ЎЗБЕКИСТОН РЕСПУБЛИКАСИ АХБОРОТ ТЕХНОЛОГИЯЛАРИ ВА КОММУНИКИЦИЯЛАРНИ РИВОЖЛАНТИРИШ ВАЗИРЛИГИ
МУХАММАД АЛ-ХОРАЗМИЙ НОМИДАГИ ТОШКЕНТ АХБОРОТ ТЕХНОЛОГИЯЛАРИ

МАЪРУЗАЛАР МАТНИ

Фан: Криптография усуллари

Фан тури: Амалий

Йўналиш: 5330300- Ахборот хавфсизлиги (ахборот коммуникацияси технологиялари ва сервис)

ФАРҒОНА - 2018

Ушбу маъруза матни таянч университетнинг ишчи ўқув дастури асосида тайёрланган.

Тузувчилар:
АТТ кафедраси ассистенти **У.Худойназаров**

Тақризчилар:
Телекоммуникация инж.
кафедраси доценти **Н.Умаралиев**

«**ТАСДИҚЛАНГАН**»
ТАТУ Фарғона Филиали Кенгашининг
2018 йил 29 августдаги йиғилиши
№ _____баённомаси
Ўқув ва тарбиявий ишлар
бўйича директор ўринбосари
_____ А.Расулов

«Маъқулланган»
Ахборот-таълим технологиялари кафедраси йиғилишининг 2018 йил 27 августдаги 1-сонли баённомаси.

Кафедра мудири _____ С.М.Абдурахмонов

«Маъқулланган»
“Телекоммуникация технологиялари ва касбий таълим” факультети ўқув-услубий Кенгашининг 2018 йил 27 августдаги 1-сонли баённомаси

Кенгаш раиси: _____ О.Қўлдошев

«Тавсия этилган»
Ўқув-услубий бўлим бошлиғи _____ Ш.Умаров
2018 й “____”_____

1 - маъруза

Мавзу: Криптографиянинг мухим масалалари ва ривожи.

Режа:

1. Ахборотни ҳимоялашда криптографиянинг ўрни.
2. Асосий тушунчалар.
3. Криптологиянинг фан сифатида шаклланиши.

Таянч атамалар: криптография, криптология, криптотаҳлил, хэш функция, электрон рақамли имзо, конфиденциаллик, бутунлик, калитларни бошқариш.

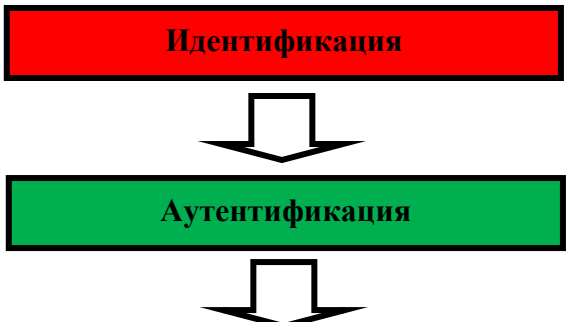
Ахборотни ҳимоялашда криптографиянинг ўрни

Электрон кўринишдаги маълумотларни ҳажмини ортиши, уни сақлаш билан боғлиқ бўлган муаммолар ҳажмини ҳам ортишига олиб келади. Ушбу муаммоларни ҳал қилишда мавжуд бўлган усуллар эса, кундан-кунга янгиланаверади. Шунга қармасдан ахборот хавфсизлигини таъминлашда қадимда ҳам фойдаланилаган ва ҳозирда ҳам фойдаланилаётган усуллардан бири бу – криптографик ҳимоя усулларидир. Криптографик ҳимоя усуллари ўзининг ишончлилиги, самарадорлиги ва фойдаланиш даражаси қамрови кенглиги билан бошқа усуллардан фарқ қилади. Ҳозирда ахборот хавфсизлигини таъминлашнинг ҳар бир жабҳасида криптографик усуллардан фойдаланилмоқда. Бу эса унинг муҳимлигидан дарак беради.

Умумий ҳолда ахборот хавфсизлиги консепсияси учта ташкил этувчидан иборатлигини эътиборга олсак, ахборот хавфсизлигини таъминлаш дэганда маълумотнинг қуйидаги учта хусусиятини таъминлаш тушуниш мумкин. Қуйида келтирилган 1.1- расмда ушбу учта хусусиятни таъминлашда криптографик усулларнинг тутган ўрни келтирилган.

1.1-расм. Ахборот хавфсизлиги хусусиятлари

Ушбу учта хусусият ахборот ҳимоясининг асосий ташкил этувчилари саналиб, ахборотни ҳимоялаш дэганда асосан шу учта хусусиятни таъминлаш тушинилади. Аммо ушбу учта хусусият тўлиқ бажарилиши учун бир нечта бажарилиши мумкин бўлган ишлар талаб этилади. Бошқача қилиб айтганда ушбу учта хусусиятни бажаришдан олдин, қуйида келтирилган амалиётларни бажаришга тўғри келади. 1.2-расмда келтирилган жараёнларда криптографик ҳимоя усулларидан фойдаланиш даражаси эса қуйидагича.



1.2-расм. Фойдаланишни бошқариш

Аутентификация жараёни фойдаланувчини тизимдан фойдаланиш учун уни ҳақиқийлигини текшириш саналиб, 2-расмда келтирилганидек, аутентификациялаш жараёни криптографик усуллардин фойдаланилган ҳолатда амалги оширилиб, бунда криптографик калит узутиш протоколлари, аутентификациялаш протоколлари, маълумотни аутентификациялаш кодлари ва ҳак. фойдаланилади. Ушбу жараёнда ҳам криптографик ҳимоя усуллари ўзининг бардошлиги, ишончлилиги билан ажралиб туради.

Криптография - ахборотларни аслидан ўзгартирилган ҳолатга акслантириш услубларини топиш ва такомиллаштириш билан шуғилланади. Дастлабки системалашган криптографик услублар эрамиз бошида, Юлий Цезарьнинг иш юритиш ёзишмаларида учрайди. У, бирор маълумотни маҳфий ҳолда, бирор кишига етказмоқчи бўлса, алфавитнинг биринчи ҳарфини алфавитнинг тўртинчи ҳарфи билан, иккинчисини бешинчиси билан ва ҳоказо шу тартибда алмаштириб матннинг асли ҳолатидан шифрланган матн ҳолатига ўтказган.

Ахборотларнинг мухофазаси масалалари билан криптология (*kryptos*- маҳфий, **logos**- илм) фани шуғилланади. Криптология мақсадлари ўзаро қарама-қарши бўлган икки йўналишга эга: – *криптография* ва *криптоанализ.*

Криптографиянинг очиқ маълумотларни шифрлаш масалаларини математик услублари билан шуғилланиши тўғрисида юқорида айтиб ўтилди.

Криптоанализ эса шифирлаш услубини (калитини ёки алгоритмини) билмаган ҳолда шифрланган маълумотни асли ҳолатини (мос келувчи очиқ маълумотни) топиш масалаларини ечиш билан шуғилланади.

Ҳозирги замон криптографияси қуйидаги тўртта бўлимни ўз ичига олади:

Симметрик криптотизимлар.

Очиқ калит алгоритмига асосланган криптотизимлар.

Электрон рақамли имзо криптотизимлари.

Криптотизимлар учун криптобардошли калитларни ишлаб чиқиш ва улардан фойдаланишни бошқариш.

Криптографик услублардан фойдаланишнинг асосий йўналишлари: маҳфий маълумотларни очиқ алоқа канали бўйича муҳофаза қилиш ҳолда узатиш, уларнинг хақиқийлигини таъминлаш, ахборотларни (электрон хужжатларни, электрон маълумотлар жамғармасини) компьютерлар тизими хотирасида шифрланган ҳолда сақлаш ва шу каби масалаларнинг ечимларини ўз ичига олади.

Такидлаш жоизки, криптография узоқ вақт давомида давлат органлари алоқа тармоқларида алмашинадиган маълумотлар муҳофазасининг таҳминланишида қўлланиб келинди. Компьютер тармоқлари ва электрон ҳужжат алмашинуви технологияларининг ривожланиши молия, банк ишлари,

савдо-сотиқ каби соҳаларда қўлланилиши ахборот муҳофазасининг криптографик усулларини умумжамият фаолиятининг турли соҳаларига кенг кириб боришига сабаб бўлди. Ҳақиқатан ҳам, алоқа тармоқларида ахборотни муҳофаза қилиниши, криптографик усулда таъминлаш умумжамият тараққиётининг ривожланиш босқичлари билан боғлиқ бўлган узоқ тарихий манбаларига эга бўлиб, умуминсоният жамиятига хҳизмат қилмаслиги (яъни криптографик усулларни кенг омма томонидан фойдаланилишининг чекланиши) таажубланарли ҳолат бўлар эди.

Асосий тушунчалар

Шундай қилиб, ахборот муҳофазасининг криптографик услублари очиқ маълумотларни ўзгартириб, фақат калит маълум бўлгандагина уни асл ҳолатига қайтариш имкониятини беради.

Шифрлаш ва дешифрлаш масалаларига тегишли бўлган, маълум бир алифбода тузилган маълумотлар *матнларни* ташкил этади.

Алифбо - ахборотни кодлаш учун фойдаланиладиган чекли сондаги белгилар тўплами. Мисол сифатида:

- ўттиз олтита белгидан (ҳарфдан) иборат ўзбек тили алифбоси;
- ўттиз иккита белгидан (ҳарфдан) иборат рус тили алфавити;
- йигирма саккизта белгидан (ҳарфдан) иборат лотин алфавити;
- икки юз эллик олтита белгидан иборат ASCII ва КОИ–8 стандарт компьютер кодларининг алифбоси;
- бинар алфавит, яъни 0 ва 1 белгилардан иборат алфавит;
- саккизлик ва ўн олтилик саноқ системалари белгиларидан иборат алфавитларни келтириш мумкин.

Матн - алифбонинг элементларидан (белгиларидан) ташкил топган тартибланган тузилма.

Шифрлаш - очиқ матн деб аталувчи *дастлабки маълумотни шифрланган маълумот (криптограмма)* ҳолатига ўтказиш жараёни.

Дешифрлаш - шифрлашга тескари бўлган жараён, яъни калит ёрдамида шифрланган маълумотни дастлабки ҳолатга ўтказиш.

Калит - дастлабки маълумотни бевосита шифрлаш ва дешифрлаш учун зарур манба.

Криптографик тизим - очиқ маълумотни шифрлаш ва дешифрлаш жараёнини ташкил этувчи амаллар мажмуи бўлиб, алфавит белгиларини алмаштириш кетма-кетлигидан иборат.

Шифрлаш тизимлари фойдаланиладиган калитлар сонига кўра икки қисмга бўлинади: **симметрик** ва **асимметрик** - очиқ калитли.

Симметрик криптотизимларда шифрлаш учун ҳам ва дешифрлаш учун ҳам бир ҳил калитдан фойдаланилади.

Очиқ калитли криптотизимларда иккита калитдан фойдаланилади -– ўзаро математик боғлиқ бўлган очиқ ва ёпиқ калитлардан. Бунда маълумотлар ҳаммага маълум бўлган маълумот юборилаётган шахснинг очиқ калити билан шифрланади ва фақат маълумот юборилаётган шахснинг ўзигагина маълум бўлган ёпиқ калит билан дешифрланади.

Калитларни тақсимлаш ва бошқариш – криптобардошли калитларни

ишлаб чиқиш (ёки яратиш), уларни муҳофазали сақлаш, ҳамда калитларни фойдаланувчилар орасида муҳофазаланган ҳолда тақсимлаш жараёнларини ўз ичига олади.

Электрон рақамли имзо - электрон матнга илова қилинадиган криптографик алмаштиришдан иборат бўлиб, шу электрон матн жўнатилган шахсга қабул қилинган электрон матннинг ва матинни рақамли имзоловчининг ҳақиқий ёки ноҳақиқий эканлигини аниқлаш имконини беради.

Криптологиянинг фан сифатида шаклланиши

Қадимги шифрлаш услублари ҳар-хил жадвалларга асосланган бўлиб, бу жадваллар маълумотлар матнидаги алфавит белгиларининг маълум тартибдаги ўрин алмаштиришларини ифодаловчи оддий амаллардан иборат бўлган. Бунда калит вазифасини жадвалнинг ўлчами, алфавит белгиларининг алмаштирилишини таминловчи бирор аниқ жумла ёки жадвалнинг ўрин алмаштиришларини тартибловчи алоҳидалик хусусияти ва шу кабилар ўтаган.

Мисол учун, ушбу

АНГЛАШИЛМОВЧИЛИК ТУШИНАРСИЗЛИККА ОЛИБ КЕЛДИ

жумла устунларининг сони 5 та ва сатрларининг сони 8 та бўлган жадвалнинг устунлари бўйича ёзиб чиқилса, сўнгра шу жадвалнинг сатрлари бўйича гуруҳланса:

А М Т И Л, Н О У З И, Г В Ш Л Б, Л Ч И И К,

А И Н К Е, Ш Л А К Л, И И Р А Д, Л К С О И

каби шифрланган сўзлар ҳосил бўлади.

Маълумотларни шифрлаб муҳофаза қилишнинг турли мақсадларда қўлланиб ривожланиб бориши, шифрлаш услубларининг фойдаланувчилар томонидан алоқа тармоқларида қўллаш учун қулай бўлишини талаб қилиниши билан бирга, унинг бардошлилигига бўлган талабнинг ҳам кучайишига олиб келди. XIX асрда алоқа коммуникацияларининг ривожланиб бориши, табиий равишда, шифрлаш жараёнларини автоматлаштирилишини талаб эта бошлади. Телеграф алоқа системалари вужудга келди ва улар ҳам, ўз навбатида, маълумотларни шифрлашни талаб эта бошлади. Махсус ғилдирак кўринишидаги, сонли шифрлаш қурилмаси 1790 йилда Америка қўшма Штатларининг (АҚШ) давлат котиби, кейинчалик эса АҚШнинг учинчи Президенти Томас Жефферсон томонидан яратилган ва шунга ўхшаш сонли шифрлаш қурилмалари иккинчи жаҳон уруши йилларидан кейин ҳам АҚШ қуролли кучларида қўлланилиб келинган. Бундай қурилмаларнинг ишлаши, етарли даражада узун берилган калит бўйича маълумотлар матнини кўп алфавитли алмаштиришга асосланган бўлиб, арифмометрнинг ишлаш асосларига ўхшашдир. Калитнинг (даврий) узунлиги шифрлаш қурилмасининг махсус ғилдиракларини бир марта тўла айланишларининг умумий даври билан аниқланади. Масалан, мос ҳолда 13, 15, 17, ва 19 даврий айланишларга эга бўлган махсус тўртта ғилдиракли қурилма 62985 (даврий) узунликка эга бўлган калитни беради. Яъни, қурилма ғилдираклари бирор аниқ ҳолатда турган бўлса, мана шу ҳолатга қайтадан кетма-кет 1-

ғилдиракни 13 марта, 2-ғилдиракни 15 марта, 3-ғилдиракни 17 марта, 4-ғилдиракни 19 марта айлантириш билан эришилади.

Ҳозирги замон криптографик машиналари асосини, 1917 йилда Эдвард Хеберн томонидан яратилган, «Enigma - Энигма» («Жумбоқ» маъносини англатувчи) деб аталувчи роторли криптографик машинанинг ишлаш тамоиллари ташкил этади. «Энигма» машиналарининг саноат наъмуналари Siemens фирмаси томонидан ишлаб чиқилиб, дастлаб битта ўққа ўрнатилган тўртта айланувчи ғилдиракдан иборат бўлиб, бирор аниқ ҳолатнинг, оддий алмаштиришлар ёрдамида, миллиондан ортиқ шифрланган ҳолатини олиш имконини берган. Ҳар бир ғилдиракнинг иккала томонида 25 тадан (лотин алфавитининг белгилари (ҳарфлари) сонича) электр боғланиш тугунлари жойлашган бўлиб, ғилдираклар айланганда электр боғланиш импульслари рўй бериб, ҳарфларнинг алмашув жараёни юзага келади. Шифрлаш жараёни бошланиши олдидан ғилдираклар калитни белгиловчи сўзни аниқлаш ҳолатига ўрнатилади. Алфавит ҳарфларини белгиларини бошқа белгилар билан алмаштириб шифрлаш жараёни, шифрланиши керак бўлган белгининг тугмачаларини босиш натижасида амалга оширилган. Бунда шифрланиши керак бўлган белгининг тугмачаларини босиш натижасида, аввал 1-ғилдирак, сўнгра 2 - ғилдирак бир қадамга бурилган ва ҳоказо. Натижада, калитнинг узунлиги очиқ матн узунлигига нисбатан узун бўлган. Масалан, чап ва ўнг томондаги ғилдиракларнинг U белгисига мос келувчи электр боғланиш тугунлари ғилдиракларнинг бошқа томонидаги F белгига мос келувчи электр боғланиш тугунлари билан боғланган. Агар ғилдирак бир қадамга бурилса, бу ҳолат U белгидан кейинги V белгини F белгидан кейинги G белгига алмаштириш жараёнини ифодалайди. Тўрт ғилдиракли криптографик машиналарда алфавит белгиларини шифрлаш жараёнида ҳамма белги ҳар бир ғилдиракда ўзгариш жараёнидан ўтиб, тўрт карра шифрланади. Дешифрлаш жараёнини мураккаблаштириш мақсадида ғилдиракларнинг ўрни вақти-вақти билан алмаштирилиб турилган. Кейинчалик эса ғилдиракларнинг сони 5 ва 6 тага кўпайтирилиб, уларнинг ҳаракатининг маълум маънода тартибсиз бўлиши таъминланган. Бу қурилманинг ҳажми катта бўлмаганлиги ҳамда ундан фойдаланиш мураккаб эмаслиги сабабли, оддий алоқа хизматчилари ҳам ишлата олганлар. Шу даврга келиб, маълумотларни ишончли шифрлаш масаласи тўла ҳал қилингандек эди. Лекин, Англия криптографик хизматининг хизматчилари Лондондан 80 км шимолда жойлашган «Блетчли Боғ» қароргоҳида иккинчи жаҳон уруши йиллари давомида немислар шифрмаълумотларини ўқиб боришга муваффақ бўлганлар. Бунга Польша разведка хизмати томонидан 1939 йилда қўлга киритилган «Энигма» криптографик машинасининг чизмалари асос бўлди. Гитлерчиларнинг Польшага хужумидан сўнг машина чизмалари Англиянинг тегишли хизмат ташкилотларига берилди. Тез орада, Англия криптоаналитика хизмати ходимлари, «Энигма» машинасининг шифрлаш калитини билиш учун, машина махсус ғилдиракларидаги электр боғланиш тугунларининг схемасини билиш кераклигини аниқладилар. Шундан сўнг, «Энигма» машинасининг қурилма наъмунасини қўлга киритиш

учун ҳаракатлар бошланди. Биринчи намунани Германиянинг жанубий-шарқий қисмида жойлашган заводдан олинишига эришилди, иккинчиси Норвегия ҳаво ҳудудларида уриб туширилган немис ҳужумчи самолётларидан, учинчиси эса Франция учун бўлган жангларда аср тушган немис ҳарбий алоқачи аскаридан олинган. Кейинги намуналар эса ғоввослар махсус қисмлари томонидан немис сув ости кемаларидан олинган. 1942 йилда Алан Тьюринг томонидан махсус электрон ҳисоблаш машинаси яратилгунга қадар, «Энигма» шифрларини дешифрлаш анча мураккаб бўлди. Алан Тьюрингнинг дешифрлаш учун махсус яратган ва «Колосс» деб номланган ушбу машинаси инсоният дунёсида биринчи тез ишловчи электрон ҳисоблаш машинаси (ЭҲМ) эди. Шундан сўнг Англия криптоаналитиклари, намуналари олинган «Энигма» машиналарининг ғилдиракларидан фойдаланиб, қисқа вақт ичида мумкин бўлган барча калитларни танлаб чиқиб, дешифрлаш масаласини ҳал эта бошладилар. Немислар эса дешифрлашда ЭҲМнинг қўлланилишини ҳисобга олмаган эдилар. Шуни ҳам айтиб ўтиш керакки, 1930 йилда немис криптоаналитиги Георг Шредернинг «Энигма» криптографик машинасининг шифрлаш услубига ишончсизлик билдириб келтирган далиллари кўпчилик масъул мутахассислар назаридан четда қолган. 1926 йилда Америка телефон ва телеграф компанияларидан бирининг маҳандиси Г.С. Вернам ўзининг иккилик саноқ системаси асосида яратган шифрлаш алгоритмини эълон қилди. Вернамнинг шифрлаш алгоритми Цезарнинг шифрлаш алгоритмига ўхшаш бўлиб, у қуйидаги

$y=x\oplus z,$ (1.1)

тенглама билан ифодаланади ва бунда x, y, z ўзгарувчилар иккилик саноқ системаси алфавитларида қийматлар қабул қилади, ⊕ белги эса 2 модуль бўйича қўшиш амалини билдиради, яъни: 0⊕0=0, 0⊕1=1, 1⊕0=1, 1⊕1=0. Бу алгоритмнинг моҳияти дешифлаш калитининг фақат бир марта ишлатилишига асосланган бўлиб, бунда шифрлаш ҳар сафар янги тасодифий битлардан иборат калит билан амалга оширилади. Бундай шифрлаш услубидан кўриниб турибдики, шифрлаш ва дешифрлаш учун очиқ матн узунлиги билан тенг бўлган битта калитдан фойдаланилади, ҳамда бу калитнинг фойдаланувчига муҳофазаланган алоқа канали орқали узатилиши талаб этилади. Бундан ташқари, шу усул билан шифрланган матнни дешифрлаш имконияти мураккаб бўлиб, бу унингмуаллифи Г. С. Вернам томонидан ҳам такидлаган бўлсада, исботи келтирмаган. Криптология соҳасидаги илмий ишларнинг авторлари, 1949 йилгача бўлган даврни қатъий исботсиз - фақат интуиция ва «ишончга» асосланган - илмий асосланмаган криптология даври, деб атайдилар. Таъкидлаб ўтиш жоизки, *Англия криптология хизмати иккинчи жаҳон уруши йиллари даврида математиклар криптологиянинг ривожланишига ўзларининг катта ҳиссаларини қўшишлари мумкинлигига иқрор бўлдилар.* Алан Тьюринг ҳам криптология хизмати мутахассисларидан бири бўлган. К.Э. Шенноннинг 1949 йилда чоп этилган «Маҳфий тизимларда алоқа назарияси», деб номланган илмий мақоласи илмий асосланган *маҳфий калитли криптография даврини* бошлаб берди.

Шеннон ўзининг электротехника ва математикага оид билимларидан келиб чиқиб, маҳфий алоқа тизими назариясининг асосини 1948 йилда эълон қилинган – ахборотлар назариясига бағишланган илмий мақоласи асосида яратди. Шеннон ўзининг бу илмий мақолаларида Вернам услубида шифрлашнинг ишончлилиги даражасига тўхталиб, дешифрлаш максимал мураккабликка эгалигини, ҳамда шу услубда шифрлашдан фойдаланувчига маҳфий алоқа канали орқали узатиладиган маҳфий калит ҳажми (узунлиги) учун аниқ қуйи чегаранинг қандай бўлишини илмий асосда исботлаб берди Шенноннинг 1948 йилда эълон қилинган илмий мақоласи криптология соҳасидаги илмий мақолаларнинг пайдо бўлишига олиб келди. Унинг томонидан 1948-1949 йилларда эълон қилинган илмий мақолалари катта аҳамиятли бўлсада, криптология соҳасидаги илмий мақолаларнинг сезиларли кўпайишига олиб келмади. Бунга сабаб, эҳтимолки, Шенноннинг маҳфий тизимларда алоқа назариясининг маҳфий калитга асосланган бўлиб, маҳфий калитни фойдаланувчига етказиш масалалари ечимининг мураккаблиги билан боғлиқлигидадир. 1976 йилда У. Диффи ва М.Е. Хеллманнинг «Криптографияда янги йуналиш», деб номланган мақоласининг эълон қилиниши шу соҳадаги очиқ илмий ишлар ривожининг жуда юқори поғонага кўтарилишига сабаб бўлди. Улар ушбу ишлари орқали, маҳфий алоқа тизимларида маълумотларни шифрлаш ва дешифрлашда маҳфий калитнинг тизим фойдаланувчилари орасида махсус муҳофазаланган алоқа канали орқали узатилиши ва қабул қилинишига ҳожат бўлмайдиган илмий-амалий услуб асосларини яратиб, бугунги кунда ҳам ривожланиб ва долзарблашиб бораётган *очиқ (маҳфий бўлмаган) калитли криптография даврини* бошлаб бердилар. Таъкидлаб ўтиш жоизки, Р. К. Мерклининг У. Диффи ва М.Е. Хеллманга боғлиқ бўлмаган ҳолда, лекин улар билан деярли бир пайтда бошқа илмий журналга берган мақоласида ҳам маълумотларни *очиқ калитли шифрлаш* ғоясининг асослари келтирилган. Аммо Р. К. Меркли мақоласининг нашриётда узоқ вақт эълон қилинмай тўхтаб қолиши, уни муаллифлик ҳуқуқидан деярли маҳрум этди.

Назорат саволлари

Криптогия фанининг асосий вазифаси.
Криптография фани ва унинг мақсади.
Замонавий криптографиянинг бўлимлари.
Криптографиянинг асосий тушунчалари.
Криптография фанинг ривожланиши.

2 - маъруза

Мавзу: Криптографик тизимларга қўйиладиган талаблар

Режа:

Маълумотларни муҳофаза қилиш қоидаларини бузувчининг мақсади.
Криптотизмларга қўйиладиган талаблар.
Таянч иборалар: бузғунчи, калит, Кирхгоф қонуни, криптографик тизим.

Маълумотларни муҳофаза қилиш қоидаларини бузувчининг мақсади

Маълумотларни муҳофаза қилиш қоидаларини бузувчининг мақсади ва уни

амалга ошириш услублари:
Руҳсат этилмаган маълумотларни беруҳсат олиш ва унга эга бўлиш, яъни маълумотларнинг маҳфий сақланиш қоидаларини бузиш.
Махфий ахборотлар тизимида фойдаланувчиларнинг бирор маълумот юзасидан ўзини жавобгарликдан (маъсулликдан) холос этиш учун ўзини бошқа фойдаланувчи сифатида ифодалаш ёки бошқа фойдаланувчининг ваколатидан фойдаланиш мақсадида:
ёлғон маълумотларни ташкиллаштириш;
ҳақиқий (қонуний) маълумотларни ўзгартириш;
рухсат этилмаган маълумотни олиш учун ўзини шу маълумотни олишга ваколати бўлган шахс сифатида ифодалаш;
ёлғон маълумотларни ахборот-коммуникация тизимига тушишига йўл қуйиб бериш ёки ёлғон маълумотларни тасдиқлаш.
Мавжуд бўлган маълумотларни ташкиллаштиришни рад этиш.
Қоидабузар томонидан ёлғон маълумотлар ташкиллаштирилиб, уни ахборот-коммуникация тизимининг бошқа бир фойдаланувчиси томонидан ташкиллаштирилган, деб ифодалаш.
Бирор аниқ кўрсатилган вақтда маълумот олувчига юборилмаган маълумотни юборилган, деб ифодалаш ёки маълумотни юборилган вақтни ёлғон кўрсатиш.
Ҳақиқатан ҳам олинган маълумотларни олинганлигини рад этиш ёки маълумотларнинг ҳақиқий олинган вақтини сохталаштириш.
Ахборотлар тизимидан фойдаланувчиларнинг ўзларига берилган ваколатланган маълумотларни ташкиллаштириш, узатиш, тарқатиш ва бошқа йўналишларда рухсат этилмаган ҳолда кенгайтириш.
Фойдаланувчиларнинг ваколатларини рухсат этилмаган тарзда ўзгартириш.
Маҳфий маълумотни маҳфий бўлмаган маълумотлар каби ифодалаш.
Алоқа тизими фойдаланувчиларининг ўзаро алоқа шаҳобчаларига руҳсат этилмаган ҳолда боғланиб, ундан олинган маълумотларни бошқа алоқа тизимларига мунтазам равишда тарқатиб туриш.
Алоқа каналидаги маълумотлар оқимини таҳлил қилиб, маълумотлар жамғармасининг тузилиш тартибига қараб, дастурий таъминот ва бошқа хосликларга кўра, фойдаланувчилар томонидан қандай маълумотлар қачон олинишини ғаразли мақсадларда ўрганиш.
Протокол (маълум тартиб ҳамда қоида) бўйича ҳар қандай ҳолларда ҳам махфий қолиши керак бўлган маълумотни маҳфийлигига путур етказган ҳолда, ушбу протокол маълумотлари софлигига шубҳа билан қараш.
Бирор яққол сезилмайдиган муолажа (процедура) билан маълумотларни муҳофаза қилиш алгоритми дастурига ўзгартиришлар киритиш.
Бошқа фойдаланувчиларни ёлғон маълумотлар асосида муҳофаза протоколини бузишга ундаш.
Протоколни бузиш билан ушбу муҳофаза протоколига ишончни йўқотишга олиб келадиган очиқдан-очиқ ҳатти-ҳаракатлар.
Ахборот тизимининг бошқа фойдаланувчиларига маълумотларни сифатли узатилишига, хусусан узатилаётган маълумотга яққол сезилмайдиган техник,

дастурий ва бошқа услублар билан ҳалақит берган ҳолда, узатилган маълумотнинг ҳақиқийлигини (аутентификациясини) рад этишга олиб келадиган ҳатти-ҳаракатлар.

Юқорида келтирилган муносабатлар (айниқса келишмовчилик) муаммоларини сабабларини мантиқан таҳлил қилишда ҳам асос қилиб олиниши мумкин. Месси ўзининг «Ҳозирги замон криптология фанига кириш», деб номланган илмий мақоласида қанчалик ишончли криптобардошли алгоритм яратилмасин, бари-бир ўз ечимини кутаётган бошқа криптографик масалалар келиб чиқиши мумкинлигини таъкидлаб, фойдаланувчиларга протокол бўйича ўз вазифаларини бажаришлари учун маҳфий калитни қандай узатиш ва олинган маълумотлар ҳақиқийлигига ишонч ҳосил қилиш масалалари тўғрисида тўхталади. Шундай масаланинг қўйилиши, калитларни ахборотлар тизими фойдаланувчиларига тақсимлашда келиб чиқадиган муаммоларни ҳал этувчи, очиқ калитли криптография йўналишининг вужудга келишига сабаб бўлди. Бундан ташқари, тизим фойдаланувчиларининг ҳар бири бутун тизим протоколи ичида ўзларининг қисм протоколи бўйича фаолият кўрсатаётганлигига ҳамда бошқа фойдаланувчиларнинг ҳам умумий тизим протоколини бузмаган ҳолда фаолият кўрсатаётганлигига ишонч ҳосил қилиниши, яъни умумий тизим протоколининг бардошлилик даражасига ишонч масалалари ҳам муҳим аҳамият касб этади. Содда қилиб ифодалаганда, ахборот-коммуникация тизимидаги ҳар бир фойдаланувчи шахсий калитининг муҳофазасини таъминлаш долзарб масаладир.

Криптографик алгоритмнинг бардошлилик даражаси қанчалик мустаҳкам бўлишидан қатъий назар, ахборотлар тизимининг фаолият жараёнларини бузиш усуллари мавжуд бўлиб, бу усуллар криптографик алгоритмнинг бардошлилик даражасига боғлиқ эмас. Масалан, калитларни тақсимлаш жараёни протоколининг камчилиги билан, бир нечта фойдаланувчилар ўз калитларини бир-бирларига ошкор қилган ҳолларда, криптографик алгоритимнинг маҳфийлигига зарар етказилиши мумкин. Умуман олганда ахборот-коммуникация тизими фойдаланувчиларининг протокол бўйича ишлаш жараёни камчилиги криптоалгоритм бардошлилик даражасининг сунъий равишда пасайишига олиб келади. Бундай камчиликларни олдини олишда протоколнинг бир қисми иккинчи қолган қисми тўғрисидаги маълумотни муҳофазаланган ҳолда ахборотлар тизими бўйича очиқ (маҳфий бўлмаган) алоқа тармоғи орқали узатилишини таъминлаш имконини бериши керак.

Криптотизмларга қўйиладиган талаблар

Маълумотларни криптографик услублар билан муҳофазалаш жараёнлари алгоритмик тиллар билан махсус криптобардошли алгоритмларни дастурлаш орқали ёки махсус техник аппаратлар ёрдамида амалга оширилади. Бунда дастурлаш услублари ўзининг қўлланилиши жиҳатидан қулайлиги билан ажралиб туради. Техник аппаратлардан фойдаланиш услублари катта қийматдаги моддий маблағни талаб қилсада, ўзининг самарадорлиги, қулайлиги, ишончлилиги ва шу каби хусусиятлари билан фарқланади.

Криптографик тизимлар хавфсизлиги криптографик алгоритм ва фойдаланилган калит хавфсизлигига асосланади. Заиф калит фойдаланилганлиги бардошли алгоритм фойдаланилган тақдирда ҳам криптотизим заифлигига олиб келади. Бундан ташқари, *Кирхгоф принципига* биноан криптографик тизим фақат калит номаълум бўлган тақдирдагина махфийлик таъминланади.

Ахборотлар тизими муҳофазасининг замонавий криптографик услубларига қуйидаги умумий талаблар қўйилади:

шифрланган маълумотни асл нусҳасига эга бўлиш имконияти фақат дешифрлаш калити маълум бўлгандагина мумкин бўлсин;

фойдаланилган шифрлаш калитини шифрматннинг бирор маълум қисми бўйича ёки унга мос келувчи очиқ қисми бўйича аниқлаш учун, бажарилиши зарур бўлган амаллар сони калитни аниқ топиш учун бажарилиши керак бўлган барча амаллар сонидан кам бўлмаслиги керак, яъни калит танлаб олиниши керак бўлган тўплам элементларининг сонидан кам бўлмаслиги керак;

шифрлаш алгоритмининг маълумлиги унинг бардошлилигига салбий таъсир кўрсатмаслиги керак;

калитнинг ҳар қандай даражадаги (озми, кўпми) ўзгариши шифрланган маълумотнинг жиддий ўзгаришига олиб келиши керак;

шифрлаш алгоритми таркибидаги элементлар ўзгармас бўлиши керак;

шифрлаш жараёни давомида маълумотларга киритиладиган қўшимча битлар (элементлар) шифрланган матнда (маълумотда) тўла ва ишончли холда қўлланилган бўлиши керак;

шифрлаш жараёнида қўлланиладиган калитлар орасида содда ва осонлик билан ўрнатиладиган боғлиқликлар бўлмаслиги керак;

калитлар таркиби тўпламидан олинган ихтиёрий калит ахборотнинг ишончли муҳофазасини таъминлаши керак;

криптоалгоритм дастурий ҳамда техник жиҳатдан амалий қўлланишга қулай бўлиб, калит узунлигининг ўзгариши шифрлаш алгоритмининг сифатсизлигига олиб келмаслиги керак.

Назорат саволлари

Бузғунчининг мақсади ва вазифаси.

Кирхгоф принципи нимадан иборат.

Криптографик тизимларга қўйилган умумий талаблар.

3 - маъруза

Мавзу: Криптографик тизимларнинг назарий ва амалий бардошлиги

Режа:

Криптографик бардошлилик.

Шеннон тамоилида криптографик тизимларнинг бардошлилиги.

Таянч атамалар: бардошлилик, исботланарли бардошлилик, сўзсиз, фараз бўйича, калит бардошлиги, амалий ва назарий бардошлилик.

Криптографик бардошлилик

Криптобардошлилик (бардошлилик) деб - криптотизимнинг ҳужумларга қарши тура олиш қобилиятига айтилади. Миқдорий жиҳатдан криптобардошлилик етарли эҳтимоллик билан криптотаҳлилчини муваффақиятга элтадиган энг яхши криптотаҳлил алгоритмининг мураккаблиги билан ўлчанади.

Криптоалгоритмлар улар хавфсизлигининг исботлана олувчанлик даражаси билан фарқланадилар.

Сўзсиз бардошли, исботланарли бардошли ва фараз бўйича бардошли криптоалгоритмлар мавжуд. Сўзсиз бардошли криптоалгоритмларнинг хавфсизлиги калитни очиш мумкин эмаслигини исботловчи теоремаларга асосланади. Масалан, Вернам шифри (бир марта фойдаланиладиган калитли) сўзсиз бардошлидир.

Исботланарли бардошли криптотизимларнинг бардошлилиги барча томонидан мураккаблиги тан олинган ва кўплаб математиклар ечишга уриниб еча олмаган яхши маълум математика масаласи (муаммо)нинг ечиш мураккаблиги билан аниқланади. Масалан, Диффи-Хеллман ёки Райвест-Шамир-Адлеман (RSA) алгоритмлари шу синфга оид. Буларнинг бардошлилиги дискрет логарифмлаш ва бутун сонни туб кўпайтувчиларга ажратиш масалаларининг мураккаблиги билан белгиланади.

Фараз бўйича бардошли криптоалгоритмлар бир ёки бир неча киши уриниб кўрган ва яхши ўрганилган масалаларга келтирилмайдиган хусусий математика масалаларига асосланади. Лекин, уларга катта эпчиллик хос бўлиб, криптоалгоритмлардан бўш жойлар пайқалганда улардан воз кечмай буни ҳисобга олиб яна қўшимча ишлаш кўп вақтни олмайди. Масалан, DES, ГОСТ 28147-89, FEAL, IDEA ва бошқалар. Афсуски, сўзсиз бардошли криптотизимлар амалиётда ноқулайдир.

Исботланарли бардошли криптоалгоритмларнинг хавфсизлиги улар асосига олинган масалаларнинг яхши ўрганилганлигидадир. Камчилиги зарурат туғилганда криптоалгоритмни тезкор тарзда қайта қуриш имконияти йўқлигидадир. Улар "қаттиқ" тизимлар бўлиб, уларнинг бардошлилигини оширишга математика масаласи ўлчамларини ошириш ёки алмаштириш орқали эришилади. Бу албатта, шифрланган аппаратдагина эмас, балки унга қўшни жиҳозларда ҳам ўзгаришлар занжирини юзага келтиради.

Фараз бўйича бардошли криптоалгоритмлар тегишли математика масалаларининг нисбатан кам ўрганилганлиги билан характерланади.

Калит бардошлилиги, калитсиз ўқишга бардошлилик, имитобардошлилик (тақлидга бардошлилик) ва ёлғон ахборотни тиқиштириш тушунчаларини фарқлаш лозим.

Калит бардошлилиги - бу энг яхши маълум алгоритм билан калитни топиш мураккаблигидир.

Имитобардошлилик - бу энг яхши маълум алгоритм ёрдамида ёлғон ахборотни рўкач қилишдир.

Шунга ўхшаш, криптоалгоритмнинг ўз бардошлилиги, протокол бардошлилиги, калитлар ҳосил қилиш алгоритми ва тарқатиш бардошлилиги фарқланади.

