ЎЗБЕКИСТОН РЕСПУБЛИКАСИ

АЛОҚА, АХБОРОТЛАШТИРИШ ВА ТЕЛЕКОММУНИКАЦИЯ ТЕХНОЛОГИЯЛАРИ ДАВЛАТ ҚЎМИТАСИ

ЎЗБЕКИСТОН ОЛИЙ ВА ЎРТА МАХСУС ТАЪЛИМ ВАЗИРЛИГИ

ТОШКЕНТ АХБОРОТ ТЕХНОЛОГИЯЛАРИ УНИВЕРСИТЕТИ ФАРҒОНА ФИЛИАЛИ

Қўлёзма ҳуқуқида
УДК 004.056.5

Қаюмов Ахрор Мўминжонович

ЭЛЬ-ГАМАЛ АССИММЕТРИК ШИФРЛАШ АЛГОРИТМИНИНГ КРИПТОГРАФИК ТАҲЛИЛИ ВА ҚЎЛЛАНИЛИШИ

5А330201 - Компьютер тизимлари ва уларнинг дастурий таъминоти (тармоклар бўйича)

Магистр академик даражасини олиш учун ёзилган
ДИССЕРТАЦИЯ

Илмий раҳбар
доцент Д. Е.Акбаров

Фаргона -2014

КИРИШ

Мавзунинг асосланиши ва унинг долзарблиги. Инсон тафаккури ривожининг манбаи маълумотлар (ахборотлар) мажмуидан иборатдир. Шак-шубҳасиз ўз вақтида олинган тўла ва ишончли маълумот, шу маълумот билан боғлиқ бўлган ҳолатдан келиб чиқадиган амалий фаолиятларнинг мақсадли кечишларини мувофиқлаштиришда муҳим аҳамият касб этади. Фаолият мақсадларининг турлича бўлиши табиий равишда ахборотлардан турли мақсадларда фойдаланиш асосларига сабаб бўлади. Шунинг учун бугунги, ахборотларни сақлаш ва узатиш тизимлари бир томондан такомиллашиб мураккаблашган ва иккинчи томондан ахборотлардан фойдаланувчилар учун кенг қулайликлар вужудга келган даврда, ахборотларни мақсадли бошқаришнинг қатор муҳим масалалари келиб чиқади. Бундай масалалар қаторига катта ҳажмдаги ахборотларнинг тез ва сифатли узатиш ҳамда қабул қилиш, ахборотларни ишончлилигини таъминлаш, ахборотлар тизимида ахборотларни бегона шахслардан (кенг маънода) муҳофаза қилиш каби кўплаб бошқа масалалар киради. Ахборот ва ахборот тизимидан фойдаланиш инсоният фаолиятининг барча соҳаларига кириб бориб, муҳим аҳамият касб этиб, ривожланиб бораётган бугунги жамиятда ахборотларни мақсадли бошқариш фаоллашмоқда. Компьютерлар ва компьютер тизимлари ахборот тизимининг муҳим бўғимидир. ИНТЕРНЕТ тармоқлари жамият фаолиятининг барча соҳаларини қамраб олиб, ахборотни тез ва сифатли алмашинувини таъминлаш технологияларининг ривожланишига ижобий манба бўлиб келмокда. Юқоридаги келтирилган асосли мулоҳазалардан келиб чиқиб, ахборотларни асли ҳолидан ўзгартирилган ҳолда, яъни шифрланган ҳолда, сақлаш ва узатиш масалаларининг муҳим эканлигига шубҳа йўқдир.

Ахборот-коммуникация тизимларида маълумотлар алмашинувини самарали амалга оширишни ташкил этиш бугунги ривожланган жамиятда катта аҳамият касб этади. Ахборот технологияларининг жадал ривожланиб

бориши, жамият фаолиятининг кенг соҳасида турли ахборот хизматларининг вужудга келишига олиб келди. Айниқса банк ва бошқа тўлов тизимларида, давлат ва жамият манфаатлари билан боғлиқ муҳим маълумотларни алмашиш ҳамда таҳлил қилишда, тез ва ишончли маълумот алмашинуви талаб этиладиган тизимларда ахборот муҳофазаси масалалари долзарб ҳисобланади. Ҳақиқатан ҳам, ҳар қандай маълумот у ёки бу маънода ахборот-коммуникация тизими фойдаланувчиларининг манфаати билан боғлиқ. Ахборот муҳофазасини таъминлаш: ҳуқуқий-меъёрий ҳужжатлар, техник воситалар ва криптографик алгоритмлар ҳамда протоколлар негизида яратилган дастурий, аппарат-дастурий ва аппарат-техник воситаларнинг биргаликда қўллаш билан самарали амалга оширилади.

Ўзбекистон Республикаси Президенти И.А. Каримов ва Ўзбекистон Республикаси Вазирлар Маҳкамасининг қатор фармон ва қарорларида Республикамизда ахборот технологияларини ривожлантиришнинг аниқ йўналишлари белгилаб берилиб, бу соҳа мутахассисларига фаоллик кўрсатиш учун шарт-шароитлар яратилиб берилмоқда.

Криптографик тизимлар йўналишидаги изланишлар айниқса биринчи ва иккинчи жаҳон уруши йиллари даврида муҳим аҳамият касб этди ва жадал ривожланди. Урушдан кейинги йилларда, ҳисоблаш техникаларининг яратилиши, уларнинг такомиллашиб, инсоният фаолиятининг барча соҳаларига чуқур ва кенг маънода кириб бориши, криптографик услубларни табиий равишда ривожланиб ва такомиллашиб боришини таъқозо этмоқда.

Криптографик услубларнинг ахборот тизими муҳофазаси масалаларида қўлланилиши, айниқса, ҳозирги кунда фаоллашиб бормоқда. Ҳақиқатан ҳам, бир томондан компьютер тизимларида ИНТЕРНЕТ тармоқларидан фойдаланган ҳолда катта ҳажмдаги давлат ва ҳарбий аҳамиятга эга бўлган, ҳамда, иқтисодий, шахсий ва бошқа турдаги ахборотни тез ва сифатли узатиш, қабул қилиш кенгайиб бормоқда. Иккинчи томондан эса бундай ахборотларнинг муҳофаза қилиниши таъминлаш масалалари муҳимлашиб бормоқда.

Ахборотни мухофаза қилиш масалалари билан *криптология* (kryptos-махфий, logos-илм) фани шуғулланади. Криптология мақсадлари ўзаро қарама-қарши бўлган иккита йўналишига эга – *криптография* ва *криптотаҳлил.*

Криптография очиқ маълумотларни шифрлаш масалаларининг математик услублари билан шуғулланади.

Криптотаҳлил эса шифрлаш услуби (калити ёки алгоритми)ни билмаган ҳолда шифрланган маълумотни асл ҳолатини (мос келувчи очиқ маълумотни) топиш масалаларини ечиш билан шуғулланади.

Ҳозирги замон криптографияси қуйидаги тўртта бўлимни ўз ичига олади:

1. Симметрик криптотизимлар.
2. Очиқ услубга ёки яна бошқача айтганда очиқ калитлар алгоритмига асосланган ассимметрик криптотизимлар.
3. Электрон рақамли имзо криптографик тизимлари.
4. Криптотизимлар учун криптобардошли калитларни ишлаб чиқиш ва улардан фойдаланишни бошқариш.

Тадқиқотнинг объекти ва предметини белгиланиши. Ахборот-коммуникация тармоқларида алмашинадиган электрон ахборотнинг маҳфийлигини таъминловчи криптографик воситалар – асимметрик калитли шифрлаш алгоритмлари тадқиқотнинг объекти ҳисобланади. Ҳусусан Эль-Гамал очиқ калитли асимметрик шифрлаш алгоритми тадқиқотнинг предметини ташкил этади.

Тадқиқотнинг мақсади ва вазифалари. Характеристикаси етарли катта бўлган чекли майдонда дискрет логарифмлаш масаласи ечимининг мураккаблигига асосланган асимметрик шифрлаш алгоритми туркумига кирувчи Эль-Гамал очиқ калитли шифрлаш алгоритми базавий акслантиришлари моҳиятини сақлаб қолган ҳолда шифрлаш жараёнида қўлланиладиган амаллар ва акслантиришларни комбинациялаш асосида

унинг криптобардошлигини ошириш тадқиқотнинг мақсади ҳисобланади, Шу мақсаддан келиб чиқадиган тадқиқот вазифалари: Эль-Гамал очиқ калитли шифрлаш алгоритмида қўлланиладиган амаллар ва базавий акслантиришлари криптографик хусусиятларини таҳлил қилишдан, унинг бардошлиликни таъминловчи бошқа акслантиришлар билан комбинациялаш эвазига криптобардошлигини оширишдан иборат.

Тадқиқотнинг асосий масалалари ва фаразлари;

Магистрлик диссертация ишида тадқиқ қилинадиган асосий масалалар:

–Асимметрик шифрлаш алгоритмининг асосий криптографик моҳиятини ёритиш, уларнинг криптобардошлиги асосини таъминловчи амалий биртомонламалик хусусиятли функциялар турларига кўра классификацияси;

–Ахборот муҳофазасининг асимметрик шифрлаш алгоритми асосида самарали ечиладиган криптографик масалалар ва уларни ечишни усулларини таҳлил қилиш;

– Эль-Гамал асимметрик шифрлаш алгоритмининг криптографик таҳлили, уни такомиллаштириш ҳамда дастурий таъминоти асосларини яратиш;

–янги такомиллаштирилган М-Эль-Гамал–Т-Эль-Гамал асимметрик шифрлаш алгоритмининг криптографик таснифи ва унинг криптобардошлигини баҳолаш.

Тадқиқотнинг гипотезаси (илмий фарази) Эль-Гамал асимметрик шифрлаш алгоритми базавий акслантиришлари негизини сақлаб қолган ҳолда ахборот-коммуникация тармоқларида электрон ахборотнинг кафолатли маҳфийлигини таъминловчи М-Эль-Гамал–Т-Эль-Гамал такомиллаштирилган вариантини ишлаб чиқишдан иборат.

Мавзу бўйича қисқача адабиётлар таҳлили ёки муаммонинг ўрганилганлик даражаси. Ахборотнинг криптографик муҳофазаси соҳасидаги илмий ишларнинг муаллифлари, криптография фанининг

вужудга келишини қуйдаги учта даврга ажратадилар: 1949 йилгача бўлган қатъий исботсиз – фақат интуиция ва «ишончга» асосланган – илмий асосланмаган криптография даври, 1949 йилдан 1976 йилгача бўлган *илмий асосланган махфий калитли* криптография даври, 1976 йилдан кейинги очиқ *калитли криптография* даври.

К.Э. Шенноннинг 1949 йилда чоп этилган «Махфий тизимларда алоқа назарияси», деб номланган илмий мақоласи илмий асосланган *махфий калитли криптография даврини* бошлаб берди. У ўзининг 1948 йилда эълон қилинган – ахборотлар назариясига бағишланган илмий мақоласи негизида махфий алоқа тизими назариясининг асосини яратди. Унинг томонидан эълон қилинган илмий мақолалари катта аҳамиятли бўлсада, криптология соҳасидаги илмий мақолаларнинг сезиларли кўпайишига олиб келмади. Эҳтимол бунга сабаб, Шенноннинг махфий тизимларда алоқа назариясининг махфий калитга асосланган бўлиб, махфий калитни фойдаланувчига етказиш масалалари ечимининг мураккаблиги билан боғлиқлигидадир[1-5]. *1976 йилда У. Диффи ва М.Е. Хеллманнинг «Криптографияда янги йуналиш», деб номланган мақоласининг эълон қилиниши шу соҳадаги очиқ илмий ишлар ривожини берди. Уларнинг бу ишлари махфий алоқа тизимларида маълумотларни шифрлаш ва шифрни очишда махфий калитнинг тизим фойдаланувчилари орасида махсус муҳофазаланган алоқа канали орқали узатилиши ва қабул қилинишига ҳожат бўлмайдиган илмий-амалий услуб асосларини яратиб, бугунги кунда ҳам ривожланиб ва долзарблашиб бораётган очиқ калитли криптография даврини бошлаб берди* [6, 7].

Компьютер тармоқлари ва электрон ҳужжат айланиши технологияларининг ривожланиши, молия, банк ишлари, савдо-сотиқ каби йўналишларда қўлланилиши ахборот муҳофазасининг криптографик усулларини умумжамият фаолиятининг турли соҳаларига кенг кириб боришига сабаб бўлди. Бу кенг қамровли қўлланишлар ахборотни криптографик муҳофазасини таъминлашнинг асосий масалаларини қўйилишини ва уларнинг ечимларини таъминловчи криптографик усул ҳамда

воситалар моҳиятини ёритишни, маълумотларни муҳофазасига таҳдид солувчи сабабларни аниқлаш ва бартараф этиш усулларини, криптографик воситаларини қўлланиш моҳиятига кўра туркумланишини, криптографик ҳимоялаш воситаларини танлаш мезонларини, электрон хужжат айланиши жараёнлари муҳофазасини таъминлашнинг криптографик хусусиятларини ёритишни, криптографик ҳимоялаш воситаларини ахборот-коммуникация тизимларида қўллаш усулларини, калитларни муҳофазаланган тақсимоти протоколларини ишлаб чиқишни ва каби соҳалардаги масалалар ечимига бағишланган илмий тадқиқот натижаларини эълон қилинишига сабаб бўлди[8-138].

Янги асрнинг бошларидан криптология элементлари ахборот-коммуникация технологиялари фанлари билан боғлиқ ҳолда кўплаб олий ўқув юртларида у ёки бу ном билан ўрганилиб келинмоқда. Бу соҳада Ўзбекистон Республикаси олимлари томонидан ҳам етарли даражада илмий-тадқиқот ишлари олиб борилмоқда ва бунга Каримов М.М., Акбаров Д.Е., Хасанов П.Ф., Ғаниев С.К., Арипов М.М., Ахмедова О.П., Хасанов Х.П., Мусаев А.И. ва бошқалар томонидан эришилган натижаларни келтириш мумкин.

Ушбу магистрлик диссертация иши ахборот-коммуникация тизимларида алмашиладиган маълумотларни кафолатли криптографик мухофазалашнинг асимметрик тизимлари муаммолари билан боғлиқ. Бу соҳадаги муаммоларни бартараф қилиш ўз навбатида ахборот хавфсизлигини таъминлашнинг криптографик воситалари бўлган: симметрик ва асимметрик шифрлаш, хэш-функция ва электрон рақамли имзонинг мавжуд стандарт алгоритмларини, криптоалгоритмлар учун кафолатли бардошли калитлар ишлаб чиқиш ва уларни бошқариш масалаларининг мавжуд ечимларини шунингдек уларни ахборот-коммуникация тизимларида қўлланилиши услубларини чуқур таҳлил қилишни ва етарли даражада ўрганишни талаб қилади.

Ҳозирда Ўзбекистон Республикаси Ҳукумати раҳбарияти томонидан

ахборот-коммуникация тизимларини кафолатли криптографик муҳофазасини таъминлашнинг чора тадбирларини меёрий – ҳуқуқий томонларини ишлаб чиқилиши босқичма босқич амалга оширилмоқда. Аммо бу чора тадбирларни амалга оширувчи миллий кафолатли криптобардошли – криптографик муҳофаза воситалар ишлаб чиқилиши долзарб бўлиб қолмоқда.

Тадқиқотда қўлланилган услубларнинг қисқача тавсифи. Ушбу магистрлик диссертацияда ахборотни маҳфийлигини таъминловчи асимметрик шифрлаш алгоритмларини криптобардошлигини таъминловчи мураккабликларга асосланган: *етарли катта бутун сонни туб кўпайтувчиларга ажратиш, характеристикаси етарли катта бўлган чекли майдонларда дискрет логарифмлаш, эллиптик эгри чизиқ нуқталарини қўшиш, тартиби етарли катта бўлган тенгламалар системасини чекли майдонларда ечиш, номаълум параметрга боғлиқ ҳолда амаллар бажариладиган акслантиришларни ҳисоблаш, санаб ўтилган мураккабликларни комбинациялаш* каби усулларидан фойдаланилган.

