

ЎЗБЕКИСТОН РЕСПУБЛИКАСИ АХБОРОТ ТЕХНОЛОГИЯЛАРИ ВА КОММУНИКАЦИЯЛАРИНИ РИВОЖЛАНТИРИШ ВАЗИРЛИГИ

**ЎЗБЕКИСТОН РЕСПУБЛИКАСИ АХБОРОТ
ТЕХНОЛОГИЯЛАРИ ВА КОММУНИКАЦИЯЛАРНИ
РИВОЖЛАНТИРИШ ВАЗИРЛИГИ**

ТОШКЕНТ АХБОРОТ ТЕХНОЛОГИЯЛАРИ УНИВЕРСИТЕТИ ҚАРШИ ФИЛИАЛИ

“ТИ” кафедраси

РЕФЕРАТ

МАВУ: Тармокда ахборот хавфсизлигини таъминлаш усуллари, ҳамда уларда ишлатиладиган протоколлар

Бажарди: ТТ-11-13 гурух талабаси А.Ф.Хайруллаев

Қабул қилды: **3.3.Нигматов**

Карши 2017

**Тармоқда ахборот хавфсизлигини таъминлаш усуллари, ҳамда уларда
ишлатиладиган протоколлар**

Режа

1. Идентификациялаш ва аутентификациялаш усуллари, ҳамда уларнинг дастурий ва техник воситалари
2. Идентификация ва аутентификация протоколлари
3. Ахборот бутунлигининг бузилиш сабаблари ва уларнинг бутунлигини таъминлаш усуллари
4. Электрон рақамли имзо ва унинг замонавий турлари
5. Фойдаланилган адабиётлар

Идентификациялаш усуллари. Идентификациялашнинг дастурий ва техник воситалари

Компьютер тизимида рўйхатга олинган ҳар бир субъект (фойдаланувчи ёки фойдаланувчи номидан ҳаракатланувчи жараён) билан уни бир маънода идентификацияловчи ахборот боғлиқ.

Бу ушбу субъектга ном берувчи сон ёки символлар сатри бўлиши мумкин. Бу ахборот субъект *идентификатори* деб юритилади. Агар фойдаланувчи тармоқда рўйхатга олинган идентификаторга эга бўлса у легал (қонуний), акс ҳолда легал бўлмаган (ноқонуний) фойдаланувчи ҳисобланади. Компьютер ресурсларидан фойдаланишдан аввал фойдаланувчи компьютер тизимининг идентификация ва аутентификация жараёнидан ўтиши лозим.

Идентификация (Identification) - фойдаланувчини унинг идентификатори (номи) бўйича аниқлаш жараёни. Бу фойдаланувчи тармоқдан фойдаланишга уринганида биринчи галда бажариладиган функциядир. Фойдаланувчи тизимга унинг сўрови бўйича ўзининг идентификаторини билдиради, тизим эса ўзининг маълумотлар базасида унинг борлигини текширади.

Охирги вақтда инсоннинг физиологик параметрлари ва характеристикаларини, хулқининг хусусиятларини ўлчаш орқали фойдаланувчини ишончли аутентификациялашга имкон берувчи биометрик аутентификациялаш кенг тарқалмоқда.

Биометрик аутентификациялаш усуллари анъанавий усулларга нисбатан қўйидаги афзалликларга эга:

- биометрик алломатларнинг ноёблиги туфайли аутентификациялашнинг ишончлилик даражаси юқори;
- биометрик алломатларнинг соғлом шахсадан ажратиб бўлмаслиги;
- биометрик алломатларни сохталаштиришнинг қийинлиги.

Фойдаланувчини аутентификациялашда фаол ишлатиладиган биометрик алгоритмлар қўйидагилар:

- бармоқ излари;
- қўл панжасининг геометрик шакли;
- юзнинг шакли ва ўлчамлари;
- овоз хусусиятлари;
- қўз ёйи ва тўр пардасининг нақши.

Аутентификациялаш усуллари. Аутентификациялаш дастурий ва техник воситалари

Аутентификация (Authentication) – маълум қилинган фойдаланувчи, жараён ёки қурилманинг ҳақиқий эканлигини текшириш муолажаси. Бу

текшириш фойдаланувчи (жараён ёки қурилма) ҳақиқатан айнан ўзи эканлигига ишонч ҳосил қилишига имкон беради. Аутентификация ўтқазишида текширувчи тараф текширилувчи тарафнинг ҳақиқий эканлигига ишонч ҳосил қилиши билан бир қаторда текширилувчи тараф ҳам ахборот алмашинув жараёнида фаол қатнашади. Одатда фойдаланувчи тизимга ўз хусусидаги ноёб, бошқаларга маълум бўлмаган ахборотни (масалан, парол ёки сертификат) киритиши орқали идентификацияни тасдиқлади.

Идентификация ва аутентификация субъектларнинг (foyдаланувчиларнинг) ҳақиқий эканлигини аниқлаш ва текширишнинг ўзаро боғланган жараёнидир. Муайян фойдаланувчи ёки жараённинг тизим ресурсларидан фойдаланишига тизимнинг рухсати айнан шуларга боғлик. Субъектни идентификациялаш ва аутентификациялашдан сўнг уни авторизациялаш бошланади.

Маълумотларни узатиш каналларини ҳимоялашда *субъектларнинг ўзаро аутентификацияси*, яъни алоқа каналлари орқали боғланадиган субъектлар ҳақиқийлигининг ўзаро тасдиғи бажарилиши шарт. Ҳақиқийликнинг тасдиғи одатда сеанс бошида, абонентларнинг бир-бирига уланиш жараёнида амалга оширилади. “Улаш” атамаси орқали тармоқнинг иккита субъекти ўртасида мантиқий боғланиш тушунилади. Ушбу муолажанинг мақсади – улаш қонуний субъект билан амалга оширилганлигига ва барча ахборот мўлжалланган манзилга боришлигига ишончни таъминлашдир.

Ўзининг ҳақиқийлигининг тасдиқлаш учун субъект тизимга турли асосларни кўрсатиши мумкин. Субъект кўрсатадиган асосларга боғлик ҳолда аутентификация жараёнлари қўйидаги категорияларга бўлиниши мумкин:

- *бирор нарсани билиши асосида*. Мисол сифатида парол, шахсий идентификация коди PIN (Personal Identification Number) ҳамда “сўров жавоб” хилидаги протоколларда намойиш этилувчи маҳфий ва очиқ қалитларни кўрсатиш мумкин;

- *бирор нарсага эгалиги асосида*. Одатда булар магнит карталар, смарт-карталар, сертификатлар ва touch memory қурилмалари;

- *қандайдир дахлсиз характеристикалар асосида*. Ушбу категория ўз таркибига фойдаланувчининг биометрик характеристикаларига (овозлар, кўзининг рангдор пардаси ва тўр пардаси, бармоқ излари, кафт геометрияси ва х.) асосланган усулларни олади. Бу категорияда криптографик усуллар ва воситалар ишлатилмайди. Беометрик характеристикалар бинодан ёки қандайдир техникадан фойдаланишни назоратлашда ишлатилади.

Парол – фойдаланувчи ҳамда унинг ахборот алмашинувидаги шериги биладиган нарса. Ўзаро аутентификация учун фойдаланувчи ва унинг шериги ўртасида парол алмашиниши мумкин. Пластик карта ва смарт-карта эгасини аутентификациясида шахсий идентификация номери PIN синалган усул ҳисобланади. PIN – коднинг маҳфий қиймати факат карта эгасига маълум бўлиши шарт.

Динамик – (бир марталик) парол- бир марта ишлатилганидан сўнг бошқа умуман ишлатилмайдиган парол. Амалда одатда доимий паролга ёки таянч иборога асосланувчи мунтазам ўзгариб турувчи қиймат ишлатилади.

“Сўров-жавоб” тизими - тарафларнинг бири ноёб ва олдиндан билиб бўлмайдиган “сўров” қийматини иккинчи тарафга жўнатиш орқали аутентификацияни бошлаб беради, иккинчи тараф эса сўров ва сир ёрдамида ҳисобланган жавобни жўнатади. Иккала тарафга битта сир маълум бўлгани сабабли, биринчи тараф иккинчи тараф жавобини тўғрилигини текшириши мумкин.

Сертификатлар ва рақамли имзолар - агар аутентификация учун сертификатлар ишлатилса, бу сертификатларда рақамли имзонинг ишлатилиши талаб этилади. Сертификатлар фойдаланувчи ташкилотининг масъул шахси, сертификатлар сервери ёки ташкилотининг томонидан берилади. Internet доирасида очиқ калит сертификатларини тарқатиш учун очиқ калитларни бошқарувчи қатор тижорат инфратузилмалари PKI (Public Key Infrastructure) пайдо бўлди. Фойдаланувчилар турли даражага сертификатларини олишлари мумкин.

Аутентификация жарёнларини таъминланувчи хавфсизлик даражаси бўйича ҳам туркумлаш мумкин. Ушбу ёндашишга биноан аутентификация жараёнлари қуйидаги турларга бўлинади:

- пароллар ва рақамли сертификатлардан фойдаланувчи аутентификация;
- криптографик усуслар ва воситалар асосидаги қатъий аутентификация;
- нуллик билим билан исботлаш хусусиятига эга бўлган аутентификация жараёнлари (протоколлари);
- фойдаланувчиларни биометрик аутентификацияси.

Хавфсизлик нуқтаи назаридан юқорида келтирилганларнинг ҳар бири ўзига хос масалаларни ечишга имкон беради. Шу сабабли аутентификация жараёнлари ва протоколлари амалда фаол ишлатилади. Шу билан бир қаторда таъкидлаш лозимки, нуллик билим билан исботлаш хусусиятига эга бўлган аутентификацияга қизиқиши амалий характерга нисбатан қўпроқ назарий характерга эга. Балким, яқин келажакда улардан ахборот алмашинувини ҳимоялашда фаол фойдаланишлари мумкин.

Аутентификация протоколларига бўладиган асосий хужумлар қуйидагилар:

- *маскарад* (impersonation). Фойдаланувчи ўзини бошқа шахс деб кўрсатишга уриниб, у шахс тарафидан харакатларнинг имкониятларига ва имтиёзларига эга бўлишни мўлжаллайди;
- аутентификация алмашинуви *тарафини алмаштириб қўйши* (interleaving attack). Нияти бузук одам ушбу хужум мобайнида икки тараф орасидаги аутенфикацион алмашиниш жараённада трафикни модификациялаш ниятида қатнашади. Алмаштириб қўйишнинг қуйидаги хили мавжуд: иккита фойдаланувчи ўртасидаги аутентификация муваффақиятли ўтиб, уланиш ўрнатилганидан сўнг бузғунчи

фойдаланувчилардан бирини чиқариб ташлаб, унинг номидан ишни давом эттиради;

- *такрорий узатиш* (replay attack). Фойдаланувчиларнинг бири томонидан аутентификация маълумотлари такроран узатилади;

- *узатишни қайтариш* (reflection attack). Олдинги хужум вариантларидан бири бўлиб, хужум мобайнида нияти бузук одам протоколнинг ушбу сессия доирасида ушлаб қолинган ахборотни орқага қайтаради.

- *мажбурий кечикиши* (forced delay). Нияти бузук одам қандайдир маълумотни ушлаб қолиб, бирор вақтдан сўнг узатади.

- *матн танлашили хужум* (chosen text attack). Нияти бузук одам аутентификация трафигини ушлаб қолиб, узоқ муддатли криптографик калитлар хусусидаги ахборотни олишга уринади.

Юқорида келтирилган хужумларни бартараф қилиш учун аутентификация протоколларини қуришда қуйидаги усуллардан фойдаланилади:

- “сўров–жавоб”, вақт белгилари, тасодифий сонлар, индентификаторлар, рақамли имзолар каби механизмлардан фойдаланиш;

- аутентификация натижасини фойдаланувчиларнинг тизим доирасидаги кейинги харакатларига боғлаш. Бундай мисол ёндашишга тариқасида аутентификация жараёнида фойдаланувчиларнинг кейинга ўзаро алоқаларида ишлатилувчи махфий сеанс калитларини алмашишни кўрсатиш мумкин;

- алоқанинг ўрнатилган сеанси доирасида аутентификация муолажасини вақти-вақти билан бажариб туриш ва ҳ.

