Shifrlangan matn: 1000101110010110...

Kalitni ifodalovchi gamma: 1110110010110101...

Ochiq matn: 0110011100100011...

Bu misoldan ko‘rinadiki, deshifrlash uchun kalit bo‘yicha (ya’ni kalitni tashkil etuvchi gamma elementlari bo‘yicha) shifrma’lumotning mos elementlarini 2 modul bo‘yicha qo‘shishdan foydalanib qayta gammalashtirish kifoya. Bunday shifrlash va deshifrlash jarayonlari akslantirishlarining matematik modeli mos ravishda ushbu: $x_i \oplus k_i = y_i$ va $y_i \oplus k_i = x_i$ (analitik) formulaviy ifodalarga ega. Bu yerda x_i- ochiq ma’lumotning *i*-biti, k_i- kalitni ifodalovchi gammaning *i*-biti, y_i-shifrlangan ma’lumotning *i*-biti, $\oplus$- modul 2 bo‘yicha qo‘shish amalidan iborat. Ya’ni yuqoridagi ifodalar ushbu: $(x_i + k_i) \bmod 2 = y_i$ va $(y_i + k_i) \bmod 2 = x_i$ formulalarga teng kuchli. Biror n-xarakteristikaga ega bo‘lgan chekli maydonlarda $\bmod n$ bo‘yicha amallar bajarish ochiq ma’lumot alifbosi belgilari yoki belgilar birikmalarini ifodalovchi shifr qiymat va shifrma’lumot alifbosi belgilari yoki belgilar birikmalarini ifodalovchi shifrbelgilarning chekli sonda ekanligi bilan uzviy bog‘liq. Misol uchun ochiq ma’lumotni tashkil etuvchi alifbo kirillcha 32 ta belgilardan iborat bo‘lsin.

Ularni $A \to 0, Б \to 1, В \to 2, \ldots, Я \to 30,$ *bo‘shliq(probel)* $\to 31$ moslik bilan ifodalab, kalit gammasini ushbu *ТГЗ...ЯЛ...КЗУ* ko‘rinishdagi

tasodifiy ketma-ketlikdan iborat deb olib, “*gammalashtirish*” – ochiq ma’lumotni shifrlashni quyidagicha amalga oshirish mumkin:

$(Г+Т)\text{mod}32=(4+19)\bmod 32=23\to Ц$, $(А+Г)\text{mod}32=(0+4)\bmod 32=4\to Г$,

$(М+3)\text{mod}32=(13+8)\bmod 32=21\to Ф,\ldots,(А+Я)\text{mod}32=(0+30)\bmod 32=30\to Я$,

$(Ш+Л)\text{mod}32=(25+12)\bmod 32=5\to Д,\ldots,$

$(Р+К)\text{mod}32=(17+11)\bmod 32=28\to Ь$, $(И+3)\text{mod}32=(9+8)\bmod 32=17\to Р$,

$(Ш+У)\text{mod}32=(25+20)\bmod 32=13\to М$,

va natijada “*SGF...YaD...RM*” –shifrma’lumotga ega bo‘lamiz.

Deshiflash esa quyidagicha amalga oshiriladi:

$(Ц-Т)\text{mod}32=(23-19)\bmod 32=4\to Г$, $(Г-Г)\text{mod}32=(4-4)\bmod 32=0\to А$,

$(Ф-3)\text{mod}32=(21-8)\bmod 32=13\to М,\ldots,(Я-Я)\text{mod}32=(30-30)\bmod 32=0\to А$,

$(Д-Л)\text{mod}32=(5-12)\bmod 32=(32-7)\bmod 32=25\to Ш,\ldots,$

$(Ь-К)\text{mod}32=(28-11)\bmod 32=17\to Р$, $(Р-3)\text{mod}32=(17-8)\bmod 32=9\to И$,

$(М-У)\text{mod}32=(13-20)\bmod 32=(32-7)\bmod 32=25\to Ш$.

Xuddi yuqorida keltirilgan misoldagi kabi, agarda ochiq ma’lumot kompyuterdan foydalanilgan holda tuzilib, standart ASCII kodi alifbosi belgilaridan iborat bo‘lsa, u holda ochiq ma’lumotning X_i-belgisini, unga mos ASCII_i kodi qiymatiga, shifrlash jarayonida unga mos keluvchi kalit gammasi $Г_j$ -elementining ASCII_j kodi qiymatini xarakteristikasi 256 bo‘lgan chekli maydonda qo‘shib, natijaning qiymatiga teng bo‘lgan ASCII kodli Y_i belgiga almashtiriladi: $(X_i+Г_j)\bmod 256=Y_i$ va shifrma’lumot hosil qilinadi. Deshifrlash ushbu: $(Y_i-Г_j)\bmod 256=X_i$ formula orqali amalga oshirilib, shifrma’lumotga mos ochiq ma’lumot hosil qilinadi.

Agarda kalit gammasi qaytariluvchi davrga ega bo‘lgan bitlardan iborat bo‘lmasa, olingan shifrma’lumotni ochish yetarli darajada qiyin bo‘ladi. Buning uchun kalit gammasini tashkil etuvchi elementlar tasodifiy o‘zgarishi kerak. Amalda kalit gammasining davri butun shifrma’lumot uzunligidan katta bo‘lib, ochiq ma’lumotning hyech bir qismi ma’lum bo‘lmasa, bunday shifrma’lumotga mos keluvchi ochiq ma’lumotni topish murakkab bo‘ladi. Bunday hollarda shifrma’lumot faqat uzunligi uning uzunligiga teng bo‘lgan kalit gammasining mumkin bo‘lgan barcha variantlarini tanlash orqali ochiladi.

Agarda raqib tomonga ochiq ma’lumotning biror qismi va unga mos keluvchi shifrma’lumot ma’lum bo‘lib qolsa, u holda

shifrlashning gammalashtirish uslubi o‘z kuchini yo‘qotadi. Chunki bunday holda raqib tomon ochiq ma’lumotning ma’lum bo‘lgan qismi mazmuniga ko‘ra butun shifrma’lumotni ochishga harakat qiladi. Misol uchun, ko‘plab maxfiy hujjatlar «Mutlaqo maxfiy» yoki boshqa shu kabi so‘zlar bilan boshlanib, kriptoanalitik uchun tahlil yo‘nalishini aniqlashga yordam beradi. Bunday holatlarni axborot tizimi muhofazasi kriptotizimining amalda qo‘llanilishida albatta hisobga olish kerak.

4.5. Ma’lumotlarni shifrlash algoritmlari

Yuqorida o‘rniga qo‘yish va o‘rin almashtirishga asoslangan shifrlash algoritmlarini, ularning asosidagi akslantirishlarni matematik modellarining asosiy xususiyatlari ko‘rib o‘tildi.

O‘rniga qo‘yishga asoslangan shifrlash jarayonida ochiq ma’lumotni tashkil etuvchi alifbo belgilarini ayrim (alohida) olingan holda, shifrma’lumot alifbosining ayrim (alohida) olingan belgilariga almashtirish yoki o‘rin almashtirishga asoslangan shifrlash jarayonida ochiq ma’lumotni tashkil etuvchi alifbo belgilarini ayrim (alohida) olingan holda o‘rinlarini almashtirish amalga oshirilgan bo‘lsin. Bunday holatda shifrlash jarayoni algoritmining kriptobardoshliligini oshirish uchun kalit uzunligi shifrlanishi kerak bo‘lgan ma’lumot uzunligi darajasida bo‘lishi zarur bo‘ladi. Misol uchun, shartli ravishda, biror alifboda tuzilgan ushbu “$x_1 x_2 ... x_N$” – ochiq ma’lumotdan, uni tashkil etuvchi alifbo belgilarining o‘rinlarini almashtirish natijasida “$x_{i_1} x_{i_2} ... x_{i_N}$” –shifrma’lumot hosil qilingan bo‘lsa, u holda kalitni ifodalovchi $1 \to i_1, 2 \to i_2, ..., N \to i_N$ - o‘rin almashtirishlar soni ochiq ma’lumotni tashkil etuvchi alifbo belgilarining soni bilan teng. Xuddi shu kabi, o‘rniga qo‘yishga asoslangan shifrlash algoritmlaridan foydalanishda ochiq ma’lumot chastotaviy xususiyatlarining shifrma’lumotga ko‘chmasligini ta’minlash uchun ko‘p alifboli shifrlash algoritmlaridan foydalaniladi, bunga erishish uchun esa, yuqorida ko‘rilganidek shifrlash jarayoni bosqichlarida bir xil belgilarni har xil belgilarga almashtirish, ya’ni kalit uzunligini oshirish zarurati tug‘iladi. Shifrlanishi kerak bo‘lgan ma’lumot hajmining ortishi bilan, shifrlash jarayonini amalga oshirishda qo‘llaniladigan algoritm kaliti uzunligining mos ravishda

ortib borishi, kriptobardoshlilikni ta’minlash nuqtai nazaridan samarali bo‘lsada, bunday holat algoritmlarning amalda qo‘llanishlari nuqtai nazaridan: kalitlarni saqlashda, ularni tarqatishda, apparat-texnik ta’minotlarni amalga oshirishda va boshqa shu kabi holatlarda noqulayliklar tug‘diradi. Shuning uchun shifrlanishi kerak bo‘lgan ma’lumotni, uni tashkil etuvchi alifbo belgilarining ma’lum bir uzunlikdagi birikmalari (bloklari) birlashmasi (konkatenasiyasi) ko‘rinishda ifodalab, ana shu bloklarning alohida-alohida samarali va kriptobardoshli shifrlanishini amalga oshirish masalasi kelib chiqadi. Bu masala simmetrik blokli shifrlash algoritmlari orqali amalga oshirildi. Simmetrik blokli shifrlash algoritmlarining asosini ochiq ma’lumot bloklarini yuqori darajada *aralashtirish* va *tarqatish* (yoyilish, taralish) xossalariga ega bo‘lgan akslantirishlar tashkil etadi [13, 59-60]. *Samarali aralashtirish* beruvchi ($\oplus$, $\bmod 2^n$, *o‘rin almashtirish jadvallari*, *siklik surishlar* va hokazo) amallar *korrelyasion immunstlik* – shifrlanishi kerak bo‘lgan yoki kalit bloklarini tashkil etuvchi alifbo belgilaridan birining o‘zgarishi, akslantirish natijasida olingan shifrblokni tashkil etuvchi alifbo belgilarining faqat birgina mos belgisi o‘zgarishiga ta’sir qilib, boshqa qismiga ta’sir etmasligini ta’minlovchi o‘rin almashtirishga asoslangan shifrlash akslantirishlaridan iborat. *Samarali tarqatish* beruvchi bir alifboli va ko‘p alifboli o‘rniga qo‘yish akslantirishlarga asoslangan S blok akslantirishlari *chiziqsizlikni* - shifrlanishi kerak bo‘lgan yoki kalit bloklarini tashkil etuvchi alifbo belgilaridan birining o‘zgarishi, akslantirish natijasida olingan shifrblokni tashkil etuvchi alifbo belgilarining ikki va undan ortiq qismiga ta’sir etishini ta’minlovchi o‘rniga qo‘yishga asoslangan shifrlash algoritmlari akslantirishlaridan iborat.

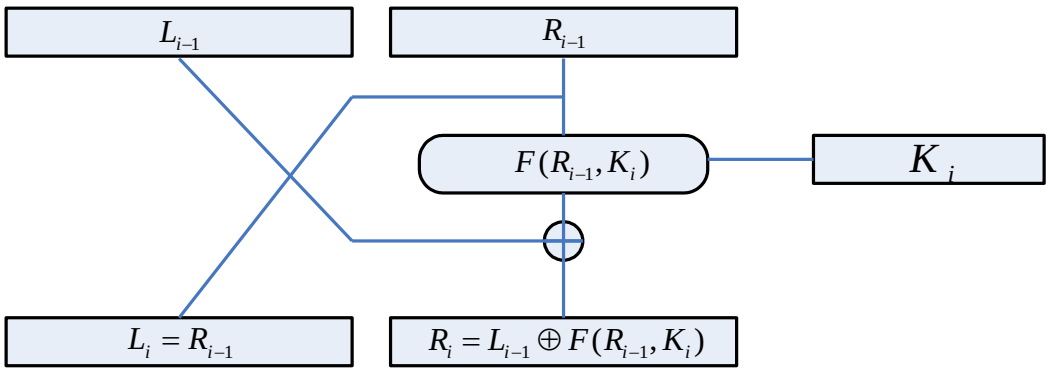
Aralashtiruvchi akslantirishlar ochiq ma’lumot va unga mos keluvchi shifrma’lumot bloklarining chastotaviy (statistik) va analitik bog‘liqlik xususiyatlarini o‘rnatishni murakkablashtirsa, tarqatuvchi akslantirishlar ochiq ma’lumot bloki bitta belgisining o‘zgarishini mos shifrma’lumot blokining ko‘p belgilari o‘zgarishiga ta’sir qilishini yuzaga keltirib, ochiq ma’lumotning chastotaviy (statistik) xususiyatlarini shifrma’lumotga ko‘chmasligini ta’minlaydi.

Simmetrik blokli shifrlash algoritmlari bir nechta bosqichlardan (raundlardan) iborat bo‘lib, har bir raund

aralashtiruvchi va tarqatuvchi akslantirishlardan tuzilgan. Bunday asosda tuzilish tamoyili, har bir raund shifrlash jarayonini har xil kalitlar bilan bir xil turdagi akslantirishlarni amalga oshirishga hamda deshifrlash jarayonini raund akslantirishlari va kalitlarini teskari tartibda qo‘llashning samarali imkonini beradi. Algoritm asosini tashkil etuvchi, raund shifrlash jarayonini amalga oshiruvchi, aralashtirish va tarqatish xususiyatlariga ega bo‘lgan funksiyalar *asosiy akslantirishlar* deyiladi. *Asosiy akslantirish*larning apparat-texnik jihatdan qulay qo‘llanish modeli sifatida teskari bog‘liqlikka ega bo‘lgan siljitish registlarini keltirish mumkin [13, 59-60]. Bunda tarqatuvchi akslantirish teskari bog‘liqlikni ta’minlovchi funksiya bilan, aralashtiruvchi akslantirish esa, registrdagi ma’lumotlarni siljitish bilan amalga oshiriladi.

Shifrlanishi kerak bo‘lgan ma’lumot blokini siljitish registrlariga kiritib (yuklab), registrdagi ma’lumotni shartli ravishda chap va o‘ng qism blok vektorlariga bo‘lib, ular ustida har xil kalitlar bilan bir xil turdagi akslantirishlarni bosqichma-bosqich amalga oshirishga asoslangan – *Feystel (Feyshtel) tarmog‘i* deb ataluvchi shifrlash jarayoni funksional qurilmasiga asoslangan algoritmlar keng tarqalgan. Bular jumlasiga DES va GOST 28147-89 kiradi.

Faystel teskarisi mavjud kriptobardoshli akslantirishlarni tadqiq qilmay, bunday akslantirishlar qatnashmagan kriptobardoshliligi yuqori bo‘lgan shifrlash tizimlarini topish masalasining yechimiga kirishgan. U bu masalaning yechimini quyidagicha hal etgan. Shifrlanadigan blok ikkita L_0, R_0 qismlarga ajratiladi. Feystel tarmog‘i i – raundi iterativ blokli shifrlash quyidagi sxema bo‘yicha aniqlanadi (4.2-rasm).



4.2- rasm. Feystel tarmog‘i i – raundi

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

Feystel tarmog‘i i – raundi shifrlash jarayoning matematik modeli quyidagicha ifodalanadi:

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

Bunday tarmoqqa asoslangan algoritmlar bir necha iterasiyadan tashkil topgan K_i kalitlarda shifrlanadigan akslantirishlardan (funksiyalardan) tashkil topgan.

Feystel tarmog‘i akslantirishlarining asosiy xossasi F -raund funksiyasi teskarisi mavjud bo‘lmasa ham, Feystel tarmog‘i bu akslantirishlarining teskarisini topish imkonini beradi. Haqiqatan ham, shifrlash jarayoni i – raund matematik modelidagi $\oplus$ - modul 2 bo‘yicha ikkilik sanok tizimida qo‘shish amali xossasidan foydalangan holda quyidagi tenglikka ega bo‘linadi:

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

Bu tengliklar Feystel tarmog‘i asosida qurilgan shifrlash algoritmlarini deshifrlashning matematik modelini ifodalaydi.

4.6. Blokli shifrlar

Feystel tarmog‘iga asoslanmagan simmetrik blokli shifrlash algoritmlariga: AQSh davlat standarti **AES FIPS-197**, O‘zbekiston milliy standarti **O‘z DSt 1105:2009** simmetrik blokli shifrlash algoritmlari misol bo‘la oladi.

Quyida Feystel tarmog‘iga asoslanmagan simmetrik blokli shifrlash algoritmlari matematik asoslarini va [13, 23, 26] da keltirilgan algoritmlar akslantirishlari asosida yoritiladi.

AES kriptoalgoritmining matematik asosi

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

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

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

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

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

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

Ko‘phadlarni qo‘shish

AES algoritmida ko‘phadlarni qo‘shish $\oplus$ **(XOR)** (berilgan ko‘phadlarga mos keluvchi ikkilik sanoq tizimidagi sonlarning mos bitlarini mod 2 bo‘yicha qo‘shish) amali orqali bajariladi. Masalan, $x^7 + x^6 + x^4 + x^2 + x$ va $x^7 + x^5 + x^3 + x + 1$ ko‘phadlar natijasi quyidagicha hisoblanadi:

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

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

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

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

Ko‘phadlarni ko‘paytirish

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

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

AES FIPS-197 algoritmi raundlarining shifrlash jarayonlari: *SubBytes* –berilgan jadval asosida baytlarni almashtirish, *ShiftRows* – berilgan jadval asosida baytlarni siklik surish, *MixColumns* –teskarisi

mavjud bo‘lgan berilgan matrisa bo‘yicha baytlarni aralashtirish, *AddRoundKey* –raund kalitlari bloki bitlariga mos bloklar bitlarini *XOR* amali bilan qo‘shish akslantirishlarida iborat bo‘lib, bu akslantirishlarning bittasi, ya’ni *AddRoundKey* akslantirishi bir tomonlama hisoblanadi. Chunki raund kaliti bloki va unga *XOR* amali bilan qo‘shiluvchi mos blok noma’lum bo‘lib, bu akslantirish natijasi ma’lum bo‘lganda unga mos keluvchi blokni aniqlash uchun raund kalitini topish kerak bo‘ladi. Bunday holat esa raund kalitlarining barcha mumkin bo‘lgan qiymatlarini tanlab chiqishni talab etadi. Raund kalit uzunligining qanchalik katta bo‘lishi va raundlar sonining ko‘p bo‘lishi algoritm kriptobardoshliligini ifodalaydi. **AES FIPS-197** algoritmi raund kalitining eng kichik uzunligi 128 bit bo‘lib, barcha mumkin bo‘lgan qiymatlari soni 2^{128}ta, bu uzunlikdagi barcha mumkin bo‘lgan holatlarni tanlab chiqishni bugungi hisoblash texnika va texnologiyalari imkoniyatlaridan samarali foydalanilganda ham mumkin qadar qisqa vaqt ichida amalga oshirish ilojisi mavjud emas. Algoritm 10 raunddan iborat.

O‘z DSt 1105:2009 «Axborot texnologiyasi. Axborotning kriptografik muhofazasi. Ma’lumotlarni shifrlash algoritmi» standarti elektron ma’lumotlarni muhofaza qilish uchun mo‘ljallangan kriptografik algoritmni ifodalaydi. Ma’lumotlarni shifrlash algoritmi (MShA) - simmetrik blokli shifr bo‘lib, axborotni shifrmatnga o‘girish va dastlabki matnga o‘girish uchun foydalaniladi. MShA *256* bit uzunlikdagi ma’lumotlar blokini shifrmatnga o‘girish va shifrmatnni dastlabki matnga o‘girish uchun *256* yoki *512* bit uzunlikdagi kriptografik kalitdan foydalanishi mumkin.

O‘z DSt 1105:2009 kriptoalgoritmining matematik asosi

MShAda modul arifmetikasining diamatrisalar algebrasidan foydalaniladi, bunda hisoblashning qiyinlik darajasi matrisalar algebrasidagi singari bajariladi.

Shifrmatnga o‘girish va dastlabki matnga o‘girish proseduralarida foydalaniladigan diamatrisalar algebrasining asosiy amali diamatrisani *p* modul bo‘yicha diamatrisaga teskarilash amali hisoblanadi. Bu amallarda ikki o‘lchamli seans kaliti massivining maxsus tuzilmali *4*x*4* tartibli kvadrat diamatrisa bilan aks ettiriluvchi qismlari ishtirok etadi; maxsus tuzilmali diamatrisa uchun barcha diagonal elementlar bir xilligi, *1*-satrdagi nodiagonal elementlar,

shuningdek *2*-satrning boshi va oxiridagi elementlar ham bir xilligi xosdir.

Maxsus tuzilmali diamatrisaning muhim xossasi diamatrisaning diaaniqlovchisini hisoblash formulasining soddaligidir, bu esa diamatrisani teskarilash shartlarini tekshirish ishlarini soddalashtiradi. Maxsus tuzilmali diamatrisaga nisbatan teskari diamatrisa o‘zining dastlabki tuzilmasini saqlaydi.

*4*x*4* tartibli maxsus tuzilmali diamatrisa 10 ta har xil elementlar $a_0, \ldots, a_9$ dan tuzilgan bo‘lib, uning diaaniqlovchisi diagonal element a_7 ni uchta yig‘indiga ko‘paytmasi sifatida topiladi, bu yig‘indilardan har biri diagonal element bilan bitta satrda joylashgan unga o‘ngdan qo‘shni element bilan ustun elementlarining yig‘indisini ifodalaydi.

Maxsus diamatrisa uchun diaaniqlovchi *a* quyidagicha topiladi:

$d \equiv a_7 \text{ x } (a_7 + a_0 + a_8 + a_3 + a_5) \text{ x } (a_7 + a_1 + a_8 + a_9 + a_6) \text{ x } (a_7 + a_2 + a_8 + + a_9 + a_4) \ (mod\ p)$.

Maxsus tuzilmali diamatrisani teskarilash shartlarini tekshirish MShA parametrlariga qo‘yiladigan asosiy talab hisoblanadi. U diagonal elementning qiymatlarini va aytib o‘tilgan ko‘paytmalarni *2* moduli bo‘yicha nol bilan taqqoslashga keltiriladi. Bu har qanday shifrlash kaliti va funksional kalitdan teskari diamatrisani shakllantirishga imkon beradi.

MShAda, shuningdek butun sonlarni parametrli ko‘paytirish, teskarilash va darajaga oshirish deb atalgan parametrli gruppa amallaridan ham foydalaniladi.

MShA uchun bosqich (raund)lar soni *ye=8* qilib belgilangan.

Ma’lumotlarni shifrlash algoritmining parametrlari va funksiyalari

MShA quyidagi parametr va funksiyalardan foydalanadi:

a) *k – 256* yoki *512* bit uzunlikdagi shifrlash kaliti;

b) k_f *– 256* bit uzunlikdagi funksional kalit;

c) K_{ye} *– 8*x*4 (*yoki *4*x*8)* tartibli ikki o‘lchamli massiv shaklidagi bosqich kaliti;

d) *b – 256* bit li kirish bloklari soni;

e) *ye* – bosqichlar soni, *ye=8*;

f) *r, (r +1)* – modul, *r=256*;

g) *Aralash()* – oddiy shifralmashtirish bo‘lib, dastlabki matnni shifrmatnga va teskari yo‘nalishda almashtirish uchun diamatrisaviy

qismlar ustida amalga oshiriladi; mazkur shifralmashtirish kirishi *Holat* massivining diamatrisaviy qismlari hamda K_1 va K_2 massivlari bo‘lib, chiqishi *Holat* massividir;

h) *BaytAlmash()* – oddiy shifralmashtirish bo‘lib, dastlabki matnni shifrmatnga va teskari yo‘nalishda *Holat* massivi elementlarini almashtirish massivi elementlari bilan bayt sathida almashtirish uchun foydalaniladi; mazkur shifralmashtirish kirishi bayt sathida *Holat* massivi, almashtirish massivi chiziqli massiv B_{sA} *[256]* yoki B_{sAD} *[256]* bo‘lib, chiqishi bayt sathida *Holat* massividir;

i) *Sur()* – *Holat* massivi elementlarini yanada yaxshiroq aralashtirish uchun dastlabki matnni shifrmatnga va teskari yo‘nalishda almashtirishda foydalaniladi; mazkur almashtirish kirishi bayt sathida *Holat* massivi, chiqishi ustun bo‘ylab shifrlashda pastga va satr bo‘ylab o‘ngga yoki shifrni ochishda ustun bo‘ylab yuqoriga va satr bo‘ylab chapga surilgan bayt sathida *Holat* massividir;

j) *ShaklSeansKalitBayt()* – seans uchun kalit shakllantirish bo‘lib, dastlabki matnni shifrmatnga va teskari yo‘nalishda almashtirishda *BaytAlmash()* shifralmashtirishini bajarish uchun foydalaniladi; mazkur shifralmashtirish kirishi shifrlash kaliti *k* va funksional kalit k_f bo‘lib, chiqishi bayt sathida chiziqli massivlar B_{sA} *[256]* va B_{sAD} *[256]*;

k) *ShaklSeansKalit()* – seans uchun kalitni shakllantirish bo‘lib, dastlabki matnni shifrmatnga va teskari yo‘nalishda almashtirishda *Aralash()* shifralmashtirishni bajarish uchun foydalaniladi; mazkur shifralmashtirish kirishi baytli elementlardan tarkib topgan chiziqli massiv K_{st}*=[32]* bo‘lib, chiqishi maxsus tuzilmali diamatrisalardan tashkil topgan $(K_{1t}\ ,\ K_2\ )$ yoki $(K_1\ ,\ K_{2t}\ )$ massivlar juftliklaridir;

l) *ShaklBosqichKalit()* – seans davomida seans-bosqich kalitidan bosqich kalitini shakllantirish bo‘lib, dastlabki matnni shifrmatnga va teskari yo‘nalishda almashtirishda *Qo‘shBosqichKalit()* almashtirishini bajarish uchun foydalaniladi; mazkur almashtirish kirishi chiziqli seans-bosqich kaliti massivi k_{se}, chiqishi bayt sathida berilgan ikki o‘lchamli K_e*[8,4]* massividir;

m) *Qo‘shBosqichKalit()* – oddiy shifralmashtirish bo‘lib, dastlabki matnni shifrmatnga va teskari yo‘nalishda *Holat* va bosqich kaliti massivi K_e elementlari ustida istisnoli YoKI (*2* moduli bo‘yicha

bitlab qo‘shish) amalini bajarishdan iborat; mazkur shifralmashtirish kirishi bayt sathida *Holat* massivi, K_e massivi bo‘lib, chiqishi bayt sathida *Holat* massividir;

n) *Qo‘shHolat()* – oddiy shifralmashtirish bo‘lib, shifrlash bloklari ustida amalga oshiriladigan elektron kod kitobi rejimidan boshqa rejimlarda dastlabki matnni shifrmatnga va teskari yo‘nalishda *XOR* amali ishtirokida foydalaniladigan almashtirish.

MShA belgilab qo‘yilgan ikki xil - *256* va *512* bit uzunlikdagi kalitlar yordamida amalga oshiriladi.

Birinchi holatda, shifrlash kriptografik moduliga *256* bitli kalit kiritiladi. Bu kalit to‘laligicha shifrlash kaliti *k* sifatida olinadi, dastlabki seansning k_f funksional kaliti esa, shifrlash kalitining xesh-funksiyasi qiymati sifatida hisoblab topiladi.

Ikkinchi holatda, shifrlash kriptografik moduliga *512* bitli kalit kiritiladi. Bu kalitning *256* bitli birinchi yarmi, shifrlash kaliti *k* sifatida olinadi, uning *256* bitli ikkinchi yarmi birinchi seansning funksional kaliti k_f sifatida olinadi.

Uchinchi holatda, shifrlash kriptografik moduliga hyech qanday yangi kalit kiritilmaydi. Shifrlash kaliti *k* sifatida oldingi seansda ishlatilgan shifrlash kaliti olinadi, funksional kalit k_f sifatida esa oldingi seansda ishlatilgan funksional kalit k_{f-1} ning shifrlash kaliti *k* dan foydalanib xeshlangan qiymati olinadi.

Yuqorida ko‘rib o‘tilgan birinchi va ikkinchi holatlarda joriy seans uchun yangilangan funksional kalit k_f bundan oldingi seansda foydalanilgan funksional kalit k_{f-1} ning xesh-funksiyasi sifatida hisoblab topiladi. Xeshlash kaliti sifatida qoidaga ko‘ra shifrlash kalitidan foydalaniladi, xeshlash funksiyasini hisoblash dasturi esa MShAning dastur (yoki apparat) ta’minotiga qo‘shib qo‘yiladi. Funksional kalitni yangilash davri foydalanilayotgan shifrdan foydalanish rejimi va dastlabki ma’lumotlarning maxfiylik darajasini hisobga olgan holda MShA bayonnomasi bilan belgilanadi.

4.7. OQIMA SHIFRLASH algoritmlarining matematik modellari va xususiyatlari

Simmetrik blokli shifrlash algoritmlari kabi, oqimli shifrlash algoritmlarining yaratilishi ham tabiiy zarurat asosida vujudga kelgan.