Тадқиқот натижаларининг назарий ва амалий аҳамияти

–асимметрик шифрлаш алгоритмларни улар асосини ташкил этувчи биртомонламалик хусусиятли функцияларга акслантиришларнинг хусусиятларига кўра туркумлаш асимметрик криптотизимларнинг таҳлил усулларини яратишнинг тизимли илмий ёндошувига асос бўлади;

–турли криптобардошли амаллар ва акслантиришларни биртомонламалик хусусиятлари билан комбинациялаш такомиллаштириш усули мавжуд асимметрик шифрлаш алгоритмларининг бардошлигини ҳисоблаш техника ва технологияларини ривожланишига мос равишда самарали модификациялашни амалга ошириб боришни илмий ҳамда амалий асосини таъминлайди;

– Эль-Гамал асимметрик шифрлаш алгоритмининг базавий акслантиришлари негизини сақлаб қолган ҳолда ишлаб чиқилган янги такомиллаштирилган М-Эль-Гамал–Т-Эль-Гамал асимметрик шифрлаш

алгоритмининг ахборот-коммуникация тармоқларида электрон ахборотнинг кафолатли маҳфийлигини таъминлайди.

Тадқиқотнинг илмий янгилиги:

– Эль-Гамал асимметрик шифрлаш алгоритмининг базавий акслантиришлари негизини сақлаб қолган ҳолда ишлаб чиқилган янги такомиллаштирилган М-Эль-Гамал–Т-Эль-Гамал асимметрик шифрлаш алгоритми ахборот-коммуникация тармоқларида электрон ахборотнинг кафолатли маҳфийлигини таъминлайди;

– Янги такомиллаштирилган М-Эль-Гамал–Т-Эль-Гамал асимметрик шифрлаш алгоритмини ишлаб чиқишда қўлланилган усуллар бошқа ҳисоблаш мураккабликларга эга бўлган барча асимметрик шифрлаш алгоритмларини такомиллаштириш учун ҳам ўринли;

–Ҳисоблаш техника ва технологияларини ривожланиб боришига мос равишда таклиф этилган такомиллаштириш усулини қўллаб керакли кафолатли криптобардошликка эга бўлган симметрик блоклаб шифрлаш алгоритмига самарали эришиш мумкин.

Диссертация таркибининг қисқача тавсифи: Диссертация мундарижа, кириш, учта бўлим, хулоса, 104 та номдаги фойдаланилган адабиётлар руйхати, иловадан иборат. Диссертациянинг асосий хажми ... бет матн, ... та жадвал ташкил топган.

1-БЎЛИМ. АХБОРОТ МУҲОФАЗАСИ МАСАЛАЛАРИНИ КРИПТОГРАФИК УСУЛЛАР БИЛАН ЕЧИШДА АСИММЕТРИК ШИФРЛАШ АЛГОРИТМЛАРИНИНГ ЎРНИ ВА МОҲИЯТИ

Биринчи бўлимда ахборот муҳофазасини таъминлашнинг криптографик усуллари масалаларининг қўйилиши, симметрик ва асимметрик шифрлаш алгоритмларининг моҳияти ҳамда уларнинг хусусиятлари, асимметрик шифрлаш алгоритмлар яратишга асос бўлувчи биртомонлама функциялар криптографик хусусиятлари, асимметрик шифрлаш алгоритмларига қўйиладиган талаблар илмий асосланган ҳолда ёритилади.

1.1. Ахборот муҳофазасини таъминлашнинг криптографик масалаларининг қўйилиши

Ахборот-коммуникация тармоқларида маълумотлар алмашинуви технологияларининг бугунги ривожланган инсоният жамиятининг турли соҳаларига кенг ва чуқур кириб бориб, ахборотлар мажмуаси - маълумотлар тўплами барча кундалик фаолият жараёнларини мақсадли режалаштиришни талаб этади, у ёки бу соҳага тегишли бўлган муҳим ахборотлар мажмуасини муҳофазасини таъминлаш масалалари ва уларнинг ечимлари долзарблашиб бормоқда. Аахборот-коммуникация тармоқларида ахборотларнинг криптографик муҳофазасини таъминлашнинг асосий масалалари қуйидагилардан иборат:

- ахборотнинг махфийлигини (конфиденциаллигини) таъминлаш;

- ахборотнинг тўлалигини (ўзгармаганлигини) таъминлаш;

-ахборотнинг аутентификациясини (маълумот субъектларини ҳақиқийлигини) таъминлаш;

- ахборотнинг муаллифини ва муаллифликдан бош тортмаслигини таъминлаш;

- криптографик алгоритмлар учун криптобардошли калитлар ишлаб чиқариш ва уларни тармоқ фойдаланувчиларига муҳофазаланган ҳолда тарқатилишини бошқариш.

Ахборот муҳофазасининг санаб ўтилган масалаларини криптографик усуллар билан ечиш воситаси шифрлаш алгоритмларидир [1].

Ахборот махфийлигини (конфиденциаллигини) таъминлашнинг асосий мақсади очиқ алоқа тармоғида махфийликни таъминлаган ҳолда махфий маълумотларни алмашинуви масалаласини ечишдан иборат. Ахборот-коммуникация тизимлари очиқ алоқа тармоғи фойдаланувчиларининг маълумотлар мажмуасидан турли мақсадларни, баъзан эса ўзаро қарама-қарши мақсадларни назарда тутиши, махфийлигини кафолатли таъминлаган ҳолда маълумотлар алмашинувини амалга оширишни тақазо этади. Ўзаро қарама-қарши мақсадларни назарда тутувчи томонлар криптотаҳлилчилари бугунги ривожланган ахборот технологиялари ютуқларидан фойдаланиб, алоқа тармоғига боғланиб, маълумотлар алмашинувини кузатиш (мониторингини олиб бориш), шифрлаш алгоритмларини қўллаш билан махфийлиги таъминланган маълумотларга эга бўлиш, уларни дешифрлаш чора - тадбирларини амалга оширишга ҳаракат қилиш имкониятларига эга. Бундай ҳатти-ҳаракатлар (ҳужумлар) икки турда бўлади: *фаол* (*актив*) ва *фаол бўлмаган* (*пассив*). Фаол бўлмаган ҳужумлар эшитиш, алоқа тармоғида алмашинаётган маълумотларни мазмунини кузатиш ва таҳлил қилиш, шифрланган маълумотларни ёзиб олиш ва дешифрлаш каби хатти-ҳаракатлар билан боғлиқ. Фаол ҳужумлар маълумотлар алмашинуви жараёнига тўсқинлик қилиш, узатилаётган маълумотлар мазмунини ўзгартириш каби хатти-ҳаракатларни ўз ичига олади.

Очиқ маълумот *M*, шифрланган маълумот *C*, шифрлаш алгоритми *E* ва калити k_1, дешифрлаш алгоритми *D* ва калити k_2, деб белгиланса, шифрлаш жараёни $E_{k_1}(M) = C$, дешифрлаш жараёни $D_{k_2}(C) = D_{k_2}(E_{k_1}(M)) = M$ кўринишда ифодаланади.

Турли хусусиятли - ҳужжатли, овозли, тасвирли маълумотларнинг барчасини шифрлаб, алоқа тармоғида узатилиши ва қабул қилинишини кафолатли мухофаза қилинишини самарали кечишини таъминловчи ягона криптографик алгоритм мавжуд эмас. Чунки, криптографик воситалар маълумотларнинг физик хусусиятлари, уларнинг махфийлик даражаси, хажми, сигнал кўринишида ифодаланиш усули, алоқа тармоғида узатилиш технологиялари хусусиятлари, қўлланиладиган техник қурилмаларнинг қиймати,

фойдаланишга қулайлиги каби хосликларни ҳисобга олган ҳолда танланади.

Ахборот тўлалигини таъминлашнинг асосий мақсади очиқ алоқа тармоғида маълумотлар алмашинуви жараёнларида рақиб томоннинг алмашинаётган маълумотларни ўз манфаатидан келиб чиққан ҳолда ўзгартиришларини аниқлашнинг имконини берувчи криптографик воситаларни (алгоритмларни) яратишдан иборат. Бунинг учун узатилаётган маълумотга, уни қабул қилувчи томон учун, маълумотни ўзгарган ёки ўзгармаганлигини текшириш имконини берувчи, махсус алгоритм билан ҳисобланадиган - *назорат йиғиндиси* ёки *маълумотнинг аутентификация коди*, деб аталувчи қўшимча қўшилади. Бундай қўшимча қўшиш усулининг кодлаштириш усулидан фарқи, назорат йиғиндиси ҳисобланадиган криптографик алгоритмнинг махфий калитга боғлиқлигидадир. Махфий калитни билмаган ҳолда узатилаётган маълумотга рақиб томонидан ўзгартириш киритиш эҳтимоллиги деярли йўқ. Шундай эҳтимоллик ўлчови *шифрнинг имитобардошлилиги* – фаол ҳужумларга бардошлилик ўлчови дейилади. Берилган M -маълумотни аутентификациясини (ҳақиқийлигини) текшириш имконини берувчи қайд қилинган узунликдаги қиймат қабул қиладиган назорат йиғиндисини ҳисоблаш алгоритмининг калит деб аталувчи махфий k -параметрга ва M –маълумотга боғлиқ функцияси $h_k(M) = S$ -хэшлаш функцияси деб юритилади. Хэш-функцияга қуйдаги талаблар қўйилади:

- калитни билмаган ҳолда берилган M – маълумотнинг $h_k(M) = S$ қийматини ҳисоблаш мумкин эмас;

- берилган M –маълумот ва унинг хэш-функция қийматини $h_k(M) = S$ билган ҳолда шу M – маълумотдан фарқли $M \neq M_1$, лекин хэш-функция қиймати тенг $h_k(M) = h_k(M_1) = S$ бўлган M_1-маълумотни топиш имкони йўқ.

Келтирилган биринчи талаб маълумотнинг қалбакилаштирилишига йўл қўймасликни таъминлайди, иккинчи талаб эса бирор маълумотни бошқа маълумот билан алмаштириш имкониятини чекланишини таъминлайди.

Ахборотнинг аутентификацисини (маълумот субъектларининг

ҳақийқийлигини) таъминлашнинг мақсади ахборот алмашинуви тўғри ўрнатилганлигини, томонларнинг ҳақиқийлигини, маълумот ва унинг муаллифи каби субъектларнинг ҳақиқийлигини текширишни таъминлашдан иборат.

Ахборот алмашинуви жараёни (сеанси) тўғри ўрнатилганлигини аутентификациси: тармоқ бўғинлари боғланишларининг тўғри амалга оширилганлигини текширишни, рақиб томонидан маълумотларни қайта узатиш имконияти йўқлигини ва маълумотлар алмашинувининг ўз вақтида кечишини таъминлаш каби тадбирларни ўз ичига олади. Бунинг учун узатилаётган маълумотларга осон текшириладиган қўшимча параметрлар киритишдан фойдаланилади.

Ахборот муаллифлигини ва муаллифликдан бош тортмаслигини таъминлашнинг мақсади бир-бирига ишонмайдиган томонларнинг маълумотлар алмашинуви жараёнларида жўнатувчи маълумотни юборганлигини рад этиб, бу маълумотни олувчининг ўзи тузганлигини даъво қилиши ёки ҳақиқатан ҳам, олувчи ўзи қабул қилиб олган маълумотни ўзгартириши, қалбакилаштириши ва янги маълумот тузиши, сўнгра бу маълумотни жўнатувчидан олганлигини даъво қилиши мумкин бўлган ҳолатларда келиб чиқадиган муаммо ва низоларни тўғри ҳал этишдан иборат. Бундай муаммо ва низоларни ҳал этишнинг фундаментал механизми электрон рақамли имзо (ЭРИ) ҳисобланади. ЭРИ жўнатилаётган маълумотни ташкил этувчиларига ва жўнатувчининг махфий калитига боғлиқ ҳолда ҳисобланиб, жўнатилаётган маълумотга илова қилинадиган рақамли кетма-кетликдан ташкил топади. Маълумотни қабул қилувчи томон қабул қилинган маълумотни бу рақамлар кетма-кетлиги ва жўнатувчининг очиқ калитига боғлиқ ҳисоблашларни бажариб, маълумотнинг аутентификацисини амалга оширади. Шундай қилиб ЭРИ жарёни алгоритми икки қисмдан рақамли имзони ҳисоблаш (шакллантириш) ва рақамли имзони текширишдан иборат. Рақамли имзони ҳисоблаш махфий калитга боғлиқ бўлгани учун ҳам уни фақат маълумотни жўнатувчи (яъни маълумотнинг ҳақиқий муаллифи) тўғри шакллантира олади. Рақамли имзони текшириш очиқ калит орқали амалга оширилади, яъни исталган томон учун унинг тўғрилигини

текшира олиш имконияти мавжуд.

Криптобардошли калитлар ишлаб чиқариш мақсади калит блокини ташкил этувчи элементлар (битлар ёки байтларнинг) тасодифийлигини таъминлашдан иборат.

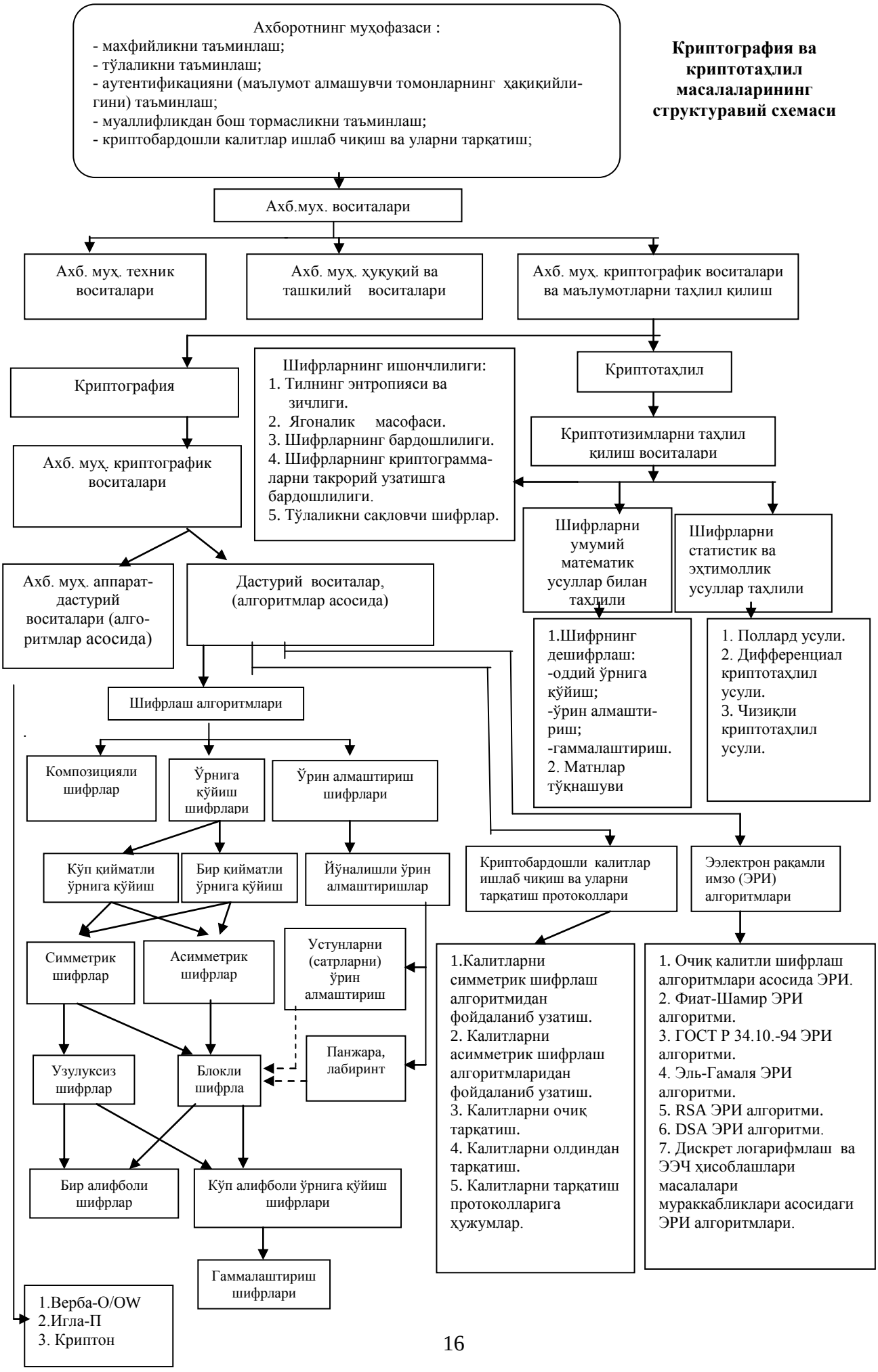
Шифрлаш алгоритмлари: *калит деб аталувчи махфий параметрларга асосланган - симметрик калитли ва қўлланиш протоколи билан аниқланувчи - махфий ҳамда очиқ параметрларга асосланган - асимметрик шифрлаш криптоалгоритмларидан* иборат.