Вақтни белгилаш механизми ҳар бир хабар учун вақтни қайдлашни кўзда тутади. Бунда тармоқнинг ҳар бир фойдаланувчиси келган хабарнинг қанчалик эскирганини аниқлаши ва уни қабул қиласлик қарорига келиши мумкин, чунки у ёлғон бўлиши мумкин. Вақтни белгилашдан фойдаланишда сеанснинг хақиқий эканлигини тасдиқлаш учун *кечикишининг жоиз вақт оралиги* муаммоси пайдо бўлади. Чунки, “вақт тамғаси”ли хабар, умуман, бир лахзада узатилиши мумкин эмас. Ундан ташқари, қабул қилувчи ва жўнатувчининг соатлари мутлақо синхронланган бўлиши мумкин эмас.

Аутентификация протоколларини таққослашда ва танлашда қуйидаги характеристикаларни ҳисобга олиш зарур:

- *ўзаро аутентификациянинг мавжудлиги*. Ушбу хусусият аутентификацион алмашинув тарафлари ўртасида иккиёклама аутентификациянинг зарурлигини акс эттиради;

- *ҳисоблаш самарадорлиги*. Протоколни бажаришда зарур бўлган амаллар сони;

- *коммуникацион самарадорлик*. Ушбу хусусият аутентификацияни бажариш учун зарур бўлган хабар сони ва узунлигини акс эттиради;

- *учинчи тарафнинг мавжудлиги*. Учинчи тарафга мисол тариқасида симметрик калитларни тақсимловчи ишончли серверни ёки очиқ калитларни тақсимлаш учун сертификатлар дарахтини амалга оширувчи серверни кўрсатиш мумкин;

- *хавфсизлик кафолати асоси*. Мисол сифатида нуллик билим билан исботлаш хусусиятига эга бўлган протоколларни кўрсатиш мумкин;

- сирни сақлаши. Жиддий калитли ахборотни сақлаш усули күзда тутилади.

Идентификация ва аутентификация протоколлари

SKID2, SKID3 протоколлари RACE RIPE проекти учун ишлаб чиқилған симметрик криптографик идентификациялаш протоколи ҳисобланади. Улар хавфсизликни таъминлаш учун МАС ни қўллаб иккала фойдаланувчи бир-бiri билан алоқа қилишида умумий маҳфий калит К ни ишлатиш йўли билан амалга оширилади.

SKID2 протоколи 1-фойдаланувчини 2-фойдаланувчига ҳақиқийлигини исботлаб беради. SKID3 протоколи ўзаро аутентификациялашни таъминлайди.

Бу протокол МИТМ бузиш усулига бардошли эмас, умуман олганда қанақадир сир ётмаган ҳар қандай протокол бардош бера олмайди.

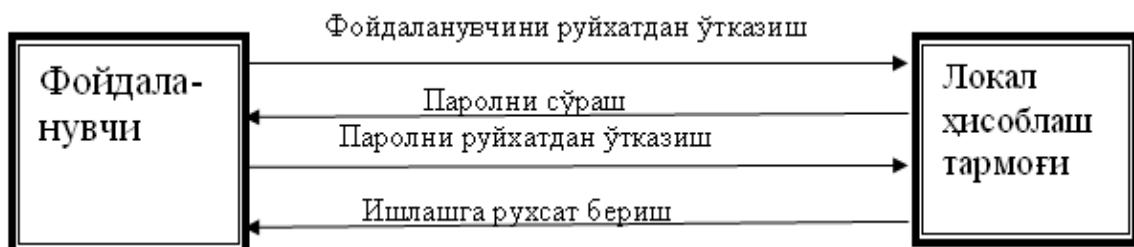
Компьютер тармоқларида аутентификациялаш протоколларининг 2 тури мавжуд:

1. Фойдаланувчини аутентификациялаш
2. Маълумотларни аутентификациялаш

Фойдаланувчини аутентификациялаш бу фойдаланувчи томонидан кўрсатилган аутентификатор ёрдамида ҳақиқийлигини тасдиқлаш жараёнидир. Аутентификатор бу аутентификациялаш воситаси бўлиб, фойдаланувчини фарқ қиласиган белгилари бўйича характерлайди. Аутентификатор сифатида компьютер тармоқларида одатда парол ва фойдаланувчини биометрик маълумотлари қўлланилади. Биометрик маълумотлар сифатида бармоқ излари, кўз тур пардаси ва панжа изи ишлатилиши мумкин.

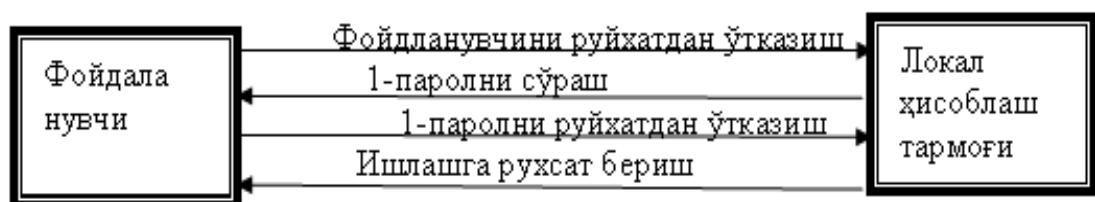
Парол бу кодланган сўз бўлиб, ҳарфли, рақамли ва ҳарфли-рақамли шаклда компьютер билан мулоқат бошланишидан олдин ишлайди.

Замонавий компьютер тармоқларида ҳар бир фойдаланувчи фойдаланувчини ҳақиқийлигини тасдиқлаш ва тармоқда ишлаш имкониятини таъминлаш мақсадида парол ва идентификатор билан таъминланган бўлади. Шу билан биргаликда аутентификациялаш протоколлари ҳам ишлаб чиқлади. Улардан энг оддийси оддий паролларни ёки (пароллар руйхатида ўзгариб турадиган) ҳосил қилинган пароллар рўйхатидан ўзгариб турадиган паролларни қўллаш ёрдамида шаклланади.



1-расм. Оддий пароллар ёрдамида ишлаб чиқилган аутентификациялаш протоколи

Ушбу протокол жуда содда ва паст химояланган, фойдаланувчини идентификаторлари ўзининг ходимлари орасида сир бўлмайди. Паролни эса фойдаланиш ҳукуки юқори бўлган фойдаланувчи қийинчиликсиз билиб олиши мумкинлиги унинг камчилигидир. Фойдаланувчини аутентификациялаш протоколи пароллар руйхати асосида ишлаб чиқилса 1-усулга нисбатан химояланганлиги юқори бўлади. Бундан фойдаланувчи ва тармоқ пароллар рўйхатига эга бўлади.



2-расм. Фойдаланувчини аутентификациялаш протоколи пароллар руйхати асосида ишлаб чиқиш

Пароллар асосида қурилган аутентификациялаш протоколида қўйидаги жараёнлар амалга оширилади:

Биринчи навбатда фойдаланувчи ўзининг идентификаторини тармоқга киргизади, сўнг тармоқ пароллар руйхатидан 1-паролни сўрайди. Фойдаланувчи пароллар рўйхатидан мос келадиган 1-паролни киргизади ва тасдиқдан ўтгандан сўнг тармоқда ишлашга рухсат олади. Агарда у тармоқга қайтадан кирадиган бўлса пароллар руйхатидан 2-парол сўралади. Бу протоколни камчилиги: узун пароллар рўйхатини эслаб қолиши зарурияти, алоқа линияларида бузилишлар бўлганда паролни танлаш ноаниклиги.

Маълумотларни аутентификациялаш бу электрон формада келтирилган маълумотларни ҳақиқийлигини тасдиқлаш жараёнидир. Маълумотлар, хабарлар, файллар фойдаланувчиларнинг аутентификаторлари кўринишида бўлиши мумкин.

Паролли химоя ва уларнинг турлари

Пароллар, одатда, тизимга кириш учун калит сифатида ишлатилади, лекин улар бошқа мақсадлар учун ҳам ишлатилади: дискга блоклаш, маълумотларни шифрлашдаги буйруқларда, яъни мос харакатлар фақатгина дастур таъминотининг қонуний эгалари ва фойдаланувчилари томонидан амалга оширилишга қатъий ишонч талаб этиладиган барча холатлардир.

Ишлатиладиган паролларни қуидаги гурухларга ажратиш мумкин:

- фойдаланувчи томонидан ўрнатиладиган пароллар;
- тизим ишлаб чиқарадиган пароллар;
- тизим ишлаб чиқарадиган мурожаат қилишнинг тасодифий кодлари;
- яримта сўз;
- таянч иборалар;
- “савол- жавоб” туридаги интерактив кетма-кетликлар;
- “қатъий пароллар”.

Фойдаланувчи томонидан ўрнатиладиган пароллар энг кўп тарқалган гурухдир. Кўпчилик холатларда бундай паролни фойдаланувчининг ўзи ўрнатади, парол етарлича узун бўлиши керак. Мувафаккиятсиз паролни яратишига имкон бермайдиган усуллар бор. Масалан, тизим парол ўз ичига ёзма ва босма ҳарфларни рақамлар билан аралашганини олишини талаб этиши мумкин; очикдан-очиқ пароллар тизим томонидан инкор қилинади.

Тасодифий пароллар ва кодлар тизим томонидан ўрнатилади. Тизимли Дастур Таъминоти белгиларнинг тасодифий кетма-кетлигини тўлиқ ишлатилиши мумкин. Регистр, рақам, узунликларини тасодифий танлашгача ёки ишлаб чиқарадиган жараёнларда чекланишларини ишлатиш керак.

Яримта сўз қисман фойдаланувчи, қисман тасодифий жараён томонидан яратилади. Агар фойдаланувчи енгил топиладиган парол ўйлаб топса, компьютер уни янада мураккаб тўлдиради (Масалан : абзац-абзац).

“Қатъий пароллар” одатда бирорта ташқи электрон ёки механик курилма билан бирга ишлатилади. Бу ҳолда компьютер таклифларнинг бир нечта вариантини таклиф этади, фойдаланувчи эса уларга тўғри келадиган жавобларни бериши керак. Паролларнинг бу кўриниши кўпинча бир марталик кодли тизимларда учрайди. Бир марталик кодлар ҳақиқий фойдаланувчи тизимга биринчи марта киришида ишлатилиши мумкин, кейин фойдаланувчи ўзининг паролини янада маҳфийроқ шахсий код билан алмаштириши керак. Тизимдан одамлар гурухи фойдаланган, лекин бунда маҳфийликни бузиш мумкин бўлмаган ҳолларда бир марталик кодларнинг рўйхатига мурожаат қилинади. У ёки бу фойдаланувчи вақт, сана ёки ҳафтанинг кунига мос келадиган код киритади.

Паролнинг ишончлиги қуидаги талабларнинг бажарилиши билан таъминланади:

- маълум бир узунликда бўлиши керак;
- ўз таркибига ҳам ёзма, ҳам босма ҳарфларни олиши керак;
- ўз таркибига битта ва ундан ортиқ рақамларни олиши керак;
- ўз таркибига битта рақамсиз ва битта алфавитсиз белгини олиши керак.

Пароллар асосида аутентификациялаш

Аутентификациянинг кенг тарқалган схемаларидан бири *оддий аутентификациялаш* бўлиб, у анъанавий кўп мартали паролларни ишлатишига асосланган. Тармоқдаги фойдаланувчини оддий аутентификациялаш муолажасини қуидагича тасаввур этиш мумкин. Тармоқдан фойдаланишга уринган фойдаланувчи компьютер клавиатурасида ўзининг идентификатори ва паролини теради. Бу маълумотлар аутентификация серверига ишланиш учун тушади. Аутентификация серверида сақланаётган фойдаланувчи идентификатори бўйича маълумотлар базасидан мос ёзув топилади, ундан паролни топиб фойдаланувчи киритган парол билан таққосланади. Агар улар мос келса, аутентификация муваффақиятли ўтган ҳисобланади ва фойдаланувчи легал (қонуний) мақомини ва авторизация тизими орқали унинг мақоми учун аниқланган хукуқларни ва тармок ресурсларидан фойдаланишга рухсатни олади.