Nisbatan kichik uzunlikka ega bo‘lgan, ya’ni kafolatlangan kriptobardoshlilikni ta’minlovchi uzunlikka ega bo‘lgan – bugungi kunda *128* bitdan kam bo‘lmagan kalit bilan bir tomonlama kriptografik akslantirishlar asosida, yetarli darajada katta uzunlikdagi psevdotasodifiy ketma-ketlik (PTKK) gammasini ishlab chiqaruvchi generatorlar negizida oqimli shifrlash algoritmlari yaratiladi. Uzunligi *128* bitdan kam bo‘lmagan kalitlarning mumkin bo‘lgan barcha variantlari soni 2^{128} tadan kam bo‘lmay, ularning hammasini tanlab chiqish jarayonini amalga oshirish, bugungi kun hisoblash texnika va texnologiyalarining mavjud ilg‘or imkoniyatlaridan foydalanilganda har doim ham samarali natijalar beravermaydi. Ana shunday generatorlar ishlab chiqargan gamma ketma-ketlikni tashkil etuvchi alifbo belgilarini ochiq ma’lumot mos alifbo belgilari bilan biror amal bajarish orqali shifrma’lumot alifbosi belgilariga almashtirish – gammalashtirish amalga oshiriladi. Bunday shifrlash jarayoni ko‘p alifboli o‘rniga qo‘yishga asoslangan shifrlashni amalga oshirishni samarali usulini ifodalaydi – kafolatli kriptobardoshlilikni ta’minlovchi kichik uzunlikdagi kalit bilan, ochiq ma’lumotning chastotaviy xususiyatlarini shifrma’lumotga ko‘chirmaydigan yetarli kriptobardoshlilikni ta’minlovchi shifrlashni amalga oshiradi.

Oqimli shifrlash algoritmlari asosini PTKK ishlab chiqaruvchi generatorlar tashkil etadi. Bunday generatorlarning asosiy kriptobardoshlilik xarakteristikasi ushbu generatorlar hosil qilgan ketma-ketlikning tasodifiyligidadir. Hosil qilingan ketma-ketliklar bloklarining tasodifiylik darajasi bloklarni tashkil etuvchi alohida elementlar va elementlar birikmalari sonlari bilan bog‘liq nisbatlar orqali ifodalanuvchi va aniqlanuvchi mezonlar orqali baholanadi. Tasodifiylik darajasi yuqori bo‘lgan psevdotasodifiy ketma-ketlikni ishlab chiqaruvchi generatorlar kriptografik jihatdan samarali bo‘lgan 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 kalitlarning generasiyasida;
- nosimmetrik kriptotizimlarda qo‘llaniladigan katta qiymatlar qabul qiluvchi parametrlarning tasodifiy boshlang‘ich qiymatlari generasiyasida;

- blokli shifrlash algoritmlarining boshlang‘ich tasodifiy qiymat talab qiluvchi SVS, OFB va boshqa qo‘llanish tartib-qoidalari uchun tasodifiylik darajasi yuqori bo‘lgan boshlang‘ich vektorlar hosil qilishda;

- elektron raqamli imzo tizimlarida katta qiymatga ega parametrlar uchun dastlabki tasodifiy qiymatlarni generasiyasida;

- bitta protokol orqali bir xil ma’lumotlarni har xil kalitlar qo‘llash bilan shifrlab turli ko‘rinishda uzatish uchun talab qilinadigan holatlarda kalit uchun yetarli uzunlikdagi tasodifiy ketma-ketlik hosil qilishda, masalan, SSL va SET protokollarida.

Tashkil etuvchi elementlari va elementlar birikmalari deyarli teng ehtimollik bilan taqsimlangan tasodifiy ketma-ketlik hosil qilish masalasini yechish ketma-ketlikni tashkil etuvchi elementlar va elementlar birikmalarining tekis taqsimlangan generasiyasi masalasini yechish bilan bog‘liq. Biror ketma-ketlikni tashkil etuvchi elementlar va elementlar birikmalari, shu ketma-ketlikda deyarli teng miqdorda qatnashgan bo‘lsa, bu ketma-ketlik tekis taqsimotga ega deyiladi. Agar A -ketma-ketlikni tashkil etuvchi $x_t \in A$ element va element birikmalari soni N ta bo‘lsa, u holda ixtiyoriy $t \in N$ uchun, A -ketma-ketlikni tashkil etuvchi $x_t \in A$ element va elementlar birikmasining shu ketma-ketlikdagi chastotasi boshqa element va elementlar birikmasining chastotasi bilan deyarli bir xil bo‘ladi, ya’ni har bir $x_t \in A$ element va elementlar birikmasi shu ketma-ketlikda deyarli bir xil ehtimollik bilan qatnashadi.

Tasodifiy ketma-ketliklar haqiqiy tasodifiy va psevdotasodifiy ketma-ketliklarga bo‘linadi.

Tasodifiy ketma-ketlik fizik generatorlar va dasturiy generatorlardan foydalanib hosil qilinishi mumkin.

Fizik hodisalarning o‘zgarish majmuiga asoslangan generatorlar orqali ishlab chiqilgan ketma-ketlik **haqiqiy tasodifiy** bo‘lib, bu ketma-ketlik bir martagina ishlab chiqilib, uni keyinchalik biror bir usul yoki vosita bilan xuddi shunday tarzda takrorlanishini boshqarish murakkab hisoblanadi. Shu sababli ma’lumotlarni shifrlash jarayonida bevosita fizik generatorlar bilan ishlab chiqilgan ketma-ketlikni kalitlar gammasi sifatida qo‘llash maqsadga muvofiq emas. Chunki deshifrlash jarayonida qo‘llaniladigan fizik generatorning

aynan shifrlash jarayonida qo‘llanilgan ketma-ketlikni ishlab chiqishi kafolatlanmaydi.

Biror noma’lum parametrga (kalitga) bog‘liq bo‘lgan matematik model asosida psevdotasodifiy ketma-ketlik ishlab chiquvchi dasturiy generatorlar hosil qilgan **psevdotasodifiy** ketma-ketlikni, noma’lum parametr qiymatini bilgan holda, xuddi shu matematik model va uning dasturiy ta’minoti asosida ketma-ketlikning qayta takrorlanishini boshqarish mumkin. Bunday holat ma’lumotlarni shifrlash jarayonida bevosita dasturiy generatorlar bilan ishlab chiqilgan psevdotasodifiy ketma-ketlikni kalitlar gammasi sifatida qo‘llash maqsadga muvofiqligini anglatadi va deshifrlash jarayonida qo‘llaniladigan dasturiy generatorning aynan shifrlash jarayonida qo‘llanilgan psevdotasodifiy ketma-ketlikni ishlab chiqishi kafolatlanadi.

Yuqorida keltirilgan amaliy masalalarni yechishda haqiqiy tasodifiy ketma-ketliklar ishlab chiquvchi tasodifiy fizik hodisalarga asoslangan generatorlar oldindan kalitlar bloklari majmuini yaratishda, generatorlarning boshlang‘ich parametrlari qiymatlarini o‘rnatishda va boshqa shu kabi masalalarni yechishda samarali natijalar beradi.

Yetarli katta davr uzunligiga ega va tasodifiylik darajasi yuqori bo‘lgan ketma-ketliklar hosil qiluvchi dasturiy PTKK generatorining amalda qo‘llanilishi samarali va qulay bo‘lib, kriptografik vositalarda keng qo‘llaniladi.

Uzluksiz shifrlash tizimlarida shifrlash va deshifrlash jarayonlarining tez amalga oshirilishi uchun tashkil etuvchi elementlari va elementlar birikmalari tekis taqsimlangan, tasodifiylik darajasi yuqori bo‘lgan psevdotasodifiy ketma-ketlik ishlab chiqaruvchi dasturiy generatorlardan foydalaniladi.

Mavjud dasturiy generatorlar va ular asosidagi oqimli shifrlash tizimlari ma’lum bir yondashuvlar asosida yaratilgan.

Oqimli shifrlash algoritmlariga qo‘yiladigan asosiy talablardan biri ularning kriptografik bardoshliligini ta’minlovchi, kriptografik tatbiqlarda “kalit” deb ataluvchi noma’lum parametr qiymatini bilmagan holda, teskari akslantirish qiymatini bir qiymatli aniqlash biror yechilishi murakkab bo‘lgan matematik muammolarni hal qilishni talab etuvchi bir tomonlamalik xususiyatga ega akslantirishlar

negizida yaratilishidir. Algoritmlar kriptobardoshliligining yetarli darajada ta’minlanganligini kafolatlash va isbotlash asoslari nuqtai nazaridan mavjud uzluksiz shifrlash algoritmlarini asosan uchta yo‘nalishga ajratish mumkin [13]:

1. Tizimli-nazariy yondashuv yo‘nalishidagi PTKK generatorlari asosida yaratilgan algoritmlar;
2. Murakkablikka asoslangan nazariy yondashuv yo‘nalishidagi PTKK generatorlari asosida yaratilgan algoritmlar;
3. Kombinasiyalash yo‘nalishidagi PTKK generatorlari asosida yaratilgan algoritmlar.

Tizimli yondashuv asosida oqimli shifrlash algoritmlarini yaratish ko‘p jihatdan blokli shifrlash algoritmlarini yaratish usullari kabi bo‘lib, oqimli shifrlash algoritmining kriptobardoshliligi fundamental matematik me’zonlar va qonuniyatlar asosida shu paytgacha murakkab va samarali yechish usuli mavjud emas deb hisoblangan muammoning qiyinchiligiga tenglashtiriladi. Bunday holatlarda ko‘proq nazariy va amaliy jihatdan kriptografik samara beruvchi matematik akslantirishlar qo‘llanilgan holda kriptografik tuzilma (sxema) taklif qilinadi va bu tuzilmaning (sxemaning) kriptografik bardoshliligi tadqiq qilinadi. Matematikaning nazariy yutuqlariga asoslangan holda: *bir tomonlamalik xususiyatga ega akslantirishlarga asoslangan, akslantirishlarining analitik va mantiqiy (chinlik jadvali asosidagi Bul funksiyasi) matematik modellarini ifodalovchi funksiyalar chiziqsizlik darajasi yuqori bo‘lishini, yetarli katta davr uzunligini hamda bitlar va bayt bloklarining tekis taqsimotini ta’minlovchi* xususiyatlarga ega bo‘lgan ketma-ketlikni ishlab chiquvchi algoritmlar yaratiladi.

Yaratilgan algoritmlar akslantirishlarining turli xil kriptotahlil usullariga bardoshliligi asoslanadi. Agar yaratilgan algoritmlar shu paytgacha mavjud bo‘lgan kriptotahlil usullariga bardoshli bo‘lsa hamda hosil qilingan ketma-ketlik tasodifiylik mezonlari testlari talablariga javob bersa, bu algoritmni amaliyotda qo‘llash mumkinligi to‘g‘risida xulosa qilinadi.

Mavjud oqimli shifrlash algoritmlari asosan tizimli-nazariy yondashuv natijasida yaratilgan algoritmlar sinfiga (turkumiga) kiradi.

Tizimli-nazariy yondashuv asosidagi oqimli shifrlash algoritmlariga qo‘yiladigan asosiy talablar quyidagilardan iborat [13]:

- algoritm asosidagi PTKK generatori yetarli uzun davrga ega bo‘lgan ketma-ketlik ishlab chiqishni ta’minlashi kerak;
- generator akslantirishlarining analitik va mantiqiy (chinlik jadvali asosidagi Bul funksiyasi) matematik modellarini ifodalovchi funksiyalar chiziqsizlik darajasi yuqori bo‘lishi kerak;
- ishlab chiqilgan PTKK bloklari tekis statistik taqsimot ko‘rsatkichiga ega bo‘lishi kerak;
- psevdotasodifiy ketma-ketlikning gamma elementlari (bit, bayt, qism bloklari) barcha boshqa elementlarining hissasi orqali hosil qilinishi ─ aralashish samarali bo‘lishi kerak;
- PTKK gamma elementlarining keskin o‘zgarishi ─ tarqalishi samarali bo‘lishi kerak;
- algoritm akslantirishlari Bul funksiyalarining chiziqsizlik sharti bajarilishi hamda jadal samara (“lavinniy effekt”) berishi ta’minlanishi kerak.

Tizimli-nazariy yondashuv asosida yaratilgan oqimli shifrlash algoritmlarining kriptobardoshliligi, bu algoritmlarda qo‘llanilgan akslantirishlarning nazariy va amaliy bir tomonlamalik xususiyatlarining qay darajada ishonchliligini baholash bilan isbotlanadi.

Hisoblash murakkkabligiga asoslangan nazariy yondashuv negizida qurilgan oqimli shifrlash algoritmlari PTKK ishlab chiqaruvchi generatorlarining kriptobardoshliligi: *yetarli darajada katta sonni tub ko‘paytuvchilarga ajratish, xarakteristikasi yetarli katta bo‘lgan chekli maydonlarda diskret logarifmlash, chekli maydonlarda yetarli darajada yuqori tartibli chiziqli tenglamalar tizimlarini yechish, EEChnuqtalari ustida amallar bajarish bilan bog‘liq bo‘lgan masalalarni yechish murakkabliklari bilan aniqlanuvchi bir tomonlama funksiyalar bilan ifodalanadi.*

Sanab o‘tilgan hisoblash murakkabliklari negizida aniqlangan bir tomonlama funksiyalar asosida yaratilgan PTKK generatorlar sinfiga katta sonlarni tub ko‘paytuvchilarga ajratish masalasi murakkabligiga asoslangan RSA generatori, katta sonlarni tub ko‘paytuvchilarga ajratish masalasi murakkabligiga asoslangan Kvadratik chegirma usuli orqali aniqlangan BBS generatori va diskret logarifmlash masalasining murakkabligiga asoslangan Blyum-Mikali generatori kiradi.

Nazorat savollari

1. Shifrlash algoritmlari qanday sinflarga bo‘linadi?
2. Oddiy o‘rniga qo‘yishga asoslangan shifrlash algoritmlarining jadvalli va analitik matematik modellarini tushuntirib bering?
3. Bir qiymatli o‘rniga qo‘yishga asoslangan shifrlash algoritmlarining matematik modellarini misollar yordamida tushuntiring?
4. Ko‘p qiymatli o‘rniga qo‘yishga asoslangan shifrlash algoritmlarining matematik modellarini misollar yordamida tushuntiring?
5. Bir alifboli va ko‘p alifboli o‘rniga qo‘yishga asoslangan shifrlash algoritmlari akslantirishlarining matematik asoslari xususiyatlari nimalardan iborat?
6. Gammalashtirish shifrlash algoritmlarining matematik asoslarini tushuntiring?
7. O‘rin almashtirishga asoslangan shifrlash algoritmlarining asosiy xususiyatlari va matematik modeli haqida nimalarni bilasiz?
8. Dastlabki milliy standartlarga asos bo‘lgan simmetrik blokli shifrlarning matematik va kriptografik xususiyatlarini tushuntiring?
9. Zamonaviy simmetrik blokli shifrlash algoritmlarining matematik asoslarini tushuntiring?
10. Feystel tarmog‘iga asoslanmagan simmetrik blokli shifrlash algoritmlariga misollar keltiring?
11. AES kriptoalgoritmining matematik asosini tushuntiring?
12. AES algoritmida ko‘phadlarni ko‘paytirish qanday amalga oshiriladi?
13. AES algoritmida qanday almashtirishlardan foydalaniladi?
14. O‘z DSt 1105:2009 kriptoalgoritmining matematik asosini tushuntiring?
15. O‘z DSt 1105:2009 kriptoalgoritmi qanday parametr va funksiyalardan foydalanadi?
16. Oqimli shifrlash algoritmlariga ta’rif bering?

17. Oqimli shifrlash algoritmlari qanday generatorlar negizida yaratiladi?

18. Tasodifiy ketma-ketlik qanday hosil qilinishi mumkin?

19. Oqimli shifrlash algoritmlariga qo‘yiladigan qanday asosiy talablarni bilasiz?

20. Nazariy yondashuv negizida qurilgan oqimli shifrlash algoritmlari PTKK ishlab chiqaruvchi generatorlarining kriptobardoshliligi nimalarga bog‘liq?

5. OSHKORA KALITLI KRIPTOTIZIMLAR

5.1. Oshkora kalitli kriptotizimlarning umumiy xususiyatlari

Simmetrik kalitli krpitoalgoritmlar asosida yaratilgan kriptotizim axborot-kommunikasiya tarmoqlarida ma'lumotlar almashinuvining muhofazasini ta'minlash masalalarini yechishda qanchalik ishonchli bo‘lmasin, bari bir undan amalda foydalanish jarayonida ayrim qo‘shimcha xavfsizlikni ta'minlash masalalari kelib chiqib, ularning yechilishi talab etiladi. Shunday masalalardan biri kalitlarni tizim foydalanuvchilariga tarqatish masalasidir. Ishlab chiqilgan bardoshli kalitlarni tizim foydalanuvchilariga yetkazish xavfsizligi kafolatli ta'minlangan bo‘lishi talab etiladi. Buning uchun esa qo‘shimcha holda yana biror boshqa kriptotizimdan foydalanishga to‘g‘ri keladi. Bu masala yechimining qo‘shimcha kriptotizimdan foydalanmay hal etilishi klassik va zamonaviy algebrada olingan ilmiy natijalar asosida yaratilgan *ochiq kalitli (oshkora kalitli, nosimmetrik) kriptotizim*larning vujudga kelishi bilan amalga oshirildi [2, 14].

Ochiq kalitli kriptotizim mohiyati har bir foydalanuvchi uchun birini bilgan holda ikkinchisini topish, yechilishi murakkab bo‘lgan masala bilan bog‘liq kalitlar juftligini yaratishdan iborat. Bu juftlikni tashkil etuvchi kalitlardan biri ochiq (oshkora), ikkinchisi maxfiy (shaxsiy) deb e'lon qilinadi. Ochiq kalit oshkora e'lon qilinadi, maxfiy kalit faqat uning egasigagina ma'lum bo‘ladi. Biror foydalanuvchining ochiq kalitini bilgan holda uning maxfiy kalitini topishning amaliy jihatdan mumkin emasligi, yechilishi murakkab bo‘lgan masalaning hal etilishini talab qilishi bilan kafolatlanadi. Ochiq ma'lumot, shu ma'lumotni olishi kerak bo‘lgan foydalanuvchining ochiq kaliti bilan shifrlanib unga uzatiladi. Shifrlangan ma'lumotni olgan foydalanuvchi faqat uning o‘ziga ma'lum bo‘lgan maxfiy kalit bilan uni deshifrlab, ochiq ma'umotga ega bo‘ladi.

Kriptotizimning har bir i - foydalanuvchilarining ochiq k_i^o va maxfiy $k_i^м$ kalitlari maxfiy tutilishi lozim va shart bo‘lgan $p_i^м$-parametrga yoki barcha foydalanuvchilar uchun umumiy bo‘lgan $p^м$-parametrga bog‘liq holda biror Q-qoida bo‘yicha ishlab chiqiladi (generasiya qilinadi). Bunda ochiq kalit k_i^o va generasiya qoidasi Q

ma’lum bo‘lsada, maxfiy $p_i^м$ yoki $p^м$ parametrni bilmaslik $k_i^м$- maxfiy kalitni aniqlash imkoniyatini bermaydi.

Shifrlash qoidasi E va deshifrlash qoidasi D deb belgilansa, *j*–foydalanuvchi M-ochiq ma’lumotni shifrlab, C-shifrlangan ma’lumotni *i*–foydalanuvchiga jo‘natishi uchun *i*–foydalanuvchining barchaga ma’lum bo‘lgan k_i^o -ochiq kalitidan foydalanadi, ya’ni $E_{k_i^o}(M) = C$- shifrma’lumotni *i*–foydalanuvchiga ochiq aloqa tarmog‘i orqali yuboradi. Bu $E_{k_i^o}(M) = C$-shifrma’lumotni qabul qilib olgan *i* – foydalanuvchi, faqat uning o‘ziga ma’lum bo‘lgan o‘zining $k_i^м$- maxfiy kaliti bilan deshifrlaydi, ya’ni $D_{k_i^м}(C) = M$- ochiq ma’lumotga ega bo‘ladi. Shifrlash qoidasini aniqlovchi akslantirish $E_{k_i^o}(M) = C$ bir tomonlamalik xususiyatiga ega bo‘lishi kerak, ya’ni E- akslantirish, k_i^o- ochiq kalit va C- shifrma’lumotni bilgan holda M- ochiq ma’lumotni aniqlash imkoniyati yo‘q.

5.2. Bir tomonlama funksiyalar

Ochiq kalitli kriptotizimlar *bir tomonlama* akslantirishlarga (funksiyalarga) asoslanadi.

Nosimmetrik kriptotizimlarning matematik asosini katta tartibli chekli to‘plamlarda berilgan chekli maydon, halqa, gruppa, qismgruppa ko‘rinishidagi algebraik strukturalar va shaxsiy maxfiylikga ega bo‘lgan uch turdagi bir tomonlama funksiyalar tashkil etadi. Nosimmetrik kriptotizimlarning turli hujumlarga bardoshliligi esa bir tomonlama funksiyalarning teskarilanishi o‘ta murakkab muammo (masala) bo‘lishiga asoslanadi.

Bir tomonlama funksiyalar birinchi turining hujumlarga bardoshliligi diskret logarifmlash masalasining murakkabligiga asoslangan. Bu funksiya U. Diffi va M. Xellman taklif etgan tub maydon *F(p)* hosil qiluvchi (generator, boshlang‘ich ildiz) element *a* ni maxfiy *x* darajaga oshirish funksiyasidir.

Bir tomonlama funksiyalarning ikkinchi turi K. Koks, R. Rayvest, A. Shamir, L. Adleman tomonidan taklif etilgan bo‘lib, uning hujumlarga bardoshliligi chekli halqada faktorlash muammosining murakkabligiga asoslangan.

Bir tomonlama funksiyalarning uchinchi turining hujumlarga bardoshliligi EECh nuqtalari gruppasida diskret logarifmlash masalasining murakkabligiga asoslangan. Bu funksiya N. Koblis va V. Miller taklif etgan hosil qiluvchi (generator, boshlang‘ich ildiz) element *G* ni maxfiy *d* butun songa ko‘paytirish funksiyasidir.

Bir tomonlama funksiya – shunday $y = f(x)$ funksiyaki, uning aniqlanish sohasidan bo‘lgan ixtiyoriy x uchun $f(x) = y$ qiymat oson hisoblanadi, qiymatlar sohasining barcha y qiymatlariga mos keluvchi x qiymatlarni hisoblash esa amaliy jihatdan murakkab bo‘lgan masala (muammo)ni yechishni talab etadi.

Ko‘rinib turibdiki, bir tomonlama funksiyaning bunday ta’rifi «oson hisoblanadigan», «barcha qiymatlar uchun», «amaliy jihatdan», «murakkab bo‘lgan masalani yechishni talab etadi» iboralar asosida berilib, matematika nuqtai nazaridan aniq emas. Shunday bo‘lsada, bu ta’rif amaliy kriptotizim masalalari nuqtai nazaridan yetarli darajada aniq bo‘lib, alohida olingan kriptotizimlar uchun takomillashtirilib, mutlaqo aniq ifodalanishi mumkin. Shunday funksiyalardan kriptografiyada qanday foydalanilishi haqida qisqacha to‘xtalamiz. Yashirin yoki maxfiy uslubli bir tomonlama funksiya, ta’rif bo‘yicha biror $z \in Z$ parametrlarga bog‘liq bo‘lib, teskarisiga ega bo‘lgan shunday f_z funksiyalar sinfiki, berilgan z parametrda aniqlanish sohasidagi barcha $x \in X$ argumentlar uchun $f_z(x) = y$ qiymatlarni oson hisoblash algoritmi E_z mavjud bo‘lib, qiymatlar sohasidagi barcha $y \in Y$ qiymatlar uchun $f_z^{-1}(y) = x$ qiymatlarni ma’lum bo‘lgan E_z algoritm bilan hisoblashning imkoniyati yo‘q (yoki boshqacha aytganda $f_z^{-1}(y) = x$ qiymatlarni hisoblash sarf-xarajatlari va vaqti maqsadga muvofiq emas). Bunday ta’rif matematika nuqtai nazaridan aniq bo‘lmasada, amaliy kriptologiya masalalarida samarali qo‘llanilishi mumkinligiga shak-shubha yo‘q.

Ochiq kalitli kriptotizimlar algoritmlari ularning asosini tashkil etuvchi bir tomonlama funksiyalar bilan farqlanadi. Har qanday bir tomonlama funksiya ham ochiq kalitli kriptotizimlar yaratish uchun va ulardan amaldagi axborotlar tizimida maxfiy aloqa xizmatini o‘rnatish algoritmini qurish uchun qulaylik tug‘dirmaydi.

Bir tomonlama funksiyalarning aniqlanish ta’rifida nazariy jihatdan teskarisi mavjud bo‘lmagan funksiyalar emas, balki berilgan

funksiyaga teskari bo‘lgan funksiyaning qiymatlarini hisoblash amaliy jihatdan maqsadga muvofiq bo‘lmagan funksiyalar tushunilishi ta’kidlangan edi. Shuning uchun, ma’lumotning ishonchli muhofazasini ta’minlovchi ochiq kalitli kriptotizimlarga quyidagi muhim talablar qo‘yiladi:

1. Dastlabki (ochiq) ma’lumotni shifrmatn ko‘rinishiga o‘tkazish bir tomonlama jarayon va shifrlash kaliti bilan shifrmatn ochish – deshifrlash mumkin emas, ya’ni shifrlash kalitini bilish shifrmatn deshifrlash uchun yetarli emas.

2. Ochiq kalitning ma’lumligiga asoslanib, maxfiy kalitni zamonaviy fan va texnika yutuqlari yordamida aniqlash uchun zarur bo‘ladigan sarf-xarajatlar hamda vaqt maqsadga muvofiq emas. Bunda shifrni ochish uchun bajrilishi kerak bo‘ladigan eng kam miqdordagi amallar sonini aniqlash muhimdir.

Zamonaviy ochiq kalitli kriptotizimlar quyidagi turdagi masalalarni yechishning ko‘p vaqt talab qilishi va hisob-kitoblar uchun hisoblash qurilmalarida katta hajmdagi xotira talab etilishi bilan bog‘liq bo‘lgan murakkabliklarga tayanadi:

1. Yetarli katta sonlarni tub ko‘paytuvchilarga yoyish (faktorlash).

2. Xarakteristikasi yetarli katta bo‘lgan chekli maydonlarda diskret logarifmlarni hisoblash.

3. Yetarli katta tartibdagi algebraik tenglamalar tizimining ildizlarini chekli maydonlarda hisoblash.

4. Elliptik egri chiziqlarda rasional koordinatali nuqtalarni topish, ularni qo‘shish hamda tartibini aniqlash.

5. Xarakteristikasi yetarli katta bo‘lgan chekli parametrli gruppalarda parametrni topish.

Quyida nisbatan ommaviylashgan ochiq kalitli kriptotizimlar qisqacha ko‘rib o‘tiladi.

5.3. Faktorlash murakkabligiga asoslangan nosimmetrik shifrlar

RSA ochiq kalitli shifrlash algoritmi berilgan yetarli katta toq sonni tub ko‘paytuvchilarga ajratishning rasional usuli mavjud emasligiga asoslangan.

Maxfiy tutiladigan hamda yetarli katta bo‘lgan p va q -tub sonlari olinib, $n = pq$-soni va Eyler funksiyasining qiymati $\varphi(n)=(p-1)(q-1)$ hisoblanadi. Bu $\varphi(n)$ -son ochiq va maxfiy kalitlarni generasiya qilish qoidasining maxfiy tutiladigan parametri hisoblanadi. So‘ngra, $(e_i, \varphi(n))=1$ shartni qanoatlantiruvchi, ya’ni $\varphi(n)$ soni bilan o‘zaro tub bo‘lgan e_i -son bo‘yicha d_i-soni ushbu $e_i d_i = 1 \bmod \varphi(n)$ formula orqali Yevklid algoritmi bo‘yicha hisoblanadi. Bu $(e_i; d_i)$ juftlikda e_i -ochiq kalit va d_i-maxfiy kalit deb e’lon qilinadi. Shunday qilib RSA kriptotizimi foydalanuvchisining ochiq kaliti *(n, e)* bo‘lsa, shaxsiy kaliti *(d_i, $\varphi(n)$)* juftligidir.

RSA kriptotizimida i- foydalanuvchidan j- foydalanuvchiga shifrlangan ma’lumotni jo‘natish quyidagicha amalga oshiriladi:

1. **Shifrlash qoidasi**: ushbu ifoda $M^{e_j} \bmod n = C$ hisoblanadi, bu yerda M -ochiq ma’lumot, *S* –shifrlangan ma’lumot;

2. **Deshifrlash qoidasi**: ushbu ifoda $C^{d_j} \bmod n = M^{e_j d_j} \bmod n = M$ hisoblanib, ochiq ma’lumot M hosil qilinadi.

Deshifrlash qoidasidagi $C^{d_j} \bmod n = M^{e_j d_j} \bmod n = M$ munosabatning o‘rinliligi quyidagi teoremalardan kelib chiqadi.

5.1-teorema. Agar $n = pq$, $p \neq q$- tub sonlar va $(x, p)=1, (x, q)=1$ bo‘lsa, u holda

$$x^{\varphi(n)} = 1 \bmod n.$$

Isboti. Agar $(x, p)=1, (x, q)=1$ munosabatlar o‘rinli bo‘lsa, u holda

$$x^{p-1} = 1 \bmod p$$
$$x^{q-1} = 1 \bmod q,$$

bo‘lib, $y = x^{\varphi(n)} = x^{(p-1)(q-1)}$ modul p bo‘ycha ham, modul q bo‘yicha ham 1 ga teng bo‘ladi. Haqiqatan ham:

$$y = x^{\varphi(n)} \bmod p = x^{(p-1)(q-1)} \bmod p = [x^{(p-1)} \bmod n]^{(q-1)} \bmod n = 1^{(q-1)} \bmod n = 1$$

yoki

$$y = x^{\varphi(n)} \bmod p = x^{(p-1)(q-1)} \bmod p = [x^{(q-1)} \bmod n]^{(p-1)} \bmod n = 1^{(p-1)} \bmod n = 1.$$

Bundan esa, (y – 1) ning p va q sonlariga qoldiqsiz bo‘linishi kelib chiqadi hamda y=1 mod pq tenglik o‘rinli bo‘ladi.