Ахборот-коммуникация тармоқларида ахборот муҳофазасини таъминлашнинг криптографик воситалари: криптографик алгоритмларнинг дастурий таъминоти ва аппарат-дастурий қурилмаларидан иборат бўлади. Нисбатан содда, аммо криптобардошли бўлган алгоритмларнинг аппарат-техник қурилмалари самарали қўлланилади.

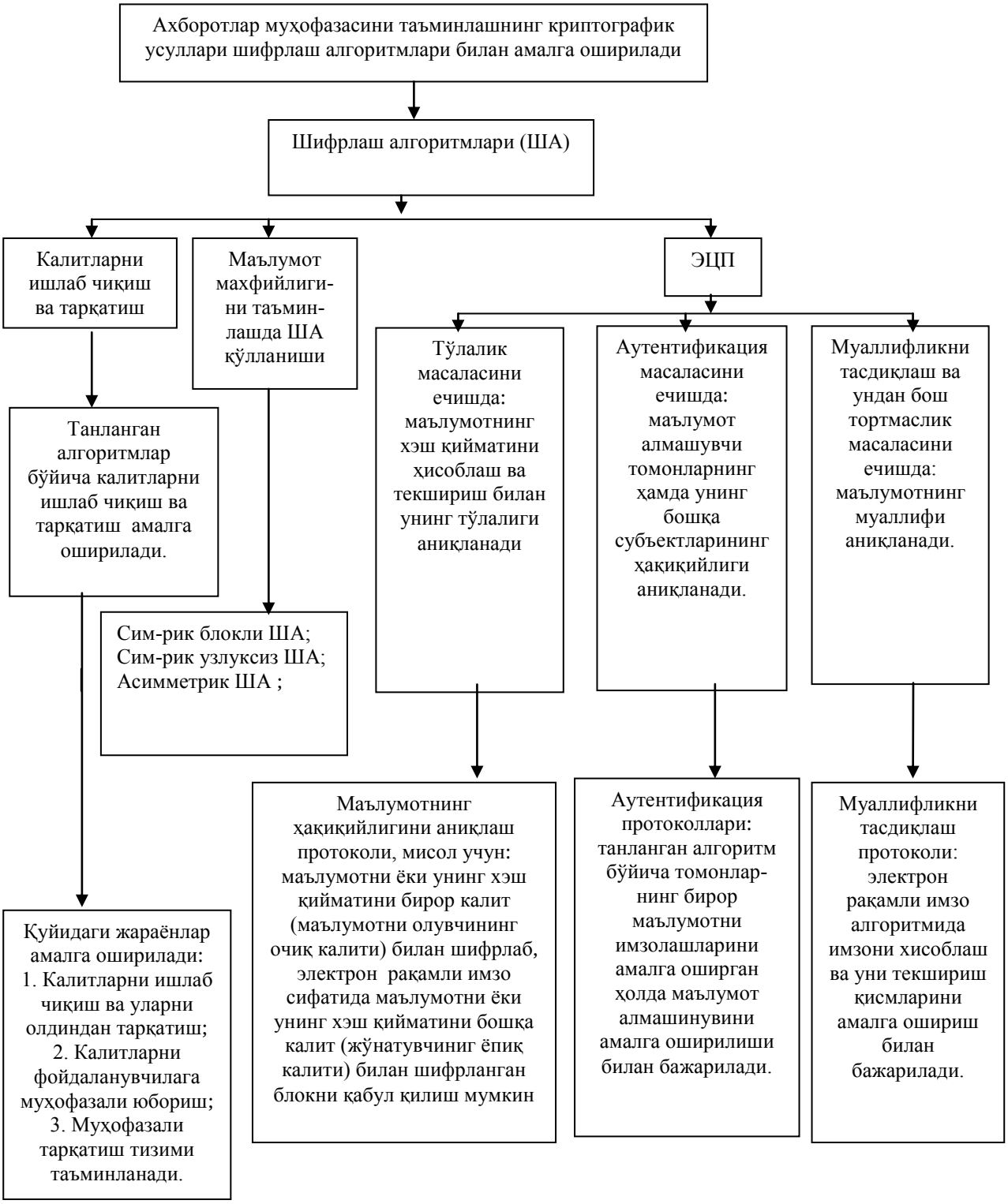
Шифрлаш алгоритмларининг асосий криптографик хусусиятларга эга бўлган математик моделларда ифодаланувчи акслантиришлар билан аниқланади.

Ахборотнинг муҳофазасини таъминлашнинг санаб ўтилган масалалари ва уларнинг криптографик ечимлари ҳамда очиқ ва шифрланган маълумотларни таҳлил қилиш усулларининг боғлиқликларини қуйидагича ифодалаш мумкин [1]:

Криптография ва криптотаҳлил масалаларининг структуравий схемаси



Ахборот муҳофазасини криптографик усуллар билан таъминлаш воситалари асосини шифрлаш алгоритмлари ташкил этади. Бу фикр қуйидаги схемада ўз аксини топган [1]:



1.2. Асимметрик шифрлаш алгоритмларининг моҳияти ҳамда уларнинг хусусиятлари

Ахборот-коммуникация тармоқларида маълумотлар алмашинувининг муҳофазасини таъминлаш масалаларини ечишда симметрик калитли крпитоалгоритмлар асосида яратилган криптотизим қанчалик ишончли бўлмасин, бари-бир ундан амалда фойдаланиш жараёнида баъзи ечилиши керак бўлган муҳим ҳавфсизликни таъминлаш масалалари келиб чиқиши мумкин. Масалан, калитларни тизим фойдаланувчиларига тарқатиш масаласи. Бу масалани ечиш учун, ишлаб чиқилган бардошли калитларни тизим фойдаланувчиларига етказиш хавфсизлиги кафолатли таъминланган бўлиши талаб этилади. Бунинг учун эса яна бирор криптотизимдан фойдаланишга тўғри келади. Бу масаланинг ечими классик ва замонавий алгебрада олинган илмий натижалар асосида яратилган *очиқ калитли криптотизим*ларнинг вужудга келиши билан ҳал этилди.

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, иккинчиси махфий 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 ўзигагина маълум бўлган махфий калит билан уни дешифрлаб, очиқ маъумотга эга бўлади.

Таъкидлаш лозимки, очиқ калитли криптотизимлар алгоритмларидан қуйидаги мақсадларда фойдаланилади:

1. Сақланадиган ва узатиладиган маълумотларнинг махфийлиги муҳофазасини таъминловчи мустақил восита сифатида.

2. Калитлар тақсимотининг муҳофазасини таъминловчи восита сифатида. Очиқ калитли криптотизимлар алгоритмлари анъанавий криптотизимлар алгоритмларига нисбатан мураккаб ҳисоблаш жараёнларини талаб этиши натижасида паст тезликка эга бўлиб, ундан кўпроқ калитларни тақсимлашда фойдаланилади. Сўнгра, катта ҳажмдаги маълумотларни узатишда соддароқ ҳисоблашларга асосланган юқори тезликка эга бўлган тизимлардан фойдаланилади.

3. Аутентификация, яъни маълумотлар ва уларнинг муаллифлари ҳақиқийлигини аниқлаш услублари воситаси «Электрон рақамли имзо» сифатида.

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

1.3.Асимметрик шифрлаш алгоритмлар яратишга асос бўлувчи биртомонлама функциялар криптографик хусусиятлари

К.Э. Шенноннинг 1949 йилдаги мақоласи [5] криптология соҳасидаги очиқ илмий изланишларнинг кўпайишига олиб келмади. Биринчидан, бу мақолада келтирилган «махфий алоқа тизимларининг назарий бардошлилик назарияси» моҳияти жиҳатидан атрофлича ва тўлиқ бўлиб, бундай назарияга кўра, махфий алоқа канали бўйлаб узатиладиган калитнинг ҳажми, узатиладиган маълумот ҳажмининг катталашиб бориши билан, катталашиб боради. Иккинчидан, амалий бардошлилик масалаларининг ечимлари ҳақидаги илмий натижалар, янги криптотизимлар яратиш йўналишларининг вужудга келишидан кўра, кўпроқ мавжуд криптотизимларнинг такомиллашувига олиб келди. Шундай бўлсада, Шенноннинг бу назарясидаги «етарли даражадаги (амалий) бардошли криптотизимлар яратиш масаласи, моҳияти жиҳатидан, маълум шартларни қаноатлантирувчи ва ечими сарф-ҳаражатларни қопламайдиган мураккаб масалага асосланиши

керак», деб ифодаланган изоҳи, станфордлик олимлар У. Диффи ва М.Е. Хеллман илмий изланишларининг самарали натижаларида ўз аксини топди. Улар томонидан 1976 йилда «Криптологияда янги йўналиш» [6], деб номланган илмий мақоланинг чоп этилиши, махфий алоқа тизимларида махфий калитни махфий алоқа канали бўйлаб узатишга ҳожат йўқ бўлган амалий бардошли криптотизимлар яратишнинг асосини очиб берди. У. Диффи ва М.Е. Хеллманнинг илгари сурган ғоялари «бир томонлама функция»нинг Р.М. Нидхэмнинг ҳисоблаш тизимларига киришнинг муҳофазаси ҳақидаги ишларидан олинган таърифини криптотизимлар учун мослаштирилган ва такомиллаштирилган ифодасидир.

Бир томонлама функция – бу, таъриф бўйича, шундай $y = f(x)$ функцияки, унинг аниқланиш соҳасидан бўлган ихтиёрий x учун $f(x) = y$ қиймат осон ҳисобланиб, қийматлар соҳасининг барча y қийматларига мос келувчи x қийматларни ҳисоблаб топишни амалий жиҳатдан имконияти йўқ. Кўриниб трубдики, бир томонлама функциянинг бундай таърифи «осон ҳисобланадиган», «барча қийматлар учун», «амалий жиҳатдан», «ҳисоблашнинг имконияти йўқ» 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 ифодланиши 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 $f_z^{-1}(y) = x$ қийматлар маълум бўлган E_z алгоритм билан ҳисоблашнинг имконияти йўқ (ёки бошқача айтганда $f_z^{-1}(y) = x$ қийматларни ҳисоблаш сарф-ҳаражатлари ва

вақти мақсадга мувофиқ эмас). Бундай таъриф математика нуқтаи назаридан аниқ бўлмасада, амалий криптология масалаларида самарали қўлланилиши мумкинлигига шак-шубҳа йўқ.

1.4. Асимметрик шифрлаш алгоритмларига қўйиладиган талаблар

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

Бир томонлама функцияларнинг аниқланиш таърифида назарий жиҳатдан тескариси м*а*вжуд 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 шифрмаълумот кўринишига ўтказиш бир томонлама жараён ва шифрлаш калити билан шифрмаълумотни очиш – дешифрлаш мумкин эмас, яъни шифрлаш калитини билиш шифрмаълумотни дешифрлаш учун етарли эмас.*

2. *Очиқ калитнинг маълумлигига асосланиб, махфий калитни замонавий фан ва техника ютуқлари ёрдамида аниқлаш учун бўладиган сарф-ҳаражатлар ҳамда вақт мақсадга мувофиқ эмас. Бунда, шифрни очиш учун бажарилиши керак бўладиган энг кам миқдордаги амаллар сонини аниқлаш муҳимдир.*

Очиқ калитли шифрлаш алгоритмларидан ахборот тизимида маълумотларнинг махфийлигини таъминлашда замонавий илғор услуб

сифатида фойдаланиб келинмоқда. Очиқ калитли криптотизимларни яратишнинг RSA алгоритми жаҳон стандарти сифатида қабул қилинган. Умуман олганда, **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]:**

1. *Етарли катта сонларни туб кўпайтувчиларга ёйиш*.

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. Номаълум параметрга боғлиқ ҳолда амал бажариш.

6. Ҳисоблаш мураккабликларини комбинациялаш каби.

Кейинги бўлимда очиқ калитли асимметрик криптотизимлар таҳлиллари тадқиқ этилади.

1-бўлим бўйича хулосалар

Ушбу бўлимда:

1. Аахборот-коммуникация тармоқларида ахборотларнинг криптографик муҳофазасини таъминлашнинг асосий масалаларини: ***ахборотнинг махфийлигини (конфиденциаллигини) таъминлаш; ахборотнинг бутунлигини (ўзгармаганлигини) таъминлаш; ахборотнинг аутентификациясини (маълумот субъектларини ҳақиқийлигини) таъминлаш; ахборотнинг муаллифини ва муаллифликдан бош тортмаслигини таъминлаш; криптографик алгоритмлар учун криптобардошли калитлар ишлаб чиқариш ва уларни тармоқ фойдаланувчиларига муҳофазаланган ҳолда тарқатилишини бошқариш;***

қўйилиши ва улар ечимларининг моҳиятлари, бу масалаларни ечишнинг

криптографик воситалари илмий ҳамда амалий жиҳатдан асосланди. Яъни маҳфийлигини шифрлаш, бутунлигини хэш-функция, ахборотнинг муаллифини ва унинг муаллифликдан бош тортмаслигини, аутентификациясини (маълумот субъектларини ҳақиқийлигини) таъминловчи ЭРИ алгоритмлари моҳиятлари тадқиқ қилинди.

2. Асимметрик шифрлаш алгоритмларининг моҳияти ҳамда уларнинг хусусиятлари тадқиқ қилиниб, бундай шифрлаш алгоритмлар яратишга асос бўлувчи: ***етарли катта сонларни туб кўпайтувчиларга ёйиш, характеристикаси етарли катта бўлган чекли майдонларда дискрет логарифмларни ҳисоблаш, етарли катта тартибдаги алгебраик тенгламалар тизимининг илдизларини чекли майдонларда ҳисоблаш, эллиптик эгри чизиқларда рационал координатали нуқталарни топиш, уларни қўшиш ҳамда тартибини аниқлаш, номаълум параметрга боғлиқ ҳолда амал бажариш, ҳисоблаш мураккабликларини комбинациялаш*** каби биртомонлама функциялар криптографик хусусиятлари ёритилди.

3. Очиқ калитли криптотизимларга қуйидаги муҳим талаблар: ***дастлабки очиқ маълумотни шифрмаълумот кўринишига ўтказиш бир томонлама жараён ва шифрлаш калити билан шифрмаълумотни очиш – дешифрлаш мумкин эмас, яъни шифрлаш калитини билиш шифрмаълумотни дешифрлаш учун етарли бўлмаслиги; очиқ калитнинг маълумлигига асосланиб, махфий калитни замонавий фан ва техника ютуқлари ёрдамида аниқлаш учун бўладиган сарф-ҳаражатлар ҳамда вақт мақсадга мувофиқ эмас. Бунда, шифрни очиш учун бажарилиши керак бўладиган энг кам миқдордаги амаллар сонини аниқлашнинг муҳимлиги*** алоҳида асосланди ва такидланди**.**

2-БЎЛИМ. ЭЛЬ-ГАМАЛ АСИММЕТРИК ШИФРЛАШ АЛГОРИТМИНИНГ КРИПТОГРАФИК ТАҲЛИЛИ, УНИ ТАКОМИЛЛАШТИРИШ ҲАМДА ДАСТУРИЙ ТАЪМИНОТИ АСОСЛАРИНИ ЯРАТИШ

2.1. Дискрет логарифимлаш масаласи ечими мураккаблиги асосидаги асимметрик шифрлаш алгоритмларининг криптографик хусусиятлари таҳлили

Асимметрик шифрлар криптобардошлиги бўйича *ишончли бардошли криптоалгоритмлар* туркумига киради. *Ишончли бардошли криптоалгоритмлар* мутахасислар томонидан ечилиши мураккаб деб тан олинган математик масалага асосланади. Ишончли бардошли криптоалгоритмлар туркумига:

– ***етарли катта сонни туб кўпайтувчига ажратиш*** **(ТКА)** ***мураккаблигига асосланган*** **RSA** ***шифрлаш алгоритми***[1-8];

– ***характеристикаси етарли катта бўлган чекли майдонда дискрет логарифмлаш*** **(ДЛ)** ***мураккаблигига асосланган*** **Эль-Гамал** ***шифрлаш алгоритми***[1-8];

–***эллиптик эгри чизиқ*** **(ЭЭЧ)** ***нуқталари устида амал бажариш мураккаблигига асосланган шифрлаш алгоритмлари*** [1];

–***параметрли алгебра амаллари асосида санаб ўтилган мавжуд мураккабликларни комбинациялашга асосланган*** ADE-AShSh1, ADE-AShSh2, ADE-AShSh3 ***шифрлаш алгоритмлари*** [76] ***кабилар киради***.