Сертификатлар асосида аутентификациялаш

Тармоқдан фойдаланувчилар сони миллионлаб ўлчанганида фойдаланувчилар паролларининг тайинланиши ва сақланиши билан боғлиқ фойдаланувчиларни дастлабки рўйхатга олиш муолажаси жуда катта ва амалга оширилиши қийин бўлади. Бундай шароитда рақамли сертификатлар асосидаги аутентификациялаш пароллар қўлланишига рационал альтернатива ҳисобланади.

Рақамли сертификатлар ишлатилганида компьютер тармоғи фойдаланувчилари хусусидаги ҳеч қандай ахборотни сақламайди. Бундай ахборотни фойдаланувчиларнинг ўзи сўров-сертификатларида тақдим этадилар. Бунда махфий ахборотни, хусusan махфий калитларни сақлаш вазифаси фойдаланувчиларнинг ўзига юкландади.

Қатъий аутентификациялаш

Криптографик протоколларида амалга оширилувчи қатъий аутентификациялаш ғояси қуидагича: Текширилувчи (исботловчи) тараф қандайдир сирни билишини намойиш этган ҳолда текширувчига ўзининг ҳақиқий эканлигини исботлайди. Масалан, бу сир аутентификацион алмашиш тарафлари ўртасида олдиндан хавфсиз усул билан тақсимланган бўлиши мумкин. Сирни билишлик исботи криптографик усул ва воситалардан фойдаланилган ҳолда сўров ва жавоб кетма-кетлиги ёрдамида амалга оширилади.

Энг муҳими, исботловчи тараф фақат сирни билишлигини намойиш этади, сирни ўзи эса аутентификацион алмашиш мобайнида очилмайди. Бу текширувчи тарафнинг турли сўровларига исботловчи тарафнинг жавоблари ёрдами билан таъминланади. Бунда якуний сўров фақат фойдаланувчи сирига ва протокол бошланишида ихтиёрий танланган катта сондан иборат бошланғич сўровга боғлиқ бўлади.

Аксарият ҳолларда қатъий аутентификациялашга биноан ҳар бир фойдаланувчи ўзининг махфий калитига эгалиги аломати бўйича

аутентификацияланади. Бошқача айтганда фойдаланувчи унинг алоқа бўйича шеригининг тегишли махфий калитга эгалигини ва у бу калитни ахборот алмашинуви бўйича ҳақиқий шерик эканлигини исботлашга ишлата олиши мумкинлигини аниқлаш имкониятига эга.

Охирги вақтда инсоннинг физиологик параметрлари ва характеристикаларини, хулқининг хусусиятларини ўлчаш орқали фойдаланувчини ишончли аутентификациялашга имкон берувчи биометрик аутентификациялаш кенг тарқалмоқда.

Биометрик аутентификациялаш усуллари анъанавий усулларга нисбатан қўйидаги афзалликларга эга:

- биометрик аломатларнинг ноёблиги туфайли аутентификациялашнинг ишончлилик даражаси юқори;
- биометрик аломатларнинг соғлом шахсдан ажратиб бўлмаслиги;
- биометрик аломатларни сохталашибтиришнинг қийинлиги.

Ахборот бутунлигининг бузилиш сабаблари ва уларнинг бутунлигини таъминлаш усуллари

Хавф-хатарларни тахлиллаш ва бошқариш ахборот тизимидағи таҳдидлар, заифликлар ва хавф-хатарларни баҳолаш ҳамда ушбу ахборот тизими хавфсизлигининг етарли даражасини таъминловчи қарши чораларни аниқлаш учун ишлатилади.

Хавф-хатарларни тахлиллаш-таҳдидларни, заифликларни ва корпоратив ахборот тизими хавфсизлигига бўлиши мумкин бўлган заарларни аниқлаш жараёни. Хавф-хатарларни тахлиллашдан мақсад мавжуд хавф-хатарларни аниқлаш ва улар меъёрини баҳолаш (уларга миқдорий баҳо бериш). Хавф-хатарларни тахлиллаш компьютер ахборот тизими хавфсизлигини текшириш бўйича тадбирни ўз ичига олади. Бу тадбирга биноан кайси ресурсларни қайси таҳдидлардан химоялаш зарурлиги ҳамда у ёки бу ресурслар қандай даражада химояга муҳтоҷ эканлиги аникланади.

Хавф-хатарларни тахлиллашга турли ёндашишлар мавжуд. Ёндашишни танлаш ташкилотда ахборот хавфсизлиги режимига қўйиладиган талаблар даражасига ва эътиборга олинувчи таҳдидлар характеристига (таҳдидлар таъсири спектрига) боғлиқ. Талаблариинг иккита даражаси фарқланади:

- ахборот хавфсизлиги режимига минимал талаблар;
- ахборот хавфсизлиги режимига оширилган талаблар.

Ахборот хавфсизлиги режимига минимал талаблар ахборот хавфсизлигининг базавий даражасига мос келади. Бу даражадан, одатда, намунавий лойиха счимларида фойдаланилади. Хавф-хатарларни тахлиллаш соддалаштирилган схема бўйича ттказилади: хавфсизликка таҳдидларнинг кўп тарқалган тўплами уларнинг эҳтимоллигини баҳоламасдан кўрилади. Вируслар, асбоб-ускуналарнинг бузилиши, рухсатсиз фойдаланиш ва х, каби эҳтимоллиги юқори таҳдидларнинг

минимал тўплами кўриладиган қатор стандартлар ва спецификациялар мавжуд. Бундай таҳдидларни бетарафлаштириш учун уларнинг амалга оширилиши эҳтимоллиги ва ресурсларнинг заифлигидан катъий назар, қарши чоралар кўрилиши лозим, яъни базавий даражада таҳдидлар характеристикаларини кўриш шарт эмас.

Ахборот хавфсизлиги режимига оширилган талаблар, ахборот хавфсизлиги режимининг бузилиши оғир оқибатларга сабаб бўлганида ва ахборот хавфсизлиги режимига минимал талаблар етарли бўлмаганида ишлатилади.

Ахборот хавфсизлиги режимига оширилган талабларни таърифлаш учун ресурслар ахамиятини аниқлаш, тадқиқланувчи ахборот тизими учун долзарб бўлган таҳдидлар рўйхати билан стандарт тўпламни тўлдириш, таҳдидлар эҳтимоллигини баҳолаш ва ресурслар заифлигини аниқлаш зарур.

Хавф-хатарни таҳлиллаш жараёнини қуидаги босқичларга ажратиш мумкин:

- корпоратив ахборот тизимининг таянч ресурсларини идентификациялаш;
- ёки бу ресурснинг муҳимлигини аниқлаш;
- таҳдидларнинг амалга оширилишига имкон берувчи мавжуд хавфсизлик таҳдидларни ва заифликларни идентификациялаш;
- хавфсизликка таҳдидларни амалга оширилиши билан боғлиқ хавф-хатарларни хисоблаш.

Ресурслар учта категорияга ахборот ресурсларига, дастурий таъминотга ва техник воситаларга (файл серверлари, ишчи станциялар, кўприклар, маршрутизаторлар ва х.) бўлинади. Хар бир категория ичida ресурсларни синфларга ва қисм синфларга ажратиш мумкин. Фақат корпоратив ахборот тизими функционаллигини белгиловчи ва хавфсизликни таъминлаш нуктаи назаридан муҳим бўлган ресурлар идентификацияланиши лозим.

Ресурснинг муҳимлиги (нархи) бу ресурснинг конфиденциаллиги, яхлитлиги ёки фойдаланувчанлиги бузилганида етказилган зарар миқдори билан белгиланади. Ресурслар нархини баҳолашда ресурсларининг хар бир категорияси учун бўлиши мумкин бўлган зарар миқдори белгиланади.

Намунавий хавфсизлик таҳдидларига корпоратив ахборот тизими ресурсларига локал масофадан хужумлар, табиий оғат, ходимлар хатоси, дастурий таъминотдаги хатолик ёки аппаратуранинг носозлиги сабаб бўлувчи корпоратив ахборот тизим ишидаги бузилишлар тааллуқли. Таҳдид даражаси деганда унинг амалга оширилиши эҳтимоллиги тушунилади.

Химоянинг бўшлиги корпоратив ахборот тизимидағи заифликларга сабаб бўлади. Заифликларни баҳолаш хавфсизлик таҳдидларининг муваффақиятли амалга оширилиш эҳтимоллигини аниқлашни назарда тутади. Шундай қилиб, зарар етказиш эҳтимоллиги таҳдидларининг амалга оширилиши эҳтимоллиги ва заифлик миқдори орқали аниқланади.

Хавф-хатар даражаси ресурс нархи, таҳдид даражаси ва заифлик миқдори асосида аниқланади. Ресурс нархи, таҳдид даражаси ва заифлик

микдори ошиши билан хавф-хатар даражаси хам ошади. Хавф-хатарлар даражасини баҳолаш асосида хавфсизлик талаблари белгиланади.

3-расмда хавф-хатарларни бошқариш технологиясининг босқичлари келтирилган.



3-расм. Хавф-хатарларни бошқариш технологиясининг босқичлари

Хавф-хатарларни бошқариш масаласи, хавф-хатар даражасини мақбул микдоргача камайтиришга имкон берувчи қарши чораларни асосли танлашни ва амалга ошириш нархини баҳолашни ўз ичига олади.

Табиийки, қарши чораларни амалга ошириш нархи бўлиши мумкин бўлган зарар микдоридан кам бўлиши керак.

Ахборот хавфсизлиги сиёсатини аниқлаш. Бу босқичда ахборот хавфсизлиги соҳасидаги қўлланма-хужжатлар, стандартлар, ахборот хавфсизлигининг асосий коидалари, хавф-хатарларни бошқаришга ёндашишлар аниқланади хамда қарши чоралар структуризацияланади ва корпоратив ахборот тизимини сертификациялаш тартиби белгиланади.

Корпоратив ахборот тизимини (КАТ) тавсифлаш. Ушбу босқичда ахборот хавфсизлиги соҳасидаги халқаро, давлат ва корпоратив стандартларга биноан корпоратив ахборот тизимнинг функционал вазифалари тавсифланади. Компаниянинг критик ахборот ресурслари, жараёнлари ва сервислари тавсифланади; корпоратив ахборот тизимининг чегаралари хамда бошқариш ва маълумотлар бўйича энг муҳим компонентларининг таркиби ва боғланишлари аниқланади.

Тахдидларни иденшификациялаш. Ушбу босқичда тахдидлар рўйхати тузилади ва уларнинг даражаси баҳоланади. Бунда турли ташкилотларнинг тахдидлар синфлари рўйхатидан хамда берилган тахдидни амалга ошириш эҳтимоллигининг рейтинги ёки ўртacha қийматидан фойдаланиш мумкин.

Заифликларни идентификациялаш. Ушбу босқичда берилган корпоратив ахборот тизимининг заифликлари рўйхати, уларнинг амалга оширилишидаги жоиз натижалар қўрсатилган холда тузилади. Мавжуд корпоратив ахборот тизими учун рўйхатлар қатор манбалардан фойдаланилиб тузилади. Бу манбадарга заифликларни тармоқ сканерлари, турли ташкилотларнинг заифликлар каталоги хавф-хатарларни тахлилловчи ихтисослаштирилган усууллар киради.

Корпоратив ахборот тизимининг бошқариш тизимшш тщиллаш. Ушбу босқичда бошқариш, тизими, аниқланган тахдидларга ва заифликларга жоиз бўлган таъсир нуқтаи назаридан тахлилланади.

Тахдидлар параметрларини баҳолаш. Ушбу босқичда ходисага олиб келувчи заифликнинг амалга оширилиши имконияти баҳоланади. Баҳолашнинг намунавий шкаласи - бир неча рутбали (масалан, паст, ўрта ва юқори сатҳ) сифатий (балли) шкаладир. Бундай баҳо эксперт томонидан мавжуд объектив факторларни хисобга олган холда берилади.

