ЎЗБЕКИСТОН АЛОҚА ВА АХБОРОТЛАШТИРИШ АГЕНТЛИГИ

«UNICON.UZ» - Фан-техника ва маркетинг тадқиқотлари маркази
давлат унитар корхонаси

КРИПТОГРАФИЯНИНГ МАТЕМАТИК АСОСЛАРИ

Ўқув қўлланма

Тошкент 2010

УДК 681.3

Акбаров Давлатали Егиталиевич, Хасанов Пўлат Фаттохович, Хасанов Хислат Пўлатович, Ахмедова Ойдин Пўлатовна

(т.ф.д., профессор П.Ф. Хасанов таҳрири остида)

Криптографиянинг математик асослари – Тошкент, 2010 – 210 бет

Ушбу ўқув қўлланмада криптография тарихи, криптографиянинг асосий математик тушунчалари, таърифлари, теоремалари ҳамда симметрик ва носимметрик криптографик алгоритмларнинг математик асослари баён этилган.

Ўқув қўлланмада параметрли функциялар ва уларнинг асосий хоссалари, диаматрицалар алгебраси ва параметрли эллиптик эгри чизиқли функциялар ҳамда улар асосида ишлаб чиқилган криптоалгоритмлар келтирилган.

Ушбу ўқув қўлланма ахборот хавфсизлиги ва криптография йўналишида таълим олаётган магистрлар учун мўлжалланган. Шунингдек ушбу ўқув қўлланмадан ахборот хавфсизлиги йўналишида бакалаврлар тайёрлаш жараёнида ҳамда криптография йўналишида илмий-тадқиқот олиб бораётган аспирант-тадқиқотчилар, илмий ходимлар ва соҳа мутахассислари фойдаланишлари мумкин.

МУНДАРИЖА

ҚИСҚАРТМАЛАР

1.	AES (Advanced Encryption Standard) –	АҚШнинг маълумотларни шифрлаш стандарти.
2.	АҚШ –	Америка Қўшма штатлари.
3.	ГОСТ 28147-89 –	Россия Федерациясининг маълумотларни шифрлаш стандарти.
4.	ГОСТ Р 34.10–94 –	Россия Федерациясининг дискрет логарифмлашга асосланган электрон рақамли имзо стандарти.
5.	ГОСТ Р 34.10-2001 –	Россия Федерациясининг эллиптик эгри чизиқда дискрет логарифмлашга асосланган электрон рақамли имзо стандарти.
6.	DES (Data Encryption Standard) –	АҚШнинг маълумотларни шифрлаш стандарти.
7.	DSA (Digital Signature Algorithm) –	АҚШнинг дискрет логарифмлашга асосланган электрон рақамли имзо алгоритми.
8.	EC-DSA-2000 (Elliptic Curve Digital Signature Algorithm) –	АҚШнинг эллиптик эгри чизиқда дискрет логарифмлашга асосланган электрон рақамли имзо алгоритми.
9.	EC-KCDSA –	Кореянинг эллиптик эгри чизиқда дискрет логарифмлашга асосланган электрон рақамли имзо алгоритми.
10.	EC-GDSA –	Германия Федератив Республикасининг эллиптик эгри чизиқда дискрет логарифмлашга асосланган электрон рақамли имзо алгоритми.
11.	EKUB –	Энг катта умумий бўлувчи.
12.	FEAL (Fast Data Encryption Algorithm) –	Япония маълумотларни шифрлаш алгоритми.

13.	IDEA (International Data Encryption Algorithm) –	Халқаро маълумотларни шифрлаш алгоритми.
14.	КРОМ –	Калитларни рўйхатга олиш маркази.
15.	NIST (National Institute of Standards and Technology) –	Стандартлар ва технологиялар миллий институти
16.	МША –	Маълумотларни шифрлаш алгоритми.
17.	ПТКК –	Псевдотасодифий кетма-кетлик.
18.	RSA –	Райвест-Шамир-Адлеман алгоритми.
19.	XOR –	2 модул бўйича қўшиш.
20.	O’z DSt 1092:2005, O’z DSt 1092:2009 –	Ўзбекистоннинг даража параметри муаммоларининг мураккаблигига асосланган электрон рақамли имзо бўйича давлат стандартлари.
21.	ЭРИ –	Электрон рақамли имзо.
22.	ЭРИА –	Электрон рақамли имзо алгоритми.
23.	ЭЭЧ –	Эллиптик эгри чизиқ.

КИРИШ

Ахборот ва телекоммуникация технологияларининг жадал суръатлар билан ривожланиб бориши турли манбалардан тез ва осон йўл билан ахборот олиш имкониятларини оширди. Давлат муассасалари, тижорат корхоналари ва алоҳида шахслар ахборотни электрон шаклда яратиб сақлай бошладилар. Тармоқ орқали ахборот узатиш бир онда юз бериши, уни сақлаш эса ихчам жой эгаллаши, бой маълумотлар базаларидан самарали фойдаланиш имкониятлари кенгая бориши ахборот миқдорининг жадал суръатлар билан ўсишига олиб келди. Илм-фан, таълим, ишлаб чиқариш, бошқарув, тижорат ва кўпгина бошқа соҳалар учун яхлит ахборот энг қимматли мулкдир [1-2].

Йигирма биринчи аср ахборотлаштириш асри эканига тобора кўпчилик ишонч ҳосил қилмоқда. Бу албатта оммавий ахборот ва ҳамма билиши мумкин ва зарур бўлган ахборот ҳақида гап борганда ўта ижобий ҳодиса. Лекин конфиденциал ва ўта махфий ахборот оқимлари учун замонавий ахборот-коммуникация технологиялари қулайликлар билан бир қаторда янги муаммоларни ўртага қўймоқда. Ахборот базаларида сақланадиган ва телекоммуникация тизимларида айланаётган ахборот хавфсизлигига таҳдид кескин ошди. Кейинги вақтда, айниқса, Интернет пайдо бўлгандан бошлаб, ахборот ўғирлаш, ахборот мазмунини бузиб қўйиш, эгасидан изнсиз ўзгартириб қўйиш, тармоқ ва серверлардан берухсат фойдаланиш, тармоққа тажовуз қилиш, аввал қўлга киритилган узатмаларни қайта узатиш, хизматдан ёки ахборотга дахлдорликдан бўйин товлаш, жўнатмаларни рухсат этилмаган йўл орқали жўнатиш ҳоллари кўпайди.

Натижада ахборот хавфсизлиги муаммоси Ўзбекистон Республикаси учун ҳам долзарб муаммога айланди. Бу ўз навбатида криптология фанини ривожлантириш вазифаларини долзарб муаммолар қаторига қўйди, чунки ҳозирги кунда бу йўл ахборот хавфсизлигини таъминлаш соҳасида асосий йўлдир.

Ахборотни муҳофаза қилиш масалалари билан *криптология* фани шуғулланади. Кейинги охириги йилларда криптология йўналишини ривожлантиришга давлатимиз томонидан катта аҳамият берилмоқда. Ўзбекистон Республикаси Президенти И. А. Каримовнинг 2007 йил 3 апрелда қабул қилган «Ўзбекистон Республикасида ахборотнинг криптографик ҳимоясини ташкил этиш чора-тадбирлари тўғрисидаги» ПҚ-614–сон қарори шулар жумласидандир. Мазкур қарорнинг асосий вазифаларидан бири ахборотнинг криптографик муҳофазаси соҳасида юқори малакали кадрларни тайёрлашдан иборат. Бунинг учун криптография йўналишида давлат тилида таълим олаётган талабалар, аспирант-тадқиқотчилар ва илмий ходимлар учун мўлжалланган ўқув қўлланмалар, дарсликлар, услубий қўлланмалар ва китоблар ишлаб чиқиш муҳим аҳамият касб этади.

Тақдим этилаётган ўқув қўлланма ана шу соҳада бажарилган ишлардан бири ҳисобланиб, у “Криптография ва криптотаҳлил” мутахассислигининг ўқув таълим стандарти ва ўқув дастурига мувофиқ ишлаб чиқилди.

Ушбу ўқув қўлланма ахборот хавфсизлиги ва криптография йўналишида таълим олаётган магистрлар учун мўлжалланган. Шунингдек ушбу ўқув қўлланмадан ахборот хавфсизлиги йўналишида бакалаврлар тайёрлаш жараёнида ҳамда криптография йўналишида илмий-тадқиқот олиб бораётган аспирант-тадқиқотчилар, илмий ходимлар ва соҳа мутахассислари фойдаланишлари мумкин.

1. КЛАССИК ШИФРЛАР ВА АСОСИЙ ТУШУНЧАЛАР

1.1. Таърифлар ва атамалар

Қадим замонлардан бери инсон мўъжизалар, сирли воқеа ва ҳодисалар сабаби ҳамда моҳияти ҳақида ахборот олишга интилган. Ахборот инсон тили ва ёзувида ўз аксини топади. Дастлабки ёзувлар ўзига хос бўлган криптографик тизим бўлиб, қадимги жамоаларда уларни фақат нуфузли шахсларгина тушунишган. Қадимий Миср ва Ҳиндистонда мавжуд бўлган илоҳий китоблар бунга мисол бўла олади. Бундан 4000 йил аввалги даврга оид энг қадимий шифрматн Мессопатамия қазилмаларида топилган. Унда лойдан ишланган тахтачада ўймакор ёзувда тижорат сири – кулолчилик буюмларини глазурлаш рецепти ёзилган. Қадимий Мисрда шифрланган диний матнлар ва тиббий рецептлар ҳам мавжуд бўлган.

Криптология (грекчада *kryptos* - “сирли” ва *logos* -“хабар”) деганда алоқа хавфсизлиги ҳақидаги фан тушунилади. У алоқа каналлари орқали ахборотнинг хавфсизлигини таъминлаб сақлаш ҳамда узатиш тизимларини яратиш ва таҳлиллаш тўғрисидаги фандир. Криптология икки илмий ирмоққа ажралади. Булар криптография ва криптотаҳлилдир [1-10].

Криптография ахборот алмаштириш тамойиллари, восита ва усуллари билан шуғулланадиган фан соҳаси бўлиб, унинг мақсади ахборот мазмунидан берухсат эркин фойдаланишдан муҳофазалаш ва ахборотни бузишнинг олдини олиш ҳисобланади.

Криптотаҳлил шифрни ёки ҳар қандай бошқа шаклдаги криптография объектининг сирини очиш санъати ва илми бўлиб, калитни билмасдан туриб шифрланган матндан дастлабки матнни олиш ёки дастлабки матн ва шифрланган матн бўйича калитни ҳисоблаш жараёнидир.

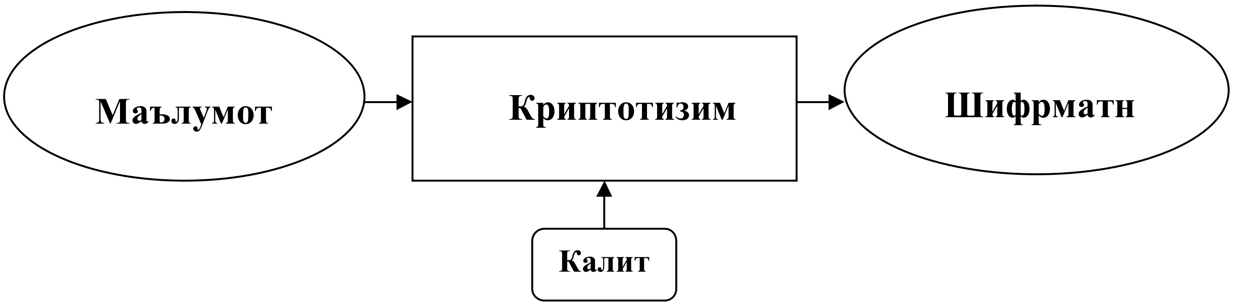
Криптотаҳлил усуллари тарихи криптография тарихи билан эгиздир.

Калитдан фойдаланган ҳолда алоҳида қоидалар бўйича очиқ (дастлабки) маълумотлар тўпламини шифрланган маълумотлар тўпламига алмаштириш учун амалга ошириладиган қайтар алмаштиришлар мажмуи *шифр* деб аталади.

Дастлабки очиқ матнни унинг маъносини беркитиш мақсадида шифрланган маълумотга ўгириш натижаси *шифрматн* (шифрмаълумот) деб аталади.

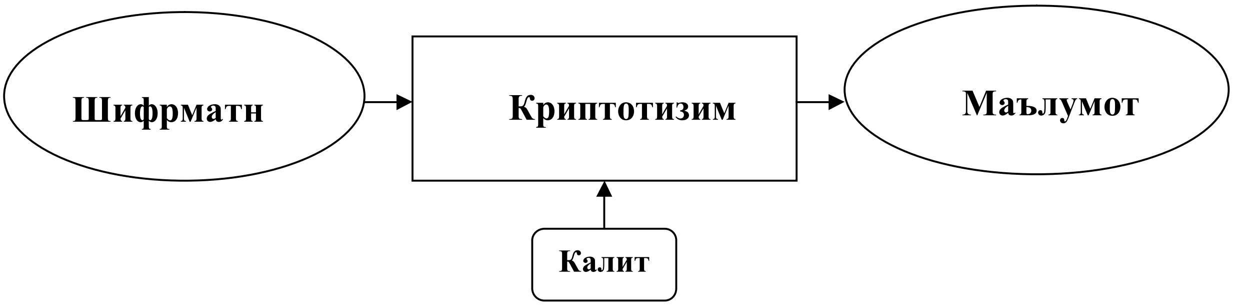
Кенг маънода *ахборотни шифрлаш* деганда шифрматнга ўгириш жараёни тушунилади.

Дастлабки маълумотлар (ахборотлар)ни шифр (калит) ёрдамида шифрланган маълумотларга алмаштириш жараёни *маълумотларни шифрматнга ўгириш (ёки тор маънода шифрлаш) жараёни* дейилади (1-расм).



1-расм. Маълумотларни шифрматнга ўгириш жараёни

Шифрматнга ўгирилган маълумотларни шифр (калит) ёрдамида дастлабкисига алмаштириш *маълумотларни дастлабки матнга ўгириш* (ёки тор маънода дешифрлаш) жараёни дейилади (2-расм).



2-расм. Маълумотларни дастлабки матнга ўгириш жараёни

Параметрларнинг бир қисми махфий ҳолда бўлган криптографик алгоритм бўйича маълумотларни алмаштириш *криптографик ўзгартириш* дейилади.

Криптология бирор чекли сондаги алифбо белгиларининг кетма-кетлиги орқали ифодаланган маълумотни ва унинг ўзгаришлари (акслантиришлари) билан боғлиқ жараёнларни тадқиқ қилади. Криптографик тизимлар математиканинг: тўпламлар ва функциялар назарияси, алгебра, дискрет математика, сонлар назарияси, эҳтимоллар назарияси, ҳақиқий ва комплекс ўзгарувчи функциялар назарияси, мураккаблик назарияси, ахборотлар назарияси ва шу каби бўлимларга тегишли бўлган математик моделлар асосида яратилади ва тадқиқ этилади. Алоҳида олинган криптографик моделларнинг математик асослари билан чуқурроқ танишишни истаганлар криптографияга оид адабиётлар рўйхатида келтирилган манбалардан фойдаланишлари мумкин.

Математик модел бошланғич кузатув, фикр ва мулоҳазалар асосида ўтказилган тажрибалар натижаларини солиштириш ҳамда тадқиқ қилинаётган объект хусусиятларини белгиловчи параметрларнинг боғлиқлиги қонуниятларини ифодаловчи тенглик, тенгсизлик ва тегишлилик муносабатлари билан аниқланади. Илмий тадқиқ қилинаётган объектлар математик моделларининг мослик даражаси - адекватлиги улар билан боғлиқ бўлган жараёнларни қанчалик тўлиқ ва аниқ ифодаланиши билан белгиланади. Криптографик алгоритмлар асосини ташкил этувчи акслантиришларнинг моделлари асосан хусусиятлари ва хоссалари жиҳатидан бир-бирига боғлиқ бўлмаган кўп ўзгарувчили дискрет функцияларнинг чекли сондаги кетма-кетлигидан иборат мажмуани ташкил этади. Бу функциялар параметрлари очиқ маълумот, калит ва акслантиришлар оралиқ натижалари блокларини ўз ичига олади.

Очиқ маълумотлар *алифбо* деб аталувчи чекли сондаги белгилар тўплами элементларининг маъно берувчи тартибли кетма-кетлигидан иборат [11-13]. Очиқ маълумотни ташкил этувчи алифбо белгилари ёки белгилар бирикмаларини акслантиришлар натижасида ҳосил қилинган шифрматн ҳам ўз навбатида бирор чекли сондаги белгилар тўпламидан иборат бўлиб, бу белгилар тўплами *шифрматн алифбосини* ташкил этади. Шифрлаш жараёнида бажариладиган акслантиришлар очиқ маълумот алифбоси белгилари тўплами элементларини шифрматн алифбоси белгилари тўплами элементларига бирор амал бажариш орқали алмаштирилади, яъни тўпламлар ва уларнинг элементлари устида амаллар бажарилади. Шунинг учун ҳам берилган тўпламда аниқланган амал ва тўпламнинг бу амал билан боғлиқ хоссаларини ўрганиш математиканинг асосларини ташкил этгани каби криптология фанининг математик асосларига ҳам пойдевор бўлишига шубҳа йўқ. Тўплам элементлари устида бирор амал аниқлаш билан бу тўпламда шу амал билан боғлиқ тизим ёки тузилма аниқланади. Тўпламда аниқланган амаллар сони ва уларнинг хоссаларига кўра тўплам элементлари *группа*, *ҳалқа*, *майдон* ва шу каби *алгебраик тизим (тузилма, структура)лар* деб аталувчи тизимларни ташкил этади. Бу алгебраик тизимлар бугунги кунда математиканинг турли бўлимларида атрофлича ўрганилган бўлиб, бу ўрганишларнинг илмий натижалари криптология масалалари тадқиқини, ечиш усулларини ва тадбиқини илмий асослаш воситасининг математик моделлари негизини ташкил этади.

Криптографик алгоритмлар акслантиришларининг математик моделлари асосларини чуқур ва кенг илмий ўрганиш мавжуд алгоритмларни таҳлил қилиш ва мақсадли такомиллаштиришни, криптобардошли ва амалий қўлланиши самарали бўлган янги алгоритмлар яратиш каби имкониятларни вужудга келтиради.

1.2. Криптография тарихи

Минг йилликлар давомида криптографиядан давлат қурилишида, ҳарбий ва дипломатия алоқасини муҳофазалашда фойдаланиб келинган бўлса, ахборот асрининг бошланиши билан криптология жамиятда, хусусий секторда фойдаланиш учун ҳам зарур бўлиб қолди [14-15]. Қарийб 35 йилдан буён криптологияда кенг миқёсда очиқ тадқиқотлар олиб борилмоқда. Ҳозирги кунда конфиденциал ахборот (масалан, юридик ҳужжатлар, молиявий, кредит ставкалари тўғрисидаги ахборотлар, касаллик тарихи ва шунга ўхшаш)ларнинг талай қисми компьютерлараро одатдаги алоқа каналлари орқали узатилмоқда. Жамият учун бундай ахборотнинг конфиденциаллиги ва асл ҳолда сақланиши заруратга айланган.

Криптография тарихини шартли равишда 4 босқичга бўлиш мумкин [1, 3-6]:

1. Дастлабки криптография.
2. Формал криптография.
3. Илмий криптография.
4. Компьютер криптографияси, бу босқич криптографияда симметрик ва носимметрик криптотизимлар бўйича икки илмий йўналиш юзага келиши билан характерланади.

1.2.1. Дастлабки криптография даври

Дастлабки криптография (XVI аср бошигача) босқичи учун содда усуллардан фойдаланиб, шифрланган матн мазмунидан бегоналарни чалғитиш хосдир. Бу босқичда ахборотни муҳофаза қилиш учун криптография оиласига мансуб, аммо айнан бўлмаган кодлаш усулларидан фойдаланилган. Фойдаланилган шифрларнинг кўпчилиги бир алифболи ўрнига қўйиш ёки кўп алифболи ўрнига қўйишга асосланган.

Дастлабки криптография даврига оид шифрлар ҳақида гап борганда Европа фани тарихидан ўрин олган Плутарх, Аристотель (милоддан аввалги IV аср), Юлий Цезарь (милоддан аввалги 100-44 йй.), Р. Бекон (1214-1294 йй.) шифрларини айтиб ўтиш жоиз [1-10].

Дастлабки шифрлаш мосламаларидан бири сифатида ғалтак (скитала)дан фойдаланилган. Цилиндрсимон ғалтакка зич бир қават ўралган энсиз папирус лентасига дастлабки матн ҳарфлари цилиндр ўқи бўйлаб ёзилиб шифрматн шакллантирилган. Лента ғалтакдан ечиб олиниб қабул қилувчига жўнатилган. Қабул қилувчи шифрматнли лентани шифрлаш ғалтаги билан бир хил ғалтакка ўраб дастлабки матнни ўқиган. Ғалтак ўлчамлари махфий шифрлаш калити вазифасини ўтаган. Бундай шифр мосламасидан эрамизгача V асрда бўлиб ўтган Спартанинг Афинага қарши уруши даврида фойдаланилган. Шифрлаш ғалтаги ўлчамларини топиш ғояси Аристотелга тегишлидир. У бунинг учун узун конус олиб, унга асосидан бошлаб конус учигача шифрматнли лента ўралганда конуснинг бирор қисмида ўқиладиган матн ҳосил бўлишига қараб ғалтак ўзаги диаметрини аниқлаган [1-10].

Қадим замонларда атбаш деб аталган шифр маълум бўлган, ундан баъзан муқаддас иудей матнларини шифрлашда фойдаланилган. Шифрматн яратишда дастлабки матнга тегишли алифбонинг биринчи ҳарфи охиргисига, иккинчи ҳарфи ундан аввалгисига ва ҳ.к. алмаштирилган. Тўла баёни сақланган шифрлардан бири Цезарь шифри бўлиб, у ҳам атбаш шифри оиласига мансубдир. Юлий Цезарь ўз шифридан Цицерон (милоддан аввалги 106-43 йй.) билан ахборот алмашишда фойдалангани маълум [1, 5]. Турли даврларда бу тизимнинг турли русумларидан фойдаланиб келинган. Дастлабки матннинг қандай берилиши аҳамиятга эга эмас. Цезарь усулида шифрлаш дастлабки матнга тегишли алифбо ҳарфи ўрнига шифрлаш калити *k* қадамга сурилган ўринда жойлашган алифбо ҳарфини қўйиш асосида амалга оширилади (3-расм). Бунда суриш алифбо ҳарфлари сони *26* га тенг бўлган модуль бўйича бажарилади. Алифбо ҳарфлари бошидан охири томон, охиридан қайта бош томондан бошлаб даврий равишда суриб борилади.

Масалан, *k=3* ҳол учун қуйидаги кўринишга эга бўламиз:

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**

3-расм. Цезарь усулида шифрлаш

Бу ҳолда дастлабки матн ODAMни шифрлаш натижаси RGDP бўлади.

Цезар тизимининг калит майдони *26* та сон: *0,1,2,...,25* дан иборат. k калитли E_k шифрлаш алгоритми алифбодаги ҳарфларни k қадам билан ўнгга силжитишни ўз ичига олади. Мос равишда шифрматн D_k ни очиш алгоритми алифбодаги ҳарфларни k қадам билан чапга силжитиш натижасини беради.

Цезарь тизими ва унга ўхшаш тизимларни ҳозирги замон ўқувчиси учун ҳарфларни алифбодаги тартиб рақами билан алмаштириб сонлар устида модуль бўйича қўшиш амали ⊕ ёрдамида тушунтириш осон. Цезарь тизимига мувофиқ, шифрматн ҳосил қилишда дастлабки матннинг ҳар бир α ҳарфи шифрматнда $sh\alpha \equiv \alpha \oplus k(mod26)$га айланади. Дастлабки матн ҳарфи $\alpha \equiv sh\alpha \oplus k(mod26)$ кўринишда тикланади. Таъкидлаш жоизки, модуль арифметикасида мазкур қўшиш амали замонавий шифрларда ҳам энг кўп фойдаланиладиган амалдир.

Милоддан аввалги II асрда қадимги Грецияда “Полибий квадрати” (4-расм) деб аталмиш шифр машҳур бўлган. Шифрлаш жадвали *5* та сатр ва *5* та устундан тузилган бўлиб, улар *1* дан *5* гача рақамлар билан белгиланган ва жадвал хоналарида *25* та ҳарф жойлашган.

	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

4-расм. Полибий квадрати

Шифрматн дастлабки матнга тегишли жадвал хонасидаги ҳарфларни сатр ва устун рақамлари жуфтлиги билан алмаштириш натижасида ҳосил этилган. Шифрлаш жадвалида ҳарфларнинг жойлашиш тартиби шифрлаш калити вазифасини ўтаган. Масалан, юқорида келтирилган жадвал бўйича I, R ва M ҳарфлар ифодаси мос равишда BD, DB ва CB бўлади. Кириш хабари ODAM га мос шифрматн CDADAACB кўринишда бўлади.

Шифрматнни дастлабки матнга ўгириш сатр ва устун рақамлари жуфтлигини шифрлаш жадвали ҳарфига алмаштиришдан иборат бўлган.

1.2.2. Формал криптография даври

Формал криптография (XV аср охири – XX аср бошлари) босқичи қўлда криптотаҳлиллашга бардошли ва формаллаштирилган шифрлар пайдо бўлиши билан характерланади. Криптография тарихининг бу даврида Леон Батиста Альберти (1404-1472 йй.), Иоганн Трисемус (1462-1516 йй.), Джиролано Кардоно, Кардинал Ришелье, Джованни Батиста Порт, Блез де Виженер (1523-1596 йй.), Франсуа Виет (1540-1603 йй.), Френсис Бекон (1562-1626 йй.), Карл Фридрих Гаусс (1777-1855 йй.), Огюст Керкхофф (1835-1903 йй.) ва Г.С.Вернамлар [1, 3, 8, 16-17] ижодиёти алоҳида чуқур из қолдирган.

Итальян архитектори Леон Батиста Альберти муҳим ҳисса қўшганлардан бири ҳисобланади. У кўп алифболи ўрнига қўйиш усулини биринчилардан бўлиб таклиф этган. Бу шифр XVI аср дипломати Блейз де Виженер номи билан аталган. Унинг 1466 йилдаги «Шифрлар ҳақида трактат» асари криптологияга оид дастлабки илмий асар ҳисобланади [1, 3-8].

Немис аббати Иоганн Трисемус томонидан 1508 йилда нашр қилинган «Полиграфия» рисоласи ўша вақтда маълум бўлган шифрлаш алгоритмлари умумлаштирилган ва тўпланган дастлабки асар ҳисобланади. Иоганн Трисемус муҳим иккита янги шифрлаш усулини таклиф этган: булар Полибий квадратини тўлдириш усули (дастлабки катаклар осон эсда қоладиган калит сўзи ёрдамида, бошқалари эса алифбонинг қолган ҳарфлари билан тўлдирилади) ва биграмма, яъни ҳарфларни жуфтлаб шифрлаш усулидир.

Шифр муаллифлари орасида давлат бошлиқлари ҳам бўлганлиги эътиборга лойиқ. Милоддан аввалги биринчи асрда Юлий Цезарь шифри машҳур бўлган бўлса, XIX аср бошларида АҚШ давлат секретари, кейинчалик президент Томас Жефферсон ўз дискли шифратори билан танилган. Жефферсон шифратори ёғоч цилиндрдан кесиб тайёрланган бир-биридан мустақил равишда умумий ўқда айланувчан 36та дискдан таркиб топган бўлиб, ҳар бир дискнинг ён сиртида инглиз алифбоси ҳарфлари ихтиёрий ва турли тартибда ўйиб ёзилган. Цилиндр ён сиртида ўққа параллел бўлган чизиқ ажратилган. Шифрматн шакллантиришда дастлабки матн 36 символли гуруҳларга бўлиниб, гуруҳнинг 1-ҳарфи биринчи дискнинг ажратилган чизиқда биринчи диск ҳолати билан, иккинчиси – иккинчи диск ҳолати билан ва ҳ.к. белгиланган. Шифрматн ажратилган чизиққа параллел бўлган ихтиёрий чизиқда ётган ҳарфлар кетма-кетлиги сифатида шакллантирилган. Дастлабки матнни тиклаш бунга тескари тартибда бажарилган: дискларни айлантириш натижасида шифрматн ҳарфлари ажратилган чизиқ бўйлаб жойлаштирилган. Дастлабки матн ўзаро параллел чизиқлар орасидан маънога эга матн ҳосил қилувчи чизиқда жойлашган.

Аввал маълум бўлган кўп алифболи алмаштиришга асосланган Жефферсон шифратор калитининг қисмлари сифатида ҳарфларнинг ҳар бир дискда ва дискларнинг умумий ўқда жойлашиш тартибларидан фойдаланилган. Фойдаланилиши мумкин бўлган калитларнинг умумий сони $(26!)^{36}$га тенг. Шифрнинг бундай юксак криптобардошлиликка эга эканлиги XX асрга келиб тан олинган ва АҚШ армиясида фойдаланиш учун қабул қилинган [1, 10, 12].

Т. Жефферсон ўз шифрига юқори даражада эҳтиёткорлик билан ёндашиб, уни чуқур таҳлил этиш лозим деб ҳисоблаган ва ўз амалиётида анъанавий кодлардан ва Виженер типидаги шифрлардан фойдаланишда давом этган. Унинг шифри XX асрнинг 20-йилларида тўртинчи бор қайта кашф этилган. Т. Жефферсон ихтиросининг асосий натижаси бўлиб, XX асрда дастлабки мураккаб электромеханик шифраторлар юзага келиши учун замин яратди. У америка шифр мактабининг отаси деб бежиз тан олинмаган.

XIX аср криптографияси тараққиётига сезиларли ҳисса қўшганлардан бири Пруссия армияси офицери Фридрих Казисскийдир [1-6]. У 1863 йилда 100 бетли “Махфий ёзув ва шифрни калитсиз очиш санъати” китобини чоп этган. Криптография соҳасида машҳур тарихчи Д. Кан “Казисский криптографияда инқилоб қилган” деб ёзган [1-10]. Асосан мазкур китоб Виженер шифри синфига оид қисқа даврий гаммалаш шифрларини калитсиз очиш усулларига бағишланган. Бундай шифрдан фойдаланилганда дастлабки матнда даврий такрорланувчи ҳарфий бирикма калитга оид дастлабки гамманинг даврий давомлари билан мос келиб, шифрматнда шунга мос ҳарфий бирикмалар ҳосил этади. Бундай такрорланишлар шифрни калитсиз очишда жуда қўл келган.

XIX аср охирига келиб криптография аниқ фан сифатларига эга бўла бошлади ва у ҳарбий академияларда ўрганила бошланди.

XIX асрда яратилган шифрлар орасида Виженер шифри оиласига оид Сен-Сир Франция ҳарбий-дала академияси шифри - “Сен-Сир чизғичи” машҳур бўлган. Бундай шифратор логарифмик чизғичга ўхшаш тузилган бўлиб, алифбо ҳарфлари босмаланган узун картон бўлаги шаклидаги қўзғалмас шкала қисмдан ва алифбо ҳарфлари икки қайта босмаланган тор картон бўлаги шаклидаги қўзғалувчан қисмдан иборат. Шифрлаш жараёни қўзғалувчан қисмни калитнинг 1-ҳарфи шкаланинг «А» ҳарфи остида жойлашув ҳолатига мос бўлгунча силжитишдан иборат. Бунда дастлабки матннинг 1-ҳарфини калитнинг шу ҳарфи билан алмаштирилади. Шу зайлда дастлабки матннинг 2-ҳарфи қўзғалувчан қисмни калитнинг 2-ҳарфи шкаланинг «А» ҳарфи остида жойлашув ҳолатига мос бўлгунча силжитиб у билан алмаштирилади ва ҳ.к. “Сен-Сир чизғичи” Виженер шифрининг содда механик қурилмаси бўлгани учун шифрловчилар меҳнатини осонлаштирган. Бу ғоя қўзғалувчан қисмда алифбо ҳарфларини ихтиёрий жойлаштириш орқали ўз ривожини топган ва криптобардошлиликнинг янада ошишига олиб келган. “Сен-Сир чизғичи”дан Германияда ҳам такомиллаштирилган шаклда фойдаланилган [1].

XIX аср охирида Франция бош вазири Леон Гамбетта шифр асбобларидан фойдаланишнинг ўрнига оддий алгебраик амаллардан фойдаланишни таклиф этган. Бунда матн ҳарфлари сонлар билан алмаштирилиб, алифбо ҳажмига тенг модуль бўйича қўшиш амалидан фойдаланилади. Замонавий Гамма шифри атамаси Гамбетта номидан келиб чиққанлиги эътиборга лойиқ.

Шу муносабат билан, шифрлар назариясида буюк ватандошимиз Муҳаммад ал-Хоразмийнинг алгебра фани ва алгоритм тушунчаси мустаҳкам ўрин олганини таъкидлаш ўринлидир [1].

Электротехника соҳасида фундаментал илмий асарлари билан машҳур бўлган Голландиялик йирик аллома Огюст Керхгофф XIX аср криптографияси тарихида ўз номини абадийлаштирган. У криптография билан бошланғич танишувни ҳарбий–дала телеграф шифрларидан бошлаб, 1880-йилларда 64 бетли “Ҳарбий криптография” китобини босмадан чиқарган. Китобда шифрга қўйиладиган қуйидаги умумий талаблар шакллантириб берилган:

- фойдаланиш осонлиги;
- ишончлилик (юқори криптобардошлилик);
- тезкорлик (шифрматнни шакллантиришда ва дастлабки манни тиклашда криптографик алмаштиришлар учун оз вақт сарф бўлиши);
- криптобардошлилик фақат шифрлаш калитига боғлиқ бўлиши.

Шифр, яъни криптографик алмаштиришлар алгоритми рақиб томонга маълум бўлганда ҳам юқори криптобардошлиликнинг таъминланиши талаб этилган. Шифр қурилмаси битта фойдаланувчи учун осон ва қулай бўлишга мўлжалланиши талаб этилган. Лекин иккинчи жаҳон уруши йилларида Германия қўшинларида тезкорликни таъминлаш мақсадида ҳар бир шифраторда учта фойдаланувчи хизмат кўрсатган эди. Мазкур талаблар бугунги кунда ҳам яратиладиган шифрлар учун мажбурий талаблар тўпламининг асосини ташкил этади.

Ноёб истеъдод эгаси Керхгофф икки соҳа - адабиёт ва фан бўйича илмий даражаларга эга бўлган, Голландия ва Франция ўқув юртларида таълим берган. Унинг криптотаҳлил соҳасидаги фаолияти Францияда юксак қадрланган. Д. Каннинг фикрича, биринчи жаҳон уруши арафасида Франция криптография дунёсида илғор ўринлардан бирини эгаллашида Керхгоффнинг ҳиссаси бор [1, 16]. Германия ўз навбатида асосий эътиборни асосан ҳарбий қуролларга қаратган ва бу бундан кейинги урушларда Германия учун қимматга тушган.

XIX аср криптографиясида инглиз алломаси, компьютер кашфиётчиси Чарльз Беббидж ёрқин сиймолардан бири бўлган. Инглиз олими Чарльз Беббидж механик калькуляторни ишлаб чиққан ва 1823 йилда уни қурган. Механик калькулятор буғ ёрдамида ҳаракатга келтирилган ва тўла автоматик бўлган ҳамда ичига ўрнатилган дастур орқали бошқарилган. Шуниси эътиборга лойиқки, унинг схемаси асосида қурилган илк компьютер “Энигма” (5-расм) иккинчи жаҳон уруши даврида немислар фойдаланган шифраторни нейтраллаш учун яратилиб, бу вазифани аъло даражада ҳал этиб берган эди. Ч. Беббидж ўзининг асосий эътиборини Виженер шифрига, гамма-даврасига қаратган ва XIX аср ўрталарида ўз шифрини яратган. Бироқ архив маълумотлари тадқиқотлари шуни кўрсатадики, Казисский 1863 йилда Ч. Беббидж шифрини қайта кашф этиб, тарихда шифр унинг номида қолган. Ч. Беббидж биринчи бўлиб шифрга оид асосий тушунчаларни жиддий математик тарзда шакллантирган, кўп алифболи шифрларни ечиш алгоритмини берган ва биринчилардан бўлиб алгебрадан фойдаланган. Дастлабки матнга боғлиқ калит – «хос калит»га асосланган шифрларни очиш ғояси ҳам унга тегишлидир.

5-расм. Энигма шифратори

XIX аср бошларида Чарльз Уитстон томонидан кашф қилинган Плейфер шифри кўп алифболи ўрнига қўйишнинг содда, лекин криптотаҳлилга бардошли усулларидан ҳисобланади. Такомиллаштирилган шифрлаш усулларидан бири бўлган «қўша квадрат» усули ҳам Уитстонга тегишли. Плейфер ва Уитстон шифридан биринчи жаҳон уруши бошлангунга қадар фойдаланилган, унинг криптотаҳлили қўлда бажарилиши қийин эди.

XX аср бошларида америкалик машҳур криптограф Уильям Фридман томонидан 1918 йилда тайёрланган 8 та маърузадан иборат «Ривербэн нашрлари» асари назарий криптографияга муҳим ҳисса бўлиб қўшилган. «Ривербэн нашрлари» биринчи жаҳон уруши даврида криптография ва криптотаҳлил хизматида тўпланган катта тажрибага асосланган эди. У ўз асарида криптография масалаларини ечишда эҳтимоллар назариясидан фойдаланиш самарали эканлигини намойиш қилган [1, 18-19].

Коммуникация соҳасида юзага келган ихтиролар ўз даврида яратилган шифрлар моҳияти ўзгариши билан узвий боғланган. Бунга америкалик Гильберт Вернамнинг криптографияни ривожланишига қўшган муҳим ҳиссаси мисол бўлади. Телеграф компаниясининг бўлғуси ходими 1917 йилда телеграф хабарларини автоматик шифрлаш ғоясини таклиф этган. Унинг моҳияти шундаки, дасталабки матн Бодо коди (беш белгили «импульс бирикмалари») кўринишида тасвирланади. Бу кодда масалан, «А» ҳарфи (++---) учун қоғоз лентада тешикчалар қатори қуйидагича кўриниш олади:

● ● · · ·

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

«+» тешикча борлигини, «-» унинг йўқлигини билдиради. Уни ўқишда беш тишли электромагнит ўқиш қурилмасидан фойдаланилган. Тўғри чизиқ бўйлаб (айланма) ҳаракат қилувчи лента тешикчалари кетма-кетлиги ток импульслари кетма-кетлигига айлантирилган.

Вернам шифрлашда электромеханик координаталар бўйлаб дастлабки матн белгиларига оид импульсларни махфий калит - гамма импульслари билан 2 модули бўйича қўшишни (замонавий математика тилида) таклиф этган. Шифрматнни дастлабки матнгга ўгиришда яна шу амалдан фойдаланилган. Вернам бу амалларни операторсиз автоматик тарзда амалга ошириш қурилмасини ҳам яратган. Шундай қилиб, шифрматн ҳосил қилиш ва узатиш жараёни бир пайтда бажариладиган «чизиқли шифрлаш»га, замонавий оқимли шифрларга асос солган. Бу алоқа тезкорлигини кескин оширган. Вернам шифри америкалик мумтоз криптограф Клод Шеннон томонидан мукаммал шифр назариясини асослаш учун база бўлиб хизмат қилганини эслаб ўтиш ўринлидир. Вернам шифри ҳаддан ташқари бардошли шифр ҳисобланади. Вернам ўзи математик-криптограф бўлмаса ҳам, шифр гаммаси шифрлашда қайтарилмаслигини талаб қилиб тўғри йўл тутганлиги ўз исботини топган. Унинг ғоялари катта ҳажмли хабарларни узатишда ахборотни ишончли муҳофазалашга оид янгича ёндашувларнинг юзага келишига сабаб бўлган.

Ўрта Осиё республикаларининг криптография тарихи формал криптографиянинг охириги йиллари (1900-1929 йиллар) ва илмий криптография даври (1930-1960 йиллар)да Россия криптография тарихининг таркибий қисми бўлганлигини эътиборга олмоқ лозим [1, 3].

Криптография асосан урушлар замонида ва терроризм авжига чиққан даврларда ҳал қилувчи аҳамиятга эга бўлган. Бу криптографияни ривожлантириш борасида кенг миқёсли тадбирлар амалга оширилишига туртки бўлган. Масалан, 1866 йил 4 апрелда Д.В. Каракозов томонидан рус подшоҳи Александр II га қарата ўқ отилгандан сўнг чор Россияси криптография хизматининг фаолиятида янги давр бошланган [1, 3].

XX аср бошларида юзага келган радиоалоқа армия қисмларида фойдаланиладиган шифрлар бардошлилигига бўлган талабни ошириб юборди, бу даврда рус криптография мактаби жаҳонда илғор мактаблар қаторига кўтарилган. Бир томондан инқилобчилар, иккинчи томондан чор жандармчилари орасида муросасиз тарафкашлик кураши авж олган. Бунда ахборот хавфсизлиги воситалари ҳал қилувчилардан бири бўлиб, устунлик то XX асрнинг 30 йилигача чор Россияси тарафдорларида бўлган.

Криптография тарихи бўйича биринчи асар [16] муаллифи Дэвид Каннинг ёзишича, Биринчи жаҳон уруши (1914-1917 йиллар)да рус армиясининг мағлуб бўлишига армияда фойдаланилган шифрлаш воситаларининг заифлиги сабаб бўлган. Рус армиясида фойдаланилган шифр тизими кўп алифболи шифр алмаштиришларга асосланган бўлса-да, шифртелеграммалар аслида битта алифбо билан шифрланган ҳарфлар гуруҳидан иборат бўлиб, криптобардошлилиги паст бўлган.

Биринчи жаҳон уруши бошида рус армияси учун калитларни бот-бот янгилашга мўлжалланган икки карра ўрин алмаштиришга асосланган мураккаб шифр яратилди. Аммо, эски шифрдан ҳам бир вақтда фойдаланиш тартибсизликларни вужудга келтириб, очиқ матндан фойдаланишгача бориб етган, бунда шифр операторларининг яхши тайёргарликдан ўтмагани панд берган.

1916 йилга келиб янги шифр билан барча ҳарбий қисмларни таъминлаш имконияти туғилди. Лекин, 1917 йил октябрь инқилоби Россия криптография хизматининг батамом издан чиқишига олиб келди. Кўпчилик юқори ихтисосли криптографлар ва криптотаҳлилчилар «оқлар» тарафида бўлган. Баъзилари хорижга қочиб кетганлар ва улар ўз хизматларини хорижий давлатларга таклиф этганлар ва у ерда Советларга қарши ишлаганлар. Масалан, код ва шифрлар бўйича инглиз ҳукумати мактабининг рус секцияси раҳбари Эрнест Феттерлейн революцияга қадар чор Россиясида етакчи криптотаҳличилардан бўлган ва Англияда совет дипломатик шифрларини бузиб очиш бўйича ихтисослаштирилган. У Советлар Россиясининг ҳар қандай шифрини ҳеч қандай қийинчиликсиз оча олар эди. Бу Совет Россияси халқаро муносабатларида йўқсиллар диктатураси раҳбарларининг ғирром ҳатти-ҳаракатларини ўз вақтида фош бўлишига, халқаро муносабатларнинг кескинлашувига олиб келган. Большевиклар тарафида бўлган кам сонли криптологлар ягона раҳбариятга ҳам эга бўлмаган. Шундай қилиб, 1920 йилларда Россияда ахборот муҳофазасини таъминлашга қодир криптологик марказ бўлмаган.

Формал криптографиянинг, умуман бутун криптография тараққиётининг юксак чўққиси бўлиб илк бора амалиётда фойдаланила бошланган 1917 йилда Эдвард Хеберн томонидан ишлаб чиқилган ва Артур Кирх томонидан такомиллаштирилган немис «Enigma» ротор шифрлаш машинаси тан олинган. Эдвард Хеберннинг криптографик жараёнларни механизациялаш борасида инқилобий тамойили ротор қурилмалар учун асос сифатида қабул қилинган. Немис Enigmaсидан бошқа яна АҚШнинг SIGABA, Буюк Британиянинг TYPEX, Япониянинг RED, ORANGE ва PURPLE қурилмаларидан ҳам фойдаланганлар.

АҚШда криптотаҳлил бўйича мутахассислар тайёрлаш Биринчи жаҳон уруши бошланишидан бир неча йил аввал бошланган. Улар дастлаб алоқа қўшинлари мактабида, кейинчалик ҳарбий разведка бошқармаси қошида ташкил этилган армия криптология мактабида тайёрланди.

XX асрнинг 1917 йил бошларида криптотаҳлил соҳасидаги энг катта ютуқлардан бири Германиянинг собиқ ташқи ишлар вазири Циммерман мактуби сифатида машҳур. Британия денгиз разведкаси томонидан трансатлантик кабелдан тутиб олинган махфий телеграмма матни АҚШ ҳукуматига топширилган. Унда Америка штатлари бўлган Техас, Нью-Мехико ва Аризонани Мексикага қўшиб олиш ҳақида Мексикадаги немис элчисига Мексика ҳукумати билан иттифоқ тузиш таклиф этилган. Тарихчиларнинг таъкидлашича, телеграмма шундай портлаш содир этганки, бунинг натижасида 1917 йил 6 апрелда Америка конгресси Германияга қарши уруш эълон қилган. Шундай қилиб, криптография *биринчи марта* ўзининг аҳамияти қанчалар муҳимлигини намойиш этган.

Немис ҳарбий кодларини ва шифрларини криптотаҳлил этиш мақсадида бу ишга армия криптология мактаби собиқ битирувчилари ва ўқитувчилари жалб этилган. Улар қаторидан XX аср АҚШ криптография тарихида ёрқин сиймолардан бири Уильям Фридман ҳам ўрин олган эди. Унинг рафиқаси ҳам криптограф эди. Эр-хотин Фридманлар ўзларининг фаолиятларини «Энигматология» («сирларни ўрганиш»)ни ўрганишдан бошлаганлар. Уильям Фридман АҚШ радиоразведка хизматининг бошлиғи сифатида фаолият кўрсатиб, армия кодлари ва шифрларини ишлаб чиқиш, душманнинг радио ва алоқа каналларидан узатилаётган хабарларини тутиб олиш, код ва шифрларни криптотаҳлил этиш, сирли ёзув соҳасида лаборатория тадқиқотларини ўтказиш билан шуғулланган [10].

1919 йилда таниқли инглиз криптографи, «Америка қора кабинети» китоби муаллифи Герберт Ярдли вертикал ўрнига қўйишга асосланган катта ҳажмдаги инглиз агентлиги шифрини очишга муваффақ (мушарраф) бўлди. Бу шифрхабар собиқ Совет Иттифоқи ҳаво йўли бўйлаб Латвияга қўнаётган немис аэропланидан қўлга киритилган. Шифрланган хатдан унинг муаллифи - Ғарбий Европанинг катта агентлик тармоғи ишига раҳбарлик қилувчи шахс экани аниқланган. Ҳужжатлар ичида «Дипломатик миссияларда жосусликка жалб этилган агентлар учун йўриқнома» ҳам бўлган. Дипломатик ёки ҳарбий шифрлардан фарқли равишда совет агентлик шифрларини очиш ҳоллари ҳам баъзида содир бўлиб турган [10].

«Қора кабинет» 1917 йилдан 1929 йилгача фаолияти даврида Европа ва Жанубий Америка давлатларининг 10 000 дан ортиқ телеграммалари фош этилган. Япон дипломатик код ва шифрларини фош этиш «Қора кабинет» фаолиятининг энг йирик муваффақияти ҳисобланади [10].

Россия криптография тарихида асосий ташкилий ишлар 1921 йил май ойидан бошланган. Шу ойда Бутунроссия Фавқулодда Комиссиясининг криптография бўлими базасида криптография махсус бўлими (8-махсус бўлим) ташкил топган. Махсус бўлим доирасида меҳнат тақсимоти аниқ белгилаб қўйилган, масалан, иккинчи бўлинма - криптологиянинг назарий муаммолари ва янги шифрлар яратиш, учинчи бўлинма турли совет идоралари (ведомство)да шифралоқани ташкил этиш, тўртинчи бўлинма - тутиб олинган шифрхабарни криптотаҳлиллаш билан шуғулланган.

1921-22 йиллларда дастлабки дипломатик ва ҳарбий Туркия шифрларини дешифрлаш (шифрни калитсиз очиш), 1925 йилга келиб ўн бешта Европа давлатлари шифрлари билан ишлаш, 1927 йил Япония хабарларини ўқиш, 1930 йилда АҚШнинг баъзи шифрларини бузиб очиш мумкин бўлган [1, 10].

1.2.3. Илмий криптография даври

Криптография тарихининг навбатдаги босқичи ***илмий криптография даври*** XX асрнинг 30-60 йилларини ўз ичига олади. Бу даврнинг фарқли томони криптобардошлилиги жиддий математик асосланган криптотизимларнинг юзага келишидир. XX асрнинг 30 йиллари бошларида криптологиянинг илмий асоси бўлган математиканинг бўлимлари батамом шаклланиб бўлди. Буларга *эҳтимоллар назарияси ва математик статистика, умумий алгебра, сонлар назарияси* киради. Улар билан биргаликда *алгоритмлар назарияси, ахборот назарияси ва кибернетика* фаол ривожлана бошлади [20].

1930 йил бошида армия криптографларини тайёрлашнинг кенг миқёсли дастури амалга оширилди ва Совет Иттифоқида криптографик хизмат ходимлари сони 500 нафарга ортди. Бу Иккинчи жаҳон уруши даврида муҳим роль ўйнади. Лекин совет шифрлари даражаси Энигмага нисбатан анча паст бўлган. Энигмадан Иккинчи жаҳон урушининг охиригача катта муваффақият билан фойдаланилди. У Иккинчи жаҳон уруши даврида иттифоқчилар учун катта тўсиққа айланган эди. Энигма шифрларини самарали дешифрлаш учун ҳар бир барабан ичидаги симларнинг уланишини билиш талаб этиларди. Унинг биринчи намунаси чизмалари билан биргаликда Польша разведкаси томонидан, иккинчиси Норвегия немис бомбардимончи самолётидан қўлга киритилган [10, 20].

1942 йилда Англияда немисларнинг шифрини дешифрлаш мақсадида яратилган биринчи ЭҲМ «Колосс» Энигма шифрини 1.5 соат мобайнида дешифрлашнинг уддасидан чиққан.

1941 йил декабр ойида АҚШнинг иккинчи жаҳон урушига қўшилиши муносабати билан АҚШ радиоразведка ва криптотаҳлил хизматининг иш кўлами ортиб кетди. Улар томонидан душманнинг ошкора ва шифрланган радиохабарлари тутиб олиниб, уларни баҳолаш ва улардан фойдаланиш учун ҳарбий разведка бошқармаларига юборилар эди. Иккинчи жаҳон уруши йилларида америкалик криптотаҳлилчилар томонидан душман томонининг бир қатор код ва шифрлари дешифрланган. 1942 йилда Япониянинг Ҳарбий Денгиз Кучлари шифри дешифрланган, 1943 йилда эса япон армияси шифрлари фош этилган. Америкада тезкорлиги бўйича инглизлар фойдаланган ЭҲМдан устун RAM юзага келгач, Арлингтон-Холл ва Блетчли-Парк орасида махсус алоқа канали ўрнатилди. Бу канал орқали Буюк Британиядан инглиз радиоразведкаси томонидан тутиб олинган Энигма шифрматнлари узатилар эди. 1943 йил июлдан 1945 йил январигича Арлингтон-Холлга 1357 немис шифрлари келиб тушган, улардан 413 таси муваффақиятли дешифрланган.

Америкалик криптологлар 1943 йилда «одамхўр-қўмондон» деб ном қозонган адмирал Ямоматонинг (Ямомато шахсан ўзи Перл Харборедаги операцияга бошчилик қилган) ягона самолётини қўлга тушириб йўқ қилганликларини ўзларининг энг катта ютуқлари деб биладилар [10, 20].

Иккинчи жаҳон урушида Девид Кан ёзишича I жаҳон уруши давридаги «Совет шифрлаш хизмати кўз ёшлари тўла тажрибасини асосан ҳисобга олди». Бу ҳақида 22 июнь 1941 йилда ҳарбий қисмлараро криптограммалар алмашиши тарихи гувоҳлик беради [20-21]. Совет Иттифоқига Германиянинг қўққисдан ҳужумидан сўнг бир зумда Қизил Армиянинг етакчи постларидан бири очиқ матнда «Бизни отмоқдалар. Нима қилайлик?» деб мамлакат ичкарисига қилган мурожаатига «Сизлар ақлдан озибсиз! Нега хабарингиз шифрланмаган» деган жавоб қайтарилган. Иккинчи жаҳон уруши даврида Қизил Армия шифрлаш хизмати асосан «қайта шифрлаш кодлари»дан фойдаланган. Қайта шифрлаш махсус код китобидан фойдаланишга асосланган бўлиб, унда ҳар бир сўз рақамлар комбинацияси билан алмаштирилган. Масалан, «Батария - ўт оч!» буйруғи ва шунга ўхшаш буйруқлар учун бу қулай, «атака», «дивизия» сўзлари 032, 1458 кодлари билан алмаштирилгач, кодга бирор гамма қўшиш (XOR амали асосида) орқали у қайта шифрланиб рация орқали узатилган. Агар рация орқали код тўғридан-тўғри узатилса, 1914 йилдаги ҳол юз берган бўлар эди, чунки код китоби матн статистикасини яшира олмайди.

Совет Иттифоқига қарши немис разведкаси самарадорлиги паст бўлган. Улар стратегик нуқтаи назардан арзигулик муваффақиятга эришмаганлар. Немислар Олий Совет Ҳарбий Қўмондонлигининг ёзишмаларида фойдаланилган шифр тизимларини бузиб очишга қодир бўлмаганлар. Бежиз немис криптографларидан бири «Россия эфирда Биринчи жаҳон урушида мағлуб бўлган бўлса-да, Иккинчи жаҳон уруши даврида реванш олишга муваффақ бўлди, деб тан олмаган. Айниқса, Совет разведкачиларининг шифр ёзишмаларини дешифрлаш мумкин бўлмаган. Уларнинг кўпчилиги у давр учун стандарт саналган шифр санъатининг чўққиси бўлган. Фойдаланилган шифр рус инқилобчилари ишлатган эски шифр тизимида қўшимча бир маротабалик гаммалаш амалини қўллаш орқали такомиллаштирилган. Уни Москвада абсолют бардошли шифр бўлган деб ҳисоблашади.

Иккинчи жаҳон уруши тугагач Совет Иттифоқи Ғарб билан жиддий муҳолифатга юз тутди. Бу ўз навбатида Совет Иттифоқи криптологиясининг ривожланишига катта ҳисса қўшиб янги замонавий криптография фанининг ривожланиш босқичини бошлаб берди.

Илмий криптография даврининг муҳим муваффақиятлари рўйхати бошида Клод Эльвуд Шенноннинг *«Махфий тизимларда алоқа назарияси»* (1949) асари туради [15, 20]. Унда ахборот муҳофазасининг назарий тамоиллари шакллантириб берилган.

К.Э. Шеннон томонидан қилинган бундай кашфиёт, албатта, унинг электротехника ва математика бўйича чуқур билимлари ва бундан бир йил олдин у яратган ахборот назарияси фани туфайли юзага келган эди. У нафақат Вернамнинг тасодифий шифрини бузиб очиб бўлмаслигини, балки ҳимояланган канал орқали узатиладиган махфий калит миқдори (битлар сони) чегараларини ҳам аниқ кўрсатиб берди. У чекланмаган ресурсларга эга бўлган криптотаҳлилчи бирор «тасодифий шифр»ни очишида махфий калитни топиши учун зарур бўлган шифрланган матндаги символлар сони s қуйидагича ифодаланишини кўрсатди:

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

бу ерда: $H(k)$ - калит энтропияси, яъни калитнинг ҳар битта символига тўғри келадиган ахборот миқдори, r - очиқ матннинг сериборалиги (русча, избыточность), n - алифбо ҳажми.