Ишончли бардошли криптоалгоритмлар туркумига шифрлаш алгоритмларидан ташқари ЭРИ алгоритмлари ҳам киради:

–**ДЛ** ***мураккаблигига асосланган*** . **DSA, ГОСТ 34.10-94, Ўзбекистон Республикаси стандарти – O’zDSt 1092:2005 каби**;

–**ЭЭЧ** ***нуқталари устида амал бажариш мураккаблигига***

асосланган **ГОСТ Р 34.10-2001, ECDSA -2000, Украина ЭРИ стандарти – ДСТУ 4145-2002, Корея ЭРИ стандарти – EC-KCDSA**;

– ДЛ ***ва*** **ТКА** ***ҳамда*** **ЭЭЧ** ***нуқталари устида амал бажариш каби ––мавжуд мураккабликлар композициясига асосланган*** . ADE1– ERI ***алгоритми*** [73];

–мавжуд мураккабликларни параметрли алгебра амаллари билан композициялаш билан такомиллаштирилган **ЭРИ** ***алгоритмлари*** ADE2–ERI [10-14], ADE3– ERI [79, 84,85,86];

–мавжуд мураккабликлар ва хеш-функция алгоритми акслантиришларининг биртомонламалик хусусиятига асосланган ADE4–ERI[84-86] ***алгоритми***;

– мавжуд мураккабликлар ва шифрлаш алгоритмининг биртомонламалик хусусияти мураккаблигига асосланган ADE5– ERI [73,76,79, 84-86] ***алгоритми***;

– матрицалар устида параметрли алгебра амалларини бажаришни мавжуд мураккабликлар билан композициялашга асосланган ADE-AShSh1–ERI, ADE-AShSh2 – ERI, ADE-AShSh3 – ERI [1, 73,76,79, 84-86]. ***алгоритмлар ҳам ишончли бардошли криптоалгоритмлар туркумига киради.***

Ишончли бардошли криптоалгоритмларнинг ютуғи – улар асосидаги ечилиши мураккаб деб тан олинган математик масаланинг чуқур ўрганилганида.

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, иккинчиси махфий 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 маҳфий $k_i^м$ калитлари маҳфий 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, маҳфий $p_i^м$ ёки $p^м$ параметрни билмаслик $k_i^м$ -маҳфий калитни аниқлаш имкониятини бермайди.

Шифрлаш қоидасини E ва дешифлаш қоидасини D деб белгиланса, j – фойдаланувчи $м$ -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 $k_i^м$ -маҳфий 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.

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

Юқорида келтирилганидек *бир томонлама функция* – бу, 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 масалани ечишни талаб этади. Кўриниб трубдики, 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 ифодланиши 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-ҳаражатлари 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 аҳборотлар тизимида махфий алоқа хизматини ўрнатиш алгоритмини қуриш учун қулайлик туғдирмайди.

Бир томонлама функцияларнинг аниқланиш таърифида назарий жиҳатдан тескариси м*а*вжуд 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 шифрмаълумот кўринишига ўтказиш бир томонлама жараён ва шифрлаш калити билан шифрмаълумотни очиш – дешифрлаш мумкин эмас, яъни шифрлаш калитини билиш шифрмаълумотни дешифрлаш учун етарли эмас;

2) Очиқ калитнинг маълумлигига асосланиб, махфий калитни замонавий фан ва техника ютуқлари ёрдамида аниқлаш учун бўладиган сарф-ҳаражатлар ҳамда вақт мақсадга мувофиқ эмас. Бунда, шифрни очиш учун бажрилиши керак бўладиган энг кам миқдордаги амаллар сонини аниқлаш муҳимдир.

Қуйида оммавийлашган **RSA** очиқ калитли криптотимини юқорида келтирилган илмий фикр ва мулоҳазаларни асослашга мисол сифатида кўриб ўтилади.

Очиқ калитли RSA криптоалгоритми

У. Диффи ва М.Е. Хеллман махфий услубли бир томонлама функциянинг аниқланишига асосланиб, махфий алоқа тизими фойдаланувчилари учун, очиқ калитли криптотизимлар тузилишини (структурасини) таклиф этдилар. Ҳар бир i – фойдаланувчи бирор Z_i бутун сонни (даража кўрсаткичини) танлайди ва уни махфий сақлайди. Сўнгра, бу Z_i асосида E_{Z_i} алгоритм тузиб очиқ маълумотлар китобига бу алгоритмни жойлаштиради. Бундан ташқари Z_i асосида махфий сақланадиган D_{Z_i} алгоритмни ҳам тузади ва уни сир тутади. Агарда j – фойдаланувчи i – фойдаланувчига X махфий маълумотни узатмоқчи бўлса, у ҳолда j – фойдаланувчи очиқ маълумотлар китобидан E_{Z_i} алгоритмни олиб, $Y = f_{Z_i}(x),\ \ x \in X$, услуб билан шифрмаълумотни тузиб (ҳосил қилиб), i – фойдаланувчига жўнатади. Махфий маълумотни шифрмаълумот кўринишида қабул қилиб олган i – фойдаланувчи ўзининг махфий

D_{z_i} алгоритмидан фойдаланиб $f_{z_i}^{-1}(Y) = X$ услуб билан очиқ маълумотни ҳосил қилади. Агарда f_z, ҳақиқатан ҳам махфий услубли бир томонлама функция бўлса, у ҳолда бу функция асосида қурилган алгоритм амалий бардошлиликни таъминлайди. У. Диффи ва М.Е. Хеллман, агарда бир томонлама f_z функциянинг аниқланиш соҳасидаги даража кўрсаткичининг барча $z \in Z$ қийматлари тўплами билан, айнан шу функциянинг қийматлари тўплами устма-уст тушса, яъни f_z функциянинг аниқланиш соҳаси билан қийматлар соҳаси бир хил тўпламни ташкил этса, бундай бир томонлама функция асосида рақамли имзо олиш мумкинлигини таъкидлаганлар. Агарда i – фойдаланувчи алоқа тизими бўйича махфий бўлмаган X маълумотни барча фойдаланувчиларга етказиб, бу махфий бўлмаган маълумотни жўнатувчини маълумотни қабул қилиб олувчилар томонидан беҳато аниқланиши учун, ўз махфий калити билан алгоритм $Y = f_{z_i}^{-1}(X)$ асосида рақамли имзо қўяди. Ҳар бир фойдаланувчи очиқ калит билан алгоритм E_{z_i} ни билган ҳолда $f_{z_i}(Y) = X$ ни олади, лекин i – фойдаланувчидан бошқа фойдаланувчи X маълумотни $Y = f_{z_i}^{-1}(X)$ криптограмма кўринишидаги рақамли имзо ифодасига ўтказа олмайди, чунки фақат i – фойдаланувчининг ўзигина очиқ алгоритм асосланган f_{z_i} функцияга тескари бўлиб, махфий алгоритм асосини ташкил этувчи $f_{z_i}^{-1}$ ни ҳисоблай олади. Ўз-ўзидан тушинарлики, i – фойдаланувчи j – фойдаланувчига махфий маълумотни ҳам рақамли имзо билан жўнатиши мумкин. Бунинг учун, i – фойдаланувчи j – фойдаланувчининг f_{z_j} функцияга асосланган очиқ алгоритми (очиқ шифрлаш калити) E_{z_j} дан фойдаланиб, жўнатилиши керак бўлган маълумотни шифрлайди. Бу шифрланган маълумотни қабул қилиб олган j – фойдаланувчи ўзининг $f_{z_j}^{-1}$ функцияга асосланган махфий D_{z_j} дешифрлаш алгоритми билан очади.

1976 йилда У. Диффи ва М.Е. Хеллман ўзларининг «Криптологияда янги

йўналиш» [6] деб номланган илмий ишларида бир томонлама функция сифатида $y = g^a \bmod n$ ифода билан аниқланган дискрет даражага кўтариш функциясини таклиф қилиб, $a = \log_g y \bmod n$ ифодадаги дискрет логарифмни ҳисоблашнинг амалий жиҳатдан мураккаблигига асосланган эдилар. 1978 йилда эса, Массачусетс технология институтининг олимлари: Р.Л. Ривест, А. Шамир, Л. Адлман, ўзларининг илмий мақолаларида биринчи бўлиб махфий услубли (йўлли) ва ҳақиқатан ҳам бир томонлама бўлган функцияни таклиф этдилар. Бу мақола «Рақамли имзоларни қуриш услублари ва очиқ калитли криптотизимлар» деб аталиб, кўпроқ аутентификация масалаларига эътибор қаратилган. Ҳозирги кунда, юқорида номлари келтирилган олимлар таклиф этган функцияни, уларнинг шарафига RSA бир томонлама функцияси дейилади. Бу функция мураккаб бўлмай, унинг аниқланиши учун, элементар сонлар назариясидан баъзи маълумотлар керак бўлади.

Мусбат бутун бўлган i ва n сонларининг энг катта умумий бўлувчисини ЭКУБ (i,n) деб белгилаймиз. Мисол учун: ЭКУБ(12, 18)=6, ЭКУБ(9, 27)=9. Ҳар қандай мусбат бутун сон n учун Эйлер функцияси $\varphi(n)$, n дан катта бўлмаган ЭКУБ(i,n) =1 шартни қаноатлантирувчи барча i сонларининг саноғини билдиради. Мисол учун:

$\varphi(2)=1, \varphi(3)=2, \varphi(4)=2, \varphi(5)=4, \varphi(6)=2$ ва ҳоказо. Ихтиёрий туб сон p учун $\varphi(p)=p-1$, ҳамда $\varphi(1)=1$ деб қабул қилинган. Бундан ташқари, ихтиёрий p ва q туб сонлари учун ушбу $\varphi(pq)=(p-1)(q-1)$ ифода ўринли бўлади. Мисол учун:

$\varphi(6)=\varphi(2x3)=1\cdot 2=2$.

Буюк математик олим Эйлер(1707-1783) теоремасига кўра ихтиёрий мусбат бутун x ва n ($0<x<n$) сонлари учун ЭКУБ(x,n)=1 шартини қаноатлантирувчи $x^{\varphi(n)} = 1 (\bmod\ n)$ тенглик бажарилади. Мисол учун:

ЭКУБ(5,6)=1 ва $5^2 = 1 (\bmod\ n)$.

Сонлар назарияси курсидан маълумки, агарда, e ва m бутун сонлар $0<e<m$

ва ЭКУБ*(m,e)=1* шартларни қаноатлантирса, у ҳолда *0<d<m* тенгсизликни ва

$$de = 1 \bmod n$$

тенгликни қаноатлантирувчи ягона *d* бутун сон мавжуд бўлиб, ЭКУБ*(m,e)* ни топишнинг «кенгайтирилган» Евклид алгоритмидан фойдаланиб *d* ни топиш мумкин.

Юқорида келтирилган маълумотлардан фойдаланиб махфий услубли RSA бир томонлама функциянинг аниқланишини кўриб чиқамиз. Бу функция бирор *n* сони модули бўйича дискрет даражага кўтариш функцияси, яъни

$$f_z(x) = x^e \bmod n$$

кўринишида аниқланади. Бу ерда: *x*- мусбат бутун сон бўлиб, *n=pq* сондан катта эмас; *n=pq*, яъни *p* ва *q* туб сонлари учун $\varphi(n) = (p-1)(q-1)$; бутун е сони $\varphi(n)$ дан кичик ва ЭКУБ$(e, \varphi(n)) = 1$. Шифрлашнинг E_z очиқ алгоритми асосини ташкил этувчи $y = f_z(x) = x^e (\bmod n)$ функция қийматларини ҳисоблашни осонгина квадратга кўтариш ва кўпайтириш амалларига келтириш мумкин. E_z алгоритмни очиқ калитлар базасига (китобига) киритиш, *n* ва *e* сонларини фойдаланувчилар учун очиқ эълон қилиш демакдир ва бунда *n* сонининг кўпайтувчилари бўлган *p* ва *q* туб сонлари махфий тутилади. Тескари функция қуйидаги

$$f_z^{-1}(y) = y^d \bmod n$$

кўринишда бўлиб, бу ерда *d* сони *n* сонидан кичик ва ушбу

$$de = 1 \bmod \varphi(n)$$

тенгликни қаноатлантиради.

p,q,d –сонларидан иборат*{p,q,d}=z* параметрлар тўплами $f_z(x) = x^e \bmod n$ тенглик билан аниқланган бир томонлама функциянинг криптографик махфийлик услуби хоссасининг асосини ташкил этади. Махфий D_z дешифрлаш алгоритмининг асосини ташкил этувчи тескари f_z^{-1}

функциянинг қийматларини ҳисоблаш ҳам квадратга кўтариш ва кўпайтириш амаллари орқали амалга оширилади ва бунда даража кўрсаткичи бўлган d сони ЭКУБ($e,\varphi(n)$) ни ҳисоблашнинг Евклид алгоритми бўйича аниқланади. Юқорида $f_z^{-1}(y) = y^d \bmod n$ ифода билан аниқланган функциянинг $f_z(x) = x^e \bmod n$ ифода билан аниқланган функцияга ҳақиқатан ҳам тескари функция эканлиги қуйидагича кўрсатилади. Бутун сонлар арифметикасидан маълумки, бирор бутун Q сонида

$$de = 1 \bmod n = \varphi(n) \cdot Q + 1$$

тенглик ўринли бўлади. Юқоридаги тенгликларга ва Эйлер теоремасига кўра

$$f_z^{-1}(y) = y^d \bmod n = (x^e)^d \bmod n =$$
$$= x^{\varphi(n)Q+1} \bmod n = (x^{\varphi(n)Q} x) \bmod n = x \bmod n$$

тенгликка эга бўлинади. Демак, $de = 1 \bmod n = \varphi(n) \cdot Q + 1$ тенгликни қаноатлантирувчи d ва e сонлари учун: бирор $x<n$ сонларнинг n модуль бўйича d даражага кўтариш амали, шу x сонларни худди шу n модуль бўйича e даражага кўтариш амалига тескари экан. Энди нима учун Р.В. Ривест, А.Шамир ва Л. Адлман юқорида келтирилган ифода билан аниқланган $f_z(x)$ функцияни n ва e сонларини билган ҳолда, унга тескари $f_z^{-1}(y)$ функцияни ҳисоблаш мумкин эмаслиги таъкидлаганганлигини кўриб чиқамиз. Бундан ташқари p ва q туб сонлари қандай қилиб танланганда, рақиб томоннинг бу сонларни била олмаслигини ҳам кўриб чиқамиз.

Рақиб томонга n ва e сонлари маълум бўлсин. Агарда рақиб томон n сонини p ва q туб сонларининг кўпайтмасидан иборат, яъни $n=pq$ кўринишида ифодалай олса, у ҳолда махфийлик параметри $z=\{p,q,d\}$ ни тўла аниқлаган ҳолда, маълумотлар криптограммасини, маълумотни ҳақиқатан ҳам олиши керак бўлган фойдаланувчи каби, қийинчиликсиз дешифрлаш имкониятига эга бўлади. Шунинг учун RSA криптотизимининг бардошлилик даражаси n сонини p ва q туб сонларининг кўпайтмасига ёйишнинг қийинлик

даражасига эквивалентдир, яъни тенг кучлидир. Агарда p ва q сонларининг узунлиги 300 дан ортиқ ўнли рақамдан иборат бўлса, ҳозирги замонавий ҳисоблаш техникаларидан фойдаланилганда, n сонини туб кўпайтувчиларга ажратиш учун сарфланадиган вақт етарли даражада кўп бўлиб, бундай туб кўпайтувчиларга ажратиш билан шуғулланишининг амалий жиҳатдан мақсадга муофиқ эмаслиги келиб чиқади.

Юқоридаги мулоҳазалардан табиий равишда, «етарли даражада катта p ва q туб сонларини қандай аниқлаш мумкин?" –деган савол туғилади. Бундай саволга жавоб топиш учун Чебешев теоремасига мурожаат қиламиз: бирор бутун m сонидан кичик бўлган барча бутун сонлар тўпламидан танлаб олинган бирор сонни, туб сон бўлиш эҳтимоллиги $(\ln\ m)^{-1}$ қийматга яқин.

