bilimger.kz
Республикалық білім және ғылым порталы
https://bilimger.kz
ҚР Мәдениет және Ақпарат министрлігі тіркелген — Куәлік нөмірі: ***KZ45VPY00102718***
2021

БӨЛІМ: ЖАЛПЫ РУБРИКА

"Ұялы байланыс жүйелерінде криптографиялық қорғау аппараттық жүйесін жобалау" тақырыбында ғылыми жұмыс

ЖАРИЯЛАНДЫ
25.09.2021

СІЛТЕМЕ
https://bilimger.kz/107029/

ҚАЗАҚСТАН РЕСПУБЛИКАСЫНЫҢ БІЛІМ ЖӘНЕ ҒЫЛЫМ МИНИСТРЛІГІ

«Түркістан облысының адами әлеуетті дамыту басқармасы» ММ

«Түлкібас агробизнес және саяхат колледжі» МКҚК

БЕКІТЕМІН

Директордың оқу ісі жөніндегі
орынбасары _____ Л.Байсеитова «___»_____20___
ж.

ҒЫЛЫМИ ЖҰМЫС

Тақырыбы: Ұялы байланыс жүйелерінде криптографиялық қорғау аппараттық жүйесін жобалау

«Есептеу техникасы және бағдарламалық қамтамасыз ету»

мамандығы бойынша

ҒЖ орындаған Өндірістік оқыту шебері

Темирова Клара Фарзалиевна

Т.Рысқұлов 2021ж.

Кіріспе

XXI ғасырда қоғамның ақпараттандырылуы мәдениеттің дамуында басым үрдіс болды. Информатиканың көптеген құралдарының, телекоммуникациондық құрадарының және жаңа ақпараттық технологиялардың жетімді болуы негізінде ақпараттық орта құрылады. Бұл ортада адамзат үшін тек жаңа мүмкіндіктер ғана емес, сонымен қатар бұрын белгісіз болған мәселелер туындайды.

Криптография мен криптоанализдің байланысы: криптография – қорғаныс, ал криптоанализ – бұзу. Криптограф тапсырмасы – жіберілетін ақпараттың құпиялығын және түпнұсқасын қамтамасыз ету. Криптоаналитиктің тапсырмасы – жіберілетін ақпараттың жүйесін бұзу. Ол шифрленген хабарламаны бұзуға тырысады немесе жалған хабарламаны түпнұсқаның орнына береді. Бірақ бұл екі пән бір-бірімен байланысты және де криптоанализ тәсілдерін білмейтін жақсы криптографтар болмайды.

Криптография облысында өңдеу тәсілдері құпия болады және көбіне мамандардың өзіне белгісіз болады.

Сонымен қатар, криптографиялық алгоритмнің мемлекеттік стандарттарға қатысын ескеру керек. Себебі, криптографияның дамуымен кейбір политикалық мәселелер туындап отыр. Мысалы, үкімет криптографияны қоғамның жеке мақсаттарда қолданғанын ұнатпайды. Мысалыға американдық үкімет шифрлеу алгоритмін стандарттауға тырысып жатыр, бұл шифрленген ақпаратқа соттың шешімімен қол жеткізуге болады. Криптографияны мемлекеттік реттеу мысалы ретінде Ресейдің 1995 жылдың 3 сәуірінен № 334-ші бұйрығы бойынша сертификатталмаған криптографиялық құралдарды мемелекеттік органдардың көмегімен қолдануға және арнайы лицензиясыз өңдеуге тыйым салады.

Мәліметтің криптографиялық түрледіру процессі бағдарламалық және аппараттық жүзеге асырылуы мүмкін. Аппараттық іске асырылуы қымбат бағасымен ерекшеленеді, бірақ жоғары өнімділікпен, қарапаймыдылығымен және қорғаныштылығымен икемді.

Бағдарламалық іске асырылуы тиімді және қолдануды ыңғайлы.

Ұялы байланыс – бұл принципті қолданған жүйелер 1970-ші жылдардың аяғында шыға бастады. Мобильді байланыстың ұялы мекемемен алғашқы ұрпағы ұқсас болды және транкілі жүйелердің дамытылған түрі болды.

Ғылыми жұмыстың тақырыбы: «Ұялы байланыс жүйелерінде криптографиялық қорғау аппараттық жүйесін жобалау». Осы ғылыми жобасын құру кезінде жасаушы

құралдардың жаңашыл тәсілі Java программалау ортасы қолданылды.

Ғылыми жұмыс тақырыбының өзектілігі: Кез-келген бағдарламалы-аппараттық қамтама жетілген болмайды, сондықтан да ақаулар болады. Реалды уақытта маңызды ақпаратты рұқсаты жоқ қолданушылардан құпия түрде сақтау практикалық түрде мүмкін емес. Осы себептен көптеген қолданушылар өзінің ақпаратын сақтау үшін арнайы бағдарламаларға ие болуды қалайды. Қазіргі уақытта шифрлейтін бағдарлалардың көптеген түрлері бар, бірақ олар шартты түрде ғана ақысыз немесе ақылы болады, көптеген қолданушылар бұған ие бола алмайды.

Ғылыми жұмысымның мақсаты: екі сымысыз байланыс арқылы байланысқан құрылғы арасында хабарлама жіберу барысындағы шифрлеудің бағдарламалы-аппараттық жобаның іске асырылуы.

Тапсырманың қойылуы:

- Ұялы байланыс жүйелерінде криптографиялық қорғаныс жүйесін зерттеп қарастыру;
- Симметриялық шифрлау алгоритмінің және ұялы байланыс жүйесінің қолданыста бар түрлерін оқып уйрену;
- Ұялы байланыс стандарттарын және мәліметті шифрлеу алгоритмін таңдап қарастыру.

Зерттеу обьектісі: ұялы байланыс жүйелері.

*Зерттеу пәні:*криптография және ұялы байланыс жүйесі.

Ғылыми жұмыстың жаңалығы: жасалған өнім тәуелсіз бағдарлама болып табылады. Маңызды ақпараттың таңдалған алгоритм негізінде шифрлеу тәсілі арқылы қауіпсіздікті қамтамасыз етеді. Бағдарлама қолданушыға түсінікті және қарапайым интерфейстен тұрады. Екі құрылғы арасында сымсыз ұялы байланыс жүйесі арқылы мәлімет жіберуде қажет болады.

Ғылыми жұмыстың құрлымы: ғылыми жұмыс кіріспеден, үш тараудан, қортындыдан және қолданылған әдебиеттер тізімі мен қосымшадан, 25 суреттен және 9 кестеден құралған.

Бірінші бөлімде криптографияның негізгі түсінігі мен даму тарихы, криптографияның түрлері, хэштеу тәсілдері, криптографиялық хаттамалар қарастырылған.

Екінші бөлімде сымсыз байланыс негізінде мәліметті шифрлеу үшін қолданылатын ұялы байланыстың тәсілдері мен түрлері қарастырылады.

Үшінші бөлімде мәліметті шифрлеу бағдарламасының негізгі элементтері көрсетіліп және де java тілі қарастырылған.

Ғылыми жұмыс қорытындымен аяқталады. Барлық жасалған практикалық және теориялық қорытынды, қолданылған әдебиетер көрсетілген.

1 Криптографияның негізгі түсінігі мен даму тарихы

Криптография –бұл мәліметтерді алмастыру әдістерінің жиынын көрсетеді, қарсы жақ үшін бұл мәліметтерді пайдасыз ету үшін бағытталған.(Криптография — cryptos — құпия, белгісіз logos – хабар байланыс)

Криптоанализ – (қорғаныс жүйесін бұзу) бұл кілтке ену рұқсатынсыз шифрленген хабардың бастапқы мәтінін ашу жөніндегі ғылым.

Сурет 1. Криптожүйенің жалпы схемасы.

Жіберуші қорғалмаған канал бойынша заңды қабылдаушыға берілуі қажет бастапқы хабарының ашық текстін генерациялайды. Каналды ұстап алушы берілетін хабарды ашу және ұстап алу мақсатында бақылайды. Ұстап алушы хабарының мазмұнын біліп алмау үшін, жіберуші оны алмастыру көмегімен шифрлейді, және қабылдаушыға жіберілетін шифртекстті алады.

Қабылдаушы С шифрді кері алмастыру көмегімен ашады және бастапқы хабарды алады.

(1.1)

Ек алмастыру криптоалгоритмі деп аталатын криптографиялық алмастыру түрлерінен таңдалады.

Жеке қолданылатын алмастыру таңдалатын параметр криптографиялық кілт К деп аталады.

Криптографиялық жүйе – бұл түрге келтіретін ашық тексті хабарды кеңістіктен шифрленген текстті кеңістікке көшірілетін бір параметрлік () түрі.

К(кілт) параметрі кілттер кеңістігі деп аталатын ақырлы К жиынынан таңдап алынады [1-6].

1.1 КРИПТОГРАФИЯ ТАРИХЫ

Адам – әлеуметтік жан, көп мыңжылдықтар бойы ол өзіне ұқсас жандардың қатарында тұрады. Сондықтан оның негізгі қасиеті басқа адамдармен қатынас құру болып табылады – оларға қоршаған ортада не болып жатқанын, өздерінің субъективті нақтылықта қандай фактілер пайда болатыны жайлы таратады. Екінші сигналдық жүйе — сөйлеу – бұл қасиет адамның маңызды ерекшелігі болып табылады, бұл қасиет сапалық түрде адамдарды жануар әлемінен ерекшелендіреді. Ең жабайы тайпа мүшелері арасындағы ақпараттық алмасу сипатының өзі жануарлардың қатынасынан көп есе күрделі болады. Адам қоғамындағы коммуникацияның бір ерекшелігі болады – ол тар мағынада таңдаулы болады. Біз алуан түрлі адамдармен әр түрлі деңгейде сөйлесеміз және біреулерге айтқаны кейбіреулерден жасыруға тырысамыз.

Ендеше адам өркениеті пайда болғаннан кейін ақпаратты адамдарға таратқанда оны жасуру мүмкіндігі де пайда болды. Адамдар хаттамаларды жібергенде тек дауыс пен қимылдарды қолданған кезде ақпаратты жасыру онша қиын болмады, ол үшін ақпарат жіберілгенде салыстырмалы жақын араға ол ақпарат арналмаған адамды жақындатпады. Бірақ та сыртқы факторлар кейбір кездері әңгімелесуші адамның тәртібіне шектеулер қойды, осы шектеулерге қатысты әңгімелесуші адамдар сырт көзден немесе құлақтардан жасырына алмады. Осындай жағдайлар үшін өзімен-өзі сөйлеумен немесе қимыл негізіндегі хаттамалардың кодталуы пайда болды. Әр түрлі жағдайларда ол алуан түрлі сипатта болды – белгілі бір оқиғаның болуын хабарлайтын жекеленген құпия белгіден бастап, алуан түрлі қиындықтағы ойларды бейнелеуге қолданылатын дамыған құпия тілдеріне дейін. Тіпті ең қарапайым жағдайдың өзінде бұл миниатюрадағы екінші дарынды жүйе болып саналды, ол көбіне шетелген мәліметтер жиынын беріп жіберуге арналатын және ол арнаулы кішкентай топқа ғана белгілі болатын, яғни бұл альтернативті тілдің үлкен немесе кішкентай бөлшегі болды. Осы бөлшек негізінде болашақта хаттамаларды құпия түрде жіберу өнері пайда болды.