Келтирилган ифода умумий ҳолда исботланмаган бўлса-да маълум хусусий ҳоллар учун тўғри. Бундан қуйидаги муҳим хулоса келиб чиқади: криптотаҳлилчининг ишини нафақат криптотизимни мукаммаллаштириш орқали, балки шифрланадиган матннинг сериборалиги нолгача пасайтирилса, криптотаҳлилчи кичик калит билан шифрланган матнни ҳам оча олмайди. Демак, шифрлаш олдидан ахборотни статистик кодлаш (зичлаштириш, архивлаш) лозим. Бунда ахборотнинг ҳажми ва сериборалиги камаяди, энтропияси ошади. Чунки, ихчамлашган матнда қайтарилувчи сўзлар ва ҳарфлар камайиб шифрни бузиб очиш қийинлашади.

К. Шеннон криптотизимлар бардошлилигини *назарий* ва *амалий* турларга ажратади. Назарий бардошлилик деганда рақиб томоннинг таҳлилчиси у қўлга туширган криптограммаларни таҳлиллашда чекланмаган вақтга ва барча зарур воситаларга эга бўлган ҳолда криптотизимнинг бардошлилиги тушунилади. Амалий бардошлилик деганда криптотаҳлилчининг вақти ва ҳисоблаш имкониятлари чекланган ҳолга оид бардошлилик тушунилади. К. Шеннон амалий шифрларда ишлатиладиган икки тамойилни ажратади. Булар *ёйиш ва аралаштиришдир*. Ёйиш деганда, очиқ матннинг битта символини шифрланган матннинг кўп символларига таъсир этиши тушунилади. Бу очиқ матннинг статистик хоссаларини яширишга имкон беради. Бу тамойил калит символларига нисбатан ҳам қўлланилади. Аралаштириш деганда, К. Шеннон шифрланадиган ва шифрланган матнлар статистик хоссаларининг бир-бирига боғланишини тиклашни қийинлаштирувчи шифрлашга оид ўзгартиришларни назарда тутган.

К. Шенноннинг илмий криптология асосларини ўзида мужассамлаштирган мақоласи бу соҳада очиқ тадқиқотларнинг сезиларли ўсишига туртки бўла олмади. Чунки, биринчидан, махфий алоқа тизимларининг назарий бардошлилик назарияси ўз моҳиятига кўра тўла эди. Унга кўра назарий жиҳатдан бардошли махфий тизимларни ҳосил қилиш учун ҳимояланган каналлар бўйлаб ҳаддан ташқари катта ҳажмдаги калитларни узатиш лозим бўларди. Иккинчидан, амалий бардошлилик масалаларини ечиш мавжуд криптография усулларини такомиллаштириш билангина чекланиб қолди.

К. Шенноннинг «яхши» шифр яратиш муаммоси маълум шартларни қондирувчи энг мураккаб масалаларни топишга келтирилади. «Бизнинг шифримизни шундай тузиш мумкинки, уни бузиб очиш ечилиши катта ҳажмдаги ишларни талаб қилиши маълум бўлган муаммони ўз ичига олсин ёки унга эквивалент бўлсин» луқмаси яна чорак аср эътиборсиз қолди.

Девид Каннинг «Криптографлар» асари криптография тарихи бўйича мумтоз асар бўлиб қолган. Бу асар XX асрнинг 70 йиллари охиригача ҳам Давлат Хавфсизлиги Назоратининг махсус кутубхонасида сақланиб ундан фойдаланишга рухсати бўлган кимсалар davраси «идеологик мулоҳазалар асосида» жиддий чекланган. Унда Россия ҳақидаги бўлимда «Махфий полициянинг вазифаларидан бири бўлиб йўқсиллар диктатурасини йўқсилларнинг ўзидан муҳофаза қилиш бўлган» дейилади. Бу XX асрнинг 70 йилларида ҳам қўрқинчли сир бўлган [16, 20].

Иккинчи жаҳон уруши тугагач, совет криптографларидан ундан кам бўлмаган кучларни сарфлашни талаб этган «совуқ уруш» даври бошланди.

Бу даврда ҳарбий криптографик хизматнинг кўплаб илмий ходимлари ҳарбий хизматдан бўшатилган эди. Бу шароитларда ҳарбий чақириқ ёшида бўлган юқори малакали криптографлар «халқлар отаси»га тўғридан-тўғри мурожаат этишга ўзларида жасурлик топдилар ва уларнинг мурожаатига эътибор берилди.

1949 йил кузида Совет криптографияси учун катта аҳамиятга эга бўлган Бутуниттифоқ коммунистик большевиклар партияси қарорлари қабул қилинди. Қарорга мувофиқ, бир-бирига боғланмаган бўлинмалар асосида Бутуниттифоқ коммунистик большевиклар партияси Марказий комитети Махсус хизмат бош бошқармаси ташкил этилди ва унинг оёққа туриши ва ривожланиши учун восита ва катта маблағлар ажратилди; криптография хизмати тезкор вазифаларни бажариш, ҳамда янги юқори малакали кадрларни тайёрлаш учун энг кучли олимларни жалб этиш чоралари кўрилди, бу мақсадга эришиш учун криптографлар олий мактаби ва Москва Давлат Университети механика-математика факультетининг ёпиқ бўлинмаси ташкил этилди.

Бу қарорлар амалга оширила борилиб, 3 йил ичида Совет криптографиясининг сиймоси батамом янгиланди.

Шу ўринда криптографияга Совет раҳбарияти муносабатини тасаввур этиш учун Михаил Масленников [21] хотираларидан парча келтириш ўринли. У 1949 йил Москва авиация институтини тамомлагандан сўнг Ильюшин конструкторлик бюросига ишга жўнатилгач, бир йилдан сўнг криптография бўйича ўқишга танланган ва 1800 рубль стипендия билан таъминланган. Унинг подполковник Д. Щукин билан бўлиб ўтган суҳбати алоҳида эътиборга лойиқ. «Биз криптографлармиз, шифрлар билан махфий алоқа соҳасида ишлаймиз. Лекин, ўрток Сталин бизга ҳам «Ҳаммани ўқиш, лекин бизнинг суҳбатлар ва ёзишмаларни ҳеч ким ўқий олмаслиги зарур»лиги вазифасини қўйди. Д. Щукин суҳбатдошига телеграф алоқасини махфийлаштириш учун махсус техника яратиш билан шуғулланишини, лекин бу ҳақда ҳеч ким на онаси, на яқин дўстларидан бирортаси билмаслиги зарурлигини уқтирган. Бундан бу даврларда криптография билан шуғулланганлар ҳам махфий сир сақланиши ва улар етарли даражада иқтисодий ҳимояланганлиги кўриниб турибди.

XX асрнинг 60 йилларига келиб криптографик мактаблар ротор криптотизимларга нисбатан бардошлилиги юксак бўлган блокли шифрлар яратишгача етиб келдилар.

Криптография тарихи бўйича биринчи асар Дэвид Каннинг «Код бузувчилар» монографияси бўлди. АҚШда XX асрнинг 60 йил охирларида юзага келган бу асар криптология соҳасидаги биринчи фундаментал иш бўлиб, у узоқ вақт давомида криптологияга бағишланган умумий тадқиқот йўналишларини аниқлаб берди. Аммо бу иш ҳар томонлама криптологияни қамраб олган дейиш қийин, чунки у криптологиянинг бир йўналиши бўлган криптотаҳлилни асос қилиб олган. Каннинг бу асарида криптотаҳлилнинг назарий асослари ва уни амалиётда қўллаш кўриб ўтилган. Лекин бу асарнинг аҳамияти шундаки, муаллиф ўқувчиларни криптологиянинг асосий тушунчалари билан таништириб ўтган. Каннинг бу асари фақат тадқиқотчилар учун эмас, балки кенг китобхонлар оммаси учун мўлжалланган илмий асар ҳисобланади.

1.2.4. Компьютер криптографияси даври

Компьютер криптографияси даври XX асрнинг 70 йилларида авваллари қўлда бажариб келинган, ундан сўнг механик ва электромеханик қурилмалар ёрдамида амалга оширилган шифрлар ўрнига улардан ҳаддан зиёд юқори критобардошлиликка ва тезкорликка эга криптотизимлар яратишга янгича ёндашувларни амалга оширишга қодир бўлган электрон ҳисоблаш машина (компьютер)ларнинг юзага келиши билан характерланади. Юқори қувватли ва ихчам компьютерларнинг пайдо бўлиши ахборот технологияларининг мисли кўрилмаган ривожига, компьютер ва коммуникация тармоқларининг, Интернет тармоғининг кенг қулоч ёйишига, алоқа воситаларининг рақамлашишига олиб келди ва ахборот хавфсизлиги муаммоси янада долзарб муаммолар қаторидан жой олди. Натижада криптологияда иккита *муҳим воқеа* содир бўлди [22].

Компьютер криптографияси даврининг *биринчи муҳим воқеаси* симметрик криптотизимларнинг биринчи синфи бўлган блокли шифрлар юзага келиб, улар тарихда биринчи марта Давлат стандарти мақомига эга бўлиши бўлса, даврнинг аҳамиятга молик *иккинчи тамойилли муҳим кашфиёти* криптологияга янгича ёндашувларни бошлаб берган ошкора криптографиянинг юзага келишидир.

Бу даврдан бошлаб криптографик тизимлар иккита синфга бўлина бошлади: *симметрик (махфий калитли, бир калитли)* ва *носимметрик (ошкора (очиқ) калитли, икки калитли) криптотизимлар.* Ўз навбатида симметрик криптотизимлар милоддан аввалги даврлардан маълум бўлиб, улар оқимли ва блокли шифр турларига бўлинади.

1.2.4.1. Симметрик криптотизимлар

Симметрик криптотизимларнинг илмий назарияси яратилиши ва амалиёти ривожига илмий криптография асосчиси К. Шеннон, А.Н. Колмогоров ва формал криптография намояндалари О. Керхгофф, Ч. Беббидж, У. Фридман, Г. Вернам, Э. Хеберн ва бошқалар катта ҳисса қўшган [23].

Ахборот узатиш ва сақлаш жараёнларининг рақамлаштирилиши узлукли (нутқ) ва узлуксиз (матн, факс, телекс, тасвир, анимация) ахборотларни муҳофазалаш учун ягона алгоритмлардан фойдаланиш имконини беради. Шифрлаш алгоритмларига қуйидагича асосий талаблар қўйилади:

- шифрланган ахборотни ўзгартириб қўйиш ёки унинг шифрини бузиб – очишга йўл қолдирмаслик;

- ахборот муҳофазаси фақат калитнинг маълумлигига боғлиқ бўлиб, алгоритмнинг маълум ё номаълумлигига боғлиқ эмас (О.Керкгофф қоидаси);

- дастлабки ахборот (маълумот)ни ёки калитни бироз ўзгартириш шифрланган матннинг бутунлай ўзгартириб юбориши лозим (К. Шеннон тамойили, “ўпирилиш” ҳодисаси);

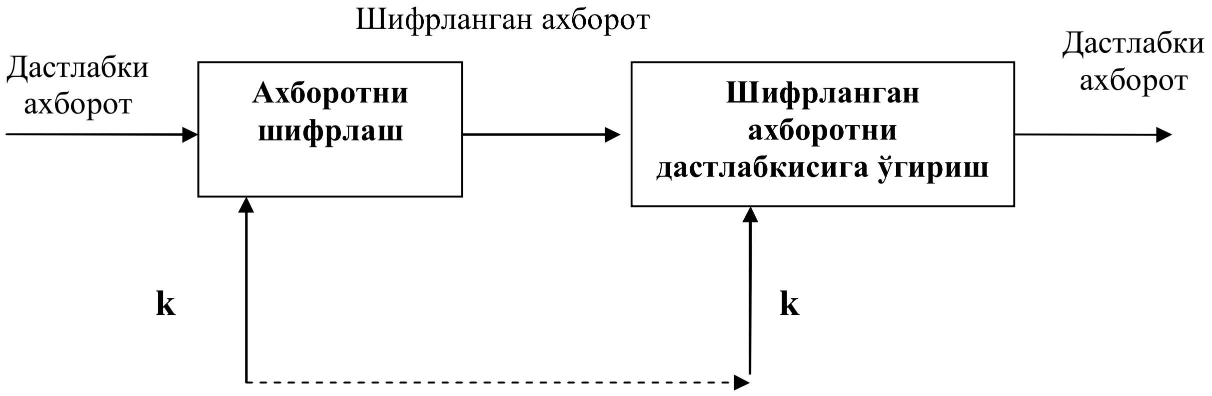
- калит қийматлари соҳаси шундай катта бўлиши керакки, ундан калит қийматларини бир бошдан кўриб чиқиш асосида шифрни бузиб очиш имкони бўлмаслиги лозим;

- алгоритм иқтисодий жиҳатдан тежамли ва етарли тезкорликка эга бўлиши лозим;

- шифрматнни бузиб очишга кетадиган сарф-харажатлар ахборот баҳосидан юқори бўлиши лозим [23-24].

Криптографик тизим, ё қисқача, криптотизим, шифрлаш ҳамда шифрни очиш алгоритмлари, бу алгоритмларда ишлатиладиган калитлар, шифрланадиган ҳамда шифрланган матнлар ва буларнинг ўзаро мослашиш қоидаларини ўзида мужассамлантирган протокол (баённома)дан иборат мажмуадир.

Криптотизимдан фойдаланишда матн муаллифи шифрлаш алгоритми ва шифрлаш калити воситасида аввало дастлабки матнни шифрланган матнга ўгиради. Матн муаллифи уни ўзи фойдаланиши учун шифрлаган бўлса (бунда калитларни бошқарув тизимига ҳожат ҳам бўлмайди) уни сақлаб қўяди ва керакли вақтда шифрланган матнни очади. Очилган матн асли (дастлабки матн)га айнан бўлса, сақлаб қўйилган ахборотнинг яхлитлигига ишонч ҳосил бўлади. Акс ҳолда ахборот бутунлиги бузилган бўлиб чиқади (6-расм). Бу ерда *k* – юборувчи ва қабул қилувчининг симметрик махфий калити.



6-расм. Симметрик криптотизимларда ахборот алмашиш

Агар шифрланган матн уни яратган кимсадан ўзга қонуний фойдаланувчига (олувчига) мўлжалланган бўлса, у тегишли манзилга жўнатилади. Сўнгра шифрланган матн олувчи томонидан унга аввалдан маълум бўлган шифрни очиш калити ва алгоритми воситасида дастлабки матнга ўгирилади.

Криптографлар орасида машҳур бўлган маълумотларни шифрлаш алгоритмлари гуруҳига АҚШ давлат стандартлари – DES [11, 25], AES [26], Россия Федерацияси давлат стандарти ГОСТ 28147-89 [27], IDEA [11, 25], FEAL [11, 25] киради.

DES IBM фирмасининг бутун бир криптографлари гуруҳи томонидан ишлаб чиқилган [11, 25]. Маълумотларни шифрлаш стандарти 1976 йил 23 ноябрда Миллий Стандартлар Бюроси томонидан АҚШнинг давлат стандарти сифатида қабул қилинган ва у 1977 йил июль ойидан 2000 йил октябрь ойигача рақамли маълумотларни шифрлаш учун стандарт бўлиб хизмат қилган. Ҳозирги вақтда у фақат назарий аҳамиятга эга. DES занжирсимон тузилмали мувозанатланган Фейстал тармоғи архитектурасига эга. Мутахассисларнинг фикрига кўра бу стандарт ёйиш ва аралаштириш тамойилларига асосланган энг яхши криптоалгоритмлардан биридир. Шифрлаш алгоритмида шифрматннинг ҳар бир бити дастлабки матн ва калит барча битларининг функцияси бўлади. Стандартда ўрнига қўйиш, ўрин алмаштириш ва 2 модуль бўйича қўшиш амалларининг комбинациясидан фойдаланилади.

ГОСТ 28147-89 - собиқ Совет Иттифоқида ишлаб чиқилган DES каби мувозанатланган Фейстал тармоғи [27] архитектурали *64*-бит блокли ва калит узунлиги *256* бит бўлган криптографик ўзгартириш алгоритмидир [27]. Алгоритм босқичлари сони *32* га тенг бўлса-да, у DESга нисбатан тезкордир.

Шифрматнни дастлабки матнга ўгириш ҳам худди дастлабки матнни шифрматнга ўгириш каби бажарилади, фақат бунда калитлар кетма-кетлиги ўзгартирилади.

ГОСТ 28147-89да DES, AESга хос электрон код китоби режимига жуда ўхшаш оддий алмаштириш режими, DES, AESга хос режимлардан бироз фарқли бўлган гаммалаштириш, тескари боғланишли гаммалаштириш режимлари ва улардан тамойилли фарқли имитоқистирма ишлаб бериш режимидан фойдаланади.

ГОСТ 28147-89 алгоритми DESга нисбатан анча юқори криптобардошлиликни таъминлайди. Бу кунгача у энг самарали ҳисобланган дифференциал ва чизиқли криптотаҳлил усулларига нисбатан етарли даражада криптобардошли саналадиган алгоритмлардан биридир. Бу асосан, DESга нисбатан узун, яъни 256 битли калитдан ва S-блокларга тегишли деярли 354 бит (S-блок генерацияловчилар ва фойдаланувчилар гуруҳидан ўзгалар учун) махфий маълумотдан фойдаланилиши билан изоҳланади.

AES алгоритмида кириш ва чиқиш блоклари узунлиги *128* бит шифрлаш калитининг узунлиги *128*, *192* ёки *256* бит этиб белгиланди.

Шифрлашда қўлланиладиган барча алмаштиришлар ёйилиш ва тарқалиш тамойилларини амалга оширишга қаратилган. Стандартда блок ва калитнинг узунлигига боғлиқ равишда босқич (раунд)лар сони 10 дан 14 гача белгилаб қўйилди.

Шифрлаш процедураси босқич калитларини генерациялаш процедурасини ҳам, босқичлар сонига мос узунликдаги шифрматнга ўгириш (дастлабки матнга ўгириш) учун босқич калитларини юклашни ҳам ўз ичига олади.

Шифрматнни дастлабки матнга ўгириш амалларни инверсия (тескари) тарзида бажариш орқали амалга оширилади.

Ҳозирги кунгача AES юқори криптобардошлиликка эга бўлган шифрлар қаторига киради.

IDEA – яна бир *64*-битли блокли шифрлаш алгоритми бўлиб, калитининг узунлиги *128* битга тенг [11, 25]. IDEA шифрининг биринчи варианти Ксуеджи Лай ва Джеймс Масси томонидан *1990* йилда таклиф этилган. У тезлиги бўйича DES алгоритмидан қолишмайди, криптотаҳлилга бардошлилиги жиҳатидан эса ундан ҳам устун.

IDEAда дастлабки матнни шифрматнга ўгириш ва шифрматнни дастлабки матнга ўгиришда ягона алгоритмдан фойдаланилади.

IDEA алгоритмида ҳам бошқа блокли шифрлаш алгоритмларидаги каби аралаштириш ва ёйиш тамойиллари етарли даражада амалга оширилган. Унинг асосида “турли алгебраик группаларнинг амалларини бирлаштириш” фалсафаси ётади. Унда уч алгебраик группа аралаштирилган ва уларнинг барчаси ҳам қурилма, ҳам дастур кўринишида осон амалга оширилади.

Шифрни очиш амали ҳам худди шифрлаш амали каби бажарилади, бунда фақат қисм калитлар бироз ўзгартирилади.

FEAL алгоритми япон мутахассислари Акихиро Шимузу ва Шоджи Миягучи томонидан таклиф этилган бўлиб, унда кириш ва чиқишда *64*-битли блоклардан ва *64*-битли калитдан фойдаланилади [11, 25]. Унинг мақсади DESга нисбатан кучли алгоритм яратишдан иборат бўлган, лекин пировардида бу алгоритм бошланғич мақсаддан узоқлашиб кетган.

FEAL алгоритми дифференциал ва чизиқли криптотаҳлилга нисбатан етарли криптобардошлиликни таъминлай олмаганлиги маълум [11, 25]. Шу боис, у асосан криптотаҳлилчилар орасида машҳур, чунки кимда-ким янги криптотаҳлил усулини яратса, уни аввало **FEAL** алгоритми учун синаб кўриши одат тусига кирган.

O‘z DSt 1105:2005 ва **O‘z DSt 1105:2009** «Ахборот технологияси. Ахборотнинг криптографик муҳофазаси. Маълумотларни шифрлаш алгоритми» (МША)да модуль арифметикасининг диаматрицалар алгебрасидан фойдаланилади, бунда ҳисоблашнинг қийинлик даражаси матрицалар алгебрасидаги сингари бажарилади [23, 28].

Шифрматнга ўгириш ва дастлабки матнга ўгириш процедураларида фойдаланиладиган диаматрицалар алгебрасининг асосий амали диаматрицани p модуль бўйича диаматрицага тескарилаш амали ҳисобланади. Бу амалларда икки ўлчамли сеанс калити массивининг махсус тузилмали *4*x*4* тартибли квадрат диаматрица билан акс эттирилувчи қисмлари иштирок этади. Махсус тузилмали диаматрицанинг муҳим хоссаси диаматрицанинг диааниқловчисини ҳисоблаш формуласининг соддалигидир, бу эса диаматрицани тескарилаш шартларини текшириш ишларини соддалаштиради.

Махсус тузилмали диаматрицани тескарилаш шартларини текшириш МША параметрларига қўйиладиган асосий талаб ҳисобланади. МШАда шунингдек бутун сонларни параметрли кўпайтириш, тескарилаш ва даражага ошириш деб аталган параметрли группа амалларидан ҳам фойдаланилади. МША белгилаб қўйилган икки хил - *256* ва *512* бит узунликдаги калитлар ёрдамида амалга оширилади.

Барча юқорида баён этилган ГОСТ 28147-89дан бошқа алгоритмлар бўйича маълумотларни шифрлашда 5 хил иш режимини қўллаш мумкин [27]: электрон код китоби; шифр блокларнинг илашиши; чиқиш орқали тескари боғланиш; шифрматн орқали тескари боғланиш (тескари боғланишли гаммалаштириш); саноқчи. Табиийки, ҳар бир иш режимининг ўзига хос афзаллиги ва камчилиги бўлади. Масалан, калитларни шифрлашда электрон код китоби иш режимини, алоҳида белгилар учун шифр матн орқали тескари боғланиш иш режимини, алоқа тизимида (одатда, бирор шифрматнни такрор узатиш имконияти бўлмаганда) чиқиш орқали тескари боғланиш иш режимини қўллаш қулай ҳисобланади.

1.2.4.2. Носимметрик криптотизимлар

Носимметрик криптографик тизимлар яратиш тамойили жаҳон криптография тарихида илк бор бундан 35 йил муқаддам америкалик олимлар Уитфильд Диффи ва Мартин Хеллман [29-30] томонидан таклиф этилган бўлиб, улар катта сонли чекли тўпламларда бир томонлама функциялардан фойдаланишга асосланган. У. Диффи ва М. Хеллманнинг 1976 йилда босилиб чиққан “Криптологияда янги йўналишлар” мақоласида илгари сурилган ”махфий калитни узатишни талаб этмайдиган амалий бардошли махфий тизимларни тузиш мумкин” деган фикри криптологияда носимметрик криптотизимларнинг юзага келиши ҳамда уларнинг ривожланиш даврининг бошланишига сабаб бўлди. У. Диффи ва М. Хеллман мақоласининг ҳал қилувчи ҳиссаси иккита таърифда мужассамланган. Булар «бир томонлама функция» ва «яширин йўлли бир томонлама функция «тушунчаларидир.

Носимметрик криптотизимлар назарияси ва амалиёти ривожига У. Диффи ва М. Хеллман [29-30] билан бир қаторда Р. Райвест, А. Шамир, Л. Адлеман [31-36], Эль Гамал [37-38], К. Шнорр [39-41], Н. Коблиц [42-44], А. Менезец [45-46], Б. Шнайер [11, 25, 47] ва бошқалар катта ҳисса қўшган.

Шифрлаш ва шифр очиш калитлари ўзаро функционал боғланган бўлиб, улардан бири асосида иккинчиси амалий жиҳатдан (мавжуд ҳисоблаш воситалари тараққиёти даражасида) ҳисоблаб топилиши мумкин бўлмаган ва улардан бири фақат алоқа иштирокчисига маълум бўлиб, бошқалардан махфий тутиладиган, иккинчиси эса алоқа иштирокчиларининг ҳаммасига ошкора бўлган криптотизим *носимметрик (ошкора калитли) криптотизим* деб аталади [2, 22]. Қуйидаги 7-расмда носимметрик криптографик тизимда ахборот узатиш жараёни акс этган. Бу ерда $\mathbf{k_e}$ – қабул қилувчининг ошкора калити, $\mathbf{k_d}$ – қабул қилувчининг махфий калити.

7-расм. Носимметрик криптографик тизимда ахборот узатиш жараёни

Носимметрик криптотизимда алоқа иштирокчиларининг ҳар бири ўзининг шахсий махфий ва ошкора калитлари жуфтига эга бўлиб ўз ошкора калитини бошқа алоқа иштирокчиларига эълон қилади. Шахсий махфий калит қабул қилинадиган ахборот конфиденциаллигини таъминлаш учун яратилганда шифрни очиш калити бўлиб хизмат қилади. Бунда кимга конфиденциал ахборот жўнатиладиган бўлса унинг ошкора калитидан фойдаланиб шифрланган ахборот жўнатилади. Бундай ахборотнинг шифрини фақат ягона махфий калит эгасигина оча олади. Агар махфий калит аутентификация мақсадида хабарларга электрон рақамли имзо босиш учун ҳосил қилинган бўлса, у шифрлаш калити сифатида фойдаланилади. Ошкора калит эса юқоридаги биринчи ҳолда шифрлаш калити бўлиб, иккинчи ҳолда шифрни очиш (текшириш) калити бўлиб хизмат қилади.

Носимметрик криптотизимлар асосида симметрик тизимларда ечилмай қолган калит тарқатиш ва электрон рақамли имзо масалаларининг ечимини излаш йўлларида У. Диффи ва М. Хеллман кўпгина таклифларни илгари сурганлар.

Ошкора калитли криптография асосида ривожланган мамлакатлар орасида биринчи бўлиб АҚШ электрон рақамли имзо бўйича миллий стандарт яратишга киришган. Авваллари Миллий Хавфсизлик Агентлигида ишлаган Дэвид Кравиц DSA патенти эгаси ҳисобланади. 1993 йил июнда технологиялар ва стандартлар миллий институти (NIST) DSA учун патент лицензиясини беришни таклиф этган. Аслида АҚШ стандарти DSAда 1985 йилда Тохир Эль Гамал томонидан ишлаб чиқилган алгоритм хусусиятларидан ва К. Шнорр ғояси асосида имзо узунлигини қисқартиришга қаратилган иккинчи туб модулдан фойдаланилган. DSAнинг криптобардошлилиги чекли майдонларда бутун сонларни логарифмлаш муаммоси математикада амалий ҳисоблаш нуқтаи назаридан ҳануз ечилмаганлигига асосланади.

АҚШдан кейин Европа давлатлари ва Японияда электрон рақамли имзо бўйича қонун ва дастлабки давлат стандартлари қабул этилди. Бошқа ошкора калитли криптографияга асосланган воситалар яратилди, экспортга мўлжалланган ахборот-коммуникация тизимларида жорий этилди. Кўпчилик давлатлар, шу жумладан Ҳамдўстлик давлатлари ҳам ошкора калитли криптография воситаларини яратишда АҚШга эргашдилар. Бу ошкора калитли криптографиянинг дастлаб АҚШда юзага келганлиги билан боғлиқ албатта. Улар ахборот–телекоммуникация тармоқларида махфий ахборотларни хавфсиз узатиш ва электрон рақамли имзо яратишда ўз миллий алгоритмларидан фойдаланмоқдалар.

Очиқ калитли криптотизимлар ахборот хавфсизлигининг кўплаб муаммоларини ечиб беришга қодир бўлиб, уларнинг муҳим қўлланиш соҳаларидан бири *электрон рақамли имзо* (ЭРИ) ҳисобланади.

Юқорида келтирилган криптотизимларнинг асосий камчиликларидан бири, бузғунчи криптотизим асосига олинган муаммони етарлича аниқ қўя олганда ва унинг бу муаммони ҳал қилишга ресурслари етарлича бўлганда, қабул қилувчига келиб тушган рақамли имзо сохта бўлса, имзоловчи шахсда имзонинг сохталигини исботловчи далиллар ва маълумотларнинг йўқлигидир. Ўзбекистон миллий стандартларини яратишда бу камчиликларни бартараф этишга эътибор берилди ва 2005-2009 йиллларда

Ўзбекистон алоқа ва ахборотлаштириш агентлигининг «UNICON.UZ» - Фан-техника ва маркетинг тадқиқотлари маркази давлат унитан корхонаси O‘z DSt 1092:2005, O‘z DSt 1092:2009 «Ахборот технологияси. Ахборотнинг криптографик муҳофазаси. Электрон рақамли имзони шакллантириш ва текшириш жараёнлари» [48], O‘z DSt 1106:2009 Ахборот технологияси. Ахборотнинг криптографик муҳофазаси. Хэшлаш функцияси» [49] давлат стандартлари ишлаб чиқилди ва Ўзбекистон стандартлаштириш, метрология ва сертификатлаштириш агентлиги томонидан тасдиқланди.

Ишлаб чиқилган электрон рақамли имзо алгоритми (ЭРИА)да ЭРИни шакллантириш жараёнига ЭРИнинг ҳақиқийлигини тасдиқлаш жараёнида қўлланиладиган сеанс калити процедурасини киритиш билан ЭРИ сохталигини аниқлашнинг заҳиравий йўли ҳам назарда тутилган.

Электрон рақамли имзо механизми қуйидаги жараёнларни амалга ошириш орқали аниқланади:

- ЭРИ ва сеанс калитини шакллантириш;
- ЭРИ ҳақиқийлигини тасдиқлаш.

Ишлаб чиқилган ЭРИА икки асосий режим - сеанс калитсиз ва сеанс калитли қўлланилади:

Сеанс калитли режимда ЭРИАнинг криптографик бардошлилиги ЭРИнинг очиқ калитини генерациялаш жараёнида қўлланиладиган, даражага кўтариш асосининг махфийлигига асосланади. Бу электрон рақамли имзони сохталаштириш учун дискрет логарифмлаш масаласининг қўйилиш имкониятини истисно этади, чунки сеанс калитидан фойдаланиш, агар сохталаштириш юз берган бўлса, ЭРИ сохталаштирилганлигини аниқлаш имконини беради. Натижада ЭРИАнинг криптобардошлилиги етарли даражада юқори бўлади. Сеанс калитисиз режимда ЭРИАнинг криптографик бардошлилиги дискрет логарифмлаш масаласи ечимининг мураккаблигига, шунингдек бошқа унга ўхшаш алгоритмлар каби қўлланиладиган хэш-функциянинг бардошлилигига асосланади.

O‘z DSt 1092:2005, O‘z DSt 1092:2009да П.Ф. ва Х.П. Хасановлар томонидан таклиф этилган модуль арифметикасининг ***янги бир томонлама функцияси*** қўлланилади, бунда ҳисоблашлар қийинлик даражаси бўйича даражага кўтариш амаллари каби енгил амалга оширилади, функцияни тескарилаш эса дискрет логарифм муаммосини ечиш жараёнидагидан кам бўлмаган ҳисоблаш сарфлари ва вақт талаб қилади [48]. Анъанавий (классик) бир томонлама даражага кўтариш функцияси ушбу бир томонлама функциянинг хусусий ҳолидир.

Назорат саволлари

1. Криптологияга таъриф беринг?
2. Криптографиянинг криптотаҳлилдан фарқи нима?
3. Ахборотни шифрлаш деганда нима тушунилади?
4. Шифр ва шифрматн деб нимага айтилади?
5. Криптографик ўзгартириш деб нимага айтилади?
6. Алифбо деганда нимани тушунасиз?
7. Криптография тарихи қандай даврларга бўлинади?
8. Дастлабки криптография даврининг муҳим жиҳатлари нималардан иборат?
9. Формал криптография даврининг асосий воқеалари нималардан иборат?
10. Илмий криптографиянинг ривожланишида Клод Эльвуд Шенноннинг ўрни қандай?
11. Компьютер криптографияси даврининг муҳим воқеалари нималардан иборат?
12. Симметрик криптотизимларнинг илмий назарияси асосчиларидан кимларни биласиз?
13. Ошкора криптотизимларнинг асосий жиҳатлари нималардан иборат?
14. Бир томонлама функциялар ҳақида маълумот беринг?

2. ТЎПЛАМ ВА АКСЛАНТИРИШЛАР

2.1. Тўпламлар

Тўплам математиканинг кўплаб соҳаларида бошланғич - фундаментал тушунча ҳисобланиб, белгиси, хусусияти ёки хоссалари бир хил нарсаларнинг мажмуи тушунилади [12-13, 50]. Тўпламни ташкил этувчи нарсалар тўпламнинг элементлари деб юритилади.

Ушбу $x \in X$ ифода x элементнинг X тўпламга тегишли эканлигини билдиради, акс ҳолда $x \notin X$ ифода билан белгиланади. Тўплам одатда бирор алифбонинг бош ҳарфи билан, унинг элементлари фигурали қавслар ичига олинган ёки талқини берилган кичик ҳарфлар билан белгиланади. Муҳим аҳамиятга молик тўпламлар учун стандарт белгилардан фойдаланилади. **N, Z, Q, R** белгилари мос тарзда натурал, бутун, рационал ва ҳақиқий сонлар тўпламларини белгилашда фойдаланилади.

Агар ҳар иккала тўплам ҳам бир хил элементлардан ташкил топган бўлса, берилган X ва Y тўпламлар тенг дейилади, акс ҳолда тенг эмас дейилади.

Мисол учун:

$X = \{0;0;0;0\} = \{0;0;0;0\} = Y$, $X = \{0;0;0;0\} \neq \{0;0;0\} = Y$, яъни тўпламлар элементлари сони тенг эмас.

Элементлари сони чекли (чексиз) бўлган тўплам чекли (чексиз) тўплам дейилади.

Ҳар бир олинган $x \in X$ элементга битта $\varphi(x) \in Y$ элемент мос келиб, ҳар бир олинган $y \in Y$ элементга $\varphi(x) = y$ тенгликни қаноатлантирувчи $x \in X$ элемент мос келса, унда берилган X ва Y тўпламлар ўзаро бир қийматли (биектив) φ - мосликка эга дейилади, Бундай биектив мослик $\varphi : X \leftrightarrow Y$ кўринишда ифодаланади. Умуман олганда “ φ - акслантириш X - тўплам элементларини Y - тўплам элементларига акслантиради” ибораси: $\varphi : X \to Y$ кўринишда ифодаланади.

Тўпламлар билан боғлиқ бўлган тушунчалар, таъриф ва тасдиқлар жуда кенг тарқалган бўлиб, фан ва техниканинг кўплаб соҳаларига тегишли бўлган адабиётларда турли шаклларда келтирилганлиги учун, қуйида уларни тартиб рақамларисиз келтирилади.

Агар берилган X - чексиз тўпламнинг элементларини номерлаб чиқиш мумкин бўлса, яъни X - тўплам билан N - натурал сонлар тўплами ўзаро бир қийматли мосликка эга бўлса, бу чексиз тўплам саноқли дейилади. Бошқа чексиз тўпламлар саноқсиз дейилади. Мисол учун, исбот қилиш мумкинки, барча рационал сонлар тўплами саноқли, $[0;1]$ - кесмадаги барча ҳақиқий сонлар тўплами эса саноқсиздир.

Берилган чекли тўплам элементлари сони унинг қувватини аниқлайди. Элементлари сони n та бўлган X -тўпламнинг қуввати n га тенг бўлиб, $|X| = n$, деб ифодаланади. Саноқсиз тўпламлар “континиум” қувватга эга деб ҳам юритилади.

Тўпламни аниқлаш унинг элементларини бевосита кўрсатиш билан амалга оширилади. Бундан ташқари, тўпламни, унинг элементлари хусусиятларини сўзлар орқали ёритиш:

M={i∈N: I –натурол сон бўлиб, 2 га қолдиқсиз бўлинади}

ёки формулалар билан ифодалаш (рекурсив усул):

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

орқали аниқлаш мумкин.

Агарда Y - тўпламнинг ҳар бир элементи X - тўпламнинг ҳам элементи бўлса, у ҳолда Y - тўплам X -тўпламга қисм тўплам бўлади ва $Y \subseteq X$ кўринишда ифодаланади.

Агарда $Y \subseteq X$ бўлиб, $Y \neq X$ бўлса, у ҳолда $Y \subset X$ кўринишда ифодаланади ва Y -тўплам X -тўпламнинг хос қисм тўплами дейилади.

Агар $Y \subseteq X$ ва $X \subseteq Y$ бўлса, у ҳолда $Y = X$ бўлади.

Бирорта ҳам элементга эга бўлмаган тўплам бўш тўплам дейилади ва $\varnothing$ белги билан ифодаланади. Бўш тўплам $\varnothing$ ихтиёрий тўпламга қисм тўплам бўлади ва унинг қуввати нолга тенг, яъни $|\varnothing| = 0$.

Ҳар қандай X ва Y - тўпламлар жуфтлиги учун қуйидаги амаллар аниқланган:

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

2) кесишма (кўпайтма) $X \cap Y = \{x : x \in X \text{ ва } x \in Y\}$;

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

Бу амаллар қуйидаги хоссаларга эга:

1) коммутативлик: $X \cup Y = Y \cup X$ ва $X \cap Y = Y \cap X$;

2) ассоциативлик: $(X \cup Y) \cup Z = X \cup (Y \cup Z)$ ва $(X \cap Y) \cap Z = X \cap (Y \cap Z)$;

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

ва

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

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

Агар $X \subseteq U$ бўлса, у ҳолда X - тўпламнинг U - тўпламга нисбатан тўлдирувчиси деб

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

тўпламга айтилади.

Қуйидаги муносабатлар ўринли:

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

Берилган $X_1, X_2, \ldots, X_m$ - тўпламларнинг Декарт кўпайтмаси деб, ушбу $X = X_1 \times X_2 \times \ldots \times X_m = \{(x_1, x_2, \ldots, x_m) = x \in X : x_i \in X_i\}$ - тўпламга айтилади. Математик индукция усулидан фойдаланиб $X_1, X_2, \ldots, X_m$ - тўпламлар Декарт кўпайтмасини ташкил этувчи тўпламнинг қуввати ушбу

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

тенглик билан аниқланишини исбот қилиш мумкин, яъни берилган тўпламлар Декарт кўпайтмасини ташкил этувчи тўпламнинг қуввати кўпайтувчилар қувватларининг кўпайтмасидан иборат.

Берилган X - тўплам $\leq$ - муносабат билан тартибланган (чизиқли тартибланган, тўла тартибланган) дейилади, агарда $\forall a,b,c \in X$ - элементлар учун қуйидаги хоссалар бажарилса:

1) рефлексивлик $a \leq a$;
2) антисимметриклик – агар $a \leq b$ ва $b \leq a$ бўлса, у ҳолда $a = b$;
3) транзитивлик – агар $a \leq b$ ва $b \leq c$ бўлса, у ҳолда $a \leq c$;
4) чизиқлилик – ёки $a \leq b$, ёки $b \leq a$.

Агар $\forall a,b,c \in X$ - элементлар учун (1)-(3) хоссалар бажарилса, берилган X - тўплам қисман тартибланган тўплам дейилади.

X - қисман тартибланган тўпламнинг *диаграммаси* (*Хаас диаграммаси*) деб, шу тўплам элементлари жуфтликларининг $(a,b) \in X$ ёй (йўналтирилган кесма) билан боғланган ифодасини текисликдаги тасвирига айтилади. Графлар таърифида, X - қисман тартибланган тўплам – бу йўналишга эга бўлган граф бўлиб, унинг учлари X - тўпламдан иборат эканлиги, (a,b) - жуфтлик фақат ва фақат ушбу $a \leq b$ ва $a \neq b$ - шартлар билан биргаликда a ва b элементлардан фарқли бўлган $a \leq c \leq b$ шартни қаноатлантирувчи $c \in X$ элемент мавжуд бўлмагандагина ёй ташкил этиши таъкидланади.

Y - тўплам берилган X - қисман тартибланган тўпламнинг қисм тўплами бўлиб, $a \in X$ бўлсин. У ҳолда $a \in X$ бўлган элемент Y - қисм тўпламнинг юқори (қуйи) чегараси дейилади, агарда барча $b \in Y$ элементлар учун $b \leq a$ $(a \leq b)$ шарт бажарилса. Y - тўпламнинг юқори чегараси a унинг аниқ юқори (қуйи) чегараси дейилади, агарда Y -тўпламнинг барча c-юқори (қуйи) чегаралари учун $a \leq c$ $(c \leq a)$ шарт бажарилса, $a = \sup Y$ $(a = \inf Y)$ деб белгиланади.

Агар $\forall a,b \in X$ элементлар учун $\sup(a,b) \in X$ ҳамда $\inf(a,b) \in X$ бўлса, қисман тартибланган тўплам X *панжара* дейилади.

Тўпламларнинг хоссалари билан боғлиқ бўлган криптология масалаларини таҳлил қилишда қўлланиладиган тушунча ва тасдиқларни тўпламлар назариясининг амалий тадбиқлари ёритилган ўқув қўлланмаларидан топиш мумкин.

2.2. Акслантиришлар

Акслантиришлар берилган тўпламлар устида амаллар бажариш билан уларнинг элементлари орасида мослик ўрнатиш жараёнини ифодалайди. Акслантиришларнинг хоссаларини таҳлил қилиш билан боғлиқ бўлган айрим тушунча ва таърифларни келтирамиз.

Берилган φ-акслантириш (функция) X - тўпламни Y - тўпламга *бир қийматли* акслантиради дейилади (ва $\varphi : X \to Y$ кўринишда белгиланади), агарда ҳар бир $x \in X$ элементга фақат битта $y = \varphi(x) \in Y$ элемент мос қўйилса. Бу ерда X - тўплам φ-акслантиришнинг *аниқланиш соҳаси*, Y - тўплам эса *қийматлар соҳаси*, y-элемент x-элементнинг *акси*, x-элемент y-элементнинг *асли* дейилади.

Агарда берилган φ ва ψ акслантиришларнинг аниқланиш ва қийматлар соҳалари тўла устма-уст тушиб, $\forall x \in X$ элемент учун $\varphi(x) = \psi(x)$ тенглик бажарилса, бундай акслантиришлар *тенг* дейилади.

Ушбу $\varphi : X \to Y$ акслантириш берилган бўлсин, у ҳолда $\psi : X' \to Y$ акслантириш φ акслантиришнинг $X' \subseteq X$ тўпламдаги *изи* дейилади, агарда $\forall x \in X'$ учун $\varphi(x) = \psi(x)$ тенглик ўринли бўлса.

Берилган $\varphi : X \to Y$ акслантириш учун:

1) ихтиёрий $x \in X$ учун $\varphi(x) = y \in Y$ элемент мавжуд бўлиб, баъзи $y \in Y$ элементлар учун $\varphi^{-1}(y) = x$ тенгликни қаноатлантирувчи $x \in X$ элементлар

мавжуд бўлмаса, бундай акслантириш *сюръектив* ёки устига акслантириш дейилади;

2) $x_1 \neq x_2$ бўлган $\forall x_1, x_2 \in X$ элементлар учун $y_1 = \varphi(x_1) \neq \varphi(x_2) = y_2$ шу каби бўлса, бундай акслантириш *инъектив* акслантириш дейилади.

3) бир пайтнинг ўзида ҳам *сюръективлик* ҳам *инъективлик* шартлари бажарилса, бундай акслантириш *биектив* ёки *ўзаро бир қийматли* акслантириш дейилади.

Ушбу $\varphi : X \to Y$ ва $\psi : Y \to Z$ акслантиришларнинг *кўпайтмаси* (*композицияси*, *суперпозицияси*) деб, $\sigma(x) = \psi(\varphi(x))$ тенгликни қаноатлантирувчи $\sigma : X \to Z$ акслантиришга айтилади ҳамда $\sigma = \psi \cdot \varphi$ кўринишда ифодаланади.

$\varphi : X \to X$ акслантириш X - тўпламни *ўзини-ўзига* акслантириш дейилади.

$\forall x \in X$ элемент учун $I(x) = x$ тенгликни қаноатлантирувчи X - тўпламни ўзини-ўзига акслантирувчи I - акслантириш *бирлик* (*айнан*) акслантириш дейилади.

Агар $\psi \cdot \varphi = \varphi \cdot \psi = I$ шарт бажарилса, берилган $\varphi : X \to Y$ ва $\psi : Y \to X$ - акслантиришлар *ўзаро тескари* акслантиришлар дейилади ҳамда $\psi^{-1} = \varphi, \quad \varphi^{-1} = \psi$ деб ёзилади.

Тескариси мавжуд бўлмаган акслантиришлар *бир томонлама* акслантиришлар дейилади.

Бирор $x \in X$ элемент учун $\varphi(x) = x$ тенглик бажарилса, бу элемент φ акслантиришнинг қўзғалмас элементи дейилади.

Элементлари сони n та бўлган X - тўпламни ўзини-ўзига биектив акслантирувчи φ - акслантириш X - тўпламда *n-даражали ўрнига қўйиш* дейилади. Агарда тўплам $X = \{x_1, \dots, x_n\}$ бўлса, у ҳолда φ - акслантириш қуйидагича:

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

ёзилади, бу ерда $(i_1, \dots, i_n)$ - индекслар $(1,2,\dots,n)$ - сонларнинг ўрин алмаштиришларидан иборат.

Агарда ўрнига қўйиш акслантириши φ ушбу $\varphi^{-1} = \varphi$ тенгликни қаноатлантирса, у ҳолда бу акслантириш *инволюция* дейилади.

X -тўпламни ўзини-ўзига акслантирувчи φ - ўрнига қўйиш акслантириши $x_i, x_j \in X$ элементлар учун $\varphi(x_i) = x_j$ ва $\varphi(x_j) = x_i$ тенгликларни қаноатлантириб, X -тўпламнинг бошқа элементлари бу акслантиришга нисбатан қўзғалмас элементлар бўлса, бундай φ -акслантириш x_i ва x_j элементларнинг X -тўпламдаги *транспозицияси* дейилади.

2.3. Бинар муносабатлар

Исталган иккита X ва Y тўплам учун барча $O \subset X \times Y$ қисм тўпламлар X ва Y тўплам ўртасидаги бинар муносабат деб айтилади [12].

X га нисбатан $\sim$ бинар муносабат эквивелентлик муносабати дейилади, агарда барча $x, x_1, x_2 \in X$ учун қуйидаги шартлар бажарилса:

1. $x \sim x$ (рефлексивлик);
2. $x \sim x_1 \Rightarrow x_1 \sim x$ (симметриклик);
3. $x \sim x_1,\ x_1 \sim x_2 \Rightarrow x_2 \sim x$ (транзитивлик).

Берилган x га эквивалент бўлган барча элементлар қисм тўплами $H = \{x' \in X | x' \sim x\} \subset X$ x ни ўз ичига олган эквивалентлик синфи дейилади.

$x \sim x$ (1-шарт) бажарилса, у ҳолда $x' \in H$ бўлади. $x' \in H$ нинг исталган элементи H синфининг вакили дейилади.

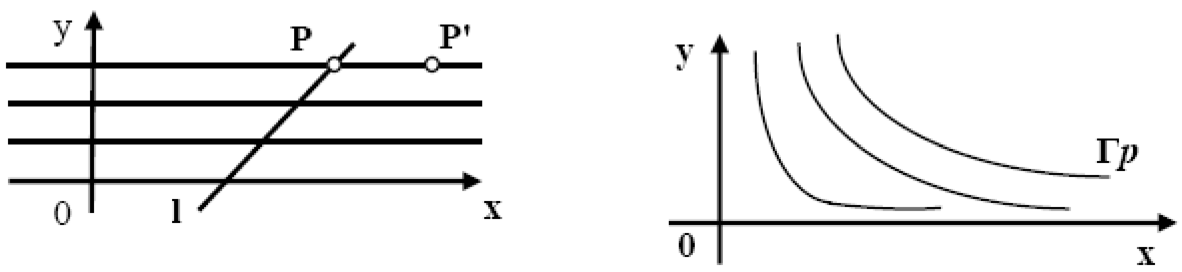
Теорема. X кесишмайдиган қисмтўпламлар бирлашмаси бўлиб, $\sim$ муносабат бўйича эквивалентлик синфи тўплами унинг таркибий қисми ҳисобланади.

Исбот. $x\in H$ дан $X=\cup H_i$ келиб чиқади. Сўнгра ихтиёрий вакили орқали H аниқлаб олинади, яъни $H_i=H_j \Leftrightarrow x_i\sim x_j$. Бир томонга: $x_i\sim x_j$ ва $x\in H_i \Rightarrow x\sim x_i \Rightarrow x\sim x_j \Rightarrow x\in H_j \Rightarrow H_i\subset H_j$ бажарилади. Аммо $x_i\sim x_j \Rightarrow x_j\sim x_i$ (2-шарт). бўлгани учун $H_j\subset H_i$ бажарилади. Демак $H_j=H_i$ яъни $x\in H$ бўлса, у ҳолда $H_i=H \Rightarrow x\in H_i \Rightarrow x\sim x_i$.

Агар $H_j\cap H_i\neq\varnothing$ ва $x\in H_j\cap H_i$ бўлса, у ҳолда $x\sim x_i$ ва $x\sim x_j$ бўлади, транзитивлик шартидан $x_i\sim x_j$ ва $H_j=H_i$ га эга бўлинади.. Демак турли синфлар кесишмайди. Теорема исботланди.

Мисол. Тўғрибурчакли координаталар тизимида $V=R^2$ – текислик берилган бўлсин. У ҳолда ~ хоссасидан келиб чиқиб $P,\ P'\in V$ нуқталарнинг бирор горизонтал тўғри чизиққа тегишлилигидан горизонтал тўғри чизиқлар синфи билан эквивалентлик муносабати келиб чиқади (8 а)-расм).

$xy=p>0$ шаклдаги $Гр$ гипербола $V_+\subset V$ соҳада $x>0,\ y>0$ координатали $P(x,\ y)$ нуқта билан эквивалентлик муносабатини аниқлайди. (8 b)-расм)



а) b)

8-расм. Эквивалентлик муносабати

2.4. Арифметиканинг асосий теоремаси

Арифметика натурал сонлар хоссалари билан шуғулланувчи фан бўлиб, унда қадимдан асосий эътибор туб сонларга қаратилиб келинган. Туб сонларнинг фундаментал хоссасини *арифметиканинг асосий теоремаси очиб беради* [12].

Асосий теорема. Бирдан бошқа ихтиёрий натурал сон туб сон ёки туб сонлар кўпайтмаси шаклида ёзилади, агар бу кўпайтмада кўпайтувчиларнинг ўрни эътиборга олинмаса, у ҳолда бу кўпайтма ягона бўлади.

Бу теорема биринчи қисмининг содда исботи Евклиднинг VII "Бошланғич" китобида келтирилган ва унинг тўла шакли (кўпайтманинг ягоналиги билан биргаликда) К.Ф. Гаусс томонидан берилган.

Мазкур теоремадан бирдан бошқа ихтиёрий натурал сон a нинг каноник ёйилмаси

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

шаклида ифодаланиши аён бўлади. Бу ерда $p_1, p_2, \dots, p_n$ ҳар хил туб сонлар, $\alpha_1, \alpha_2, \dots, , \alpha_n$ - бирга тенг ёки ундан катта даража кўрсаткичлари, $n \geq 1$.

Назорат саволлари

1. Тўплам деб нимага айтилади ?
2. Қандай тўпламларни биласиз?
3. Тўпламлар жуфтлиги учун қандай амаллар аниқланган?
4. Амалларнинг асосий хоссалари нималардан иборат?
5. Тўпламнинг асосий хоссалари нималардан иборат?
6. Тўпламларни акслантириш деганда нимани тушунасиз?
7. Бинар муносабатлар деганда нимани тушунасиз?
8. Арифметиканинг асосий теоремасига таъриф беринг?

3. ТЎПЛАМЛАР УСТИДА АЛГЕБРАИК АМАЛЛАР

3.1. Бинар амаллар

Фараз қилинсинки, ихтиёрий X тўплам берилган бўлсин. Декарт квадрат $X^2=X\mathrm{x}X$ ни X га ихтиёрий (фиксирланган) акслантириш φ: $X\mathrm{x}X\to X$ шу тўплам X да берилган *бинар алгебраик амал* деб аталади [12-13].

Шундай қилиб, X нинг ҳар қандай тартибланган элементлари жуфти (a, b) га $\varphi\ (a, b)$ мос қўйилади. Баъзида $\varphi\ (a, b)$ ўрнига $a\varphi b$ ёзилади, кўпинча φ ўрнида махсус символлар “*” ёки “+” ишлатилади.

3.1-таъриф. Бинар амал:

1) комутатив дейилади, агарда амал натижаси унинг операнд(элемент)лари ўрнини алмаштиришга боғлиқ бўлмаса, яъни

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

2) ассоциатив дейилади, агарда $(a*b)*c=a*(b*c),\qquad \forall a,b,c\in X$ тенгликни қаноатлантирса;

3) альтернатив дейилади, агарда $(a*a)*b=a(a*b)$ ва $y*(x*x)=(y*x),$ $\forall a,b,c\in X$ тенгликларни қаноатлантирса.

3.2. Яримгруппалар ва моноидлар

3.2-таъриф. Битта ва ундан ортиқ амаллар аниқланган бирор G-тўплам *алгебраик тизим* ёки *алгебраик тузилма (структура)* дейилади.

3.3-таъриф. Бирор G-тўпламда “*” - бинар амал (муносабат) аниқланган бўлиб, қуйидаги:

1) *ёпиқлилик* – ихтиёрий элементлар a, $b\in G$ жуфтига элемент $c\in G$ мос қўйилган, бунда c-элемент a ёки b - элемент билан мос тушиши ҳам мумкин;

2) “*”- амал *ассоциатив*, яъни $\forall a, b, c \in G$ бўлган элементлар учун ушбу

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

муносабат ўринли;

3) G-тўпламда ушбу $a*e = e*a = a$ шартни қаноатлантирувчи e бирлик элемент мавжуд;

3.4-таъриф. Ёпиқлилик шартини қаноатлантирувчи алгебраик тузилма $<G, *>$ *группоид* дейилади.

3.5-таъриф. Ёпиқлилик ва *ассоциативлик* шартларини қаноатлантирувчи алгебраик тузилма $<G, *>$ *яримгуппа* дейилади.

3.6-таъриф. Ёпиқлилик ва *ассоциативлик* шартларини қаноатлантирувчи ҳамда бирлик элементга эга бўлган алгебраик тузилма $<G, *>$ *моноид* дейилади.

3.3. Группалар. Асосий тушунчалар ва таърифлар

Элементар арифметикада ассоциативлик хоссасига эга бўлган қўшиш ва кўпайтириш амалларидан фойдаланилади. *Ассоциативлик хоссасига эга бўлган битта амал аниқланган алгебраик тузилма группа ҳисобланади.*

Агар $\forall a \in G$ элемент учун $a*a^{-1} = a^{-1}*a = e$ муносабатни қаноатлантирувчи тескари элемент $a^{-1} \in G$ мавжуд шартлари бажарилган бўлса, бу $<G, *>$ - алгебраик тузилма *группа* ташкил этади дейилади.

3.7-таъриф. Группада аниқланган амал “+” - қўшиш амали хусусиятларига эга бўлиб, a-элементга қарама-қарши ишорали $-a$ – элементдан иборат ҳамда шунга мос равишда бирлик элемент 0 (ноль) бўлса, бундай группа *аддитив группа* дейилади.

3.8-таъриф. Группада аниқланган амал “*”- кўпайтириш амали хусусиятларига эга бўлиб, a-элементга тескари элемент $a^{-1} = \frac{1}{a}$ ҳамда шунга мос равишда бирлик элемент 1 (бир) бўлса, бундай группа *мультипликатив группа* дейилади.