Мисол учун 10^{300} дан кичик бўлган барча мусбат бутун сонлар тўпламидан танлаб олинган бирор сонни туб сонга бўлиш эҳтимоллиги $(\ln 10^{300})^{-1} = -\frac{1}{300\ \ln 10}$ қийматга эга. Агарда бу танлаб олиш фақат 10^{300} дан кичик бўлган барча бутун мусбат тоқ сонлар тўпламида амалга оширилаётган бўлса, бу эҳтимоллик қиймати икки баробар кўпаяди. Тоқ сонлардан туб сонларни фарқлаш Ферма теоремасига асосланади: бирор p туб сонидан катта бўлмаган бутун мусбат сон учун

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

тенглик ўринлидир.

Мисол учун, 2^4=1mod5 ёки 3^4=1mod5. Агарда r сонининг туб ёки туб эмаслигини текширмоқчи бўлсак, r сонидан кичик бўлган бутун мусбат b сонини олиб

$$b^{r-1} = 1 \bmod\ r$$

тенглик бажарилишини текшириш кифоя:

- тенглик бажарилса r туб сон бўлиши мумкин, чунки бу муносабат r туб бўлишини зарурий шарти;

-тенглик бажарилмаса r туб сон эмас.

Шундай қилиб, агарда $b^{r-1} = 1 \bmod r$ муносабат ўринли бўлмаса қатъий ҳолда r сони туб эмас, деб айта оламиз. Аммо, $b^{r-1} = 1 \bmod r$ муносабат ўринли бўлса, фақат, r сони туб бўлиши мумкин, лекин қатъий ҳолда r туб сон, деб тасдиқлай олмаймиз.

Шунинг учун, r сони етарли даражада катта бўлиб, тасодифий олинган мумкин қадар кўп бутун мусбат b $(1 \le b < r)$ сонлари учун $b^{r-1} = 1 \bmod r$ муносабат бажарилса r сонининг туб эканлигига шунчалик кўп даражада ишонч ҳосил қилиш мумкин. Агарда b нинг уч юзта қийматида бу муносабат ўринли бўлса, у ҳолда r сонининг туб бўлмаслиги ҳодисасининг эҳтимоли қиймати $\frac{1}{2^{300}} = 2^{-300}$ га тенг бўлади.

Юқорида келтирилган алгоритмдан бугунги кунда ҳам бирор r сонининг тублигини аниқлашда фойдаланиб келинмокда.

Ҳар қандай очиқ калитли криптотизимнинг бардошлилиги очиқ маълумотга ёки унинг бирор қисмига мос келувчи шифрмаълумот маълум бўлганда, ҳамда шифрлаш алгоритми E_z маълум бўлганда, тўла шифрмаълумот дешифрлаш имконияти қанчалик мураккаблиги билан баҳоланади.

Шундай қилиб, очиқ калитли RSA алгоритми тизимидан фойдаланувчиларга калитлар генерация қилиш қуйидаги олдиндан маълум бўлган теоремаларнинг тадбиқига асосланган.

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, хамда $y=1 \bmod pq$ тенглик ўринли бўлади.

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

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

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

муносабат ўринли бўлади. Бундан эса ушбу муносабат

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

$(x, n) = 1$ 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 модул p бўйича ҳам ва модул q бўйича ҳам 0 га тенг бўлиб, бундан ушбу

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

тенгликнинг ўринлилиги келиб чиқади.

Келтирилган теоремалардан фойдаланиб, тизимнинг ҳар бир i-фойдаланувчиси учун (e_i, d_i) -калитлар жуфтлиги яратилади (генерация қилинади). 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 калит деб эълон қилинади.

Шундан сўнг 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 хосил қилинади.

Кўриб ўтилганидек, RSA очиқ калитли шифрлаш алгоритми берилган етарли катта тоқ сонни туб кўпайтувчиларга ажратишнинг рационал усули мавжуд эмаслигига асосланган. Кейинги параграфда дискрет логарифмлаш

масаласини характеристикаси етарли катта бўлган чекли майдонда ҳисоблашнинг мураккаблигига асосланган Эл-Гамал алгоритми ўрганилади.

2.2. Эль-Гамал асимметрик шифрлаш алгоритми таҳлили ва уни такомиллаштириш

Эл–Гамал алгоритми RSA алгоритмига муқобил (алтернатив) бўлиб, бу криптоалгоритмларнинг калитларини ўлчов узунликлари тенг бўлганда бир хил криптобардошлиликга эга бўладилар.

Эл–Гамал криптоалгоритми Диффи-Хеллман алгоритмига ўхшаш бўлиб, дискрет логарифмларни ҳисоблаш масаласи ечимининг мураккаблигига асосланган. Бу криптоалгоритм асосини туб бўлган p ва бутун бўлган a сонлари ташкил этади. Қуйида ушбу алгоритмнинг моҳиятини очиб берувчи мисолни келтирамиз.

Бирор фойдаланувчи (А) махфий калит x сонини танлаб олади ва $y = a^x \bmod p$ бўлган очиқ калитни ҳисоблайди. Агарда мана шу фойдаланувчи (А) билан бирор бошқа фойдаланувчи (Б) махфий маълумот алмашинувини амалга оширмоқчи бўлса, у ҳолда (Б) p сонидан кичик бўлган бирор криптотизим сони k ни танлаб олиб

$$y_1 = a^k \bmod p \quad \text{ва} \quad y_2 = (m / y^k) \bmod p,$$

сонларини ҳисоблайди. Сўнгра (Б) $(y_1;y_2)$ маълумотларини (А)га жўнатади. Ўз навбатида (А) бу шифрланган маълумотни қабул қилиб, қуйидагича

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

ҳисоблаш билан очиқ маълумотни тиклайди.

Эл-Гамал криптоалгоритмига асосланган криптотизимнинг ҳар бир i-

фойдаланувчиси учун (y_i, x_i) -калитлар жуфтлиги қуйидагича яратилади: 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 $y_i = g_i^{x_i} \bmod p_i$ (фойдаланучилар гуруҳи учун $x_i < p$ ҳамда $y_i = g^{x_i} \bmod p$) орқали ҳисобланади. Шундай қилиб, (p_i, g_i, y_i) –учлик (фойдаланувчилар гуруҳи учун p ва g умумий бўлиб, (p, g, y_i)) –учлик) очиқ калит, x_i -эса махфий 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**: $b_j \Big/ a_j^{x_j} \bmod p_j = M$ (p ва g умумий бўлганда: $b \Big/ a^{x_j} \bmod p = M$), ҳақиқатан ҳам, $b_j \Big/ a_j^{x_j} \bmod p_j \equiv g_j^{x_j k} M \Big/ g_j^{k x_i} \bmod p_j \equiv M$ (p ва g умумий бўлганда: $b \Big/ a^{x_j} \bmod p \equiv y_j^k M \Big/ a^{x_j} \bmod p \equiv g^{x_j k} M \Big/ g^{k x_j} \bmod p = M \bmod p = M$, чунки $M < p$).

Юқорида кўриб ўтилган У. Диффи ва М.Е. Хеллиманнинг бир томонлама функцияси ҳамда RSA бир томонлама функцияси очиқ калитли

криптотизимларнинг хоссаларини етарли даражада очиб беради. Бу бир томонлама функциялардан ташқари ҳам кўплаб бир томонлама функциялар криптология соҳасидаги илмий нашрётларда эълон қилинган. Уларнинг баъзилари криптотизимларга қўйилган талабларга етарли даражада жавоб бермаган. Шуни таъкидлаш жоизки, назарий жиҳатдан бир томонлама бўлган функция сифатида ихтиёрий иккита сатри ёки устуни пропорционал бўлган $A_{n\times n}$-матрицали $A_{n\times n}x_{n\times 1} \bmod 256 = y_{n\times 1}$ акслантиришни мисол сифатида келтириш мумкин, бу ерда $x_{n\times 1}$ ва $y_{n\times 1}$ вектор элементлари байтлардан иборат. Бундай хоссага эга бўлган матрицанинг деатамаанти нолга тенг бўлиб, унинг тескариси мавжуд эмас. Бу матрицани бирор бошқа матрицага кўпайтмасидан ҳосил бўлган матрицанинг деатамаанти ҳам яна нолга тенг бўлиб, унга тескари матрица топиш имконияти йўқ. Матрицали акслантиришлар кўплаб шифрлаш алгоритмларида самарали қўлланилган [1-8].

Қуйида эллиптик эгри чизиқ нуқталари устида амал бажариш мураккаблиги асосида яратилган такомиллашган Эль-Гамал типидаги янги асимметрик шифрлаш алгоритми модели келтирилади.

Шундай қилиб, **биртомонламалик муносабати ифодаси функцияси модели:**

$Q = [d]G = (x_Q, y_Q)$ бўлиб, $G = (x_G, y_G)$-тартиби n- етарли катта сон бўлган маълум базавий нуқта, d - маҳфий ҳисобланиб 0<*d*<*n*.

Очиқ калит : $Q = (x_Q, y_Q)$.

Маҳфий калит: d - маҳфий калит, деб қабул қилинади.

Вариант-1. Шифрлаш акслантиришлари ифодалари модели:

$[k]G = T = (x_T, y_T)$ ҳамда $[k]Q = F = (x_F, y_F)$ бўлиб, $y_1 = (x_T, y_T) \bmod p$ ва $y_2 = M/x_F \pmod p$ ёки $y_2 = M/y_F \pmod p$, k-шифрловчи томонидан танлаб олинадиган ихтиёрий сон, p-маълум етарли катта туб сон.

Жуфтлик $(y_1, y_2) = C$ - шифр маълумот.

Бўлиш амали ўрнига бошқа амалдан, мисол учун ⊕-XOR амалидан

фойдаланиш мумкин.

Дешифрлаш акслантиришлари ифодалари модели: Очиқ маълумот ушбу $(w_1 \cdot y_2) \bmod p = M$ акслантириш билан олинади, бу ерда $[d]y_1 = [d]T = W = (x_W, y_W)$ бўлиб, $w_1 = x_W \bmod p$ ёки $w_1 = y_W \bmod p$

Агар шифрлашда бўлиш амалидан бошқа амал фойдаланилганда, дешифрлашда кўпайтмадан эмас, шу амалга тескари амалдан фойдаланилган бўлар эди.

Вариант-2. Шифрлаш акслантиришлари ифодаси модели:

$[k]G = T = (x_T, y_T)$ ҳамда $[k]Q = F = (x_F, y_F)$ бўлиб, $y_1 = (x_T, y_T) \bmod p$ ва $y_2 = M \oplus x_F (\bmod p)$ ёки $y_2 = M \oplus y_F (\bmod p)$, k -шифрловчи томонидан танлаб олинадиган ихтиёрий сон. p -маълум етарли катта туб сон.

Жуфтлик $(y_1, y_2) = C$ - шифр маълумот ҳисобланади.

Дешифрлаш акслантиришлари ифодаси модели:

Очиқ маълумот $(w_1 \oplus y_2) \bmod p = M$ акслантириш билан олинади, бу ерда $[d]y_1 = [d]T = W = (x_W, y_W)$ бўлиб, $w_1 = x_W \bmod p$ ёки $w_1 = y_W \bmod p$.

Умумий ҳолда, бўлиш ва $\oplus$-XOR амаллари ўрнига бошқа криптобардошликни таъминловчи амаллардан фойдаланиш мумкин. Дешифрлаш жараёни шифрлашда фойдаланилган амалга тескари амал билан амалга оширилади.

Такидлаш жоизки, Эль-Гамал шифрлаш алгоритмида очиқ ва маҳфий калитлар ушбу $y = g^x \bmod p$ –биртомонли функция асосида генерация қилинади, яъни x_i қиймат – маҳфий калит, унга мос келувчи $g^{x_i} \bmod p = y_i$ – очиқ калит деб қабул қилинади, y_i –қийматни билган ҳолда x_i –қийматни аниқлаш дискрет логарифмлаш масаласи ечими мураккаблиги билан боғлиқ.

Таклиф этилган янги асимметрик шифрлаш алгоритмларида очиқ ва маҳфий калитлар ушбу $Q = [d]G = (x_Q, y_Q)$ –биртомонли акслантириш асосида генерация қилинади, яъни d қиймат – маҳфий калит, унга мос келувчи $Q = [d]G = (x_Q, y_Q)$ – нуқта координаталари очиқ калит деб қабул қилинади,

Бунда $Q = (x_Q, y_Q)$ –нуқтани билган ҳолда d –қийматни аниқлаш эллиптик эгри чизиқ нуқталарини қўшишда келиб чиқадиган катта сонлар устида амаллар бажарилиши билан боғлиқ ҳисоблаш мураккабликларига асосланади.

2.3. Янги таклиф этилган такомиллаштирилган Эль-Гамал асимметрик шифрлаш алгоритмининг қўллашни функционал схемаси асослари

Янги таклиф этилган Эль-Гамал туркумидаги асимметрик шифрлаш алгоритмини амалда қўлланилишини таъминлаш учун криптографик тизим фойдаланувчилари учун умумий бўлган эллиптик эгри чизиқни (ЭЭЧни) ва унда тартиби туб ва етарли катта бўлган рационал координатали базавий нуқтани олдиндан танлаб олиш лозим.

ЭЭЧқа асосланган криптографик алгоритмлар билан иш кўрилганда унинг қуйидаги кўринишдаги ифодасидан фойдаланилади [1-3, 6-10, 15, 41, 53, 63, 101-104]:

$$(E): \quad y^2 = (x^3 + ax + b) \bmod p, \qquad (1)$$

бу ерда коэффициентлар a, $b \in F_p$ нолдан фарқли бўлиб, характеристикаси $p>3$ бўлган F_p сонли майдонда аниқланган, бундан ташқари $4a^3 + 27b^2$ ифоданинг қиймати p модуль бўйича нолдан фарқли, яъни $(4a^3 + 27b^2) \bmod p \neq 0$.

Ушбу ифода

$$J(E) \equiv 1728 \frac{4a^3}{4a^3 + 27b^2} (\bmod \ p)$$

(E) ЭЭЧ инвариати дейилади ва шу (1) ифода билан аниқланган ЭЭЧ инварианти билан аниқланган мос

$$(E_1): y^2 \equiv (x^3 + 3kx + 2k) \bmod p$$

ЭЭЧ инвариантига тенг, бу ерда:

$a \equiv 3k \pmod{p}, \quad b \equiv 2k \pmod{p}$, где $k \equiv \frac{J(E)}{1728 - J(E)} \pmod{p}$, $J(E) \neq 0$ ва $J(E) \neq 1728$.

Шундай қилиб, агар:

1) Коэффициентлар $a, b \in F_p$, $p>3$, сонли майдоннинг нолдан фарқли эдементлари бўлса;

2) Ушбу $4a^3 + 27b^2$ ифоданинг $p>3$ модуль бўйича қиймати нолдан фарқли, яъни $(4a^3 + 27b^2) \bmod p \neq 0$ бўлса, $y^2 = x^3 + ax + b = 0$ куб тенгламанинг дискриминанти

$$D = \left(\frac{a}{3}\right)^3 + \left(\frac{b}{2}\right)^2 = \frac{4a^3 + 27b^2}{108} = \frac{16 \cdot 4a^3 + 27 \cdot 16b^2}{16 \cdot 108} =$$

$$\frac{16 \cdot 4(3k)^3 + 27 \cdot 16(2k)^2}{1728} = \frac{4^3 \cdot 3^3 \cdot k^3 + 3^3 \cdot 4^3 \cdot k^2}{4^3 \cdot 3^3} = k^3 + k^2$$

қийматининг нолдан фарқли бўлиши ҳамда унинг қийматининг ишораси касрнинг суратидаги ифода $4a^3 + 27b^2$ қиймати билан аниқланади: $D > 0$, $D < 0$, $D = 0$ бўлиб, бу шартларга мос равишда битта ҳақийқий ва иккита комплекс, учта ҳар хил ҳақийқий, учта ҳақийқий ва булардан иккитаси тенг бўлган илдизларга эга бўлишлигини аниқлайди ҳамда мос графикларга эга[1];

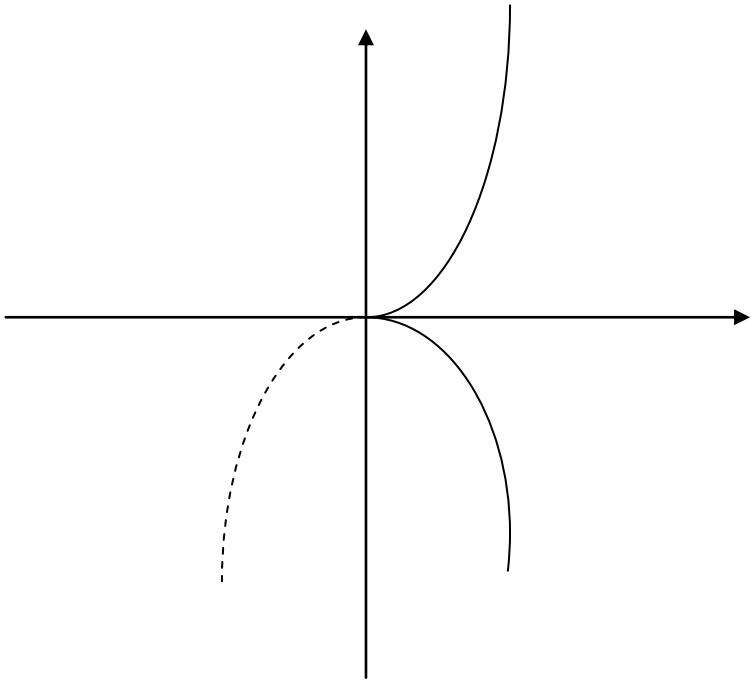
3) инвариант $J(E) \neq 0$ и $J(E) \neq 1728$ бўлса;

у ҳолда ЭЭЧ криптографиқ тадбиқлар учун самарали хусусиятларга эга бўлади, айниқса ЭРИ алгоритмларига тадбиқида муҳим аҳамиятга эга.