Әрине, жіберілетін деректерді қорғау үшін әңгімелесуші жақтардың алдын-ала келісіп алған бірнеше құпия белгілерді қолдануға қарағанда дамытылған «құпия» тілді қолдану коммуникацияда кең масштабты бостандықты қамтамасыз етеді. Бірақ та бұл тәсілдеме үлкен шығындарды тудырады. Барлық арнаулы адамдарды бақылау, әрине, қиын әрекет, сондықтан ерте ма кеш па мұндай тілді жасырып жатқан адамдар біліп алады. Мұндай жағдайда ол тілді басқа тілмен ауыстыру қажеттілігі туындайды, ал басқа салыстырмалы түрде қуатты тілді жасау және аз уақыт мерзімінде қажетті мөлшерлі адамдарды оған үйрету – өте күрделі және шығынды болып табылады, оны оперативті түрде жасау – мүмкін емес әрекет. Сондықтан мәселеге алынатын мұндай тәсілдеме тек ерекше жағдайларда ғана жүзеге асырылады. Осы тәсілдемені екінші дүние жүзілік соғысы кезінде американдықтар пайдаланды: АҚШ елінің ӘТФ кемелері аз мөлшерлі және жинақы өмір сүретін индейлер тайпасының тіл негізінде байланыс құрды. Әрбір кемеде бірнеше индейлер-шифрлеушілер болды, қарсыласта ондай криптографты алып алуға еш мүмкіндік берілмеді.

Жазу пайда болғасын жіберілетін хаттамалардың құпиялығын және шынайлығын сақтау одан сайын өзекті мәселеге айналды. Шынымен де, қимылмен немесе сөйлеумен жіберілетін хаттама қоршаған ортаға тек оның жіберу мезетінде ғана қолжетімді болады, ал оның шынайлығы немесе авторлығында еш күмән тумайды, себебі әңгімелесуші адам оны өз көзбен көре алады. Ал хаттама жазбаша түрде болғанда, ол жеке өмір сүреді және оның жекеленген өз авторымен қиылыспайтын жолы болады. Қағазда жазылған хаттама материалды дүниеде салыстырмалы түрде көп уақыт бойы өмір сүреді де, оны білгісі келетін адамдар жіберуші мен қабылдаушыларды елемей оны көріп алу мүмкіндігі көбірек болады. Сондықтан жазу пайда болғаннан кейін құпия жазу өнері пайдабола бастады, «құпия жазу» өнері – бір адамнан басқа адамға арналып

жазылған хаттамалардың құпия тасымалдануына арналған тәсілдер жиыны.

Құпия жазу тәсілдері жайлы мәліметтер үзінді ретінде сақталған. Бұл жазу түрі Мысыр мен Вавилон елінде болған деп болжанады. Қазіргі кезде біздерге құпия жазу ерте Греция елінде болған деген мәліметтер жетті. Шифрлеу тәсілдерінің сипаттамалары бар ең алғашқы дәлелденген мәліметтер ескі және жаңа ғасырдың ауысу мерзіміне жатады және Цезарь шифрін сипаттайды – бұл тәсіл негізінде Юлий Цезарь өз жазбаларын керек емес артық көздерден жасырды. Заманауи криптографияның жетілу биіктігінен Цезарь шифрі қарапайым болып табылады: хаттаманың әрбір әрпі әліпби бойынша келесі әріпке ауыстырылады. Бірақ та жазу мен оқу сирек ерекшелік болған уақыт үшін оның крипто беріктілігі сол уақытқа сай болды. Шифрді қолдану жіберілетін хаттаманың құпиялық мәселесін шешті, ал оның тұпнұсқалық мәселесі өзімен-өзі шешілді:

- біріншіден, шифр білмейтін адам үшін мәтіндік сипатта болатын шифрленген хаттамаларға мәнді өзгерістерді енгізу мүмкін емес әрекет, ал асығыста енгізілген өзгерістер дешифрлеуден кейін мәні жоқ әріптер жиынтығының шығуына себеп болды;
- екіншіден, уақыттың талабына сай барлық жазылған хаттамалар тарихи өлшемдерге сәйкес қолмен жазылды, ал әрбір адам өзіне тән жазу қолтаңбаларына ие, оны басқа адам ұқсата алмайды; маңызды корресподенттердің жазуын есте сақтау – кейбір адамдар үшін қиындықты тудырмайды.

Адамзат құпия жазудың алуан түрлі тәсілдерін ойлап тапты, олардың көбісі ертеден бастау алады. Құпия жазудың кейбір тәсілдерінде ақпарат тасушының физикалық ерекшеліктері қолданылады. Мысалға, симпатикалық сиямен жазылған мәтін басында немесе жазғаннан кейін біршама уақыттан кейін көрінбей қалады. Бірақ оларды қайтадан көрінетін күйге келтіруге болажы, ол үшін құжатты арнайы химиялық реактив немесе спектрдің белгілі бір бөлігімен, көбіне ультрафиолет жарықтарымен өңдеп алу керек.

Стенографияның болжауы бойынша: жіберілетін мәтін үлкен мөлшердегі мәтінде жоғалады, егер онда қажетті емес, басқа мағына болатын болса. Егер де одан кейбір символдарды алып, белгілі бір заңдалық бойынша өзгертетін болсақ, мысалға – әрбір екінші немесе әрбір үшінші, және т.б., бізде нақты құпия хаттама пайда болады. Шифрлеу хаттаманы белгілі бір заңдылықтар негізінде түрлендіру әрекеті болып табылады, бұл әрекет шифр құриясын білмейтін адамға көбіне хаттамаларды белгілердің мәнсіз жиынына айналдырады.

Жіберілетін хаттамалардың құпияландыру тәсілдерін классифицирлеуге алуан түрде жүргізуге болады, бірақ та оларды анықтайтын факторлар саны тек екеу болады:

- материалды тасуыштардың және материалды ортаның қасиеттері қолданылады ма, әлде олар онсыз да қолданыла береді ме;
- құпия хаттама жасырылады ма әлде ол қабылдаушыдан басқа қолжетімсіз күйге келтіріледі ме [5].

Жоғарыда айтылғандай, хаттаманы жасырудың көптеген тәсілдері оның материалды объекті мен тасуышқа тигізетін әсеріне тәуелді болады. Бұл қызықты тақырып, бірақ та ол физика мен химия ғылымдарын үйренудің себебі болып табылады да, ақпараттар теориясына еш қатысы болмай қалады. Жаппай практикалық қолданыс үшін көбіне мәліметтердің қасиеттеріне негізделетін және олардың физикалық бейнелерімен байланыссыз болатын мәліметтерді қорғау тәсілдеріне көп көңіл бөлінеді. Яғни жалпылап айтсақ, осы типтегі тәсілдерді қолданған кезінде хаттама мен оны рұқсатсыз оқығысы немесе бүлдіргісі келетін зиянкес арасындағы кедергі тосқауыл ең біріншіден ақпарат үшін қойылады. Енді тек ақпаратты қорғаудың осындай тәсілдері жайлы қарастырамыз.

Жоғарыда қойылған екінші сұрақтың жауабына байланысты мәліметтерді құпияландыру тәсілдерінің алуан түрлі кластары пайда болады — стеганография және шифрлеу. Егер де ақпаратты оның материалдық бейнеден бөлек қарастыратын болсақ, онда оны қайда жасыра аламыз? Жауап бір мәнді болады: ақпарат одан сайын көп мөлшерлі болса, бұл бір мая шөптен инені іздегендей болады. Бұл әрекет стенографияның негізгі әрекет принципі болып табылады. Мысалға, біз өзіміздің кореспондентімізге электронды пошта арқылы растрлік қара-ақ түсті сурет жібереміз, онда суреттің әрбір айқындылықтың ең жарық биті біздің құпия хаттаманың элементі болады. Хатты алатын адам хаттан барлық осындай биттерді алып, олардан шынайы керекті хаттама құрастырады. Көзді жалған етіп бұру үшін қолданылатын сурет арнайы адамдарға қарапайым сурет ретінде қала береді. Стенография құпия хаттамаларды жай жіберуімен қатар, хаттаманың жіберілу фактын жасырған кезде өте пайдалы болып табылады. Құпия коммуникацияны жүргізудің мұндай тәсілі, бірақ та бірнеше кемшіліктерден тұрады:

- біріншіден, оның беріктілігін шарттауға қиын әрекет болып табылады — мысалға, кенеттен зиянкестерге болванканың құпия мәліметтерінің араластыру тәсілі белгілі болып кетсе – ашық мәліметтер массиві;
- екіншіден, осы тәсілді қолдану кезінде жіберілетін немесе сақталатын мәліметтердің мөлшері шұғыл түрде үлкейеді, осының бәрі жүйелердің өнімділігіне және олардың өңделуіне теріс әсер етеді.

Басқа тәсілдеме – хаттаманы жіберу фактын жасырмау, бірақ та хаттаманы басқалар үшін қолжетімділікті шектеуге негізделеді. Ол үшін хаттама кореспонденттерден басқа ешкім ашып, оқи алмайтындай етіп жазылуы тиіс – бұл шифрлеудің негізгі мәні болып

табылады. Криптография хаттамалардың шифрлеу тәсілдерін зерттеп, әзірлейтін практикалық пән ретінде пайда болып, дамыды.

Тарихқа оралатын болсақ. Қоғамда хат жазу белсенді болған сайын, оны құпияландыру әрекетіне деген қажеттілік те өсті. Сәйкесінше, одан сайын жетілдірілген және айлалы шифрлер пайда болды. Алдымен қызығушылық тудырған адамдардың жанында шифрлеуші адамдар пайда болды, содан кейін бірнеше шифрлеуші адамдардан тұратын топтар, соңында үлкен шифрлеуші бөлімдер пайда болды. Құпияландыруға берілетін ақпарат мөлшері көп болып, шекті мәнге жеткенде,адамдарға көмек үшін механикалық құралдар пайда болды. Криптографиялық қызметтерді көп пайдаланғандар қатарына дипломатты және шпиондық миссиялар, басшылардың құпия канцеляриялары мен әскери бірігулердің штабтары жатады. Криптографияның бұл даму кезеңі үшін мына жағдайлар сипатты болып табылады:

- қорғауға тікелей табиғи тілде жазылған мәтіндік хаттамалар ұшырады – дискретті түрде берілген мәліметтердің басқа типтері ол уақытта болған жоқ;
- басында шифрлеу қолмен жасалды, соңыра салыстырмалы түрде күрделі емес механикалық жабдықтар жасалды, сондықтан сол уақытта қолданылған және ойлап табылған шифрлер қарапайым және онша күрделі болмады;
- криптография және криптоанализ ғылым болғанша, сәл өнерге ұқсады, оларды шешуге ғылыми тәсілдеме болмады;
- криптография тар аймақта қолданылды тек басқару қабаттары мен мемлекеттің әскери төбелері үшін ғана пайдаланды;
- криптографияның негізгі міндеті ретінде жіберілетін аттамалардың басқа қажетті емес адамдардан қорғау әрекеті алынады, себебі көбіне тек мәтіндік хаттар құия болып жасырынды, басқа жалған мәліметтерді қорғау үшін басқа тәсілдер қолданылмады – дешифрлеу өткізгесін сәл болса да мағыналы бірдеңе алу аз үлесті құрды, себебі табиғи тіл көп дәрежелі молшылықта болды.

Біздің жүзжылдықтың ортасы тұсында электрлік-санауыш машиналардың пайда болуы бұл жағдайды күрт өзгертті. Өмірдің алуан түрлі аймақтарына компьютерлердің енуімен бірге шаруашылықтың жаңа тармағы пайда болды – ақпараттық өнеркәсіп. Қоғамда айналып жүретін ақпараттың мөлшері сол уақыттан бастап экспоненциалды заң бойынша өсу жолында – ол шамамаен әрбір бес жылда екі есе өседі. Адамзат жаңа мыңжылдықтың басында жаңа ақпаратық өркениетті ойлап тапты, онда ақпаратты өңдеу жабдықтарының табысты жұмысынан қазіргі таңдағы сапаға қатысты адамзаттың аман қалуы мен саулығы тікелей байланысты болады. Осы кезеңде болған өзгерістерді осы түрде сипаттауға болады:

- өңделетін ақпараттың мөлшері жарты ғасырда бірнеше тәртіпке өсе түсті;
- қазіргі таңда мынадай заңдылық орнықты: белгілі бір мәліметтерге болатын қол жетімділік мәнді материалдық және қаржылық құндылықтарды бақылауға мүмкіндік береді; ақпарат белгілі бір бағаға ие болды, оны кейбір жағдайда санауға да болады;
- өңделетін мәліметтердің сипаты алуан түрлі болып кетті және енді мәтіндік типпен ғана шектелмейді;
- ақпарат енді толығымен «иесізденді», яғни оның материалдық бейненің ерекшеліктері өз мағынасын жоғалтты – кеткен ғасырдың хатын электронды поштамен жіберілген хаттамамен салыстырыңыз;
- ақпараттық арақатынастардың сипаты мәнді түрде күрделінді, және мәтіндік хаттамаларды көріп қалудан қорғау сферасындағы классикалық қорғау міндетімен бірге қорғау облысында басқа да жаңа міндеттер пайда болды. Олар ертеде қағаздық технологиялармен бірге орындалды – мысалға, электронды құжаттың астында болатын қол таңба және электрондық құжатты қолхат бойынша жіберу – криптографияның осындай жаңа міндеттері туралы әңгіме әлі қарастырылмады;
- ақпараттық процестердің субъектілері ретінде адамдардан басқа, адамдармен жасалған және белгілі бір программа бойынша жұмыс жасайтын автоматтандырылған жүйелер де жатады;
- заманауи компьютерлердің есептеу мүмкіндіктері өздерінің күрделі механизмдерінің көмегімен шифрлерді жүзеге асыру процесін жаңа деңгейге көтерді.