Ахборот хавфсизлиги режимиининг бузилиши оқибатларини тахлиллаш. Ушбу босқичда ахборот хавфсизлиги режимиининг бузилиши баҳоси аниқланади. Бузилиш оқибатлари молиявий йукотишларга, обрўсизланишга, расмий тузилмалар томонидан қўнгилсизликларга ва х. сабаб бўлиши мумкин. Бузилиш оқибатларини баҳолаш учун мезонлар тизими танланади ва оқибатлар оғирлигини баҳолаш учун интеграцияланган шкала белгиланади.

Хавф-хатарларни баҳолаш. Ушбу босқичда ахборот ресурслари хавфсизлигининг бузилиши хавф-хатар даражаси баҳоланади. Хавф-хатар даражаси қиймати тахдидлар, заифликлар даражасига ва бўлиши мумкин бўлган оқибатлар оғирлигига боғлик. Хавф-хатарларни баҳолашда сифатий

ва миқдорий усуллардан фойдаланилади. Сифатий усул ишлатилганда ахборот хавфсизлиги бузилишининг бўлиши мумкин бўлган хавф-хатарлар хавфлилиги даражаси бўйича рутбаланиши лозим. Миқдорий усул ишлатилганда хавф-хатарлар миқдорий шкалаларда баҳоланиши мумкин. Бу тавсия этилаётган қарши чораларнинг нархи-самарадорлигини тахлиллашниосонлаштиради. Аммо бу ходда дастлабки маълумотларни ўлчаш шкалаларига ва ишлатилаёгган моделнинг адекватлигига жуда юқори талаблар қўйилади. Оддий холда хавф-хатарни баҳолашда иккита омил-ходиса эҳтимоллиги ва бўлиши мумкин бўлган оқибатлар оғирлигиишлатилиши мумкин.

Хавф-хатарларни бошқариш бўйича тавсияларни ишлаб чиқиши. Ушбу босқичда турли сатхлар (ташкилий, дастурий-техник) ва хавфсизликнинг алоҳида жихатлари бўйича структуризацияланган қарши чораларнинг комплекси тавсия этилиши лозим. Таклиф этилувчи қарши чоралар комплекси хавф-хатарларни бошқаришнинг танланган стратегиясига биноан курилади.

Хисобот хужжатларни ишлаб чиқиши. Ушбу босқичда хавф-хатарларни тахлилаш ва бошқаришнинг барча босқичлари бўйича иш натижалари акслантирилган хисобот хужжатлари тайёрланади.

Таъкидлаш лозимки, хозирда ахборот хавф-хатарларини баҳолашни автоматлаштириш мақсадида дастурий маҳсулотлар ишлаб чиқилган.

Криптография усуллари

Жамиятни компьютерлаштириш, бир қатор фойдалардан ташқари, ўзи билан бир қатор муаммоларни олиб келди. Жуда ҳам мураккаб бўлган бундай муаммолардан биттаси ахборотни қайта ишлаш ва узатиш тизимларида махфий ахборот хавфсизлигини таъминлашдадир.

Бу муаммони ҳал қилиш учун ахборотни ҳимоя қилишнинг криптографик усуллари кенг ишлатилмоқда, бунда бошланғич ахборот шундай ўзгартириладики, бунинг натижасида ахборот керакли ваколатларга эга бўлмаган шахсларга танишиш ва ишлатиш учун мумкин бўлмай қолади.

Жамиятни компьютерлаштириш, бир қатор фойдалардан ташқари, ўзи билан бир қатор муаммоларни олиб келди. Жуда ҳам мураккаб бўлган бундай муаммолардан биттаси ахборотни қайта ишлаш ва узатиш тизимларида махфий ахборот хавфсизлигини таъминлашдадир.

Бу муаммони ҳал қилиш учун ахборотни ҳимоя қилишнинг криптографик усуллари кенг ишлатилмоқда, бунда бошланғич ахборот шундай ўзгартириладики, бунинг натижасида ахборот керакли ваколатларга эга бўлмаган шахсларга танишиш ва ишлатиш учун мумкин бўлмай қолади.

Бошланғич ахборотга таъсир кўриниши бўйича криптографик ўзгартиришни қўйидаги усуллари мавжуд: **шифрлаш, стенография, кодлаш, зичлаштириш.**

Шифрлаш жараёни бошланғич ахборот устида орқага қайтадиган математик, мантикий, комбинаторлик ва бошқа ўзгартришларни ўтказишидир, бунинг натижасида шифрланган ахборот ҳарфларнинг, рақамларнинг, бошқа белгилар ва иккилиқ кодларнинг тартибсиз түплами кўринишига эгадир.

Ахборотни шифрлаш учун ўзгартриш алгоритми ва калит ишлатилади. Одатда, маълум бир шифрлаш алгоритми учун ўзгартриш алгоритми ўзгармас ҳисобланади. Шифрлаш алгоритми учун бошланғич қийматлар бўлиб шифрлаш учун ахборот ва шифрлаш калити хизмат килади. Калит бошқарувчи ахборотни ўз ичига олади, у шифрлаш алгоритмини амалга оширишда ишлатиладиган операндлар катталикларини ва алгоритмнинг маълум қадамларида ўзгартришларни ташлашни аниқлайди.

Стенография усуллари нафаҳатгина сақланаётган ёки узатилаётган ахборотни маъносини беркитиб қолмасдан, балки ёпиқ ахборотни сақлаш ёки узатиш омилини хам яшириш имконини хам беради. Стенография усулларининг барчаси асосида ёпиқ ахборотни очиқ файллар ичida ниқоблаш ётади. Стенография воситалари ёрдамида матн, тасвир, нутқ, рақамли имзо, шифрланган хабар ниқбланиши мумкин. Стенографияни ва шифрлашни комплекс ишлатиш маҳфий ахборотни пайқаш ва очиш масаласини ечишнинг мураккаблигини оширади.

Ахборотни **кодлаш** жараёнининг мазмунини бошланғич ахборот (гаплар, сўзлар) маъносига кўра тузилишларини кодлар билан алмаштириш ҳисобланади. Кодлар сифатида ҳарфлар, рақамлар, рақамлар ва ҳарфларнинг бирлашмалари ишлатилиши мумкин. Кодлашда ва тескари ўзгартришда маҳсус жадвал ёки луғатлар ишлатилади. Камчилиги кодлайдиган жадвалларни сақлаш ва тарқатишнинг зарурлигидир, уларни, ушлаб олинган хабарларни қайта ишлашнинг статистик усуллари билан кодларни очишдан сақланиш учун, тез-тез алмаштириш керакдир. Кодлаш усулини маъносига кўра тузилишлари чекланган тўпламли тизимларда кўллаш мақсадга мувофиқдир.

Зичлаштириш ахборот хажмини қисқартиришдир. Зичлаштирилган ахборот тескари ўзгартришсиз ўқилиши ёки ишлатилиши мумкин эмас. Зичлаштириш ва қайта ўзгартриш воситаларига мурожаат қила олишликни инобатга олиб, маҳфий ахборотни зичлаштирилган файллари кейинчалик шифрланади. Вақтни қисқартириш учун ахборотни зичлаштириш учун ахборотни зичлаштириш ва шифрлаш жараёнини биргаликда ишлатиш мақсадга мувофиқдир.

Шифр ва калит, шифрлаш ва қайта шифрлаш тўғрисида тушунчалар

Шифрлаш криптографик ўзгартришнинг асосий кўринишидир. Бу очиқ ахборотни шифрланган ахборотга (шифрматн) ўзгартриш ёки

шифрланган ахборотни очик ахборотга тескари ўзгартириш жараёнларидир.

Очиқ ахборотни ёпиқ ахборотга ўзгартириш жараёни шифрлаш, тескариси эса - қайта шифрлаш дейилади.

Шифрлаш усулларининг ва шифрларнинг кўплаб турлари мавжуд. Бу шифрлаш алгоритмига мос равишда очик ахборотни ёпиқ ахборотга орқага қайтмайдиган ўзгартиришлар тўпламидир. Замонавий шифрлаш усулларига қуйидаги талаблар кўйилади:

- Крипточидамлилик (криптотахлил қилишга қарши туриш) шундай бўлиши керакки, шифрни очиш калитларини тўлик танлаб олиш масаласини ечиш йўли билан амалга оширилиши керак;
- Крипточидамлилик шифрлаш алгоритмининг маҳфийлиги билан эмас, балки калитнинг маҳфийлиги билан таъминланади;
- Шифрматн ўзи ҳажми бўйича бошланғич ахборотдан кўпайиб кетмаслиги керак;
- Шифрлаш вақти катта бўлмаслиги керак;
- Нархи беркитиладиган ахборотнинг нархи билан мослаштирилиши керак.

Шифрлашнинг симметрик криптотизимида шифрлаш ва расшифровка қилиш учун битта калитнинг ўзи ишлатилади. Демак, шифрлаш калитидан фойдаланиш хуқуқига эга бўлган ҳар қандай одам ахборотни расшифровка қилиши мумкин. Шу сабабли, симметрик криптотизимлар маҳфий калитли криптотизимлар деб юритилади.

Шифрлаш усуллари турли аломатлари бўйича туркумланиши мумкин. Туркумланиш варианларидан бири 4 –расмда келтирилган.



4 - расм. Шифрлаш усулларининг туркумланиши.

Алмаштириш усуллари. Алмаштириш (подстановка) усулларининг моҳияти бир алфавитда ёзилган ахборот символларини бошқа алфавит

символлари билан маълум қоида бўйича алмаштиришдан иборатdir. Энг содда усул сифатида *тўғридан тўғри алмаштириши* кўрсатиш мумкин. Дастребаки ахборот ёзилувчи A_0 алфавитнинг s_{0i} символларига шифрловчи A_1 алфавитнинг s_{1i} символлари мос қўйилади. Оддий ҳолда иккала алфавит ҳам бир хил символлар тўпламига эга бўлиши мумкин.

Иккала алфавитдаги символлар ўртасидаги мослик маълум алгоритм бўйича К символлар узунлигига эга бўлган дастребаки матн T_0 символларининг рақамли эквивалентларини ўзгартириш орқали амалга оширилади. Иккала алфавит белгилари ўртасидаги мувофиқликни берилиши маълум бир алгоритм бўйича узунлиги K та белгилардан ташкил топган T_0 матн белгиларининг сонли тенг кучлиларини ўзгартириш ёрдамида амалга оширилади.

Моноалфавитли ўзгартириш алгоритми қадамлар кетма-кетлиги кўринишида берилиши мумкин. (масалан, Вижинер матрицаси)

Ўрин алмаштириши усуллари. Ўрин алмаштириш усулларига биноан дастребаки матн белгиланган узунликдаги блокларга ажратилиб ҳар бир блок ичидаги символлар ўрни маълум алгоритм бўйича алмаштирилади.

Энг осон ўрин алмаштиришга мисол тариқасида дастребаки ахборот блокини матрицага қатор бўйича ёзишни, ўқишини эса устун бўйича амалга оширишни кўрсатиш мумкин. Матрица қаторларини тўлдириш ва шифрланган ахборотни устун бўйича ўқиш кетма-кетлиги калит ёрдамида берилиши мумкин. Усулнинг криптобардошлиги блок узунлигига (матрица ўлчамига) боғлиқ. Масалан узунлиги 64 символга тенг бўлган блок (матрица ўлчами 8x8) учун калитнинг $1,6 \cdot 10^9$ комбинацияси бўлиши мумкин. Узунлиги 256 символга тенг бўлган блок (матрица ўлчами 16x16) калитнинг мумкин бўлган комбинацияси $1,4 \cdot 10^{26}$ га етиши мумкин. Бу ҳолда калитни саралаш масаласи замонавий ЭҲМлар учун ҳам мураккаб ҳисобланади. Гамильтон маршруtlарига асосланган усулда ҳам ўрин алмаштиришлардан фойдаланилади.

1-қадам. Бошланғич ахборот блокларга бўлиб чиқилади. Агар шифрланадиган ахборотнинг узунлиги блок узунлигига каррали бўлмаса, унда охирги блокнинг бўш жойларига маҳсус хизмат белги-тўлдирувчилар (масалан,*) жойлаштирилади.

2-қадам. Блок белгилари билан жадвал тўлдирилади, унда белгининг ҳар бир тартиб номери учун блок жуда аниқ жой ажратиласди.

