АССИММЕТРИК КРИПТОТИЗИМЛАРГА АСОСЛАНГАН КАЛИТЛАРНИ ТАҚСИМЛАШ АЛГОРИТМЛАРИНИНГ ТАДҚИҚИ

Мундарижа

КИРИШ

Бутун жаҳонда сўнгги йилларда ахборот технологияларининг жадал суръатлар билан ривожланиб бориши натижасида ахборот хавфсизлиги муаммоси Ўзбекистон Республикаси учун ҳам долзарб муаммога айланди. Ҳозирги кунга қадар ахборот хавфсизлигини таъминлашда энг ишончли воситалардан бири ахборотни криптографик ҳимоя қилиш воситалари ҳисобланади. Шу боис Республикамизда бу йўналиш жадал суръатлар билан ривожланмоқда. Президентимизнинг 2007 йил 3 апрелда қабул қилган «Ўзбекистон Республикасида ахборотнинг криптографик ҳимоясини ташкил этиш чора-тадбирлари тўғрисидаги» ПҚ-614–сон қарори шулар жумласидандир [2].

Ахборот-коммуникация тизимида маълумотларни махфий ёки конфиденциал алмашув жараёни учун криптографик тизимлар яратиш билан бир қаторда шу тизимда калитлар бошқариш масаласини ишончли ҳал этиш муҳим ўрин тутади. Чунки танланган криптотизим қанчалик мураккаб ва ишончли бўлмасин, ундан амалда фойдаланиш жараёнлари калитларни бошқариш масаласи билан боғликдир [1-5]. Агар маълумотларнинг махфий алмашинуви оз сонли фойдаланувчилар билан бўлса, калитлар алмашинуви жараёнида ноқулайликлар туғилмайди. Аммо ахборот-коммуникация тизимида маълумотларнинг махфий алмашинуви юзлаб, минглаб ва ҳатто миллионлаб фойдаланувчилар билан бўлса, калитларни бошқаришнинг ўзига хос алоҳида муҳим масалалари келиб чиқади.

Ҳозирги кунда ҳужжат алмашув тизимларида махфий шифрлаш калитларини тақсимлаш учун Диффи-Хеллман усулидан фойдаланилади ва бу усулга асосланган хорижий алгоритмлар ишлаб чиқилган [1-10].

Мазкур битирув малакавий иши ассимметрик криптотизимларга асосланган калитларни тақсимлаш алгоритмларининг тадқиқига қаратилганлиги унинг долзарблилигидан далолат беради.

Ушбу битирув малакавий ишини бажаришдан кўзланган мақсад эллиптик эгри чизиқларга асосланган ассимметрик калитларни тақсимлаш алгоритмларининг таҳлили ва тадқиқини амалга ошириш иборат.

Битирув малакавий ишининг вазифаси. Кўзланган мақсадни амалга ошириш учун битирув малакавий ишини бажаришда қуйидаги вазифалар қўйилди:

– калитларни тақсимлаш бўйича мавжуд алгоритмлар ва протоколларни тадқиқ ва қиёсий таҳлил этиш;

– калитларни тақсимлаш алгоритмларини маълум белгилар асосида таснифлаш;

– Ассимметрик алгоритмларга асосланган калитларни тақсимлаш алгоритмларининг таҳлил ва тадқиқи

– Ассимметрик калитларни тақсимлаш алгоритмларининг қиѐсий таҳлили ва криптобардошлилигининг таснифлашдан иборат.

1-БОБ. МАВЖУД ХАЛҚАРО КРИПТОГРАФИК КАЛИТЛАРНИ ТАҚСИМЛАШ УСУЛЛАРИ ВА ВОСИТАЛАРИ

1.1. Калитларни бошқариш масаласи

Ҳозирги кунда криптографик тизимлар ахборот хавфсизлигини таъминлашда энг ишончли воситалардан бири бўлиб, электрон ҳужжат айланиш ва электрон тўлов тизимларида электрон рақамли имзо шакллантириш ва аутентификация масалаларини ечиш учун фойдаланилади [8-11]. Криптографик тизимларда асосий тушунчалардан бири калит тушунчаси ҳисобланади. Криптографик калитлар носимметрик криптотизимлар учун очиқ ва махфий калитларнинг умумий номи бўлиб, электрон рақамли имзони ҳисоблаш ёки текшириш, шунингдек шифрлаш ва дастлабки матнга ўгириш учун қўлланиладиган символлар кетма-кетлигини ифодалайди. Криптографик алмаштиришларни амалга оширувчи шахсгагина тегишли ва маълум бўлган калит махфий калит деб аталади [12].

Калитлар ҳақидаги маълумот деганда, ахборот-коммуникация криптотизимида мавжуд бўлган барча калитлар тўплами ва уларнинг муҳофазаси билан боғлиқ маълумотлар тушунилади. Агарда калитлар ҳақидаги маълумотларни етарли даражадаги ишончли муҳофазали бошқаруви таъминланмаса, табиийки, рақиб томонга ахборот-коммуникация тизимидаги деярли ихтиёрий маълумотни олиш учун тўла имконият туғилади. Калитларни бошқариш криптографик калитлар ва хавфсизлик билан боғлиқ бошқа параметрлар (масалан, инициализациялаш векторлари ва пароллар)ни бошқаришни, шунингдек, уларни генерация қилиш, сақлаш, ўрнатиш, киритиш, чиқариш ва ноллашни ўз ичига оладиган калитлар ҳаётининг тўлиқ цикли давомида бажариладиган амалларни ўз ичига олади.

Криптографик калитларни бошқариш соҳасида асосий халқаро стандарт сифатида 3 қисмдан иборат ISO/IEC 11770 стандартидан фойдаланилади [39-41].

Калитларни бошқариш жараёни қуйидаги учта муҳим бўлган жараёнларга аҳамият беришни талаб этади:

- калитлар генерацияси;
- калитларнинг тўпланиши;
- калитларларнинг тақсимланиши.

Калитларни осон эслаб қолиш мақсадида тасодифий танланмаган калитлардан фойдаланиш хавфсизликни таъминлай олмайди. Ахборот-коммуникация тизимларида тасофий калитларни генерациялашнинг махсус аппарат ва дастурий усулларидан фойдаланилади.

Калитларнинг тўпланиши деганда, уларни сақлаш, ҳисобга олиш ва йўқотишни ташкиллаштириш тушунилади. Калит бузғунчи учун ўзига энг жалб этувчи объект ҳисобланиб, унга конфиденциал ахборот учун йўл очади, шунинг учун ҳам калитлар тўпламига катта аҳамият бериш талаб этилади. Махфий калитлар ҳеч қачон ошкора ҳолда ахборот ташувчиларга ёзилмаслиги, яъни уни ўқиб ва кўчириб бўлмаслик керак. Етарли даражада мураккаб ахборот-коммуникация тизимларида битта фойдаланувчи катта ҳажмдаги калит ахборотлар билан ишлаши мумкин ва баъзида эса калит ахборотлар бўйича кичик маълумотлар базаси ташкил этиш зарурияти пайдо бўлади. Бундай маълумотлар базаси фойдаланилган калитларни қабул қилишга, сақлашга, ҳисобга олишга ва йўқотишга жавобгар ҳисобланади. Шундай қилиб ишлатилган калитлар ҳақидаги барча ахборотлар шифрланган ҳолда сақланиши керак. Ахборот тизимларидаги калит ахборотларни мунтазам равишда янгилаб туриш ахборот хавфсизлигининг муҳим шарти ҳисобланади.

Симметрик криптотизимлардан муваффақиятли фойдаланиш учун махфий калит тўғрисида келишиб олиш, яъни турли фойдаланувчилар ўртасида калитлар тақсимланган бўлиши керак. Тақсимланган калитларга тақсимлашнинг тезкорлиги ва аниқлиги, тақсимланадиган калитларнинг махфийлиги каби талаблар қўйилади [3-5].

Статик (узоқ вақтли) калит. Узоқ вақт давомида ишлатиладиган калит статик калит дейилади. “узоқ” сўзининг маъноси калитнинг қаерда ва қанча вақт давомида (бир неча соатдан бир неча йилгача) ишлатилишга боғлиқ. Статик калитни очилиши одатда асосий муаммонинг ҳалокатли оқибати ҳисобланади.

Сеанс (қисқа муддатли) калитидан қисқа вақт (бир неча сониядан бир кунгача) оралиғида фойдаланилади. Одатда ундан бир мартали алоқада

махфийликни таъминлаш учун фойдаланилади. Сеанс калитининг очилиши фақат сеанснинг махфийлигини бузилишига олиб келади, лекин бу бутун криптотизимнинг криптобардошлилигига ҳеч қандай таъсир кўрсатмаслиги керак.

Калит тақсимоти - криптографиянинг асосий масалаларидан бири бўлиб, унинг бир қанча ечимлари мавжуд, улардан моси вазиятга боғлиқ ҳолда танланади [3-5].

Физик тақсимот. Ишончли курьерлар ёки қуролланган соқчилар ёрдамида калитлар анъанавий физик усул билан юборилиши мумкин. XX асрнинг етмишинчи йилларига қадар тармоқ ўрнатишда бу ҳақиқатан ҳам калит тақсимотининг ягона хавфсиз усули эди. Бунинг ўзига хос қийинчиликлари ҳам мавжуд бўлиб, улардан энг асосийси криптотизимларнинг криптобардошлилиги фақат калитга боғлиқ бўлмай, курьерга ҳам боғлиқ бўлади. Агар курьерни сотиб олиш, ўғирлаш ёки ўлдириш мумкинлиги эътиборга олинса, у ҳолда тизим обрўсизланиши мумкин.

Махфий калитли протоколлар ёрдамида тақсимлаш. Агар узоқ муддатли махфий калитлар фойдаланувчилар ва бирор ишонч маркази орасида тақсимланган бўлса, у ҳолда ундан калитларни генерация қилишда ва ихтиёрий иккита фойдаланувчи орасида алмашинув зарурати туғилганда фойдаланилади.

Носимметрик калитли протоколлар ёрдамида тақсимлаш. Носимметрик (очиқ) калитли криптотизимлардан фойдаланувчи шериклар воситачига ишонмаса ва учрашиш имконига эга бўлмасалар, калит тақсимлаш протоколига мувофиқ онлайн режимида умумий махфий калит тўғрисида келишиб олишлари мумкин. Бу очиқ калитли шифрлаш техникасининг энг кўп тарқалган иловасидир. Катта ҳажмдаги маълумотни очиқ калит ёрдамида бевосита шифрлаш ўрнига томонлар олдиндан махфий калитни келишиб олишади. Кейин аниқ маълумотларни шифрлаш учун келишилган калит билан симметрик шифр қўлланилади.

Муаммонинг кўламини тушунтириш учун ўзаро бир-бирлари билан махфий ахборот алмашинувчи n та иштирокчига хизмат кўрсатиш учун

$\frac{n(n-1)}{2}$ та турли махфий калит керак бўлади. n ошиши билан катта миқдордаги калитларни бошқариш муаммоси пайдо бўлади. Масалан, 20 000 талаба бўлган университетга 199 миллиондан кўп алоҳида махфий калитлар керак бўлади [3-4]. Катта миқдордаги махфий калитларнинг ҳосил қилиниши уларнинг бошқарувида катта муаммоларни келтириб чиқаради.

Бундай муаммонинг ечимларидан бири шундаки, ҳар бир иштирокчига фақат битта калит бириктириб қўйилади ва бу калитдан фойдаланиб у ИМ (ИМ) билан боғланади. Бу ҳолда n фойдаланувчили тизим n та калит талаб этади. Агар икки иштирокчи махфий ахборот алмашмоқчи бўлса, улар фақат шу ахборотни узатишда қўллаш учун калит генерация қилишади. Бу калитни сеанс калити деб аталади.

Махфий калит тўла маънода тасодифий бўлиши керак, чунки бузғунчи аввалдан калит ва хабарларнинг тақсимланиш эҳтимоллигини билса, калит ҳақида ҳам маълумотга эга бўлиши мумкин. Барча калитлар бир хил эҳтимолликка эга бўлиши ва тасодифий сонларнинг ҳақиқий генератори ёрдамида ҳосил қилиниши керак. Лекин бутунлай тасодифий сонлар манбаини яратиш жуда ҳам қийин. Бундан ташқари ҳақиқий тасодифий калит амалиёт учун қулай бўлгани билан уни инсон миясида сақлаб туриш мураккаб. Шунинг учун кўпгина тизимлар махфий калитни генерация қилишда парол ёки мос иборалардан фойдаланади. PIN – кодга ўхшайдиган парол, яъни 0 дан 9999 оралиғида ётувчи оддий сонни тўғридан-тўғри ҳужум билан осон топиш мумкин. 8 хонали сонлардан иборат паролдан фойдаланиш ҳам бизга етарли хавфсизликни таъминламайди.

Калитларни танлашда 20-30 символли узун иборалардан фойдаланиш мумкин, бироқ бу ҳам ечим бўлмайди, сабаби табиий тилдаги ҳарфлар кетма-кетлиги бутунлай тасодифий эмас.

Исмларга ёки ибораларга асосланган қисқа пароллар кўплаб катта корхоналарнинг умумий муаммосидир. Улардан кўпчилига паролда

- ҳеч бўлмаганда битта бош ҳарф иштирок этишини;
- ҳеч бўлмаганда битта катта ҳарф иштирок этишини;
- ҳеч бўлмаганда битта рақам иштирок этишини;

– ҳеч бўлмаганда битта рақам ва ҳарфдан бошқа белги иштирок этишини;

– паролнинг узунлиги 8 символдан кам бўлмаслигини талаб этишади.

Лекин келтирилган қоидалар луғат бўйича ҳужумдан ташқари саккизта символни ҳақиқатан тасодифий танлагандаги мумкин бўлагн максимал пароллар сонини таъминламайди.

Калитларни генерациялаганда ва сақлаганда калитларнинг яроқлилик муддатига аҳамият бериш керак. Фойдаланилаётган калит қанча кўп муомалада бўлса, бузғунчига уни очиш шунчалик осон бўлади ва у шунчалар катта қийматга эга бўлади. Бу асосий қоида бўлиб калитнинг яроқлилик муддати тугаши билан уни тўғри йўқотиш керак. Муаммони “del” ёки “rem” командаси орқали операцион тизим зиммасига юклаш бузғунчининг қаттиқ дискдаги ахборотни қайта тиклай олмаслигини кафолатламайди. Чунки файлни йўқотишда унинг ичидаги нарсалар йўқолмайди, балки тизимга фақат хотиранинг унга ажратилган ячейкалари энди бошқа янги маълумотларни ёзиш учун бўшлигини билдиради.

Асосий муаммолардан бири махфий калит тақсимотининг хавфсиз бошқарувидир. ИМ ишлатилганда ҳам унинг ҳар бир иштирокчиси учун қандайдир калит олиш усули керак бўлади.

Бу муаммони ечиш йўлларидан бири калитни парчалаш (ёки махфийликни бўлиш) бўлиб, бунда калит бир неча бўлакларга бўлинади [3-4, 6]:

$$k = k_1 \oplus k_2 \oplus \ldots \oplus k_r .$$

Унинг ҳар бир қисми ўзининг канали бўйича юборилади. Калитни аниқлаши учун бузғунчи барча каналларга бир вақтда уланиши керак бўлади. Бунда агар бузғунчи калит қисми узатиладиган каналлардан бирига киришга муваффақ бўлса, у калитнинг қонуний тикланишига тўсқинлик қилиши мумкин.

Юқорида айтиб ўтилгандек, n та иштирокчи ўзаро бир-бирлари билан махфий ахборот алмашиниши учун $\frac{n(n-1)}{2}$ та узоқ муддатли турли махфий калит керак бўлади. Таъкидлаб ўтилганидек, бу ўз навбатида катта миқдордаги калитларни бошқариш ва уларни тақсимлаш муаммосини келтириб чиқаради. Аввал айтилгандек бунда сеанс калитларидан ва бир нечта статик калитлардан фойдаланиш афзалроқ.

Бу масалани ечиш учун кўплаб протоколлар ишлаб чиқилган, уларда сеанс калитини тақсимоти учун симметрик калитли криптографиядан фойдаланилади.

1.2 Калитларни генерация қилиш муаммолари

Дастлаб криптографик методлар ҳақида гапирилганда “осон эслаб қолиш мақсадида тасодифий бўлмаган калитларни ишлатиш тавсия қилинмайди” дейилган эди. Муҳим АТларда махсус дастурий ва аппаратли тасодифий калитларни ҳосил қилиш усулларидан фойланилади. Яъни тасодифий сонлар генератори ишлатилади. Лекин уларни ҳосил қилишнинг тасодифийлик даражаси юқори бўлиши керак. Идеал генератор бу “табиий” тасодифий жараён асосидаги қурилмадир. Масалан, “оқ радиошовқин” калитларини ҳосил қилиш намуналари яратилган. Бошқа бир тасодифий математик объектлар сифатида стандарт математик усуллар орқали ҳисобланадиган π ва е сонларининг ўнлик қисмини олиб ишлатилиш мумкин.

Ўртача хавфсизлик талабларига эга бўлган АТ ларда тайёр дастурий калитларни генерация қилиш фойдалидир, қайсики тасодифий сонлар абонент киритган вақт ёки сана асосида ҳисобланади.

1.3 Калитларни очиқ каналларда хавфсиз тақсимлаш масалалари

Калитларни тақсимлаш - калитларни бошқаришда энг масъулиятли жараён саналади. Унга 2 та талаб қўйилади:

Тез ва аниқ тақсимлаш

Тақсимланаётган калитларни махфийлиги

Охирги пайтларда калитларни тақсимлаш муаммосига эга бўлмаган очиқ калитли криптотизимларни ишлатишга мойиллик бўлмоқда. Бунга қарамасдан, АТ да калитларни тақсимлашнинг янги эффектив ечимлари талаб қилинмоқда.

Абонентлар ўртасида калитларни тақсимлаш 2 та ҳар хил йўл орқали амалга оширилади:

1. Бир ёки бир нечта калитларни тақсимлаш марказларини очиш билан. Бу тизим камчилиги марказда кимга ва қандай калит тақсимланганлиги аниқ бўлади ва АТда бўлаётган барча ахборотларни ўқиш имкониятига эга бўлинади.

2. Абонентлар ва АТ ўртасида тўғридан тўғри калит алмашиш. Камчилиги, субъектлар шахсини тасдиқлаш ишончлилиги.

Иккала ҳолда ҳам алоқа сеанси ҳаққонийлиги кафолатланиши керак. Буни икки усулда таъминлаш мумкин:

1. Сўров - жавоб механизми. Агар А абонент қабул қилиб олаётган ахборотини ҳақиқатдан ҳам В абонентдан эканлигига ишонч ҳосил қилмоқчи бўлса, у В га юбораётган ахборотига тасодифий элемент қўшади. Жавоб пайтида В абонент бу элемент устида маълум ҳаракатни амалга оширади(масалан, 1 қўшади). Буни олдиндан ўзлаштириш мумкин эмас, чунки сўров жараёнида қандай тасодифий элемент келганлиги номаълум. Жавобни қабул қилиб олганидан кейин А абонент ҳаракат натижасини кўради ва сеанс ҳаққоний эканлигига ишонч ҳосил қилади. Бу усулнинг камчилиги сўров ва жавоб ўртасида маълум мураккаб қонуниятлар ўрнатишдир.

2. Вақтни белгилаб қўйиш механизми(“вақтинчалик штемпэл”). У ҳар бир ахборот учун маълум бир вақтни белгилаб қўяди. Бу ҳолда АТ нинг ҳар бир абоненти келган ахборотни қанчалик “эскилигини” билиши мумкин.

Иккала ҳолда ҳам жавоб учинчи шахсдан келмаганлигига ва вақт штемпэли ўзгартирилмаганлигига ишонч ҳосил қилиш мақсадида шифрлаш керак бўлади.

Вақтни белгилашни ишлатишда сеанс ҳаққонийлигини тасдиқловчи вақт интервали белгилаш муаммоси туради. Чунки, одатда “вақтинчалик штемпэл”ли ахборотни бир зумда юбориб бўлмайди. Бундан ташқари қабул қилувчи ва юборувчининг компьютер соатлари бир хил бўлмаслиги мумкин.

Шунинг учун реал АТларда, масалан кредит карта тўловлари тизимида ҳаққонийликни ўрнатиш ва қалбакилаштиришдан ҳимоя сифатида иккинчи механизм ишлатилади. Бунда ишлатилаётган вақт интервали бир минутдан бир неча минутгача оралиқни ташкил этади. Энг катта электрон пул ўғирланишларининг кўп қисми шу вақт оралиқларида пул ечиб олишга ёлғон сўровлар беришга асосланган.

1.4. Криптографик калитларни тақсимлаш усуллари ва схемалари

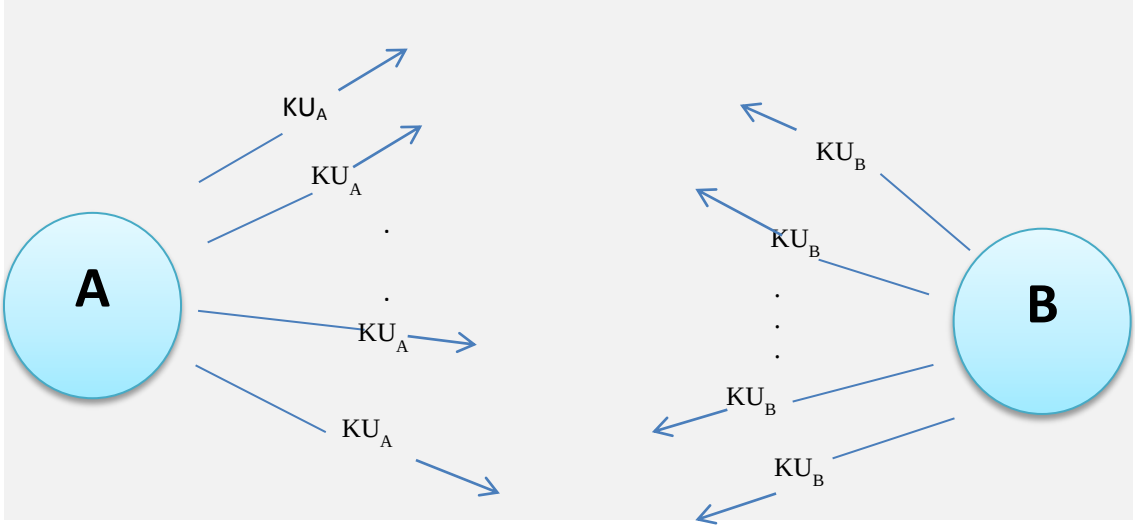
Калит тақсимлаш криптографиянинг асосий масалаларидан бири ҳисобланиб, калит тақсимлаш қандай вазиятда амалга оширилаётганига қараб уни ечишнинг бир қанча усуллари мавжуд [5-7]. Бугунги кунда калитларни тақсимлашда бир қанча усуллардан фойдаланилади, бу усулларни қуйидаги синфларга жамлаш мумкин:

1. Ошкора эълон қилиш.
2. Ошкора фойдаланиш мумкин бўлган каталог.
3. Очиқ калитларнинг ИМ.
4. Очиқ калитлар сертификатлари.

Очиқ калитларни ошкора эълон қилиш

Маълумот алмашинувида иштирок этувчи ихтиёрий томон ўзининг очиқ калитини коммуникация воситалари орқали барча иштирокчиларга тақдим этиши мумкин. Бундай ёндашувнинг қулай бўлиши билан бирга, заиф

томони ҳам мавжуд: ихтиёрий киши бундай ошкора эълонни бериши мумкин. Яъни, ихтиёрий киши (бузғунчи) ўзини **А** иштирокчи деб таништириб, очиқ калитини тармоқдаги бошқа иштирокчига юбориши мумкин ёки очиқ калитини барчанинг фойдаланиши учун тақдим этиши мумкин. Фирибгарлиги очилгунга қадар бузғунчи **А** иштирокчига келган барча шифр матнларни ўқиш ва очиқ калит ёрдамида аутентификациялаш (текшириш ва ҳақийқийлигини тасдиқлаш) имконига эга бўлади (1-расм).



1-расм. Очиқ калитларни ошкора эълон қилиш

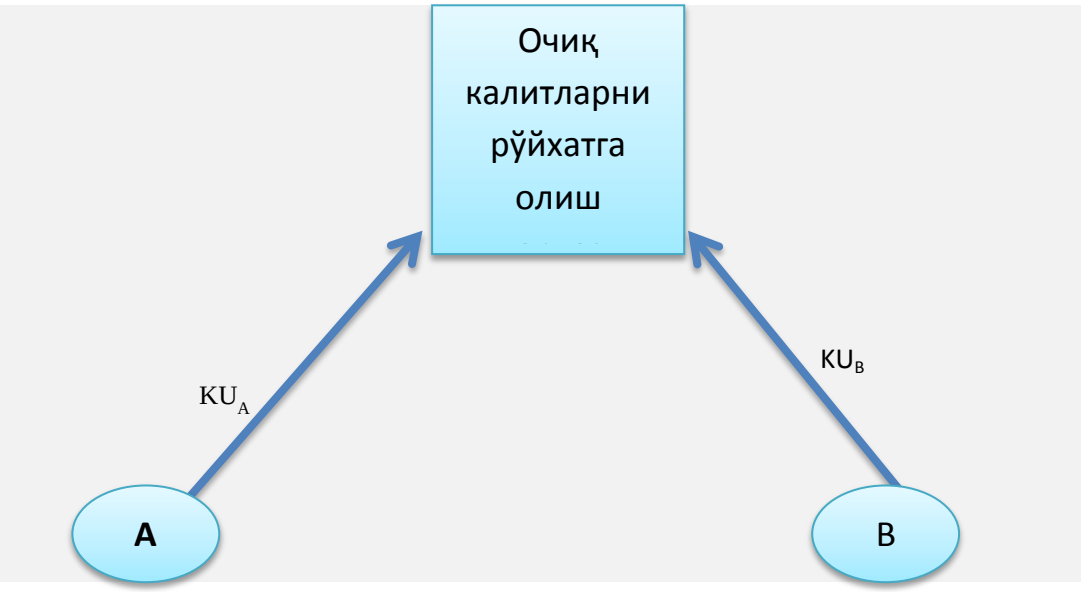
Ошкора фойдаланиш мумкин бўлган каталог

Очиқ калитларнинг ошкора фойдаланиш мумкин бўлган бирор динамик каталогини яратиш, ҳимояланиш даражасини нисбатан ошишини таъминлаши мумкин. Очиқ калитларнинг ошкора фойдаланиш мумкин бўлган динамик каталогини кузатиш ва тарқатиш жавобгарлиги бирор бир ишончли марказ ёки ташкилот зиммасида бўлиши лозим.

Бу жараён қуйидаги босқичларни ўз ичига олади [38]:

- ваколатланган ташкилот ҳар бир иштирокчининг исми ва очиқ калити қайд этилган каталогни шакллантиради;
- ҳар бир иштирокчи ўзининг очиқ калитини ваколатланган ташкилот ёрдамида рўйхатдан ўтказади. Бундай рўйхатдан ўтказиш иштирокчининг шахсан келишини ёки ҳимояланган коммуникация каналлари орқали бажарилишини талаб этади;

- ҳар бир иштирокчи очиқ калитдан катта ҳажмдаги маълумотни юбориш учун фойдалангани учун ёки калитнинг обрўси тушгани боис ихтиёрий вақтда мавжуд калитни бошқа янгиси билан алмаштириши мумкин;
- вақти-вақти билан ваколатланган ташкилот каталогни тўлалигича ёки унга қўшимчаларни эълон қилиб боради;
- иштирокчилар шунингдек каталогнинг электрон кўринишига кириш ҳуқуқига ҳам эга бўлиши мумкин. Бунинг учун маълумот алмашувчи иштирокчилар ва ваколатланган ташкилот орасида аутентификация воситалари қўлланилган алоқа канали талаб қилинади (2-расм).



2-расм. Ошкора фойдаланиш мумкин бўлган каталог

Бу схема якка тартибда ошкора эълон қилишга нисбатан анча ҳимояланган бўлсада, унинг ҳам заиф томонлари мавжуд. Агар бузғунчи ваколатланган ташкилотнинг махфий калитини олишга ёки ҳисоблаб топишга муваффақ бўлса, у қатъий ишонч билан сохталаштирилган очиқ калитни бериши, демакки, маълумот алмашинувида ихтиёрий иштирокчи номидан иштирок этиши ва ихтиёрий иштирокчига мўлжалланган маълумотни ўқиши мумкин бўлади. Каталогда сақланувчи қайдларни ўзгартириш ёрдамида ҳам бузғунчи шундай натижага эришиши мумкин.