Жоғарыда келтірілген өзгерістер компьютерлердің қызметтік ортада жылдам таралуынан байланысты практикалық криптографияның өзінің дамуында үлкен секіріс жасауына өзінің оң әсерін тигізді. Яғни, оның оң әсері бірнеше бағыт бойынша дамуына мүмкіндік туғызды:

- біріншіден, құпия кілті болатын тұрақты блоктық шифрлер жасалды, олар классикалық есептерді шешуге арналып жасалды –жіберілетін немесе сақталатын мәліметтердің құпиялығын және бүтінділігін қамтамасыз ету, олар әлі де криптографияның «жұмыс аты» болып саналады, яғни криптографияда жиі қолданылатын жабдық болып табылады;
- екіншіден, ақпаратты сақтау ортасында жаңа, дәстүрлік емес есептерді шешетін тәсілдер ойлап табылды, олардың ішінен салыстырмалы түрде кең таралғандарға электрондық құжаттың қолтаңбасы мен ашық кілттердің таралу есептерінің шешімдері жатады.

Яғни, криптография термині өзінің құпия жазу, құпия хат бастапқы міндетінен алысқа

кетіп қалды. Қазіргі таңда бұл пән алуан түрлі сипаттағы ақпараттық қатынастағы мәліметтерді қорғау тәсілдерін біріктіреді, бұл тәсілдер құпия алгоритмдер, сонымен қатар құпия параметрлерді қолданатын алгоритмдердер негізінде мәліметтерді түрлендіруге арналған. Ақпараттық арақатынас термині немесе ақпараттық арақатынас процесі» ақпаратты тасымалдау немесе өңдеу мақсатында екі немесе бірнеше субъектілердің арасында қатынас құру процесі дегенді білдіреді. Көбіне, криптографиялық функция деп кез келген мәліметтерді түрлендіру функциясын атауға болады, ол өзімен өзі құпия болады немесе белгілі бір құпия параметріне тәуелді,немесе формулаларымен анықталады [27].

1.2 ЗАМАНАУИ КРИПТОГРАФИЯНЫҢ МІНДЕТТЕРІ

Жетпісінші жылдардың ортасынан бастап асимметриялық (кілті ашық) криптография, сенімділігі күрделі математикалық есептерді шешу арқылы дәлілденген төзімді протоколдар сияқты фундаменталды ойлардың пайда болуына байланысты криптография шифрлеу-дешифрлеу тәсілдерінің құпия жиынтығы болуымен қатар, өзінің жеке математикалық теориясын құра бастады.

Заманауи криптография төрт ірі бөлімнен тұрады:

1. Симметриялық криптожүйелер (классикалық криптография);
2. Ашық кілттері бар криптожүйелер;
3. Электронды қолтаңба жүйелері;
4. Криптографиялық протоколдар.

Криптографиялық тәсілдерді қолданудың негізгі бағыттары:

- байланыс каналдары арқылы құпия жекеленген ақпараттың тасымалдануы (мысалға, электронды пошта),
- шифрленген түрде тасуыштарда ақпаратты сақтау (құжаттар, деректер қоры),
- жіберілетін және жүйе абоненттері арасында орнатылған хаттамалардың шынайылығын орнату (аутенфикация),
- электронды төлеу жүйелерінде ақпаратты қорғау, мұнда әмбебап төлеу құралы ретінде банктің пластик карталары қолданылады [1].

Криптография облысындағы көптеген әзірлемелер құпия болып табылады және ашық мамандарға жабық аймақтың жетістіктері белгісіз болып қала береді.

Криптографиялық алгоритмдер мемлекеттік стандарттарға да тиісті екенін ескерту керек. Себебі криптографияның дамуы кезінде кейбір саяси мәселелер туындайды. Мысалға, саясаттағы тұлғаларға кейбір адамдар криптографияны өз мақсаттарында қолданатыны ұнамайды. Иллюстрация ретінде американдық үіметінің шифрлеу алгоритмдерін стандарттауға жасап жатқан тырысуын көрсетуге болады, осының бәрі биліктегі адамдарға сот шешімі бойынша жасырып тұрған ақпаратқа қолжетімділікті алуға мүмкіндік береді. Криптография облысындағы мемлекеттік реттеу әрекетінің мысалына Ресей Федерациясының Президентінің 1995 жылы 3 сәуірде берген № 334 жарлығын алуға болады, ол жарлық мемлекеттік мүшелермен қатынас кезінде сертикацияланбаған криптографиялық жабдықтарды қолдануға тыйым салады, сонымен қатар осындай жабдықтарды арнайы лицензиясыз қолдануға рұқсат бермейді.

Саяси мәселелермен сонымен қата криптографиялық жабдықтарды экспорттау жайлы берілетін шектеулер байланысты. АҚШ мемлекетінде оларды әскери жабдықтарға ұқсатып, теңестіреді. Экспорттауға кілт ұзындығы 40 биттен аспайтын криптографиялық жабдықтар қолданылады. Практиканың көрсетілімі бойынша, осындай ұзындықтағы кілтті бірнеше дербес компьютерлер арқылы бірнеше сағатта теріп алуға болады.

Криптографияда тарихқа сәйкес бірнеше әскери сөздер тұрақталды: қарсылас, шифрге жасалатын шабуыл және т.б. Олар сәйкес криптографиялық ұғымдардың мағынасын толық ашады. Сонымен қоса кодты ұғынуға негізделген кең таралған әскери терминология қазіргі кезде теориялық криптографияда қолданылмайды. Бұл ақпараттың математикалық теориясында код түсінігі кодтау теориясы негізінде тұрақталғанына байланысты, кодтау теориясы байланыс каналында ақпаратты кездейсоқ өзгерістерден сақтауға арналған қорғау тәсілдерін зерттейді. Баяғыда «кодтау» мен «шифрлеу» терминдері синоним ретінде қолданылса, қазіргі кезде олар бұл мағынада қолданыла алмайды[7-8].

Қазіргі симметриялы криптожүйелер. К.Шеннон пікірі бойыша шифрларларда екі жалпы ұстанымды пайдалану қажет: шашырау және араластыру.

Шышырау кезінде ашық мәтіндегі бір таңбаның шифрмәтіндегі көп таңбаға ықпалының таралуы болады. Ол ашық мәтіннің статистикалық қасиеттерін жасыруға мүмкіндік береді. Араластыру кезінде шифрлаушы түрлендірулер пайдаланылады. Олар ашық және шифрланған мәтіндердің статистикалық қасиеттерінің өзара байланысын қалпына келтіруді қиындатады. Дегенмен шифр ашуды қиындатып қана қоймай (егер пайдаланушыға құпия кілт белгілі болған жағдайда) шифрлау мен оны қайта ашудың оңай болғанын да қамтамасыз етуі керек [9].

Шашырау мен араластыруды іске асыруға арналған тәсілдердің біріне құрама шифрды пайдалану тәсілі жатады. Бұл тәсілде пайдаланылатын шифр қарапайым шифрлер тізбегінен тұрады. Мұндағы әрбір шифр не шашырау, не араластыру арқылы нәтижеге өз үлесін қосады. Құрама шифрлерде қарапайым шифр есебінде, әдетте ауыстыру және қарапайым орын ауыстыру жиі пайдаланылады. Орын ауыстыру кезінде ашық мәтін символдарын тек араластырады және араластырудың нақты түрін құпия кілт анықтайды. Ауыстыру кезінде ашық мәтіннің әрбір символы, сол алфавиттегі басқа символмен ауыстырылады, ал алмастырып қоюдың нақты түрін, бұл жерде де құпия кілтпен анықтайды. Сонымен бірге мынаны еске ала кету керек: қазіргі кездегі блоктық шифрда ашық мәтін мен шифрмәтіннің блоктары әдетте ұзындықтары 64 бит болатын екілік тізбектерден тұрады. Әрбір блок 264 мән қабылдауы мүмкін. Сондықтан ауыстыру құрамында264=1019 символдары бар өте үлкен алфавитте орындалады [2].

*Асимметриялық криптожүйелер.*Деректерді криптографиялық қорғау жүйелерінің ішінде ассиметриялық криптожүйелер тиімді жүйелер қатарына жатады. Оларды ашық кілтті криптожүйелер деп те атайды. Мұндай жүйелерде деректерді шифрлау үшін бір кілт, ал оларды кері шифрлауға басқа кілт қолданылады (ассиметриялық деп аталу себебі осында). Бірінші кілт ашық (public key) болады және ол деректерін шифрлаймын деген барлық пайдаланушылар қолдану үшін жария етілуі мүмкін. Деректерді кері шифрлауға ашық кілт жарамайды [9].

Шифрланып келген деректерді кері шифрлау үшін қабылдаушы жақ екінші кілтті пайдаланады. Ол құпия кілт (private key) деп аталады.

Сөйтіп бұл криптожүйеде екі түрлі кілт қолданылады: — жіберушінің ашық кілті, — алушының құпия кілті. Құпия кілтті қорғалмаған арна арқылы жібермеу үшін кілттер генераторын алушы жағында орналастырған тиімді болады. құпия кілтін белгілі ашық кілт бойынша ашу шешілмейтін мәселе болуы керек [10].

Ассиметриялық криптожүйелерге тән ерекшеліктер:

- КА ашық кілті мен криптограммасы қорғалмаған арна бойынша жіберіледі, яғни қарсы жаққа және белгілі;
- шиФрлау және кері шиФрлау алгоритмдері ашық болады.

Ассиметриялық криптожүйелердегі ақпаратты қорғау кілтінің құпиялығына тікелей байланысты.

У.Деффи және М.Хеллман ассиметриялық криптожүйелерінің қауіпсіздігін қамтамасыз ететін талаптарды қойды:

- Алушы үшін бастапқы жағдай негізінде (,) кілттер жұбын есептеп шығару қарапайым болу керек.

- А жіберуші ашық кілтін және хабарын біліп, криптограмманы өте оңай есептей шығара алады: .
- В алушы құпия кілтін және криптограммасын пайдаланып бастапқы хабарды оңай қалпына келтіре алады.
- Қарсы жақ ашық кілтін біліп құпия кілтін есептеп табу кезінде шешуге болмайтын есептеу проблемасына кез болады.
- Қарсы жақ (,) жұбын біліп бастапқы хабарын есептеп табуды еш қандай жолмен шеше алмайды.

Ашық кілтті ассиметриялық криптожүйелер концепциясында бір бағыттық Функцияларды қолдану көзделген. және — кез келген жиын түрі берілген дейік. Егер барлық үшін оңай есептеп табуға болатын болса (мұнда), онда f: Функциясы бірбағытты деп саналады [2].

*Электрондық сандық қолтаңба.*Электрондық сандық қолтаңба (ЭСҚ) телеқатынас арналарымен тасымалданатын мәтіндерді аутентификациялау үшін пайдаланылады. Цифрлық қолтаңба — қол қойылатын мәтінмен бірге жіберілетін қосымша онша көп емес циФрлық ақпарат.