Коэффициентлар $a, b \in F_p$ майдоннинг нолдан фарқли элементлари бўлса, ЭЭЧ (1) ифодаси

$$y^2 = x^3 \bmod p, \qquad (2)$$

унинг графиги кўриниши



Ифода (2) билан аниқланган ЭЭЧнинг иҳтиёрий иккита P ва Q нуқталардан ўтувчи тўғри чизиқ уни улар йиғиндисини аниқловчи учинчи нуқтада кесиб ўтмаслиги мумкин. Коэффициентларнинг $a, b \in F_p$ нолдан фарқли бўлиши шартини талаб қилиниши шу ҳолат билан асосланади.

Қуйидаги шартни

$$(4a^3 + 27b^2) \bmod p \neq 0,$$

бажарилишини талаб этилиши танланаётган ЭЭЧнинг инварианти ифодаси махражида $4a^3 + 27b^2$ йиғиндининг қатнашиши билан боғлиқ:

$$J(E) \equiv 1728 \frac{4a^3}{4a^3 + 27b^2} (\bmod\ p) = [1728 \cdot 4a^3 \cdot (4a^3 + 27b^2)^{-1}] \bmod p =$$

$$= [1728 \cdot 4a^3 \cdot (4a^3 + 27b^2)^{p-2}] \bmod p.$$

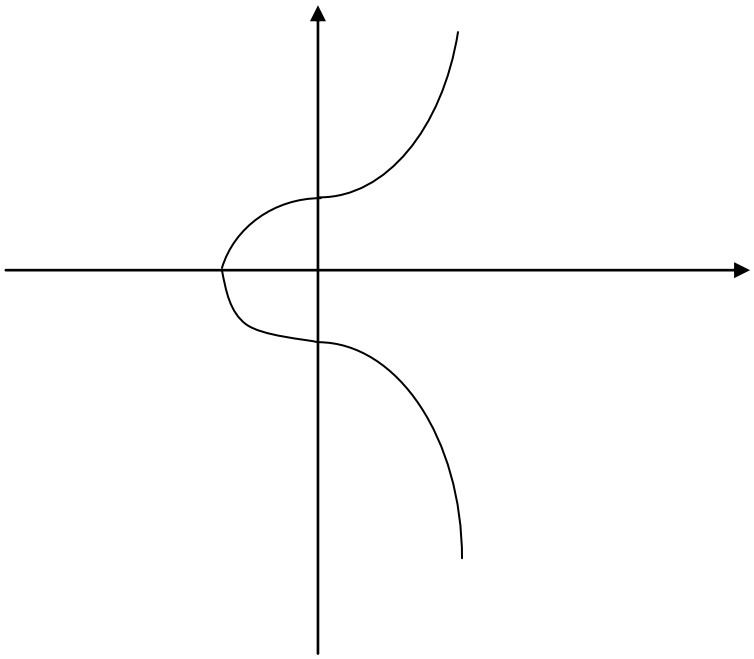
Агар $(4a^3 + 27b^2) \bmod p = 0$ бўлса, бундан $a \bmod p = 0$ ва $b \bmod p = 0$ келиб чиқади, чунки туб сон $p > 3$, яъни $p \neq 2$ ва $p \neq 3$ бўлиб, $(4a^3 + 27b^2) \bmod p = 0$ тенглик фақат ва фақат $a \bmod p = 0$ ҳамда $b \bmod p = 0$ бўлганда бажарилади. У ҳолда инвариантни ҳисоблашда аниқмаслик 0/0 келиб чиқади

$$J(E) = [1728 \cdot 4a^3 / (4a^3 + 27b^2)^{-1}] \bmod p = (1728 \cdot 0/0) \bmod p = (0/0) \bmod p.$$

Агар $a \bmod p = 0$ ва $b \bmod p \neq 0$ бўлса, у ҳолда ЭЭЧ тенгламаси ифодаси

$$y^2 = (x^3 + b) \bmod p, \qquad (3)$$

унинг графиги кўриниши



Ифода (3) билан аниқланган ЭЭЧнинг иҳтиёрий иккита P ва Q нуқталардан ўтувчи тўғри чизиқ уни улар йиғиндисини аниқловчи учинчи нуқтада кесиб ўтади. Аммо инвариант

$$J(E)=[1728\cdot 4a^3/(4a^3+27b^2)^{-1}]\bmod p=0,$$

бундан эса

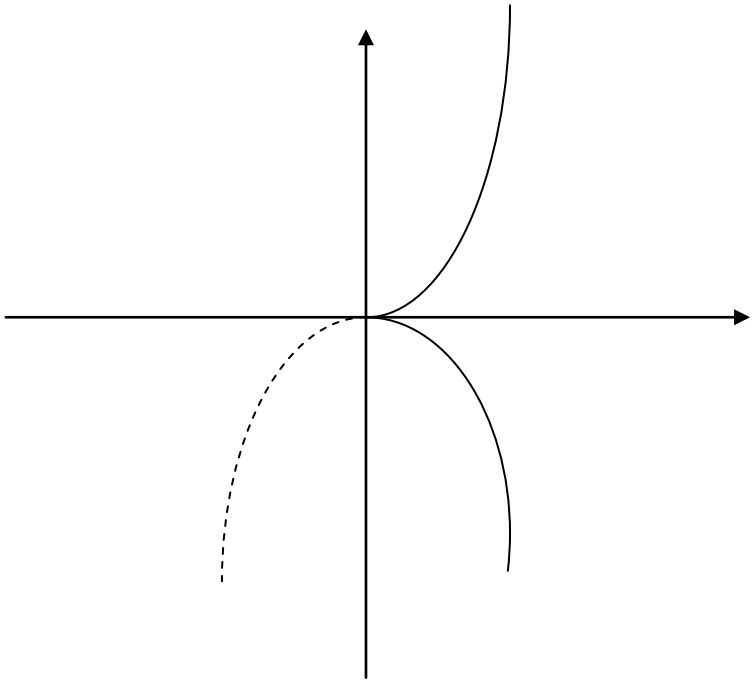
$$k \equiv \frac{J(E)}{1728 - J(E)} (\bmod\ p) = 0.$$

У ҳолда инвариант бўйича аниқланувчи ЭЭЧ коэффициентлари $a \equiv 3k (\bmod\ p) = 0, \quad b \equiv 2k (\bmod\ p) = 0$ бўлиб, унинг тенгламаси ифодаси (2) кўринишда бўлади ҳамда амалий тадбиққа қулайлик туғдирмайди.

Агар $a \bmod p \neq 0$ ва $b \bmod p = 0$ бўлса, у ҳолда ЭЭЧ тенгламаси ифодаси

$$y^2 = (x^3+ax) \bmod p = x(x^2+a) \bmod p, \qquad (4)$$

унинг графиги кўриниши (2) ифодадаги каби бўлиб, фарқи чизиқли қўшилувчи ax ҳад ҳисобига $0Y$ ўқи томонга кўпроқ ёндошган бўлади



Бундан ташқари инвариант

$$J(E)=(1728\cdot 4a^3/4a^3)\bmod p=1728 \bmod p\ ,$$

натижада

$$k \equiv \frac{J(E)}{1728 - J(E)} (\text{mod}\quad p) \equiv \frac{1728}{1728 - 1728} (\text{mod}\quad p) \equiv \frac{1728}{0} (\text{mod}\quad p) = \infty$$

бўлиб, ЭЭЧнинг $J(E) = 1728 \mod p$ инварианти бўйича топиладиган коэффициентлари аниқланмаган:

$$a \equiv 3k (\text{mod}\quad p) = \infty, \quad b \equiv 2k (\text{mod}\quad p) = \infty\ , \quad (4')$$

ҳамда бундай ЭЭЧ амалий тадбиқларга яроқсиз. Майдон характеристикасига қўйилган шарт $p. > 3$, инвариант бўйича ЭЭЧ коэффициентларини $a \equiv 3k (\text{mod}\quad p), \quad b \equiv 2k (\text{mod}\quad p)$ кўринишда аниқланиши билан боғлиқ, бундай аниқланган коэффициентлар 2 ва 3 сонларига пропорционал.

Бевосита ҳисоблаш орқали (1) ифодали (E) ЭЭЧ инварианти $J(E) \equiv 1728\ \frac{4a^3}{4a^3 + 27b^2} (\text{mod}\quad p)$ қиймати, унга мос равишда $k \equiv \frac{J(E)}{1728 - J(E)} (\text{mod}\quad p)$, бу ерда $J(E) \neq 0$ ва $J(E) \neq 1728$, қиймати билан коэффициентлари $a_1 \equiv 3k (\text{mod}\quad p)$ ва $b_1 \equiv 2k (\text{mod}\quad p)$ ифода билан аниқланадиган (5) ифодали (E_1) ЭЭЧ инварианти қийматига тенг. Ҳақиқатан ҳам:

$$J(E_1) \equiv 1728\ \frac{4\cdot(3k)^3}{4\cdot(3k)^3 + 27\cdot(2k)^2} (\text{mod}\quad p) \equiv 1728\cdot 4\cdot 27\cdot k^3\cdot(4\cdot 27\cdot k^3+27\cdot 4\cdot k^2)^{-1} (\text{mod}\ p) \equiv$$

$$\equiv 1728\cdot k\cdot(k+1)^{-1} (\text{mod}\ p) \equiv$$

$$\equiv 1728\cdot J(E)\cdot[1728- J(E)]^{-1}\cdot\{J(E)\cdot[1728- J(E)]^{-1}+1\}^{-1} (\text{mod}\ p) \equiv$$

$$\equiv 1728\cdot J(E)\cdot[1728- J(E)]^{-1}\cdot\{1728\cdot[1728- J(E)]^{-1}\}^{-1} (\text{mod}\ p) \equiv$$

$$\equiv 1728\cdot J(E)\cdot[1728- J(E)]^{-1}\cdot 1728^{-1}\cdot[1728- J(E)] (\text{mod}\ p) \equiv J(E) (\text{mod}\ p).$$

Юқорида такидланганидек:

$k \equiv J(E) \cdot [1728 - J(E)]^{-1} \pmod p \equiv$
$\equiv 1728 \cdot 4 \cdot a^3 \cdot (4 \cdot a^3 - 27 \cdot b^2)^{-1} \cdot (4 \cdot a^3 - 27 \cdot b^2) \cdot 1728^{-1} \cdot (27 \cdot b^2)^{-1} \pmod p \equiv$
$\equiv 4 \cdot a^3 / (27 \cdot b^2) (\mathrm{mod}\ p).$

Бундан, $a_1 \equiv 3 \cdot \frac{4a^3}{27b^2} (\mathrm{mod}\ p)$, $b_1 \equiv 2 \cdot \frac{4a^3}{27b^2} (\mathrm{mod}\ p)$.

ЭЭЧлар (1) ва (5) инвариантлари бўйича мос тушади, яъни инвариантлари тенг:

$$a_1 = 3 \cdot \frac{4a^3}{27b^2} (\mathrm{mod}\ p) = 3 \cdot \frac{4(3k)^3}{27(2k)^2} (\mathrm{mod}\ p) = 3k (\mathrm{mod}\ p)$$

ҳамда

$$b_1 = 2 \cdot \frac{4a^3}{27b^2} (\mathrm{mod}\ p) = 2 \cdot \frac{4(3k)^3}{27(2k)^2} (\mathrm{mod}\ p) = 2k (\mathrm{mod}\ p).$$

бўлиб, бу келтирилган шартларни қаноатлантирувчи ЭЭЧлар амалий тадбиқлар учун қулайлик туғдиради: характеристикаси $p > 3$ етарли катта туб сон бўлган чекли майдонда аниқланган ЭЭЧда рационал координатали нуқталарини қўшиш қоидасига зид бўлган муамолар келиб чиқмайди.

Шундай қилиб, қуйида **ЭЭЧда амаллар бажариш мураккаблиги билан боғлиқ асимметрик алгоритмларни амалий тадбиқлари асослари жараёнларининг функционал схемасини келтирилади:**

1. Амалий тадбиққа қулай ЭЭЧ танланади.

2. Танланган ЭЭЧда координаталарининг қиймати рационал сонлардан иборат $G = (x_G, y_G)$-тартиби n - етарли катта сон бўлган маълум базавий нуқта, Бу тартибни аниқловчи n соннинг туб сон бўлиши мақсадга мувофиқ, туб бўлмаса шу тартибни аниқловчи сондан кичик бўлган биринчи туб сонни ЭЭЧ нуқталари устида амал бажариш майдонининг характеристикаси сифатида қабул қилиш мумкинлиги алгоритм ҳусусиятларидан келиб чиққан ҳолда асосланади.

3. Биртомонламалик муносабати ифодаси функцияси модели асосида маҳфий ахборот алмашинуви тармоғининг ҳар бир i-фойдаланувчиси учун очиқ ва маҳфий калитлар ишлаб чиқарилади:

$Q_i = [d_i]G = (x_{Q_i}, y_{Q_i})$ бўлиб, $Q_i = (x_{Q_i}, y_{Q_i})$ -очиқ калит, d_i- маҳфий калит деб ҳисобланади, бу ерда такидланганидек, $G = (x_G, y_G)$-тартиби n - етарли катта сон бўлган маълум базавий нуқта, $0<d_i<n$.

4. Шундан сўнг i-фойдаланувчи томонидан j-фойдаланувчига шу j-фойдаланувчининг очиқ калитидан фойдаланиб M –очиқ маълумотни C – шифрланган маълумот кўринишида жўнатиш қуйидагича амалга оширилади:

Шифрлаш акслантиришлари ифодалари модели:

$[k]G = T = (x_T, y_T)$ ҳамда $[k]Q_j = F_j = (x_{F_j}, y_{F_j})$ бўлиб, $y_1 = (x_T, y_T) \bmod p$ ва $y_2 = M / x_{F_j} \pmod p$ ёки $y_2 = M / y_{F_j} \pmod p$, k-шифрловчи, яъни i-фойдаланувчи томонидан танлаб олинадиган ихтиёрий сон, p-базавий нуқтанинг туб тартиби ёки тартиби туб бўлмаган базавий нуқтанинг тартибидан кичик унга энг яқин бўлган туб сон.

Жуфтлик $(y_1, y_2) = C$ - шифр маълумот.

Бўлиш амали ўрнига бошқа амалдан, мисол учун $\oplus$-XOR амалидан фойдаланиш мумкин.