Бардошлилик сатҳи криптотаҳлилчининг имкониятларига ва фойдаланувчига боғлиқ.

Шеннон тамоилида криптографик тизимларнинг бардошлилиги

Шеннон криптографик тизимларнинг (системаларнинг) бардошлилиги масаласига икки хил нуқтаи назар билан қаради. Биринчидан, *назарий бардошлилик* масаласини кўрди: «Рақиб криптоаналитиги криптографик системанинг криптоанализи учун етали даражадаги техник ва бошқа керакли воситаларга эга бўлса ҳамда криптотаҳлил муддати чегараланмаган бўлса, ушбу криптографик тизимнинг бардошлилиги қандай?». Криптографик тизимнинг назарий бардошлилиги тушунчаси криптографик тизимларни баҳолашга аниқлик киритади, лекин бардошлилиги юқори бўлган криптотизимларнинг яратилиши нуқтаи назардан тушкунликка олиб келади. Амалда кўплаб ҳолларда назарий бардошли криптотизимларнинг яратилиши маҳфий калит ҳажмининг чексиз катта бўлиб кетиши масаласи билан боғлиқ. Шунинг учун Шеннон криптотизимларнинг *амалий бардошлилиги* масаласини ҳам кўрди, агар рақиб криптоаналитиги криптотаҳлил учун етарли даражадаги воситалар билан таъминланмаган бўлса ва анализ муддати чекланган бўлса криптотизимнинг бардошлилиги қандай? Шу ерда алоҳида таъкидлаб ўтамизки, очиқ калитли криптотизимлар амалий бардошли бўлиб, назарий бардошли бўлишлари шарт эмас.

Назарий саволлар

Сўзсиз бардошлилик тушунчаси.
Фараз бўйича бардошлилик тушунчаси.
Исботланарли бардошлилик тушунчаси.
Калит бардошлилиги.
Амалий ва назарий бардошлилик.

4 - маъруза

Мавзу: Криптографиянинг математик асоси
Режа:

Модуль арифметикаси.
Галуа майдони.
Эллиптик эгри чизиқлар.
Таянч атамалар: модуль, галуа майдони, нуқталарни қўшиш, нуқталарни иккилантириш, чекланган майдон.

Модуль арифметикаси

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

Нолдан фарқли бўлган *а* сони ва *в* сонлар Z –тўпламга тегишли, яъни $a,b \in Z$ бўлиб, $a \neq 0$ бўлсин., агарда шундай *с* сони мавжуд бўлиб, $в=ас$ тенглик бажарилса, у ҳолда, *а* сони *в* сонини бўлади дейилади.

Берилган *а* ва *в* сонларни бўлувчи бутун сон, уларнинг *умумий бўлувчиси* дейилади. Умумий бўлувчилар ичида энг каттаси *энг катта умумий бўлувчи* (ЭКУБ) дейилади ва (*а, в*) кўринишда белгиланади. Агарда *а* ва *в* сонларнинг энг катта умумий бўлучиси 1, (*а, в*)=1 бўлса, *а* ва *в* сонлар *ўзаро туб* дейилади.

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

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

$a=qn+r$, бу ерда $0 \le r < n$,

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

Бутун *а* ва *b* сонлари *модуль n бўйича таққосланадиган* дейилади, агарда уларни *n* га бўлганда қоладиган қолдиқлари тенг бўлса, ҳамда,

$a \equiv b \pmod{n}$

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

Қолдиқни ифодалаш учун ушбу

$b=a \bmod n$

тенгликдан фойдаланилади, ҳамда $b=a \bmod n$ тенгликни қаноатлантирувчи *b* сонини топиш *а сонини модуль n бўйича келтириш* дейилади.

Бирор *n* модул бўйича қўшиш, айириш ва кўпайтириш амалларига нисбатан қуйидаги коммутативлик, ассоциативлик ва дистрибутивлик муносабатлари

ўринли:
$(a+b)\bmod n=((a \bmod n)+(b \bmod n))\bmod n$,
$(a-b)\bmod n=((a \bmod n)-(b \bmod n))\bmod n$,
$(a\cdot b)\bmod n=((a \bmod n)\cdot(b \bmod n))\bmod n$,
$(a\cdot(b+c)\bmod n=(((a\cdot b) \bmod n)+(a\cdot c) \bmod n))\bmod n$.
Қуйида модул амаллари билан боғлиқ бир нечта мисоллар келтириб ўтилган:
$b=a \bmod n$ тенгликда a>n>0 бўлган ҳолда, натижани ҳисоблаш учун a ни n га бўлиб, қолдиғи олинади. Масалан, 12mod5=2; 15mod6=3;
$b=a \bmod n$ тенгликда n>0 ва a<0 бўлган ҳолда, a га токи йиғинда нолдан катта бўлгунга қадар n қўшилади. Масалан, -5mod6=1; -12mod5=3;
$b=a \bmod n$ тенгликда a каср сон бўлган ҳолда, тенглик қуйидаги (b*c)modn=1 тенгликка келтирилади. a=1/c га тенг бўлса, c бутун сон бўлади. Олинган тенгликдан b нинг ўрнига қиймат бериш орқали тенглик бажаралиши текширилади. Тенглик бажарилса, унда b га ўзлаштирилади. Бу усул кўп вақт талаб этади. Шунинг учун амалда Эвклиднинг кенгайтирилган аалгоритмининг хусусий ҳолидан фойдаланилади. Ушбу алгоритмнинг кетма-кетлиги қуйидагича:
(e*d)modn=1 тенгликда e ва n маълум бўлиб, d ни топиш талаб этилсин. Бунинг учун қуйидаги белгиланишлар киритилади a=n ва b=e. Учта элементдан иборат бўлган, учта тўплам қуйидагича тузилади:
U={a, 1, 0}, V={b, 0, 1}, T={U[1]modV[1], U[2]-[U[1]/V[1]]*V[2], U[3]-[U[1]/V[1]]*V[3]}. Бу ерда дастлабки қийматлардан U ва V тўпламлар ҳосил қилинади ва улар асосида T тўплам ҳисобланади. Агар T тўпламнинг биринчи элементи T[1]=1 га тенг бўлганда ҳисобланишлар тўхтатилади ва d=T[3] га тенг бўлади. Акс ҳолда, V тўпламнинг қийматлари U тўпламга, T тўпламнинг қийматлари V тўпламга ўзлаштирилади (U=V, V=T) ва улар асосида янгидан T тўплам ҳисобланади ва яна T[1]=1 тенгилиги текширилади. Ушбу кетма-кетлик T[1]=1 тенглик бажаррилгунга қадар амалга оширилади ва тенг бўлган ҳолда d=T[3] деб олинади ва ҳисоблашлар тўхтатилади.
Масалан, (d*8)mod23=1; a=23, b=8; У ҳолда тўпламлар: U={23, 1, 0}, V={8, 0, 1} ва T={23mod8, 1-[23/8]*0, 0-[23/8]*1}={7, 1, -2} Демак, T[1]=1 шарт бажарилмади. U=V={8, 0, 1}, V=T={7, 1, -2}, T={8mod7, 0-[8/7]*1, 1-[8/7]*(-2)}={1, -1, 3}. Демак T[1]=1 га тенг ва d=T[3]=3. Натижани: (3*8)mod23=1 тенглиги билан исботлаш мумкин.

Галуа майдони

Агар p –туб сон бўлса, у ҳолда 0 дан p-1 гача бўлган барча натурал сонлар тўплами {0, 1, 2, …, p-1} элементлари сони p та бўлган чекли майдон ташкил этади ва бу майдон *Галуа майдони* деб юритилади, ҳамда, $GF(p)$ кўринишда белгиланади. Галуа майдонида қўшиш, айириш, кўпайтириш ва нолдан фарқли бўлган элементга бўлиш амаллари аниқланган. Ҳамда, бу майдонда: қўшиш амалига нисбатан ихтиёрий $a \in GF(p)$ учун $a + 0 = a$ тенгликни қаноатлантирувчи 0 (ноль) элемент мавжуд; кўпайтириш амалига нисбатан иҳтиёрий $a \in GF(p)$ учун $a \cdot 1 = a$ тенгликни қаноатлантирувчи 1 (бир) элемент мавжуд; иҳтиёрий нолдан фарқли $a \in GF(p)$ учун $(a\cdot b)\bmod p = 1$

тенгликни қаноатлантирувчи $b \in GF(p)$ элемент мавжуд бўлиб, бу b элемент a элементга *тескари* элемент дейилади ва a^{-1} деб белгиланади; аниқланган амаллар коммутативлик, ассоциативлик ва дистрибутивлик хоссаларига эга.

Галуа майдони билан боғлиқ бўлган математик тушунча ва тасдиқлар криптографида кенг қўлланилади.

Криптографик масалаларни яна ҳам мураккаблаштириш мақсадида келтирилмайдиган (кўпайтувчиларга ажрамайдиган), коэфициентлари ушбу $\{0,1,\ldots,q\text{-}1\}$ (бу ерда q –туб сон) тўпламдан бўлган барча n –тартибгача кўпҳадлар тўпламидан фойдаланилади. Бу кўпҳадлар майдони $GF(q^n)$ деб белгиланади. Ҳамма амаллар характеристикаси n –тартибли келтирилмайдиган кўпҳад $p(x) \in GF(q^n)$ билан аниқланадиган майдонда бажарилади. Мисол учун, $GF(2^3)$ майдон ушбу: 0,1, x, $x+1$, x^2 , x^2+1, x^2+x, x^2+x+1 элементларни ўз ичига олади.

Берилган $GF(q^n)$ майдондан олинган $p(x)$ кўпҳаднинг коэффициентлари ўзаро туб бўлса, бу кўпҳад *ясовчи* бўлади, ҳамда, *примитив* (*содда*) дейилади. Примитив кўпҳадлар *чизиқли тескари боғлиқликга эга* бўлган силжиш регистрлари билан узвий боғлиқликга эга, яъни $q=2$ бўлганда $GF(2^n)$ майдонда бажариладиган амалларни чизиқли тескари боғлиқликка эга бўлган силжитиш регистларининг аппарат-техник қурилмалари ёрдамида тез бажариш мумкин. Ҳақиқатан ҳам, даражага кўтариш амалини бажариш $GF(q^n)_{q<2}$ майдондагидан кўра $GF(2^n)$ майдонда самаралидир. Бундан эса $GF(2^n)$ майдонда дискрет логарифмларни ҳисоблашнинг ҳам самарали эканлиги келиб чиқади.

Коэффициентлари иккилик саноқ системаси элементларидан иборат n – тартибгача бўлган барча кўпҳадлар тўплами $GF(2^n)$ –Галуа майдонида модуль - майдон характеристикаси сифатида $p(x)=x^n+x+1$ кўринишдаги уч ҳаддан иборат бўлган n –тартибли примитив кўпҳад олинади. Майдон характеристикасининг бундай танлаб олиниши, яъни x^n ва x ҳадлар оралиғидаги: x^{n-1} , x^{n-2} , …, x^2 ҳадларнинг йўқлиги модуль бўйича кўпайтириш амалининг самарали бажарилишини таъминлайди. Майдон характеристикасини ифодаловчи $p(x)=x^n+x+1$ кўпҳад примитив бўлмаса, амалларнинг бажарилиши мураккаблашади ҳамда криптографик самарадорликка эришилмайди. Мисол учун, бевосита ҳисоблаш натижасида, n нинг 1000 дан кичик бўлган: 1, 3, 4, 6, 9, 15, 22, 28, 30, 46, 60, 63, 127, 153, 172, 303, 471, 532, 865, 900) қийматларида $p(x)=x^n+x+1$ кўпҳад примитивлик хоссасига эга бўлади.

Эллиптик эгри чизиқлар

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

$$y^2 + a_1xy + a_3y = x^3 + a_2x^2 + a_4x + a_6 \qquad (4.1)$$

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

Эллиптик эгри чизиқ одатда E ёки E/K билан белгиланади ва эллиптик эгри чизиққа тегишли нуқталар, яъни (4.1) тенглама ечимлари шу эллиптик эгри чизиқнинг **аффин нуқталари** дейилади.

Бундан сўнг эллиптик эгри чизиқларнинг умумий каноник кўриниши ҳисобланган ушбу

$$y^2 = x^3 + ax^2 + bx + c, \qquad (4.2)$$

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

Юқорида келтирилган (4.2) кўринишдаги эгри чизиқ графигини чизиш учун

$$y = \sqrt{x^3 + ax^2 + bx + c}, \qquad (4.3)$$

чизиш ва Ox – ўқига нисбатан симметрик акслантириш лозим. Бу (4.3) берилган функция графигини чизиш учун эса квадратсиз ҳолидаги функция

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

графигини чизиб олиш керак бўлади. Функция графигининг Оx-ўқи билан кесишиш нуқталарини

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

тенгламанинг ечимларини топиш орқали аниқланади. Бу тенгламадан,

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

алмаштиришдан фойдаланиб,

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

келтирилган тенглама олинади, бу ерда $p = \frac{3b - a^2}{3}$, $q = \frac{2a^3}{27} - \frac{ab}{3} + c$.

$D = \left(p/3\right)^3 + \left(q/2\right)^2$ ифода дискриминант деб аталалиб, келтирилган тенгламанинг илдизлари сони дискриминант қийматининг ишорасига боғлиқ:

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

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

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

Эллиптик эгри чизиқларнинг рационал нуқталарини қўшиш

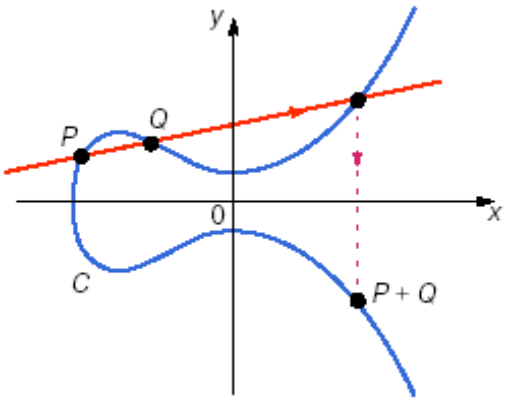
Ушбу

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

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

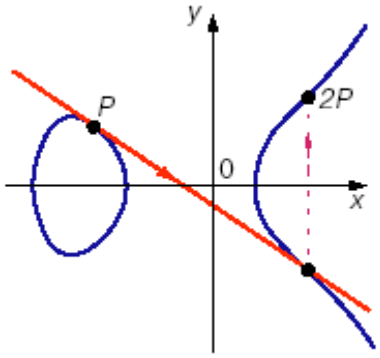
$B`(x_3, -y_3) = P(x_1, y_1) + Q(x_2, y_2)$

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



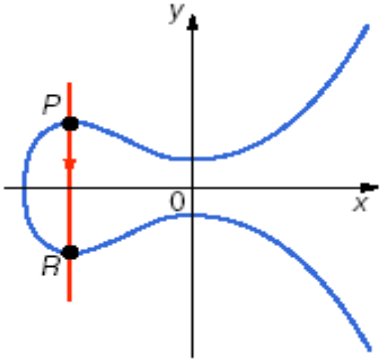
Бу график $x^3+ax^2+bx+c=0$ тенглама битта ечимга эга бўлган ҳол учун келтирилди.

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



Сўнгра, $3P$-ни топиш учун, $3P=P+2P$, шу каби $4P=P+3P$, $5P=4P+P$ ва ҳоказолар амалга оширилади.

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



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

Аниқланган майдонда эллиптик эгри чизиқ

$$y^2 mod p = (x^3 + ax + b) mod p$$

Бу ерда $4a^3 + 27b^2 \ mod p \neq 0, \quad x, y, a, b \in [0, p-1]$ - F_p майдонда аниқланган эллиптик эгри чизиқ, p – туб сон.

Аниқланган майдонда нуқталарни қўшиш ва иккилантириш:

Нуқталарни қўшиш

$$x_R = \lambda^2 - x_P - x_Q \ mod p$$
$$y_R = \lambda \ x_P - x_R \ - y_P \ mod p$$
$$\lambda = \frac{y_Q - y_P}{x_Q - x_P} mod p$$

Нуқталарни иккилантириш

$$x_R = \lambda^2 - 2x_P \ mod p$$
$$y_R = \lambda \ x_P - x_R \ - y_P \ mod p$$
$$\lambda = \frac{3x_P^2 + a}{2y_P} mod p$$

Назорат саволлари

Модуль арифметикасининг хусусиятлари.

Галуа майдони.

Эллиптик эгри чизиқларда нуқталарни қўшиш ва иккилантириш.

5 - маъруза

Мавзу: Криптографик тизимларнинг тавсифи. Классик криптотизимлар.

Режа:

Шифрлаш алгоритмлари классификацияси.
Ўрнига қўйиш шифрлари.
Ўрин алмаштириш шифрлари.
Энигма криптомашинаси.

Таянч атамалар: симметрик, ассиметрик, оқимли, блокли, ўрин алмаштириш, ўрнига қўйиш, бир алфавитли, кўп алфавитли, энигма машинаси.

Шифрлаш алгоритмлари классификацияси

Шифрлаш алгоритмлари асосларини очиқ маълумотни ифодаловчи алфавит белгиларини ёки белгилар бирикмаларини (уларни *шифр қийматлар* деб ҳам аталади) шифрмаълумотни ифодаловчи алфавит белгиларига ёки белгилар бирикмаларига (уларни *шифрбелгилар* деб ҳам аталади) акслантирувчи математик моделлар ташкил этиши юқорида таъкидланган эди. Шунинг учун ҳам шифрлаш алгоритмларини синфларга ажратишнинг бошланғич босқичи, улар негизидаги акслантириш турлари асосида амалга оширилади. Агар шифрлаш жараёнида очиқ маълумот алфавити белгилари шифр маълумот алфавити белгиларига алмаштирилса, бундай акслантиришга асосланган шифрлаш алгоритми *ўрнига қўйиш шифрлаш* синфига киради. Агар шифрлаш жараёнида очиқ маълумот алфавити белгиларининг ўринлари алмаштирилса, бундай шифрлаш алгоритми *ўрин алмаштириш шифрлаш* синфига киради. Кўриниб турибдики, ўрин алмаштириш шифрлаш алгоритмларида очиқ маълумотни ташкил этувчи алфавит белгиларининг маъноси шифр маълумотда ҳам ўзгармасдан қолади. Аксинча, ўрнига қўйиш шифрлаш алгоритмларида шифрмаълумотни ташкил этувчи алфавит белгилари маъноси очиқ маълумотни ташкил этувчи алфавит белгиларининг маъноси билан бир ҳил бўлмайди. Шифрлаш жараёнида ўрнига қўйиш ва ўрин алмаштириш акслантиришларининг комбинацияларидан биргаликда фойдаланилса, бундай шифрлаш алгоритми *композицион шифрлаш* туркумига киради. Демак, шифрлаш алгоритмлари акслантириш турларига қараб *ўрнига қўйиш, ўрин алмаштириш* ва *композицион шифрлаш* синфига бўлинади.

Умумий тасаввурга кўра, ўрнига қўйиш шифрлаш алгоритмлари акслантиришларининг математик моделлари кўп қийматли функциялар билан ифодаланади. Бундай ҳолат дешифрлаш жараёнида турли ноқулайликларни келтириб чиқаради. Шунинг учун бир қийматли (тескариси мавжуд бўлган) функциялар билан ифодаланувчи акслантиришларни қўллаш қулайлик туғдиради. Шундай қилиб, табиий равишда, ўрнига қўйиш шифрлаш алгоритмлари *бир қийматли* ва *кўп қийматли шифрлаш* синфига бўлинади. Бир қийматли шифрлаш алгоритмларида очиқ маълумот алфавити белгиларининг ҳар бирига шифр маълумот алфавитининг битта белгиси мос

қўйилади. Кўп қийматли шифрлаш алгоритмларида очиқ маълумот алфавити белгиларининг ҳар бирига шифр маълумот алфавитининг иккита ёки ундан ортиқ чекли сондаги белгилари мос қўйилади, яъни очиқ маълумот алфавитининг бирор x_i белгисига шифр маълумот алфавитининг чекли $y_{i1}, y_{i2}, ..., y_{it}$ тўпламдан олинган бирор y_{ij} , $1 \le j \le t$, белгиси мос қўйилади.

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

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

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

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

Шифрлаш жарёнида очиқ маълумот алфавити белгилари ёки алфавит белгилари бирикмалари бирор амал бажариш билан шифрмаълумот алфавити белгилари ёки уларнинг бирикмаларига алмаштирилса, бундай шифрлаш алгоритми *гаммалаштирилган шифрлаш* синфига киради.

Ўрнига қўйиш шифрлари

Шифрлаш алгоритмлари очиқ маълумот алфавити белгиларини шифрмаълумот белгиларига акслантиришдан иборат эканлиги такидланди. Акслантиришлар функциялари (калит деб аталувчи номаълум) параметрга боғлиқ ҳолда: жадвал ва аналитик ифода кўринишларида берилиши мумкин. Ўрнига қўйиш шифрлаш алгоритмларининг дастлабки намуналари бўлган тарихий шифрлаш алгоритмларининг деярли ҳаммаси жадвал кўринишида ифодаланади. Ўрнига қўйиш шифрлаш алгоритмларининг умумий хусусиятини ҳисобга олиб, бу синфдаги алгоритмларни жадвал кўринишда

қуйидагича ифодалаш мумкин:

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

Ўрнига қўйиш шифрлаш алгоритмлари, уларнинг асосини ташкил этувчи акслантиришнинг бир қийматли ёки кўп қийматлилигига кўра, бир қийматли ва кўп қийматли синфларга бўлинади.

Агар ўрнига қўйиш шифрлаш алгоритмида очиқ маълумот алфавити белгиларининг ҳар бирига шифр маълумот алфавитининг битта белгиси мос қўйилса, бундай алгоритм бир қийматли ўрнига қўйиш шифрлаш алгоритми синфига киради.

Кўп қийматли шифрлаш алгоритмларида очиқ маълумот алфавити белгиларининг ҳар бирига шифр маълумот алфавитининг икки ёки ундан ортиқ чекли сондаги белгилари мос қўйилади, яъни очиқ маълумот алфавитининг бирор x_i белгисига шифр маълумот алфавитининг чекли $\{y_{i1}, y_{i2}, ..., y_{it}\} \subseteq \{y_1, y_2, ..., y_M\}$ тўпламдан олинган бирор y_{ij} , $(1 \le j \le t)$, белгиси мос қўйилади.

Ўрин алмаштириш шифрлари

Ўрин алмаштириш шифрлаш алгоритмларининг асосий хусусияти очиқ маълумот ва шифрмаълумот алфавити белгиларининг бир хиллигидадир, яъни шифрмаълумотни ташкил этувчи белгиларнинг маъноси мос келувчи очиқ маълумотдаги белгиларнинг маъноси билан бир хил бўлади. Ҳақиқатан ҳам, ўрин алмаштириш шифрлаш жараёнида очиқ маълумот алфавити белгилари ўринлари алмаштирилиши натижасида шифрмаълумот ҳосил қилинади. Шунинг учун ҳам бундай шифрлаш алгоритмларининг калити узунлиги, умуман олганда, шифрланиши керак бўлган маълумот узунлигига, яъни очиқ маълумот ташкил этувчи алфавит белгиларининг сонига тенг. Бундан ташқари, очиқ маълумотни ташкил этувчи алфавит белгиларининг частотавий хусусиятлари тўлалигича шифрмаълумотга ўтади. Бундай ҳолатлар амалий тадбиқ имкониятларини чеклайди. Шундай бўлсада уларнинг самарали тадбиқларини таъминлашга қаратилган синфлари мавжуд. *Йўналишли ўрин алмаштириш* синфидаги шифрларнинг қўлланилиши амалда кўп тарқалган. Бундай шифрлаш алгоритмлари бирор геометрик шаклга асосланган бўлади. Очиқ маълумот блоклари геометрик шаклга бирор траектория (узлуксиз из) бўйича жойлаштирилади. Шифрмаълумот эса бошқа траектория бўйича ҳосил қилинади. Геометрик шакл сифатида (nx m) ўлчамли жадвал олиб, унинг биринчи сатри бошидан бошлаб очиқ маълумот белгиларини чапдан ўнгга кетма-кет жойлаштириб, сатр тугагач иккинчи

сатрга, очиқ маълумот белгиларини ўнгдан чапга кетма-кет жойлаштириб, бу сатр тамом бўлгач, кейинги сатрга олдингисига тескари йўналишда жойлаштирилади ва ҳоказо. Охирида тўлмай қолган сатр ячейкалари очиқ маълумот алфавитидан фарқли бўлган белгилар билан тўлдирилади. Сўнгра, очиқ маълумотни жойлаштириш тартибидан фарқли бўлган бирор йўналиш танлаб олиниб, шу йўналиш асосида шифрмаълумот ҳосил қилинади. Шифрмаълумот ҳосил қилиш йўналиши калит вазифасини бажаради.

Энигма криптомашинаси

Энигма шифри дастаб немис нацислари томонидан II жаҳон уруши давомида фойдаланилган. Ҳарбий Энигма машинаси Артур Шербуюс томонидан сотиш мақсадида ишлаб чиқилган. Энигма 1920 йилда патентланган, аммо, у вақт ўтиши билан шакллантирилган ва Немис ҳарбийлар учун яратилган версия ҳақиқий версиядан жиддий фарқ қилади. Ҳақиқатда, “Энигма” шифр машиналарнинг оиласини намойиш этади, аммо, “бир Энигма” фақат Немис ҳарбий соҳаси учун махсус таклиф этилган ва уни биз бу бўлимда таҳлил этамиз.

Тақрибан 100 000 та Энигма машинаси ишлаб чиқарилган ва улардан 40 000 таси II жаҳон уруши даврига тўғри келади. Биз таҳлил этадиган Энигма варианти Немис армияси томонидан II жаҳон урушида фойдаланилган. Қурилма мақсадли урушга тегишли хабарларни юбориш ва юқори даражадаги тизимли алоқа учун фойдаланилган.

Энигма машинаси союзлар томонидан бузилган ва бу зукколикни ULTRA деб номлашган. Немислар Энигмани бузилмаслигига қатий ишонишган ва улар ундан муҳим алоқаларда фойдаланишни давом эттирганлар. Албатта, уруш натижаларида Энигма дешифрланганлигига боғлаб бўлмайди, аммо, Энигмани бузиш натижасида Европадаги уруш бир неча йилга қисқарди ва юз минглаб инсонларни ҳаёти сақлаб қолинди.

Энигма машинаси иккинчи бўлимдаги 5.1 – расмда келтирилган. Эсда тутинг, албатта, тугмалар тўплами, механик ёзиш ва белгиларнинг ёрқин – шчитдан ташкил топган. Эски кўринишдаги телефон коммутаторига ўхшаш бўлиб, олд панелида белгилар жуфтини боғловчи кабеллар мавжуд. Бу коммутатор немисча ном, *stecker* деб номланган. Бундан ташқари, бу ерда, яна учта ротор мавжуд бўлиб, у машинанинг тепаси яқинида кўриниб турибти.

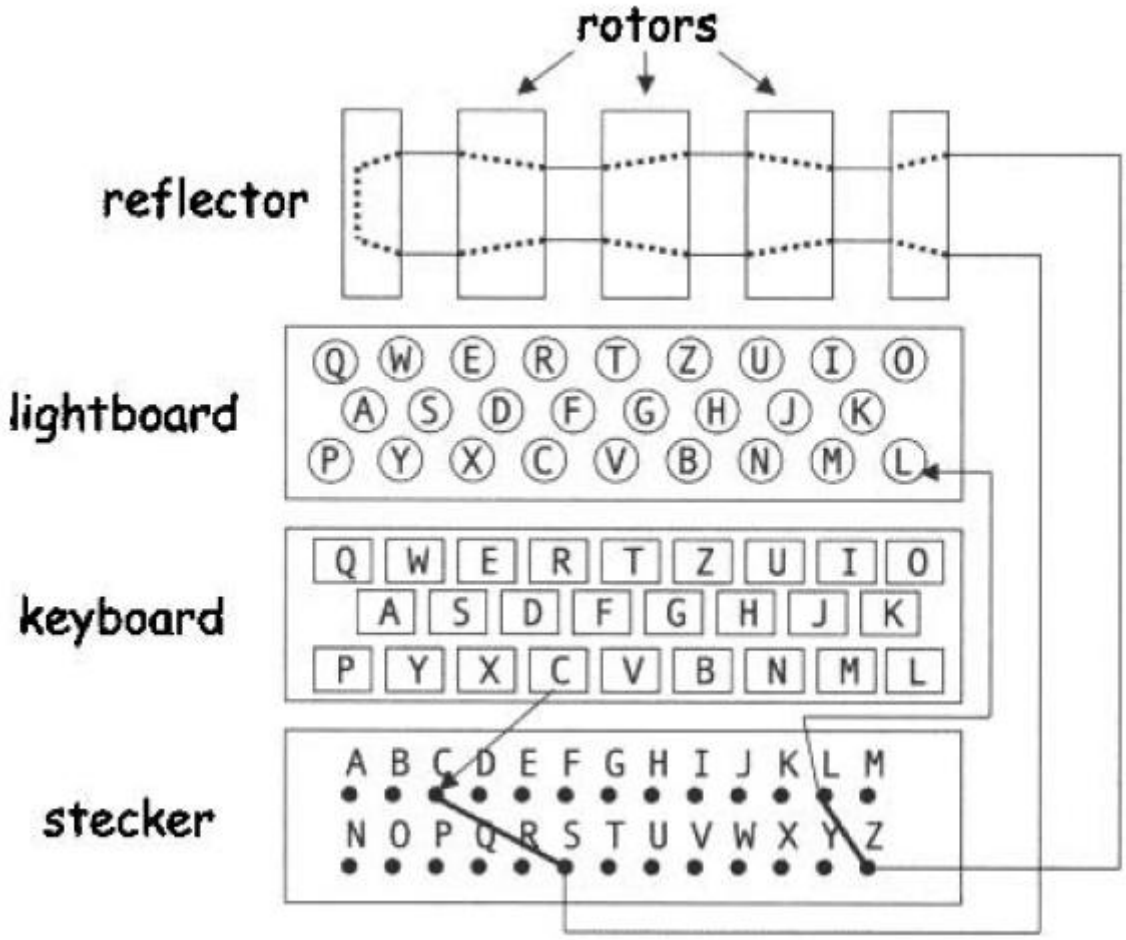
5.1 - расм. Энигма машинаси

Хабарни шифрлашдан олдин, оператор қурилмани созлаган. Дастлабки созланиш ўз ичига роторларни турли созланишларини ва стекерни кабели уланишини олган. Дастлабки созланиш калитни ташкил этган.

Машина созлангандан сўнг, тугмалар тўплами орқали хабар ёзилади ва унга мос шифрматн ёрқин – шчитда намаён бўлади. Шифрматн белгилари ёрқин – шчитда кўриниши билан ёзиб борилади ва кетма – кетлик одатда овоз ёки радио кўринишида ўтказилган.

Дешифрлаш учун, қабул қилувчи машинани юборувчи каби бир – хил сошлаши шарт. Шундан сўнг, шифрматн тугмалар тўплами орқали киритилганда, мос очиқ матн ёрқин – шчитда намаён бўлади.

5.2 – расмда Энигманинг криптографик муҳим ташкил этувчилари акс эттирилган. Бу ташкил этувчилар ва уларнинг ўзаро алоқаси қуйида таҳлил эттирилган.



5.2 – расм. Энигма диаграммаси

Шифрлаш учун, очиқ матн белгилари тугмалар орқали киритилади. Бу белгилар дастлаб стикер орқали ўтади ва кейин навбат билан ҳар бир роторлардан ўтади, рефлектордан ўтади, ҳар бир ротордан қайта ўтади, стикердан қайта ўтади ва ниҳоят шифрматн белгилари ёрқин – шчитда намоён бўлади. Ҳар бир ротор, шунингдек, рефлектор – 26 – ҳарфни алмаштириш учун кабел билан уланган. Роторлар криптографик элементлар сифатида қуйида таҳлил қилинган.

5.2 – расмда намойиш этилган мисолда, очиқ матн C белгини киритилади ва стекер кабели C ни S га боғланганлиги учун, S га алмаштирилади. Кейин, S роторлар, рефлектор орқали ўтади ва роторлар орқали қайтади. Барча роторлар ва рефлекторнинг натижаси алфавитни алмаштиришдан иборат. 5.2 – расмдаги мисолда, S белгиси Z белгисига алмашган ва стекер L ва Z ни боғлаганлиги сабабли, Z белгисини L га алмаштиради.

Биз Энигмада турли ўзгаришлар учун қуйидаги белгиланишлардан фойдаланамиз:

R_r – ўнг томондаги ротор;

R_m – ўртадаги ротор;

R_l – чап томондаги ротор;

T – рефлектор;

S - стекер.

Бу белгиланишлар орқали, 5.2 – расмдан биз қуйидаги кўришимиз мумкин:

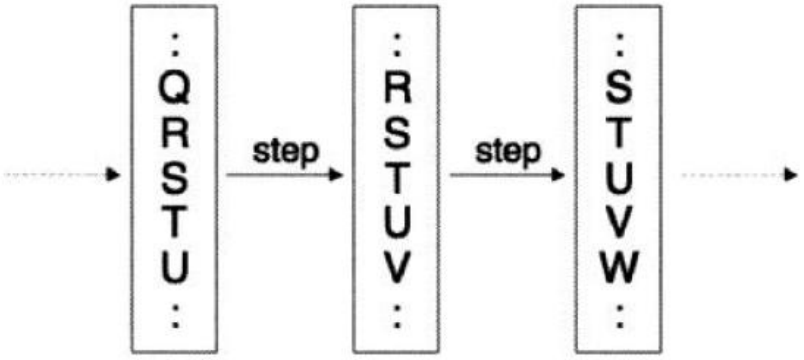
$$y = S^{-1}R_r^{-1}R_m^{-1}R_l^{-1}TR_rR_mR_lS\ x\ =\ R_rR_mR_lS^{-1}T\ R_rR_mR_l\ S\ x\ ,$$

Бу ерда х очиқ матн белгиси ва у унга мос шифрматн белгиси.

Агар бу Энигма юқорида айтилганидек бўлса, у ҳолда у дастлабки созланиш орқали ўрин алмашадиган мақталган содда ўрнига қўйиш шифридан ортиқ ҳеч нарса эмас. Бироқ, ҳар тугмача босилганда, ўнг томондаги ротор бир ҳолатга юради ва қолганлаги милометрга ўзшаш ҳаракат қилади. Яъни, ўртадаги ротор ўнг томондаги роторнинг ҳар 26 қадамида бир қадамга юради ва чапдаги ротор ўртадаги роторнинг ҳар 26 қадамида бир қадам юради. Рефлектор белгиларни ўринини алмаштирганлиги, аммо, айлантирмайди, сабабли у маҳкамланган ротор каби кўринади. Натижада, босилган ҳар бир ҳарф алмаштирилади. Шуни эсда тутиш керакки, милометр тасири натижасида, R_r, R_m, R_l ларнинг ўрин алмашиши турлича, аммо, T ва S ники эмас.

5.3 – расмда Энигманинг ягона ротор қадами акс эттирилган. Бу мисол ротор қадами йўналишини кўрсатади. Операторнинг нуқтаи – назаридан, белгилар алфавит тартибида кўринган.

Энигма ўрнига қўйиш шифри бўлиб, ҳар бир белги ўрни алмаштирилган алфавит асосида шифрланади. Аммо, Энигма хох шифрлашда бўлсин, ҳоҳ дешифрлашда бўлсин содда кўринишдан йироқ, милометр тасирида ўрин алмашиш амалга оширилади. Бу шифрлаш кўп алфавитли ўрнига қўйиш сифатида маълум. Энигма учун, бўлиши мумкин бўлган “алфавитлар” (ўрин алмашинишлар) сони жуда кўп.



5.3 – расм. Энигма ротори

ЭНИГМА КАЛИТ МАЙДОНИ. Энигманинг криптографик муҳим ташкил этувчиси бу – стикер, учта ротор ва рефлектор. Энигма калити бу ташкил этувчиларнинг дастлабки сошланиши бўлиб, улар шифрлаш ёки дешифрлаш учун фойдаланилади. Турли созланишларни ўз ичига олган калит:

Роторларнинг танлаш;

Икки ўнг томондаги роторларнинг ҳар биридаги ҳаракатланувчи ҳалқанинг ҳолати. Бу ҳалқа роторнинг ташқи қисмига (26 та ҳар билан белгиланган) ҳалқанинг ички қисми (ҳақиқий ўрин алмаштириш боғланган) билан биргаликда айлантиришга рухсат беради. Бу ҳалқанинг айлантириш натижасида кўрсаткич милометр натижасида ротордаги мос ҳарфга силжийди.

Ҳар бир роторнинг дастлабки ҳолати.

Рефлекторни танлаш.

Юқорида эслатиб ўтилганидек, ҳар бир ротор алфавитдаги 26 та ҳарфнинг ўрин алмашишини амалга оширади. Ҳаракатланувчи ҳалқа эса, белгига мос ҳолда, 26 та ҳолатдан бирига ўрнатилиши мумкин.

Ҳар бир ротор дастлаб ротордаги 26 та ҳолатдан бирига ўрнатилиши мумкин, бу ҳолатлар A дан Z гача белгиланган. Стикер эски кўринишдаги телефон коммутатори каби бўлиб, 26 та чуқурчадан иборат ва улар ҳарфлар билан белгиланган. Стикерда 0 – 13 тагача кабел мавжуд ва ҳар бир кабел бир жуфт ҳарфларни бир – бирига улайди. Рефлектор 26 та белгиларни ўрин алмашишини таъминлайди, белги бўлмаганлар эса ўзига алмаштирилади ва натижада қисқа айланиш ҳосил бўлади. Натижада, рефлектор 13 та кабелга эга стикерга тенг бўлади.

Учта ротор бўлганлиги учун ва уларнинг ҳар бири 26 та ҳарфнинг алмашинишинишидан иборат бўлганлиги учун, бу ерда танлаш ва машинада роторларни жойлаштириш учун:

$26!*26!*26!\approx 2^{265}$

та йўл мавжуд бўлади. Бундан ташқари, йўллар сони иккита ҳаракатланувчи ҳалқаларга ўрнатилади ва бу тасир $26*26\approx 2^{9.4}$ га тенг бўлади.

Ҳар бир роторнинг дастлабки ҳолати 26 тадан бирига ўрнатилиши мумкин ва шунинг учун $26*26*26\approx 2^{14.1}$ йўлдан фойдаланиб роторни созлаш мумкин. Бундан ташқари, бу рақам турли дастлабки ҳолатлар бир хил стандарт ҳолда бошқа роторлар учун тенг бўлганлиги учун бизни ҳисобимизга тенг бўлмайди. Яъни, агар бир ҳар бир роторни A га ўнатилган деб фараз қилсак, у ҳолда, бирор роторни айтайлик B га созланганлиги қолган роторларни A га созланганлигига еквивалент. Натижада, олдинги парагрифда келтирилган факторлашдан олинган 2^{265} қиймат барча дастлабки ротор ҳолатларини ўз ичига олади.