5.2-teorema. Agar $n = pq$, $p \neq q$ – tub sonlar va $(e, \varphi(n))=1$ bo‘lsa, u holda ushbu

$$E_{e,n} : x \to x^e \bmod n$$

akslantirish $\mathbf{z}_n = \{0;1;2;...;n-1\}$-chekli maydonda o‘zaro bir qiymatli akslantirish bo‘ladi.

Isboti. Agar $(e,\varphi(n)) = 1$ bo‘lsa, u holda shunday d - haqiqiy son mavjud bo‘ladiki, uning uchun

$$ed = 1 \bmod \varphi(n),$$

munosabat o‘rinli bo‘ladi. Bundan esa ushbu munosabat

$$(x^e)^d = x^{ed} = x^{1+K\varphi(n)} = x(\bmod n)$$

EKUB$(x,n) = 1$ ifodani qanoatlantiruvchi barcha x lar uchun bajariladi.

Agar $x = py$ bo‘lsa, bu yerda $(y,q) = 1$, u holda

$$p \mid x^{1+K\varphi(n)} - x.$$

Bu yerda x soni q ga qoldiqsiz bo‘linmaganligidan

$$x^{1+K\varphi(n)} - x = x\left[(x^{q-1})^{K(p-1)} - 1\right]$$

kelib chiqadi.

Fermaning kichik teoremasiga ko‘ra $x^{q-1} = 1 \bmod q$ va natijada, kvadrat qavs ichidagi ifoda modul p bo‘yicha ham va modul q bo‘yicha ham 0 ga teng bo‘lib, bundan ushbu

$$x^{1+K\varphi(n)} - x = 0 \bmod n$$

tenglikning o‘rinliligi kelib chiqadi.

Xuddi shu kabi, agar $x = qy$ bo‘lsa, bu yerda $(y, p) = 1$, u holda

$$q \mid x^{1+K\varphi(n)} - x.$$

Bu yerda x soni q ga qoldiqsiz bo‘linmaganligidan

$$x^{1+K\varphi(n)} - x = x\left[(x^{p-1})^{K(q-1)} - 1\right]$$

kelib chiqadi.

Fermaning kichik teoremasiga ko‘ra $x^{p-1} = 1 \bmod p$ va natijada, kvadrat qavs ichidagi ifoda modul p bo‘yicha ham va modul q bo‘yicha ham 0 ga teng bo‘lib, bundan ushbu

$$x^{1+K\varphi(n)} - x = 0 \bmod n$$

tenglikning o‘rinliligi kelib chiqadi.

Shunday qilib, keltirilgan teoremalarga ko‘ra

$$C^{d_j} \bmod n = M^{e_j d_j} \bmod n = M^{K\varphi(n)+1} \bmod n = [(M^{\varphi(n)})^K \bmod n \cdot M \bmod n] \bmod n =$$
$$= [1^K \bmod n \cdot M \bmod n] \bmod n = M \bmod n = M$$

chunki, $M < n$.

Ochiq va maxfiy kalitlarning generasiyasi chog‘ida $e_i d_i = 1 \bmod \varphi(n)$ tenglikni qanoatlantiruvchi d_i- sonini $\varphi(n)$- soni ma’lum bo‘lganda Yevklid algoritmi bo‘yicha topiladi. Ammo $\varphi(n)$- soni foydalanuvchilarga noma’lum bo‘lganda d_i- sonidan tashqari $\varphi(n)$-soni ham maxfiy bo‘lib, $\varphi(n)$ - sonini aniqlash uchun n–sonini tub ko‘paytuvchilarga ajratib, r va q sonlarini topish talab etilib, so‘ngra $\varphi(n) = (p-1)(q-1)$ hisoblanadi. n–soni yetarli katta bo‘lganda uni tub ko‘paytuvchilarga ajratib, r va q sonlarini topishning rasional usuli bugungi kunda mavjud emas. Adabiyotlar ro‘yxatida keltirilgan [60] da yetarli katta natural sonlarni eksponensial va subeksponensial murakkabliklarga ajratib, ularni tub ko‘paytuvchilarga ajratishning ba’zi usullari keltirilgan.

Keyingi paragrafda diskret logarifmlash masalasi yechimini xarakteristikasi yetarli katta bo‘lgan chekli maydonda amalga oshirishning murakkabligiga asoslangan El Gamal algoritmi keltirilgan.

5.4. Chekli maydonlarda diskret logarifmlash masalasining yechimi murakkabligiga asoslangan nosimmetrik shifrlar

El Gamal algoritmida kriptotizimning har bir i-foydalanuvchisiga tub modul r va hosil qiluvchi (generator) g ma’lum hisoblanadi va i-foydalanuvchi uchun shaxsiy kalitni ifodalovchi x_i- son bo‘yicha hisoblanadigan $y_i = a^{x_i} \bmod p$- ochiq kalit generasiya qilinadi va u barchaga oshkor etiladi. Agarda mana shu i-foydalanuvchi bilan biror boshqa j-foydalanuvchi ochiq ma’lumot M ni shifrmatnga o‘girilgan holda axborot almashuvini amalga oshirmoqchi bo‘lsa, u holda j-foydalanuvchi r sonidan kichik bo‘lgan biror k -sonini tanlab olib

$$y_1 = g^k \pmod p \text{ va } y_2 = (M / y^k) \pmod p,$$

sonlarini hisoblaydi. So‘ngra j-foydalanuvchi $(y_1;y_2)$ ma’lumotlarini i-foydalanuvchiga jo‘natadi. O‘z navbatida i-foydalanuvchi bu shifrlangan ma’lumotni qabul qilib, quyidagicha

$$(y_1^x \cdot y_2) \bmod p = M$$

hisoblash bilan ochiq ma’lumotni tiklaydi.

El Gamal kriptoalgoritmiga asoslangan kriptotizimning har bir i-foydalanuvchisi uchun (y_i, x_i) - kalitlar juftligi quyidagicha yaratilishi ham mumkin: biror p_i-tub soni va $g_i < p_i$- tengsizlikni qanoatlantiruvchi g_i (foydalanuvchilar guruhi uchun umumiy p va $g < p$ tengsizlikni qanoatlantiruvchi g) sonlari tanlanadi. Ushbu $x_i < p_i$ tengsizlikni qanoatlantiruvchi maxfiy bo‘lgan x_i- soni bo‘yicha ochiq deb e’lon qilinadigan y_i-soni ushbu formula $y_i = g_i^{x_i} (\mathrm{mod}\ p_i)$ (foydalanuvchilar guruhi uchun $x_i < p$ hamda $y_i = g^{x_i} \bmod p$) orqali hisoblanadi. Shunday qilib, El Gamal kritotizimida (p_i, g_i, y_i) – uchlik (foydalanuvchilar guruhi uchun p va g umumiy bo‘lib, (p, g, y_i)) – uchlik) ochiq kalit, x_i - esa maxfiy (shaxsiy) kalit deb olinadi.

Shundan so‘ng i-foydalanuvchidan j- foydalanuvchiga shifrlangan ma’lumotni jo‘natish quyidagicha amalga oshiriladi:

1. **Shifrlash qoidasi**: ushbu ifoda $a_j = g_j^k \bmod p_j$, $b_j = y_j^k M \bmod p_j$ (foydalanuvchilar guruhi uchun p va g umumiy bo‘lganda: $a = g^k \bmod p$, $b = y_j{}^k M \bmod p$) hisoblanadi, bu yerda M- ochiq ma’lumot, k- ma’lumotni shifrlab jo‘natuvchi tomonidan tanlangan tasodifiy son bo‘lib, u ($p_j - 1$) –soni bilan o‘zaro tub, $(a_j, b_j) = C$ (p va g umumiy bo‘lganda $(a, b) = C$–shifrlangan ma’lumot);

2. **Deshifrlash qoidasi**: $b_j \big/ a_j^{x_j} \bmod p_j = M$ (p va g umumiy bo‘lganda: $b \big/ a^{x_j} \bmod p = M$), haqiqatan ham,

$b_j \big/ a_j^{x_j} \bmod p_j \equiv g_j^{x_i k} M \big/ g_j^{k x_i} \bmod p_j \equiv M$ (p va g umumiy bo‘lganda:

$b \big/ a^{x_j} \bmod p \equiv y_j^k M \big/ a^{x_j} \bmod p \equiv g^{x_j k} M \big/ g^{k x_j} \bmod p = M \bmod p = M$, chunki $M < p$).

Kriptotizimning har bir i-foydalanuvchisi uchun ochiq va maxfiy kalitlarni x_i- soni ma’lum bo‘lganda $y_i = g_i^{x_i} \bmod p_i$ (foydalanuvchilar guruhi uchun $x_i < p$ hamda $y_i = g^{x_i} \bmod p$) tenglik bo‘yicha generasiya qilinadi. Ammo x_i- soni foydalanuvchilarga noma’lum bo‘lganda, ochiq kalitni ifodalovchi $y_i = g_i^{x_i} \bmod p_i$ tenglikdan $x_i = \log_{g_i} y_i (\mathrm{mod}\ p_i)$ - sonini topish, chekli maydon xarakteristikasi p_i yetarli katta bo‘lganda, murakkablashadi va bugungi kunda chekli maydonlarda logarifmlash masalasi yechimining rasional (samarali)

usullari mavjud emas. [60] da xarakteristikasi katta bo‘lgan chekli maydonlarda diskret logarifmlashning ba’zi usullari keltirilgan.

5.5. Elliptik egri chiziq gruppasida diskret logarifmlashga asoslangan kriptotizimlar

5.5.1. Elliptik kriptografiyaning yuzaga kelishi

EECh nazariyasini yaratishda so‘nggi qadimiy grek matematigi Diofantdan boshlab o‘tmishning ko‘pgina eng yirik olimlari qatnashgan. EECh gruppasi strukturasini mashhur fransuz matematigi Anri Puankare taklif etgan. Yillar davomida EECh hyech qanday amaliy ahamiyatga ega bo‘lmagan sof matematika sohasi bo‘lib kelgan. O‘tgan asrning 80-yillarida EECh katta sonlarni faktorlash algoritmlarini tuzish sohasida qo‘llanila boshladi [56-60] va bu qo‘llanishlar orqali kriptografiya sohasiga kirib keldi (nosimmetrik tizimlar, psevdotasodifiy sonlarni generasiyalash). Elliptik kriptografiyada haqiqiy burilish 1985 yilda N. Koblis va V. Miller ilmiy ishlari [42-44] chop etilgandan so‘ng yuz berdi. Shu damdan boshlab mashhur jahon kritologlari elliptik kriptografiya bilan shug‘ullana boshladilar.

Faktorlash va EECh gruppasida diskret logarifmlash murakkabliklarini taqqoslama tahlili EEChlarning bahslashuvdan holi afzalliklarini namoyon etdi [61-65]. 5.1- jadvalda taqqoslama ma’lumotlar keltirilgan (ma’lumotlar tub maydonda diskret logarifmlash muammosi uchun ham oson hisoblanadi).

5.1- jadval

Kriptotahlil murakkabliklari bo‘yicha ma’lumotlar

Almashtirish moduli uzunligi	EECh gruppasida kriptotahlil murakkabligi	RSA modulini faktorlash murakkabligi
192 bit	$2^{95,82} \approx 10^{29,21}$	$2^{40,41} \approx 10^{12,32}$
256 bit	$2^{127,82} \approx 10^{39}$	$2^{40,56} \approx 10^{14,5}$
512 bit	$2^{255,82} \approx 10^{78}$	$2^{65,15} \approx 10^{19,86}$
1024 bit	$2^{511,82} \approx 10^{156}$	$2^{88,47} \approx 10^{27}$

XXI asrning boshidan boshlab nosimmetrik kriptografiyaning an’anaga aylanib qolgan kriptotizimlardan bardoshliligi EECh gruppasida diskret logarifmlash muammosining murakkabligiga asoslangan tizimlarga o‘tish boshlangani ko‘zga tashlandi [61-65].

Elliptik kriptografiyaga alohida qiziqish quyidagi sabablar bilan bog‘liq:

- birinchidan, diskret logarifmlash va faktorlash muammolarini yechishga qaratilgan sonli maydon va halqalarda *n* moduli bo‘yicha sonlar silliqligi xossasidan foydalanadigan umumlashgan g‘alvir usuliga asoslangan tezkor algoritmlarning yuzaga kelishi. EECh gruppasida esa silliqlik tushunchasi nuqtalarga tegishli bo‘lib, tezkor kriptotahlillash algoritmlarini tuzish imkoniyatini bermaydi;

- ikkinchidan, EECh gruppasida nisbatan qisqa kalit uzunligi asosida kriptotizimlar ishlab chiqarish imkoniyati mavjudligi. Bular simsiz kommunikasiyalarda va resurs cheklangan hollarda (smart-kartalar, mobil qurilmalar) asosiy hisoblanadi. Masalan, EECh gruppasida tuzilgan kalitning binar uzunligi *150* dan *350* gacha bo‘lgan qurilmalarda an’anaviy qurilmalardagi kalitning binar uzunligi *600* dan *1400* gacha bo‘lgandagidek kriptografik bardoshlilik darajasiga erishiladi [56-58, 61-65].

Yuqorida keltirilgan sabablar AQSh va Rossiya Federasiyasida amaldagi standartlarni elliptik kriptografiyaga oid standartlar bilan almashtirishga olib keldi. Hozirgi kunda EEChlarga asoslangan algoritmlar ko‘plab xalqaro, milliy va sohaga oid standartlar qatoridan o‘rin olgan [66-68]. Elliptik kriptografiyada foydalanish uchun asosan $GF(2^m)$ maydonida aniqlangan singulyar yoki $GF(p)$ maydonida aniqlangan nosupersingulyar EEChlardan foydalanish tavsiya etiladi. Barcha hollarda EECh gruppasida katta tartibga ega bo‘lgan elementlar mavjudligiga ishonch hosil qilish muhimdir.

Kriptografiyada chekli algebraik strukturalarda, masalan, chekli maydonlarda berilgan EEChdan keng foydalaniladi. Tub maydon $GF(p)$ da berilgan EECh

$$y^2 = x^3 + ax + b \ (mod\ p) \quad (14)$$

taqqoslamaning $P = (x, y)$ nuqtalari (yechimlari) to‘plamini tashkil etadi. Bu yerda a va b kattaliklari $4a^3 + 27b \neq 0 \ (mod\ p)$ shartini qanoatlantiruvchi doimiylar, $p>3$. To‘plam gruppani tashkil etishi uchun unga cheksiz uzoqlashgan $0_{Ye}=(x,\infty)$ nuqta birlashtiriladi,

natijada gruppa tashuvchisi *E={14 yechimlari} U{0}* ko‘rinishni oladi. Mazkur gruppaning kriptografiya uchun asosiy amali nuqtalarni takroran *m* marta qo‘shish amali *[m]P* bo‘lib, uni *[m]* ga ko‘paytirish deb ataladi va u rekursiv suratda amalga oshiriladi. Oshkora kriptografiyada yaratilgan ko‘pchilik algoritmlarning EEChli analoglari ishlab chiqilgan. Elliptik egri chiziqli kriptotizimlar kriptobardoshliligi EEChda diskret logarifmlash muammosining murakkabligi bilan belgilanadi. Bu muammoni diskret logarifm muammosiga keltirish [38]da bayon etilgan.

5.5.2. Elliptik egri chiziq nuqtalari gruppasi asosida yaratilgan nosimmetrik shifrlarning umumiy funksional modeli

EECh nuqtalari ustida amallar bajarish masalalari yechimlari murakkabliklariga asoslangan nosimmetrik algoritmlarni yaratishda kriptotizimning har bir i- foydalanuvchisining shaxsiy kalitini ifodalovchi k_i^M-son bo‘yicha hisoblanadigan $[k_i^M]G = Q_i = (x_i^o, y_i^o)$- ochiq kalit generasiya qilinadi, bu yerda G-tanlab olingan elliptik egri chiziqqa tegishli barchaga ma’lum bo‘lgan hosil qiluvchi (generator) nuqta. Bu yerda $G = (x_G, y_G)$ va $Q_i = (x_i^o, y_i^o)$- nuqtalarni bilgan holda k_i^M- shaxsiy kalitni aniqlash o‘zining rasional yechimiga ega emas.

Kriptotizimning *j*-foydalanuvchisi M- ochiq ma’lumotni shifrlab, C- shifrlangan ma’lumotni *i*-foydalanuvchiga jo‘natishi uchun, *i*-foydalanuvchining barchaga ma’lum bo‘lgan ochiq kaliti $Q_i = (x_i^o, y_i^o)$ dan foydalanadi, ya’ni $E_{(x_i^o, y_i^o)}(M) = C$ shifrmatnni *i*-foydalanuvchiga ochiq aloqa tarmog‘i orqali yuboradi. Bu $E_{x_i^o}(M) = C$ (yoki $E_{x_i^o}(M) = C$ yoki $E_{(x_i^o, y_i^o)}(M) = C$) -shifrma’lumotni qabul qilib olgan *i* –foydalanuvchi, faqat uning o‘ziga ma’lum bo‘lgan o‘zining shaxsiy kaliti k_i^M- bilan deshifrlaydi, ya’ni $D_{k_i^M}(C) = M$-ochiq ma’lumotga ega bo‘ladi. Shifrlash qoidasini aniqlovchi akslantirish $E_{(x_i^o, y_i^o)}(M) = C$ bir tomonlamalik xususiyatiga ega bo‘lishi kerak, ya’ni E- akslantirish, $Q_i = (x_i^o, y_i^o)$ ochiq kalit va C- shifrmatnni bilgan holda M- ochiq ma’lumotni aniqlash imkoniyati yo‘q bo‘lishi kerak.

5.6. Parametrli gruppadan foydalanishga asoslangan nosimmetrik shifrlar

Ochiq kalitli kriptoalgoritmlar asosini tashkil etuvchi yetarli katta sonlarni tub ko‘paytuvchilarga yoyish, xarakteristikasi yetarli katta bo‘lgan chekli maydonlarda diskret logarifmlarni hisoblash, EEChlarda rasional koordinatali nuqtalarni topish, ularni qo‘shish hamda tartibini aniqlash masalalarini yechish murakkabliklari bilan bog‘liq holda parametrli gruppa amallaridan foydalanish yangi nosimmetrik algoritmlar yaratish usullariga olib keladi.

Parametrli gruppaning ushbu

$$a \circledR b = a + b + aRb (\mathrm{mod}\ p)$$

ko‘rinishdagi amal asosida shakllangan parametrli gruppa 3-bo‘limda bayon etilgan.

Chekli maydonning a va b - elementlari uchun kiritilgan amalni turlicha aniqlash mumkin. Kiritilgan amalni shifrlash algoritmlarida ochiq kalit va ochiq ma’lumot yoki oraliq natija bloki ustida bajarilishini hisobga olib hamda deshifrlash algoritmlarida shifrma’lumot va maxfiy kalit bloki qiymatlari ustida bajariladigan akslantirishlarga tatbiq qilinishini nazarda tutib, kiritilgan amal bo‘yicha teskari element mavjud bo‘ladigan qilib aniqlanadi. Xeshlash funksiyasi, oqimli shifrlash, kalitlar generasiyasi algoritmlarida va Feystel tarmog‘i akslantirishlarida kiritilgan amal bo‘yicha teskari elementni topishning rasional usuli yo‘q bo‘ladigan yoki umuman mavjud bo‘lmaydigan qilib aniqlash maqsadga muvofiqdir.

5.6.1. Parametrli shifrlash usuli

Kiritilgan amaldan foydalanib, xarakteristikasi yetarli katta bo‘lgan chekli maydonlarda diskret logarifmlash masalasining murakkabligiga asoslangan nosimmetrik shifrlash algoritmini yaratish masalasini yechish sxemasi [13] da keltirilgan. Parametrli shifrlashda, avvalo tub modul r va hosil qiluvchi $g \in F_p$ tanlanib, ushbu son $R_i = g^{x_i} \bmod p$ hisoblanadi, bu yerda x_i - shaxsiy kalit. So‘ngra $(a_i; R_i)$ -juftlikni ochiq kalit deb qabul qilamiz.

Kriptotizimning j - foydalanuvchisi i - foydalanuvchiga M - ochiq ma’lumotni shifrlab jo‘natishni quyidagicha amalga oshiradi:

1. Faqat j- foydalanuvchining o‘zigagina ma’lum bo‘lgan biror k-sonini tasodifiy holda tanlab, $R = (R_i)^k \bmod p = g^{kx_i} \bmod p$ - qiymatni hisoblaydi.

2. Shifrlashni

$a_i \circledR M = a_i + M + a_i RM (\bmod p) = a_i + M + a_i (g^{kx_i} \bmod p) M (\bmod p) = w$ ko‘rinishda amalga oshirib, shifrma’lumot sifatida $C = (w; d = g^k \bmod p)$- juftlik jo‘natiladi.

Shifrma’lumot $C = (w; d = g^k \bmod p)$ni qabul qilib olgan i-foydalanuvchi deshifrlashni quyidagicha amalga oshiradi:

1. Faqat i- foydalanuvchining o‘ziga ma’lum bo‘lgan x_i- maxfiy kalitdan foydalanib, $d^{x_i} \bmod p = g^{kx_i} \bmod p = D$ - qiymat hisoblanadi.

2. Ochiq a_i- kalitga teskari bo‘lgan element

$(a_i)^{\backslash -1} = -a_i (1 + a_i D)^{-1} \bmod p$ hisoblanadi.

3. Ushbu $R = D$ qiymatning almashtirish amalini bajarib, deshifrlash amalga oshiriladi:

$$(a_i)^{\backslash -1} \circledR w = [-a_i (1 + a_i D)^{-1} \bmod p] \circledR [a_i + M + a_i RM (\bmod p)] =$$

$$= [-a_i (1 + a_i R)^{-1} \bmod p] \circledR [a_i + M + a_i RM (\bmod p)] =$$

$$\equiv [-a_i (1 + a_i R)^{-1}] + [a_i + M (1 + a_i R)] +$$

$$[-a_i (1 + a_i R)^{-1}] R [a_i + M (1 + a_i R)] (\bmod p) \equiv$$

$$\equiv [-a_i (1 + a_i R)^{-1}] (1 + a_i R) + [a_i + M (1 + a_i R)] - a_i RM \ (\bmod p) \equiv$$

$$\equiv -a_i + a_i + M + a_i RM - a_i RM \ (\bmod p) = M.$$

Bu keltirilgan nosimmetrik shifrlash algoritmi g‘oyasini saqlab qolgan holda, shifrlash va deshifrlash jarayonlarini ifodalovchi formulalarda qatnashuvchi parametrlarning matrisalar ko‘rinishida aniqlanishi ular xossalaridan foydalanib kriptografik samaradorlikni oshirish imkoniyatlarini beradi. Quyida aynan shunday masala yechimi haqida so‘z yuritiladi.

5.6.2. Matrisaviy parametrli shifrlash usuli

Avvalo yuqoridagi kabi ushbu:

$A_{n \times m} \circledR B_{n \times m} = A_{n \times m} + B_{n \times m} + A_{n \times m} R_{m \times n} B_{n \times m} (\bmod p)$ parametrli ko‘paytirish amali kiritiladi [23, 69].

5.1-ta’rif. $B_{n\times m}$ - matrisa $A_{n\times m}$ - matrisaga teskari deyiladi, agarda $A_{n\times m} \circledR B_{n\times m} = 0_{n\times m}$ bo‘lsa hamda $A_{n\times m}$ - matrisaga teskari bo‘lgan matrisa $A_{n\times m}^{\backslash -1}$ deb belgilanadi.

Endi berilgan matrisaga teskari matrisani qanday topishni ko‘rib o‘tamiz.

Agar $B_{n\times m}$ - matrisa $A_{n\times m}$ - matrisaga teskari bo‘lsa, $C_{n\times m} = A_{n\times m} \circledR B_{n\times m} = B_{n\times m} = 0_{n\times m}$ munosabat bajarilishi kerak. Bu munosabatdan ushbu

$$C_{n\times m} - A_{n\times m} \equiv B_{n\times m} + A_{n\times m} R_{m\times n} B_{n\times m} (\mathrm{mod}\ p)$$ yoki

$C_{n\times m} - A_{n\times m} \equiv (I_{n\times n} + A_{n\times m} R_{m\times n}) B_{n\times m} (\mathrm{mod}\ p)$ yoki $B_{n\times m} \equiv (I_{n\times n} + A_{n\times m} R_{m\times n})^{-1}$ $(C_{n\times m} - A_{n\times m})(\mathrm{mod}\ p)$

taqqoslamaga ega bo‘lamiz. Bu yerda $C_{n\times m} = 0_{n\times m}$ bo‘lganda $B_{n\times m}$ - matrisa $A_{n\times m}$ -matrisaga teskari bo‘lishini hisobga olsak

$B_{n\times m} \equiv (I_{n\times n} + A_{n\times m} R_{m\times n})^{-1} (C_{n\times m} - A_{n\times m})(\mathrm{mod}\ p) = (I_{n\times n} + A_{n\times m} R_{m\times n})^{-1} (-$ $A_{n\times m})(\mathrm{mod}\ p) = A_{n\times m}^{\backslash -1}$ bo‘lishi kelib chiqadi.

Matrisaviy parametrli shifrlash usulida, avvalo *t*-foydalanuvchi tomonidan tub modul *r*, hosil etuvchi *g* elementlar tanlanadi.

Ushbu sonlar $R_{il}^t = g^{x_{il}^t} \bmod p$ hisoblanadi, bu yerda x_{il}^t - noma’lumlar (baytlardan iborat bo‘lishi mumkin), $i = 1,\ldots,m$; $l = 1,\ldots,n$. So‘ngra $(A_{n\times m}^t; R_{m\times n}^t)$ -juftlikni t - foydalanuvchining ochiq kaliti, x_{il}^t - noma’lumlarni esa maxfiy kalit elementlari deb e’lon qilinadi.

Kriptotizimning j - foydalanuvchisi t - foydalanuvchiga $M_{n\times m}$ – ochiq ma’lumotni shifrlab jo‘natishni quyidagicha amalga oshiradi:

1. Faqat j - foydalanuvchining o‘zigagina ma’lum bo‘lgan biror k -sonini tasodifiy holda tanlab, $R = R^t{}_{m\times n} = (R_{il}^t)^k \bmod p = g^{kx_{il}^t} \bmod p$ - matrisa elementlari hisoblab olinadi.

2. Shifrlashni $A_{n\times m}^t \circledR M_{n\times m} = A_{n\times m}^t + M_{n\times m} + A_{n\times m}^t R_{n\times m}^t M_{n\times m} (\mathrm{mod}\ p) = w_{n\times m}$ ko‘rinishda amalga oshirib, shifrma’lumot sifatida $C_{n\times m} = (w_{n\times m}; d = g^k \bmod p)$ - juftlik jo‘natiladi.

Shifrma’lumot $C = (w; d = g^k \bmod p)$ ni qabul qilib olgan t - foydalanuvchi deshifrlashni quyidagicha amalga oshiradi:

3. Faqat t- foydalanuvchining o‘ziga ma’lum bo‘lgan x_{il}^t- maxfiy kalitdan foydalanib, $d^{x_{il}^t} \bmod p = g^{kx_{il}^t} \bmod p = D_{il}^t$ - qiymatlar hisoblanib, $D_{m\times n}$ - matrisa hosil qilinadi.

4. Ochiq $A_{n\times m}^t$ - kalitga teskari bo‘lgan element $(A_{n\times m}^t)^{\setminus -1} = (I_{n\times n} + A_{n\times m}^t D_{m\times n}^t)^{-1}(-A_{n\times m}^t) \bmod p$ hisoblanadi.

5. Ushbu $R = D_{n\times m}^t$ qiymatning almashtirish amalini bajarib, deshifrlash amalga oshiriladi:

$$(A_{n\times m}^t)^{\setminus -1} \circledR\, w_{n\times m} = (I_{n\times n} + A_{n\times m}^t D_{m\times n}^t)^{-1}(-A_{n\times m}^t) \circledR (A_{n\times m}^t + M_{n\times m} + A_{n\times m}^t R_{m\times n}^t M_{n\times m}) (\bmod p) =$$
$$= (I_{n\times n} + A_{n\times m}^t R_{m\times n}^t)^{-1}(-A_{n\times m}^t) + (A_{n\times m}^t + M_{n\times m} + A_{n\times m}^t R_{m\times n}^t M_{n\times m}) +$$
$$+ (I_{n\times n} + A_{n\times m}^t R_{m\times n}^t)^{-1}(-A_{n\times m}^t)\ R_{m\times n}^t\ (A_{n\times m}^t + M_{n\times m} + A_{n\times m}^t R_{m\times n}^t M_{n\times m}) (\bmod p) =$$
$$= (I_{n\times n} + A_{n\times m}^t R_{m\times n}^t)^{-1}(-A_{n\times m}^t)\ (I_{m\times m} + R_{m\times n}^t A_{n\times m}^t) + A_{n\times m}^t + (I_{n\times n} + A_{n\times m}^t R_{m\times n}^t) M_{n\times m} +$$
$$+ (I_{n\times n} + A_{n\times m}^t R_{m\times n}^t)^{-1}(-A_{n\times m}^t) R_{m\times n}^t\ (I_{n\times n} + A_{n\times m}^t R_{m\times n}^t) M_{n\times m}\ (\bmod p).$$

Bu oxirgi tenglik ifodasidagi matrisalarning faqat diagonal elementlarining hammasi nol bo‘lmay, boshqa barcha elementlari nollardan iborat bo‘lsa, u holda matrisalar ko‘paytmalari qatnashgan hadlarda ular o‘rinlarini almashtirsa ham tenglik o‘zgarmaydi. Ana shunday matrisalar uchun ushbu tenglik o‘rinli:

$$(A_{n\times m}^t)^{\setminus -1} \circledR\, w_{n\times m} = (I_{n\times n} + A_{n\times m}^t R_{m\times n}^t)^{-1}(-A_{n\times m}^t)\ (I_{m\times m} + R_{m\times n}^t A_{n\times m}^t) + A_{n\times m}^t +$$
$$+ (I_{n\times n} + A_{n\times m}^t R_{m\times n}^t) M_{n\times m} +$$
$$+ (I_{n\times n} + A_{n\times m}^t R_{m\times n}^t)^{-1}(-A_{n\times m}^t) R_{m\times n}^t\ (I_{n\times n} + A_{n\times m}^t R_{m\times n}^t) M_{n\times m}\ (\bmod p) =$$
$$= (-A_{n\times m}^t)(I_{n\times n} + A_{n\times m}^t R_{m\times n}^t)^{-1}\ (I_{m\times m} + R_{m\times n}^t A_{n\times m}^t) + A_{n\times m}^t + (I_{n\times n} + A_{n\times m}^t R_{m\times n}^t) M_{n\times m} +$$
$$+ (-A_{n\times m}^t) R_{m\times n}^t (I_{n\times n} + A_{n\times m}^t R_{m\times n}^t)^{-1}\ (I_{n\times n} + A_{n\times m}^t R_{m\times n}^t) M_{n\times m} (\bmod p) =$$
$$= -A_{n\times m}^t + A_{n\times m}^t + M_{n\times m} + A_{n\times m}^t R_{m\times n}^t M_{n\times m} - A_{n\times m}^t R_{m\times n}^t\ M_{n\times m} (\bmod p) = M_{n\times m}.$$

Umuman olganda bu tenglik ifodalarida qatnashuvchi matrisalar kommutativlik xossasiga ega bo‘ladigan qilib tanlab olinsa, yuqorida keltirilgan deshifrlash jarayoni ijobiy amalga oshiriladi.