5. i-фойдаланувчидан C –шифрланган маълумотни қабул қилиб олган j-фойдаланувчи ўзининг маҳфий калитидан фойдаланиб M –очиқ маълумотни ҳосил қилади:

Дешифрлаш акслантиришлари ифодалари модели: Очиқ маълумот ушбу $(w_{1j} \cdot y_2) \bmod p = M$ акслантириш билан олинади, бу ерда

$[d_j]y_1 = [d_j]T = W_j = (x_{W_j}, y_{W_j})$ бўлиб, $w_{1j} = x_{W_j} \bmod p$ ёки $w_{1j} = y_{W_j} \bmod p$

Агар шифрлашда бўлиш амалидан бошқа амал фойдаланилганда, дешифрлашда кўпайтмадан эмас, шу амалга тескари амалдан фойдаланилган бўлар эди.

2-бўлим бўйича хулоса

1. Дискрет логарифимлаш масаласи ечими мураккаблиги асосидаги асимметрик шифрлаш алгоритмларининг криптографик хусусиятлари таҳлил қилиниб, уларнинг криптобардошлиги бўйича *ишончли бардошли криптоалгоритмлар* туркумига кираиши ҳамда *ишончли бардошли криптоалгоритмлар* мутахасислар томонидан ечилиши мураккаб деб тан олинган математик масалага асосланиши моҳияти тадқиқ қилинди. Дискрет

логарифимлаш масаласи ечими мураккаблиги асосидаги асимметрик шифрлаш ва ЭРИ алгоритмларининг криптографик хусусиятлари тадқиқ лари ёритилди.

2. Эль-Гамал асимметрик шифрлаш алгоритми таҳлил қилиниб, унинг ЭЭЧдаги такомиллаштирилган варианти ишлаб чиқилди. Бунда, биртомонламалик муносабати ифодаси функцияси модели:

$Q = [d]G = (x_Q, y_Q)$ бўлиб, $G = (x_G, y_G)$-тартиби n-етарли катта сон бўлган маълум базавий нуқта, d -маҳфий ҳисобланиб 0<*d*<*n*, Очиқ калит: $Q = (x_Q, y_Q)$

Маҳфий калит: d - маҳфий калит, деб қабул қилинади.

3. ЭЭЧда амаллар бажариш мураккаблиги билан боғлиқ асимметрик алгоритмларни амалий тадбиқлари асослари жараёнларининг функционал схемасини келтирилади:

1) Амалий тадбиққа қулай ЭЭЧ танланади.

2) Танланган ЭЭЧда координаталарининг қиймати рационал сонлардан иборат $G = (x_G, y_G)$-тартиби n - етарли катта сон бўлган маълум базавий нуқта, Бу тартибни аниқловчи n соннинг туб сон бўлиши мақсадга мувофиқ, туб бўлмаса шу тартибни аниқловчи сондан кичик бўлган биринчи туб сонни ЭЭЧ нуқталари устида амал бажариш майдонининг характеристикаси сифатида қабул қилиш мумкинлиги алгоритм ҳусусиятларидан келиб чиққан ҳолда асосланади.

3) Биртомонламалик муносабати ифодаси функцияси модели асосида маҳфий ахборот алмашинуви тармоғининг ҳар бир i-фойдаланувчиси учун очиқ ва маҳфий калитлар ишлаб чиқарилади.

4) Шундан сўнг i-фойдаланувчи томонидан j-фойдаланувчига шу j-фойдаланувчининг очиқ калитидан фойдаланиб M –очиқ маълумотни C – шифрланган маълумот кўринишида жўнатишни амалга оширилишининг ҳамда i-фойдаланувчидан C –шифрланган маълумотни қабул қилиб олган j-фойдаланувчи ўзининг маҳфий калитидан фойдаланиб M –очиқ маълумотни ҳосил қилиши жараёнлари кўрсатилди.

3-БЎЛИМ. ЯНГИ ТАКОМИЛЛАШТИРИЛГАН ЭЛЬ–ГАМАЛ АСИММЕТРИК ШИФРЛАШ АЛГОРИТМИНИНГ КРИПТОГРАФИК ТАСНИФИ ВА УНИНГ КРИПТОБАРДОШЛИГИНИ БАҲОЛАШ

3.1. Такомиллаштирилган Эль-Гамал асимметрик шифрлаш алгоритми криптобардошлик хусусиятлари кўрсаткичлари

Эл-Гамал шифрлаш алгоритми характеристикаси етарли катта бўлган чекли майдонда дискрет логарифмлаш масаласи мураккаблигини аниқловчи амалий биртомонламалик хусусиятли $y = g^x \bmod p$ функцияга асосланиб, маълум бўлган $\{y, g, p\}$-учлик орқали $x = \log_g x \bmod p$ қийматни топиш мураккаблиги билан боғлиқ. Маҳфий алоқа алмашинуви тармоғининг ҳар бир i-фойдаланувчиси учун $y_i = g^{x_i} \bmod p$ тенгликни қаноатлантирувчи y_i–очиқ ва x_i–маҳфий калитлар (y_i, x_i)–жуфтлиги ишлаб чиқилади.

Такомиллаштирилган янги Эл-Гамал шифрлаш алгоритмида очиқ ва маҳфий калитлар ушбу $Q = [d]G = (x_Q, y_Q)$–биртомонли акслантириш асосида генерация қилинади, яъни d қиймат – маҳфий калит, унга мос келувчи $Q = [d]G = (x_Q, y_Q)$– нуқта координаталари очиқ калит деб қабул қилинади, Бунда $Q = (x_Q, y_Q)$ –нуқтани билган ҳолда d –қийматни аниқлаш эллиптик эгри чизиқ нуқталарини қўшишда келиб чиқадиган катта сонлар устида амаллар бажарилиши билан боғлиқ ҳисоблаш мураккабликларига асосланади.

Бундан ташқари бир хил маълумотни ҳар хил шифрлаш ҳамда бир хил электрон хужжатга ҳар хил имзо қўйиш имкониятини берувчи шифрловчи томонидан танлаб олинадиган ихтиёрий k –сони ҳам мос равишда: Эл-Гамал шифрлаш алгоритмида дискрет логарифмни ҳисоблаш кўринишида қўлланилади, яъни $a = g^k \bmod p$, $b = y^k M \bmod p$; ЭЭЧ билан боғлиқ такомиллаштирилган янги Эл-Гамал шифрлаш алгоритмида $[k]G = T = (x_T, y_T)$ ҳамда $[k]Q_j = F_j = (x_{F_j}, y_{F_j})$ кўринишида.

Мутахасислар томонидан таън олинишича, кейинги йиллардаги тадқиқод, ҳисоб-китоб технологияларининг тадбиқи ЭЭЧда ҳисоблаш мураккаблиги билан боғлиқ алгоритмларнинг криптобардошлигини ишончли эканлигини тасдиқламоқда. АҚШ, Россия, Украина, Белорусия, Жанубий Корея стандарт ЭРИ алгоритмлари ЭЭЧга боғлиқ ҳисоблаш мураккаблиги билан боғлиқ.

3.2. Ахборот муҳофазасини таъминлашда такомиллаштирилган Эль-Гамал асимметрик шифрлаш алгаритмининг криптографик масалаларни ечишдаги моҳияти ва самарадорлиги

Юқорида i-фойдаланувчидан j-фойдаланувчига шу j-фойдаланувчининг очиқ калитидан фойдаланиб M–очиқ маълумотни C–шифрланган маълумот кўринишида жўнатиш протоколи (кетма-кетлиги) келтирилди. Такомиллаштирилган янги Эль-Гамал асимметрик шифрлаш алгаритмидан қуйидаги криптографик масалаларни ечишда самарали фойдаланиш мумкин [1-3]:

1. Калитларни рўйҳатга олиш маркази – КРОМ томонидан муҳофазаланган тизим фойдаланувчиларига маҳфий калитларни тарқатишда.

2. Маълумот маҳфийлигини таминлаш воситаси симметрик шифрлаш алгоритмлари калитларни ва асимметрик шифрлаш алгоритми калитларини тарқатишда.

3. Асимметрик шифрлаш алгоритмидан фойдаланган ҳолда имзоланадиган маълумотнинг хэш-функция қиймати (ва имкони бўлса имзоловчи томонидан иҳтиёрий танлаб олинадиган k-сонига) боғлиқ рақамли имзони амалга оширишда.

4. Махсус ЭРИ алгоритмлари маҳфий калитларини тарқатишда.

5. Глобал INTERNET ахборот тармоғининг иҳтиёрий иккита фойдаланувчиси томонидан Диффи-Хеллиман усули билан дискрет логарифмлаш ифодаси асосида RSA шифрлаш алгоритмидан фойдаланиш учун ўзларига очиқ ва маҳфий калитларни бевосита генерация қилишда.

Бу санаб ўтилганлардан ташқари электрон маълумотнинг тўлалиги ва бошқа келишмовчилик ҳамда мажаролик ҳолатларни ечимида самарали қўлланилади [1].

3-бўлим бўйича хулоса:

Янги такомиллаштирилган Эль–Гамал асимметрик шифрлаш алгоритмининг криптографик таснифи ва унинг криптобардошлигини баҳоланиб, криптографик масалаларни ечишдаги самарали тадбиқлари ёритилди.

ХУЛОСА

1. Ахборот муҳофазаси масалаларини криптографик усуллар билан ечишда асимметрик шифрлаш алгоритмларининг ўрни ва моҳияти тадқиқ этилиб, етарли катта натурал сонни туб кўпайтувчиларга ажратиш, характепистикаси етарли катта бўлган чекли майдонда дискрет логарифмлаш, ЭЭЧ нуқталарини қўшиш амали, номаълум параметрга боғлиқ ҳолда амаллар бажариш каби ҳисоблаш мураккабликларига асосланган амалий биртомонламалик хусусиятли акслантириш ифодаларига – функцияларига асосланиши ёритилди.

2. Очиқ ва маҳфий калитларни ишлаб чиқишда характеристикаси етарли катта бўлган чекли майдонда дискрет логарифмлаш мураккаблиги масаласи ечими мураккаблиги билан боғлиқ биртомонламалик хоссасига асосланган Эль-Гамал асимметрик шифрлаш алгоритмининг криптографик хусусиятлари таҳлил қилиниб, унинг очиқ ва маҳфий калитларни ишлаб чиқишда ЭЭЧ рационал координатали нуқталарини қўшиш билан боғлиқ ҳисоблаш мураккабликлари негизидаги варианти таклиф этилди. Бунда Эль-Гамал асимметрик шифрлаш алгоритмининг асосини ташкил этувчи акслантиришлар ифодалари сақлаб қолинган.

3. ЭЭЧ рационал координатали нуқталарини қўшиш билан боғлиқ ҳисоблаш мураккабликлари негизидаги биртомонламаликка боғлиқ ҳолда очиқ ва маҳфий калитлар ишлаб чиқишга асосланган янги такомиллаштирилган Эль-гамал асимметрик шифрлаш алгоритмининг амалий тадбиқининг дастурий таъминотини яратишнинг функционал схемаси асослари яратилди.

4. Янги такомиллаштирилган Эль–Гамал асимметрик шифрлаш алгоритмининг криптографик таснифи ва унинг криптобардошлиги баҳоланиб, криптографик масалаларни ечишдаги самарали тадбиқлари ёритилди.

5. Дискрет логарифимлаш масаласи ечими мураккаблиги асосидаги асимметрик шифрлаш алгоритмларининг криптографик хусусиятлари

таҳлил қилиниб, уларнинг криптобардошлиги бўйича *ишончли бардошли криптоалгоритмлар* туркумига карши ҳамда *ишончли бардошли криптоалгоритмлар* мутахасислар томонидан ечилиши мураккаб деб тан олинган математик масалага асосланиши моҳияти тадқиқ қилинди. Дискрет логарифимлаш масаласи ечими мураккаблиги асосидаги ассимметрик шифрлаш ва ЭРИ алгоритмларининг криптографик хусусиятлари тадқиқ лари ёритилди.

6. Эль-Гамал асимметрик шифрлаш алгоритми таҳлил қилиниб, унинг ЭЭЧдаги такомиллаштирилган варианти ишлаб чиқилди. Бунда, биртомонламалик муносабати ифодаси функцияси модели:

$Q = [d]G = (x_Q, y_Q)$ бўлиб, $G = (x_G, y_G)$-тартиби n-етарли катта сон бўлган маълум базавий нуқта, d-маҳфий ҳисобланиб $0<d<n$, Очиқ калит: $Q = (x_Q, y_Q)$

Маҳфий калит: d - маҳфий калит, деб қабул қилинади.

7. ЭЭЧда амаллар бажариш мураккаблиги билан боғлиқ асимметрик алгоритмларни амалий тадбиқлари асослари жараёнларининг функционал схемасини келтирилади:

1) Амалий тадбиққа қулай ЭЭЧ танланади.

2) Танланган ЭЭЧда координаталарининг қиймати рационал сонлардан иборат $G = (x_G, y_G)$-тартиби n - етарли катта сон бўлган маълум базавий нуқта, Бу тартибни аниқловчи n соннинг туб сон бўлиши мақсадга мувофиқ, туб бўлмаса шу тартибни аниқловчи сондан кичик бўлган биринчи туб сонни ЭЭЧ нуқталари устида амал бажариш майдонининг характеристикаси сифатида қабул қилиш мумкинлиги алгоритм ҳусусиятларидан келиб чиққан ҳолда асосланади.

3) Биртомонламалик муносабати ифодаси функцияси модели асосида маҳфий ахборот алмашинуви тармоғининг ҳар бир i-фойдаланувчиси учун очиқ ва маҳфий калитлар ишлаб чиқарилади.

4) Шундан сўнг i-фойдаланувчи томонидан j-фойдаланувчига шу j-фойдаланувчининг очиқ калитидан фойдаланиб M –очиқ маълумотни C –

шифрланган маълумот кўринишида жўнатишни амалга оширилишининг ҳамда i-фойдаланувчидан C –шифрланган маълумотни қабул қилиб олган j-фойдаланувчи ўзининг маҳфий калитидан фойдаланиб M –очиқ маълумотни ҳосил қилиши жараёнлари кўрсатилди.

ФОЙДАЛАНИЛГАН АДАБИЁТЛАР РЎЙХАТИ

1. Акбаров Д. Е. Ахборот хавфсизлигини таъминлашнинг криптографик усуллари ва уларнинг қўлланилиши – Тошкент, «Ўзбекистон маркаси», 2009 – 434 бет.

2. Алферов А. П., Зубов А. Ю., Кузьмин А. С., Черемушкин А. В. Основы криптографии: Учебное пособие, 2-е изд. –М.: Гелиос АРВ, 2002.- 480 с.

3. Шнайер Б. Прикладная криптография. Протоколы, алгоритмы, исходные тексты на языке Си. –М.: издательство ТРИУМФ, 2003 - 816 с.

4. Шенон К. Э. Теория связи в секретных тизимх. В кн.: Шенон К.Э. Работы по теории информации и кибернетике. М.: ИЛ, 1963, том 1. - С. 333-402.

5. Шенон К. Э. Теория связи в секретных тизимх. В кн.: Шенон К.Э. Работы по теории информации и кибернетике. М.: ИЛ, 1963, том 2. -С. 243-332.

6. Diffie W. and Hellman M.E. «New directions in cryptography» IEEE Trans. Informat. Theory, vol. IT-22, pp. 644-654, Nov. 1976.

7. R. C. Merkle «Secure communication over insecure channels», Comm. ACM, pp. 294-299, Apr. 1978.

8. Харин Ю. С., Берник В.И., Матвеев Г. В., Агиевич С. Г. «Математические и комьютерные основы криптологии» ООО «Новое знание» 2003 г. 381 стр.

9. Ростовцев А. Г., Маховенко Е. Б., Теоретическая криптография. НПО «Профессионал», Санкт-Петербург. 2004г. - 478 стр.

10. Молдовян А. А., Молдовян Н. А., Советов Б. Я.. Криптография. – Санкт-Петербург, Изд. «Лань», 2001. – 224 с.

11. Венбо Мао. Современная криптография. Теория и практика. – Москва–Санкт-Петербург–Киев: Лори Вильямс, 2005. –768 с.

12. Коблиц Н. Курс теории чисел и криптографии. – М. Научное изд-во ТВП, 2001г. – 261 стр.

13. Акбаров Д.Е., Ахмадалиев Ш.Ш., Нуриев Ш.З. Криптология асосларида математика. Ўқув қўлланма. – Фарғона, 2003. – 48 б.

14. Акбаров Д. Е., Ясинский. Математика в становлении науки криптологии. – Киев. “Политехника”. 2001. – 42с.

15. Хасанов Х. П. Такомиллашган диаматрицалар алгебралари ва параметрли алгебра асосида криптотизимлар яратиш усуллари ва алгоритмлари. –Тошкент, 2008. -208 б.