Ниҳоят, биз стикерни кўриб чиқсак. Келинг, стикердаги p та кабелларни уларнишлар сонини $F(p)$ деб белгилайлик. Иккинчи муаммодан келиб чиқиб, бизда мавжуд уланишлар

$$F\ p\ = \begin{matrix} 26 \\ 2p \end{matrix} \quad 2p-1 \quad 2p-3 \quad \ldots\ldots 1$$

$F\ p$ нинг барча қийматлари 6.1 – жадвалда келтирилган.

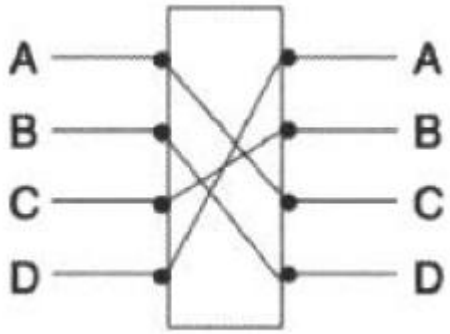
5.1 – жадвал

Стикернинг комбинациялари сони

$F(0)=2^{0}$	$F(1)\approx 2^{8.3}$
$F(2)\approx 2^{15.5}$	$F(3)\approx 2^{21.7}$
$F(4)\approx 2^{27.3}$	$F(5)\approx 2^{32.2}$
$F(6)\approx 2^{36.5}$	$F(7)\approx 2^{40.2}$
$F(8)\approx 2^{43.3}$	$F(9)\approx 2^{45.6}$
$F(10)\approx 2^{47.1}$	$F(11)\approx 2^{47.5}$
$F(12)\approx 2^{46.5}$	$F(13)\approx 2^{42.8}$

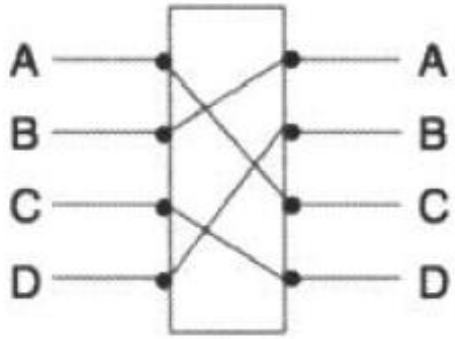
Жадвалда келтирилганидек, бизда $2^{48.9}$ дан ортиқ стикернинг комбинацияси мавжуд. Максимум кўриниш 11 та кабел орқали $F(10)\approx 2^{47.1}$ га тенг бўлади. Юқорида эслатиб ўтилганидек, Энигманинг рефлектори 13 кабелга эга стикерга эквивалент. Натижада, бу ерда турли $F(13)\approx 2^{42.8}$ рефлектор мавжуд.
Барча бу натижаларни комбинациясидан келиб чиқиб, Энигманинг калит майдони тақрибан қуйидагига тенг.
$2^{265} * 2^{9.4} * 2^{48.9} * 2^{42.8} \approx 2^{366}$
Яъни, назарий томондан Энигманинг калит майдони 366 битга тенг. Ҳаттоки, замонавий шифрлар камдан – кам ҳолларда 256 битдан узун калитдан фойдаланади. Бу Немислар учун Энигмада буюк – аммо охир оқибатда асоссиз конфиденциялликка эга бўлган кўрсаткичдир.
Бундан ташқари, калитларнинг бу астрономик сони адаштирувчидир. Биринчи муаммодан, биз Немис ҳарбийлари томонидан фойдаланилган Энигма машинасининг калитларини амалий томондан 2^{77} га тенглигини кўришимиз мумкин. Шундай бўлсада, бу катта сондир ва 1940 йилдаги технология орқали калитларни тўлиқ танлашни амалга ошириб бўлмасди. Маданиятли дунё халқлари бахтига эса, бу ҳол учун қисқартирилган таҳдидлар мавжуд. Аммо, биз таҳдидни таҳлил қилишдан олдин, роторни криптографик элемент сифатида қисқача кўриб чиқсак.
РОТОРЛАР. 20 асрнинг биринчи ярми давомида кўплаб шифрлаш машиналарида роторлар фойдаланилган – Энигма буларнинг ичида жуда ҳам машҳури, аммо, бундан ташқари шифр машиналар ҳам мавжуд. Роторли шифр машинасига бошқа қизиқарли мисол сифатида Америкда II жаҳор урушида яратилган Сигабани олишимиз мумкин. Сигаба шифр машинаси Энигмага қараганда юқори хавфсизликни таъминлайдиган ажойиб лойихага эга.
Крипто-муҳандислик нуқта – назиридан, роторнинг ажойиблиги содда электро-механик қурилмадан бардошли усулда катта сондаги алоҳида ўрин алмаштиришларни ҳосил қилишнинг мумкинлиги. Бу қариш компьютер эрасидан олдинги эра учун муҳим эди. Шуниси аниқки, Энигма ҳақиқатда қурилманинг мустаҳкам қисми бўлган ва уруш ҳолатларида кенг фойдаланилган.
Қурилмавий роторлар тушунишга осон, аммо, турли ротор ҳолатларига мос ўрин алмаштиришларни ифодалашда бир оз ноқулай.
Соддалик учун, тўртта, A дан D гача ҳарфдан иборат роторни қарайлик. Сигнални чапдан – ўнга келишини фараз қилсак, 6.3 – расмда ифодаланган ротор ABCD киришни CDBA га алмаштиради, яъни, A белги C га, B белги D га, C белги B га ва D белги A га алмаштирилади. Тескари алмаштириш, бизнинг ҳолда DCAB, чапдан – ўнга ротор ўрнига ўнгдан – чапга йўналиш орқали ўтади. Бу хусусият фойдали бўлиб, бир қурилмада ҳам шифрлаш ҳам дешифрлаш имконини беради. Энигма бу қадамни янада ривожлантирган. Яъни, Энигма машинаси ўзининг тескарисига эга, яъни, бир турдаги машина бир хил созланиш билан шифрлаш ёки дешифрлаш учун фойдаланилади.
Фараз қилайлик, 5.4 – расмдаги ротор ягона қадамга эга. Этибор беринг, бу ерда роторнинг ўзи айлантириш учун тўртбурчак шаклида ифодаланган,

ротор четларида электр контакрлар йўқ. Бу мисолда, фараз қилайлик ротор “юқорига” ҳаракатланади, яъни, В белги А ни ўрнига ва ҳак. тартибда, А дан D гача айлантирилади.



5.4 – расм. Ротор

5.4 – расмдаги роторнинг силжиши 5.5 – расмда ифодаланган. Натижавий силжитилган алмаштириш CADB га тенг, балки, ҳақиқий алмаштириш CDBA га тенглигини кўриш бир мунча қийиндир.



5.5 – расм. Ҳаракатланган ротор

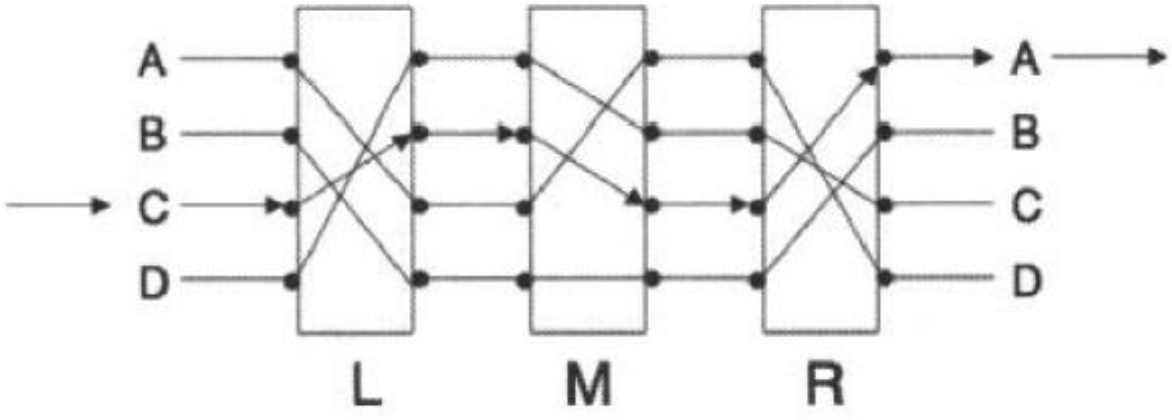
Одатда, ўрин алмашинишнинг ротор силжишини ҳисоблаш мураккаб эмас. Муҳим нуқта шундаки, силжишдаги аралашишни билиш. Масалан, CDBA ўрин алмашинишида, аралашиш қуйидагича: А ҳарфи С га, яъни, иккита қадамда аралашди, В ҳарфи D га алмашти, яъни, иккита қадамда аралашди, С ҳарфи эса В алмашди ва учта қадам аралашди, D ҳарфи эса А га алмашди, яъни, битта қадамда. Яъни, алмаштиришдаги қадамлар (2,2,3,1) га тенг. CADB алмаштириш учун эса бу қадамлар (2,3,1,2) га тенг ва у 6.4 – расмда келтирилган.

Бундан ташқари, физик роторлар жуда оддий қурилма, аммо, абстракт ҳолда баъзи тушунмовчиликлар мавжуд.

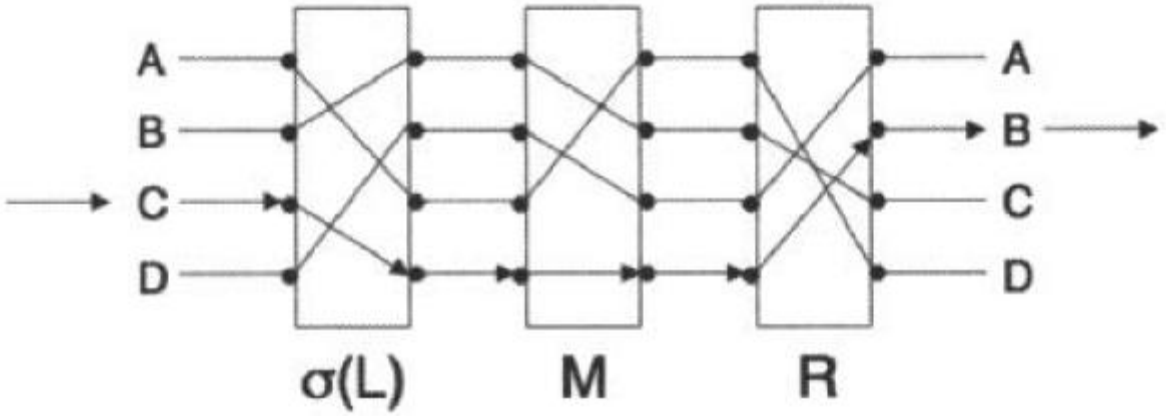
Юқорида эслатиб ўтилганидек, роторнинг бир афзаллиги шундаки, улар катта сондаги ўрин алмашинишларни ҳосил қилиш учун содда электро – механик воситаларни таъминлайди. Ўрин алмашинишлар сонини ортириш учун, роторлар комбинациясини ортириш керак. Масалан, 5.6 – расмда, С ҳарфи А га алмашди, L роторнинг силжиши σ(L) орқали ифодаланади ва С белгини В га алмашиниши 5.7 – расмда акс эттирилган. Яъни, битта роторнинг силжиши умумий алмашиниш ўзгаришига таъсир қилади.

Учта ротордан иборат схемада, биз учта ротор учун 64 ни ўрнатиш орқали

содда силжитиш томонидан ABCD ҳарфларнинг 64 та алмашинишининг циклини ҳосил қилиш мумкин.



5.6 – расм. Учта ротор



5.7 – расм. L роторнинг қадами

Албатта, барча алмашинишлар бир хил бўлмайди, яъни, ABCD, тўрт ҳарф учун 24 та алмашиниш мавжуд. Шунингдек, роторлар учун турли дастлабки созланишларни танлаш орқали, биз турли алмаштириш кетма – кетлигини ҳосил қилишимиз мумкин. Бир ротордаги каби, бир нечта роторлар учун ҳам уларни тескарисини аниқлаш осон, бу роторлар орқали сигнални тескари тартибда юбориш орқали амалга оширилади. Бу тескари алмаштиришлар дешифрлаш жараёни учун керак.

Назорат саволлари

Шифрлаш алгоритмларининг классификацияси.
Ўрин алмаштириш шифрлари.
Ўрнига қўйиш шифрлари.
Энигма машинаси.

6 - маъруза

Мавзу: Симметрик криптографик алгоритмлар. Блокли шифрлаш алгоритмлари.

Режа:

Блокли шифрларни яратиш усуллари.
Блокли шифрлаш режимлари.
Замонавий блокли шифрлаш усуллари.

Таянч иборалар: фейстел тармоғи, алмаштириш-ўрнига қўйиш тармоғи, Lai-Massey тармоғи, шифрлаш режимлари, Camellia, DES, AES шифри.

Блокли шифрларни яратиш усуллари

Блокли шифрлаш алгоритмлари криптографик алгоритмлар орасида кенг тарқалган алгоритм тури бўлиб, моҳият жихатдан маълум узунликдаги маълумот битлари устида қайта-қайта амаллар бажарилиш орқали амалга оширилади. Блокли симметрик шифрлаш алгоритмлари маълумотни махфийлигини таъминлашда кенг фойдаланилиб, бошқа шифрлаш алгоритмларига қараганда ўзининг тезкорлиги ва криптобардошлиги билан ажралиб туради.

Блокли симметрик шифрлаш алгоритмларига хос бўлган хусусиятлардан бири бу – маълум узунликдаги маълумот блоки устида қайта-қайта амаллар бажарилиши бўлиб, бу *раунд* деб аталади. Ушбу раунд функцияси ўзгармас саналиб, ҳар раундда кирувчи параметрлар ўзгариши натижасида маълум марта амалга оширилади.

Блокли симметрик шифрлаш алгоритмлари раунд функцияларида ARX (add-rotate-xor) амалларидан фойдаланилади. Ушбу амаллар:

Модул асосида қўшиш;

Суриш (циклик суриш, мантиқий суриш);

XOR амали.

Бундан ташқари блок симметрик шифрлаш алгоритмларида махсус алмаштириш жадвалларидан кенг фойдаланилади.

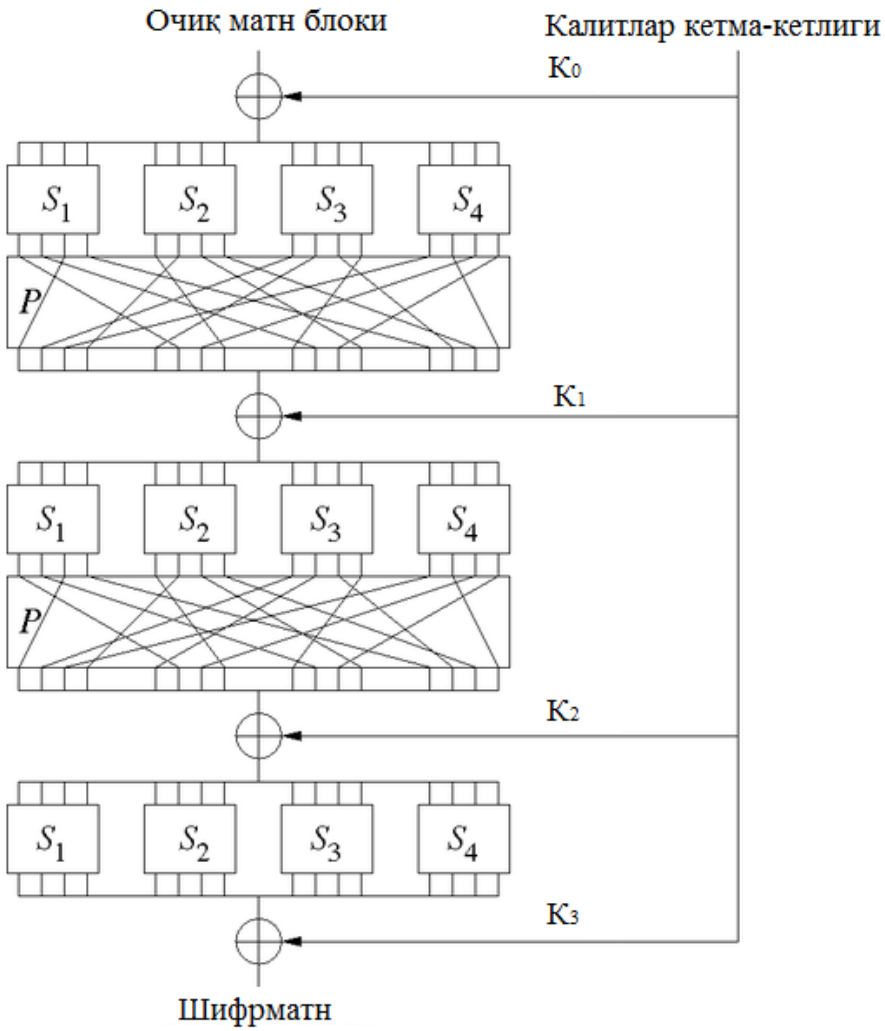
Ҳозирда симметрик блокли шифрлаш алгоритмлари амалда кенг қўлланилиб, уларни яратиш қуйидаги асосларга бўлинади:

Алмаштириш-ўрнига қўйиш тармоғига асосланган (Substitution-permutation networks, SPN);

Фейстел тармоғига асосланган шифрлаш алгоритмлари;

Lai-Massey тармоғига асосланган шифрлаш тизимлари.

Алмаштириш-ўрнига қўйиш тармоқлари. Бу турдаги симметрик блокли шифрлаш алгоритмлари янгидан асос солинган бўлиб, амалда кенг қўлланилади. Маълум узунликдаги маълумот блоклари ва ҳосил қилинган калит жуфти асосида маълум раундлар ичида амаллар бажарилади.



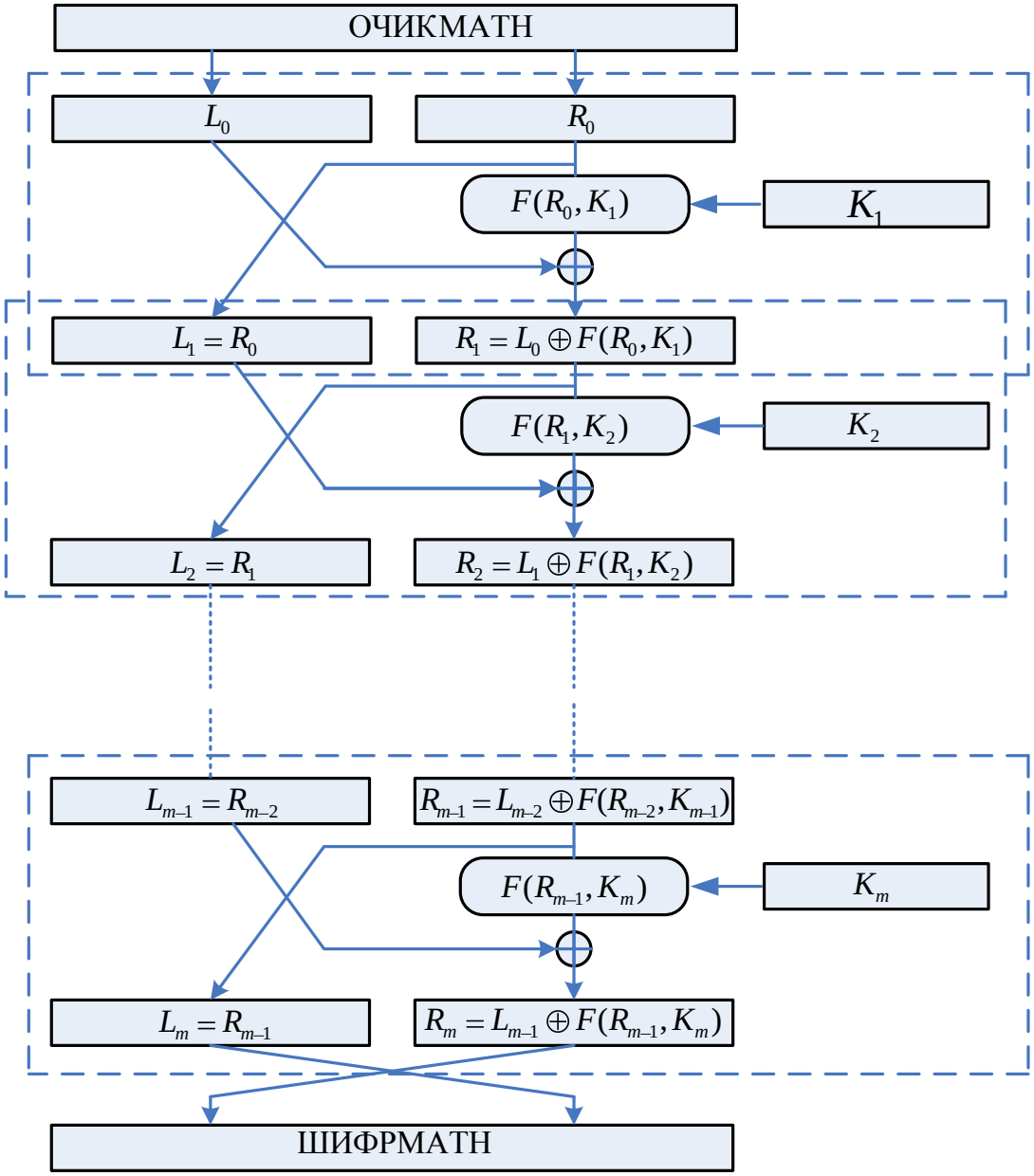
6.1-расм. SPN тармоқ архитектураси

Юқорида келтирилган 6.1-расмда маълумот блоки устида калитга боғлиқ ҳолда бир функциядан фойдаланган ҳолда амаллар бажарилади. Дешифрлаш жараёнида фойдаланилган жадвалларга тескари бўлган жадвалдан фойдаланиб, калитларни тескари тартибда фойдаланиш орқали амалга оширилади. Ушбу усулда асосланган симметрик блокли шифрлаш алгоритмларига мисол тариқасида AES (Advanced Encryption Standard) шифрлаш стандартини олиш мумкин.

Фейстел тармоғига асосланган блокли симметрик шифрлаш алгоритмлари. Илк яратилган ва ҳозирда ҳам кенг фойдаланилаётган блокли симметрик шифрлаш алгоритмлари ушбу усул асосида яратилган бўлиб, моҳият жихатдан маълумот блоки тенг узунликдаги икки қисмда ажратилиб (чап ва ўнг қисмларга), улар устида маълум амаллар кетма-кетлиги бажарилади. Раунд амаллари турли калитлар билан бир қисм бўлак устида амалга оширилади.

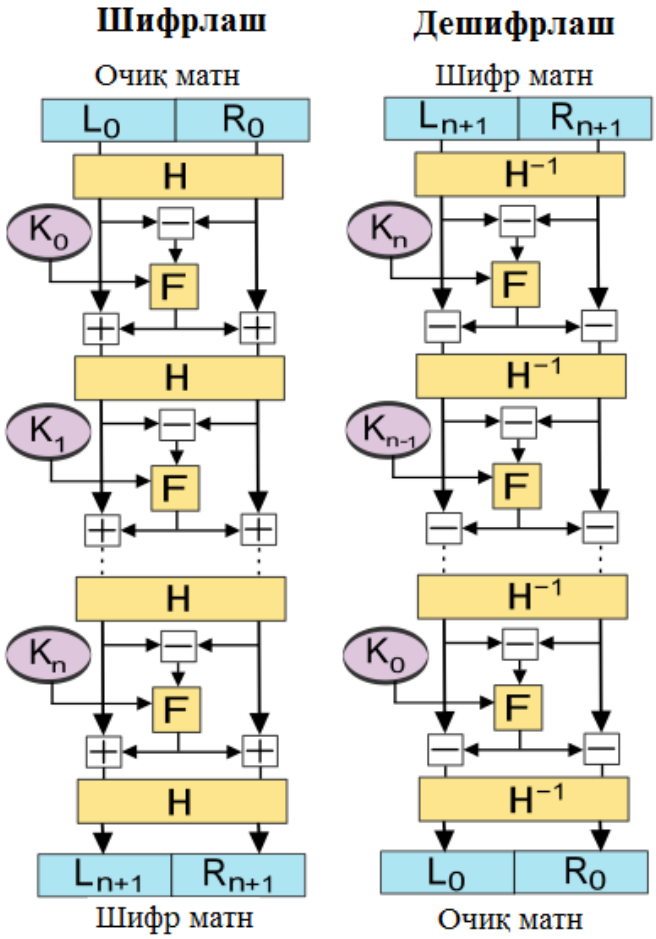
Фейстел тармоғи асосида қурилган симметрик блокли шифрлаш алгоритмларида шифрлаш ва дешифрлаш учун бир хил алгоритмдан фойдаланилади. Фарқли томони, раунд калитларининг қўлланилиши тескарисига ўзгаради, яъни дешифрлашда 1-раундда K_m, 2-раундда K_{m-1} ва ҳакозо охирги раундда K_1 ишлатилади. $F(R_{i-1}, K_i)$ функция бир томонлама

бўлса ҳам, дешифрлаш натижасида бу функция қайтади.



6.2-расм. *m*-раундли Фейстел тармоғи

Lai-Massey тармоғига асосланган блокли шифрлаш тизимлари. Ушбу архитектура, Фейстель тармоғига асосланган тизимга хавфсизлик параметрларини қўшиб, раунд функцияси тескари функцияси мавжуд бўлмаган функциялардан фойдаланилади.



6.3-расм. Lai-Massey шифрлаш тизими

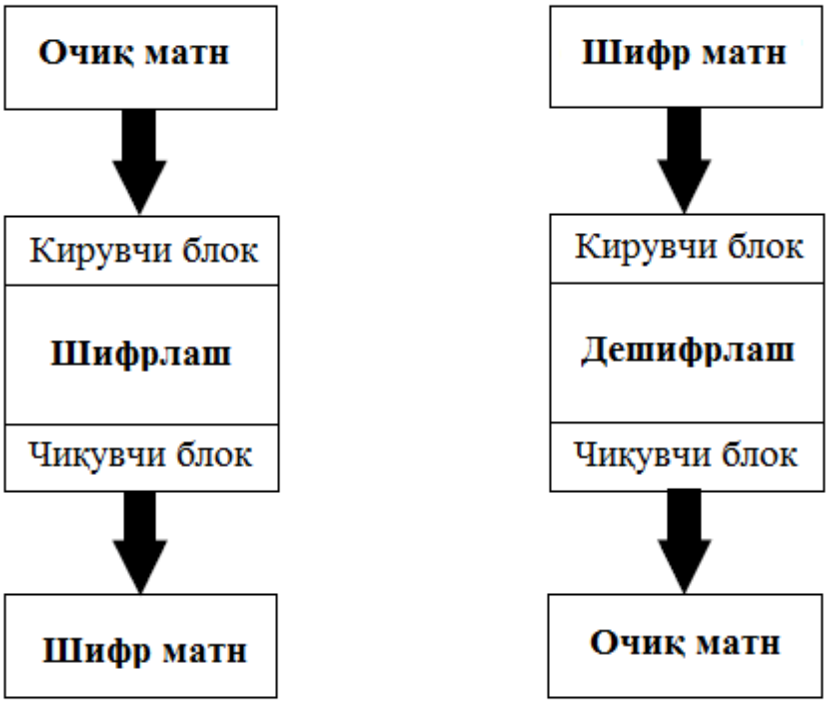
Блокли шифрлаш режимлари

Блокли шифрлаш алгоритмларида шифрлаш режимлари деган тушинча мавжуд бўлиб, блокли шифрлаш алгоритмларининг барчаси бу режимларда амалга оширилиши мумкин. Шифрлаш режимлари блокли шифрлаш алгоритмларига хавфсизлик ва амалга оширишда қулайлик туғдириш мақсадида ишлаб чиқилади.

Ҳозирда қуйидаги шифрлаш моделларидан кенг қўлланилади:

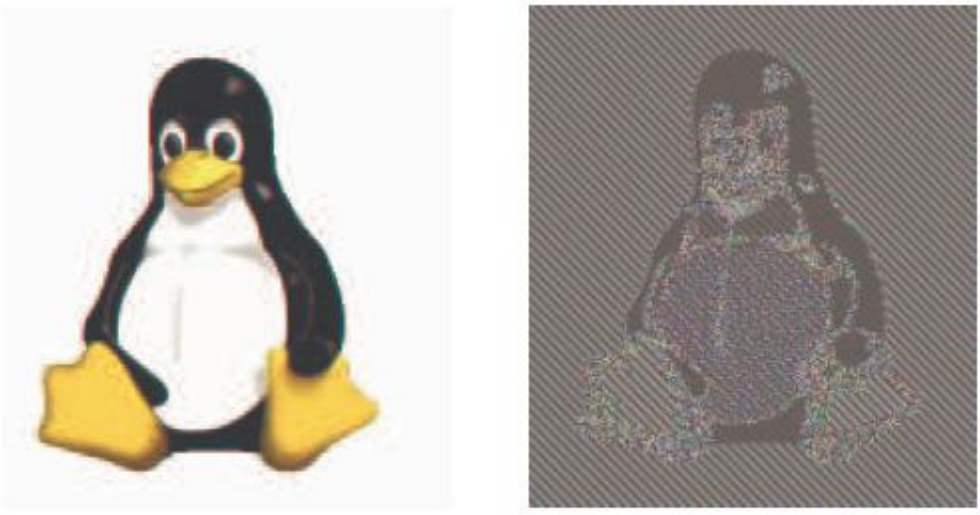
- Electronic codebook (ECB) режими;
- Cipher-block chaining (CBC) режими;
- Propagating cipher-block chaining (PCBC) режими;
- Cipher feedback (CFB) режими;
- Output feedback (OFB) режими;
- Counter (CTR) режими;
- Galois/Counter Mode (GCM) режими.

Electronic codebook (ECB) режими. Дастлабки содда моделлардан бири бўлиб, очиқ мант бир нечта блокларга бўлинади ва ҳар бир блок устида калит билан амаллар бажарилади (6.4-расм).



6.4-расм. ECB режимда шифрлаш ва дешифрлаш

Ушбу моделнинг асосий камчилиги бир хил очиқ матн бир хил шифр матнга алмашади. Булардан ташқари бу модел матнни яшириш каби вазифаларни бажармайди. Шуларни ҳисобга олган ҳолда ўта махфий ахборотлар билан ишлашда ушбу моделдан фойдаланиш тавсия этилмайди. Дастурий томондан амалга оширишда параллел ҳисоблашларга асосланган ҳолда шифрлашни амалга ошириш имконияти мавжуд. Қуйида ECB режимида шифрлаганда ҳосил бўлган 6.5-расм келтирилган.



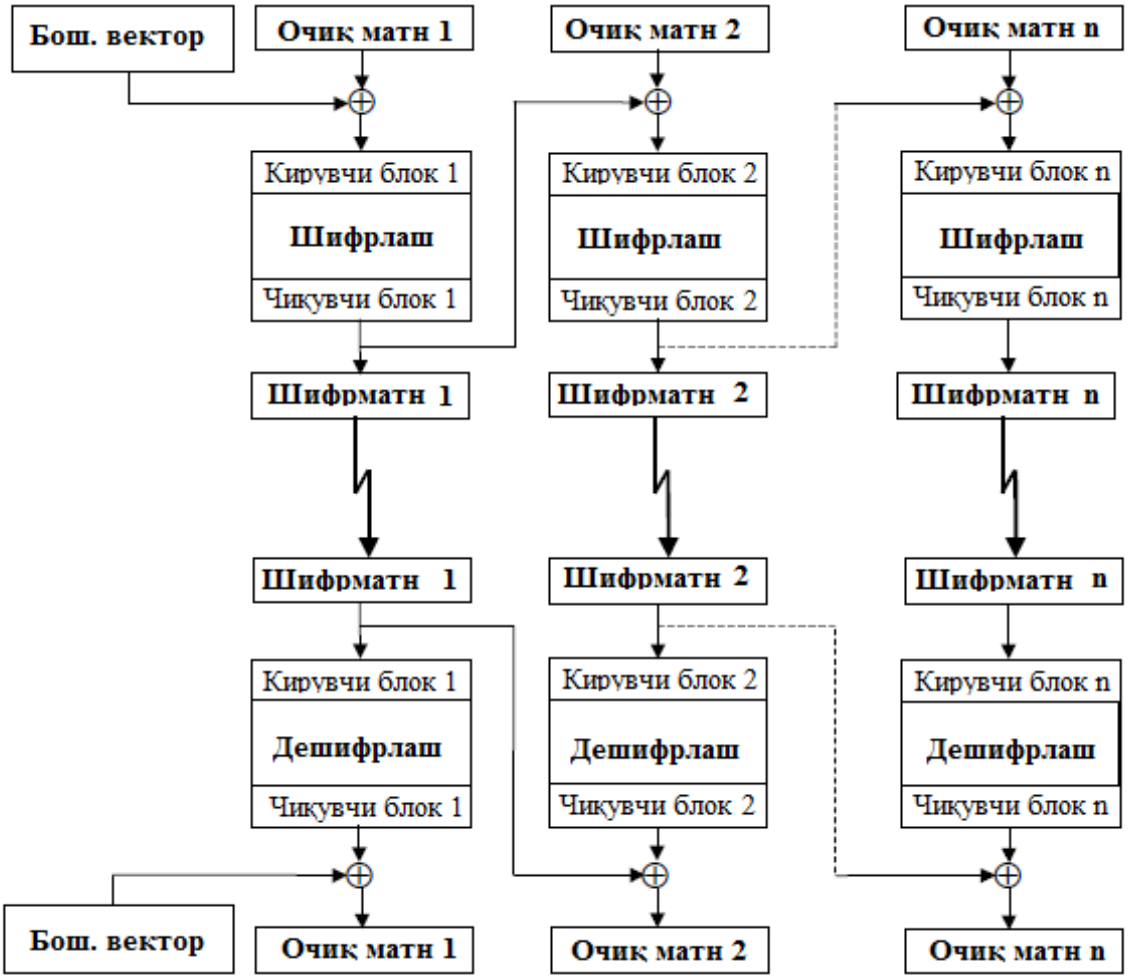
6.5-расм. ECB режимида шифрланган расм пикселлари

Бундан кўриниб турибдики, очиқ матнинг бир хил блоки бир хил шифрматнга аксланади.

Cipher-block chaining (CBC) режими. Ушбу шифрлаш режими 1976 йилда IBM томонидан ишлаб чиқилган. Дастлаб очиқ матнга бошланғич вектор қўшилиб, натижа калит ёрдамида шифрланади.

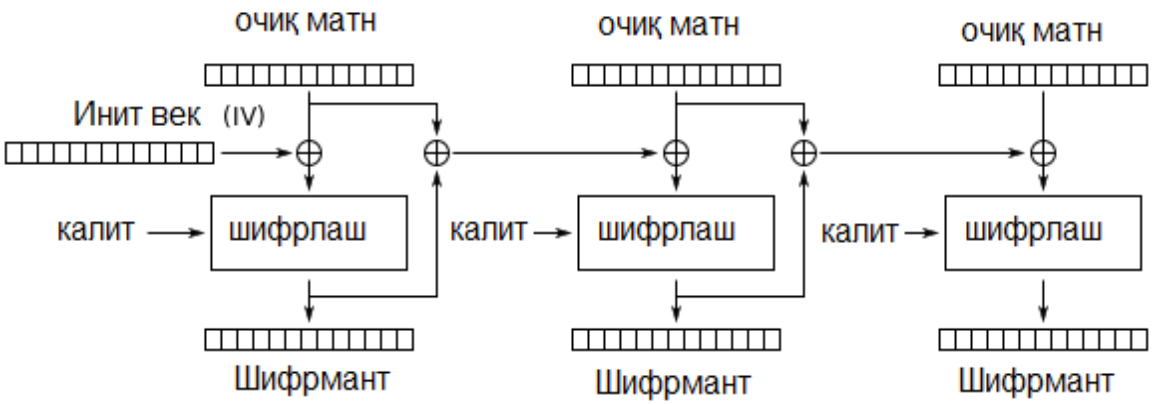
Дешифрлаш жараёнида шифрматн калит ёрдамида дешифрланади,

бошланғич векторга қўшилади ва натижавий кўриниш, очиқ матн олинади. Ушбу шифрлаш режимда бир хил маълумот блоклари турли хил шифрматн блокларига алмашади. Бу эса шифрматн асосида криптотаҳлил усулига бардошлигини таъминлайди. Камчилиги эса алгоритмни амалга оширишда, параллел тарзда амалга ошириш мумкин эмас, сабаби кейинги босқич натижаси олдинги босқич натижасига боғлиқ бўлади (6.6-расм).

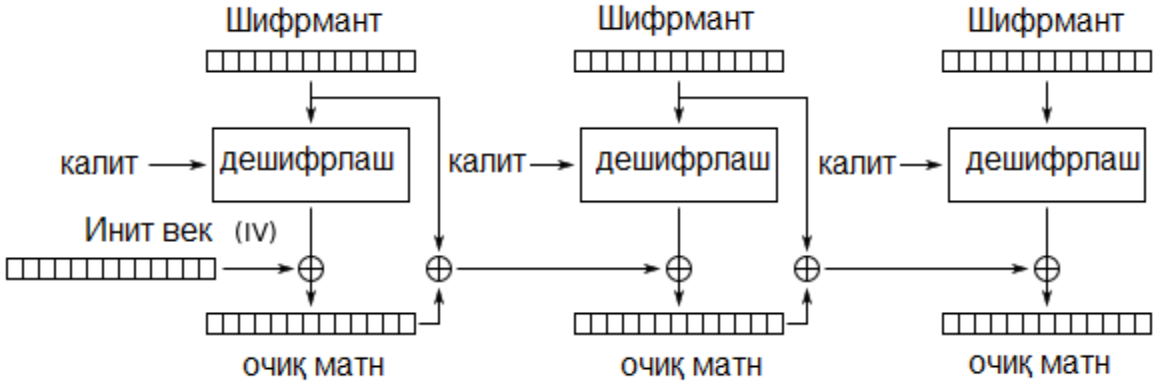


6.6-расм. CBC режимида шифрлаш ва дешифрлаш

Propagating cipher-block chaining (PCBC) режими. Ушбу шифрлаш режими Керберос v4 ва WASTE протоколларида фойдаланилган. Бардошсизлиги сабабли амалда кенг қўлланилмайди. Ушбу шифрлаш режимида ҳам ҳисоблашни параллел тарзда амалга ошириш имкониятини мавжуд эмас (6.7,6.8-расмлар).