5.6.3. Elliptik egri chiziqlardan foydalanishga asoslangan shifrlash usuli

Quyida tanlangan elliptik egri chiziqning rasional nuqtalari ustida amallar bajarish masalasining murakkabligiga asoslangan nosimmetrik shifrlash algoritmini yaratish masalasini yechishga to‘xtalib o‘tiladi.

Mazkur usul bo‘yicha ushbu nuqta $R_{m\times n} = R_{il} = [x_{il}]G$ koordinatalari, tanlab olingan elliptik egri chiziqqa tegishli bo‘lgan G- rasional koordinatali yetarli katta tartibga ega bo‘lgan va barcha foydalanuvchilarga ma’lum generator nuqta orqali hisoblanadi, bu yerda x_{il}-noma’lumlar. So‘ngra $(A_{n\times m}; R_{m\times n})$ - juftlik ochiq kalit deb e’lon qilinadi, x_{il}-noma’lumlar esa shaxsiy kalit sifatida olinadi.

Kriptotizimning j-foydalanuvchisidan t- foydalanuvchiga *M*–ochiq ma’lumotni shifrlab jo‘natish quyidagicha amalga oshiriladi:

1. Faqat j-foydalanuvchining o‘zigagina ma’lum bo‘lgan biror k- sonini tasodifiy holda tanlab, elliptik egri chiziqda $R = [k]R^t_{m\times n} = [k][x^t_{il}]G = [kx^t_{il}]G = (x^t_{il}(G), y^t_{il}(G))$-nuqtalar topiladi va bu nuqtalarning *Ox* o‘qidagi $x^t_{il}(G)$-koordinatalari (yoki *Oy* o‘qidagi $y_{il}(G)$-koordinatalari) $R^t_{il} = x^t_{il}(G)$ (yoki $R^t_{il} = y^t_{il}(G)$ yoki $R^t_{il} = f(x^t_{il}(G), y^t_{il}(G))$) deb qabul qilinadi. Shifrlashni $A^t_{n\times m} \text{®} M_{n\times m} = A^t_{n\times m} + M_{n\times m} + A^t_{n\times m}R^t_{n\times m}M_{n\times m} (\text{mod } p) = w_{n\times m}$ ko‘rinishda amalga oshirib, shifrma’lumot sifatida $C_{n\times m} = (w_{n\times m}; d = [k]G)$-juftlik jo‘natiladi.

Shifrma’lumot $C_{n\times m} = (w_{n\times m}; d = [k]G)$ni qabul qilib olgan t-foydalanuvchi tomonidan deshifrlash quyidagicha amalga oshiriladi:

2. Faqat t- foydalanuvchining o‘ziga ma’lum bo‘lgan x^t_{il}-maxfiy kalit elementlaridan foydalanib $[x^t_{il}]d = [x^t_{il}][k]G = [x^t_{il}k]G = D^t_{m\times n}$ - matrisa hisoblab olinadi.

3. Ochiq $A^t_{n\times m}$- kalitga teskari bo‘lgan matrisa $(A^t_{n\times m})^{\setminus -1} = (I_{n\times n} + A^t_{n\times m}D^t_{m\times n})^{-1}(-A^t_{n\times m}) \text{ mod } p$ hisoblanadi.

4. Ushbu $R = D^t_{n\times m}$ qiymatni almashtirish amalini bajarib, deshifrlash jarayoni 5.6.2-banddagi kabi amalga oshiriladi.

5.6.4. RSA shifriga o‘xshash parametrli shifrlash usuli

Quyida yetarli katta sonni tub ko‘paytuvchilarga ajratish masalasining murakkabligiga asoslangan nosimmetrik shifrlash algoritmi yaratish masalasini yechish keltirib o‘tiladi [1].

Yetarli katta va maxfiy tutilishi kerak bo‘lgan p va q- tub sonlari tanlab olinib, $n = pq$ hisoblanadi. Ushbu $e_t d_t \equiv 1 \text{ mod } \varphi(n)$ taqqoslamadan (bu yerda $\varphi(n) = (p-1)(q-1)$- maxfiy) e_t-parametrga biror qiymat berib $e_t d_t \equiv 1 \text{ mod}(p-1)(q-1)$ munosabatni qanoatlantiruvchi d_t-

sonini topish mumkin. So‘ngra $(A_{n\times m};e_t;n)$ - uchlikni ochiq kalit, $(d_t;\varphi(n))$ - juftlikni shaxsiy deb, shifrlash va deshifrlash jarayonlari quyidagicha amalga oshiriladi.

Kriptotizimning j- foydalanuvchisi tomonidan t - foydalanuvchiga $M_{n\times m}$– ochiq ma’lumotni shifrlab jo‘natish qo‘yidagicha amalga oshiriladi:

1. Faqat j- foydalanuvchining o‘zigagina ma’lum bo‘lgan biror k_{il}^j-sonlarini tasodifiy holda tanlab, $R=R_{m\times n}^j=(k_{il}^j)\bmod n$ - qiymatlar hisoblanadi (bu erda $k_{il}^j\neq p$ va $k_{il}^j\neq q$).

Shifrlash 5.6.2-banddagi kabi $A_{n\times m}^t \text{®} M_{n\times m}=A_{n\times m}^t+M_{n\times m}+A_{n\times m}^t R_{m\times n}^j M_{n\times m}(\bmod p)=w_{n\times m}$ ko‘rinishda amalga oshirilgach, shifrma’lumot sifatida $C_{n\times m}=(w_{n\times m};d_{m\times n}^j=(k_{il}^j)^{e_t}\bmod n)$ - juftlik jo‘natiladi.

2. Shifrma’lumot $C=(w;d_{m\times n}^j=(k_{il}^j)^{e_i}\bmod n)$ni qabul qilib olgan t-foydalanuvchi tomonidan deshifrlash quyidagicha amalga oshiriladi:

1. Faqat t- foydalanuvchining o‘ziga ma’lum bo‘lgan d_t- maxfiy kalitdan foydalanib $(d_{m\times n}^j)^{d_t}\bmod n=(k_{il}^j)^{e_t d_t}\bmod n=(k_{il}^j)\bmod n=D_{m\times n}^j$- matrisa hisoblanadi.

2. Ochiq $A_{n\times m}^t$-kalitga teskari bo‘lgan matrisa $(A_{n\times m}^t)^{\backslash -1}=(I_{n\times n}+A_{n\times m}^t D_{m\times n}^t)^{-1}(-A_{n\times m}^t)\bmod p$ hisoblanadi.

3. Ushbu $R=D_{n\times m}^t$ qiymatni almashtirish amalini bajarib, deshifrlash jarayoni 5.6.2-banddagi kabi amalga oshiriladi.

Yuqorida keltirilganlardan parametrli gruppa amallari xususiyatlari mavjud murakkabliklarni kompozisiyalari negizida takomillashgan yangi nosimmetrik algoritmlar yaratish imkoniyatlarini berishi ayon bo‘ladi.

5.7. Kalitlar generasiyasi

5.7.1. Bardoshli kalitlarni ishlab chiqish usullarining matematik asoslari va algoritmlari

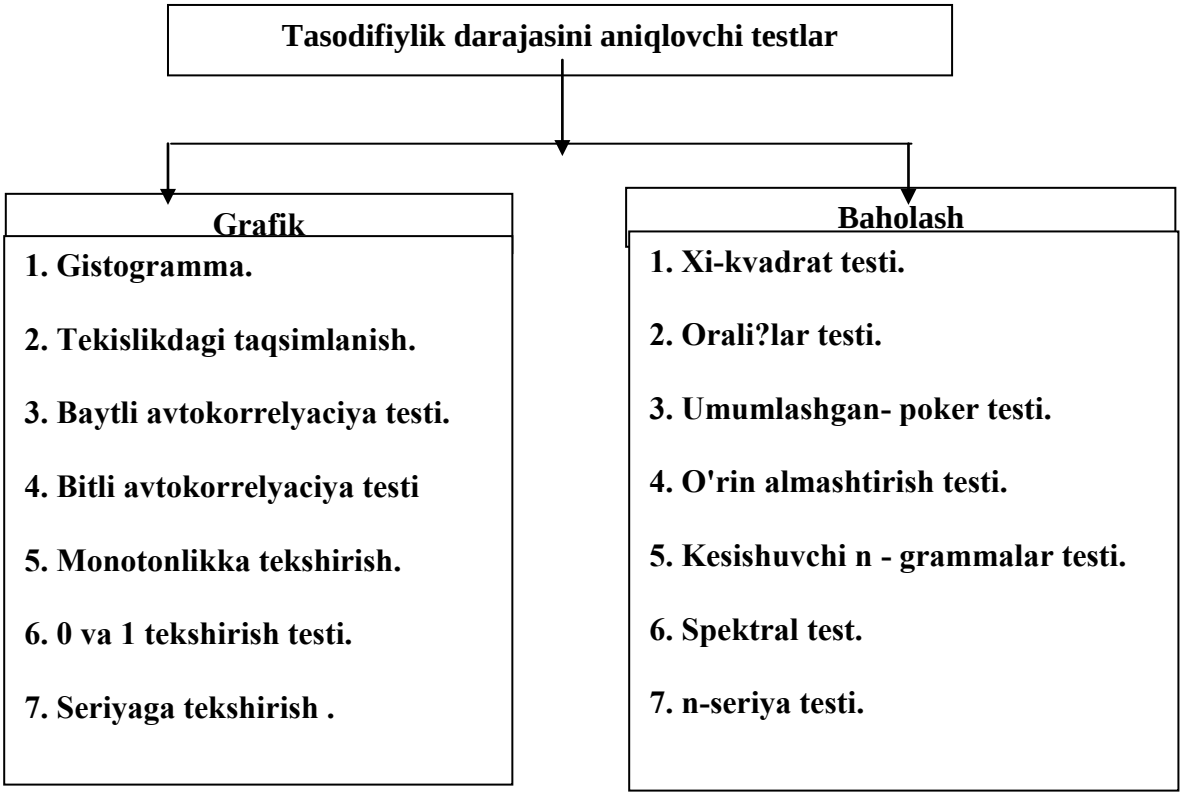
Kriptoalgoritmlar, xususan blokli simmetrik shifrlash algoritmlari DES, AES, GOST 28147-89, O‘z DSt 1106:2009, mos ravishda 56 bit, 128, 256 bit yoki 512 bit, 256 bit, 256 yoki 512 bit

uzunlikdagi oldindan belgilab qo‘yilgan qoida bo‘yicha generasiya qilingan kalitlardan foydalanadi. Biroq standart algoritmlarda belgilab qo‘yilgan qoida bo‘yicha generasiya qilingan barcha kalitlar har doim ham shifrmatnni ochish maqsadida ochiq aloqa tarmog‘ini nazorat qiluvchi kriptotahlilchi tomonidan uyushtiriladigan turli kriptohujumlarga bardoshli bo‘lmasligi mumkin. Masalan, kalitni tashkil etuvchi bitlar ketma-ketligi faqat nollardan yoki birlardan yoki bo‘lmasa, nol va birlarning kombinasiyasi fiksirlangan davr bilan takrorlanishi yordamida tuzilgan bo‘lsa, bu toifa kalitlar bardoshsiz hisoblanadi. Chunki ushbu tur bitlar ketma-ketligida, shu ketma-ketlikni tashkil etuvchi nol va bir elementlari davriy takrorlanishining matematik qonuniyatini oldindan bilish imkoniyati mavjud. U holda bu zaylda generasiya qilingan bitlar ketma-ketligidan simmetrik shifrlash algoritmlari uchun maxfiy kalit sifatida foydalanish maqsadga muvofiq emas. Demak, yuqoridagi fikr-mulohazalardan kelib chiqib, «kriptoalgoritmlar maxfiy kalit bloklari uchun tasodifiy bitlar ketma-ketligi qanday quriladi?» degan savolning tug‘ilishi tabiiy, yani agar biror qoida bo‘yicha kalit blokining $k = k_1 k_2 ... k_m$, ketma-ketligi olingan bo‘lsa, bu yerda $k_i \in \{0;1\}$ va m=56, 128, 192, 256 bo‘lishi mumkin. U holda $k = k_1 k_2 ... k_m$, kalit blokida k_i - bitlarning taqsimoti tasodifiy yoki tasodifiy emasligi qanday aniqlanadi? Ushbu savolga javob olish uchun kalit blokida k_i-bitlarning taqsimotini amaliyotda keng tarqalgan va boshqa mavjud tasodifiylik testlarining asoslarini tashkil etuvchi “Xi-kvadrat” taqsimotidan foydalanib aniqlash kerak bo‘ladi.

Tasodifiylikka tekshiruvchi testlar 2 xil bo‘ladi (5.1-rasm).

Grafik testlar - Grafik testlar foydalanuvchiga tekshirilayotgan ketma-ketlikning ma’lum bir grafik bog‘liqligi haqidagi ma’lumotni berib, u bo‘yicha tekshirilayotgan ketma-ketlik xossalari to‘g‘risida xulosa chiqarish imkoniyatini beradi.

Baholash testlari - Baholash testlari tekshirilayotgan ketma-ketlik statistik xossalarini tahlil qilib, uning chin tasodifiylik darajasi haqida xulosa chiqarish imkoniyatini beradi [12-13].



5.1- rasm. Tasodifiylik darajasini aniqlovchi testlar

Kalit blokini tashkil etuvchi belgilar taqsimotini tasodifiylikka tekshirishda, avvalo, bu kalit blokini biror qoida bo‘yicha hosil qilib olish zarur. Bu kabi ishlar odatda, psevdotasodifiy ketma-ketliklar generatorlari orqali amalga oshiriladi. Psevdotasodifiy ketma-ketlik ishlab chiqaruvchi generatorlar haqida, ularning tuzilish asoslariga ko‘ra turkumlari, xususiyatlari, xossalari, kriptografik masalalarni yechishdagi qo‘llanishlari 5-bo‘limda batafsil tahlil qilingan.

Quyida misol sifatida bir tomonlama funksiyalarga asoslangan psevdotasodifiy ketma-ketlik ishlab chiqaruvchi generatorlar keltirib o‘tiladi [13]:

1) **ANSI X9.17 generatori.** Bu algoritm AQShda psevdotasodifiy ketma-ketlik ishlab chiquvchi Milliy standart hisoblanib, FIPS (USA Federal Information Processing Standart) tarkibiga kiradi. Algoritmda bir tomonlama funksiya sifatida 3DES ikkita *K1, K2* $\in V64$ kalit ishlatiladi: *DESK1DESK2 DESK1*(64 bit) .

2) FIPS-186 generatori. Bu algoritm ham AQSh Milliy standarti sifatida qabul qilingan bo‘lib, DSA elektron raqamli imzo algoritmining maxfiy parametrlarini va kalitlarini generasiya qilish

uchun mo‘jallangan. Algoritm bir tomonlama funksiya sifatida DES shifrlash algoritmi va SHA-1 xeshlash algoritmini ishlatadi.

3) Yarrow-160 generatori. Yarrow-160 psevdotasodifiy ketma-ketlik ishlab chiqaruvchi generatori Kelsi, Shnayer va Fergyuson tomonidan taklif qilingan. Bu yerda uchlik DES va SHA-1 xeshlash algoritmi ishlatilgan.

Sonlar nazariyasi muammolariga asoslangan generatorlar sifatida:

1) RSA algoritmi asosidagi;

2) Mikali-Shnorr RSA algoritmi asosidagi;

3) BBS (Blum-Blum-Shub) - algoritmi asosidagi generatorlarni keltirish mumkin.

Agar chiziqli va multiplikativ kongruent generatorlar bilan aniqlangan sonlar ketma-ketligi uchun z_n, z_{n+1} – bitlari ma’lum bo‘lsa, u holda hosil qilingan ketma-ketlikning qolgan hadlarini topish imkoniyati mavjud [13, 69].

Sonlar nazariyasining muammolariga (tub ko‘paytuvchilarga ajratish va diskret logarifmlash) asoslangan generatorlardan simmetrik shifrlash algoritmlari bardoshli kalitlarining generasiya qilinishida foydalanish maqsadga muvofiq, chunki bu generatorlardan foydalanib, hosil qilingan ketma-ketlik hadlarining biror qismini bilgan holda undan oldingi yoki keyingi qismlarini aniqlash imkoniyati murakkab masala hisoblanadi.

Biz bundan keyingi fikr-mulohazalarimizda, biror tanlangan psevdotasodifiy ketma-ketliklar generatori orqali kerakli uzunlikdagi kalit bloki generasiya qilib olingan deb hisoblaymiz.

5.7.2. Taqsimotni tasodifiylikka tekshirishning “Xi-kvadrat” mezoni

Biror o‘tkazilayotgan tajriba natijalarining barcha mumkin bo‘lgan holatlari $y_1, y_2, ..., y_k$, dan iborat va ularning soni *k* ga teng bo‘lib, bu tajriba bir-biriga bog‘liqsiz holda *n* marta o‘tkazilsin. Shunda, $y_1, y_2, ..., y_k$ -holatlarni, ularning *n* marta o‘tkazilgan tajribada, bir xil sonda takrorlanishidan (tekis taqsimotdan yoki bir xil chastotaga ega bo‘lishdan) qanchalik chetlanganligini baholash

masalasining yechilishi ko‘rib chiqiladi. Buning uchun quyidagicha belgilashlar kiritiladi:

p_s - tajriba natijasi y_s bo‘lishining ehtimollik qiymati;

Y_s - tajriba natijalarining y_s holatga tegishlilari (tenglari) soni.

U holda, bu belgilashlarga nisbatan “Xi-kvadarat” deb ataluvchi taqsimot mezoni ushbu

$$V = \sum_{s=1}^{k} \frac{(Y_s - np_s)^2}{np_s},$$

formula orqali aniqlanadi.

Agar tajriba *n* martadan bir necha marta o‘tkazilganda, har doim $y_1, y_2, ..., y_k$ - holatlar teng Y_i martadan takrorlansa (tekis taqsimlangan yoki bir xil chastotali bo‘lsa), ya’ni $Y_1 = Y_2 = ... = Y_k$ bo‘lsa, u holda $p_1 = p_2 = ... = p_k = \frac{1}{k}$, deb xulosa qilinadi va

$$V = \sum_{s=1}^{k} \frac{\left(Y_s - \frac{n}{k}\right)^2}{\frac{n}{k}} = \sum_{s=1}^{k} \frac{\left(\frac{n}{k} - \frac{n}{k}\right)^2}{\frac{n}{k}} = 0$$

tenglik o‘rinli bo‘ladi. Bunday jarayonning ilmiy-tadqiqot uchun qizig‘i yo‘q. Ammo amaldagi aksariyat jarayonlarda bunday holat kuzatilmaydi, ya’ni biror tajriba bir-biriga bog‘liqsiz ravishda *n* marta o‘tkaziliganda: $Y_1 = Y_2 = ... = Y_k = \frac{n}{k}$ holat kuzatilmaydi. Shuning uchun $y_1, y_2, ..., y_k$ - holatlarni ro‘y berish ehtimolliklari bir xil $p_1 = p_2 = ... = p_k = \frac{1}{k}$ bo‘lib, tajriba bir-biriga bog‘liq bo‘lmagan ravishda *n* marta o‘tkazilganda, bu holatlarning ro‘y berishi soni mos ravishda $Y_1, Y_2, ..., Y_k$ bo‘lsa, u holda ushbu

$$V = \sum_{s=1}^{k} \frac{\left(Y_s - \frac{n}{k}\right)^2}{\frac{n}{k}} = \frac{k}{n} \sum_{s=1}^{k} \left(Y_s - \frac{n}{k}\right)^2$$

formula $Y_1 = Y_2 = ... = Y_k = \frac{n}{k}$ bo‘lgan teng taqsimotdan $Y_1, Y_2, ..., Y_k$ -teng bo‘lmagan taqsimotni o‘rtacha kvadratik chetlanishini ifodalaydi. Bu oxirgi formuladagi $\left(Y_s - \frac{n}{k}\right)$ - ifoda biror o‘zgarmas son bilan chegaralangan, ya’ni $\left|Y_s - \frac{n}{k}\right| \le C = const$.

Shuning uchun

$$V=\sum_{s=1}^{k}\frac{\left(Y_s-\frac{n}{k}\right)^2}{\frac{n}{k}}=\frac{k}{n}\sum_{s=1}^{k}\left(Y_s-\frac{n}{k}\right)^2 \qquad \le \frac{k}{n}\sum_{s=1}^{k}C^2=\frac{(kC)^2}{n}\to 0, \qquad \text{agar}$$

$n\to\infty$ bo‘lsa.

Bu oxirgi formuladan, biror generator orqali hosil qilingan psevdotasodifiy ketma-ketlikning davri yetarli uzun bo‘lib, barcha mumkin bo‘lgan bitlar, baytlar va qism bloklarining taqsimoti deyarli tekis (teng taqsimlangan) bo‘lsa, u holda “Xi-kvadarat” taqsimot mezonining bu ketma-ketlikka nisbatan qiymati nolga yaqin bo‘lib, uning tasodifiylik darajasi yuqori hisoblanadi.

Quyida standart DES, GOST 28147-89, AES-FIPS-197, O‘z DSt 1106:2009 va boshqa simmetrik shifrlash algoritmlari uchun maxfiy kalitni tasodifiy qilib generasiya qilishning Xi-kvadrat taqsimoti orqali qanday amalga oshirilishini ko‘rib o‘tamiz.

Berilgan kalit bloki bo‘yicha quyidagi jadvalni tuzib olamiz:

Qiymat (s) : 0 1 ;

Ehtimollik (p_s) : $\frac{1}{2}$ $\frac{1}{2}$;

Kuzatilayotgan son (Y_s) : N_0 N_1 ,

bu yerda N_0 va N_1 mos ravishda kalit blokida ishtirok etuvchi nollar va birlar, $N_0+N_1=n$, orqali kalit uzunligini belgilaydi, masalan $n=256$;

Kutilayotgan son (np_s) : $\frac{n}{2}$ $\frac{n}{2}$;

Xi-kvadrat taqsimoti formulasi bo‘yicha [74]:

$$V=\sum_{s=0}^{k-1}\frac{(Y_s-np_s)^2}{np_s}$$ hisoblanadi.

Ushbu qaralayotgan holatda:

$k=2;\ s=0,1;\ p_0=p_1=\frac{1}{2};\ Y_0=N_0;\ Y_1=N_1;\ n=256$; u holda quyidagicha kattalikka ega bo‘lamiz:

$$V=\frac{(N_0-128)^2+(N_1-128)^2}{128}.$$

Bu kattalikni hisoblash uchun bizga Xi-kvadrat taqsimotining kritik nuqtalari jadvali deb ataluvchi jadval kerak bo‘ladi (5.2- jadval).

5.2- jadval

Xi-kvadrat taqsimotining kritik nuqtalari

	p=1%	p=5%	p=25%	p=50%	p=75%	p=95%	p=99%
N=*1*	**0.00016**	**0.00393**	**0.1015**	**0.4549**	**1.323**	**3.841**	**6.635**
N=*2*	**0.02010**	**0.1026**	**0.5754**	**1.386**	**2.773**	**5.991**	**9.210**
N =*3*	**0.1148**	**0.3518**	**1.213**	**2.366**	**4.108**	**7.815**	**11.34**
N =*4*	**0.2971**	**0.7107**	**1.923**	**3.357**	**5.385**	**9.488**	**13.28**
N =*5*	**0.5543**	**1.1455**	**2.675**	**4.351**	**6.626**	**11.07**	**15.09**
N =*6*	**0.8721**	**1.635**	**3.455**	**5.348**	**7.841**	**12.59**	**16.81**
N =*7*	**1.239**	**2.167**	**4.255**	**6.346**	**9.037**	**14.07**	**18.48**
N =*8*	**1.646**	**2.733**	**5.071**	**7.344**	**10.22**	**15.21**	**20.09**
N =*9*	**2.088**	**3.325**	**5.899**	**8.343**	**11.39**	**16.92**	**21.67**
N =*10*	**2.558**	**3.940**	**6.737**	**9.342**	**12.55**	**18.31**	**23.21**
N =*11*	**3.053**	**4.575**	**7.584**	**10.34**	**13.70**	**19.68**	**24.72**
N =*12*	**3.571**	**5.226**	**8.438**	**11.34**	**14.85**	**21.03**	**26.22**
N =*15*	**5.229**	**7.261**	**11.04**	**14.34**	**18.25**	**25.00**	**30.58**
N =*20*	**8.260**	**10.585**	**15.45**	**19.34**	**23.83**	**31.41**	**37.57**
N =*30*	**14.95**	**18.49**	**24.48**	**29.34**	**34.80**	**43.77**	**50.89**
N =*50*	**29.71**	**34.76**	**42.94**	**49.33**	**56.33**	**67.50**	**76.15**
N >*30*	$v + \sqrt{2v}\,x_p + \frac{2}{3}x_p^2 - \frac{2}{3} + O(\frac{1}{\sqrt{v}})$						
x_p =*8*	**-2.33**	**-1.36**	**-0.674**	**0.00**	**0.674**	**1.64**	**2.33**

“Xi-kvadrat” mezoni jadvali $\nu = k - 1 = 2 - 1 = 1$, satridan V qiymat joylashish oralig‘ini topamiz. Agar V qiymat jadval ustunining $p = 25\%$ dan $p = 75\%$ oralig‘ida bo‘lsa, u holda psevdotasodifiy generator yordamida hosil qilingan kalit blok bitlari ketma-ketligi tasodifiy deb olinadi.

Garchand psevdotasodifiy generator yordamida hosil qilingan kalit blok bitlari ketma-ketligi tasodifiylikka “Xi-kvadrat” mezoni bo‘yicha tekshirilganda ijobiy javob olingan bo‘lsa ham, undan ko‘ra ishonchli va mukammal bo‘lgan javob olish uchun qaralayotgan bitlar ketma-ketligini boshqa mavjud tasodifiylik testlariga ham tekshirib ko‘rish lozim. Bu me’onlarga tekshiruv natijalarida qanchalik ko‘p ijobiy javoblar olinsa, mezon shunchalik yaxshi natija deb qaraladi. Bundan tashqari quyidagi jarayon ham tasodifiylikka tekshirishda chiqariladigan xulosaning ijobiyligiga sezilarli darajada ta’sir

ko‘rsatadi, ya’ni psevdotasodifiy generator yordamida ishlab chiqilgan kalitlarning amaliyotda o‘rnatilgan bardoshsiz kalitlardan o‘rtacha kvadrat chetlanishining o‘rtacha qiymatini ifodalovchi jarayon.

Aytaylik, psevdotasodifiy generator yordamida hosil qilingan kalit bloki:

$k = k_1 k_2 ... k_n = k_1 k_2 ... k_{256}$, bu yerda $k_i \in \{0;1\}$, *i=1,2, …, n = 256,* yuqorida keltirilgan mezon bo‘yicha tasodifiylikka tekshirilgan va qoniqarli javob olingan. Amaliyot jarayonida shifrlash tizimlari bilan ishlashda aniqlangan bardoshsiz kalitlarni $k_{н1}, k_{н2}, ..., k_{нт}$ kabi belgilaymiz.

Psevdotasodifiy generator yordamida hosil qilingan kalit bloki: $k = k_1 k_2 ... k_n = k_1 k_2 ... k_{256}$va amaliyot jarayonida bardoshsiz deb topilgan $k_{н1}, k_{н2}, ..., k_{нт}$ kalitlarning farqi ko‘rib o‘tiladi:

$r_1 = k_{н1} \oplus k = r_1(1) r_2(1) ... r_{256}(1)$, bu farq bo‘yicha mos ravishda 0 va 1 bitlar soni $N_0(1)$, $N_1(1)$;

$r_2 = k_{н2} \oplus k = r_1(2) r_2(2) ... r_{256}(2)$, bu ayirma bo‘yicha mos ravishda 0 va 1 bitlar soni $N_0(2)$, $N_1(2)$;

$r_m = k_{нт} \oplus k = r_1(m) r_2(m) ... r_{256}(m)$, bu ayirma bo‘yicha mos ravishda 0 va 1 bitlar soni $N_0(m)$, $N_1(m)$; bu kattaliklardan foydalangan holda, quyidagilarni hisoblaymiz:

$$V_1 = \frac{(N_0(1) - 128)^2 + (N_1(1) - 128)^2}{128};$$

$$V_2 = \frac{(N_0(2) - 128)^2 + (N_1(2) - 128)^2}{128};$$

$$V_m = \frac{(N_0(m) - 128)^2 + (N_1(m) - 128)^2}{128};$$

$$V = \frac{V_1 + V_2 + ... + V_m}{m} .$$

“Xi-kvadrat” mezoni jadvali $\nu = k - 1 = 2 - 1 = 1$, satridan V - qiymat joylashish oralig‘ini topamiz. Agar V qiymat jadval ustunining $p = 25\%$ dan $p = 75\%$ oralig‘ida bo‘lsa, u holda psevdotasodifiy generator yordamida hosil qilingan kalit blok bitlari ketma-ketligi tasodifiy deb olinadi.