3.9-таъриф. Мультипликатив группа <*G*, *> *циклик* дейилади, агарда шундай элемент $a \in G$ мавжуд бўлсаки, ҳар бир элемент $b \in G$ учун шундай натурал сон k мажуд бўлиб, $b=a^{k}$ тенглик ўринли бўлса. Бу сон a мультипликатив группанинг *ясовчиси* (*тузувчиси*) дейилади. Келтирилган таърифдан ихтиёрий циклик группанинг коммутатив эканлиги келиб чиқади.

3.10-таъриф. Группа *чекли* дейилади, агарда у чекли сондаги элементлардан иборат бўлса. Бунда чекли группа элементларининг сони унинг *тартиби* дейилади ҳамда $|G|$ ёки $\#G$ кўринишида белгиланади.

3.11-таъриф. Агарда <*G*, *> - алгебраик тузилма *группа* ташкил этиб, $\forall a, b \in G$ учун ушбу $a*b = b*a$ тенглик ўринли бўлса, бундай группа *коммутатив* ёки *Абель* группаси дейилади.

3.12-таъриф. Группада аниқланган амал “+” - қўшиш амали хусусиятларига эга бўлиб, *a*-элементга қарама-қарши ишорали -*a* – элементдан иборат ҳамда шунга мос равишда бирлик элемент *0* (ноль) бўлса, бундай группа *аддитив группа* дейилади.

3.13-таъриф. Группада аниқланган амал “*”- кўпайтириш амали хусусиятларига эга бўлиб, *a*-элементга тескари элемент $a^{-1}=\frac{1}{a}$ ҳамда шунга мос равишда бирлик элемент 1 (бир) бўлса, бундай группа *мультипликатив группа* дейилади.

3.14-таъриф. Мультипликатив группа <*G*, *> *циклик* дейилади, агарда шундай элемент $a \in G$ мавжуд бўлсаки, ҳар бир элемент $b \in G$ учун шундай натурал сон k мажуд бўлиб, $b=a^{k}$ тенглик ўринли бўлса. Бу сон a мультипликатив группанинг *ясовчиси* (*тузувчиси*) дейилади. Келтирилган таърифдан ихтиёрий циклик группанинг коммутатив эканлиги келиб чиқади.

3.15-таъриф. Группа *чекли* дейилади, агарда у чекли сондаги элементлардан иборат бўлса. Бунда чекли группа элементларининг сони унинг *тартиби* дейилади ҳамда $|G|$ ёки $\#G$ кўринишида белгиланади.

3.3.1. Параметрли мультипликатив группа

Параметрли группа қуйидагича таърифланади [23].

3.16-таъриф. F_n – чекли, яъни, n та элементдан иборат бутун сонлар тўплами, ® – F_n устида $a®b \equiv a + b + a*R*b \ (mod\ n)$ кўринишидааниқланган алгебраик амал бўлса, (F_n; Ώ) – жуфтлик параметрли мультипликатив группа деб аталади; бу ерда $a, b, R \in F_n,$ параметр $R>0$,+, * – бутун сонлар устида қўшиш, кўпайтириш амалларининг ва ® – параметрли кўпайтириш амалининг белгилари.

Параметрли кўпайтириш амали ўз моҳияти бўйича тернар амалдир.

Нолдан фарқли тўплам элементи a учун тескари элемент $a^{\backslash-1}$ ва қарама-қарши элемент $n\text{-}a$ мавжуд. $a^{\backslash-1}$ параметрли тескари элемент деб аталади ва $a®a^{\backslash-1} \equiv 0 \ (mod\ n)$ шартини қаноатлантиради. Бу ерда 0 – параметрли бирлик элементи бўлиб, $a®0 \equiv a$ аксиомани қаноатлантиради.

Параметрли тескари элемент қуйидагича ҳисобланади:

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

Бу ерда $^{-1}$ - n модуль бўйича тескарилаш амалининг белгисидир.

Изоҳ – Бу ерда ва кейинги ҳарфли ифодаларда (зарурат бўлмаган ҳолларда) кўпайтириш белгиси “*” тушириб қолдирилган.

Параметрли мультипликатив коммутатив группа қуйидаги хоссаларга эга.

1-хосса: агар параметрли мультипликатив коммутатив группанинг параметри жуфт сон ва модули $n=2k$ (k - ихтиёрий натурал сон) га тенг бўлса, унинг тартиби (группа элементлари сони) $2k$ га тенг.

2-хосса: агар модули n туб сон бўлган параметрли мультипликатив коммутатив группанинг параметри ихтиёрий натурал сон бўлса, унинг тартиби $\varphi(n)$ га тенг, бу ерда $\varphi(n)$ – Эйлер пи-функцияси қиймати.

Мисол:

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

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

3-хосса: агар мураккаб модулли параметрли мультипликатив коммутатив группанинг параметри модуль *n* билан ўзаро туб бўлса, унинг тартиби $\varphi(n)$ га тенг, бу ерда $\varphi(n)$ – Эйлер пи-функцияси қиймати.

4-хосса: агар мураккаб модуль $n=pq$, бу ерда *p, q* – ҳар хил туб сонлар, параметрли мультипликатив коммутатив группанинг параметри *R* модуль *q* билан ўзаро туб бўлиб, *p* билан ўзаро туб бўлмаса, унинг тартиби $p(q\text{-}1)$ га тенг.

Параметрли мультипликатив коммутатив группанинг 1-, 2- , 4-хоссалари анъанавий мультипликатив группа $(F_n;\ *)$ хоссаларидан ўз тартиби билан фарқ қилади. Масалан, анъанавий бинар кўпайтириш амали асосида шаклланган мультипликатив группа модули $2k$ бўлганда, фақат тоқ элементлардан ташкил топган чекли тўпламда мавжуд бўлса, параметрли мультипликатив коммутатив группа бутун сонлар тўпламида мавжуддир. Мураккаб модуль $n=pq$ учун параметрли мультипликатив коммутатив группанинг параметри *R* модуль *p* билан ўзаро туб бўлиб, *q* билан ўзаро туб бўлмаса, унинг тартиби анъанавий мультипликатив группа $(F_n;\ *)$ тартибига нисбатан юқори бўлади. Булар криптотизим яратиш ва уларни таҳлиллашнинг янги имкониятларини юзага чиқариши мумкин.

3.3.2. Параметрли функцияларнинг дискрет даражага ошириш функцияси хоссаларига ўхшаш хоссалари

Ошкора криптографияга [2, 23, 50] оид носимметрик криптотизимларни яратиш битта махфийликка эга бўлган бир томонлама функциялардан фойдаланишга асосланади. Энг машҳур носимметрик криптотизимларнинг криптобардошлилиги дискрет логарифм, эллиптик эгри чизиқда дискрет логарифм ва факторлаш масалаларини ечиш асосида махфийликни топишнинг мураккаблигига асосланади. Бунда мураккаблик даражаси криптотизимдан ноқонуний (хакер) ва қонуний фойдаланувчилар учун бир хил бўлиб, катта ҳисоблаш ресурсига эга бўлган ташқи ноқонуний бузғунчилар учун криптотизимни кўпориш хавфига ўрин қолдиради. Қуйида ноқонуний бузғунчиларнинг кўпорувчилик имкониятларини йўққа чиқаришга имкон берувчи, фақат қонуний фойдаланувчилар учунгина маълум бўлган анъанавий махфийлик(даража кўрсаткичи – дискрет логарифм учун, Эйлер пи-функцияси – факторлаш учун)ка қўшимча R параметрли бир томонлама функциянинг модуль $n\in\{p,\ p_1p_2\}$ ҳоллари учун анъанавий даражага ошириш функцияси хоссаларига ўхшаш хоссалари баён қилинган [23, 51-54]. Бу ерда p – туб сон, p_1, p_2 – ҳар хил туб сонлар, R – параметр.

Хоссалар таърифларида модуль n бўйича асос a ни R параметрли x даражага ошириш натижаси $a^{\backslash x}(mod\ n)$ шаклида ифодаланган, бу ерда $x\in\{0,1,-1,e,\ d,\ z\}$, $^{\backslash}$ – R параметрли даражага ошириш белгисидир**.**

3.17-таъриф. Модуль арифметикасида параметр $R\geq 1$ билан даражага ошириш функцияси параметрли функция деб аталади.

Параметрли функцияларнинг чекли группа ва ҳалқада дискрет даражага ошириш функцияси хоссаларига ўхшаш хоссаларига *қуйидагилар киради:*

1-хосса. $a^{\backslash z+d}\equiv a^{\backslash z} ® a^{\backslash d}\ (mod\ n),\ a^{\backslash z}\equiv a^{\backslash z}®0\ (mod\ n),$ бу ерда ® – модуль n бўйича R параметрли кўпайтириш амалининг белгиси, 0 – бирлик элементи, $^{\backslash}$ – параметр R билан даражага ошириш белгиси, $a,\ z,\ d\ \in\{1,2,.\ ..,\ n\text{-}1\};$ анъанавий (параметрсиз) даражага ошириш функциясида $a^{z+d}\equiv a^z a^d\ (mod\ n),$ $a^{z}\equiv a^{z}\ 1\ (mod\ n).$

2-хосса. $a^{\backslash zd}\equiv(a^{\backslash z})^{\backslash d}\equiv\ (a^{\backslash d})^{\backslash z}(mod\ n),$ бу ерда $a\in\{1,2,.\ ..,\ n\text{-}1\},$ $^{\backslash}$ – параметр R билан даражага ошириш белгиси, $z,\ d\in\{1,2,.\ ..,\ \varphi(n)\ \text{-}1\};$ анъанавий (параметрсиз) даражага ошириш функциясида $a^{zd}\equiv(a^{z})^{d}\equiv(a^{d})^{z}$ $(mod\ n).$

Юқорида келтирилган хоссалар параметрли функция қийматини исталган даража кўрсаткичи учун самарали ҳисоблаш учун етарлидир. Бу ерда катта даражага ошириш жараёни, экспоненциал функцияни ҳисоблаш жараёни каби кечиб, даврий тарзда $x=2$ (квадратлаш) даражага ошириш ва ҳосил бўлган аввалги натижани асосга параметрли кўпайтириш амалларидан фойдаланишдан иборат бўлади.

3-хосса. $a^{\backslash\varphi(n)+1} \equiv a(mod\ n)$, $a^{\backslash 0} = 0$, $a^{\backslash 1} = a$, бу ерда $\varphi(n)$ – Эйлер пи-функцияси, $a \in\{1,2,. .., n-1\}$; анъанавий (параметрсиз) даражага ошириш функциясида $a^{\varphi(n)+1} \equiv a\ (mod\ n)$, $a^0 = 1$, $a^1 = a$.

4-хосса. Агар d , e $\varphi(n)$ билан ўзаро туб бўлиб, $\varphi(n)$ модули бўйича ўзаро тескари жуфтлик бўлса, унда $(a^{\backslash d})^{\backslash e} \equiv a\ (mod\ n)$, бу ерда $a \in\{1,2,. .., n-1\}$, $^{\backslash}$ – параметр R билан даражага ошириш белгиси; анъанавий (параметрсиз) даражага ошириш функциясида $(a^d)^e \equiv a\ (mod\ n)$.

Мисол:

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-хосса (ечим мавжудлиги шарти). Агар $a \circledR x \equiv b\ (mod\ n)$ бўлса, унда ечим x мавжуд бўлиши учун $a^{\backslash -1}(mod\ n)$ мавжуд бўлиши шарт, бу ерда $a, b \in\{1,2,. .., n-1\}$, $\circledR$ – модуль n бўйича R параметрли кўпайтириш амалининг белгиси, $x \equiv b \circledR a^{\backslash -1}(mod\ n)$; анъанавий (параметрсиз) таққослама $ax \equiv b\ (mod\ n)$ учун $x \equiv ba^{-1}\ (mod\ n)$.

Мисол:

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

6-хосса (параметрли квадратик чегирма). Параметрли Z^*_n группанинг элементи бўлган a сони учун, бу ерда $n>1$, параметрли Z_n группада $b^{\backslash 2} \equiv a\ (mod\ n)$ шартни қаноатлантирувчи b сони мавжуд бўлса, унда a сони модуль n бўйича R параметрли квадратик чегирма, акс ҳолда R параметрли квадратик чегирма эмас;

анъанавий квадратик чегирма a учун $b^2 \equiv a\ (mod\ p)$ шартни қаноатлантирувчи b сон мавжудлиги назарда тутилади.

7-хосса (параметрли Лежандр символи). Агар a сони р тоқ туб модуль параметрли квадратик чегирма бўлса, унда параметрли Лежандр символи $(a/p)=0$, акс ҳолда $(a/p)= (-2)R^{-1}(mod\ p);$

a сони р тоқ туб модуль квадратик чегирма бўлса, унда анъанавий (параметрсиз) Лежандр символи $(a/p)=1$, акс ҳолда $(a/p)= -1$.

8-хосса (Қулай ҳисобланадиган квадратик илдиз). 1) Агар туб модуль $p \equiv 3,7\ (mod\ 8)$, $4\,|\,(p+1)$ шартни қаноатлантирса ва a параметрли квадратик чегирма бўлса, унда квадратик илдиз $x=a^{\backslash(p+1)/4}\ (mod\ p);$

2) Агар туб модуль $p \equiv 5\ (mod\ 8)$, $8\,|\,(p+3)$ шартни қаноатлантирса ва a параметрли квадратик чегирма бўлса, унда квадратик илдиз $x=a^{\backslash(p+3)/8}\ (mod\ p);$

анъанавий ифодаларда даражага ошириш белгиси қатнашмайди.

9-хосса (Қолдиқлар ҳақида параметрли хитойча теорема). Агар $i=1,2,\ldots,k$ учун берилган тенгламалар системаси $x\equiv c_i\ (mod\ p_i)$ бўлса, $1\leq p_i< p_j \leq k$ бўлганда $EKUB(p_i, p_j) =1$ бўлса, унда

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

таққосламалар системасини қаноатлантирувчи параметрли чегирмалар синфи $\underline{I_{pi}}$ ва ягона ечим мавжуд:

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

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

модуль $n=p_1\ p_{2***}\ p_k,$ ® – модуль n бўйича R параметрли кўпайтириш амалининг белгиси, EKUB - энг катта умумий бўлувчи функциясининг номи, c_i - параметрли алгебра амаллари асосида аниқланган катталик, масалан, p_i модуль бўйича R параметр билан берилган катталикни илдиздан чиқариш натижаси;

анъанавий (параметрсиз) *қолдиқлар ҳақида* хитойча теоремада

$x \equiv \sum^{k}_{i} \underline{I_{pi}}\ c_i\ (mod\ n)$, бу ерда $\underline{I_{pi}}=((n/p_i)^{-1}(mod\ p_i))n/p_i$.

Қуйида қолдиқлар ҳақида анъанавий ва параметрли хитойча теоремаларни $a=9$ ва $a=48$ сонларининг $n=7*11=77$ бўйича квадрат илдизларидан бирини топишга мисол келтирилган.

Мисол:

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

$\underline{I_7}=2*11$	$\underline{I_{11}}=8*7$	*Квадратик илдиз*	*Илдиз*^{2} *(текшириш)*
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. Группалар морфизми

Изоморфизм

Агар $f{:}G \to G'$ акслантириш мавжуд бўлиб, f биектив бўлса (1-шарт), барча $a, b \in G$ учун $f(a*b) = f(a) \circ f(b)$ (2-шарт) ўринли бўлса, унда $<G,*>$ ва $<G,\circ>$ группалар *изоморф* дейилади,

Группаларнинг изоморфлиги $\cong$ каби белгиланади, яъни $G \cong G'$.

Изоморфизмларнинг энг содда хоссалари қуйидагилардан иборат:

1. Бирлик элемент бирлик элементга ўтади.

Ҳақиқатан, агар e – G нинг бирлик элементи бўлса, у ҳолда $e{\ast}a=a{\ast}e=a$ ва демак $f(e) \circ f(a) = f(a) \circ f(e) = f(a)$, бундан келиб чиқадики $f(e) = e'$ – G' группанинг бирлик элементи. Бунда қисман бўлса ҳам f – изоморфизмнинг иккала хусусиятидан ҳам фойдаланилади.

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

Ҳақиқатан ҳам $f(a)\circ f(a^{-1}) = f(a *a^{-1}) = f(e) = e'$. e' – G' группанинг бирлик элементи. Демак, $f(a)^{-1} = f(a)^{-1}\circ e' = f(a)^{-1}\circ (f(a)\circ f(a^{-1})) = =(f(a)^{-1}\circ f(a))\circ f(a)^{-1} = e'\circ f(a)^{-1}= f(a)^{-1}$.

3. Тескари акслантириш $f^{-1}:G\to G'$ ҳам изоморфизм бўлади. Бунинг учун f^{-1} да ҳам 2- шарт тўғрилигини текшириш етарли.

Фараз қилайлик, $a', b'\in G'$. У ҳолда f нинг биективлигига кўра $a'= f(a), b'= f(b)$ қандайдир $a,b\in G$ учун ўринли. f – изоморфизм бўлгани учун $a'\circ b' = f(a)\circ f(b) = f(a*b)$. Бундан эса $a*b = f^{-1}(a'\circ b')$ эканлиги келиб чиқади. $a= f^{-1}(a')$ ва $b= f^{-1}(b')$ эканлигини эътиборга олсак, $f^{-1}(a'\circ b') = f^{-1}(a')*f^{-1}(b')$. Демак бу хосса ҳам исботланди.

Мисол. $(R_+,*,1)$ мусбат сонларнинг мультипликатив группасини барча ҳақиқий сонларнинг аддитив группаси $(R, +,0)$га изоморф акслантириш деб $f=\ln$ ни олиш мумкин. Логарифмнинг $\ln ab=\ln a+\ln b$ хоссаси таърифидаги 2-шартни қаноатлантиради. f га тескари акслантириш $f^{-1}: x\to e^x$ бўлади. Изоморфизм таърифида $G = \cong G'$ деб $\varphi:G\to G$ изоморф акслантиришни ҳосил қиламиз. Бу акслантириш G группанинг автоморфизми дейилади.

Мисол. $e_g:g\to g$ бирлик акслантириш автоморфизмдир.

Одатда G тривиал бўлмаган автоморфизмларга ҳам эга.

Изоморф акслантиришларнинг 3-хоссаси автоморфизмга тескари бўлган акслантириш ҳам автоморфизм бўлишини кўрсатади.

Агар $\varphi,\psi \in G$ группанинг автоморфизмлари бўлса, у ҳолда $\forall\ a,b\in G$ учун $(\varphi\circ\psi)(ab)= \varphi(\psi(ab))=\varphi(\psi(a)\psi(b))=(\varphi\circ\psi)(a)*(\varphi\circ\psi)(b)$ ўринли.

Демак, G группанинг барча автоморфизмлари тўплами $G\to G$ акслантирувчи барча биекциялар тўплами $S(G)$ нинг қисм группаси бўлган $Aut(G)$ группани ҳосил қилади.

Гомоморфизмлар

G группанинг автоморфизмлари группаси $Aut(G)$да битта махсус қисм группа бор. Уни $Inn(G)$ билан белгиланади ва ички автоморфизмлар группаси деб аталади. Қуйидаги акслантиришлар бу группанинг элементлари бўлади: I_a: $g\rightarrow aga^{-1}$. Бу ерда $I_a^{-1}= I_{a-1}$, I_e – бирлик автоморфизм, $I_a o\, I_b= I_{ab}$, чунки $(I_a o\, I_b)(g)= I_a(I_b (g))= I_a(bgb^{-1})=abgb^{-1}a^{-1}= abg(ba)^{-1}= I_{ab}(g)$.

Сўнгги тенглик G группани унинг ички автоморфизмлар группаси $Inn(G)$ га акслантирувчи $f(a)=I_a$, $a \in G$ формула билан аниқланган акслантириш изоморф акслантиришнинг $f(a) \circ f(b) = f(a*b)$ шартини қаноатлантиради, бироқ бунда биективлик шарти бажарилмайди.

Агар G Абель группаси бўлса, у ҳолда барча $a \in G$ учун $aga^{-1}=g$ ўринли ва демак, $I_a= I_e$, яъни бутун $Inn(G)$ группа фақат битта I_e элементдан иборат.

Агар барча $a, b \in G$ учун $f(a*b) = f(a) \circ f(b)$ ўринли бўлса, унда $<G,*>$ группани $<G, \circ >$ группага акслантирувчи $f:G \rightarrow G'$ акслантириш гомоморфизм деб аталади.

$Ker\ f=\{g \in G\ |f(g)=e'$ – G' группанинг бирлик элементи$\}$ тўплам f гомоморфизмнинг ядроси деб аталади.

Группани ўз-ўзига гомоморф акслантириш эндоморфизм деб аталади. Гомоморфизмнинг таърифида f акслантиришдан биективлик талаб қилинмайди. Лекин шунга қарамай f гомоморфизмнинг изоморфизмдан асосий фарқи, унда тривиал бўлмаган $Ker\, f$ ядронинг мавжудлигидир.

Агар $Ker\, f=\{e\}$ бўлса, у ҳолда $f:G\rightarrow Inn\, f$ – изоморфизм бўлади.

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

Демак, $Ker\, f$ ядро G группанинг қисм группаси экан.

Фараз қилайлик, $H= Ker\ f\subset G$ бўлсин. У ҳолда $\forall h \in H$, $g \in G$ учун $f(ghg^{-1})=f(g)f(h)f(g^{-1})=f(g)e' f(g^{-1})= e'$, *яъни* $ghg^{-1} \in H$ бўлади. Бу дегани $ghg^{-1}\subset H$ бунда g *ни* g^{-1} билан, g^{-1} ни g билан алмаштириб, $g^{-1}\ hg\subset H$ *яъни*, $H\subset ghg^{-1}$ эканини аниқлаймиз. Демак, $\forall g \in G$ учун $H= ghg^{-1}$. Бу хосса эга бўлган қисм группа нормал қисм группа деб аталади.

3.5. Ҳалқа. Таъриф ва умумий хоссалар

3.18-таъриф. Бирор G-тўпламда иккита “+” - қўшиш ва “*” - кўпайтириш бинар амаллар (муносабатлар) аниқланган бўлиб, қуйидаги:

1) G-тўплам аддитив Абель группасини ташкил этади;

2) кўпайтириш амали ассоциатив, яъни $\forall$ a, b, $c \in G$ бўлган элементлар учун ушбу

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

муносабат ўринли;

3) дистрибутивлик қонуни ўринли, яъни $\forall$ a, b, $c \in G$ бўлган элементлар учун ушбу

$$a\,(b+c) = ab+ac \text{ ва } (a+b)\,c = ac+bc$$

муносабатлар ўринли шартлари бажарилган бўлса, бу $<G, +, *>$ - алгебраик тузилма *ҳалқа* ташкил этади дейилади.

Битта (тегишли хоссаларга эга бўлган) амал аниқланган группа ташкил этувчи тўпламдан фарқли равишда ҳалқа ташкил этувчи тўпламда унинг таърифида келтирилган хоссаларга эга бўлган иккита амал аниқланган.

3.19-таъриф. Ҳалқа *бирлик элементли* дейилади, агарда мультипликатив бирлик элементга эга бўлса, яъни шундай элемент $1 \in G$ мажуд бўлсаки, унинг учун ушбу $a1=1a=a$ муносабат $\forall\, a \in G$ элементда бажарилади.

3.20-таъриф. Ҳалқа *коммутатив* дейилади, агарда кўпайтириш амали коммутативлик хоссасига эга бўлса.

3.21-таъриф. Ҳалқа *бутун* ёки *бутун соҳали* дейилади, агарда у $e \neq 0$-бирлик элементли коммутатив ҳалқа ташкил этиб, a, $b \in G$ элементлар учун $ab=0$ муносабатдан $a=0$ ёки $b=0$ келиб чиқса.

3.22-таъриф. G – ихтиёрий ҳалқа бўлсин. Шундай натурал сон $p \in \{1,2,3,\ldots\}$ мавжуд бўлсаки, ҳар бир элемент $g \in G$ учун $pg = 0$ бажарилса, у ҳолда энг кичик шундай p-сон G-ҳалқанинг *характеристикаси* дейилади.

Агарда шундай натурал сон мавжуд бўлмаса, у ҳолда ҳалқа *0* (ноль) характеристикага эга дейилади. Ҳалқанинг *тартиби* шу ҳалқанинг аддитив группаси тартиби билан аниқланиб, ҳалқанинг элементлари сонига тенг.

3.6. Майдонлар

3.23-таъриф. Бирор G-тўпламда иккита “+” - қўшиш ва “*” - кўпайтириш бинар амаллар (муносабатлар) аниқланган бўлиб, қуйидаги:

1) G-тўплам *0* (ноль) бирлик элементли аддитив Абель группасини ташкил этади;

2) G-тўпламнинг нолдан фарқли элементлари *1*(бир) бирлик элементли мультипликатив Абель группасини ташкил этади; кўпайтириш амали ассоциатив, яъни $\forall a, b, c \in G$ бўлган элементлар учун ушбу

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

муносабат ўринли;

3) қўшиш ва кўпайтириш амаллари дистрибутивлик қонуни билан боғланган;

4) қўшиш ва кўпайтириш амаллари учун тескари амаллар мавжуд: айириш ва бўлиш (нолга бўлишдан ташқари) шартлари бажарилган бўлса бу $<G, +, *>$ - алгебраик тузилма *майдон* ташкил этади дейилади.

3.24-таъриф. Агар майдон ташкил этувчи тўплам q-чекли сондаги элементлардан иборат бўлса, у ҳолда майдон *чекли майдон* ёки *Галуа майдони* дейилади ва $GF(q)$ ёки F_q деб белгиланади.

1-тасдиқ. Чекли майдон мавжуд бўлиши учун майдоннинг элементлари сонини ифодаловчи q-туб сон бўлиши ёки туб соннинг даражаси $q=p^m$, бу ерда p - туб сон, m - натурал сон кўринишида ифодаланаши зарур ва етарли. Бунда p - туб сон $GF(q)$ - чекли майдоннинг *характеристикаси*, m сони $GF(q)$ майдоннинг $GF(p)$ қисм майдонга нисбатан *даражаси* дейилади ҳамда $m=1$ бўлса, *оддий*, акс ҳолда *кенгайтирилган* майдон дейилади. Агар *p* - туб сон бўлмаса, у ҳолда <*G*, +, *> - алгебраик тузилмада аниқланган қўшиш ва кўпайтириш амаллари бирор *n*-асосли модуль (mod *n*) бўйича аниқланган бўлса, ҳатто нолдан фарқли элементга бўлиш ҳар доим ҳам мумкин бўлавермайди ва бу тузилма майдон ташкил этмай ҳалқа ташкил этади.

Ҳар қандай майдоннинг барча элементлари тўплами қўшиш амалига кўра аддитив Абель группасини ва нолдан фарқли барча элементлари тўплами кўпайтириш амалига нисбатан мультипликатив циклик группа ташкил этади.

Мумкин бўлган ҳар бир *q* – тартиб учун фақат битта майдон мавжуд, яъни барча *q* – тартибли чекли майдонлар изоморфдир. Мисол учун, агарда *q*=*p* – туб сон бўлса, у ҳолда майдоннинг элементлари *0, 1, ..., (p-1)* – сонлар бўлиб, қўшиш ва кўпайтириш амаллари mod *p* қўшиш ва кўпайтириш амалларидан иборат, яъни $GF(p)=Z/p$. Шундай қилиб, туб сонли модуль бўйича чегирмалар ҳалқаси оддий майдон ташкил этади.

2-тасдиқ. Ихтиёрий $GF(q)$ - чекли майдоннинг нолдан фарқли элементлари мультипликатив циклик группа ташкил этади.

3.20-таъриф. Циклик группанинг α - *ясовчиси* (*тузувчиси, генератори*) чекли майдоннинг примитив элементи дейилади ҳамда бу майдоннинг барча элементларини қуйидагича ифодалаш мумкин:

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

3.6.1. Майдон устида берилган диаматрицалар алгебраси

3.21-таъриф. Ď – чекли, яъни *n* та элементдан иборат бутун сонлар майдони устида аниқланган квадрат диаматрицалар чекли тўплами, *Ώ = {+, ®'}* – *Ď* устида аниқланган алгебраик амаллар тўплами бўлса, *<Ď; Ώ>* – жуфтлик диаматрицалар алгебраси деб аталади; бу ерда ўзаро мос тарзда + – қўшиш, ®' – диаматрицавий кўпайтириш амалларининг белгиларидир.

Мазкур такомиллашган диаматрицалар алгебраси [23] да келтирилган алгебрадан амаллар чекли тўплам устида берилган диаматрицалар тўплами устида аниқланиши, барча амаллар диаматрицалар тўплами устида аниқланиб диаматрица ҳосил этилиши билан фарқланади.

Натижавий диаматрица $C \equiv A\text{®}'B \ (mod \ n)$ элементлари диагонал ҳамда нодиагонал элементлар учун турлича ифодалар асосида ҳисобланади.

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

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

Диаматрицавий кўпайтириш амали матрицавий кўпайтириш амалига нисбатан мукаммал шифрлар яратиш муаммоси нуқтаи назаридан қулай эканлигини илмий криптология асосчиси Клод Шенноннинг [24] мукаммал шифр яратишда ишлатиладиган алмаштиришлари яхши аралашиш ва кенг ёйилишга олиб келиши лозимлиги ҳақидаги тавсиялари кўпроқ мос келиши сабабли O‘z DSt 1105:2006, O‘z DSt 1105:2009 - Маълумотларни шифрлаш алгоритмларига асос этиб олинган. Буни қуйидаги мисоллардан кўриш мумкин.

3.1- ва 3.2-мисолларда модуль $n=256$ бўлганда 4-тартибли диаматрицаларнинг ва матрицаларнинг 1 тадан элементлари ўзгарганда натижавий матрицаларда ўзгарган соҳалар акс этган:

3.1-мисол: *d* матрицавий кўпайтма

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

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

3.2-мисол: Матрицавий кўпайтма

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

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

Мисоллардан кўриниб турибдики, диаматрицавий кўпайтма натижасида *A* нинг *1* та элементи ўзгарганда *C* да *7* та элемент ўзгарган; матрицавий кўпайтмада эса, *1* та устун ёки сатр элементлари, яъни *4* та элемент ўзгарган.

3.6.2. Майдон устида берилган эллиптик эгри чизиқ нуқталари группаси

Эллиптик эгри чизиқ

Ҳозирда эллиптик эгри чизиқларнинг криптография соҳасига татбиқи кенг қўлланилмоқда. Ушбу параграфда эллиптик эгри чизиқ ва унинг нуқталари ҳақида умумий тушунчалар ҳамда уларга боғлиқ бўлган амаллар билан танишиш мумкин.

3.22-таъриф. Бирор *K*-майдонда олинган эллиптик эгри чизиқ деб, қуйидаги Вейерштрасс тенгламаси деб аталувчи тенглик орқали аниқланувчи

$$y^2 + a_1xy + a_3y = x^3 + a_2x^2 + a_4x + a_6 \tag{1}$$

эгри чизиққа айтилади, бу ерда $a_1, a_2, a_3, a_4, a_6 \in K$.

Эллиптик эгри чизиқ одатда E ёки E/K билан белгиланади ва эллиптик эгри чизиққа тегишли нуқталар, яьни (1) тенглама ечимлари шу эллиптик эгри чизиқнинг *аффин нуқталари* дейилади.

3.23-таъриф. $P(x_0,y_0)\in E$ нуқта эллиптик эгри чизиқнинг силлиқ нуқтаси дейилади, агар

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

бўлиб, қуйидаги шартлардан биттаси ўринли бўлса:

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

3.24-таъриф. E/K – эллиптик эгри чизик силлиқ деб аталади, агар унинг ҳар бир аффин нуқтаси силлиқ бўлса.

1-мисол. $y^2=x^3$ эллиптик эгри чизиқ учун *(0;0)* нуқта силлиқ нуқта эмаслиги кўрсатилсин.

Ечиш.

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

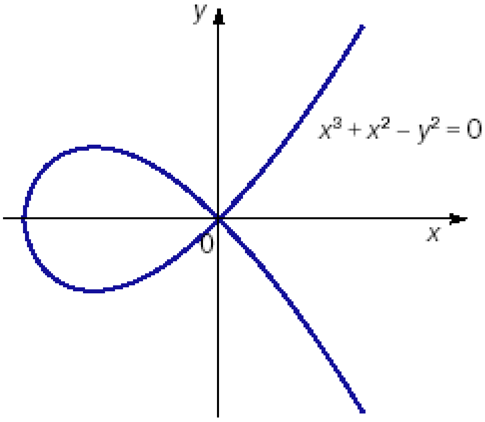
бўлиб, (2) шартга нисбатан зиддиятга келинади. Натижада, *(0;0)* нуқтанинг ҳақиқатан ҳам силлиқ нуқта бўла олмаслиги келиб чиқади.

2-мисол. $y^2=x^3+x^2$ эллиптик эгри чизиқ учун *(0;0)* нуқта силлиқ нуқта эмаслиги кўрсатилсин.

Ечиш. Ҳақиқатан ҳам,

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

бўлиб, (2) шартга нисбатан зиддиятга келинади. Натижада, *(0;0)* нуқтанинг ҳақиқатан ҳам силлиқ нуқта бўла олмаслиги келиб чиқади:



Қуйида эллиптик эгри чизиқларнинг умумий каноник кўриниши ҳисобланган ушбу

$$y^2 = x^3 + ax^2 + bx + c, \tag{3}$$

тенглама билан иш кўрамиз, бу ерда $a,b,c \in Z$ (a,b,c - бутун сонлар) ва кўпҳад $p(x) = x^3 + ax^2 + bx + c$ каррали илдизга эга эмас деб қаралади.

Эллиптик эгри чизиқларнинг графиклари

Юқорида келтирилган (3) кўринишдаги эгри чизиқ графигини чизиш учун

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

чизиш ва Ox – ўқига нисбатан симметрик акслантириш лозим. Бу (4) берилган функция графигини чизиш учун эса квадратсиз ҳолидаги функция

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

графигини чизиб олиш керак бўлади. Функция графигининг Ox-ўқи билан кесишиш нуқталари

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

тенгламанинг ечимларини топиш орқали аниқланади. Бу тенгламадан,

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

алмаштиришдан фойдаланиб,

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

келтирилган тенглама олинади, бу ерда $p = \dfrac{3b - a^2}{3}$, $q = \dfrac{2a^3}{27} - \dfrac{ab}{3} + c$. $D = \left(p\big/3\right)^3 + \left(q\big/2\right)^2$ ифода дискриминант деб аталиб, келтирилган тенгламанинг илдизлари сони дискриминант қийматининг ишорасига боғлиқ:

а) $D > 0$ бўлса, битта ҳақиқий илдизга эга, яъни функция графиги Ox-ўқи билан битта нуқтада кесишади;

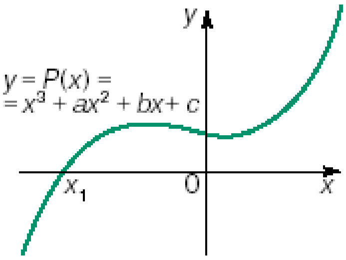
б) $D<0$ бўлса, учта ҳақиқий илдизга эга, яъни функция графиги Ox-ўқи билан учта нуқтада кесишади;

с) $D=0$ бўлса, учта ҳақиқий илдизга эга бўлиб, уларнинг иккитаси тенг (каррали), яъни функция графиги Ox-ўқи билан иккита нуқтада кесишади.

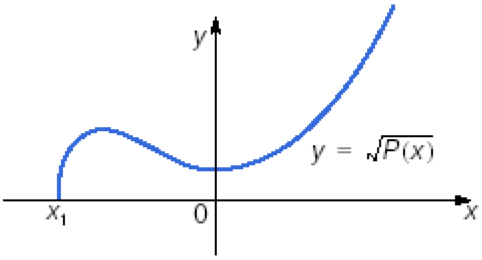
Келтирилган ҳол учун

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

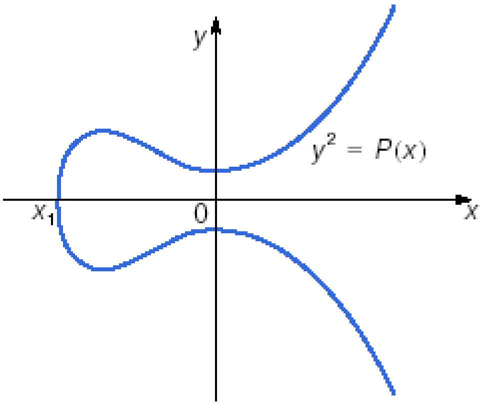
функция графиги қуйидаги кўринишга эга:



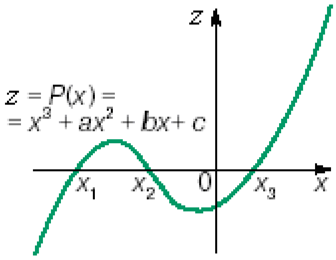
Бу графикдан (4) функция графигини олиш учун, квадрат илдиз остидаги ифоданинг манфий бўлмаган қийматлар соҳасига мос келувчи - аниқланиш соҳасининг қисми



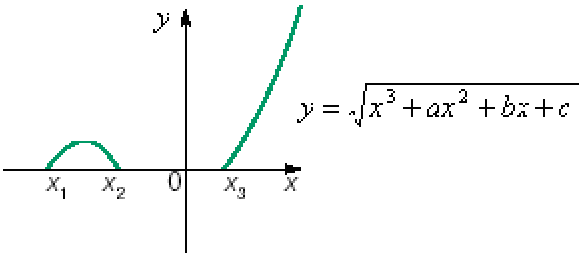
Ox - ўқига нисбатан симметрик кўчирилади, яъни:



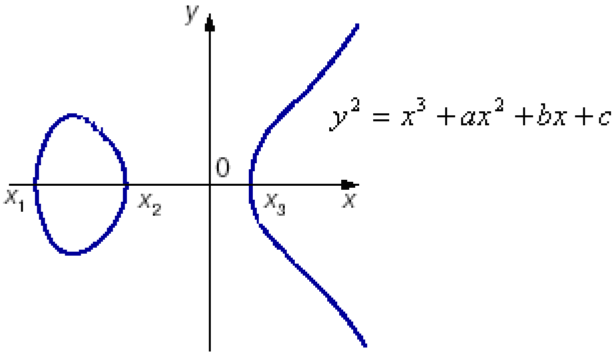
Учта ҳақиқий илдизга эга бўлган б) ҳол учун $z=x^3+ax^2+bx+c$, функция графиги қуйидаги кўринишга эга:



Худди юқоридаги фикр ва мулоҳазаларга кўра, бу графикдан (4) функция графигини олиш учун, квадрат илдиз остидаги ифоданинг манфий бўлмаган қийматлар соҳасига мос келувчи - аниқланиш соҳасининг қисми



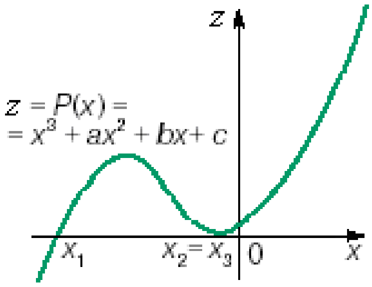
Ox - ўқига нисбатан симметрик кўчирилади, натижада график эллипс ва гиперболадан иборат бўлган иккита қисмлар билан ифодаланади:



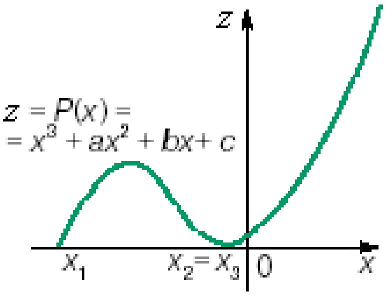
Учта ҳақиқий илдизга эга бўлиб, уларнинг иккитаси тенг (каррали) бўлган c) ҳол учун

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

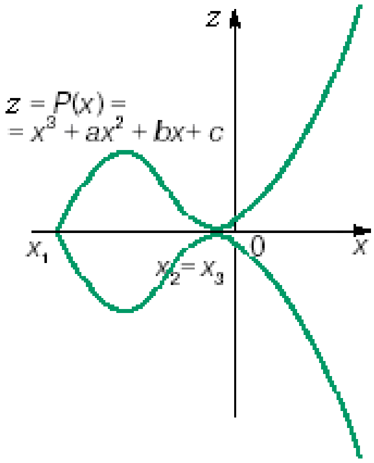
функция графиги қуйидаги кўринишга эга:



Бу графикдан (4) функция графигини олиш учун, квадрат илдиз остидаги ифоданинг манфий бўлмаган қийматлар соҳасига мос келувчи - аниқланиш соҳасинин қисми



Ox - ўқига нисбатан симметрик кўчирилади, натижада график умумий нуқтага эга бўлган эллипс ва гиперболадан иборат бўлган иккита қисмлар билан ифодаланади:



Амалда, $y^2 = x^3 + ax^2 + bx + c$ - эллиптик эгри чизиқ коэффициенти $a = 0$ бўлган $y^2 = x^3 + bx + c$ - эллиптик эгри чизиқнинг келтирилган кўринишидаги ифодасидан ҳамда унинг дискриминанти $D < 0$ бўлиб, учта ҳақиқий илдизга эга, яъни функция графиги Оx-ўқи билан учта нуқтада кесишадиган ҳолатидан фойдаланиш қулай ва самарали татбиққа эга.

Эллиптик эгри чизиққа тегишли рационал нуқталарни аниқлаш усуллари

Олдиндан шуни айтиш лозимки, ҳозирги кунда

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

тенгламанинг барча рационал ечимларини топиш математикада номаьлумлигича қолиб келмокда. Лекин, қуйидаги иккита усулдан фойдаланиб, рационал ечимларни топиш мумкин.

1-усул. Танланган $y^2=x^3+ax+b$ тенгламага x_i қийматларни бериб, тенгламанинг ўнг томони тўла квадрат ташкил қилиш текширилади. Агар бирор x_k қийматда тенгликни ўнг томонидаги ифоданинг қиймати тўла квадрат ташкил қилса, у ҳолда тенгламага тегишли нуқта координаталарини

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

жуфтликлар билан фиксирланади.

2- усул. Бу усулда нуқта координаталари (x; y) ва тенгламанинг битта a –коэффициентини фиксирлаб: (a; x; $y \in R$) ,

$$b=y^2-x^3-ax \tag{6}$$

формула орқали b–коэффициент ҳисоблаб топилади ва унинг асосида тенглама қурилади. Эллиптик эгри чизиқ коэффициентларини олинган рационал координатали нуқта орқали аниқлашнинг бундай усули самарали ҳисобланади.

Эллиптик эгри чизиқларнинг рационал нуқталарини қўшиш

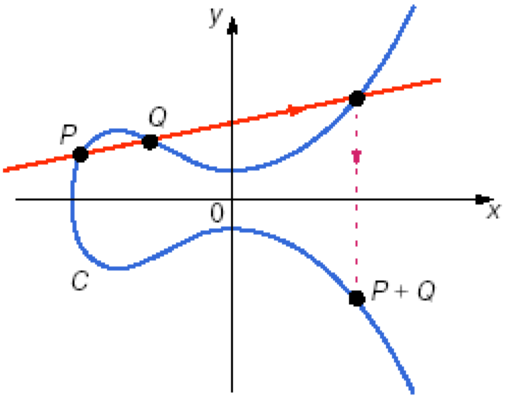
Ушбу

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

эллиптик эгри чизиқда $P(x_1, y_1)$, $Q(x_2, y_2)$ нуқталар берилган бўлсин. Бу нуқталар орқали тўғри чизиқ ўтказилади. У ҳолда ўтказилган чизиқ, E - эгри чизиқни учинчи нуқтада кесиб ўтади. Бу $B(x_3, y_3)$ нуқтани Ox - ўқига симметрик кўчирилади ва ҳосил бўлган:

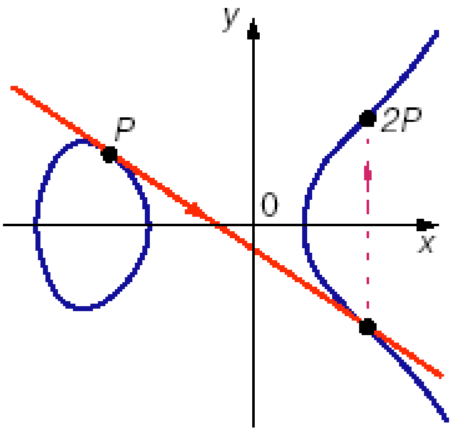
$$B^{`}(x_3, -y_3) = P(x_1, y_1) + Q(x_2, y_2)$$

нуқта $P(x_1, y_1)$ ва $Q(x_2, y_2)$ нуқталарнинг эллиптик эгри чизиқ устида йиғиндиси деб эьлон қилинади:



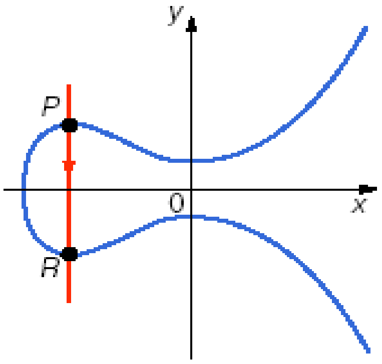
Бу график $x^3 + ax^2 + bx + c = 0$ тенглама битта ечимга эга бўлган ҳол учун келтирилди.

Юқорида эллиптик эгри чизиқда координаталари ҳар хил бўлган, яъни $P(x_1, y_1) \neq Q(x_2, y_2) \neq 0$ бўлган нуқталар йиғиндисини $P(x_1, y_1) + Q(x_2, y_2)$ топиш кўриб чиқилди. Энди $P + P = ?$ қандай амалга оширилиши ҳақида тўхтаб ўтилади. Бунинг учун эллиптик эгри чизиқдаги P -нуқта орқали уринма тўғри чизиқ ўтказилади. Бу уринма эллиптик эгри чизиқ графигидаги иккинчи қисмни (гипербола қисмида) бирор нуқтада кесиб ўтади. Ана шу кесиб ўтган нуқта Ox -ўқига нисбатан симметрик кўчирилади ва бу нуқта *[2]P* деб эьлон қилинади:



Сўнгра, *[3]P* ни топиш учун, *[3]P=[2]P+P,* шу каби *[4]P=[3]P+P, [5]P=[4]P+P* ва ҳоказолар амалга оширилади.

Ҳар доим ҳам $P(x_1, y_1)$ ва $Q(x_2, y_2)$ нуқталар орқали ўтувчи тўғри чизиқ эллиптик эгри чизиқни учинчи нуқтада кесиб ўтавермайди. Масалан, $P(x_1, y_1)$ ва $Q(x_1, -y_1)$ нуқталардан ўтувчи тўғри чизиқ Ox -ўқига перпендикуляр бўлиб, у эллиптик эгри чизиқни учинчи нуқтада кесиб ўтмайди:



Бундай ҳолда ўтказилган тўғри чизиқ эллиптик эгри чизиқни чексизликда кесиб ўтади деб қабул қилиниб, чексизликдаги барча нуқталар битта ноль нуқтага бирлаштирилган деб ҳисобланади, яъни чексизликдаги барча нуқталар, эллиптик эгри чизиқ нуқталари устида аниқланган қўшиш амалига нисбатан, ҳақиқий сонларни қўшишдаги ноль қиймати каби хоссага эга. Ҳақиқатан ҳам, $P(x_1, y_1)$ ва $Q(x_1, -y_1)$ нуқталардан ўтувчи тўғри чизиқ Ox -ўқига перпендикуляр бўлиб, у эллиптик эгри чизиқни учинчи нуқтада кесиб ўтмай, чексизликдаги 0_E нуқтага йўналади. Чексизликдаги 0_E нуқта билан $P(x_1, y_1)$ -нуқтани қўшишни $0_E + P(x_1, y_1)$ шаклида кўриб чиқадиган бўлсак, бу нуқталардан ўтувчи тўғри чизиқ Ox -ўқига перпендикуляр бўлиб, эллиптик эгри чизиқни $Q(x_1, -y_1)$ - нуқтада кесиб ўтади, сўнгра $0_E + P(x_1, y_1)$ - йиғиндини ифодаловчи нуқтани топиш учун бу $Q(x_1, -y_1)$ - нуқта Ox - ўқига симметрик акслантирилса, $P(x_1, y_1)$ - нуқта билан устма-уст тушади, яъни киритилган қўшиш амали қоидасига кўра $0_E + P(x_1, y_1) = P(x_1, y_1)$ тенглик ўринли бўлади. Бу 0_E нуқта Ox - ўқига нисбатан акслантирилса, яна қарама-қарши томон чексизлигидаги (-0_E) - нуқтага йўналади. Аммо, чексизликдаги барча нуқталар битта ноль нуқтага бирлаштирилганда $(-0_E) + P(x_1, y_1) = P(x_1, y_1)$

тенгликнинг ўринли бўлишига келтирилган фикр-мулоҳозалар асосида ҳам ишонч ҳосил қилиш мумкин.

Бевосита ҳисоблашлар билан кўрсатиш мумкинки, эллиптик эгри чизиқ нуқталарини қўшиш амали Абель группасини ташкил этади, яьни эллиптик эгри чизиққа тегишли бўлган a, b, c - нуқталар учун:

1) коммутативлик $a + b = b + a$;

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

3) ноль элементининг мавжудлиги $a + 0_E = a;$

4) тескари (қарама-қарши ишорали) элементнинг мавжудлиги

$a+(-a)= 0_E$ каби Абельь группасининг аксиомалари ўринлидир.

Эллиптик эгри чизиқнинг нуқталарини қўшиш формулалари унинг геометрик маъносидан келиб чиққан ҳолда келтириб чиқарилади. Кўриб ўтилганларга мувофиқ, агар $P(x_1, y_1)$ ва $Q(x_2, y_2)$- нуқталар E-эллиптик эгри чизиқда ётса, яъни $P(x_1, y_1)$, $Q(x_2, y_2) \in E$ нуқталар бўлса, унда улар орқали кесувчи тўғри чизиқ ўтказилиб, бу кесувчи тўғри чизиқ E-эллиптик эгри чизиқни бирор учинчи $R(x_3, y_3)$ нуқтада кесиб ўтади.

3-тасдиқ. Агар $P(x_1, y_1)$, $Q(x_2, y_2) \in E$ нуқталар рационал координатали бўлса, у ҳолда $R(x_3, y_3)$ нуқта координаталари ҳам рационал бўлади.

Исботи. $P(x_1, y_1)$, $Q(x_2, y_2) \in E$ нуқталар орқали ўтувчи тўғри чизиқнинг умумий кўриниши:

$$y = kx + d$$

ифодага эга бўлиб, бу ерда k, d – коэффициентлар $P(x_1, y_1)$ ва $Q(x_2, y_2)$ нуқталарнинг координаталари орқали ифодаланади. $P(x_1, y_1)$, $Q(x_2, y_2)$ - нуқталар $y = kx + d$ чизиққа тегишли. Бундан эса:

$$\begin{cases} y_1 = kx_1 + d, \\ y_2 = kx_2 + d, \end{cases} \qquad y_1 - y_2 = k(x_1 - x_2) \text{ ва } \quad k = \frac{y_1 - y_2}{x_1 - x_2} \quad ,$$

эканлиги келиб чиқади.

Шунингдек,

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

Шундай қилиб, $y = к\,x + d$ тўғри чизиғи тиклаб олинди. Кейинги қадамда

$y = кx{+}d$ – ифода $y^2 = x^3 + ax^2 + bx + c$,

эллиптик эгри чизиқнинг тенгламасига қўйилади, яьни

$$(kx + d)^2 = x^3 + ax^2 + bx + c,$$

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

у ҳолда учинчи тартибли тенглама учун Виет теоремасига кўра:

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

тенглик ўринли бўлиб, бу охирги тенгликда x_1, x_2 - рационал сонлар бўлгани учун, x_3 ҳам рационал сон бўлади. Худди шунингдек,

$$y_3 = kx_3 + d$$

ифодага кўра y_3 - сонининг ҳам рационал эканлиги келиб чиқади.

Бу келтирилган тасдиқ исботидан эса $P + Q$ йиғинди нуқта координатасини ҳисоблаш формуласини келтириб чиқариш мумкин. $P + Q$ нуқта R – нуқтани Ox - ўқига симметрик кўчиришдан ҳосил бўлар эди. Натижада, йиғинди нуқтанинг координаталари (u, v) , деб белгиланса, бу координаталар қуйидаги формулалар орқали топилади:

$$u = k^2 - a - x_1 - x_2,$$

$$v = -ku - d = -(k(u - x_1) + y_1)$$

чунки $u = x_3$, $v = -y_3$. Бу формулада k -коэффициенти қийматининг ўрнига $\frac{y_1 - y_2}{x_1 - x_2}$ қўйилса, қуйидаги тенгликлар ҳосил бўлади:

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

Бу ерда, $x_1 \neq x_2$.

Агар $x_1 = x_2$ бўлса, у ҳолда кесувчи тўғри чизиқ ўрнига уринма ўтказилиб, қуйидаги формулалар келтириб чиқарилади:

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

Шундай қилиб, ҳеч бўлмаса битта P - рационал нуқта эллиптик эгри чизиқдаги нуқта бўлса, у ҳолда (7), (8) - формулалар орқали *[2]P*-ни топиш учун, *[2]P=P+P, [3]P*-ни топиш учун, *[3]P=[2]P+P,* шу каби *[4]P=[3]P+P, [5]P=[4]P+P* ва ҳоказоларни топишимиз мумкин бўлади.

Шуни алоҳида таъкидлаш керакки, келтирилган (7) ва (8) формулалар (3) тенгламага нисбатан келтириб чиқарилди. Энди эллиптик эгри чизиқнинг криптографияда кенг қўлланиладиган

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

тенгламаси учун рационал нуқталарини қўшиш формулалари келтириб ўтилади:

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

бу ерда, $x_1 \neq x_2$.

Агар $x_1 = x_2$ бўлса, у ҳолда

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

Олдиндан берилган $y^2 = x^3 + ax^2 + bx + c$ - ЭЭЧ рационал нуқталарини топишнинг самарали усулини аниқлаш ҳозирги кунда сонлар назариясининг муаммоларидан бири ҳисоблансада, эгри чизиққа тегишли битта нуқта топилса, қолганлари (7), (8) формулалар орқали аниқланади.

ЭЭЧ нуқталарини қўшиш жараёнида қуйидаги иккита ҳолат бўлиши мумкин:

1. Бирор n –қадамда $[n]P= 0_E$ тенглик бажарилиши мумкин;
2. $[2]P$, $[3]P$, $[4]P$ ва ҳоказо $[n]P$ – нуқталар ҳар хил қийматга эга бўлиши мумкин.

3.25-таъриф. Агар барча $m < n$ ҳолатларда $[m]P\neq 0_E$ бажарилиб, $[n]P = 0_E$ бўлса, у ҳолда P – нуқта n – чекли тартибга эга дейилади.

3.6.3. Майдон устида берилган параметрли эллиптик эгри чизиқ нуқталари группаси

3.6.3.1. Параметрли эллиптик эгри чизиқ нуқталари группаси

Ошкора криптографиянинг анъанавий эллиптик эгри чизиқ (ЭЭЧ)ли носимметрик криптотизимларидан қўшимча махфийликка эга бўлган янги криптотизимларга ўтиш долзарб муаммо ҳисобланади.

Қуйида анъанавий ЭЭЧлар асосида шакллантирилган параметрли алгебраик группа ҳақида сўз боради [55].