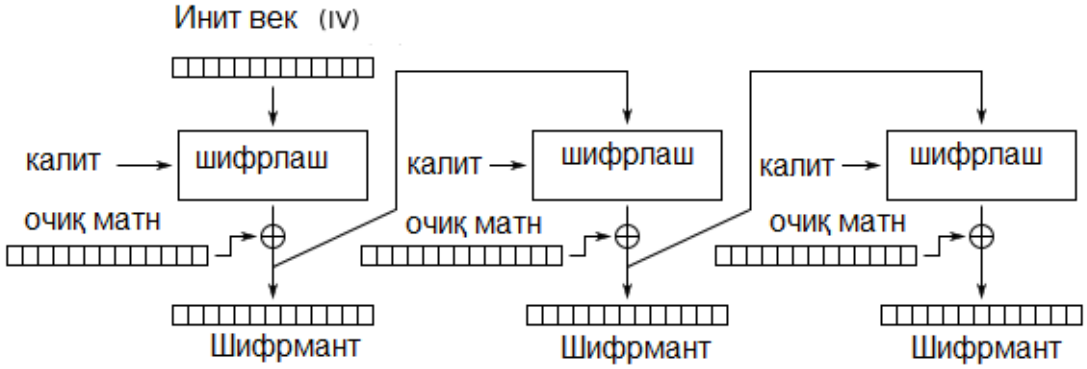


6.7-расм. PCBC режимида шифрлаш

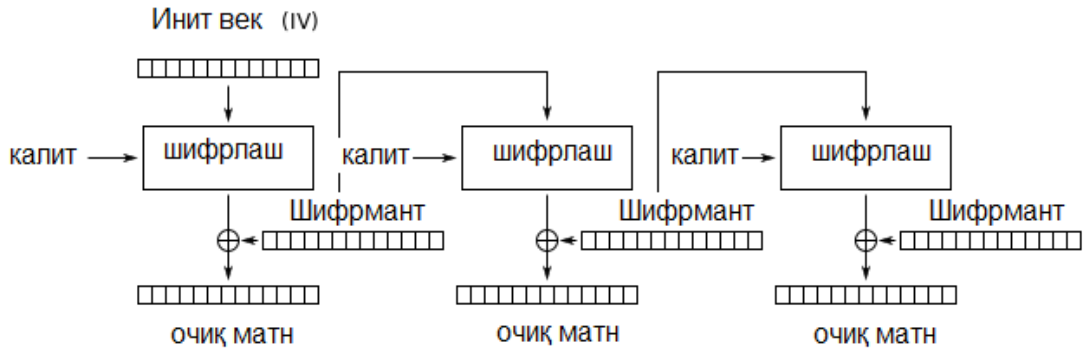


6.8-расм. PCBC режимида дешифрлаш

Cipher feedback (CFB) режими. Бу шифрлаш режими CBC режимига яқин бўлиб, ушбу режимда дешифрлаш CBC режимида шифрлаш амалига ўхшайди. Ушбу режимда дешифрлаш амали ўрнида ҳам шифрлаш амалидан фойдаланилади. Ушбу режимда ҳам параллел ҳисоблаш имконияти мавжуд эмас (6.9,6.10-расмлар).

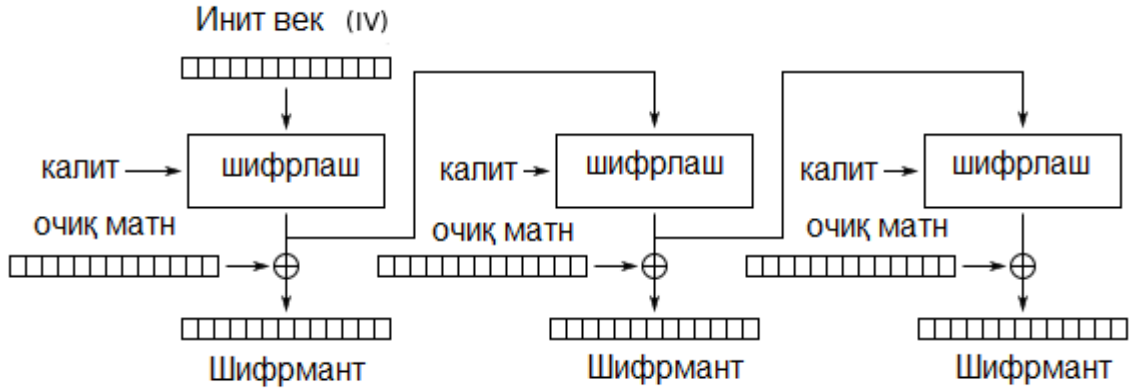


6.9-расм. CFB режимида шифрлаш

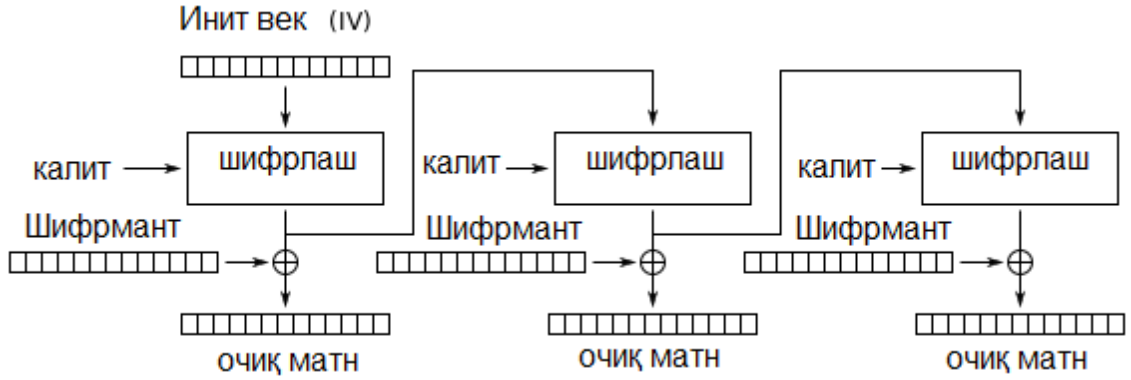


6.10-расм. CFB режимида дешифрлаш

Output feedback (OFB) режими. Бу режимда шифрлаш амали синхрон оқимли шифрлаш алгоритмларида блокли шифрлашни амалга ошириш учун амалда фойдаланилади. Ушбу режимда шифрлашда кейинги блок олдинги блокга боғлиқ бўлганлиги сабабли, параллел равишда ҳисоблаш имконияти мавжуд эмас (6.11,6.12-расмлар).



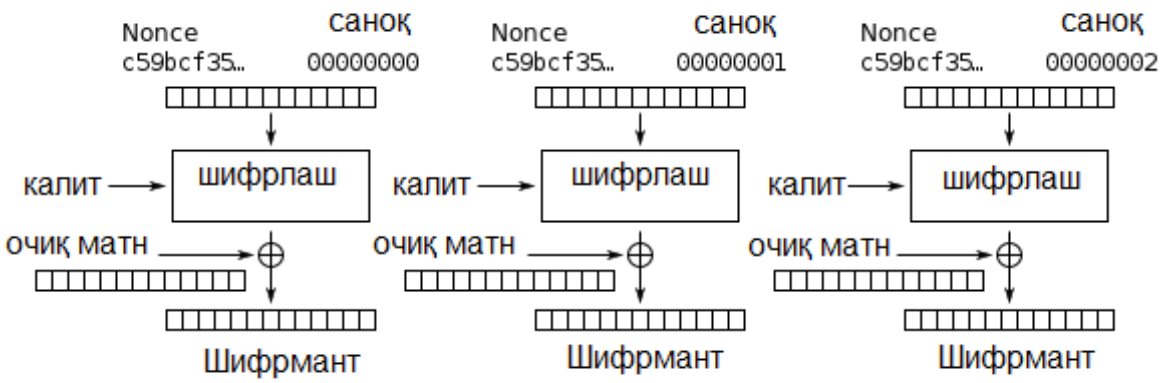
6.11-расм. OFB режимида шифрлаш



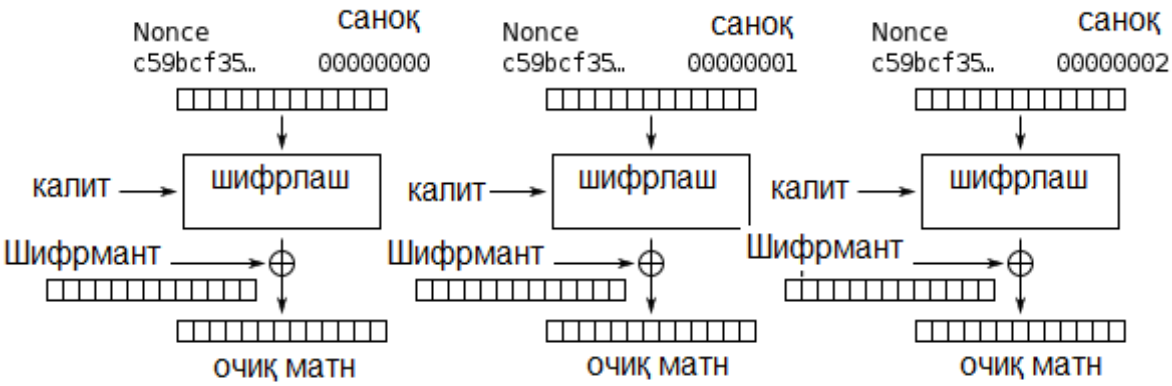
6.12-расм. OFB режимида дешифрлаш

Counter (CTR) режими. OFB шифрлаш режими каби, бу моделда ҳам оқимли шифрлашда блокли мифрлашни амалга ошириш учун амалда фойдаланилади. Бу кейинги калит кетма-кетлиги санагич қийматини шифрлаш амали орқали амалга оширади. Санагич қиймати эса такрорланмайдиган алгоритм асосида ҳосил қилинади. Бу усул амалда кенг фойдаланилиб, криптобардошлиги билан ва параллел ҳисоблаш имконини

бериши билан белгиланади (6.13,6.14-расмлар).



6.13-расм. CTR режимида шифрлаш



6.14-расм. CTR режимида дешифрлаш

Galois/Counter Mode (GCM) шифрлаш режими. Ушбу блокли шифрлаш режими симметрик шифрлаш алгоритмлари учун ишлаб чиқилган бўлиб, ушбу режим маълумотнинг ҳам бутунлигини ҳам махфийлигини таъминлашда кенг қўлланилади. Шунинг учун ҳам аутентификацияланган шифрлаш алгоритми деб ҳам юритилади. Ушбу режимда маълумот махфийлиги таъминланиб, бошқа маълумотнинг (қўшича қўшилган) бутунлиги таъминланади. Ушбу режим санаш (Counter) режими асосида ишлайди.

Қуйида келтирилган жадвалда ҳар бир режимда маълумотни шифрлаш ва дешифрлаш учун бажарилиши керак бўлган амаллар тури келтирилган.

6.1-жадвал

Шифрлаш режимларида фойдаланилган амалиётлар

Амаллар/ режим	**ECB**	**CBC**	**OFB**	**CFB**	**CTR**	**CTS**
Шифрлаш	Шифрлаш	Шифрлаш	Шифрлаш	Шифрлаш	Шифрлаш	Шифрлаш
Дешифрла	Дешифрла	Дешифрл	Шифрла	Шифрл	Шифрл	Дешифрл

ш	ш	аш	ш	аш	аш	аш

Юқоридаги жадвалдан кўриниб турибдики, баъзи режимлар учун ҳар икки амал шифрлаш/дешифрлаш амаллари талиб этилса, баъзи режимларда фақат шифрлаш амали талаб этилар экан.

Замонавий блокли шифрлаш усуллари

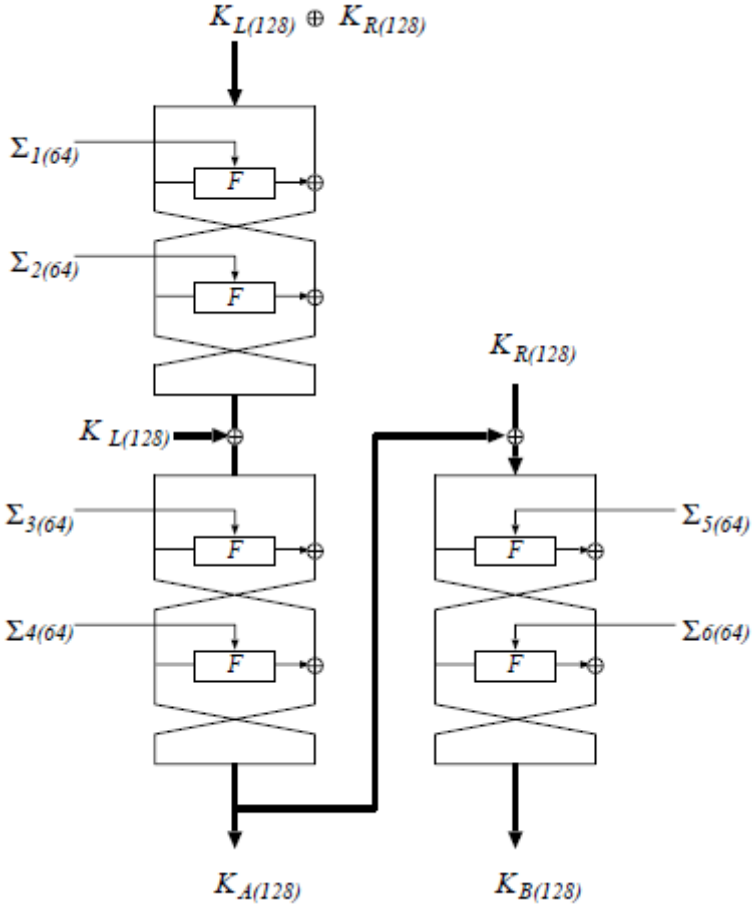
Camellia шифрлаш алгоритми. Ушбу блокли шифрлаш алгоритми NTT and Mitsubishi Electric Corporation томонидан ишлаб чиқилган. Camella симметрик блокли шифрлаш алгоритмида AES га ўхшаш блок узунлиги 128-бит бўлиб, калитлар эса 128, 192 ва 256-битга эга. Ушбу шифрлаш алгоритмнинг афзаллиги эса унинг хавфсизлик даражаси юқорилиги, шифрлашда ва дешифрлашда юқори тезликка эгалиги ва унинг аппарат-дастурий кўринишда ишлаб чиқишда қулайлиги.

Camellia алгоритмида калит генерацияси. Camellia блокли шифрлаш алгоритми калит генератори 6.15-расмда келтирилган. 128-битли K_L ва K_R калитлар қуйидагича ҳисобланади:

128 битли калит генератори учун, 128-битли К калит K_L га ўзлаштирилиб K_R калит эса 0 (нўл)га тенглаштирилади;

192-битли калит генаратори учун эса, К калитнинг дастлабки 128 бити K_L га ўзлаштирилиб, K_R га эса К калитнинг 64 битли ўнг қисми ва 64 битли чап қисмлари бирлашмасидан ташкил топган 128 битли қисм ўзлаштирилади;

256-битли калит генератори учун эса, К калитнинг дастлабки 128-битли қисми K_L ва қолган 128 битли қисми K_R ўзлаштирилади.



6.15-расм. Калит генерацияси

Бу ерда: 64-битли ўзгармаслар: Sigma1, Sigma2, ..., Sigma6 лар "калитлар" каби F-функцияда фойдаланилади. Уларнинг қийматлари қуйидагича:

Sigma1 = 0xA09E667F3BCC908B;
Sigma2 = 0xB67AE8584CAA73B2;
Sigma3 = 0xC6EF372FE94F82BE;
Sigma4 = 0x54FF53A5F1D36F1C;
Sigma5 = 0x10E527FADE682D1D;
Sigma6 = 0xB05688C2B3E6C1FD;

64-битли қисм калитлар эса KL, KR, KA, ва KB калитларни суриш ва уларнинг чап ёки ўнг-ярим қисмини олиш билан амалга оширилади.

128-битли очиқ матн M иккита қисмга: чап томон 64-битли D1 ва ўнг томон эса 64-битли D2 билан белгиланади, Яъни:

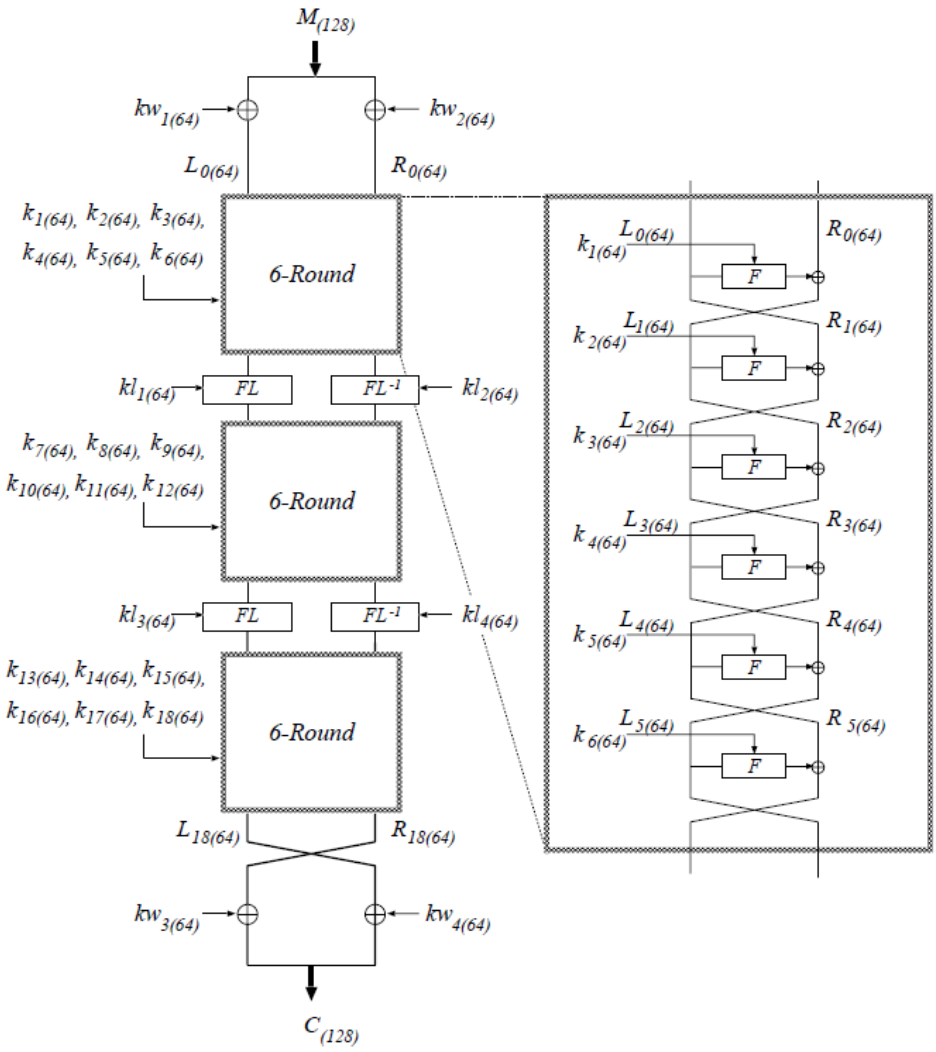
D1 = M >> 64;
D2 = M & MASK64;

Шифрлаш жараёни 18-раунд давомида амалга оширилади ва FL ва FLINV-функциялар эса ҳар 6- раундда амалга оширилади.

Натижавий 128-битли шифрматн C ўзгарувчилар D1 ва D2 ларни бирлаштириш орқали олинади:

C = (D2 << 64) | D1;

Camellia алгоритмида дешифрлаш. Camellia симметрик шифрлаш алгоритми Фейстел тармоғининг бир афзаллигига асосланган ҳолда, дешифрлашда калитларнинг тескари кетма-кетлигидан фойдаланган ҳолда амалга оширилади.



6.16-расм. Camellia шифрлаш алгоритмида шифрлаш

Camellia алгоритми ташкил этувчилари. Фойдаланилган F-функция иккита кирувчи параметрга эга бўлиб, бири 64-битли кирувчи F_IN ва бошқаси 64-битли KE қисм калит. F-функция натижасида 64-битли F_OUT қиймат қайтариди:

```
F(F_IN, KE)
  begin
     var x as 64-bit unsigned integer;
     var t1, t2, t3, t4, t5, t6, t7, t8 as 8-bit unsigned integer;
     var y1, y2, y3, y4, y5, y6, y7, y8 as 8-bit unsigned integer;
     x  = F_IN ^ KE;
     t1 =  x >> 56;
     t2 = (x >> 48) & MASK8;
     t3 = (x >> 40) & MASK8;
     t4 = (x >> 32) & MASK8;
     t5 = (x >> 24) & MASK8;
     t6 = (x >> 16) & MASK8;
     t7 = (x >>  8) & MASK8;
     t8 =  x & MASK8;
```

```
t1 = SBOX1[t1];
t2 = SBOX2[t2]= SBOX1[t2] <<< 1;
t3 = SBOX3[t3]= SBOX1[t3] <<< 7;
t4 = SBOX4[t4]= SBOX1[t4 <<< 1];
t5 = SBOX2[t5]= SBOX1[t5] <<< 1;
t6 = SBOX3[t6]= SBOX1[t6] <<< 7;
t7 = SBOX4[t7]= SBOX1[t7 <<< 1];
t8 = SBOX1[t8];
y1 = t1 ^ t3 ^ t4 ^ t6 ^ t7 ^ t8;
y2 = t1 ^ t2 ^ t4 ^ t5 ^ t7 ^ t8;
y3 = t1 ^ t2 ^ t3 ^ t5 ^ t6 ^ t8;
y4 = t2 ^ t3 ^ t4 ^ t5 ^ t6 ^ t7;
y5 = t1 ^ t2 ^ t6 ^ t7 ^ t8;
y6 = t2 ^ t3 ^ t5 ^ t7 ^ t8;
y7 = t3 ^ t4 ^ t5 ^ t6 ^ t8;
y8 = t1 ^ t4 ^ t5 ^ t6 ^ t7;
F_OUT = (y1 << 56) | (y2 << 48) | (y3 << 40) | (y4 << 32)
| (y5 << 24) | (y6 << 16) | (y7 <<  8) | y8;
return FO_OUT;
end.
```

SBOX1, SBOX2, SBOX3, ва SBOX4 жадваллар 8-битли кирувчи/чиқувчи битлардан иборат. SBOX2, SBOX3, ва SBOX4лар SBOX1дан қуйидагича ҳосил қилинади:

```
SBOX2[x] = SBOX1[x] <<< 1;
SBOX3[x] = SBOX1[x] <<< 7;
SBOX4[x] = SBOX1[x <<< 1];
```

SBOX1 жажвал кўриниши қуйидагича. Қийматни олиш қуйидача амалга оширилади. Масалан, SBOX1[0x3d]= 86.

6.2-жадвал

SBOX1 жадвали

	0	**1**	**2**	**3**	**4**	**5**	**6**	**7**	**8**	**9**	**a**	**b**	**c**	**d**	**e**	**f**
00	112	130	44	236	179	39	192	229	228	133	87	53	234	12	174	65
10	35	239	107	147	69	25	165	33	237	14	79	78	29	101	146	189
20	134	184	175	143	124	235	31	206	62	48	220	95	94	197	11	26
30	166	225	57	202	213	71	93	61	217	1	90	214	81	**86**	108	77
40	139	13	154	102	251	204	176	45	116	18	43	32	240	177	132	153
50	223	76	203	194	52	126	118	5	109	183	169	49	209	23	4	215
60	20	88	58	97	222	27	17	28	50	15	156	22	83	24	242	34
70	254	68	207	178	195	181	122	145	36	8	232	168	96	252	105	80
80	170	208	160	125	161	137	98	151	84	91	30	149	224	255	100	210
90	16	196	0	72	163	247	117	219	138	3	230	218	9	63	221	148
a0	135	92	131	2	205	74	144	51	115	103	246	243	157	127	191	226
b0	82	155	216	38	200	55	198	59	129	150	111	75	19	190	99	46
c0	233	121	167	140	159	110	188	142	41	245	249	182	47	253	180	89
d0	120	152	6	106	231	70	113	186	212	37	171	66	136	162	141	250
e0	114	7	185	85	248	238	172	10	54	73	42	104	60	56	241	164
f0	64	40	211	123	187	201	67	193	21	227	173	244	119	199	128	158

FL ва FLINV-функциялар. Алгоритмда фойдаланилган FL-функция кирувчи

иккита параметрга эга бўлиб, бири 64-битли кирувчи FL_IN ва иккинчиси 64-битли қисм калит KE. FL-функция натижасида чиқувчи 64-битли FL_OUT қиймат қайтарилади.

```
FL(FL_IN, KE)
begin
    var x1, x2 as 32-bit unsigned integer;
    var k1, k2 as 32-bit unsigned integer;
    x1 = FL_IN >> 32;
    x2 = FL_IN & MASK32;
    k1 = KE >> 32;
    k2 = KE & MASK32;
    x2 = x2 ^ ((x1 & k1) <<< 1);
    x1 = x1 ^ (x2 | k2);
    FL_OUT = (x1 << 32) | x2;
end.
```

FLINV-функция FL-функцияни инверти.

```
FLINV(FLINV_IN, KE)
begin
    var y1, y2 as 32-bit unsigned integer;
    var k1, k2 as 32-bit unsigned integer;
    y1 = FLINV_IN >> 32;
    y2 = FLINV_IN & MASK32;
    k1 = KE >> 32;
    k2 = KE & MASK32;
    y1 = y1 ^ (y2 | k2);
    y2 = y2 ^ ((y1 & k1) <<< 1);
    FLINV_OUT = (y1 << 32) | y2;
end.
```

Camellia шифрлаш алгоритми AES алгоритмига рақобатдош алгоритм сифатида ишлаб чиқилган. Кичик хотирага эга бўлган қурилмаларда ва дастурий тарзда амалга оширишга жуда қулай. Ушбу алгоритм ҳозирда Transport Layer Security (TLS) протоколида кенг қўлланилади.

Бу шифрлаш алгоритми хавфсизлик юзасидан фойдаланишда AES шифрлаш алгоритмига тенг криптобардошликка эга. Бундан ташқари энг кичик калит узунлигида ҳам (128-бит) “brute-force” ҳужумига бардошли саналади.

Назарий саволлар

Блокли шифрларни яратиш усуллари.

Фейстел тармоғининг асосий моҳияти.

Блокли шифрларда фойдаланилган режимлар.

Camellia шифри хусусиятларини айтинг.

7 - маъруза

Мавзу: Симметрик криптогрфик алгоритмлар. Оқимли шифрлаш алгоритмлари.

Режа:

Оқимли шифрлаш алгоритмларининг умумий моҳияти.

Псевдотасодифий сонларни генерациялаш.

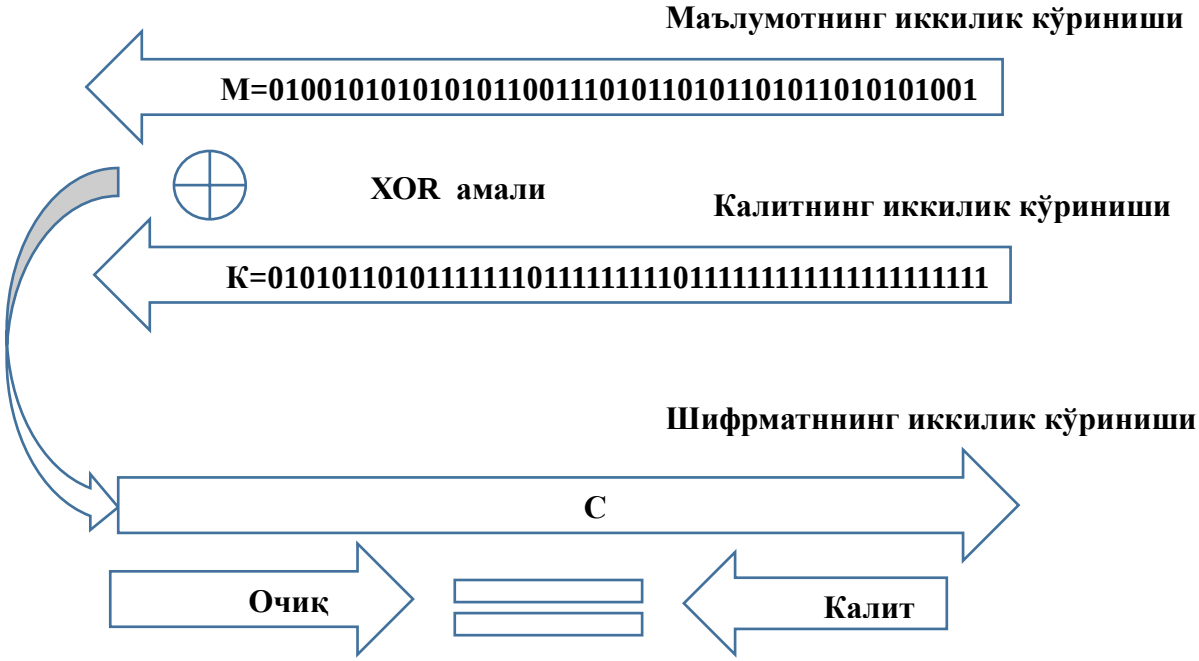
Замонавий оқимли шифрлаш усуллари.

Таянч иборалар: тасодифий сонлар генератори, псевдотасодифий сонлар генератори, XOR амали, RC4 шифри, A5/1 шифри.

Оқимли шифрлаш алгоритмларининг умумий моҳияти

Оқимли шифрлашда эса шифрлаш бирлиги бир бит ёки бир байт бўлади. Натижа одатда ундан олдин ўтган шифр оқимига боғлиқ бўлади. Бундай шифрлаш схемаси маълумотлар оқимини узатиш тизимларида қўлланилади, яъни бунда маълумотни узатиш ихтиёрий вақтда бошланиши ва тугатилиши мумкин.

Агар шифрлаш жараёни очиқ маълумотни ифодаловчи элементар (масалан: бит, ярим байт, беш бит, байт) белгиларни шифрмаълумотни ифодаловчи элементар белгиларга акслантириш асосида амалга оширилса, бундай шифрлаш алгоритми узлуксиз (оқимли) шифрлаш синфтуркумига киради. Ушбу тоифадаги шифрлаш алгоритмларининг умумий схемаси қуйидагича (7.1-расм).



7.1-расм. Оқимли шифрлаш тизими

Оқимли шифрлаш алгоритмлари олдин оммабоп саналган ва кичик имкониятга эга қурилмаларда хос бўлган. Оқимли шифрлаш алгоритмлари маълумот узунлигига тенг бўлган калит кетма-кетлигидан фойдаланганлиги сабабли ва ҳозирда компьютер техникаси имкониятини ортиши натижасида оқимли шифрлаш алгоритмлари ўрнини блокли шифрлаш алгоритмлари эгалламоқда.

Псевдотасодифий сонларни генерациялаш

Узлуксиз шифрлаш алгоритмлари асосини ПТКК ишлаб чиқарувчи генераторлар ташкил этади. Бундай генераторларнинг асосий криптобардошлилик характеристикаси ушбу генераторлар ҳосил қилган кетма-кетликнинг тасодифийлигидадир. Ҳосил қилинган кетма-кетликлар блокларининг тасодифийлик даражаси маълум бир критерийлар орқали баҳоланади. Тасодифийлик даражаси юқори бўлган псевдотасодифий кетма-кетликни ишлаб чиқарувчи генераторлар замонавий криптотизимларнинг ажралмас қисми ҳисобланади. Тасодифий кетма-кетликлар криптографияда қуйдаги мақсадларда қўланилади:

симметрик криптотизимлар учун тасодифийлик даражаси юқори бўлган сеанс калитлари ва бошқа калитларни генерация қилишда;

асимметрик криптотизимларда қўлланиладиган катта қийматлар қабул қилувчи параметрларнинг тасодифий бошланғич қийматлари генерациясида;

блокли шифрлаш алгоритмларининг бошланғич тасодифий қиймат талаб қилувчи CBC, OFB ва бошқа қўлланиш тартиб-қоидалари учун тасодифийлик даражаси юқори бўлган бошланғич векторлар ҳосил қилишда;

электрон рақамли имзо тизимларида катта қийматга эга параметрлар учун дастлабки тасодифий қийматларни генерациясида;

битта протокол орқали бир хил маълумотларни ҳар-хил калитлар қўллаш билан шифрлаб ҳар-хил кўринишда узатиш учун талаб қилинадиган ҳолатларда калит учун етарли узунликдаги тасодифий кетма-кетлик ҳосил қилишда, масалан SSL ва SET протоколларида.

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

Тасодифий кетма-кетликни: физик генераторлар ва дастурий генераторлардан фойдаланиб ҳосил қилиш мумкин.

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

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

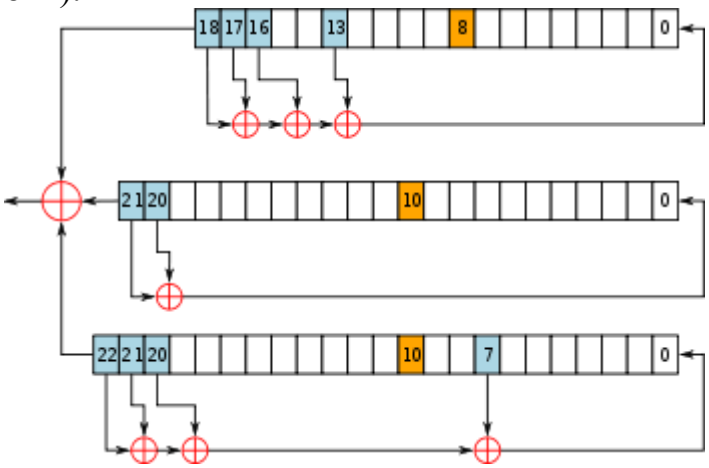
псевдотасодифий кетма-кетликни ишлаб чиқиши кафолатланади.
Юқорида кўрсатиб ўтилган амалий масалаларни ечишда хақиқий тасодифий кетма-кетликлар ишлаб чиқувчи тасодифий физик ходисаларга асосланган генераторлар олдиндан калитлар блоклари мажмуини яратишда, генераторларнинг бошланғич параметрлари қийматларини ўрнатишда ва бошқа шу каби масалаларни ечишда самарали натижалар беради.

Етарли катта давр узунлигига эга ва тасодифийлик даражаси юқори бўлган кетма-кетликлар ҳосил қилувчи дастурий ПТКК генераторини амалда қўланишлари самарали ва қулай бўлиб, криптографик воситаларда кенг қўлланилади.
Узлуксиз шифрлаш тизимларида шифрлаш ва дешифрлаш жараёнларини тез амалга оширилиши учун ташкил этувчилари текис тақсимланган, тасодифийлик даражаси юқори бўлган псевдо-тасодифий кетма-кетлик ишлаб чиқарувчи дастурий генераторлардан фойдаланилади.
Мавжуд дастурий генераторлар ва улар асосидаги узлуксиз шифрлаш тизимлари маълум бир ёндашувлар асосида яратилган.
Мавжуд дастурий генераторлар ва улар асосидаги узлуксиз шифрлаш тизимлари маълум бир ёндашувлар асосида яратилган.
Узлуксиз шифрлаш алгоритмларига қўйиладиган асосий талаблардан бири уларнинг криптографик бардошлилигини таъминловчи бирор ечилиши мураккаб бўлган математик муаммолар асосида яратилишидир.
Алгоритмларни криптобардошлилигини етарли даражада таминланганлигини кафолатлаш ёки исботлаш асослари нуқтаи - назаридан мавжуд узлуксиз шифрлаш алгоритмларини асосан учта йўналишга ажратиш мумкин:
Тизимли-назарий ёндашув йўналишидаги ПТКК генераторлари асосида яратилган алгоритмлар;
Мураккабликка асосланган назарий ёндашув йўналишидаги ПТКК генераторлари асосида яратилган алгоритмлар;
Комбинациялаш йўналишидаги ПТКК генераторлари асосида яратилган алгоритмлар.

Замонавий оқимли шифрлаш усуллари

Оқимли шифрлаш алгоритмларига мобил алоқа воситалари алоқа стандарти GSM (Global System for Mobile Communications) протоколида фойдаланилган A5 силжитиш регисторларига асосланган оқимли шифрлаш алгоритми, симсиз алоқа воситалариларида мавжуд WEP протоколида фойдаланилган RC4 оқимли шифрлаш алгоритмларини мисол қилиб олишимиз мумкин.
A5/1 оқимли шифрлаш алгоритми GSM стандартида маълумотни махфийлигини таъминлаш мақсадида фойдаланилган ва силжитиш регисторларига (СР) асосланган. Ушбу алгоритм 1987 йилда ишлаб чиқилган, европа ва қўшма штатларда дастлаб фойдаланилган.
A5/1 силжитиш регисторида кирувчи калит узунлиги 64 бит бўлиб, бу бит учта қисмга (19, 22, 23 битли) ажратилиб, регисторларга дастлабки қиймат сифатида берилади.
Ушбу алгоритм аппарат тарзда амалга оширишда жуда қулай саналиб,

алгоритм учта силжитиш регисторидан фойдаланилади. Ушбу алгоритмнинг ишлаш принципи 7.2-расмда келтирилган. Унга кўра учта X, Y ва Z регисторлар (ўлчамлари мос равишда, 19, 22 ва 23 бит)дан фойдаланилади. Ҳар бир регистор учун бошқариш битлари мавжуд бўлиб, улар регистор қийматини ўзгартиришда фойдаланилади (X учун 9, Y учун 11 ва Z учун 11 бит).



7.2-расм. A5/1 алгоритми

7.1-жадвал

A5/1 да фойдаланилган кўпҳадлар

CP рақами	Бит узунлиги	Кўпҳад кўриниши	Бошқариш бити	Олинадиган битлар
1	19	$x^{19} + x^{18} + x^{17} + x^{14} + 1$	8	13, 16, 17, 18
2	22	$x^{22} + x^{21} + 1$	10	20, 21
3	23	$x^{23} + x^{22} + x^{21} + x^8 + 1$	10	7, 20, 21, 22

Масалан (7.3-расм)**:**

A5/1 учта силжитиш регисторидан фойдаланилади

X: 19 bit (x_0,x_1,x_2, ...,x_{18})

Y: 22 bit (y_0,y_1,y_2, ...,y_{21})

Z: 23 bit (z_0,z_1,z_2, ...,z_{22})

Ҳар бир қадамда: m = maj(x_8, y_{10}, z_{10})

Масалан: maj(0,1,0) = 0 ва maj(1,1,0) = 1

агар x_8 = m u ҳолда X *қадам*

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

$x_i = x_{i-1}$ for i = 18,17,…,1 ва $x_0 = t$

агар y_{10} = m y ҳолда Y қадам

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

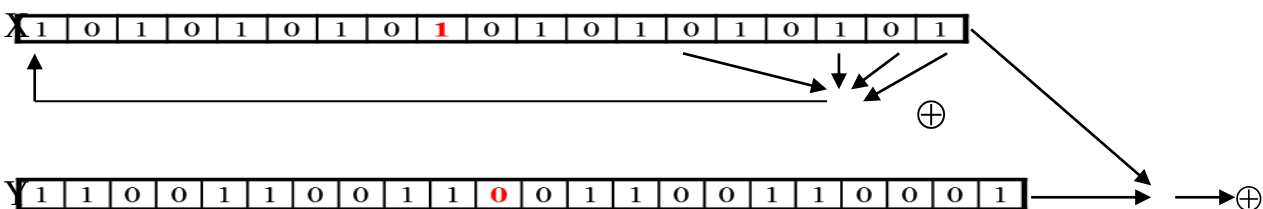
$y_i = y_{i-1}$ for i = 21,20,…,1 ва $y_0 = t$

агар z_{10} = m y ҳолда Z *қадам*

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

$z_i = z_{i-1}$ for i = 22,21,…,1 ва $z_0 = t$

Kalit ketma-ketligi $x_{18} \oplus y_{21} \oplus z_{22}$



7.3-расм. A5/1 шифрлаш алгоритмининг ишлаш принципи

Масалан, m = maj(x_8, y_{10}, z_{10}) = maj(1,0,1) = 1. Регистор X силжийди, Y силжимайди ва Z силжийди. Ўнг томондаги битлар XOR амали бўйича қўшилади. Масалан: $0 \oplus 1 \oplus 0 = 1$.