5.7.3. Kalitlar ochiq taqsimlanish algoritmining matematik asosi haqida

Agarda $y = f(x) = a^x$ bo‘lsa, u holda tabiiyki, bu funksiyaga teskari funksiya

$$x = f^{-1}(y) = \log_a y$$

bo‘lib, berilgan y lar bo‘yicha x qiymatlarni topish diskret logarifmlarni topish masalasi deyiladi. Hattoki, p ning yetarli katta bo‘lgan qiymatlarida ham, $f(x)$ funksiyani oson hisoblash mumkin.

Agarda diskret darajaga ko‘tarish funksiyasi haqiqatan ham bir tomonlama bo‘lsa, u holda $\log_a y$ ifodani y ning barcha, ya’ni ushbu $1 \le y \le p$ tengsizlikni qanoatlantiruvchi barcha qiymatlarida hisoblashni amaliy jihatdan imkoniyati yo‘q bo‘lishi kerak. M.Ye. Xellman va uning shogirdi Polig, faqatgina p soni katta tub son bo‘lgandagina emas, balki $(p-1)$ soni katta tub ko‘paytuvchi q ga ega (yoki shu q tub son 2 ga ko‘paytirilgan) bo‘lganda, funksiyaning y qiymatlariga ko‘ra $\log_a y$ ifodani hisoblash amaliy jihatdan murakkab ekanligini ko‘rsatdilar. U. Diffi va M.Ye. Xellman maxfiy aloqa tizimlari foydalanuvchilari uchun diskret logarifmlardan foydalanib, maxfiy kalitlarni o‘zaro almashuvini alohida maxfiy kanalsiz amalga oshirish algoritmini yaratdilar. Bu algoritm bo‘yicha:

1. α va p sonlari hamma foydalanuvchilarga ma’lum.

2. Har bir foydalanuvchi, masalan, $i-$ foydalanuvchi 1 bilan $(p-1)$ sonlari oralig‘idagi biror butun X_i sonini tanlab oladi va bu sonni maxfiy tutadi.

3. $i-$foydalanuvchi $Y_i = \alpha^{X_i} (\mathrm{mod}\, p)$ qiymatni hisoblab, bu Y_i qiymatni maxfiy tutmay, hamma foydalanuvchilar tomonidan tasdiqlangan va ular har doim foydalana oladigan ochiq ma’lumotlar kitobiga kiritadi.

4. Agarda maxfiy aloqa tizimining $i-$ foydalanuvchisi $j-$ foydalanuvchi bilan maxfiy aloqa o‘rnatmoqchi bo‘lsa, $i-$ foydalanuvchi ochiq ma’lumotlar kitobidan Y_j ni olib, o‘zining maxfiy kaliti X_i yordamida

$$Z_{ij} = \left(Y_j\right)^{X_i} = \left(\alpha^{X_j}\right)^{X_i} = \alpha^{X_i X_j} (\mathrm{mod}\, p)$$

qiymatni hisoblaydi.

5. Xuddi shu kabi $j-$ foydalanuvchi ham Z_{ji} ni hisoblaydi. Bunda $Z_{ij} = Z_{ji}$ bo‘lib, i va j foydalanuvchilar o‘z maxfiy aloqalarini ta’minlovchi simmetrik kalitli kriptotizimda Z_{ij} qiymatni maxfiy kalit sifatida ishlatishlari mumkin. Agar raqib tomon diskret logarifmlarni hisoblash masalasini yecha olsa, ochiq ma’lumotlar kitobidan Y_i va Y_j larni olib, $X_i = \log_\alpha Y_i$ va $X_j = \log_\alpha Y_j$ qiymatlarni hisoblab, Z_{ij} maxfiy kalitga ega bo‘lgan bo‘lar edi (i va j - foydalanuvchilar kabi).

Shu yerda ta’kidlab o‘tish joizki, ochiq ma’lumotlar kitobi axborotlarning maxfiy aloqa tizimi foydalanuvchilarigagina ochiq.

Yuqorida keltirilgan algoritmdan ko‘rinib turibdiki, hali bu narsa nazariy jihatdan to‘la isbotlangan bo‘lmasada, raqib tomon Z_{ij} qiymatni boshqa biror uslub bilan hisoblay olmaydi. Keltirilgan algoritm U.Diffi va M.Ye. Xellmanning kalitlarni ochiq taqsimlash tizimi deyiladi. Bu maxfiy aloqa tizimida maxfiy kalitlarni maxfiy kanal bilan uzatishning hojati yo‘qligini ta’minlovchi birinchi tizim bo‘lib, bugungi kunda ham bardoshli va qulay ochiq kalitli boshqa kriptotizimlarning asosini tashkil etadi.

U. Diffi va M.Ye. Xellmanning kalitlarni ochiq taqsimlash tizimi ochiq kalitli boshqa kriptotizimlar kabi maxfiy kalitni maxfiy kanal orqali uzatilishining hojati yo‘qligini ta’minlaydi, ammo autentifikasiya masalasini yechmaydi.

Maxfiy aloqa tizimida ochiq ma’lumotlar kitobini saqlovchi, maxfiy bo‘lmagan Y_i ni, ochiq ma’lumotlar kitobiga $i-$ foydalanuvchining faqat o‘zi tomonidangina kritilganiga ishonch hosil qilishi kerak, $i-$foydalanuvchi esa, o‘z navbatida, Y_j ni faqat ochiq ma’lumotlar kitobini saqlovchi tomonidan berilganiga ishonch hosil qilishi kerak. Ya’ni ochiq kalitlar to‘plami ham muhofaza qilinishi kerak. Chunki biror subyekt tomonidan noqonuniy (ruxsatsiz) ravishda ochiq kalitlar to‘plamiga o‘zining ochiq kalitini joylashtirishi uning uchun shu tizimga noqonuniy (ruxsatsiz) foydalanish imkoniyatiga ega bo‘lganligini ta’minlaydi. Shuning uchun ham sertifikatlangan kalitlar to‘plami umumfoydalanish axborot-kommunikasiya tizimida saqlanmaydi, u alohida faoliyat ko‘rsatuvchi kompyuter yoki nisbatan kichik sondagi kompyuterlar tizimida saqlanadi. Tizimning biror i-foydalanuvchisi biror j- foydalanuvchi

bilan muhofazalangan aloqa o‘rnatish uchun j- foydalanuvchining ochiq kalitiga ega bo‘lishi kerak. Buning uchun:

1) Umumfoydalanish tizimidagi barcha foydalanuvchilar komp’yuterlariga va ular bevosita bog‘langan bosh kompyuterga axborot muhofazasining kriptografik usullarining asosiy vositalari bo‘lgan shifrlash, xesh-funksiya va ERI algoritmlarining dasturiy ta’minotlari o‘rnatilgan bo‘lib, bosh kompyuter administratorining ochiq kaliti hamma foydalanuvchilarga ma’lum bo‘ladi.

2) i- foydalanuvchi bosh kompyuter administratoriga j- foydalanuvchi bilan aloqa o‘rnatmoqchi ekanligini M- ochiq matnni bosh kompyuter administratorining k_A^o - ochiq kaliti bilan shifrlagan holda $E_{k_A^o}(M)$ hamda administrator bu ma’lumotni va uning muallifining haqiqiyligiga ishonch hosil qilishi uchun, M- ma’lumot xesh-qiymatini $h(M)$ ushbu $E_{k_A^o}(M) \cup h(M)$ ko‘rinishda birlashtirib va hosil bo‘lgan kengaytirilgan $M' = E_{k_A^o}(M) \cup h(M)$ ma’lumotni o‘zi k_i^M – maxfiy kaliti bilan shifrlab, $E_{k_i^M}(M') = C$ (yoki $M' = [M \cup P(k_i^M, h(M))]$- kengaytirilgan ma’lumotni administratorning ochiq kaliti k_A^o bilan shifrlab, $E_{k_A^o}[M \cup P(k_i^M, h(M))]$=C) yuboradi.

3) Administrator $C = E_{k_i^M}(M')$-shifrlangan ma’lumotni k_i^o-kalit bilan ochadi: $D_{k_i^o}(C) = D_{k_i^o}(E_{k_i^M}(M')) = M' = E_{k_A^o}(M) \cup h(M)$. So‘ngra administrator o‘zining k_A^M-maxfiy kaliti bilan $D_{k_A^M}(E_{k_A^o}(M))$=M_1 – ochiq ma’lumotga ega bo‘ladi.

4) Bu olingan ochiq ma’lumot xeshlanadi $h(M_1)$ hamda $h(M_1) = h(M)$ tenglik tekshiriladi. Agar tenglik o‘rinli bo‘lsa, ma’lumot va uning muallifi haqiqiy, agar tenglik o‘rinli bo‘lmasa, ma’lumot va uning muallifi haqiqiy emas degan xulosa chiqariladi.

5) Agar administratorga C= $E_{k_A^o}[M \cup P(k_i^M, h(M))]$ - shifrma’lumot yuborilgan bo‘lsa, u o‘zining k_A^M-maxfiy kaliti bilan bu ma’lumotni deshifrlaydi:

$D_{k_A^M}(C) = D_{k_A^M}\{E_{k_A^o}[M \cup P(k_i^M, h(M))]\} = M \cup P(k_i^M, h(M))$. So‘ngra $P(k_i^M, h(M))$ -ERI to‘g‘riligini tekshiradi, agar to‘g‘ri bo‘lsa, ma’lumot va uning muallifi haqiqiy, aksincha bo‘lsa ma’lumot va uning muallifi haqiqiy emas deb xulosa chiqariladi.

6) Yuborilgan ma’lumot va uning muallifining (i-foydalanuvchining) haqiqiyligi o‘rnatilgandan so‘ng, administrator j-foydalanuvchining k_j^o -ochiq kalitini va u bilan bog‘liq bo‘lgan (masalan, amal qilish vaqti va shu kabi) boshqa M_j-ma’lumotlarni alohida faoliyat ko‘rsatuvchi komp’yuterdan olib, bosh komp’yuter orqali i- foydalanuvchining k_i^o -ochiq kaliti bilan shifrlab $E_{k_i^o}(M_j)=C_j$ hamda i-foydalanuvching bu ma’lumotni va uning muallifini haqiqiyligiga ishonch hosil qilishi uchun M_j-ma’lumotning xesh-qiymatini $h(M_j)$ ushbu $E_{k_i^o}(M_j)\cup h(M_j)$ ko‘rinishda birlashtirib va hosil bo‘lgan kengaytirilgan $M_j^{'}=E_{k_i^o}(M_j)\cup h(M_j)$-ma’lumotni o‘zining $k_A^м$ – maxfiy kaliti bilan shifrlab $E_{k_A^м}(M_j^{'})=C_j^{'}$ (yoki $M_j^{'}=[M_j\cup P(k_A^м,h(M_j))]$ -kengaytirilgan ma’lumotni i-foydalanuvchining ochiq kaliti k_i^o bilan shifrlab $E_{k_i^o}[M_j\cup P(k_A^м,h(M_j))]$=C$_j^{'}$) ochiq aloqa kanali orqali yuboradi.

7) i- foydalanuvchi $C_j^{'}=E_{k_A^м}(M_j^{'})$-shifrlangan ma’lumotni k_A^o-kalit bilan ochadi $D_{k_A^o}(C_j^{'})=D_{k_A^o}(E_{k_A^м}(M_j^{'}))=M_j^{'}=E_{k_i^o}(M_j)\cup h(M_j)$. So‘ngra i-foydalanuvchi o‘zining $k_i^м$- maxfiy kaliti bilan $D_{k_i^м}(E_{k_i^o}(M_j))=M1_j$ – ochiq ma’lumotga ega bo‘ladi.

8) Bu olingan ochiq ma’lumot xeshlanadi $h(M1_j)$ hamda $h(M1_j)=h(M_j)$ tenglik tekshiriladi. Agar tenglik o‘rinli bo‘lsa, ma’lumot va uning muallifi haqiqiy, agar tenglik o‘rinli bo‘lmasa, ma’lumot va uning muallifi haqiqiy emas degan xulosa chiqariladi.

9) Agar i- foydalanuvchiga $C_j=E_{k_ш^o}[M_j\cup P(k_A^м,h(M_j))]$ - shifrma’lumot yuborilgan bo‘lsa, u o‘zining $k_i^м$-maxfiy kaliti bilan bu ma’lumotni deshifrlaydi:
$D_{k_i^м}(C_j)=D_{k_i^м}\{E_{k_i^o}[M_j\cup P(k_A^м,h(M_j))]\}=M_j\cup P(k_A^м,h(M_j))$. So‘ngra $P(k_A^м,h(M_j))$ -ERI to‘g‘riligini tekshiradi, agar to‘g‘ri bo‘lsa, ma’lumot va uning muallifi haqiqiy, aksincha bo‘lsa, ma’lumot va uning muallifi haqiqiy emas deb xulosa chiqariladi.

Shunday qilib, i-foydalanuvchi j-foydalanuvchi bilan ochiq aloqa tarmog‘ida muhofazalangan axborot almashinuvini o‘rnatishi uchun j-foydalanuvchining k_i^o - sertifikatlangan ochiq kalitiga ega bo‘ldi. Ochiq kalitlar to‘plamining alohida komp’yuterda saqlanishi va ochiq kalitlarning 1) – 9) bosqich jarayonlarida tarqatilishi samarali

kriptografik muhofazani tashkil etish uslubini yoki protokolini belgilaydi. Haqiqatan ham bunday tashkiliy jarayon faqat shifrlash, xeshlash va ERI algoritmlaridan foydalangan holda kafolatli muhofazaning ta’minlashini tushunish qiyin emas.

5.7.4. Kriptotizim foydalanuvchilari uchun kalitlarni taqsimlash protokoli

Maxfiy yo‘lli bir tomonlama funksiyaga asoslangan ochiq kalitli kriptotizimlar o‘z mohiyatiga ko‘ra undan foydalanishning alohida protokolini talab etadi. Bu alohida tartib va qoidalarga ko‘ra, tizimning foydalanuvchilari va tizim foydalanuvchilarigagina ochiq bo‘lgan ochiq ma’lumotlar to‘plamining (kitobining) administratori (saqlovchisi) birgalikda shu tizimda uzatiladigan ma’lumotlarning maxfiyligini ta’minlaydilar.

Ochiq kalitli kriptotizimlarning bardoshliligiga to‘la ishonch bildirmay ishonchsizlik va ikkilanish bilan qaraydigan ba’zi kriptolog mutaxassislar, foydalanuvchilarga muhofazalangan uslubda ochiq kalitlarni taqsimlash va maxfiy kalitlarni uzatish masalalarini, ya’ni kalitlar bilan bog‘liq jarayonlarni maqsadli boshqarishni kriptografiyaning bosh amaliy masalasi, deb biladilar. Misol uchun, agarda kriptotizim foydalanuvchilarining soni S ta bo‘lsa va har bir mumkin bo‘lgan aloqa juftlari uchun alohida maxfiy kalit talab etilsa, ularning soni $c_s^2 = s(s-1)/2$ bo‘lib, foydalanuvchilar soni ko‘p bo‘lgan tizimlar uchun bunday holat ba’zida maqsadga muvofiq bo‘lmasligi mumkin. Biror foydalanuvchining boshqa barcha foydalanuvchilarga maxfiy bo‘lgan ma’lumotni yuborishi maxfiy aloqa mohiyatiga zid jarayon. Bundan tashqari maxfiy (muhofazalangan) aloqa tizimida qaysi foydalanuvchining boshqa qaysi bir foydalanuvchi bilan maxfiy aloqa qilishni xohlashi oldindan ma’lum emas. Mana shunday holatlar foydalanuvchilarga kalitlarni taqsimlash tartibi va qoidalari masalalarini keltirib chiqaradi. Bunday masalalarning yechilishi esa, axborot-kommunikasiya tizimida ma’lumotlarning maxfiyligi muhofazasini ta’minlovchi kriptotizimda kalitlarni ro‘yxatga olish markazi (KROM) tashkil etishni taqozo etadi. Kalitlarni taqsimlash protokoli quyidagicha:

1. KROM muhofazalangan aloqa tarmog‘i orqali barcha i=1,2,...,S foydalanuvchilarga maxfiy Z_i kalitlarni taqdim etadi.

2. Foydalanuvchi i foydalanuvchi j bilan maxfiy aloqa o‘rnatmoqchi bo‘lsa, u umumiy aloqa tarmog‘i orqali (ochiq matn bilan bo‘lishi mumkin) KROMga murojaat qilib, foydalanuvchi j bilan maxfiy aloqa qilish kalitini so‘raydi.

3. KROM maxfiy aloqa uchun ochiq matnning biror qismini tashkil etuvchi Z_{ij} maxfiy kalitni tanlab oladi. Qolgan qismini i va j foydalanuvchilar ko‘rsatilgan “bosh qism” (“zagolovok”) yoki “nomlanish qismi” deb ataluvchi bo‘lak tashkil etadi. KROM bu ochiq matnni kriptotizimda qabul qilingan shifrlash algoritmiga ko‘ra Z_i va Z_j kalitlar bilan shifrlab, umumiy aloqa tarmog‘i orkali Z_i kalit bilan shifrlangan kriptogrammani i foydalanuvchiga va Z_j kalit bilan shifrlangan kriptogrammani j foydalanuvchiga jo‘natadi.

4. Olingan kriptogrammalarni i va j foydalanuvchilar deshifrlab, keyingi olingan ma’lumotlarni deshifrlashning maxfiy kalitiga ega bo‘ladilar.

Kalitlarni taqsimlashning bunday protokoli oddiy bo‘lib, uning bardoshliligi shifrlash algoritmining bardoshliligi bilan belgilanadi. Haqiqatdan ham 3-bandda (qadamda) keltirilganidek, kriptotahlilchiga har xil kalitlar bilan shifrlangan bir xil ochiq matnning kriptogrammasi ma’lum bo‘lib, bunday holat unga kriptotahlil qilishda qo‘l keladi. Shunday qilib, ochiq matnni shifrlash algoritmi kriptotahlilga bardoshli bo‘lsa, kalitlarni taqsimlash protokoli ham bardoshli bo‘ladi. Bu yerda shuni ham unutmaslik kerakki, kalitlarni taqsimlashda shifrlash algoritmidan foydalanish shu taqsimlash protokolining buzilishiga, kriptobardoshsizlikka va shu kabi nomutanosibliklarga olib kelmasligi kerak.

Nazorat savollari

1. Oshkora kalitli kriptotizimlarning asosiy xususiyatlari nimalarda namoyon bo‘ladi?

2. Bir tomonlama funksiyalarga ta’rif bering?

3. Bir tomonlama funksiyalarning qanday turlarini bilasiz?

4. Oshkora kalitli kriptotizimlar simmetrik kriptotizimlardan farqli qanday masalalarni yechishga qodir?

5. Ochiq kalitli kriptotizimlar qanday murakkabliklarga asoslanadi?

6. Qanday kalitlar bardoshli kalitlar deyiladi?

7. Qanday kalitlar bardoshsiz hisoblanadi?

8. Tasodifiylikka tekshiruvchi qanday testlarni bilasiz?

9. Bir tomonlama funksiyalarga asoslangan psevdotasodifiy ketma-ketlik ishlab chiqaruvchi generatorlardan qaysilarini bilasiz?

10. Sonlar nazariyasi muammolariga asoslangan generatorlardan qaysilarini bilasiz?

11. Taqsimotni tasodifiylikka tekshirishning “Xi-kvadrat” mezonidan qanday foydalaniladi?

12. Simmetrik shifrlash algoritmlari uchun maxfiy kalitni tasodifiylikka tekshirish qanday amalga oshiriladi?

13. Kalitlar ochiq taqsimlanish algoritmining matematik asosi haqida nimalarni bilasiz?

14. Kriptotizim foydalanuvchilari uchun kalitlarni taqsimlash protokolini misollar yordamida tushuntirib bering?

15. Faktorlash murakkabligiga asoslangan nosimmetrik shifrlarni misollar bilan tushuntiring?

16. Chekli maydonlarda diskret logarifmlash masalasining yechimi murakkabligiga asoslangan nosimmetrik shifrlarga misollar keltiring?

17. Elliptik kriptografiyaning yuzaga kelishi haqida nimalarni bilasiz?

18. EECh gruppasida diskret logarifmlashga asoslangan kriptotizimlarni tushuntiring?

19. EECh nuqtalari gruppasi asosida yaratilgan nosimmetrik shifrlarning umumiy funksional modeli haqida nimalarni bilasiz?

20. Parametrli gruppadan foydalanishga asoslangan nosimmetrik shifrlarni misollar bilan tushuntiring?

21. Parametrli shifrlash usuli deb qanday usulga aytiladi?

22. Matrisaviy parametrli shifrlash usulini tushuntirib bering?

23. Elliptik egri chiziqlardan foydalanishga asoslangan parametrli shifrlash usuli haqida nimalarni bilasiz?

24. RSA shifriga analog parametrli shifrlash usulini tushuntirib bering?

6. AUTENTIFIKASIYA VA ELEKTRON RAQAMLI IMZO ALGORITMLARI

6.1. Autentifikasiya protokollari

Autentifikasiya protokoli autentifikasiya prosedurasi bo‘lib, unda bir-biri bilan o‘zaro muloqotga kirishayotgan ikki tomondan biri (yoki ikkalasi ham) boshqasining haqiqiyligini tekshiradi.

Autentifikasiyani uch turga ajratish mumkin: ma’lumotlar manbai autentifikasiyasi (data – origin authentication), mohiyat autentifikasiyasi (entity authentication) va autentifikasiyalangan kalitlarni generasiyalash (authenticationed key establishment). Autentifikasiyaning birinchi turi ma’lumotning e’lon etilgan xossasini tekshirishni bildiradi, ikkinchisi ko‘proq e’tiborni ma’lumot jo‘natuvchi haqidagi xabarlarning haqiqiyligiga qaratadi, uchinchisi esa maxfiy ma’lumotlar almashish uchun himoyalangan kanalni tashkil etish uchun mo‘ljallangan [50].

Ma’lumotlar manbai autentifikasiyasi

Ma’lumotlar manbai autentifikasiyasi (avvallari, ma’lumotlar autentifikasiyasi (message authentication) deb ham atalib kelingan) ma’lumotlar yaxlitligi bilan uzviy bog‘langan. Zero, ataylab o‘zgartirilgan axborotni qabul qilib olishdagi tavakkalchilik (xavfi) ishonchli bo‘lmagan manbadan axborot qabul qilish tavakkalchiligiga (xavfiga) yaqin. Ammo aslida ma’lumotlar manbai autentifikasiyasi va ma’lumotlarni yetishmasligidan himoyalash tushunchalari farqli tushunchalardir. Chunki ma’lumotlar manbai autentifikasiyasi albatta aloqa kanali bilan bog‘liq holda qaralib, manba identifikasiyasi (manbani uning identifikatori (nomi, simvollarning noyob satri) bo‘yicha aniqlash jarayoni) va ma’lumotlarning yangiligi bilan aloqador bo‘lsa, ma’lumotlar yaxlitligini himoyalashda aytilgan belgilar asosiy emas.

Ma’lumotlar manbai autentifikasiyasi quyidagi amallarni bajarishni nazarda tutadi [70].

1. Ma’lumot uni qabul etuvchiga shunday tarzda jo‘natiladiki, ma’lumotning haqiqiyligini uni qabul qilishdan avval tekshirib chiqishga imkoniyat bo‘lsin.

2. Ma’lumot jo‘natuvchisini identifikasiyalash.

3. Jo‘natuvchi yuborgan ma’lumotlarning yaxlitligini tekshirish.

4. Ma’lumot jo‘natuvchisining kimligini (realligini) tekshirish.

Mohiyat autentifikasiyasi

Mohiyat autentifikasiyasi axborot almashuv jarayoni, ya’ni protokoli bo‘lib, uning davomida foydalanuvchi boshqa foydalanuvchining haqiqiyligiga (lively correspondence) amin bo‘ladi.

Aslida autentifikasiya protokoli davomida ma’lumotning haqiqiyligi yoki haqiqiy emasligi ayon bo‘ladi. Bunday hollarda ma’lumot va uni muallifining haqiqiyligiga ishonch hosil qilish uchun ma’lumotlar manbai autentifikasiyasi mexanizmlaridan foydalanish lozim.

Tarmoqlangan tizimlarda quyidagi mohiyat autentifikasiyasi ssenariylari amal qiladi. Ulardan ikkitasiga to‘xtalamiz.

Ikkita bosh kompyuterlararo ma’lumotlar almashuv (host-host type).

Protokol ishtirokchilari kompyuterlar bo‘lib, ular tarmoqlangan tizimning tugunlari yoki platformalari deb yuritiladi. Kompyuterlar ishi o‘zaro moslashgan bo‘lishi zarur. Masalan, agar uzoqlashgan platformalardan biri “qayta yuklanmoqchi bo‘lsa” (takroriy inisializasiyalanish), u haqiqiy serverni identifikasiya qilishi lozim va unga kerakli axborotni jo‘natishi lozim, masalan, operasion tizimning haqiqiy nusxasini, taymerni yoki atrof-muhitni to‘g‘ri o‘rnatish. Axborot haqiqiyligini aniqlash odatda autentifikasiya protokoli yordamida amalga oshiriladi. Qoida tarzida, ikki bosh kompyuterlararo ma’lumotlar almashuv kliyent-server tizimi sifatida bo‘lib, biriga (kliyent) ikkinchisi (server) tomonidan xizmat ko‘rsatiladi.

Foydalanuvchi va bosh kompyuterlararo ma’lumotlar almashinuvi (user-host type). Foydalanuvchi bosh kompyuterda ro‘yxatdan o‘tib, kompyuter tizimiga kirishga ruxsat oladi. Odatda mijoz bosh kompyuterda tarmoqqa uzoqdan kirish (telnet) orqali ro‘yxatdan o‘tadi yoki o‘z faylini fayl uzatish protokoliga (ftp -file transfer protocol) muvofiq bosh kompyuterga jo‘natadi. Ikkala holda ham parolni autentifikasiyalash protokoli ishga tushadi. Ayrim hollarda, masalan, kredit kartochkalar bo‘yicha to‘lovlarda, o‘zaro autentifikasiyalash (mutual authentication) zarur bo‘ladi.

Subyekt o‘zining haqiqiyligini tasdiqlash uchun tizimga turli ma’lumotlarni taqdim etishi mumkin, masalan, parol, shaxsiy identifikasiya kodi, shaxsiy kalit bilan shifrlangan xabar, smart-karta, biometrik belgi, barmoq izi, so‘rovga javob, raqamli sertifikat va imzo va shunga o‘xshashlar [50].

Odatda axborot almashuvchi tomonlar muloqotni yanada yuqsakroq pog‘onaga ko‘tarish maqsadida mohiyat autentifikasiyasi protokolini ishga tushiradilar. Zamonaviy kriptografiyada himoyalangan aloqa kanallarini tashkil etishda kriptografik kalitlardan foydalaniladi. Binobarin, mohiyat autentifikasiyasi protokoli himoyalangan aloqa kanallari orqali axborot almashish uchun tarkibiy qism sifatida **autentifikasiyalangan kalitlarni generasiyalash** yoki **kalit almashish (**key exchange**)** yoki **kalitlarni muvofiqlashtirish** (key agreement) mexanizmlarini o‘z ichiga olishi lozim.

Autentifikasiyalangan kalitlarni generasiyalash protokolida protokol ma’lumotlari o‘zida kalitlar parametrlarini aks ettirgani bois, ularning manbaini ham autentifikasiyadan o‘tkazish lozim.

Adabiyotlarda autentifikasiyalangan kalitlarni generasiyalash protokoli, mohiyat autentifikasiyasi protokoli, ma’lumotlarni himoyalash protokoli, hattoki kriptografik protokollar ham ko‘pincha aloqa protokollari deb nomlanadi.

Autentifikasiya protokollari quyidagi turlarga bo‘linadi:

1. Parollar va raqamli sertifikatlardan foydalanishga asoslangan autentifikasiya protokollari.

2. Kriptografik usullar va vositalarga asoslangan qatiy autentifikasiya protokollari.

3. Yo‘q (nollik) bilim bilan isbotlanadigan autentifikasiya protokollari.

4. Biometrik autentifikasiya protokollari.

Quyida qatiy autentifikasiya protokollaridan biri sifatida sertifikat va elektron raqamli imzodan foydalanishga asoslangan autentifikasiya protokoli bayon etilgan [70].

Xalqaro X.509 standarti ERI, vaqt belgisi va tasodifiy sonlardan foydalanib, quyidagi bir tomonlama autentifikasiyalash protokollarini tavsiya etadi.

Foydalanuvchi B tomonidan foydalanuvchi A ni bir tomonlama autentifikasiyalash.

1. Foydalanuvchi *A* o‘z shaxsiy kaliti bilan shifrmatn $S_A(t_A, B)$ ni shakllantiradi va uni o‘z ichiga olgan quyidagi xabarni foydalanuvchi *B* manziliga jo‘natadi:

$$A \rightarrow B: cert_A, t_A, B, S_A(t_A, B),$$

bu yerda $\rightarrow$ - jo‘natma yo‘nalishi belgisi, $cert_A$ - foydalanuvchi *A* ning sertifikati, *B* - foydalanuvchining identifikatori, t_A - vaqt belgisi.