16. Rueppel R. A. Stream ciphers // Contemporary Cryptology, The Science of Information Integrity. - New York, 1992. - P.p. 65-134.

17. Shamir A. On the generation of cryptografically strong pseudo-random sequences // ACM Trasaction on Computer Systems. 1983. vol. 1. - Pp. 38-44.

18. Siegenthaler T. Correlation-immunity of nonlinear combining functions for cryptographic applications // IEEE Trans. Inform. Theory. 1984. - Pp. 776-780.

19. Siegenthaler T. Decrypting a class of stream ciphers using ciphertext only // IEEE Trans. Comput. 1985. vol. C-34, - P.p. 81-85.

20. Арипов М., Пудовченко Ю. Основы криптологии. -Т.:НУУ, 2004. - 136 с.

21. Арипов М., Пудовченко Ю. Современные суперкомпьютеры и проблемы криптографической силовой атаки // - Т., НУУ, 2000. - 16 с.

22. Каримов М.М. Организация корпоративных компьютерных сетей с интегрированной системой защиты информации // Дис. на соискание доктора техн.наук. - Т.: ТашГТУ, 2003.

23. Каримов М.М., Сапарова Т.А. Шифрлашнинг блокли ва оқимли тизимларида махфий калитли замонавий криптография тенденциялари // ТАТУ хабарлари. - Т., 2008. - №4. - Б.35-39.

24. Агибалов Г.П. 50 лет криптографии в Томском государственном университете // Прикладная дискретная математика. 2009. - №2. - С.104-126.

25. Аграновский А.В., Хади Р.А. Практическая криптография. - М.: СОЛОН-Пресс, 2002. - 254 с.

26. Асосков А.В., Иванов М.А., Мирский А.А. Поточные шифры. - М.: Кудиц-Образ, 2003. - 336 с.

27. Винокуров А. Современность практической криптографии // Системы безопасности связи и телекоммуникаций. 2003. - №10. - С.218-221.

28. Гатчин Ю.А., Коробейников А.Г. Основы криптографических алгоритмов. Учебное пособие. - СПб.: ГИТМО(ТУ), 2002. - 29 с.

29. Щеглов А.Ю. Защита копьютерной информации от несанкционированного доступа. - СПб.: Наука и Техника, 2004. - 386 с.

30. Дернова Е.С., Костина А.А., Молдовяну П.А. Конечные группы матриц как примитив алгоритмов цифровой подписи // Вопросы защиты информации. - М., 2008. - №3(82). - С. 8-11.

31. Докучаев Д. Неслучайные числа. Взлом генератора случайных чисел -ULTIMATE-БАГ движка PHP // Хакер. - М., 2008. - №119. - С.58-59.

32. Дударев Д.А., Панасенко С.П. Аппаратные шифраторы фирмы «Анкад» гарантия надежной защиты данных // Вопросы защиты информации. - М., 2006. - №2(73). - С. 12-14.

33. Дуйков Е.А., Сотский С.В., Щербаков А.Ю., Кирин В.И. Формулирование требований к защищенному электронному документообороту // Вопросы защиты информации. - М., 2008. -№4(83). - С. 28-32.

34. Жельников В. Криптография от папируса до компьютера. - М.: ABF, 1997. - 336 с.

35. Жуков И.Ю., Иванов М.А., Осмоловский С.А. Принципы построения криптостойких генераторов псевдослучайных кодов // Проблемы информационной безопасности компьютерных систем.-М.,2001.№1. -С.55-65.

36. Жўраев И., Назаров А., Тешабекова Х. Ўзбекистон Республикаси давлат ахборот ресурслари: уларнинг ҳолати ва ривожлантириш йўллари // InfoCOM.UZ. - Т., 2008. - №3. - Б. 28-29.

37. Завгородний В.И., Комплексная защита информации в компьютерных системах. Учебное пособие. - М.: Логос, 2001. - 264 с.

38. Задонский А.Ю. Защита от утечек конфиденциальной информации в центрах обработки и хранилищах данных // Защита информации. INSIDE. - М., 2007. - №5. - С. 41-45.

39. Мусаев А.И. Криптобардошли алгоритмларни комбинациялашга асосланган узлуксиз шифрлаш алгоритми // ТАТУ хабарлари. - Т., 2010. - №2. - Б.21-24.

40. Мусаев А.И. Узлуксиз шифрлаш алгоритмларидан универсал криптобардошли хеш-функция яратиш // ТАТУ хабарлари. - Т., 2010. - №2. - Б.15-19.

41. Коробейников А.Г., Гатчин Ю.А. Математические основы криптологии. Учебное пособие. - СПб.: ИТМО, 2004. - 106 с.

42. Косов А.В. Современные методы тестрования криптографических программных средств // Защита информации. INSIDE.-М.,2007.-№6.-С.64-66.

43. Коутинхо С. Введение в теорию чисел. Алгоритм RSA. - М.: Постмаркет, 2001. - 323 с.

44. Куприянов А.О. Основы методологии проведения аудита информационной безопасности // Вопросы защиты информации. - М., 2006. - №4(75). - С. 2-5.

45. Минаси М. Шифровальщик Cipher // Windows IT Pro/RE. - М., 2008. - №3. - С. 94-95.

46. Моисеева П.Ю. Оценка возможностей организации по проектированию безопасных систем на основе стандарта ISO/IEC 21827 // Вопросы защиты информации. - М., 2006. - №3(74). - С.26-36.

47. Молдовян Н.А. Проблематика и методы криптографии. - СПб.:БХВ-Петербург, 1998. - 212 с.

48. Молдовян Н.А., Нгуен Л.М., Хо Н.З. Синтез поточных шифров на основе блочных преобразований : метод латинских квадратов // Вопросы защиты информации. - М., 2008. -№1(80). - С. 27-34.

49. Молдовян Н.А., Щилков М.В., Филиппов Д.М. Реализация процедуры усложнения ключа в скоростных шифрах на основе управляемх подстановочно-перестановочных сетей // Вопросы защиты информации. - М., 2007. - №4(79). - С.2-7.

50. Молдовян П.А., Дернова Е.С., Молдовян Д.Н. Синтез конечных расширенных полей для криптографических приложений // Вопросы защиты информации. - М., 2008. - №3(82). - С.12-16.

51. Молдовян Н. А., Молдовян А. А., Еремеев М. А. Криптография: от примитивов к синтезу алгоритмов. –СПб.: БХВ-Петербург, 2004. - 448 с.

52. Молдавян А. А., Молдавян Н. А., Гуц Н. Д., Изотов Б.В. Криптография. Скоростные шифры. –Санкт-Петербург. «БХВ-Петербург» 2002г. – 439 стр.

53. Молдавян А. А., Молдавян Н.А. Введение в криптосистемы с открытым ключом. Санкт – Петербург «БХВ-Петербург» 2005г. – 288с.

54. Зензин О. С., Иванов М. А.. Стандарт криптографической защиты – AES. Конечные поля /Под ред. М. А. Иванова – М.: КУДИЦ-ОБРАЗ, 2002. - 176 с.

55. Акбаров Д. Е. Криптография, Стандарты алгоритмов криптографической защиты информации и их приложения. –Ташкент, 2007. -188 с.

56. Иванов М. Криптографические методы защиты информации в компьютерных системах и сетях. – М., «Кудиц-Образ», 2001, –368с

57. Мухачев В.А., Хорошко В.А. Методы практической криптографии. Киев: Полиграф-Консалтинг, 2005. - 215 с.

58. Ожиганов А.А. Основы криптоанализа симметричных шифров. Учебное пособие. - СПб.: ИТМО, 2008. - 44 с.

59. Панасенко С.П. Защита от несанкционированного доступа // Вопросы защиты информации. - М., 2006. - №3(74). - С. 37-39.

60. Петров А.А. Компьютерная безопасность. Криптографические методы защиты. - М.:ДМК, 2000. - 448 с.

61. Романец Ю.В., Тимофеев П.А. Защита информации в компьютерных системах и сетях. - М.: Радио и Связь, 2001. - 376 с.

62. Ростовцев А.Г. Алгебраические основы криптографии. - СПб.:Мир и Семья, 2000. - 296 с.

63. Ростовцев А.Г., Маховенко Е.Б. Введение в криптографию с открытым ключом. - СПб.: Мир и Семья, 2001. - 336 с.

64. Рябко Б.Я., Фионов А.Н. Криптографические методы защиты информации: Учебное пособие для вузов. - М.: Горячая линия-Телеком, 2005. - 229 с.

65. Рябко Б.Я., Фионов А.Н. Основы криптографии для специалистов в информационных технологиях. - М.:Научный мир, 2004. - 173 с.

66. Скляров Д.В. Исскуство защиты и взлома информации. - СПб.: БХВ-Петербург, 2004. - 288 с.

67. Снеддон Р., Вилански Э. Технология Kerberos для обеспечения безопасности MOSS 2007 // Windows IT Pro/RE. - М., 2008. - №5. - С.38-45.

68. Стахов А.П. «Золотая» криптография // Перспективные информационные технологии и интеллектуальные системы. 2006. № 4. - С.48-55.

69. Тужилин М.Э. Почти совершенные нелинейные функции // Прикладная дискретная математика. 2009. - № 3. - С.14-20.

70. Фергюсон Н., Шнайер Б., Практическая криптография. - М.: Вильямс, 2005. - 424 с.

71. Шалыто А.А. Методы аппаратной и программной реализации алгоритмов. - СПб.:Наука, 2001. - 777 с.

72. Хасанов П.Ф., Исаев Р.И., Назарова М.Х., Хасанов Х.П., Ахмедова О.П. Ахборотнинг криптографик муҳофазаси тарихи. Компьютер криптографияси даври // Алоқа дунёси. - Т., 2006, - №1(6). - Б. 59-74.

73. Акбаров Д. Е. Разработка алгоритма цифровой подписи на основе композиции существующих сложностей // Инфокоммуникации: Сети-Технологии-Решения.-3 (7)/2008. -с. 46-49.

74. Акбаров Д. Е. Об одном алгоритме шифрования данных с симметричным ключом. // Инфокоммуникации: Сети-Технологии-Решения. -4(8)/2008. -с. 25-36.

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.

76. Акбаров Д. Е., Ахмадалив Ш.Ш., Хасанов П. Ф. Параметрли алгебра амалларидан фойдаланиб мавжуд ҳисоблаш мураккабликлари асосида янги асимметрик алгоритмлар яратиш усуллари //Инфокоммуникации: Сети-Технологии-Решения. -1(9)/2009. -с. 31-35.

77. Акбаров Д. Е., Мусаев А. И. Мавжуд узликсиз шифрлаш алгоритмлари асосларини тадқиқи ва уларнинг туркумлари //Инфокоммуникации: Сети-Технологии-Решения. -1(9)/2009. -с. 36-45.

78. Акбаров Д.Е., Камолов М.Э. Гаммалаштиришга асосланган самарали блоклаб шифрлаш алгоритми ва унинг аппарат қурилмасини яратишнинг функционал модели // ТАТУ хабарлари. Т., 2009. - №3. - Б.14-18.

79. Акбаров Д. Е., Собиров Ш.О. Скрытое использование параметра R эллиптической кривой, связанного случайно выбранной величиной, как параметр проверки подписи ЭЦП. //ФарПИ Илмий-техника журнали. -2009, №1.-с. 3-11.

80. Акбаров Д. Е., Мусаев А. И. Чекли майдонда матрицали кенгайтириш ва жадвалли сиқиш акслантиришларига асосланган узликсиз шифрлаш алгоритми //Кимёвий технология, назорат ва бошқарув. Илмий-техникавий журнал. -3/2009. - с. 47-50.

81. Акбаров Д.Е., Собиров Ш.О., Саидов М.И. О функциональной схеме приложения электронно-цифровой подписи в электронном документообороте // ФерГУ. Научный вестник. 2009 № 1. с. 3-9.

82. Акбаров Д.Е., Собиров Ш.О., Саидов М.И. Алгоритм ЭЦП со скрытым использованием параметра R эллиптической кривой, связанного

случайно выбранным параметром // ФерГУ. Научный вестник. -2009 № 2. -с. 3-11

83. Акбаров Д.Е., Собиров Ш.О. Маълумотларни шифрлашнинг симметрик калитли алгоритми яратиш // ФарПИ Илмий-техника журнали. -2009 № 2. -с. 3-6.

84. Акбаров Д.Е., Собиров Ш.О. Азизов Э.Ю. Шифрлаш алгоритм орқали эллиптик эгри чизиқ *R* параметрини ЭРИ текширишнинг яширин параметри сифатида ишлатиш // ФарПИ Илмий-техника журнали. -2009 № 3. -с. 3-7

85. Акбаров Д.Е., Собиров Ш.О. Алгоритм ЭЦП на эллиптической кривой в композиции сложностей вычисления дискретного логарифмирования и факторизации натуральных чисел на простые множители // Интернет журнал «Аспирант и соискатель» www.sputnikplus 2000 @ mail. ru. -2009 г. июнь.

86. Акбаров Д.Е., Собиров Ш.О., Азизов Э.Ю. Latent use of parameter R of the elliptic curve, as parameter ofcheck eds, with application of algorithm of enciphering It promotion in asia 2009, September 21-25, Tashkent University of IT) // Труды ммеждународной конференции. -с. 187-191.

87. Акбаров Д.Е., Тураев Б.Т. Электрон ҳужжатли маълумот алмашинуви муҳофазасида криптографик воситалар композицияси моделларидан фойдаланиш // ТАТУ хабарлари. Т., 2009. - №2. - Б.32-37.

88. Акбаров Д.Е., Тураев Б.Т. Калитларни муҳофазаланган ҳолда тақсимлашни бошқариш алгоритмлари математик ва функционал асослари// ТДУ Хабарлари журнали. - **********

89. Тураев Б.Т. Ахборот коммуникация тизимида маълумот алмашинуви муҳофазасида криптографик воситалар композицияси моделларидан фойдаланиш // Республиканский семинар: «Информационная безопасность в сфере связи и информатизации. Проблемы и пути их решения» Сборник тезисов и докладов Ташкент 29 октября 2010 год

90. Turaev B.T, Komolov M.E, Adenov B.E., Cryptographic protection of

the information in information-telecommunication systems with application of composite models It promotion in asia 2009, September 21-25, Tashkent University of IT) // Труды ммеждународной конференции. -с. 192-195.

91. Тураев Б.Т., Ходжаев А.М. Компьютер тармокларида хужжатли маълумотларни кафолатли алмашинувини таъминлаш. // ********

92. Дейтель Г. Введение в операционные системы. Том 2. М.: Мир, 1987, с. 357-371.

93. Феллер В. Введение в теорию вероятностей и ее приложения. Том 2. М.: Мир, 1984.

94. Кнут Д. Искусство программирования для ЭВМ. Том 1. Основные алгоритмы. М.: Мир, 1976.

95. Гэри М. , Джонсон Д. Вычислительные машины и труднорешаемые задачи. М.: Мир, 1982.

96. Simmons G. J. «Authentication theory/coding theory, in Advances in Cryptology, Proceedings of CRYPTO 84, G. R. Blakley and D. Chaum, Eds. Lecture Notes in Computer Sciense, No. 196. New York, NY: Springer, 1985, pp. 411-431

97. Xiao G. Z., Massey J. L.A spectral characterization of correlation-immune functions. // IEEE Trans. Inform. Theory. 1988. - Pp. 569-571

98. Бабаш А. В., Шанкин Г. П. Криптография. –Москва: Лори Гелиос АРВ, 2002. –512 с.

99. Бабенко Л.К., Мишустина Е.А. Методическое пособие по изучению современных методов криптоанализа. - Таганрог, ТРТУ, 2003. - 66 с.

100. Баричев С.Г., Гончаров В.В., Серов Р.Е. Основы современной криптографии. - М.: Горячая линия-Телеком, 2001. – 250

101. Болотов А.А, Гашков С.Б., Фролов А.Б., Часовских А.А. Алгоритмические основы эллиптической криптографии.-Москва: Мэи, 2000.-100 стр.

102. Коблиц Н. Курс теории чисел и криптографии. – М. Научное изд-во ТВП, 2001г. – 261 стр.

103. Василенко О. Н. Теоретико-числовые алгоритмы в криптографии. – М., МЦНМО, 2003. – 328 с.

104. Венбо Мао. Современная криптография. Теория и практика. – Москва–Санкт-Петербург–Киев: Лори Вильямс, 2005. –768 с.