Очиқ калитларнинг ишончли манбаи

Бу схемада маълумотлар алмашинувида қатнашувчи барча иштирокчилар очиқ калитларининг динамик каталогини таъминловчи бирор бош ваколатланган объект борлигини фараз қилади. Бундан ташқари ҳар бир иштирокчига марказнинг очиқ калити маълум, лекин фақатгина марказ унга мос махфий калитни билади. Бунда қуйидагилар бажарилади (3-расм):

1. **А** бошлаб берувчи сана/**ВБ** (вақт белгиси) қўйилган хабарни очиқ калитларнинг ИМга **В** иштирокчининг жорий очиқ калити сўровномаси билан юборади.

2. ИМ ўз махфий калити ёрдамида шифрланган хабар билан жавоб беради. Бу хабарнинг шифрини **А** бошлаб берувчи ИМнинг очиқ калитидан фойдаланиб очиши мумкин.

Бу хабар қуйидагиларни ўз ичига олиши лозим:

– **А** иштирокчи **В** иштирокчига юборадиган хабарларни шифрлаши учун В иштирокчининг очиқ калитини;

– **А** томонга жавобни аввалги юборилган сўровнома билан таққослаши ва ИМга юборилганда йўлда ўзгартириб қўйилмаганига ишонч ҳосил қилиши учун ўзига хос сўровномани;

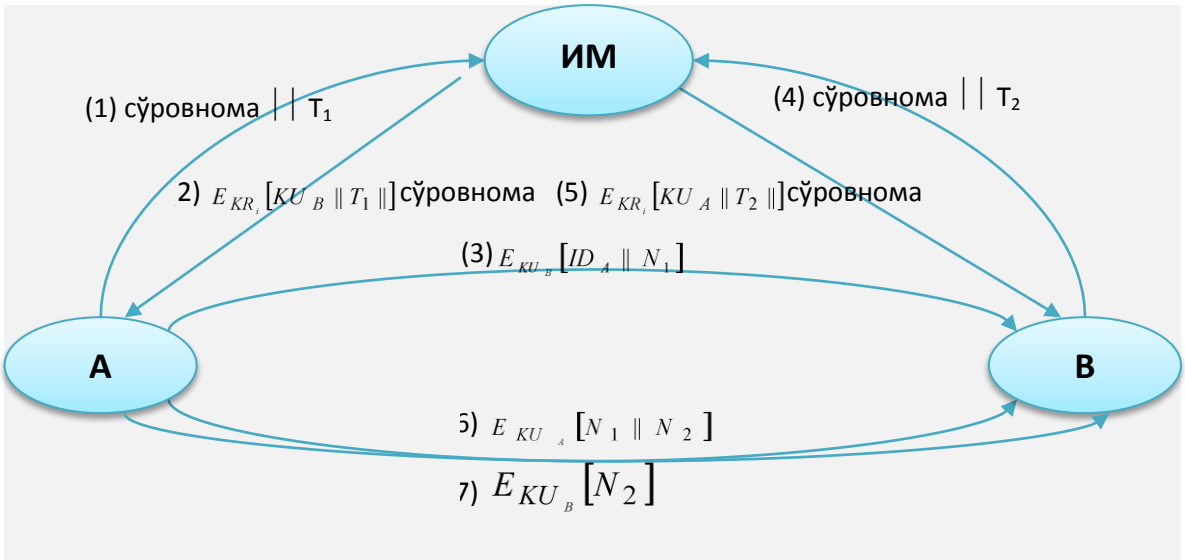
– махсус сана/ВБни, **А** иштирокчи хабар ИМнинг **В** иштирокчини жорий калитидан фарқ қилувчи калитли эски хабарлардан бири эмаслигига инонмоғи учун;

3. **А** бошлаб берувчи **В** иштирокчининг очиқ калитини сақлаб қўяди ва ундан В иштирокчига юбориладиган хабарларни шифрлашда фойдаланади, бу хабарда **А** иштирокчининг идентификатори ва ушбу хабарнинг махсус белгиси бўлган сана ҳам қайд этилади;

4. **В** жавоб йўлловчи **А** иштирокчининг очиқ калитини ИМдан А юборувчи В қабул қилувчининг очиқ калитини олган усул билан олади;

5. **В** жавоб йўлловчи **А** бошлаб берувчига **В** нинг калити билан шифрланган хабарни ва **А** юборувчининг қўйган санасини, шунингдек қабул қилинган маълумотнинг юборувчиси **В** эканлигига ишонтириш учун, В иштирокчи томонидан генерацияланган янги санани ҳам қўшиб юборади;

6. **А** бошлаб берувчи, **В** иштирокчини жавоб юборувчи **А** иштирокчи эканлигига ишониши учун, унинг очиқ калити билан шифрланган санани қайтариб юборади.



3-расм. Очиқ калитларнинг ИМ

Шундай қилиб, олтита хабар юбориш талаб қилинар экан, лекин бошидаги тўрттасини юбориш кўпинча талаб қилинмайди, чунки иккала томон ҳам бир-бирининг очиқ калитини кейинчалик фойдаланиш учун сақлаб қўйиши мумкин, буни кешлаш дейилади. Вақти-вақти билан иштирокчи кафолатланган хавфсиз маълумот алмашиниш имкониятига эга бўлиши учун ўз адресатларининг янги очиқ калит нусхаларини сўраши лозим. Очиқ калитнинг ИМ тармоқнинг чекланган қисми бўлиб, иштирокчи унга ёзишма олиб бормоқчи бўлган ҳар бир янги адресатнинг очиқ калитини олиш учун мурожаат қилиши лозим. ИМ томонидан юритилувчи исмлар ва очиқ калитлар каталоги рухсатсиз киришга нисбатан заиф бўлиб қолади.

Очиқ калитлар сертификатлари

Сертификатлар иштирокчилар томонидан очиқ калитларнинг ИМ билан алоқасиз калит алмашинуви учун ишлатилиши мумкин бўлиб, алмашинув усули худди очиқ калитларнинг ИМнинг ўзидан олиш усулидек ишончли усулни таъминлаши зарур. Ҳар бир сертификат очиқ калит ва бошқа маълумотни ўз ичига олган бўлиб, сертификатларнинг ИМ томонидан ишлаб чиқилади ва иштирокчига мос махфий калити билан бирга берилади.

Бир иштирокчи ўзининг калити тўғрисидаги маълумотни бошқа иштирокчига ўзининг сертификатини бериш орқали етказади. Бошқа иштирокчилар эса сертификат ИМ томонидан берилганлигини текширишлари мумкин. Келтирилган схемага қуйидаги талаблар қўйилади [38-39]:

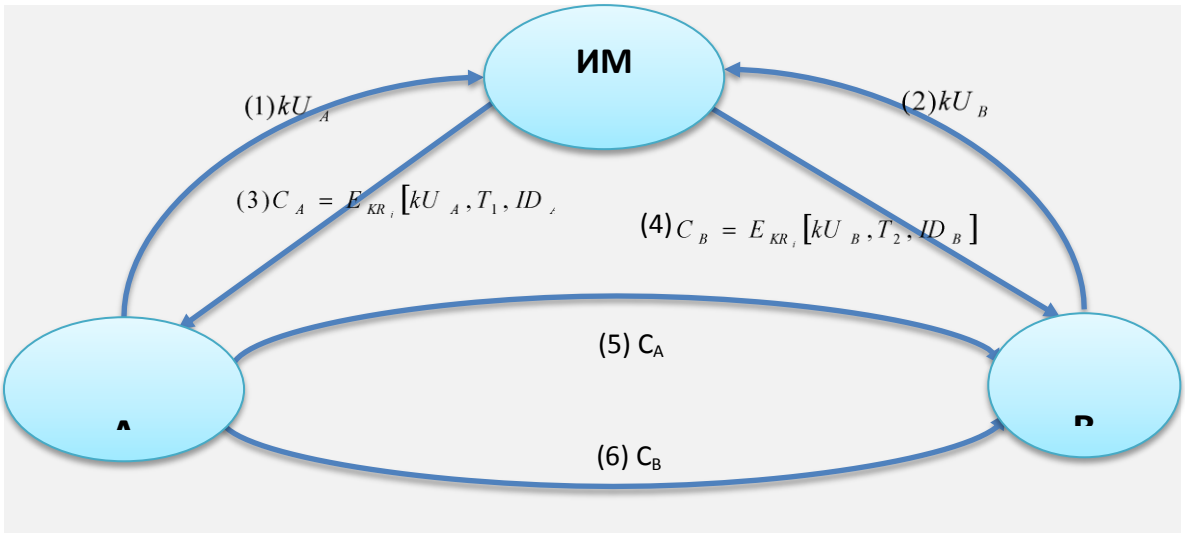
- ҳар бир иштирокчи сертификат эгасининг исми ва очиқ калитини аниқлаши учун сертификатни ўқиш имкониятига эга бўлиши керак;
- ҳар бир иштирокчи сертификат сертификатларнинг ИМ томонидан берилганлигига ва у сохта эмаслигини текшириш имкониятига эга бўлиши керак;
- фақатгина сертификатларнинг ИМгина сертификатларни яратиш ва ўзгартириш имкониятига эга бўлиши керак.

Сертификатни ишлатилиш схемаси қуйидагича (4-расм). Ҳар бир иштирокчи сертификатларнинг ИМга очиқ калитни тақдим этган ҳолда ўзига сертификат сўраб мурожаат қилади. Сўровнома шахсан ёки бирор ҳимояланган алоқа воситаси орқали мурожаат қилишни талаб этади. **А** иштирокчи учун ишонч манбаи $C_A = E_{KR_{им}}[T, ID_A, KU_B]$ сертификат беради,

бунда $kR_{им}$ – ИМнинг махфий калити; kU_B – **В** иштирокчининг очиқ калити; ID_A – **А** иштирокчининг идентификатори; T – юборилган сана/вақт. **А** иштирокчи бу сертификатни ихтиёрий бошқа иштирокчига ўқиши ва қабул қилиши учун юбориши мумкин:

$$D_{kU_{ei}}[C_A] = D_{kU_{ei}}[E_{kR_{ei}}[T, ID_A, kU_A]] = (T, ID_A, kU_A),$$

бунда, $kU_{им}$ – ИМнинг очиқ калити; kU_A – **А** иштирокчининг очиқ калити.



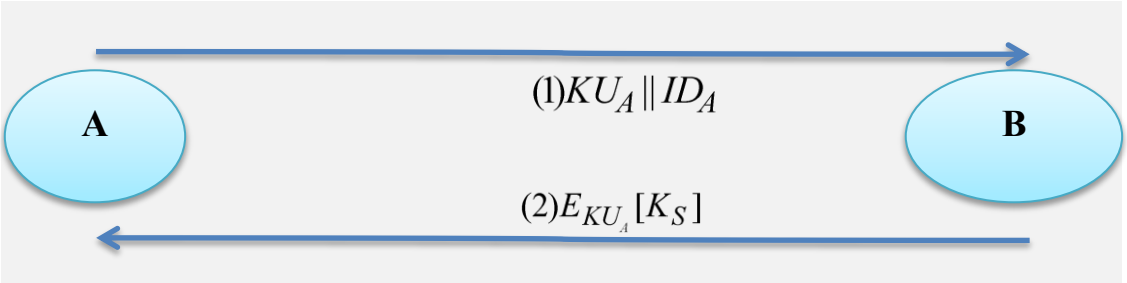
4-расм. Очиқ калитлар сертификатлари

Сертификатни сертификатлар ИМнинг очиқ калити билан ўқиш мумкинлиги, сертификат айнан сертификатлар ИМдан келганлигини кафолатлайди. ID_A, kU_A элементлар олувчига сертификат эгасининг исми ва очиқ калитини билдиради. Сана/ВБ T сертификатнинг қўлланилиш муддатини аниқлайди. Сана/ВБ қуйидаги таъсирлар кетма-кетлигидан муҳофазаланган бўлиши керак. Бузғунчи **А** иштирокчининг махфий калитини билиб олган бўлсин. У ҳолда **А** иштирокчи янги (махфий ва очиқ) калитлар жуфтини генерациялайди ва сертификатларнинг ИМга янги сертификат олиш учун мурожаат қилади. Бу вақтда бузғунчи эски сертификат асосида хабар ишлаб, уни **В** иштирокчига юборади. Агар **В** иштирокчи хабарни эски очилган калит билан шифрласа, бузғунчи бу хабарни ўқий олади. Бунда вазият мумкин бўлган тизимларни эски тизим бекор қилингани тўғрисида хабардор қилинмагунча қалтислигича қолади.

Очиқ калитлар тақсимлангандан кейин хабарларни қўлга киритиш ва бузишдан ҳимояланган алоқани ташкил этиш мумкин бўлади. Лекин очиқ калитли шифрлашни қўлланилганда маълумотларни узатиш тезлиги нисбатан секинлашади, бу кўпинча иштирокчилар учун тўғри келмайди. Шунинг учун асосан Меркель томонидан таклиф этилган махфий калитларнинг тақсимлаш схемасидан фойдаланилади [38-39].

Таклиф этилган схема қуйидагидан иборат (5-расм). Агар **A** бошлаб берувчи **B** иштирокчи билан маълумот алмашмоқчи бўлса, қуйидаги жараён таклиф этилади:

1. **A** иштирокчи (очиқ/махфий) калитлар жуфтини генерациялайди ва **B** иштирокчига kU_A ва **A** иштирокчининг идентификатори бўлган ID_A ни ўз ичига олган хабарни юборади.
2. Қабул қилувчи **B** махфий калит k ни генерациялайди ва бу калитни **A** иштирокчининг очиқ калити билан шифрлаб, **A** иштирокчига юборади.
3. **A** иштирокчи $D_{kU_A}[E_{kU_A}[k_S]]$ ни махфий калитни тиклаш учун ҳисоблайди. Фақатгина **A** иштирокчи бу хабарнинг шифрини очиши мумкин бўлгани сабабли фақат шу икки иштирокчи **A** ва **B** k_A нинг қийматни билади.
4. **A** иштирокчи kR_A калитни, **B** иштирокчи эса kU_A ни йўқ қилади.



5-расм. Махфий калитлар тақсимлашнинг Меркель схемаси

Иккала **A** ва **B** иштирокчи k_A сеанс калитини қўллаб анъанавий шифрлаш ёрдамида ҳимояланган алоқадан фойдаланиши мумкин. Маълумот алмашинуви сўнгида **A** иштирокчи ҳам, **B** иштирокчи ҳам k_A ни йўқ қилади. Содда тузилишига қарамай, бу протокол эътиборга лойиқ. Алоқа бошлангунга қадар ҳам, алоқа тугагандан сўнг ҳам, ҳеч қандай калит мавжуд бўлмайди. Шунинг учун калитнинг компроментацияланиш (обрўсизланиш) хавфи жуда кичик ва бу вақтда алоқа ҳимояланган бўлади. Лекин бу протокол фаол ҳужумга нисбатан заиф. Агар **E** бузғунчининг алоқа каналига суқилиб кириш имконияти мавжуд бўлса, у аниқлангунга қадар алоқага қуйидагича путур етказиши мумкин:

1. **A** иштирокчи бир жуфт очиқ/махфий (kU_A, kR_A) калитларни генерациялайди, сўнгра kU_A ни ва **A** иштирокчининг идентификатори ID_A мавжуд бўлган хабарни **B** иштирокчига юборади.

2. **E** бузғунчи хабарни тутиб қолади, ўзининг хусусий бир жуфт очиқ/махфий (kU_E, kR_E) калитларини ҳосил қилади ва kU_E, ID_A мавжуд бўлган хабарни **B** иштирокчига юборади.

3. **B** иштирокчи k_S махфий калитни генерация қилади ва $E_{kU_A}[k_S]$ ни юборади.

4. **E** бузғунчи хабарни тутиб қолади ва $D_{kU_E}[E_{kU_E}[k_S]]$ ҳисоблаш ёрдамида k_S нинг қийматини топади.

5. Бузғунчи **A** иштирокчига $E_{kU_A}[k_S]$ ни юборади.

A иштирокчи ҳам **B** иштирокчига ҳам k_S маълум бўлади, лекин улар **E** бузғунчига ҳам k_S маълумлигини билишмайди. Шунинг учун **A** ва **B** иштирокчилар k_S дан фойдаланиб хабар алмашинишлари мумкин. **E** бузғунчи алоқа каналида бошқа фаол суқилиб кирмайди, фақатгина хабарларни тутиб қолади. k_S ни билган ҳолда бузғунчи ихтиёрий хабарни шифрини очиши мумкин, аммо **A** ва **B** иштирокчилар бу муаммодан бехабар бўлишади. Демак, бу протокол фақатгина хабарларни пассив тутиб қолиш мумкин бўлганида фойда беради.

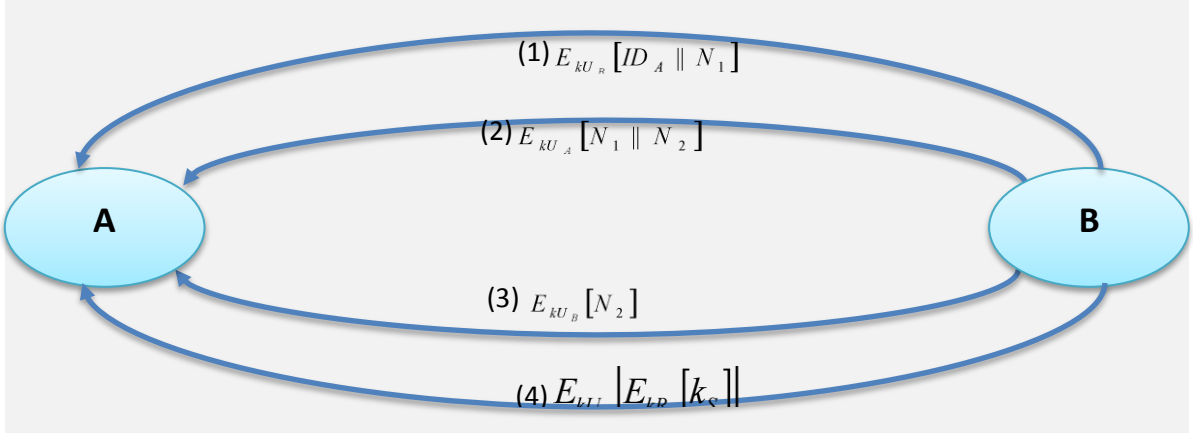
Ҳозирги кунда криптографик калитларни тақсимлашнинг бир нечта схемалари мавжуд. Қуйида уларнинг баъзиларини кўриб чиқилади.

Дастлабки калит тарқатиш схемалари иккита алгоритмдан ташкил топган: бошланғич калитга оид ахборотни тақсимлаш ва калитни шакллантириш. Биринчи алгоритм ёрдамида калитга оид ахборотнинг очиқ қисми ва махфий қисми (ҳар бир томон учун) генерация қилинади, очиқ калит ҳамма кириши мумкин бўлган очиқ серверга жойлаштирилади. Иккинчи алгоритм абонентларда мавжуд бўлган махфий ва бошланғич калит маълумотининг умумий очиқ қисми ёрдамида, улар орасидаги ўзаро боғланишни амалдаги калитини ҳисоблаш учун мўлжалланган. Сақланадиган ва тақсимланадиган махфий калитли ахборотнинг ҳажмини камайтириш учун қўлланилади. Дастлабки калит тақсимлаш схемаси турғун бўлиши, яъни компроментацияда, фирибгарликда ёки баъзи абонентларнинг махфий келишувида калитнинг бир қисмини очилишини эътиборга олиниши ва тез

мослашувчан – яъни обрўсизлантирилган калитларни чиқариб ташлаш орқали тезликда тиклаш ва янги абонентларни улаши имкониятини бериши керак.

Махфий калитларни конфиденциаллигини ва аутентификациясини таъминлаб тақсимлаш схемаси

Қуйидаги 6-расмда келтирилган схема фаол ва пассив ҳужумлардан ҳимояни таъминлайди.



6-расм. Фаол ва пассив ҳужумлардан ҳимояни таъминлаш схемаси

A ва **B** юқорида келтирилган схемалардан бири ёрдамида очиқ калитларини алмашинишган бўлсин. Бунда қуйидаги амаллар бажарилади:

1. **A** иштирокчи **B** иштирокчига шифрланган ахборот жўнатиш учун **A** иштирокчининг ID_A идентификаторини ва N_1 псевдотасодифий сонни ўз ичига олган хабарни **B** нинг очиқ калити kU_B ёрдамида шифрланб **B** иштирокчига юборади.
2. **B** иштирокчи **A** иштирокчига ундан олинган N_1 псевдотасодифий сонни ва янги **B** иштирокчи томонидан генерацияланган N_2 псевдотасодифий сонни ўз ичига олган, ҳамда kU_A ёрдамида шифрланган хабарни жўнатади. N_1 нинг хабарда мавжудлиги **A** иштирокчини хабар юборувчи **B** иштирокчи эканлигига ишонтиради.
3. **A** иштирокчи хабарни **B** иштирокчининг очиқ калити билан шифрлаб N_2 ни қайтариши хабар юборувчи **A** эканлигига **B** ни ишонтиради.

4. **A** иштирокчи k_S махфий калитни танлаб **B** иштирокчига $M = E_{kU_B}\left[E_{kR_A}[k_S]\right]$ хабарни юборади. **B** иштирокчининг очиқ калити билан шифрланган матнни фақатгина **B** иштирокчигина ўқий олишини, **A** иштирокчи хабарини махфий калити билан шифрлаши эса хабарни фақатгина **A** иштирокчи юборганини кафолатлайди.

5. **B** иштирокчи эса $D_{kU_A}[E_{kU_B}[M]]$ ни ҳисоблаб махфий калитни тиклайди.

Бу схеманинг бошидаги учта амал ИМдаги очиқ калит тарқатишининг учта сўнгги амалига мос келади. Натижада, махфий калитлар алмашинишда бу схема конфиденциаллик ва аутентификацияни кафолатлайди.

Гибрид схема

Махфий калит тарқатишидаги очиқ калит билан шифрлашнинг яна бир схемаси гибрид ёндашуви бўлиб, у IBM фирмасининг супер компьютерларида қўлланилади [39-40]. Бу схема калит тарқатиш маркази иштирокини кўзда тутади. Бундай уч босқичли ёндашувнинг асосида қуйидаги мантиқ ётади:

– *процедураларнинг бажарилиш тезлиги*. Бу мантиққа транзакцияларни узатишга ихтисослашган иловалар (приложение) мосланган бўлиб, бунда сеанс калитлари тез-тез алмаштириб турилиши лозим. Сеанс калитларини ошкора калитли схема ёрдамида тарқатилиши, бу схемада шифрлаш ва шифрни очиш жараёнида ишлатиладиган ҳисоблаш ресурсларига қўйиладиган катта талаблар ҳисобига тизимнинг унумдорлигини жуда ҳам пасайтириб юбориши мумкин эди. Уч босқичли иерархияда очиқ калит билан шифрлаш иштирокчилар билан калит тарқатувчи марказ орасида тақсимланувчи асосий калитни ўзгартириш каби баъзи ҳоллардагина ишлатилади;

– *қайтарилувчи мослик (обратная совместимость)*. Гибрид схемани мавжуд схеманинг калит тарқатиш маркази процедура ва дастур таъминотида минимал ўзгартиришлар кўзда тутган кенгайтмаси кўринишида осонгина тадбиқ этиш мумкин.

Ошкора калит билан шифрлаш босқичини қўшиш асосий калит тақсимоти воситасини муҳофазасини ва самарадорлигини таъминлайди. Бу эса битта калит тақсимоти марказининг кўплаб бир-биридан етарлича узоқ масофада жойлашган иштирокчиларга хизмат кўрсатгандаги афзаллигидир.

2-БОБ. ХАЛҚАРО КРИПТОГРАФИК КАЛИТЛАРНИ ТАҚСИМЛАШ АЛГОРИТМЛАРИ ВА ПРОТОКОЛЛАРИНИНГ ТУРЛАРИ ВА МУАММОЛАРИ

2.1 Ассимметрик алгоритмларга асосланган калитларни тақсимлаш алгоритмлари ва протоколлари

Калитларни тақсимлаш масаласи қуйидагиларни таъминловчи калитларни тақсимлаш протоколини қуришга келтирилади:

- сеанс қатнашчиларининг ҳақиқийлигига иккала томоннинг тасдиғи;
- сеанс ҳақиқийлигининг тасдиғи;
- калитлар алмашинувида хабарларнинг минимал сонидан фойдаланиш.

Биринчи усулга мисол тариқасида Kerberos деб аталувчи калитларни аутентификациялаш ва тақсимлаш тизимини кўрсатиш мумкин.

Иккинчи усулга-тармоқ фойдаланувчилари ўртасида калитларни тўғридан-тўғри алмашишга батафсил тўхталамиз.

Симметрик калитли криптотизимдан фойдаланилганда криптографик ҳимояланган ахборот алмашинувини истаган иккала фойдаланувчи умумий махфий калитга эга бўлишлари лозим. Бу фойдаланувчилар умумий калитни алоқа канали бўйича хавфсиз алмашишлари лозим. Агар фойдаланувчилар калитни тез-тез ўзгартириб турсалар калитни етказиш жиддий муаммога айланади.

Бу муаммони ечиш учун қуйидаги иккита асосий усул қўлланилади:

1. Симметрик криптотизимнинг махфий калитини ҳимоялаш учун очиқ калитли асимметрик криптотизимдан фойдаланиш
2. Диффи-Хеллманнинг калитларни очиқ тақсимлаш тизимидан фойдаланиш.

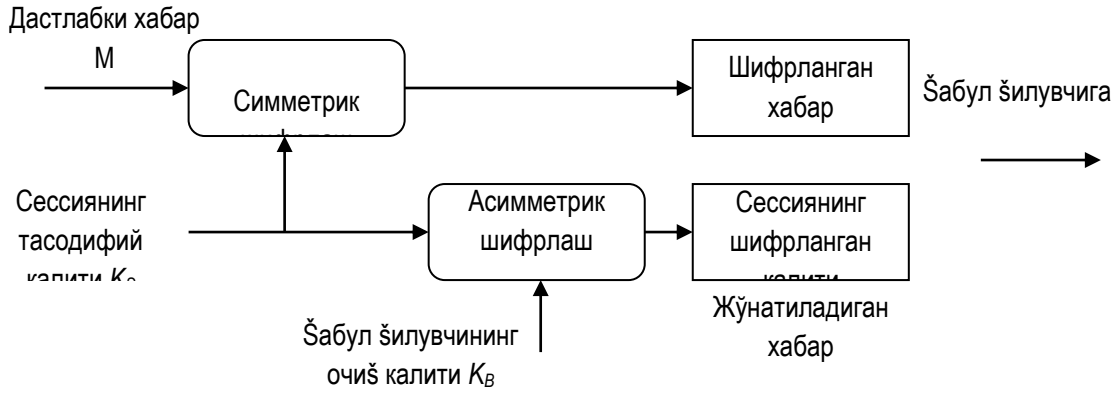
Биринчи усул симметрик ва асимметрик калитли комбинацияланган криптотизим доирасида амалга оширилади. Бундай ёндашишда симметрик криптотизим дастлабки очиқ матнни шифрлаш ва узатишда ишлатилса, очиқ калитли асимметрик криптотизим фақат симметрик криптотизимнинг махфий калитини шифрлаш, узатиш ва кейинги расшифровка қилишда ишлатилади. Шифрлашнинг бундай комбинацияланган (гибрид) усули очиқ калитли асимметрик криптотизимнинг юқори махфийлиги билан махфий калитли симметрик криптотизимнинг юқори тезкорлигининг уйғунлашишга олиб келади. Бундай ёндашиш баъзида электрон рақамли конверт схемаси деб юритилади.

Фараз қилайлик, фойдаланувчи А хабар М ни фойдаланувчи В га ҳимояланган узатиш учун шифрлашнинг комбинацияланган усулидан фойдаланмоқчи. Унда фойдаланувчиларнинг ҳаракатлари қуйидагича бўлади.