ЭСҚ жүйесінің өз құрамында екі процедура бар: 1) қолтаңбаны қою процедурасы; 2) қолтаңбаны тексеру процедурасы. Қолтаңбаны қою процедурасында хабар жіберушінің құпия кілті пайдаланылады, ал қолтаңбаны тексеру процедурасында — жіберушінің ашық кілті.

ЭСҚ-ны қалыптастыру кезіндехабар жіберуші ең алдымен қол қойылатын M мәтіннің ¿(M) хэш-Функциясын есептеп шығарады. Есептеп табылған ¿(M) хэш-функциясы бүкіл M мәтінін сипаттай алатын бір қысқа ғана ақпараттардың m блогінентұрады. Содан сон m саны жіберушінің құпия кілті арқылы шифрланады. Осылайша алынған сандар жұбы берілген M мәтінінің ЭЦҚ-сы болып шығады.

ЭСҚ-ны тексеру үшін хабар алушы M мәтінді қабылдаған кезде қайтадан m=¿(M) хэш-функциясын есептейді. Содан соң жіберушінің ашық кілті көмегімен хэш-функцияның есептеп табылған m мәнінің алынған қолтаңбаға сәйкестігі тексеріледі.

ЭСҚ жүйесінде пайдаланушының құпия кілтін білмей оның ЭЦҚ-сын қолдан(жалған) жасауға мүмкіндік жоқ екендігін атап кетуге болады.

Әр қолтаңбада мынадай ақпарат болады:

- қол қойылған дата;
- осы қолтаңба кілтінің жарайтын мерзімінің аяқталу уақыты;
- Файлға қол қойған адам туралы мәлімет (аты-жөні, қызметі, жұмыс орнының қысқаша аты);

- қол қоюшының ұқсастырғышы (ашық кілттің аты);
- цифрлық қолтаңбаның өзі [11].

- **Криптографиялық протокол**

Протокол — бұл қадамдар тізбегі, олар бір тапсырманы шешу үшін екі немесе бірнеше жақтардың санын иеленіп алады. Ескертетін жағдай, барлық қадамдар тұрақты тізбектелген тәртіп бойынша алынады, сондықтан оның біреуі екіншісі аяқталмағанша басталынбайды.

Сонымен қатар кез келген протокол екі жақтың қатысуын болжайды. Жалғыз болып, бір коктейльді жасап, ішуге болады, ал протокол үшін міндетті түрде екі адамның қатысуы қажет. Сондықтан протокол үшін өзіңіздің жасаған коктейліңізді сіз біреуге дәмін тату үшін беруіңіз керек, себебі коктейльдің жасалуы және дәм тату әрекеті сіздің нақты протоколыңызға айналады. Және нәтижесінде протокол міндетті түрде кез келген мақсатқа жету үшін арналған, егер де оның ондай мақсаты болмаса, онда протоколыңыз жай құр уақыт өткізу болып шығады.

Протоколда сонымен қатар басқа да ерекше белгілері болады:

- протоколдың әрбір қатысушысы алдын-ала жасайтын қадамдары туралы білуі керек;
- протоколдың барлық қатысушылары оның ережелерін еркін, ешбір күшсіз жасауы керек;
- протокол міндетті түрді бірмәнді баяндауда болуы керек, ал оның қадамдары нақты анықталып, дұрыс емес ұғынуды тудырмау қажет;
- протокол қатысушылардың оны жүргізу кезінде туатын кез келген жағдайға туатын сезімін көрсетуі керек. Яғни, басқаша айтсақ, протокол кез келген жағдай туындаған кезде сол уақытта қатысушының жасайтын әрекетін алдын-ала анықтап көрсетуі қажет.

Криптографиялық протокол дегенеміз негізінде криптографиялық алгоритм болатын протоколды атаймыз. Бірақ та криптографиялық протоколдың мақсаты тек ақпаратты басқалардан жасырын, құпия түрінде сақтау әрекеті ғана болмайды. Криптографиялық протокол қатысушылары жақын достар болуы мүмкін, оларда әрине бір-бірінен ешбір құпия болмайды немесе керісінше қатысушылар ретінде бір-бірімен ымырасыз күресте

болатын және бір-біріне белгілі бір санды айтқысы келмейтін жаулар да болуы мүмкін. Бірақ та оларға ортақ келісімшартқа өз қолтаңбаларын қою керек немесе өз тұлғасын дәлелдеп анықтап алу керек. Бұл жағдайда криптография тек бөтен бетпен жасырын тыңдауды алдын алуға немесе анықтау үшін қажет, сонымен қатар алаяқтылыққа да жол берілмейді. Сондықтан криптографиялық протокол оның қатысушылары осы протокол бойынша рұқсат етілмейтін немесе анықтауға жол берілмейтін жағдайларда қажет болады.

*Криптографиялық протоколдар не үшін қажет.*Күнделікті өмірде біз әрбір қадамда протоколдарға тап боламыз – кез келген ойындарды ойнағанда немесе дүкенде заттарды сатып алғанда, немесе сайлауда дауыс беріп жатқанда. Көптеген протоколдарды қолдануды біздерді ата-аналарымыз, мектеп оқытушылары және достарымыз үйретті. Басқа қалғандарының қолдану тәсілдерін біз өздігімізше үйрендік.

Қазіргі таңда адамдар бір-бірімен көбіне компьютерлер арқылы қатынас құрайды. Компьютерлер болса адамдарға қарағанда ешқашан мектепке бармады, олардың ата-аналары жоқ, содан басқа компьютерлер адамсыз еш жаңа нәрсені ұғынып біле алмайды. Сондықтан компьютерлерді адам сияқты ойламайтындай белгілі бір әрекеттерді жүзеге асыру үшін қалыптанған протоколдармен жабдықтау қажеттілігі туды. Мысалға, егер де дүкенде кассалық аппарат болмаса да, сіз кез келген затты сата аласыз. Ал протоколдың ондай үлкен мөлшердегі өзгерісі компьютерді тұйыққа тіреліп тастайды.

Бір-бірімен көзбе-көз сөйлесіп жатқан адамдардың қолданатын протоколдардың көбісі өздерін жақсы жақтан көрсете білді, себебі бұл протоколдар көмегімен олар тікелей қатынас құрай алады. Компьютерлік желі арқылы басқа адамдармен жасалатын қарым-қатынас, керісінше, жасырын болуды болжайды. Сіз бөтен адаммен преферанс ойынын ойнайсыз ба, егер оның карталарды қалай таратып, колоданы араластыратынын көрмесеңіз? Ақшаны білмейтін адамға беріп, оған дүкеннен бір затты алуға тапсыра аласыз ба? Сіз өзіңіздің сайлау парағыңызды пошта арқылы жібере аласыз ба, егер ондағы жасайтын адамдардың оны көріп, соған өз көзқарастарын қоятынын білсеңіз? Менің ойымша, осы сұрақтардың бәріне жоқ деп жауап бересіз.

Компьютерді күнделікті пайдаланатын қолданушылар кездейсоқ адамдардан адалды болатынына сену орынсыз болып саналады. Осының бәрі желілік администраторларға да, компьютерлік желілер жобалаушыларға тиісті болып табылады. Олардың көбісі шынымен де әділ, бірақ та кейбіреулер сізге үлкен көңілсіз жағдайларды тудыруы мүмкін. Сондықтан олардан қорғану үшін және олардың әрекеттерін алдын-алу үшін криптографиялық протоколдарды қолдану қажетті болып саналады.

Рөлдердің үлестірілуі. Протоколдардың сипаттамасы мәнді түрде көрнекті болуы үшін олардың қатысушыларының аттары болуы керек, бұл аттар олардың рөлін көрсетіп

анықтауы керек. Антон мен Борис барлық екі жақты протоколдарға белсене қатысады. Көбіне Антон протоколмен анықталған қадамдарды бастаса, Борис жауап ретінде әрекеттерді жүзеге асыруды бастайды. Егер де протокол үш немесе төрт жақты болса, онда сәйкес рөлдерді Владимир мен Георгий атқарады.

*Арбитраждары бар протоколдар.*Арбитр ретінде протоколдың істеріне, негіздеріне қызықпайтын қатысушылар болады, оларға көбіне басқа протокол мүшелері еш күмәнсіз сеніп, протоколдың келесі қадамын аяқтау үшін алуан түрлі әрекеттер жасайды. Яғни, арбитрда кез келген немесе белгілі бір мақсатты жету сияқты қызығушылығы болмайды, сондықтан ол кез келген осы қатысушы жағына өте алмайды. Протокол қатысушылары арбитрдің барлық айтқанына және жасағанына күмәнсіз сеніп, оның айтқандарын бәрі жасайды.

Күнделікті өмірде тұратын және жүргізетін протоколдардың арбитрі ретінде адвокат алынады. Бірақ та арбитрі адвокат болатын осындай протоколдарды компьютерлік желіге ауыстыру әрекеттері мәнді тосқауылдарға тап болады:

- Егер де адвокаттың беделі дақ түспеген әйгілі болса, онда онымен жеке контакт орнатып, оған сену оңай болады. Бірақ та егер де протоколдың екі қатысушысы бір-біріне сенбесе, денелік қаптамаға оранбаған және компьютерлік желінің бір аймағына тиісті болатын арбитр сенімді болмай, үлкен күмән тудырады.
- Адвокатпен көрсетілетін қызметтерге төленетін бағалар бәрімізге белгілі. Компьютер желісіндегі адвокатқа ұқсас арбитр қызметін кім және қалай төлейді?
- Арбитрді кез келген протоколға енгізу осы протоколды жүзеге асыру уақытына кететін мерзімнен ұлғая түседі.
- Арбитр протоколдың әрбір қадамына бақылау жүргізгесін, оның күрделі протоколдарға қатысуы осы протоколдарды жүзеге асыруы кезінде тар аймаққа айналуы мүмкін. Сәйкес арбитрлердің көбеюі осы тар аймақты алып тастауға көмектеседі, бірақ та онымен бірге протоколды жүзеге асырудың шығындары да өседі.
- Протоколдың қатысушылары бір арбитрдің қызметін пайдаланатындықтан, оларға зиян келтіргісі келетін зиянкес әрекеттері бастысы осы арбитрға қарсы бағытталады. Сәйкесінше, арбитражы бар протоколдағы қатысушылар тізбегінде арбитр әлсіз бөлшек болады. Айтылған кемшіліктерге қарамастан арбитражы бар протоколдар практика жүзінде кең қолданылады.

*Төрешілігі бар протокол.*Арбитр қатысатын протоколда арбитражға кететін шығынды азайту үшін протокол екі бөлікке бөлінеді. Бірінші бөлік арбитражы жоқ қарапайым протоколға сәкес келсе, ал екіншісіне қатысушылар арасында қайшылық пайда

болғанда жүгінеді. Жанжалдарды шешу үшін арбитрдің ерекше түрі қолданылады, олар – төрешілер. Арбитр сияқты төрешілер протоколдың мүддесіне қызықпайтын адам болады да, протокол қатысушылары оған мінсіз сенеді. Бірақ та арбитрға қарағанда төреші протоколдың әрбір қадамын бақыламай, оған жауап бермейді.Төреші қызметіне тек протоколдың жасаған әрекеттерінің жүзеге асырылуы кезінде туатын күмән кезінде ғана жүгінеді. Егер де протокол қатысушылары арасында ондай күмән тумаса, онда төрешіліктің де қажеті болмайды.

Компьютерлік протоколдарда төрешілік болған жағдайда тексеруге келетін мәліметтер болады, оларды тексерген кезде үшінші тұлға протоколға қатысушылардың қайсысы әділ әрекет жасап, ал қайсысы алдағанын біле алады. Төрешілігі бар жақсы протокол сонымен қатар нақ қайсы адамның әділ емес әрекет жасап жатқанын көрсетеді. Осының бәрі осындай протоколдың қатысушылары жағынан жасалатын алауыздыққа қарсы күшті ескертетін құрал болуына себепкер болады.