Маълумки, фойдаланиш учун қулай бўлган ЭЭЧ тенгламаларининг кўпчилиги Вейерштрасс [56-58] тенгламасини умумлашган шаклининг хусусий ҳолларидир. Шу жумладан, ГОСТ Р 34.10-2001га асос қилиб олинган Вейерштрасс тенгламаси умумлашган шаклининг хусусий ҳоли

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

кўринишга эга бўлиб, ўзгарувчиларни ва коэффициентларни алмаштириш, параметр R ни киритиш орқали қуйидаги модуляр кўринишга келтирилади:

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

бу ерда:

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

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

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

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

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

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

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

$y_0,\ x_0,y,\ y^{-},\ x$ - ўзгарувчилар,

$a,\ B$ **-** бутун сонли коэффициентлар,

R – параметр, $0<R<n,\ (R;\ n)=1$ шартларини қаноатлантиради**.**

$Q_{1=}(x_1,\ y_1)$ ва $Q_2=(x_2,\ y_2)$ нуқталар устида ***параметрли қўшиш*** амали “$+^{\backslash}$ **“** билан белгиланади ва $Q_3 = Q_1 +{}^{\backslash}Q_2$ кўринишида ифодаланади. $(x_1,\ y_1)$ ва $(x_2,\ y_2)$ нуқталар устида ***параметрли қўшиш*** қуйидаги таққосламалар асосида амалга оширилади:

1) $x_1 \neq x_2$ ҳол учун $Q_3=(x_3,\ y_3)$**:**

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

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

бу ерда:

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

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

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

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

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

3) $x_1=x_2,\ y_2=\ y_1^{\ -}$ ҳол учун $Q_1=(x_1,\ x_2)$ ва $Q_2=(x_2,\ y_1^{\ -})$ нуқталарнинг ***параметрли*** йиғиндиси ноллик (чексизликдаги) нуқта 0_E га тенг.

Ноллик нуқта учун $Q+^{\backslash}\ 0_E\ =0_E\ +^{\backslash}Q=Q$ (13)

тенглик ўринлидир.

ЭЭЧ нуқтасини ўзига ўзини *d* марта параметрли қўшиш натижаси нуқтани скаляр сон *d* га кўпайтириш амалини беради. ЭЭЧ нуқтасини скаляр сон *d* га кўпайтириш амали “ $*^{\backslash}$“ белгиси билан ифодаланади.

Шуни таъкидлаш керакки, Вейерштрасс [56-58] умумий кўринишдаги тенгламасининг қолган барча хусусий ҳоллари бўлган ЭЭЧ тенгламалари учун ҳам юқорида келтирилган ЭЭЧ нуқталари устида параметрли қўшиш $+^{\backslash}$ ва ЭЭЧ нуқтасини скаляр сон *d* га кўпайтириш амали $*^{\backslash}$ ни аниқлаш ҳеч қандай қийинчилик туғдирмайди.

ЭЭЧ барча нуқталари устида параметр $R\geq 1$ билан қўшиш амали чекли аддитив коммутатив группани ташкил этади.

3.26-таъриф. $PE(F_n) = \{$параметрли ЭЭЧ нуқталари$\}\ U\{0_E\}$, яъни параметрли ЭЭЧ барча нуқталари тўплами ва ноллик нуқта, параметр $0< R\in F_n$ бўлса, $+^{\backslash}$ – $PE(F_n)$ устида аниқланган параметрли қўшиш амали бўлса, $(PE(F_n);\ +^{\backslash})$ – жуфтлик параметрли ЭЭЧ нуқталари группаси деб аталади.

Анъанавий ЭЭЧ ва параметрли ЭЭЧ нуқталари тўпламлари ўзаро изоморфлиги туфайли ***аддитив коммутатив группанинг*** барча аксиомалари параметрли ЭЭЧ нуқталари группасини ҳам қаноатлантиради.

Бу ҳолат параметрли ЭЭЧ нуқталари группаси асосида қўшимча махфийликка эга бўлган бир томонлама функциялар асосида мавжуд криптотизимларга аналог бўлган янги криптотизимларни ва янги криптотаҳлиллаш усулларини яратишга йўл очади.

3.6.3.2. Параметрли эллиптик эгри чизиқ функцияси хоссаларининг эллиптик эгри чизиқ функциясига ўхшаш хоссалари

Аввалги бандда келтирилган параметрли ЭЭЧ нуқталари группаси $(PE(F_p);\ +^{\backslash})$ дан фойдаланиш қўшимча махфий параметр *R* туфайли ҳозирча маълум бўлмаган ошкормас ЭЭЧ параметри муаммоси юзага келиши ва бунинг оқибатида криптобардошлилик ортиши қайд этилган эди.

Параметрли ЭЭЧлардан фойдаланишга асосланган алгоритмлар бардошлилиги улар махсус аппаратли модуль сифатида амалга оширилганда энг юқори даражада бўлиши [55] да изоҳланган.

3.27-таъриф. $y^{\backslash 2} \equiv x^{\backslash 3}+ax+B \ (mod\ p)$ таққосламани қаноатлантирувчи ЭЭЧ нуқталари группаси $PE(F_p)$ да ЭЭЧ нуқтасини параметрлар учлиги $<R,\ a,\ B>$ билан скаляр сонга кўпайтириш $(*^{\backslash})$ функцияси параметрли ЭЭЧ функцияси деб аталади.

Бу ерда:

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

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

$a,\ B$ – бутун сонли коэффициентлар,

R – параметр, $0 <R < p,\ (R;\ p)=1$ шартларини қаноатлантиради**,**

q – параметрли ЭЭЧ нуқталари тартиби,

p – туб сон.

G нуқтани скаляр сон d га параметрли кўпайтириш натижаси $d*^{\backslash}G$ шаклида ифодаланган, $^{\backslash}$ – R параметрли даражага ошириш белгиси, $*^{\backslash}$ – скаляр сонга параметр R билан кўпайтириш белгиси**.**

Параметрли ЭЭЧ функцияси хоссаларининг ЭЭЧ функциясига ўхшаш хоссаларига ***қуйидагилар киради:***

2.3.1-хосса. $(d_1+d_2\ mod\ q)*^{\backslash}G = (d_2*^{\backslash}G)+^{\backslash}(d_1*^{\backslash}G),$ бу ерда $d_1,\ d_2 \in\{1,2,...,\ q-1\};$ анъанавий (параметрсиз) нуқтани скаляр сонга кўпайтириш функциясида $(d_1 +d_2\ mod\ q)"*"\ G = (d_2"*"\ G)\ "+"(\ d_1\ "*"\ G).$

Мисол.

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-хосса. $(d_1d_2 \bmod q)*^{\backslash}G = d_2*^{\backslash}(d_1 *^{\backslash}G)$, бу ерда $d_1, d_2 \in\{1,2,. .., q-1\}$; анъанавий (параметрсиз) нуқтани скаляр сонга кўпайтириш функциясида $(d_1d_2 \bmod q)$ ”*” $G = d_2$”*”$(d_1$ ”*” $G)$.

Мисол.

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-хосса. $q*^{\backslash} G = 0_E$, $(q+1)*^{\backslash} G = G$, $1*^{\backslash} G = G$, $1*^{\backslash} G = G$, $0_E*^{\backslash} G =0_E$, $d_1*^{\backslash} (d_2 *^{\backslash} G) = d_2 *^{\backslash} (d_1*^{\backslash} G)$, бу ерда q - параметрли ЭЭЧ нуқталари тартиби; анъанавий (параметрсиз) нуқтани скаляр сонга кўпайтириш функциясида q”*”$G=0_E$, $(q+1)$”*”$G=G$, 1”*”$G=G$, 0_E”*”$G=0$, d_1”*”$(d_2$”*”$G)=d_1$”*” $(d_1$”*”$G)$.

Мисол.

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-хосса. Агар d, e q модули бўйича ўзаро тескари жуфтлик бўлса, унда $d *^{\backslash} G =S$, $e*^{\backslash} S =G$, $e*^{\backslash} (d *^{\backslash} G) =G$,

бу ерда G - дастлабки матнга тегишли S - шифрланган матнга тегишли параметрли ЭЭЧ нинг тартиби q бўлган нуқталари; анъанавий (параметрсиз) нуқтани скаляр сонга кўпайтириш функциясида d”*”$G=S$, e”*”$S=G$, e”*”$(d$ ”*”$G)=G$.

Мисол.

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

Юқорида келтирилган 1-4 хоссалар анъанавий ЭЭЧ функцияси хоссаларига ўхшаш бўлиб, улардан биринчиси ва иккинчиси параметрли ЭЭЧ функцияси қийматини исталган скаляр сон учун самарали ҳисоблаш учун етарлидир. Бу ерда, катта скаляр сонга параметрли кўпайтириш жараёни экспоненциал функцияни ҳисоблаш жараёни каби кечиб, d ни 2 нинг даражалари йиғиндиси сифатида ифодалашга ва даврий тарзда йиғиндини ташкил этувчи 2 нинг даража кўрсаткичи, агар жуфт қийматли бўлса, 2 га параметрли кўпайтириш, акс ҳолда жорий қийматни берилган нуқтага параметрли кўпайтириш амалларидан фойдаланишдан иборат бўлади.

1-4 хоссалар анъанавий ЭЭЧ функцияси хоссаларидан фойдаланишга асосланган криптографик тизимларга ўхшаш криптотизимлар яратишга имкон беради.

3.7. Кўпҳадлар тўплами. Алгебранинг асосий теоремаси

Агар q сон p туб соннинг даражаси бўлса $q=p^m$, у ҳолда бундай майдоннинг элементлари коэффициентлари $GF(p)$ - оддий майдон элементларидан иборат $(m\text{-}1)$-даражагача *кўпҳадлар тўпламини* ўз ичига олади. Бундай кўпҳадларни қўшиш ва кўпайтириш кўпҳадларни оддий қўшиш ва кўпайтириш қоидалари бўйича бажарилиб, ҳосил бўлган кўпҳад асос сифатида олинган m-даражали $g_m(x)$-кўпҳадга бўлишдан ҳосил бўлган қолдиқ натижа сифатида қабул қилинади. Берилган кўпҳадни бирор асос сифатида олинган $g_m(x)$-кўпҳад бўйича модулини $(mod g_m(x))$ ҳисоблаш ушбу $a(x)=b(x)$ (mod $g_m)(x)$ таққослама билан боғлиқ: унда $a(x)$ ва $b(x)$ кўпҳадлар $g_m(x)$-модуль бўйича тенг (ёки таққосланувчи) дейилади, агарда бу кўпҳадларни $g_m(x)$-кўпҳадга бўлинганда бир хил қолдиққа эга бўлса ёки $a(x)$-$b(x)$ – кўпҳад $g_m(x)$-кўпҳадга қолдиқсиз бўлинса. Шундай қилиб, кўпҳадларни таққослаш бутун сонларни таққослаш каби тушунча эканлиги келиб чиқади. Асос сифатида олинган $g_m(x)$-кўпҳадни коэффициентлари $GF(p)$-оддий майдон элементларидан иборат бўлган кўпҳадларнинг кўпайтмаси шаклида ифодалаш имконияти йўқлиги хусусиятига эга. Бундай кўпҳад келтирилмайдиган дейилади ва моҳиятига кўра туб сонларга ўхшашдир. Мисол учун, коэффициентлари $GF(2)$-оддий майдон элементларидан *{0;1}* иборат бўлган $g_3(x)=1+x+x^3$ – келтирилмайдиган кўпҳад бўлиб, ундан $GF(8)$-кенгайтирилган майдонни қуришда фойдаланиш мумкин. $GF(8)$-кенгайтирилган майдон элементлари: 1, x, x^2, $1+x$, $1+x^2$, $x+x^2$, $1+x+x^2$.

Алгебранинг асосий теоремаси. Даражаси *1* дан кичик бўлмаган комплекс коэффициентли ҳар қандай кўпҳад камида битта комплекс илдизга эга.

Тоқ даражали кўпҳад доимо илдизга эга эканлиги маълум. Бундан комплекс коэффициентли даражаси *1* дан кичик бўлмаган жуфт даражали кўпҳадлар камида битта комплекс илдизга эканлиги ўз исботини топади.

Қуйида алгебра асосий теоремасининг баъзи натижаларини келтирамиз.

1-натижа. Комплекс сонлар майдонидаги n-даражали кўпҳаднинг n та илдизи мавжуд.

2-натижа. n-даражали $f(x)$ кўпҳад x нинг n тадан ортиқ ҳар хил қийматларида нолга тенг бўлса, унда $f(x)$ ноль кўпҳад бўлади.

3-натижа. Даражалари n дан юқори бўлмаган $f(x)$ ва $\varphi(x)$ кўпҳадлар x нинг n тадан ортиқ ҳар хил қийматларида бир-бирига тенг бўлса, унда $f(x)$ ва $\varphi(x)$ кўпҳадлар ўзаро тенг кўпҳадлар бўлади.

3.8. Сонлар назарияси элементлари

Сонлар назарияси криптографик масалаларнинг тадқиқ қилиниши ҳамда уларнинг ечимларида муҳим роль ўйнайди.

Натурал сонлар тўпламини $N=\{1, 2,3, \ldots\}$ ва бутун сонлар тўпламини $Z=\{0, \pm1, \pm 2, \pm3, \ldots\}$ кўринишда белгилаймиз.

Нолдан фарқли бўлган a сони ва b сонлар Z –тўпламга тегишли, яъни

$a,\ b \in Z$ бўлиб, $a \neq 0$ бўлсин, агарда шундай c сони мавжуд бўлиб, $b = ac$ тенглик бажарилса, у ҳолда a сони b сонини бўлади, дейилади.

3.8.1. Энг катта умумий бўлувчи

Берилган *а* ва *в* сонларни бўлувчи бутун сон, уларнинг *умумий бўлувчиси* дейилади. Умумий бўлувчилар ичида энг каттаси *энг катта умумий бўлувчи* (ЕКUB) дейилади ва ЕКUB($a,\ b$) кўринишда белгиланади. Агарда a ва b сонларнинг энг катта умумий бўлувчиси 1, ЕКUB ($a,\ b$)=1 бўлса, a ва b сонлар *ўзаро туб* дейилади. Энг катта умумий бўлувчиларни топишга оид тасдиқларни келтирамиз.

1-лемма. Агар b сони a сонини бўлса, у ҳолда бу сонларнинг энг катта умумий бўлувчиси ЕКUB ($a,\ b$)= b, яъни a сонининг умумий бўлувчилари тўплами b сонининг умумий бўлувчилари тўплами билан устма-уст тушади.

2-лемма. Агар $a=bq+c$ бўлса, у ҳолда a ва b сонларининг энг катта умумий бўлувчиси b ва c сонларининг энг катта умумий бўлувчиси билан устма-уст тушади, яъни ЕКUB ($a,\ b$)= ЕКUB ($b,\ c$): a ва b сонларининг умумий бўлувчилари тўплами b ва c сонларининг умумий бўлувчилари тўплами билан устма-уст тушади.

Юқорида келтирилган леммалардан ЕКUBни топиш – Евклид алгоритми келиб чиқади.

Ҳақиқатан ҳам қуйидаги бўлиш амалларини бажарамиз:

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

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

$$\ldots\ldots\ldots\ldots, \qquad \ldots\ldots\ldots\ldots,$$

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

$$r_{n-1}=r_nq_{n+1}.$$

У ҳолда ЕКUB ($a,\ b$)= ЕКUB ($b,\ r_1$)=…=($r_{n-2},\ r_{n-1}$)= r_n .

Берилган натурал сон $p>1$ туб дейилади, агарда бу сон ўзи p ва 1 дан бошқа натурал сонга бўлинмаса. Мисол учун: *2, 3, 5, 7, 11, 13, 17, 19, 23, 29,* ..., туб сонлар, улар саноқли ва чексиз қувватли тўпламни ташкил этади.

Келгусида барча бутун сонларни *модуль* (*характеристика*) деб аталувчи бирор фиксирланган натурал n сонига бўлганда қоладиган қолдиқлар билан боғлиқ ҳолда қараймиз. Бунда чексиз қувватли (элементлари сони чексиз) бўлган барча бутун сонлар тўпламига, 0 дан n-1 гача бўлган бутун сонларни ўз ичига оладиган чекли, қуввати n га тенг бўлган $\{0;\ 1;\ 2;\ 3;\ldots;n\text{-}1\}$ – тўплам мос қўйилади. Бу қуйидагича амалга оширилади: a ва n – натурал сонлар бўлса, “a сонини n сонига қолдиқ билан бўлиш”, деганда ушбу

$$a=qn+r, \quad \text{бу ерда } 0\le r<n,$$

шартни қаноатлантирувчи натурал q ва r сонларини топиш тушунилади. Бу охирги тенгликда қолдиқ деб аталувчи r сони нолга тенг бўлса r=0, натурал a сони n сонига бўлинади ёки n сони a сонининг бўлувчиси дейилади.

3.8.2. Таққосламалар

Бутун a ва b сонлари *модуль n бўйча таққосланадиган* дейилади, агарда уларни n га бўлганда қоладиган қолдиқлари тенг бўлса,

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

деб ёзилади. Бундан эса a ва b сонлар айирмасининг n га қолдиқсиз бўлиниши келиб чиқади.

Қолдиқни ифодалаш учун ушбу

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

тенгликдан фойдаланилади ҳамда $b=a\ (mod\ n)$ тенгликни қаноатлантирувчи b сонини топиш *a сонини модуль n бўйича келтириш* дейилади.

Ихтиёрий бутун b сони учун ушбу

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

тўпламга тегишли $a_k \equiv b$ $(mod\ n)$ муносабатни қаноатлантирувчи сон a_k , $k \in \{0,1,\ldots,$ n-1$\}$ мавжуд бўлса, тўплам M модуль n бўйича *тўлиқ чегирмалар синфи* дейилади. Кўриниб турибдики, тўлиқ чегирмалар *синфи*

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

Бирор n модуль бўйича қўшиш, айириш ва кўпайтириш амалларига нисбатан қуйидаги коммутативлик, ассоциативлик ва дистрибутивлик муносабатлари ўринли:

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

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

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

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

1-теорема. Бутун a ва b сонлари ўзаро туб бўлади, қачонки шундай бутун u ва v сонлари топилсаки, улар учун $au+bv=1$ тенглик ўринли бўлса.

Бу келтирилган теоремани қуйидагича ҳам ифодалаш мумкин: *бутун a ва b сонлари ўзаро туб бўлиши учун, бутун бўлган u ва v сонлари топилиб, улар учун au+bv=1 тенгликнинг бажарилиши зарур ва етарли.*

Агарда бутун a ва b сонлари ўзаро туб бўлса, яъни ЕКUB (a, n)=1 бўлса, у ҳолда ушбу $aa' \equiv 1(\mathrm{mod}\ n)$ муносабатни қаноатлантирувчи бутун a' сони мавжуд бўлиб, бу a' *сон а сонига модуль n бўйича тескари* дейилади ҳамда $a' \equiv a^{-1}(\mathrm{mod}\ n)$ деб белгиланади. Тескари a' элементни a ва n сонларининг чизиқли комбинациясидан иборат бўлган уларнинг ЕКUB ифодасидан $au+bn=1$ фойдаланган ҳолда, бу тенгликнинг ҳар иккала томонини модуль n бўйича келтириш (ҳисоблаш) билан $a' \equiv u$ $(\mathrm{mod}\ n)$ эканлиги топилади.

Қуйида тескари элементни ҳисоблашнинг яна бир усули келтирилади.

Берилган n сони билан ўзаро туб бўлган $(1;\ n)$ оралиқдаги барча элементларнинг сони билан аниқланувчи $\varphi(n)$ функцияга *Эйлер функцияси* дейилади:

$\varphi(n)=|M|$, бу ерда $|M|$ M – тўпламнинг қуввати, $M=\{m_i \in N: 1 \le m_i \le n;\ \ (m_i,n)=1\}$.

Агарда $n = p_1^{k_1} \cdot \ldots \cdot p_t^{k_t}$ бўлиб, $p_1, \ldots, p_t$ - ҳар хил туб сонлар бўлса, у ҳолда Эйлер функциясининг қиймати $\varphi(n) = \prod_{j=1}^{t} (p_j - 1) \cdot p_j^{k_j - 1}$ ифода билан ҳисобланади.

Ферманинг кичик теоремаси деб аталувчи ушбу тасдиқ ўринли, агар n – туб сон бўлса, $a^{n-1} \equiv 1(\mathrm{mod}\ n)$ ўринли.

Эйлер томонидан олинган, *Ферма кичик теоремасининг умумлашгани* деб аталувчи ушбу тасдиқ ўринли, агар *n* – туб сон бўлса, $a^{\varphi(n)} \equiv 1(mod\ n)$ муносабат бажарилади.

Юқоридагилардан келиб чиққан ҳолда, $a^{-1} \equiv a^{\varphi(n)-1}\ (mod\ n)$ муносабатнинг ўринлигига ишонч ҳосил қилинади.

Агар *n*–туб сон бўлса, у ҳолда $\varphi(n) = n - 1$. Агар *n=pq* бўлиб, *p* ва *q*–туб сонлар бўлса, у ҳолда $\varphi(n) = (p-1)(q-1)$. Бу каби хоссалардан очиқ калитли криптоалгоритмлар яратишда фойдаланилади. Масалан, қандай сон модуль 7 бўйича 5 сонига тескари эканлигини топайлик. Бу ерда, *7* сони туб бўлгани учун, унинг Эйлер функцияси $\varphi(7) = 7 - 1$ =6, модуль *7* бўйича *5* сонига тескари сон эса $a^{-1} \equiv a^{\varphi(n)-1}\ (mod\ n)$ формулага кўра $5^{-1} = 5^{6-1} \mathrm{mod} 7 = 5^5 \mathrm{mod} 7 = 3125 \mathrm{mod} 7$.

Ҳақиқатан ҳам, $5 \cdot 3 \mathrm{mod} 7 = 15 \mathrm{mod} 7 = 1 \mathrm{mod} 7 = 1$. Бирор модуль бўйича берилган сонга тескари бўлган сон ҳар доим ҳам мавжуд бўлавермайди. Мисол учун, *5* сонига модуль *14* бўйича тескари сон *3*: $5 \cdot 3 \mathrm{mod} 14 = 15 \mathrm{mod} 14 = 1 \mathrm{mod} 14 = 1$. Аммо, *2* сонининг модуль *14* бўйича тескариси мавжуд эмас, яъни $2x \equiv 1\ (mod\ 14)$ ёки $2x=14k+1$ тенглама *x* ва *k* номаълумларнинг бутун қийматларида ечимга эга эмас, чунки *x* ва *k* номаълумларнинг бутун қийматларида ҳар доим тенгликнинг чап томонида жуфт сон, ўнг томонида эса тоқ сон ҳосил бўлади.

Умумий ҳолда, агар *a* ва *n* сонлари ўзаро туб бўлса, тенглама $a^{-1} \equiv x\ \mathrm{mod}\ n$ ягона ечимга эга бўлади; агар *a* ва *n* сонлари ўзаро туб бўлмаса, тенглама $a^{-1} \equiv x\ (\mathrm{mod}\ n)$ ечимга эга эмас. Бевосита ҳисоблашлар асосида, ушбу (ax) mod $n = b$ тенглама a, n, b – сонларининг қандай қийматлар қабул қилишига қараб ёки бир нечта ечимларга эга бўлиши мумкинлигига ёки битта ҳам ечимга эга бўлмаслигига ишонч ҳосил қилиш мумкин.

Қуйидагиларни таъкидлаш жоиз: агар a сони M сонини бўлса ва b сони ҳам M сонини бўлса, у ҳолда бу $M \in N$ сони $a,b \in Z$ сонларнинг *умумий бўлинувчиси* (*карралиси*) дейилади. Умумий бўлинувчилар ичида энг кичиги *энг кичик умумий бўлинувчи* дейилади ҳамда $[a, b]$ деб белгиланади.

2-теорема. Агар $M \in N$ сон $a,b \in Z$ сонларнинг умумий бўлинувчиси бўлса, у ҳолда M сони бу сонларнинг энг кичик бўлинувчиси $[a, b]$ га ҳам бўлинади.

3-теорема. Ушбу $[a, b] = ab/ EKUB\ (a, b)$ муносабат ўринли.

3.8.3. Квадратик чегирмалар

Агар p – туб сон ва $0< a< p$ бўлиб, ушбу

$$x^2 \equiv a(mod\, p)$$

муносабатни қаноатлантирувчи x – номаълумнинг қийматлари мавжуд бўлса, у ҳолда a сони модуль p бўйича квадратик чегирма ҳисобланади.

Мисол учун, $p=7$ бўлса, квадратик чегирма ташкил этувчилар: $1, 2$ ва 4 сонларидан иборат, яъни $a =1$, $a =2$ ва $a=4$ қийматларда, ушбу таққосламалар

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

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

ўринли.

Номаълум x нинг қуйидаги муносабатларни:

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

қаноатлантирувчи қийматлари мавжуд эмас, шунинг учун $a =3$, $a =5$ ва $a=6$ сонлари модуль 7 бўйича квадратик чегирма эмас, яъни берилган квадратик таққосламалар ечимга эга эмас.

Модуль p жуфт бўлса, у ҳолда $(p-1)/2$ та квадратик чегирма мавжуд ва шунча квадратик чегирма мавжуд эмас, яъни ушбу

$$x^2 \equiv a(mod\, p)$$

муносабатни қаноатлантирувчи x –номаълум мавжуд бўладиган a параметрнинг мумкин бўлган қийматлари сони $(p-1)/2$ та, бу муносабатни қаноатлантирувчи x –номаълум мавжуд бўлмайдиган a параметрнинг мумкин бўлган қийматлари сони ҳам $(p-1)/2$ та. Бундан ташқари, агарда a сони модуль p бўйича квадратик чегирма бўлса, у ҳолда a учун иккита квадрат илдиз мавжуд бўлиб, улардан бири $[0; (p-1)/2]$ оралиқда, иккинчиси $[(p-1)/2; p-1]$ оралиқда, шу билан бирга улардан бири модуль p бўйича квадратик чегирма бўлади ва у *бош квадратик илдиз* дейилади.

3.8.4. Мураккаб масалалар

Қуйида носимметрик криптотизимлар бардошлилигини таъминловчи мураккаб масалалар (муаммолар)га тўхталиб ўтилади.

Туб кўпайтувчиларга ажратиш (факторлаш)

Берилган сонни кўпайтувчиларга ажратиш деганда, унинг туб кўпайтувчиларини топиш тушунилади.

Мисол учун:

1) 100 сони $2, 2, 5$ ва 5 туб сонларидан иборат кўпайтувчиларга эга, яъни $100=2\cdot2\cdot5\cdot5;$

2) 6279 сони $3, 7, 13$ ва 23 туб сонларидан иборат кўпайтувчиларга эга, яъни $6279=3\cdot7\cdot13\cdot23.$

Берилган сонни кўпайтувчиларга ажратиш сонлар назариясининг энг дастлабки масалаларидан бири ҳисобланади. Берилган сонни (ёки тўпламни) бирор амал ёки хусусиятга кўра унинг ташкил этувчилари орқали ифодаланиши шу сонни (ёки тўпламни) факторлаш (ажратиш) дейилади. Сонни кўпайтувчиларга ажратиш қийин жараён эмас, аммо кўпайтувчиларга ажратилиши керак бўлган соннинг қиймати катталашиб бориши билан уни кўпайтувчиларга ажратиш жараёнига сарфланадиган вақт ҳам кўпайиб боради. Шундай бўлсада, кўпайтувчиларга ажратиш жараёнини тезлаштирувчи қуйидаги алгоритмлар мавжуд [12-13]:

1. *Сонли майдон умумий ғалвир усули* – ўнлик саноқ тизимида 110 та ва ундан кўп разрядли (рақамли) сонларни кўпайтувчиларга ажратишнинг маълум бўлган энг самарали (тез, кам вақт сарфланадиган) алгоритми;

2. *Квадратик ғалвир усули* – ўнлик саноқ тизимида 110 тадан кам бўлмаган разрядли (рақамли) сонларни кўпайтувчиларга ажратишнинг маълум бўлган энг самарали (тез ва кам вақт сарфланадиган) алгоритми;

3. *ЭЭЧусули* – ўнлик саноқ тизимида туб кўпайтувчиларнинг разряди (рақамлари сони) 43 тадан кўп бўлмаган сонларни кўпайтувчиларга ажратишда фойдаланилган;

4. *Полларднинг Монте-Карло усули* – амалда кам ишлатилади;

5. *Узулуксиз касрлар усули* – қўллашга кўп вақт сарфланади;

6. *Танлаб бўлиш усули* – энг дастлабки усуллардан бўлиб, кўпайтувчиларга ажратилиши керак бўлган (берилган) соннинг квадрат илдизига тенг ва ундан кичик бўлган ҳар бир туб сонни берилган сонни қолдиқсиз бўлиши ёки бўлмаслиги текшириб чиқилиши натижасида, берилган соннинг туб кўпайтувчилари аниқланади.

Модуль n бўйича квадрат илдиз. Агарда майдон характеристикасини ифодаловчи *n* сони иккита туб соннинг кўпайтмасидан иборат бўлса, у ҳолда соннинг квадрат илдизини модуль *n* бўйича топиш масаласини ечиш *n* сонини кўпайтувчиларга ажратиш масаласини ечиш ҳисоблаш нуқтаи назаридан тенг кучли масалалар ҳисобланади. Яъни майдон характеристикасини ифодаловчи *n* сонининг кўпайтувчилари маълум бўлса, берилган ихтиёрий соннинг квадрат илдизини модуль *n* бўйича ҳисоблаш қийинчилик туғдирмайди, акс ҳолда ҳисоблашлар *n* сонининг туб кўпайтувчиларини топиш масаласи каби мураккабликларни ўз ичига олади. Майдон характеристикаси етарлича катта бўлганда криптобардошлилиги квадрат илдизни ҳисоблаш масаласининг мураккаблигига асосланган очиқ калитли криптоалгоритмлар мавжуд.

Туб сонлар генерацияси (ишлаб чиқариш). Очиқ калитли криптоалгоритмлар асослари яратилишида туб сонларнинг хоссаларидан фойдаланилади. Бирор берилган сонни туб кўпайтувчиларга ажратиш, уни туб ёки туб эмаслигини аниқлашга нисбатан мураккаб бўлган масала. Етарли катта разряддаги тоқ сонни тасодифий танлаб олиб, уни кўпайтувчиларга ажратиш билан туб ёки туб эмаслигини аниқлашдан кўра, уни тублигини бирор мавжуд усул билан текшириш осонроқ. Бунинг учун турли эҳтимоллик тестлари мавжуд бўлиб [12-13], соннинг тублигини берилган даражадаги ишонч билан аниқлаб беради. Криптобардошлилиги етарли даражада катта разрядли сонни туб кўпайтувчиларга ажратиш масаласининг мураккаблигига асосланган очиқ калитли криптоалгоритмлар мавжуд.

Чекли майдонларда дискрет логарифмлаш. Криптографияда бир томонлама (тескариси йўқ) функция сифатида бирор модуль n бўйича даражага кўтариш амалини ҳисоблашдан фойдлаланилади:

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

Бу функциянинг y–қийматини x–аргументнинг берилган қиймати бўйича ҳисоблаш қийинчилик туғдирмайди. Аммо, y нинг қийматини билган ҳолда x нинг қийматини топиш мураккаб масала ҳисобланади. Умуман олганда,

$$a^x \equiv b(\mathrm{mod}\, n)$$

муносабатни қаноатлантирувчи x номаълумнинг бутун қийматлари ҳар қандай n лар учун ҳам мавжуд бўлавермайди. Мисол учун, ушбу

$$3^x \equiv 7(\mathrm{mod} 13)$$

муносабат x нинг ҳеч бир бутун қийматида бажарилмайди. a, b, n – параметрларнинг етарли катта қийматларида юқорида келтирилган масаланинг ечими яна ҳам мураккаблашади.

Криптографияда носимметрик шифрлаш алгоритмларининг асослари билан боғлиқ бўлган қуйидаги:

- туб сонлар майдонида $GF(p)$ дискрет логарифмлаш;
- характеристикаси асоси 2 бўлган $GF(2^n)$ майдонда дискрет логарифмлаш;
- ЭЭЧнуқталари устида бажариладиган амалларни бирор чекли F майдонда амалга ошириш масалаларини ечишнинг мураккаблиги билан боғлиқ бўлган муаммолар асосида иш кўрилади.

Криптобардошлилиги дискрет логарифмлаш масаласининг мураккаблигига асосланган кўплаб очиқ калитли криптоалгоритмлар мавжуд.

Назорат саволлари

1. Бинар амал деб нимага айтилади?
2. Алгебраик тузилма деганда нимани тушунасиз?
3. Группа деб нимага айтилади ва у қандай шартларни бажариши керак?
4. Коммутатив группага таъриф беринг?
5. Группоидга таъриф беринг?
6. Яримгуппа қандай группа?
7. Моноидга таъриф беринг?
8. Аддитив группа деб нимага айтилади ?
9. Қандай группа мультипликатив группа дейилади?
10. Қандай мультипликатив группа циклик дейилади?
11. Параметрли группага таъриф беринг?
12. Параметрли мультипликатив коммутатив группа қандай хоссаларга эга?
13. Параметрли функцияларнинг дискрет даражага ошириш функцияси хоссаларига ўхшаш хоссаларини тушунтиринг?
14. Ҳалқанинг таърифи ва умумий хоссалари ҳақида маълумот беринг?
15. Майдон деб нимага айтилади ва у қандай шартларни бажариши керак?

16. Группалар морфизми деганда нимани тушунасиз?

17. Кўпҳадлар тўплами деганда нимани тушунасиз?

18. Алгебранинг асосий теоремасига таъриф беринг?

19. Диаматрицалар алгебрасига таъриф беринг?

20. Диаматрицалар алгебрасиннг афзаллигини қандай мисоллар билан исботлаш мумкин?

21. ЭЭЧ деб қандай чизиққа айтилади?

22. ЭЭЧ қачон силлиқ деб аталади ва уни мисоллар билан тушунтиринг?

23. ЭЭЧга тегишли рационал нуқталарни аниқлашнинг қандай усулларини биласиз?

24. ЭЭЧларнинг рационал нуқталарини қўшиш қандай амалга оширилади?

25. ЭЭЧга тегишли бўлган нуқталар учун қандай аксиомалар ўринли?

26. ЭЭЧ нуқталарини қўшиш формулалари қандай келтириб чиқарилади?

27. Параметрли ЭЭЧ нуқталари группасига таъриф беринг?

28. Параметрли ЭЭЧ функциясига таъриф беринг?

29. Параметрли ЭЭЧ функциясининг хоссаларини анханавий ЭЭЧ функцияси хоссаларига ўхшаш хоссаларини тушунтиринг?

30. Сонлар назариясининг криптография учун аҳамияти нимада?

31. Энг катта умумий бўлувчи деб нимага айтилади?

32. Таққосламалар ҳақида маълумот беринг?

33. Квадратик чегирма деганда нимани тушунасиз?

34. Носимметрик криптотизимлар бардошлилигини таъминловчи қандай мураккаб масалалар (муаммолар)ни биласиз?

35. Туб кўпайтувчиларга ажратиш жараёнини тезлаштирувчи қандай алгоритмлар мавжуд?

4. СИММЕТРИК КРИПТОТИЗИМЛАР

Шифрлаш алгоритмларининг таснифланиши [13] да атрофлича ёритилган. Унда калитлардан фойдаланиш қоидасига кўра шифрлар симметрик ва носимметрик синфларга бўлиниши таъкидланиб, агар шифрлаш ва дешифрлаш жараёнлари мос равишда махфий маълумотни жўнатувчи ва қабул қилиб олувчи томонидан битта калит билан амалга оширилса, бундай алгоритм симметрик шифрлаш синфига кириши таърифланган. Агар шифрлаш жараёнида бирор акслантириш орқали очиқ маълумот алифбоси белгилари шифрмаълумот алифбоси белгиларига алмаштирилса, бундай акслантиришга асосланган шифрлаш алгоритми *ўрнига қўйишга асосланган шифрлаш* синфига киради. Агар шифрлаш жараёнида бирор акслантириш орқали очиқ маълумот алифбоси белгиларининг ўринлари алмаштирилса, бундай шифрлаш алгоритми *ўрин алмаштиришга асосланган шифрлаш* синфига киради. Ўрин алмаштиришга асосланган шифрлаш алгоритмларида очиқ маълумотни ташкил этувчи алифбо белгиларининг маъноси шифрмаълумотда ҳам ўзгармасдан қолади. Ўрнига қўйишга асосланган шифрлаш алгоритмларида шифрмаълумотни ташкил этувчи алифбо белгилари маъноси очиқ маълумотни ташкил этувчи алифбо белгиларининг маъноси билан бир хил бўлмайди. Шифрлаш жараёнида ўрнига қўйиш ва ўрин алмаштириш акслантиришларининг комбинацияларидан биргаликда фойдаланилса, бундай шифрлаш алгоритми *композицион шифрлаш* синфига киради. Умуман олганда, ўрнига қўйишга асосланган шифрлаш алгоритмлари акслантиришларининг математик моделлари кўп қийматли функциялар билан ифодалансада, амалда бир қийматли (тескариси мавжуд бўлган, қайтар) функциялар билан ифодаланувчи акслантиришларни қўллаш қулайлик туғдиради. Умумий ҳолда, ўрнига қўйишга асосланган шифрлаш алгоритмлари *бир қийматли* ва *кўп қийматли шифрлаш* синфига бўлинади. Бир қийматли шифрлаш алгоритмларида очиқ маълумот алифбоси белгиларининг ҳар бирига шифрмаълумот алифбосининг битта белгиси мос қўйилади. Кўп қийматли шифрлаш алгоритмларида очиқ маълумот алифбоси белгиларининг ҳар бирига шифрмаълумот алифбосининг иккита ёки ундан ортиқ чекли сондаги белгилари мос қўйилади, яъни очиқ маълумот алифбосининг бирор x_i белгисига шифрмаълумот алифбосининг чекли $\{y_{i1}, y_{i2}, ..., y_{it}\}$ тўпламдан олинган бирор y_{ij} , $(1 \le j \le t)$ белгиси мос қўйилади.

Шифрлаш алгоритмлари, калитлардан фойдаланиш турларига кўра, *симметрик* ва *носимметри* синфларга бўлинади. Агар шифрлаш ва дешифрлаш жараёнлари бир хил калит билан амалга оширилса, бундай шифрлаш алгоритми симметрик шифрлаш алгоритми синфига киради. Агар шифрлаш жараёни бирор k_1 калит билан амалга оширилиб, дешифрлаш жараёни $k_2 \ne k_1$ бўлган k_2 калит билан амалга оширилиб, k_1 калитни билган ҳолда k_2 калитни топиш ечилиши мураккаб бўлган масала билан боғлиқ бўлса, бундай шифрлаш алгоритми носимметрик шифрлаш алгоритми синфига тааллуқли бўлади.

Шифрлаш жараёни очиқ маълумотни ифодаловчи элементар (масалан: бит, ярим байт, беш бит, байт) белгиларни шифрмаълумотни ифодаловчи элементар белгиларга акслантириш асосида амалга оширилса, бундай шифрлаш алгоритми *оқимли (узлуксиз) шифрлаш* синфига киради.

Шифрлаш жараёни очиқ маълумот алифбоси белгиларининг икки ва ундан ортиқ чекли сондаги бирикмаларини шифрмаълумот алифбоси белгиларининг бирикмаларига акслантиришга асосланган бўлса, бундай шифрлаш алгоритми *блокли шифрлаш* синфига киради.

Шифрлаш жараёнида очиқ маълумот алифбосининг бирор алоҳида олинган a_i белгиси ҳар доим шифрмаълумот алифбосининг бирор фиксирланган b_j белгисига алмаштирилса, бундай шифрлаш алгоритми *бир алифболи шифрлаш* синфига киради. Агар шифрлаш жараёнининг ҳар хил босқичларида очиқ маълумот алифбосининг бирор алоҳида олинган a_i белгиси шифрмаълумот алифбосининг ҳар хил b_j , b_l , ..., b_t белгиларига алмаштирилса, бундай шифрлаш алгоритми *кўп алифболи шифрлаш* синфига киради.

Шифрлаш жараёнида очиқ маълумот алифбоси белгилари ёки алифбо белгилари бирикмалари бирор амал бажариш билан шифрмаълумот алифбоси белгилари ёки уларнинг бирикмаларига алмаштирилса, бундай шифрлаш алгоритми *гаммалаштирилган шифрлаш* синфига киради.

Қуйида ўрнига қўйиш ва ўрин алмаштиришга асосланган шифрлаш алгоритмларининг туркумларининг математик асослари алоҳида-алоҳида кўриб чиқилади.

4.1. Бир алифболи ва кўп алифболи ўрнига қўйишлар

4.1.1. Оддий ўрнига қўйишга асосланган шифрлаш алгоритмларининг жадвалли ва аналитик математик моделлари

Шифрлаш алгоритмлари очиқ маълумот алифбоси белгиларини шифрмаълумот белгиларига акслантиришдан иборат эканлиги юқорида таъкидланган эди. Акслантиришлар функциялари (калит деб аталувчи номаълум) параметрга боғлиқ ҳолда: жадвал ва аналитик (формулали) ифода кўринишларида берилиши мумкин. Ўрнига қўйишга асосланган шифрлаш алгоритмларининг дастлабки намуналари бўлган тарихий шифрлаш алгоритмларининг деярли ҳаммаси жадвал кўринишида ифодаланади. Улар ҳақидаги тўлиқ маълумотлар [13] да мавжуд. Ўрнига қўйишга асосланган шифрлаш алгоритмларининг умумий хусусиятини ҳисобга олиб, бу синфдаги алгоритмларни 4.1-жадвал кўринишида қуйидагича ифодалаш мумкин.

4.1-жадвал

Ўрнига қўйишга асосланган шифрлаш алгоритмлари

Очиқ маълумот алифбоси (кириллча белгилар)	А	Б	...	...	Я
Шифрмаълумот алифбоси (иккилик саноқ тизими белгилари)	$x_0^0 x_1^0 x_2^0 x_3^0 x_4^0$	$x_0^1 x_1^1 x_2^1 x_3^1 x_4^1$	...	...	$x_0^{31} x_1^{31} x_2^{31} x_3^{31} x_4^{31}$

Кириллча алифбо белгилари сони *32* та, шу *32* та ҳар хил белгиларни битлар билан ифодалаш учун беш бит кифоя, яъни $2^5 = 32$. Келтирилган 4.1-жадвалдан фойдаланиб, кириллча алифбода ифодаланган очиқ малумот белгиларини уларга мос келувчи иккилик саноқ тизимидаги беш битлик белгиларга алмаштириб шифрмаълумот ҳосил қилинади, яъни $x_i^j \in \{0;1\}$. Агарда, келтирилган жадвалда очиқ маълумот алифбоси белгиларига шифрмаълумот алифбосининг қандай беш битлик белгилари мос қўйилганлиги номаълум бўлса, бу жадвал калит бўлиб, шифрмаълумотдан очиқ маълумотни тиклаш масаласи мураккаблашади. Бундай шифрлаш жараёнини ифодаловчи алгоритм калитларининг умумий сони $32!$ бўлиб, ушбу $n! \approx \left(\frac{n}{e}\right)^n \sqrt{2\pi n}$ - Стирлинг формуласига кўра қуйидагича

$$32! = \left(\frac{32}{2,7}\right)^{32} \sqrt{2 \cdot 3,14 \cdot 32} > \qquad \left(\frac{32}{4}\right)^{32} \sqrt{2 \cdot 2 \cdot 32} > \qquad \left(\frac{32}{4}\right)^{32} \sqrt{2 \cdot 2 \cdot 32} = 2^{96} \cdot 2^3 \cdot \sqrt{2} > 2^{99}$$

ҳисобланади. Бундай ҳолат эса калитни билмаган ҳолда дешифлаш жараёнини амалга оширишни жиддий мураккаблаштиради.

Агарда очиқ маълумот компьютердан фойдаланилган ҳолда тузилиб, стандарт ASCII коди алифбоси белгиларидан иборат бўлиб, шифрмаълумот стандарт ASCII коди алифбоси белгиларини бирини бошқаси билан алмаштиришдан иборат бўлган ўрнига қўйишга асосланган шифрлаш алгоритмини қўллаш натижасида ҳосил қилинган бўлса, у ҳолда шифрлаш жараёни асосини қуйидаги ўрнига қўйиш алмаштириш 4.2-жадвали ташкил этади.

4.2-жадвал

Ўрнига қўйиш алмаштириш (ASCII коди алифбоси белгилари асосида) жадвали

Очиқ маълумот алифбоси (стандарт ASCII коди белгилари)	$ASCII_0$	$ASCII_1$	…	…	$ASCII_{255}$
Шифрмаълумот алифбоси (иккилик саноқ тизими белгилари)	$x_0^0 x_1^0 ... x_7^0$	$x_0^1 x_1^1 ... x_7^1$			$x_0^{255} x_1^{255} ... x_7^{255}$

бу ерда $x_i^j \in \{0;1\}$ бўлиб, стандарт ASCII коди алифбоси *256* та ҳар хил белгиларини битлар билан ифодалаш учун саккиз бит кифоя, яъни $2^8 = 256$.

Бу шифрлаш жараёнини ифодаловчи алгоритм калитларининг умумий сони $256!$ бўлиб, ушбу $n! \approx \left(\frac{n}{e}\right)^n \sqrt{2\pi n}$ - Стирлинг формуласига кўра қуйидагича

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

ҳисобланади. Бундай ҳолат эса калитни билмаган ҳолда дешифрлаш жараёнини амалга оширишни етарли даражада мураккаблаштиради.

Юқорида келтирилган жадваллар ўрнига қўйишга асосланган шифрлаш алгоритмларининг энг оддий кўринишлари моделини ифодалайди. Яъни шифрлаш жараёнида шифр қийматлар деб аталувчи очиқ маълумот алифбоси белгиларига мос келувчи шифрбелгилар деб аталувчи шифрмаълумот алифбоси белгилари ўзгармайди.

Агарда очиқ маълумот компьютердан фойдаланилган ҳолда тузилиб, стандарт ASCII коди алифбоси белгиларини кенгайтирилган компьютер стандарт ANSI коди алифбоси белгиларидан иборат бўлиб, шифрмаълумот стандарт ANSI коди алифбоси белгиларини бирини бошқаси билан алмаштиришдан иборат бўлган ўрнига қўйишга асосланган шифрлаш алгоритмини қўллаш натижасида ҳосил қилинган бўлса, у ҳолда шифрлаш жараёни асосини қуйидаги ўрнига қўйиш алмаштириш 4.3-жадвали ташкил этади.

4.3-жадвал

Ўрнига қўйиш алмаштириш (ANSI коди алифбоси белгилари асосида) жадвали

Очиқ маълумот алифбоси (стандарт ANSI коди белгилари)	ANSI $_0$	ANSI $_1$	…	…	ANSI $_{2^{32}-1}$
Шифрмаълумот алифбоси (иккилик саноқ тизими белгилари)	$x_0^0 x_1^0 \ldots x_{31}^0$	$x_0^1 x_1^1 \ldots x_{31}^1$	…	…	$x_0^{2^{32}-1} x_1^{2^{32}-1} \ldots x_{31}^{2^{32}-1}$

Оддий ўрнига қўйишга асосланган шифрлаш алгоритмларининг аналитик (формулали) ифодасини иккита тенг кучли тўпламлар, яъни элементлари сони тенг бўлган тўпламлар, элементлари устида ўрнатилган ўзаро бир қийматли акслантиришлардан (функциялардан) иборат деб тушуниш мумкин. Бундай акслантиришлар ҳар доим тескарисига эга бўлади, яъни ўзаро бир қийматлилик хоссаси акслантиришнинг тескариси мавжудлигининг етарлилик шартини таъминлайди. Ўзаро бир қийматли функция одатда чизиқлилик хоссасига эга. Масалан, юқорида келтирилган жадвалли оддий ўрнига қўйишга асосланган шифрлаш алгоритмларининг моделларини мос равишда уларнинг ушбу кўринишдаги: $f(x_i) = kx_i + b(\mathrm{mod}\,32), \quad i = 0,1,\ldots,31;$ $f(x_j) = kx_j + b(\mathrm{mod}\,256), \quad j = 0,1,\ldots,255;$ $f(x_l) = kx_l + b(\mathrm{mod}\,2^{32})$, $l = 0,1,\ldots,2^{32}-1;$ аналитик (формулали) ифодалари билан алмаштириш мумкин, бу ерда k ва b ўзгармас сонлар. $f(x_i)$ -функция чизиқсиз бўлса, у кўп қийматли бўлиб, унинг тескарисини ҳар доим ҳам аналитик (формулали) кўринишда ифодалаш имкони мавжуд бўлавермай, умумий кўринишда тўпламга тегишлилик ифодасига эга бўлади: $f^{-1}(y_i) \in \{x_{i_1}, x_{i_2}, \ldots, x_{i_t}\}$.

4.1.2. Бир қийматли ва кўп қийматли ўрнига қўйишга асосланган шифрлаш алгоритмларининг математик моделлари

Ўрнига қўйишга асосланган шифрлаш алгоритмлари, уларнинг асосини ташкил этувчи акслантиришнинг бир қийматли ёки кўп қийматлигига кўра, бир қийматли ва кўп қийматли синфларга бўлинади.

Агар ўрнига қўйишга асосланган шифрлаш алгоритмида очиқ маълумот алифбоси белгиларининг ҳар бирига шифрмаълумот алифбосининг битта белгиси мос қўйилса, бундай алгоритм бир қийматли ўрнига қўйишга асосланган шифрлаш алгоритми синфига киради. Очиқ маълумот алифбоси белгилари $x_1, x_2, \ldots, x_N$ деб белгиланса, масалан, лотин алифбоси белгилари учун $N = 26$, кирилл алифбоси белгилари учун $N = 32$, стандарт ASCII коди алифбоси белгилари учун $N = 256$ ва ҳоказо. Шифрмаълумот алифбоси белгилари $y_1, y_2, \ldots, y_M$ деб белгиланса, у ҳолда бир қийматли ўрнига қўйишга асосланган шифрлаш алгоритмининг умумий ҳолдаги модели 4.4-жадвал кўринишда қуйидагича ифодаланади:

4.4-жадвал

Ўрнига қўйишга асосланган шифрлаш алгоритмининг умумий модели

Очиқ маълумот алифбоси белгилари	x_1	x_2	…	…	x_N
Шифрмаълумот алифбоси белгилари	y_{i_1}	y_{i_2}	…	…	y_{i_N}

бу ерда $y_{i_j} \in \{y_1, y_2, ..., y_M\}$. Бу ерда M сони N сонидан қанча катта бўлса, яъни шифрбелгилар тўпламининг қуввати шифр қийматлар тўпламининг қувватидан қанча катта бўлса, калитларни ифодаловчи мумкин бўлган барча жадваллар сони шунча кўп бўлиб, бундай шифрлаш алгоритмининг криптобардошлилиги ортади. Аналитик ифодасининг умумий кўриниши ушбу чизиқли функциядан иборат: $y_{i_j} = kx_j + b(\mathrm{mod}\, N)$ бўлиб, бу ерда $j = 0,1,...,M-1;\ i = 0,1,...,N-1$.

Мисол сифатида қуйидаги *(2*х*26)*-ўлчамли 4.5-жадвални келтириш мумкин.

4.5-жадвал

(2х26) - ўлчамли жадвал

Очиқ маълумот алифбоси (лотинча белгилар 26 та)	A	B	..	...	Z
Шифрмаълумот алифбоси (кириллча белгилар 32 та)	И	Л	..	...	У

Кўп қийматли шифрлаш алгоритмларида очиқ маълумот алифбоси белгиларининг ҳар бирига шифрмаълумот алифбосининг икки ёки ундан ортиқ чекли сондаги белгилари мос қўйилади, яъни очиқ маълумот алифбосининг бирор x_i белгисига шифрмаълумот алифбосининг чекли $\{y_{i1}, y_{i2}, ..., y_{it}\} \subset \{y_1, y_2, ..., y_M\}$ тўпламидан олинган бирор y_{ij} , $(1 \le j \le t)$, белгиси мос қўйилади. Кўп қийматли ўрнига қўйишга асосланган шифрлаш алгоритмининг умумий ҳолдаги модели 4.6-жадвал кўринишида қуйидагича ифодаланади.

4.6-жадвал

Кўп қийматли ўрнига қўйишга асосланган шифрлаш алгоритмининг умумий модели

Очиқ маълумот алифбоси белгилари	x_1	x_2	...	x_N
Шифрмаълумот алифбоси белгилари	$\{y_{i_1^1}, y_{i_2^1}, ..., y_{i_t^1}\} = sh1$	$\{y_{i_1^2}, y_{i_2^2}, ..., y_{i_r^2}\} = sh2$	...	$\{y_{i_1^N}, y_{i_2^N}, ..., y_{i_p^N}\} = shN$

бу ерда: $y_{i_l^d} \in \{y_1, y_2, ..., y_M\}$. 4.6-жадвалдаги $sh1, sh2, ..., shN$ - тўпламлар тенг қувватли бўлса, яъни элементлари сони тенг бўлса, алгоритм тенг қийматли ўрнига қўйишга асосланган шифрлаш алгоритми бўлади, акс ҳолда ҳар хил қийматли шифрлаш алгоритми бўлади.

Агар $\max\{y_1, y_2, ..., y_M\} + 1 = D$ бўлса, бу жадвалнинг аналитик ифодаси: $y_{i_l}^{d} = f(x_d)(\mathrm{mod}\, D) \in shd$ бўлади, бу ерда $f(\cdot)$ - ирор ўзгарувчан параметрга боғлиқ ёки чизиқсизлик каби кўп қийматлилик хоссасига эга бўлган функция,$1 \le i_l \le M$, $1 \le d \le N$.

Мисол сифатида қуйидаги *(2x32)*-ўлчамли 4.7-жадвални келтириш мумкин.

4.7-жадвал

(2x32)-ўлчамли жадвал

Очиқ маълумот алифбоси (кириллча белгилар)	А	Б	...	...	Я
Шифрмаълумот алифбоси (стандарт ASCII коди белгилари)	*, d, n	W, &, s, g	...	...	14, !, /, j, a

Кўп қийматли шифрлаш алгоритмларининг аппарат-техник ва аппарат-дастурий таъминотлари нисбатан самарасиз бўлганлиги сабабли амалда кам қўлланилади.

Ўрнига қўйишга асосланган шифрлаш алгоритмлари, уларнинг асосидаги акслантиришни шифрлаш жараёнида босқичма-босқич ўзгариб туришига кўра бир алифболи ва кўп алифболи шифрлаш синфларига бўлинади.

4.1.3. Бир алифболи ва кўп алифболи ўрнига қўйишга асосланган шифрлаш алгоритмлари акслантиришларининг математик асослари ва хусусиятлари

Олдинги параграфларда бир қийматли ва кўп қийматли ўрнига қўйишга асосланган шифрлаш алгоритмларининг умумий моделини мос равишда сатрлари сони иккига ва устунлари сони очиқ маълумот алифбоси белгилари сонига тенг бўлган *(2xN)* – ўлчамли жадваллар ва уларга мос келувчи аналитик формулалар билан ифодаланди. Бу жадваллар ўрнига қўйиш акслантиришни ифодалайди ва шифрлаш жараёнида фақат битта жадвалдан фойдаланилади, яъни очиқ маълумот алифбосининг бирор алоҳида олинган белгиси, шифрлаш жараёнида унинг неча марта такрорланишидан қатъий назар, ҳар доим жадвалнинг шифрмаълумот алифбоси белгилари сатридаги мос белгига алмаштирилади. Шифрмаълумот алифбоси ўзгармайди. Агарда ўрнига қўйишга асосланган шифрлаш алгоритми акслантиришининг асосини ташкил этувчи жадвалнинг шифрмаълумот алифбоси белгилари сатридаги мос белгиларининг жойлашиш тартиби шифрлаш жараёни босқичларида ўзгариб турмаса, бундай алгоритм бир алифболи ўрнига қўйишга асосланган шифрлаш алгоритми синфига киради. Аксинча бўлса, яъни шифрмаълумот алифбоси белгилари сатридаги мос белгиларнинг жойлашиш тартиби шифрлаш жараёни босқичларида ўзгариб турса, бундай алгоритм кўп алифболи ўрнига қўйишга асосланган шифрлаш алгоритми синфига киради. Бундан келиб чиқадики, кўп алифболи ўрнига қўйишга асосланган шифрлаш алгоритмининг моделини ифодаловчи акслантириш жадвалининг сатрлари сони учта ва ундан ортиқ бўлади, уларнинг сони қанча кўп бўлса, мос алгоритмнинг бардошлилиги шунча юқори бўлади. Шундай қилиб, кўп алифболи ўрнига қўйишга асосланган шифрлаш алгоритмининг умумий ҳолдаги модели 4.8-жадвал кўринишида қуйидагича ифодаланади.