Фойдаланувчи А нинг ҳаракатлари:

1. Симметрик сеанс махфий калит $К_S$ ни яратади (масалан, тасодифий тарзда генерациялайди).
2. Хабар М ни симметрик сеанс махфий калит $К_S$ да шифрлайди.
3. Махфий сеанс калит $К_S$ ни фойдаланувчи (хабар қабул қилувчи) Внинг очиқ калити $К_B$ да шифрлайди.
4. Фойдаланувчи В адресига алоқанинг очиқ канали бўйича шифрланган хабар М ни шифрланган сеанс калити $К_S$ билан биргаликда узатади.

Фойдаланувчи А нинг харакаталарини 5.17-расмда келтирилган хабарларни комбинацияланган усул бўйича шифрлаш схемаси орқали тушуниш мумкин.



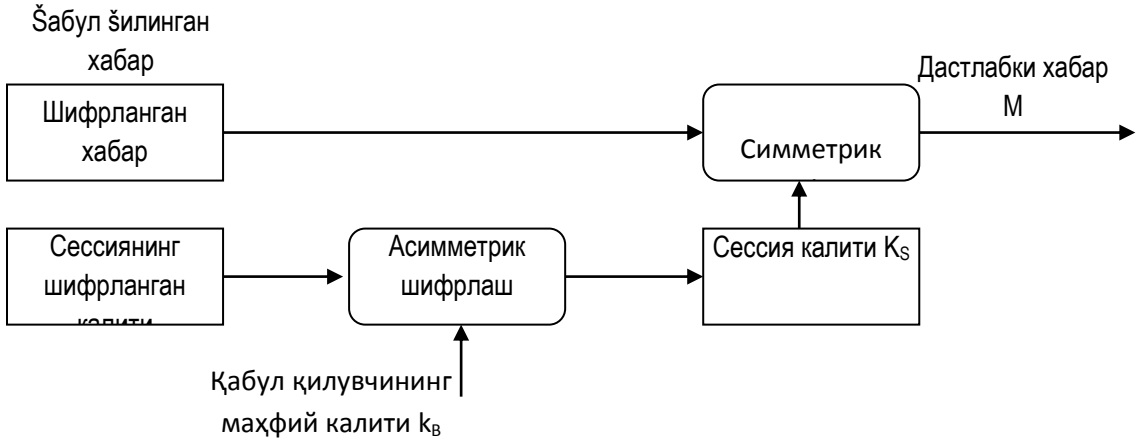
5.17–расм. Комбинацияланган усул бўйича хабарни шифрлаш схемаси.

Фойдаланувчи В нинг ҳаракатлари (электрон рақамли конвертни-шифрланган хабар М ни ва шифрланган сеанс калити $К_S$ ни олганидан сўнгги) қуйидагича:

1. Ўзининг махфий калити k_B бўйича сеанс калити $К_S$ ни расшифровка қилади.
2. Олинган сеанс калити $К_S$ бўйича олинган хабар М ни расшифровка қилади.

Фойдланувчи В нинг харакатларини 5.18-расмда келтирилган хабарларни комбинацияланган усул бўйича расшифровка қилиш схемаси орқали тушуниш мумкин.

Олинган электрон рақамли конвертни фақат қонуний қабул қилувчи-фойдаланувчи В очиши мумкин. Фақат шахсий махфий калит k_B эгаси бўлган фойдаланувчи В махфий сеанс калити $К_S$ ни тўғри расшифровка қилиш ва сўнгра бу калит ёрдамида олинган хабар М ни расшифровка қилиши ва ўқиши мумкин.



5.18–расм. Комбинацияланган усул бўйича хабарни расшифровка қилиш.

Рақамли конверт усулида симметрик ва асимметрик криптоалгоритмларнинг камчиликлари қуйидагича компенсацияланади:

- симметрик криптоалгоритм калитларини тарқатиш муаммоси бартараф қилинади, чунки хабарни шифрловчи сеанс калити K_S очиқ канал бўйича шифрланган кўринишда узатилади, калит K_Sни расшифровка қилиш учун асимметрик криптоалгоритмдан фойдаланилади;
- бу ҳолда асимметрик шифрлаш тезкорлигининг секинлиги муаммоси пайдо бўлмайди, чунки асимметрик алгоритм бўйича фақат қисқа калит K_S шифрланади, барча маълумотлар эса тезкор симметрик криптоалгоритм бўйича шифрланади.

Натижада тезкор шифрлаш билан биргаликда калитларнинг қулай тақсимланиши амалга оширилади.

Шифрлашнинг комбинацияланган усулида симметрик ҳам асимметрик криптотизимларнинг криптографик калитларидан фойдаланилади. Равшанки, криптотизимнинг ҳар бир тури учун калитлар узунлигини шундай танлаш лозимки, нияти бузуқ одамга комбинацияланган криптотизим ҳимоясининг ҳар қандай механизмига хужум қилиш бир хил қийинчилик туғдирсин.

5.1-жадвалда кўп учрайдиган симметрик ва асимметрик криптотизимлар калитларининг узунлиги келтирилган.

5.1-жадвал

Симметрик криптотизим калитлари узунлиги, битлар	Асимметрик криптотизим калитлари узунлиги, битлар
56	384
64	512
80	768
112	1792
128	2304

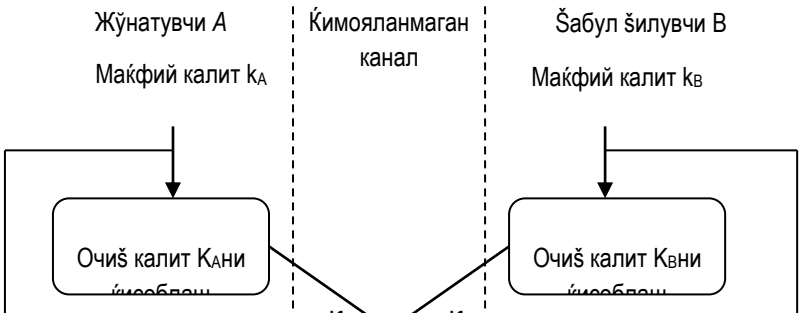
У. Диффи ва М.Хеллман томонидан кашф этилган калитларни очиқ тақсимлаш усули фойдаланувчиларга калитларни ҳимояланмаган алоқа каналлари орқали алмашишга имкон беради. Унинг хавфсизлиги чегараланган соҳада дискрет логарифмларни ҳисоблашнинг мушкуллигига асосланади.

Диффи-Хеллман усулининг моҳияти қуйидагича (5.19-расм).

Ахборот алмашинувида иштирок этувчи фойдаланувчилар А ва В мустақил равишда ўзларининг махфий калитларини k_A ва k_B ни генерациялайдилар (k_A ва k_B калитлар фойдаланувчилар А ва В лар сир сақловчи тасодифий катта бутун сонлар).

Сўнгра фойдаланувчи А ўзининг махфий калити k_A асосида очиқ калитни ҳисоблайди:

$$K_A = g^{K_A} (\mathrm{mod}\quad N).$$



Бир вақтнинг ўзида фойдаланувчи В ўзининг махфий калити k_B асосида очиқ калитни ҳисоблайди:

$$K_B = g^{K_B} (\mathrm{mod}\quad N).$$

Бу ерда N ва g – катта бутун оддий сонлар. Арифметик амаллар Nнинг модулига келтириш орқали бажарилади. N ва g сонларни сир сақлаш шарт эмас, чунки одатда, бу қийматлар тармоқ ва тизимдан фойдаланувчиларнинг барчаси учун умумий ҳисобланади.

Сўнгра фойдаланувчилар А ва В ўзларининг очиқ калитларини ҳимояланмаган канал орқали алмаштирадилар ва умумий сессия махфий калити Кни (бўлинувчи сирни) ҳисоблашда ишлатадилар:

фойдаланувчи А: $K = (K_B)^{k_A} (\mathrm{mod}\quad N) = (g^{k_B})^{k_A} (\mathrm{mod}\quad N),$

фойдаланувчи В: $K' = (K_A)^{k_B} (\mathrm{mod}\quad N) = (g^{k_A})^{k_B} (\mathrm{mod}\quad N),$

бунда $K = K'$, чунки $(g^{k_B})^{k_A} = (g^{k_A})^{k_B} (\mathrm{mod}\quad N).$

Шундай қилиб, ушбу амаллар натижасида иккала махфий калит k_A ва k_Bларнинг функцияси бўлган умумий сессия махфий калити ҳосил қилинади.

Очиқ калитлар $К_А$ ва $К_В$ қийматларини ушлаб қолган нияти бузуқ одам сессия махфий калити К ни ҳисоблай олмайди, чунки у махфий калитлар k_A ва k_B қийматларини билмайди. Бир томонлама функциянинг ишлатилиши

сабабли очиқ калитни ҳисоблаш амали қайтарилмайдиган амал, яъни абонентнинг очиқ калити қиймати бўйича унинг махфий калитини ҳисоблаш мумкин эмас.

Диффи-Хеллман усулининг ноёблиги шундан иборатки, абонентлар жуфти тармоқ орқали очиқ калитларни узатганларида фақат ўзларига маълум махфий сонни олиш имкониятига эга. Сўнгра абонентлар узатилаётган ахборотни маълум текширилган усулни – олинган умумий сессия махфий калитидан фойдаланган ҳолда симметрик шифрлашни ишлатиб ҳимоялашга киришишлари мумкин.

Диффи-Хеллман схемаси маълумотларни ҳар бир сеансда янги калитларда шифрлаш имконини беради. Бу сирларни дискетларда ёки бошқа элтувчиларда сақламасликка имкон беради, чунки бундай сақлаш уларни рақиблар ёки нияти бузуқ одамлар қулига тушиб қолиш эҳтимоллигини оширади.

Диффи-Хеллман схемаси узатилаётган маълумотларнинг конфиденциаллигини ва аутентлигини (аслига тўғрилигини) комплекс ҳимоялаш усулини ҳам амалга ошириш имконини беради. Алгоритм фойдаланувчига рақамли имзони ва симметрик шифрлашни бажаришда бир хил калитларни шакллантириш ва ишлатиш имконини беради.

Маълумотлар яхлитлигини ва конфиденциаллигини бир вақтда ҳимоялаш учун шифрлаш ва электрон рақамли имзодан комплекс фойдаланиш мақсадга мувофиқ ҳисобланади. Диффи-Хеллман схемаси ишлашининг оралиқ натижаларидан узатилаётган маълумотларнинг яхлитлигини ва конфиденциаллагини комплекс ҳимоялаш усулини амалга оширишда фойдаланиш мумкин. Ҳақиқатан, ушбу алгоритмга биноан фойдаланувчилар А ва В аввал ўзларининг махфий калитлари k_A ва k_B ни генерациялайдилар ва очиқ калитлари $К_A$ ва $К_B$ ни ҳисоблайдилар. Сўнгра абонентлар А ва В бу оралиқ натижалардан маълумотларни симметрик

шифрлашда фойдаланилиши мумкин бўлган умумий бўлинувчи махфий калити К ни бир вақтда ҳисоблаш учун ишлатади.

Узатилаётган маълумотларнинг конфиденциаллигини ва аутентилигини комплекс ҳимоялаш усули қуйидаги схема бўйича ишлайди:

- абонент А рақамли имзонинг стандарт алгоритмидан фойдаланиб, ўзининг махфий калити k_A ёрдамида хабар М га имзо чекади;

- абонент А ўзининг махфий калити k_A ва абонент В нинг очиқ калити $К_B$ дан Диффи-Хеллман алгоритми бўйича умумий бўлинувчи махфий калити К ни ҳисоблайди.

- абонент А олинган ўзаро бўлинувчи махфий калитда алмашинув бўйича шериги билан келишилган симметрик шифрлаш алгоритмидан фойдаланган ҳолда хабар М ни шифрлайди;

- абонент В шифрланган хабар М ни олиши билан ўзининг махфий калити k_B ва абонент А нинг очиқ калити $К_A$ дан Диффи-Хеллман алгоритми бўйича ўзаро бўлинувчи махфий калит К ни ҳисоблайди;

- абонент В олинган хабар М ни калити К да расшифровка қилади;

- абонент В абонент А нинг очиқ калит $К_A$ ёрдамида расшифровка қилинган хабар М имзосини текширади.

Диффи-Хеллман схемаси асосида тармоқ сатҳида ҳимояланган виртуал тармоқлар VPN қурилишида қўлланилувчи криптокалитларни бошқариш протоколлари SKIP (Simple Key Management for Internet Protocols) ва IKE (Internet Key Exchange) ишлайди.

2.2 Симметрик криптотизимларга асосланган калитларни тақсимлаш алгоритмлари ва протоколлари

2.2.1. Шамир протоколи

Симметрик криптотизимлардан муваффақиятли фойдаланиш учун махфий калит тўғрисида келишиб олиш, яъни турли иштирокчилар ўртасида калитлар тақсимланган бўлиши керак.

Қуйида **Шамир протоколи** деб аталувчи (калитсиз) умумий махфий маълумотдан фойдаланмаган ҳолда калитни узатиш протоколини кўриб чиқилади. Бу протокол қадамларига мувофиқ калитнинг махфийлик масаласи таъминланади.

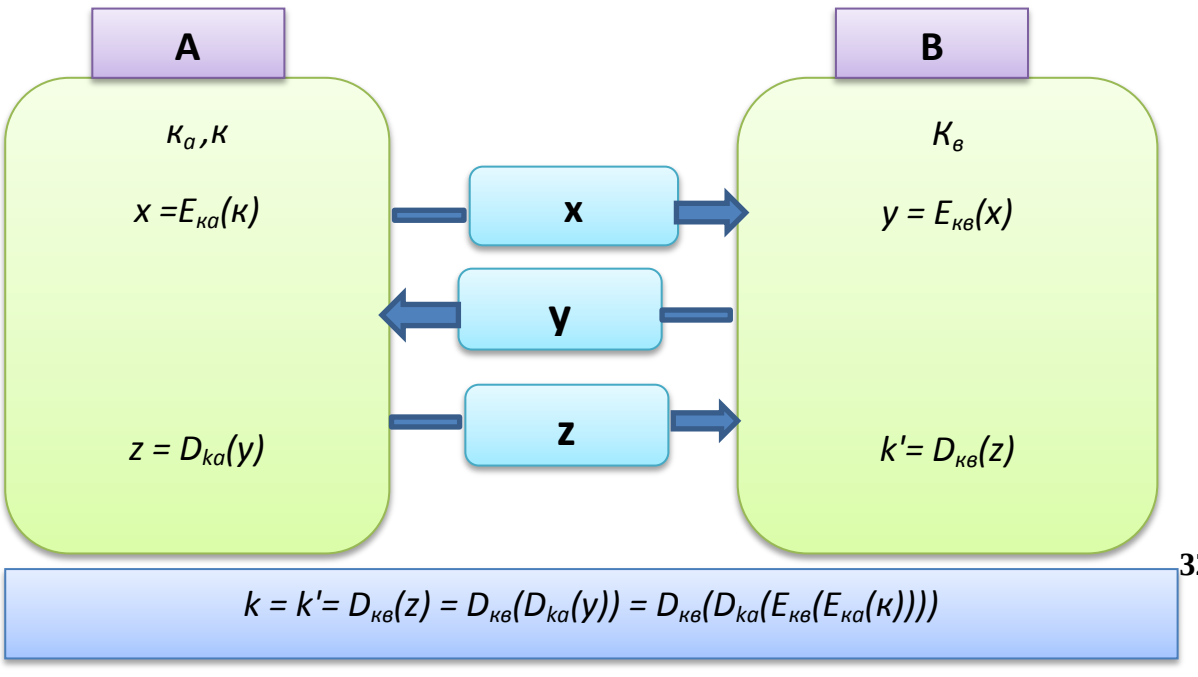
Шундай шифрлаш ва дешифрлаш ўзгартиришлари мавжудки [2,14] барча x маълумотлар, k_1 ва k_2 калитлар учун қуйидаги шарт бажарилади:

$$E_{k_1}(E_{k_2}(x)) = E_{k_2}(E_{k_1}(x)) .$$

У ҳолда **A** ва **B** иштирокчилар k сеанс калитини узатувчи қуйидаги 3-босқичли протоколдан фойдаланишлари мумкин:

1. **A** $\rightarrow$ **B**: $E_{k_A}(k)$,

2. **B** $\rightarrow$ **A** : $E_{k_B}(E_{k_A}(k))$,



3. **A → B:** $D_{k_A}(E_{k_B}(E_{k_A}(k)))$.

13-расм. Шамир протоколи

Хусусан, Шамир протоколида модуль бўйича даражага кўтариш амалидан фойдаланиш таклиф этилган, яъни $E_{k_A}(k) = k^{k_A} \bmod p$. Шундай қилиб, бу протоколнинг криптобардошлиги дискрет логарифмлаш масаласининг мураккаблигига асосланган [2, 20]. Шамир протоколининг камчилиги шундаки, бу протоколда аутентификация масаласи ҳал этилмаган.

2.2.2. Нидхем-Шрёдер протоколи

Рожер Нидхем ва Михаэл Шрёдерлар томонидан яратилган бу протоколда арбитр ва симметрик криптотизимдан фойдаланилади (14-расм):

1. **A** иштирокчи ишончли томонга (**W**) ўзининг исмини, **B** иштирокчининг исмини ва ўзининг тасодифий сонини узатади.

A → W : A, B, R_A .

2. 3-ишончли томон сеанс калитни генерация қилади. Бу сеанс калитни ва **A** иштирокчининг исмини **B** иштирокчи билан умумий бўлган калит орқали шифрлайди. Сўнгра **A** иштирокчи ва ўзи учун умумий бўлган калит ёрдамида **A** иштирокчининг тасодифий сони, **B** иштирокчининг исми, калит ва шифрматнни шифрлайди. Ниҳоят у шифрланган маълумотни **A** иштирокчига узатади:

W → B : $E_A(R_A, B, k, E_B(k, A))$.

3. **A** иштирокчи маълумотни дешифрлаб, k калитни олади. У R_A ва 1-босқичда узатилган R_A ни солиштиради. Сўнгра **A** иштирокчи ишончли томон шифрлаган маълумотни **B** иштирокчига узатади:

A → B : $E_B(k, A)$.

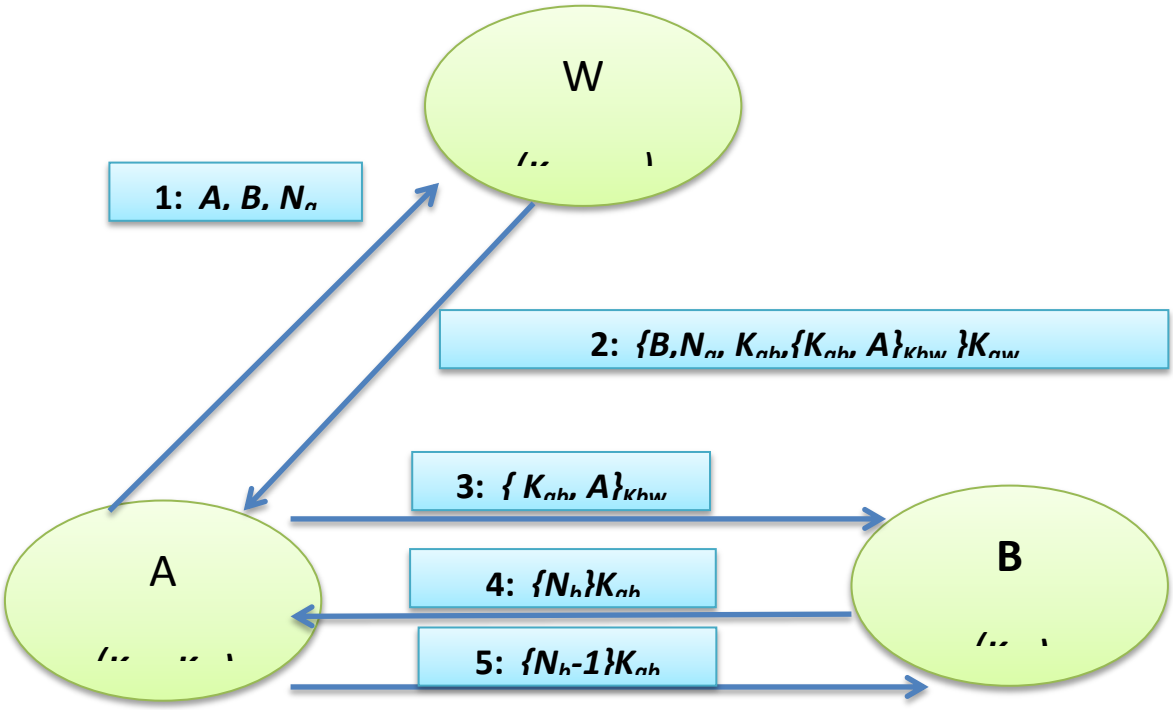
4. **B** иштирокчи бу маълумотни дешифрлайди ва k калитни олади. Сўнгра у тасодифий R_B сонини генерация қилади. Бу тасодифий сонни k калит ёрдамида шифрлайди ва **A** иштирокчига узатади:

B → A : $E_k(R_B)$.

5. **A** иштирокчи k калит ёрдамида маълумотни дешифрлайди. **A** иштирокчи тасодифий $R_B - 1$ сонини генерация қилади. Бу сонни k калит ёрдамида шифрлаб қайта **B** иштирокчига узатади:

A → B : $E_k(R_B - 1)$.

6. **B** иштирокчи маълумотни дешифрлаб, $R_B - 1$ сонини текширади ва ҳақиқатдан **A** иштирокчи билан алоқа ўрнатаётганига ишонч ҳосил қилади.



14-расм. Нидхем-Шрёдер протоколи

Бу протоколда R_A, R_B ва $R_B - 1$ сонларидан такроран фойдаланилади. Агар криптотаҳлилчи аввал фойдаланилган k калитни қўлга киритса,

3-босқичда **A** иштирокчи номидан **B** иштирокчига маълумот узатиши мумкин.

2.2.3. Wide-Mouth Frog протоколи

Wide-Mouth Frog протоколини ишончли сервер учун фойдаланиладиган калитларни алмашувчи симметрик протокол дейиш мумкин. **A** ва **B** иштирокчилар арбитр билан биргаликда умумий калитлардан фойдаланадилар. Wide-Mouth Frog протоколида **A** иштирокчи **B** иштирокчига сеанс калитни қуйидагича узатади (15-расм):

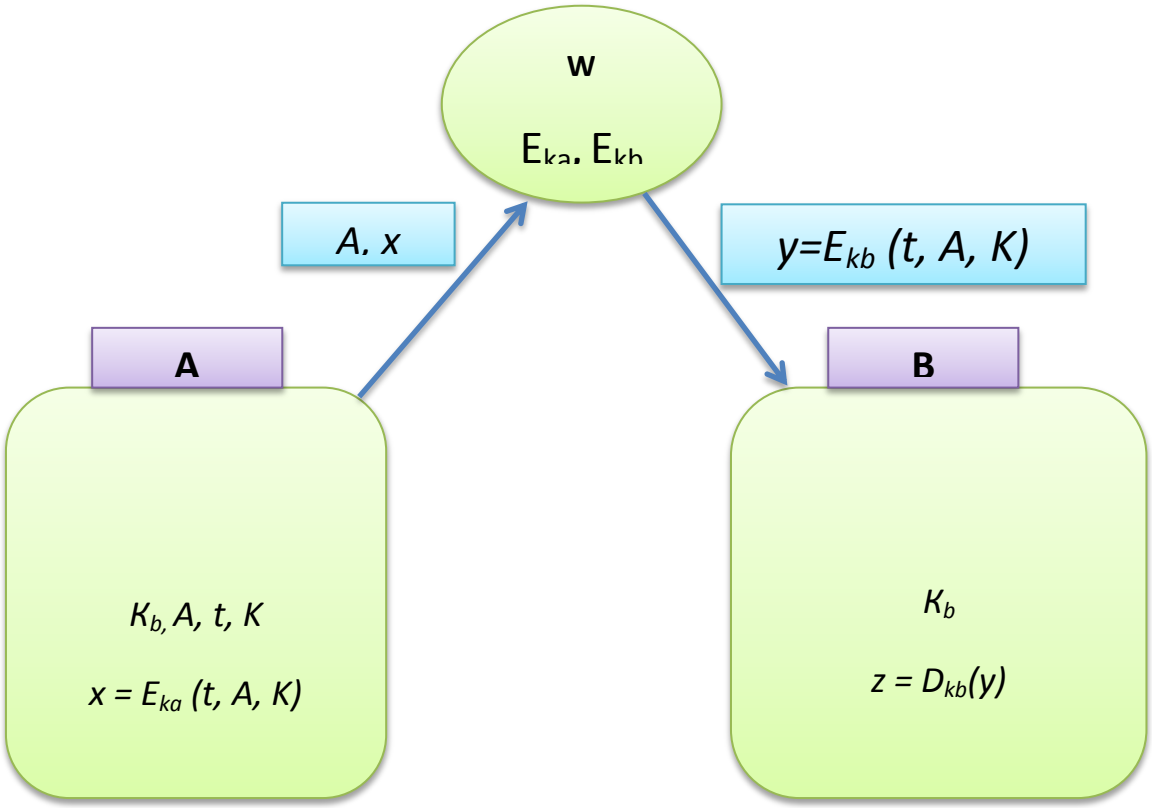
1. **A** иштирокчи вақт белгисини, **B** иштирокчининг исмини ва сеанс калитни бирлаштириб умумий калит билан шифрлайди. Ўзининг исмини ва шифрматнни арбитр (**W**) га узатади:

$$\mathbf{A} \rightarrow \mathbf{W}: \; A, E_A(t, A, k) .$$

2. Арбитр **A** иштирокчининг маълумотини дешифрлайди. Сўнгра янги вақт белгисини, **A** иштирокчининг исмини ва сеанс калитни бирлаштириб ўзи ва **B** иштирокчи учун умумий бўлган калит билан шифрлайди. Натижани **B** иштирокчига узатади:

$$\mathbf{W} \rightarrow \mathbf{B}: \; E_B(t, A, k) .$$

3. **B** иштирокчи бу маълумотни қабул қилиб умумий калит билан дешифрлайди ва вақт белгисини олиб, қабул қилган вақти билан солиштиради. Агар бу вақтлар орасидаги фарқ белгиланган интервалдан ошмаса, k калитни ҳақиқий деб қабул қилади.



15-расм. Wide-Mouth Frog протоколи

2.2.4. Yahalom протоколи

Yahalom протоколига мувофиқ **A** ва **B** иштирокчилар арбитр билан умумий калитдан фойдаланадилар. Протокол қадамлари кетма-кетлиги қуйидагидан иборат:

1. **A** иштирокчи ўзи исми ва тасодифий сонини бирлаштириб, **B** иштирокчига узатади:

$$\mathbf{A} \rightarrow \mathbf{B:}\ A, R_A\ .$$

2. **B** иштирокчи **A** иштирокчининг исмини, унинг тасодифий сонини ва ўзининг тасодифий сонини бирлаштириб умумий калит билан шифрлайди. Ўзининг исмини ва натижани бирлаштириб арбитрга узатади:

$$\mathbf{B} \rightarrow \mathbf{W:}\ B, E_B(A, R_A, R_B)\ .$$

3. Арбитр иккита маълумотни ҳосил қилади. Биринчи маълумот **B** иштирокчининг исми, сеанс калит, **A** ва **B** иштирокчиларнинг тасодифий сонларидан ташкил топган. Бу маълумотни ўзининг ва **A** иштирокчининг умумий калити билан шифрлайди. Иккинчи маълумот **A** иштирокчининг исми ва сеанс калитидан ташкил топган. Арбитр бу маълумотни ўзи ва **B** иштирокчи учун умумий бўлган калит билан шифрлайди. Сўнгра бу маълумотларни **A** иштирокчига узатади:

$$\mathbf{W} \rightarrow \mathbf{A:}\ E_A(B, k, R_A, R_B),\ E_B(A, k)\ .$$

4. **A** иштирокчи биринчи маълумотни дешифрлайди ва k калитни олади. У R_A ни 1-босқичда узатилган қиймати билан солиштиради ва тўғри эканлигига ишонч ҳосил қилади. Сўнгра **A** иштирокчи **B** иштирокчига иккита маълумот узатади, биринчи – арбитрнинг маълумоти, иккинчиси – сеанс калит билан шифрланган R_B - тасодифий сон:

$$\mathbf{A} \rightarrow \mathbf{B:}\ E_B(A, k),\ E_k(R_B)\ .$$

5. **B** иштирокчи биринчи маълумотни дешифрлаб, k калитни олади. Бу калит ёрдамида иккинчи маълумотни очиб, R_B нинг қиймати 2-босқичда юборилгани билан мос келишига ишонч ҳосил қилади.