*Өзін-өзі бекітетін протокол.*Өзін-өзі бекітетін протокол протоколдың әрбір қадамын аяқтау үшін арбитрдің болуын қажет етпейді. Сонымен қатар жанжалдық жағдайларды шешу үшін төрешіні де талап етпейді. Өзін-өзі бекітетін протокол құрамындағы мүшелердің біреуі алауыздық әрекеттер жасап бастаса, қалғандары соны біліп, протоколдың басқа қадамдарын жасауды тоқтататындай ғып ұйымдастырылған. Әрине, өмірдің кез келген талабына сай әмбебап өзін-өзі бекітетін протокол болса барлығымызға да жеңіл болар еді. Бірақ та практика жүзінде әрбір нақты жағдайға сәйкес өзін-өзі бекітетін протоколды жасау қажеттілігі туындайды.

*Протоколға жасалатын шабуылдардың алуан түрлілігі.*Протоколға жасалатын шабуылдар оларда жүзеге асырылатын криптографиялық алгоритмдерге, протоколды жүзеге асыру үшін қолданылатын криптографиялық тәсілдерге, сонымен қатар протоколдардың өздеріне де қарсы бағытталады. Алдымен, қолданылатын криптографиялық алгоритмдер мен тәсілдер төзімді деп болжайық та, протоколдарға қарсы бағытталатын шабуылдар жайлы қарастырайық.

Протокол қатысушысы болмайтын кез келген тұлға қатысушылар алмасатын ақпаратты естіп алуға тырысады. Бқл протоколға жасалатын бейтарап шабуыл, оның осылайша аталу себебі шабуылшы (оны Петр деп атайық) алмасатын деректерді жинап, қадамдардың өту барысын ғана бақылайп, оған еш әсер ете алмайды. Бейтарап шабуыл шифр мәтіні белгілі криптосараптамалық шабуылға ұқсайды. Себебі протокол қатысушыларында олар бейтарап шабуылдың объектілеріне айналғанын көрсететін сенімді жабдықтары болмайды да, қорғану үшін бейтарап шабуылдың жағымсыз нәтижелерін анықтап тауныдың орнына алдын алатын протоколдар қолданылды.

Шабуылшы протоколға өз пайдасы үшін алуан түрлі өзгерістерді енгізе алады. Ол өзін протокол қатысушысы ретінде көрсете алады, протокол қатысушылары алмасатын

хаттамаларға өзгерістер енгізе алады, көмпьютерде сақталған және протокол қатысушыларымен шешімдерді шешкен кезінде қолданатын ақпаратты ауыстыра алады. Бұл белсенді шабуыл болып табылады, себебі шабуылшы (оны Зиновий деп атайық) протокол қатысушылары жасайтын әрекеттер қадамдарына араласып, оларды ауыстыра алады. Сонымен, Петр протокол қатысушылары жайлы максимум ақпарат жинауға тырысады. Ал Зиновийде оған қарағанда басқа қызығушылықтары болады – компьютерлік желінің өнімділігін нашарлату, оның ресурстарына қорғалмаған қолжетімділікті иеленіп алу, компьютерде сақталған деректер қорына өзгерістер енгізу.

Сонымен қатар Петр мен Зиновий барлық жағдайда да бөтен адам бола бермейді, Олардың арасында жарияланған қолданушылар, жүйелік немесе желілік администраторлар, программалық қамтаманың әзірлеушілері, сонымен қатарөздерін адал емес ұстайтын немесе протокол заңдылықтарын сақтамайтын протоколдың тікелей қатысушыларының бірі болуы мүмкін. Соңғы жағдайда шабуылшы зиянкес деп аталады. Бейтарап зиянкес протоколмен анықталған барлық ережелерді сақтап әрекет етеді де, осы протоколдан тыс басқа қатысушылар туралы артық ақпарат алуға тырысады. Белсенді зиянкес протоколға еркін өзгерістер енгізеді де, әділ емес жолмен өзіне көп пайда табуға тырысады.

Протоколды бірнеше белсенді зиянкестерден қорғау әрекеті өте күрделі процесс болып табылады. Бірақ та кейбір жағдайлар кезінде бұл процессті шешуге болады, ол үшін протокол қатысушыларына белсенді алауыздықты анықтау мүмкіндігі беріледі. Ал бейтарап алауыздықтан қорғау әрекетін оның қатысушылары қай жағдайда да болса кез келген протокол беруі керек [12].

1.4 КРИПТОГРАФИЯДАҒЫ КІЛТТІҢ РӨЛІ

Рұқсат берілмеген қолжетімділіктен қорғау мақсатында ақпараттың түрлендіру процесі шифрлеу деп аталады. Шабуылшыға жіберілетін хаттамалардан ақпаратты алуға жол бермеу үшін байланыс каналы арқылы қорғалатын ақпарат емес, оның түрлендірілген түрі жіберіледі.

Криптографияда шифр ретінде әдетте шифрлеу алгоритмін қарастырады. Егер де құпия болып ақпаратты қорғаудың түгел алгоритмі саналса, онда оның жариялануы дереу бүкіл жүйенің құлдырауын туындатады. Жақсы шифрдің (алгоритм) өмір уақытын ұлғайту үшін және көп санды хаттамалардың жасырыну әрекеттерінде қолдану үшін

шифрға кілт енгізеді, мұндағы кілт дегеніміз – нақты бір хаттаманы шифрлеу үшін қолданылатын шифрдің айнымалы элементі. Оның негізінде шифрленген мәтін бастапқыға немесе керісінше түрлендіріледі. Мысалға, Сцитала шифрінде сциталаның диаметрі кілт ретінде алынды, ал Цезарь шифрінде кілт ретінде ашық мәтін әріптеріне қатысты шифрленген мәтін әріптерінің ығысу шамасы алынды.

Егер де шабуылшы шифрді ашып, қорғалатын ақпаратты оқып жатса, онда кілтті өзгертіп, шабуылшының әрекеттері еш әсер бермейтіндей ғып тастауға болады.

Яғни, осы айтылғанның бәрі қорғалатын ақпараттың негізгі қауіпсіздігі кілтке тәуелді екенді дәлелдеп тұр. Шифрдің өзі немесе шифрлеу алгоритмі, шифрмашинаның өздері шабуылшыға белгілі болып, оқытылуға берілсе де, оларда шабуылшыға белгісіз болып қала беретін кілт болады да, ол ақпараттың қолданатын түрлендірулерін бақылап, олар оған тәуелді болады.

Енді заңды қолданушылар шифрленген хаттамалармен ортақ қолжетімді байланыс каналы арқылы алмаса алады. Ал жасырын құпия канал тек кілттермен алмасу үшін ғана қолданылады. Бұл салыстырмалы түрде жұмысты жеңілдетеді, себебі оған берілетін жүктеме азаяды. Ал криптосараптамашы үшін жаңа тапсырма белгіленді – кілтті анықтап, сол арқылы оның негізінде барлық шифрленген хаттамаларды оқу [1].

1.5 КРИПТОЖҮЙЕНІҢ ТӨЗІМДІЛІК МӘСЕЛЕСІ

Шифрді ашу (бұзу) — қолданылған шифрді білместен шифрленген хаттамадан қорғалатын ақпаратты алу процесі. Шифрді ашу әрекетін шифрге жасалынатын шабуыл деп атайды.

Шифрдің алуан түрлі шабуылдарға қарсы түру қабілеті шифрдің төзімділігі деп аталады. Шифр төзімділік ұғымы криптография ғылымныда өзекті және негізгі болып табылады.

Криптография дамуында маңызды болып К.Шенонның абсолютті төзімді шифрдің болуы туралы жасаған қорытындысы саналады. Мұндай шифрдің жалғыз түрі ретінде бір рет қолданушы таспасы алынады, мұнда ашық мәтін бірдей ұзындықтағы кездейсоқ кілтпен «бірігеді». Бірақ та абсолютті түрде төзімді шифр өте қымбат және тиімді емес болып табылады.

Әрине, заңды тұлғалар көбіне өз ақпараттарын қорғау үшін абсолютті емес дәрежеде төзімді шифрлерді қолданады. Мұндай шифрлер көбіне, теориялық түрде, ашылып, оқылуы мүмкін. Ең маңызды қойылатын сұрақ: шабуылшыда сәйкес алгоритмдерді ашып, жүзеге асыру үшін күші, қаражаты және уақыты жетеді ме? Әдетте бұл сұрақты былайша көрсетеді: шектелмеген ресурстары бар шабуылшы кез келген абсолютті емес төзімді шифрді аша алады.

Көп ғасырлар бойы ғалымдардың арасында шифрлердің төзімділігі туралы және абсолютті төзімді шифрді құру мүмкіндігі туралы даулар туындап жүрді. Кибернетика әкесі Норберт Винердің айтуы бойынша: «Кез келген шифр оның қажеттілігі керек болса және қажетті ақпарат шығындалған ақшаны, күшті және тырысуларды өтеген жағдайда ашылып, оқылана алады...»

Олай болатын болса заңды қолданушы бұл жағдайда шифрді таңдау үшін қандай әрекеттер жасауы керек? Әрине, кез келген шабуылшы таңдалған шифрді айтарлық 10 жылда аша алмайтынын дәлелдеп, шифрдің төзімділік дәрежесін жоғары етіп көрсету жақсы болар еді. Бірақ та, өкінішке орай, математикалық теориялар керекті теоремаларды әлі ойлап тапқан жоқ — олар есептердің есептеу қиындығының төменгі бағаларының шешілмеген мәселесіне жатады.

Сондықтан қолданушыда жалғыз ғана жол қалады — төзімділіктің тиімді бағаларын иеленіп алу. Бұл жол бірнеше кезеңдерден тұрады:

- нақты қандай шабуылшыдан ақпаратты қорғау керектігін анықтап, мұқият түрде түсініп алу керек; шабуылшы шифр жүйесі туралы не білгенін және қандай деңгейде білгенін анықтап алу керек, сонымен қатар шабуылшы шифрді ашу үшін қандай мөлшерде күштерді және жабдықтарды жұмата алатынын анықтау керек;
- ойша шабуылшы жаққа шығып, оның позициясынан шифрді шабуылдауға тырысу, яғни шифрді ашудың алуан түрлі алгоритмдерін әзірлеу; және де бұл уақытта максималды түрде шабуылшы күшін, жабдықтарын және мүмкіндіктерін модельдеу керек;
- әзірленген алгоритмдердің ішіндегі ең жақсысы болып шифрдің практикалық бағасын жасау болып табылады [9].

Бұл жағдайда иллюстрация үшін шифрді ашатын екі қарапайым тәсіл туралы айтып кеткен пайдалы: кілтті кездейсоқ анықтап алу (бұл тәсілдің жүзеге асырылуының ықтималдығы кішкентай, бірақ та оның қиындығы аз дәрежеде болады) және барлық кілттердің нақты керекті кілтке дейін іріктеп алыну тәсілі (ол көбіне жүзеге асырылады, бірақ та оның қиындығы үлкен дәрежеде болады). Тағы ескертетін жағдай: кілтке жасалатын шабуыл әрқашан қажетті бола бермейді: кейбір шифрлер үшін кілтті білмей, шифрленген мәтін арқылы ашық кілтті бастапқы күйіне келтіруге болады.

Сонымен, нақты шифрдің төзімділігі оны ашу үшін қолданылатын алуан түрлі әрекеттер жолымен бағаланады да, шифрді шабуылдайтын криптосараптамашылардың квалификациясына тәуелді болады. Ондай процедураны кейбір кездері төзімділікті тексеру деп атайды. Криптотөзімділіктің бірнеше көрсеткіштері болады, оларға: барлық мүмкін кілттердің саны; криптосараптамаға қажетті болатын орташа уақыт.