Foydalanuvchi *B* xabar $(cert_A', t_A', B', S_A'(t_A, B))$ ni olgandan so‘ng $cert_A'$ dagi oshkora kalitdan foydalanib shifrmatn $S_A'(t_A, B)$ ni t_A, *B* ga aylantiradi va ularni xabardagi vaqt belgisi t_A', o‘zining identifikatori *B’* bilan taqqoslaydi. Agar taqqoslanuvchi qiymatlar teng bo‘lmasa, unda *A* haqiqiy emas, aks holda haqiqiy degan xulosa chiqariladi va keyingi qadamga o‘tiladi.

2. Foydalanuvchi *B* r_B ni generasiyalab *A* ga jo‘natadi:

$$B \rightarrow A: r_B.$$

Foydalanuvchi *A* r_B ni qabul qilib o‘ziga tegishli tasodifiy son r_A ni generasiyalaydi va shifrmatn $S_A(r_A, r_B, B)$ ni o‘z ichiga olgan quyidagi xabarni foydalanuvchi *B* ga jo‘natadi:

$$A \rightarrow B: cert_A, r_A, B, S_A(r_A, r_B, B),$$

bu yerda, r_A, r_B mos tarzda *A* va *B* generasiyalagan tasodifiy sonlar.

Foydalanuvchi *B* xabar $(cert_A', r_A', B', S_A'(r_A, r_B, B))$ ni olgandan so‘ng $cert_A'$ dagi oshkora kalitdan foydalanib shifrmatn $S_A'(r_A, r_B, B)$ ni r_A, r_B, *B* ga aylantiradi va ularni xabardagi r_A', o‘zi jo‘natgan r_B va o‘zining identifikatori *B’* bilan taqqoslaydi. Agar taqqoslanuvchi qiymatlar teng bo‘lmasa, unda *A* haqiqiy emas, aks holda haqiqiy degan xulosa chiqariladi.

Foydalanuvchilar A va B tomonidan ikki tomonlama autentifikasiyalash quyidagi jo‘natmalar ketma-ketligidan iborat :

$$B \rightarrow A: r_B.$$

$$A \rightarrow B: cert_A, r_A, B, S_A(r_A, r_B, B),$$

$$B \rightarrow A: cert_B, A, S_B(r_A, r_B, A),$$

Prosedura tasodifiy sonlarni generasiyalash va ularni tomonlarga tegishli identifikatorlar bilan birgalikda shaxsiy kalit bilan shifrlash va shifrmatnlarni oshkora kalit bilan ochish va natijalarni taqqoslash amallarini bajarish natijasida tomonlarning haqiqiy yoki aksinchaligi haqida xulosa chiqarishni nazarda tutadi.

6.2. Elektron raqamli imzo

Elektron raqamli imzo axborot-kommunikasiya tarmog‘ida almashinadigan hujjatli ma’lumotlar va ularning manbalarini haqiqiy yoki haqiqiy emasligini aniqlash masalasini, ya’ni ma’lumotlar autentifikasiyasi masalasining yechimini ta’minlovchi kriptografik vosita hisoblanadi.

Har qanday qog‘ozli yozma xat yoki hujjatning oxirida shu hujjatni tuzuvchisi yoki tuzish uchun javobgar bo‘lgan shaxsning imzosi bo‘lishi tabiiy holdir. Imzo quyidagi ikkita maqsaddan kelib chiqib qo‘yiladi. Birinchidan, ma’lumotni olgan tomon o‘zida mavjud imzo namunasiga olingan ma’lumotdagi imzoni solishtirib, imzoning haqiqiy yoki soxtaligiga ko‘ra shu ma’lumotning haqiqiy yoki soxta ekanligini aniqlaydi. Ikkinchidan, shaxsiy imzo ma’lumot hujjatining yuridik maqomini ta’minlaydi. Bunday kafolat esa savdo–sotiq, ishonchnoma, majburiyat va shu kabi bitimlarda alohida muhimdir.

Qog‘ozli hujjatlarga qo‘yilgan shaxsiy imzolarni soxtalashtirish nisbatan murakkab. Chunki shaxsiy imzo faqat uning muallifi tafakkurining o‘ziga xos bo‘lgan ko‘pqirrali tomonlari mahsulidir. Shuning uchun bunday imzo muallifini hozirgi zamonaviy ilg‘or kriminalistika uslublaridan foydalanish orqali aniqlash mumkin.

Axborot-kommunikasiya tarmog‘ida almashinadigan elektron hujjatli ma’lumotlar ham qog‘ozli hujjat almashinuvidagi an’anaviy shaxsiy imzo vazifasini bajaruvchi kabi elektron raqamli imzo bilan ta’minlanib, elektron hujjat va uning manbasini haqiqiy yoki haqiqiy emasligini aniqlash masalasi yechimini hal etilishini talab etadi.

6.2.1. Elektron raqamli imzo algoritmlarining umumiy kriptografik xossalari

Elektron raqamli imzo qog‘ozli hujjat almashinuvidagi an’anaviy shaxsiy imzo xususiyatlaridan farqli bo‘lib, ikkilik sanoq tizimi xususiyatlari bilan belgilanadigan xotira registrlari bitlariga bog‘liq. Xotira bitlarining ma’lum bir ketma-ketligidan iborat bo‘lgan elektron imzoni ko‘chirib biror joyga qo‘yish yoki o‘zgartirish kompyuterlar asosidagi aloqa tizimlarida murakkablik tug‘dirmaydi.

Bugungi yuqori darajada rivojlangan butun dunyo sivilizasiyasida hujjatlar, jumladan maxfiy hujjatlarning ham, elektron koʻrinishda ishlatilishi va aloqa tizimlarida uzatilishi keng qoʻllanilib borilayotganligi elektron hujjatlar va elektron imzolarning haqiqiyligini aniqlash masalalari yechimlarining muhimligini keltirib chiqarmoqda.

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

- foydalanuvchi (B) tomonidan qabul qilib olingan elektron hujjatga qoʻyilgan raqamli imzoning haqiqiy yoki haqiqiy emasligini faqat (A) - foydalanuvchining ochiq kaliti bilan ta'minlangan shaxsiy kalit faqat oʻzidan boshqa shaxsga ma'lum boʻlmasligi, ma'lumotni faqat (A) - foydalanuvchi tomonidan joʻnatilganligini rad etib boʻlmaydi;

- qonunbuzar (raqib tomon) shaxsiy kalitni bilmagan holda modifikasiyalash, soxtalashtirish, faol modifikasiyalash, niqoblash va boshqa shu kabi aloqa tizimi qoidalarining buzilishiga imkoniyat tugʻdirmaydi;

- aloqa tizimidan foydalanuvchilarning oʻzaro bogʻliq holda ish yuritishi munosabatidagi koʻplab kelishmovchiliklarni bartaraf etadi va bunday kelishmovchiliklar kelib chiqqanda vositachisiz aniqlik kiritish imkoniyati tugʻiladi.

Koʻp hollarda uzatilayotgan ma'lumotlarni shifrlashga hojat boʻlmay, uni elektron raqamli imzo bilan tasdiqlash kerak boʻladi. Bunday holatlarda ochiq matn joʻnatuvchining yopiq kaliti bilan shifrlanib, olingan shifrmatn ochiq matn bilan birga joʻnatiladi. Ma'lumotni qabul qilib olgan tomon joʻnatuvchining ochiq kaliti yordamida shifrmatnni deshifrlab, ochiq matn bilan solishtirishi mumkin.

1991 yilda AQShdagi Standartlar va Texnologiyalar Milliy Instituti DSA raqamli imzo algoritmining standartini DSS yuqorida keltirilgan El Gamal va RSA algoritmlari asosida yaratib, foydalanuvchilarga taklif etgan.

ERI axborot-kommunikasiya tarmogʻida elektron hujjat almashinuvi jarayonida quyidagi uchta masalani yechish imkonini beradi:

- elektron hujjat manbasining haqiqiyligini aniqlash;

- elektron hujjat yaxlitligini (o‘zgarmaganligini) tekshirish;

- elektron hujjatga raqamli imzo qo‘ygan subyektni mualliflikdan bosh tortmasligini ta’minlash.

Har qanday ERI algoritmi ikkita qismdan iborat bo‘ladi:

– imzo qo‘yish;

– imzoni tekshirish.

Imzo qo‘yish muallif tomonidan, faqat unga ma’lum bo‘lgan shaxsiy kalit bilan amalga oshiriladi. Imzoning haqiqiyligini tekshirish esa istalgan shaxs tomonidan, imzo muallifining ochiq kaliti bilan amalga oshirilishi mumkin.

Elektron kommunikasiyalar va elektron hujjat almashinuvi hozirgi kunda ish yuzasidan bo‘ladigan munosabatlarning ajralmas qismi hisoblanib, har qanday zamonaviy tashkilotni elektron hujjatlar almashinuvi va Internetsiz tasavvur qilish qiyin.

Internet tarmog‘idan elektron hujjatlar almashinuvi asosida moliyaviy faoliyat olib borishda ma’lumotlar almashinuvini himoya qilish va elektron hujjatning yuridik maqomini ta’minlash birinchi darajali ahamiyat kasb etadi.

Elektron hujjatli ma’lumot almashinuvi jarayonida ERIni qo‘llash har xil turdagi to‘lov tizimlari (plastik kartochkalar), bank tizimlari va savdo sohalarining moliyaviy faoliyatini boshqarishda elektron hujjat almashinuvi tizimlarining rivojlanib borishi bilan keng tarqala boshladi.

Hozirda ERI tizimini yaratishning bir nechta yo‘nalishlari mavjud. Bu yo‘nalishlarni uchta guruhga bo‘lish mumkin:

1) ochiq kalitli shifrlash algoritmlariga asoslangan;

2) simmetrik shifrlash algoritmlariga asoslangan;

3) imzoni hisoblash va uni tekshirishning maxsus algoritmlariga asoslangan raqamli imzo tizimlaridir.

Ochiq kalitli shifrlash algoritmlariga asoslangan ERI tizimlari quyidagicha tashkil qilinadi. Agar axborot-kommunikasiya tarmog‘ining i- foydalanuvchisi j- foydalanuvchisiga imzolangan elektron hujjat jo‘natmoqchi bo‘lsa, i-foydalanuvchi o‘zining maxfiy kaliti k_i^M bilan imzolanishi kerak bo‘lgan hujjatning o‘zini shifrlab yoki uning xesh qiymatini shifrlab, shu hujjat bilan birgalikda jo‘natadi. Bu elektron hujjatni qabul qilib olgan j- foydalanuvchi, shifrlangan ma’lumotni i- foydalanuvchining ochiq kaliti k_i^o bilan

deshifrlab, hosil bo‘lgan matnni hujjat matniga yoki uning xesh qiymatiga solishtiradi. Agar matnlar bilan xesh qiymatlar bir xil bo‘lsa, imzo haqiqiy, aks holda haqiqiy emas deb qabul qilinadi.

Simmetrik shifrlash algoritmlariga asoslangan ERI tizimlari quyidagicha tashkil etiladi. i- foydalanuvchi bir vaqtning o‘zida i-foydalanuvchiga ham, j- foydalanuvchiga ham ma’lum bo‘lib, boshqa foydalanuvchilarga ma’lum bo‘lmagan $k_{ij}^{м}$- kalit bilan imzolanishi kerak bo‘lgan elektron hujjatni yoki uning xesh qiymatini shifrlab, shu hujjat bilan birgalikda jo‘natadi. Elektron hujjatni qabul qilib olgan j-foydalanuvchi, shifrlangan ma’lumotni $k_{ij}^{м}$- kalit bilan deshifrlab, hosil bo‘lgan matnni hujjat matniga yoki uning xesh qiymatiga solishtiradi. Agar matnlar bilan xesh qiymatlar bir xil bo‘lsa, imzo haqiqiy, aks holda haqiqiy emas deb qabul qilinadi. Bunday ERI tizimi bir martalik hisoblanadi, chunki $k_{ij}^{м}$ - kalitdan ikkinchi marta foydalanish imkoniyati elektron hujjatlarni soxtalashtirish imkoniyatini yaratadi. Bunday holatga chek qo‘yish uchun elektron hujjat almashinuvi ishonchli uchinchi tomon orqali amalga oshirilishi mumkin: i-foydalanuvchi o‘ziga va faqat ishonchli uchinchi tomonga ma’lum bo‘lgan kalit $k_{i3}^{м}$ bilan raqamli imzoni amalga oshirib, imzolangan elektron hujjatni uchinchi ishonchli tomonga jo‘natadi, uchinchi tomon imzoning haqiqiyligini $k_{i3}^{м}$ - kalit bilan tekshirib, agar haqiqiy bo‘lsa, j- foydalanuvchining o‘ziga va faqat ishonchli uchinchi tomonga ma’lum bo‘lgan kalit $k_{j3}^{м}$ bilan raqamli imzoni amalga oshirib, imzolangan elektron hujjatni j- foydalanuvchiga jo‘natadi. Bunday ERI tizimi foydalanuvchilar uchun noqulay bo‘lib, ko‘plab kelishmovchiliklarni keltirib chiqaradi.

Amalda uchinchi turdagi imzoni hisoblash va uni tekshirishning maxsus algoritmlariga asoslangan ERI tizimlaridan keng foydalaniladi.

Maxsus ERI algoritmlari raqamli imzoni hisoblash va imzoni tekshirish qismlaridan iborat. ERIni hisoblash qismi imzo qo‘yuvchining maxfiy kaliti va imzolanishi kerak bo‘lgan hujjatning xesh qiymatiga bog‘liq bo‘ladi. Imzoni tekshirish qismi imzo egasining ochiq kalitiga va qabul qilib olingan hujjatning xesh qiymatiga bog‘liq holda amalga oshiriladi.

Maxsus ERI standartlari turkumiga:

1. Rossiya ERI standarti: GOST R 34.10-94 va uning elliptik egri chiziqda takomillashtirilgan varianti GOST R 34.10-2001;

2. Amerika ERI standarti: DSA va uning elliptik egri chiziqda takomillashtirilgan varianti ECDSA -2000;

3. O‘zbekiston Respublikasi standarti: O‘z DSt 1092:2005; O‘z DSt 1092:2009;

4. Germaniya standarti EC-GDSA [66, 71];

5. Koreya standarti EC-KCDSA [66, 71] algoritmlari misol bo‘la oladi.

Elektron raqamli imzo bitlar ketma-ketligida ifodalangan biror sondan iborat. Shuning uchun uni boshqa elektron hujjatlarga ko‘chirish yoki o‘zgartirish kiritish katta qiyinchilik tug‘dirmaydi. Shu sababli elektron hujjat almashinuvi tizimida ERIni soxtalashtirishning oldini olish chora-tadbirlari – ERI algoritmining elektron hujjatlarni soxtalashtirishga bardoshliligi masalasini yechish talab etiladi.

ERI algoritmining bardoshliligi quyidagi uchta masalaning murakkabligi bilan aniqlanadi:

- *imzoni soxtalashtirish*, berilgan hujjatga, maxfiy kalitga ega bo‘lmagan holda to‘g‘ri imzo hisoblash;

- *imzolangan ma’lumotni tashkil etish*, maxfiy kalitga ega bo‘lmagan holda to‘g‘ri imzolangan ma’lumotni topish;

- *ma’lumotni almashtirish*, bir xil imzoga ega bo‘lgan ikkita har xil ma’lumotni topish.

Keltirilgan ERI algoritmlari standartlari bardoshliliklari diskret logarifmlash, EEChrasional nuqtalari ustida amallar bajarish va parametrli gruppa parametrini topish masalalarining murakkabligiga asoslangan.

6.2.2. Ochiq kalitli shifrlash algoritmlariga asoslangan elektron raqamli imzo algoritmlari qo‘llanilishining umumiy matematik modeli

Axbort-kommunikasiya tarmog‘ining maxfiy elektron hujjat almashish tizimi nosimmetrik shifrlash algoritmidan iborat bo‘lganda ERIni ochiq kalitli shifrlash algoritmi asosida amalga oshirish misol tariqasida ko‘rib o‘tiladi.

Kriptotizimning i- foydalanuvchisi M- maxfiy ma'lumotni j- foydalanuvchiga imzo qo'ygan holda jo'natmoqchi bo'lsa, u holda i- foydalanuvchi quydagilarni amalga oshirishi kerak:

1. Ma'lumot M tizim foydalanuvchilarining barchasiga ma'lum bo'lgan xesh-funksiya $h: X \to Y$ (bu yerda X- ochiq matnlar to'plami, Y- xeshlash natijasida hosil bo'lgan qiymat) bilan qayd qilingan bit uzunligidagi ifodaga siqiladi.

2. Ma'lumotning xesh qiymati $h(M) = H$ faqat i- foydalanuvchining o'ziga ma'lum bo'lgan maxfiy kalitga $k_i^м$ bog'liq bo'lgan bir tomonlama funksiya E orqali shifrlanadi, ya'ni $E_{k_i^м}(h(M)) = S$.

3. So'ngra j- foydalanuvchining ochiq kaliti k_j^o bilan ma'lumot M va S birlashtirilgan kengaytirilgan ma'lumot shifrlanadi, ya'ni $E_{k_j^o}(M \cup S) = E_{k_j^o}(M) \cup E_{k_j^o}(S) = E_{k_j^o}(M) \cup E_{k_j^o}\left(E_{k_i^м}(h(M))\right) = C_1 \cup C_2 = C$.

4. Shifrlangan ma'lumot C ochiq aloqa tarmog'i orqali j- foydalanuvchiga jo'natiladi.

Shifrlangan ma'lumotni olgan j- foydalanuvchi, faqat uning o'ziga ma'lum bo'lgan maxfiy kalit $k_j^м$ bilan deshifrlashni amalga oshiradi, ya'ni

$$D_{k_j^з}(C) = D_{k_j^з}(C_1 \cup C_2) = D_{k_j^з}(C_1) \cup D_{k_j^з}(C_2) = D_{k_j^з}\left(E_{k_j^o}(M)\right) \cup D_{k_j^з}\left(E_{k_j^o}\left(E_{k_i^з}(h(M))\right)\right) =$$
$$= M \cup E_{k_i^з}(h(M)),$$

bu yerda ERI ifodasi $E_{k_i^м}(h(M))$ hali deshifrlanmagan.

5. Ma'lumot egasini va ma'lumotning o'zini haqiqiyligiga ishoch hosil qilish uchun j- foydalanuvchi i- foydalanuvchining ochiq kaliti k_i^o bilan ERI qismini $E_{k_i^м}(h(M))$ deshifrlab $h(M)$- ifodani oladi, ya'ni

$$D_{k_i^o}\left(E_{k_i^м}(h(M))\right) = h(M).$$

6. So'ngra j- foydalanuvchi deshifrlash natijasida olgan $D_{k_j^м}(C_1)$ ochiq ma'lumotni kalitsiz xesh funsiya bilan xeshlaydi $h\left(D_{k_j^з}(C_1)\right)$ va ushbu $D_{k_i^o}\left(E_{k_i^м}(h(M))\right) = h(M)$ taqqoslash bilan imzoning to'g'riligiga ishonch hosil qilishi mumkin, agarda $h\left(D_{k_j^м}(C_1)\right) = D_{k_i^o}\left(E_{k_i^з}(h(M))\right) = h(M)$ bo'lsa, aks holda imzo noto'g'ri hamda elektron hujjat haqiqiy bo'lmaydi.

ERI imzoning to‘g‘riligi ma’lumotning o‘zini, uning muallifini va manbasining haqiqiyligini kafolatlaydi.

Ta’kidlash joizki, 1-6-bandlar nosimmetrik kriptotizimlarda ma’lumot almashinuvchi tomonlarning ERI protokolini ifodalaydi. Kriptografik protokol deb, ikki va undan ortiq tomonlar qatnashgan holda maxfiy ma’lumot almashinuvi jarayonida tomonlarning o‘z vazifalarini bajarishi ketma-ketligi tushuniladi.

Quyida ochiq kalitli shifrlash algoritmlariga asoslangan ERI algoritmlari ko‘rib o‘tiladi.

6.2.3. RSA ochiq kalitli shifrlash algoritmi asosidagi elektron raqamli imzo

Tizimning har bir i- foydalanuvchisi (e_i, d_i)- kalitlar juftligini yaratadi. Buning uchun yetarli katta bo‘lgan p va q-tub sonlari olinib (bu sonlar maxfiy tutiladi), $n = pq$-soni va Eyler funksiyasining qiymati $\varphi(n)=(p-1)(q-1)$ hisoblanadi (bu son ham maxfiy tutiladi). So‘ngra $(e_i, \varphi(n)) = 1$ shartni qanoatlantiruvchi, ya’ni $\varphi(n)$- soni bilan o‘zaro tub bo‘lgan e_i -son bo‘yicha d_i-soni ushbu $e_i d_i = 1 \bmod \varphi(n)$ formula orqali hisoblanadi. Bu (e_i ; d_i) –juftlikda e_i - ochiq kalit va d_i- maxfiy (shaxsiy) kalit deb e’lon qilinadi.

Shundan so‘ng i-foydalanuvchidan j-foydalanuvchiga shifrlangan ma’lumotni imzolagan holda jo‘natishi quyidagicha amalga oshiriladi:

1. Shifrlash qoidasi: $M^{e_j} \bmod n = C$, bu yerda M-ochiq ma’lumot, *S* – shifrlangan ma’lumot;

2. Deshifrlash qoidasi: $C^{d_j} \bmod n = M^{e_j d_j} \bmod n = M$;

3. ERIni hisoblash: $H(M)^{d_i} \bmod n = P_i$,

bu yerda i-foydalanuvchining P_i-imzosi M-ma’lumotning $H(M)$- xesh funksiya qiymati bo‘yicha hisoblangan;

4. ERIni tekshirish: $(P_i)^{e_i} \bmod n = H(M)^{e_i d_i} \bmod n = H(M)$, agar $H(M) = H(M_1)$ bo‘lsa (bu yerda M_1 -deshifrlangan ma’lumot), u holda elektron hujjat haqiqiy, aks holda haqiqiy emas, chunki xesh funksiya xossasiga ko‘ra $M = M_1$ bo‘lsa, ularning xesh qiymatlari ham teng bo‘ladi.

5. Ma’lumotni maxfiy uzatish protokoli:

$\left[M \cup H(M)^{d_i}\right]^{e_j} \bmod n = \left[M \cup P_i\right]^{e_j} \bmod n = C$;

6. Maxfiy uzatilgan ma’lumotni qabul qilish protokoli:

$C^{d_j} \bmod n = \left[M \cup P_i\right]^{e_j d_j} \bmod n = M \cup P_i$, umuman qaraganda dastlabki ma’lumot o‘zgartirilgan bo‘lishi mumkin, shuning uchun $C^{d_j} \bmod n = M_1 \cup P_i$ bo‘lib, natijada xesh qiymat imzo bo‘yicha ushbu ifoda $(P_i)^{e_i} \bmod n = H(M)^{e_i d_i} \bmod n = H(M)$ bilan hisoblanadi va qabul qilib olingan ma’lumotning xesh qiymati $H(M_1)$ bo‘lsa, u holda $H(M) = H(M_1)$ bo‘lganda elektron hujjat haqiqiy, aksincha bo‘lsa, soxta hisoblanadi.

6.2.4 El Gamal ochiq kalitli shifrlash algoritmi asosidagi elektron raqamli imzo

El Gamal ochiq kalitli shifrlash algoritmiga asoslangan kriptotizimning har bir i- foydalanuvchisi uchun ochiq va maxfiy kalitlar generasiyasi quyidagicha amalga oshiriladi, ochiq e’lon qilinadigan p_i- tub son (yoki foydalanuvchilar guruhi uchun umumiy bo‘lgan p-tub son) tanlanadi, ushbu $g_i < p_i$ (yoki foydalanuvchilar guruhi uchun $g < p$) shartni qanoatlantiruvchi g_i (yoki foydalanuvchilar guruhi uchun g) soni tanlanadi, ushbu $y_i = g^{x_i} \bmod p_i$ (p-umumiy bo‘lganda $y_i = g^{x_i} \bmod p$, $x_i < p$) formula bilan x_i - maxfiy kalit bo‘yicha y_i soni hisoblanadi. Shunday qilib, (p_i, g_i, y_i)-parametrlar birikmasi (umumiy p va g uchun (p, g, y_i)- parametrlar birikmasi ochiq kalitni tashkil etadi, maxfiy kalit x_i hisoblanadi.

Tizimda i-foydalanuvchidan j-foydalanuvchiga shifrlangan ma’lumotning imzolangan holda jo‘natilishi quyidagicha amalga oshiriladi:

1. **Shifrlash qoidasi**: $a_j = g_j^k \bmod p_j$, $b_j = y_j^k M \bmod p_j$ (umumiy p va g lar uchun $a = g^k \bmod p$, $b_j = y_j^k M \bmod p$), bu yerda k-tasodifiy son bo‘lib ma’lumotni imzolovchi tomonidan tanlanadi, bu son $(p_j - 1)$ soni bilan o‘zaro tub EKUB$(k, p_j - 1) = 1$ (p va g umumiy bo‘lganda EKUB(k, $p-1$) =1), M-ochiq ma’lumot, shifrlangan ma’lumot $(a_j, b_j) = C$ (p va g umumiy bo‘lganda, $(a, b_j) = C$).

2. **Deshifrlash qoidasi**: $b_j \big/ a_j^{x_j} \bmod p_j = M$ (p va g umumiy bo‘lganda $b \big/ a^{x_j} \bmod p = M$), haqiqatan ham $b_j \big/ a_j^{x_j} \bmod p_j \equiv g_j^{x_i k} M \big/ g_j^{k x_i} \bmod p_j \equiv M$ (p va g umumiy bo‘lganda $b \big/ a^{x_j} \bmod p \equiv y_j^k M \big/ a^{x_j} \bmod p \equiv g^{x_j k} M \big/ g^{k x_j} \bmod p = M \bmod p = M$, $M < p$);

3. ERIni hisoblash qoidasi: $a_i = g_i^{\,k} \bmod p_i$, b_i soni esa $M = (x_i a_i + k b_i) \bmod (p_i - 1)$ yoki $H(M) = (x_i a_i + k b_i) \bmod (p_i - 1)$ tenglamadan topiladi, ya’ni $b_i = (M - a_i x_i) k^{-1} \bmod (p_i - 1)$ yoki $b_i = (H(M) - a_i x_i) k^{-1} \bmod (p_i - 1)$ (p va g umumiy bo‘lganda $a = g^k \bmod p$, b soni esa $M = (x_i a + k b) \bmod (p - 1)$ yoki $H(M) = (xa + kb) \bmod (p - 1)$ tenglamadan topiladi, ya’ni $b = (M - a x_i) k^{-1} \bmod (p - 1)$ yoki $b = (H(M) - a x_i) k^{-1} \bmod (p - 1)$, $\text{EKUB}(k, p-1) = 1$) $H(M)$-ma’lumotning xesh qiymati, x_i-maxfiy kalit, imzo sifatida a_i va b_i juftlik, ya’ni $(a_i, b_i) = P_i$, (p va g umumiy bo‘lganda (a, b)) imzo deb qabul qilinadi.

4. Imzoni tekshirish qoidasi:

Agar $y_i^{a_i} a_i^{b_i} \bmod p_i = g_i^M \bmod p_i$ yoki $y_i^{a_i} a_i^{b_i} \bmod p_i = g_i^{H(M)} \bmod p_i$ bo‘lsa, u holda elektron hujjat haqiqiy, aks holda soxta hisoblanadi. Chunki

$y_i = g_i^{x_i} \bmod p_i$ va $a_i = g_i^{\,k} \bmod p_i$

tengliklar o‘rinli bo‘lib, Ferma teoremasiga ko‘ra ushbu ayniyat o‘rinli:

$$y_i^{a_i} a_i^{b_i} \bmod p_i = (g_i^{x_i})^{a_i} (g_i^{\,k})^{b_i} \bmod p_i = g_i^{a_i x_i + k b_i} \bmod p_i = g_i^{d(p_i - 1) + M} \bmod p_i =$$
$$= g_i^{d(p_i - 1)} g_i^M \bmod p_i = (g_i^{(p_i - 1)})^d \bmod p_i \cdot g_i^M \bmod p_i (\bmod p_i) =$$
$$= 1^d \bmod p_i \cdot g_i^M \bmod p_i (\bmod p_i) = g_i^M \bmod p_i;$$

5. **Ma’lumotni maxfiy uzatish protokoli**:

$a_j = g_j^k \bmod p_j$, $b_j = y_j^k M' \bmod p_j = y_j^{\,k} [M \cup P_i] \bmod p_j$,

$(a_j, b_j) = C$ - shifrma’lumot;

5. **Maxfiy uzatilgan ma’lumotni qabul qilish protokoli:**

$$b_j \big/ a_j^{x_j} \bmod p_j = M' = M \cup P_i,$$

umuman qaraganda, dastlabki ma’lumot o‘zgartirilgan bo‘lishi mumkin, shuning uchun

$$b_j \big/ a_j^{x_j} \bmod p_j = M' = M_1 \cup P_i,$$

bo‘lib, $H(M_1)$ - xesh qiymat hisoblanadi. Agar $y_i^{a_i} a_i^{b_i} \bmod p_i = g_i^{M_1} \bmod p_i$ yoki $y_i^{a_i} a_i^{b_i} \bmod p_i = g_i^{H(M_1)} \bmod p_i$ bo‘lsa, u holda elektron hujjat haqiqiy, aks holda soxta hisoblanadi.