Натижада **A** ва **B** иштирокчилар айнан бир-бирлари билан алоқа боғлаганларига ишонч ҳосил қиладилар.

2.2.5. Отвей-Риис протоколи

Бу протоколда ҳам симметрик шифрлаш алгоритмидан фойдаланилади. Протокол қадамлари кетма-кетлиги қуйидагича:

1. **A** иштирокчи тартиб рақами, ўзининг исми, **B** иштирокчининг исми ва тасодифий R_A сонидан ташкил топган маълумотни ҳосил қилади ва уни шифрлайди. Сўнгра у шифрматнни, тартиб рақамини, ўзининг ва **B** иштирокчининг исмини **B** иштирокчига узатади:

$$\mathbf{A \rightarrow B:}\ I, A, B, E_A(R_A, I, A, B).$$

2. **B** иштирокчи тасодифий R_B сони, тартиб рақами, **A** иштирокчи ва ўзининг исмидан ташкил топган маълумотни ҳосил қилади. Бу маълумот умумий калит билан шифрланади. Сўнгра **B** иштирокчи бу маълумотни, **A** иштирокчи юборган маълумотни, тартиб рақами, ўзи ва **A** иштирокчининг исмини арбитрга узатади:

$$\mathbf{B \rightarrow W:}\ I, A, B, E_A(R_A, I, A, B),\ E_B(R_B, I, A, B).$$

3. Арбитр тасодифий сеанс калитини хосил қилади. Сўнгра иккита маълумотни ҳосил қилади, биринчиси – **A** иштирокчининг умумий калити билан шифрланган **A** иштирокчининг тасодифий R_A сони, иккинчиси – **B** иштирокчининг умумий калити билан шифрланган **A** иштирокчининг тасодифий R_A сони. Арбитр тартиб рақамини ва иккала маълумотни бирлаштириб **B** иштирокчига узатади:

$$\mathbf{W \rightarrow B:}\ I, E_A(R_A, k),\ E_B(R_B, k).$$

4. **B** иштирокчи **A** иштирокчининг калити билан шифрлаган тасодифий сон ва k сеанс калитни **A** иштирокчига узатади:

$$\mathbf{B} \rightarrow \mathbf{A:}\ I, E_A(R_A, k).$$

5. **A** иштирокчи маълумотни дешифрлаб, ўзининг тасодифий сони ва k сеанс калитига эга бўлади. **A** иштирокчи протокол бажарилиши натижасида улар ўзгармасдан қолганига ишонч ҳосил қилади .

Агар протокол бажарилиши натижасида барча тасодифий сонлар тўғри ва тартиб рақами ўзгармаган бўлса, у ҳолда **A** ва **B** иштирокчилар бир-бирларининг ҳақ эканликларига ишонч ҳосил қиладилар ва ўзаро маълумот алмашиш учун махфий калитни қабул қиладилар.

2.2.6 Ньюман-Стабблбайн протоколи

Ньюман-Стабблбайн протоколи калит тақсимоти ва аутентификациясининг ИМ иштирокидаги симметрик протоколи бўлиб, Яхалом протоколининг такомиллаштирилган русуми ҳисобланади [10]. Ньюман - Стабблбайн протоколининг ўзига хос хусусияти шундан иборатки, унда томонлараро вақтни синхронлаштириш зарурати ва ИМни иштирокисиз такрорий аутентификация қилиш имконияти мавжуд.

Ньюман - Стабблбайн протоколининг схемаси қуйидагича (16-расм):

$$A \rightarrow B: A, R_A,$$

$$B \rightarrow S: B, R_b, \{A, R_A, t_B\}_{k_{bs}},$$

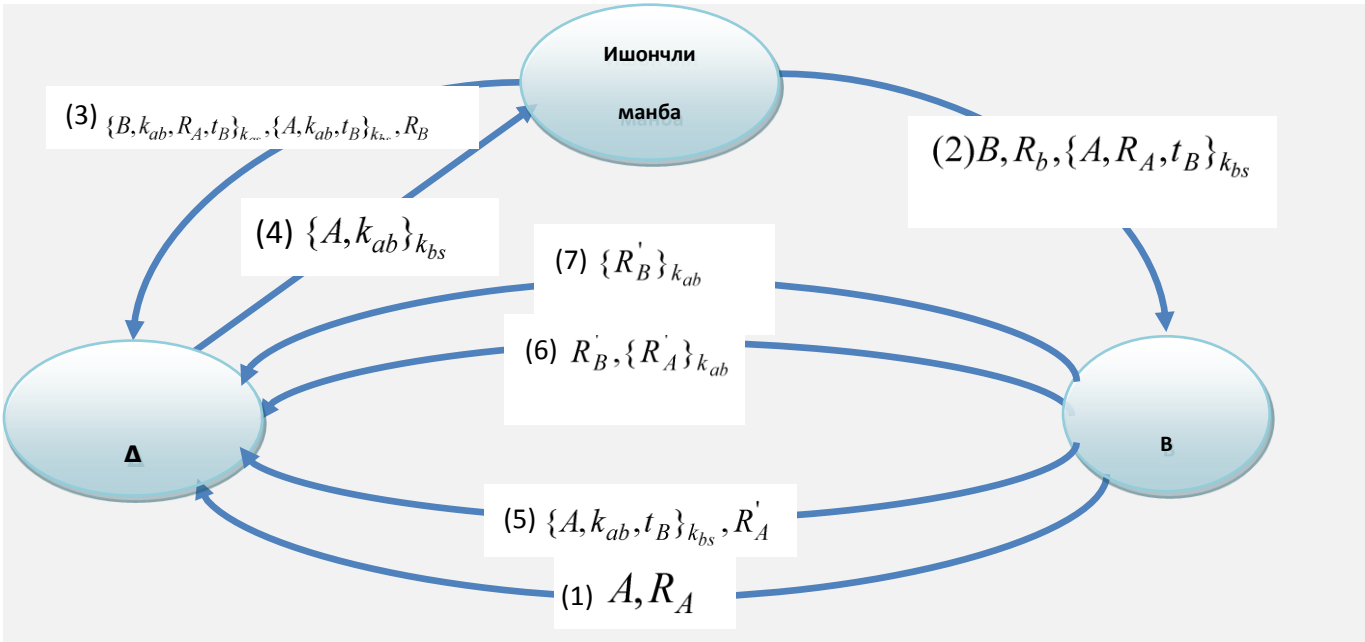
$$S \rightarrow A: \{B, k_{ab}, R_A, t_B\}_{k_{as}}, \{A, k_{ab}, t_B\}_{k_{bs}}, R_B$$

$$A \rightarrow B: \{A, k_{ab}\}_{k_{bs}}, \{R_B\}_{k_{ab}}$$

$$A \rightarrow B: \{A, k_{ab}, t_B\}_{k_{bs}}, R'_A$$

$$B \rightarrow A: R'_B, \{R'_A\}_{k_{ab}},$$

$$A \rightarrow B: \{R'_B\}_{k_{ab}}.$$



16-расм. Ньюман-Стабблбайн протоколи

А иштирокчи **В** иштирокчига тасодифий танланган сон R_A ни ва ўз идентификаторини юборади.

– **В** иштирокчи хабарни ўзининг ВБ t_B билан тўлдиради, сўнгра k_{bs} калит билан шифрлаб, ўз идентификаторини ва тасодифий танлаган R_B сонни қўшиб ИМга узатади.

– ИМ **В** иштирокчи идентификаторини, **А** иштирокчининг тасодифий танланган сон R_A ни, сеанс калити k_{ab} ни ва t_B ни k_{as} калит билан, А иштирокчидан идентификаторини, сеанс калити k_{ab} ни ва t_B ни k_{bs} калит билан шифрлаб, сўнгра тасодифий танлаган R_B сонни қўшиб **А** иштирокчига юборади.

– **А** иштирокчи R_A ни 1-хабарда ўзи юборгани билан таққослаб, бир хиллигига ишонч ҳосил қилиб, сўнгра ўз идантификаторини ва сеанс калити k_{ab} ни k_{bs} калит билан шифрлаб, унга R_B сонини сеанс калити k_{ab} билан шифрланганини қўшиб **В** иштирокчига узатади.

– **В** иштирокчи ўз навбатида t_B ва R_B қийматларни текшириб, ўзгармаганлигига ишонч ҳосил қилади.

Юқорида айтиб ўтганимиздек, бу протоколда ИМнинг иштирокисиз, янги тасодифий танланган сонлардан фойдаланиб такрорий аутентификация қилиш имконияти мавжуд, яъни

– **A** иштирокчи ўз идентификаторини, сеанс калити k_{ab} ни ва t_B ни k_{bs} калит билан шифрлаб уни янги тасодифий танланган сон $R_A^{'}$ билан тўлдириб **B** иштирокчига юборади.

– **B** иштирокчи янги тасодифий танланган сон $R_A^{'}$ ни сеанс калити k_{ab} билан шифрлаб, уни ўзи тасодифий танлаган янги $R_B^{'}$ билан тўлдириб **A** иштирокчига қайтаради.

– **A** иштирокчи эса ўз навбатида **B** тасодифий танлаган янги $R_B^{'}$ ни сеанс калити k_{ab} билан шифрлаб **B** иштирокчига юборади.

Бунда янги тасодифий танланган $R_A^{'}$ ва $R_B^{'}$ сонлардан фойдаланиш қайта юборишга бўладиган ҳужумдан ҳимоя қилади

2.3 Эллиптик эгри чизиқларга асосланган калитларни тақсимлаш алгоритмлари ва протоколлари

Кўплаб ошкора калитли криптографик маҳсулотлар ва стандартлар деярли анъанавий мавқега эришган RSA ва Эль Гамал алгоритмларига асосланган [18-20]. Сўнгги вақтларда криптотаҳлил усулларининг ва ҳисоблаш техникасининг кескин ривожланиши тизимларнинг ишончли ҳимояси учун калит битлари сонининг ҳам катта бўлишига олиб келди, бу эса анъанавий тизимларни қўлловчи тизимлар иловасини юкланиш вақтининг ортишига олиб келди. Бу ўз навбатида катта транзакцияларни ҳимоялаш талаб этиладиган, электрон тижоратга ихтисослашган алоқа тугунларида кўплаб муаммоларни келтириб чиқарди. Шу боис анъанавий мавқега эришган тизимларга рақиб бўлган эллиптик эгри чизиқларга асосланган криптография вужудга келди [21-25]. Ҳозирги кунда эллиптик эгри чизиқларнинг криптография соҳасига тадбиқи кенг қўлланилмоқда. Эллиптик эгри чизиқлар назарияси замонавий криптография ва сонлар назариясида асосий ўрганиш объектларидан бири ҳисобланади. Мисол учун, булар Эндрю Уайлс (Ричард Тейлор билан биргаликда) Ферманинг буюк теоремасини исботлашда фойдаланилган.

Эллиптик эгри чизиқлар криптографияси — криптографиянинг мустақил бир бўлими ҳисобланиб, чекли майдонлардаги эллиптик эгри чизиқларга асосланган носимметрик криптотизимларни ўрганади. Эллиптик эгри чизиқлар криптографиясининг асосий афзаллиги ҳозирги кунгача эллиптик эгри чизиқлардаги нуқталар группасини дискрет логарифмлаш масаласи асосида субэкспоненциал алгоритмларни ечишга қаратилган муаммонинг аниқланмаганлиги ҳисобланади.

Криптотизимларни яратишда эллиптик эгри чизиқлардан фойдаланиш бир-биридан мустақил равишда Нил Коблиц ва Виктор Миллерлар томонидан 1985 йилда тавсия этилган.

Носимметрик криптотизимлар криптобардошлиги бир қатор математик масалаларнинг ечиш мураккаблигига асосланган. Илк очиқ калитли криптотизим, яъни алгоритм RSAнинг криптобардошлиги мураккаб

сонларни туб кўпайтувчиларга ажратиш муаммосига асосланганлигидадир. Эллиптик эгри чизиқларда худди шу криптобардошликда RSAга нисбатан калит ўлчами қисқа бўлади, бу маълумотни сақлаш ва узатишда сезиларли даражада сарфнинг камайишига олиб келади.

Мисол учун RSA-2005 конференциясида Миллий хавфсизлик агентлиги “Suite B” ни яратишда фақат эллиптик эгри чизиқли алгоритмлардан фойдаланилганлигини баён қилган.

Шундай қилиб, эллиптик эгри чизиқларга асосланган криптографик тизимларнинг анъанавий тизимларга нисбатан афзаллиги, уларда фойдаланиладиган калит узунлиги разряди кичик бўлганда ҳам, эквивалент ҳимоя билан таъминлашидадир. Бу эса қабул қилувчи ва узатувчи мослама процессорларининг юкланиш вақтини камайтиради.

Эллиптик эгри чизиқлар қуйидаги кўринишдаги тенгламалар ёрдамида берилади:

$$y^2 + axy + by = x^3 + cx^2 + dx + g,$$

бунда a, b, c, d бутун сонлар.

Эллиптик эгри чизиқ O деб белгиланган махсус бўлмаган (чексизликдаги нуқта, нол элемент) элементни ўз ичига олади.

Эллиптик эгри чизиқ таърифидан агар учта нуқта бир тўғри чизиқда ётса, уларнинг йиғиндиси O эканлиги келиб чиқади. Бу таърифдан эллиптик эгри чизиқ нуқталарининг қўшишни қуйидаги қоидалари келиб чиқади:

1. Қўшишда O нол элементи сифатида қатнашади, яъни $O=-O$ бўлиб, эллиптик эгри чизиқнинг ихтиёрий нуқтаси учун $P+O=P$.
2. Вертикал чизиқ эллиптик эгри чизиқни бир хил x абциссали иккита нуқтада кесиб ўтади. Бу чизиқ эгри чизиқни чексизлик нуқтасида ҳам кесиб ўтади. Шунинг учун $P_1+P_2+O=O$ ва $P_1=-P_2$, бунда $P_1=(x,y)$, $P_2=(x,-y)$. “Манфий” ишорали нуқта бу x координатаси худди ўша қийматга, y координатаси эса ишораси бўйича қарама-қарши қийматга эга бўлган нуқтадир.
3. Турли x координатали Q ва R нуқталарни қўшиш учун, бу икки нуқта орқали тўғри чизиқ ўтказилади ва бу тўғри чизиқнинг эллиптик эгри

чизиқ билан кесишган учинчи нуқтаси P_1 топилади. Агар бу нуқталарнинг бирортасида тўғри чизиқ эллиптик эгри чизиққа уринма бўлмайдиган бўлса, у ҳолда бу тўғри чизиқнинг ЭЭЧ билан фақат битта кесишиш нуқтаси топилади. Бунда $Q + R = -P_1$.

4. Q нуқтани иккилантириш учун Q нуқтадан уринма ўтказиш керак ва бошқа S кесишиш нуқтасини топиш керак. Бунда $Q + Q = 2Q = -S$.

Қўшишнинг юқорида келтирилган хоссалари қўшишнинг барча оддий хоссаларига, масалан, коммутативлик ва ассоциативлик қонунларига бўйсунади. Эллиптик эгри чизиқнинг P нуқтасини k сонга кўпайтириш P нуқтанинг k та нусхасининг йиғиндиси шаклида аниқланган. $2P = P + P$, $3P = P + P + P$ ва ҳоказо.

p - туб сонли модуль бўйича эллиптик группа криптографияда алоҳида қизиқиш касб этади. Бундай группа қуйидагича аниқланади. Иккита манфий бўлмаган ва p дан кичик бўлган бутун a ва b сонлар танланади, бунда

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

шарт бажарилсин, у ҳолда $E_p(a,b)$ p модуль бўйича эллиптик группани билдиради. Бу группанинг элементлари манфий бўлмаган p дан кичик (x,y) сонлар жуфтлиги бўлиб, чексизликдаги O нуқта билан $y^2 \equiv (x^3 + ax + b) \pmod p$ шартни қаноатлантиради.

Эллиптик группа учун $(0,0)$ дан (p,p) гача бўлган, квадрати манфий сон бўлмаган p модуль бўйича тенгламани қаноатлантирадиган фақат бутун қийматлар қаралади.

Эллиптик эгри чизиқда нуқтани топиш қуйидаги алгоритм ёрдамида амалга оширилади:

1. x нинг $0 \le x < p$ шартни қаноатлантирувчи ҳар бир қиймати учун $(x^3 + ax + b) \bmod p$ ҳисобланади.

2. Аввалги қадамда ҳосил қилинган ҳар бир қиймат учун бу қийматнинг p модуль бўйича квадрат илдизи мавжудлиги текширилади. Агар квадрат илдиз мавжуд бўлмаса, у ҳолда $E_p(a,b)$ тўпламда x нинг бу қийматига мос нуқта мавжуд эмас. Агар илдиз мавжуд бўлса, у ҳолда y

илдиздан чиқаришга мос келувчи (нол бўлмаган ҳолда) иккита қийматга эга бўлади. *(x,y)* нинг бу қийматлари $E_p(a,b)$ нинг нуқталари бўлади.

$E_p(a,b)$ да қўшиш қоидасини геометрик формулаларга мос ҳолда қуйидагича ёзиш мумкин:

1. $P + O = P$.

2. Агар $P = (x, y)$ бўлса, у ҳолда $P + (x, -y) = O$. *(x,-y)* нуқта *P* нуқтанинг манфий қиймати дейилади ва *(-P)* каби белгиланади. *(x,-y)* нуқта эллиптик эгри чизиқда ётади ва демак, $E_p(a,b)$ га тегишли бўлади.

3. Агар $P = (x_1, y_1)$ ва $Q = (x_2, y_2)$ бўлса, бунда $P \neq Q$, у ҳолда $P + Q = (x_3, y_3)$ қуйидаги қоидалар асосида аниқланади:

$$x_3 \equiv (\lambda^2 - x_1 - x_2) \bmod p,$$

$$y_3 \equiv (\lambda\ (x_1 - x_2) - y_1) \bmod p,$$

бунда

$$\lambda = \begin{cases} \dfrac{y_2 - y_1}{x_2 - x_1} \Rightarrow P \neq Q \\ \dfrac{3x_1^2 + a}{2y_1} \Rightarrow P = Q \end{cases}.$$

Эллиптик эгри чизиқ нуқталари қўшиш амалига нисбатан коммутатив ва ассоциатив, яъни нуқталар тўплами чексизлик нуқтаси *O* билан бирга абель группасини ташкил қилади.

Хусусияти 2 бўлган майдонлардаги эллиптик эгри чизиқлар икки хил кўринишда қаралади:

- Суперсингуляр эллиптик эгри чизиқ:

$y^2 + ay = x^3 + bx + c.$

- Суперсингуляр бўлмаган эллиптик эгри чизиқ:

$y^2 + axy = x^3 + bx^2 + c.$

Суперсингуляр эллиптик эгри чизиқнинг ўзига хос афзаллиги шундаки, у учун нуқталар тўпламини ҳисоблаш енгил ҳисобланади, суперсингуляр бўлмаган эллиптик эгри чизиқларни нуқталарини топиш бир қанча

қийинчиликлар туғдиради. Суперсингуляр эллиптик эгри чизиқ қўлбола ECC-криптотизимларни яратишда жуда қўл келади. Улардан фойдаланиш унчалик мураккаб бўлмаган процедураларни хисоблаш орқали амалга ошириш мумкинлиги билан бошқаларидан ажралиб туради.

Эллиптик криптографияда асосан қуйидаги ЭЭЧ кўринишларидан фойдаланилади:

- $K = F(p)$ майдон устида, бу ерда туб сон $p>3$, ва туб майдон кенгайтмаси $K = F(p^n)$ устида аниқланган *носуперсингуляр ЭЭЧ,*

- $K = F(2^m)$ майдони устида аниқланган *носуперсингуляр ЭЭЧ.*

Криптографияда эллиптик эгри чизиқдан фойдаланишда барча қатнашувчилар эллиптик эгри чизиқни қуриш учун керак бўладиган барча параметрлар тўпламини келишиб олиши лозим. Эллиптик эгри чизиқ a ва b константалар билан аниқланади: $E: \quad y^2 = x^3 + Ax + B \pmod p$, Кофактор $h = \frac{|E|}{n}$, бу ерда n — G даги нуқталарнинг тартиби, у унча катта бўлиши муҳим эмас ($h \le 4$, одатда $h = 1$ олинади).

Демак, хусусияти 2 бўлган майдон майдон параметрлари тўплами: (m, f, a, b, G, n, h), $\mathbb{Z}_p$ чекли майдон учун (бу ерда $p > 3$) эса (p, a, b, G, n, h).

Бир қанча параметрлар тўплами учун тавсиялар мавжуд:

- NIST (Стандартлар ва тенологиялар миллий институти).
- SECG

Хусусий параметрлар тўпламини яратиш учун қуйидагиларни амалга ошириш зарур:

1. Параметрлар тўпламини танлаш.
2. Шу параметрлар тўпламини қаноатлантирадиган эллиптик эгри чизиқни топиш.

Берилган параметрлар бўйича эллиптик эгри чизиқни аниқлашда қуйидаги икки хил усулдан фойдаланилади:

- Ихтиёрий эллиптик эгри чизиқни танлаш ва нуқталарни аниқлаш алгоритмларидан фойдаланиш.
- Нуқталарни танлаш ва шу асосида кўпайтириш техникасидан фойдаланиб эллиптик эгри чизиқни қуриш.

Бир қанча криптографик ”кучсиз” параметрлар тўплами мавжуд. Улардан фойдаланиш тавсия этилмайди, булар қуйидагилар:

- $\mathbb{F}_{2^m}$ устидаги эллиптик эгри чизиқлар, бу ерда m – туб бўлмаган сон. Бундай эгри чизиқлар билан шифрлаш Вейл атакалари билан тасдиқланган.
- $|E(\mathbb{F}_q)| = q$ ли эллиптик эгри чизиқлар ҳужумларга бардошли эмас. Бундай нуқталар $\mathbb{F}_q$ майдоннинг аддитивлик группасини намоён қилади.

p модуль асосида бўлиш (кўпайтириш ва қўшиш жараёни учун керак)да, агар p га 2 ни даражасидаги туб сонлар олинса, тезроқ ишлаши мумкин. p Мерсен туб сонларини ишлатиш ҳам мумкин. Мисол учун, $p = 2^{251} - 1$ ёки $p = 2^{256} - 2^{32} - 2^9 - 2^8 - 2^7 - 2^6 - 2^4 - 1$ лар яхши танлов ҳисобланади. Стандартлар ва тенологиялар миллий институти p учун туб сонларни қўллашни тавсия этади.

Эллиптик эгри чизиқларнинг яна бир ютуқларидан бири NIST тавсия этишича $a = -3$ ни танлаш Якоби координталарида қўшиш жараёнини анча тезлаштиради.

NIST 15 та эллиптик эгри чизиқни тавсия этади. FIPS-186-3 (маълумотларни қайта ишлаш бўйича федерал стандарт) эса тавсиясига асосан 10 та чекли майдонларни ишлатишни тавсия этади. Шулардан бир нечтаси қуйидагилар:

- $\mathbb{F}_p$ майдон, бу ерда p нинг узунлиги 192, 224, 256, 384 ёки 521 бит.
- $\mathbb{F}_{2^m}$ майдон, бу ерда m = 163, 233, 283, 409 ёки 571 бит.

Ҳар бир чекли майдон учун битта эллиптик эри чизиқ тавсия этилади. Бу чекли майдонлар ва эгри чизиқлар юқори криптобардошлик ҳамда дастурий таъминот ишлаб чиқишда самарадорлиги сабабли танлаб олинган.

Хусусан олганда эллиптик эгри чизиқлар электрон рақамли имзо стандартлари (ГОСТ Р 34.10-2001, ECDSA), калитларни тақсимлаш алгоритмлари (ECDH, ECMO ва ECMQV), сонларни тубликка текшириш, факторлаш алгоритмлари (Ленстри алгоритми) ва бошқа кўплаб ҳолатларда ишлатилади.

2.3.1. Диффи–Хеллманнинг ECDH калитларни тақсимлаш алгоритми

Диффи-Хеллманнинг эллиптик эгри чизиқларга асосланган аналоги ECDH қуйидаги кўринишда бўлади: аввал катта туб p сон ва ЭЭЧ учун a, b параметрлар танланади [20, 25-26]. Бу эллиптик нуқталар группаси $E_p(a, b)$ ни беради. Сўнгра $E_p(a, b)$ да генерацияловчи нуқта $G=(x,y)$ танланади. G ни танлаганда $nG=0$ шартни қаноатлантирувчи n нинг энг кичик қиймати жуда ҳам катта туб сон бўлиши муҳим. Криптотизимнинг G ва $E_p(a, b)$ параметрлари барча иштирокчиларга маълум параметр ҳисобланади.

A ва **B** иштирокчилар орасидаги калит тақсимоти қуйидаги схема бўйича амалга оширилади:

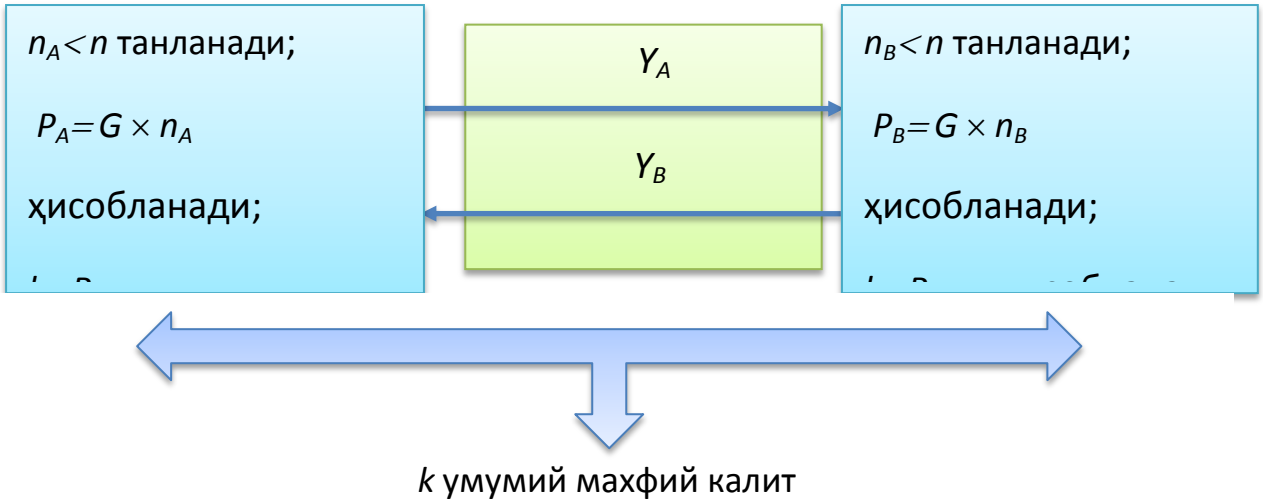
1. **A** иштирокчи бутун $n_A < n$ сонни танлайди. Бу сон **A** иштирокчининг махфий калити бўлади. Сўнгра **A** иштирокчи очиқ калити $P_A = G \times n_A$ генерация қилади. Очиқ калит $E_p(a, b)$ га тегишли нуқта бўлади.
2. **B** иштирокчи ҳам худди шундай n_B махфий калитни танлайди ва $P_B = G \times n_B$ очиқ калитни ҳисоблайди.
3. **A** иштирокчи $k = P_B \times n_A$ махфий калитни, **B** иштирокчи эса $k = P_A \times n_B$ махфий калитни генерация қилади.

3-қадамдаги иккала формула ҳам бир хил қийматни беради

$$P_B \times n_A = (G \times n_B) \times n_A = (G \times n_A) \times n_B = P_A \times n_B.$$

Бу схемани бузиши учун бузғунчи G ва G k нинг қийматларидан k ни ҳисоблаб топиши керак бўлади (18-расм). Бу эса қийин ечиладиган масала ҳисобланади.

A **B**



18-расм. ЭЭЧларга асосланган Диффи- Хеллман схемасининг аналоги

Модуль $p=211$ ва эллиптик нуқталар тўплами $E_{211}(0,-4)$ ни танлаймиз. Уларга мос келувчи ЭЭЧ $y^2=x^3-4$ ва $G=(2,2)$. Ҳисоблашлар $241\,G=0$ эканини кўрсатади. **A** иштирокчининг махфий калити $n_A = 121$ бўлсин, у ҳолда **A** иштирокчининг очиқ калити $P_A = 121\,(2,2) = (115\,,48)$ бўлади. **B** иштирокчининг махфий калити $n_B = 203$ бўлсин, у ҳолда **B** иштирокчининг очиқ калити $P_B = 203\,(2,2) = (130\,,203)$ бўлади. У ҳолда умумий махфий калит 121(130,203)=203(115,48)=(161,169) бўлади.