Шифр төзімділігін тексеру үшін маңызды дайындау кезеңі ретінде шабуылшы шифрлерді шабуылдайтын барлық мүмкін болатын мүмкіндіктердің ойлану әрекеттерін алуға болады. Шабуылшыда осындай мүмкіндіктердің пайда болуы әдетте крипографияға тәуелсіз болады, бұл белгілі бір шамадағы сыртқы сыбыр болып, шифр төзімділігіне әсер етеді. Сондықтан шифр төзімділігінің бағалары көбіне осы бағалар алынған жағдайдағы шабуылшының мақсаттары мен мүмкіндіктерінен тұрады.

Жалпы жағдайда жүйенің барлық төзімділік бағалары зиянкеске қолданылатын шифр белгілі деген болжау кезінде жүргізілуі керек. Яғни, көбіне шабуылшыға шифрлеу алгоритмі белгілі деп саналады және онда хаттаманы оқитын мүмкіндіктері бар деп болжанады. Шабуылшы сонымен қатар ашық мәтіндердің кейбір сипаттамаларын біледі, мысалға, хаттамалардың ортақ тақырыбын, олардың стилін, кейбір стандарттарын, форматтарын және т.б. сипаттамаларын біледі [13].

- **Криптожүйелерге қойылатын талаптар**

Деректердің криптографиялық түрлендіру процесі программалық та, аппаратты түрде де жүзеге асырыла береді. Аппаратты жүзеге асырылу қымбат болып табылады, бірақ та оның артықшылықтары да көп: жоғары өнімділік, қарапайымдылық, қорғану дәрежесі және т.б. Программалық жүзе асыру салыстырмалы түрде үнемдірек және қолдану кезінде икемдірек болып табылады.

Криптожүйелерге қойылатын талаптар:

- Шифрленген хаттама тек кілт қолданылғанда ғана оқылуы керек.
- Шифрлеу кезіндегі қателер ақпараттың жоғалуын тудырмау керек.
- Қолданылған кілтті анықтау үшін керекті операциялардың саны шифрленген мәтіннің үзіндісі бойынша және оған сәйкес келетін ашық мәтіннің үзіндісі бойынша барлық мүмкін кілттердің санынан аз болмауы қажет.
- Барлық мүмкін болатын кілттерден керекті кілтті анықтау үшін жасалатын

іріктеу жолымен дешифрлеуге керекті операциялардың саны қатаң астыңғы шекараға ие болуы керек және заманауи компьютерлердің мүмкіндіктер шегінен кетпеуі керек (желілік мүмкіндіктерді ескере отырып).

- Шифрлеу алгоритмдерін білу жүйенің сенімділігіне әсер етпеуі керек.
- Кілттің үлкен емес өзгерістері шифрленген мәтіннің мәнді өзгерісін тудыруы керек.
- Шифрлеу алгоритмінің құрылымдық элементтері тұрақты болып қалуы керек.
- Хаттаманың ішіне енгізілетін қосымша биттер шифрлеу процесі кезінде толығымен және сенімді түрде шифрленген мәтінде жасырынуы керек.
- Шифрленген мәтіннің ұзындығы ашық мәтіннің ұзындығына тең болуы керек.
- Кілттер арасында шифрлеу процесінде тізбектеп қолданылатын қарапайым және жеңіл орнатылатын байланыстар болмауы қажет.
- Мүмкін болатын сандардың жиынынан алынатын кез келген кілт ақпараттың сенімді қорғалуын қамтамасыз етуі керек.
- Алгоритм аппаратты да, программалық та жүзеге асырылуды да қамтамасыз етуі керек және де кілт ұзындығының өзгеруі шифрлеу алгоритмінің сапалық нашарлауын тудырмау қажет [1].

- **Хештеу тәсілдері**

Хештеу – ақпарат сақталу үшін оны шифрлеу тәсілдерінің бірі. Көбіне хештеудің алуан түрлі тәсілдеріне әр түрлі жүйелерде парольдерді шифрлеу әрекеттері жатады. Мысалға, Linux, Windows XP/NT/2000/ME, FreeBSD, OpenBSD және т.б. операциялық жүйелерде; алуан түрлі форумдарда, қонақ кітаптарында, админкаларда және т.б. – хештеу тәсілдерімен қорғалған желідегі парольдерді көп кездестіруге болады. Парольдерді хештелген түрде сақтаған тиімді, себебі жүйенің паролін ашық түрде ұстау, әрине, бұл ақымақтың ісі болып табылады. Сонымен қатар хештер ашудан қорғалған және төзімді деп саналған, сондықтан оларға сенімді крипто қорғау жүйесі ретінде қатты сенді. Сондықтан барлық парольдер хеште сақталады. Бұл сұрақ бізді тек ақпарат қауіпсіздігі жағынан қызықты болғасын, алгоритм неге негізделетінін және хештеу тәсілдерінің бір-бірінен айырмашылығы неде екенін қарастырайық. Хештеу процесінің мәні кез келген құпия мәтіндік ақпарат (көбіне парольдер) бірнеше мөлшері бірдей бөлшектерге (сегмент) бөлінетініне негізделеді. Бөлінуден кейін бұл сегменттер бір-

бірінен тәуелсіз хеш-функциясы арқылы шифрленеді, мысалға, нақты бір сегментке биттеліп (ақпараттың әрбір битіне) кездейсоқ бит мәндері жазылады[28]. Егер де түсінбесеңдер, қарапайымдырақ айтсақ – пароль бөліктерге бөлінеді де, әрбір символға, пробелдарды да санаймыз (яғни, бөліктің әрбір битіне) кездейсоқ символдардың жиыны қосылып жазылады. Бұл жалпы түсінікте осы түрде орындалады. Енді хештеу тәсілдерін жеке-жеке қарастырайық.

Қазір мен ең негізгілер атап өтемін:

- DES/Triple DES
- AES
- RSA
- MD4/5 , SHA

DES. (Data Encryption Standart) стандартын 1977 жылы АҚШ-тың ұлттық стандарттар бюросы жарияланған [Романец].

DES алгоритмінің негізгі жағымды жақтары:

- ұзындығы 56 бит болатын бір ғана кілт пайдаланылады;
- DES стандартына сәйкес болатын программалардың бір дестесінің көмегімен хабарларды шифрланған соң, осы стандартқа сәйкес кез келген шифрды ашу программалар дестесін пайдалануға болады;
- алгоритмнің қарапайымдылығы өңдеудің жоғары шапшаңдығын қамтамасыз етеді;
- алгоритмнің жеткілікті түрдегі криптоберіктілігі.

DES алгоритмі орын ауыстыру мен ауыстырулар қисындасуын пайдаланады. DES 64-биттік кілт көмегімен 64-биттік деректер блогын шифрлауға мүмкіндік береді. Кілттегі 8 бит — жұптылықты бақылауға арналған тексеру биттері болып табылады. Шифрды ашу — шифрлауға кері операция болып табылады.

*AES(Advanced Encryption Standard).*1997 жылы АҚШ – тың Ұлттық стандарттау және технология институты (NIST – National Institute of Standarts and Technology) жаңа блоктық шифрлау алгоритмінің стандартына ашық конкурс жариялады. Бұл конкурстың жүлдегері шифрлаудың жаңа стандарты AES (Advanced Encryption Standart) статусын алып, АҚШ территориясында пайдалануға ұсынылатын болған.

Жаңа криптостандартқа қойылатын негізгі талаптар – алгоритмнің мәліметтер блогының ұзындығы 128 бит болу керек және кілттің 128, 192 мен 256 бит ұзындығын қолдау керек.

*RSA*алгоритмін 1978 жылы үш автор ұсынған: Р.Райвест (Rivest), А.Шамир (Shamir)

және А.Адлеман (Adleman). RSA алгоритмі ашық кілтті алгоритмдердің біріншісі болып саналады. Ол деректерді шиФрлау режімінде де, электрондық циФрлық қолтаңба режімінде де жұмыс істей алады.

Алгоритм сенімділігі үлкен сандарды жіктеу қиындығы мен дискретті логариФмдерді есептеу қиындығына негізделген.

MD4 алгоритмінде мәтінді 512 модуль бойынша 448 битке тең ұзындыққа дейін толықтыру, мәтіннің 64-биттік көрсетімдегі үзындығын қосу және 512-биттік блоктарды Damgard-Merkle процедурасымен өңдеу көзделген. Бұл алгоритмде әрбір блок әр түрлі үш циклға қатысады.

MD4 алгоритмінде біраз кемшіліктер табылған соң ол MD5 алгоритмімен ауыстырылған. Бұл алгоритмде енді әрбір блок әр түрлі (үш емес) төрт циклға қатысатын болды.

MD5 хэштеу фнкциясын қысқаша қарастырайық [Баришев]. µзындығы b бит хабар бар деп есептейік. Мұнда b — кез келген теріс емес бүтін сан. Хабардың биттері m_0,m_1, ..., $m_{(b-1)}$ тәртіпте жазылатын болсын.

Хабардың үйірткісін (орамын) есептеу үшін мынодай бес қадам орындалады:

- Толтыру биттерін толықтыру. Хабар оның ұзындығы 512 модул бойынша 448-бен салыстырмалы болатындай етіліп толықтырылады (кеңейтіледі). Толықтыру былайша жүргізіледі: хабарға алдымен бірге тең 1 бит қосылады, ал қалған биттер нөлмен толтырылады. Сонымен, қосымша биттердің саны 1¸512 аралығында болады.
- ұзындығын толықтыру.
- үірткінің арашығын (буфферін) инициализациялау.
- Хабарды 16-сөздік блок-блокпен өңдеу.
- Шығу. Хабардың үйірткісі A, B, C, D регистрларында сақталады, яғни А-ның кіші байтынан басталып D-ның үлкен байтына дейін орналасады.

*SHA алгоритмі.*Қауіпсіз хэштеу алгоритмі SHA (Secure Hash Algorithm) АҚШ-та 1992 жылғы SHS (Secure Hash Standard) қауіпсіз хэштеу стандартықұрамында жасалған. SHA хэштеу алгоритмі DSA цифрлық қолтаңба алгоритмімен бірге пайдалануға арналған.

Ұзындығы 2^{64} биттен кем M хабарды енгізгенде SHA алгоритмі 160 биттік шықпа хабарын жасап шығарады. Ол хабардың дайджесті MD (Message Digest)деп аталады. Содан соң хабардың дайджесті DSA алгоритмінің кірмесіретінде пайдаланылады. DSA алгоритмі M хабарының цифрлық қолтаңбасын есептеп шығарады. Хабардың дайджесті хабардың өзіне қарағанда қысқа болғандықтанцифрлық қолтаңбаны хабардың дайджесті үшін қалыптастыру қол қою процесінің тиімділігін арттырады [9].

- **Ұялы байланыс жүйелерінің аппараттық іске асырылуы**
- **Ұялы байланыс жүйесінің тарихы**

*Ұялы желілерді құру.*Қазіргі заманғы ұялы байланыс жүйелері бұрынғы транкілік байланыс стандарттарының принциптеріне негізделіп жасалған. Транкілік хаттамаларды пайдалануға берген кезде абоненттердің саны көп үлкен аумақта жүйенің жұмысын қамтамасыз ету мәселесі туды. Транкілік стандартта жұмыс жасайтын құрылғы, дыбыстық ақпараттан бөлек, үлкен көлемде сервистік (қолданушының растайтын ақпарат, ретранслятор жұмыс жасауы үшін пилот-тон) мәліметті жібереді. Транкілік желіде қуаттылығы үлкен қайталағыштар қолданылады.Сигналдың жақсы жүрісін тек қайталағыш-станция жолы арқылы жүщеге асыруға болады. Сигналдың кері жүрісі кезінде қайталағыштан үзаған сайын нашарлайды. Бұл мәселені шешудің бірнеше нұсқасы ұсынылған болатын, олардың ішінде қуаттылығы төмен, бір желіге біріктірілген, белігілі бір аймақта жататын бірнеше қайталағыштарды орнату. Осындай қайталағыштардың біреуін ашу барысында қолданушылық радиостанция тек соларға ғана қызмет ететін, ал одан алыстаған сайын қолданушыға байланысты қайтадан орнату керек болады. Мұндай сұлба басқаруды эстафеталық түрде ұйымдастыра алмады. Кейіннен жетілген қайталағыштардың желісі орнына қабылдағыш желісін орнату шешілді. Олар бір-бірінен алыс емес қашықтықта орналасқан және үлкен аумақты қамтыды және де барлық қабылдағыштар ұқсас сымдармен (өткізгіштермен) байланыстырылды және ретрансляторда орналасқан ортақ коммутаторға жалғанды. Абонент бір қабылдағыштан екінші коммутаторға қозғалатын болса, онда интенсивтілігі жоғары CTCSS-тоны орқылы анықталатын сигнал таңдалады. Ескі транкілік жүйелерде сияқты мұнда да шығу және шақыру сигналдары бір ретранслятордан трансляцияланған, бірақ қуаттылығы жоғары болады [14].