3-қадам. Белгиларни жадвалдан ўқиш маршрутларнинг биттаси бўйича амалга оширилади. Маршрутлар ёки кетма-кет танланади ёки уларнинг навбати K калит билан берилади.

4-қадам. Белгиларнинг шифрланган кетма-кетлиги маълум бир L узунликдаги блокларга бўлиб чиқилади. L катталик бошланғич ахборот 1-қадамда бўлиб чиқиладиган блокларнинг узунлигидан фарқ қилиши мумкин.

Қайта шифрлаш тескари тартибда амалга оширилади. Калитга мос равишда маршрут танланади ва бу маршрутга кўра жадвал тўлдирилади.

Қайта жойлаштиришлар усули оддийгина амалга оширилади, лекин иккита жиддий камчиликка эгадир. Биринчидан, улар шифр-матнни

статистик қайта ишлаш ёрдами билан очилишига йўл қўяди. Иккинчидан, агар бошлангич матн К та белги узунликдаги блокларга бўлиб чиқилса, унда криптотахлил қилувчига шифрни очиш учун шифрлаш тизимиға тестли ахборотнинг К-1 блокини юбориш етарлидир, бу блокда биттадан ташқари барча белгилар бир хилдир.

Шифрлашнинг аналитик усуллари. Матрица алгебрасига асосланган шифрлаш усуллари энг кўп тарқалган. Дастребки ахборотнинг $B_k = \{b_j\}$ вектор кўринишида берилган k - блокини шифрлаш $A = \{a_{ij}\}$ матрица калитни B_k векторга кўпайтириш орқали амалга оширилади. Натижада $C_k = \{c_i\}$ вектор кўринишидаги шифрматн блоки ҳосил қилинади. Бу векторнинг элементлари $c_i = \sum_j a_{ij} b_j$ ифодаси орқали аниқланади.

Ахборотни расшифровка қилиш C_k векторларини A матрицага тескари бўлган A^{-1} матрицага кетма-кет кўпайтириш орқали аниқланади.

Шифрлашнинг аддитив усуллари. Шифрлашнинг **аддитив усуллари** биноан дастребки ахборот символларига мос келувчи рақам кодларини кетма-кетлиги **гамма** деб аталувчи қандайдир символлар кетма-кетлигига мос келувчи кодлар кетма-кетлиги билан кетма-кет жамланади. Шу сабабли, шифрлашинг аддитив усуллари **гаммалаш** деб ҳам аталади.

Ушбу усуллар учун калит сифатида гамма ишлатилади. Аддитив усулнинг криптобардошлиги калит узунлигига ва унинг статистик характеристкаларининг текислигига боғлиқ. Агар калит шифрланувчи символлар кетма-кетлигидан қисқа бўлса, шифрматн криptoаналитик томонидан статистик усуллар ёрдамида расшифровка қилиниши мумкин. Калит ва дастребки ахборот узунлеклари қанчалик фарқланса, шифр-матнга муваффақиятли хужум эҳтимоллиги шунчалик ортади. Агар калит узунлиги шифрланувчи ахборот узунлигидан катта бўлган тасодифий сонларнинг даврий бўлмаган кетма-кетлигидан иборат бўлса, калитни билмасдан туриб шифрматнни расшифровка қилиш амалий жиҳатдан мумкин эмас. Алмаштириш усулларидагидек гаммалашда калит сифатида рақамларнинг такрорланмайдиган кетма-кетлиги ишлатилиши мумкин.

Амалиётда асосини псевдотасодифий сонлар генераторлари (датчиклари) ташкил этган аддитив усуллар энг кўп тарқалган ва самарали ҳисобланади. Генератор псевдотасодифий сонларнинг чексиз кетма-кетлигини шакллантиришда нисбатан қисқа узунликдаги дастребки ахборотдан фойдаланади.

Шифрлашнинг комбинацияланган усуллари. Қудратли компьютерлар, тармоқ технологиялари ва нейронли ҳисоблашларнинг пайдо бўлиши ҳозиргача умуман фош қилинмайди деб ҳисобланган криптографик тизимларни обрўсизлантиришига сабаб бўлди. Бу эса ўз навбатида юқори бардошликка эга криптографик тизимларни яратиш устида ишлашни тақозо этди. Бундай криптографик тизимларни яратиш усулларидан бири шифрлаш усулларини комбинациялашдир. Қўйида энг кам вақт сарфида криптобардошлини жиддий ошишини таъминловчи шифрлашнинг комбинацияланган усули устида сўз боради. Шифрлашнинг ушбу

комбинацияланган усулига биноан маълумотларни шифрлаш икки босқичда амалга оширилади. Биринчи босқичда маълумотлар стандарт усул (масалан, DES усул) ёрдамида шифрланса, иккинчи босқичда шифрланган маълумотлар махсус усул бўйича қайта шифрланади. Махсус усул сифатида маълумотлар векторини элементлари нолдан фарқли бўлган сон матрицасига кўпайтиришдан фойдаланиш мумкин.

Гаммалашни қўллашда агар шифр гаммаси сифатида рақамларнинг такрорланмайдиган кетма-кетлиги ишлатилса шифрланган матнни фош қилиш жуда қийин. Одатда шифр гаммаси ҳар бир шифрланувчи сўз учун тасодифий ўзгариши лозим. Агар шифр гаммаси шифрланган сўз узунлигидан катта бўлса ва дастлабки матннинг ҳеч қандай қисми маълум бўлмаса, шифрни фақат тўғридан-тўғри саралаш орқали фош этиш мумкин. Бунда криптобардошлиқ калит ўлчами орқали аниқланади. Шифрлашнинг бу усулидан кўпинча ҳимоя тизимининг дастурий амалга оширилишида фойдаланилади ва шифрлашнинг бу усулига асосланган тизимларда бир секундда маълумотларнинг бир неча юз Кбайтини шифрлаш имконияти мавжуд. Расшифровка қилиш жараёни-калит маълум бўлганида шифр гаммасини қайта генерациялаш ва уни шифрланган маълумотларга сингдиришдан иборат.

Асимметрик шифрлаш тизимларида иккита калит ишлатилади. Ахборот очиқ калит ёрдамида шифрланса, маҳфий калит ёрдамида расшифровка қилинади. Асимметрик шифрлаш тизимларини очиқ калитли шифрлаш тизимлар деб ҳам юритилади.

Шифрлашнинг аналитик усувлари матрицали алгебрани ишлатишга асосланган.

Шифрлашнинг аддитив усувлари (гаммалаш) кодлари бошланғич ахборотнинг рақамли кодлари билан қўшиладиган рақамли кортежнинг тасодифий кетма-кетлтгини ишлатади. Гамма калит хисобланади. Калит қанчалик узун бўлса, криптоидамлилик шунчалик юқори бўлади.

Очиқ калитли шифрлаш тизимларида шифрлаш учун очиқ калит ва қайта шифрлаш учун маҳфий калит ишлатилади.

Замонавий криптотизимлардан қўйидагиларни таъкидлаш мумкин:

а) симметрик – Цезарь тизими, Трисемус жадвали, Плейфер – нинг биграммли шифри, Хилл криптотизими, Вижинер шифрлаш тизими ва бошқалар;

б) носимметрик – RSA криптотизими (Райвест Р., Шамир А ва Адлеман А – Rivest, Shamir ва Adleman), Полига – Хелман, Эль Гамаил шифрлаш тизимлари ва бошқалар.

Замонавий шифрлаш стандартларидан ахборотни шифрлашга Россия стандартини ГОСТ 28147-89, АҚШнинг DES (Data Encryption Standard) стандартини келтириш мумкин.

КТ ва Т ларида криптохимоя қилишни ишлатиш истиқболларига тўхталарадиган бўлсак, қўйидагилага эътиборни қаратиш керак:

- калит узунлиги замонавий тизимлар учун >90 бит бўлиши керак;

- жуда маъсулиятли қўлланишлар учун нафақатгина калит, балки шифрлаш алгоритми хам махфий хисобланади;
- стенография криптохимоя қилишнинг истиқболли йўналиши хисобланади.

Хулоса қилиб шуни айтиш мумкинки, замонавий симметрик ва носимметрик криптотизимларни, замонавий шифрлаш стандартларини хамда стенография ва шифрлашни комплекс ишлатиш ёпиқ ахборотнинг криптоидамлилигини бирмунча оширади

Ушбу "Маълумотларни шифрлаш алгоритми" стандарти Ўзбекистон алоқа ва ахборотлаштириш агентлигининг илмий-техник ва маркетинг тадқиқотлари маркази томонидан ишлаб чиқилган ва унда Ўзбекистон Республикасининг "Электрон рақамли имзо хусусида"ги ва "Электрон хужжат алмашинуви хусусида"ги қонунларининг меъёрлари амалга оширилган.

Ушбу стандарт – криптографик алгоритм, электрон маълумотларни ҳимоялашга мўлжалланган. Маълумотларни шифрлаш алгоритми симметрик блокли шифр бўлиб, ахборотни шифрлаш ва расшифровка қилиш учун ишлатилади. Алгоритм 128 ёки 256 бит узунлигидаги маълумотларни шифрлашда ва расшифровка қилишда 128, 256, 512 битли калитлардан фойдаланиши мумкин.

Стандарт ШЭҲМ тармоқларида, телекоммуникацияда, алоҳида ҳисоблаш комплекслари ва ШЭҲМда ахборотни ишлаш тизимлари учун ахборотни шифрлашнинг умумий алгоритмини ва маълумотларни шифрлаш қоидасини белгилайди.

Шифрлаш алгоритми дастурий ва аппарат усулларда амалга оширилиши мумкин.

Симметрик шифрлашнинг барча тизимлари қўйидаги камчиликларга эга:

- ахборот алмашувчи икала субъект учун махфий калитни узатиш каналининг ишончлилиги ва хавфсизлигига қўйиладиган талабларнинг қатъийлиги;

- калитларни яратиш ва тақсимлаш хизматига қўйиладиган талабларнинг юқорилиги. Сабаби, ўзаро алоқанинг «ҳар ким – хар ким билан» схемасида «и» та абонент учун $n(n-1)/2$ та калит талаб этилади, яъни калитлар сонининг абонентлар сонига боғлиқлиги квадратли. Масалан, $n=1000$ абонент учун талаб қилинадиган калитлар сони $n(n-1)/2=499500$. Шу сабабли, фойдаланувчилари юз миллиондан ошиб кетган «Internet» тармоғида симметрик шифрлаш тизимини қўшимча усул ва воситаларсиз қўллашнинг иложи йўқ.

Асимметрик шифрлашнинг биринчи ва кенг тарқалган криptoалгоритми RSA 1993 йилда стандарт сифатида қабул қилинди. Ушбу криptoалгоритм ҳар тарафлама тасдиқланган ва калитнинг етарли узунлигига бардошлиги эътироф этилган. Ҳозирда 512 битли калит бардошликни таъминлашда етарли ҳисобланмайди ва 1024 битли калитдан фойдаланилади. Баъзи муаллифларнинг фикрича процессор қувватининг ошиши RSA

криптоалгоритмининг тўлиқ саралаш хужумларга бардошлигининг йўқолишига олиб келади. Аммо, процессор қувватининг ошиши янада узун калитлардан фойдаланишга, ва демак, RSA бардошлигини ошишига имкон яратади.

Асимметрик криптоалгоритмларда симметрик криптоалгоритмлардаги камчиликлар бартарф этилган:

- калитларни маҳфий тарзда етказиш зарурияти йўқ; асимметрик шифрлаш очик калитларни динамик тарзда етказишга имкон беради, симметрик шифрлашда эса ҳимояланган алоқа сеанси бошланишидан аввал маҳфий калитлар алмашиниши зарур эди;
- калитлар сонининг фойдаланувчилар сонига квадратли боғланишлиги йўқолади; RSA асимметрик криптотизимда калитлар сонининг фойдаланувчилар сонига боғлиқлиги чизиқли кўринишга эга (N фойдаланувчиси бўлган тизимда $2N$ калит ишлатилади).