ЭЭЧларга асосланган криптографияда махфий калит сифатида сонлар жуфтлиги қаралади. Агар бу калитдан анъанавий шифрлашда фойдаланилмоқчи бўлса, у ҳолда бу иккита сондан мос битта қиймат генерация қилинади. Ёки бўлмаса x ё y координаталардан бирини ишлатиш мумкин.

2.3.2 Эллиптик эгри чизиқли MQV калитларни тақсимлаш алгоритми

MQV (Менезес-Кью-Ванстоун) калитларни тақсимлаш протоколи бўлиб, Диффи-Хеллман алгоритми базасида қурилган. Протокол каноник чекли майдонлар учун ҳам ишлаши мумкин, хусусий ҳолда эллиптик эгри чизиқларга асоланган ECMQV алгоритми мавжуд.

MQV алгоритми биринчи марта Алфред Менезис, Кью, Скотт Ванстоунлар томонидан 1985 йилда тавсия этилган. 1998 йилда эса унинг модификацияланган варианти ишлаб чиқилган. Алгоритмнинг бир, икки ва уч ўтишли турлари мавжуд. MQV алгоритми очиқ калитли криптотизимлар бўйича IEEE P1363 стандартига киритилган.

MQV алгоритмининг бир нечта турлари учун олинган патентлар Certicom компаниясига тегишли ҳисобланади. MQV алгоритмининг бир қанча камчиликлари 2005 йилда такомиллаштирилган HMQV алгоритмида бартараф этилган.

Келтирилган иккала MQV ва HMQV алгоритмлар бир қатор заифликларга эга бўлиб, бу камчиликлар FHMQV протоколида бартараф этилган. Криптобардошлигини ошириш, алгоритм ва калит узунлигига бўлган сарф-ҳаражатларни пасайтириш учун эллиптик эгри чизиқларга асосланган ECMQV алгоритми таклиф этилган.

ECMQV алгоритмининг тавсифи қуйидагича баён этилади:

A иштирокчида статик калитлар жуфтлиги (W_a, w_a)лар мавжуд, бу ерда W_a унинг очиқ калити ва w_a унинг ёпиқ калити. **B** иштирокчида статик калитлар жуфтлиги (W_b, w_b) лар мавжуд, бу ерда W_b унинг очиқ калити ва w_b унинг ёпиқ калити ҳисобланади. $\bar{R}$ ни аниқлаймиз. $R = (x, y)$ эллиптик эгри чизиқдаги нуқта бўлсин. Унда $\bar{R} = (x \bmod 2^L) + 2^L$бўлади, бу ерда $L = \left\lceil \frac{\lfloor \log_2 n \rfloor + 1}{2} \right\rceil$ га тенг ва n эса P генератордаги тартиби ҳисобланади. Бундан ташқари кофактор h ни ҳам аниқлаймиз $h = \frac{|G|}{n}$, бу ерда $|G|$ G группанинг тартиби ҳисобланади ва техник жиҳатдан қуйидаги тенгликни қаноатлантириши керак (3-жадвал): $gcd(n, h) = 1$.

3-жадвал

ECMQV алгоритмининг бажарилиш жараёни

Қадам	Жараён
1	**A** иштирокчи (R_a, r_a) калитлар группасини ҳосил қилади, r_a ни ихтиёрий генерация қилади ва R_a=$r_a P$ ни ҳисоблайди. Бу ерда P — эллиптик эгри чизиқдаги нуқта. Шундан сўнг **B** иштирокчига вақтинчалик очиқ калит R_a ни жўнатади.
2	**B** иштирокчи (R_b, r_b) калитлар группасини ҳосил қилади, r_b ни ихтиёрий генерация қилади ва R_b=$r_b P$ ни ҳисоблайди. Шундан сўнг **A** иштирокчига вақтинчалик очиқ калит R_b ни жўнатади
3	**A** иштирокчи R_b вақтинчалик очиқ калитни G группага тегишлилигини текширади, ундан ташқари R_b нол элемент эмаслигига ҳам текширади. Шундан сўнг группа элементи Kab ни ҳисоблайди, $Kab = hs_a S_b$, бу ерда $s_a = (r_a + \bar{R}_a w_a) mod n$ ва $S_b = R_b + \bar{R}_b W_b$. Агар $Kab = O$ бўлса **A** иштирокчи **B** иштирокчи дан келган маълумотларни бекор қилади. Акс ҳолда натижани умумий махфий калит сифатида қабул қилади.
4	**B** иштирокчи R_a вақтинчалик очиқ калитни G группага тегишлилигини текширади, ундан ташқари R_a нол элемент эмаслигига ҳам текширади. Шундан сўнг группа элементи Kba ни ҳисоблайди, $Kba = hs_b S_a$, бу ерда $s_a = (r_a + \bar{R}_a w_a) mod n$ ва $S_b = R_b + \bar{R}_b W_b$. Агар $Kba = O$ бўлса **A** иштирокчи **A** иштирокчи дан келган малумотларни бекор қилади. Акс ҳолда натижани умумий махфий калит сифатида қабул қилади.

Асосий протокол қуйидаги сабабларга кўра ажойиб ечим ҳисобланади:

1. У калит ошкора бўлмаган тарзда идентификация қилади ва ҳар бир шерик учун навбатдаги ҳимоя ҳосил қилинади.

2. Фақат хисоблаш жараёнида самарали бўлмай, балки ўтказиш қобилиятидан ҳам ютуққа эришади. Бундан ташқари жараёнлар фақат майдонларда ва оддий ҳолда амалга оширилади. Ҳар бир фойдаланувчи учун 2.5 та ҳисоблаш (кўпол баҳолаганда) бажарилади, яни биттаси вақтинчалик калит жуфтлигини ҳосил қилиш бўлса, қолгани s_a ёки s_b скаляр кўпайтириш учун.

B иштирокчининг ҳисоблашлари:

$$Kba = h{\cdot}s_b(R_a+\bar{R}_aW_a) = h{\cdot}s_b(r_aP+\bar{R}_aw_aP) = h{\cdot}s_b(r_a+\bar{R}_aw_a)P = h{\cdot}s_bs_aP$$

A иштирокчининг ҳисоблашлари:

$$Kab = h{\cdot}s_a(R_b+\bar{R}_bW_b) = h{\cdot}s_a(r_bP+\bar{R}_bw_bP) = h{\cdot}s_a(r_b+\bar{R}_bw_b)P = h{\cdot}s_bs_aP$$

Шунинг учун ҳам $Kab = Kba$ га ҳақиқатдан тенг ва $K = h \cdot s_bs_aP$ калитга эквивалент ҳисобланади.

2.3.3. Эллиптик эгри чизиқли Месси-Омар калитларни тақсимлаш алгоритми

Фараз қилайлик *E - n* тартибли ЭЭЧ, *e* эса *(e, n)= 1, 1<e<n* шартни қаноатлантирувчи сон. Инвертлаш алгоритмидан фойдаланиб $d \equiv e^{-1} \bmod n$ ни топамиз. Бутун сонлар устидаги модуль арифметикаси қонунлари билан ЭЭЧ нуқталари устидаги модуль арифметикаси қонунлари бир хил бўлгани учун, ЭЭЧнинг ихтиёрий *P* нуқтасини қуйидаги формулалар ёрдамида ҳисоблаш мумкин:

$$Q = eP ,$$

$$R = dQ .$$

Месси – Омур протоколи ЭЭЧнинг берилган нуқтасини базавий нуқтага нисбатан скаляр кўпайтувчисини аниқлаш муаммосининг ечилишига, яъни ЭЭЧларда дискрет логарифм масаласини ечишга асосланган [10-12].

A ва **B** иштирокчилар орасида калит тақсимотини қуйидаги схема ёрдамида амалга оширилади (19-расм):

1. **A** иштирокчи $e_A < n$ бутун сонни танлайди ва $d_A \equiv e^{-1}{}_A \bmod n$ ни ҳисоблайди. e_A сон **A** иштирокчининг махфий калити бўлади. d_A эса **A** иштирокчининг шахсий шифрни очиш калити бўлади. Сўнгра **A** иштирокчи ўзининг m хабарини P_m ЭЭЧнинг бирор нуқтасига жойлаштиради ва ўзининг махфий e_A га кўпайтириб, (очиқ калит генерация қилади): яъни

$P_A = e_A P_m$ нуқтани ҳосил қилади.

2. **B** иштирокчи ҳам ўзи учун худди шундай шахсий шифрлаш ва шифрни очиш калитлари e_B ва d_B калитларни ҳосил қилади. Сўнгра **B** иштирокчи ўзининг махфий калити қийматини **A** иштирокчининг ошкора P_A калитига кўпайтириб (ошкора калитни генерация қилади): яъни

$$P_B = e_B P_A$$

нуқтани ҳосил қилади.

3. Бу қийматни **A** иштирокчига жўнатади.
4. **A** иштирокчи

$P_O = d_A P_B$ ни ҳисоблайди.

5. Ҳисоблаб топилган қийматни **B** иштирокчига юборади.
6. **B** иштирокчи юборилган қийматни ўзининг махфий шифрни очиш калитига d_B кўпайтириб, **A** иштирокчининг m хабарига мос P_m нуқтани топади:

$$P_m = d_B P_O .$$

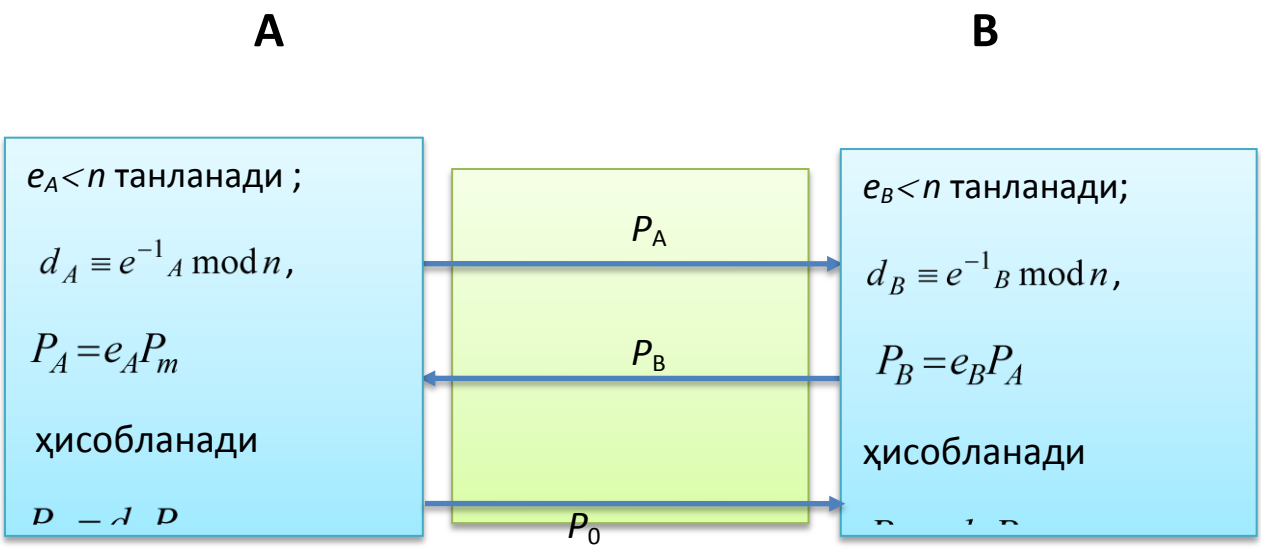
P_O ни ҳисоблаб **A** иштирокчи ўзининг шифрлаш калитининг фаолиятини бартараф қилади:

$$P_O = d_A P_B = d_A (e_B P_A) = d_A (e_B (e_A P_m)) = e_B (d_A (e_A P_m)) = e_B P_m .$$

Демак, **B** иштирокчи қуйидагини олади:

$$d_B P_O = d_B (d_A P_m) = P_m .$$

m хабар анъанавий криптотизимлар учун калит ўрнида ишлатилиши мумкин. Бу ҳолда ЭЭЧнинг ўзидан бошқа протокол параметрлари тўғрисида ҳеч қандай ахборотни эълон қилиш талаб этилмайди. Бунинг эвазига очиқ канал бўйлаб уч марта узатиш амалга оширилади.



19-расм. Месси – Омур схемаси бўйича калит тақсимлаш протоколи

2.3.4. Эллиптик эгри чизиқли криптотизимлар учун Эль Гамал калитларни тақсимлаш алгоритми

RSA криптотизимида Эль Гамал протоколининг қўлланилиши қуйидагича бўлади. n туб сон ва ихтиёрий $p < n$ ва $q < n$ сонлар танланади. Очиқ калит сифатида $(n, p, p^q \bmod n = y)$ учлик, махфий калит сифатида эса q дан фойдаланилади.

Очиқ m матнни шифрлаш учун $a \equiv p^k (\bmod n), b(m) \equiv (y^k m)(\bmod n)$ ҳисоблаш керак бўлади, бунда k - ихтиёрий n билан ўзаро туб бўлган сон.

$a, b(m)$ жуфтлик шифрматн бўлади. Равшанки, матнни шифрини очиш учун $m = (b(m) / a^q) \bmod n$ ҳисобланади.

ЭЭЧнинг мультипликатив группасини қўлловчи Эль Гамал протоколининг модификацияси қуйидагича:

Фараз қилайлик, *M* очиқ матн *E* ЭЭЧнинг нуқтаси бўлсин. Агар очиқ матн бир қанча нуқталар тўпламидан иборат бўлса, қуйида келтириладиган алмаштиришлар ҳар бир нуқта учун алоҳида бажарилади.

Криптотизимнинг **А** ва **В** иштирокчилари Диффи-Хеллман протоколи бўйича $k_A Q$ ва $k_B Q$ калит қисмларини алмаштиришди. **А** иштирокчи **В** иштирокчига *M* хабарни юбормоқчи бўлса, l махфий сонни танлайди ва **В** иштирокчига ЭЭЧнинг $E = (lQ, M + l(k_B Q))$ нуқталар жуфтини юборади. Олинган ахборотни шифрини очиш учун **В** иштирокчи $T = k_B(lQ)(l(k_B Q))$ ни ҳисоблаши керак. Бунда $M = M + l(k_B Q) - T$.

Эътиборли жиҳати шундаки, lQ нуқта шифрни йиғиш функциясини бажаради ва демак, бирон бир Q нуқта икки марта ишлатилиши мумкин эмас. Агар икки марта ишлатилса, икки хил шифрматнни таққослаш натижасида нафақат шифрматннинг шифрини синдириш, балки тизимнинг махфий компонентларини аниқлашнинг ҳам имкони туғилади.

2.3.5. Модуль арифметикасига асосланган протоколлар

Модуль арифметикасига асосланган калитларни тақсимлаш протоколи ҳар иккала томондан симметрик бажараладиган уч босқичдан иборат [1-5].

Биринчи босқичда **А** ва **В** иштирокчилар ўзининг махфий k_A, d_A ҳамда k_B, d_B маълумотларидан фойдаланиб, қуйидагиларни ҳисоблайди:

$$s_A = (k_A + x_A a_A d_A) \bmod n,$$

$$s_B = (k_B + x_B a_B d_B) \bmod n .$$

Иккинчи босқичда улар эллиптик эгри чизиқнинг нуқталарини ҳисоблашади:

$$U_A = R_B + x_B a_B Q_B ,$$

$$U_B = R_A + x_A a_A Q_A .$$

Учинчи босқичда улар эллиптик эгри чизиқ нуқтасини ҳисоблашади:

$$W = s_A U_A ,$$

$$W = s_B U_B .$$

Чап тарафидаги белгилашнинг бир хиллиги бу иккала тенгликнинг қиймати тенглигини билдиради. Буни эса қуйидагича исботлаш мумкин.

A иштирокчи учун

$$s_A U_A = ((k_A + x_A a_A d_A) \bmod n)(R_B + x_B a_B Q_B) =$$

$$= ((k_A + x_A a_A d_A) \bmod n)(k_B P + x_B a_B d_B P) =$$

$$= ((k_A + x_A a_A d_A) \bmod n)(k_B + x_B a_B d_B) P =$$

$$= ((k_A + x_A a_A d_A)(k_B + x_B a_B d_B) \bmod n) * P .$$

B иштирокчи учун

$$s_B U_B = ((k_B + x_B a_B d_B) \bmod n)(R_A + x_A a_A Q_A) =$$

$$= ((k_B + x_B a_B d_B) \bmod n)(k_A P + x_A a_A d_A P) =$$

$$= ((k_B + x_B a_B d_B) \bmod n)(k_A + x_A a_A d_A) P =$$

$$= ((k_B + x_B a_B d_B)(k_A + x_A a_A d_A) \bmod n) * P .$$

Қараб чиқилаётган протоколнинг талқинида модуль арифметикаси эллиптик эгри чизиқлар арифметикаси билан уйғунлаштирилган.

Модуль арифметикасидан фойдаланилмаган ва s_A, s_B сонлар аввалдан ҳисобланмаган ҳолдаги талқинни кўриб чиқамиз.

A иштирокчи Q_B нуқтани a_B константага ва x_B константага кўпайтириб, сўнгра ҳосил бўлган нуқтани R_B нуқта билан қўшиб эллиптик эгри чизиқнинг U_A нуқтасини ҳисоблаб топиши мумкин. Худди шундай B иштирокчи ҳам U_B нуқтани ҳисоблаб топиши мумкин.

W нуқтани олиш учун **A** ва **B** иштирокчилар олинган нуқталарни s_A, s_B константаларга кўпайтириш лозимлигини кўзда тутган ҳолда, қуйидаги алгоритм бўйича амалга оширишлари мумкин (**A** иштирокчи учун):

1) Эллиптик эгри чизиқ нуқтасини константага кўпайтириш натижасида $k_A U_A$ ни ҳисоблаш.

2) Мос катталикларни кетма-кет кўпайтириш йўли билан $x_A(a_A(d_A U_A))$ ни аниқлаш.

3) 1) ва 2) пунктларда топилган эллиптик эгри чизиқнинг иккита нуқтаси қўшилади.

Протокол тугалланишида **A** ва **B** иштирокчилар анъанавий шифрлаш тизимларида координаталари махфий калитнинг бинар кодини қурувчиси сифатида қўлланилиши мумкин бўлган эллиптик эгри чизиқнинг махфий W нуқтасига эга бўладилар.

2.4 Параметрли алгебрага асосланган калитларни тақсимлаш алгоритмларининг

Носимметрик криптографиянинг математик асоси бўлиб бирор алгебраик структура (АС) ва унда криптографик алгоритмга асос қилиб олинган яширин йўлли (махфийликка эга) бир томонлама функция хизмат қилади. АС деганда бирор тўплам ва алгебраик амаллар жуфтлиги тушунилади [9]. Криптографик алгоритмнинг ҳар хил ташқи ва ички ҳужумларга бардошлилиги АС бир томонлама функциясини тескарилаш мураккаблигига асосланади.

1985 йилдан бошлаб Н.Коблиц [10, 11] ва В.Миллер [12] таклиф этган носимметрик криптографиянинг традицияга айланиб қолган криптотизимларидан бардошлилиги ЭЭЧ группасида дискрет логарифмлаш муаммосининг мураккаблигига асосланган тизимларга ўтиш бошлангани кўзга ташланди. Эллиптик криптографияга алоҳида қизиқиш қуйидаги сабаблар [13] билан белгиланади:

- биринчидан, дискрет логарифмлаш ва факторлаш муаммоларини ечишга қаратилган сонли майдонларда *n* модули бўйича сонлар силлиқлиги хоссасидан фойдаланадиган умумлашган ғалвир усулига асосланган тезкор алгоритмларнинг юзага келиши. ЭЭЧ группасида эса силлиқлик тушунчаси аниқланмаганлиги уларда тезкор криптотаҳлиллаш алгоритмларини тузиш имкониятини бермайди, бу ерда силлиқ сон унча катта бўлмаган туб сонлар кўпайтмаси;
- иккинчидан, ЭЭЧ группасида калит узунлиги бўйича криптотизимлар ишлаб чиқариш афзалликларга эга эканлиги. Булар симсиз коммуникацияларда ва ресурс чекланган ҳолларда (смарт-карталар, мобиль қурилмалар) асосий ҳисобланади. Масалан, ЭЭЧ группасида тузилган калитнинг бинар узунлиги *150* дан *350* гача бўлган қурилмаларда анъанавий қурилмалардаги калитнинг бинар узунлиги *600* дан *1400* гача бўлгандагидек криптографик бардошлилик даражасига эришилади.

Юқорида келтирилган сабаблар АҚШ ва Россия Федерациясида амалдаги стандартларни эллиптик криптографияга оид стандартлар билан алмаштиришга олиб келди. Ҳозирги кунда ЭЭЧларга асосланган алгоритмлар кўплаб халқаро, миллий ва соҳага оид стандартлар қаторидан ўрин олган.

Эллиптик криптографияда туб майдон *GF(p)*да берилган ЭЭЧдан кенг фойдаланилади. *GF(p)*да берилган ЭЭЧ тенгламаси $y_0^2 \equiv x_0^3+ax_0+b \ (mod\ p)$ кўринишга эга.

Фан-техника ва маркетинг тадқиқотлари маркази («UNICON. UZ».ДУК) нинг «Ахборот хавфсизлиги ва криптология» илмий-тадқиқот департаментида диаматрицалар алгебрасини криптология масалалари учун такомиллаштириш натижасида 1999 йилда диамарицавий устунлар АС ва параметрли АС юзага келди [9]. Натижада аввал маълум бўлган махфийликка қўшимча махфийлик киритиш орқали ҳужумларга бардошлиликни янада ошириш мақсадида ундан янгича фойдаланиш имконияти туғилди. Шундан буён такомиллашган диаматрицавий ва параметрли алгебралар ҳамда параметрли ЭЭЧ группаси ахборотни ҳимоялаш воситаларини ишлаб чиқиш ва криптотаҳлил жараёнларини амалга оширишда математик база сифатида фойдаланилмоқда.

Параметрли АС

Элементлари бир хил *a* ва *b* лардан таркиб топган *m* x *1* тартибли диаматрицавий устунлар *A* ва *B* дан битта элементли *a* ва *b* лардан таркиб топган *1* x *1* тартибли устунларга ўтилса, параметрли кўпайтириш амали қуйидаги кўринишда ифодаланиб

$$a®b \equiv a + b + aRb \ (mod\ n) \qquad (1)$$

формула асосида аниқланади.

Параметрли тескари элемент қуйидагича ҳисобланади:

$$a^{\backslash -1} \equiv -a(1+ aR)^{-1} \ (mod\ n). \qquad (2)$$

Бу ерда $^{\backslash -1}$ - *n* модуль бўйича параметрли тескарилаш, $^{-1}$ - *n* модуль бўйича тескарилаш амалининг рамзи.

Оқибатда параметрли АС (*GF(n); ®)* кўринишига эга бўлади; бу ерда *GF(n)* – *n* тартибли бутун сонлар чекли тўплами, ® - *GF(n)* элементлари устида параметрли кўпайтириш амалининг рамзи.

Параметр муаммоси

Параметр муаммоси тўртта мураккаблик поғонаси билан фарқланади:

Агар параметрли АС *(GF(n); ®)* да ташувчи *GF(n)*нинг

- элементи $y \equiv a^{\backslash x} (mod\ n)$ берилган бўлса, унда параметр *R,* даража кўрсаткичи *x* ва элемент *a* топилсин, *(3*-поғона*),*
- элементлар *y* ва *a* берилган бўлса, унда параметр *R* ва даража кўрсаткичи *x* топилсин *(2*-поғона*),*
- элементлар *y* ва даража кўрсаткичи *x* берилган бўлса, унда параметр *R* ва элемент *a* топилсин, *(1*-поғона*),*
- элементлар *y, a* ва даража кўрсаткичи *x* берилган бўлса, унда параметр *R* топилсин, бу ерда $R > a+2^{160}$, *(0*-поғона*).*

Бу ерда *GF(n)– n* та бутун сонлардан тузилган чекли тўплам.

Мазкур муаммонинг юзага чиқиши бир томонлама параметрли функциянинг қуйидаги хоссаси билан боғлиқ:

$a^{\backslash x} \equiv a\Sigma_{i=0}^{i=x-1} F^i\ (mod\ n)$, бу ерда $F=1+Ra.$ (3)

Мазкур муаммо параметрли ЭЭЧ группасида хам ўхшаш талқинга эга. Унда элемент ўрнида нуқтанинг *x-, y-* координаталари жуфтлиги қатнашади.

2.4.1. Параметрли Диффи-Хеллман калит алмашиш алгоритми

Фараз қилайлик, *j*-томон параметрли алгебра асосида такомиллаштирилган Диффи-Хеллман калит алмашиш алгоритми асосида ишлайдиган тизимга, *i*-томон эса мавжуд Диффи-Хеллман калит алмашиш алгоритми асосида ишлайдиган тизимга эга.

Махфий калит алмашиш жараёни *(p, a)* жуфтлик маълум саналиб, қуйидаги қадамларни ўз ичига олади:

1-қадам: *i*-томон, ўз махфий калити e_i ни тасодифий сон сифатида танлаб, ўз ошкора калити

$y_i \equiv a\ e_i\ (mod\ p)$ ни ҳисоблайди ва уни умумий маълумотлар базасига ёки *j*-томонга жўнатади;

2-қадам: *j*-томон, ўз махфий калити d_j ни тасодифий сон сифатида танлаб, ўз ошкора калити

$y_j \equiv (a\text{-}1)^{\backslash dj}+1(mod\ p)$ ни ҳисоблайди ва уни умумий маълумотлар базасига ёки *i*-томонга жўнатади. Бу ерда параметр $R = 1$;

3-қадам: *j*-томон *i*-томоннинг ошкора калитини қабул қилиб,

$k_j \equiv (y_i\text{-}1)^{\backslash dj} + 1(mod\ p)$ ни ҳисоблайди;

4-қадам: *i*-томон *j*-томоннинг ошкора калитини қабул қилиб,

$k_i \equiv y_j\ e_i\ (mod\ p)$ ни ҳисоблайди, бу ерда *i*-, *j*-томонларнинг умумий махфий калити $k=k_i= k_j$.

Параметрли Диффи-Хеллман калит алмашиш алгоритмига оид мисол қуйидаги 6-жадвалда келтирилган:

6-жадвал

p	a	R	e_i	d_j	y_i	y_j	k_j	k_i
17	5	1	11	13	11	3	7	7

Модуль *p* фойдаланувчилар гуруҳи учун умумий, асос *a* эса фойдаланувчилар гуруҳи учун бир хил ёки фойдаланувчилар жуфтлари учун ҳар хил бўлиши мумкин.

Параметр *R=1* бўлганда, худди шундай услубда бошқа ишлаб чиқилган алгоритмларни ҳам мавжуд алгоритмлар билан гармонизациялаш мумкин.

Бунда жорий криптотизимларнинг бардошлилиги иккала томон учун ҳам, бошқа томонлар учун ҳам бир хил бўлади. Агар, параметр $R>>1$ олинса ва бу параметр ёпиқ калит вазифасини бажарса, унда жорий криптотизимларнинг бардошлилигини оширишга эришилади.

2.4.2. Параметрли эллиптик эгри чизиққа асосланган Диффи-Хеллман калит алмашиш алгоритми

Параметрли эллиптик эгри чизиқли Диффи-Хеллман калит алмашиш алгоритми эллиптик эгри чизиқли Диффи-Хеллман алгоритмига нисбатан криптобардошлиги юқори ҳисобланади. Эллиптик эгри чизиқли алгебрадан параметрли алгебрага ўтиш қуйидагича амалга оширилади:

ЭЭЧ тенгламасидан параметрли ЭЭЧ (ПЭЭЧ) тенгламасига ўтиш.

Хосса. Агар $y^{\backslash 2} \equiv x^{\backslash 3}+ax+B \pmod p$ ва $y_0^{\ 2} \equiv x_0^{\ 3}+ax_0+b \pmod p$ лар ўзаро изоморф бўлса, у ҳолда

- $B \equiv (a+b)\, R^{-1} \pmod p$,
- $y \equiv (y_0-1)\, R^{-1} \pmod p \equiv (x^{\backslash 3}+ax+B)^{\backslash 0.5} \pmod p$,
- $y - \equiv -(y_0+1)\, R^{-1} \pmod p \equiv -(y+2R^{-1}) \pmod p$,
- $y^{\backslash 2} \equiv (y_0^{\ 2}-1)\, R^{-1} \pmod p$,
- $x \equiv (x_0-1)\, R^{-1} \pmod p$,
- $x^{\backslash 3} \equiv (x_0^{\ 3}-1)\, R^{-1} \pmod p$.