RC4. RC4 – узлуксиз шифрлаш алгоритми бўлиб, у SSL(Secure Sockets Layer) пратаколи ва WEP (симсиз тармоқларда хавфсизликни таъминлашда) кенг фойдаланилади. RC4 узлуксиз шифрлаш алгоритми Ron Rivest томонидан 1987 йилда яратилган ва шунинг учун RC4(Rivest Cipher 4) деб номланган.

RC4 псевдотасодифий битлар кетма-кетлигини ҳосил қилади ва ҳосил қилишда икки қисмдан иборат бўлган махфий оралиқ ҳолатидан фойдаланилади:

барча мумкин бўлган 256 байтнинг жойлашишдаги ўрни(S ни топиш);

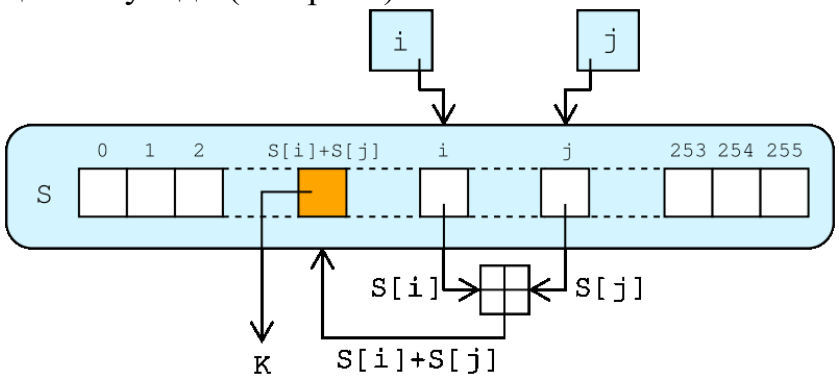
иккита 8 – битли индекслар (*i* ва *j* ларни топиш).

Байтларнинг келиш тартиби калит узунлиги билан амалга оширилади, одатда 40-256 бит оралиғида бўлиб, калит жадвали(key-scheduling) алгоритми орқали ҳосил қилиниди. Бу жараён тугагандан сўнг псевдотасодифий сонлар генератори алгоритми ёрдамида битлар кетма-кетлиги ҳосил қилинади.

Калит жадвали алгоритми қуйидагича:

```
for i from 0 to 255
   S[i] := i
endfor
j := 0
for i from 0 to 255
   j := (j + S[i] + key[i mod keylength]) mod 256
   swap values of S[i] and S[j]
endfor
```

Псевдотасодифий сонлар генератори алгоритми орқали ҳосил бўлган кетма-кетлик танланган S(i) ва S(j) ўзгарувчиларни mod256 бўйича қўшишдан ҳосил бўлади (7.4- расм).



7.4-расм. RC4 генератори алмаштириши

Псевдотасодифий сонлар генератори алгоритми қуйидагича:

```
i := 0
j := 0
while GeneratingOutput:
   i := (i + 1) mod 256
   j := (j + S[i]) mod 256
```

```
    swap values of S[i] and S[j]
    k := inputByte XOR S[(S[i] + S[j]) mod 256]
    output K
endwhile
```

Алгоритмда i ўзгарувчини қиймати ортиши билан ҳосил бўлган байтлар сони ҳам ортиб боради.

Бу ерда алмаштириш функцияси *swap* қуйидаги кўринишга ега:

```
byte temp = array[ind1];
array[ind1] = array[ind2];
array[ind2] = temp;
```

Ушбу генератор криптобардошли саналиб, ушбу хусусият кирувчи калит тасодифийлик даражаси билан белгиланади. Ҳозирда ушбу алгоритмнинг бир нечта вариантлари мавжуд бўлиб(RC4A, VMPC, RC4+), уларда дастлабкиларида мавжуд камчиликлар бартараф этилган.

ISAAC. Ушбу ПТСКК генератори 1966 йилда Роберт Женкинс томонидан яратилган бўлиб, RC4 алгоритмига ўхшашдир. Кирувчи параметр сифатида 32 бит ўлчамдаги сўзлардан иборат бўлган 256 узунликдаги массивдир. Чиқишнинг ҳар бир босқичида худди шу ўлчамдаги массив ҳосил бўлади. Ушбу ПТСКК генераторида ^(XOR), +(mod2^k) ва чапга ва ўнга суриш амаллари(<<, >>)дан ташкил топган.

f(a,i) функция эса қуйидагича ҳисобланади:

$$f(a,i)=\begin{cases} a<<13 & \text{if } i=0 \bmod 4 \\ a>>6 & \text{if } i=1 \bmod 4 \\ a<<2 & \text{if } i=2 \bmod 4 \\ a>>16 & \text{if } i=3 \bmod 4 \end{cases}$$

бу ерда $i \in \{0,\ldots..,255\}$ оралиққа тегишли сон.

Ушбу генераторнинг алгоритми қуйидагича:

Кирувчи параметрлар: a, b, c ва s ҳолат массиви, 256 ўлчамга ега бўлган 32 битли сўзлардан ташкил топган.

Чиқиш r массив, 256 ўлчамли 32 битли сўздан иборат бўлади.

1: $c \leftarrow c + 1$
2: $b \leftarrow b + c$
3: for $i = 0, \ldots, 255$ do
4: $x \leftarrow s_i$
5: $a \leftarrow f(a, i) + s_{i+128 \bmod 256}$
6: $s_i \leftarrow a + b + s_{x>>2 \bmod 256}$
7: $r_i \leftarrow x + s_{si>>10 \bmod 256}$
8: $b \leftarrow r_i$
9: end for
10: return r

Ушбу генератор бардошли генератор саналиб, ундаги мавжуд камчиликлар ISAAC+ генератор алгоритмида тузатилган. Ушбу генераторда бир неча марта назарий ҳужумлар амалга оширилган, аммо амалий томондан ҳужумга учрамаган.

Назорат саволлари

Оқимли шифрларнинг умумий моҳияти.

Псевдотасодифий сонлар генератори.
Замонавий оқимли шифрлаш алгоритмлари.

8 - маъруза

Мавзу: Очиқ калитли криптографик тизимлар

Режа:

Муаммо тури бўйича ассимметрик криптотизимлар таснифи.

Катта сонни туб кўпайтувчиларга ажратиш ва дискрет логарифмлаш муаммосига асосланган шифрлаш усуллари.

Эллиптик эгри чизиқ ва параметрли алгебра муаммосига асосланган шифрлаш усуллари.

Ассиметрик шифрлаш усулларини ахборот хавфсизлигини таъминлашда фойдаланиш таҳлили.

Таянч иборалар: очиқ калит, махфий калит, ассиметрик шифр, туб сон, факторлаш, дискрет логарифмлар, эллиптик эгри чизиқ.

Муаммо тури бўйича ассимметрик криптотизимлар таснифи

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

Носимметрик криптотизимлар бундан 32 йил муқаддам АҚШ олимлари У. Диффи ва М. Хэллман томонидан кашф этилган бўлиб, улар катта сонли чекли тўпламларда бир томонлама функциялардан фойдаланишга асосланган. У. Диффи ва М. Хэллманнинг 1976 йилда босилиб чиққан “Криптологияда янги йўналишлар” мақоласида илгари сурилган “махфий калитни узатишни талаб этмайдиган амалий бардошли махфий тизимларни тузиш мумкин” деган фикри криптологияда носимметрик криптотизимларнинг юзага келиши ҳамда уларнингривожланиш даврининг бошланишига сабаб бўлди.

Носимметрик криптотизимларнинг юзага келиши симметрик тизимларда ечилмай қолган махфий шифрлаш калитларини тарқатиш ва электрон рақамли имзо тизимларини яратиш ҳамда қатор замонавий масалаларни ечиш имкониятини берди.

Носимметрик криптотизимлар симметрик криптотизимларга нисбатан ўнлаб марта катта узунликдаги (*512, 1024, 2048, 4096* битли) калитлардан фойдаланади ва шу сабаб юзлаб марта секинроқ ишлайди. Носимметрик криптотизимларнинг математик асосида бир томонлама осон ҳисобланадиган функциялар (модуль бўйича дискрет даражага ошириш функцияси, эгри

чизиқли эллиптик функция ва ш.к.) ётади. Носимметрик криптотизимлар ахборот хавфсизлигининг барча муаммоларини ечиб беришга қодир ҳисобланади.

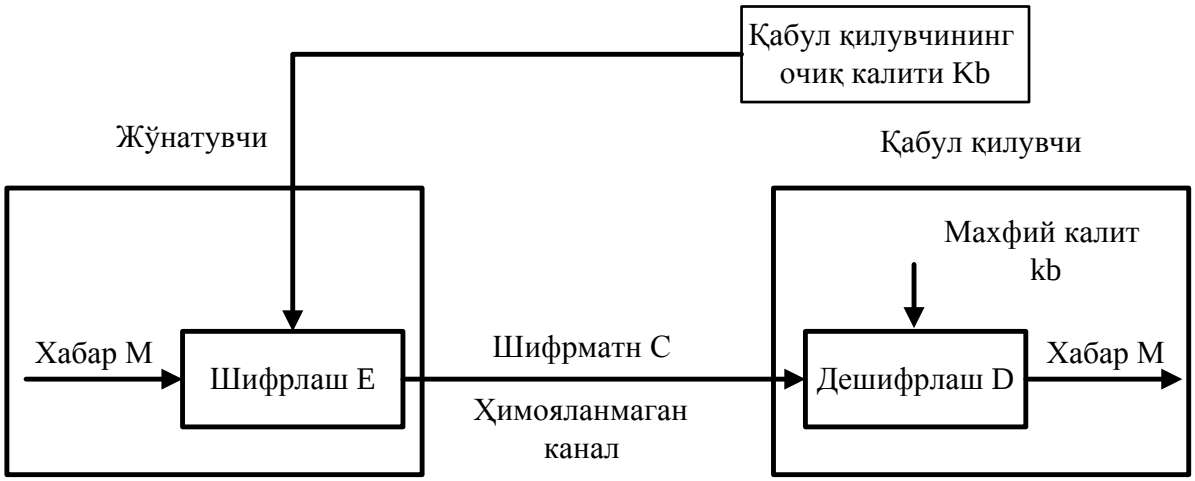
Очиқ калитли криптотизим моҳияти ҳар бир фойдаланувчи учун бирини билган ҳолда иккинчисини топиш, ечилиши мураккаб бўлган масала билан боғлиқ калитлар жуфтлигини яратишдан иборат. Бу жуфтликни ташкил этувчи калитлардан бири очиқ (ошкора), иккинчиси махфий (шахсий) деб эълон қилинади. Очиқ калит ошкора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

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

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

1. Дастлабки очиқ маълумотни шифрмаълумот кўринишига ўтказиш биртомонли жараён ва шифрлаш калити билан шифрмаълумотни очиш-дешифрлаш мумкин эмас, яъни шифрлаш калитини билиш шифрмаълумотнидешифрлаш учун етарли эмас.
2. Очиқ калитнинг маълумлигига асосланиб, маҳфий калитни замонавий фан ва техника ютуқлари ёрдамида аниқлаш учун бўладиган сарф-ҳаражатлар ҳамда вақт мақсадга мувофиқ эмас. Бунда, шифрни очиш учун бажарилиши керак бўладиган энг кам миқдордаги амаллар сонини аниқлаш муҳимдир.

Ассиметрик шифрлаш усуллари маълумотларни шифрлашда ва дешифрлашда алоҳида алоҳида калитлардан фойдаланади. Шунинг учун уларда калитларни тақсимлаш муаммоси мавжуд эмас (8.1 – расм).



8.1 - расм. Ассиметрик шифрлаш усулларининг умумий кўриниши

Ассиметрик ширфлаш алгоритмларидан фойдаланиб маълумотларни ширфлаш қуйидаги жараёнлардан иборат:

Калитлар генерацияси.

Б фойдаланувчи k_B махфий калит асосида K_B очиқ калитни генерация қилади. Очиқ калит K_B очиқ тармоқ орқали А фойдаланувчига ёки тармоқнинг бошқа фойдаланувчиларига узатади.

Маълумотларни ширфлаш.

А фойдаланувчи ёки тармоқнинг бошқа фойдаланувчиси K_B очиқ калитдан фойдаланган ҳолда очиқ маълумотни шифрлайди ва уни очиқ тармоқ орқали юборади.

Шифрмалумотни дешифрлаш.

Б фойдаланувчи қабул қилинган шифрматнни ўзининг k_B махфий калит билан дешифрлайди ва очиқ матнга эга бўлади.

Ассиметрик шифрлаш усулларини яратишда одатда ҳозирда ечими мавжуд бўлмаган математик муаамодан фойдаланилади. Бу математик муаммолар одатда бир томонлама функция сифатида ифодаланади. Бир томонлама функция деб, ўзига тескари бўлган функция мавжуд бўлмаган функцияга айтилади.

Мавжуд носимметрик криптотизимлар бардошлилигини таъминлашга асос бўлган мураккаб муаммо (масала) тури бўйича қуйидагича таснифланади (8.1-жадвал):

факторлаш муаммосининг мураккаблигига асосланган криптотизимлар;

дискрет логарифм муаммосининг мураккаблигига асосланган криптотизимлар;

эллиптик эгри чизиқда дискрет логарифм муаммосининг мураккаблигига асосланган криптотизимлар;

бошқа муаммоларга асосланган криптотизимлар.

8.1-жадвал

Муаммо тури бўйича носимметрик криптотизимлар таснифи

Муаммо	**Баёни**
Факторлаш	Бутун факторлаш муаммоси: бутун мусбат n берилган,

	унинг Туб факторларини топиш керак: яъни, $n = p_1^{e_1} p_2^{e_2} \ldots . p_k^{e_k}$ кўринишда ёзиш керак, бу ерда p^i - турли туб сонлар ва ҳар бири $e_i \geq 1$.
RSA муаммоси (RSAP)	RSA муаммоси (RSA инверсия каби маълум): иккита турли *p* ва *q* тоқ сонларнинг кўпайтмаси бўлган бутун мусбат *n* сони, *EKUB (e, (p-1)(q-1))=1* га тенг бўлган бутун мусбат *e* сони ва бутун *c* берилган, шундай бутун *m* ни топиш керакки, унда $m^e \equiv c(\mathrm{mod}\, n)$ бўлсин.
Квадратик чегирма муаммоси (QRP)	Квадратик чегирма муаммоси: тоқ мураккаб бутун *n* ва $\left(\frac{\mathrm{a}}{\mathrm{n}}\right) = 1$ Якоби белгисига эга бўлган бутун *a* сони берилган, *a* сони *n* модуль бўйича квадратик чегирма эканлиги ёки чегирма эмаслиги аниқлансин.
n модули бўйича квадрат илдиз (SQROOT)	*n* модули бўйича квадрат илдиз: мураккаб бутун *n* сони ва $\mathrm{a} \in \mathrm{Q}_\mathrm{n}$ (*n* модули бўйича квадратик чегирма тўплами) берилган, *n* модули бўйича *a* дан шундай бутун квадратик илдиз *x* топилсинки, унда $x^2 = a(mod\ n)$ бўлсин.
Дискрет логарифм муаммоси (DLP)	Дискрет логарифм муаммоси: Туб сон *p* учун, чекли майдон Z_{p^*} да ҳосил қилувчи (генератор) элемент α ҳамда $\beta \in Z_{p^*}$ берилган бўлса, шундай $0 \leq x \leq p-2$ бўлган бутун *x* сон топилсинки, унда $\alpha^x \equiv \beta\ (mod\ p)$ бўлсин, бу ерда *x* – даража кўрсаткичи.
Умумлашган дискрет логарифм муаммоси (GDLP)	Умумлашган дискрет логарифм муаммоси: *n* тартибли чекли циклик группа *G*, *G* нинг ҳосил қилувчиси α ва $\beta \in G$ элемент берилган, шундай $0 \leq x \leq n-1$ бўлган бутун *x* сони топилсинки, унда $\alpha^x = \beta$ бўлсин.
Диффи-Хеллман муаммоси (DHP)	Диффи-Хеллман муаммоси: туб сон *p*, *Zp** ҳосил қилувчиси - α ва $\alpha^a\ (mod\ p)$ ва $\alpha^b\ (mod\ p)$ элементлари берилган, $\alpha^{ab}\ (mod\ p)$ топилсин.
Умумлашган Диффи-Хеллман муаммоси (GDHP)	Умумлашган Диффи-Хеллман муаммоси: чекли циклик группа *G*, *G* ҳосил қилувчиси - α ва группа элементлари α^{a} ва α^b лар берилган, α^{ab} топилсин.
Қисм тўплам - йиғиндиси (SUBSET-SUM)	Қисм тўплам-йиғиндиси муаммоси: бутун мусбат сонлар тўплами $a_1, a_2, \ldots, a_n$ ва бутун мусбат сон *S* берилган, йиғиндиси *S* га тенг бўлган a_j қисм тўплам мавжудми ёки йўқми аниқлансин.
Эллиптик эгри	Эллиптик эгри чизиқли дискрет логарифм муаммоси:

чизиқда дискрет логарифм муаммоси (ECDLP)	*K* чекли майдон ва *G* нуқтада тартиби *n* бўлган *G* нуқта, *Q∈E(K)* нуқтада *E* ЭЭЧ берилган. *Q=[d]G* шартни қаноатлантирувчи *d, 0≤d≤n-1* бутун сонни топиш талаб этилади, агарда у мавжуд бўлса.
Даража параметри муаммоси	*1-таъриф.* Агар параметрли группа *(F_n; ®)* да ташувчи F_n нинг элементи *y* берилган бўлса, унда параметр *R*, даража кўрсаткичи *e* ва элемент *a* топилсин. *2-таъриф.* Агар параметрли группа *(F_n; ®)* да ташувчи F_n нинг элементлари *y* ва *a* берилган бўлса, унда параметр *R* ва даража кўрсаткичи *e* топилсин. Бу ерда F_n – *n* та бутун сонлардан тузилган чекли тўплам, $y \equiv a^{\backslash e} (mod\ n)$, $^{\backslash e}$ – *a* ни параметр *R* билан *e*-даражаси рамзи, $\varphi(n)>R>1$, элемент *a* $a^{\backslash \omega} (mod\ n)\equiv 0$ шартини фақат $\omega = q$ бўлгандагина қаноатлантиради, $q - \varphi(n)$ нинг бутун сонли бўлувчиси, *φ(n) – Эйлер пи-функцияси*, $n\in\{p, p_1*p_2\}$, p, p_1, p_2 – туб сонлар.

Катта сонни туб кўпайтувчиларга ажратиш ва дискрет логарифмлаш муаммосига асосланган шифрлаш усуллари

Маълумки, энг кўп фойдаланиб келинган носимметрик тизимларга бардошлилиги учта муаммонинг, яъни факторлаш, дискрет логарифмлаш ва ЭЭЧ группасида дискрет логарифмлаш мураккаблиги муаммоларидан бири билан белгиланадиган криптотизимлар киради. Булар билан бир қаторда қўшимча махфийликка эга бўлган носимметрик криптотизимлар ҳам юзага келмоқда.

RSA шифрлаш алгоритми. Диффи ва Хелман критография соҳасида янгича ёндашишни тарғиб қилиб, очиқ калитли криптотизимларнинг барча талабларига жавоб берадиган криптографик алгоритм яратиш таклифибилан чиқди. Биринчилардан бўлиб бунга жавобан 1997 йил Рон Райветс (Ron Rivest), Ади Шамир (Adi Shamir) ва Лен Адлмен (Len Adlmen)лар шу вақтгача тан олинган ва амалий кенг қўлланиб келинган очиқ калитли шифрлаш алгоритм схемасини таклиф қилди ва бу алгоритм уларнинг номи шарафига RSA алгоритми деб аталди. RSA алгоритми факторлаш мураккаблигига асосланган шифрлаш алгоритми ҳисобланади.

Райвест, Шамир ва Адлмен томонидан яратилган схема даража кўрсаткичига асосланган. Очиқ матн блокларга ажратилиб шифрланади, ҳар бир блок баъзи берилган n сонидан кичик бўлган иккилик қийматга эга бўлади. Бундан келиб чиқадики блок узунлиги $log_2(n)$дан кичик ёки тенг бўлиши керак. Умуман олганда амалиётда блок узунлиги 2^kга тенг деб олинади, бу ерда $2^k < n \leq 2^{k+1}$. Очиқ матн M блоки ва шифрланган матн Cблоки учун шифрлаш ва дешифрлаш қуйидаги формула билан ҳисоблаш мумкин.

$M = M^e mod n,$

$$M = C^d mod n = (M^e)^d mod n = M^{ed} mod n.$$

Жўнатувчи ҳам, қабул қилувқи ҳам n ни қийматини билиши керак.

Жўнатувчи e ни қийматини, қабул қилувчи эса фақат d ни қийматини билишади. Ушбу схема очиқ калитли шифрлаш алгоритми ҳисобланади, $KU=\{e,n\}$- очиқ калит ва $KR=\{d,n\}$-махфий калит ҳисобланади. Бу алгоритм очиқ калит ёрдамида шифрланиши учун, қуйидаги талаблар бажарилиши керак.

1. Шундай e, d ва n қийматлар мавжуд бўлиш керакки, барча $M < n$ учун $M^{ed} = Mmodn$ тенглик ўринли бўлиши керак.

2. Барча $M < n$ учун M^e ва C^dни ҳисоблаш осон бўлиши керак.

3. Амалий жиҳатдан e ва n ни билмасдан туриб d ни қийматини билиш мумкин бўлмаслиги керак.

Биринчи шартга биноан қуйидаги муносабатни топиш керак

$$M^{ed} = Mmodn.$$

Эйлер функциясига асосан: ҳар қандай иккита p ва q туб сонва ҳар қандай n ва m бутун сонлар учун, $n=pq$ ва $0 < m < n$, ва ихтиёрий k бутун сон учун қуйидаги муносабат бажарилади.

$$m^{k\varphi\ n\ +1} = m^{k\ p-1\ \ q-1\ +1} \equiv mmodn,$$

Бу ерда $\varphi(n)$ Эйлер функцияси бўлиб, n дан кичик ва n билан ўзаро туб бўлган мусбат бутун сон. Эйлер функцияси $\varphi\ n$ билан ўзаро туб бўлган e сон танлаб олинади ва талаб қилинаётган муносабат қуйидаги шарт асосида бажарилади.

$$ed = k\varphi\ n\ + 1.$$

Бу қуйидаги муносабат билан эквивалент:

$$ed \equiv 1\ mod\varphi\ n\ ,$$
$$d \equiv e^{-1}mod\varphi\ n\ ,$$

e ва d, $\varphi(n)$ модул бўйичаўзаро тескари сон, яъни

$gcd(\varphi\ n\ ,e) = 1.$

Юқорида келтирилган параметрлар асосида RSA схемасини қуйидаги таьснифлаш мумкин:

p ва q - туб сонлар (махфий, танлаб олинади),

$n=pq$ (очиқ, ҳисобланади),

шундай e, $gcd(\varphi\ n\ ,e) = 1,\ 1 < e, \varphi\ n$ (очиқ, танлаб олинади),

$d \equiv e^{-1}mod\varphi(n)$ (махфий, ҳисобланади).

Махфий калит $\{d,n\}$ дан, очиқ калит эса $\{e,n\}$ дан иборат бўлади. Фараз қилайлик A фойдаланувчи очиқ калитини элон қилди ва B фойдаланувчи унга M хабарни жўнатмоқчи. Bфойдаланувчи $C = M^e(modn)$ҳисоблаб Cни жўнатади. Шифрланган матнни қабул қилган A фойдаланувчи $M = C^d(modn)$ ёрдамида дешифрлаб дастлабки очиқ матнга эга бўлади.

Қуйида келтирилган мисолда RSA алгоритми амалий қўллаш кўрсатилган.

1. Иккита туб сон танлаб олинади, $p=7$ ва $q=17$.

2. $n=p*q=7*17$ ҳисобланади.

3. Эйлер функцияси ҳисобланади $\varphi\ n\ =\ p-1\ \ q-1\ = 96.$

4. Эйлер функцияси $\varphi\ n\ = 96$ билан ўзаро туб бўлган ва ундан кичкина бўлнаг e танлаб олинади; бизни, мисолимизда $e=5$.

5. $de=1mod\ \ 96$ ваd<96шартни қаноатлантирувчи dсони топилади. $d=77$,

*77*5=385=4*96+1.*

Натижада очиқ калит *KU={5,119}* ва ёпиқ калит *KR={77,119}*ҳосил бўлади. Юқоридаги мисолда очиқ матн қиймати *M=19* олинган. Шифрлаш формуласига кўра очиқ матн қиймати очиқ калит қиймати ёрдамида даражага кўтарилиб, *n* модул бўйича қиймати олинади, яъни 19 сони 5 даражага кўтарилади, натижада 2476099 ҳосил бўлади. Натижани 119 га бўлинса, қолдиқ 66 га тенг бўлади. $19^5 = 66\, mod\, 119$ ва шунинг учун ҳам шифрланган матн 66 га тенг бўлади. Дешифрлаш учун эса шифрланган матн қиймати махфий калит қиймати ёрдамида даражага кўтарилиб, *n* модул бўйича қиймати олинади, яъни$66^{77} = 19\, mod\, 119$ амални ҳисобланади ва дастлабки очиқ матн қийматига эга бўлинади, яъни 19 га.

Калитларни ҳисоблаш. Очиқ калитли криптотизимларга калитларни генерацтя қилиш муҳим аҳамият касб этади. Ҳар бир томон иккитадан калит генерация қилиши керак бўлади. Буни амалга ошириш учун эса қуйидаги вазифаларни бажариш керак бўлади:

иккита *p* ва *q* дан иборат туб сон аниқлаб олиниш;

иккинчисини ҳисоблаш учун, *e* ёки *d* сонларидан бирини танлаш.

Биринчи бўлиб *p* ва *q* ни танлаш процедурасини кўриб ўтилса. *n=pq* қиймати ҳамма маълумлигини инобатга олган ҳолда, *p* ва *q* ни қийматини оддий перебор усулда топиш имкониятига йўл қўймаслик учун, бу туб сонлар етарли даражада катта бўлиши керак. Шу билан бир қаторда катта туб сонларни топиш методи амалий жиҳатдан унумли бўлиши керак.

Ҳозирги кундагача самарадорлиги яхши бўлган, иҳтиёрий катта сондаги туб сонни ҳисоблаш методи ишлаб чиқилмаган. Бу методларда кўпроқ тахминан исталган узунликдаги ва аниқликдаги, танлаб олинган тоқ сонни тубликка текшириш процедураси ётади. Агар танлаб олинган сон туб бўлиб чиқмаса, кейинги туб сон танлаб олинади токи туб сон танлаб олинмашунча. Сонларни тубликка текширувчи бир қатор тестлар мавжуд бўлиб, бу тестларининг деярли барчаси эҳтимоллик характерига эга. Яъни тестлаш натижаси берилган бутун сонни эҳтимолий тублигини аниқлайди. Тўлиқ ишонч бўлмаслигига қарамасдан, бундай тестларнинг бажарилиши, ишончлилиги таъминланганлиги эҳтимоли бирга яқин бўлади.

Раббин-Миллер ва аксарият шунга ўхшаш алгоритмларда, берилган бутун *n* сонни тубликка синаш процедураси, тасодифий танлаб олинган бутун сон *a* ва *n* иштироидаги бир қатор ҳисоблашларни бажаришдан иборат. Агар *n* бундай тестлашларга жавоб бера олса, у ҳолда *n* туб сон бўлиб чиқади, акс ҳолда туб эмас. Агар *n* ҳар хил тасодифий танланган *a* нинг қийматларида,бир қатор шундай синовлардан муваффақиятли ўтса, *n* нинг туб сон эканлигининг ишончлилиги даражаси ортади.

Ҳулоса қилиб шуни айтиш мумкинки, туб сонни танлаб олиш процедурасини қуйидаги кўринишда кўрсатиш мумкин.

Тоқ бўлган бутун *n* сонни қандайдир тасодифий равишда танлаб олиш(масалан псевдотасодифий генератор орқали).

Тасодифий равишда *a<n* бўлган бутун *a* сон танлаб олиш.

Танлаб олинган сонни тубликка синаш тестидан ўтказиш. Агар *n* сони

тестдан ўта олмаса, кейинги тасодифий равишда танлаб олинган сонни шу кетма-кетликда бажариш керак.

Агарn етарлича қайта тестлардан муваффақиятли ўтса, n қийматни муносиб деб олиш керак, акс ҳолда 2 қадамга ўтиш керак.

Шуни эсдан чиқармаслик керакки, бу жараён фақат, қачонки янги калитлар жуфтлигини (KU,KR) яратиш талаб қилинсагина бажарилади. Сонлар назарияси ҳақидаги теоремаларидан бири, туб сонлар ҳақидаги теорема шуни тасдиқлайдики, N гача бўлган бутун сонлардан $ln(N)$ таси туб бўлиши мумкин. Бундан келиб чиқадикитуб сонни топиш учун, $ln(N)$гача бўлган бутун сонларни тубликка синашга тўғри келади, бунга эса ўз-ўзидан кўп вақт ҳамда супер замонавий ҳисоблаш машинаси керак бўлади. Жуфт сонларни чиқариб ташлашсак сонлар тартиби $ln(N)/2$ тага етади. Масалан туб сонни узунлиги тартиби 2^{2000} бўлган ораликда излайдиган бўлсак, туб сонни топиш учун $ln(N)/2=70$ га яқин уриниш керак бўлади. p ва q туб сонни аниқлагандан кейин, e қийматни танлаб d ни ҳисоблаш ёки тескари, d қийматни танлаб e ни ҳисоблаш билан калитларни ҳисоблаш жараёни тугайди. Биринчи навбатда e ни шундай танлиш керакки, у Эйлер функцияси билан ўзаро туб бўлиши керак яъни $gcd(\varphi\ n\ ,e)=1$, шундан сўнг e га ўзаро тескари бўлган d топилади $d = e^{-1} mod \varphi(n)$. Бундай ўзаро туб сонларни топиш Евклиднинг умумлашган алгоритми бўйича топилади, яъни процедура шундан иборатки тасодифий равишда генерацияланган сонни $\varphi\ n$ билан ўзаро туб бўлмагунча таққосланади. Танлаб олинган сонларнинг туб бўлиш эҳтимоли 0.6 га тенг бўлиб, тўғри келадиган қийматни топиш учун бир неча текширишлар етарли бўлади.

RSA алгоритмининг ҳимояланганлиги. RSA алгоритмининг уч хил мумкин бўлган криптотиҳлил усули мавжуд бўлиб, улар қуйидагилардан иборат:

Оддий танлаш усули. Бунда барча мумкин бўлган махфий калитларни текшириш таклиф қилинади.

Математик анализ. Бундай бир нечта усуллар мавжуд бўлиб, уларнинг ҳаммаси иккита туб сонли кўпайтманинг кўпайтувчиларини топиш моҳияти бўйича эквивалентдир.

Вақт сарфи бўйича анализ. Шифрлаш алгориминининг бажарилишига кетган вақтни анализ қилишга қаратилган.

Оддий танлаш усулига қарши ҳимоя RSA да ҳам, қолган барча криптотизимлардагидек катта ҳажмдаги калитларни ишлатишдир. Бундай ёндашишда e ва d қанча катта битдан иборат бўлса шунча яхши. Лекин калитларни генерация қилишда мураккаб ҳисоблашларни ишлатиш ҳамда шифрлаш/дешифрлаш калитларининг узунлигининг катта бўлиши тизимни секин ишлашига олиб келади.

RSA криптотаҳлилида 3 хил математик ёндашувни ажратиб кўрсатиш мумкин.

nни иккита туб кўпайтувчиларга ажратиш. Бу ўз навбатида $\varphi\ n = p-1\ \ q-1$ ҳисоблашни, бу эса $d = e^{-1}(mod\varphi(n))$ ни аниқлаб олиш имконини беради.

Олдиндан p ва q ни ҳисобламасдан туриб, тўғридан тўғри $\varphi(n)$ аниқлаш.
Олдиндан $\varphi(n)$ ни аниқламасдан туриб, тўғридан тўғри d ни аниқлаш.
Кўп ҳолларда RSA шифри криптотаҳлилида n қийматни иккита туб кўпайтувчига ажратиш масаласи муҳокама қилинади. Берилган n бўйича $\varphi(n)$ ни аниқлаш масаласи билан n ни кўпайтувчиларга ажратиш масаласи билан эквивалент ҳисобланади. Ҳозирги кундаги маълум алгоритмларда e ва n орқали d ни аниқлаш муаммосига кетадиган вақт билан, кўпайтувчиларга ажратиш муаммосига кетадиган вақт бир хил. Шундай экан кўпайтувчиларга ажратиш масаласини ечишга кетадиган вақтни RSA ни ҳимояланганлини баҳолашга сарфлаш мумкин.
Эг-Гамал шифрлаш алгоритми. Ушбу очиқ калитли шифрлаш алгоритми дискерт логарифмлаш муаммосига асосланган бўлиб, калитлар узунлиги тенг бўлган ҳолда бардошлиги RSA алгоритми алгоритми бардошлигига тенг.
Калит генератори. Эл-Гамал алгоритмида калит генератори қуйидаги босқичлардан иборат:
p – туб сон танланади;
$g<p$ шартни қаноатлантирувчи g бутун сон танланади;
махфий калит сифатида $a<p$ шартни қаноатлантирувчи бутун сон танланади;
очиқ калит сифатида $y = g^a mod p$ ҳисобланади;
очиқ калитлар жуфти (y, g, p) маълумотни шифрловчи томонларга ёки ихтиёрий одамларга тарқатилади.
Очиқ матнни шифрлаш. Шифрланиши керак бўлган M очиқ матн ва очиқ калитлар жуфтига эги фойдаланувчи қуйидаги кетма – кетликдаги амалларни бажаради:
p сонидан кичик бўлган ва *ЭКУБ(k, p-1)=1* шартни бажарувчи k -сонини танлаб олинади;
k сон асосида $r = g^k mod p$ ҳисобланади;
очиқ матннинг ҳар бир белгиси учун $c = M * y^k mod p$ тенгликни ҳисоблаш орқали шифрматн олинади;
шифрлаш амалга оширилгач, k сон ўчириб ташланади ва қабул қилувчига *(r, c)* жуфтлик юборилади.
Шифрматнни дешифрлаш. Шифрматн ва махфий калитга эга фойдаланувчи қуйидаги кетма – кетликларни бажариш орқали очиқ матнга эга бўлади:
қабул қилинган маълумотлар асосида $m = c * r^{p-a-1} mod p$ очиқ матн ҳисобланади.
Ушбу алгоритм асосида содда мисол қуйида келтирилган:
А томон ўзининг махфий калити асосида очиқ калит жуфтини ҳосил қилади ва уни Б томонда юборади. Олинган қийматлар қуйидагилар:
$g=3;\ p=31;\ a=4;\ y = g^a mod p$ =(3^4)mod31=19. Бу ерда *(p,g,y)* – очиқ калитлар жуфти ва a махфий калит.
Шифрлаш. Бу босқич А томоннинг очиқ калитларига эса Б томондан амалга оширилади. Очиқ маълумот сифатида M=CDEF (2,3,4,5 –алфавитдани ўрни) олиниб, ЭКУБ(k , $p-1$) =1 шартни қаноатлантирувчи $k=7$ танланди. Шундан сўнг қуйидагилар ҳисобланади:

$r = g^k modp$ =(3^7)mod31=17;
C1= $m * y^k modp$ =2*(19^7)mod31=14;
C2= $m * y^k modp$ =3*(19^7)mod31=21;
C3= $m * y^k modp$ =4*(19^7)mod31=28;
C4= $m * y^k modp$ =5*(19^7)mod31=4;
Шундан сўнг C1,C2,C3,C4 лардан иборат C ва r A томонга юборилади.
Дешифрлаш. Бу жараён махфий калитга эга бўлган A томондан амалга оширилади ва очиқ матн олинади:
M1= $C1 * r^{p-a-1} modp$ =14*17^(31-1-4)mod31=2;
M2= $C2 * r^{p-a-1} modp$ =21*17^(31-1-4)mod31=3;
M3= $C3 * r^{p-a-1} modp$ =28*17^(31-1-4)mod31=4;
M4= $C4 * r^{p-a-1} modp$ =4*17^(31-1-4)mod31=5.
Бу ерда дискерт логарифмлаш муаммоси сифатида очиқ калитлар жуфти берилганда $y = g^a modp$ тенгламадан a махфий калитни топиш бўлиб, ҳозирда ушбу муаммонинг оптимал усули мавжуд эмас.

Эллиптик эгри чизиқ ва параметрли алгебра муаммосига асосланган шифрлаш усуллари

Сўнги йилларда яратилган ассимтерик шифрлаш усулларига асос бўладиган муаммолардан бири бу – *эллиптик эгри чизиқлар* (ЭЭЧ) муаммосидир. Ушбу муаммо асосида ишлаб чиқилган алгоритмлар шифрлашда ва электрон рақамли имзо алгоритмларида фойдаланилади. Ушбу муаммо тури юқорида келтирилган алгоритмларга қараганда самарали бўлиб, бир бардошлиликга эга эга бўлганда, кичик калит узунлигига тенг бўлади ва кам ресурс талаб этади.

Амалда эллиптик эгри чизиқлардан фойдаланилганда майддон тушинчаси киритилган бўлиб, уларда ечимларни чеклаш учун ишлатилади. Қуйида фойдаланиладиган майдон турлари келтирилган:

F_p майдонда, бу ерда *p – туб сон* ва p>3;

F_{2^m} майдон.

Эллиптик эгри чизиқ тенгламаси чекланган майдонда қуйидагича ифодаланади:

$$y^2 modp = (x^3 + ax + b) modp$$

Бу ерда $4a^3 + 27b^2 \ modp \neq 0, \quad x, y, a, b \in [0, p-1]$ - F_p майдонда аниқланган эллиптик эгри чизиқ, p – туб сон.