4.8-жадвал

Кўп алифболи ўрнига қўйишга асосланган шифрлаш алгоритмининг умумий модели

Очиқ маълумот алифбоси белгилари	x_1	x_2	...	...	x_N
Шифрмаълумот алифбоси белгилари	$y_{i_1}^1$	$y_{i_2}^1$	...	...	$y_{i_N}^1$
Шифрмаълумот алифбоси белгилари	$y_{i_1}^2$	$y_{i_2}^2$	...	...	$y_{i_N}^2$
...	...	...	...	...	...
...	...	...	...	...	...
Шифрмаълумот алифбоси белгилари	$y_{i_1}^w$	$y_{i_2}^w$	...	...	$y_{i_N}^w$

Бу ерда $y_l^d \in \{y_1, y_2, ..., y_M\}$. Бу жадвалга мос келувчи кўп алифболи шифрлаш жараёнининг аналитик ифодаси: $y_{i_j}^d = f(x_j)$, $d-$ босқич тартиби, $1 \leq d \leq w$, $f(\cdot)$ -акслантириш d -параметрга боғлиқ бўлган чизиқли функция, яъни $f(x_j) = k_d x_j + b_d (\mathrm{mod}\, D)$, бу ерда $D = \max\{y_1, y_2, ..., y_M\} + 1$, k_d ва b_d - босқичларга мос келувчи натурал сонли коэффициентлар.

Мисол сифатида қуйидаги 4.9- ва 4.10-жадваллар билан ифодаланувчи кўп алифболи ўрнига қўйишга асосланган шифрлаш алгоритмларининг моделларини келтириш мумкин:

4.9-жадвал

Очиқ маълумот алифбоси (лотинча белгилар)	A	B	...	...	Z
Шифрмаълумот алифбоси (кириллча белгилар)	И	Л	...	...	У
...	...	...	...	...	...
Шифрмаълумот алифбоси (кириллча белгилар)	Д	Я	...	...	З

ҳамда

4.10-жадвал

Очиқ маълумот алифбоси (лотинча белгилар)	A	B	...	...	Z
Шифрмаълумот алифбоси (кириллча белгилар)	И	Л	...	...	У
Шифрмаълумот алифбоси (стандарт ASCII коди белгилари)	*	G	…	…	&
...	...	...	...	...	...
Шифрмаълумот алифбоси (кириллча белгилар)	Д	Я	...	...	З

Юқорида ўрнига қўйишга асосланган шифрлаш жараёни модели жадваллари ва уларга мос келиши мумкин бўлган аналитик ифодалар ҳақида сўз юритилди. Ўрнига қўйишга асосланган шифрлаш жараёнларини ифодаловчи акслантиришлар функцияларини ҳар доим ҳам аппаратли қўлланиши амалий жиҳатдан қулай бўлган жадвал кўринишда ифодалаш имкони бўлавермайди. Хусусан, қуйида ўрнига қўйишга асосланган шифрлаш жараёни шифр қиймат ва махфий калит устида бирор амални қўллаш билан амалга ошириладиган алгоритмлар моделининг математик ифодалари ҳақида сўз юритилади.

4.2. Виженер шифрлаш тизими

Француз криптографи Блейз де Виженер қадимда энг машҳур бўлган кўп алифболи тизимларга асос солган. Бу тизим унинг шарафига Виженер тизими деб аталган. Виженер тизими ҳам Цезарь тизимига ўхшаш бўлиб, унда калит қадам-бақадам ўзгаради. Шифрматн ҳосил қилиш ва уни дастлабки матнга ўгиришда Виженер квадратидан фойдаланилади [9-расм]. Ҳар бир устун *0,1,2,..,25* калитли Цезарь тизими каби қаралиши мумкин. Шифрлаш учун дастлабки матн ҳарфлари квадрат жадвал сатридан Цезарь тизими калитини эса квадрат жадвал устунидан ўқилади.

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

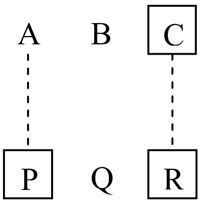
9-расм. Виженер квадрати

Калитлар одатда калит сўзи атамаси билан ифодаланади. Масалан, дастлабки матнда ODAMGA сўзи калит сўз CRYPTO ёрдамида шифрматн биринчи ҳарфи O–сатр ва C-устунга тегишли катакда жойлашган Q ҳарфи бўлади. Шундай қилиб, шифрматн бўлаги QUYBZO шаклини олади. Бу ерда калит сўзининг даври 6 га тенг бўлиб, одатда кўп ҳарфли хабарларни шифрлашда даврий равишда такрорланади. Масалан, агар хабар 15 ҳарфдан иборат бўлса, калит сўзи CRYPTOCRYPTOCRY кўринишида бўлади. Шифрматнни дастлабки матнга ўгиришда сатр ва устунларнинг ўрни ўзаро алмаштирилган квадратдан фойдаланиш кифоядир [17].

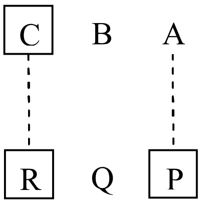
Виженер квадратини тўлдириш тартиби ҳам аслида калитнинг бир қисми бўлиб хизмат қилади. Шунинг учун Виженер квадрати сифатида осон эслаб қолинадиган квадратлардан фойдаланилган. Булар орасида адмирал Фрэнсис Бьюфорт квадрати машҳурдир [17].

Унинг сатрлари бўлиб тескари тартибда ёзилган Виженер квадрати сатрлари хизмат қилади. Бу тизим шамол тезлигини аниқловчи шкалани яратган адмирал Френсис Бтюфорт шарафига номланган.

Агар Виженер квадратида биринчи устун ва биринчи сатр, сатр ва устунларни кўрсатса, Бьюфорт квадратида эса бу вазифани биринчи сатр ва охирги устун бажаради. Шундай қилиб, CRYPTO хабарини шифрлашда криптотизимнинг биринчи ҳарфи икки квадратдан қуйидагича ҳосил бўлади:



Виженер



Бьюфорт

XVI асрда Джиролано Кардано Виженер тизимининг навбатдаги модификацияси AUTOCLAVEни яратди. У математиклар орасида учинчи ва тўртинчи даражали тенгламалар тизимини ечишга бағишланган формулалари билан машҳурдир. AUTOCLAVE тизимида шифрланадиган хабар маълум қадамга сурилган ҳолда шифрматн калити вазифасини ҳам ўтайди, яъни хабар ўзи-ўзига калит бўлиб хизмат қилади. Калит бош қисми сифатида калит сўзидан ёки хабарнинг даврий охиридан фойдаланилган.

4.3. Ўрин алмаштиришга асосланган шифрлаш алгоритмларининг хусусиятлари ва математик модели

Ўрин алмаштиришга асосланган шифрлаш алгоритмларининг асосий хусусияти очиқ маълумот ва шифрмаълумот алифбоси белгиларининг бир хиллигидадир, яъни шифрмаълумотни ташкил этувчи белгиларнинг маъноси мос келувчи очиқ маълумотдаги белгиларнинг маъноси билан бир хил бўлади. Ҳақиқатан ҳам, ўрин алмаштиришга асосланган шифрлаш жараёнида очиқ маълумот алифбоси белгилари ўринлари алмаштирилиши натижасида шифрмаълумот ҳосил қилинади. Мисол учун, шартли равишда, бирор алифбода тузилган ушбу “$x_1 x_2 ... x_N$” – очиқ маълумотдан, уни ташкил этувчи шифр қийматлар ўринларини алматириш натижасида “ $x_{i_1} x_{i_2} ... x_{i_N}$ ” – шифрмаълумот ҳосил қилинган бўлса, у ҳолда калитни ифодаловчи $1 \to i_1, 2 \to i_2, ..., N \to i_N$ - ўрин алмаштиришлар сони очиқ маълумотни ташкил этувчи алифбо белгиларининг сони билан тенг. Калитни ифодаловчи функцияни ушбу 4.11-жадвал кўринишида бериш мумкин.

4.11-жадвал

Тартиб сонлар	1	2	3	...	*N*-2	*N*-1	*N*
Шифр қийматларининг очиқ маълумотдаги ўрни	x_1	x_2	x_3		x_{N-2}	x_{N-1}	x_N
Шифр қийматларининг шифрмаълумотдаги ўрни	x_{i_1}	x_{i_2}	x_{i_3}		$x_{i_{N-2}}$	$x_{i_{N-1}}$	x_{i_N}

бу ерда $1 \le i_j \le N$. Умумий ҳолда ўрин алмаштиришга асосланган шифрлаш алгоритмлари акслантиришлари очиқ маълумот шифр қийматларининг шифрланувчи маълумот матнида жойлашган ўрнини белгиловчи индекслар устида амалга оширилиб, шифр қийматларнинг шифрмаълумотда жойлашиш ўрнини белгиловчи индексларини аниқлайди, яъни ўрин алмаштириш қоидасини – функциясини аниқлайди. Келтирилган жадвалли функцияга мос аналитик формула кўринишидаги функция:

$f(i)\bmod(N+1) = j_i$ ёки $x_i = x_{f(i)\bmod(N+1)} = x_{i_j}$ бўлиши мумкин. Бу ерда $f(\cdot)$ - индекслар ўрин алмаштириш қоидасини аниқловчи функция.

Ўрин алмаштиришга асосланган шифрлаш алгоритмларининг калити узунлиги, умуман олганда, шифрланиши керак бўлган маълумот узунлигига, яъни очиқ маълумотни ташкил этувчи алифбо белгиларининг сонига тенг. Бундан ташқари, очиқ маълумотни ташкил этувчи алифбо белгиларининг частотавий хусусиятлари тўлалигича шифрмаълумотга ўтади. Бундай ҳолатлар амалий татбиқ имкониятларини чеклайди. Шундай бўлсада уларнинг самарали татбиқларини таъминлашга қаратилган синфлари мавжуд. *Йўналишли ўрин алмаштириш* синфидаги шифрларнинг қўлланилиши амалда кўп тарқалган. Бундай шифрлаш алгоритмлари бирор геометрик шаклга асосланган бўлади. Очиқ маълумот блоклари геометрик шаклга бирор траектория (узлуксиз из) бўйича жойлаштирилади. Шифрмаълумот эса бошқа траектория бўйича ҳосил қилинади. Геометрик шакл сифатида (*n*x*m*) ўлчамли жадвал олиб, унинг биринчи сатри бошидан бошлаб очиқ маълумот белгиларини чапдан ўнгга кетма-кет жойлаштириб, сатр тугагач иккинчи сатрга, очиқ маълумот белгиларини ўнгдан чапга кетма-кет жойлаштириб, бу сатр тамом бўлгач, кейинги сатрга олдингисига тескари йўналишда жойлаштирилади ва ҳоказо. Охирида тўлмай қолган сатр ячейкалари очиқ маълумот алифбосидан фарқли бўлган белгилар билан тўлдирилади. Сўнгра очиқ маълумотни жойлаштириш тартибидан фарқли бўлган бирор йўналиш танлаб олиниб, шу йўналиш асосида шифрмаълумот ҳосил қилинади. Шифрмаълумот ҳосил қилиш йўналиши калит вазифасини бажаради. Мисол сифатида "*йўналишли ўрин алмаштиришга асосланган шифрлаш алгоритми*" жумласини шифрлашни *(4*x*10)–*ўлчамли жадвал асосида қуйидагича амалга ошириш мумкин (амалда жадвалнинг ўлчами калит сифатида махфий ҳисобланади):

1	2	3	4	5	6	7	8	9	10
Й	*ў*	*н*	*а*	*л*	*и*	*ш*	*л*	*и*	*ў*
и	*т*	*ш*	*а*	*м*	*л*	*а*	*н*	*и*	*р*
р	*и*	*ш*	*ш*	*и*	*ф*	*р*	*л*	*а*	*ш*

...	*и*	*м*	*т*	*и*	*р*	*о*	*г*	*л*	*а*

Бу жадвал устунлари кетма-кетликларини аралаштирган ҳолда (бундай аралаштиришларнинг умумий сони *10!=3628800* та бўлади), масалан, *72968411035* тартиб (калит) билан

“*шароўтиииалилфрлнлгааштйирўршанишмлмии*”

шифрмаълумотни ҳосил қиламиз. Шифрмаълумотни ҳосил қилиш жараёнини жадвалнинг сатрлари ўринларини ёки ҳар бир устунлари сатрларини алоҳида алмаштиришлар билан яна ҳам мураккаблаштириш мумкин. Сатрлар, устунлар ва алоҳида олинган сатр устунларини ёки алоҳида олинган устун сатрларини шифрлаш жараёни босқичларида ўзгартириб туриш билан яна ҳам мураккаб бўлган шифрлаш алгоритмларини ҳосил қилиш мумкин.

Берилган *4*x*10* ўлчамли жадвал *4*x*10* ўлчамли $A_{4\times10}$ - матрица кўринишида ифодаланса, унинг элементлари a_{ij} , $i=1,2,3,4;$ $j=1,2,...,8;$ сатр ва устунлари устида акслантиришларни бажариш қулай бўлиб, матрицалар назариясининг айрим хоссаларидан фойдаланиб, криптографик самарадорликни оширишнинг илмий асосланган усуллари келиб чиқади. Бу фикрларнинг исботи ҳозирги кунда матрицаларни криптология соҳасида кенг ва самарали қўлланилаётгани ҳамда янги илмий изланиш ғоялари натижалари билан тасдиқланади.

Ўрин алмаштиришга асосланган шифрлаш алгоритмлари ҳақида тўлароқ маълумотларни [12-13, 59-60] дан топиш мумкин.

4.4. Гаммалаштиришга асосланган шифрлаш алгоритмларининг математик асослари

Шифрлаш жараёнида очиқ маълумотни ташкил этувчи мос алифбо белгилари билан “калит” деб аталувчи параметрнинг мос элементлари устида бирор амал бажариш натижасида шифрмаълумотни ташкил этувчи алифбо бегиларига акслантириш амалга оширилса, бундай шифрлаш алгоритми гаммалаштириш шифрлаш алгоритми туркумига киради.

Гаммалаштириш билан шифрлаш услубининг моҳияти очиқ маълумотни (ёки шифрмаълумотни) ташкил этувчи алифбо белгилари билан, шифрлаш калитини ифодаловчи псевдотасодифий кетма-кетликнинг мос элементлари гаммасини ташкил этувчи элементлар устида бирор амал бажариш билан шифрмаълумот ҳосил қилишдан иборат. Бунда очиқ, шифрланган ва калитни ифодаловчи гамма маълумотларнинг алифбо белгилари битта тўпламдан олинган бўлиши зарур. Мисол учун *2* модуль бўйича қўшиш амалидан фойдаланиб, иккилик саноқ тизими алифбосида рақамли кўринишда берилган маълумотни қуйидагича шифрлаш ва дешифрлаш мумкин:

Очиқ матн: 0110011100100011...
Калитни ифодаловчи гамма: 110110010110101...
Шифрланган матн: 1000101110010110...
Калитни ифодаловчи гамма: 1110110010110101...
Очиқ матн: 0110011100100011...

Бу мисолдан кўринадики, дешифрлаш учун калит бўйича (яъни калитни ташкил этувчи гамма элементлари бўйича) шифрмаълумотнинг мос элементларини 2 модуль бўйича қўшишдан фойдаланиб қайта гаммалаштириш кифоя. Бундай шифрлаш ва дешифрлаш жараёнлари акслантиришларининг математик модели мос равишда ушбу: $x_i \oplus k_i = y_i$ ва $y_i \oplus k_i = x_i$ (аналитик) формулавий ифодаларга эга. Бу ерда x_i - очиқ маълумотнинг *i*-бити, k_i - калитни ифодаловчи гамманинг *i*-бити, y_i-шифрланган маълумотнинг *i*-бити, $\oplus$- модуль 2 бўйича қўшиш амалидан иборат. Яъни юқоридаги ифодалар ушбу: $(x_i + k_i)\bmod 2 = y_i$ ва $(y_i + k_i)\bmod 2 = x_i$ формулаларга тенг кучли. Бирор n -характеристикага эга бўлган чекли майдонларда $\bmod n$ бўйича амаллар бажариш очиқ маълумот алифбоси белгилари ёки белгилар бирикмаларини ифодаловчи шифр қиймат ва шифрмаълумот алифбоси белгилари ёки белгилар бирикмаларини ифодаловчи шифрбелгиларнинг чекли сонда эканлиги билан узвий боғлиқ. Мисол учун очиқ маълумотни ташкил этувчи алифбо кириллча 32 та белгилардан иборат бўлсин.

Уларни $А \to 0, Б \to 1, В \to 2, \ldots, Я \to 30,$ *бўшлиқ(пробел)* $\to 31$ мослик билан ифодалаб, калит гаммасини ушбу *ТГЗ...ЯЛ...КЗУ* кўринишдаги тасодифий кетма-кетликдан иборат деб олиб, “*гаммалаштириш*” – очиқ маълумотни шифрлашни қуйидагича амалга ошириш мумкин:

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

$(М+З)\mathrm{mod}32 = (13+8)\,\mathrm{mod}\,32 = 21 \to Ф, \quad \ldots, \quad (А+Я)\mathrm{mod}32 = (0+30)\,\mathrm{mod}\,32 = 30 \to Я,$

$(Ш+Л)\mathrm{mod}32 = (25+12)\,\mathrm{mod}\,32 = 5 \to Д, \ \ldots, \ (Р+К)\mathrm{mod}32 = (17+11)\,\mathrm{mod}\,32 = 28 \to Ь,$

$(И+З)\mathrm{mod}32 = (9+8)\,\mathrm{mod}\,32 = 17 \to Р, \ (Ш+У)\mathrm{mod}32 = (25+20)\,\mathrm{mod}\,32 = 13 \to М,$

ва натижада “*ЦГФ...ЯД...ЬРМ*” –шифрмаълумотга эга бўламиз. Дешифлаш эса қуйидагича амалга оширилади:

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

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

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

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

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

Худди юқорида келтирилган мисолдаги каби, агарда очиқ маълумот компьютердан фойдаланилган ҳолда тузилиб, стандарт ASCII коди алифбоси белгиларидан иборат бўлса, у ҳолда очиқ маълумотнинг X_i-белгисини, унга мос ASCII$_i$ коди қийматига, шифрлаш жараёнида унга мос келувчи калит гаммаси $Г_j$ -элементининг ASCII$_j$ коди қийматини характеристикаси 256 бўлган чекли майдонда қўшиб, натижанинг қийматига тенг бўлган ASCII кодли Y_i белгига алмаштирилади: $(X_i + Г_j)\,\mathrm{mod}\,256 = Y_i$ ва шифрмаълумот ҳосил қилинади. Дешифрлаш ушбу: $(Y_i - Г_j)\,\mathrm{mod}\,256 = X_i$ формула орқали амалга оширилиб, шифрмаълумотга мос очиқ маълумот ҳосил қилинади.

Агарда калит гаммаси қайтарилувчи даврга эга бўлган битлардан иборат бўлмаса, олинган шифрмаълумотни очиш етарли даражада қийин бўлади. Бунинг учун калит гаммасини ташкил этувчи элементлар тасодифий ўзгариши керак. Амалда калит гаммасининг даври бутун шифрмаълумот узунлигидан катта бўлиб, очиқ маълумотнинг ҳеч бир қисми маълум бўлмаса, бундай шифрмаълумотга мос келувчи очиқ маълумотни топиш мураккаб бўлади. Бундай ҳолларда шифрмаълумот фақат узунлиги унинг узунлигига тенг бўлган калит гаммасининг мумкин бўлган барча вариантларини танлаш орқали очилади.

Агарда рақиб томонга очиқ маълумотнинг бирор қисми ва унга мос келувчи шифрмаълумот маълум бўлиб қолса, у ҳолда шифрлашнинг гаммалаштириш услуби ўз кучини йўқотади. Чунки бундай ҳолда рақиб томон очиқ маълумотнинг маълум бўлган қисми мазмунига кўра бутун шифрмаълумотни очишга ҳаракат қилади. Мисол учун, кўплаб махфий ҳужжатлар «Мутлақо махфий» ёки бошқа шу каби сўзлар билан бошланиб, криптоаналитик учун таҳлил йўналишини аниқлашга ёрдам беради. Бундай ҳолатларни ахборот тизими муҳофазаси криптотизимининг амалда қўлланилишида албатта ҳисобга олиш керак.

4.5. Маълумотларни шифрлаш алгоритмлари

Юқорида ўрнига қўйиш ва ўрин алмаштиришга асосланган шифрлаш алгоритмларини, уларнинг асосидаги акслантиришларни математик моделларининг асосий хусусиятлари кўриб ўтилди.

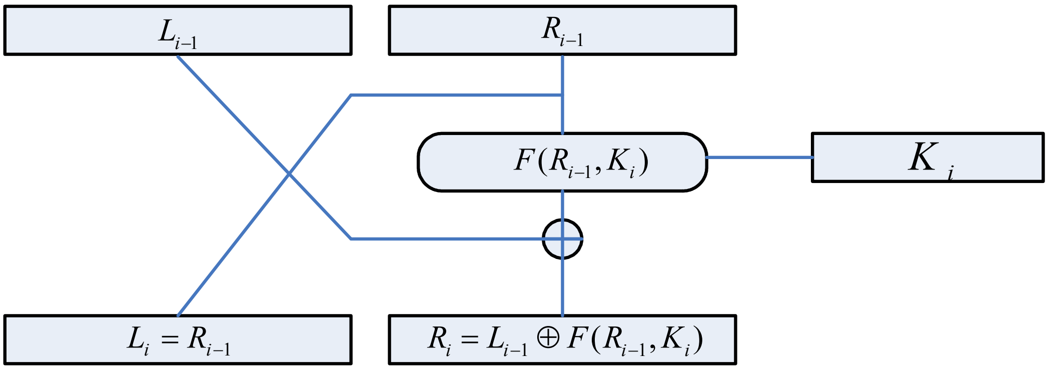
Ўрнига қўйишга асосланган шифрлаш жараёнида очиқ маълумотни ташкил этувчи алифбо белгиларини айрим (алоҳида) олинган ҳолда, шифрмаълумот алифбосининг айрим (алоҳида) олинган белгиларига алмаштириш ёки ўрин алмаштиришга асосланган шифрлаш жараёнида очиқ маълумотни ташкил этувчи алифбо белгиларини айрим (алоҳида) олинган ҳолда ўринларини алмаштириш амалга оширилган бўлсин. Бундай ҳолатда шифрлаш жараёни алгоритмининг криптобардошлилигини ошириш учун калит узунлиги шифрланиши керак бўлган маълумот узунлиги даражасида бўлиши зарур бўлади. Мисол учун, шартли равишда, бирор алифбода тузилган ушбу “$x_1x_2...x_N$” – очиқ маълумотдан, уни ташкил этувчи алифбо белгиларининг ўринларини алмаштириш натижасида “ $x_{i_1}x_{i_2}...x_{i_N}$ ” – шифрмаълумот ҳосил қилинган бўлса, у ҳолда калитни ифодаловчи $1 \to i_1, 2 \to i_2, ..., N \to i_N$ - ўрин алмаштиришлар сони очиқ маълумотни ташкил этувчи алифбо белгиларининг сони билан тенг. Худди шу каби, ўрнига қўйишга асосланган шифрлаш алгоритмларидан фойдаланишда очиқ маълумот частотавий хусусиятларининг шифрмаълумотга кўчмаслигини таъминлаш учун кўп алифболи шифрлаш алгоритмларидан фойдаланилади, бунга эришиш учун эса, юқорида кўрилганидек шифрлаш жараёни босқичларида бир хил белгиларни ҳар хил белгиларга алмаштириш, яъни калит узунлигини ошириш зарурати туғилади. Шифрланиши керак бўлган маълумот ҳажмининг ортиши билан, шифрлаш жараёнини амалга оширишда қўлланиладиган алгоритм калити узунлигининг мос равишда ортиб бориши, криптобардошлиликни таъминлаш нуқтаи назаридан самарали бўлсада, бундай ҳолат алгоритмларнинг амалда қўлланишлари нуқтаи назаридан: калитларни сақлашда, уларни тарқатишда, аппарат-техник таъминотларни амалга оширишда ва бошқа шу каби ҳолатларда ноқулайликлар туғдиради. Шунинг учун шифрланиши керак бўлган маълумотни, уни ташкил этувчи алифбо белгиларининг маълум бир узунликдаги бирикмалари (блоклари) бирлашмаси (конкатенацияси) кўринишда ифодалаб, ана шу блокларнинг алоҳида-алоҳида самарали ва криптобардошли шифрланишини амалга ошириш масаласи келиб чиқади. Бу масала симметрик блокли шифрлаш алгоритмлари орқали амалга оширилди. Симметрик блокли шифрлаш алгоритмларининг асосини очиқ маълумот блокларини юқори даражада *аралаштириш* ва *тарқатиш* (ёйилиш, таралиш) хоссаларига эга бўлган акслантиришлар ташкил этади [13, 59-60]. *Самарали аралаштириш* берувчи ($\oplus$, $\mathrm{mod}\, 2^n$, *ўрин алмаштириш жадваллари*, *циклик суришлар* ва ҳоказо) амаллар *корреляцион иммунстлик* – шифрланиши керак бўлган ёки калит блокларини ташкил этувчи алифбо белгиларидан бирининг ўзгариши, акслантириш натижасида олинган шифрблокни ташкил этувчи алифбо белгиларининг фақат биргина мос белгиси ўзгаришига таъсир қилиб, бошқа қисмига таъсир этмаслигини таъминловчи ўрин алмаштиришга асосланган шифрлаш акслантиришларидан иборат. *Самарали тарқатиш* берувчи бир алифболи ва кўп алифболи ўрнига қўйиш акслантиришларга асосланган S блок акслантиришлари *чизиқсизликни* - шифрланиши керак бўлган ёки калит блокларини ташкил этувчи алифбо белгиларидан бирининг ўзгариши, акслантириш натижасида олинган шифрблокни ташкил этувчи алифбо белгиларининг икки ва ундан ортиқ қисмига таъсир этишини таъминловчи ўрнига қўйишга асосланган шифрлаш алгоритмлари акслантиришларидан иборат.

Аралаштирувчи акслантиришлар очиқ маълумот ва унга мос келувчи шифрмаълумот блокларининг частотавий (статистик) ва аналитик боғлиқлик хусусиятларини ўрнатишни мураккаблаштирса, тарқатувчи акслантиришлар очиқ маълумот блоки битта белгисининг ўзгаришини мос шифрмаълумот блокининг кўп белгилари ўзгаришига таъсир қилишини юзага келтириб, очиқ маълумотнинг частотавий (статистик) хусусиятларини шифрмаълумотга кўчмаслигини таъминлайди.

Симметрик блокли шифрлаш алгоритмлари бир нечта босқичлардан (раундлардан) иборат бўлиб, ҳар бир раунд аралаштирувчи ва тарқатувчи акслантиришлардан тузилган. Бундай асосда тузилиш тамойили, ҳар бир раунд шифрлаш жараёнини ҳар хил калитлар билан бир хил турдаги акслантиришларни амалга оширишга ҳамда дешифрлаш жараёнини раунд акслантиришлари ва калитларини тескари тартибда қўллашнинг самарали имконини беради. Алгоритм асосини ташкил этувчи, раунд шифрлаш жараёнини амалга оширувчи, аралаштириш ва тарқатиш хусусиятларига эга бўлган функциялар *асосий акслантиришлар* дейилади. *Асосий акслантириш*ларнинг аппарат-техник жиҳатдан қулай қўлланиш модели сифатида тескари боғлиқликка эга бўлган силжитиш регистларини келтириш мумкин [13, 59-60]. Бунда тарқатувчи акслантириш тескари боғлиқликни таъминловчи функция билан, аралаштирувчи акслантириш эса, регистрдаги маълумотларни силжитиш билан амалга оширилади.

Шифрланиши керак бўлган маълумот блокини силжитиш регистрларига киритиб (юклаб), регистрдаги маълумотни шартли равишда чап ва ўнг қисм блок векторларига бўлиб, улар устида ҳар хил калитлар билан бир хил турдаги акслантиришларни босқичма-босқич амалга оширишга асосланган – *Фейстел (Фейштел) тармоғи* деб аталувчи шифрлаш жараёни функционал қурилмасига асосланган алгоритмлар кенг тарқалган. Булар жумласига DES ва ГОСТ 28147-89 киради.

Файстел тескариси мавжуд криптобардошли акслантиришларни тадқиқ қилмай, бундай акслантиришлар қатнашмаган криптобардошлилиги юқори бўлган шифрлаш тизимларини топиш масаласининг ечимига киришган. У бу масаланинг ечимини қуйидагича ҳал этган. Шифрланадиган блок иккита L_0 , R_0 қисмларга ажратилади. Фейстел тармоғи $i-$ раунди итератив блокли шифрлаш қуйидаги схема бўйича аниқланади (10-расм).



10-расм. Фейстел тармоғи $i-$раунди

Бу ерда $X_i=(L_{i-1},R_{i-1})-$ i -раунд учун L_{i-1}ва R_{i-1}қисмларга ажратилган кирувчи маълумот, $Y_i=(L_i,R_i)$ эса X_i ни $i-$ раунд калити K_i билан F акслантириш натижасида ҳосил бўлган шифрмаълумот.

Фейстел тармоғи $i-$раунди шифрлаш жараёнинг математик модели қуйидагича ифодаланади:

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

Бундай тармоққа асосланган алгоритмлар бир неча итерациядан ташкил топган K_i калитларда шифрланадиган акслантиришлардан (функциялардан) ташкил топган.

Фейстел тармоғи акслантиришларининг асосий хоссаси F -раунд функцияси тескариси мавжуд бўлмаса ҳам, Фейстел тармоғи бу акслантиришларининг тескарисини топиш имконини беради. Ҳақиқатан ҳам, шифрлаш жараёни $i-$ раунд математик моделидаги $\oplus$ - модуль 2 бўйича иккилик санок тизимида қўшиш амали хоссасидан фойдаланган ҳолда қуйидаги тенгликка эга бўлинади:

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

Бу тенгликлар Фейстел тармоғи асосида қурилган шифрлаш алгоритмларини дешифрлашнинг математик моделини ифодалайди.

4.6. Блокли шифрлар

Фейстел тармоғига асосланмаган симметрик блокли шифрлаш алгоритмларига: АҚШ давлат стандарти **AES FIPS-197**, Ўзбекистон миллий стандарти **O‘z DSt 1105:2009** симметрик блокли шифрлаш алгоритмлари мисол бўла олади.

Қуйида Фейстел тармоғига асосланмаган симметрик блокли шифрлаш алгоритмлари математик асосларини ва [13, 23, 26] да келтирилган алгоритмлар акслантиришлари асосида ёритилади.

AES криптоалгоритмининг математик асоси

AES алгоритмида байтлар устида амаллар бажарилади. Байтлар $GF(2^8)$ чекли майдон элементлари сифатида қаралади. $GF(2^8)$ майдон элементларининг даражаси 7 дан катта бўлмаган кўпҳад сифатида тасвирлаш мумкин. Агарда байтлар

$$\{a_7 a_6 a_5 a_4 a_3 a_2 a_1 a_0\},\ a_i \in \{0,1\},\ i = \overline{0...7}\,,$$

кўринишда тасвирланган бўлса, у ҳолда майдон элементлари қуйидагича кўпҳад кўринишда ёзилади:

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

Мисол учун $\{11010101\}$ байтга $x^7 + x^6 + x^4 + x^2 + a_0$ кўринишдаги кўпҳад мос келади.

Чекли $GF(2^8)$ майдон элементлари учун аддитивлик ва мультипликативлик хоссаларига эга бўлган қўшиш ва кўпайтириш амаллари аниқланган.

Кўпҳадларни қўшиш

AES алгоритмида кўпҳадларни қўшиш $\oplus$ **(XOR)** (берилган кўпҳадларга мос келувчи иккилик саноқ тизимидаги сонларнинг мос битларини mod 2 бўйича қўшиш) амали орқали бажарилади. Масалан, $x^7 + x^6 + x^4 + x^2 + x$ ва $x^7 + x^5 + x^3 + x + 1$ кўпҳадлар натижаси қуйидагича ҳисобланади:

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

Бу амал иккилик ва ўн олтилик саноқ системаларида қуйидагича ифодаланади:

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

Чекли майдонда исталган нолга тенг бўлмаган a элемент учун унга тескари бўлган $-a$ элемент мавжуд ва $a + (-a) = 0$ тенглик ўринли, бу ерда ноль элементи сифатида $\{00\}_{16}$ қаралади. $GF(2^8)$ майдонда $a \oplus a = 0$ тенглик ўринли.

Кўпҳадларни кўпайтириш

AES алгоритмида кўпҳадларни кўпайтириш қуйидагича амалга оширилади:

- иккита кўпҳад ўнлик саноқ тизимида кўпайтирилади;

- еттинчи даражадан катта бўлган ҳар қандай кўпҳадни саккизинчи даражали $\varphi(x) = x^8 + x^4 + x^3 + x + 1$ келтирилмайдиган кўпҳадга бўлганда қолдиқда етти ва ундан кичик бўлган даражадаги кўпҳадлар ҳосил бўлиб, улар натижа сифатида олинади, бунда бўлиш жараёнида бажариладиган айириш амали иккилик саноқ тизимида, юқорида келтирилгани каби, $\oplus$ амали асосида бажарилади.

AES FIPS-197 алгоритми раундларининг шифрлаш жараёнлари: *SubBytes* –берилган жадвал асосида байтларни алмаштириш, *ShiftRows* – берилган жадвал асосида байтларни циклик суриш, *MixColumns* –тескариси мавжуд бўлган берилган матрица бўйича байтларни аралаштириш, *AddRoundKey* –раунд калитлари блоки битларига мос блоклар битларини *XOR* амали билан қўшиш акслантиришларида иборат бўлиб, бу акслантиришларнинг биттаси, яъни *AddRoundKey* акслантириши бир томонлама ҳисобланади. Чунки раунд калити блоки ва унга *XOR* амали билан қўшилувчи мос блок номаълум бўлиб, бу акслантириш натижаси маълум бўлганда унга мос келувчи блокни аниқлаш учун раунд калитини топиш керак бўлади. Бундай ҳолат эса раунд калитларининг барча мумкин бўлган қийматларини танлаб чиқишни талаб этади. Раунд калит узунлигининг қанчалик катта бўлиши ва раундлар сонининг кўп бўлиши алгоритм криптобардошлилигини ифодалайди. **AES FIPS-197** алгоритми раунд калитининг энг кичик узунлиги 128 бит бўлиб, барча мумкин бўлган қийматлари сони 2^{128} та, бу узунликдаги барча мумкин бўлган ҳолатларни танлаб чиқишни бугунги ҳисоблаш техника ва технологиялари имкониятларидан самарали фойдаланилганда ҳам мумкин қадар қисқа вақт ичида амалга ошириш иложиси мавжуд эмас. Алгоритм 10 раунддан иборат.

O‘z DSt 1105:2009 «Ахборот технологияси. Ахборотнинг криптографик муҳофазаси. Маълумотларни шифрлаш алгоритми» стандарти электрон маълумотларни муҳофаза қилиш учун мўлжалланган криптографик алгоритмни ифодалайди. Маълумотларни шифрлаш алгоритми (МША) - симметрик блокли шифр бўлиб, ахборотни шифрматнга ўгириш ва дастлабки матнга ўгириш учун фойдаланилади. МША *256* bit узунликдаги маълумотлар блокини шифрматнга ўгириш ва шифрматнни дастлабки матнга ўгириш учун *256* ёки *512* bit узунликдаги криптографик калитдан фойдаланиши мумкин.

O‘z DSt 1105:2009 криптоалгоритмининг математик асоси

МШАда модуль арифметикасининг диаматрицалар алгебрасидан фойдаланилади, бунда ҳисоблашнинг қийинлик даражаси матрицалар алгебрасидаги сингари бажарилади.

Шифрматнга ўгириш ва дастлабки матнга ўгириш процедураларида фойдаланиладиган диаматрицалар алгебрасининг асосий амали диаматрицани p модуль бўйича диаматрицага тескарилаш амали ҳисобланади. Бу амалларда икки ўлчамли сеанс калити массивининг махсус тузилмали 4x4 тартибли квадрат диаматрица билан акс эттирилувчи қисмлари иштирок этади; махсус тузилмали диаматрица учун барча диагонал элементлар бир хиллиги, *1*-сатрдаги нодиагонал элементлар, шунингдек *2*-сатрнинг боши ва охиридаги элементлар ҳам бир хиллиги хосдир.

Махсус тузилмали диаматрицанинг муҳим хоссаси диаматрицанинг диааниқловчисини ҳисоблаш формуласининг соддалигидир, бу эса диаматрицани тескарилаш шартларини текшириш ишларини соддалаштиради. Махсус тузилмали диаматрицага нисбатан тескари диаматрица ўзининг дастлабки тузилмасини сақлайди.

4x4 тартибли махсус тузилмали диаматрица 10 та ҳар хил элементлар $a_0, \ldots, a_9$ дан тузилган бўлиб, унинг диааниқловчиси диагонал элемент a_7 ни учта йиғиндига кўпайтмаси сифатида топилади, бу йиғиндилардан ҳар бири диагонал элемент билан битта сатрда жойлашган унга ўнгдан қўшни элемент билан устун элементларининг йиғиндисини ифодалайди.

Махсус диаматрица учун диааниқловчи a қуйидагича топилади:

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

Махсус тузилмали диаматрицани тескарилаш шартларини текшириш МША параметрларига қўйиладиган асосий талаб ҳисобланади. У диагонал элементнинг қийматларини ва айтиб ўтилган кўпайтмаларни 2 модули бўйича ноль билан таққослашга келтирилади. Бу ҳар қандай шифрлаш калити ва функционал калитдан тескари диаматрицани шакллантиришга имкон беради.

МШАда, шунингдек бутун сонларни параметрли кўпайтириш, тескарилаш ва даражага ошириш деб аталган параметрли группа амалларидан ҳам фойдаланилади.

МША учун босқич (раунд)лар сони $e=8$ қилиб белгиланган.

Маълумотларни шифрлаш алгоритмининг параметрлари ва функциялари

МША қуйидаги параметр ва функциялардан фойдаланади:

a) k – 256 ёки 512 bit узунликдаги шифрлаш калити;

b) k_f – 256 bit узунликдаги функционал калит;

c) K_e – 8x4 (ёки 4x8) тартибли икки ўлчамли массив шаклидаги босқич калити;

d) b – 256 bit ли кириш блоклари сони;

e) e – босқичлар сони, $e=8$;

f) p, $(p+1)$ – модуль, $p=256$;

g) *Aralash()* – оддий шифралмаштириш бўлиб, дастлабки матнни шифрматнга ва тескари йўналишда алмаштириш учун диаматрицавий қисмлар устида амалга оширилади; мазкур шифралмаштириш кириши *Holat* массивининг диаматрицавий қисмлари ҳамда K_1 ва K_2 массивлари бўлиб, чиқиши *Holat* массивидир;

h) *BaytAlmash()* – оддий шифралмаштириш бўлиб, дастлабки матнни шифрматнга ва тескари йўналишда *Holat* массиви элементларини алмаштириш массиви элементлари билан байт сатҳида алмаштириш учун фойдаланилади; мазкур шифралмаштириш кириши байт сатҳида *Holat* массиви, алмаштириш массиви чизиқли массив B_{sA} $[256]$ ёки B_{sAD} $[256]$ бўлиб, чиқиши байт сатҳида *Holat* массивидир;

i) *Sur()* – *Holat* массиви элементларини янада яхшироқ аралаштириш учун дастлабки матнни шифрматнга ва тескари йўналишда алмаштиришда фойдаланилади; мазкур алмаштириш кириши байт сатҳида *Holat* массиви, чиқиши устун бўйлаб шифрлашда пастга ва сатр бўйлаб ўнгга ёки шифрни очишда устун бўйлаб юқорига ва сатр бўйлаб чапга сурилган байт сатҳида *Holat* массивидир;

j) *ShaklSeansKalitBayt()* – сеанс учун калит шакллантириш бўлиб, дастлабки матнни шифрматнга ва тескари йўналишда алмаштиришда *BaytAlmash()* шифралмаштиришини бажариш учун фойдаланилади; мазкур шифралмаштириш кириши шифрлаш калити k ва функционал калит k_f бўлиб, чиқиши байт сатҳида чизиқли массивлар B_{sA} *[256]* ва B_{sAD} *[256]*;

k) *ShaklSeansKalit()* – сеанс учун калитни шакллантириш бўлиб, дастлабки матнни шифрматнга ва тескари йўналишда алмаштиришда *Aralash()* шифралмаштиришни бажариш учун фойдаланилади; мазкур шифралмаштириш кириши байтли элементлардан таркиб топган чизиқли массив $K_{st}=[32]$ бўлиб, чиқиши махсус тузилмали диаматрицалардан ташкил топган (K_{1t}, K_2) ёки (K_1, K_{2t}) массивлар жуфтликларидир;

l) *ShaklBosqichKalit()* – сеанс давомида сеанс-босқич калитидан босқич калитини шакллантириш бўлиб, дастлабки матнни шифрматнга ва тескари йўналишда алмаштиришда *Qo'shBosqichKalit()* алмаштиришини бажариш учун фойдаланилади; мазкур алмаштириш кириши чизиқли сеанс-босқич калити массиви k_{se}, чиқиши байт сатҳида берилган икки ўлчамли $K_e[8,4]$ массивидир;

m) *Qo'shBosqichKalit()* – оддий шифралмаштириш бўлиб, дастлабки матнни шифрматнга ва тескари йўналишда *Holat* ва босқич калити массиви K_e элементлари устида истисноли ЁКИ (*2* модули бўйича битлаб қўшиш) амалини бажаришдан иборат; мазкур шифралмаштириш кириши байт сатҳида *Holat* массиви, K_e массиви бўлиб, чиқиши байт сатҳида *Holat* массивидир;

n) *Qo'shHolat()* – оддий шифралмаштириш бўлиб, шифрлаш блоклари устида амалга ошириладиган электрон код китоби режимидан бошқа режимларда дастлабки матнни шифрматнга ва тескари йўналишда *XOR* амали иштирокида фойдаланиладиган алмаштириш.

МША белгилаб қўйилган икки хил - *256* ва *512* бит узунликдаги калитлар ёрдамида амалга оширилади.

Биринчи ҳолатда, шифрлаш криптографик модулига *256* битли калит киритилади. Бу калит тўлалигича шифрлаш калити k сифатида олинади, дастлабки сеанснинг k_f функционал калити эса, шифрлаш калитининг хэш-функцияси қиймати сифатида ҳисоблаб топилади.

Иккинчи ҳолатда, шифрлаш криптографик модулига *512* битли калит киритилади. Бу калитнинг *256* битли биринчи ярми, шифрлаш калити k сифатида олинади, унинг *256* битли иккинчи ярми биринчи сеанснинг функционал калити k_f сифатида олинади.

Учинчи ҳолатда, шифрлаш криптографик модулига ҳеч қандай янги калит киритилмайди. Шифрлаш калити k сифатида олдинги сеансда ишлатилган шифрлаш калити олинади, функционал калит k_f сифатида эса олдинги сеансда ишлатилган функционал калит k_{f-1} нинг шифрлаш калити k дан фойдаланиб хэшланган қиймати олинади.

Юқорида кўриб ўтилган биринчи ва иккинчи ҳолатларда жорий сеанс учун янгиланган функционал калит k_f бундан олдинги сеансда фойдаланилган функционал калит k_{f-1} нинг хэш-функцияси сифатида ҳисоблаб топилади. Хэшлаш калити сифатида қоидага кўра шифрлаш калитидан фойдаланилади, хэшлаш функциясини ҳисоблаш дастури эса МШАнинг дастур (ёки аппарат) таъминотига қўшиб қўйилади. Функционал калитни янгилаш даври фойдаланилаётган шифрдан фойдаланиш режими ва дастлабки маълумотларнинг махфийлик даражасини ҳисобга олган ҳолда МША баённомаси билан белгиланади.

4.7. Оқимли шифрлаш алгоритмларининг математик моделлари ва хусусиятлари

Симметрик блокли шифрлаш алгоритмлари каби, оқимли шифрлаш алгоритмларининг яратилиши ҳам табиий зарурат асосида вужудга келган. Нисбатан кичик узунликка эга бўлган, яъни кафолатланган криптобардошлиликни таъминловчи узунликка эга бўлган – бугунги кунда *128* битдан кам бўлмаган калит билан бир томонлама криптографик акслантиришлар асосида, етарли даражада катта узунликдаги псевдотасодифий кетма-кетлик (ПТКК) гаммасини ишлаб чиқарувчи генераторлар негизида оқимли шифрлаш алгоритмлари яратилади. Узунлиги *128* битдан кам бўлмаган калитларнинг мумкин бўлган барча вариантлари сони 2^{128} тадан кам бўлмай, уларнинг ҳаммасини танлаб чиқиш жараёнини амалга ошириш, бугунги кун ҳисоблаш техника ва технологияларининг мавжуд илғор имкониятларидан фойдаланилганда ҳар доим ҳам самарали натижалар беравермайди. Ана шундай генераторлар ишлаб чиқарган гамма кетма-кетликни ташкил этувчи алифбо белгиларини очиқ маълумот мос алифбо белгилари билан бирор амал бажариш орқали шифрмаълумот алифбоси белгиларига алмаштириш – гаммалаштириш амалга оширилади. Бундай шифрлаш жараёни кўп алифболи ўрнига қўйишга асосланган шифрлашни амалга оширишни самарали усулини ифодалайди – кафолатли криптобардошлиликни таъминловчи кичик узунликдаги калит билан, очиқ маълумотнинг частотавий хусусиятларини шифрмаълумотга кўчирмайдиган етарли криптобардошлиликни таъминловчи шифрлашни амалга оширади.

Оқимли шифрлаш алгоритмлари асосини ПТКК ишлаб чиқарувчи генераторлар ташкил этади. Бундай генераторларнинг асосий криптобардошлилик характеристикаси ушбу генераторлар ҳосил қилган кетма-кетликнинг тасодифийлигидадир. Ҳосил қилинган кетма-кетликлар блокларининг тасодифийлик даражаси блокларни ташкил этувчи алоҳида элементлар ва элементлар бирикмалари сонлари билан боғлиқ нисбатлар орқали ифодаланувчи ва аниқланувчи мезонлар орқали баҳоланади. Тасодифийлик даражаси юқори бўлган псевдотасодифий кетма-кетликни ишлаб чиқарувчи генераторлар криптографик жиҳатдан самарали бўлган замонавий криптотизимларнинг ажралмас қисми ҳисобланади. Тасодифий кетма-кетликлар криптографияда қуйидаги мақсадларда қўлланилади:

- симметрик криптотизимлар учун тасодифийлик даражаси юқори бўлган сеанс калитлари ва бошқа калитларнинг генерациясида;
- носимметрик криптотизимларда қўлланиладиган катта қийматлар қабул қилувчи параметрларнинг тасодифий бошланғич қийматлари генерациясида;
- блокли шифрлаш алгоритмларининг бошланғич тасодифий қиймат талаб қилувчи CBC, OFB ва бошқа қўлланиш тартиб-қоидалари учун тасодифийлик даражаси юқори бўлган бошланғич векторлар ҳосил қилишда;
- электрон рақамли имзо тизимларида катта қийматга эга параметрлар учун дастлабки тасодифий қийматларни генерациясида;
- битта протокол орқали бир хил маълумотларни ҳар хил калитлар қўллаш билан шифрлаб турли кўринишда узатиш учун талаб қилинадиган ҳолатларда калит учун етарли узунликдаги тасодифий кетма-кетлик ҳосил қилишда, масалан, SSL ва SET протоколларида.

Ташкил этувчи элементлари ва элементлар бирикмалари деярли тенг эҳтимоллик билан тақсимланган тасодифий кетма-кетлик ҳосил қилиш масаласини ечиш кетма-кетликни ташкил этувчи элементлар ва элементлар бирикмаларининг текис тақсимланган генерацияси масаласини ечиш билан боғлиқ. Бирор кетма-кетликни ташкил этувчи элементлар ва элементлар бирикмалари, шу кетма-кетликда деярли тенг миқдорда қатнашган бўлса, бу кетма-кетлик текис тақсимотга эга дейилади. Агар A -кетма-кетликни ташкил этувчи $x_t \in A$ элемент ва элемент бирикмалари сони N та бўлса, у ҳолда ихтиёрий $t \in N$ учун, A -кетма-кетликни ташкил этувчи $x_t \in A$ элемент ва элементлар бирикмасининг шу кетма-кетликдаги частотаси бошқа элемент ва элементлар бирикмасининг частотаси билан деярли бир хил бўлади, яъни ҳар бир $x_t \in A$ элемент ва элементлар бирикмаси шу кетма-кетликда деярли бир хил эҳтимоллик билан қатнашади.

Тасодифий кетма-кетликлар ҳақиқий тасодифий ва псевдотасодифий кетма-кетликларга бўлинади.

Тасодифий кетма-кетлик физик генераторлар ва дастурий генераторлардан фойдаланиб ҳосил қилиниши мумкин.

Физик ҳодисаларнинг ўзгариш мажмуига асосланган генераторлар орқали ишлаб чиқилган кетма-кетлик **ҳақиқий тасодифий** бўлиб, бу кетма-кетлик бир мартагина ишлаб чиқилиб, уни кейинчалик бирор бир усул ёки восита билан худди шундай тарзда такрорланишини бошқариш мураккаб ҳисобланади. Шу сабабли маълумотларни шифрлаш жараёнида бевосита физик генераторлар билан ишлаб чиқилган кетма-кетликни калитлар гаммаси сифатида қўллаш мақсадга мувофиқ эмас. Чунки дешифрлаш жараёнида қўлланиладиган физик генераторнинг айнан шифрлаш жараёнида қўлланилган кетма-кетликни ишлаб чиқиши кафолатланмайди.

Бирор номаълум параметрга (калитга) боғлиқ бўлган математик модель асосида псевдотасодифий кетма-кетлик ишлаб чиқувчи дастурий генераторлар ҳосил қилган **псевдотасодифий** кетма-кетликни, номаълум параметр қийматини билган ҳолда, худди шу математик модель ва унинг дастурий таъминоти асосида кетма-кетликнинг қайта такрорланишини бошқариш мумкин. Бундай ҳолат маълумотларни шифрлаш жараёнида бевосита дастурий генераторлар билан ишлаб чиқилган псевдотасодифий кетма-кетликни калитлар гаммаси сифатида қўллаш мақсадга мувофиқлигини англатади ва дешифрлаш жараёнида қўлланиладиган дастурий генераторнинг айнан шифрлаш жараёнида қўлланилган псевдотасодифий кетма-кетликни ишлаб чиқиши кафолатланади.

Юқорида келтирилган амалий масалаларни ечишда ҳақиқий тасодифий кетма-кетликлар ишлаб чиқувчи тасодифий физик ҳодисаларга асосланган генераторлар олдиндан калитлар блоклари мажмуини яратишда, генераторларнинг бошланғич параметрлари қийматларини ўрнатишда ва бошқа шу каби масалаларни ечишда самарали натижалар беради.

Етарли катта давр узунлигига эга ва тасодифийлик даражаси юқори бўлган кетма-кетликлар ҳосил қилувчи дастурий ПТКК генераторининг амалда қўлланилиши самарали ва қулай бўлиб, криптографик воситаларда кенг қўлланилади.

Узлуксиз шифрлаш тизимларида шифрлаш ва дешифрлаш жараёнларининг тез амалга оширилиши учун ташкил этувчи элементлари ва элементлар бирикмалари текис тақсимланган, тасодифийлик даражаси юқори бўлган псевдотасодифий кетма-кетлик ишлаб чиқарувчи дастурий генераторлардан фойдаланилади.

Мавжуд дастурий генераторлар ва улар асосидаги оқимли шифрлаш тизимлари маълум бир ёндашувлар асосида яратилган.

Оқимли шифрлаш алгоритмларига қўйиладиган асосий талаблардан бири уларнинг криптографик бардошлилигини таъминловчи, криптографик татбиқларда “калит” деб аталувчи номаълум параметр қийматини билмаган ҳолда, тескари акслантириш қийматини бир қийматли аниқлаш бирор ечилиши мураккаб бўлган математик муаммоларни ҳал қилишни талаб этувчи бир томонламалик хусусиятга эга акслантиришлар негизида яратилишидир. Алгоритмлар криптобардошлилигининг етарли даражада таъминланганлигини кафолатлаш ва исботлаш асослари нуқтаи назаридан мавжуд узлуксиз шифрлаш алгоритмларини асосан учта йўналишга ажратиш мумкин [13]:

1. Тизимли-назарий ёндашув йўналишидаги ПТКК генераторлари асосида яратилган алгоритмлар;
2. Мураккабликка асосланган назарий ёндашув йўналишидаги ПТКК генераторлари асосида яратилган алгоритмлар;
3. Комбинациялаш йўналишидаги ПТКК генераторлари асосида яратилган алгоритмлар.

Тизимли ёндашув асосида оқимли шифрлаш алгоритмларини яратиш кўп жиҳатдан блокли шифрлаш алгоритмларини яратиш усуллари каби бўлиб, оқимли шифрлаш алгоритмининг криптобардошлилиги фундаментал математик меъзонлар ва қонуниятлар асосида шу пайтгача мураккаб ва самарали ечиш усули мавжуд эмас деб ҳисобланган муаммонинг қийинчилигига тенглаштирилади. Бундай ҳолатларда кўпроқ назарий ва амалий жиҳатдан криптографик самара берувчи математик акслантиришлар қўлланилган ҳолда криптографик тузилма (схема) таклиф қилинади ва бу тузилманинг (схеманинг) криптографик бардошлилиги тадқиқ қилинади. Математиканинг назарий ютуқларига асосланган ҳолда: *бир томонламалик хусусиятга эга акслантиришларга асосланган, акслантиришларининг аналитик ва мантиқий (чинлик жадвали асосидаги Буль функцияси) математик моделларини ифодаловчи функциялар чизиқсизлик даражаси юқори бўлишини, етарли катта давр узунлигини ҳамда битлар ва байт блокларининг текис тақсимотини таъминловчи* хусусиятларга эга бўлган кетма-кетликни ишлаб чиқувчи алгоритмлар яратилади.

Яратилган алгоритмлар акслантиришларининг турли хил криптотаҳлил усулларига бардошлилиги асосланади. Агар яратилган алгоритмлар шу пайтгача мавжуд бўлган криптотаҳлил усулларига бардошли бўлса ҳамда ҳосил қилинган кетма-кетлик тасодифийлик мезонлари тестлари талабларига жавоб берса, бу алгоритмни амалиётда қўллаш мумкинлиги тўғрисида хулоса қилинади.

Мавжуд оқимли шифрлаш алгоритмлари асосан тизимли-назарий ёндашув натижасида яратилган алгоритмлар синфига (туркумига) киради.

Тизимли-назарий ёндашув асосидаги оқимли шифрлаш алгоритмларига қўйиладиган асосий талаблар қуйидагилардан иборат [13]:

- алгоритм асосидаги ПТКК генератори етарли узун даврга эга бўлган кетма-кетлик ишлаб чиқишни таъминлаши керак;

- генератор акслантиришларининг аналитик ва мантиқий (чинлик жадвали асосидаги Буль функцияси) математик моделларини ифодаловчи функциялар чизиқсизлик даражаси юқори бўлиши керак;
- ишлаб чиқилган ПТКК блоклари текис статистик тақсимот кўрсаткичига эга бўлиши керак;
- псевдотасодифий кетма-кетликнинг гамма элементлари (бит, байт, қисм блоклари) барча бошқа элементларининг ҳиссаси орқали ҳосил қилиниши ─ аралашиш самарали бўлиши керак;
- ПТКК гамма элементларининг кескин ўзгариши ─ тарқалиши самарали бўлиши керак;
- алгоритм акслантиришлари Буль функцияларининг чизиқсизлик шарти бажарилиши ҳамда жадал самара (“лавинный эффект”) бериши таъминланиши керак.