Параметрли ЭЭЧ нуқтасининг чекли аддитив группа элементига мослиги.

Хосса. Агар $y^{\backslash 2} \equiv x^{\backslash 3}+ax+B \pmod p$ *ПЭЭЧ* таққосламаси бўлиб, $Y=(x,y)=d^{*\backslash}G$ нуқта шу таққосламани қаноатлантирса, у ҳолда *ПЭЭЧ* нуқтаси x-, y- координаталарига чекли q тартибли аддитив группа $(GF(p);"+")$ нинг элементлари $x= d*g_1 \pmod q$, $y = d* g_2 \pmod q$ ўзаро мос келади, бу ерда "$*^{\backslash}$" - параметрли кўпайтириш, "+" - қўшиш, "*" - кўпайтириш амаллари рамзлари, $G=(g_1, g_2)$.

ПЭЭЧ нуқтасининг чекли q тартибли аддитив группа элементига мослиги хоссасидан фойдаланиш *ЭЭЧ*ларда дискрет логарифмлаш масаласини чекли аддитив группанинг базис элементини топиш асосида ҳал этишга йўл очади.

a, B - бутун сонли коэффициентлар,

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

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

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

$$x_3 \equiv (L^2-3)R^{-1}-x_1- x_2) \pmod p, \quad (4)$$

$$y_3 \equiv L(x_1- x_3)+ y_1^- \pmod p, \quad (4')$$

бу ерда:

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

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

$$x_3 \equiv (L^2-3)R^{-1}-2x_1 \pmod p, \quad (5)$$

$$y_3 \equiv L(x_1- x_3) + y_1^- \pmod p, \quad (5')$$

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

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

Ноллик нуқта учун $Q+\backslash 0_E = 0_E +\backslash Q = Q$ (6)

тенглик ўринлидир.

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

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

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

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

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

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

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

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

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

Бу ерда:

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

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

a, B – бутун сонли коэффициентлар,

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

q – параметрли ЭЭЧ нуқталари тартиби,

p – туб сон.

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

Параметрли ЭЭЧ функцияси хоссалари анъанавий ЭЭЧ функцияси хоссаларига ўхшаш бўлиб, параметрли ЭЭЧ функцияси қийматини исталган скаляр сон учун самарали ҳисоблаш учун етарлидир. Бу ерда, катта скаляр сонга параметрли кўпайтириш жараёни экспоненциал функцияни ҳисоблаш жараёни каби кечиб, d ни 2 нинг даражалари йиғиндиси сифатида ифодалашга ва даврий тарзда йиғиндини ташкил этувчи 2 нинг даража кўрсаткичи, агар жуфт қийматли бўлса, 2 га параметрли кўпайтириш, акс ҳолда жорий қийматни берилган нуқтага параметрли кўпайтириш амалларидан фойдаланишдан иборат бўлади. Бу хоссалар анъанавий ЭЭЧ функцияси хоссаларидан фойдаланишга асосланган криптографик тизимларга ўхшаш криптотизимлар яратишга имкон беради.

3-БОБ. АССИММЕТРИК АЛГОРИТМЛАРГА АСОСЛАНГАН КАЛИТЛАРНИ ТАҚСИМЛАШ АЛГОРИТМЛАРИНИНГ ТАҲЛИЛ ВА ТАДҚИҚИ.

3.1 Диффи-Хеллман алгоритми

У. Диффи ва М. Хеллман тарихда биринчи очиқ калитли алгоритм бўлиб, у 1976 йилда ишлаб чиқилган. Унинг хавфсизлиги (криптобардошлиги) чекли майдонда дискрет логарифмлаш муаммоларини ечиш қийинлигига асосланган.

Диффи-Хеллман алгоритмидан **A** иштирокчи ва **B** иштирокчи ўртасида калитларни тақсимлаш алгоритми сифатида калитни генерация қилишда ишлатилиши мумкин, аммо маълумотларни шифрлаш ва дешифрлашда ишлатиб бўлмайди.

Диффи-Хеллман алгоритмининг математикаси содда. Аввал **A** иштирокчи ва **B** иштирокчи биргаликда катта туб n ва g сонларни танлашади. Бу икки туб сон махфий сақланиши шарт эмас, **A** ва **B** иштирокчилар очиқ махфий булмаган канал орқали келишиб олиши мумкин. Бу сонлар ҳатто фойдаланувчилар гуруҳида биргаликда ҳам (барча фойдаланувчилар учун умумий) ишлатилиши мумкин.

Кейин қуйидаги протокол амалга оширилади (7-расм):

1. **A** иштирокчи ихтиёрий катта туб сон x ни танлайди ва **B** иштирокчига жўнатади:

$$X = g^x \bmod n.$$

2. **B** иштирокчи ҳам ихтиёрий катта туб сон y ни танлайди ва **A** иштирокчига жўнатади:

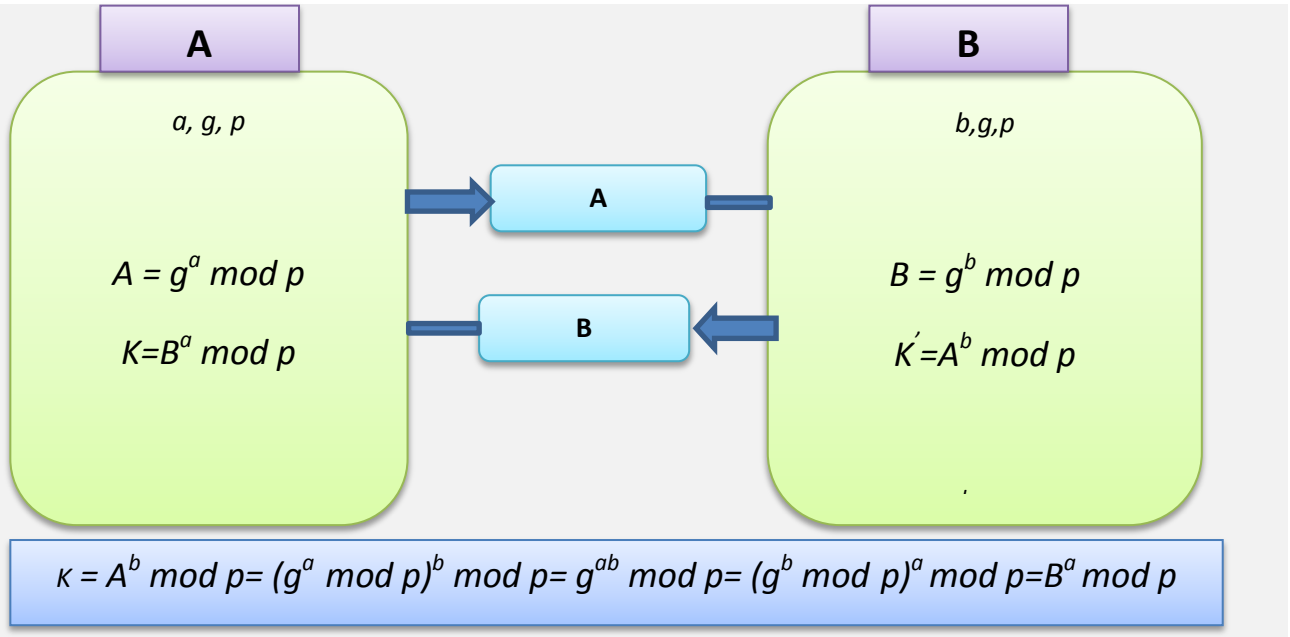
$$Y = g^y \bmod n$$

3. **A** иштирокчи қуйидагини ҳисоблайди:

$$k = Y^x \bmod n = g^{xy} \bmod n.$$

4. **B** иштирокчи эса қуйидагини ҳисоблайди:

$k' = X^y \bmod n = g^{xy} \bmod n.$



7-расм. Диффи-Хеллман алгоритми

Бу ерда *k* ва *k'* тенг *(k=k')*. Ҳеч қандай ўртада кузатиб турган учинчи киши бу қийматни ҳисоблаб топа олмайди, чунки унга фақат *n, g, X* ва *Y* лар маълум. Қачонки улар дискрет логарифм муммосини ечиб *x* ва *y* ларни топа олмас эканлар, улар бу муаммони ҳам ҳал эта олмайдилар. Чунки бу ерда *k* – махфий калитни **A** иштирокчи ва **B** иштирокчи бир-биридан мустақил равишда ҳисоблайди. *n* ва *g* ни танлаш ҳам тизим хавфсизлигига катта таъсир кўрсатади. *(n-1)/2* сони ҳам туб сон бўлиши керак. Ва энг муҳими *n* жуда катта туб сон бўлиши керак, чунки тизим хавфсизлиги шу ўлчамдаги сонларни туб кўпайтувчиларга ажратиш муаммосига асосланган. *g* учун ҳар қандай сон олиниши мумкин, чунки *g* барча ҳолларда модуль (*mod n)* бўйича ҳисобланади. (Аслини олганда *g* ҳам кичкина бўлмаслиги керак, унинг ҳам етарли даражада катта сон бўлиши хавфсизликни таъминлаб беришда муҳим аҳамиятга эга).

3.2. Уч ва ундан ортиқ фойдаланувчилар иштирокидаги Диффи-Хеллман алгоритми

Диффи-Хеллман калитларни тақсимлаш протоколини осонгина уч ва ундан ортиқ иштирокчилар учун кенгайтириш мумкин. Масалан, **A** иштирокчи, **B** иштирокчи ва **C** иштирокчи биргаликда махфий калитларни генерация қиляпти.

1. **A** иштирокчи ихтиёрий катта сон x ни танлайди ва қуйидагини ҳисоблайди:

$X = g^x \bmod n.$

2. **B** иштирокчи ихтиёрий катта сон y ни танлайди ва қуйидагини ҳисоблайди:

$Y = g^y \bmod n,$

ва уни **C** иштирокчига жўнатади.

3. **C** иштирокчи ихтиёрий катта сон z ни танлайди ва қуйидагини ҳисоблайди:

$Z = g^z \bmod n,$

ва уни **A** иштирокчига жўнатади.

4. **A** иштирокчи **B** иштирокчига жўнатади:

$Z' = Z^x \bmod n.$

5. **B** иштирокчи **C** иштирокчига жўнатади:

$X' = X^y \bmod n.$

6. **C** иштирокчи **A** иштирокчига жўнатади:

$Y' = Y^z \bmod n.$

7. **A** иштирокчи қуйидагини ҳисоблайди:

$k = Y'^x \bmod n.$

8. **B** иштирокчи қуйидагини ҳисоблайди:

$k = Z'^y \bmod n.$

9. **C** иштирокчи қуйидагини ҳисоблайди:

$k = X'^z \bmod n.$

Махфий калит $k=X^z \ mod \ n$ га тенг бўлади ва ҳеч қандай ўртадаги кишилар бу қийматни ҳисоблай олмайдилар. Протоколни тўрт ва ундан ортиқ қатнашувчилар учун осон кенгайтирш мумкин, фақат фойдаланувчилар ва ҳисоблаш босқичлари ошади.

3.3. Hughes алгоритми

Hughes алгоритми Диффи-Хеллман алгоритмининг ўзгартирилган варианти ҳисобланади. Hughes алгоритми қуйидаги тартибда амалга оширилади (8-расм):

1. **A** иштирокчи катта туб сон x ни генерация қилади ва қуйидагини ҳисоблайди:

$k = g^x \ mod \ n.$

2. **B** иштирокчи катта туб сон y ни генерация қилади ва қуйидагини ҳисоблаб уни **A** иштирокчига жўнатади:

$Y = g^y \ mod \ n.$

3. **A** иштирокчи **B** иштирокчига қуйидагини жўнатади:

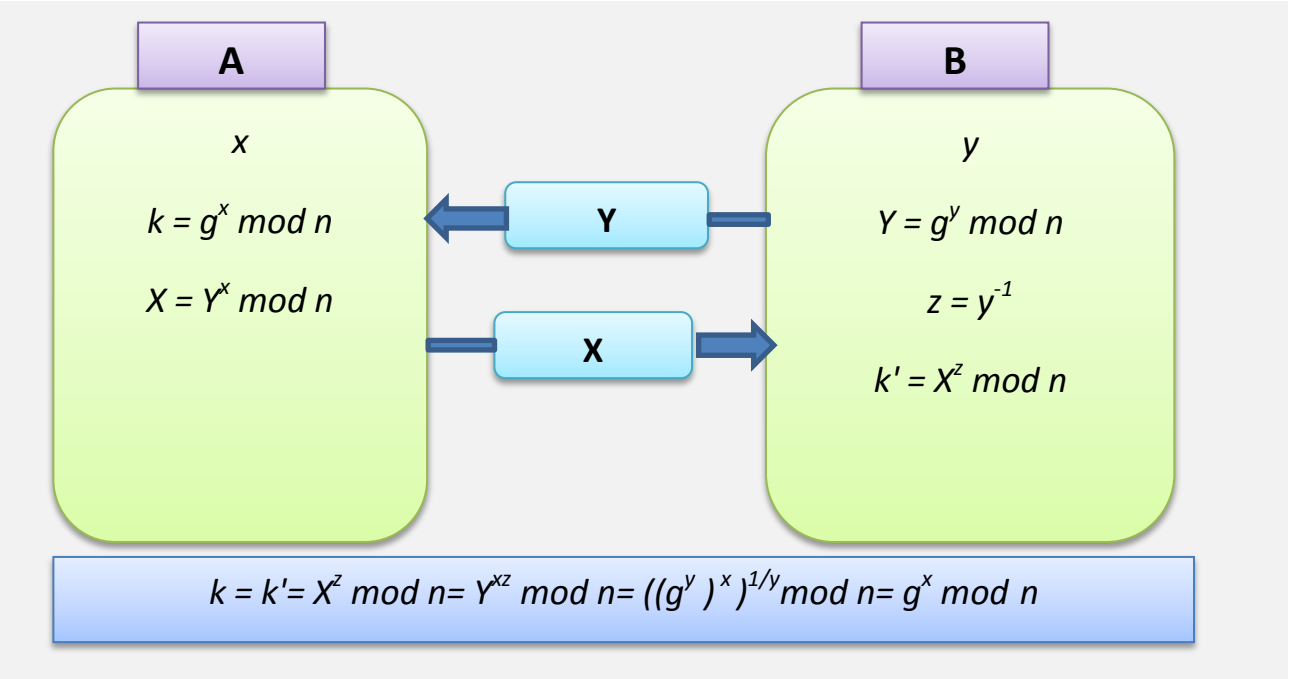
$X = Y^x \ mod \ n.$

4. **B** иштирокчи қуйидагини ҳисоблайди:

$z = y^{-1},$

$k' = X^z \ mod \ n.$

Агар ҳаммаси тўғри бажарилган бўлса, $k = k'$ бўлади.



8-расм. Hughes алгоритми

Hughes протоколининг Диффи-Хеллман протоколидан афзаллиги, *k* махфий сеанс калитини боғланиш бўлмасдан аввал ҳисоблаб қўйиш мумкин ва бу калит орқали **A** иштирокчи маълумотларни шифрлаб қўйиши мумкин бўлади, яъни **B** иштирокчи билан боғланмасдан туриб амалга ошириши мумкин.

У шифрланган маълумотни бир вақтнинг ўзида бир неча кишига жўнатиши мумкин, калитни эса кейинроқ ҳар бирига алоҳида-алоҳида жўнатиши мумкин.

3.4. MTI протоколи

MTI протоколининг номи унинг муаллифлари ҳисобланган *Т. Мацумото И. Такашима ва Х. Имаи*лар шарафига қўйилган. Бу протокол ҳам Диффи-Хеллман протоколига ўхшаш бўлиб, унинг криптобардошлилиги чекли майдонда дискрет логарифмлашга асосланган [14, 20]. Бироқ ундан

фарқли томони шундаки, MTI протоколида криптобардошлилигини ошириш мақсадида қўшимча a ва b ўзгарувчилардан фойдаланилади. Ушбу протоколнинг амаллар кетма-кетлиги қуйидагича бажарилади (9-расм). Энг аввало **A** ва **B** иштирокчилар катта туб сон p ва унинг примитив илдизи α нинг қиймати ҳақида келишиб оладилар.

A иштирокчи ўз махфий калити a, $1 \le a \le p-2$ ни генерация қилади ва бу калит ёрдамида

$$z_A = \alpha^a \bmod p$$

ифодани ҳисоблайди. **A** иштирокчи ҳосил бўлган қийматни **B** иштирокчига узатади:

$$\mathbf{A} \to \mathbf{B}: z_A = \alpha^a \bmod p,$$

B иштирокчи бу маълумотни қабул қилади. У ўзининг ёпиқ калити b, $1 \le b \le p-2$ ни генерация қилади. Бу ёпиқ калит ёрдамида

$$z_B = \alpha^b \bmod p$$

ифодани ҳисоблайди ва натижани **A** иштирокчига узатади:

$$\mathbf{B} \to \mathbf{A}: z_B = \alpha^b \bmod p.$$

A иштирокчи z_B ни қабул қилади. **A** ва **B** иштирокчилар умумий махфий калитни генерация қилиш учун мос ҳолда ўзларининг x, $1 \le x \le p-2$ ва y, $1 \le y \le p-2$ тасодифий сонларини генерация қилишлари зарур. **A** иштирокчи ўзининг тасодифий x сонини генерация қилиб,

$$\alpha^x \bmod p$$

ифодани ҳисоблайди ва уни **B** иштирокчига узатади:

$$\mathbf{A} \to \mathbf{B}: \alpha^x \bmod p.$$

B иштирокчи бу маълумотни қабул қилади. У ўзининг тасодифий y сонини генерация қилиб, $\alpha^y \bmod p$ ифодани ҳисоблайди. Ҳосил бўлган натижани **A** иштирокчига узатади. Шу вақтдан бошлаб, **B** иштирокчи α^x ва

z_A маълумотларга эга. Энди у ўзининг тасодифий сони ва ёпиқ калитидан фойдаланиб қуйидаги ифодани ҳисоблайди:

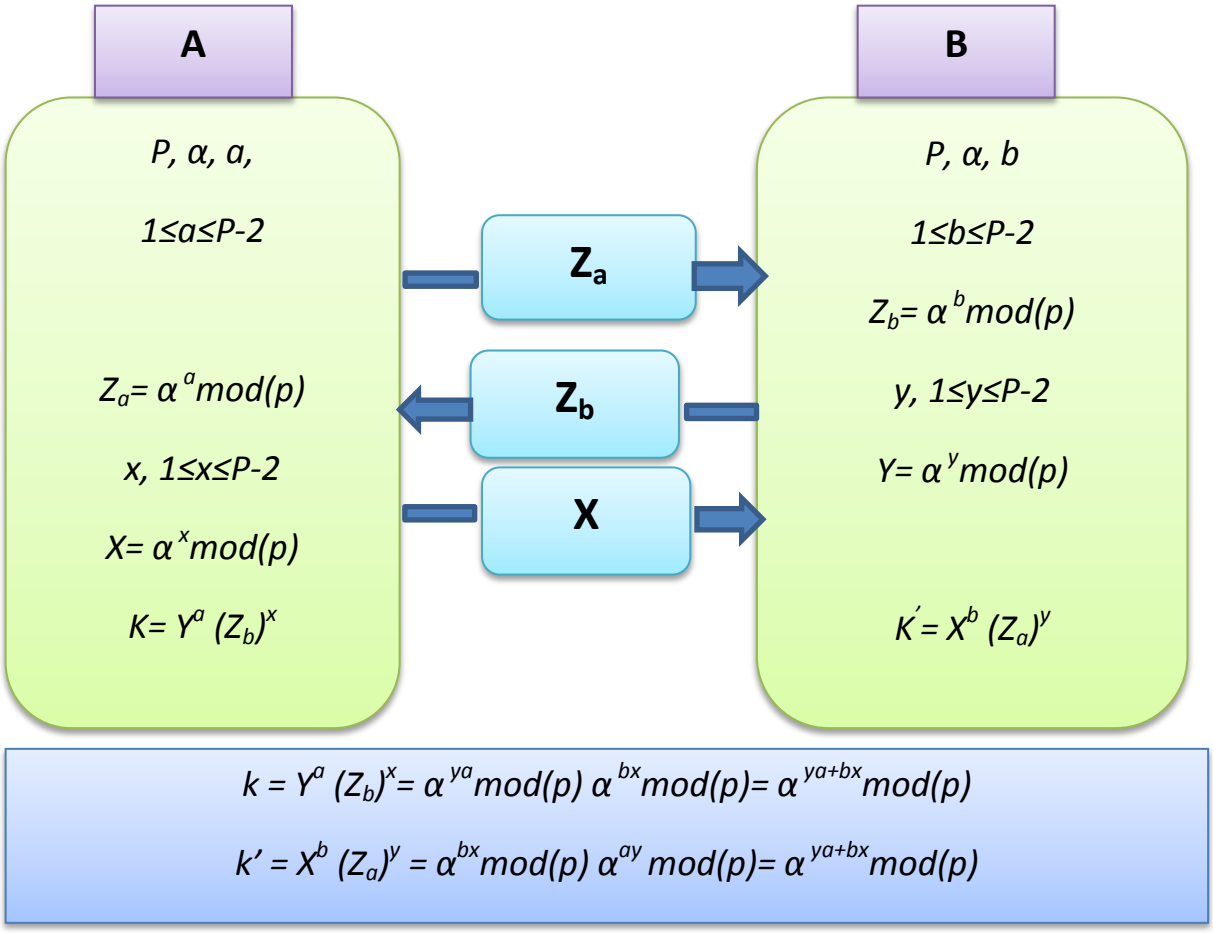
$$k = (\alpha^x)^b \cdot z_A^y ,$$

$$\mathbf{B \rightarrow A:}\ \alpha^y \bmod p .$$

A иштирокчи бу маълумотни қабул қилади. Энди **A** иштирокчи α^y ва z_B маълумотларга эга. У ўзининг тасодифий сони ва ёпиқ калитидан фойдаланиб ушбу ифодани ҳисоблайди: $k = (\alpha^y)^a \cdot z_B^x$.

Натижавий калитнинг умумий кўриниши эса қуйидагича:

$$k = (\alpha^y)^a \cdot z_B^x = (\alpha^x)^b \cdot z_A^y = \alpha^{xb+ya} \bmod p .$$



9-расм. MTI протоколи

MTI протоколи шу тартибда амалга оширилади. Унда криптотаҳлилчининг ихтиёрий алмаштириши томонлардаги калитнинг қиймати турлича бўлишига олиб келади. Бу эса узатилаётган маълумотни ўқиш имкониятини бутунлай йўқотади.9-расм. MTI протоколи

Қуйида MTI пртоколи учун ҳам мисол келтирилади.

$p = 9531$

$\alpha = 1647$

$A: a = 126$

$A: Z_a = \alpha^a \bmod p = 1647^{126} \bmod 9531 = 3375$

$A \to B: Z_a = 3375$

$B: b = 98$

$B: Z_B = \alpha^b \bmod p = 1647^{98} \bmod 9531 = 8775$

$B \to A: Z_B = 8775$

$A: x = 8643$

$A: X = \alpha^x \bmod p = 1647^{8643} \bmod 9531 = 972$

$A \to B: X = 972$

$B: k_1 = (\alpha^x)^b Z_A^y \bmod p = X^b Z_A^y \bmod p = 972^{98} \cdot 3375^{6983} \bmod 9531 = 3564$

$B: y = 6983$

$B: Y = \alpha^y \bmod p = 1647^{6983} \bmod 9531 = 4131$

$B \to A: Y = 4131$

жавоб: $k_1 = k_2 = k = 3564$.

3.5. DASS протоколи

DASS протоколи калит тақсимоти ва аутентификациясининг ИМ иштирокидаги симметрик ва носимметрик алгоритмларга асосланган протоколдир [10-12]. Бунда **A** ва **B** иштирокчилар ҳамда ИМ S ўзларининг очиқ ва ёпиқ калитлари жуфтига эгалар, яъни k_a, k_b, k_s ўзаро мос ҳолатда. Бу калитлар билан мос равишда хабарларни имзолаш s_a, s_b, s_S.

DASS протоколи схемасини қуйидаги келтирилади (10-расм):

$A \to S : B,$

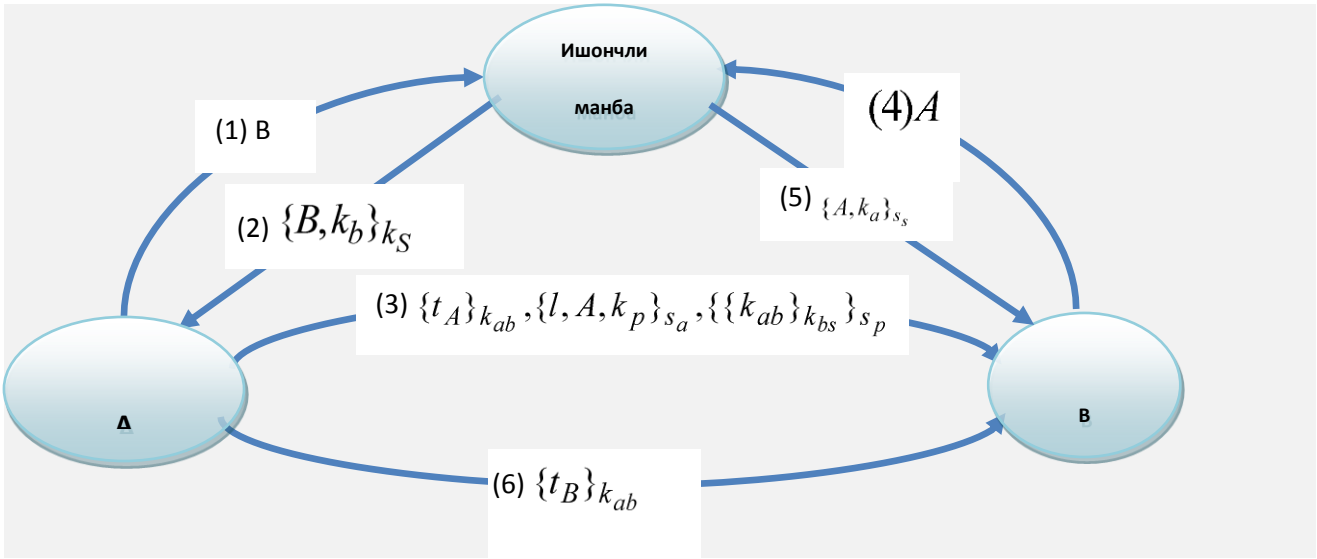
$S \to A : \{B, k_b\}_{k_s},$

$A \to B : \{t_A\}_{k_{ab}}, \{l, A, k_p\}_{s_a}, \{\{k_{ab}\}_{k_{bs}}\}_{s_p},$

$B \to S : A,$

$S \to B : \{A, k_a\}_{s_s},$

$B \to A : \{t_B\}_{k_{ab}}.$



10-расм. DASS протоколи

DASS протоколининг тўлиқ баёни қуйида келтирилади:

– **A** иштирокчи ИМга **B** иштирокчининг очиқ калитини олиш учун сўровнома юборади.

– ИМ **B** иштирокчининг калити k_b ни ўзининг калити билан имзолаб узатади.

– **A** иштирокчи маълумотларни ИМнинг аввалдан маълум бўлган очиқ калити билан текширади, сўнгра сеанс калити k_{ab} ни ва тасодифий сеанс катити k_p ни генерация қилади, ВБ t_a ни ва калитнинг яроқлилик муддатини қўшиб, бир қисмини шифрлаб, бир қисмини имзолаб **B** иштирокчига юборади.

– **B** иштирокчи ИМга **A** иштирокчининг идентификаторини олиш учун сўровнома юборади.

– ИМ **B** иштирокчининг калитини ўзининг калити билан имзолаб юборади.

– **A** иштирокчининг ва ИМнинг хабарларидаги маълумотлардан фойдаланиб, **B** иштирокчи **A** иштирокчининг имзосини текширади, тасодифий сеанс калити k_p ни, сеанс калити k_{ab} ни чиқариб олади ва t_A нинг шифрини очиб такрорланганидан эмас, балки шу вақтдаги хабардан фойдаланилаётганига ишонч ҳосил қилади.