Жүйенің кемішілігі болып қабылдағыш станциялардың бір нүктеде өткізгішьтер

арқылы байланысуы болатын. Егер қабылдағыш қайталағыштан бірнеше шақырым қашықтықта орналасса, онда аралық телефон байланысын қолданған жөн. Желілік транкінің бұл тәсілі икемді болды. Мәскеуде бұл тәсіл арқылы өрт сөндірушілерге арналған байланыс жүйесі жасалды. 1990 ж-да жасалған байланыс әлі күнге дейін бір де бір бұзылған емес. Тура осылай ұялы байланыс желісі де транкілік желіден біршама алды. Негізінен NMT450 стандарты транкілік хаттама арқылы қиындатылды. Ұялы телефонияны жасау барысында бірнеше өз бетімен жұмыс жасайтын қайталағыштарды қолдану шешілді [15]. Өңдеушілер абоненттік құрылғының байланыс сапасын анықтайтын алгоритм жасап, қайталағыштарды басқаруды телефон арқылы бір-біріне беру ақрылы өзара қатынасуға «үйретті». Күшейткіштің аз коэффициентін және жіберу кезіндегі үлкен жоғалтуларды ескере отырып, домалақ диаграммалы антенналардан (GroundPlain) бас тартылды. Оларды кең бұрышты (120о) бағытталған антенналармен алмастырды. Кең бұрышты антенналарды қолдану кезінде қайталағыштардың орналасуы бұрыштарында ретранслятор орналасқан үшбұрышқа ұқсас болатын. Ұялы стандарттардың көптеген санына қарамастан жіберуді басқару алгоритмі бірдей. Байланысты жүргізетін қайталағыш белгілі бір параметрлер (AMPS-тегі SAT, NMT-дегі пилот-тон) арқылы анықталатын байланыс сапасы төмендеген кезде бірнеше қайталағыштарға байланыс сигналын тексеруд тапсырмасын береді. Егер байланыс сигналы қойылған шектен тым төмен болса, онда басқару сигналды бірқалыпты қабылдап отырған қайталағышқа беріледі. Сигнал маршрутизациясының принципі қазіргі заманғы радиорелелық станциялардағы сигналдардың маршрутизациясына ұқсас. Ретранслятордың сымды байланысының қолайсыздығынан өңдеушілер оларды СВЧ түзулері арқылы желіге біріктірді. Осылайша, басқаруды келесі бір қайталағышқа берген кезде ортада телефон-қайталағыш-коммутатор- қосымша буын пайда болады. Басқаруды бірнеше қайталағышқа жіберу кезінде ортада бірнеше қосымша буын пайда болады. Осындай қосымша буындардың шексіз саны пайда бол бермес үшін телефон белгілі бір уақыт аралығында қайталағыштың командасымен өзінің идентификационды кодын жібере отырып, тіркеліп отырады. Кодты алған қайталағыш кейіннен абнентке қызмет етеді. Мұндай операция сөйлесу кезінде де жүріп отыруы мүмкін [16].

*Ұялы байланыстың дамуы.*Ұялы байланыс тарихы қысқаша – бұл принципті қолданған жүйелер 1970-ші жылдардың аяғында шыға бастады. Мобильді байланыстың ұялы мекememен алғашқы ұрпағы ұқсас болды және транкілі жүйелердің тдамытылған түрі болды.

Содан соң, абоненттердің саны өскен сайын FDMA (Frequency Division Multiple Access — (бөлінген каналдар арқылы қол тжетімділік) тәсілдерін қолдану арқылы ұялы байланыс иелерін сапалы байланыспен қамтамасыз ету мүмкін болмады. NMT және AMPS стандартты жүйелерінің орнына жаңа екінші ұрпақ — GSM, DAMPS стандарттары келді [14-15].

Бірінші және екінші ұрпақ ақпаратты жібері жылдамдығы 4,8 және 9,6 Кбит/с болды, бұл жылдамдық тек электронды пошта арқылы хабар алмасуға ғана жеткілікті болатын. Бұндай жылдамдықпен Интернет-сайттарда қолайлы жұмысты ұйымдастыру, видеоны реалды уақытта қосу сияқты жабдықтаумен қамтамасыз ету мүмкін емес. Сондықтан да ұялы байланыстың үшінші ұрпағын өндірушілер мәліметтерді жоғары жылдамдықпен жіберуді қамтамасыз ету жағдайын алдын ала қарастыру керек. Ұялы байланыстың үшінші буынын жасау 1985 ж-дан бері келе жатыр. 1996 жылдан бері IMT-2000 (International Mobile Telecommunication) деп аталатын жұмысшылар тобы UMTS (Universal Mobile Telecommunications System — әмбебап мобильді байланыс жүйесі) стандартты байланыс жүйесін жасап жатыр, диапазоны екі гигагерц шамасында, W-CDMA (Wide band CDMA — CDMA кең диапазонды) технологиясын қолданады, кең сервистік функциялары бар, мәліметті секундына 144 Кбит-тен 2 Мбит-ке дейін жіберу және видеоны орташа сапамен қарауға мүмкіндік береді. Кейбір провайдерлер үшінші буын ұялы байланыс жүйесін енгізбекші. Үшінші буын желілеріне өту үшін бірнеше стандарттар жасалды, құралдарды азғана шығынмен ауыстыру мүмкіндігімен жоғары жылдамдықты TDMA-қызмет жүйесін енгізуден басталды. HSCSD технологиясы (High Speed Circuit switched data) мәліметті жіберу жылдамдығын 38,4 Кбит/с-қа дейін жоғарылатуға мүмкіндік берелді. Дамытылған телнология GPRS (General Packet Radio Service) мәліметтерді 115 Кбит/с жылдамдықпен жібереді. Үшінші буынға өтудің соңғы қадамы болып EDGE (Enhanced Data GSM Environment) технологиясы болды, оның мәлімет жіберу жылдамдығы 384 Кбит/с болды. 2000 жылдың соңына қарай дүние жүзінде ұялы телефон қолданушыларының саны (EMC World Cellular Database деректері бойынша) жер бетіндегі адамзат санының 11% дейін жетті, бұл шамамен 685 млн адам. Кең тараған стандарт – GSM стандарты болды. Екінші орында – жаңа және тез дамып келе жатқан CDMA стандарты, негізінен АҚШ-та көбіне қолданылады. Болжам бойынша тек Еуропада 2005 жылға адамзаттың 60% ұялы телефонды қолданатын болды [17].

- **Ұялы байланыс жүйесінің архитектурасы**

Абоненттердің саны көбеюі және қызмет көрсетудің төмен сапасы ұялы байланыс қызметін ұсынатын өндірушілер сапаны арттырып, олардың жүйелерінде көп қолданушылар санын қолдай алатын жүйе құру керек болатын. Мобильді байланыс үшін спектр жылдамдығы шектеулі болғандықтан, желіде дұрыс жұмыс жасау үшін қажет жылдамдықты тиімді қолдану керек болатын. Қазіргі заманғы ұялы байланыстар калада және ауылдарда белгілі бір принциптерге сай бөліктерге бөлінген. Жаю параметрлері

және сота өлшемі инженермен анықталады. Әрбір аудан үшін қамтама құрамына ұяшықтар, ұяшықтар топтары және жиіліктері кіретін техникалық жоспар бойынша жасалады.

Ұяшық – ұялы байланыс жүйесінің негізгі географиялық бірлігі. Ұялы байланыс термині ұяшық түрдегі облыстан келеді. Ұяшықтарға қамтитын аумақ кіреді.

Ұяшықтар – алтыбұрыш ретінде берілген, кішігірім географиялы аумақыт алып жататын базалық станциялар. Әрбір ұяшықтың өлшемі пейзажға байланысты алынады. Табиғи ландшафтымен салынған және жасанды құрылым сияқты шектеулер үшін ұяшықтардың түрі дұрыс немсе алтыбұрыш [17].

Жиіліктік қайталау. Мобильді жүйелер үшін каналдың радиожиіліктігі шектеулі болғандықтан, инженерлер радиоканалдырды бірлесе қолданып, бірден артық сөйлесуді қамтамасыз ету жолын қарастыру керек болатын. Қабылданған шешімді жиіліктік жобалау немесе жиіліктік қайталау деп атады. Жиіліктік қайталау мобильдік телефонның құрылымдық сұлбасын ұялы түсінігіне қайта өзгерту арқылы жасалды.

Кластер – ұяшықтардың тобы. Каналдар топтардың шегінде қолданылады. Сурет 2 жеті ұяшығы бар кластерді суреттейді.

Сурет 2. Жеті ұяшықтан тұратын кластер.

Жиіліктік қайталануды қолдану ұғымы кішігірім географиялық аумақта қолданылатын радиоканалда әрбір кластердегі ұяшық мағынасына негізделген. Ұяшықтарға алғашқы каналды топты тағайындайды, ол көрші тұрған ұяшықтардан өзгеше болады. Ұяшықтардың қамтитын аумағы із деп аталады. Бұл із шекарамен шектеледі, алғашқы топ басқа да ұяшықтарда қолданылуы үшін, бірақ бір-бірімен қиылыспайтындай(сурет 3 қара).

Сурет 3. Жиіліктік қайталау.

Бірдей санды ұяшықтарда жиіліктер саны да сондай болады. Солай қабылданған, себебі рұқсат етілген жиіліктер саны – 7, жиіліктік қайталануды пайдаланудың факторы – 1/7. Осылайша, әрбір ұяшық рұқсат етілген каналдардың 1/7 бөлігін пайдаланады.

*Жиіліктің бөлінуі.*Көптеген кішігірім аумақты жүйелерді құру экономикалық жақтан

тиімсіз. Бұл қиындықтан өті үшін жүйенің операторлары ұяшықты бөлу идеясын қарастырды.

Қызмет көрсету аймағында қолданушылардың саны көп болғандықтан, бір облысты бірнеше аймаққа бөлу деп қарастырылады. Осылайша, қалалық орталықтар қолданушылардың жүктемесі көпоблысты сапалы байланыспен қамтамасыз ету үшін қажетінше кішігірім аумақтарға бөліне алады. Ал арзандау ұяшықтар бөлек тұрған аймақтарды қамтиды (сурет 4 қара).

Сурет 4. Ұяшықтардың бөлінуі.

*Ұяшықтар арасында ауысу.*Ұялы байланыс жүйесінің дамуындағы соңғы кедергі, бұл абоненттің қозғалуы кезінде бір ұяшықтан екінші ұяшыққа ауысуы. Аралас аумақтар бір жиілікті қолданбағандықтан сұраныс төмендетілуі керек немесе абонент аралас ұяшықтар арасындағы сызықтан өткен кезде бір радиоканал екіншісіне сұраныс жіберуі қажет.

Сұраныстың төмендетілуі мүмкін болмағандықтан, ұяшықтардан өту процессі іске асырылған болатын. Мұнда ұяшықтар арасында жиілікті беру арқылы жасалды, яғни телефондық желі автоматты түрде абонентті бір жиіліктен екінші жиілікке жібереді (сурет 5 қара).

Қоңырау шалынған кезде екі жақ бір телефондық радиобайланыс каналында болады. Қабылдау ұяшықтың бұл бөлігінде төмен болған кезде, жүйе қоңырауды үзбей жаңа жоғары жиілікті каналға ауыстырады.

Сурет 5. Ұяшықтар арасындағы алмасу.