Тизимли-назарий ёндашув асосида яратилган оқимли шифрлаш алгоритмларининг криптобардошлилиги, бу алгоритмларда қўлланилган акслантиришларнинг назарий ва амалий бир томонламалик хусусиятларининг қай даражада ишончлилигини баҳолаш билан исботланади.

Ҳисоблаш муракккаблигига асосланган назарий ёндашув негизида қурилган оқимли шифрлаш алгоритмлари ПТКК ишлаб чиқарувчи генераторларининг криптобардошлилиги: *етарли даражада катта сонни туб кўпайтувчиларга ажратиш, характеристикаси етарли катта бўлган чекли майдонларда дискрет логарифмлаш, чекли майдонларда етарли даражада юқори тартибли чизиқли тенгламалар тизимларини ечиш, ЭЭЧнуқталари устида амаллар бажариш билан боғлиқ бўлган масалаларни ечиш мураккабликлари билан аниқланувчи бир томонлама функциялар билан ифодаланади.*

Санаб ўтилган ҳисоблаш мураккабликлари негизида аниқланган бир томонлама функциялар асосида яратилган ПТКК генераторлар синфига катта сонларни туб кўпайтувчиларга ажратиш масаласи мураккаблигига асосланган RSA генератори, катта сонларни туб кўпайтувчиларга ажратиш масаласи мураккаблигига асосланган Квадратик чегирма усули орқали аниқланган BBS генератори ва дискрет логарифмлаш масаласининг мураккаблигига асосланган Блюм-Микали генератори киради.

Назорат саволлари

1. Шифрлаш алгоритмлари қандай синфларга бўлинади?
2. Оддий ўрнига қўйишга асосланган шифрлаш алгоритмларининг жадвалли ва аналитик математик моделларини тушунтириб беринг?
3. Бир қийматли ўрнига қўйишга асосланган шифрлаш алгоритмларининг математик моделларини мисоллар ёрдамида тушунтиринг?
4. Кўп қийматли ўрнига қўйишга асосланган шифрлаш алгоритмларининг математик моделларини мисоллар ёрдамида тушунтиринг?
5. Бир алифболи ва кўп алифболи ўрнига қўйишга асосланган шифрлаш алгоритмлари акслантиришларининг математик асослари хусусиятлари нималардан иборат?
6. Гаммалаштириш шифрлаш алгоритмларининг математик асосларини тушунтиринг?
7. Ўрин алмаштиришга асосланган шифрлаш алгоритмларининг асосий хусусиятлари ва математик модели ҳақида нималарни биласиз?
8. Дастлабки миллий стандартларга асос бўлган симметрик блокли шифрларнинг математик ва криптографик хусусиятларини тушунтиринг?
9. Замонавий симметрик блокли шифрлаш алгоритмларининг математик асосларини тушунтиринг?
10. Фейстел тармоғига асосланмаган симметрик блокли шифрлаш алгоритмларига мисоллар келтиринг?
11. AES криптоалгоритмининг математик асосини тушунтиринг?

12. AES алгоритмида кўпҳадларни кўпайтириш қандай амалга оширилади?

13. AES алгоритмида қандай алмаштиришлардан фойдаланилади?

14. O‘z DSt 1105:2009 криптоалгоритмининг математик асосини тушунтиринг?

15. O‘z DSt 1105:2009 криптоалгоритми қандай параметр ва функциялардан фойдаланади?

16. Оқимли шифрлаш алгоритмларига таъриф беринг?

17. Оқимли шифрлаш алгоритмлари қандай генераторлар негизида яратилади?

18. Тасодифий кетма-кетлик қандай ҳосил қилиниши мумкин?

19. Оқимли шифрлаш алгоритмларига қўйиладиган қандай асосий талабларни биласиз?

20. Назарий ёндашув негизида қурилган оқимли шифрлаш алгоритмлари ПТКК ишлаб чиқарувчи генераторларининг криптобардошлилиги нималарга боғлиқ?

5. ОШКОРА КАЛИТЛИ КРИПТОТИЗИМЛАР

5.1. Ошкора калитли криптотизимларнинг умумий хусусиятлари

Симметрик калитли крпитоалгоритмлар асосида яратилган криптотизим ахборот-коммуникация тармоқларида маълумотлар алмашинувининг муҳофазасини таъминлаш масалаларини ечишда қанчалик ишончли бўлмасин, бари бир ундан амалда фойдаланиш жараёнида айрим қўшимча хавфсизликни таъминлаш масалалари келиб чиқиб, уларнинг ечилиши талаб этилади. Шундай масалалардан бири калитларни тизим фойдаланувчиларига тарқатиш масаласидир. Ишлаб чиқилган бардошли калитларни тизим фойдаланувчиларига етказиш хавфсизлиги кафолатли таъминланган бўлиши талаб этилади. Бунинг учун эса қўшимча ҳолда яна бирор бошқа криптотизимдан фойдаланишга тўғри келади. Бу масала ечимининг қўшимча криптотизимдан фойдаланмай ҳал этилиши классик ва замонавий алгебрада олинган илмий натижалар асосида яратилган *очиқ калитли (ошкора калитли, носимметрик) криптотизим*ларнинг вужудга келиши билан амалга оширилди [2, 14].

Очиқ калитли криптотизим моҳияти ҳар бир фойдаланувчи учун бирини билган ҳолда иккинчисини топиш, ечилиши мураккаб бўлган масала билан боғлиқ калитлар жуфтлигини яратишдан иборат. Бу жуфтликни ташкил этувчи калитлардан бири очиқ (ошкора), иккинчиси махфий (шахсий) деб эълон қилинади. Очиқ калит ошкора эълон қилинади, махфий калит фақат унинг эгасигагина маълум бўлади. Бирор фойдаланувчининг очиқ калитини билган ҳолда унинг махфий калитини топишнинг амалий жиҳатдан мумкин эмаслиги, ечилиши мураккаб бўлган масаланинг ҳал этилишини талаб қилиши билан кафолатланади. Очиқ маълумот, шу маълумотни олиши керак бўлган фойдаланувчининг очиқ калити билан шифрланиб унга узатилади. Шифрланган маълумотни олган фойдаланувчи фақат унинг ўзига маълум бўлган махфий калит билан уни дешифрлаб, очиқ маъумотга эга бўлади.

Криптотизимнинг ҳар бир i - фойдаланувчиларининг очиқ k_i^o ва махфий $k_i^м$ калитлари махфий тутилиши лозим ва шарт бўлган $p_i^м$ - параметрга ёки барча фойдаланувчилар учун умумий бўлган $p^м$ - параметрга боғлиқ ҳолда бирор Q -қоида бўйича ишлаб чиқилади (генерация қилинади). Бунда очиқ калит k_i^o ва генерация қоидаси Q маълум бўлсада, махфий $p_i^м$ ёки $p^м$ параметрни билмаслик $k_i^м$ - махфий калитни аниқлаш имкониятини бермайди.

Шифрлаш қоидаси E ва дешифрлаш қоидаси D деб белгиланса, *j*–фойдаланувчи M -очиқ маълумотни шифрлаб, C -шифрланган маълумотни *i*–фойдаланувчига жўнатиши учун *i*–фойдаланувчининг барчага маълум бўлган k_i^o -очиқ калитидан фойдаланади, яъни $E_{k_i^o}(M) = C$ - шифрмаълумотни *i*–фойдаланувчига очиқ алоқа тармоғи орқали юборади. Бу $E_{k_i^o}(M) = C$ - шифрмаълумотни қабул қилиб олган i –фойдаланувчи, фақат унинг ўзига маълум бўлган ўзининг $k_i^м$ - махфий калити билан дешифрлайди, яъни $D_{k_i^м}(C) = M$ - очиқ маълумотга эга бўлади. Шифрлаш қоидасини аниқловчи акслантириш $E_{k_i^o}(M) = C$ бир томонламалик хусусиятига эга бўлиши керак, яъни E - акслантириш, k_i^o - очиқ калит ва C - шифрмаълумотни билган ҳолда M - очиқ маълумотни аниқлаш имконияти йўқ.

5.2. Бир томонлама функциялар

Очиқ калитли криптотизимлар *бир томонлама* акслантиришларга (функцияларга) асосланади.

Носимметрик криптотизимларнинг математик асосини катта тартибли чекли тўпламларда берилган чекли майдон, ҳалқа, группа, қисмгруппа кўринишидаги алгебраик структуралар ва шахсий махфийликга эга бўлган уч турдаги бир томонлама функциялар ташкил этади. Носимметрик криптотизимларнинг турли ҳужумларга бардошлилиги эса бир томонлама функцияларнинг тескариланиши ўта мураккаб муаммо (масала) бўлишига асосланади.

Бир томонлама функциялар биринчи турининг ҳужумларга бардошлилиги дискрет логарифмлаш масаласининг мураккаблигига асосланган. Бу функция У. Диффи ва М. Хеллман таклиф этган туб майдон $F(p)$ ҳосил қилувчи (генератор, бошланғич илдиз) элемент a ни махфий x даражага ошириш функциясидир.

Бир томонлама функцияларнинг иккинчи тури К. Кокс, Р. Райвест, А. Шамир, Л. Адлеман томонидан таклиф этилган бўлиб, унинг ҳужумларга бардошлилиги чекли ҳалқада факторлаш муаммосининг мураккаблигига асосланган.

Бир томонлама функцияларнинг учинчи турининг ҳужумларга бардошлилиги ЭЭЧ нуқталари группасида дискрет логарифмлаш масаласининг мураккаблигига асосланган. Бу функция Н. Коблиц ва В. Миллер таклиф этган ҳосил қилувчи (генератор, бошланғич илдиз) элемент G ни махфий d бутун сонга кўпайтириш функциясидир.

Бир томонлама функция – шундай $y = f(x)$ функцияки, унинг аниқланиш соҳасидан бўлган ихтиёрий x учун $f(x) = y$ қиймат осон ҳисобланади, қийматлар соҳасининг барча y қийматларига мос келувчи x қийматларни ҳисоблаш эса амалий жиҳатдан мураккаб бўлган масала (муаммо)ни ечишни талаб этади.

Кўриниб турибдики, бир томонлама функциянинг бундай таърифи «осон ҳисобланадиган», «барча қийматлар учун», «амалий жиҳатдан», «мураккаб бўлган масалани ечишни талаб этади» иборалар асосида берилиб, математика нуқтаи назаридан аниқ эмас. Шундай бўлсада, бу таъриф амалий криптотизим масалалари нуқтаи назаридан етарли даражада аниқ бўлиб, алоҳида олинган криптотизимлар учун такомиллаштирилиб, мутлақо аниқ ифодаланиши мумкин. Шундай функциялардан криптографияда қандай фойдаланилиши ҳақида қисқача тўхталамиз. Яширин ёки махфий услубли бир томонлама функция, таъриф бўйича бирор $z \in Z$ параметрларга боғлиқ бўлиб, тескарисига эга бўлган шундай f_Z функциялар синфики, берилган z параметрда аниқланиш соҳасидаги барча $x \in X$ аргументлар учун $f_Z(x) = y$ қийматларни осон ҳисоблаш алгоритми E_Z мавжуд бўлиб, қийматлар соҳасидаги барча $y \in Y$ қийматлар учун $f_Z^{-1}(y) = x$ қийматларни маълум бўлган E_Z алгоритм билан ҳисоблашнинг имконияти йўқ (ёки бошқача айтганда $f_Z^{-1}(y) = x$ қийматларни ҳисоблаш сарф-харажатлари ва вақти мақсадга мувофиқ эмас). Бундай таъриф математика нуқтаи назаридан аниқ бўлмасада, амалий криптология масалаларида самарали қўлланилиши мумкинлигига шак-шубҳа йўқ.

Очиқ калитли криптотизимлар алгоритмлари уларнинг асосини ташкил этувчи бир томонлама функциялар билан фарқланади. Ҳар қандай бир томонлама функция ҳам очиқ калитли криптотизимлар яратиш учун ва улардан амалдаги ахборотлар тизимида махфий алоқа хизматини ўрнатиш алгоритмини қуриш учун қулайлик туғдирмайди.

Бир томонлама функцияларнинг аниқланиш таърифида назарий жиҳатдан тескариси мавжуд бўлмаган функциялар эмас, балки берилган функцияга тескари бўлган функциянинг қийматларини ҳисоблаш амалий жиҳатдан мақсадга мувофиқ бўлмаган функциялар тушунилиши таъкидланган эди. Шунинг учун, маълумотнинг ишончли муҳофазасини таъминловчи очиқ калитли криптотизимларга қуйидаги муҳим талаблар қўйилади:

1. Дастлабки (очиқ) маълумотни шифрматн кўринишига ўтказиш бир томонлама жараён ва шифрлаш калити билан шифрматн очиш – дешифрлаш мумкин эмас, яъни шифрлаш калитини билиш шифрматн дешифрлаш учун етарли эмас.

2. Очиқ калитнинг маълумлигига асосланиб, махфий калитни замонавий фан ва техника ютуқлари ёрдамида аниқлаш учун зарур бўладиган сарф-харажатлар ҳамда вақт мақсадга мувофиқ эмас. Бунда шифрни очиш

учун бажрилиши керак бўладиган энг кам миқдордаги амаллар сонини аниқлаш муҳимдир.

Замонавий очиқ калитли криптотизимлар қуйидаги турдаги масалаларни ечишнинг кўп вақт талаб қилиши ва ҳисоб-китоблар учун ҳисоблаш қурилмаларида катта ҳажмдаги хотира талаб этилиши билан боғлиқ бўлган мураккабликларга таянади:

1. Етарли катта сонларни туб кўпайтувчиларга ёйиш (факторлаш).

2. Характеристикаси етарли катта бўлган чекли майдонларда дискрет логарифмларни ҳисоблаш.

3. Етарли катта тартибдаги алгебраик тенгламалар тизимининг илдизларини чекли майдонларда ҳисоблаш.

4. Эллиптик эгри чизиқларда рационал координатали нуқталарни топиш, уларни қўшиш ҳамда тартибини аниқлаш.

5. Характеристикаси етарли катта бўлган чекли параметрли группаларда параметрни топиш.

Қуйида нисбатан оммавийлашган очиқ калитли криптотизимлар қисқача кўриб ўтилади.

5.3. Факторлаш мураккаблигига асосланган носимметрик шифрлар

RSA очиқ калитли шифрлаш алгоритми берилган етарли катта тоқ сонни туб кўпайтувчиларга ажратишнинг рационал усули мавжуд эмаслигига асосланган.

Махфий тутиладиган ҳамда етарли катта бўлган p ва q -туб сонлари олиниб, $n = pq$ -сони ва Эйлер функциясининг қиймати $\varphi(n) = (p-1)(q-1)$ ҳисобланади. Бу $\varphi(n)$ -сон очиқ ва махфий калитларни генерация қилиш қоидасининг махфий тутиладиган параметри ҳисобланади. Сўнгра, $(e_i, \varphi(n)) = 1$ шартни қаноатлантирувчи, яъни $\varphi(n)$ сони билан ўзаро туб бўлган e_i -сон бўйича d_i -сони ушбу $e_i d_i = 1 \bmod \varphi(n)$ формула орқали Евклид алгоритми бўйича ҳисобланади. Бу ($e_i ; d_i$) жуфтликда e_i -очиқ калит ва d_i-махфий калит деб эълон қилинади. Шундай қилиб RSA криптотизими фойдаланувчисининг очиқ калити *(n, e)* бўлса, шахсий калити *(d_i, $\varphi(n)$)* жуфтлигидир.

RSA криптотизимида i - фойдаланувчидан j - фойдаланувчига шифрланган маълумотни жўнатиш қуйидагича амалга оширилади:

1. **Шифрлаш қоидаси**: ушбу ифода $M^{e_j} \bmod n = C$ ҳисобланади, бу ерда M -очиқ маълумот, C –шифрланган маълумот;

2. **Дешифрлаш қоидаси**: ушбу ифода $C^{d_j} \bmod n = M^{e_j d_j} \bmod n = M$ ҳисобланиб, очиқ маълумот M ҳосил қилинади.

Дешифрлаш қоидасидаги $C^{d_j} \bmod n = M^{e_j d_j} \bmod n = M$ муносабатнинг ўринлилиги қуйидаги теоремалардан келиб чиқади.

5.1-теорема. Агар $n = pq$, $p \neq q$- туб сонлар ва $(x, p) = 1, (x, q) = 1$ бўлса, у ҳолда

$$x^{\varphi(n)} = 1 \bmod n\,.$$

Исботи. Агар $(x, p) = 1, (x, q) = 1$ муносабатлар ўринли бўлса, у ҳолда

$$x^{p-1} = 1 \bmod p$$

$$x^{q-1} = 1 \bmod q\,,$$

бўлиб, $y = x^{\varphi(n)} = x^{(p-1)(q-1)}$ модуль p бўйча ҳам, модуль q бўйича ҳам 1 га тенг бўлади. Ҳақиқатан ҳам:

$$y = x^{\varphi(n)} \bmod p = x^{(p-1)(q-1)} \bmod p = [x^{(p-1)} \bmod n]^{(q-1)} \bmod n = 1^{(q-1)} \bmod n = 1$$

ёки

$$y = x^{\varphi(n)} \bmod p = x^{(p-1)(q-1)} \bmod p = [x^{(q-1)} \bmod n]^{(p-1)} \bmod n = 1^{(p-1)} \bmod n = 1\,.$$

Бундан эса, (y – 1) нинг p ва q сонларига қолдиқсиз бўлиниши келиб чиқади ҳамда y=1 mod pq тенглик ўринли бўлади.

5.2-теорема. Агар $n = pq$, $p \neq q$ – туб сонлар ва $(e, \varphi(n)) = 1$ бўлса, у ҳолда ушбу

$$E_{e,n}: x \to x^e \bmod n$$

акслантириш $\mathbf{Z}_n = \{0;1;2;...;n-1\}$ -чекли майдонда ўзаро бир қийматли акслантириш бўлади.

Исботи. Агар $(e,\varphi(n))=1$ бўлса, у ҳолда шундай d - ҳақиқий сон мавжуд бўладики, унинг учун

$$ed = 1 \bmod \varphi(n),$$

муносабат ўринли бўлади. Бундан эса ушбу муносабат

$$(x^e)^d = x^{ed} = x^{1+K\varphi(n)} = x(\bmod n)$$

EKUB $(x,n)=1$ ифодани қаноатлантирувчи барча x лар учун бажарилади.

Агар $x = py$ бўлса, бу ерда $(y,q)=1$, у ҳолда

$$p \mid x^{1+K\varphi(n)} - x.$$

Бу ерда x сони q га қолдиқсиз бўлинмаганлигидан

$$x^{1+K\varphi(n)} - x = x\left[(x^{q-1})^{K(p-1)} - 1\right]$$

келиб чиқади.

Ферманинг кичик теоремасига кўра $x^{q-1} = 1 \bmod q$ ва натижада, квадрат қавс ичидаги ифода модуль p бўйича ҳам ва модуль q бўйича ҳам 0 га тенг бўлиб, бундан ушбу

$$x^{1+K\varphi(n)} - x = 0 \bmod n$$

тенгликнинг ўринлилиги келиб чиқади.

Худди шу каби, агар $x = qy$ бўлса, бу ерда $(y,p)=1$, у ҳолда

$$q \mid x^{1+K\varphi(n)} - x.$$

Бу ерда x сони q га қолдиқсиз бўлинмаганлигидан

$$x^{1+K\varphi(n)} - x = x\left[(x^{p-1})^{K(q-1)} - 1\right]$$

келиб чиқади.

Ферманинг кичик теоремасига кўра $x^{p-1} = 1 \bmod p$ ва натижада, квадрат қавс ичидаги ифода модуль p бўйича ҳам ва модуль q бўйича ҳам 0 га тенг бўлиб, бундан ушбу

$$x^{1+K\varphi(n)} - x = 0 \bmod n$$

тенгликнинг ўринлилиги келиб чиқади.

Шундай қилиб, келтирилган теоремаларга кўра

$$C^{d_j} \bmod n = M^{e_j d_j} \bmod n = M^{K\varphi(n)+1} \bmod n = [(M^{\varphi(n)})^K \bmod n \cdot M \bmod n] \bmod n =$$
$$= [1^K \bmod n \cdot M \bmod n] \bmod n = M \bmod n = M$$

чунки, $M < n$.

Очиқ ва махфий калитларнинг генерацияси чоғида $e_i d_i = 1 \bmod \varphi(n)$ тенгликни қаноатлантирувчи d_i - сонини $\varphi(n)$ - сони маълум бўлганда Евклид алгоритми бўйича топилади. Аммо $\varphi(n)$ - сони фойдаланувчиларга номаълум бўлганда d_i - сонидан ташқари $\varphi(n)$-сони ҳам махфий бўлиб, $\varphi(n)$ - сонини аниқлаш учун n–сонини туб кўпайтувчиларга ажратиб, p ва q сонларини топиш талаб этилиб, сўнгра $\varphi(n) = (p-1)(q-1)$ ҳисобланади. n–сони етарли катта бўлганда уни туб кўпайтувчиларга ажратиб, p ва q сонларини топишнинг рационал усули бугунги кунда мавжуд эмас. Адабиётлар рўйхатида келтирилган [60] да етарли катта натурал сонларни экспоненциал ва субэкспоненциал мураккабликларга ажратиб, уларни туб кўпайтувчиларга ажратишнинг баъзи усуллари келтирилган.

Кейинги параграфда дискрет логарифмлаш масаласи ечимини характеристикаси етарли катта бўлган чекли майдонда амалга оширишнинг мураккаблигига асосланган Эль Гамал алгоритми келтирилган.

5.4. Чекли майдонларда дискрет логарифмлаш масаласининг ечими мураккаблигига асосланган носимметрик шифрлар

Эль Гамал алгоритмида криптотизимнинг ҳар бир i-фойдаланувчисига туб модуль p ва ҳосил қилувчи (генератор) g маълум ҳисобланади ва i-фойдаланувчи учун шахсий калитни ифодаловчи x_i -сон бўйича ҳисобланадиган $y_i = a^{x_i} \bmod p$ - очиқ калит генерация қилинади ва у барчага ошкор этилади. Агарда мана шу i-фойдаланувчи билан бирор бошқа

j-фойдаланувчи очиқ маълумот Mни шифрматнга ўгирилган ҳолда ахборот алмашувини амалга оширмоқчи бўлса, у ҳолда j-фойдаланувчи p сонидан кичик бўлган бирор k-сонини танлаб олиб

$$y_1 = g^k(\mathrm{mod} p) \text{ ва } y_2 = (M / y^k)(\mathrm{mod}\, p),$$

сонларини ҳисоблайди. Сўнгра j-фойдаланувчи (y_1;y_2) маълумотларини i-фойдаланувчига жўнатади. Ўз навбатида i-фойдаланувчи бу шифрланган маълумотни қабул қилиб, қуйидагича

$$(y_1^x \cdot y_2) \bmod p = M$$

ҳисоблаш билан очиқ маълумотни тиклайди.

Эль Гамал криптоалгоритмига асосланган криптотизимнинг ҳар бир i-фойдаланувчиси учун (y_i, x_i) - калитлар жуфтлиги қуйидагича яратилиши ҳам мумкин: бирор p_i-туб сони ва $g_i < p_i$- тенгсизликни қаноатлантирувчи g_i (фойдаланувчилар гуруҳи учун умумий p ва $g < p$ тенгсизликни қаноатлантирувчи g) сонлари танланади. Ушбу $x_i < p_i$ тенгсизликни қаноатлантирувчи махфий бўлган x_i - сони бўйича очиқ деб эълон қилинадиган y_i-сони ушбу формула $y_i = g_i^{x_i} (\mathrm{mod} \quad p_i)$ (фойдаланувчилар гуруҳи учун $x_i < p$ ҳамда $y_i = g^{x_i} \bmod p$) орқали ҳисобланади. Шундай қилиб, Эль Гамал критотизимида (p_i, g_i, y_i) – учлик (фойдаланувчилар гуруҳи учун pва g умумий бўлиб, $(p, g, y_i))$ – учлик) очиқ калит, x_i - эса махфий (шахсий) калит деб олинади.

Шундан сўнг i-фойдаланувчидан j - фойдаланувчига шифрланган маълумотни жўнатиш қуйидагича амалга оширилади:

1. **Шифрлаш қоидаси**: ушбу ифода $a_j = g_j^k \bmod p_j$, $b_j = y_j^k M \bmod p_j$ (фойдаланувчилар гуруҳи учун p ва g умумий бўлганда: $a = g^k \bmod p$, $b = y_j{}^k M \bmod p$) ҳисобланади, бу ерда M - очиқ маълумот, k - маълумотни шифрлаб жўнатувчи томонидан танланган тасодифий сон бўлиб, у ($p_j - 1$) –

сони билан ўзаро туб, $(a_j, b_j) = C$ (p ва g умумий бўлганда $(a,b) = C$ – шифрланган маълумот);

2. **Дешифрлаш қоидаси**: ${b_j}/{a_j^{x_j}} \bmod p_j = M$ (p ва g умумий бўлганда: ${b}/{a^{x_j}} \bmod p = M$), ҳақиқатан ҳам, ${b_j}/{a_j^{x_j}} \bmod p_j \equiv {g_j^{x_i k} M}/{g_j^{kx_i}} \bmod p_j \equiv M$ (p ва g умумий бўлганда: ${b}/{a^{x_j}} \bmod p \equiv {y_j^k M}/{a^{x_j}} \bmod p \equiv {g^{x_j k} M}/{g^{kx_j}} \bmod p \; = M \bmod p = M$, чунки $M < p$).

Криптотизимнинг ҳар бир i-фойдаланувчиси учун очиқ ва махфий калитларни x_i - сони маълум бўлганда $y_i = g_i^{x_i} \bmod p_i$ (фойдаланувчилар гуруҳи учун $x_i < p$ ҳамда $y_i = g^{x_i} \bmod p$) тенглик бўйича генерация қилинади. Аммо x_i - сони фойдаланувчиларга номаълум бўлганда, очиқ калитни ифодаловчи $y_i = g_i^{x_i} \bmod p_i$ тенгликдан $x_i = \log_{g_i} y_i (\bmod p_i)$ - сонини топиш, чекли майдон характеристикаси p_i етарли катта бўлганда, мураккаблашади ва бугунги кунда чекли майдонларда логарифмлаш масаласи ечимининг рационал (самарали) усуллари мавжуд эмас. [60] да характеристикаси катта бўлган чекли майдонларда дискрет логарифмлашнинг баъзи усуллари келтирилган.

5.5. Эллиптик эгри чизиқ группасида дискрет логарифмлашга асосланган криптотизимлар

5.5.1. Эллиптик криптографиянинг юзага келиши

ЭЭЧ назариясини яратишда сўнгги қадимий грек математиги Диофантдан бошлаб ўтмишнинг кўпгина энг йирик олимлари қатнашган. ЭЭЧ группаси структурасини машҳур француз математиги Анри Пуанкаре таклиф этган. Йиллар давомида ЭЭЧ ҳеч қандай амалий аҳамиятга эга бўлмаган соф математика соҳаси бўлиб келган. Ўтган асрнинг 80-йилларида

ЭЭЧ катта сонларни факторлаш алгоритмларини тузиш соҳасида қўлланила бошлади [56-60] ва бу қўлланишлар орқали криптография соҳасига кириб келди (носимметрик тизимлар, псевдотасодифий сонларни генерациялаш). Эллиптик криптографияда ҳақиқий бурилиш 1985 йилда Н. Коблиц ва В. Миллер илмий ишлари [42-44] чоп этилгандан сўнг юз берди. Шу дамдан бошлаб машҳур жаҳон критологлари эллиптик криптография билан шуғуллана бошладилар.

Факторлаш ва ЭЭЧ группасида дискрет логарифмлаш мураккабликларини таққослама таҳлили ЭЭЧларнинг баҳслашувдан ҳоли афзалликларини намоён этди [61-65]. 5.1-жадвалда таққослама маълумотлар келтирилган (маълумотлар туб майдонда дискрет логарифмлаш муаммоси учун ҳам осон ҳисобланади).

5.1-жадвал

Криптотаҳлил мураккабликлари бўйича маълумотлар

Алмаштириш модули узунлиги	ЭЭЧ группасида криптотаҳлил мураккаблиги	RSA модулини факторлаш мураккаблиги
192 бит	$2^{95,82} \approx 10^{29,21}$	$2^{40,41} \approx 10^{12,32}$
256 бит	$2^{127,82} \approx 10^{39}$	$2^{40,56} \approx 10^{14,5}$
512 бит	$2^{255,82} \approx 10^{78}$	$2^{65,15} \approx 10^{19,86}$
1024 бит	$2^{511,82} \approx 10^{156}$	$2^{88,47} \approx 10^{27}$

XXI асрнинг бошидан бошлаб носимметрик криптографиянинг анъанага айланиб қолган криптотизимлардан бардошлилиги ЭЭЧ группасида дискрет логарифмлаш муаммосининг мураккаблигига асосланган тизимларга ўтиш бошлангани кўзга ташланди [61-65].

Эллиптик криптографияга алоҳида қизиқиш қуйидаги сабаблар билан боғлиқ:

- биринчидан, дискрет логарифмлаш ва факторлаш муаммоларини ечишга қаратилган сонли майдон ва ҳалқаларда *n* модули бўйича сонлар силлиқлиги хоссасидан фойдаланадиган умумлашган ғалвир усулига асосланган тезкор алгоритмларнинг юзага келиши. ЭЭЧ группасида эса силлиқлик тушунчаси нуқталарга тегишли бўлиб, тезкор криптотаҳлиллаш алгоритмларини тузиш имкониятини бермайди;

- иккинчидан, ЭЭЧ группасида нисбатан қисқа калит узунлиги асосида криптотизимлар ишлаб чиқариш имконияти мавжудлиги. Булар симсиз коммуникацияларда ва ресурс чекланган ҳолларда (смарт-карталар, мобил қурилмалар) асосий ҳисобланади. Масалан, ЭЭЧ группасида тузилган калитнинг бинар узунлиги *150* дан *350* гача бўлган қурилмаларда анъанавий қурилмалардаги калитнинг бинар узунлиги *600* дан *1400* гача бўлгандагидек криптографик бардошлилик даражасига эришилади [56-58, 61-65].

Юқорида келтирилган сабаблар АҚШ ва Россия Федерациясида амалдаги стандартларни эллиптик криптографияга оид стандартлар билан алмаштиришга олиб келди. Ҳозирги кунда ЭЭЧларга асосланган алгоритмлар кўплаб халқаро, миллий ва соҳага оид стандартлар қаторидан ўрин олган [66-68]. Эллиптик криптографияда фойдаланиш учун асосан $GF(2^m)$ майдонида аниқланган сингуляр ёки $GF(p)$ майдонида аниқланган носуперсингуляр ЭЭЧлардан фойдаланиш тавсия этилади. Барча ҳолларда ЭЭЧ группасида катта тартибга эга бўлган элементлар мавжудлигига ишонч ҳосил қилиш муҳимдир.

Криптографияда чекли алгебраик структураларда, масалан, чекли майдонларда берилган ЭЭЧдан кенг фойдаланилади. Туб майдон $GF(p)$ да берилган ЭЭЧ

$$y^2 = x^3 + ax + b \pmod p \qquad (14)$$

таққосламанинг $P = (x, y)$ нуқталари (ечимлари) тўпламини ташкил этади. Бу ерда a ва b катталиклари $4a^3 + 27b \neq 0 \pmod p$ шартини қаноатлантирувчи доимийлар, $p>3$. Тўплам группани ташкил этиши учун унга чексиз узоқлашган $0_E=(x, \infty)$ нуқта бирлаштирилади, натижада группа ташувчиси $E=\{14\ \text{ечимлари}\}\ U\{0\}$ кўринишни олади. Мазкур группанинг криптография учун асосий амали нуқталарни такроран m марта қўшиш амали $[m]P$ бўлиб, уни *[m]* га кўпайтириш деб аталади ва у рекурсив суратда амалга оширилади. Ошкора криптографияда яратилган кўпчилик алгоритмларнинг ЭЭЧли аналоглари ишлаб чиқилган. Эллиптик эгри чизиқли криптотизимлар криптобардошлилиги ЭЭЧда дискрет логарифмлаш муаммосининг мураккаблиги билан белгиланади. Бу муаммони дискрет логарифм муаммосига келтириш [38]да баён этилган.

5.5.2. Эллиптик эгри чизиқ нуқталари группаси асосида яратилган носимметрик шифрларнинг умумий функционал модели

ЭЭЧ нуқталари устида амаллар бажариш масалалари ечимлари мураккабликларига асосланган носимметрик алгоритмларни яратишда криптотизимнинг ҳар бир i - фойдаланувчисининг шахсий калитини ифодаловчи $k_i^м$ -сон бўйича ҳисобланадиган $[k_i^м]G = Q_i = (x_i^o, y_i^o)$ - очиқ калит генерация қилинади, бу ерда G -танлаб олинган эллиптик эгри чизиққа тегишли барчага маълум бўлган ҳосил қилувчи (генератор) нуқта. Бу ерда $G = (x_G, y_G)$ ва $Q_i = (x_i^o, y_i^o)$ - нуқталарни билган ҳолда $k_i^м$ -шахсий калитни аниқлаш ўзининг рационал ечимига эга эмас.

Криптотизимнинг j-фойдаланувчиси M - очиқ маълумотни шифрлаб, C - шифрланган маълумотни i-фойдаланувчига жўнатиши учун, i-фойдаланувчининг барчага маълум бўлган очиқ калити $Q_i = (x_i^o, y_i^o)$ дан фойдаланади, яъни $E_{(x_i^o, y_i^o)}(M) = C$ шифрматнни i-фойдаланувчига очиқ алоқа тармоғи орқали юборади. Бу $E_{x_i^o}(M) = C$ (ёки $E_{x_i^o}(M) = C$ ёки $E_{(x_i^o, y_i^o)}(M) = C$) - шифрмаълумотни қабул қилиб олган i –фойдаланувчи, фақат унинг ўзига маълум бўлган ўзининг шахсий калити $k_i^м$ - билан дешифрлайди, яъни $D_{k_i^м}(C) = M$ -очиқ маълумотга эга бўлади. Шифрлаш қоидасини аниқловчи акслантириш $E_{(x_i^o, y_i^o)}(M) = C$ бир томонламалик хусусиятига эга бўлиши керак, яъни E - акслантириш, $Q_i = (x_i^o, y_i^o)$ очиқ калит ва C - шифрматнни билган ҳолда M - очиқ маълумотни аниқлаш имконияти йўқ бўлиши керак.

5.6. Параметрли группадан фойдаланишга асосланган носимметрик шифрлар

Очиқ калитли криптоалгоритмлар асосини ташкил этувчи етарли катта сонларни туб кўпайтувчиларга ёйиш, характеристикаси етарли катта бўлган чекли майдонларда дискрет логарифмларни ҳисоблаш, ЭЭЧларда рационал координатали нуқталарни топиш, уларни қўшиш ҳамда тартибини аниқлаш масалаларини ечиш мураккабликлари билан боғлиқ ҳолда параметрли группа амалларидан фойдаланиш янги носимметрик алгоритмлар яратиш усулларига олиб келади.

Параметрли группанинг ушбу

$$a \circledR b = a + b + aRb(\bmod p)$$

кўринишдаги амал асосида шаклланган параметрли группа 3-бўлимда баён этилган.

Чекли майдоннинг a ва b - элементлари учун киритилган амални турлича аниқлаш мумкин. Киритилган амални шифрлаш алгоритмларида очиқ калит ва очиқ маълумот ёки оралиқ натижа блоки устида бажарилишини ҳисобга олиб ҳамда дешифрлаш алгоритмларида шифрмаълумот ва махфий калит блоки қийматлари устида бажариладиган акслантиришларга татбиқ қилинишини назарда тутиб, киритилган амал бўйича тескари элемент мавжуд бўладиган қилиб аниқланади. Хэшлаш функцияси, оқимли шифрлаш, калитлар генерацияси алгоритмларида ва Фейстел тармоғи акслантиришларида киритилган амал бўйича тескари элементни топишнинг рационал усули йўқ бўладиган ёки умуман мавжуд бўлмайдиган қилиб аниқлаш мақсадга мувофиқдир.

5.6.1. Параметрли шифрлаш усули

Киритилган амалдан фойдаланиб, характеристикаси етарли катта бўлган чекли майдонларда дискрет логарифмлаш масаласининг мураккаблигига асосланган носимметрик шифрлаш алгоритмини яратиш масаласини ечиш схемаси [13] да келтирилган. Параметрли шифрлашда, аввало туб модуль p ва ҳосил қилувчи $g \in F_p$ танланиб, ушбу сон $R_i = g^{x_i} \bmod p$ ҳисобланади, бу ерда x_i - шахсий калит. Сўнгра $(a_i; R_i)$ - жуфтликни очиқ калит деб қабул қиламиз.

Криптотизимнинг j - фойдаланувчиси i- фойдаланувчига M - очиқ маълумотни шифрлаб жўнатишни қуйидагича амалга оширади:

1. Фақат j - фойдаланувчининг ўзигагина маълум бўлган бирор k -сонини тасодифий ҳолда танлаб, $R = (R_i)^k \bmod p = g^{kx_i} \bmod p$ - қийматни ҳисоблайди.
2. Шифрлашни $a_i \circledR M = a_i + M + a_i RM(\bmod p) = a_i + M + a_i(g^{kx_i} \bmod p)M(\bmod p) = w$ кўринишда амалга ошириб, шифрмаълумот сифатида $C = (w; d = g^k \bmod p)$ - жуфтлик жўнатилади.

Шифрмаълумот $C = (w; d = g^k \bmod p)$ ни қабул қилиб олган i-фойдаланувчи дешифрлашни қуйидагича амалга оширади:

1. Фақат i - фойдаланувчининг ўзига маълум бўлган x_i - махфий калитдан фойдаланиб, $d^{x_i} \bmod p = g^{kx_i} \bmod p = D$ - қиймат ҳисобланади.
2. Очиқ a_i- калитга тескари бўлган элемент

   $(a_i)^{\backslash -1} = -a_i(1 + a_i D)^{-1} \bmod p$ ҳисобланади.
3. Ушбу $R = D$ қийматнинг алмаштириш амалини бажариб, дешифрлаш амалга оширилади:

$$(a_i)^{\backslash -1} \circledR w = [-a_i(1 + a_i D)^{-1} \bmod p] \circledR [a_i + M + a_i RM(\bmod p)] =$$

$$= [-a_i(1 + a_i R)^{-1} \bmod p] \circledR [a_i + M + a_i RM(\bmod p)] =$$

$$\equiv [-a_i(1+a_iR)^{-1}] + [\,a_i + M(1+a_iR)\,] +$$

$$[-a_i(1+a_iR)^{-1}]R[\,a_i + M(1+a_iR)](\mathrm{mod}\, p) \equiv$$

$$\equiv [-a_i(1+a_iR)^{-1}](1+\ a_iR) + [\,a_i + M(1+a_iR)\,]\text{-}\, a_iRM\ (\mathrm{mod}\, p)\ \equiv$$

$$\equiv\text{-}\, a_i + a_i + M + a_iRM\ \text{-}\ a_iRM\ \ (\mathrm{mod}\, p\ ) = M.$$

Бу келтирилган носимметрик шифрлаш алгоритми ғоясини сақлаб қолган ҳолда, шифрлаш ва дешифрлаш жараёнларини ифодаловчи формулаларда қатнашувчи параметрларнинг матрицалар кўринишида аниқланиши улар хоссаларидан фойдаланиб криптографик самарадорликни ошириш имкониятларини беради. Қуйида айнан шундай масала ечими ҳақида сўз юритилади.

5.6.2. Матрицавий параметрли шифрлаш усули

Аввало юқоридаги каби ушбу:

$A_{n\times m}$ ® $B_{n\times m}$ $=$ $A_{n\times m} + B_{n\times m} + A_{n\times m}R_{m\times n}B_{n\times m}(\mathrm{mod}\, p)$ параметрли кўпайтириш амали киритилади [23, 69].

5.1-таъриф. $B_{n\times m}$ - матрица $A_{n\times m}$ - матрицага тескари дейилади, агарда $A_{n\times m}$ ® $B_{n\times m} = 0_{n\times m}$ бўлса ҳамда $A_{n\times m}$ - матрицага тескари бўлган матрица $A_{n\times m}^{\backslash -1}$ деб белгиланади.

Энди берилган матрицага тескари матрицани қандай топишни кўриб ўтамиз.

Агар $B_{n\times m}$ - матрица $A_{n\times m}$ - матрицага тескари бўлса, $C_{n\times m} = A_{n\times m}$ ® $B_{n\times m} = B_{n\times m} = 0_{n\times m}$ муносабат бажарилиши керак. Бу муносабатдан ушбу

$$C_{n\times m} - A_{n\times m} \equiv B_{n\times m} + A_{n\times m}R_{m\times n}B_{n\times m}(\mathrm{mod}\, p)\ \text{ёки}$$

$C_{n\times m} - A_{n\times m} \equiv (I_{n\times n} + A_{n\times m}R_{m\times n})B_{n\times m}(\mathrm{mod}\, p)$ ёки $B_{n\times m}\ \equiv\ (I_{n\times n} + A_{n\times m}R_{m\times n})^{-1}$ $(C_{n\times m} - A_{n\times m})(\mathrm{mod}\, p)$

таққосламага эга бўламиз. Бу ерда $C_{n\times m} = 0_{n\times m}$ бўлганда $B_{n\times m}$ - матрица $A_{n\times m}$ - матрицага тескари бўлишини ҳисобга олсак

$$B_{n\times m} \equiv (I_{n\times n} + A_{n\times m}R_{m\times n})^{-1}(C_{n\times m} - A_{n\times m})(\operatorname{mod} p) = (I_{n\times n} + A_{n\times m}R_{m\times n})^{-1}(- A_{n\times m})(\operatorname{mod} p) = A_{n\times m}^{\backslash -1}$$

бўлиши келиб чиқади.

Матрицавий параметрли шифрлаш усулида, аввало t-фойдаланувчи томонидан туб модуль p, ҳосил этувчи g элементлар танланади.

Ушбу сонлар $R_{il}^{t} = g^{x_{il}^{t}} \operatorname{mod} p$ ҳисобланади, бу ерда x_{il}^{t} - номаълумлар (байтлардан иборат бўлиши мумкин), i=1,…,m ; l=1,…,n. Сўнгра $\left(A_{n\times m}^{t}; R_{m\times n}^{t}\right)$ - жуфтликни t - фойдаланувчининг очиқ калити, x_{il}^{t} - номаълумларни эса махфий калит элементлари деб эълон қилинади.

Криптотизимнинг j - фойдаланувчиси t - фойдаланувчига $M_{n\times m}$ – очиқ маълумотни шифрлаб жўнатишни қуйидагича амалга оширади:

1. Фақат j - фойдаланувчининг ўзигагина маълум бўлган бирор k-сонини тасодифий ҳолда танлаб, $R \ = R^{t}{}_{m\times n} = (R_{il}^{t})^{k} \operatorname{mod} p = g^{kx_{il}^{t}} \operatorname{mod} p$ -матрица элементлари ҳисоблаб олинади.

2. Шифрлашни $A_{n\times m}^{t} ® M_{n\times m} = A_{n\times m}^{t} + M_{n\times m} + A_{n\times m}^{t}R_{n\times m}^{t}M_{n\times m}(\operatorname{mod} p) = w_{n\times m}$ кўринишда амалга ошириб, шифрмаълумот сифатида $C_{n\times m} = (w_{n\times m}; d = g^{k} \operatorname{mod} p)$ - жуфтлик жўнатилади.

Шифрмаълумот $C = (w; d = g^{k} \operatorname{mod} p)$ ни қабул қилиб олган t - фойдаланувчи дешифрлашни қуйидагича амалга оширади:

3. Фақат t - фойдаланувчининг ўзига маълум бўлган x_{il}^{t} - махфий калитдан фойдаланиб, $d^{x_{il}^{t}} \operatorname{mod} p = g^{kx_{il}^{t}} \operatorname{mod} p = D_{il}^{t}$ - қийматлар ҳисобланиб, $D_{m\times n}$ - матрица ҳосил қилинади.

4. Очиқ $A_{n\times m}^{t}$ - калитга тескари бўлган элемент $(A_{n\times m}^{t})^{\backslash -1} = (I_{n\times n} + A_{n\times m}^{t}D_{m\times n}^{t})^{-1}(-A_{n\times m}^{t}) \operatorname{mod} p$ ҳисобланади.

5. Ушбу $R = D_{n\times m}^{t}$ қийматнинг алмаштириш амалини бажариб, дешифрлаш амалга оширилади:

$$(A_{n\times m}^{t})^{\backslash -1} ® w_{n\times m} = (I_{n\times n} + A_{n\times m}^{t}D_{m\times n}^{t})^{-1}(-A_{n\times m}^{t}) ® (A_{n\times m}^{t} + M_{n\times m} + A_{n\times m}^{t}R_{m\times n}^{t}M_{n\times m})(\operatorname{mod} p) =$$

$$=(I_{n\times n}+A^t_{n\times m}R^t_{m\times n})^{-1}(-A^t_{n\times m})+(A^t_{n\times m}+M_{n\times m}+A^t_{n\times m}R^t_{m\times n}M_{n\times m})+$$

$$+(I_{n\times n}+A^t_{n\times m}R^t_{m\times n})^{-1}(-A^t_{n\times m})\ R^t_{m\times n}\ (A^t_{n\times m}+M_{n\times m}+A^t_{n\times m}R^t_{m\times n}M_{n\times m})(\mathrm{mod}\, p\ )=$$

$$=(I_{n\times n}+A^t_{n\times m}R^t_{m\times n})^{-1}(-A^t_{n\times m})\ (I_{m\times m}+R^t_{m\times n}A^t_{n\times m})+A^t_{n\times m}+(I_{n\times n}+A^t_{n\times m}R^t_{m\times n})M_{n\times m}+$$

$$+(I_{n\times n}+A^t_{n\times m}R^t_{m\times n})^{-1}(-A^t_{n\times m})R^t_{m\times n}\ (I_{n\times n}+A^t_{n\times m}R^t_{m\times n})M_{n\times m}\ (\mathrm{mod}\, p).$$

Бу охирги тенглик ифодасидаги матрицаларнинг фақат диагонал элементларининг ҳаммаси ноль бўлмай, бошқа барча элементлари ноллардан иборат бўлса, у ҳолда матрицалар кўпайтмалари қатнашган ҳадларда улар ўринларини алмаштирса ҳам тенглик ўзгармайди. Ана шундай матрицалар учун ушбу тенглик ўринли:

$$(A^t_{n\times m})^{\backslash-1} \circledR\, w_{n\times m}=(I_{n\times n}+A^t_{n\times m}R^t_{m\times n})^{-1}(-A^t_{n\times m})\ (I_{m\times m}+R^t_{m\times n}A^t_{n\times m})+A^t_{n\times m}+$$

$$+(I_{n\times n}+A^t_{n\times m}R^t_{m\times n})M_{n\times m}+$$

$$+(I_{n\times n}+A^t_{n\times m}R^t_{m\times n})^{-1}(-A^t_{n\times m})R^t_{m\times n}\ (I_{n\times n}+A^t_{n\times m}R^t_{m\times n})M_{n\times m}\ (\mathrm{mod}\, p)=$$

$$=\ (-A^t_{n\times m})(I_{n\times n}+A^t_{n\times m}R^t_{m\times n})^{-1}\ (I_{m\times m}+R^t_{m\times n}A^t_{n\times m})+A^t_{n\times m}+\ (I_{n\times n}+A^t_{n\times m}R^t_{m\times n})M_{n\times m}+$$

$$+(-A^t_{n\times m})R^t_{m\times n}(I_{n\times n}+A^t_{n\times m}R^t_{m\times n})^{-1}\ (I_{n\times n}+A^t_{n\times m}R^t_{m\times n})M_{n\times m}(\mathrm{mod}\, p)=$$

$$=\ -A^t_{n\times m}+A^t_{n\times m}+M_{n\times m}+A^t_{n\times m}R^t_{m\times n}M_{n\times m}-A^t_{n\times m}R^t_{m\times n}\ M_{n\times m}(\mathrm{mod}\, p)=M_{n\times m}\,.$$

Умуман олганда бу тенглик ифодаларида қатнашувчи матрицалар коммутативлик хоссасига эга бўладиган қилиб танлаб олинса, юқорида келтирилган дешифрлаш жараёни ижобий амалга оширилади.

5.6.3. Эллиптик эгри чизиқлардан фойдаланишга асосланган шифрлаш усули

Қуйида танланган эллиптик эгри чизиқнинг рационал нуқталари устида амаллар бажариш масаласининг мураккаблигига асосланган носимметрик шифрлаш алгоритмини яратиш масаласини ечишга тўхталиб ўтилади.

Мазкур усул бўйича ушбу нуқта $R_{m\times n}=R_{il}=[x_{il}]G$ координаталари, танлаб олинган эллиптик эгри чизиққа тегишли бўлган G -рационал координатали етарли катта тартибга эга бўлган ва барча фойдаланувчиларга маълум генератор нуқта орқали ҳисобланади, бу ерда x_{il} -номаълумлар. Сўнгра $(A_{n\times m};R_{m\times n})$ - жуфтлик очиқ калит деб эълон қилинади, x_{il} - номаълумлар эса шахсий калит сифатида олинади.

Криптотизимнинг j -фойдаланувчисидан t - фойдаланувчига *M*–очиқ маълумотни шифрлаб жўнатиш қуйидагича амалга оширилади:

1. Фақат j -фойдаланувчининг ўзигагина маълум бўлган бирор k - сонини тасодифий ҳолда танлаб, эллиптик эгри чизиқда $R=[k]R^t_{m\times n}=[k][x^t_{il}]G=[kx^t_{il}]G = (x^t_{il}(G),y^t_{il}(G))$ -нуқталар топилади ва бу нуқталарнинг *Ox* ўқидаги $x^t_{il}(G)$ -координаталари (ёки *Oy* ўқидаги $y_{il}(G)$ -координаталари) $R^t_{il}=x^t_{il}(G)$ (ёки $R^t_{il}=y^t_{il}(G)$ ёки $R^t_{il}=f(x^t_{il}(G),y^t_{il}(G))$) деб қабул қилинади. Шифрлашни $A^t_{n\times m}$ ® $M_{n\times m}=A^t_{n\times m}+M_{n\times m}+A^t_{n\times m}R^t_{n\times m}M_{n\times m}(\mathrm{mod}\, p)=w_{n\times m}$ кўринишда амалга ошириб, шифрмаълумот сифатида $C_{n\times m}=(w_{n\times m};d=[k]G)$ - жуфтлик жўнатилади.

Шифрмаълумот $C_{n\times m}=(w_{n\times m};d=[k]G)$ ни қабул қилиб олган *t*-фойдаланувчи томонидан дешифрлаш қуйидагича амалга оширилади:

2. Фақат t - фойдаланувчининг ўзига маълум бўлган x^t_{il} - махфий калит элементларидан фойдаланиб $[x^t_{il}]d=[x^t_{il}][k]G=[x^t_{il}k]G=D^t_{m\times n}$ - матрица ҳисоблаб олинади.

3. Очиқ $A^t_{n\times m}$ - калитга тескари бўлган матрица $(A^t_{n\times m})^{\backslash -1}=(I_{n\times n}+A^t_{n\times m}D^t_{m\times n})^{-1}(-A^t_{n\times m})\,\mathrm{mod}\, p$ ҳисобланади.

4. Ушбу $R=D^t_{n\times m}$ қийматни алмаштириш амалини бажариб, дешифрлаш жараёни 5.6.2-банддаги каби амалга оширилади.

5.6.4. RSA шифрига ўхшаш параметрли шифрлаш усули

Қуйида етарли катта сонни туб кўпайтувчиларга ажратиш масаласининг мураккаблигига асосланган носимметрик шифрлаш алгоритми яратиш масаласини ечиш келтириб ўтилади [1].

Етарли катта ва махфий тутилиши керак бўлган p ва q - туб сонлари танлаб олиниб, $n = pq$ ҳисобланади. Ушбу $e_t d_t \equiv 1 \bmod \varphi(n)$ таққосламадан (бу ерда $\varphi(n) = (p-1)(q-1)$ - махфий) e_t -параметрга бирор қиймат бериб $e_t d_t \equiv 1 \bmod (p-1)(q-1)$ муносабатни қаноатлантирувчи d_t - сонини топиш мумкин. Сўнгра $(A_{n\times m}; e_t; n)$ - учликни очиқ калит, $(d_t; \varphi(n))$ - жуфтликни шахсий деб, шифрлаш ва дешифрлаш жараёнлари қуйидагича амалга оширилади.

Криптотизимнинг j - фойдаланувчиси томонидан t - фойдаланувчига $M_{n\times m}$ – очиқ маълумотни шифрлаб жўнатиш қўйидагича амалга оширилади:

1. Фақат j - фойдаланувчининг ўзигагина маълум бўлган бирор k_{il}^j -сонларини тасодифий ҳолда танлаб, $R = R_{m\times n}^j = (k_{il}^j) \bmod n$ - қийматлар ҳисобланади (бу ерда $k_{il}^j \neq p$ ва $k_{il}^j \neq q$).

Шифрлаш 5.6.2-банддаги каби

$A_{n\times m}^t \circledR M_{n\times m} = A_{n\times m}^t + M_{n\times m} + A_{n\times m}^t R_{m\times n}^j M_{n\times m} (\bmod p) = w_{n\times m}$ кўринишда амалга оширилгач, шифрмаълумот сифатида $C_{n\times m} = (w_{n\times m}; d_{m\times n}^j = (k_{il}^j)^{e_t} \bmod n)$ - жуфтлик жўнатилади.

2. Шифрмаълумот $C = (w; d_{m\times n}^j = (k_{il}^j)^{e_t} \bmod n)$ ни қабул қилиб олган t-фойдаланувчи томонидан дешифрлаш қуйидагича амалга оширилади:

1. Фақат t - фойдаланувчининг ўзига маълум бўлган d_t - махфий калитдан фойдаланиб $(d_{m\times n}^j)^{d_t} \bmod n = (k_{il}^j)^{e_t d_t} \bmod n = (k_{il}^j) \bmod n = D_{m\times n}^j$ -матрица ҳисобланади.

2. Очиқ $A_{n\times m}^t$ -калитга тескари бўлган матрица

$(A_{n\times m}^t)^{\backslash -1} = (I_{n\times n} + A_{n\times m}^t D_{m\times n}^t)^{-1} (-A_{n\times m}^t) \bmod p$ ҳисобланади.

3. Ушбу $R = D_{n\times m}^t$ қийматни алмаштириш амалини бажариб, дешифрлаш жараёни 5.6.2-банддаги каби амалга оширилади.

Юқорида келтирилганлардан параметрли группа амаллари хусусиятлари мавжуд мураккабликларни композициялари негизида такомиллашган янги носимметрик алгоритмлар яратиш имкониятларини бериши аён бўлади.