– Заруратга кўра протокол томонларни ўзаро идентификациясини таъминлаш мақсадида давом эттирилиши мумкин.

3.6. Деннинг – Сакко протоколи

Деннинг–Сакко *(Denning-Sacco)* протоколи ошкора калитли аутентификациялаш ва калит тақсимлаш протоколи бўлиб, DASS протоколидаги каби ИМ барча очиқ калитларнинг маълумотлар базасини тутиб туради [3-6, 17].

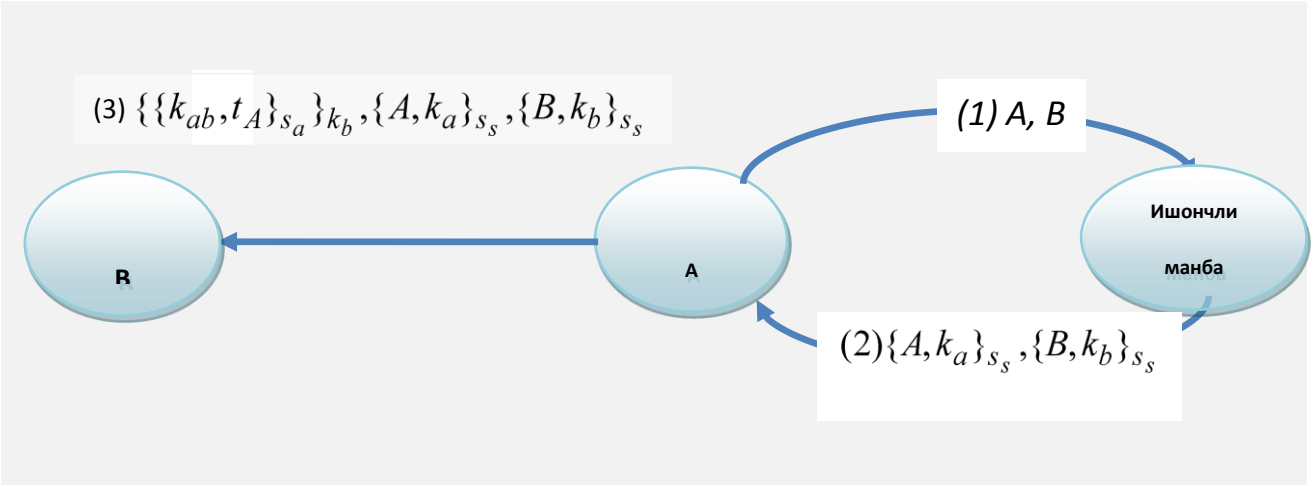
Деннинг–Сакко протоколининг заифлиги шундан иборатки, томонлардан бири сеанс тугагандан сўнг ўзини бошқа томондан деб кўрсатиш имкониятига эга.

Деннинг– Сакко протоколининг схемаси (11-расм) :

$$A \rightarrow S : A, B,$$

$$S \rightarrow A : \{A, k_a\}_{s_s}, \{B, k_b\}_{s_s},$$

$$A \rightarrow B : \{\{k_{ab}, t_A\}_{s_a}\}_{k_b}, \{A, k_a\}_{s_s}, \{B, k_b\}_{s_s},$$



11-расм. Деннинг – Сакко протоколи

– **A** иштирокчи ИМга ўзининг ва **B** иштирокчининг идентификаторини юборади.

– ИМ **A** иштирокчига ўзининг махфий калити билан имзолаган **A** ва **B** иштирокчиларнинг очиқ калитларини ва идентификаторларини узатади.

– **A** иштирокчи сеанс калити ва вақт белгисини ўзининг калити билан имзолаб, сўнгра уни **B** иштирокчининг очиқ калити билан шифрлаб ва ИМнинг хабари билан тўлдириб **B** иштирокчига юборади.

– **B** иштирокчи хабарни шифрини очиб, ИМнинг очиқ калитидан фойдаланиб калитлардаги имзони текширади, **A** иштирокчининг очиқ калитидан фойдаланиб сеанс калитидаги имзони текширади, бунда сеанс калити k_{ab} дан **A** иштирокчи билан хавфсиз маълумот алмашинувида фойдаланиши мумкин бўлади.

A иштирокчидан келган хабарда $\{\{k_{ab}, t_A\}_{s_a}\}_{k_b}$ олувчининг идентификатори қатнашмаслиги, **B** иштирокчига **A** иштирокчидан олган маълумотларни бошқа иштирокчи билан бўладиган янги сеансда ўзини

A иштирокчи деб кўрсатиши имконини беради. Бу муаммони хабарга **A** ва **B** иштирокчиларнинг идентификаторини қўшиб, яъни бу хабарни ишлатилишини фақат шу сеанс билан чегаралаб осон ҳал қилиш мумкин.

3.7. Ву – Лама протоколи

Ву – Лама *(Woo-Lam)* протоколи ҳам Деннинг – Сакко протоколи каби ошкора калитли аутентификациялаш ва калит тақсимлаш протоколи бўлиб [3-6, 17], DASS протоколидаги каби ИМ барча очиқ калитларнинг маълумотлар базасини тутиб туради.

Ву – Лама протоколи схемаси 12-расмда келтирилган:

$$A \rightarrow S : A, B,$$

$$S \rightarrow A : \{k_b\}_{s_s},$$

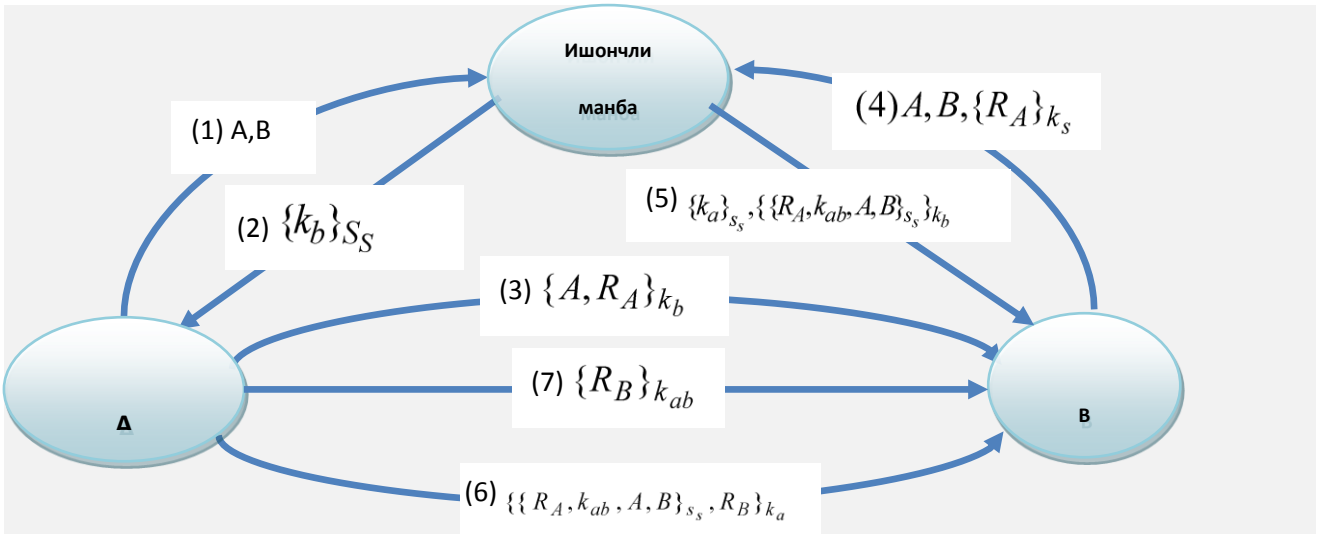
$$A \rightarrow B : \{A, R_A\}_{k_b},$$

$$B \rightarrow S : A, B, \{R_A\}_{k_s},$$

$$S \rightarrow B : \{k_a\}_{s_s}, \{\{R_A, k_{ab}, A, B\}_{s_s}\}_{k_b},$$

$$B \rightarrow A : \{\{R_A, k_{ab}, A, B\}_{s_s}, R_B\}_{k_a},$$

$$A \rightarrow B : \{R_B\}_{k_{ab}}.$$



12-расм. Ву – Лама протоколи

Энди Ву – Лама протоколининг тўлиқ баёнини келтирамиз:

– **A** иштирокчи ИМга ўзининг ва **B** иштирокчининг идентификаторини юборади.

– ИМ **A** иштирокчига ўзининг махфий калити билан имзолаган B иштирокчининг очиқ калитларини узатади.

– **A** иштирокчи имзони текширади, сўнгра **B** иштирокчига ўзининг идентификатори ва тасодифий танланган сонни **B** иштирокчининг очиқ калити билан шифрлаб юборади.

– **B** иштирокчи эса ИМга ўзининг ва **A** иштирокчининг идентификаторини ва тасодифий танлаган сонни ИМнинг очиқ калити билан шифрлаб узатади.

– ИМ **B** иштирокчига иккита хабар юборади. Биринчисида **A** иштирокчининг ИМнинг калити ёрдамида имзоланган очиқ калити бўлса, иккинчисида ИМ калити билан имзоланган ва **B** иштирокчининг очиқ калити билан шифрланган **A** иштирокчининг тасодифий танлаган сони, тасодифий танланган сеанс калити ва **A** ва **B** иштирокчиларнинг идентификатори бўлади.

– **B** иштирокчи ИМ очиқ калити ёрдамида хабарнинг ҳақиқийлигини текширади, сўнгра **A** иштирокчига ИМ хабарининг иккинчи қисмини, унинг имзоси билан, ўзининг тасодифий танлаган сони билан тўлдириб **A** иштирокчининг очиқ калити билан шифрлаб юборади.

– **A** иштирокчи ИМ имзосини ва ўзининг тасодифий танлаган сонининг тенглигини текширади, сўнгра **B** иштирокчига **B** тасодифий танлаган сонни унинг сеанс калити билан шифрлаб қайта юборади.

– **B** иштирокчи соннинг шифрини очиб унинг ўзгармаганлигига ишонч ҳосил қилади.

Носимметрик алгоритмларга асосланган калитларни тақсимлаш протоколларига юқорида келтирилган протоколлардан ташқари COMSET (Communications Setup, алоқа ўрнатиш), EKE (Encrypted Key Exchange, шифрланган калитлар билан алмашиш) протоколлари ва SKEY (маълумотнинг ҳақиқийлигини текширувчи) дастури мавжуд бўлиб улардан маълумотнинг хавфсизлигини таъминлаш учун фойдаланиш мумкин.

3.8 Ассимметрик калитларни тақсимлаш алгоритмларининг қиѐсий таҳлили ва криптобардошлилигининг таснифи

Калитларни тақсимлаш бўйича мавжуд хорижий алгоритмларнинг таҳлили шуни кўрсатдики, уларнинг бардошлилигини таъминлашга асос бўлган мураккаб муаммолар қуйидагилардан иборат:

- дискрет логарифм муаммосининг мураккаблигига асосланган;
- Диффи-Хеллман муаммосининг мураккаблигига асосланган;
- эллиптик эгри чизиқ (ЭЭЧ)да дискрет логарифм муаммосининг мураккаблигига асосланган;
- бошқа муаммоларга асосланган алгоритм ва протоколлардир.

Калитларни тақсимлаш бўйича мавжуд алгоритмлар ва протоколларнинг кўпчилиги дискрет логарифмлаш ва ЭЭЧда дискрет логарифмлаш муаммоларининг мураккаблигига асослангандир.

Охириги йилларда калитларни тақсимлаш алгоритмлари ЭЭЧларга асосланиб ишлаб чиқилмоқда. Шу боис, ЭЭЧда дискрет логарифмлаш муаммосиини ҳал этиш кўпчилик криптотаҳлилчиларнинг эътиборини ўзига тортмоқда.

Калитларни тақсимлаш протоколларига ҳужумлар турлича таъсир қилади. Қуйидаги 1-жадвалда носимметрик алгоритмларга асосланган

калитларни тақсимлаш протоколларига қилинадиган ҳужум турлари кўрсатилган.

1-жадвал

Ҳужумларнинг ассимметрик калитларни тақсимлаш протоколларига таъсири

№	Протокол номи	Ҳужум турлари
1	**Диффи- Хеллман протоколи**	“Ўртадаги киши ” ҳужумига бардошли эмас. Криптотаҳлилчи бу маълумотларни маълум вақтдан кейин **B** иштирокчига қайта жўнатиши мумкин
2	**Уч ва ундан ортиқ фойдаланувчилар иштирокидаги Диффи-Хеллман протоколи**	“Ўртадаги киши ” ҳужумига бардошли эмас.
3	**Hughes протоколи**	“Ўртадаги киши ” ҳужумига бардошли эмас
4	**MTI протоколи**	Криптотаҳлилчининг ихтиёрий алмаштириши томонлардаги калитнинг қиймати турлича бўлишига олиб келади.
5	**DASS протоколи**	**B** иштирокчи ЭРИни текшириш имконига эга бўлмайди Томонлар ўртасида ўзаро идентификация таъминланмайди
6	**Деннинг – Сакко протоколи**	Протокол якунлангандан сўнг **B** иштирокчи бошқа **C** иштирокчи билан алоқа ўрнатиши учун **A** иштирокчининг номидан иш кўриши мумкин

7	**By – Лама протоколи**	**A** иштирокчи арбитрни идентификация қилмайди Иштирокчилар бир-бирини идентификация қилмайдилар

Шундай қилиб, калитларни тақсимлаш протоколларидан фойдаланилаётганда протоколларга қилинаётган ҳужумларни албатта инобатга олиш талаб этилади.

Криптографик калитларни тақсимлаш алгоритми ва протоколларини қуйидаги белгилар асосида таснифлаш мумкин:

1. Калит тури.

2. Калитни тақсимлаш вазияти.

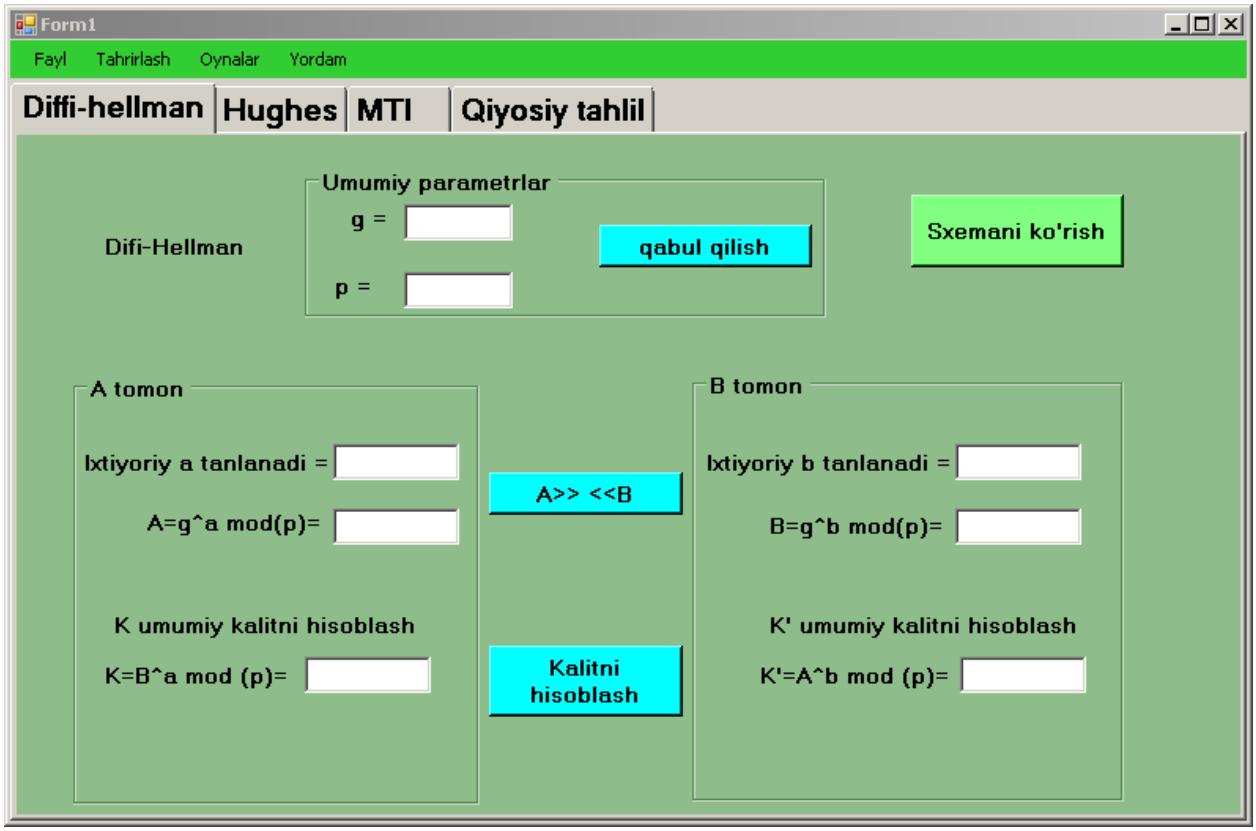
3. Калитларни тақсимлаш усули.

4. Калитларни тақсимлаш схемаси.

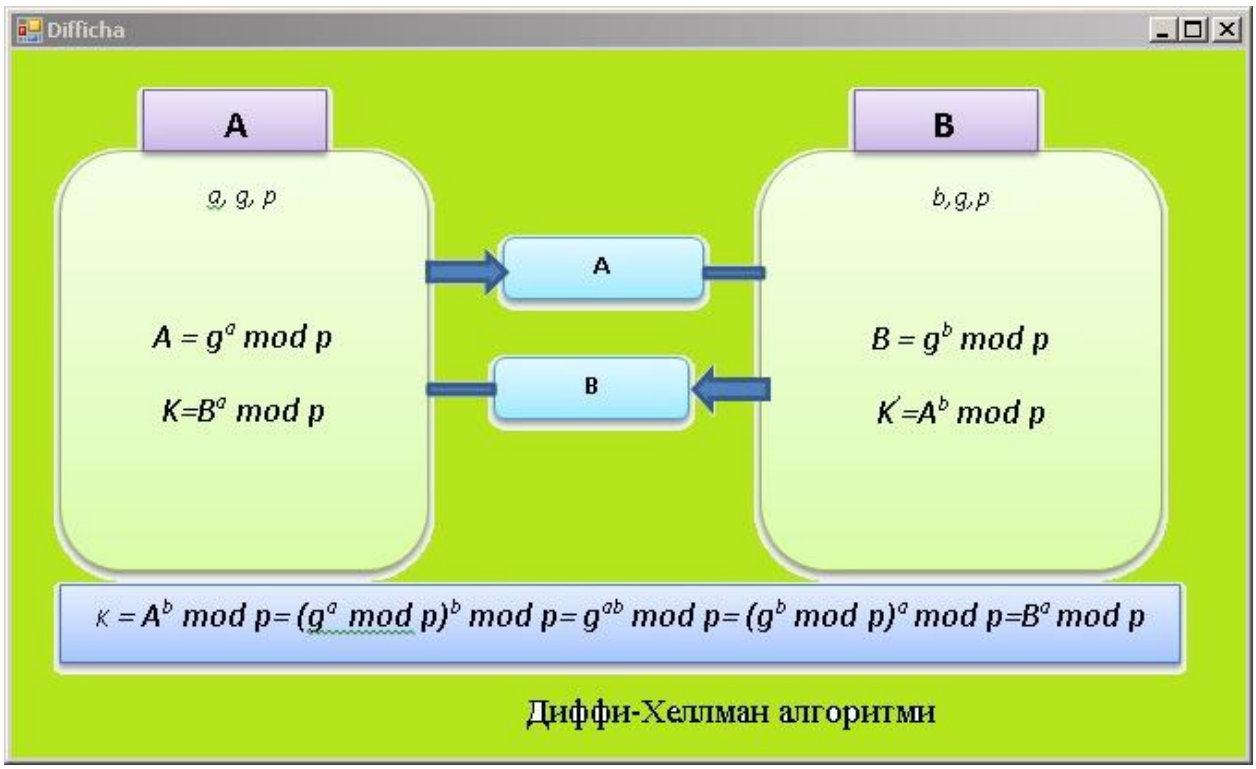
5. Калитларни тақсимлаш протоколи бардошлилигини таъминловчи муаммо тури.

3.9. Ассимметрик алгоритмларга асосланган калитларни тақсимлаш алгоритмларининг дастурий таъминотини ишлаб чиқиш

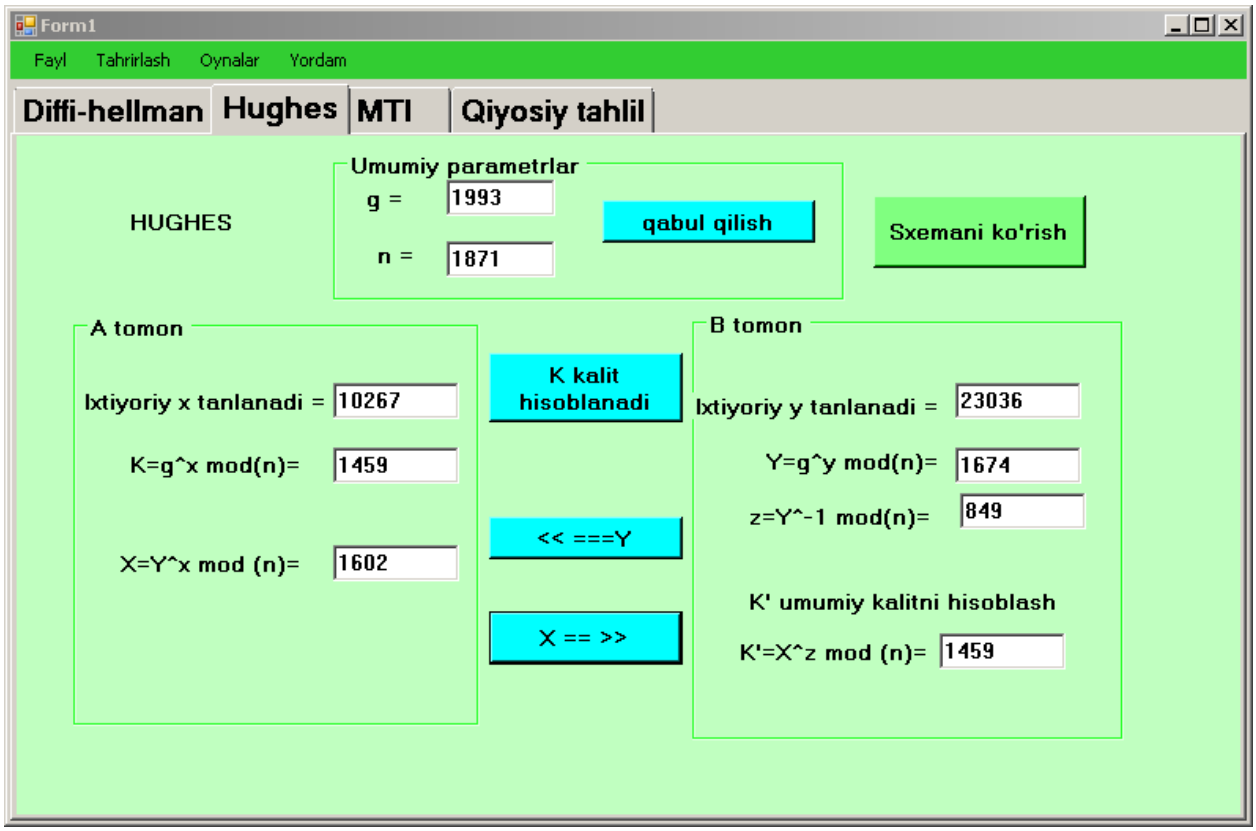
Қуйидаги дастурий таъминотда ассимметрик алгоритмларга асосланган калиларни тақсимлаш алгоритмларининг таҳлили келтириб ўтилган. 1-расмда Диффи-Хеллман калитларни тақсимлаш алгоритмнинг ишлаш фаолияти кўрсатилган**.**



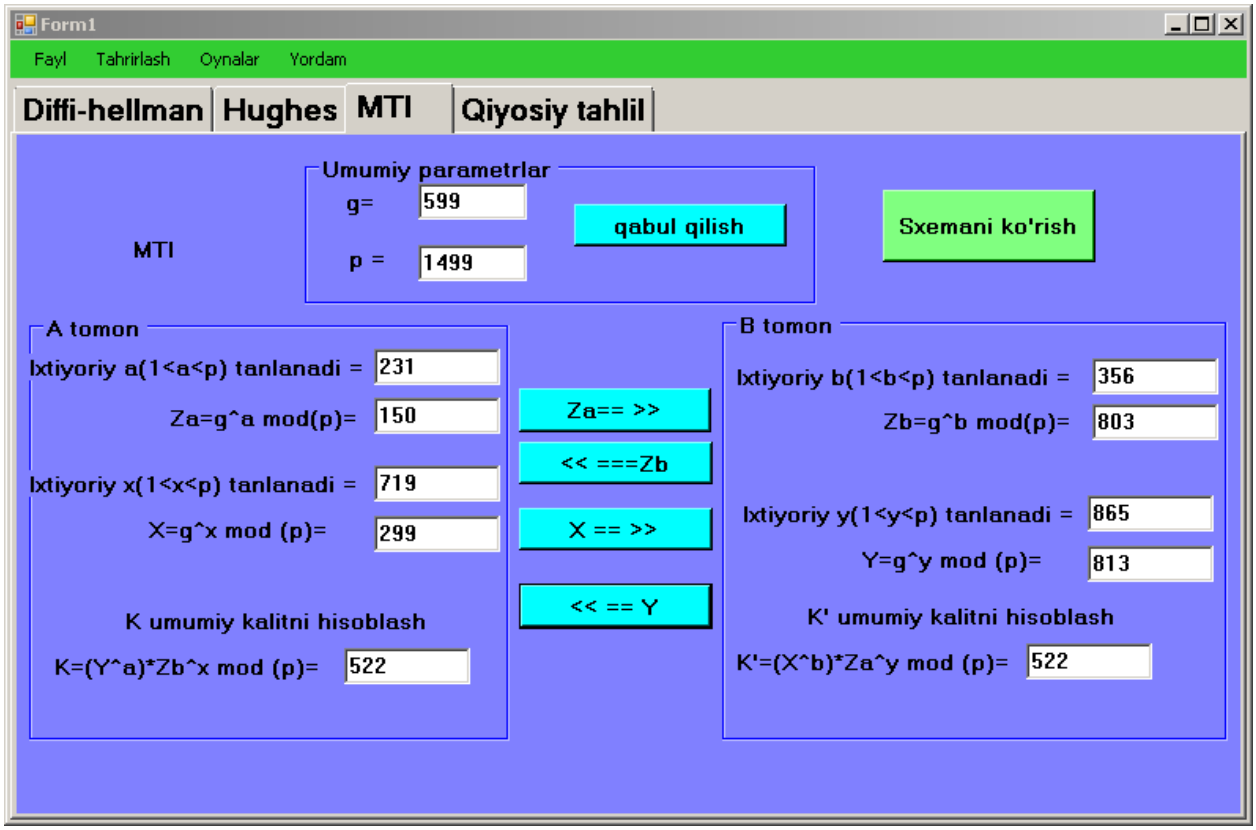
Кейинги расмда Диффи-Хеллман алгоритмининг функционал кўриниши тасвирланган



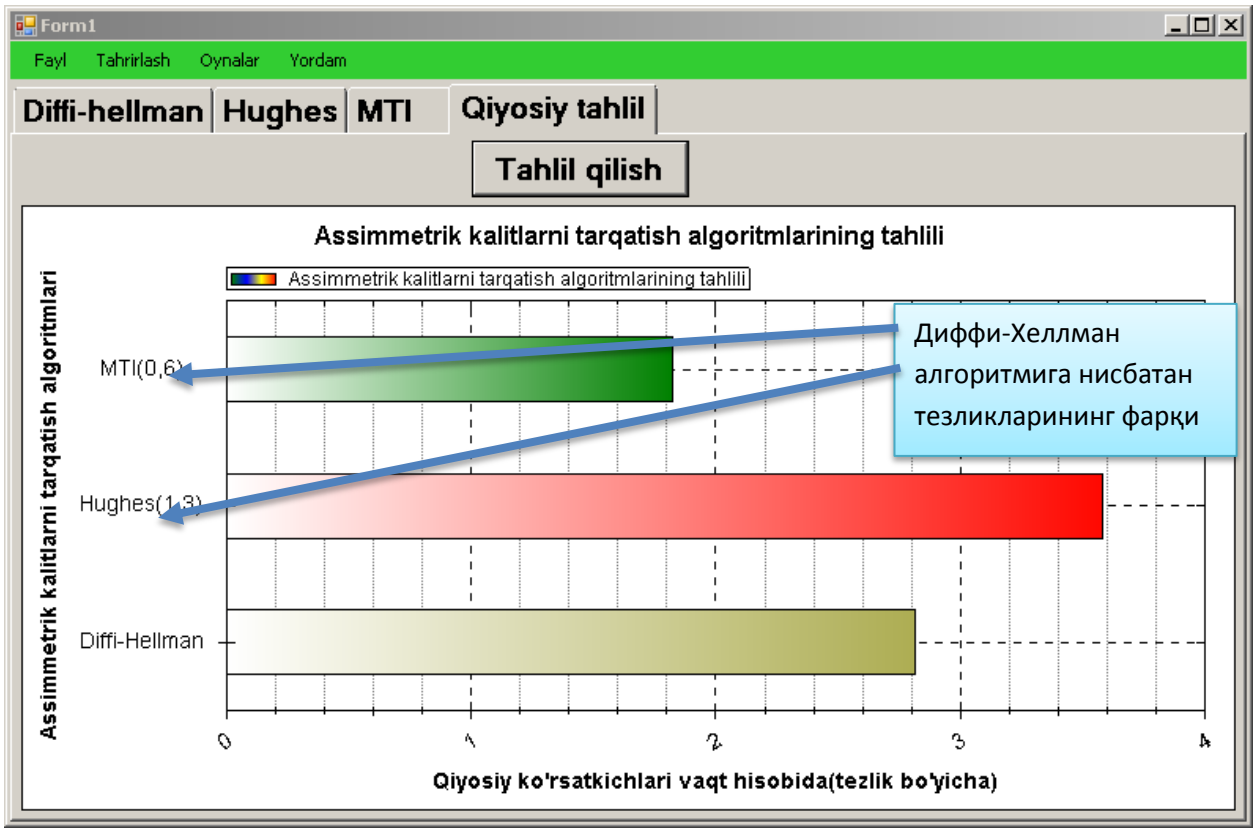
3-расмда Hughes алгоритмининг ишлаш ҳолати тасвирланган. Умумий параметрлар ва ноъмалум ўзгарувчилар орқали калит алмашинув жараёни амалга оширилади.