Ochiq kalitli shifrlash algoritmlari bitta (bir xil) elektron hujjatga har xil ERIni qo‘yish imkoniyatini bermaydi. Bunday holat esa bitta elektron hujjatni har xil tomonlarga bitta imzolovchi tomonidan har xil ERI bilan yuborilish zarurati masalasi yechimini ta’minlamaydi va kriptotahlilchiga kriptohujumni muvaffaqiyatli amalga oshirish imkoniyatini beradi. Bu masalaning yechimini ta’minlash yo‘nalishida olib borilgan ilmiy-tadqiqot ishlari maxsus ERI algoritmlarining ishlab chiqilishi bilan amalga oshirildi.

6.2.5. Maxsus elektron raqamli imzo algoritmlarining matematik modellari

Imzoni hisoblash va uni tekshirishga asoslangan maxsus ERI algoritmlari turkumidagi DSA va GOST R 34.10-94 standart algoritmlarining asosini El Gamal shifrlash algoritmi tashkil etadi, ya’ni bu algoritmlar bardoshliligi diskret logarifmlash masalasi yechimining matematik murakkabligi bilan ta’minlangan.

EECh gruppasida tuzilgan ERI sxemalarining [56-68] tahlili shuni ko‘rsatadiki, avvalgi sxemalarni (aslida, El Gamal sxemalari modifikasiyalarini) yangilari bilan almashtirish ikki xil algebraik struktura – EECh nuqtalarining chekli additiv gruppasi va chekli maydon *F(q)* asosida amalga oshirilgan, bu yerda *q* – hosil qiluvchi (generator) nuqta *G* asosida yuzaga kelgan gruppaning tartibi. Bunda maydonning chekli multiplikativ gruppasi elementlari ustida darajaga oshirish algebraik amali EECh nuqtalari chekli additiv gruppasi elementlari ustida ko‘p marta qo‘shish (skalyar songa ko‘paytirish) amali bilan almashtirilgan. ERI sxemalarida chekli maydon elementlari ustida bajariladigan amallar o‘zgarmagan.

Shunday qilib EECh gruppasida ERI algoritmini shakllantirish uchun quyidagi almashtirishlarni amalga oshirish kifoya:

- chekli maydon generator elementi *g* ni EEChning generator elementi (nuqtasi) *G* bilan;
- *g* element tartibi *q* ni *G* nuqta tartibi *q* bilan;
- shaxsiy kalit *d* ni shaxsiy kalit *d* bilan;

- oshkora kalit $y=g^d \ (mod\ p)$ni oshkora kalit $Y = [d]G$.

EECh gruppasida har qanday kriptografik algoritmni tuzish tizim parametrlarini spesifikasiyalashdan boshlanib, kriptografik algoritmni tuzish va uni sinab koʻrish bilan yakunlanadi.

6.2.6. Oʻzbekiston Respublikasining elektron raqamli imzo boʻyicha davlat standarti

Yuqorida keltirilgan ERI algoritmlarining asosiy kamchiliklaridan biri, buzgʻunchi kriptotizim asosiga olingan muammoni yetarlicha aniq qoʻya olganda va uning bu muammoni hal qilishga resurslari yetarlicha boʻlganda, qabul qiluvchiga kelib tushgan raqamli imzo soxta boʻlsa, imzolovchi shaxsda imzoning soxtaligini isbotlovchi dalillar va maʼlumotlarning yoʻqligidir. Oʻzbekiston milliy ERI standartini yaratishda bu kamchiliklarni bartaraf etishga eʼtibor berildi. Shu maqsadda kriptografiya sohasidagi Oʻzbekiston Respublikasining dastlabki davlat standarti Oʻz DSt 1092:2009 «Axborot texnologiyasi. Axborotning kriptografik muhofazasi. Elektron raqamli imzoni shakllantirish va tekshirish jarayonlari»ni yaratish uchun matematik asos sifatida parametrli algebra qabul qilingan. Unda modul arifmetikasining yashirin yoʻllar juftiga ega boʻlgan ***bir tomonlama (parametrli) funksiyasi*** qoʻllaniladi, bunda hisoblashlar qiyinlik darajasi boʻyicha darajaga koʻtarish amallari kabi yengil amalga oshiriladi, funksiyani teskarilash esa diskret logarifm muammosini yechish jarayonidagidan kam boʻlmagan hisoblash sarflari va vaqt talab qiladi. Anʼanaviy bir tomonlama darajaga koʻtarish funksiyasi bitta yashirin yoʻlga ega boʻlib, u ushbu bir tomonlama funksiyaning xususiy holidir. Unda yashirin yoʻllar sonining uchta boʻlishi mumkinligi bardoshlilikni oshirish uchun qoʻshimcha imkoniyatlar yaratadi.

Oʻz DSt 1092:2009 «Axborot texnologiyasi. Axborotning kriptografik muhofazasi. Elektron raqamli imzoni shakllantirish va tekshirish jarayonlari»da quyidagi parametrlardan foydalaniladi:

a) p - modul, tub son, bunda $p>2^{255}$. Bu sonning yuqori chegarasi elektron raqamli imzo algoritmi muayyan amalga oshirilganda aniqlanishi kerak;

b) q – p-1 ning faktori (tub ko‘paytuvchisi) bo‘lgan tub son, bu yerda $2^{254} < q < 2^{256}$.

s) R – parametr, $R<q$ shartni qanoatlantiruvchi natural son; R parametri foydalanuvchilarning cheklangan guruhi uchun ochiq yoki birgalikdagi maxfiy kalit bo‘lishi mumkin;

d) $m = H(\bullet)$ - xesh-funksiya, cheklangan uzunlikdagi M xabarni 256 bit uzunlikdagi ikkilik vektorida aks ettiradi.

ERIAning har bir foydalanuvchisi quyidagi shaxsiy kalitlarga ega bo‘lishi kerak:

a) (x, u, g) – butun sonlar uchligi – ERIning yopiq kaliti;

bu yerda: x, u – yopiq kalitlar, $1<x$, $u<q$ shartlarni qanoatlantiruvchi tasodifiy yoki psevdotasodifiy generasiyalangan butun sonlar;

g – yopiq kalit, $g \equiv h^{\backslash(r-1)/q} \ (mod\ p)$ yordamida hisoblanadigan butun son;

bu yerda: $h<p$ – yopiq natural son bo‘lib, ω ning $1 \div q$ oraliq qiymatlarida faqat $\omega=q$ bo‘lgandagina $g^{\backslash\omega}(mod\ p) \equiv 0$ shartni qanoatlantiradi;

b) (y, z) - butun sonlar juftligi – ERIning ochiq kaliti;

bu yerda: y, z – ochiq kalitlar, $y \equiv g^{\backslash x}(mod\ p)$ va $z \equiv g^{\backslash u}\ (mod\ p)$ ifodalar yordamida hisoblanadi;

s) (R_1, y_1) – butun sonlar juftligi – ERIning soxtaligini aniqlash kaliti;

bu yerda: R_1 – nazorat kaliti (ochiq yoki yopiq), $1 \div q$-1 oraliqda tanlab olingan; agar R_1 yopiq bo‘lsa, unda R_1 imzolovchi shaxs va tekshiruvchi tomon uchun birgalikdagi maxfiy kalit bo‘lishi kerak;

y_1 - seans (ochiq) kaliti, har bir elektron raqamli imzo uchun parametr bilan darajaga oshirish natijasi kabi hisoblanadi.

Foydalanuvchilar guruhi uchun p, q tub sonlari ochiq va umumiy, R esa birgalikdagi maxfiy bo‘lishi mumkin.

Standartda imzolangan xabarni p-**NEW** sxemasi bo‘yicha tiklash g‘oyasi va K. Shnorrning imzo uzunligini qisqartirishga yo‘naltirilgan g‘oyasidan ham foydalanilgan [2, 11].

Standartda qo‘llanilgan parametrli algebra amallari nafaqat bir tomonlama funksiyani hosil etishda, balki ERIni shakllantirish va uning haqiqiyligini tasdiqlash jarayonlarida ham keng qo‘llanilgan.

Elektron raqamli imzoni shakllantirish

1) Birinchi qism

$$r \equiv m \circledR g^{\backslash -k} \ (mod\ p),$$

bu yerda: $m=H(M)$, $k=H(m \circledR x)$.

2) Ikkinchi qism

$$s \equiv u^{-1}*(k- r*x) \ (mod\ q).$$

3) Agar $\mu=1$, unda

$$r_1 \equiv r \circledR R_1 \ (mod\ q),$$

$$x_1 \equiv (k - s*u*R_1)* r_1^{\ -1} \ (mod\ q),$$

$$y_1 \equiv g^{\backslash x1} \ (mod\ p).$$

Bu yerda $\mu=0$ seans kalitisiz ish rejimini, $\mu=1$ seans kaliti bilan ishlash rejimini belgilaydi.

ERIning haqiqiyligini tasdiqlash

1) ERI autentifikasiyasi

$$m \equiv z^{\backslash s} \circledR y^{\backslash r'} \circledR r \ (mod\ p),$$

bu yerda: $m = H(M)$, $r' \equiv r \ (mod\ q)$.

2) Agar $\mu=1$ bo‘lsa, unda ERI soxtalashtirilganligini tekshirish amalga oshiriladi;

$$(z^{\backslash s} \circledR y^{\backslash r'})* R_1^{-1} \equiv (z *R_1^{-1})^{\backslash\backslash s*R1} \circledR' (y_1* R_1^{-1})^{\backslash\backslash r1} \ (mod\ p).$$

Bu yerda: ® - R parametr bilan ko‘paytirish amalining belgisi;

®’ - $R*R_1$ parametr bilan ko‘paytirish amalining belgisi;

$\backslash$ - R parametr bilan darajaga oshirish amalining belgisi;

$\backslash\backslash$ - $R*R_1$ parametr bilan darajaga oshirish amalining belgisi.

Kriptobardoshliligi daraja parametri muammosining murakkabligiga asoslangan ERI kriptotizimlarini yaratishga ham [11, 23] da tilga olingan umumiy sxema usulida yondashuv maqsadga muvofiqdir.

Diskret logarifmlashning murakkabligiga asoslangan sxemalarning zaif tomoni shundaki, badniyat kriptotahlilchi diskret logarifm muammosini hal qilish uchun yetarli resurslarga ega bo‘lib, uni soxtalashtirgan bo‘lsa, unda soxta ERI ham haqiqiy deb qabul qilinadi. Natijada qonuniy huquqqa ega foydalanuvchi tomonlarning ERI soxtaligini isbotlash imkoniyatlari yo‘qqa chiqadi. Buning oldini olish yo‘llaridan biri oshkora kalit ifodasida parametrli funksiyadan foydalanishdir. Bunda ERI kriptotizimining bardoshliligi daraja parametri muammosining murakkabligi bilan belgilanadi.

6.2.7 Elliptik egri chiziqlarga asoslangan elektron raqamli imzo algoritmlari matematik modellari

Elliptik egri chiziqli diskret logarifm muammosining murakkabligiga asoslangan ERI kriptotizimlarida juda qisqa kalitlar qo‘llaniladi, ammo uning ishonchliligini asoslab berish ancha murakkab masaladir. Elliptik egri chiziqli diskret logarifm muammosining diskret logarifm muammosiga keltirilishi A. Menezis [45] tomonidan ko‘rsatilgan. Lekin elliptik egri chiziqli diskret logarifm muammosining murakkabligiga asoslangan ERI algoritmlarida RSA algoritmiga ko‘ra kalitlar 100 marta tezroq hosil qilinadi va ancha kam joy egallaydi. Masalan, 97 bitli kalitga ega bo‘lgan shifrlangan axborotni buzishga urinish 512 bitli kalitga ega bo‘lgan RSA nosimmetrik shifrini buzishdan ko‘ra ikki marta qiyinroqdir [2, 11].

Hozirgi vaqtda eng murakkab hisoblangan elliptik egri chiziqli diskret logarifm muammosiga asoslangan ERI algoritmlari qatoriga GOST R 34.10-2001 bilan bir qatorda xalqaro standart maqomini olgan AQShning ESDSA, Koreyaning ES-KCDSA, Germaniyaning standarti EC-GDSA kiradi.

2001 yilda Rossiyada ERI uchun yangi GOST R 34.10-2001 standarti shu vaqtgacha qo‘llanib kelingan GOST R 34.10-94 standarti o‘rnida foydalanish uchun qabul qilindi va bunga ERI bardoshliligini oshirishga bo‘lgan zarurat sabab bo‘ldi. Bu standartning bardoshliligi EEChnuqtalari guruhida diskret logarifmlarni hisoblashning murakkabligiga hamda foydalaniladigan xesh-funksiya - GOST R 34.11-94 [72] ning bardoshliligiga asoslanadi.

ERI parametrlariga quyidagilar kiradi:

a) r tub son – $r > 2^{255}$ tengsizlikni qanoatlantiruvchi EECh moduli. Ushbu sonning yuqori chegarasi ERIni muayyan amalga oshirish jarayonida belgilanadi;

b) o‘zining $J(E)$ invarianti yoki $a, b \in F_r$ koeffisiyentlari bilan berilgan E elliptik egri chiziq;

d) w butun son - E EEChnuqtalari gruppasining tartibi;

e) t tub son - quyidagi shartlar bajarilgan E EEChnuqtalari gruppasi siklik qism gruppasining tartibi:

$$\begin{cases} w = lt, l \in Z, l \geq 1 \\ 2^{254} < t < 2^{256} \end{cases}$$

f) (x_r, y_r) koordinatali va $[t]N=0$ tenglikni qanoatlantiruvchi E elliptik egri chiziqning $N \neq 0$ nuqtasi;

g) $m = H(M) – M$ xabarni 256 bit uzunlikdagi qatorda aks ettiruvchi xesh-funksiya.

Yuqorida keltirilgan ERIA parametrlariga quyidagi talablar qo‘yiladi:

- barcha butun $i=1,2…, B$ sonlar uchun $r^i \neq 1 \ (\text{mod } t)$ shart bajarilishi lozim, bu yerda V uchun $B \geq 31$ tengsizlikni qanoatlantiradi;
- $w \neq r$ tengsizlik bajarilishi lozim;
- egri chiziq invarianti $J(E) \neq 0$ yoki 1728 shartlarini qanoatlantirishi lozim.

Algoritmning har bir foydalanuvchisi quyidagi shaxsiy kalitlarga ega bo‘lishi kerak:

a) ERI yopiq kaliti $d – 0<d<t$ tengsizlikni qanoatlantiruvchi butun son;

b) ERI ochiq kaliti $T – (x_t, y_t)$ koordinatali, $[d]N=T$ tenglikni qanoatlantiruvchi elliptik egri chiziqning nuqtasi.

$M \in V_\infty$ axborotga ERIni shakllantirish jarayoni algoritmi quyidagi qadamlar ketma-ketligini o‘z ichiga oladi:

1-qadam: xabarning xesh-funksiyasini hisoblang: $m=H(M)$;

2-qadam: $e \equiv m \ (mod\ t)$ ni hisoblang. Agar $ye=0$ bo‘lsa, u holda $ye=1$ ni aniqlang;

3-qadam: ushbu $0 < k < t$ tengsizlikni qanoatlantiruvchi tasodifiy (psevdotasodifiy) k butun sonini generasiya qiling;

4-qadam: elliptik egri chiziqning $C=[k]N$ nuqtasini hisoblang va $r=x_s \ (mod\ t)$ ni aniqlang, bu yerda $x_s – S$ nuqtaning x koordinatasi. Agar $r=0$ bo‘lsa, u holda 3-qadamga qayting;

5-qadam: $s \equiv (rd+ke) \ (mod\ t)$ ifodaning qiymatini hisoblang. Agar $s=0$ bo‘lsa, 3-qadamga qayting;

6-qadam: r va s larni ERI sifatida chiqishga bering.

Ushbu jarayon uchun dastlabki (kirishdagi) ma’lumotlar M xabar va ERIning yopiq kaliti d, chiqish natijasi bo‘lib esa, (r, s) elektron raqamli imzo hisoblanadi.

Qabul qilib olingan *M* axborotidagi ζ raqamli imzo haqiqiyligini tasdiqlash algoritmi quyidagi qadamlar ketma-ketligini o‘z ichiga oladi:

1-qadam: agar $0 < r < t$, $0 < s < t$ tengsizliklar bajarilsa, navbatdagi qadamga o‘ting, aks holda “imzo haqiqiy emas” qabul qilinadi;

2-qadam: *M* xabar bo‘yicha xesh-funksiyani hisoblang: $m=H(M)$;

3-qadam: $e \equiv m \pmod t$ ni hisoblang. Agar $ye=0$ bo‘lsa, u holda $ye=1$ ni aniqlang;

4-qadam: $v \equiv e^{-1} \pmod t$ ifodaning qiymatini hisoblang;

5-qadam: ushbu $z_1 \equiv sv \pmod t$, $z_2 \equiv -rv \pmod t$ ifodalar qiymatlarini hisoblang;

6-qadam: elliptik egri chiziqning $C=[z_1]N$ “+” $[z_2]T$ nuqtasini hisoblang va $R \equiv x_s \pmod t$ ni aniqlang, bu yerda x_s - *S* nuqtaning *x* koordinatasi.

7-qadam: agar $R=r$ tenglik bajarilsa, u holda “imzo haqiqiy”, aks holda “imzo haqiqiy emas” qabul qilinsin.

Ushbu jarayon uchun dastlabki (kirishdagi) ma’lumotlar bo‘lib, imzolangan *M* xabar, (r, s) elektron raqamli imzo va ERI ochiq kaliti, chiqish natijasi bo‘lib esa, mazkur ERI haqiqiyligi yoki haqiqiy emasligi haqidagi axborot hisoblanadi.

ECDSA

AQShning ERI uchun DSA ning elliptik egri chiziqlarga asoslangan analogi ESDSA 1992 yilda taklif etilgan va 1998 yilda ISO (International Standart Organization) standarti sifatida qabul qilingan. 1999 yilda esa ANSI X9.62 ESDSA standarti sifatida, 2000 yilda federal va IEEE standarti sifatida qabul qilingan [73].

Quyida ESDSA bo‘yicha ERIni shakllantirish va uning haqiqiyligini tasdiqlash algoritmlari keltirilgan.

ESDSA bo‘yicha ERIni shakllantirish algoritmi quyidagi qadamlar ketma-ketligini o‘z ichiga oladi:

1) $k \in [1, n-1]$ tasodifiy soni tanlanadi;

2) $[k]P = (x_1, y_1)$ hisoblanadi;

3) $r \equiv x_1 \pmod n$ hisoblanadi. Agar $r=0$ bo‘lsa, *k* qayta tanlanadi;

4) $e = H(M)$ xesh-funksiya hisoblanadi;

5) $s \equiv k^{-1}(e+dr) \ (mod\ n)$ hisoblanadi; bu yerda *(r, s)* juftligi *M* axborotning elektron raqamli imzosi.

ESDSA bo‘yicha ERI haqiqiyligini tasdiqlash algoritmi quyidagi qadamlar ketma-ketligini o‘z ichiga oladi:

1) agar $r=0$ bo‘lsa, imzo haqiqiy emas deb topiladi;

2) $h = H(M)$ xesh-funksiya hisoblanadi;

3) $u_1 \equiv hs^{-1} \ (mod\ n)$ hisoblanadi;

4) $u_2 \equiv rs^{-1} \ (mod\ n)$ hisoblanadi;

5) $[u_1]P + [u_2]Q = (x_1, y_1)$ hisoblanadi;

6) $v \equiv x_1 \ (mod\ n)$ hisoblanadi.

Agar $v = r$ bo‘lsa, imzo haqiqiy, aks holda haqiqiy emas deb topiladi.

Quyida xalqaro standart sifatida qabul qilingan Koreya, Germaniya elliptik egri chiziqlarga asoslangan elektron raqamli imzo algoritmlari ko‘rib o‘tiladi.

EC-GDSA standartida prototip sifatida GDSA tanlangan. Algoritmda ERIni generasiya qilishda dastlab *M* xabar uchun xesh-qiymat hisoblanadi, $1 \le k \le q-1$ oraliqda *k* soni tanlanadi, shundan so‘ng ketma-ket ERI elementlari hisoblanadi:

xesh-qiymat $e \equiv H(M), \ (x_1, y_1) = [k]G, \ r \equiv x_1 (mod\ q), \ s \equiv (kr-e)d \ (mod\ q).$

ERIni tekshirish jarayonida avvalo imzoning uzunligi tekshiriladi va u to‘g‘ri bo‘lsa, ketma-ket quyidagi qiymatlar hisoblanadi:

xesh-qiymat $e \equiv H(M), \ u_1 \equiv r^{-1}e (mod\ q), \ u_2 \equiv r^{-1}s \ (mod\ q)$ va $X = [u_1]\ G\ "+"[u_2]Q = (x_X, y_X)$. u_1 va u_2 qiymatlarni hisoblash uchun prototipda foydalanilganidek tenglamadan foydalaniladi.

Germaniyaning milliy algoritmida ochiq kalit *Q* Koreyaning milliy algoritmidagidek $Q = [d^{-1}]G$ shaklga ega, bu yerda *d* – ERI egasining tasodifiy tanlangan shaxsiy kaliti, *G* - *q* tartibli asos nuqta. Bu esa ERIni shakllantirish jarayonini osonlashtirishga yordam beradi va imzoni soxtalashtirishni cheklab qo‘yadi. Imzoni tekshirishda, agarda $x_x (mod\ q) \equiv r$ bo‘lsa, u holda imzo haqiqiy, aks holda haqiqiy emas.

EC-KCDSA standartida prototip sifatida KCDSA tanlangan. Algoritmda ERIni generasiya qilishda ERI egasining xesh-kodi *z* dan foydalaniladi. Dastlab *M* xabar bilan konkatenasiya qilish uchun xesh-

qiymat hisoblanadi, $1 \le k \le q-1$ oraliqda k soni tanlanadi, shundan so‘ng ketma-ket ERI elementlari hisoblanadi:

xesh-qiymat $e=H(z||M)$, $(x_1, y_1)=[k]G$, $r = H([k]G)$, $w=r \oplus e$; agar $w \ge q$ bo‘lsa , u holda $w=w-q$ qabul qilinadi; $s \equiv d\,(k-w)\,(mod\ q)$.

ERIni tekshirish jarayonida avvalo imzoning uzunligi tekshiriladi va u to‘g‘ri bo‘lsa ketma-ket quyidagi qiymatlar hisoblanadi:

xesh-qiymat $e=H(z||M)$; $w=r \oplus e$; agar $w \ge q$ bo‘lsa, u holda $w=w-q$ qabul qilinadi; $X=[s]Q''+''[w]\ G =(x_X, y_X)$, bu yerda $s=d(k-w)(mod\ q)$, G –q tartibli asos nuqta (bazovaya tochka), ochiq kalit $Q = [d^{-1}]G$, bu yerda $d - 1<d<q$ oraliqdagi shaxsiy maxfiy kalit. Agar $H(x_x)=r$ bo‘lsa, u holda imzo haqiqiy, aks holda haqiqiy emas.

Ko‘rinib turganidek s va w (u_1 va u_2 analoglari, mos ravishda) bir-biriga o‘zaro bog‘liqdir, bundan tashqari w imzolanuvchi xabar M va r parametrning xesh-funksiya qiymati $e=H(z||M)$ ga ham bog‘liq. Bu esa ECDSA-2000 va GOST R 34.10-2001 algoritmlaridagidek kriptografik samarani beradi.

Bundan tashqari r parametr $[k]G=(x_1, y_1)$ nuqtaning xesh-funksiya qiymati sifatida, ya’ni $r=H(x_x)$ kabi hisoblanadi. Bu esa algoritmda qo‘llanilgan xesh-funksiya hisobiga ERI algoritmi bardoshliligini yanada oshiradi, chunki x_1 – tasodifiy son sifatida faqatgina imzo qo‘yadigan shaxsga ma’lum. x_x – imzoni tekshirish algoritmi bo‘yicha sertifikatlangan ochiq kalitga bog‘liq hisoblanadi. Ya’ni tasodifiy tanlangan noma’lum x_1 parametr r ni shakllantirishda kalitsiz xesh-funksiyaning kaliti bo‘lib hisoblanadi, x_x qiymati esa oldindan noma’lum va imzoni tekshirish algoritmining yakuniy natijasi bo‘lib hisoblanadi.

Nazorat savollari

1. Autentifikasiyaga ta’rif bering?
2. Autentifikasiya qanday turlarga bo‘linadi?
3. Autentifikasiya protokoli nimaga zarur?
4. Ma’lumotlar manbai autentifikasiyasi qanday amallarni bajarishni nazarda tutadi?
5. Mohiyat autentifikasiyasi haqida nimalarni bilasiz?
6. Autentifikasiyalangan kalitlarni generasiyalash qanday amalga oshiriladi?

7. Autentifikasiya protokollari qanday turlarga bo‘linadi?

8. Elektron raqamli imzoga ta’rif bering?

9. Elektron raqamli imzo algoritmlarining qanday umumiy kriptografik xossalarini bilasiz?

10. Qanday elektron raqamli imzo algoritmlarini bilasiz?

11. Maxsus ERI standartlari turkumiga qanday algoritmlar kiradi?

12. Elektron raqamli imzo algoritmining bardoshliligi qanday masalalar murakkabligi bilan aniqlanadi?

13. Ochiq kalitli shifrlash algoritmlariga asoslangan ERI algoritmlarining qo‘llanilishi haqida nimalarni bilasiz?

14. RSA ochiq kalitli shifrlash algoritmi qanday qadamlarni o‘z ichiga oladi?

15. El Gamal ochiq kalitli ERI algoritmi qanday amalga oshiriladi?

16. Maxsus ERI algoritmlarining matematik modellari haqida nimalarni bilasiz?

17. O‘zbekiston Respublikasi standarti: O‘z DSt 1092da qanday bir tomonlama funksiyadan foydalaniladi?

18. O‘z DSt 1092 «Axborot texnologiyasi. Axborotning kriptografik muhofazasi. Elektron raqamli imzoni shakllantirish va tekshirish jarayonlari»da qanday parametrlardan foydalaniladi?

19. Elliptik egri chiziqlarga asoslangan elektron raqamli imzo algoritmlari matematik modellarini tushuntirib bering?

XULOSA

Ming yilliklar davomida kriptografiyadan davlat qurilishida, harbiy va diplomatiya aloqasini muhofazalashda foydalanib kelingan bo‘lsa, axborot asrining boshlanishi bilan kriptologiya jamiyatda, xususiy sektorda foydalanish uchun ham zarur bo‘lib qoldi. Qariyb 35 yildan buyon kriptologiyada keng miqyosda ochiq tadqiqotlar olib borilmoqda. Hozirgi kunda konfidensial axborot (masalan, yuridik hujjatlar, moliyaviy, kredit stavkalari to‘g‘risidagi axborotlar, kasallik tarixi va shunga o‘xshash)larning talay qismi kompyuterlararo odatdagi aloqa kanallari orqali uzatilmoqda. Jamiyat uchun bunday axborotning konfidensialligi va asl holda saqlanishi zaruratga aylangan.

Kriptografiya tarixida *birinchi muhim voqyea* simmetrik kriptotizimlarning birinchi marta Davlat standarti maqomiga ega bo‘lishi bo‘lsa, keyingi o‘n yilliklarning *muhim kashfiyoti* kriptologiyaga yangicha yondashuvlarni boshlab bergan oshkora kriptografiyaning yuzaga kelib uning muttasil rivojlanib borayotganligidir.

AQShdan keyin Yevropa davlatlari va Yaponiyada elektron raqamli imzo bo‘yicha qonun va dastlabki davlat standartlari qabul etildi. Ko‘pchilik davlatlar, shu jumladan O‘zbekiston Respublikasi ham kriptografiya vositalaridan axborot–telekommunikasiya tarmoqlarida maxfiy axborotlarni xavfsiz uzatish va elektron raqamli imzo yaratishda o‘z milliy algoritmlaridan foydalanmoqdalar.

Ushbu o‘quv qo‘llanmada kriptografiya tarixi, kriptografiyaning asosiy matematik tushunchalari, ta’riflari, teoremalari hamda simmetrik va nosimmetrik kriptografik algoritmlarning matematik asoslari bayon etilgan. Unda O‘zbekiston davlat standartlarini ishlab chiqishga asos bo‘lgan alebraik strukturalar va funksiyalar - diamatrisalar algebrasi, parametrli elliptik egri chiziqli funksiyalar va ularning asosiy xossalari, hamda ishlab chiqilgan kriptoalgoritmlar keltirilgan.

Ushbu o‘quv qo‘llanma axborot xavfsizligi va kriptografiya yo‘nalishida davlat tilida ta’lim olayotgan magistrlar uchun mo‘ljallangan. Shuningdek ushbu o‘quv qo‘llanmadan axborot xavfsizligi yo‘nalishida bakalavrlar tayyorlash jarayonida hamda kriptografiya yo‘nalishida ilmiy-tadqiqot olib borayotgan tadqiqotchilar, ilmiy xodimlar va soha mutaxassislari foydalanishlari mumkin.

GLOSSARIY –ГЛОССАРИЙ - GLOSSARY

Algoritm – amallarning cheklangan soni yordamida masala echimini belgilovchi buyruqlarning cheklangan to‘plami.

Алгоритм - упорядоченный конечный набор четко определенных правил для решения задач за конечное количество шагов.

Algorithm - an ordered finite set of clearly defined rules for solving a finite number of steps.

Shifrlash algoritmi - shifrlash funksiyasini amalga oshiruvchi kriptografik algoritm.

Алгоритм шифрования - алгоритм криптографический, реализуюший функцию зашифрования.

Encryption algorithm - a cryptographic algorithm that implements the encryption function.

Kriptografik algoritm – kriptografik funksiyalarning birini xisoblashni amalga oshiruvchi algoritm.

Алгоритм криптографический - алгоритм, реализующий вычисление одной из функций криптографических.

Cryptographic algorithm - the algorithm that implements the computation of one of the cryptographic functions.