8.2 - жадвал

Аниқланган майдонда нуқталарни қўшиш ва иккилантириш

Нуқталарни қўшиш	Нуқталарни иккилантириш
$x_R = \ \lambda^2 - x_P - x_Q \ modp$	$x_R = \ \lambda^2 - 2x_P \ modp$
$y_R = \ \lambda \ x_P - x_R \ - y_P \ modp$	$y_R = \ \lambda \ x_P - x_R \ - y_P \ modp$
$\lambda = \frac{y_Q - y_P}{x_Q - x_P} modp$	$\lambda = \frac{3x_P^2 + a}{2y_P} modp$

Эллиптик эгри чизиқли дискрет логарифм муаммоси: *K* чекли майдон ва *G* нуқтада тартиби *n* бўлган *G* нуқта, *Q∈E(K)* нуқтада *E* ЭЭЧ берилган. *Q=[d]G*

шартни қаноатлантирувчи d, $0 \le d \le n-1$ бутун сонни топиш талаб этилади.

8.3 – жадвал

Қуйида ЭЭЧ ларга асосланган шифрлаш алгоритми

$$E_p \ a, b \ , p - \text{туб сон. C} - \text{E ЭЭЧдаги иётиёрий нуқта}$$

Алиса

α (α <p) ва E ЭЭЧда A нуқта олинади.

$$A_1 = \alpha \ C + A \ , \ A_2 = \alpha A$$

α, A – махфий калит

$A_1, A_2 -$ очиқ калит

$A_b = \alpha * B_2$ – Боб учун Алиснинг махсус очиқ калити

Дешифрлаш

$$M = E_2 - (\alpha E_1 + \alpha B_1 + B_a)$$

Боб

β (β <p) ва E ЭЭЧда B нуқта олинади.

$$B_1 = \beta \ C + B \ , \ B_2 = \beta B$$

β, B – махфий калит

$B_1, B_2 -$ очиқ калит

$B_a = \beta * A_2$ – Алис учун Бобнинг махсус очиқ калити

Шифрлаш

$$E_1 = \gamma * C;$$

$$E_2 = M + \ \beta + \gamma \ A_1 - \gamma A_2 + A_b$$

$\gamma -$ матнинг ҳар бир байти учун ихтиёрий танланади

Шифрлаш амалига очиқ маълумотлардан нуқта сифатида фойдаланилган. Яъни, маълум жадвалдан фойдалунилган ҳолда, ЭЭЧ нуқталарига алифбо белгилари бириктирилади ва ҳар бир белгини шифрлашда унга мос нуқта олинади (8.2 - расм).

*	a	b	c	d	e	f	g	h
∞	(5,25)	(1,30)	(21,32)	(7,25)	(25,12)	(4,28)	(0,34)	(16,17)
I	j	k	l	m	n	o	p	q
(15,26)	(27,32)	(9,4)	(2,24)	(26,5)	(33,14)	(11,17)	(31,22)	(13,30)
r	s	t	u	v	w	x	y	z
(35,21)	(23,7)	(10,17)	(29,6)	(29,31)	(10,20)	(23,30)	(35,16)	(13,7)

1	2	3	4	5	6	7	8	9	0
(31,15)	(11,20)	(33,23)	(26,32)	(2,13)	(9,33)	(27,5)	(15,11)	(16,20)	(0,3)
#	@	!	&	$	%				
(4,9)	(25,25)	(7,12)	(21,5)	(1,7)	(5,12)				

8.2 – расм. Белгиларни ЭЭЧдаги белгилар орқали ифодалаш

Даража параметрли муаммосига асосланган ассиметрик шифрлаш аалгоритмлари. Очиқ калитли криптоалгоритмлар асосини ташкил этувчи етарли катта сонларни туб кўпайтувчиларга ёйиш, характеристикаси етарли катта бўлган чекли майдонларда дискрет логарифмларни ҳисоблаш, ЭЭЧларда рационал координатали нуқталарни топиш, уларни қўшиш ҳамда тартибини аниқлаш масалаларини ечиш мураккабликлари билан боғлиқ ҳолда параметрли группа амалларидан фойдаланиш янги носимметрик алгоритмлар яратиш усулларига олиб келади [4].

Агар параметрли группа $(F_p; ®)$ да группа ташувчиси F_p нинг g ва y элементлари берилган бўлса, R параметр ва даража кўрсаткичи x ни топинг;

бу ерда $y \equiv g^{\backslash x} \ (\text{mod } p)$ p модули бўйича R параметр билан g нинг x-даражасини ифодалайди, бунда p – туб сон, $R< p$.

Параметрли даражага кўтаришда қуйидаги амаллардан фойдаланилади:

R параметр билан p модули бўйича кўпайтириш амали

$X \circledR Y \ (\text{mod } p) \equiv X + (1 + X R)Y \ (\text{mod } p)$ каби ифодаланади.

X ўзгарувчининг p модуль бўйича R параметр билан тескарилаш амали $X^{\backslash -1}$ кўринишда белгиланади ва қуйидагича ифодаланади:

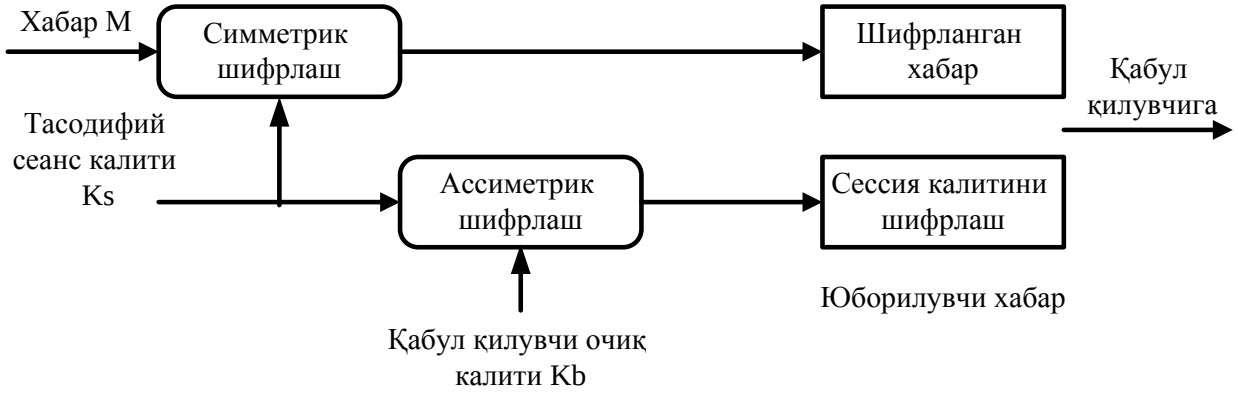
$X^{\backslash -1} \equiv - X(1 + XR)^{-1} \ (\text{mod } p)$.

Ушбу муаммога асосланган ҳолда Ўзбекистон олимлари томонидан шифрлаш алгоритмлари, электрон рақамли имзо алгоритмлари ва хэш функция алгоритмлари ишлаб чиқилган.

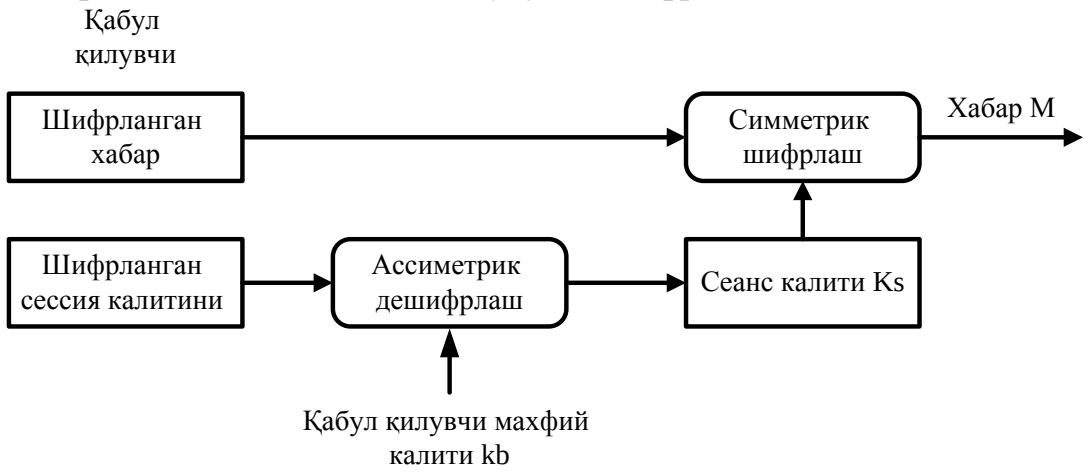
Ассиметрик шифрлаш усулларини ахборот хавфсизлигини таъминлашда фойдаланиш таҳлили

Ассиметрик шифрлаш усуллари симметрик шифрлаш усулларига қараганда маълумотларни шифрлаш ва дешифрлашда кўп вақт талаб этади. Бу камчилик уларда катта сонлар устида математик амаллар бажарилиши билан белгиланади. Бу эса катта ҳажмдаги маълумотларни шифрлашда ноқулайлик туғдиради.

Шунинг учун одатда катта ҳажмдаги маълумотлар симметрик шифрлаш алгоритми асосида шифрланиб, унинг калити ассиметрик шифрлаш алгоритмидан фойдаланилиб юборилади (8.3, 8.4 - расмлар).



8.3 - расм. Комбинацияланган усулда шифрлаш



8.4 - расм. Комбинацияланган усулда дешифрлаш

Қуйидаги жадвалда симметрик ва турли ассиметрик шифрлаш усулларида бир хил бардошлиликка эга бўлганда, калит узунликлари нисбати берилган.

8.4 – жадвал

Шифрлаш алгоритмларининг калит узунлиги нисбатлари (NIST маълумоти)

Симметрик	Ассиметрик алгоритмлар (бит)	
алгоритмлар (бит)	RSA ва Эл-Гамал	ЭЭЧ
56	512	112
80	1024	160
112	2048	224
128	3072	256
192	7680	384
256	15360	521

Юқоридаги жадвалдан келиб чиқиб ва ассиметрик шифрлашларда калит узунликлари муҳимлигини билган ҳолда, мос шифрлаш алгоритми танланиши шарт. Маълумотларни шифрлашда симметрик шифрлаш алгоритмлардан фойдаланиш катта самара беради.

Юқоридаги комбинацион усулдан:

тармоқда маълумотларни шифрлаб юборишда;

протоколларда махфий калитларни узатишда ва ҳак. соҳаларда фойдланиш мумкин.

Бундан ташқари ассиметрик шифрлаш усулларидан асосан электрон рақамли имзо алгоритмларида фойдаланилади.

Назарий саволлар

Симметрик шифрларнинг камчиликлари нимадан иборат.

Ассиметрик шифрларнинг умумий моҳияти нимада.

Ассиметрик шифрларни яратишда фойдаланилган математик муаммолар.

Ассиметрик шифрлардан хавфсизлик соҳасида фойдаланиш.

9 - маъруза

Мавзу: Хэш функциялар ва маълумотни бутунлигини таъминлаш

Режа:

CRC тизимлари.

Калитли хэш функциялар

Калитсиз хэш функциялар.

Маълумотни бутунлигини таъминлаш усулларининг хавфсизлиги таҳлили ва уларнинг амалда фойдаланилиши.

Таянч терминлар: CRC тизимлари, хэш функция, хабарларни аутентификациялаш тизимлари, коллизия.

CRC тизимлари

Криптографияда маълумотнинг бутунлигини текширишда кўплаб усуллардан фойдаланилади. Улар ўзларининг имкониятлари, талаблари ва хавфсизлик даражалари билан ажралиб турадилар. Қуйида уларнинг турлари келтирилган.

CRC (Cyclic Redundancy Check) тизимлар маълумотни бутунлигини текширишда хатоликни текширувчи кодлардан фойдаланади. Ушбу тизим W. Wesley Peterson томонидан 1961 йилда ихтиро қилинган бўлиб, 32 битли CRC тизим Ethernet учун фойдаланилади.

Мисол ўрнида 14 битли маълумот ва 3-битли CRC тизимидан x^3+x+1 кўпҳадига асосланган ҳолда олиб, маълумот дастлаб иккилик кўринишда ўтказилади.

M=11010011101100 ва CRC 1011 га тенг. Дастлаб маълумот битига CRC битига мос равишда 0лар қўшилади.

```
11010011101100 000      <--- 3 бит нол қўйилади
1011                    <--- бўлувчи (4 бит) = x³+x+1
----------------
01100011101100 000      <--- натижа
```

Ҳар бир CRC қўшилганда натижа узунлиги бир битга камаяди. Ушбу кетма-кетлик маълумот узунлиги тўлиқ 0 бўлмагунга қадар давом эттирилади ва тўлдирилган 0лар сонига тенг бўлган қолдиқ натижа олинади.

```
11010011101100 000
1011
01100011101100 000
 1011
00111011101100 000
  1011
00010111101100 000
    1011
00000001101100 000
         1011
00000000110100 000
           1011
00000000011000 000
```

```
              1011
00000000001110 000
               1011
00000000000101 000
                101 1
----------------
00000000000000 100
```

Ушбу олинган 100 қиймат қолдиқ саналиб, маълумот учун CRC қийматни билдиради.

Маълумотни текшириш жараёни ҳам юқоридаги жараёнга ўхшаш бўлиб, фақат қўшиладиган битларнинг биринчи бирлик битга ўзгартирилади.

```
11010011101100 100     <--- маълумот & текширувчи қиймат билан
1011                          <--- бўлувчи
01100011101100 100            <--- натижа
 1011                         <--- бўлувчи ...
00111011101100 100
......
00000000001110 100
               1011
00000000000101 100
                101 1
-----------------
                    0 <--- қолдиқ
```

Агар натижавий қолдиқ 0 га тенг бўлса, келган маълумот ўзгармаган акс ҳолда ўзгарган деб топилади.

Амалда кўплаб фойдаланиладиган CRC кўпҳади узунликлари қуйидагича:

- 9 бит (CRC-8);
- 17 бит (CRC-16);
- 33 бит (CRC-32);

65 бит (CRC-64).

Калитли хэш функциялар

Криптографияда, хэш функция деб ихтиёрий узунликдаги (битлар ёки байтлар бирликларида) маълумотни бирор фиксирланган (белгиланган) узунликдаги (битлар ёки байтлар бирликларига) қийматга ўтказиб берувчи функцияга айтилади. Хэш функциялардан амалда статистик тажрибалар ўтказишда, мантиқий қурилмаларни текширишда, маълумотлар базасида тез қидириб топиш алгоритмларини яратишда ва маълумотлар базасидаги маълумотларнинг бутунлигини текширишда фойдаланилади.

Криптографияда хэш функциялардан қуйидаги муаммоларни ҳал қилишда фойдаланилади:

маълумотни узатишда ёки сақлашда унинг тўлалигини назорат қилиш учун;

маълумотнинг манбаини аутентификация қилиш учун.

Маълумотларни узатишда ёки сақлашда уларнинг тўлалигини назоратлашда ҳар бир маълумотнинг хэш қиймати (бу хэш қиймат маълумотни аутентификация қилиш коди ёки “имитоқўйиш”-маълумот

блоклари билан боғлиқ бўлган қўшимча киритилган белги дейилади) ҳисобланилади ва бу қиймат маълумот билан бирга сақланилади ёки узатилади. Маълумотни қабул қилган фойдаланувчи маълумотнинг хэш қийматини ҳисоблайди ва унинг хэш қиймати билан солиштиради. Агар таққослашда бу қийматлар мос келмаса, маълумот бутунлиги бузилганлигини англатади.

“Имитоқўйиш”лар ҳосил қилиш учун фойдаланиладиган хэш функциялар назорат йиғиндисидан фарқли равишда маълумотни сақлаш ва узатишда рўй берадиган тасодифий хатоларни аниқлабгина қолмасдан, рақиб томонидан қилинган актив ҳужумлар тўғрисида ҳам огоҳлантиради. Бузғунчи хэш қийматни осонлик билан ўзи ҳисоблаб топа олмаслиги ва муваффақиятли имитация қилиши ёки маълумотни ўзгартира олмаслиги учун хэш функция бузғунчига маълум бўлмаган махфий калитга эга бўлиши керак. Бу махфий калит фақатгина маълумотни узатувчи ва қабул қилувчи томонларга маълум бўлиши керак. Бундай хусусиятга эга хэш функцияларга калитли хэш функциялар дейилади.

Калитли хэш функциялар ёрдамида ҳосил қилинадиган “имитоқўйиш”лар имитация (impersonation) туридаги ҳужумларда қалбаки маълумотларни ҳосил қилишга (fabrication) ва “ўзгартириш” (substitution) туридаги ҳужумларда узатиладиган маълумотни модификация (modification) қилишга йўл қўймасликда фойдаланилади.

Маълумот манбаининг аутентификациялаш масаласи ахборот-коммуникация тизимларининг бир-бирига ишонмайдиган икки томони орасида маълумот алмашинувида юзага келади. Бу масалани ҳал қилишда иккала томон ҳам биладиган махфий калитдан фойдаланиб бўлмайди. Бу ҳолатда маълумотнинг манбаини аутентификация қилишга имкон берадиган электрон рақамли имзо схемаси қўлланилади. Бунда одатда фойдаланувчининг махфий калитига асосланган имзо қўйишдан олдин хатолик кодини аниқловчи хэш функция ёрдамида маълумот сиқилади. Бу ҳолда хэш функция махфий калитга эга бўлмайди ҳамда у фиксирланган бўлиши ва ҳаммага маълум бўлиши мумкин. Унга қўйилган асосий талаб имзоланган ҳужжатни ўзгартириш ҳамда бир хил хэш қийматга эга бўлган иккита ҳар хил маълумотни танлаш имконияти йўқлигининг кафолатидир. Агар бир хил хэш қийматга эга бўлган иккита ҳар хил маълумот мавжуд бўлса, бу маълумотлар жуфти коллизия ҳосил қилади дейилади.

Юқорида келтирилганларга асосланиб, қуйидаги таъриф киритилади. М орқали элементлари маълумотлардан иборат бўлган тўплам белгиланади. Одатда маълумотлар бирор алфавитнинг, кўпинча иккилик саноқ системаси символлари кетма-кетлигидан иборат бўлади.

Хэш функция деб, ихтиёрий узунликдаги М маълумотни фиксирланган узунликдаги h(M)=H қийматга акслантиб берувчи, осон ҳисобланадиган бир томонли функцияга айтилади.

Хэш қиймат: “хэш қиймат”, “свертка”, “дайджест”, “бармоқ излари” деб ҳам аталади.

Хэш функцияга нисбатан қуйидаги талаблар қўйилади:

1.Ихтиёрий узунликдаги матн учун қўллаб бўлишлик.
2.Чиқишда белгиланган узунликдаги қийматни беришлик.
3.Ихтиёрий берилган x бўйича h(x) осон ҳисобланишлик.
4.Ихтиёрий берилган H бўйича h (x)= H тенгликдан x ни ҳисоблаб топиб бўлмаслик. (Бир томонлилик хусусияти)
5.Олинган x ва y≠x матнлар учун h(x)≠ h(y) муносабат ўринли бўлиши. (Коллизияга бардошлилик хусусияти).
Калитли хэш функциялардан фойдаланишда уларга қуйидаги асосий талаблар қўйилади:
фабрикациянинг имконияти йўқлиги;
модификациянинг имконияти йўқлиги.
Биринчи талабга кўра, хэш қиймат берилганда унга мос бўлган маълумотни танлашнинг мураккаб бўлишини билдиради. Иккинчи талаб эса, маълумот ва унинг хэш қиймати берилганда, хэш қиймати шунга тенг бўладиган бошқа маълумотни танлаш мураккаб бўлишини англатади.
Баъзида, бу иккита хоссани битта кучлироқ хоссага – *ҳисоблаш бардошлилиги* хоссасига бирлаштирилади. Бу талаб хэш қийматлари маълум бўлган берилган $x_1, x_2, \ldots, x_l$ маълумотлар учун хэш қийматлари шулардан бирига тенг бўладиган бошқа x, $x \neq x_i$, $i = 1, l$ маълумотни танлашнинг мураккаблигини билдиради.
Мураккаблик деганда, масалани реал вақт давомида замонавий ҳисоблаш қурилмаларидан фойдаланиб ҳал қилиш имконияти бўлмайдиган ҳисоблаш мураккаблиги тушунилади
Калитли хэш функциялар бир-бирига ишонувчи томонлар орасида ишлатилади ва улар умумий махфий калитга эга бўладилар. Одатда бу шароитда иккинчи томон маълумотни қабул қилиб олганлигини тан олмаслик ёки уни ўзгартириш ҳолатидан ахборот-коммуникация тизимини ҳимоя қилиш талаб қилинмайди. Шунинг учун калитли хэш функциялардан коллизияларга бардошлилик талаб қилинмайди.
Калитли хэш функцияларга хос бўлган “имитация” қилиш, яъни бўш каналда қалбаки маълумотни узатиш ҳамда узатилаётган маълумотни қалбаки маълумотга алмаштириш каби ҳужумларини келтириш мумкин.
Ҳисоблаш бардошлилиги хоссасидан, хэш функцияда фойдаланилган калитни аниқлаш имконияти йўқлиги келиб чиқади, калитни билиш эса иҳтиёрий маълумотнинг хэш қийматини ҳисоблаш имкониятини беради. Тескари тасдиқ эса ўринли эмас, сабаби баъзи бир ҳолатларда калитни олдиндан билмасдан туриб, хэш қийматни танлаш мумкин.
Мисол тариқасида кенг тарқалган, бир қадамли сиқиш функцияси ёрдамида қурилган қуйидаги кўринишдаги хэш функцияни кўриш мумкин:
$f_k(x, H) = E_k(x \oplus H)$,
бу ерда E_k - блоклаб шифрлаш алгоритми.

M маълумотларнинг $h(M)$ қийматларини ҳисоблаш учун маълумот кетма-кет келган m битли $M_1, M_2, \ldots, M_N$ блоклар кўринишида ифодаланади. Агар маълумотнинг узунлиги блокнинг узунлигига каррали бўлмаса охирги

блок бирор махсус шаклда тўлиқ блокгача тўлдирилади. Хэш қийматни ҳисоблаш алгоритми кўриниши қуйидагича бўлади:

$H_0 = 0,$

$H_i = E_k(M_i \oplus H_{i-1}), \quad i = 1, \ldots, N,$

$h(M) = H_N.$

Калитли хэш функцияларни қуришда калитсиз хэш функциялардан фойдаланган ҳолда ҳосил қилиш усули ҳам ишлатилади. Бунда хэш қийматни ҳисоблаш учун калит берилган маълумотга қўшиб ёзиб қўйилади.

Агар калит берилган маълумотдан олдин ёки маълумотдан сўнг тўғридан-тўғри қўшиб қўйилса, баъзи ҳолларда маълумотни модификация қилишга имкон бериши мумкин.

Масалан, k калит маълумотнинг бошига $h_k(x) = h(k, x)$ формулага асосан қўшиб қўйилган бўлсин. Агар h функция формулага асосан бир қадамли сиқувчи функциялар ёрдамида қурилган бўлса, у ҳолда M ва $H = h(k, M)$ ларнинг маълум қийматлари бўйича ҳоҳлаган M' қўшиб ёзилган (M, M') кўринишдаги ихтиёрий маълумот учун бу функциянинг қийматларини ҳисоблаш мумкин. Бу хэш функцияни ҳисоблашнинг итеративлиги билан изоҳланади, чунки $H' = h(k, M, M')$ қийматни топиш учун k калитнинг қийматини билиш шарт эмас, H қийматнинг ҳисобланган оралиқ қийматларидан фойдаланиш етарли. Шунинг учун бундай функция модификацияга бардошли эмас.

Агар калит маълумотнинг охирига $H = h_k(M) = h(M, k)$ формулага асосан қўшилган бўлса, h функция учун коллизияни, яъни $h(x_1) = h(x_2)$ бўладиган $x_1, x_2, x_1 \neq x_2$ жуфтликни билиш иҳтиёрий k калит учун $h(x_1, k) = h(x_2, k)$ қийматни ҳисоблашга имкон беради. Шунинг учун $M = x_1$ маълумотни модификация қилиш мураккаблиги $O(2^n)$ катталик билан эмас, коллизияларни қидириш мураккаблиги билан таққосланади ва $O(2^{n/2})$ билан баҳоланади, чунки бу ҳолда *“туғилган кун” парадокси*га асосланган ҳужум ўринли бўлади.

Шуларни эътиборга олган ҳолда, калитни маълумотга бир марта эмас, бир неча марта қўядиган усуллар фойдаланилади. Бунга қуйидаги иккита усулни мисол қилиб келтириш мумкин:

$H = h(k, y, M, k),$

$H = h(k, y_1, h(k, y_2, M)),$

бу ерда y, y_1 ва y_2 лар k калитнинг n узунликдаги блокнинг карралисигача ўлчовга тўлдирилганидир. Калитсиз хэш функциялар учун бундай усул эффектив ҳисобланадиган ва ҳужумларга бардошли калитли хэш функцияларни қуриш имконини беради. Бундай усулнинг камчилик томони шундаки, хэш қийматнинг n узунлиги жуда катта бўлади. Одатда, тўлаликни текшириш учун хэш қиймат узунлиги 32 дан 64 битгача бўлиши, $2^{32} \leq n \leq 2^{64}$ бажарилиши керак, аутентификация учун эса $n \geq 2^{128}$ шартнинг бажарилиши зарур.

Юқорида айтиб ўтилгани каби блоклаб шифрлаш алгоритмига

асосланган ёки калитсиз хэш функцияни ҳисоблашга асосланган алгоритмлардан ташқари замонавий ЭҲМларда қўллаш самарадорлигини ҳисобга олиб тузилган алгоритмлар ҳам мавжуд. Бунга MAA (Message Authenticator Algorithm) калитли хэш функция алгоритмини мисол қилиб келтиришимиз мумкин.

Калитсиз хэш функциялар

Калитсиз хэш функциялар *хатоларни аниқлаш кодлари* (modification detection code (MDC) ёки manipulation detection code, message integrity code (MIC)) деб ҳам юритилади. Калитсиз хэш функция – қўшимча воситалар (шифрлаш ёки рақамли имзо) ёрдамида маълумотнинг тўлалигини кафолатлайди. Бу хэш функциялар бир-бирига ишонувчи ҳамда бир-бирига ишонмайдиган фойдаланувчилар тизимларида ишлатилади.

Одатда калитсиз хэш функциялардан қуйидаги хоссаларни қаноатлантириши талаб қилинади:

бир томонлилик;

коллизияга бардошлилик;

хеш қийматлари тенг бўлган иккита маълумотни топишга бардошлилик.

Биринчи шарт бажарилганда, берилган хэш қийматга эга бўлган маълумотни топишнинг мураккаб эканлигини, иккинчи шарт бажарилганда бир хил хэш қийматга эга бўлган маълумотлар жуфтини топишнинг мураккаб эканлигини, учинчи шарт хэш қиймати маълум бўлган берилган маълумот учун хэш қиймати шунга тенг бўлган иккинчи маълумотни топишнинг мураккаб эканлигини билдиради.

Масалан, назорат йиғиндини топувчи CRC хэш функцияси чизиқли акслантириш бўлади ва шунинг учун ҳам бу учта шартдан биронтасини ҳам қаноатлантирмайди.

Калитсиз хэш функцияларга MD4, MD5 ва SHA хэш функциялари мисол бўла олади. Бу алгоритмлар 32 разрядли ЭҲМларда самарали қўлланилишга мўлжалланиб, махсус лойиҳалаштирилган алгоритмлардир.

Ҳозирда кўплаб давлат стандартлари хэш функциялари алгоритмлари калитсиз хэш функция алгоритмларидир. Бунга мисол қилиб Россиянинг ГОСТ Р 34.11-94 хэш функция давлат стандартини, АҚШнинг федерал стандарти FIPS PUB 180 да келтирилган SHA-0, FIPS PUB 180-1 да келтирилган SHA-1, FIPS PUB 180-2 да келтирилган SHA-256, SHA-384, SHA-512 хэш функцияларини, Беларус Республикасининг хэш функция давлат стандарти СТБ 1176.1 – 99 ни, АҚШнинг федерал стандарти SHA туридаги хэш функцияларни яратишга асос бўлган MD туридаги хэш функциялар ва уларнинг модификациялари MD2, MD4 ва MD5 хэш функцияларини (АҚШнинг федерал стандарти айнан MD5 хэш функцияси асосида ишлаб чиқилган), Европа Ҳамжамиятининг RACE дастури доирасида MD4 асосида ишлаб чиқилган RIPE-MD ва унинг модификациялари RIPEMD-160, RIPEMD-256 ва RIPEMD-320 хэш функцияларини, MD5 асосида ишлаб чиқилган HAVAL хэш функциясини ва юқоридаги хэш функциялар алгоритмларидан фарқ қилувчи алгоритмга эга бўлган TIGER хэш функциясини келтириш мумкин.

SHA-1 хэш функцияси алгоритми. Кафолатланган бардошлиликка эга бўлган хэшлаш алгоритми SHA (Secure Hash Algorithm) АҚШнинг стандартлар ва технологиялар Миллий институти (NIST) томонидан ишлаб чиқилган бўлиб, 1992 йилда ахборотни қайта ишлаш федерал стандарти (PUB FIPS 180) кўринишида нашр қилинди. 1995 йилда бу стандарт қайтадан кўриб чиқилди ва SHA-1 деб номланди (PUB FIPS 180-1). SHA алгоритми MD4 алгоритмига асосланади ва унинг тузилиши MD4 алгоритмининг тузилишига жуда яқин. Бу алгоритм DSS стандарти асосидаги электрон рақамли имзо алгоритмларида ишлатиш учун мўлжалланган.

Бу алгоритмда кирувчи маълумотнинг узунлиги 2^{64} битдан кичик бўлиб, хэш қиймат узунлиги 160 бит бўлади. Киритилаётган маълумот 512 битлик блокларга ажратилиб қайта ишланади.

Хэш қийматни ҳисоблаш жараёни қуйидаги босқичлардан иборат:

1-босқич. Тўлдириш битларини қўшиш.

Берилган маълумот узунлиги 512 модул бўйича 448 билан таққосланадиган (маълумот узунлиги ≡ 448 mod 512) қилиб тўлдирилади. Тўлдириш ҳамма вақт, ҳаттоки маълумот узунлиги 512 модул бўйича 448 билан таққосланадиган бўлса ҳам бажарилади.

Тўлдириш қуйидаги тартибда амалга оширилади: маълумотга 1 га тенг бўлган битта бит қўшилади, қолган битлар эса 0 лар билан тўлдирилади. Шунинг учун қўшилган битлар сони 1 дан 512 тагача бўлади.

2- босқич. Маълумотнинг узунлигини қўшиш.

1-босқичнинг натижасига берилган маълумот узунлигининг 64 битлик қиймати қўшилади.

3- босқич. Хэш қиймат учун буфер инициализация қилиш.

Хэш функциянинг оралиқ ва охирги натижаларини сақлаш учун 160 битлик буфердан фойдаланилади. Бу буферни бешта 32 битлик A, B, C, D, E регистрлар кўринишида тасвирлаш мумкин. Бу регистрларга 16 лик саноқ системасида қуйидаги бошланғич қийматлар берилади:

A=0x67452301,
B=0xEFCDAB89,
C=0x98BADCFE,
D=0x10325476,
E=0xC3D2E1F0.

Кейинчалик бу ўзгарувчилар мос равишда янги *a, b, c, d* ва *e* ўзгарувчиларга ёзиб олинади.

4- босқич. Маълумотни 512 битлик блокларга ажратиб қайта ишлаш.

Бу хэш функциянинг асосий цикли қуйидагича бўлади:

for ($t = 0$; $t < 80$; t++){
    $temp = (a <<< 5) + f_t(b, c, d) + e + W_t + K_t$;
    $e = d$; $d = c$; $c = b <<< 30$; $b = a$; $a = temp$;
},

Бу ерда <<< - чапга циклик суриш амали. K_t лар 16 лик саноқ системасида ёзилган қуйидаги сонлардан иборат:

$$\mathbf{K}_t = \begin{cases} \mathbf{5A827999}, & t = 0,...,19, \\ \mathbf{6ED9EBA1}, & t = 20,...,39, \\ \mathbf{8F1BBCDC}, & t = 40,...,59, \\ \mathbf{CA62C1D6}, & t = 60,...,79. \end{cases}$$

$f_t(x, y, z)$ функциялар эса қуйидаги ифодалар билан аниқланади:

$$f_t(\mathbf{x,y,z}) = \begin{cases} \mathbf{X} \wedge \mathbf{Y} \vee \neg \mathbf{X} \wedge \mathbf{Z}, & \mathbf{t} = 0,...,19, \\ \mathbf{X} \oplus \mathbf{Y} \oplus \mathbf{Z}, & \mathbf{t} = 20,...,39,\ 60,...,79, \\ \mathbf{X} \wedge \mathbf{Y} \vee \mathbf{X} \wedge \mathbf{Z} \vee \mathbf{Y} \wedge \mathbf{Z}, & \mathbf{t} = 40,...,59. \end{cases}$$

W_t лар кенгайтирилган маълумотнинг 512 битлик блокининг 32 битлик қисм блокларидан қуйидаги қоида бўйича ҳосил қилинади:

$$W_t = \begin{cases} M_t, & t = 0,...,15, \\ (W_{t-3} \oplus W_{t-8} \oplus W_{t-14} \oplus W_{t-16}) <<< 1, & t = 16,...,79. \end{cases}$$

Асосий цикл тугагандан кейин *a*, *b*, *c*, *d* ва *e* ларнинг қийматлари мос равишда A, B, C, D ва E регистрлардаги қийматларга қўшилади ҳамда шу регистрларга ёзиб қўйилади ва кенгайтирилган маълумотнинг кейинги 512 битлик блокини қайта ишлашга ўтилади.

5- босқич. Натижа.

Маълумотнинг хэш қиймати A, B, C, D ва E регистрлардаги қийматларни бирлаштириш натижасида ҳосил қилинади.

Хэшлаш функциясининг матнлар тўқнашувини топишга нисбатан бардошлилиги га тенг. АҚШда калит узунлиги 128, 192 ва 256 бит бўлган янги шифрлаш стандарти ишлаб чиқилганлиги муносабати билан шу даражадаги бардошлиликка эга бўлган янги хэш функциялар алгоритмларини яратишга эҳтиёж пайдо бўлди. Шу сабабли 2002 йилда АҚШнинг янги хэш функция стандарти PUB FIPS 180-2 қабул қилинди. Бу стандартда тўртта хэш функция - SHA-1, SHA-256, SHA-384 ва SHA-512 -алгоритмлари келтирилган.

Маълумотни бутунлигини таъминлаш усулларининг хавфсизлиги таҳлили ва уларнинг амалда фойдаланилиши

Аутентификация атамаси ахборот-коммуникация тизимларида маълумотлар алмашинуви субъектларининг ҳақиқийликни аниқлашни билдиради. Бу маълумот алмашишдаги барча аспектларга таллуқли бўлиб, алоқа сеансининг, томонларнинг, маълумотнинг ҳақиқийлигини билдиради. Бу алоқа тармоғи орқали узатилган маълумот манбаси ва мазмуни жиҳатидан, маълумотнинг яратилган вақти ҳамда жўнатилган вақти жиҳатидан текширганда ҳақиқий бўлишини англатади.

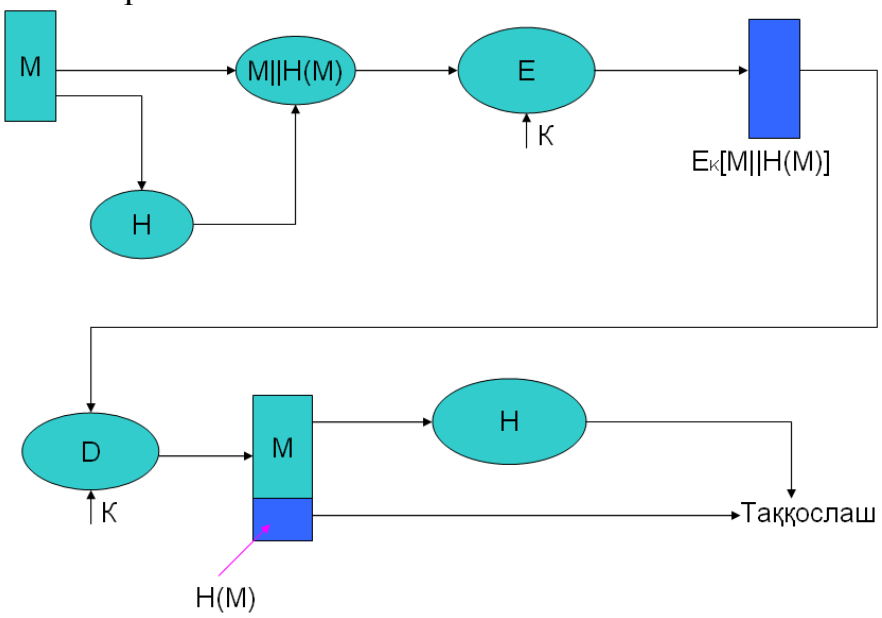
Маълумотнинг тўлалиги (бутунлиги) – маълумот яратилгандан кейин уни сақлашда ва узатишда унинг бегоналар томонидан ўзгартирилмаганлигига ишонч ҳосил қилишни билдиради. Маълумотни ўзгартириш деганда одатда унга қўшимчалар қўшиш, тушириб қолдириш, ўзгартириш ва маълумот қисмларининг ўрнини алмаштириш тушунилади.

Маълумотнинг манбаини аутентификациялаш – қабул қилинган электрон ҳужжат ҳақиқий манба томонидан юборилганлигини тасдиғини олишдир.

Бунда ҳужжат яратилган вақт ва электрон ҳужжатнинг ягоналигини текшириш талаб қилинмайди. Ҳужжат ягоналигининг бузилиши деганда уни қайтадан узатиш ёки ундан қайтадан фойдаланиш тушунилади.

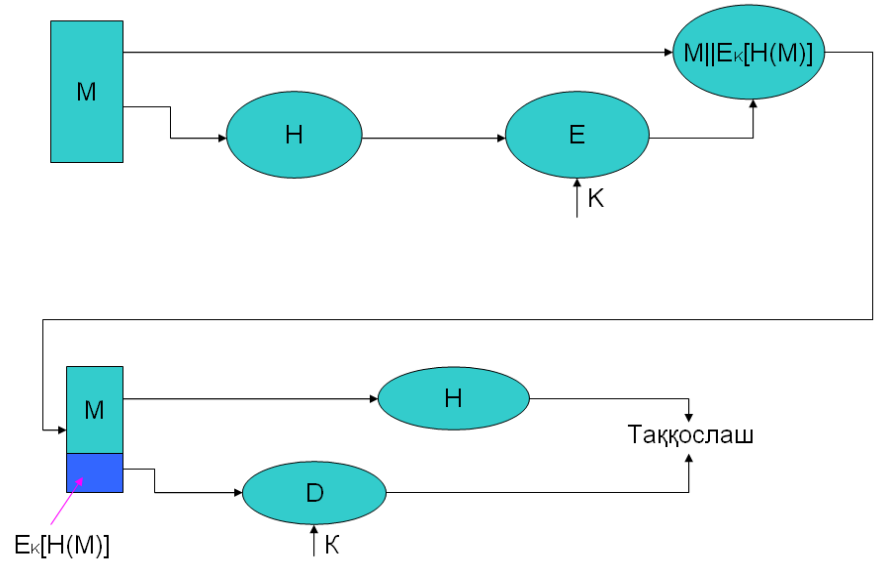
Маълумотнинг бутунлиги (тўлалигини) ва маълумотнинг манбаини аутентификациялаш тушунчалари бир-бири билан чамбарчас боғлиқдир. Ҳақиқатан ҳам, агар маълумот модификация қилинган бўлса, унинг манбаи ҳам ўзгаради. Агар манба аниқланмаган бўлса, тўлалик масаласини ҳал қилиб бўлмайди.