4-расмда МТИ алгоритмининг ишлаш жараёни тасвирланган.



Бу ерда ассимметрик калитларни тақсимлаш алгоритмларининг тезликлари бўйича таҳлили келтириб ўтилган.Бу ердан МТИ алгоритмининг тезлиги бошқа алгоритмларнинг тезлигиа нисбатан баландлиги кўриниб турибди.



ХУЛОСА

1. Криптотизим қанчалик криптобардошли ва ишончли бўлмасин, ундан амалда фойдаланиш жараёнлари калитларни бошқариш жараёнлари масалалари билан боғлиқлиги асосланди;

2. Замонавий криптографияда калитларни бошқариш масалалари қўриб ўтилди;

3. Калитларни очиқ каналларда хавфсиз тақсимлаш масалалари тадқиқ қилинди;

4. Замонавий криптографик калитларни тақсимлашнинг замонавий усуллари ва схемалари тадқиқ этилди;

5. Ассимметрик алгоритмларга асосланган калитларни тақсимлаш алгоритмлари ва протоколларидан ҳужжатли маълумотларнинг махфийлигини таъминлаш учун фойдаланиш мумкинлиги изоҳланди;

6. Ҳозирги кунда энг кўп қўлланиладиган хорижий ассимметрик алгоритмларга асосланган калитларни тақсимлаш алгоритмлари ва протоколлари таҳлил этилди;

7. Ассимметрик калитларни тақсимлаш алгоритмларининг қиѐсий таҳлили ва криптобардошлилигининг таснифланди.

ФОЙДАЛАНИЛГАН АДАБИЁТЛАР

1. «Ахборотлаштириш тўғрисида»ги Ўзбекистон Республикаси Қонуни. 11.12.2003 й. №560-II.

2. «Ўзбекистон Республикасида ахборотнинг криптографик муҳофазасини ташкил этишга доир чора-тадбирлари тўғрисида» ги Ўзбекистон Республикаси Президентининг ПҚ-614-сон қарори. – Тошкент, 3 апрел 2007 йил.

3. Шеннон К. Теория и связи в секретных системах. Работы по теории информации и кибернетике. – М.: Иностранная лит. 1963. – 243 б.

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

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

6. Federal Information Processing Standards Publication 197. Advanced Encryption Standard (AES). 2001.

7. Зензин О., Иванов М. Стандарт криптографической защиты – AES. Конечные поля. – Изд.:Кудиц - Образ, 2002. – 176 с.

8. Ғаниев С.К., Каримов М.М., Ташев К.А. Ахборот хавфсизлиги. Ахборот-коммуникацион тизимлар хавфсизлиги. Ўқув қўлланма. Т., “Aloqachi”. 2008. – 382 б.

9. Бабаш А.В., Шанкин Г.П. История криптографии. Часть I. - Изд.: Лори Гелиос АРВ, 2002.- 240 с.

10. Diffie, W., Hellman, M. New directions in cryptography // IEEE Transactionson Information Theory, vol. IT-22, 1976. – Pp. 644-654.

11.Чмора А.Л. Современная прикладная криптография. Изд.:Гелиос, 2001.- 256 с.

12. Акбаров Д.Е. «Ахборот хавфсизлигини таъминлашнинг криптографик усуллари ва уларнинг қўлланилиши» - Т.: «Ўзбекистон маркаси», 2009. - 424 б.

13. Miller V. Use of elliptic curves in cryptography // Advances in cryptology — CRYPTO’85 (Santa Barbara, Calif., 1985). 1986. (Lecture Notes in Comput. Sci.; V. 218). P. 417-426.

14. Koblitz N. and Vanstone S. The state of elliptic curve cryptography // Designs, Codes and Cryptography, 19 (2000). – Pp. 173-193.

15. Koblitz N. Elliptic Curve Cryptosystems // Mathematics of Computation, 48, 1987. – Pp. 203-209.

16. Коблиц Н. Введение в эллиптические кривые и модулярные формы // Пер с англ. – Москва: Мир, 1988. – 320 с.

17. Брюс Шнайер. Прикладная криптография. Протоколы, алгоритмы, исходные тексты на языке Си – Москва: ТРИУМФ, 2002. – 816 с.

18. Нильс Фергюсон, Брюс Шнайер. Практическая криптография – Москва: "Диалектика", 2004. – 432 с.

19. Зубов А.Ю. Криптографические методы защиты информации. Совершенные шифры. - Изд.:Лори Гелиос АРВ, 2005.- 192 с.

20. US Patent, Hellman, et al. Cryptographic apparatus and method, 4.200.770, April 29, 1980.

21. US Patent, Rivest R., Shamir A. and Adleman L.: Cryptographic Communications System and Method. 4,405,829, 1983.

22. Баричев С.Г., Гончаров В.В., Серов Р.Е. Основы современной криптографии. Учебное пособие. - Изд.:Лори Горячая Линия - Телеком, 2002.- 175 с.

23. Василенко О.Н. Теоретико-числовые алгоритмы в криптографии. – Изд.:МЦНМО, 2003. – 328 с.

24. Menezes A., van Oorschot P., Vanstone S. Handbook of Applied Cryptography. - CRC Press, 1996. – 780 pp.

25. Alfred J. Menezes: Elliptic curve public key cryptosystems, Kluwer academic publishers, 1993. – 152 pp.

26. Hankerson D., Menezes A., Vanstone S. Guide to Elliptic Curve Cryptography. Springer-Verlag New York, Inc. 2004.-456 pp.

27. Ященко В.В. Криптография, раньше была засекречена // ”Компьютера”, 1998, №20.- 250 с.

28. Коробейников А.Г., Гатчин Ю.А. Математические основы криптологии. Учебное пособие. - Санкт-Петербург, 2004. – 106 с.

29. Масленников М., Практическая криптография. - М.:Лори BHV - Санкт - Петербург, 2003.- 464 с.

30. Шнайер Б. Слабые места криптографических систем // Открытые системы. – 1999, № 1. – С. 31-36.

31. Стахов А.П. «ЗОЛОТАЯ» КРИПТОГРАФИЯ, Таганрог http://www.goldenmuseum.com/ http://www.trinitas.ru/rus/

32. Shamir, A. On the generation of cryptographically strong pseudo-random sequences // ACM Transactions on Computer Systems, vol. 1, 1983. – Pp. 38-44.

33. Biham E., Shamir A. Differential cryptanalysis of DES-like cryptosystems // Advances in Cryptology — CRYPTO ’90. LNCS. Springer–Verlag. 1991. V. 537. P.

34. Hellman M. A cryptanalytic time-memore trade-off // IEEE Transactionson Information Theory, vol. IT-26, 1980. – Pp. 401-406.

35. Kocher P.C. Timing Attacks on Implementations of Diffie-Hellman, RSA, DSS, and Other Systems. // http://citeseer.ist.psu.edu - Cryptography Research, Inc., San Francisco, USA. Matsui M. Linear cryptanalysis method for DES cipher // Advances in Cryptology — EUROCRYPT ’93. 1994. LNCS. Springer–Verlag. V. 765. P.

36. Menezes A.J. Elliptic Curve Public Key Cryptosystems, Kluwer Academic Publishers, 1993.

37. Min-Shiang Hawng, Cheng-Chi Le. Research issues and challenges for multiple digital signature // Int. J. of Network Security. – 2005. – Vol. 1, No 1. – P. 1–7.

38.Молдовян Н.А., Молдовян П.А. Новые протоколы слепой подписи // Безопасность информационных технологий. – М.:МИФИ. –2007. – № 3. – С. 17–21

39.ISO/IEC 11770 -1. “Key management – Introduction”.

40.ISO/IEC 11770 -2. “Key management – Symmetric techniques”.

41.ISO/IEC 11770 -3. “Key management – Asymmetric techniques”.

42.The Secure Sockets Layer Protocol. http://www.netscape.com/info/security-doc.html.

43. El Gamal T. A Public-key Cryptosystem and a Signature Based onDiscrete Logarithms. IEEE Trans. Inform. Theory, Vol. IT-31,pp.469-472, July 1985.

44. "Digital Signature Standard (DDS)", Federal Information Processing Standards Publication 186, May 19, 1994, pp.1-18.

45. Miller V. Use of elliptic curves in cryptography // Advances in cryptology — CRYPTO’85 (Santa Barbara, Calif., 1985). 1986. (Lecture Notes in Comput. Sci.; V. 218).

46. Koblitz N. and Vanstone S. The state of elliptic curve cryptography // Designs, Codes and Cryptography, 19 (2000).

47. Алферов А.П., Зубов А.К., Кузьмин А.С., Черемушкин А.В. Основы криптографии: Учебное пособие. - 2-е изд., испр. и доп. — М.. Гелиос АРВ, 2002. — 480 с.

48. Фомичев В.М. Дискретная математика и криптология. Курс лекций. -М., Диалог-МИФИ, 2003. - 400 с.

49. Бабаш А.В., Шанкин Г.П. Криптография. Под редакцией В.П. Шерстюка, ЭЛ. Применко / А.В. Бабаш, Г.П. Шанкин. - М.: СОЛОН-ПРЕСС, 2007. - 512 с. - (Серия книг «Аспекты защиты»). ISBN 5-93455-135-3

50. Панасенко С. Алгоритмы шифрования. Специальный справочник. - СПб: БХВ-Петербург, 2009 г., 576 с.

51. Болотов А.А., Гашков С.Б., Фролов А.Б., Часовских А.А. Элементарное введение в эллиптическую криптографию: Алгебраические н алгоритмические основы. — М.: КомКнига, 2006. — 328 с.

52. Болотов А.А., Гашков С.Б., Фролов А.Б., Часовских А.А. Элементарное введение в эллиптическую криптографию. Протоколы криптографии на эллиптических кривых.. - М.: Изд. КомКнига, 2006, 328 стр.

53. Острик В.В., Цфасман М.А. Алгебраическая геометрия и теория чисел: рациональные и эллиптические кривые - М.: МЦНМО, 2001.— 48 с. (Библиотека "Математическое просвещение", выпуск 8).

Дастур коди

```
using System;
using System.Collections.Generic;
using System.ComponentModel;
using System.Data;
using System.Drawing;
using System.Linq;
using System.Text;
using System.Windows.Forms;
using ZedGraph;
using System.Diagnostics;

namespace Assimmetrik_key_distribution_algoritms
{
    public partial class Form1 : Form
    {
        public Form1()
        {
            InitializeComponent();
        }


        public int sonniTekshir(int ji)
        {
            Random tavakkal = new Random(ji);
            int q = tavakkal.Next(201, 2001);
        f: q++;
            int j = 1;
            for (int k = 2; k < q - 1; k++)
            {
                if (q % k == 0) { j++; }
                if (j > 1) { break; }
            }
            if (j > 1) { goto f; }
            return q;
        }

        private void menuStrip1_ItemClicked(object sender, ToolStripItemClickedEventArgs
e)
        {

        }

        #region Diffi- hellman

        private void button2_Click(object sender, EventArgs e)
        {
            Difficha difi = new Difficha();
            difi.Show();
        }

        private void btnInpuit_Click(object sender, EventArgs e)
        {
            Random rnd = new Random();
            int temp = rnd.Next();
            int p = sonniTekshir(temp);
            txtP.Text = p.ToString();
            temp = rnd.Next(100);
            int g = sonniTekshir(temp);
            txtG.Text = g.ToString();
```

```
}

private long darajacha(long son, long daraja, long modul)
{

    long qoldiq = 1;
    long soncha = 0;
    for (int i = 0; i < daraja; i++)
    {
        soncha = qoldiq * son;
        qoldiq = soncha % modul;
    }

    return qoldiq;
}

private void diffiBosqich()
{
    Random rnd = new Random();
    int temp = rnd.Next();
    int p = sonniTekshir(temp);
    txtP.Text = p.ToString();
    temp = rnd.Next(100);
    int g = sonniTekshir(temp);
    txtG.Text = g.ToString();


    long a = rnd.Next(2000, 10000);
    txta.Text = a.ToString();
    long b = rnd.Next(2000, 10000);
    txtb.Text = b.ToString();
    long A = darajacha(g, a, p);
    txtAm.Text = A.ToString();
    long B = darajacha(g, b, p);
    txtBm.Text = B.ToString();


    long k1 = darajacha(B, a, p);
    txtKa.Text = k1.ToString();
    long k2 = darajacha(A, b, p);
    txtKb.Text = k2.ToString();



}

private void btnAB_Click(object sender, EventArgs e)
{
    long g = Convert.ToInt32(txtG.Text);
    long p = Convert.ToInt32(txtP.Text);
    Random rnd = new Random();
    long a = rnd.Next(2000, 10000);
    txta.Text = a.ToString();
    long b = rnd.Next(2000, 10000);
    txtb.Text = b.ToString();
    long A = darajacha(g, a, p);
    txtAm.Text = A.ToString();
    long B = darajacha(g, b, p);
    txtBm.Text = B.ToString();

}

private void btnKey_Click(object sender, EventArgs e)
{
    long g = Convert.ToInt32(txtG.Text);
```

```
    long p = Convert.ToInt32(txtP.Text);
    long B = Convert.ToInt32(txtBm.Text);
    long A = Convert.ToInt32(txtAm.Text);
    long a = Convert.ToInt32(txta.Text);
    long b = Convert.ToInt32(txtb.Text);
    long k1 = darajacha(B, a, p);
    txtKa.Text = k1.ToString();
    long k2 = darajacha(A, b, p);
    txtKb.Text = k2.ToString();
}

#endregion



#region Hughes


private void btnHug_Click(object sender, EventArgs e)
{
    HUghes hug = new HUghes();
    hug.Show();
}


private void hughesBosqich()
{
    Random rnd = new Random();
    int temp = rnd.Next(200, 30000);
    int n = sonniTekshir(temp);
    txtHugN.Text = n.ToString();
    temp = rnd.Next(100);
    int g = sonniTekshir(temp);
    txtHugG.Text = g.ToString();


    int x = rnd.Next(200, 30000);
    txtHugx.Text = x.ToString();

    long k = darajacha(g, x, n);
    txtHugK.Text = k.ToString();


    int y = rnd.Next(200, 30000);
    txtHugy.Text = y.ToString();
    long Y = darajacha(g, y, n);
    txtHugYm.Text = Y.ToString();
    teskari tes = new teskari();
    long Z = tes.teskariModul(y, n);
    txtHugZ.Text = Z.ToString();


    long X = darajacha(Y, x, n);
    txtHugXm.Text = X.ToString();


    long k2 = darajacha(X, Z, n);
    txtHugK22.Text = k.ToString();

}

private void Hughes_Click(object sender, EventArgs e)
{

}
```

```
private void btnHugIN_Click(object sender, EventArgs e)
{
    Random rnd = new Random();
    int temp = rnd.Next(200, 30000);
    int n = sonniTekshir(temp);
    txtHugN.Text = n.ToString();
    temp = rnd.Next(100);
    int g = sonniTekshir(temp);
    txtHugG.Text = g.ToString();



}

private void btnHugK_Click(object sender, EventArgs e)
{
    Random rnd = new Random();
    int x = rnd.Next(200, 30000);
    txtHugx.Text = x.ToString();
    long g = Convert.ToInt32(txtHugG.Text);
    long n = Convert.ToInt32(txtHugN.Text);
    long k = darajacha(g, x, n);
    txtHugK.Text = k.ToString();


    int y = rnd.Next(200, 30000);
    txtHugy.Text = y.ToString();
    long Ym = darajacha(g, y, n);
    txtHugYm.Text = Ym.ToString();
    teskari tes = new teskari();
    long Z = tes.teskariModul(y, n);
    txtHugZ.Text = Z.ToString();


}

private void button3_Click(object sender, EventArgs e)
{

    long n = Convert.ToInt32(txtHugN.Text);
    long Y = Convert.ToInt32(txtHugYm.Text);
    long x = Convert.ToInt32(txtHugx.Text);
    long Xm = darajacha(Y, x, n);
    txtHugXm.Text = Xm.ToString();

}

private void btnHugX_Click(object sender, EventArgs e)
{
    long X = Convert.ToInt32(txtHugXm.Text);
    long k = Convert.ToInt32(txtHugK.Text);
    long Z = Convert.ToInt32(txtHugZ.Text);
    long n = Convert.ToInt32(txtHugN.Text);
    long k2 = darajacha(X, Z, n);
    txtHugK22.Text = k.ToString();
}
#endregion


#region MTI


private void MTIBosqich()
{
```

```
        Random rnd = new Random();
        int temp = rnd.Next(200, 30000);
        int p = sonniTekshir(temp);
        txtMTI_P.Text = p.ToString();
        temp = rnd.Next(100);
        int g = sonniTekshir(temp);
        txtMTI_G.Text = g.ToString();

        int G = Convert.ToInt32(txtMTI_G.Text);
        int P = Convert.ToInt32(txtMTI_P.Text);

        long a = rnd.Next(10, P - 2);
        txtMtiA.Text = a.ToString();
        long Za = darajacha(G, a, P);
        txtMtiZa.Text = Za.ToString();
        long b = rnd.Next(10, P - 2);
        txtMtiB.Text = b.ToString();
        long Zb = darajacha(G, b, P);
        txtMtiZb.Text = Zb.ToString();


        long x = rnd.Next(10, P - 2);
        txtMtiX.Text = x.ToString();
        long Xm = darajacha(G, x, P);
        txtMtiXm.Text = Xm.ToString();


        long y = rnd.Next(10, P - 2);
        txtMtiy.Text = y.ToString();
        long Ym = darajacha(G, y, P);
        txtMtiYm.Text = Ym.ToString();

        // A tomonnnig kaliti

        long temp1 = darajacha(Ym, a, P);
        long temp2 = darajacha(Zb, x, P);
        long k1 = temp1 * temp2;
        k1 = k1 % P;
        txtMtiK1.Text = k1.ToString();

        // B tomonnnig kaliti

        long temp21 = darajacha(Xm, b, P);
        long temp22 = darajacha(Za, y, P);
        long k2 = temp21 * temp22;
        k2 = k2 % P;
        txtMtiK2.Text = k2.ToString();

    }
    private void btnMTI_Click(object sender, EventArgs e)
    {
        MTI mti = new MTI();
        mti.Show();
    }

    private void btnMtiinit_Click(object sender, EventArgs e)
    {
        Random rnd = new Random();
        int temp = rnd.Next(200, 30000);
        int p = sonniTekshir(temp);
        txtMTI_P.Text = p.ToString();
        temp = rnd.Next(100);
        int g = sonniTekshir(temp);
        txtMTI_G.Text = g.ToString();
    }
```

```
private void btnMtiZa_Click(object sender, EventArgs e)
{
    int G = Convert.ToInt32(txtMTI_G.Text);
    int P = Convert.ToInt32(txtMTI_P.Text);
    Random rnd = new Random();
    long a = rnd.Next(10, P - 2);
    txtMtiA.Text = a.ToString();
    long Za = darajacha(G, a, P);
    txtMtiZa.Text = Za.ToString();
    long b = rnd.Next(10, P - 2);
    txtMtiB.Text = b.ToString();
    long Zb = darajacha(G, b, P);
    txtMtiZb.Text = Zb.ToString();

}

private void btnMtiZb_Click(object sender, EventArgs e)
{
    int P = Convert.ToInt32(txtMTI_P.Text);
    int G = Convert.ToInt32(txtMTI_G.Text);
    Random rnd = new Random();
    long x = rnd.Next(10, P - 2);
    txtMtiX.Text = x.ToString();
    long Xm = darajacha(G, x, P);
    txtMtiXm.Text = Xm.ToString();

}

private void btnMtiX_Click(object sender, EventArgs e)
{
    int P = Convert.ToInt32(txtMTI_P.Text);
    int G = Convert.ToInt32(txtMTI_G.Text);
    Random rnd = new Random();
    long y = rnd.Next(10, P - 2);
    txtMtiy.Text = y.ToString();
    long Ym = darajacha(G, y, P);
    txtMtiYm.Text = Ym.ToString();
}

private void btnMtiY_Click(object sender, EventArgs e)
{
    // A tomonnnig kaliti
    int P = Convert.ToInt32(txtMTI_P.Text);
    int a = Convert.ToInt32(txtMtiA.Text);
    int Ym = Convert.ToInt32(txtMtiYm.Text);
    int Zb = Convert.ToInt32(txtMtiZb.Text);
    int x = Convert.ToInt32(txtMtiX.Text);
    long temp1 = darajacha(Ym, a, P);
    long temp2 = darajacha(Zb, x, P);
    long k1 = temp1 * temp2;
    k1 = k1 % P;
    txtMtiK1.Text = k1.ToString();

    // B tomonnnig kaliti
    int b = Convert.ToInt32(txtMtiB.Text);
    int Xm = Convert.ToInt32(txtMtiXm.Text);
    int Za = Convert.ToInt32(txtMtiZa.Text);
    int y = Convert.ToInt32(txtMtiy.Text);
    long temp21 = darajacha(Xm, b, P);
    long temp22 = darajacha(Za, y, P);
    long k2 = temp21 * temp22;
    k2 = k2 % P;
    txtMtiK2.Text = k2.ToString();
}
```

```
        #endregion


        #region Grafik regioni

        #region Kontext menyu

        void Grafik_ContextMenuBuilder(ZedGraphControl sender,
          ContextMenuStrip menuStrip,
          Point mousePt,
          ZedGraphControl.ContextMenuObjectState objState)
        {

            menuStrip.Items[0].Text = "Nusxa ko'chirish";
            menuStrip.Items[1].Text = "Gistogrammani boshqa nomda saqlash";
            menuStrip.Items[2].Text = "Sahifa parametrlari…";
            menuStrip.Items[3].Text = "Bosmaga chiqarish…";
            menuStrip.Items[4].Text = "Nuqta qiymatlarini ko'rsatish…";
            menuStrip.Items[7].Text = "Standart masshtabni tanlash...";

            menuStrip.Items.RemoveAt(5);
            menuStrip.Items.RemoveAt(5);
            ToolStripItem newMenuItem = new ToolStripMenuItem("Bu punkt hech qanday
vazifa bajarmaydi...");
            menuStrip.Items.Add(newMenuItem);
        }

        #endregion

        public void buildGraph()
        {
            graf.ContextMenuBuilder += new
ZedGraphControl.ContextMenuBuilderEventHandler(Grafik_ContextMenuBuilder);
            GraphPane pane = graf.GraphPane;

            //
            pane.CurveList.Clear();

            Random rnd = new Random();

            string[] nomlar = { "Diffi-Hellman", "Hughes", "MTI", };
            double[] yvalues = new double[nomlar.Length];

            #region Tezlikka tekshirish
            //Klassik



            Stopwatch st1 = new Stopwatch();
            // Diffi-Hellman
            st1.Start();
            diffiBosqich();
            st1.Stop();
            double diffi = st1.Elapsed.TotalMinutes * 1000 * 60 +
st1.Elapsed.TotalSeconds * 1000 + st1.Elapsed.TotalMilliseconds;

            Stopwatch st2 = new Stopwatch();
            // Hughes
            st2.Start();
            hughesBosqich();
            st2.Stop();
            double hughes = st2.Elapsed.TotalMinutes * 1000 * 60 +
st2.Elapsed.TotalSeconds * 1000 + st2.Elapsed.TotalMilliseconds;
```

```
            Stopwatch st3 = new Stopwatch();
            // MTI
            st3.Start();
            MTIBosqich();
            st3.Stop();
            double mti = st3.Elapsed.TotalMinutes * 1000 * 60 + st3.Elapsed.TotalSeconds
* 1000 + st3.Elapsed.TotalMilliseconds;


            #endregion
            //double foiz = huj / qolganlari;
            yvalues[0] = diffi;
            yvalues[1] = hughes;
            yvalues[2] = mti;

            //yvalues[3] = 2;
            nomlar[1] = string.Format("{0}({1:0.0})", nomlar[1], hughes / diffi);
            nomlar[2] = string.Format("{0}({1:0.0})", nomlar[2], mti / diffi);


            pane.YAxis.Title.Text = "Assimmetrik kalitlarni tarqatish algoritmlari";
            pane.XAxis.Title.Text = "Qiyosiy ko'rsatkichlari vaqt hisobida(tezlik
bo'yicha)";
            BarItem curve = pane.AddBar("Assimmetrik kalitlarni tarqatish
algoritmlarining tahlili", yvalues, null, Color.DodgerBlue);
            Color[] colors = { Color.Green, Color.Blue, Color.Yellow, Color.Red };
            curve.Bar.Fill = new Fill(colors);
            curve.Bar.Fill.Type = FillType.GradientByX;
            curve.Bar.Fill.RangeMin = yvalues.Min();
            curve.Bar.Fill.RangeMax = yvalues.Max();
            //
            pane.YAxis.Type = AxisType.Text;
            //
            pane.YAxis.Scale.TextLabels = nomlar;
            // !
            pane.BarSettings.MinClusterGap = 1.1f;
            pane.XAxis.Scale.MinAuto = true;
            pane.XAxis.Scale.MaxAuto = true;
            // burchak x uqidagi yozuvni
            pane.XAxis.Scale.FontSpec.Angle = 30;

            pane.BarSettings.Base = BarBase.Y;
            //
            pane.XAxis.MajorGrid.IsVisible = true;
            pane.XAxis.MajorGrid.DashOn = 5;
            pane.XAxis.MajorGrid.DashOff = 5;
            //
            pane.YAxis.MajorGrid.IsVisible = true;
            pane.YAxis.MajorGrid.DashOn = 5;
            pane.YAxis.MajorGrid.DashOff = 5;
            //
            pane.YAxis.MinorGrid.IsVisible = true;
            pane.YAxis.MinorGrid.DashOn = 1;
            pane.YAxis.MinorGrid.DashOff = 1;

            pane.XAxis.MinorGrid.IsVisible = true;
            pane.XAxis.MinorGrid.DashOn = 1;
            pane.XAxis.MinorGrid.DashOff = 1;

            pane.Title.Text = "Assimmetrik kalitlarni tarqatish algoritmlarining
tahlili";
            pane.IsBoundedRanges = true;
            graf.AxisChange();
            graf.Invalidate();
```

```
            graf.Refresh();

        }


        #endregion

        private void btntahlil_Click(object sender, EventArgs e)
        {
            buildGraph();
        }

    }
}
```