Аммо асимметрик криптотизимлар, хусусан RSA криптотизими, камчиликлардан ҳоли эмас:

- ҳозиргача асимметрик алгоритмларда ишлатилувчи функцияларнинг қайтариласлигининг математик исботи йўқ;
- асимметрик шифрлаш симметрик шифрлашга нисбатан секин амалга оширилади, чунки шифрлашда ва расшифровка қилишда катта ресурс талаб этиладиган амаллар ишлатилади (хусусан, RSAда катта сонни катта сонли даражага ошириш талаб этилади). Шу сабабли асимметрик алгоритмларни аппарат амалга оширилиши, симметрик алгоритмлардагига нисбатан анчагина мураккаб;
- очик калитларни алмаштириб қўйилишидан ҳимоялаш зарур. Фараз қилайлик " A " абонентнинг компьютерида " B " абонентнинг очик калити " K_B " сақланади. " n " нияти бузук одам " A " абонентда сақланаётган очик калитлардан фойдалана олади. У ўзининг жуфт (очик ва маҳфий) " K_n " ва " k_n " калитларини яратади ва " A " абонентда сақланаётган " B " абонентнинг " K_B " калитини ўзининг очик " K_n " калити билан алмаштиради. " A " абонент қандайдир ахборотни " B " абонентга жўнатиш учун уни " K_n " калитда (бу " K_B " калит деб ўйлаган ҳолда) шифрлайди. Натижада, бу хабарни " B " абонент ўқий олмайди, " n " абонент осонгина расшифровка қиласи ва ўқиёдиди. Очик калитларни алмаштиришни олдини олишда калитларни сертификациялашдан фойдаланилади.

Россия Федерациясида қабул қилинган ахборотларни криптографик ҳимоялашга оид стандартлари

Россиянинг ахборотни шифрлаш стандарти. Россия Федерациясида Ҳисоблаш машиналари, комплекслари ва тармоқларида ахборотни криптографик ўзгартириш алгоритмларига давлат стандарти (ГОСТ 2814-89) жорий этилган. Бу алгоритмлар маҳфийлик даражаси ихтиёрий бўлган

ахборотни ҳеч қандай чекловсиз шифрлаш имконини беради. Алгоритмлар аппарат ва программ усууларида амалга оширилиши мумкин.

Стандартда ахборотни криптографик ўзгартиришнинг қуидаги алгоритмлари мавжуд:

- оддий алмаштириш;
- гаммалаш;
- тескари боғланишли гаммалаш;
- имитовставка.

Бу алгоритмлар учун 8 та 32 хонали иккили сўзларга ажратилган 256 бит ўлчамли калитнинг ишлатилиши ҳамда дастлабки шифрланувчи иккили кетма-кетликнинг 64 битли блокларга ажратилиши умумий ҳисобланади.

Оддий аламштириш алгоритмининг моҳияти қуидагича. Дастлабки кетма-кетликнинг 64 битли блоки иккита 32 хонали А ва В иккили сўзларга ажратилади. А сўзлар блокнинг кичик хоналарини В сўзлар эса катта хоналарини ташкил этади. Бу сўзларга сони $i=32$ бўлган циклик итерация оператори F_i қўлланилади. Блокнинг кичик битларидаги сўз (биринчи итерациядаги А сўзи) калитнинг 32 хонали сўзи билан mod 232 бўйича жамланади; ҳар бири 4 битдан иборат қисмларга (4 хонали кириш йўли векторлари) ажратилади; маҳсус алмаштириш узеллари ёрдамида ҳар бир вектор бошқаси билан алмаштирилади; олинган векторлар 32 хонали сўзга бирлаштирилиб, чап тарафга циклик равишда силжитилади ва 64 хонали блокдаги бошқа 32 хонали сўз (биринчи итерациядаги В сўзи) билан mod 2 бўйича жамланади.

Биринчи итерация тугаганидан сўнг кичик битлар ўрнида В сўз жойланади, чап тарафда эса А сўз жойланади. Кейинги итерацияларда сўзлар устидаги амаллар такрорланади.

Ҳар бир i -итерацияда K_j калитнинг (калитлар 8 та) 32 хонали сўзи қуидаги қоидага биноан танланади

$$K_j = \begin{cases} (i-1) \bmod 8, & 1 \leq i \leq 24 \text{ бўлганда,} \\ 32-i, & i \geq 25 \text{ бўлганда,} \\ 0, & i=32 \text{ бўлганда.} \end{cases}$$
$$K_i = \begin{cases} (i-1) \bmod 8, & 1 \leq i \leq 24 \text{ бўлганда,} \\ 32-i, & i \geq 25 \text{ бўлганда,} \\ 0, & i=32 \text{ бўлганда,} \end{cases}$$

Демак, шифрлашда калитнинг танланиш тартиби қуидаги кўринишда бўлади:

K0,K1, K2, K3, K4, K5, K6, K7, K0, K1, K2, K3, K4, K5, K6, K7,
K0,K1, K2, K3, K4, K5, K6, K7, K7, K6, K5, K4, K3, K2, K1, K0,.

Расшифровка қилишда калитлар тескари тартибда ишлатилади.

Алмаштириш блоки кетма-кет танланувчи 8 та алмаштириш узелларидан иборат. Алмаштириш узели ҳар бирида алмаштириш вектори (4 бит) жойлашган 16 қаторли жадвалдан иборат. Кириш йўли вектори

жадвалдаги қатор адресини аниқласа, қатордаги сон алмаштиришнинг чиқиш йўли вектори ҳисобланади. Алмаштириш жадвалига ахборот олдиндан ёзилади ва камдан-кам ўзгартирилади.

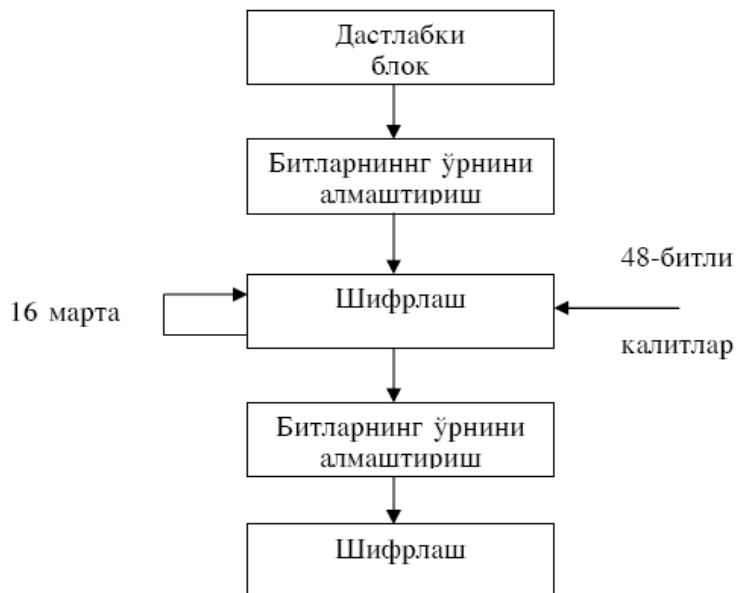
АҚШда қабул қилинган ахборотларни криптографик химоялашга оид стандартлари

АҚШда давлат стандарти сифатида DES(Data Encryption Standard) стандарти ишлатилган. Бу стандарт асосини ташкил этувчи шифрлаш алгоритми IBM фирмаси томонидан ишлаб чиқилган бўлиб, АҚШ Миллий Хавфсизлик Агентлигининг мутахасислари томонидан текширилган сўнг давлат стандарти моқомини олган. DES стандартидан нафақат федерал департаментлар, балки нодавлат ташкилотлар, нафақат АҚШда, балки бутун дунёда фойдаланилган.

DES стандартида дастлабки ахборот 64 битли блокларга ажратилади ва 56 ёки 64 битли калит ёрдамида криптографик ўзгартирилади.

Дастлабки ахборот блоклари ўрин алмаштириш ва шифрлаш функциялари ёрдамида итерацион ишланади. Шифрлаш функциясини ҳисоблаш учун 64 битли калитдан 48 битлигини олиш, 32-битли кодни 48 битли кодга кенгайтириш, 6-битли кодни 4-битли кодга ўзгартириш ва 32-битли кетма-кетликнинг ўрнини алмаштириш кўзда тутилган.

Расшифровка жараёни шифрлаш жараёнига инверс бўлиб, шифрлашда ишлатиладиган калит ёрдамида амалга оширилади.



5- расм. DES алгоритмида шифрлаш жараёнининг блок-схемаси

Хозирда бу стандарт қуйидаги иккита сабабга кўра фойдаланишга бутунлай яроқсиз ҳисобланади:

- калитнинг узунлиги 56 битни ташкил этади, бу ШЭҲМларнинг замонавий ривожи учун жуда кам;
- алгоритм яратилаётганида унинг аппарат усулда амалга оширилиши кўзда тутилган эди, яън алгоритмда микропроцессорларда бажарилишида қўп вақт талаб қилувчи амаллар бор эди (масалан, машина сўзида маълум схема бўйича битларнинг ўрнини алмаштириш каби).

Бу сабаблар АҚШ стандартлаш институтининг 1997 йилда симметрик алгоритмнинг янги стандартига танлов эълон қилишига олиб келди. Танлов шартларига биноан алгоритмга қуйидаги талаблар қўйилган эди:

- алгоритм симметрик бўлиши керак;
- алгоритм блокли шифр бўлиши керак;
- блок узунлиги 128 бит бўлиб, 128, 192, ва 256 битли калит узунликларини таъминлаши лозим.

Ундан ташқари танловда иштирок этувчилар учун қуйидаги тавсиялар берилган эди:

- ҳам аппарат усулда ҳам дастур усулда осонгина амалга оширилувчи амаллардан фойдаланиш;
- 32 хонали процессорлардан фойдаланиш;
- иложи борича шифр структурасини мураккаблаштирмаслик. Бу ўз навбатида барча қизикувчиларнинг алгоритмни мустақил тарзда криптотахлил қилиб, унда қандайдир хужжатсиз имкониятлар йўқлигига ишонч ҳосил қилишлари учун зарур ҳисобланади.

2000 йил 2 октябрда танлов натижаси эълон қилинди. Танлов ғолиби деб Бельгия алгоритми RIJNDAEL топилди ва шу ондан бошлаб алгоритм-ғолибдан барча патент чегараланишлари олиб ташланди.

Ушбу алгоритм ноанъанавий блокли шифр бўлиб, кодланувчи маълуотларнинг ҳар бир блоки қабул қилинган блок узунлигига қараб 4×4 , 4×6 ёки 4×8 ўлчамдаги байтларнинг икки ўлчамли массивлари кўринишига эга.

Шифрдаги барча ўзгартиришлар қатъий математик асосга эга. Амалларнинг структураси ва кетма-кетлиги алгоритмнинг ҳам 8-битли ҳам 32-битли микропроцессорларда самарали бажарилишига имкон беради. Алгоритм структурасида баъзи амалларнинг параллель ишланиши ишчи станцияларида шифрлаш тезлигининг 4 марта ошишига олиб келади.

Полиалфавитлиалмаштиришметодлари тарличаюқорикриптотурғунликкаэга.

Буметодларда слабкиматнисимволларини алмаштиришучун бир неча алфавитда нфойдаланишга асосланган.

Расман полиалфавитли алмаштиришни

қуйидагичатасаввурэтишмумкин.

N-

алфавитли алмаштиришда слабки А₀ алфавитдагиз₀₁ символи А₁

алфавитдагиз₁₁

символи билан алмаштириладиваҳ.

$S_{0N}HIS_{NN}$ символ билан алмаштирилгани дансүнг $S_{0(N+1)}$ символнинг ўрнини A1 алфавитдаги $S_1(N+1)$ символ олади ва x.

Полиалфавитли алмаштириш алгоритмлари ичида Вижинер жадвали (матрицаси) ТВ ни ишлатувчи алгоритм энг кенг тарқалган. Вижинер жадвали $[RxR]$ ўлчамли квадрат матрицадан иборат бўлиб, (R -ишлатилаётган алфавитдаги символлар сони) биринчи қаторида символлар алфавит тартибида жойлаштирилади. Иккинчи қатордан бошлаб символлар чапга битта ўринга силжитилган ҳолда ёзилади. Сиқиб чиқарилган символлар ўнг тарафдаги бўшаган ўринни тўлдиради (циклик силжитиш). Агар ўзбек алфавити ишлатилса, Вижинер матрицаси $[36x36]$ ўлчамга эга бўлади (22.11 - расм).