Rasshifrovkalash algoritmi – rasshifrovkalash funksiyasini amalga oshiruvchi va shifrlash algoritmiga teskari algoritm.

Алгоритм расшифрования - алгоритм криптографический, обратный к алгоритму зашифрования и реализующий функцию расшифрования.

Decryption algorithm – a cryptographic algorithm, the inverse of the algorithm encryption and decryption function implements.

Autentifikator– foydalanuvchining farqli alomatini ifodalovchi autentifikatsiya vositasi. Qo‘shimcha kod so‘zlari, biometrik ma’lumotlar va foydalanuvchining boshqa farqli alomatlari autentifikatsiya vositalari bo‘lishi mumkin.

Аутентификатор - средство аутентификации, представляющее отличительный признак пользователя. Средствами аутентификации пользователя могут быть дополнительные кодовые слова, биометрические данные и другие отличительные признаки пользователя.

Authenticator - authentication means representing the hallmark of the user. Means of user.

Autentifikatsiya – odatda tizim resurslaridan foydalanishga ruxsat etish xususida qaror qabul qilish uchun foydalanuvchining (xakikiyligini), qurilmaning yoki tizimning boshqa tashkil etuvchisining identifikatsiyasini tekshirish; saqlanuvchi va uzatiluvchi ma'lumotlarning ruxsatsiz modifikatsiyalanganligini aniqlash uchun tekshirish.

Аутентификация - проверка идентификации пользователя (проверка подлинности), устройства или другого компонента в системе, обычно для принятия решения о разрешении доступа к ресурсам системы; проверка целостности хранящихся или передающихся данных для обнаружения их несанкционированной модификации.

Authentication - checking user authentication (authentication), device or other component in the system, usually to make a decision about granting access to system resources; checking the integrity of stored or transmitted data to detect unauthorized modification.

Ikki faktorli autentifikatsiya – foydalanuvchilarni ikkita turli faktorlar asosida autentifikatsiyalash, odatda, foydalanuvchi biladigan narsa va egalik qiladigan narsa (masalan, parol va fizik identifikatori) asosida.

Аутентификация двухфакторная — аутентификация пользователей на основе двух разнородных факторов, как правило, на основе того, что знает пользователь, и того, чем он владеет (например, на основе пароля и физического идентификатора).

Two-factor authentication- user authentication based on two different factors are usually based on what the user knows, and what he owns (eg password-based and physical identifier).

Ko‘p faktorli autentifikatsiya- bir necha mustaqil faktorlar asosida foydalanuvchini identifikatsiyalash orqali foydalanish nazoratini amalga oshirish.

Аутентификация многофакторная — реализация контроля доступа, представляющая собой идентификацию пользователя на основе нескольких независимых факторов.

Multifactor Authentication - implementing access control, which is a user identification based on several independent factors.

Ma’lumotlar bazasi - tatbiqiy dasturlarga bog‘liq bo‘lmagan xolda ma’lumotlarni tavsiflashning, saqlashning va manipulyatsiyalashning umumiy prinsiplarini ko‘zda tutuvchi ma’lum qoidalar bo‘yicha tashkil etilgan ma’lumotlar majmui.

База данных - совокупность данных, организованных по определенным правилам, предусматривающим общие принципы описания, хранения и манипулирования данными, независимо от прикладных программ.

Database - a set of data organized according to certain rules, general principles providing descriptions, storing and manipulating data, regardless of the application.

Axborot xavfsizligi - axborot xolati bo‘lib, unga binoan axborotga tasodifan yoki atayin ruxsatsiz ta’sir etishga yoki uning olinishiga yo‘l qo‘yilmaydi. Yana - axborotni texnik vositalar yordamida ishlanishida uning maxfiylik (konfidensiallik), yaxlitlik va foydalanuvchanlik kabi xarakteristikalarining (xususiyatlarining) saqlanishini ta’minlovchi axborotning himoyalanish sathi xolati.

Безопасность информации - состояние информации, при котором исключаются случайные или преднамеренные несанкционированные воздействия на информацию или несанкционированное ее получение, еще - состояние уровня защищенности информации при ее обработке техническими средствами, обеспечивающее сохранение таких ее качественных характеристик (свойств) как секретность /конфиденциальность/, целостность и доступность.

Information security - state information , which prevents accidental or intentional tampering or unauthorized information to

receive it, also - state -level data protection during processing technologies to support the preservation of its qualitative characteristics (properties) as privacy / confidentiality / integrity and availability.

Tarmoq xavfsizligi - axborot tarmog‘ini ruxsatsiz foydalanishdan, me’yoriy ishlashiga tasodifan yoki atayin aralashishdan yoki tarmoq komponentlarini buzishga urinishdan extiyot qiluvchi choralar. Asbob-uskunalarni, dasturiy ta’minotni, ma’lumotlarni himoyalashni o‘z ichiga oladi.

Безопасность сетевая — меры, предохраняющие сеть информационную от доступа несанкционированного, случайного или преднамеренного вмешательства в нормальные действия или попыток разрушения ее компонентов. Включает защиту оборудования, программного обеспечения, данных.

Network Security - measures that protect the network information from unauthorized access, accidental or intentional interference with normal activities or attempts to destroy its components. Includes the protection of hardware, software, data.

Verifikatsiya – hisoblash vositalari yoki ularning kompleksi spetsifikatsiyasining ikki sathini tegishli moslikka taqqoslash jarayoni. Yana- dasturlashda – dastur to‘g‘riligining tasdig‘i. Verifikatsiyaga ikkita yondashish farqlanadi: statik va konstruktiv usullar.

Верификация - процесс сравнения двух уровней спецификации средств вычислительной техники или их комплексов на надлежащее соответствие. Еще - в программировании доказательство правильности программ. Различают два подхода к верификации: статические и конструктивные методы.

Verification - the process of comparing two levels of specification of computer equipment or systems for proper alignment. Also - programming proof of the correctness of programs. There are two approaches to verification: static and constructive methods.

Verifikatsiya – hisoblash vositalari yoki ularning kompleksi spetsifikatsiyasining ikki sathini tegishli moslikka taqqoslash jarayoni.

Yana- dasturlashda – dastur to‘g‘riligining tasdig‘i. Verifikatsiyaga ikkita yondashish farqlanadi: statik va konstruktiv usullar.

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.

Key generator- technical device or program designed to generate arrays of numbers or other data to be used as keys (cryptographic) key sequence, initialization vectors, and so on.

Foydaluvchanlik - avtorizatsiyalangan mantiqiy obekt so‘rovi bo‘yicha mantiqiy ob’ektning tayyorlik va foydalanuvchanlik holatida bo‘lish xususiyati.

Доступность — свойство объекта находиться в состоянии готовности и используемости по запросу авторизованного логического объекта.

Availability - property of an object in a state of readiness and usage upon request authorized entity.

Kalit uzunligi (o‘lchovi) - kalitni ifodalovchi ma’lum alfavitdagi so‘z uzunligi. Ikkili kalit uzunligi bitlarda o‘lchanadi.

Длина (размер) ключа — длина слова в определённом алфавите, представляющего ключ. Длина ключа бинарного измеряется в битах.

Key length - word length in a certain alphabet, representing the key. The key length is measured in binary bits.

Axborotni kriptografik himoyalash - axborotni kriptografik o‘zgartirish yordamida himoyalash.

Защита информации криптографическая — защита информации с помощью ее криптографического преобразования.

Cryptographic protection of information - information security by means of its cryptographic transformation.

Identifikator – sub’ekt yoki ob’ektning farqlanuvchi alomatidan iborat foydalanishning identifikatsiya vositasi. Foydalanuvchilar uchun asosiy identifikatsiya vositasi parol hisoblanadi.

Идентификатор - средство идентификации доступа, представляющее собой отличительный признак субъекта или объекта доступа. Основным средством идентификации доступа для пользователей является пароль.

Identifier - means of identification of the access, representing a distinctive sign of the subject or object of access. The main means of identification of access for users is the password.

Identifikatsiya – foydalanish sub'ektlari va obyektlariga identifikator berish va/yoki taqdim etilgan identifikatorni berilganlari ro'yhati bilan taqqoslash.

Идентификация- присвоение субъектам и объектам доступа идентификатора и/или сравнение предъявляемого идентификатора с перечнем присвоенных идентификаторов.

Identification -assignment to subjects and objects of access of the identifier and/or comparison of the shown identifier with the list of the appropriated identifiers.

Ochiq kalitlar infrastrukturasi – asimmetrik shifrtizim kalitlari tizimining qismtizimi. Qonuniy foydalanuvchilarning kalitlarning xaqiqiyligiga, kalitlarning foydalanuvchilarga va ular oldindan kelishilgan ishlatish shartlariga mosligiga ishonishlarini (kalitlar sertifikatlari yordamida) ta'minlashga mo'ljallangan.

Инфраструктура ключей открытых — подсистема системы ключевой шифрсистемы асимметричной. Предназначена для обеспечения (с помощью сертификатов ключей) доверия пользователей законных к подлинности ключей, соответствия ключей пользователям и оговоренным условиям их применения.

Public Key Infrastructure (PKI) — subsystem of system key cipher system of asymmetric. It is intended for providing (by means of certificates of keys) trust of users of lawful keys to authenticity, compliance of keys to users and the stipulated conditions of their application.

Mojaro – ruxsatsiz foydalanish xuquqiga ega bo'lishga yoki kompyuter tizimiga xujum o'tkazishga urinishning qayd etilgan xoli.

Инцидент — зафиксированный случай попытки получения

несанкционированного доступа или проведения атаки на компьютерную систему.

Incident— the recorded case of attempt of receiving unauthorized access or carrying out attack to computer system.

Ma’lumotlarni uzatuvchi kanal - fizik muhit, u orqali axborot bir qurilmadan ikkinchisiga uzatiladi.

Канал передачи данных — физическая среда, по которой передается информация из одного устройства в другое.

Data transmission channel — the physical environment on which information from one device is transferred to another.

Ochiq kalit –asimetrik shifrtizimning maxfiy bo‘lmagan kaliti.

Ключ открытый — несекретный ключ шифрсистемы асимметричной.

Public key — unclassified key the asymmetric cryptosystem.

Deshifrlash kaliti - deshifrlashda ishlatiluvchi kalit.

Ключ расшифрования — ключ, используемый при расшифровании.

Decryption key — the key used for decryption.

Seans kaliti - ikkita qatnashchilar (protokol qatnashchilari) orasidagi bitta aloqa seansi uchun maxsus generatsiyalangan kalit.

Ключ сеансовый — ключ, специально сгенерированный для одного сеанса связи между двумя участниками (протокола).

Session key — the key which has been specially generated for one communication session between two participants (protocol).

Maxfiy kalit - ma’lum simmetrik shifrtizim kalitlaridan yoki ma’lum asimmetrik shifrtizimning ba’zi funksiyalaridan foydalanish huquqiga ega bo‘lmagan shaxslardan maxfiy sanaluvchi kalit.

Ключ секретный — ключ, сохраняемый в секрете от лиц, не имеющих допуска к ключам данной шифрсистемы симметричной или к использованию некоторых функций данной шифрсистемы асимметричной.

Secret key — the key kept in a secret from persons, not having the admission to keys given symmetric cryptosystem or to use of some functions given the asymmetric cryptosystem.

Kriptografik tizim –axborotni kriptografik o‘zgartirishni va kalitlarni taqsimlash jarayonini boshqarishni ta’minlovchi texnik va/yoki dasturiy vositalar, tashkiliy usullar majmui.

Криптографическая система - совокупность технических и /или программных средств, организационных методов, обеспечивающих криптографическое преобразование информации и управление процессом распределения ключей.

Cryptographic system, Cryptosystem - set technical and/or software, the organizational methods providing cryptographic transformation of information and management process of distribution of keys.

Parol –tizimdan, dasturdan yoki ma’lumotlardan foydalanishga ruxsat olish uchun kompyuter so‘rovi bo‘yicha kiritiladigan simvollarning noyob ketma-ketligi.

Пароль — уникалная последовательноеть символов, которую необходимо ввести по запросу компьютера, чтобы исключить доступ к системе, программе или данным.

Password - a password is an unspaced sequence of characters used to determine that a computer user requesting access to a computer system is really that particular user.

Raqamli imzo - xabarga yoki hujjatga va faqat imzo chekuvchi sub’ektga ma’lum qandaydir maxfiy kalitga bog‘liq qandaydir alfavitdagi qatordan (masalan raqamli qatordan) iborat. Raqamli imzoning, maxfiy kalitdan foydalanmasdan osongina tekshirilishi lozimligi faraz qilinadi.

Подпись цифровая — представляет собой строку в некотором алфавите (например, цифровую), зависящую от сообщения или документа и от некоторого ключа секретного, известного только подписывающему субъекту. Предполагается, что п. ц. должна быть легко проверяемой без получения доступа к ключу секретному.

Digital signature - is a string in some alphabet (eg, digital), depending on the message or document and from a secret key known only to the signatory subject. It is assumed that digital signatur should be easily verified without access to the secret key.

Elektron imzo - boshqa elektron shakldagi axborotga (imzolanuvchi axborotga) birlashtirilgan yoki boshqa tarzda shunday axborot bilan bog‘langan va axborotni imzolovchi shaxsni aniqlashda ishlatiladigan elektron shakldagi axborot.

Подпись электронная — информация в электронной форме, которая присоединена к другой информации в электронной форме (подписываемой информации) или иным образом связана с такой информацией и которая используется для определения лица, подписывающего информацию.

Electronic signature - information in electronic form which is attached to the other information in electronic form (signed information) or otherwise relating to such information and is used to determine the person signing the information.

Protokol - qurilmalar, dasturlar, ma’lumotlarlarni ishlash tizimlari, jarayonlar yoki foydalanuvchilarning o‘zaro harakati algoritmini belgilovchi qoidalar majmui.

Протокол - совокунность правил, определящих алгоритм взаимодействия устройств, программ, систем обработки данных, процессов или пользователей.

Protocol - a set of rules that define the algorithm of interaction devices, software, data processing systems, processes or users.

Taxdid (axborot xavfsizligiga taxdid) - axborot xavfsizligini buzuvchi potensial yoki real mavjud xavfni tug‘diruvchi sharoitlar va omillar majmui.

Угроза (безопасности информации) — совокупность условий и факторов, создающих потенциальную или реально существующую опасность нарушения безопасности информации.

Threat - set of conditions and factors that create potential or actual violations of the existing danger of information security.

Xesh-funksiya - chekli alfavitdagi uzunligi chekli kirish yo‘li so‘zini berilgan, odatda, qat’iy uzunlikdagi, so‘zga akslantirish funksiyasi.

Хеш-функция - функция, отображающая входное слово конечной длины в конечном алфавите в слово заданной, обычно фиксированной длины.

Hash function - function mapping input word of finite length over a finite alphabet in a given word, usually a fixed length.

Axborot yaxlitligi - tasodifan va/yoki atayin buzilish hollarida hisoblash texnikasi vositalarining yoki avtomatlashtirilgan tizimning axborotini o‘zgartirmasligini ta’minlovchi xususiyati.

Целостность информации - способность средства вычислительной техники или системы автоматизированной обеспечивать неизменность информации в условиях случайного и/или преднамеренного искажения (разрушения).

Information Integrity - the ability of computers and automated systems to provide consistent information in a casual and / or intentional distortion (destruction).

FOYDALANILGAN ADABIYOTLAR

1. Ўзбекистон Республикасини янада ривожлантириш бўйича ҳаракатлар стратегияси тўғрисида. Ўзбекистон Республикаси Президентининг ПФ-4947- сон фармони. Тошкент, 2017 йил 7 феврал.
2. Хасанов П.Ф., Исаев Р.И., Хасанов Х.П., Назарова М.Х. Ахмедова О.П. Ахборотнинг криптографик муҳофазаси тарихи (Дастлабки ва формал криптография даври) // Aloqa dunyosi. – Тошкент, 2005, №1 (4). – 32-37 -бетлар.
3. Ахмедова О.П. Параметрлар алгебраси асосида носимметрик криптотизимлар яратиш усули ва алгоритмлари // Номзодлик диссертация иши, Тошкент-2007.
4. Бабаш А.В., Шанкин Г.П. История криптографии. Часть I. – Москва: Лори Гелиос АРВ, 2002. – 240 с.
5. Бабаш А.В., Шанкин Г.П., Криптография – Москва: Лори Гелиос АРВ, 2002. – 512 с.
6. Арипов М.М., Пудовченко Ю.Е. Основы криптологии – Ташкент: 2004. – 136 с.
7. Баричев С.Г., Серов Р.Е. Основы современной криптографии. Учебное пособие. – Москва: Лори Горячая Линия - Телеком, 2002. – 152 с.
8. Алексеев А. Криптогрфия и криптоанализ: вековая проблема человечества. http://www.nvkz.kuzbass.net/hard-soft/soft/other/kripto-analiz.html
9. Жельников В. Криптогоафия от папируса до компьютера. М.:ABF, 1996.
10. O‘z DSt 1109:2006 «Ахборот технологияси. Ахборотнинг криптографик муҳофазаси. Атамалар ва таърифлар».
11. История криптографии и криптоанализа. http://crypto hot box.ru.
12. Шнайер Б. Прикладная криптография. Протоколы, алгоритмы, исходные тексты на языке Си. –М.: издательство ТРИУМФ, 2003 - 816 с.
13. Коробейников А.Г., Гатчин Ю.А. Математические основы криптологии. Учебное пособие. Санкт-Петербург-2004.

14. Акбаров Д.Е. Ахборот хавфсизлигини таъминлашнинг криптографик усуллари ва уларнинг қўлланишлари. Тошкент. ”Ўзбекистон маркаси “, 2009. – 432 б.

15. «Ошкора калитли криптотизимларни криптотаҳлиллаш учун қуролу-воситалар ишлаб чиқиш ва уларни тадқиқ этиш» мавзуси бўйича бажарилган илмий-тадқиқот ишининг 1-8 - босқич ҳисоботлари. – ЎзААА ФТМТМ, Тошкент, 2003.

16. Защита информации. Малый тематический выпуск. ТИИЭР, 1988 г, т.76, №5.

17. Kahn D. The codebreakers. N.-Y., 1967.

18. Саломаа А. Криптография с открытым ключом. М.,1997

19. Бабаш А.В., Гольев Ю.И., Ларин Д.А. Шанкин Г.П. О развитии криптографии в XIX веке. Защита информации. Конфидент. 2003 г. №5.

20. Бабаш А.В., Гольев Ю.И., Ларин Д.А. Шанкин Г.П. Криптографические идеи XIX века. Защита информации. Конфидент. 2004 г. №1, №2.

21. Хасанов П.Ф., Исаев Р.И., Хасанов Х.П., Назарова М.Х. Ахмедова О.П. Ахборотнинг криптографик муҳофазаси тарихи (Илмий криптография даври) // Aloqa dunyosi. – Тошкент, 2005, №2 (5). – 47-53 бетлар.

22. Михаил Масленников. Практическая криптография. Санкт-Петербург «БХВ-Петербург», 2003.

23. Хасанов П.Ф., Исаев Р.И., Назарова М.Х., Хасанов Х.П., Ахмедова О.П. Ахборотнинг криптографик муҳофазаси тарихи (Компьютер криптографияси даври) // Aloqa dunyosi. – Тошкент, 2006, №1 (6). – 59-74 бетлар.

24. Хасанов Х.П. Такомиллашган диаматрицалар алгебралари ва параметрли алгебра асосида криптотизимлар яратиш усуллари ва алгоритмлари. – Тошкент, 2008. -208 б.

25. Шеннон К. Теория и связи в секретных системах. Работы по теории информации и кибернетике. – М.: Иностранная лит. 1963. – 243 б.

26. Нильс Фергюсон, Брюс Шнайер. Практическая криптография –Москва: "Диалектика", 2004 г. – 432 с.

27. Federal Information Processing Standards Publication 197. Advanced Encryption Standard (AES). 2001.

28. ГОСТ 28147-89. Государственный Стандарт Союза ССР. Системы обработки информации. Защита криптографическая. Алгоритм криптографического преобразования.

29. O‘z DSt 1105:2006 «Ахборот технологияси. Ахборотнинг криптографик муҳофазаси. Маълумотларни шифрлаш алгоритми».

30. Diffie, W., Hellman, M.E. New directions in cryptography // IEEE Transactionson Information Theory, vol. IT-22, 1976. – Pp. 644-654.

31. Диффи У. Первые десять лет криптографии с открытым ключом // Перевод с англ. Защита информации. Малый тематический выпуск ТИИЭР. – Москва, 1988. – т.76, №5. – С. 54-74.

32. Rivest R.L., Shamir A.,Adleman L.A. Method of Obtaining Digital Signature and Publice-Key Grypto System // ACM, V.21, №2, 1978. – Pp. 120-126.

33. Rivest R. RSA chips (past/present/future) // Presented at Eurocrypt 84, Paris, France, 1984. – Pp. 9-11.

34. Rivest R. L. The RC5 Encryption Algorithm // Fast Software Encryption, Second International Workshop / Lecture Notes in Computer Science. Springer-Verlag. Vol. 1008, 1995. – Pp. 86-96.

35. US Patent, Rivest, et al. Cryptographic communications system and method, 4.405.829, September 20, 1983.

36. Shamir, A. On the generation of cryptographically strong pseudo-random sequences // ACM Transactions on Computer Systems, vol. 1, 1983. – Pp. 38-44.

37. Shamir, A. A polynomial time algorithm for breaking the basic Merkle-Hellman cryptosystem // IEEE Transactionson Information Theory, vol. IT-30, 1984. – Pp. 699-704.

38. ElGamal T. On computing logarithm over finite fields // Advances in cryptology—CRYPTO‘85 (Santa Barbara, Calif., 1985). (Lect. Notes in Comput. Sci.; V. 218). – Pp. 396-402.

39. ElGamal T., A Public Key Cryptosystem and a Signature Scheme Based on Discrete Logarithms // IEEE Transactions on Information Theory, 1985, vol. IT-31. – Pp. 469-472.

40. US Patent, Schnorr. Method for identifying subscribers and for generating and verifying electronic signatures in a data exchange system. 4.995.082. – 1991.

41. Ong H. and Schnorr C.P. Signatures sheme based on quadratic forms // In Advances in Cryptology: Proceedings of CRYPTO 83. New York, NY: Plenum.1984. – Pp. 117-132.

42. Ong H., Schnorr C.P., and Shamir A. An efficient signature sheme based on quadratic equatins // In Proceedings of 16th ACM Symp. On Theory of Computing, 1984. – Pp. 208-216.

43. Koblitz N. and Vanstone S. The state of elliptic curve cryptography // Designs, Codes and Cryptography, 19 (2000). – Pp. 173-193.

44. Koblitz N. Elliptic Curve Cryptosystems // Mathematics of Computation, 48, 1987. – Pp. 203-209.

45. Коблиц Н. Введение в эллиптические кривые и модулярные формы // Пер с англ. – Москва: Мир, 1988. – 320 с.

46. Menezes A., van Oorschot P., Vanstone S. Handbook of Applied Cryptography // CRC Press, 1996. – 780 pp.

47. Menezes A., Okamoto T. & Vanstone S. Reducing elliptic curve logarithms to logarithms in a finite field // IEEE Transactions on Information Theory, 39 (1993). – Pp. 1639-1660.

48. Шнайер Б. Слабые места криптографических систем // Открытые системы. – 1999, № 1. – С. 31-36.

49. O‘z DSt 1092:2009 «Ахборот технологияси. Ахборотнинг криптографик муҳофазаси. Электрон рақамли имзони шакллантириш ва текшириш жараёнлари».

50. O‘z DSt 1106:2009 «Ахборот технологияси. Ахборотнинг криптографик муҳофазаси. Хэшлаш функцияси».

51. Венбо Мао. Современная криптография. Теория и практика. – Москва - Санкт-Петербург - Киев: Лори Вильямс, 2005. – 768 с.

52. Хасанов Х.П. Такомиллаштирилган диаматрицалар алгебраси // Infocom.uz. – Тошкент, 2005, №9. – 68-70 б.

53. Хасанов Х.П. Диаматрицалар алгебралари асосида симметрик ва носимметрик криптотизимлар яратиш усуллари ва алгоритмлари // Состояние и перспективы развития связи и информационных технологий Узбекистана: Доклады и тезисы междунар.конференции 11-12 мая 2005 г. Ташкент, 2005. – С. 50-51.

54. Хасанов Х.П. Мавжуд криптоалгоритмларни параметрлар алгебраси асосида такомиллаштиришнинг умумий усули // Информационная безопасность в сфере связи и информатизации: Тезисы докл. респ. сем. 24 ноября 2005. – Ташкент, 2005. – С. 22-24.

55. Хасанов Х.П. Криптографические системы на основе односторонних функций диапреобразования // Международная научно-практическая конференция. «Актуальные проблемы использования электронной цифровой подписи». Ташкент, 24-25 мая 2006 г. Доклады и тезисы. – Ташкент, 2006. – С. 54-59.

56. Хасанов Х.П. Криптографические системы на базе эллиптических кривых с параметром Ахборот-коммуникациялар: Тармоқлар – Технологиялар – Ечимлар. – Т.: №4, 2008.

57. Алгоритмические основы эллиптической криптографии / Болотов А.А. Гашков С.Б. Фролов А.В., Часовских А.А. – Москва МЭИ, 2000. – 100 с.

58. Элементарное введение в эллиптическую криптографию: алгебраические и алгоритмические основы / Болотов А.А. Гашков С.Б. Фролов А.В., Часовских А.А. – Москва МЭИ, 2006. – 328 с.

59. Асимметричная криптография на эллиптических кривых // Open PGP в России. – http: //www.pgpru.com.

60. Харин Ю.С., Берник В.И., Матвеев Г.В., Агиевич С.Г. «Математические и компьютерные основы криптологии» ООО «Новое знание» 2003 г. 381 стр.

61. Василенко О.Н. Теоретико-числовые алгоритмы в криптографии. – М., МЦНМО, 2003. – 328 с.

62. «Криптографик тизимларни криптотаҳлиллашнинг истиқболли усулларини ишлаб чиқиш ва уларни тадқиқ этиш» мавзуси бўйича бажарилган илмий-тадқиқот ишининг 1-босқич ҳисоботи. – ЎзААА «UNICON.UZ» ДУК, Тошкент, 2009.

63. Кобец А.М. Подмена подписанного документа в новом американском стандарте ЭЦП ECDSA// http: www.bugtrag/ru.

64. Горбенко И.Д., Збитнев С.И., Поляков А.А. Криптографические преобразования в группах точек эллиптических кривых методом Полларда // Радиотехника: Всеукр. межвед. научно-техн. сб. 2001. Вып. 119.

65. Горбенко И.Д., Збитнев С.И., Поляков А.А. Криптоанализ криптографических преобразований в группах точек эллиптических кривых методом Полларда // Харьковский государственный технический университет радиотехники.

66. Горбенко И.Д., Балагура Д.С. Схемы направленного шифрования в группах точек на эллиптических кривых //Харьковский государственный технический университет радиотехники.

67. ISO/IEC 14888-3:2006. Information technology – Security techniques – Digital signatures with appendix.

68. ГОСТ Р 34.10-2001. Информационная технология. Криптографическая защита информации. Процессы формирования и проверки электронной цифровой подписи.

69. ДСТУ 4145-2002. Информационные технологии. Криптографическая защита информации. Цифровая подпись, основанная на эллиптических кривых. Формирование и проверка // Научно-практический семинар. – Киев, 2003. – bezpeka.org/ru/activ.html.

70. Акбаров Д.Е., Хасанов П. Ф., Ахмадалив Ш.Ш. Параметрли алгебра амалларидан фойдаланиб мавжуд ҳисоблаш мураккабликлари асосида янги асимметрик алгоритмлар яратиш усуллари //Инфокоммуникации: Сети-Технологии-Решения, 1(9)/2009, с. 31-35.

71. Ростовцев А.Г., Маховенко Е.Б. Теоретическая криптография. НПО «Профессионал», Санкт-Петербург. 2004г. - 478 стр.

72. Ғаниев С.К., Каримов М.М., Ташев К.А. Ахборот хавфсизлиги. Ахборот-коммуникацион тизимлар хавфсизлиги. Ўқув қўлланма. Т., “Aloqachi”. 2008, 382бет.

73. D. Hankerson, A. Menezes, S. Vanstone Guide to Elliptic Curve Cryptography. Springer-Verlag New York, Inc. 2004.

74. ГОСТ Р 34.11-94. Государственный Стандарт Российской Федерации. Информационная технология. Криптографическая защита информации. Функция хэширования.

75. IEEE P 1363, Standard Specifications for Public-Key Cryptography. February. 2000.

76. Акбаров Д.Е., Ахмедова О.П. Генерация стойких ключей для симметричных блочных алгоритмов шифрования. //Кимёвий технология назорат ва бошқарув, 5/2008, с. 29-32

MUNDARIJA

Akbarov Davlatali Yegitaliyevich,
Xasanov Po‘lat Fattoxovich,
Xasanov Xislat Po‘latovich,
Axmedova Oydin Po‘latovna,
Xolimtayeva Iqbol Ubaydullayevna

KRIPTOGRAFIYANING MATEMATIK ASOSLARI

(O‘quv qo‘llanma)

Toshkent – «Aloqachi» – 2018

Muharrir:	M.Mirkomilov
Tex. muharrir:	A.Tog‘ayev
Musavvir:	B.Esanov
Musahhiha:	F.Tog‘ayeva
Kompyuterda sahifalovchi:	G.Tog‘ayeva

Nashr.lits. AI №176. 11.06.11.
Bosishga ruxsat etildi: 11.12.2018. Bichimi 60x841 /16.
«Timez Uz» garniturasi. Ofset bosma usulida bosildi.
Shartli bosma tabog‘i 12,5. Nashr bosma tabog‘i 12,0.
Adadi 100. Buyurtma № .

«Nihol print» Ok da chop etildi.
Toshkent sh., M. Ashrafiy ko‘chasi, 99/101.