Хэш функцияларни амалда ахборот-коммуникация тизимларида қўллаш схемалари:



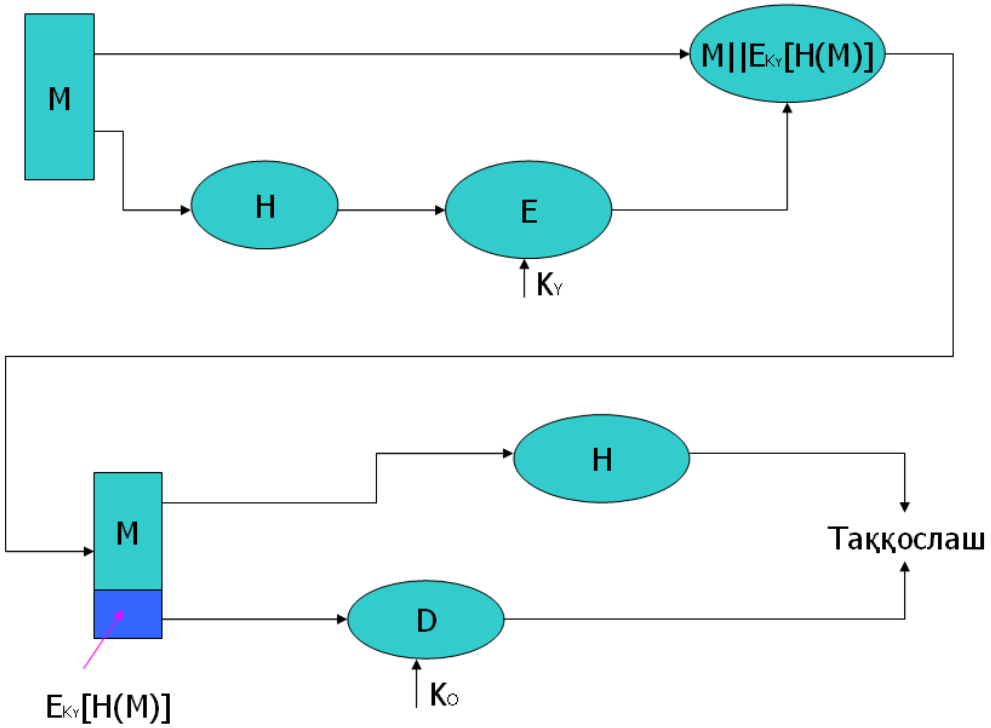
9.1 – расм. Маълумот бутунлиги ва махфийлигини таъминлаш

Юқоридаги келтирилган 9.1-расмда маълумотнинг бутунлиги таъминлаш хэш функция ёрдамида амалга оширилса, маълумот ва унинг хэш функциясини қўшиб шифрлаш орқали маълумотнинг махфийлиги таъминланади. Бунда шифрлашда симметрик ва ассиметрик шифрлаш алгоритмларидан фойдаланиш мумкин. Ассиметрик шифрлашдан фойдаланган ҳолда ушбу расмдаги тизим бизга ЭРИ алгоритмларини беради.



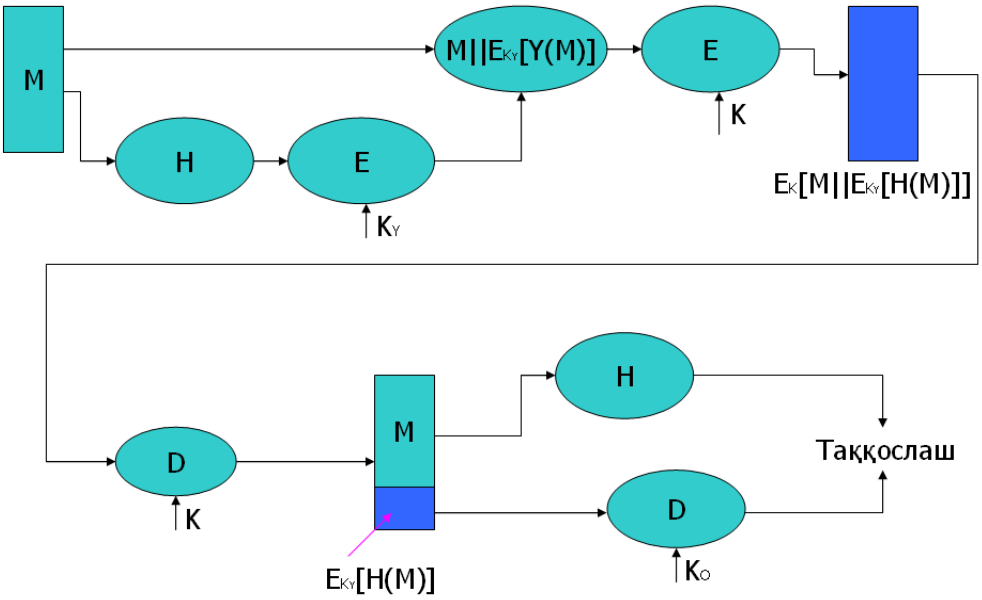
9.2 –расм. Маълумотнинг бутунлигини таъминлаш

Юқоридаги келтирилган 9.2-расмда маълумотнинг хэш функциясини шифрлаш орқали фақат маълумотнинг бутунлигини таъминланади. Маълумотнинг ўзи очиқ юборилганлиги сабабли, унинг махфийлиги таъминланмайди. Маълумотнинг хэш функциясини шифрлашдан мақсад унинг йўлда алмаштирилишини олдини олиш.



9.3 – расм. Маълумотнинг бутунлигини таъминлаш

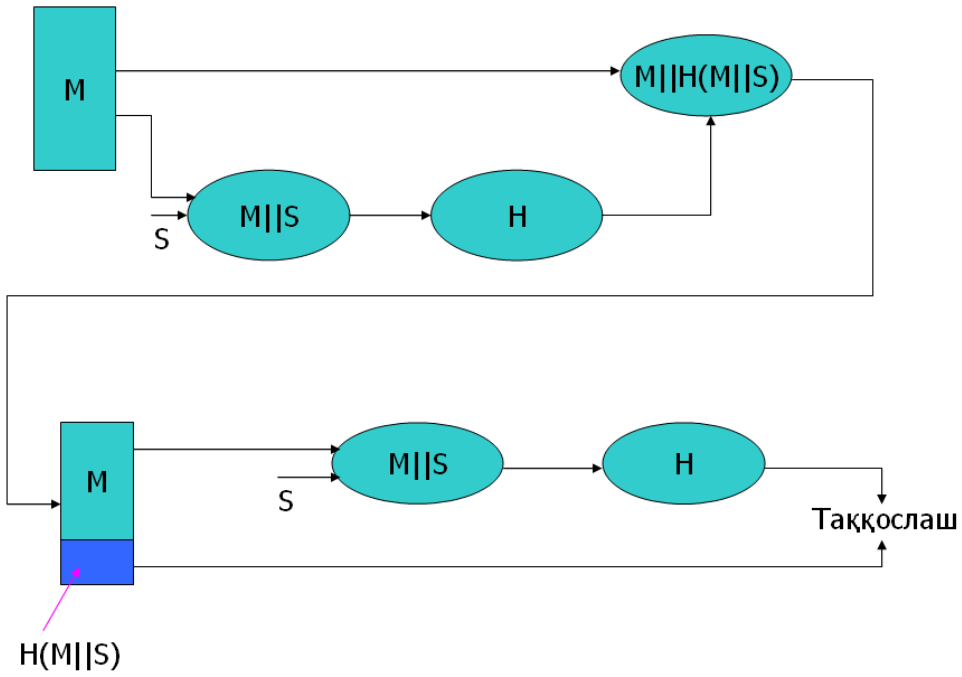
Юқоридаги келтирилган 9.3-расмда ҳам фақат маълумотнинг бутунлиги таъминланиб, уни ассиметрик шифрлаш алгоритми ёрдамида амалга оширилган ва ЭРИ алгоритмини билдиради. Маълумотни шифрлашда махфий калитдан фойдаланилиб, уни очиш очиқ калит орқали амалга оширилади.



9.4 – расм. Маълумотнинг бутунлигини ва махфийлигини таъминлаш

Юқоридаги келтирилган 9.4-расмда маълумотнинг ҳам бутунлиги, ҳам махфийлиги таъминланади. Бунда икки турдаги шифрлашдан фойдаланилган бўлиб, маълумотнинг хэш қиймати ассиметрик шифрлаш алгоритмидан фойдаланса, шифрланган хэш қиймат ва маълумотнинг ўзини симметрик шифрлаш алгоритмидан фойдаланган ҳолда шифрлайди.

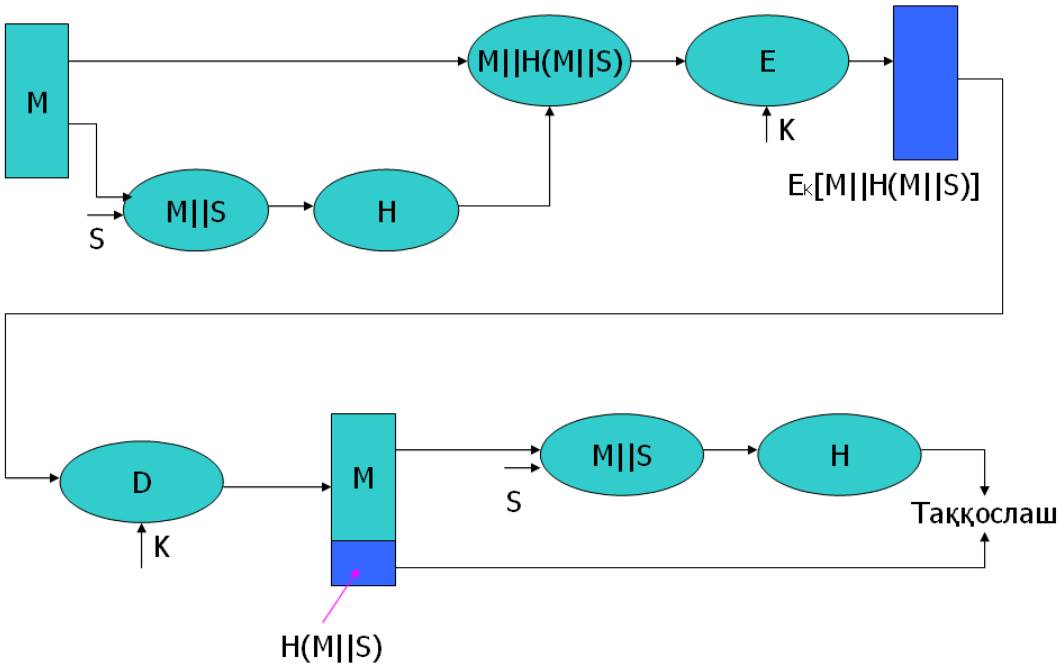
Қуйидаги 9.5-расмда маълумотнинг бутунлиги таъминланган бўлиб, бунда S(salt) деб номланган махфий калитдан фойдаланилиб маълумотнинг хеш қиймати олиняпти. Бунда келтирилган тузулиш калитли хеш функциялар вазифасини бажаради. Бунда маълумотни текшириш имконияти фақат S қийматни билган одамга мавжуд бўлади. Ушбу структурада келтирилган тизим амалда паролларни сақлашда кенг фойдаланилади.



9.5 – расм. Маълумотнинг бутунлигини таъминлаш

Қуйида келтирилган 9.6-расмда S калитдан фойдаланилган ҳолда

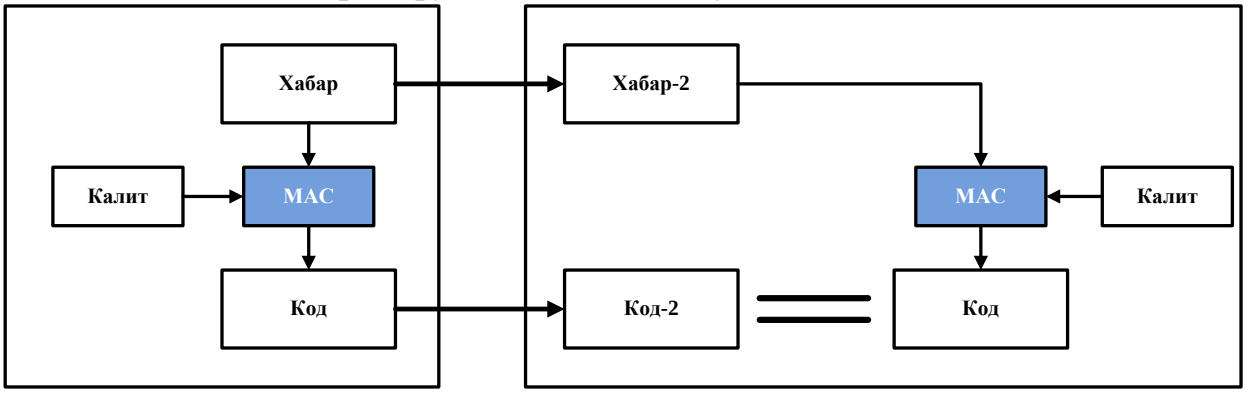
маълумотни хэш қиймати ҳисобланса, хэш қиймат ва маълумотнинг ўзи шифрлаш алгоритмидан фойдаланган ҳолда шифрланиб, махфийлиги таъминланади.



9.6 – расм. Маълумотни бутунлигини ва махфийлигини текшириш

Ҳозирги кунда амалда калитли хэш функцияларга қараганда калитсиз хэш функциялар кенг фойдаланилиб, улар асосида ишлаб чиқилган маълумотларни аутентификациялаш алгоритмлари MAC (Message authentication code) тизимлари деб аталади.

Ушбу тизимларнинг ишлаш принципи 9.7-расмда берилган бўлиб, MAC функция сифатида калитдан фойдаланган ҳолда хэш қийматни ҳисоблайдиган ихтиёрий функцияни олиш мумкин.

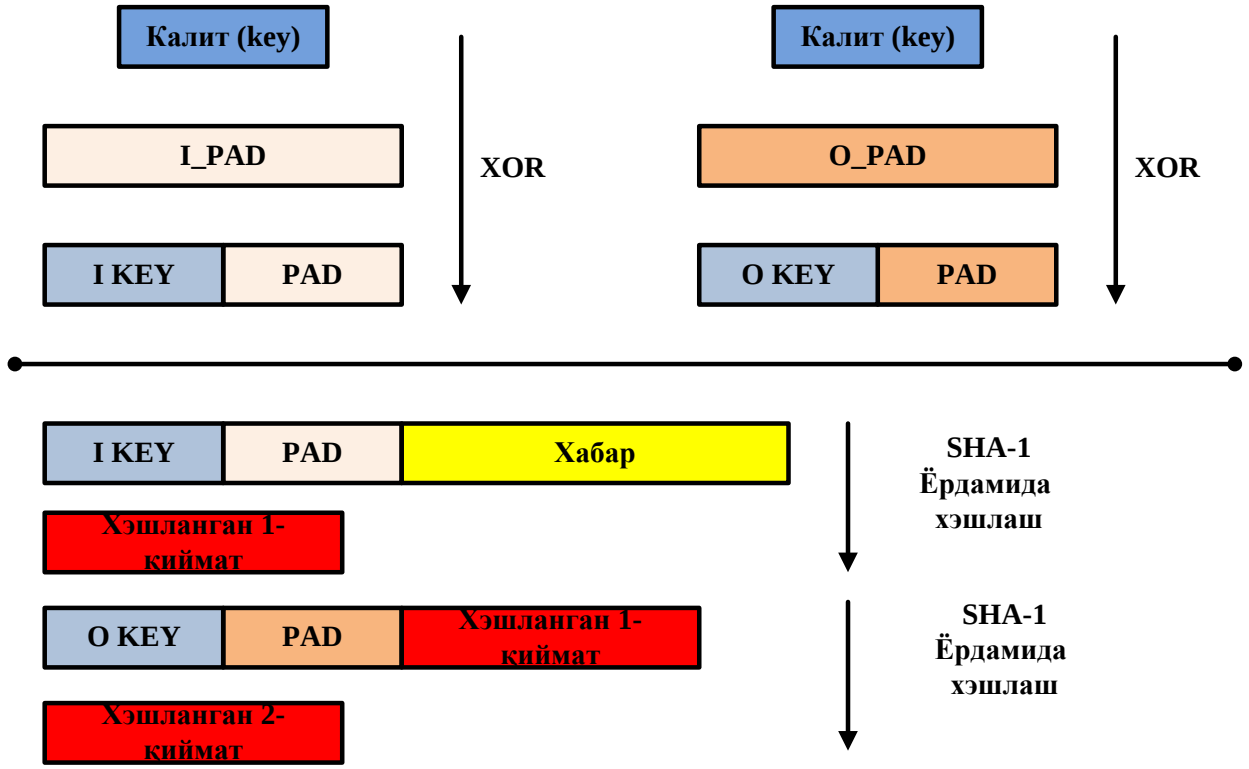


9.7-расм. MAC тизимлари

HMAC тизими MAC (message authentication code) ни ҳисоблашда криптографик калитдан фойдаланилган ҳолдаги кўринишидир. Ушбу тизимда ихтиёрий хэш функция алгоритмлари фойдаланилиши мумкин. Масалан, MD5, SHA1 ва ҳ.к. HMAC тизимлари унда фойдаланилган хэш функцияга кўра номланиши мумкин, масалан: HMAC-MD5 ёки HMAC-SHA1.

HMAC тизимларининг криптографик бардошлиги унда фойдаланилган хэш

функцияга, хэш функциядан чиқадиган натижа узунлигига, калит узунлиги ва сифатига боғлиқ. Қуйида HMAC тизимининг умумий кўриниши келтирилган:



9.8-расм. HMAC тизими

Унинг математик ифодаси эса қуйидагича:

$HMAC(K,m)=H((K \oplus opad)|H((K \oplus ipad)|m))$

Бу ерда:

H – криптографик хэш функция;

K - махфий калит, калит узунлиги хэш функция блок узунлигидан кичик бўлса ўнг томондан “0” лар билан тўлдирилади, узун бўлса калитни хэш қиймати олинади;

m - аутентификацияланувчи маълумот;

| - бирлаштириш белгиси,

⊕ - XOR амали;

opad - ташқи қўшилувчи қисм (0x5c5c5c...5c5c кўринишдаги узунлиги блок узунлигига тенг ўзгармас);

ipad - ички қўшилувчи қисм (0x363636...3636 кўринишдаги узунлиги блок узунлигига тенг ўзгармас).

Умумий ҳолда HMAC алгоритми қуйидагича:

```
function hmac (key, message)
   if (length(key) > blocksize) then
      key = hash(key) // калит узунлиг блок узунлигидан катта бўлган ҳолда
   end if
   if (length(key) < blocksize) then
      key = key ‖ [0x00 * (blocksize - length(key))] // калит узунлиги блок узунлигидан кичик бўлган ҳолда ўнг томонида 0 билан тўлдирилади.          (‖ бирлаштириш амали)
   end if
   o_key_pad = [0x5c * blocksize] ⊕ key
```

```
    i_key_pad = [0x36 * blocksize] ⊕ key // ⊕ XOR амали
    return hash(o_key_pad ‖ hash(i_key_pad ‖ message)) // ‖ бирлаштириш амали
end function
```

Блок ўлчами фойдаланилаётган хэш функция блок узунлиги билан тенг бўлади, масалан: MD5 ёки SHA1 учун 64 байт ёки 512 битга тенг.

HMAC тизими маълумотни аутентификациялаш тизими саналиб, ушбу тизим юборилаётган маълумотларни текширишда фойдаланилади. Ушбу тизимни амалга оширишни кўплаб усуллари мавжуд:

MAC = **H** (*key* ‖ *message*)

MAC = **H** (*message* ‖ *key*)

MAC = **H**(*key* ‖ *message* ‖ *key*)

Юқорида келтирилган усуллар HMAC тизимага ўхшаш бўлсада барчасида “коллизия” мавжуд бўлиши мумкин.

Шуни ҳисобга олган ҳолда амалда юқорида таклиф этилган HMAC тизими таклиф этилади. Ушбу тизим коллизияга бардошли саналиб, хэш функцияни коллизияга бардошлилик даражасидан юқоридир. HMAC тизимларга энг кўп учрайдиган ҳужум тури “brute force” саналиб, калитни топишга қаратилган.

HMAC тизими IPSec протоколида (HMAC-MD5-96 ва HMAC-SHA1-96), TLS (Transport Layer Security) протоколида (Handshake протоколида), OpenID тизимида (HMAC-SHA1 ва HMAC-SHA256) қўлланилади.

Назорат саволлари

Маълумотларни бутунлигини таъминлаш усуллари.

CRC тизимлари.

Калитли ва калитсиз хэш функциялар.

Хэш функцияларга қўйилган талаблар.

MAC тизимлари.

10 - маъруза

Мавзу: Электрон рақамли имзо алгоритмлари

Режа:

ЭРИ алгоритмлари.

RSA ва Эл-Гамал асосида ЭРИ алгоритми.

DSA ЭРИ стандарти.

ГОСТ Р 34.10-2001 ЭРИ стандарти.

Таянч атамалар: хэш қиймат, имзони шакллантириш, имзони текшириш, рад этиш, яхлитлилик.

ЭРИ алгоритмлари

Қабул қилиб олинган маълумотларнинг ҳақиқий ёки ҳақиқий эмаслигини аниқлаш масаласини, яъни маълумотлар аутентификацияси масаласининг моҳияти ҳақида тўҳталамиз.

Ҳар қандай ёзма хат ёки ҳужжатнинг охирида шу ҳужжатни тузувчиси ёки тузиш учун жавобгар бўлган шахснинг имзоси бўлиши табиий ҳолдир. Бундай ҳолат одатда қуйидаги иккита мақсаддан келиб чиқади. Биринчидан, маълумотни олган томон ўзида мавжуд имзо наъмунасига олинган маълумотдаги имзони солиштирган ҳолда шу маълумотнинг ҳақиқийлигига ишонч ҳосил қилади. Иккинчидан, шахсий имзо маълумот ҳужжатига юридик жиҳатдан муаллифликни кафолатлайди. Бундай кафолат эса савдо–сотиқ, ишончнома, мажбурият ва шу каби битимларда алоҳида муҳимдир.

Ҳужжатлардаги қўйилган шахсий имзоларни соҳталаштириш нисбатан мураккаб бўлиб, шахсий имзоларнинг муаллифларини ҳозирги замонавий илғор криминалистика услубларидан фойдаланиш орқали аниқлаш мумкин. Аммо электрон рақамли имзо хусусиятлари бундан фарқли бўлиб, иккилик саноқ системаси хусусиятлари билан белгиланадиган хотира регистрлари битларига боғлиқ. Хотира битларининг маълум бир кетмакетлигидан иборат бўлган электрон имзони кўчириб бирор жойга қўйиш ёки ўзгартириш компьютерлар асосидаги алоқа тизимларида мураккаблик туғдирмайди.

Бугунги юқори даражада ривожланган бутун дунё цивилизациясида ҳужжатлар, жумладан маҳфий ҳужжатларнинг ҳам, электрон кўринишда ишлатилиши ва алоқа тизимларида узатилиши кенг қўлланилиб борилаётганлиги электрон ҳужжатлар ва электрон имзоларнинг ҳақиқийлигини аниқлаш масалаларининг муҳимлигини келтириб чиқармоқда.

Очиқ калитли криптографик тизимлар қанчалик қулай ва криптобардошли бўлмасин, аутентификация масаласининг тўла ечилишига жавоб бера олмайди. Шунинг учун аутентификация услуби ва воситалари криптографик алгоритмлар билан биргаликда комплекс ҳолда қўлланилиши талаб этилади.

Қуйида иккита (А) ва (Б) фойдаланувчиларнинг алоқа муносабатларида аутентификация тизими рақиб томоннинг ўз мақсади йўлидаги қандай хатти-ҳаракатларидан ва криптотизим фойдаланувчиларининг фойдаланиш протоколини ўзаро бузилишлардан сақлаши кераклигини кўрсатувчи

ҳолатлар кўриб чиқилади.

Рад этиш (ренегатство). Фойдаланувчи (А) фойдаланувчи (Б) га ҳақиқатан ҳам маълумот жўнатган бўлиб, узатилган маълумотни рад этиши мумкин.

Бундай қоида бузилишининг (тартибсизликнинг) олдини олиш мақсдида электрон (рақамли) имзодан фойдаланилади.

***Модификациялаш (ўзгартириш*).** Фойдаланувчи (Б) қабул қилиб олинган маълумотни ўзгартириб, шу ўзгартирилган маълумотни фойдаланувчи (А) юборди, деб таъкидлайди (даъво қилади).

Соҳталаштириш. Фойдаланувчи (Б)нинг ўзи маълумот тайёрлаб, бу соҳта маълумотни фойдаланувчи (А) юборди деб даъво қилади.

Фаол модификациялаш (ўзгартириш). (А) ва (Б) фойдаланувчиларнинг ўзаро алоқа тармоғига учинчи бир (В) фойдаланувчи ноқонуний тарзда боғланиб, уларнинг ўзаро узатаётган маълумотларини ўзгартирган ҳолда деярли узлуксиз узатиб туради.

Ниқоблаш (имитациялаш). Учинчи фодаланувчи (В) фойдаланувчи (Б)га фойдаланувчи (А) номидан маълумот жўнатади. Юқорида санаб ўтилган: модификациялаш, сохталаштириш, фаол модификациялаш, ниқоблаш каби алоқа тизими қоидаларининг бузилишини олдини олиш мақсадида рақамли сигнатурадан – рақамли имзо ва узатиладиган маълумотнинг бирор қисмини тўла ўз ичига олувчи рақамли шифрматндан иборат бўлган маълумотдан фойдаланилади.

Такрорлаш. Фойдаланувчи (В) фойдаланувчи (А) томонидан фойдаланувчи (Б)га жўнатилган маълумотни такроран (Б)га жўнатади. Бундай ноқонуний хатти–ҳаракат алоқа усулидан банклар тармоқларида электирон ҳисоб–китоб тизимидан фойдаланишда ноқонунийлик билан ўзгалар пулларини талон-тарож қилишда фойдаланилади. Ана шундай ноқонуний усуллардан муҳофазаланиш учун қуйидаги чора - тадбирлари кўрилади.

- имитациялашга бардошлилик – имитабардошлилик;
- криптотизимга кираётган маълумотларни муҳофаза мақсадларидан келиб чиқиб тартиблаш.

Электрон рақамли имзо алоқа тизимларида бир неча тур қоида бузилишларидан муҳофаза қилинишни таъминлайди, яъни:

- махфий калит фақат фойдаланувчи (А)нинг ўзигагина маълум бўлса, у ҳолда фойдаланувчи (Б) томонидан қабул қилиб олинган маълумотни фақат (А) томонидан жўнатилганлигини рад этиб бўлмайди;
- қонун бузар (рақиб томон) махфий калитни билмаган ҳолда мадификациялаш, сохталаштириш, фаол модификациялаш, ниқоблаш ва бошқа шу каби алоқа тизими қоидаларининг бузилишига имконият туғдирмайди;
- алоқа тизимидан фойдаланувчиларнинг ўзаро боғлиқ ҳолда иш юритиши муносабатидаги кўплаб келишмовчиликларни бартараф этади ва бундай келишмовчиликлар келиб чиққанда воситачисиз аниқлик киритиш имконияти туғилади.

Кўп ҳолларда узтилаётган маълумотларни шифрлашга ҳожат бўлмай, уни электрон рақамли имзо билан тасдиқлаш керак бўлади. Бундай ҳолатларда

очиқ матн жўнатувчининг ёпиқ калити билан шифрланиб, олинган шифрматн очиқ матн билан бирга жўнатилади. Маълумотни қабул қилиб олган томон жўнатувчининг очиқ калити ёрдамида шифрматнни дешифрлаб, очиқ матн билан солиштириши мумкин.

Ассиметрик ширфлаш алгоритмлари юқорида исботланганидек, катта ҳажмдаги маълумотларни шифрлаш кенг қўлланилмайди. Ассиметрик шифрлаш алгоритмлари криптография соҳасида асосан электрон рақамли имзо тизимларида кенг фойдаланилади.

ЭРИ алгоритмлари қуйидаги вазифаларни бажаради:

имзо чекилган маълумот бутунлигини;

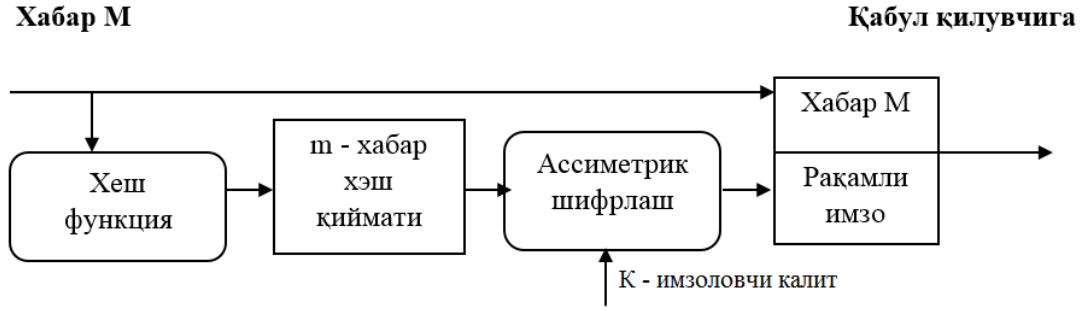
электрон ҳужжатга рақамли имзо қўйган субъектни муаллифликдан бош тортмаслигини таъминлайди;

электрон ҳужжат манбаанинг ҳақиқийлигини аниқлаш.

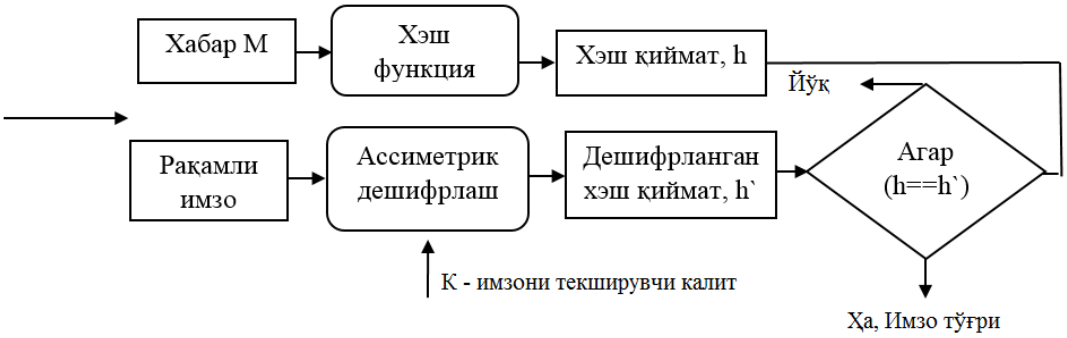
ЭРИ тизими қуйидаги икки жараёндан иборат (10.1, 10.2 - расмлар):

ЭРИни шакллантириш;

ЭРИ ҳақиқийлигини текшириш.



10.1- расм. Электрон рақамли имзони шакллантириш жараёни



10.2 - расм. Электрон рақамли имзони текшириш жараёни

RSA ва Эл-Гамал асосида ЭРИ алгоритми

RSA асосида ЭРИ. RSA алгоритмига асосланган ЭРИ алгоритмини ортиқча қийинчиликсиз амалга оширса бўлади. Бунинг учун шифрлаш ва дешифрлаш учун фойдаланилган калитлардан тескарисига ва маълумотнинг ўрнида унинг хэш қийматдан фойдаланишнинг ўзи етарли (10.3 - расм).

ЭРИ ни шакллантириш $H(M)^d mod n = P$

ЭРИ ни текшириш $P^e mod n = H(M)$

Бу ерда:

H(M) – маълумотнинг хэш қиймати;

d – имзо қўйиш калити (махфий калит);
P – имзо.

10.3– расм. RSA асосида ЭРИ алгоритми

Эл-Гамал асосида ЭРИ. Амалда Эл-Гамал шифрлаш усулига асосланган ЭРИ алгоритмалари кенг қўлланилади. Бу усулда асосланган ЭРИ да калитларни генерациялаш шифрлашдаги каби амалга оширилади. Имзо қўйиш ва имзони текшириш жараёнлари қуйидаги каби амалга оширилади.

ЭРИ ни шакллантириш

$$a = g^k mod p$$

$$b = H(M) - ax\ k^{-1} mod(p-1)$$

Бу ерда:
H(M) – маълумотнинг хэш қиймати;
x – имзо қўйиш калити (махфий калит);
ЭКУБ (k, $p-1$)=1 га тенг бутун сон.
(a,b) – имзо.

ЭРИ ни текшириш

$$y^a a^b mod p = g^{H(M)} mod p$$

тенглик ўринли бўлса имзо ҳақиқий, акс ҳолда йўқ.
Бу ерда:
$y = g^x mod p$ – очиқ калит.

10.4 – расм. Эл-Гамал асосида ЭРИ

Амалда кўплаб давлатлар ўзининг ЭРИ стандартларига эга. Уларга қуйидагиларни олиш мумкин:
Эл-Гамалга асосланган DSA стандарти (АҚШ);
Эл-Гамалга асосланган ГОСТ Р 34.10-94 стандарти (Россия);
ЭЭЧ асосланган ECDSA -2000 стандарти (АҚШ);
ЭЭЧ асосланган ГОСТ Р 34.10-2001 стандарти (Россия);
Параметрли даражага кўтариш ва ЭЭЧ асосланган O'zDSt 1092:2009 стандарти (Ўзбекистон Республикаси).

DSA ЭРИ стандарти

1991 йилда NIST (National Institute of Standard and Technology) томонидан DSA (Digital Signature Algorithm) алгоритмига асосланган DSS (Digital Signature Standard) ЭРИ стандарти яратилди. Ушбу алгоритм чекли майдонда дискрет логарифмлаш муаммосига асосланган. Хэш функция сифатида SHA1 стандартидан фойдаланилган.

Имзони шакллантириш:

Имзоланувчи M маълумотни имзолашда қуйидаги кетма – кетликлар бажарилади:
p – туб сон танланади ($2^{512} < p < 2^{1024}$ ва бит узунлиги 64 га каррали);
q - туб сон таналанади ($2^{159} < q < 2^{160}$ ва $p-1$ нинг бўлувчиси);
$0 < h < p$ ва $h^{(p-1)/q} mod\ p > 1$ шартларни қаноатлантирувчи h катталик асосида $g = h^{(p-1)/q} mod\ p$ бутун сон ҳисобланади;
x – махфий калит орқали, $y = q^x mod\ p$ очиқ калит ҳисобланади (бу ерда: 0<x<q);
маълумотнинг хэш қийматини ҳисобланади (H(M) – малумот хэш қиймати [1;q] оралиқда).
Маълумот жўнатувчиси тасодифий k сонини танлайди ($0<k<q$ шарт билан). Ушбу катталик имзо шаллантирилгандан сўнг ўчириб ташланади.

М маълумотни имзолари қуйидагиларга тенг бўлади:
$r = g^k \bmod p \bmod q$,
$s = k^{-1}(xr + H(M)) \bmod q$.
Ҳосил қилинган катталиклар (r, s) малумот М га қўшиб имзони текширувчи томонга юборилади.
Имзони текшириш жараёни:
Қабул қилинган М’ маълумот ва унга қўйилган имзо (r’, s’) асосида имзони текшириш жараёни амалга оширилади. Бу икки босқичдан иборат. Агар имзо биринчи босқичдаги текширувдан ўта олмаса, унда иккинчи босқичга ўтмайди.
Қабул қилинган имзолар учун $0 < s' < q$ ёки $0 < r' < q$ шарт текширилади. Бу шарт бажарилса иккинчи босқичга ўтилади.
Иккинчи босқич қуйидагилардан иборат:
$v = (s')^{-1} (\bmod q)$ ҳисобланади.
$z_1 = H(M')\, v \bmod q$, $z_2 = r' \, v \bmod q$ қийматлар ҳисобланади.
Шундан сўнг $u = g^{z_1} y^{z_2} \bmod p \bmod q$ қиймат ҳисобланади.
Агар $r' = u$ тенглик бажарилса, у ҳолда қўйилган электрон рақамли имзо ҳақиқий ($M = M'$) бўлади. Акс ҳолда имзо қалбаки деб топилади.

ГОСТ Р 34.10-2001 ЭРИ стандарти

Ушбу алгоритм ГОСТ Р 34.10 – 94 ЭРИ алгоритмининг эллиптик эгри чизиққа асосланган модификацияси саналган Россия стандарти. Ушбу алгоритмда имзони шакллантириш ва текшириш жараёнлари қуйида келтирилган.
Имзони шакллантириш жараёни. Бошланғич маълумотлар сифатида: M имзоланувчи маълумот, фойдаланилган эллиптик чизиқ параметрлари ва имзо учун махфий калити. Ушбу алгоритм учун эллиптик эгри чизиқ тенгламаси $p > 2^{255}$ шартни қаноатлантирувчи туб характеристикали F_p майдонда деб олиниши шарт. Қўйилган имзо (r, s) га тенг бўлади.
Имзони ҳосил қилиш босқичлари
$1 \le k \le n-1$ ораликдаги ихтиёрий k сони танланади (бу ерда n сони G нуқта тартиби ва $2^{254} < n < 2^{256}$ шартни қаноатлантирувчи бутунисон).
$(x_1, y_1) = [k]G$ ҳисобланади.
$r = x_1 \bmod n$ ҳисобланади. Агар $r=0$ га тенг бўлса, 1-қадамга қайтиб, k сони қайтадан танланади.
Имзоланувчи M маълумотнинг хэш хэш қийматини ҳисобланади, яъни $e = H(M)$. Агар $H(M) \bmod n = 0$ га тенг бўлса, $H(M) \bmod n = 1$ шарт олинади.
$0 < d < n$ ораликдан танланган d махфий калит асосида $s = (dr + ke) \bmod n$ катталик ҳисобланади.
Агар $s=0$ га тенг бўлса, 1-қадамга қайтилади ва бошқа k сони танланади.
Ҳосил қилинган (r,s) сонлар жуфти M маълумот учун электрон рақамли имзо ҳисобланади.
Имзони текшириш жараёни. Имзони текшириш қабул қилинган М’ очиқ малумот ва имзо (r’, s’) асосида амалга оширилади.
Агар $1 \le r', s' \le n-1$ шарт бажарилмаса, имзо қалбаки деб топилади ва

текшириш тўхтатилади.
$e = H(M')$ маълумотнинг хэш қиймати ҳисобланади.
$w = H(M')^{(n-2)} \bmod n$ катталик ҳисобланади.
$u_1 = s' w \bmod q$ катталик ҳисобланади.
$u_2 = (n-r') w \bmod n$ катталик ҳисобланади.
$X = [u_1] G + [u_2] Q = (x_1, y_1)$ катталик ҳисобаланади.
Агар $x_1 \bmod n = r'$ га тенг бўлса, қўйилган имзо ҳақиқий, акс ҳолда қалбаки деб топилади.
Бундан ташқари амалда кўплаб электрон рақамли имзо алгоритмлари фойдаланилади. Уларда фойдаланилган параметлар ва функциялар ўзгарсада, фойдаланилган математик муаммо юқоридаги келтирилганлардан бирига асосланади.