АБВГД.....ЎКFX_
БВГДЕ.....КFX_A
ВГДЕЖ.....FX_AB
.....
_АБВГ.....ЯЎКFX

6-расм. Вижинер матрицаси.

Шифрлаш такрорланмайдиган M символдан иборат калит ёрдамида амалга оширилади. Вижинернинг тўлиқ матрицасидан $[(M+1),R]$ ўлчамли шифрлаш матрицаси T(Ш) ажратилади. Бу матрица биринчи қатордан ва биринчи элементлари калит символларига мос келувчи қаторлардан иборат бўлади.

Вижинер жадвали ёрдамида шифрлаш алгоритми қўйидаги қадамлар кетма-кетлигидан иборат.

1-қадам. Узунлиги M символли калит K ни танлаш.

2-қадам. Танланган калит K учун $[(M+1),R]$ ўлчамли шифрлаш матрицаси $T_{ij} = (bij)$ ни қуриш.

3- қадам. Дастрлабки матннинг ҳар бир символи s_{0r} тагига калит символи km жойлаштирилади. Калит кераклича такрорланади.

4-қадам. Дастрлабки матн символлари шифрлаш матрицаси T_{ij} дан қўйидаги қоида бўйича танланган символлар билан кетма-кет алмаштирилади.

- 1) K калитнинг алмаштирилувчи s_{0r} символга мос km символи аниқланади;
- 2) шифрлаш матрицаси T_{ij} даги $km = bij$ шарт бажарилувчи i қатор топилади.
- 3) $s_{0r} = bij$ шарт бажарилувчи j устун аниқланади....
- 4) s_{0r} символи bij символи билан алмаштирилади.

5-қадам. Шифрланган кетма-кетлик маълум узунликдаги (масалан 4 символли) блокларга ажратилади. Охирги блокнинг бўш жойлари маҳсус символ-тўлдирувчилар билан тўлдирилади.

Расшифровка қилиш қўйидаги кетма-кетликда амалга оширилади.

1-қадам. Шифрлаш алгоритмининг 3-қадамидагидек шифрматн тагига калит символлари кетма-кетлиги ёзилади.

2-қадам. Шифрматндан s_{1r} символлари ва мос калит символлари кт кетма-кет танланади. Тш матрицада $km = bij$ шартни қаноатлантирувчи і қатор аниқланади. і-қаторда $bij = s_{1r}$ элемент аниқланади. Расшифровка қилинган матнда r - ўрнига bij символи жойлаштирилади.

3-қадам. Расшифровка қилинган матн ажратилмасдан ёзилади. Хизматчи символлар олиб ташланади.

Полиалфавитлиалмаштиришметодларинингкриптотурғунлигиоддийалм аштиришметодларига қарагандаайтарличаюқори, чункиулардадастлабқикетма-кетликнингбирхисимволларитурлисимволларбиланаалмаштирилишимумкин. Аммошифрнингстатистикметодларгабардошлигикалитузнлигигабоғлиқ.

Электрон рақамли имзо ва унинг замонавий турлари

Телекоммуникация тизимларнинг ривожланиши натижасида хозирги кунда ахборот алмашувини қоғозли технологиясидан электрон хужжат кўринишдаги ахборот алмашинувига ўтиш жараёни юз бермоқда. Ахборот алмашинувини электрон хужжат кўринишидаги технологиясига ўтиш натижасида телекоммуникация тармоқлари орқали узатиладиган ахборотларни муаллифини аниқлаш, унинг тўлиқлилиги таъминлаш каби муаммолар вужудга келади. Ушбу муаммони тўла-тўқис «Электрон рақамли имзо» ёрдамида хал қилиш мумкин. "Электрон рақамли имзо" бу телекоммуникация тармоқлари орқали узатишга мўлжалланган электрон хужжатни ўзини маълум бир алгоритмлар ёрдамида зичлаштириб сўнг шифрланган дискрет кўринишдаги ифодаси хисобланади.

Ахборотни алмашинувини электрон хужжат алмашинувинида электрон рақамли имзодан фойдаланиш натижасида қуидагиларга эришиш мумкин:

- қабул қилинган электрон хужжат кўринишидаги ахборотни тўлиқлигини таъминлаш;
- қабул қилинган электрон хужжат кўринишидаги ахборотни муаллифини аниқлаш;
- қабул қилинган электрон хужжат кўринишидаги ахборотнинг электрон имзони юридик жахатдан қоғоздаги шахсий имзо билан teng кучга эга бўлишини таъминлаш.

Республикамида "Электрон рақамли имзо" тўғрисидаги Қонун Олий Мажлиснинг иккинчи чақириқўн учинчи сессиясида қабул қилинди.

"Электрон рақамли имзо" тўғрисидаги Қонуннинг мақсади энг аввало, маълум шартларга риоя қилинган холда электрон рақамли имзони қоғоздаги шахсий имзо билан teng кучга эгалигини, яъни teng тан олинишини таъминлайди. Шунингдек, "электрон рақамли имзо"ни ишлатилиши

қимматли қоғозлар ва валюта операцияларини амалга оширишда, интернет савдода тартиб қойдани бир йўналишга солиб туришда ахамиятга эга.

Хозирги кунда "электрон рақамли имзо"ни жорий қилиш жараёнида Германия етакчи хисобланади. Рақамли имзо тўғрисидаги қонуннинг охирги варианти Бундестаг томонидан 1997 йил 13 июнда маъқулланган. 2000 йилда АҚШ хукумати томонидан "Электрон рақамли имзо" тўғрисидаги федерал қонун қабул қилинди. Унга кўра шартномалар ва хужжатлардаги "электрон рақамли имзо" қўл билан қўйилган имзодек юридик кучга эга. 2001 Европа комиссияси томонидан хам "Электрон рақамли имзо" ни юридик тан оловчи директивани қабул қилди ва Европа Иттифоқига аъзо 15 давлатда бир вактда ўзларининг ички қонун хужжатларини у билан мослаштирилди.

"Электрон рақамли имзо"ни хосил қилиш учун турли давлатларда турли хил шифрлаш алгоритмлари ишлатилади масалан, RSA, Эль Гамал каби шифрлаш алгоритмлари. Бу алгоритмларда мустахкамлик даражаси турли хил.

ЭРИ хабар яхлитлигини хабар яхлитлигини ва хабар муаллифининг хақиқийлигини текшириш муаммосини самарали хал этишга имкон беради.

ЭРИ телекоммунтикация каналлари орқали узатилувчи матнларни аутентификациялаш учун ишлатилади. Рақамли имзо ишлаши бўйича оддий қўлёзма имзога ўхшаш бўлиб, қўйидаги афзалликларга эга:

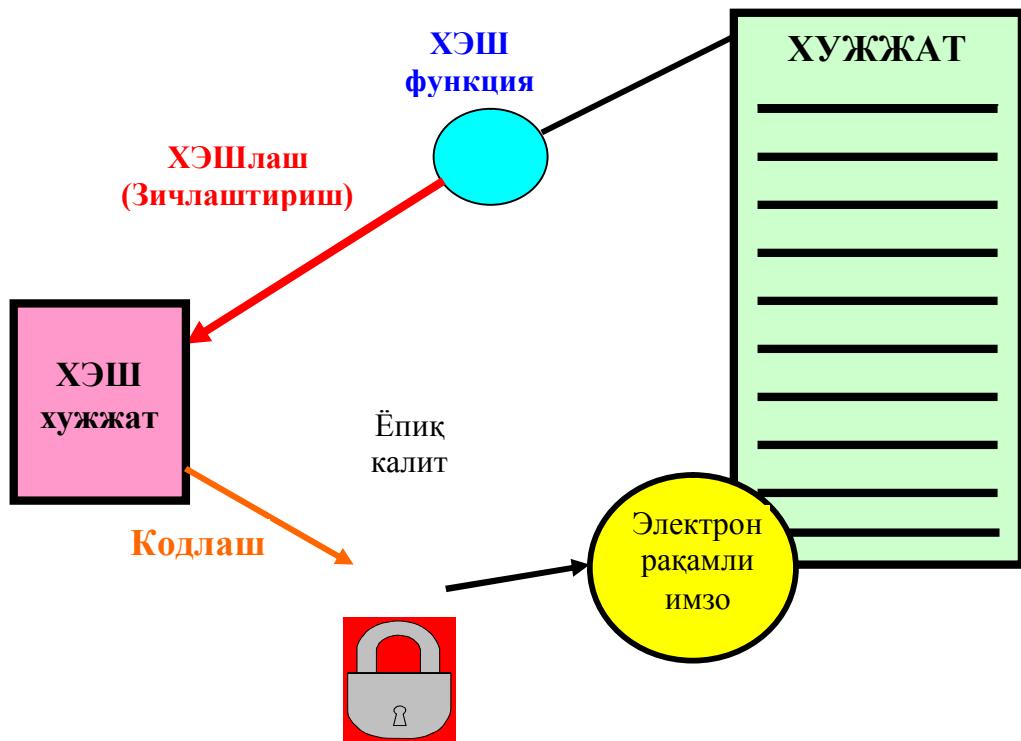
- имзо чекилган матн имзо қўйган шахсга тегишли эканлигини тасдиқлади;
- бу шахсга имзо чекилган матнга боғлиқ мажбуриятларидан тониш имкониятини бермайди;
- имзо чекилган матн яхлитлигини кафолатлади.

ЭРИ асимметрик шифрларнинг қайтарувчанлигига хамда хабар таркиби, имзонинг ўзи ва калитлар жуфтининг ўзаро боғлиқлигига асосланади (7-расм). Бу элементларнинг хатто бирининг ўзгариши Эърақамли имзонинг хақиқийлигини тасдиқлашга имкон бермайди. ЭРИ шифрлашнинг асимметрик алгоритмлари ва хэш функциялари ёрдамида амалга оширилади.

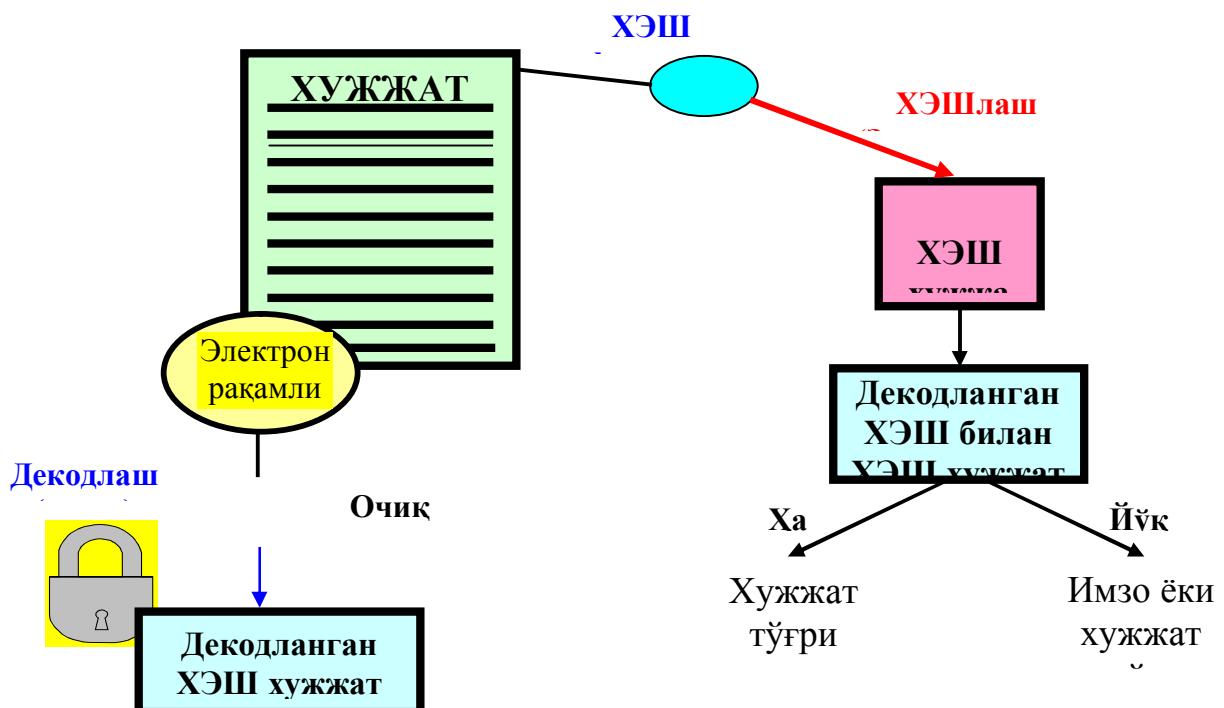
. ЭРИ тизими иккита асосий муолажани амалга оширади (8-расм):

- рақамли имзони шакллантириш муолажаси;
- рақамли имзони текшириш муолажаси.