5.7. Калитлар генерацияси

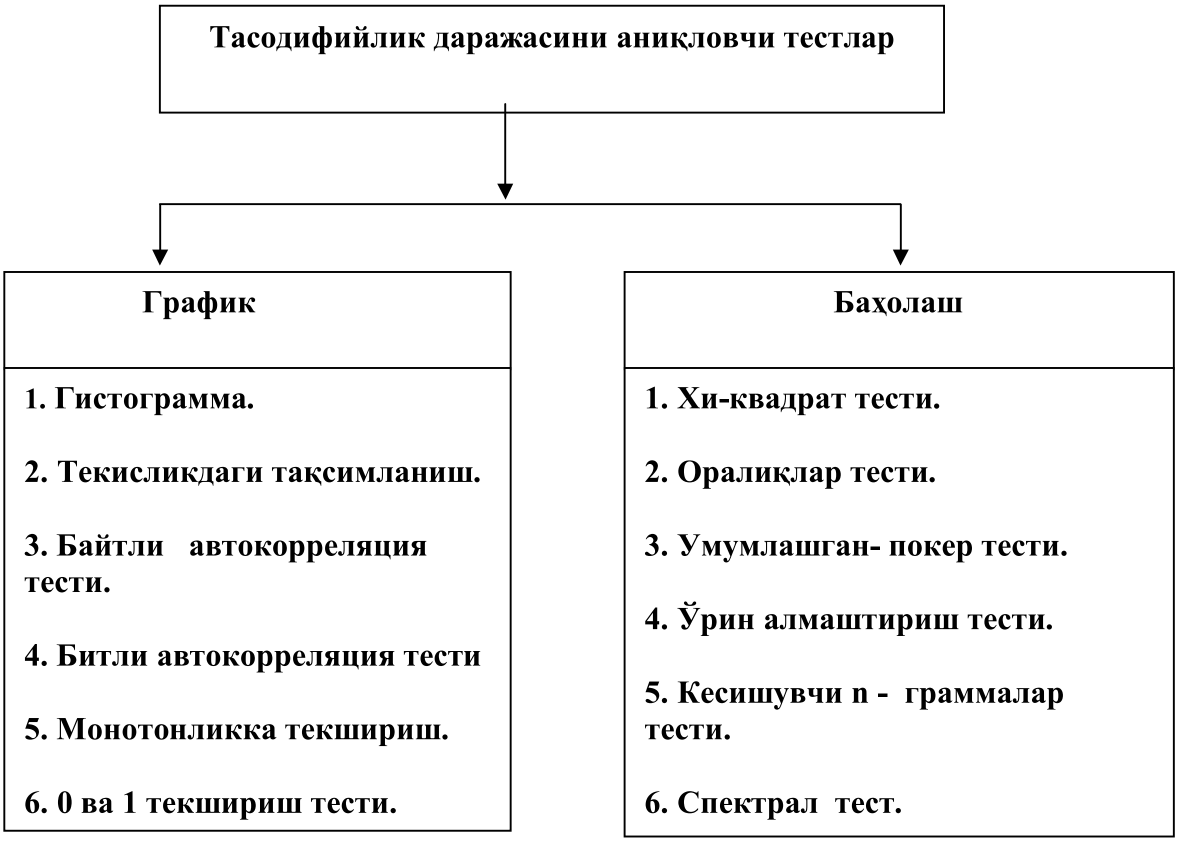
5.7.1. Бардошли калитларни ишлаб чиқиш усулларининг математик асослари ва алгоритмлари

Криптоалгоритмлар, хусусан блокли симметрик шифрлаш алгоритмлари DES, AES, ГОСТ 28147-89, O‘z DSt 1106:2009, мос равишда 56 бит, 128, 256 бит ёки 512 бит, 256 бит, 256 ёки 512 бит узунликдаги олдиндан белгилаб қўйилган қоида бўйича генерация қилинган калитлардан фойдаланади. Бироқ стандарт алгоритмларда белгилаб қўйилган қоида бўйича генерация қилинган барча калитлар ҳар доим ҳам шифрматнни очиш мақсадида очиқ алоқа тармоғини назорат қилувчи криптотаҳлилчи томонидан уюштириладиган турли криптоҳужумларга бардошли бўлмаслиги мумкин. Масалан, калитни ташкил этувчи битлар кетма-кетлиги фақат ноллардан ёки бирлардан ёки бўлмаса, ноль ва бирларнинг комбинацияси фиксирланган давр билан такрорланиши ёрдамида тузилган бўлса, бу тоифа калитлар бардошсиз ҳисобланади. Чунки ушбу тур битлар кетма-кетлигида, шу кетма-кетликни ташкил этувчи ноль ва бир элементлари даврий такрорланишининг математик қонуниятини олдиндан билиш имконияти мавжуд. У ҳолда бу зайлда генерация қилинган битлар кетма-кетлигидан симметрик шифрлаш алгоритмлари учун махфий калит сифатида фойдаланиш мақсадга мувофиқ эмас. Демак, юқоридаги фикр-мулоҳазалардан келиб чиқиб, «криптоалгоритмлар махфий калит блоклари учун тасодифий битлар кетма-кетлиги қандай қурилади?» деган саволнинг туғилиши табиий, яьни агар бирор қоида бўйича калит блокининг $k = k_1k_2...k_m$, кетма-кетлиги олинган бўлса, бу ерда $k_i \in \{0;1\}$ ва m=56, 128, 192, 256 бўлиши мумкин. У ҳолда $k = k_1k_2...k_m$, калит блокида k_i - битларнинг тақсимоти тасодифий ёки тасодифий эмаслиги қандай аниқланади? Ушбу саволга жавоб олиш учун калит блокида k_i -битларнинг тақсимотини амалиётда кенг тарқалган ва бошқа мавжуд тасодифийлик тестларининг асосларини ташкил этувчи “Хи-квадрат” тақсимотидан фойдаланиб аниқлаш керак бўлади.

Тасодифийликка текширувчи тестлар 2 хил бўлади (11-расм).

График тестлар - График тестлар фойдаланувчига текширилаётган кетма-кетликнинг маълум бир график боғлиқлиги ҳақидаги маълумотни бериб, у бўйича текширилаётган кетма-кетлик хоссалари тўғрисида хулоса чиқариш имкониятини беради.

Баҳолаш тестлари - Баҳолаш тестлари текширилаётган кетма-кетлик статистик хоссаларини таҳлил қилиб, унинг чин тасодифийлик даражаси ҳақида хулоса чиқариш имкониятини беради [12-13].



11-расм. Тасодифийлик даражасини аниқловчи тестлар

Калит блокини ташкил этувчи белгилар тақсимотини тасодифийликка текширишда, аввало, бу калит блокини бирор қоида бўйича ҳосил қилиб олиш зарур. Бу каби ишлар одатда, псевдотасодифий кетма-кетликлар генераторлари орқали амалга оширилади. Псевдотасодифий кетма-кетлик ишлаб чиқарувчи генераторлар ҳақида, уларнинг тузилиш асосларига кўра туркумлари, хусусиятлари, хоссалари, криптографик масалаларни ечишдаги қўлланишлари 5-бўлимда батафсил таҳлил қилинган.

Қуйида мисол сифатида бир томонлама функцияларга асосланган псевдотасодифий кетма-кетлик ишлаб чиқарувчи генераторлар келтириб ўтилади [13]:

1) **ANSI X9.17 генератори.** Бу алгоритм АҚШда псевдотасодифий кетма-кетлик ишлаб чиқувчи Миллий стандарт ҳисобланиб, FIPS (USA Federal Information Processing Standart) таркибига киради. Алгоритмда бир томонлама функция сифатида 3DES иккита $K1,\ K2 \in V64$ калит ишлатилади: $DESK1DESK2\ DESK1$(64 бит) .

2) FIPS-186 генератори. Бу алгоритм ҳам АҚШ Миллий стандарти сифатида қабул қилинган бўлиб, DSA электрон рақамли имзо алгоритмининг махфий параметрларини ва калитларини генерация қилиш учун мўжалланган. Алгоритм бир томонлама функция сифатида DES шифрлаш алгоритми ва SHA-1 хэшлаш алгоритмини ишлатади.

3) Yarrow-160 генератори. Yarrow-160 псевдотасодифий кетма-кетлик ишлаб чиқарувчи генератори Келси, Шнайер ва Фергюсон томонидан таклиф қилинган. Бу ерда учлик DES ва SHA-1 хэшлаш алгоритми ишлатилган.

Сонлар назарияси муаммоларига асосланган генераторлар сифатида:

1) RSA алгоритми асосидаги;

2) Микали-Шнорр RSA алгоритми асосидаги;

3) BBS (Blum-Blum-Shub) - алгоритми асосидаги генераторларни келтириш мумкин.

Агар чизиқли ва мультипликатив конгруэнт генераторлар билан аниқланган сонлар кетма-кетлиги учун z_n, z_{n+1} – битлари маълум бўлса, у ҳолда ҳосил қилинган кетма-кетликнинг қолган ҳадларини топиш имконияти мавжуд [13, 69].

Сонлар назариясининг муаммоларига (туб кўпайтувчиларга ажратиш ва дискрет логарифмлаш) асосланган генераторлардан симметрик шифрлаш алгоритмлари бардошли калитларининг генерация қилинишида фойдаланиш мақсадга мувофиқ, чунки бу генераторлардан фойдаланиб, ҳосил қилинган кетма-кетлик ҳадларининг бирор қисмини билган ҳолда ундан олдинги ёки кейинги қисмларини аниқлаш имконияти мураккаб масала ҳисобланади.

Биз бундан кейинги фикр-мулоҳазаларимизда, бирор танланган псевдотасодифий кетма-кетликлар генератори орқали керакли узунликдаги калит блоки генерация қилиб олинган деб ҳисоблаймиз.

5.7.2. Тақсимотни тасодифийликка текширишнинг “Хи-квадрат” мезони

Бирор ўтказилаётган тажриба натижаларининг барча мумкин бўлган ҳолатлари $y_1, y_2, ..., y_k$, дан иборат ва уларнинг сони k га тенг бўлиб, бу тажриба бир-бирига боғлиқсиз ҳолда n марта ўтказилсин. Шунда, $y_1, y_2, ..., y_k$ - ҳолатларни, уларнинг n марта ўтказилган тажрибада, бир хил сонда такрорланишидан (текис тақсимотдан ёки бир хил частотага эга бўлишдан) қанчалик четланганлигини баҳолаш масаласининг ечилиши кўриб чиқилади. Бунинг учун қуйидагича белгилашлар киритилади:

p_s - тажриба натижаси y_s бўлишининг эҳтимоллик қиймати;

Y_s - тажриба натижаларининг y_s ҳолатга тегишлилари (тенглари) сони.

У ҳолда, бу белгилашларга нисбатан “Хи-квадарат” деб аталувчи тақсимот мезони ушбу

$$V = \sum_{s=1}^{k} \frac{(Y_s - np_s)^2}{np_s},$$

формула орқали аниқланади.

Агар тажриба *n* мартадан бир неча марта ўтказилганда, ҳар доим $y_1, y_2, ..., y_k$ - ҳолатлар тенг Y_i мартадан такрорланса (текис тақсимланган ёки бир хил частотали бўлса), яъни $Y_1 = Y_2 = ... = Y_k$ бўлса, у ҳолда $p_1 = p_2 = ... = p_k = \frac{1}{k}$, деб хулоса қилинади ва

$$V = \sum_{s=1}^{k} \frac{\left(Y_s - \frac{n}{k}\right)^2}{\frac{n}{k}} = \sum_{s=1}^{k} \frac{\left(\frac{n}{k} - \frac{n}{k}\right)^2}{\frac{n}{k}} = 0$$

тенглик ўринли бўлади. Бундай жараённинг илмий-тадқиқот учун қизиғи йўқ. Аммо амалдаги аксарият жараёнларда бундай ҳолат кузатилмайди, яъни бирор тажриба бир-бирига боғлиқсиз равишда *n* марта ўтказилиганда: $Y_1 = Y_2 = ... = Y_k = \frac{n}{k}$ ҳолат кузатилмайди. Шунинг учун $y_1, y_2, ..., y_k$ - ҳолатларни рўй бериш эҳтимолликлари бир хил $p_1 = p_2 = ... = p_k = \frac{1}{k}$ бўлиб, тажриба бир-бирига боғлиқ бўлмаган равишда *n* марта ўтказилганда, бу ҳолатларнинг рўй бериши сони мос равишда $Y_1, Y_2, ..., Y_k$ бўлса, у ҳолда ушбу

$$V = \sum_{s=1}^{k} \frac{\left(Y_s - \frac{n}{k}\right)^2}{\frac{n}{k}} = \frac{k}{n} \sum_{s=1}^{k} \left(Y_s - \frac{n}{k}\right)^2$$

формула $Y_1 = Y_2 = ... = Y_k = \frac{n}{k}$ бўлган тенг тақсимотдан $Y_1, Y_2, ..., Y_k$ -тенг бўлмаган тақсимотни ўртача квадратик четланишини ифодалайди. Бу охирги формуладаги $\left(Y_s - \frac{n}{k}\right)$ - ифода бирор ўзгармас сон билан чегараланган, яъни $\left|Y_s - \frac{n}{k}\right| \le C = const$.

Шунинг учун

$$V=\sum_{s=1}^{k}\frac{\left(Y_s-\frac{n}{k}\right)^2}{\frac{n}{k}}=\frac{k}{n}\sum_{s=1}^{k}\left(Y_s-\frac{n}{k}\right)^2 \le\frac{k}{n}\sum_{s=1}^{k}C^2=\frac{(kC)^2}{n}\to 0,\text{ агар } n\to\infty \text{ бўлса.}$$

Бу охирги формуладан, бирор генератор орқали ҳосил қилинган псевдотасодифий кетма-кетликнинг даври етарли узун бўлиб, барча мумкин бўлган битлар, байтлар ва қисм блокларининг тақсимоти деярли текис (тенг тақсимланган) бўлса, у ҳолда “Хи-квадарат” тақсимот мезонининг бу кетма-кетликка нисбатан қиймати нолга яқин бўлиб, унинг тасодифийлик даражаси юқори ҳисобланади.

Қуйида стандарт DES, ГОСТ 28147-89, AES-FIPS-197, O‘z DSt 1106:2009 ва бошқа симметрик шифрлаш алгоритмлари учун махфий калитни тасодифий қилиб генерация қилишнинг Хи-квадрат тақсимоти орқали қандай амалга оширилишини кўриб ўтамиз.

Берилган калит блоки бўйича қуйидаги жадвални тузиб оламиз:

Қиймат (s): $0 \quad 1$;

Эҳтимоллик (p_s): $\frac{1}{2} \quad \frac{1}{2}$;

Кузатилаётган сон (Y_s): $N_0 \quad N_1$,

бу ерда N_0 ва N_1 мос равишда калит блокида иштирок этувчи ноллар ва бирлар, $N_0+N_1=n$, орқали калит узунлигини белгилайди, масалан $n=256$;

Кутилаётган сон (np_s): $\frac{n}{2} \quad \frac{n}{2}$;

Хи-квадрат тақсимоти формуласи бўйича [74]:

$$V=\sum_{s=0}^{k-1}\frac{(Y_s-np_s)^2}{np_s} \text{ ҳисобланади.}$$

Ушбу қаралаётган ҳолатда:

$k=2; s=0,1; p_0=p_1=\frac{1}{2}; Y_0=N_0; Y_1=N_1; n=256$; у ҳолда қуйидагича катталикка эга бўламиз:

$$V=\frac{(N_0-128)^2+(N_1-128)^2}{128}.$$

Бу катталикни ҳисоблаш учун бизга Хи-квадрат тақсимотининг критик нуқталари жадвали деб аталувчи жадвал керак бўлади (5.2-жадвал).

5.2-жадвал

Хи-квадрат тақсимотининг критик нуқталари

	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**

“Хи-квадрат” мезони жадвали $v = k - 1 = 2 - 1 = 1$, сатридан V қиймат жойлашиш оралиғини топамиз. Агар V қиймат жадвал устунининг $p = 25\%$ дан $p = 75\%$ оралиғида бўлса, у ҳолда псевдотасодифий генератор ёрдамида ҳосил қилинган калит блок битлари кетма-кетлиги тасодифий деб олинади.

Гарчанд псевдотасодифий генератор ёрдамида ҳосил қилинган калит блок битлари кетма-кетлиги тасодифийликка “Хи-квадрат” мезони бўйича текширилганда ижобий жавоб олинган бўлса ҳам, ундан кўра ишончли ва мукаммал бўлган жавоб олиш учун қаралаётган битлар кетма-кетлигини бошқа мавжуд тасодифийлик тестларига ҳам текшириб кўриш лозим. Бу меъонларга текширув натижаларида қанчалик кўп ижобий жавоблар олинса, мезон шунчалик яхши натижа деб қаралади. Бундан ташқари қуйидаги жараён ҳам тасодифийликка текширишда чиқариладиган хулосанинг ижобийлигига сезиларли даражада таъсир кўрсатади, яъни псевдотасодифий генератор ёрдамида ишлаб чиқилган калитларнинг амалиётда ўрнатилган бардошсиз калитлардан ўртача квадрат четланишининг ўртача қийматини ифодаловчи жараён.

Айтайлик, псевдотасодифий генератор ёрдамида ҳосил қилинган калит блоки:

$k = k_1 k_2 ... k_n = k_1 k_2 ... k_{256}$, бу ерда $k_i \in \{0;1\}$, $i=1,2, ..., n = 256,$

юқорида келтирилган мезон бўйича тасодифийликка текширилган ва қониқарли жавоб олинган. Амалиёт жараёнида шифрлаш тизимлари билан ишлашда аниқланган бардошсиз калитларни $k_{н1}, k_{н2}, ..., k_{нm}$ каби белгилаймиз.

Псевдотасодифий генератор ёрдамида ҳосил қилинган калит блоки: $k = k_1 k_2 ... k_n$ = $k_1 k_2 ... k_{256}$ ва амалиёт жараёнида бардошсиз деб топилган $k_{н1}, k_{н2}, ..., k_{нm}$ калитларнинг фарқи кўриб ўтилади:

$r_1 = k_{н1} \oplus k = r_1(1) r_2(1) ... r_{256}(1)$, бу фарқ бўйича мос равишда 0 ва 1 битлар сони $N_0(1)$, $N_1(1)$;

$r_2 = k_{н2} \oplus k = r_1(2) r_2(2) ... r_{256}(2)$, бу айирма бўйича мос равишда 0 ва 1 битлар сони $N_0(2)$, $N_1(2)$;

$r_m = k_{нm} \oplus k = r_1(m) r_2(m) ... r_{256}(m)$, бу айирма бўйича мос равишда 0 ва 1 битлар сони $N_0(m)$, $N_1(m)$; бу катталиклардан фойдаланган ҳолда, қуйидагиларни ҳисоблаймиз:

$$V_1 = \frac{(N_0(1) - 128)^2 + (N_1(1) - 128)^2}{128};$$

$$V_2 = \frac{(N_0(2) - 128)^2 + (N_1(2) - 128)^2}{128};$$

$$V_m = \frac{\left(N_0(m)-128\right)^2 + \left(N_1(m)-128\right)^2}{128};$$

$$V = \frac{V_1 + V_2 + \ldots + V_m}{m} \ .$$

“Хи-квадрат” мезони жадвали $v = k-1 = 2-1 = 1$, сатридан V - қиймат жойлашиш оралиғини топамиз. Агар V қиймат жадвал устунининг $p = 25\%$ дан $p = 75\%$ оралиғида бўлса, у ҳолда псевдотасодифий генератор ёрдамида ҳосил қилинган калит блок битлари кетма-кетлиги тасодифий деб олинади.

5.7.3. Калитлар очиқ тақсимланиш алгоритмининг математик асоси ҳақида

Агарда $y = f(x) = a^x$ бўлса, у ҳолда табиийки, бу функцияга тескари функция

$$x = f^{-1}(y) = \log_a y$$

бўлиб, берилган y лар бўйича x қийматларни топиш дискрет логарифмларни топиш масаласи дейилади. Ҳаттоки, p нинг етарли катта бўлган қийматларида ҳам, $f(x)$ функцияни осон ҳисоблаш мумкин.

Агарда дискрет даражага кўтариш функцияси ҳақиқатан ҳам бир томонлама бўлса, у ҳолда $\log_a y$ ифодани y нинг барча, яъни ушбу $1 \le y \le p$ тенгсизликни қаноатлантирувчи барча қийматларида ҳисоблашни амалий жиҳатдан имконияти йўқ бўлиши керак. М.Е. Хеллман ва унинг шогирди Полиг, фақатгина p сони катта туб сон бўлгандагина эмас, балки $(p-1)$ сони катта туб кўпайтувчи q га эга (ёки шу q туб сон 2 га кўпайтирилган) бўлганда, функциянинг y қийматларига кўра $\log_a y$ ифодани ҳисоблаш амалий жиҳатдан мураккаб эканлигини кўрсатдилар. У. Диффи ва М.Е. Хеллман махфий алоқа тизимлари фойдаланувчилари учун дискрет логарифмлардан фойдаланиб, махфий калитларни ўзаро алмашувини алоҳида махфий каналсиз амалга ошириш алгоритмини яратдилар. Бу алгоритм бўйича:

1. α ва p сонлари ҳамма фойдаланувчиларга маълум.

2. Ҳар бир фойдаланувчи, масалан, $i-$ фойдаланувчи 1 билан $(p-1)$ сонлари оралиғидаги бирор бутун X_i сонини танлаб олади ва бу сонни махфий тутади.

3. i –фойдаланувчи $Y_i=\alpha^{X_i}(\mathrm{mod}\, p)$ қийматни ҳисоблаб, бу Y_i қийматни махфий тутмай, ҳамма фойдаланувчилар томонидан тасдиқланган ва улар ҳар доим фойдалана оладиган очиқ маълумотлар китобига киритади.

4. Агарда махфий алоқа тизимининг i – фойдаланувчиси j – фойдаланувчи билан махфий алоқа ўрнатмоқчи бўлса, $i-$ фойдаланувчи очиқ маълумотлар китобидан Y_j ни олиб, ўзининг махфий калити X_i ёрдамида

$$Z_{ij}=\left(Y_j\right)^{X_i}=\left(\alpha^{X_j}\right)^{X_i}=\alpha^{X_iX_j}(\mathrm{mod}\, p)$$

қийматни ҳисоблайди.

5. Худди шу каби $j-$ фойдаланувчи ҳам Z_{ji} ни ҳисоблайди. Бунда $Z_{ij}=Z_{ji}$ бўлиб, i ва j фойдаланувчилар ўз махфий алоқаларини таъминловчи симметрик калитли криптотизимда Z_{ij} қийматни махфий калит сифатида ишлатишлари мумкин. Агар рақиб томон дискрет логарифмларни ҳисоблаш масаласини еча олса, очиқ маълумотлар китобидан Y_i ва Y_j ларни олиб, $X_i=\log_\alpha Y_i$ ва $X_j=\log_\alpha Y_j$ қийматларни ҳисоблаб, Z_{ij} махфий калитга эга бўлган бўлар эди (i ва j - фойдаланувчилар каби).

Шу ерда таъкидлаб ўтиш жоизки, очиқ маълумотлар китоби ахборотларнинг махфий алоқа тизими фойдаланувчиларигагина очиқ.

Юқорида келтирилган алгоритмдан кўриниб турибдики, ҳали бу нарса назарий жиҳатдан тўла исботланган бўлмасада, рақиб томон Z_{ij} қийматни бошқа бирор услуб билан ҳисоблай олмайди. Келтирилган алгоритм У.Диффи ва М.Е. Хеллманнинг калитларни очиқ тақсимлаш тизими дейилади. Бу махфий алоқа тизимида махфий калитларни махфий канал билан узатишнинг ҳожати йўқлигини таъминловчи биринчи тизим бўлиб, бугунги кунда ҳам бардошли ва қулай очиқ калитли бошқа криптотизимларнинг асосини ташкил этади.

У. Диффи ва М.Е. Хеллманнинг калитларни очиқ тақсимлаш тизими очиқ калитли бошқа криптотизимлар каби махфий калитни махфий канал орқали узатилишининг ҳожати йўқлигини таъминлайди, аммо аутентификация масаласини ечмайди.

Махфий алоқа тизимида очиқ маълумотлар китобини сақловчи, махфий бўлмаган Y_i ни, очиқ маълумотлар китобига $i-$ фойдаланувчининг фақат ўзи томонидангина критилганига ишонч ҳосил қилиши керак, $i-$фойдаланувчи эса, ўз навбатида, Y_j ни фақат очиқ маълумотлар китобини сақловчи томонидан берилганига ишонч ҳосил қилиши керак. Яъни очиқ калитлар тўплами ҳам муҳофаза қилиниши керак. Чунки бирор субъект томонидан ноқонуний (рухсатсиз) равишда очиқ калитлар тўпламига ўзининг очиқ калитини жойлаштириши унинг учун шу тизимга ноқонуний (рухсатсиз) фойдаланиш имкониятига эга бўлганлигини таъминлайди. Шунинг учун ҳам сертификатланган калитлар тўплами умумфойдаланиш ахборот-коммуникация тизимида сақланмайди, у алоҳида фаолият кўрсатувчи компьютер ёки нисбатан кичик сондаги компьютерлар тизимида сақланади. Тизимнинг бирор i -фойдаланувчиси бирор j - фойдаланувчи билан муҳофазаланган алоқа ўрнатиш учун j - фойдаланувчининг очиқ калитига эга бўлиши керак. Бунинг учун:

1) Умумфойдаланиш тизимидаги барча фойдаланувчилар компъютерларига ва улар бевосита боғланган бош компьютерга ахборот муҳофазасининг криптографик усулларининг асосий воситалари бўлган шифрлаш, хэш-функция ва ЭРИ алгоритмларининг дастурий таъминотлари ўрнатилган бўлиб, бош компьютер администраторининг очиқ калити ҳамма фойдаланувчиларга маълум бўлади.

2) i - фойдаланувчи бош компьютер администраторига j - фойдаланувчи билан алоқа ўрнатмоқчи эканлигини M - очиқ матнни бош компьютер администраторининг k_A^o - очиқ калити билан шифрлаган ҳолда $E_{k_A^o}(M)$ ҳамда администратор бу маълумотни ва унинг муаллифининг ҳақиқийлигига ишонч ҳосил қилиши учун, M - маълумот хэш-қийматини $h(M)$ ушбу $E_{k_A^o}(M) \cup h(M)$ кўринишда бирлаштириб ва ҳосил бўлган кенгайтирилган $M' = E_{k_A^o}(M) \cup h(M)$ маълумотни ўзи $k_i^{м}$ – махфий калити билан шифрлаб, $E_{k_i^{м}}(M')=C$ (ёки $M' = [M \cup P(k_i^{м},h(M))]$ - кенгайтирилган маълумотни администраторнинг очиқ калити k_A^o билан шифрлаб, $E_{k_A^o}[M \cup P(k_i^{м},h(M))]$=С) юборади.

3) Администратор $C=E_{k_i^{м}}(M')$ -шифрланган маълумотни k_i^o -калит билан очади: $D_{k_i^o}(C)=D_{k_i^o}(E_{k_i^{м}}(M'))= M' = E_{k_A^o}(M) \cup h(M)$. Сўнгра администратор ўзининг $k_A^{м}$ -махфий калити билан $D_{k_A^{м}}(\ E_{k_A^o}(M)\ )=M_1$ – очиқ маълумотга эга бўлади.

4) Бу олинган очиқ маълумот хэшланади $h(M_1)$ ҳамда $h(M_1)=h(M)$ тенглик текширилади. Агар тенглик ўринли бўлса, маълумот ва унинг муаллифи ҳақиқий, агар тенглик ўринли бўлмаса, маълумот ва унинг муаллифи ҳақиқий эмас деган хулоса чиқарилади.

5) Агар администраторга С= $E_{k_A^o}[M \cup P(k_i^{м},h(M))]$ - шифрмаълумот юборилган бўлса, у ўзининг $k_A^{м}$ -махфий калити билан бу маълумотни дешифрлайди:

$D_{k_A^{м}}(C)\ = D_{k_A^{м}}\ \{E_{k_A^o}[M \cup P(k_i^{м},h(M))]\}=M \cup P(k_i^{м},h(M))$. Сўнгра $P(k_i^{м},h(M))$ -ЭРИ тўғрилигини текширади, агар тўғри бўлса, маълумот ва унинг муаллифи ҳақиқий, аксинча бўлса маълумот ва унинг муаллифи ҳақиқий эмас деб хулоса чиқарилади.

6) Юборилган маълумот ва унинг муаллифининг (i - фойдаланувчининг) ҳақиқийлиги ўрнатилгандан сўнг, администратор j -

фойдаланувчининг k_j^o -очиқ калитини ва у билан боғлиқ бўлган (масалан, амал қилиш вақти ва шу каби) бошқа M_j-маълумотларни алоҳида фаолият кўрсатувчи компъютердан олиб, бош компъютер орқали i - фойдаланувчининг k_i^o -очиқ калити билан шифрлаб $E_{k_i^o}(M_j)=C_j$ ҳамда i - фойдаланувчинг бу маълумотни ва унинг муаллифини ҳақиқийлигига ишонч ҳосил қилиши учун M_j -маълумотнинг хэш-қийматини $h(M_j)$ ушбу $E_{k_i^o}(M_j) \cup h(M_j)$ кўринишда бирлаштириб ва ҳосил бўлган кенгайтирилган $M_j^{'} = E_{k_i^o}(M_j) \cup h(M_j)$ -маълумотни ўзининг $k_A^{\text{м}}$ – махфий калити билан шифрлаб $E_{k_A^{\text{м}}}(M_j^{'})=C_j^{'}$ (ёки $M_j^{'} = [M_j \cup P(k_A^{\text{м}},h(M_j))]$ -кенгайтирилган маълумотни i -фойдаланувчининг очиқ калити k_i^o билан шифрлаб $E_{k_i^o}[M_j \cup P(k_A^{\text{м}},h(M_j))]$=С$'_j$) очиқ алоқа канали орқали юборади.

7) i- фойдаланувчи $C_j^{'} = E_{k_A^{\text{м}}}(M_j^{'})$ -шифрланган маълумотни k_A^o - калит билан очади $D_{k_A^o}(C_j^{'}) = D_{k_A^o}(E_{k_A^{\text{м}}}(M_j^{'})) = M_j^{'} = E_{k_i^o}(M_j) \cup h(M_j)$. Сўнгра i - фойдаланувчи ўзининг $k_i^{\text{м}}$- махфий калити билан $D_{k_i^{\text{м}}}$($E_{k_i^o}(M_j)$)=$M1_j$ – очиқ маълумотга эга бўлади.

8) Бу олинган очиқ маълумот хэшланади $h(M1_j)$ ҳамда $h(M1_j)=h(M_j)$ тенглик текширилади. Агар тенглик ўринли бўлса, маълумот ва унинг муаллифи ҳақиқий, агар тенглик ўринли бўлмаса, маълумот ва унинг муаллифи ҳақиқий эмас деган хулоса чиқарилади.

9) Агар i- фойдаланувчига С$_j = E_{k_ш^o}[M_j \cup P(k_A^{\text{м}},h(M_j))]$ - шифрмаълумот юборилган бўлса, у ўзининг $k_i^{\text{м}}$ -махфий калити билан бу маълумотни дешифрлайди:

$D_{k_i^{\text{м}}}(C_j) = D_{k_i^{\text{м}}}\{E_{k_i^o}[M_j \cup P(k_A^{\text{м}},h(M_j))]\} = M_j \cup P(k_A^{\text{м}},h(M_j))$. Сўнгра $P(k_A^{\text{м}},h(M_j))$ - ЭРИ тўғрилигини текширади, агар тўғри бўлса, маълумот ва унинг муаллифи ҳақиқий, аксинча бўлса, маълумот ва унинг муаллифи ҳақиқий эмас деб хулоса чиқарилади.

Шундай қилиб, i-фойдаланувчи j-фойдаланувчи билан очиқ алоқа тармоғида муҳофазаланган ахборот алмашинувини ўрнатиши учун j-фойдаланувчининг k_i^o - сертификатланган очиқ калитига эга бўлди. Очиқ калитлар тўпламининг алоҳида компъютерда сақланиши ва очиқ калитларнинг 1) – 9) босқич жараёнларида тарқатилиши самарали криптографик муҳофазани ташкил этиш услубини ёки протоколини белгилайди. Ҳақиқатан ҳам бундай ташкилий жараён фақат шифрлаш, хэшлаш ва ЭРИ алгоритмларидан фойдаланган ҳолда кафолатли муҳофазанинг таъминлашини тушуниш қийин эмас.

5.7.4. Криптотизим фойдаланувчилари учун калитларни тақсимлаш протоколи

Махфий йўлли бир томонлама функцияга асосланган очиқ калитли криптотизимлар ўз моҳиятига кўра ундан фойдаланишнинг алоҳида протоколини талаб этади. Бу алоҳида тартиб ва қоидаларга кўра, тизимнинг фойдаланувчилари ва тизим фойдаланувчиларигагина очиқ бўлган очиқ маълумотлар тўпламининг (китобининг) администратори (сақловчиси) биргаликда шу тизимда узатиладиган маълумотларнинг махфийлигини таъминлайдилар.

Очиқ калитли криптотизимларнинг бардошлилигига тўла ишонч билдирмай ишончсизлик ва иккиланиш билан қарайдиган баъзи криптолог мутахассислар, фойдаланувчиларга муҳофазаланган услубда очиқ калитларни тақсимлаш ва махфий калитларни узатиш масалаларини, яъни калитлар билан боғлиқ жараёнларни мақсадли бошқаришни криптографиянинг бош амалий масаласи, деб биладилар. Мисол учун, агарда криптотизим фойдаланувчиларининг сони S та бўлса ва ҳар бир мумкин бўлган алоқа жуфтлари учун алоҳида махфий калит талаб этилса, уларнинг сони $c_s^2 = s(s-1)/2$ бўлиб, фойдаланувчилар сони кўп бўлган тизимлар учун бундай ҳолат баъзида мақсадга мувофиқ бўлмаслиги мумкин. Бирор фойдаланувчининг бошқа барча фойдаланувчиларга махфий бўлган маълумотни юбориши махфий алоқа моҳиятига зид жараён. Бундан ташқари махфий (муҳофазаланган) алоқа тизимида қайси фойдаланувчининг бошқа қайси бир фойдаланувчи билан махфий алоқа қилишни хоҳлаши олдиндан маълум эмас. Мана шундай ҳолатлар фойдаланувчиларга калитларни тақсимлаш тартиби ва қоидалари масалаларини келтириб чиқаради. Бундай масалаларнинг ечилиши эса, ахборот-коммуникация тизимида маълумотларнинг махфийлиги муҳофазасини таъминловчи криптотизимда калитларни рўйхатга олиш маркази (КРОМ) ташкил этишни тақозо этади. Калитларни тақсимлаш протоколи қуйидагича:

1. КРОМ муҳофазаланган алоқа тармоғи орқали барча i=1,2,...,S фойдаланувчиларга махфий Z_i калитларни тақдим этади.

2. Фойдаланувчи i фойдаланувчи j билан махфий алоқа ўрнатмоқчи бўлса, у умумий алоқа тармоғи орқали (очиқ матн билан бўлиши мумкин) КРОМга мурожаат қилиб, фойдаланувчи j билан махфий алоқа қилиш калитини сўрайди.

3. КРОМ махфий алоқа учун очиқ матннинг бирор қисмини ташкил этувчи Z_{ij} махфий калитни танлаб олади. Қолган қисмини i ва j фойдаланувчилар кўрсатилган “бош қисм” (“заголовок”) ёки “номланиш қисми” деб аталувчи бўлак ташкил этади. КРОМ бу очиқ матнни криптотизимда қабул қилинган шифрлаш алгоритмига кўра Z_i ва Z_j калитлар билан шифрлаб, умумий алоқа тармоғи оркали Z_i калит билан шифрланган криптограммани i фойдаланувчига ва Z_j калит билан шифрланган криптограммани j фойдаланувчига жўнатади.

4. Олинган криптограммаларни i ва j фойдаланувчилар дешифрлаб, кейинги олинган маълумотларни дешифрлашнинг махфий калитига эга бўладилар.

Калитларни тақсимлашнинг бундай протоколи оддий бўлиб, унинг бардошлилиги шифрлаш алгоритмининг бардошлилиги билан белгиланади. Ҳақиқатдан ҳам 3-бандда (қадамда) келтирилганидек, криптотаҳлилчига ҳар хил калитлар билан шифрланган бир хил очиқ матннинг криптограммаси маълум бўлиб, бундай ҳолат унга криптотаҳлил қилишда қўл келади. Шундай қилиб, очиқ матнни шифрлаш алгоритми криптотаҳлилга бардошли бўлса, калитларни тақсимлаш протоколи ҳам бардошли бўлади. Бу ерда шуни ҳам унутмаслик керакки, калитларни тақсимлашда шифрлаш алгоритмидан фойдаланиш шу тақсимлаш протоколининг бузилишига, криптобардошсизликка ва шу каби номутаносибликларга олиб келмаслиги керак.

Назорат саволлари

1. Ошкора калитли криптотизимларнинг асосий хусусиятлари нималарда намоён бўлади?
2. Бир томонлама функцияларга таъриф беринг?
3. Бир томонлама функцияларнинг қандай турларини биласиз?
4. Ошкора калитли криптотизимлар симметрик криптотизимлардан фарқли қандай масалаларни ечишга қодир?
5. Очиқ калитли криптотизимлар қандай мураккабликларга асосланади?
6. Қандай калитлар бардошли калитлар дейилади?
7. Қандай калитлар бардошсиз ҳисобланади?
8. Тасодифийликка текширувчи қандай тестларни биласиз?
9. Бир томонлама функцияларга асосланган псевдотасодифий кетма-кетлик ишлаб чиқарувчи генераторлардан қайсиларини биласиз?
10. Сонлар назарияси муаммоларига асосланган генераторлардан қайсиларини биласиз?
11. Тақсимотни тасодифийликка текширишнинг “Хи-квадрат” мезонидан қандай фойдаланилади?
12. Симметрик шифрлаш алгоритмлари учун махфий калитни тасодифийликка текшириш қандай амалга оширилади?

13. Калитлар очиқ тақсимланиш алгоритмининг математик асоси ҳақида нималарни биласиз?

14. Криптотизим фойдаланувчилари учун калитларни тақсимлаш протоколини мисоллар ёрдамида тушунтириб беринг?

15. Факторлаш мураккаблигига асосланган носимметрик шифрларни мисоллар билан тушунтиринг?

16. Чекли майдонларда дискрет логарифмлаш масаласининг ечими мураккаблигига асосланган носимметрик шифрларга мисоллар келтиринг?

17. Эллиптик криптографиянинг юзага келиши ҳақида нималарни биласиз?

18. ЭЭЧ группасида дискрет логарифмлашга асосланган криптотизимларни тушунтиринг?

19. ЭЭЧ нуқталари группаси асосида яратилган носимметрик шифрларнинг умумий функционал модели ҳақида нималарни биласиз?

20. Параметрли группадан фойдаланишга асосланган носимметрик шифрларни мисоллар билан тушунтиринг?

21. Параметрли шифрлаш усули деб қандай усулга айтилади?

22. Матрицавий параметрли шифрлаш усулини тушунтириб беринг?

23. Эллиптик эгри чизиқлардан фойдаланишга асосланган параметрли шифрлаш усули ҳақида нималарни биласиз?

24. RSA шифрига аналог параметрли шифрлаш усулини тушунтириб беринг?

6. АУТЕНТИФИКАЦИЯ ВА ЭЛЕКТРОН РАҚАМЛИ ИМЗО АЛГОРИТМЛАРИ

6.1. Аутентификация протоколлари

Аутентификация протоколи аутентификация процедураси бўлиб, унда бир-бири билан ўзаро мулоқотга киришаётган икки томондан бири (ёки иккаласи ҳам) бошқасининг ҳақиқийлигини текширади.

Аутентификацияни уч турга ажратиш мумкин: маълумотлар манбаи аутентификацияси (data – origin authentication), моҳият аутентификацияси (entity authentication) ва аутентификацияланган калитларни генерациялаш (authenticationed key establishment). Аутентификациянинг биринчи тури маълумотнинг эълон этилган хоссасини текширишни билдиради, иккинчиси кўпроқ эътиборни маълумот жўнатувчи ҳақидаги хабарларнинг ҳақиқийлигига қаратади, учинчиси эса махфий маълумотлар алмашиш учун ҳимояланган каналнинг ташкил этиш учун мўлжалланган [50].

Маълумотлар манбаи аутентификацияси

Маълумотлар манбаи аутентификацияси (авваллари, маълумотлар аутентификацияси (message authentication) деб ҳам аталиб келинган) маълумотлар яхлитлиги билан узвий боғланган. Зеро, атайлаб ўзгартирилган ахборотни қабул қилиб олишдаги таваккалчилик (хавфи) ишончли бўлмаган манбадан ахборот қабул қилиш таваккалчилигига (хавфига) яқин. Аммо аслида маълумотлар манбаи аутентификацияси ва маълумотларни етишмаслигидан ҳимоялаш тушунчалари фарқли тушунчалардир. Чунки маълумотлар манбаи аутентификацияси албатта алоқа канали билан боғлиқ ҳолда қаралиб, манба идентификацияси (манбани унинг идентификатори (номи, символларнинг ноёб сатри) бўйича аниқлаш жараёни) ва маълумотларнинг янгилиги билан алоқадор бўлса, маълумотлар яхлитлигини ҳимоялашда айтилган белгилар асосий эмас.

Маълумотлар манбаи аутентификацияси қуйидаги амалларни бажаришни назарда тутади [70].

1. Маълумот уни қабул этувчига шундай тарзда жўнатиладики, маълумотнинг ҳақиқийлигини уни қабул қилишдан аввал текшириб чиқишга имконият бўлсин.

2. Маълумот жўнатувчисини идентификациялаш.

3. Жўнатувчи юборган маълумотларнинг яхлитлигини текшириш.

4. Маълумот жўнатувчисининг кимлигини (реаллигини) текшириш.

Моҳият аутентификацияси

Моҳият аутентификацияси ахборот алмашув жараёни, яъни протоколи бўлиб, унинг давомида фойдаланувчи бошқа фойдаланувчининг ҳақиқийлигига (lively correspondence) амин бўлади.

Аслида аутентификация протоколи давомида маълумотнинг ҳақиқийлиги ёки ҳақиқий эмаслиги аён бўлади. Бундай ҳолларда маълумот ва уни муаллифининг ҳақиқийлигига ишонч ҳосил қилиш учун маълумотлар манбаи аутентификацияси механизмларидан фойдаланиш лозим.

Тармоқланган тизимларда қуйидаги моҳият аутентификацияси сценарийлари амал қилади. Улардан иккитасига тўхталамиз.

Иккита бош компьютерлараро маълумотлар алмашув (host-host type).

Протокол иштирокчилари компьютерлар бўлиб, улар тармоқланган тизимнинг тугунлари ёки платформалари деб юритилади. Компьютерлар иши ўзаро мослашган бўлиши зарур. Масалан, агар узоқлашган платформалардан бири “қайта юкланмоқчи бўлса” (такрорий инициализацияланиш), у ҳақиқий серверни идентификация қилиши лозим ва унга керакли ахборотни жўнатиши лозим, масалан, операцион тизимнинг ҳақиқий нусхасини, таймерни ёки атроф-муҳитни тўғри ўрнатиш. Ахборот ҳақиқийлигини аниқлаш одатда аутентификация протоколи ёрдамида амалга оширилади. Қоида тарзида, икки бош компьютерлараро маълумотлар алмашув клиент-сервер тизими сифатида бўлиб, бирига (клиент) иккинчиси (сервер) томонидан хизмат кўрсатилади.

Фойдаланувчи ва бош компьютерлараро маълумотлар алмашинуви (user-host type). Фойдаланувчи бош компьютерда рўйхатдан ўтиб, компьютер тизимига киришга рухсат олади. Одатда мижоз бош компьютерда тармоққа узоқдан кириш (telnet) орқали рўйхатдан ўтади ёки ўз файлини файл узатиш протоколига (ftp -file transfer protocol) мувофиқ бош компьютерга жўнатади. Иккала ҳолда ҳам паролни аутентификациялаш протоколи ишга тушади. Айрим ҳолларда, масалан, кредит карточкалар бўйича тўловларда, ўзаро аутентификациялаш (mutual authentication) зарур бўлади.

Субьект ўзининг ҳақиқийлигини тасдиқлаш учун тизимга турли маълумотларни тақдим этиши мумкин, масалан, пароль, шахсий идентификация коди, шахсий калит билан шифрланган хабар, смарт-карта, биометрик белги, бармоқ изи, сўровга жавоб, рақамли сертификат ва имзо ва шунга ўхшашлар [50].

Одатда ахборот алмашувчи томонлар мулоқотни янада юқсакроқ поғонага кўтариш мақсадида моҳият аутентификацияси протоколини ишга туширадилар. Замонавий криптографияда ҳимояланган алоқа каналларини ташкил этишда криптографик калитлардан фойдаланилади. Бинобарин, моҳият аутентификацияси протоколи ҳимояланган алоқа каналлари орқали ахборот алмашиш учун таркибий қисм сифатида **аутентификацияланган калитларни генерациялаш** ёки **калит алмашиш (**key exchange**)** ёки **калитларни мувофиқлаштириш** (key agreement) механизмларини ўз ичига олиши лозим.

Аутентификацияланган калитларни генерациялаш протоколида протокол маълумотлари ўзида калитлар параметрларини акс эттиргани боис, уларнинг манбаини ҳам аутентификациядан ўтказиш лозим.

Адабиётларда аутентификацияланган калитларни генерациялаш протоколи, моҳият аутентификацияси протоколи, маълумотларни ҳимоялаш протоколи, ҳаттоки криптографик протоколлар ҳам кўпинча алоқа протоколлари деб номланади.

Аутентификация протоколлари қуйидаги турларга бўлинади:

1. Пароллар ва рақамли сертификатлардан фойдаланишга асосланган аутентификация протоколлари.

2. Криптографик усуллар ва воситаларга асосланган қатьий аутентификация протоколлари.

3. Йўқ (ноллик) билим билан исботланадиган аутентификация протоколлари.

4. Биометрик аутентификация протоколлари.

Қуйида қатьий аутентификация протоколларидан бири сифатида сертификат ва электрон рақамли имзодан фойдаланишга асосланган аутентификация протоколи баён этилган [70].

Халқаро X.509 стандарти ЭРИ, вақт белгиси ва тасодифий сонлардан фойдаланиб, қуйидаги бир томонлама аутентификациялаш протоколларини тавсия этади.

Фойдаланувчи B томонидан фойдаланувчи A ни бир томонлама аутентификациялаш.

1. Фойдаланувчи A ўз шахсий калити билан шифрматн $S_A(t_A, B)$ ни шакллантиради ва уни ўз ичига олган қуйидаги хабарни фойдаланувчи B манзилига жўнатади:

$$A \to B: cert_A, t_A, B, S_A(t_A, B),$$

бу ерда → - жўнатма йўналиши белгиси, $cert_A$ - фойдаланувчи A нинг сертификати, B - фойдаланувчининг идентификатори, t_A - вақт белгиси.

Фойдаланувчи B хабар $(cert_A', t_A', B', S_A'(t_A, B))$ ни олгандан сўнг $cert_A$‘ даги ошкора калитдан фойдаланиб шифрматн $S_A'(t_A, B)$ ни t_A, B га айлантиради ва уларни хабардаги вақт белгиси t_A’, ўзининг идентификатори B' билан таққослайди. Агар таққосланувчи қийматлар тенг бўлмаса, унда A ҳақиқий эмас, акс ҳолда ҳақиқий деган хулоса чиқарилади ва кейинги қадамга ўтилади.

2. Фойдаланувчи B r_B ни генерациялаб A га жўнатади:

$$B \to A: r_B.$$

Фойдаланувчи A r_B ни қабул қилиб ўзига тегишли тасодифий сон r_A ни генерациялайди ва шифрматн $S_A(r_A,\ r_B,\ B)$ ни ўз ичига олган қуйидаги хабарни фойдаланувчи B га жўнатади:

$$A \to B: cert_A,\ r_A,\ B,\ S_A(r_A,\ r_B,\ B),$$

бу ерда, r_A, r_B мос тарзда A ва B генерациялаган тасодифий сонлар.

Фойдаланувчи B хабар $(cert_A',\ r_A',B',S_A'(r_A,\ r_B,\ B))$ ни олгандан сўнг $cert_A$‘ даги ошкора калитдан фойдаланиб шифрматн $S_A'(r_A,\ r_B,\ B)$ ни $r_A,\ r_B,\ B$ га айлантиради ва уларни хабардаги r_A', ўзи жўнатган r_B ва ўзининг идентификатори B' билан таққослайди. Агар таққосланувчи қийматлар тенг бўлмаса, унда A ҳақиқий эмас, акс ҳолда ҳақиқий деган хулоса чиқарилади.

Фойдаланувчилар А ва В томонидан икки томонлама аутентификациялаш қуйидаги жўнатмалар кетма-кетлигидан иборат :

$$B \to A: r_B.$$

$$A \to B: cert_A,\ r_A,\ B,\ S_A(r_A,\ r_B,\ B),$$

$$B \to A: cert_B,\ A,\ S_B(r_A,\ r_B,\ A),$$

Процедура тасодифий сонларни генерациялаш ва уларни томонларга тегишли идентификаторлар билан биргаликда шахсий калит билан шифрлаш ва шифрматнларни ошкора калит билан очиш ва натижаларни таққослаш амалларини бажариш натижасида томонларнинг ҳақиқий ёки аксинчалиги ҳақида хулоса чиқаришни назарда тутади.

6.2. Электрон рақамли имзо

Электрон рақамли имзо ахборот-коммуникация тармоғида алмашинадиган ҳужжатли маълумотлар ва уларнинг манбаларини ҳақиқий ёки ҳақиқий эмаслигини аниқлаш масаласини, яъни маълумотлар аутентификацияси масаласининг ечимини таъминловчи криптографик восита ҳисобланади.

Ҳар қандай қоғозли ёзма хат ёки ҳужжатнинг охирида шу ҳужжатни тузувчиси ёки тузиш учун жавобгар бўлган шахснинг имзоси бўлиши табиий ҳолдир. Имзо қуйидаги иккита мақсаддан келиб чиқиб қўйилади. Биринчидан, маълумотни олган томон ўзида мавжуд имзо намунасига олинган маълумотдаги имзони солиштириб, имзонинг ҳақиқий ёки сохталигига кўра шу маълумотнинг ҳақиқий ёки сохта эканлигини аниқлайди. Иккинчидан, шахсий имзо маълумот ҳужжатининг юридик мақомини таъминлайди. Бундай кафолат эса савдо–сотиқ, ишончнома, мажбурият ва шу каби битимларда алоҳида муҳимдир.

Қоғозли ҳужжатларга қўйилган шахсий имзоларни сохталаштириш нисбатан мураккаб. Чунки шахсий имзо фақат унинг муаллифи тафаккурининг ўзига хос бўлган кўпқиррали томонлари маҳсулидир. Шунинг учун бундай имзо муаллифини ҳозирги замонавий илғор криминалистика услубларидан фойдаланиш орқали аниқлаш мумкин.

Ахборот-коммуникация тармоғида алмашинадиган электрон ҳужжатли маълумотлар ҳам қоғозли ҳужжат алмашинувидаги анъанавий шахсий имзо вазифасини бажарувчи каби электрон рақамли имзо билан таъминланиб, электрон ҳужжат ва унинг манбасини ҳақиқий ёки ҳақиқий эмаслигини аниқлаш масаласи ечимини ҳал этилишини талаб этади.

6.2.1. Электрон рақамли имзо алгоритмларининг умумий криптографик хоссалари

Электрон рақамли имзо қоғозли ҳужжат алмашинувидаги анъанавий шахсий имзо хусусиятларидан фарқли бўлиб, иккилик саноқ тизими хусусиятлари билан белгиланадиган хотира регистрлари битларига боғлиқ. Хотира битларининг маълум бир кетма-кетлигидан иборат бўлган электрон имзони кўчириб бирор жойга қўйиш ёки ўзгартириш компьютерлар асосидаги алоқа тизимларида мураккаблик туғдирмайди.

Бугунги юқори даражада ривожланган бутун дунё цивилизациясида ҳужжатлар, жумладан махфий ҳужжатларнинг ҳам, электрон кўринишда ишлатилиши ва алоқа тизимларида узатилиши кенг қўлланилиб борилаётганлиги электрон ҳужжатлар ва электрон имзоларнинг ҳақиқийлигини аниқлаш масалалари ечимларининг муҳимлигини келтириб чиқармоқда.

Электрон рақамли имзо алоқа тизимларида бир неча тур қоида бузилишларидан муҳофаза қилинишни таъминлайди, яъни:

- фойдаланувчи (Б) томонидан қабул қилиб олинган электрон ҳужжатга қўйилган рақамли имзонинг ҳақиқий ёки ҳақиқий эмаслигини фақат (А) - фойдаланувчининг очиқ калити билан таъминланган шахсий калит фақат ўзидан бошқа шахсга маълум бўлмаслиги, маълумотни фақат (А) - фойдаланувчи томонидан жўнатилганлигини рад этиб бўлмайди;
- қонунбузар (рақиб томон) шахсий калитни билмаган ҳолда модификациялаш, сохталаштириш, фаол модификациялаш, ниқоблаш ва бошқа шу каби алоқа тизими қоидаларининг бузилишига имконият туғдирмайди;
- алоқа тизимидан фойдаланувчиларнинг ўзаро боғлиқ ҳолда иш юритиши муносабатидаги кўплаб келишмовчиликларни бартараф этади ва бундай келишмовчиликлар келиб чиққанда воситачисиз аниқлик киритиш имконияти туғилади.

Кўп ҳолларда узатилаётган маълумотларни шифрлашга ҳожат бўлмай, уни электрон рақамли имзо билан тасдиқлаш керак бўлади. Бундай ҳолатларда очиқ матн жўнатувчининг ёпиқ калити билан шифрланиб, олинган шифрматн очиқ матн билан бирга жўнатилади. Маълумотни қабул қилиб олган томон жўнатувчининг очиқ калити ёрдамида шифрматнни дешифрлаб, очиқ матн билан солиштириши мумкин.

1991 йилда АҚШдаги Стандартлар ва Технологиялар Миллий Институти DSA рақамли имзо алгоритмининг стандартини DSS юқорида келтирилган Эль Гамал ва RSA алгоритмлари асосида яратиб, фойдаланувчиларга таклиф этган.

ЭРИ ахборот-коммуникация тармоғида электрон ҳужжат алмашинуви жараёнида қуйидаги учта масалани ечиш имконини беради:

- электрон ҳужжат манбасининг ҳақиқийлигини аниқлаш;

- электрон ҳужжат яхлитлигини (ўзгармаганлигини) текшириш;

- электрон ҳужжатга рақамли имзо қўйган субъектни муаллифликдан бош тортмаслигини таъминлаш.

Ҳар қандай ЭРИ алгоритми иккита қисмдан иборат бўлади:

– имзо қўйиш;

– имзони текшириш.

Имзо қўйиш муаллиф томонидан, фақат унга маълум бўлган шахсий калит билан амалга оширилади. Имзонинг ҳақиқийлигини текшириш эса исталган шахс томонидан, имзо муаллифининг очиқ калити билан амалга оширилиши мумкин.

Электрон коммуникациялар ва электрон ҳужжат алмашинуви ҳозирги кунда иш юзасидан бўладиган муносабатларнинг ажралмас қисми ҳисобланиб, ҳар қандай замонавий ташкилотни электрон ҳужжатлар алмашинуви ва Интернетсиз тасаввур қилиш қийин.

Интернет тармоғидан электрон ҳужжатлар алмашинуви асосида молиявий фаолият олиб боришда маълумотлар алмашинувини ҳимоя қилиш ва электрон ҳужжатнинг юридик мақомини таъминлаш биринчи даражали аҳамият касб этади.

Электрон ҳужжатли маълумот алмашинуви жараёнида ЭРИни қўллаш ҳар хил турдаги тўлов тизимлари (пластик карточкалар), банк тизимлари ва савдо соҳаларининг молиявий фаолиятини бошқаришда электрон ҳужжат алмашинуви тизимларининг ривожланиб бориши билан кенг тарқала бошлади.

Ҳозирда ЭРИ тизимини яратишнинг бир нечта йўналишлари мавжуд. Бу йўналишларни учта гуруҳга бўлиш мумкин:

1) очиқ калитли шифрлаш алгоритмларига асосланган;

2) симметрик шифрлаш алгоритмларига асосланган;

3) имзони ҳисоблаш ва уни текширишнинг махсус алгоритмларига асосланган рақамли имзо тизимларидир.