Назарий саволлар

ЭРИ алгоритмларининг асосий вазифаси.
ЭРИ шакллантириш жараёни.
ЭРИ текшириш жараёни.
DSA ЭРИ стандарти.
ГОСТ Р 34.10-2001 ЭРИ стандарти

11 - маъруза

Мавзу: Криптографик калитларни бошқариш

Режа:

Калитларни бошқариш.

Калитларнинг очиқ тақсимланиш алгоритми ҳақида.

Криптотизим фойдаланувчиларига калитларни тақсимлашнинг тартиб ва қоидалари (протоколи).

Нидхем-Шрёдер протоколи.

Kerberos протоколи.

Таянч атамалар: калит генерацияси, калитларни тақсимлаш, калитни сақлаш, умумий калит.

Калитларни бошқариш

Ахборот-коммуникация тизимида маълумотлар амашинувига мос келувчи криптографик тизимни яратиш билан бир қаторда шу тизимда калитлар бошқариш масаласини оптимал (қулай ва ишончли) ҳал этиш муҳим ўрин тутади. Чунки танланган криптотизим қанчалик мураккаб ва ишончли бўлмасин, барибир ундан амалда фойдаланиш жараёнлари калитларни бошқариш масаласи билан боғлиқдир. Агарда маълумотларнинг маҳфий алмашинуви оз сонли фойдаланувчилар доирасида бўлса, калитлар алмашинуви жараёнида ноқулайликлар туғилмайди. Аммо ахборот-коммуникация тизимида маълумотларнинг маҳфий алмашинуви юзлаб, минглаб ва хатто миллионлаб фойдаланувчилар доирасида бўлса (мисол учун модем ва Интернет алоқа тизимлари орқали банк, савдо–сотиқ, давлат аҳамиятига боғлиқ ҳамда бошқа муҳим соҳалардаги алоқа жараёни фойдаланувчилари доирасида) калитларни бошқаришнинг ўзига хос алоҳида муҳим масалалари келиб чиқади.

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 иҳтиёрий маълумотни олиш учун тўла имконият туғилади.

Калитларни бошқариш жараёни қуйидаги учта муҳим бўлган:

барча калитларнинг ўзаро боғлиқ ҳолда, яъни бир бутун ҳолда ишлаш жараёнини таъминлаш (калитлар генерацияси);

калитлар тўпламининг мақсадли кенгайиб боришини таъминлаш (калитларларнинг тўпланиши);

калитларларни фойдаланувчилар доирасида тақсимлаш (калитларларнинг тақсимланиши) жараёнларига аҳамият беришни талаб этади.

Калитларнинг очиқ тақсимланиш алгоритми ҳақида

Диффи – Хелман калитларни очиқ тақсимлаш протоколи. У. Диффи ва М.Е. Хеллманнинг калитларни очиқ тақсимлаш системаси очиқ калитли бошқа криптотизимлар каби маҳфий калитни маҳфий канал орқали

узатилишининг ҳожати йўқлигини таъминлайди, аммо аутентификация масаласини ечмайди ва ўртадаги одам ҳужумига бардошсиз.

Мисол:

ALICE	**EVIL EVE**	**BOB**
Alice ва Bob иккита g, p (p>g) сонни ҳосил қилади. p=11, g=7	Бузғунчига ҳам p=11, g=7 маълум.	Alice ва Bob иккита g, p (p>g) сонни ҳосил қилади. p=11, g=7
Alice ўзининг махфий калитини ҳосил қилади. X_A=6		Bob ўзининг махфий калитини ҳосил қилади. X_B=9
$Y_A=g^{X(A)}(modp)$ $Y_A=7^6 mod11=4$		$Y_B=g^{X(B)}(modp)$ $Y_A=7^9 mod11=8$
Alice Y_A=8 ни қабул қилади.	Бузғунчига ҳам Y_B =4, Y_A = 8 маълум.	Bob Y_B=4 ни қабул қилади.
Махфий калит = $Y_B{}^{X_A} modp$ Махфий калит = $8^6 mod11$ = 3		Махфий калит = $Y_A{}^{X_B} modp$ Махфий калит = $4^9 mod11$ = 3

Криптотизим фойдаланувчиларига калитларни тақсимлашнинг тартиб ва қоидалари (протоколи)

Маҳфий услубли бир томонлама функцияга асосланган очиқ калитли криптотизимлар ўз моҳиятига кўра ундан фойдаланишнинг алоҳида тартиб ва қоидаларини (протоколини) талаб этади. Бу алоҳида тартиб ва қоидаларга кўра тизимнинг фойдаланувчилари ва тизим фойдаланувчиларигагина очиқ бўлган очиқ маълумотлар тўпламини (китобини) маъмури (сақловчиси) биргаликда шу тизимда узатиладиган маълумотларнинг маҳфийлигини таъминлайдилар.

Очиқ калитли криптотизимларнинг бардошлилигига тўла ишонч билдирмай ишончсизлик ва иккиланиш билан қарайдиган баъзи криптолог мутахассислар, фойдаланувчиларга муҳофазаланган услубда очиқ калитларни тақсимлаш ва маҳфий калитларни узатиш масалаларини, яъни калитлар билан боғлиқ жараёнларни мақсадли бошқаришни криптографиянинг бош амалий масаласи, деб биладилар. Мисол учун, агарда криптотизим фойдаланувчиларининг сони S та бўлса ва ҳар бир мумкин бўлган алоқа жуфтлари учун алоҳида маҳфий калит талаб этилса, уларнинг сони $c_s^2 = s(s-1)/2$ бўлиб, фойдаланувчилар сони кўп бўлган тизимлар учун бундай ҳолат баъзида мақсадга мувофиқ бўлмаслиги мумкин. Бирор фойдаланувчининг бошқа барча фойдаланувчиларга маҳфий бўлган маълумотни юбориши маҳфий алоқа моҳиятига зид жараён. Бундан ташқари маҳфий алоқа тизимида қайси фойдаланувчининг бошқа қайси бир фойдаланувчи билан маҳфий алоқа қилишни ҳоҳлаши олдиндан маълум эмас. Мана шундай ҳолатлар фойдаланувчиларга калитларни тақсимлаш тартиб ва қоидалари масалаларини келтириб чикаради. Бундай масалаларнинг ечилиши эса, аҳборот-коммуникация тизимида

маълумотларнинг маҳфийлиги муҳофазасини таъминловчи криптотизимда калитларни рўйхатга олиш маркази (КРОМ) ташкил этишни тақазо этади. Калитларни тақсимлаш тартиб ва қоидалари (протоколи) қуйидагича:

1. КРОМ муҳофазаланган алоқа тармоғи орқали барча i=1,2,...,S фойдаланувчиларга маҳфий Z_i калитларни тақдим этади.
2. Фойдаланувчи i фойдаланувчи j билан маҳфий алоқа ўрнатмоқчи бўлса, у умумий алоқа тармоғи орқали (очиқ матн билан бўлиши мумкин) КРОМга мурожаат қилиб, фойдаланувчи j билан маҳфий алоқа қилиш калитини сўрайди.
3. КРОМ маҳфий алоқа учун очиқ матннинг бирор қисмини ташкил этувчи Z_{ij} маҳфий калитни танлаб олади. Қолган қисмини i ва j фойдаланувчилар кўрсатилган "бош қисм" ("заголовка") ёки "номланиш қисми" деб аталувчи бўлак ташкил этади. КРОМ бу очиқ матнни криптотизимда қабул қилинган шифрлаш алгоритмига кўра Z_i ва Z_j калитлар билан шифрлаб, умумий алоқа тармоғи оркали Z_i калит билан шифрланган криптограммани i фойдаланувчига ва Z_j калит билан шифрланган криптограммани j фойдаланувчига жўнатади.
4. Олинган криптограммаларни i ва j фойдаланувчилар дешифрлаб, кейинги олинган маълумотларни дешифрлашнинг маҳфий калитига эга бўладилар.

Калитларни тақсимлашнинг бундай тартиб ва қоидалари (протоколи) оддий бўлиб, унинг бардошлилиги шифрлаш алгоритмининг бардошлилиги билан белгиланади. Ҳақиқатдан ҳам 3-бандда (қадамда) келтирилганидек, криптоаналитикка ҳар-хил калитлар билан шифрланган бир хил очиқ матннинг криптограммаси маълум бўлиб, бундай ҳолат унга криптотаҳлил қилишда қўл келади. Шундай қилиб, очиқ матнни шифрлаш алгоритми криптотаҳлилга бардошли бўлса, калитларни тақсимлаш протоколи ҳам бардошли бўлади. Бу ерда шуни ҳам унутмаслик керакки, калитларни тақсимлашда шифрлаш алгоритмидан фойдаланиш шу тақсимлаш тартиб ва қоидаларининг бузилишига, криптобардошсизликка ва шу каби номутоносибликларга олиб келмаслиги керак.

Нидхем-Шрёдер протоколи

Рожер Нидхем ва Михаэл Шрёдерлар томонидан яратилган бу протоколда арбитр ва симметрик криптотизимдан фойдаланилади:

1. А - фойдаланувчи ишончли томонга (W) ўзининг исмини, В-фойдаланувчининг исмини ва ўзининг тасодифий сонини узатади.

$A \to W : A, B, R_A$.

2. З - ишончли томон сеанс калитни генерация қилади. Бу сеанс калитни ва А - фойдаланувчининг исмини В - фойдаланувчи билан умумий бўлган калит орқали шифрлайди. Сўнгра А -фойдаланувчи ва ўзи учун умумий бўлган калит ёрдамида А - фойдаланувчининг тасодифий сони, В-фойдаланувчининг исми, калит ва шифрматнни шифрлайди. Ниҳоят у шифрланган маълумотни А -фойдаланувчига узатади:

$W \to B : E_A(R_A, B, k, E_B(k, A))$.

3. А - фойдаланувчи маълумотни дешифрлаб, k -калитни олади. У R_A ва 1 -

босқичда узатилган R_A ни солиштиради. Сўнгра А - фойдаланувчи ишончли томон шифрлаган маълумотни В -фойдаланувчига узатади:

$A \to B : E_B(k, A)$.

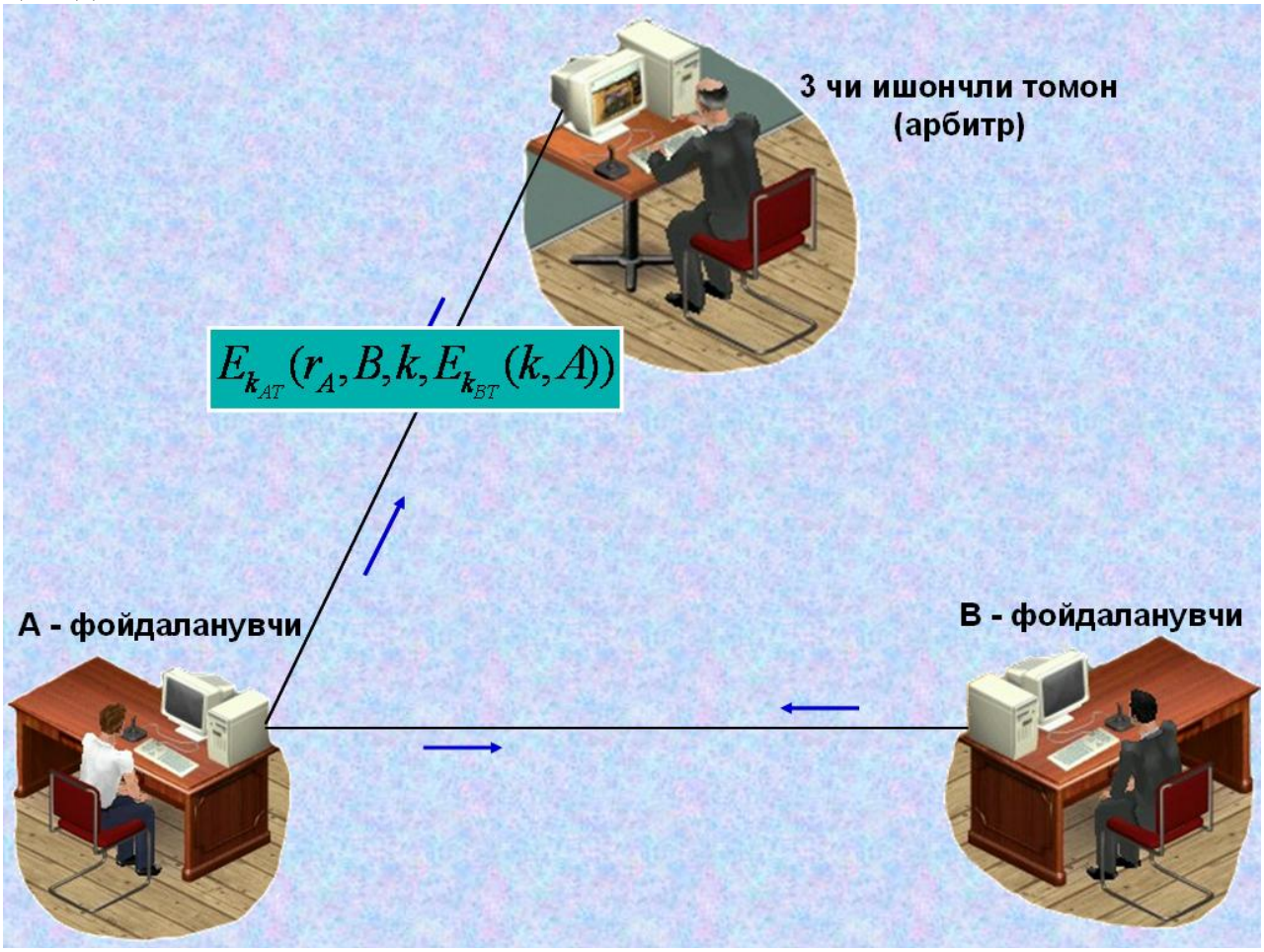
4. В - фойдаланувчи бу маълумотни дешифрлайди ва k - калитни олади. Сўнгра у тасодифий R_B - сонини генерация қилади. Бу тасодифий сонни k - калит ёрдамида шифрлайди ва А -фойдаланувчига узатади:

$B \to A : E_k(R_B)$.

5. А - фойдаланувчи k - калит ёрдамида маълумотни дешифрлайди. А-фойдаланувчи тасодифий $R_B - 1$ - сонини генерация қилади. Бу сонни k -калит ёрдамида шифрлаб қайта В -фойдаланувчига узатади:

$A \to B : E_k(R_B - 1)$.

6. В - фойдаланувчи маълумотни дешифрлаб, $R_B - 1$ - сонини текширади ва ҳақиқатдан А - фойдаланувчи билан алоқа ўрнатаётганига ишонч ҳосил қилади.



Бу протоколда R_A, R_B ва $R_B - 1$ - сонларидан такроран фойдаланилади. Агар криптоаналитик аввал фойдаланилган k -калитни қўлга киритса, 3 - босқичда А -фойдаланувчи номидан В -фойдаланувчига маълумот узатиши мумкин.

Kerberos протоколи

Kerberos протоколи **Нидхем-Шрёдер** протоколининг модификацион варианти ҳисобланади. А - фойдаланувчи В - фойдаланувчи билан маълумот алмашиши учун уларга сеанс калити қуйидагича амалга оширилади:

1. A - фойдаланувчи арбитрга ўзининг исми ва B - фойдаланувчининг исмидан ташкил топган маълумотни узатади:

A $\rightarrow$ W: A, B

2. Арбитр иккита маълумотни ҳосил қилади, биринчиси вақт белгиси, ҳаётий вақт L, тасодифий сеанс калит ва A - фойдаланувчининг исмидан ташкил топган. Арбитр бу маълумотни ўзи ва B - фойдаланувчи учун умумий бўлган калит билан шифрлайди, иккинчиси вақт белгиси, ҳаётий вақт, тасодифий сеанс калит ва B - фойдаланувчининг исмидан ташкил топган. Арбитр бу маълумотни ўзи ва A -фойдаланувчи учун умумий бўлган калит билан шифрлайди. У иккала шифрматнни A -фойдаланувчига узатади:

W $\rightarrow$ A: $E_A(t, L, k, B), E_B(t, L, k, A)$.

3. A - фойдаланувчи ўзининг калити билан биринчи шифрматнни дешифрлайди. У ўзининг исми ва вақт меткасини бирлаштириб, k - сеанс калит билан шифрлайди. Бу шифрматнни ва арбитрдан қабул қилган иккинчи шифрматнни B - фойдаланувчига узатади:

A $\rightarrow$ B: $E_k(A, t), E_B(t, L, k, A)$.

4. B - фойдаланувчи ўзининг калити ёрдамида иккинчи шифрматнни дешифрлайди ва сеанс калитига эга бўлади. Бу сеанс калит ёрдамида биринчи шифрматнни дешифрлайди. Натижада ҳосил бўлган A - фойдаланувчининг исми ва вақт белгиси аввалгиси билан мос бўлса, B - фойдаланувчи A - фойдаланувчини идентификация қилади. Энди A - фойдаланувчи уни идентификация қилиши учун вақт белгисига 1 рақамини қўшиб сеанс калит билан шифрлайди. Ҳосил бўлган шифрматнни A - фойдаланувчига узатади:

B $\rightarrow$ A : $E_k(t+1)$.

Агар ҳар бир фойдаланувчининг соатлари арбитрнинг соати билан синхрон равишда ишласа Бу протокол яхши натижа беради.

Назорат саволлари

Калитларни бошқариш тизимларининг вазифаси нимадан иборат.

Калитларни генерациялаш бўлимининг вазифаси.

Калитларни очиқ тақсимлаш протоколини тушунтиринг.

Керберос протоколи.

12 - маъруза

Мавзу: Криптографик алгоритмларни ишлаб чиқиш. Криптотаҳлил.

Режа:

Калитни тўлиқ танлаш усули.

Дифференциал криптотаҳлил.

Чизиқли криптотаҳлил.

Замонавий криптотизимларни яратиш.

Таянч атамалар: калитни тўлиқ танлаш, дифференциал таҳлил, чизиқли таҳлил, S-box.

Калитни тўлиқ танлаш усули

Тўлиқ танлаш, яъни калитларнинг *барча мумкин бўлган вариантларини танлаш усули,* криптотаҳлилчининг носимметрик криптотизим алгоритмини ва ошкора калитни билган ҳолда барча мумкин бўлган калитларни танлаш ва синаб кўришга асосланади. Симметрик криптотизимларда ҳам шифрматн ва очиқ матн асосида тўлиқ танлаш усули қўлланилади. Криптотаҳлилчилар кўпинча компьютер ёрдамида калитларни тўлиқ танлаш усулидан фойдаланиб шифрларни ошкор этадилар. Криптотаҳлил жараёнида миллиард калитларни секундига минглаб калит тезликда танлашга тўғри келади.

Фараз қилинсин, бузғунчи учун бир ёки бир неча *(x, y)* жуфтлик маълум бўлсин. Осонлик учун ҳар қандай жуфтлик *(x, y)* учун $E_k(x)=y$ муносабатни қаноатлантирувчи ягона k калит мавжуд бўлсин. Мумкин бўлган калитлар тўпламини тартибга солинади ва K даги калитларни кетма-кет равишда $E_k(x)=y$ тенглик бажарилишига текшириб чиқилади. Агар $k \in K$ калитнинг бир вариантини текшириш бир амал ёрдамида ҳисобланса, унда калитларни тўлиқ танлаш учун $|K|$ амал талаб этилади. Бунда $|K|$ - тўпламдаги элементлар сони. Шифрлаш схемасида калит тасодифий ва тенг эҳтимоллик билан K тўпламдан танланган бўлсин. Бунда калит $1/|K|$ эҳтимоллик билан билан топилади ва тўлиқ танлаш усулининг иш ҳажми *1* га тенг бўлади.

Мисол учун шахсий калит узунлиги *100* бит бўлса, унда барча шахсий калитлар сони 2^{100} га тенг, яъни калитлар тўплами қуввати $|K|=2^{100}$. Шахсий калит узунлиги *56* бит бўлганда, барча мумкин бўлган шахсий калитлар сони $|K|=2^{56} \approx 0.5*10^{17}$ га тенг. Бунда, агар ҳисоблаш қурилмаси ҳар битта махфий калитга мос ошкора калитни ҳисоблаш ва уни ҳеч қийинчиликсиз таққослаш учун 10^{-6} секунд вақт сарфласа, *24* соатда барча калитларни синаб чиқиш учун $5.787*10^5$ та ЭҲМ керак бўлади.

Шунинг учун ҳам шахсий ва шифрлашда фойдаланиладиган калитни топишни мураккаблаштириш мақсадида шахсий калитлар узунлиги *127-159* битдан катта бўлган узунликда генерацияланади.

Калитларни тўлиқ танлаш усулида сарфланган вақт фойдаланилган компьютер имконияти ва калит узунлигига боғлиқ.

Қуйида келтирилган жадвалда турли узунликдаги паролларни (улар турли 36 та белгидан иборат бўлиши мумкин) секундига 100 000 паролни ҳисоблаш имконига эга компьютерда ҳосил қилиш вақтлари келтирилган.

12.2 – жадвал

Калитларни тўлиқ танлаш усули мураккаблиги

Белгилар сони	**Вариантлар сони**	**Бардошлиги**	**Вақти**
1	36	5 бит	Секундан кам
2	1296	10 бит	Секундан кам
3	46 656	15 бит	Секундан кам
4	1 679 616	21 бит	17 секунд
5	60 466 176	26 бит	10 минут
6	2 176 782 336	31 бит	6 соат
7	78 364 164 096	36 бит	9 кун
8	2,821 109 9x10^{12}	41 бит	11 ой
9	1,015 599 5x10^{14}	46 бит	32 йил
10	3,656 158 4x10^{15}	52 бит	1 162 йил
11	1,316 217 0x10^{17}	58 бит	41 823 йил
12	4,738 381 3x10^{18}	62 бит	1 505 615 юз йил

Ушбу криптотаҳлил усули блокли симметрик шифрлаш усуллари, оқимли симметрик шифрлаш усуллари ва хэш функцияларни таҳлиллашда кенг фойдаланилади. Бу таҳлил усули киришдаги маълумотлар фарқи чиқишдаги маълумотлар фарқига таъсирини ўргинишга асосланган. Агар бу фарқ тасодифий бўлмаса, унда калитни топиш имконияти мавжуд бўлади.

Дифференциал криптотаҳлил

Дифференциал криптотаҳлил усули 1980 йиллар охирида Исроиллик математиклар Эли Бихам ва Ади Шамир томонидан таклиф этилган. Муаллифлар DES шифрлаш алгоритмини таҳлил қилиш давомида ушбу усулни кашф этишган. Кейинчалик, шу нарса аниқ бўлдики, 1970 йил ўраталарида DESни лойихаси давомида иштирокчилардан бири ундан фойдаланган. Эсда сақлаш керакки, дифференциял таҳлилда танланган очиқ матндан фойдаланилади ва уни ҳақиқий ҳаётда қўллаш жуда қийин.

Бу таҳлил тури танланган шифрматнга асосланган таҳлилга максуб бўлиб, бунда таҳлилчи танлаган очиқ матн ва унга мос шифрматн берилади. Бу усулни яна, очиқ матнга асосланган ёки фақат шифрматнга асосланган усулга ҳам киритиш мумкин.

Ушбу таҳлил усулининг ғояси иккита очиқ матн P_1 ва P_2 лар орасидаги фарқни XOR амали билан ҳисоблашга асосланган бўлиб, фарқ чизиқли ва чизиқсиз ўзгаришларни бардошлилик даражасини кўрсатади.

$$\Delta\oplus P = P_1 \oplus P_2$$

$\oplus$ – амалига асосланган фарқдан ташқари, $\boxplus$ – амалига асосланган фарқлардан ҳам кенг фойдаланилади.

F ўзгариш натижасида ҳосил бўлган тақрибий фарқ функцияга кирувчи Δ_I ва чиқувчи Δ_O катталиклар фарқига тенг бўлади:

$$\Delta_I \overset{F}{} \Delta_O$$

Чизиқли криптотаҳлил

Чизиқли криптотаҳлил усули Мицуру Мацуи томонидан таклиф этилган бўлиб, унда блокли шифр алгоритмининг криптотаҳлиллаш моделини тузишда чизиқли яқинлашишдан фойдаланилади.

DES шифри чизиқли криптотаҳлил усулига қарши қилиб лойихаланмаган ёки NSA 1970 йилда бу таҳлул усули ҳақида билмаган ёки бу турдаги таҳдидни ҳисобга олишмаган. Чизиқли криптотаҳлил дифференциял таҳдидга қараганда реал амалга ошириш эҳтимоли юқори. Сабаби, чизиқли криптотаҳлил танланган очиқ матнга эмас, балки, маълум очиқ матнга асосланган.

Чизиқли криптотаҳлилнинг асосий ғояси бу – чизиқсиз компонентларни тақрибий чизиқли функциялар орқали ифодалаш асосланган. Чизиқли яқинлашиш ўзгартиришларнинг кирувчи ва чиқувчи битлари орасидага боғлиқликдир. Математик ифодаси, берилган функция *f* бўлиб, мақсад *u* ва *v* бул векторларини етарлича катта бўлган |ε| учун эҳтимоллик ½+ε билан топиш:

$$u \cdot X = v \cdot f(X)$$

Бу ерда • амали векторлар орасидаги амаллар. Агар $f=f_K$ калитли функция бўлса, боғланиш К калитни ҳам ўз ичига олади:

$$u \cdot X \oplus v \cdot f_K\ X\ = w \cdot K$$

DES алгоритмида S жадвал таҳлилида, S_5 жадвал учун $(0,0,0,1)\bullet X=(1,1,1,1)\bullet S_5(X)$. Бу ерда эҳтимоллик ½-5/16 га тенг бўлади. Натижада, раунд функцияси F учун қуйидаги яқинлашиш ўринли бўлади:

$$X_{15} \oplus F_K\ X\ _7 \oplus F_K\ X\ _{18} \oplus F_K\ X\ _{24} \oplus F_K\ X\ _{29} = K_{22}$$

Криптотаҳлил S-блокларнинг структурасига жуда ҳам боғлиқ, аммо DES S-блоклари чизиқли криптотаҳлилга қарши оптималлаштирилмаган. DES муаллифларидан бири Дон Копперсмитнинг сўзига қараганда чизиқли криптотаҳлилга бардошлилик «DESни лойиҳалашда зарур бўлган тамойиллар қаторига киритилмаган».

Замонавий криптотизимларни яратиш

DES нинг замонавий криптографияга таъсири бу моболаға эмас. Дастлаб, ҳар иккала чизиқли ва дифференциял таҳдид айнан DES устида амалга оширилди. Юқорида айтиб ўтилганидек, ушбу таҳдидлар амалий таҳдид эмас. Унинг ўрнига, бу таҳдидлар блокли шифрлардаги заифликни кўрсатишга қаратилган. Бу технологиялар бугунги кунда блокли шифрларни таҳлил қилишда асос восита сифатида қаралади.

DESнинг дифференциал таҳлили. Дииференциал таҳлилнинг асоси кириш ва чиқиш фарқларини таққослашга асосланган. Соддалик учун, биз дастлаб соддалашган S жадвални қараб чиқайлик. Фараз қилайлик, DES да киришда уч бит чиқишда эса икки битни ташкил этувчи S жадвал мавжуд (12.1).

Қатор	Устун			
	00	01	10	11
0	10	01	11	00
1	00	10	01	11

Бу ерда кирувчи битлар $x_0x_1x_2$ га тенг бўлиб, x_0 бит қаторни кўрсатади, x_1x_2 эса усутунни кўрсатади. У ҳолда, масалан, S(010)=11 га тенг, яъни, қатор 0 га тенг ва устун 10 га тенг.

Фараз қилайлик, иккита кириш, X_1=110 ва X_2=010 га тенг ва калит K=011 га тенг. У ҳолда $X_1 \oplus K = 101$ га ва $X_2 \oplus K = 001$ га тенг ва биз қуйидаги тенгликка эга бўламиз:

$$S(X_1 \oplus K) = 10 \text{ ва } S(X_2 \oplus K) = 01 \qquad (12.2)$$

У ҳолда (6.11) тенгликда K калит номаълум, аммо, киришлар X_1=110 ва X_2=010 лар маълум ва шунга мос S жадвалдан чиқувчи қийматлар $S(X_1 \oplus K) = 10$ ва $S(X_2 \oplus K) = 01$ маълум. У ҳолда (6.10) даги S жадвалдан, биз $X_1 \oplus K \in \{000,101\}$ ва $X_2 \oplus K \in \{001,110\}$ ни кўришимиз мумкин. X_1 ва X_2 маълумлигидан қуйидагига эга бўламиз

$$K \in \{110,011\} \cap \{011,100\}$$

Бундан эса калитни K=011 га тенглигини билиш мумкин. Бу таҳдид K калит учун (12.1) тенгликдаги ягона S - жадвал учун маълум очиқматнга асосланган таҳдиддир. Худди шундай усул DES даги ягона S жадвал учун ҳам ишлайди.

Бироқ, DES нинг бир раунди учун битта S жадвалга қаратилган таҳдидни фойдали деб айтиб бўлмайди. Бундан ташқари, таҳдидчи биринчи раундан бошқа бирор раунд учун кирувчи маълумотни билмайди ва худди шундай, охирги раундан ташқари бирор раунд учун чиқувчи қийматни билмайди. Оралиқ раундлар таҳдидчи учун ноаниқ бўлади.

DES таҳлилини фойдалироқ тарзда амалга ошириш учун, бир раунд учун амалга оширилган таҳдидни кенгайтириш зарур, 8 та S жадвал учун амалга ошириш зарур. Бир қарашда бу жуда ҳам қийин вазифадек туйилади.

Бироқ, кириш ва чиқишнинг фарқларига асосланган ҳолда, S жадвалларни “актив” ва “актив бўлмаган” тоифаларга осонлик билан ажратиш мумкин. Бунинг натижасида эса, биз баъзи ҳолларда кенгайтирилган таҳдидни бир раунд учун амалга ошириш мумкин бўлади. Кейин, таҳдидни кенгайтириш учун, кейинги раунд учун фойдали бўлиши учун биз мос кириш ва чиқиш фарқини танлашимиз керак. Бу муаммо, S жадвалнинг махсус хусусиятидир, шунингдек, ҳар бир раунда чизиқли маҳкамлаш амалга оширилади.

Бу ерда муҳими шундаки, биз кириш ва чиқиш фарқини кўрсатишимиз керак. Фараз қилайлик, биз X_1 ва X_2 киришларни биламиз. У ҳолда X_1 кириш учун, S жадвал учун кириш $X_1 \oplus K$ га тенг ва X_2 кириш учун, S жадвал учун кириш $X_2 \oplus K$ га тенг бўлиб, K калит номаълум. mod2 бўйича фарқни ҳисоблаш, XOR амалида қўшиш билан бир бўлиб, S жадвалнинг киришдаги фарқлари қуйидагига тенг

$$X_1 \oplus K \ \oplus \ X_2 \oplus K \ = X_1 \oplus X_2 \qquad (12.3)$$

Демак, киришдаги фарқ калитга боғлиқ эмас. Бу дифференциял таҳдид ишлаши учун бу фундаментал кузатув.

Фараз қилайлик, $Y_1 = S(X_1 \oplus K)$ ва $Y_2 = S(X_2 \oplus K)$ га тенг бўлсин. У ҳолда чиқишдаги фарқ $Y_1 \oplus Y_2$ га тенг бўлиб, бу кейинги раунд учун кирувчи фарқни беради. Мақсад, кирувчи фарқни эҳтиёткорлик билан амалга ошириш бўлиб, бу орқали биз раундлар узра “занжир”ни ҳосил қилишимиз керак. Кириш

фарқи калитга боғлиқ бўлмаганлиги ва дифференциял таҳлил танланган очиқ матнга асосланганлиги сабабли биз киришни ихтиёрий танлашимиз мумкин ва чиқиш фарқи бирор биз истаган бўлиши мумкин.

Дифференциял таҳлилнинг яна бир муҳим элементи шуки, S жадвалда нолларнинг киришдаги фарқи ҳар доим нолларнинг чиқишдаги фарқи бўлади. Нима учун ? Киришдаги нолларнинг фарқининг содда маъноси бу чиқиш қийматларини бир хил бўлиши учун кириш қийматларини бир хиллигидир. Бу кузатувнинг муҳимлиги шундаки бунинг натижасида S жадваллар "актив бўлмаган" дейилади.

Бу ҳолатни доим бўлиши талаб этилмайди. Яъни, чиқиш баъзи аҳамиятни кутилма билан ҳосил бўлса, у ҳолда биз бу таҳдидни амалга оширишимиз мумкин бўлади.

Берилган бирор S жадвал учун, биз фойдали кириш фарқи учун қуйидагича таҳлил қилади. Ҳар бир бўлиши мумкин бўлган кириш X учун, биз X_1 ва X_2 жуфтликларни топишимиз керак.

$$X = X_1 \oplus X_2$$

Ва унга мос чиқувчи фарқни ҳисобласак

$$Y = Y_1 \oplus Y_2$$

Бу ерда, $Y_1 = S\ X_1$ ва $Y_2 = S(X_2)$ га тенг.

Натижаларни жадвал орқали ифодалаш орқали, нотўғри кирувчи қийматни топиш мумкин. Масалан, (6.10) тенгликдаги S жадвал учун олинган таҳлил натижалари 12.1 – жадвалда келтирилган.

12.1 – жадвал

S жадвал фарқларини таҳлили

	$\mathbf{Sbox}(X_1) \oplus \mathbf{Sbox}(X_2)$			
$X_1 \oplus X_2$	00	01	10	11
000	8	0	0	0
001	0	0	4	4
010	0	8	0	0
011	0	0	4	4
100	0	0	4	4
101	4	4	0	0
110	0	0	4	4
111	4	4	0	0

Ихтиёрий S жадвал учун, кириш фарқи 000 га тенг бўлгани муҳим эмас, кириш қийматлари бир хил ва S жадваллар "актив эмас". Сабаби уларнинг чиқиш қийматлари бир хил бўлади. Масалан, 6.6 – жадвалдан кириш қиймати 010 тенг бўлгани ҳар доим, 01 ни қайтаради, яъни энг нотўғри натижа. (12.3) тенгликда ифодалангандек, айтайлик, $X_1 \oplus X_2 = 010$ танлаш орқали, S жадвалга кириш 010 га тенг бўлади ва калит бу фарқни алмаштиради.

DES нинг дифференциял таҳлил етарлича комплекс. Бу технологияни янада

аниқлаштириш учун, аммо, DES нинг барча мураккабликларисиз, биз DES нинг кичиклашган версияси, TDES ни намойиш этамиз. Кейин, TDES нинг чизиқли ва дифференция таҳлилини намойиш этамиз. Аммо, бундан олдин чизиқли таҳлил ҳақида тўхталиб ўтилган.

DESнинг чизиқли криптотаҳлили. Чизиқли криптотаҳлил усуллари дифференциял криптотаҳлил усулларига ўхшаш блокли шифрларнинг чизиқсиз бўлмаган қисмини таҳлил этишга қаратилган. Чизиқли криптотаҳлил усули дифференциял криптотаҳлил усулига қараганда кейинроқ яратилган бўлсада, у тушунарли, DES учун самарали ва у фақат маълум очиқ матнни талаб этади.

Дифферентиал криптотаҳлил усулида, биз киришнинг ва чиқишнинг фарқларини олгандик. Чизиқли криптотаҳлилда эса, мақсад чизиқли тенглик билан шифрнинг чизиқсиз қисмини тахминий ифодалаш. Математиклар чизиқли тенгликни еча олишлари туфайли, агар биз бу тахминни топсак, у ҳолда биз бу таҳдидни шифрлар учун фойдаланишимиз мумкин. DES нинг чизиқсиз қисми S жадвал бўлганлиги туфайли, чизиқли криптотаҳлилни S жадвал учун қўллаймиз.

(12.1) тенгликдаги содда S жадвални қайта кўриб чиқамиз. Биз уч бит киришни $x_0x_1x_2$ орқали икки бит чиқишни эса y_0y_1 орқали белгилагандик. У ҳолда x_0 қаторни ва x_1x_2 устунни билдиради. 12.2 – жадвалда бўлиши мумкин бўлган ҳар бир яқинлик учун қийматлар берилган. Бу жадвалдаги 4 га тенг бўлмаган қийматлар тасодифий бўлмаган чиқишни билдиради.

12.2 – жадвал

S - жадвални чизиқли таҳлили

input bits	output bits		
	y_0	y_1	$y_0 \oplus y_1$
0	4	4	4
x_0	4	4	4
x_1	4	6	2
x_2	4	4	4
$x_0 \oplus x_1$	4	2	2
$x_0 \oplus x_2$	0	4	4
$x_1 \oplus x_2$	4	6	6
$x_0 \oplus x_1 \oplus x_2$	4	6	2

12.2 – жадвалда натижадан кўринадики, масалан, 1 кутилма билан $y_0 = x_0 \oplus x_2 \oplus 1$ ва ¾ кутилма билан $y_0 \oplus y_1 = x_1 \oplus x_2$ га тенг. Бу маълумотдан фойдаланиб, биз S жадвалимизни чизиқли функция билан алмаштиришимиз мумкин. Бунинг билан биз чизиқчиз қисмни чизиқли тенглик билан алмаштиришни амалга оширамиз.

Бу чизиқли тенгликлар блокли шифрларни таҳлил қилишда фойда

келтириши мумкин, масалан, DES, биз бу усулни калит учун чизиқли тенгликни аниқлаш учун ҳаракат қиламиз. Дифференциал криптотаҳлил каби, биз бу натижаларни раундлар узра боғлашимиш керак.
Қандай қилиб биз DES даги S жадвални чизиқли тенглик каби ифодалашимиз керак. DES нинг ҳар бир S жадвали киришнинг чизиқсиз комбинацияси ягона чиқувчи бит учун яхши яқинлашиш. Бироқ, бу ерда кириш битининг чизиқли комбинацияси томонидан чиқиш битининг чизиқли яқинлашиши бўлади. Натижада, DES нинг чизиқли таҳлилида яхши натижа бўлади.

Назорат саволлари

Криптографик алгоритмларни таҳлиллаш усуллари.

Калитларни тўлиқ танлаш усули.

Дифференциал таҳдид усули.

Чизиқли криптотаҳлил.