Имзони шакллантириш муолажасида хабар жўнатувчисининг махфий калити ишлатилса, имзони текшириш муолажасида жўнатувчининг очик калитидан фойдаланилади



7-расм. Асимметрик шифрлаш асосида электрон ракамли имзо ишлаб чиқиши схемаси



8-расм. Асимметрик шифрлаш асосида электрон ракамли имзони текшириши схемаси

Электрон хужжатларни тармоқ орқали алмашишда уларни ишлаш ва сақлаш харажатлари камаяди, қидириш тезлашади. Аммо, электрон хужжат муаллифини ва хужжатнинг ўзини аутентификациялаш, яъни муаллифнинг

хақиқийлигини ва олинган электрон хужжатда ўзгаришларнинг йўқлигини аниқлаш муаммоси пайдо бўлади.

Электрон хужжатларни ауентификациялашдан мақсад уларни мумкин бўлган жинояткорона харакатлардан ҳимоялашдир. Бундай харакатларга қуидагилар киради:

- **фаол ушлаб қолиши** - тармоқقا уланган бузғунчи хужжатларни (файлларни) ушлаб қолади ва ўзгартиради;
- **маскарад** – абонент *C* хужжатларни абонент *B* га абонент *A* номидан юборади;
- **ренегатлик** – абонент *A* абонент *B* га хабар юборган бўлсада, юбормаганман дейди;
- **алмаштириши** – абонент *B* хужжатни ўзгартиради, ёки янгисини шакиллантирадива уни абонент *A* дан олганман дейди;
- **такрорлаши** – абонент *A* абонент *B* га юборган хужжатни абонент *C* тақрорлайди.

Жинояткорона харакатларнинг бу турлари ўз фаолиятида компьютер ахборот технологияларидан фойдаланувчи банк ва тижорат тузилмаларига, давлат корхона ва ташкилотларига хусусий шахсларга анча- мунча зарар етказиши мумкин.

Электрон рақамли имзо методологияси хабар яхлитлигини ва хабар муаллифининг хақиқийлигини текшириш муаммосини самарали ҳал этишга имкон беради.

Электрон рақамли имзо телекоммуникация каналлари орқали узатилувчи матнларни аутентификациялаш учун ишлатилади. Рақамли имзо ишлаши бўйича оддий қўлёзма имзога ўхшаш бўлиб, қуидаги афзалликларга эга:

- имзо чекилган матн имзо қўйган шахсга тегишли эканлигини тасдиқлайди;
- бу шахсга имзо чекилган матнга боғлиқ мажбуриятларидан тониш имкониятини бермайди;
- имзо чекилган матн яхлитлигини кафолатлайди.

Электрон рақамли имзо-имзо чекилувчи матн билан бирга узатилувчи кўшимча рақамли хабарнинг нисбатан катта бўлмаган сонидир.

Электрон рақамли имзо асимметрик шифрларнинг қайтарувчанлигига ҳамда хабар таркиби, имзонинг ўзи ва калитлар жуфтининг ўзаро боғликлигига асосланади. Бу элементларнинг хатто бирининг ўзгариши рақамли имзонинг ҳақиқийлигини тасдиқлашга имкон бермайди. Электрон рақамли имзо шифрлашнинг асимметрик алгоритмлари ва хеш-функциялари ёрдамида амалга оширилади.

Электрон рақамли имзо тизимининг қўлланишида бир- бирiga имзо чекилган электрон хужжатларни жўнатувчи абонент тармоғининг мавжудлиги фараз қилинади. Ҳар бир абонент учун жуфт – маҳфий ва очик калит генерацияланади. Маҳфий калит абонентда сир сақланади ва ундан абонент электрон рақамли имзони шакиллантиришда фойдаланади.

Очиқ калит бошқа барча фойдаланувчиларга маълум бўлиб, ундан имзо чекилган электрон хужжатни қабул қилувчи электрон рақамли имзони текширишда фойдаланади.

Электрон рақамли имзо тизими иккита асосий муолажани амалга оширади:

- рақамли имзони шакллантириш муолажаси;
- рақамли имзони текшириш муолажаси.

Имзони шакллантириш муолажасида хабар жўнатувчисининг махфий калити ишлатилса, имзони текшириш муолажасида жўнатувчининг очик калитидан фойдаланилади.

Хэшлаш функцияси

Хэшлаш функциясидан хабар ўзгаришини пайқашда фойдаланиш мумкин, яъни у криптографик назорат йигиндисини шакллантиришга хизмат қилиши мумкин. Бу сифатда хэш-функция хабарнинг яхлитлигини назоратлада, ЭРИни шакллантиришда ва текширишда ишлатилади.

Хэш-функция фойдаланувчини аутентификациялашда хам кенг қўлланилади. Ахборот хавфсизлигининг қатор технологияларида шифрлашнинг ўзига хос усули бир томонлама хэш-функция ёрдамида шифрлаш ишлатилади. Бу шифрлашнинг ўзига хослиги шундан иборатки, у мохияти бўйича, бир томонламадир, яъни тескари муолажа – қабул қилувчи томонда расшифровка қилиш билан бирга олиб борилмайди. Иккала тараф (жўнатувчи ва қабул қилувчи) хэш-функция асосидаги бир томонлама шифрлаш муолажасидан фойдаланилади.

ХЭШ функция ва унинг ахборотни муҳофаза қилиш масалаларини ечишда қўлланилиши

Хэш функция деб ихтиёрий узунликдаги (бит ёки байт бирликларида) маълумотни бирор фиксиранган (кайд килинган) узунликдаги (бит ёки байт бирликларида) қийматга ўғказувчи функцияга айтилади. Хэш - функциялар статистик тажрибаларни ўтказишида, мантиқий қурилмаларни текширишда, тез қидириб топиш алгоритмларини тузишида ва маълумотлар базасидаги маълумотларнинг тўлалигини текширишда қўлланилади. Масалан, хар хил узунликдаги маълумотларнинг катта рўйхатидан керакли маълумотни тез қидириб топишда бу маълумотларни бир - бири билан таққослашдан кўра, уларнинг назорат йигиндиси вазифасини бажарувчи хэш қийматларини солиштириш қулайроқdir .

Криптографияда хэш - функциялар қуйидаги масалаларни ҳал қилиш учун ишлатилади:

- маълумотни узатишда ёки сақлашда унинг тўлалигини назорат қилиш учун;

-маълумот манбайнин аутентификация қилиш учун. Маълумотни узатища ёки сақлашда унинг тўлалигини назорат қилиш учун ҳар бир маълумотнинг хэш қиймати (бу хэш қиймат маълумотни аутентификация қилиш коди ёки «имитовставка» - маълумот блоклари билан боғлик, 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 назорат қиймати билан солиштиради. Агар таққослашда бу қийматлар мос келмаса, маълумот ўзгарганлигини билдиради.

“Имитовставка”лар ҳосил қилиш учун ишлатиладиган хэш-функциялар – назорат йифиндисидан фарқли равишда маълумотни сақлаш ва узатища рўй берадиган тасодифий хатоларни топибгина қолмасдан, рақиб томонидан қилинган актив хужумлар тўғрисида ҳам огохлантиради. Рақиб хэш қийматни мустақил ўзи ҳисоблаб топа олмаслиги ва муваффиятли олда имитация қилиши ёки маълумотни ўзгартира олмаслиги учун хэш - функция рақибга маълум бўлмаган махфий калитга эга бўлиши керак. Бу калит фақатгина маълумотни узатувчи ва қабул қилувчи томонларга маълум бўлиши керак. Бундай хэш - функцияларга *калитли хэш-функциялар* дейилади.

Калитли хэш - функциялар ёрдамида ҳосил килинадиган “имитовставка” лар имитация (*impersonation*) туридаги ҳужумларда қалбаки маълумотларни ҳосил қилишга (*fabrication*) ва “ўзгартириш” (*substitution*) туридаги ҳужумларда узатиладиган мамумотни модификация (*modification*) қилишга йўл қўймаслик учун ишлатилади.

Маълумот манбайнин аутентификация қилиш масалаласи ахборот - коммуникация тизимининг бир-бирига ишонмайдиган фойдаланувчилари ўртасида маълумот алмашинувида юзага келади. Бу масалани ҳал қилишда иккала томон ҳам биладиган махфий калитни қўллаб бўлмайди. Бу холатда маълумот манбайнин аутентификация қилишга имкон берадиган рақамли имзо схемаси қўлланилади. Бунда одатда фойдаланувчининг махфий калитига асосланган имзо қўйишдан олдин хатолик кодини аниқловчи хэш - функция ёрдамида маълумот сиқилади. Бу холда хэш - функция махфий калитга эга бўлмайди ҳамда у фиксиранган бўлиши ва хаммага маълум бўлиши мумкин. Унга қўйилган асосий талаб имзоланган хужжатни ўзгартириш ҳамда бир хил хэш қийматга эга бўлган иккита хар хил маълумотни танлаш имконияти йўқлигининг кафолатидир. Агар бир хил хэш қийматга эга бўлган иккита хар хил маълумот мавжуд бўлса бу маълумотлар жуфти *коллизия* ҳосил қиласди дейилади.

Юқорида келтирилганларни формаллаштириб, қуйидаги таъриф киритилади. *X* орқали элементлари маълумотлардан иборат бўлган тўпламни белгилаймиз. Одатда маълумотлар бирор алифбонинг, кўпинча иккилик саноқ, тизими алифбоси символлари кетма-кетлигидан тузилган бўлади. *Y* фиксиранган узунликдаги иккилик саноқ, тизимида аниқланган векторлар тўплами бўлсин.

Хэш - функция $h:X \rightarrow Y$ деб, ихтиёрий узунликдаги M маълумотни фиксиранган узунликдаги $h(M) = H$ қийматга акслантирувчи, осон хисобланадиган бир томонлама функцияга айтилади.

Хэш қиймат бошқа номлар билан -«хэш код», «свертка», «дайджест», «бармоқ излари» деб хам аталади.

Хэш-функцияга қуидаги талаблар қўйилади:

1. Ихтиёрий узунликдаги матнга қўллаб бўлади.
 2. Чиқиша тайинланган узунликдаги қийматни беради.
 3. Ихтиёрий берилган x бўйича $h(x)$ осон хисобланади.
 4. Ихтиёрий берилган H бўйича $h(x)=H$ тengликтан x ни ҳисоблаб топиб бўлмайди. (Бир томонламалик хоссаси)
5. Олинган x ва $y \neq x$ матнлар учун $h(x) \neq h(y)$ бўлади.(Коллизияга бардошлик хоссаси)

Одатда мумкин бўлган маълумотларнинг сони мумкин бўлган хэш қийматлар сонидан кўп бўлади, шунинг учун хар бир хэш қийматга бир нечта матнлар тўплами, яъни бир хил хэш қийматли маълумотлар тўплами мос келади.

Фойдаланилган адабиётлар

1. Фаниев С. К., Каримов М. М., Ташев К. А. Ахборот хавфсизлиги. Ахборот-коммуникация тизимлар хавфсизлиги. Олий ўқув юрт талабалари учун мўлжалланган. "Алоқачи", 2008.
2. Mark Stamp. Information security. Principles and Practice. Second edition. A John Wiley& Sons, Inc., publication. Printed in the United States of America. 2011y. 584p.
3. Шангин В.Ф. «Информационная безопасность и защита информации», Учебное пособие. М.: 2014 г.