Очиқ калитли шифрлаш алгоритмларига асосланган ЭРИ тизимлари қуйидагича ташкил қилинади. Агар ахборот-коммуникация тармоғининг i - фойдаланувчиси j - фойдаланувчисига имзоланган электрон ҳужжат жўнатмоқчи бўлса, i -фойдаланувчи ўзининг махфий калити $k_i^{м}$ билан имзоланиши керак бўлган ҳужжатнинг ўзини шифрлаб ёки унинг хэш қийматини шифрлаб, шу ҳужжат билан биргаликда жўнатади. Бу электрон ҳужжатни қабул қилиб олган j - фойдаланувчи, шифрланган маълумотни i - фойдаланувчининг очиқ калити k_i^{o} билан дешифрлаб, ҳосил бўлган матнни ҳужжат матнига ёки унинг хэш қийматига солиштиради. Агар матнлар билан хэш қийматлар бир хил бўлса, имзо ҳақиқий, акс ҳолда ҳақиқий эмас деб қабул қилинади.

Симметрик шифрлаш алгоритмларига асосланган ЭРИ тизимлари қуйидагича ташкил этилади. i - фойдаланувчи бир вақтнинг ўзида i - фойдаланувчига ҳам, j - фойдаланувчига ҳам маълум бўлиб, бошқа фойдаланувчиларга маълум бўлмаган $k_{ij}^{м}$ - калит билан имзоланиши керак бўлган электрон ҳужжатни ёки унинг хэш қийматини шифрлаб, шу ҳужжат билан биргаликда жўнатади. Электрон ҳужжатни қабул қилиб олган j - фойдаланувчи, шифрланган маълумотни $k_{ij}^{м}$ - калит билан дешифрлаб, ҳосил бўлган матнни ҳужжат матнига ёки унинг хэш қийматига солиштиради. Агар матнлар билан хэш қийматлар бир хил бўлса, имзо ҳақиқий, акс ҳолда ҳақиқий эмас деб қабул қилинади. Бундай ЭРИ тизими бир марталик ҳисобланади, чунки $k_{ij}^{м}$ - калитдан иккинчи марта фойдаланиш имконияти электрон ҳужжатларни сохталаштириш имкониятини яратади. Бундай ҳолатга чек қўйиш учун электрон ҳужжат алмашинуви ишончли учинчи томон орқали амалга оширилиши мумкин: i-фойдаланувчи ўзига ва фақат ишончли учинчи томонга маълум бўлган калит $k_{i3}^{м}$ билан рақамли имзони амалга ошириб, имзоланган электрон ҳужжатни учинчи ишончли томонга жўнатади, учинчи томон имзонинг ҳақиқийлигини $k_{i3}^{м}$ - калит билан текшириб, агар ҳақиқий бўлса, j - фойдаланувчининг ўзига ва фақат ишончли учинчи томонга маълум бўлган калит $k_{j3}^{м}$ билан рақамли имзони амалга ошириб, имзоланган электрон ҳужжатни j - фойдаланувчига жўнатади. Бундай ЭРИ тизими фойдаланувчилар учун ноқулай бўлиб, кўплаб келишмовчиликларни келтириб чиқаради.

Амалда учинчи турдаги имзони ҳисоблаш ва уни текширишнинг махсус алгоритмларига асосланган ЭРИ тизимларидан кенг фойдаланилади.

Махсус ЭРИ алгоритмлари рақамли имзони ҳисоблаш ва имзони текшириш қисмларидан иборат. ЭРИни ҳисоблаш қисми имзо қўювчининг махфий калити ва имзоланиши керак бўлган ҳужжатнинг хэш қийматига боғлиқ бўлади. Имзони текшириш қисми имзо эгасининг очиқ калитига ва қабул қилиб олинган ҳужжатнинг хэш қийматига боғлиқ ҳолда амалга оширилади.

Махсус ЭРИ стандартлари туркумига:

1. Россия ЭРИ стандарти: ГОСТ Р 34.10-94 ва унинг эллиптик эгри чизиқда такомиллаштирилган варианти ГОСТ Р 34.10-2001;
2. Америка ЭРИ стандарти: DSA ва унинг эллиптик эгри чизиқда такомиллаштирилган варианти ECDSA -2000;
3. Ўзбекистон Республикаси стандарти: O‘z DSt 1092:2005; O‘z DSt 1092:2009;
4. Германия стандарти EC-GDSA [66, 71];
5. Корея стандарти EC-KCDSA [66, 71] алгоритмлари мисол бўла олади.

Электрон рақамли имзо битлар кетма-кетлигида ифодаланган бирор сондан иборат. Шунинг учун уни бошқа электрон ҳужжатларга кўчириш ёки ўзгартириш киритиш катта қийинчилик туғдирмайди. Шу сабабли электрон ҳужжат алмашинуви тизимида ЭРИни сохталаштиришнинг олдини олиш чора-тадбирлари – ЭРИ алгоритмининг электрон ҳужжатларни сохталаштиришга бардошлилиги масаласини ечиш талаб этилади.

ЭРИ алгоритмининг бардошлилиги қуйидаги учта масаланинг мураккаблиги билан аниқланади:

- *имзони сохталаштириш*, берилган ҳужжатга, махфий калитга эга бўлмаган ҳолда тўғри имзо ҳисоблаш;

- *имзоланган маълумотни ташкил этиш*, махфий калитга эга бўлмаган ҳолда тўғри имзоланган маълумотни топиш;

- *маълумотни алмаштириш*, бир хил имзога эга бўлган иккита ҳар хил маълумотни топиш.

Келтирилган ЭРИ алгоритмлари стандартлари бардошлиликлари дискрет логарифмлаш, ЭЭЧрационал нуқталари устида амаллар бажариш ва параметрли группа параметрини топиш масалаларининг мураккаблигига асосланган.

6.2.2. Очиқ калитли шифрлаш алгоритмларига асосланган электрон рақамли имзо алгоритмлари қўлланилишининг умумий математик модели

Ахборт-коммуникация тармоғининг махфий электрон ҳужжат алмашиш тизими носимметрик шифрлаш алгоритмидан иборат бўлганда ЭРИни очиқ калитли шифрлаш алгоритми асосида амалга ошириш мисол тариқасида кўриб ўтилади.

Криптотизимнинг i - фойдаланувчиси M - махфий маълумотни j - фойдаланувчига имзо қўйган ҳолда жўнатмоқчи бўлса, у ҳолда i - фойдаланувчи қуйдагиларни амалга ошириши керак:

1. Маълумот M тизим фойдаланувчиларининг барчасига маълум бўлган хэш-функция $h: X \to Y$ (бу ерда X - очиқ матнлар тўплами, Y - хэшлаш

натижасида ҳосил бўлган қиймат) билан қайд қилинган бит узунлигидаги ифодага сиқилади.

2. Маълумотнинг хэш қиймати $h(M)=H$ фақат i - фойдаланувчининг ўзига маълум бўлган махфий калитга $k_i^{м}$ боғлиқ бўлган бир томонлама функция E орқали шифрланади, яъни $E_{k_i^{м}}(h(M))=S$.

3. Сўнгра j - фойдаланувчининг очиқ калити k_j^o билан маълумот M ва S бирлаштирилган кенгайтирилган маълумот шифрланади, яъни $E_{k_j^o}(M \cup S)=E_{k_j^o}(M)\cup E_{k_j^o}(S)=E_{k_j^o}(M)\cup E_{k_j^o}\left(E_{k_i^{м}}(h(M))\right)=C_1 \cup C_2=C$.

4. Шифрланган маълумот C очиқ алоқа тармоғи орқали j - фойдаланувчига жўнатилади.

Шифрланган маълумотни олган j - фойдаланувчи, фақат унинг ўзига маълум бўлган махфий калит $k_j^{м}$ билан дешифрлашни амалга оширади, яъни

$$D_{k_j^{з}}(C)=D_{k_j^{з}}(C_1 \cup C_2)=D_{k_j^{з}}(C_1)\cup D_{k_j^{з}}(C_2)=D_{k_j^{з}}\left(E_{k_j^o}(M)\right)\cup D_{k_j^{з}}\left(E_{k_j^o}\left(E_{k_i^{з}}(h(M))\right)\right)=$$
$$=M \cup E_{k_i^{з}}(h(M)),$$

бу ерда ЭРИ ифодаси $E_{k_i^{м}}(h(M))$ ҳали дешифрланмаган.

5. Маълумот эгасини ва маълумотнинг ўзини ҳақиқийлигига ишоч ҳосил қилиш учун j - фойдаланувчи i - фойдаланувчининг очиқ калити k_i^o билан ЭРИ қисмини $E_{k_i^{м}}(h(M))$ дешифрлаб $h(M)$- ифодани олади, яъни

$$D_{k_i^o}\left(E_{k_i^{м}}(h(M))\right)=h(M).$$

6. Сўнгра j - фойдаланувчи дешифрлаш натижасида олган $D_{k_j^{м}}(C_1)$ очиқ маълумотни калитсиз хэш фунция билан хэшлайди $h\left(D_{k_j^{з}}(C_1)\right)$ ва ушбу $D_{k_i^o}\left(E_{k_i^{м}}(h(M))\right)=h(M)$ таққослаш билан имзонинг тўғрилигига ишонч ҳосил қилиши мумкин, агарда $h\left(D_{k_j^{м}}(C_1)\right)=D_{k_i^o}\left(E_{k_i^{з}}(h(M))\right)=h(M)$ бўлса, акс ҳолда имзо нотўғри ҳамда электрон ҳужжат ҳақиқий бўлмайди.

ЭРИ имзонинг тўғрилиги маълумотнинг ўзини, унинг муаллифини ва манбасининг ҳақиқийлигини кафолатлайди.

Таъкидлаш жоизки, 1-6-бандлар носимметрик криптотизимларда маълумот алмашинувчи томонларнинг ЭРИ протоколини ифодалайди. Криптографик протокол деб, икки ва ундан ортиқ томонлар қатнашган ҳолда махфий маълумот алмашинуви жараёнида томонларнинг ўз вазифаларини бажариши кетма-кетлиги тушунилади.

Қуйида очиқ калитли шифрлаш алгоритмларига асосланган ЭРИ алгоритмлари кўриб ўтилади.

6.2.3. RSA очиқ калитли шифрлаш алгоритми асосидаги электрон рақамли имзо

Тизимнинг ҳар бир i- фойдаланувчиси (e_i, d_i)- калитлар жуфтлигини яратади. Бунинг учун етарли катта бўлган p ва q-туб сонлари олиниб (бу сонлар махфий тутилади), $n = pq$ -сони ва Эйлер функциясининг қиймати $\varphi(n) = (p-1)(q-1)$ ҳисобланади (бу сон ҳам махфий тутилади). Сўнгра $(e_i, \varphi(n)) = 1$ шартни қаноатлантирувчи, яъни $\varphi(n)$- сони билан ўзаро туб бўлган e_i -сон бўйича d_i-сони ушбу $e_i d_i = 1 \bmod \varphi(n)$ формула орқали ҳисобланади. Бу ($e_i; d_i$) –жуфтликда e_i - очиқ калит ва d_i- махфий (шахсий) калит деб эълон қилинади.

Шундан сўнг i -фойдаланувчидан j -фойдаланувчига шифрланган маълумотни имзолаган ҳолда жўнатиши қуйидагича амалга оширилади:

1. Шифрлаш қоидаси: $M^{e_j} \bmod n = C$, бу ерда M -очиқ маълумот, C – шифрланган маълумот;

2. Дешифрлаш қоидаси: $C^{d_j} \bmod n = M^{e_j d_j} \bmod n = M$;

3. ЭРИни ҳисоблаш: $H(M)^{d_i} \bmod n = P_i$,

бу ерда i -фойдаланувчининг P_i -имзоси M -маълумотнинг $H(M)$- хэш функция қиймати бўйича ҳисобланган;

4. ЭРИни текшириш: $(P_i)^{e_i} \bmod n = H(M)^{e_i d_i} \bmod n = H(M)$, агар $H(M) = H(M_1)$ бўлса (бу ерда M_1 -дешифрланган маълумот), у ҳолда электрон ҳужжат ҳақиқий, акс ҳолда ҳақиқий эмас, чунки хэш функция хоссасига кўра $M = M_1$ бўлса, уларнинг хэш қийматлари ҳам тенг бўлади.

5. Маълумотни махфий узатиш протоколи:

$\left[M \cup H(M)^{d_i}\right]^{e_j} \bmod n = \left[M \cup P_i\right]^{e_j} \bmod n = C$;

6. Махфий узатилган маълумотни қабул қилиш протоколи:

$C^{d_j} \bmod n = \left[M \cup P_i\right]^{e_j d_j} \bmod n = M \cup P_i$, умуман қараганда дастлабки маълумот ўзгартирилган бўлиши мумкин, шунинг учун $C^{d_j} \bmod n = M_1 \cup P_i$ бўлиб, натижада хэш қиймат имзо бўйича ушбу ифода $(P_i)^{e_i} \bmod n = H(M)^{e_i d_i} \bmod n = H(M)$ билан ҳисобланади ва қабул қилиб олинган маълумотнинг хэш қиймати $H(M_1)$ бўлса, у ҳолда $H(M) = H(M_1)$ бўлганда электрон ҳужжат ҳақиқий, аксинча бўлса, сохта ҳисобланади.

6.2.4 Эль Гамал очиқ калитли шифрлаш алгоритми асосидаги электрон рақамли имзо

Эль Гамал очиқ калитли шифрлаш алгоритмига асосланган криптотизимнинг ҳар бир i- фойдаланувчиси учун очиқ ва махфий калитлар генерацияси қуйидагича амалга оширилади, очиқ эълон қилинадиган p_i- туб сон (ёки фойдаланувчилар гуруҳи учун умумий бўлган p -туб сон) танланади, ушбу $g_i < p_i$ (ёки фойдаланувчилар гуруҳи учун $g < p$) шартни қаноатлантирувчи g_i (ёки фойдаланувчилар гуруҳи учун g) сони танланади, ушбу $y_i = g^{x_i} \bmod p_i$ (p -умумий бўлганда $y_i = g^{x_i} \bmod p$, $x_i < p$) формула билан x_i - махфий калит бўйича y_i сони ҳисобланади. Шундай қилиб, (p_i, g_i, y_i)- параметрлар бирикмаси (умумий p ва g учун (p, g, y_i) - параметрлар бирикмаси очиқ калитни ташкил этади, махфий калит x_i ҳисобланади.

Тизимда i -фойдаланувчидан j -фойдаланувчига шифрланган маълумотнинг имзоланган ҳолда жўнатилиши қуйидагича амалга оширилади:

1. **Шифрлаш қоидаси**: $a_j = g_j^k \bmod p_j$, $b_j = y_j^k M \bmod p_j$ (умумий p ва g лар учун $a = g^k \bmod p$, $b_j = y_j^k M \bmod p$), бу ерда k -тасодифий сон бўлиб маълумотни имзоловчи томонидан танланади, бу сон ($p_j - 1$) сони билан ўзаро туб $\mathrm{EKUB}(k, p_j - 1) = 1$ (p ва g умумий бўлганда EKUB(k , $p-1$) =1), M -очиқ маълумот, шифрланган маълумот $(a_j, b_j) = C$ (p ва g умумий бўлганда, $(a, b_j) = C$).

2. **Дешифрлаш қоидаси**: $\frac{b_j}{a_j^{x_j}} \bmod p_j = M$ (p ва g умумий бўлганда $\frac{b}{a^{x_j}} \bmod p = M$), ҳақиқатан ҳам $\frac{b_j}{a_j^{x_j}} \bmod p_j \equiv \frac{g_j^{x_i k} M}{g_j^{k x_i}} \bmod p_j \equiv M$ (p ва g умумий бўлганда $\frac{b}{a^{x_j}} \bmod p \equiv \frac{y_j^k M}{a^{x_j}} \bmod p \equiv \frac{g^{x_j k} M}{g^{k x_j}} \bmod p = M \bmod p = M$, $M < p$);

3. ЭРИни ҳисоблаш қоидаси: $a_i = g_i^{\,k} \bmod p_i$, b_i сони эса $M = (x_i a_i + k b_i) \bmod (p_i - 1)$ ёки $H(M) = (x_i a_i + k b_i) \bmod (p_i - 1)$ тенгламадан топилади, яъни $b_i = (M - a_i x_i) k^{-1} \bmod (p_i - 1)$ ёки $b_i = (H(M) - a_i x_i) k^{-1} \bmod (p_i - 1)$ (p ва g умумий бўлганда $a = g^k \bmod p$, b сони эса $M = (x_i a + kb) \bmod (p - 1)$ ёки $H(M) = (xa + kb) \bmod (p - 1)$ тенгламадан топилади, яъни $b = (M - a x_i) k^{-1} \bmod (p - 1)$ ёки $b = (H(M) - a x_i) k^{-1} \bmod (p - 1)$, EKUB $(k, p - 1) = 1$) $H(M)$ -маълумотнинг хэш қиймати, x_i -махфий калит, имзо сифатида a_i ва b_i жуфтлик, яъни $(a_i, b_i) = P_i$, (p ва g умумий бўлганда (a, b)) имзо деб қабул қилинади.

4. Имзони текшириш қоидаси:

Агар $y_i^{a_i} a_i^{b_i} \bmod p_i = g_i^M \bmod p_i$ ёки $y_i^{a_i} a_i^{b_i} \bmod p_i = g_i^{H(M)} \bmod p_i$ бўлса, у ҳолда электрон ҳужжат ҳақиқий, акс ҳолда сохта ҳисобланади. Чунки

$y_i = g_i^{x_i} \bmod p_i$ ва $a_i = g_i^{\,k} \bmod p_i$

тенгликлар ўринли бўлиб, Ферма теоремасига кўра ушбу айният ўринли:

$$y_i^{a_i} a_i^{b_i} \bmod p_i = (g_i^{x_i})^{a_i} (g_i^{k})^{b_i} \bmod p_i = g_i^{a_i x_i + k b_i} \bmod p_i = g_i^{d(p_i-1)+M} \bmod p_i =$$

$$= g_i^{d(p_i-1)} g_i^{M} \bmod p_i = (g_i^{(p_i-1)})^{d} \bmod p_i \cdot g_i^{M} \bmod p_i (\bmod p_i) =$$

$$= 1^d \bmod p_i \cdot g_i^{M} \bmod p_i (\bmod p_i) = g_i^{M} \bmod p_i;$$

5. **Маълумотни махфий узатиш протоколи**:

$$a_j = g_j^k \bmod p_j,\ b_j = y_j^k M' \bmod p_j = y_j^{k} [M \cup P_i] \bmod p_j,$$

$(a_j, b_j) = C$ - шифрмаълумот;

5. **Махфий узатилган маълумотни қабул қилиш протоколи:**

$$b_j / a_j^{x_j} \bmod p_j = M' = M \cup P_i,$$

умуман қараганда, дастлабки маълумот ўзгартирилган бўлиши мумкин, шунинг учун

$$b_j / a_j^{x_j} \bmod p_j = M' = M_1 \cup P_i,$$

бўлиб, $H(M_1)$ - хэш қиймат ҳисобланади. Агар $y_i^{a_i} a_i^{b_i} \bmod p_i = g_i^{M_1} \bmod p_i$ ёки $y_i^{a_i} a_i^{b_i} \bmod p_i = g_i^{H(M_1)} \bmod p_i$ бўлса, у ҳолда электрон ҳужжат ҳақиқий, акс ҳолда сохта ҳисобланади.

Очиқ калитли шифрлаш алгоритмлари битта (бир хил) электрон ҳужжатга ҳар хил ЭРИни қўйиш имкониятини бермайди. Бундай ҳолат эса битта электрон ҳужжатни ҳар хил томонларга битта имзоловчи томонидан ҳар хил ЭРИ билан юборилиш зарурати масаласи ечимини таъминламайди ва криптотаҳлилчига криптоҳужумни муваффақиятли амалга ошириш имкониятини беради. Бу масаланинг ечимини таъминлаш йўналишида олиб борилган илмий-тадқиқот ишлари махсус ЭРИ алгоритмларининг ишлаб чиқилиши билан амалга оширилди.

6.2.5. Махсус электрон рақамли имзо алгоритмларининг математик моделлари

Имзони ҳисоблаш ва уни текширишга асосланган махсус ЭРИ алгоритмлари туркумидаги DSA ва ГОСТ Р 34.10-94 стандарт алгоритмларининг асосини Эль Гамал шифрлаш алгоритми ташкил этади, яъни бу алгоритмлар бардошлилиги дискрет логарифмлаш масаласи ечимининг математик мураккаблиги билан таъминланган.

ЭЭЧ группасида тузилган ЭРИ схемаларининг [56-68] таҳлили шуни кўрсатадики, аввалги схемаларни (аслида, Эль Гамал схемалари модификацияларини) янгилари билан алмаштириш икки хил алгебраик структура – ЭЭЧ нуқталарининг чекли аддитив группаси ва чекли майдон $F(q)$ асосида амалга оширилган, бу ерда q – ҳосил қилувчи (генератор) нуқта G асосида юзага келган группанинг тартиби. Бунда майдоннинг чекли мультипликатив группаси элементлари устида даражага ошириш алгебраик амали ЭЭЧ нуқталари чекли аддитив группаси элементлари устида кўп марта қўшиш (скаляр сонга кўпайтириш) амали билан алмаштирилган. ЭРИ схемаларида чекли майдон элементлари устида бажариладиган амаллар ўзгармаган.

Шундай қилиб ЭЭЧ группасида ЭРИ алгоритмини шакллантириш учун қуйидаги алмаштиришларни амалга ошириш кифоя:

- чекли майдон генератор элементи g ни ЭЭЧнинг генератор элементи (нуқтаси) G билан;
- g элемент тартиби q ни G нуқта тартиби q билан;
- шахсий калит d ни шахсий калит d билан;
- ошкора калит $y=g^d \ (mod\ p)$ни ошкора калит $Y = [d]G$.

ЭЭЧ группасида ҳар қандай криптографик алгоритмни тузиш тизим параметрларини спецификациялашдан бошланиб, криптографик алгоритмни тузиш ва уни синаб кўриш билан якунланади.

6.2.6. Ўзбекистон Республикасининг электрон рақамли имзо бўйича давлат стандарти

Юқорида келтирилган ЭРИ алгоритмларининг асосий камчиликларидан бири, бузғунчи криптотизим асосига олинган муаммони етарлича аниқ қўя олганда ва унинг бу муаммони ҳал қилишга ресурслари етарлича бўлганда, қабул қилувчига келиб тушган рақамли имзо сохта бўлса, имзоловчи шахсда имзонинг сохталигини исботловчи далиллар ва маълумотларнинг йўқлигидир. Ўзбекистон миллий ЭРИ стандартини яратишда бу камчиликларни бартараф этишга эътибор берилди. Шу мақсадда криптография соҳасидаги Ўзбекистон Республикасининг дастлабки давлат стандарти O‘z DSt 1092:2009 «Ахборот технологияси. Ахборотнинг криптографик муҳофазаси. Электрон рақамли имзони шакллантириш ва текшириш жараёнлари»ни яратиш учун математик асос сифатида параметрли алгебра қабул қилинган. Унда модуль арифметикасининг яширин йўллар жуфтига эга бўлган ***бир томонлама (параметрли) функцияси*** қўлланилади, бунда ҳисоблашлар қийинлик даражаси бўйича даражага кўтариш амаллари каби енгил амалга оширилади, функцияни тескарилаш эса дискрет логарифм муаммосини ечиш жараёнидагидан кам бўлмаган ҳисоблаш сарфлари ва вақт талаб қилади. Анъанавий бир томонлама даражага кўтариш функцияси битта яширин йўлга эга бўлиб, у ушбу бир томонлама функциянинг хусусий ҳолидир. Унда яширин йўллар сонининг учта бўлиши мумкинлиги бардошлиликни ошириш учун қўшимча имкониятлар яратади.

O‘z DSt 1092:2009 «Ахборот технологияси. Ахборотнинг криптографик муҳофазаси. Электрон рақамли имзони шакллантириш ва текшириш жараёнлари»да қуйидаги параметрлардан фойдаланилади:

а) p - модуль, туб сон, бунда $p>2^{255}$. Бу соннинг юқори чегараси электрон рақамли имзо алгоритми муайян амалга оширилганда аниқланиши керак;

b) $q - p\text{-}1$ нинг фактори (туб кўпайтувчиси) бўлган туб сон, бу ерда $2^{254} < q < 2^{256}$.

c) R – параметр, $R<q$ шартни қаноатлантирувчи натурал сон; R параметри фойдаланувчиларнинг чекланган гуруҳи учун очиқ ёки биргаликдаги махфий калит бўлиши мумкин;

d) $m = H(\bullet)$ - хэш-функция, чекланган узунликдаги M хабарни 256 бит узунликдаги иккилик векторида акс эттиради.

ЭРИАнинг ҳар бир фойдаланувчиси қуйидаги шахсий калитларга эга бўлиши керак:

а) (x, u, g) – бутун сонлар учлиги – ЭРИнинг ёпиқ калити;

бу ерда: x, u – ёпиқ калитлар, $1<x$, $u<q$ шартларни қаноатлантирувчи тасодифий ёки псевдотасодифий генерацияланган бутун сонлар;

g – ёпиқ калит, $g \equiv h^{\backslash(p-1)/q}\ (mod\ p)$ ёрдамида ҳисобланадиган бутун сон;

бу ерда: $h<p$ – ёпиқ натурал сон бўлиб, ω нинг $1 \div q$ оралиқ қийматларида фақат $\omega=q$ бўлгандагина $g^{\backslash\omega}(mod\ p) \equiv 0$ шартни қаноатлантиради;

b) (y, z) - бутун сонлар жуфтлиги – ЭРИнинг очиқ калити;

бу ерда: y, z – очиқ калитлар, $y \equiv g^{\backslash x}(mod\ p)$ ва $z \equiv g^{\backslash\ u}\ (mod\ p)$ ифодалар ёрдамида ҳисобланади;

c) (R_1, y_1) – бутун сонлар жуфтлиги – ЭРИнинг сохталигини аниқлаш калити;

бу ерда: R_1 – назорат калити (очиқ ёки ёпиқ), $1 \div q\text{-}1$ оралиқда танлаб олинган; агар R_1 ёпиқ бўлса, унда R_1 имзоловчи шахс ва текширувчи томон учун биргаликдаги махфий калит бўлиши керак;

y_1 - сеанс (очиқ) калити, ҳар бир электрон рақамли имзо учун параметр билан даражага ошириш натижаси каби ҳисобланади.

Фойдаланувчилар гуруҳи учун p, q туб сонлари очиқ ва умумий, R эса биргаликдаги махфий бўлиши мумкин.

Стандартда имзоланган хабарни p-**NEW** схемаси бўйича тиклаш ғояси ва К. Шноррнинг имзо узунлигини қисқартиришга йўналтирилган ғоясидан ҳам фойдаланилган [2, 11].

Стандартда қўлланилган параметрли алгебра амаллари нафақат бир томонлама функцияни ҳосил этишда, балки ЭРИни шакллантириш ва унинг ҳақиқийлигини тасдиқлаш жараёнларида ҳам кенг қўлланилган.

Электрон рақамли имзони шакллантириш

1) Биринчи қисм

$$r \equiv m \circledR g^{\backslash -k} \ (mod\ p),$$

бу ерда: $m=H(M)$, $k=H(m \circledR x)$.

2) Иккинчи қисм

$$s \equiv u^{-1} * (k - r*x) \ (mod\ q).$$

3) Агар $\mu=1$, унда

$r_1 \equiv r \circledR R_1 \ (mod\ q),$

$x_1 \equiv (k - s*u*R_1) * r_1^{-1} \ (mod\ q),$

$y_1 \equiv g^{\backslash x1} \ (mod\ p).$

Бу ерда $\mu=0$ сеанс калитисиз иш режимини, $\mu=1$ сеанс калити билан ишлаш режимини белгилайди.

ЭРИнинг ҳақиқийлигини тасдиқлаш

1) ЭРИ аутентификацияси

$$m \equiv z^{\backslash s} \circledR y^{\backslash r'} \circledR r \ (mod\ p),$$

бу ерда: $m = H(M)$, $r' \equiv r \ (mod\ q)$.

2) Агар $\mu=1$ бўлса, унда ЭРИ сохталаштирилганлигини текшириш амалга оширилади;

$$(z^{\backslash s} \circledR y^{\backslash r'}) * R_1^{-1} \equiv (z * R_1^{-1})^{\backslash\backslash s*R1} \circledR' (y_1 * R_1^{-1})^{\backslash\backslash r1} \ (mod\ p).$$

Бу ерда: $\circledR$ - R параметр билан кўпайтириш амалининг белгиси;

$\circledR'$ - $R*R_1$ параметр билан кўпайтириш амалининг белгиси;

$^{\backslash}$ - R параметр билан даражага ошириш амалининг белгиси;

$^{\backslash\backslash}$ - $R*R_1$ параметр билан даражага ошириш амалининг белгиси.

Криптобардошлилиги даража параметри муаммосининг мураккаблигига асосланган ЭРИ криптотизимларини яратишга ҳам [11, 23] да тилга олинган умумий схема усулида ёндашув мақсадга мувофиқдир.

Дискрет логарифмлашнинг мураккаблигига асосланган схемаларнинг заиф томони шундаки, бадният криптотаҳлилчи дискрет логарифм муаммосини ҳал қилиш учун етарли ресурсларга эга бўлиб, уни сохталаштирган бўлса, унда сохта ЭРИ ҳам ҳақиқий деб қабул қилинади. Натижада қонуний ҳуқуққа эга фойдаланувчи томонларнинг ЭРИ сохталигини исботлаш имкониятлари йўққа чиқади. Бунинг олдини олиш йўлларидан бири ошкора калит ифодасида параметрли функциядан фойдаланишдир. Бунда ЭРИ криптотизимининг бардошлилиги даража параметри муаммосининг мураккаблиги билан белгиланади.

6.2.7 Эллиптик эгри чизиқларга асосланган электрон рақамли имзо алгоритмлари математик моделлари

Эллиптик эгри чизиқли дискрет логарифм муаммосининг мураккаблигига асосланган ЭРИ криптотизимларида жуда қисқа калитлар қўлланилади, аммо унинг ишончлилигини асослаб бериш анча мураккаб масаладир. Эллиптик эгри чизиқли дискрет логарифм муаммосининг дискрет логарифм муаммосига келтирилиши А. Менезис [45] томонидан кўрсатилган. Лекин эллиптик эгри чизиқли дискрет логарифм муаммосининг мураккаблигига асосланган ЭРИ алгоритмларида RSA алгоритмига кўра калитлар 100 марта тезроқ ҳосил қилинади ва анча кам жой эгаллайди. Масалан, 97 битли калитга эга бўлган шифрланган ахборотни бузишга уриниш 512 битли калитга эга бўлган RSA носимметрик шифрини бузишдан кўра икки марта қийинроқдир [2, 11].

Ҳозирги вақтда энг мураккаб ҳисобланган эллиптик эгри чизиқли дискрет логарифм муаммосига асосланган ЭРИ алгоритмлари қаторига ГОСТ Р 34.10-2001 билан бир қаторда халқаро стандарт мақомини олган

АҚШнинг ECDSA, Кореянинг EC-KCDSA, Германиянинг стандарти EC-GDSA киради.

2001 йилда Россияда ЭРИ учун янги ГОСТ Р 34.10-2001 стандарти шу вақтгача қўлланиб келинган ГОСТ Р 34.10-94 стандарти ўрнида фойдаланиш учун қабул қилинди ва бунга ЭРИ бардошлилигини оширишга бўлган зарурат сабаб бўлди. Бу стандартнинг бардошлилиги ЭЭЧнуқталари гуруҳида дискрет логарифмларни ҳисоблашнинг мураккаблигига ҳамда фойдаланиладиган хэш-функция - ГОСТ Р 34.11-94 [72] нинг бардошлилигига асосланади.

ЭРИ параметрларига қуйидагилар киради:

a) p туб сон – $p > 2^{255}$ тенгсизликни қаноатлантирувчи ЭЭЧ модули. Ушбу соннинг юқори чегараси ЭРИни муайян амалга ошириш жараёнида белгиланади;

b) ўзининг $J(E)$ инварианти ёки $a,\ b \in F_p$ коэффициентлари билан берилган E эллиптик эгри чизиқ;

d) w бутун сон - E ЭЭЧнуқталари группасининг тартиби;

e) t туб сон - қуйидаги шартлар бажарилган E ЭЭЧнуқталари группаси циклик қисм группасининг тартиби:

$$\begin{cases} \boldsymbol{w = lt, l \in Z, l \geq 1} \\ \boldsymbol{2^{254} < t < 2^{256}} \end{cases}$$

f) $(x_p,\ y_p)$ координатали ва $[t]N=0$ тенгликни қаноатлантирувчи E эллиптик эгри чизиқнинг $N \neq 0$ нуқтаси;

g) $m = H(M)$ – M хабарни 256 bit узунликдаги қаторда акс эттирувчи хэш-функция.

Юқорида келтирилган ЭРИА параметрларига қуйидаги талаблар қўйилади:

- барча бутун $i=1,2\ldots,\ B$ сонлар учун $p^i \neq 1\ (\mathrm{mod}\ t)$ шарт бажарилиши лозим, бу ерда B учун $B \geq 31$ тенгсизликни қаноатлантиради;

- $w \neq p$ тенгсизлик бажарилиши лозим;

- эгри чизиқ инварианти $J(E)\neq 0$ ёки 1728 шартларини қаноатлантириши лозим.

Алгоритмнинг ҳар бир фойдаланувчиси қуйидаги шахсий калитларга эга бўлиши керак:

a) ЭРИ ёпиқ калити d – $0<d<t$ тенгсизликни қаноатлантирувчи бутун сон;

b) ЭРИ очиқ калити T – (x_t, y_t) координатали, $[d]N=T$ тенгликни қаноатлантирувчи эллиптик эгри чизиқнинг нуқтаси.

$M\in V_\infty$ ахборотга ЭРИни шакллантириш жараёни алгоритми қуйидаги қадамлар кетма-кетлигини ўз ичига олади:

1-қадам: хабарнинг хэш-функциясини ҳисобланг: $m=H(M)$;

2-қадам: $e\equiv m \pmod t$ ни ҳисобланг. Агар $e=0$ бўлса, у ҳолда $e=1$ ни аниқланг;

3-қадам: ушбу $0 < k < t$ тенгсизликни қаноатлантирувчи тасодифий (псевдотасодифий) k бутун сонини генерация қилинг;

4-қадам: эллиптик эгри чизиқнинг $C=[k]N$ нуқтасини ҳисобланг ва $r=x_c \pmod t$ ни аниқланг, бу ерда x_c – C нуқтанинг x координатаси. Агар $r=0$ бўлса, у ҳолда 3-қадамга қайтинг;

5-қадам: $s\equiv (rd+ke) \pmod t$ ифоданинг қийматини ҳисобланг. Агар $s=0$ бўлса, 3-қадамга қайтинг;

6-қадам: r ва s ларни ЭРИ сифатида чиқишга беринг.

Ушбу жараён учун дастлабки (киришдаги) маълумотлар M хабар ва ЭРИнинг ёпиқ калити d, чиқиш натижаси бўлиб эса, (r, s) электрон рақамли имзо ҳисобланади.

Қабул қилиб олинган M ахборотидаги ζ рақамли имзо ҳақиқийлигини тасдиқлаш алгоритми қуйидаги қадамлар кетма-кетлигини ўз ичига олади:

1-қадам: агар $0 < r < t$, $0 < s < t$ тенгсизликлар бажарилса, навбатдаги қадамга ўтинг, акс ҳолда “имзо ҳақиқий эмас” қабул қилинади;

2-қадам: M хабар бўйича хэш-функцияни ҳисобланг: $m=H(M)$;

3-қадам: $e \equiv m (mod\ t)$ ни ҳисобланг. Агар $e=0$ бўлса, у ҳолда $e=1$ ни аниқланг;

4-қадам: $v \equiv e^{-1} (mod\ t)$ ифоданинг қийматини ҳисобланг;

5-қадам: ушбу $z_1 \equiv sv\ (\mathrm{mod}\ t),\ \ z_2 \equiv -rv\ (\mathrm{mod}\ t)$ ифодалар қийматларини ҳисобланг;

6-қадам: эллиптик эгри чизиқнинг $C=[z_1]N$ “+”$[z_2]T$ нуқтасини ҳисобланг ва $R \equiv x_c\ (\mathrm{mod}\ t)$ ни аниқланг, бу ерда x_c - C нуқтанинг x координатаси.

7-қадам: агар $R=r$ тенглик бажарилса, у ҳолда “имзо ҳақиқий”, акс ҳолда “имзо ҳақиқий эмас” қабул қилинсин.

Ушбу жараён учун дастлабки (киришдаги) маълумотлар бўлиб, имзоланган M хабар, $(r,\ s)$ электрон рақамли имзо ва ЭРИ очиқ калити, чиқиш натижаси бўлиб эса, мазкур ЭРИ ҳақиқийлиги ёки ҳақиқий эмаслиги ҳақидаги ахборот ҳисобланади.

ECDSA

АҚШнинг ЭРИ учун DSA нинг эллиптик эгри чизиқларга асосланган аналоги ECDSA 1992 йилда таклиф этилган ва 1998 йилда ISO (International Standart Organization) стандарти сифатида қабул қилинган. 1999 йилда эса ANSI X9.62 ECDSA стандарти сифатида, 2000 йилда федераль ва IEEE стандарти сифатида қабул қилинган [73].

Қуйида ECDSA бўйича ЭРИни шакллантириш ва унинг ҳақиқийлигини тасдиқлаш алгоритмлари келтирилган.

ECDSA бўйича ЭРИни шакллантириш алгоритми қуйидаги қадамлар кетма-кетлигини ўз ичига олади:

1) $k \in [1,\ n-1]$ тасодифий сони танланади;

2) $[k]P = (x_1,\ y_1)$ ҳисобланади;

3) $r \equiv x_1\ (mod\ n)$ ҳисобланади. Агар $r=0$ бўлса, k қайта танланади;

4) $e = H(M)$ хэш-функция ҳисобланади;

5) $s \equiv k^{-1}(e+dr)\ (mod\ n)$ ҳисобланади; бу ерда $(r,\ s)$ жуфтлиги M ахборотнинг электрон рақамли имзоси.

ECDSA бўйича ЭРИ ҳақиқийлигини тасдиқлаш алгоритми қуйидаги қадамлар кетма-кетлигини ўз ичига олади:

1) агар $r=0$ бўлса, имзо ҳақиқий эмас деб топилади;

2) $h = H(M)$ хэш-функция ҳисобланади;

3) $u_1 \equiv hs^{-1} \ (mod\ n)$ ҳисобланади;

4) $u_2 \equiv rs^{-1} \ (mod\ n)$ ҳисобланади;

5) $[u_1]P + [u_2]Q = (x_1, y_1)$ ҳисобланади;

6) $v \equiv x_1 \ (mod\ n)$ ҳисобланади.

Агар $v = r$ бўлса, имзо ҳақиқий, акс ҳолда ҳақиқий эмас деб топилади.

Қуйида халқаро стандарт сифатида қабул қилинган Корея, Германия эллиптик эгри чизиқларга асосланган электрон рақамли имзо алгоритмлари кўриб ўтилади.

EC-GDSA стандартида прототип сифатида GDSA танланган. Алгоритмда ЭРИни генерация қилишда дастлаб M хабар учун хэш-қиймат ҳисобланади, $1\leq k\leq q-1$ оралиқда k сони танланади, шундан сўнг кетма-кет ЭРИ элементлари ҳисобланади:

хэш-қиймат $e\equiv H(M)$, $(x_1, y_1)=[k]G$, $r \equiv x_1(mod\ q)$, $s\equiv (kr-e)d\ (mod\ q)$.

ЭРИни текшириш жараёнида аввало имзонинг узунлиги текширилади ва у тўғри бўлса, кетма-кет қуйидаги қийматлар ҳисобланади:

хэш-қиймат $e\equiv H(M)$, $u_1\equiv\ r^{-1}e(mod\ q)$, $u_2\equiv\ r^{-1}s\ (mod\ q)$ ва $X=[u_1]\ G\ "+"[u_2]Q=(x_X, y_X)$. u_1 ва u_2 қийматларни ҳисоблаш учун прототипда фойдаланилганидек тенгламадан фойдаланилади.

Германиянинг миллий алгоритмида очиқ калит Q Кореянинг миллий алгоритмидагидек $Q=[d^{-1}]G$ шаклга эга, бу ерда d – ЭРИ эгасининг тасодифий танланган шахсий калити, G - q тартибли асос нуқта. Бу эса ЭРИни шакллантириш жараёнини осонлаштиришга ёрдам беради ва имзони сохталаштиришни чеклаб қўяди. Имзони текширишда, агарда $x_x(mod\ q) \equiv r$ бўлса, у ҳолда имзо ҳақиқий, акс ҳолда ҳақиқий эмас.

EC-KCDSA стандартида прототип сифатида KCDSA танланган. Алгоритмда ЭРИни генерация қилишда ЭРИ эгасининг хэш-коди z дан фойдаланилади. Дастлаб M хабар билан конкатенация қилиш учун хэш-қиймат ҳисобланади, $1 \leq k \leq q-1$ оралиқда k сони танланади, шундан сўнг кетма-кет ЭРИ элементлари ҳисобланади:

хэш-қиймат $e=H(z||M)$, $(x_1, y_1)=[k]G$, $r = H([k]G)$, $w=r \oplus e$; агар $w \geq q$ бўлса , у ҳолда $w=w-q$ қабул қилинади; $s \equiv d\ (k-w)\ (mod\ q)$.

ЭРИни текшириш жараёнида аввало имзонинг узунлиги текширилади ва у тўғри бўлса кетма-кет қуйидаги қийматлар ҳисобланади:

хэш-қиймат $e=H(z||M)$; $w=r \oplus e$; агар $w \geq q$ бўлса, у ҳолда $w=w-q$ қабул қилинади; $X=[s]Q”+”[w]\ G =(x_X, y_X)$, бу ерда $s=d(k- w)(mod\ q)$, G –q тартибли асос нуқта (базовая точка), очиқ калит $Q = [d^{-1}]G$, бу ерда d – $1<d<q$ оралиқдаги шахсий махфий калит. Агар $H(x_x)=r$ бўлса, у ҳолда имзо ҳақиқий, акс ҳолда ҳақиқий эмас.

Кўриниб турганидек s ва w (u_1 ва u_2 аналоглари, мос равишда) бир-бирига ўзаро боғлиқдир, бундан ташқари w имзоланувчи хабар M ва r параметрнинг хэш-функция қиймати $e=H(z||M)$ га ҳам боғлиқ. Бу эса ECDSA-2000 ва ГОСТ Р 34.10-2001 алгоритмларидагидек криптографик самарани беради.

Бундан ташқари r параметр $[k]G=(x_1, y_1)$ нуқтанинг хэш-функция қиймати сифатида, яъни $r=H(x_x)$ каби ҳисобланади. Бу эса алгоритмда қўлланилган хэш-функция ҳисобига ЭРИ алгоритми бардошлилигини янада оширади, чунки x_1 – тасодифий сон сифатида фақатгина имзо қўядиган шахсга маълум. x_x – имзони текшириш алгоритми бўйича сертификатланган очиқ калитга боғлиқ ҳисобланади. Яъни тасодифий танланган номаълум x_1 параметр r ни шакллантиришда калитсиз хэш-функциянинг калити бўлиб ҳисобланади, x_x қиймати эса олдиндан номаълум ва имзони текшириш алгоритмининг якуний натижаси бўлиб ҳисобланади.

Назорат саволлари

1. Аутентификацияга таъриф беринг?
2. Аутентификация қандай турларга бўлинади?
3. Аутентификация протоколи нимага зарур?
4. Маълумотлар манбаи аутентификацияси қандай амалларни бажаришни назарда тутади?
5. Моҳият аутентификацияси ҳақида нималарни биласиз?
6. Аутентификацияланган калитларни генерациялаш қандай амалга оширилади?
7. Аутентификация протоколлари қандай турларга бўлинади?
8. Электрон рақамли имзога таъриф беринг?
9. Электрон рақамли имзо алгоритмларининг қандай умумий криптографик хоссаларини биласиз?
10. Қандай электрон рақамли имзо алгоритмларини биласиз?
11. Махсус ЭРИ стандартлари туркумига қандай алгоритмлар киради?
12. Электрон рақамли имзо алгоритмининг бардошлилиги қандай масалалар мураккаблиги билан аниқланади?
13. Очиқ калитли шифрлаш алгоритмларига асосланган ЭРИ алгоритмларининг қўлланилиши ҳақида нималарни биласиз?
14. RSA очиқ калитли шифрлаш алгоритми қандай қадамларни ўз ичига олади?
15. Эль Гамал очиқ калитли ЭРИ алгоритми қандай амалга оширилади?
16. Махсус ЭРИ алгоритмларининг математик моделлари ҳақида нималарни биласиз?
17. Ўзбекистон Республикаси стандарти: O‘z DSt 1092да қандай бир томонлама функциядан фойдаланилади?

18. O‘z DSt 1092 «Ахборот технологияси. Ахборотнинг криптографик муҳофазаси. Электрон рақамли имзони шакллантириш ва текшириш жараёнлари»да қандай параметрлардан фойдаланилади?

19. Эллиптик эгри чизиқларга асосланган электрон рақамли имзо алгоритмлари математик моделларини тушунтириб беринг?

ХУЛОСА

Минг йилликлар давомида криптографиядан давлат қурилишида, ҳарбий ва дипломатия алоқасини муҳофазалашда фойдаланиб келинган бўлса, ахборот асрининг бошланиши билан криптология жамиятда, хусусий секторда фойдаланиш учун ҳам зарур бўлиб қолди. Қарийб 35 йилдан буён криптологияда кенг миқёсда очиқ тадқиқотлар олиб борилмоқда. Ҳозирги кунда конфиденциал ахборот (масалан, юридик ҳужжатлар, молиявий, кредит ставкалари тўғрисидаги ахборотлар, касаллик тарихи ва шунга ўхшаш)ларнинг талай қисми компьютерлараро одатдаги алоқа каналлари орқали узатилмоқда. Жамият учун бундай ахборотнинг конфиденциаллиги ва асл ҳолда сақланиши заруратга айланган.

Криптография тарихида *биринчи муҳим воқеа* симметрик криптотизимларнинг биринчи марта Давлат стандарти мақомига эга бўлиши бўлса, кейинги ўн йилликларнинг *муҳим кашфиёти* криптологияга янгича ёндашувларни бошлаб берган ошкора криптографиянинг юзага келиб унинг муттасил ривожланиб бораётганлигидир.

АҚШдан кейин Европа давлатлари ва Японияда электрон рақамли имзо бўйича қонун ва дастлабки давлат стандартлари қабул этилди. Кўпчилик давлатлар, шу жумладан Ўзбекистон Республикаси ҳам криптография воситаларидан ахборот–телекоммуникация тармоқларида махфий ахборотларни хавфсиз узатиш ва электрон рақамли имзо яратишда ўз миллий алгоритмларидан фойдаланмоқдалар.

Ушбу ўқув қўлланмада криптография тарихи, криптографиянинг асосий математик тушунчалари, таърифлари, теоремалари ҳамда симметрик ва носимметрик криптографик алгоритмларнинг математик асослари баён этилган. Унда Ўзбекистон давлат стандартларини ишлаб чиқишга асос бўлган алебраик структуралар ва функциялар - диаматрицалар алгебраси, параметрли эллиптик эгри чизиқли функциялар ва уларнинг асосий хоссалари, ҳамда ишлаб чиқилган криптоалгоритмлар келтирилган.

Ушбу ўқув қўлланма ахборот хавфсизлиги ва криптография йўналишида давлат тилида таълим олаётган магистрлар учун мўлжалланган. Шунингдек ушбу ўқув қўлланмадан ахборот хавфсизлиги йўналишида бакалаврлар тайёрлаш жараёнида ҳамда криптография йўналишида илмий-тадқиқот олиб бораётган аспирант-тадқиқотчилар, илмий ходимлар ва соҳа мутахассислари фойдаланишлари мумкин.

ФОЙДАЛАНИЛГАН АДАБИЁТЛАР

1. 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.

2. Ахмедова О.П. Параметрлар алгебраси асосида носимметрик криптотизимлар яратиш усули ва алгоритмлари // Номзодлик диссертация иши, Тошкент-2007.

3. Бабаш А.В., Шанкин Г.П. История криптографии. Часть I. – Москва: Лори Гелиос АРВ, 2002. – 240 с.

4. Бабаш А.В., Шанкин Г.П., Криптография – Москва: Лори Гелиос АРВ, 2002. – 512 с.

5. Арипов М.М., Пудовченко Ю.Е. Основы криптологии – Ташкент: 2004. – 136 с.

6. Баричев С.Г., Серов Р.Е. Основы современной криптографии. Учебное пособие. – Москва: Лори Горячая Линия - Телеком, 2002. – 152 с.

7. Алексеев А. Криптогрфия и криптоанализ: вековая проблема человечества. http://www.nvkz.kuzbass.net/hard-soft/soft/other/kripto-analiz.html

8. Жельников В. Криптогоафия от папируса до компьютера. М.:ABF, 1996.

9. O‘z DSt 1109:2006 «Ахборот технологияси. Ахборотнинг криптографик муҳофазаси. Атамалар ва таърифлар».

10. История криптографии и криптоанализа. http://crypto hot box.ru.

11. Шнайер Б. Прикладная криптография. Протоколы, алгоритмы, исходные тексты на языке Си. –М.: издательство ТРИУМФ, 2003 - 816 с.

12. Коробейников А.Г., Гатчин Ю.А. Математические основы криптологии. Учебное пособие. Санкт-Петербург-2004.

13. Акбаров Д.Е. Ахборот хавфсизлигини таъминлашнинг криптографик усуллари ва уларнинг қўлланишлари. Тошкент. ”Ўзбекистон маркаси “, 2009. – 432 б.

14. «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.

15. Защита информации. Малый тематический выпуск. ТИИЭР, 1988 г, т.76, №5.

16. Kahn D. The codebreakers. N.-Y., 1967.

17. Саломаа А. Криптография с открытым ключом. М.,1997

18. Бабаш А.В., Гольев Ю.И., Ларин Д.А. Шанкин Г.П. О развитии криптографии в XIX веке. Защита информации. Конфидент. 2003 г. №5.

19. Бабаш А.В., Гольев Ю.И., Ларин Д.А. Шанкин Г.П. Криптографические идеи XIX века. Защита информации. Конфидент. 2004 г. №1, №2.

20. 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.

21. Михаил Масленников. Практическая криптография. Санкт-Петербург «БХВ-Петербург», 2003.

22. 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.

23. Хасанов Х.П. Такомиллашган диаматрицалар алгебралари ва параметрли алгебра асосида криптотизимлар яратиш усуллари ва алгоритмлари. – Тошкент, 2008. -208 б.

24. Шеннон К. Теория и связи в секретных системах. Работы по теории информации и кибернетике. – М.: Иностранная лит. 1963. – 243 б.

25. Нильс Фергюсон, Брюс Шнайер. Практическая криптография – Москва: "Диалектика", 2004 г. – 432 с.

26. Federal Information Processing Standards Publication 197. Advanced Encryption Standard (AES). 2001.

27. ГОСТ 28147-89. Государственный Стандарт Союза ССР. Системы обработки информации. Защита криптографическая. Алгоритм криптографического преобразования.

28. O‘z DSt 1105:2006 «Ахборот технологияси. Ахборотнинг криптографик муҳофазаси. Маълумотларни шифрлаш алгоритми».

29. Diffie, W., Hellman, M.E. New directions in cryptography // IEEE Transactionson Information Theory, vol. IT-22, 1976. – Pp. 644-654.

30. 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.

31. 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.

32. Rivest R. RSA chips (past/present/future) // Presented at Eurocrypt 84, Paris, France, 1984. – Pp. 9-11.

33. 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.

34. US Patent, Rivest, et al. Cryptographic communications system and method, 4.405.829, September 20, 1983.

35. Shamir, A. On the generation of cryptographically strong pseudo-random sequences // ACM Transactions on Computer Systems, vol. 1, 1983. – Pp. 38-44.

36. Shamir, A. A polynomial time algorithm for breaking the basic Merkle-Hellman cryptosystem // IEEE Transactionson Information Theory, vol. IT-30, 1984. – Pp. 699-704.

37. 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.

38. 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.

39. US Patent, Schnorr. Method for identifying subscribers and for generating and verifying electronic signatures in a data exchange system. 4.995.082. – 1991.

40. 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.

41. 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.

42. Koblitz N. and Vanstone S. The state of elliptic curve cryptography // Designs, Codes and Cryptography, 19 (2000). – Pp. 173-193.

43. Koblitz N. Elliptic Curve Cryptosystems // Mathematics of Computation, 48, 1987. – Pp. 203-209.

44. Коблиц Н. Введение в эллиптические кривые и модулярные формы // Пер с англ. – Москва: Мир, 1988. – 320 с.

45. Menezes A., van Oorschot P., Vanstone S. Handbook of Applied Cryptography // CRC Press, 1996. – 780 pp.

46. 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.

47. Шнайер Б. Слабые места криптографических систем // Открытые системы. – 1999, № 1. – С. 31-36.

48. O'z DSt 1092:2009 «Ахборот технологияси. Ахборотнинг криптографик муҳофазаси. Электрон рақамли имзони шакллантириш ва текшириш жараёнлари».

49. O'z DSt 1106:2009 «Ахборот технологияси. Ахборотнинг криптографик муҳофазаси. Хэшлаш функцияси».

50. Венбо Мао. Современная криптография. Теория и практика. – Москва - Санкт-Петербург - Киев: Лори Вильямс, 2005. – 768 с.

51. Хасанов Х.П. Такомиллаштирилган диаматрицалар алгебраси // Infocom.uz. – Тошкент, 2005, №9. – 68-70 б.

52. 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.

53. 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.

54. 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.

55. Хасанов Х.П. Криптографические системы на базе эллиптических кривых с параметром Ахборот-коммуникациялар: Тармоқлар – Технологиялар – Ечимлар. – Т.: №4, 2008.

56. Алгоритмические основы эллиптической криптографии / Болотов А.А. Гашков С.Б. Фролов А.В., Часовских А.А. – Москва МЭИ, 2000. – 100 с.

57. 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.

58. Асимметричная криптография на эллиптических кривых // Open PGP в России. – http: //www.pgpru.com.

59. Харин Ю.С., Берник В.И., Матвеев Г.В., Агиевич С.Г. «Математические и компьютерные основы криптологии» ООО «Новое знание» 2003 г. 381 стр.

60. Василенко О.Н. Теоретико-числовые алгоритмы в криптографии. – М., МЦНМО, 2003. – 328 с.

61. «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.

62. Кобец А.М. Подмена подписанного документа в новом американском стандарте ЭЦП ECDSA// http: www.bugtrag/ru.

63. 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.

64. Горбенко И.Д., Збитнев С.И., Поляков А.А. Криптоанализ криптографических преобразований в группах точек эллиптических кривых методом Полларда // Харьковский государственный технический университет радиотехники.

65. Горбенко И.Д., Балагура Д.С. Схемы направленного шифрования в группах точек на эллиптических кривых //Харьковский государственный технический университет радиотехники.

66. ISO/IEC 14888-3:2006. Information technology – Security techniques – Digital signatures with appendix.

67. ГОСТ Р 34.10-2001. Информационная технология. Криптографическая защита информации. Процессы формирования и проверки электронной цифровой подписи.

68. 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.

69. 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.

70. Ростовцев А.Г., Маховенко Е.Б. Теоретическая криптография. НПО «Профессионал», Санкт-Петербург. 2004г. - 478 стр.

71. Ғаниев С.К., Каримов М.М., Ташев К.А. Ахборот хавфсизлиги. Ахборот-коммуникацион тизимлар хавфсизлиги. Ўқув қўлланма. Т., “Aloqachi”. 2008, 382бет.

72. D. Hankerson, A. Menezes, S. Vanstone Guide to Elliptic Curve Cryptography. Springer-Verlag New York, Inc. 2004.

73. ГОСТ Р 34.11-94. Государственный Стандарт Российской Федерации. Информационная технология. Криптографическая защита информации. Функция хэширования.

74. IEEE P 1363, Standard Specifications for Public-Key Cryptography. February. 2000.

75. Акбаров Д.Е., Ахмедова О.П. Генерация стойких ключей для симметричных блочных алгоритмов шифрования. //Кимёвий технология назорат ва бошқарув, 5/2008, с. 29-32