Ауысу кезінде қоңырау жалғаса береді және абонент ұяшықтар арасында аласуды байқамайды [29].

- **Ұялы байланыстың стандарттары**

*AMPS.*Ұялы байланыстың аналогты стандарты AMPS (АМПС) – NMT баламасы. Модификация DAMPS / ADC (ДАМПС), Is-54 және Is-55. AMPS FDMA (Frequency Division Multiple Access — жиіліктік бөліктерге көпшіліктік қол жетімділік) қолданатын, NMT аналогты жүйесіне балама болып келеді. AMPS жүйесінің жұмысының ерекшелікері (соның ішінде қызметтік сигналдың сапасын бақылау көмегімен іске асырылатын әр түрлі базалық станциялар арасында эстафеталық алмасу механизмі) NMT принципіне ұқсас. Ұялы желілердің дамуы және абоненттердің санының өсуі жүйенің өткізгіштік қабілетін дамыту қажет болды. Осылайша NAMPS және DAMPS жүйелері пайда болды [18]. Оның бірінші түрінде бір канал үшін қолданылатын жиіліктер жолағы азайтылды да, каналдар саны болса керісінше көбейтілді, бірақ стандарт сол түрінде қалды. Екінші жүйеде (Digital AMPS — AMPS стандартының сандық модификациясы) TDMA прогрессивті технологиясы (Time Division Multiple Access — уақыттық бөлінуі бар көп санды қолжетімділік) қолданылды, осының бәрі бірнеше абоненттердің бірдей жұмысына қажетті әрбір жиілікті каналды қолдануға мүмкіндік берді. Осыған ұқсас тәсілдеме GSM жүйесінде қолданылды.

AMPS жүйесі стандартты 30 кГц жолақ кеңдігі болатын 666 дуплексттік каналдардан тұрады да, 800 МГц (AMPS/DAMPS) және 1900 МГц (DAMPS 1900) аралығында жұмыс жасайды. Ретрансляциялық негізгі базаның қуаты 45 Вт болады, ұялы станцияның қуаты 12 Вт-тан аспайды, тасылатын телефонның қуаты 0,3 тен 1 Вт аралығында болады. AMPS жүйесінде бағыттылық диаграммалары 120о болатын базалық станциялар қолданылады, олар ұялы ұяшықтардың бұрыштарында орнатылады. Базалық станциялар ертеде ортақ желіге сым (фидерлік) сызықтары арқылы бірікті, бірақ та қазіргі кезде трафик үлкейгесін, оларды жекеленген ЖЖЖ-құралдары көмегімен біріктіре бастады, олар барлық дауыстық трафикті жинап, оны негізгі телефондық комутаторға жібереді. Дауыстық хаттамалардан басқа ЖЖЖ-сызықтары арқылы ретрансляторларды (репитер) басқару үшін серверлік ақпарат жіберіледі. 1990-шы жылдардың өзінде AMPS жүйесіне ұқсас жүйе нұсқалары ескерді: жетпейтін өткізгіштік қабілеті, бөтен тыңдаудан әлсіз қорғау, сервистік функциялардың аз саны. AMPS жүйенің сандық модификацияның сапалы үлгілері 1987 жылдан бастап қолданыла бастады. Сандық байланысқа қойылатын жаңа стандарт 1990 жылы әзірленіп, D-AMPS немесе ADC деп аталды [19]. 1991-1992 жылдары жүйенің үш негізгі типтері ерекшелінді: IS-54 (DAMPS жүйесіне), IS-55 (DAMPS және AMPS жүйелерін қамтамасыз ететін екі стандартты аппаратураға) және IS-56 (базалық станцияларға). Атауына қарамастан IS-54 сандық шешімі болмады, бірақ та оған қарамастан оның қолданылуы байланыс жүйелерінің өткізгіштік қабілетін үш есе көбейтуге мүмкіндік берді. 2001 жылы IS-54 стандартын 2 млн. абоненттен астам адамдар қолданды. 1994 жылы жаңа IS-136 стандарты пайда болды, ол жетілдірілген сандық IS-54 стандартының түрі болып саналды. Бұл стандарт өзінің мүмкіндіктері мен функционалдық қанықтылығы бойынша

еуропалық GSM стандартына ұқсайды және роумингтің мөлдір механизмін қолдайды. Бірақ та ақырындап болса да DAMPS стандартының одан сайын жетілдірілген және прогрессивті GSM стандартына ауысу процесі даму жолында. Ресейде 2000 жылы В России с в связи с тем, что часть диапазона 900 мГц аралықтың бір бөлігі цифрлік теледидар үлесіне берілгесін, радио жиіліктерін бақылайтын Мемлекеттік комиссия D-AMPS аппаратурасына берілетін лицензиялар санын шектеді де, провайдер-компанияларға өз аппаратураларын GSM-1800-ге ауыстыруға кеңес берді. АҚШ мемлекетінде 2001 жылға қарай DAMPS стандарты толығымен ұялы байланыстың цифрлік технологияларымен ығыстырылды, көбіне GSM мен жаңа CDMA стандарты [30].

*CDMA.*CDMA (Code Division Multiple Access — код бойынша бөлінген көпшіліктік рұқсат) – ұялы байланыстың жаңа технологиясы. IS-95 және CDMA PCS CDMA (Code Division Multiple Access — код бойынша бөлінген көпшіліктік рұқсат) ерекшелігі – 800 немесе 1900 МГц диапазонындағы кеңжиекті каналдарды пайдалану негізінде құрылған ұялы байланыстың сандық технологиясы. CDMA технологиясының принциптері 20ғ-дың ортасында жасалды. Бірақ, оның техникалық іске асырылуы тек 1990 ж-ры компьютерлік аппаратураның дамуы мен жасалуы негізінде ғана мүмкін болды. технологиялық жасалуын Qualcomm фирмасы іске асырды. Ең басында бұл технология IS-95 стандарты деп белгілі болды [19]. CDMA қазіргі таңда ұялы байланыстың ең дамыған үші типтің бірі болып саналады (FDMA, Frequency Division Multiple Access — жиіліктер бойынша бөлінуі бар көп санды қолжетімділік және TDMA, Time Division Multiple Access — уақыт бойынша бөлінуі бар көп санды қолжетімділік). CDMA технологиясының артықшылығы ретінде жоғары бөгеуілге қарсы қорғаныш, шағылған сигналы бар мәселелердің болмауы, сотының мүмкін болатын үлкен мөлшері және абоненттердің ең үлкен мүмкін болатын саны. Басқа әйгілі ұқсас жүйелерге қарағанда бұл стандартта абоненттер саны 10-20 есе көбірек, ал цифрлік жүйелермен салыстырғанда — 3-5 есе көп. CDMA кемшіліктеріне базалық станциялардың және ұялы телефонды аппараттардың жоғары күрделігін және бағасын жатқызуға болады. Бірақ та әйгілі GSM мен TDMA-стандартына қарағанда CDMA жүйесінің негізіндегі ұялы байланыс қызметтерінің бағасы төменірек болады [20].

CDMA жүйесінде ұялы байланыстың басқа жүйелеріне қарағанда таржолақты каналдар емес, кеңдігі 1,23 Мгц болатын 55 салыстырмалы түрде кеңжолақты каналдар қолданылады. Ол каналдар 800 МГц (IS-95 стандарты) немесе 1900 МГц (CDMA PCS стандарты) аралығында болады. Пішінделетін сигнал модульденген кездейсоқ цифрлік тізбектегі цифрлік код ретінде болады, яғни сигнал аралық бойымен 1,23 Мгц кеңдігінде жайылады(осыдан технологияның екінші аты шығады — spread spectrum — жайылған спектр).

Бұл жағдайда бір жиілікте бірнеше абоненттердің жұмыс істеуі мүмкін болып табылады. Әмбебап кездейсоқ тізбектілік (CDMA терминдерінде: DS, Direct Sequence —

тура тізбектілік) әрбір «ұялы телефон – базалық станция» тізбегі үшін генерацияланады. Бұл жағдай кезінде қалған сигналдар декодермен декодтауға бөгет болмайтын ақпарат шум ретінде алынады. Мұндай тәсілдеме байланыстың жоғары бөгеуіл қорғанышын жоғарлатуыға мүмкіндіктер береді, себебі CDMA каналына түсетін салыстырмалы түрде таржолақты бөгеуіл сигналға фатальдік залал түсірмейді. Сонымен қатар келісімдердің жысырындылығы да жоғарлайды, себебі осы байланыс протоколы негізінде жүргізілетін әңгімені тыңдау GSM және басқа ұқсас стандарттарға қарағанда салыстырмалы түрде күрделі болып саналады. Кездейсоқ тізбектер өзара ортогональді Уолш функцияларына негізделеді, осының бәрі бір жиілікті каналда бір уақытта 64 абоненттерге дейін жұмыс жасауды қамтамасыз етеді, бұл қабілет TDMA-жүйелеріне қарағанда жоғарырақ болады.

IS-95 стандартындағы ұялы телефон бірнеше базалық станциялармен жұмыс жасауға мүмкіндігі болады, бұл қабілет алуан түрлі базалық станциялардан келетін дестелерден салыстырмалы түрде қатесі азын таңдауға мүмкіндік береді. Бұл принцип soft hand-off (жұмсақ қайта қосу) деп аталады. Базалық станцияға жақын орналасқан ұялы телефондар алыста орналасқан станцияладың сигналын баспау үшін IS-95 стандарттарында телефонның шығатын қуатын басқаратын қуатты және нақты жүйесі қолданылады. Сөйлеуді кодтау үшін деректерді тасымалдауда қолданылатын (8 ден 13 кбитке дейін) сөйлеудің қарқындылығына қатысты өзгеретін кодек қолданылады. Жабдықты синхронизациялау үшін GPS жүйесі қолданылады. Ұялы байланыстың басқа стандарттарына қарағанда CDMA стандарты каналдың өткізгіш жолағы бойынша үлкен қорға ие болады, бұл қабілет ұялы телефонды Интернетте қолдану үшін маңызды болып табылады. Заманауи жүйелер үшін Интернетте қолданылатын стандартты жылдамдық CDMA-телефондары 14,4 кбит болады, бұл жылдамдық теориялық түрде 144 кбитке және одан жоғары болуы мүмкін [30].

*GSM.*GSM (Global Standard for Mobile communications — ұялы байланыстың ғаламдық стандарты). SMS пен WAP қызметтері

GSM — ұялы байланыстың стандарты ортақ еуропалық стандарт ретінде әзірленді. 1982 жылы еуропалық пошталық және телеграфтық қызметтердің Конференцияның бастауымен (Conference of European Posts and Telegraphs, CEPT) дыбысты тасымалдаудың жоғары сапасы болатын, сандық мәліметтерді жіберу мүмкіндігі болатын және роумингті қолдайтын, яғни осы стандарттағы басқа оператор желісі кезінде телефонның жұмысын қолдау, ұялы байланыс жүйесін жасау жұмыстары басталды. Тек 1990 жылы GSM инициативалық топтың әзірлемесінен стандартқа айналды және ол ETSI – ді қолдады (European Telecommunication Standards Institute) [21]. Әзірлеме табысты болып шықты, сол себепті 1990 жылдардың ортасында GSM стандартының операторлар саны ондаған шамаларға жетті, сонымен қатар басында тек Еуропа еліне саналып жасалған стандарт, уақыт өте ол барлық әлем бойынша таралды.

GSM стандарты толығымен де сандық және TDMA / FDMA жүйесінің класы болып

табылады (Time Division Multiple Access / Frequency Division Multiple Access — көптеген қолжетімділік уақыт бойынша / және жиілік бойынша көптеген қолжетімділік). Жүйенің кең таралған үш нұсқасы бар: GSM 900, GSM 1800 (DCS 1800) және GSM 1900 (PCS 1900 нұсқасы Америка Құрама Штаттарында қолданылады), олар бір-бірінен тек қолданылатын жиіліктер аралығы негізінде ғана ерекшелінеді. Көбіне барлық шығарылатын GSM ұялы телефондары екі аралықты қолдайды(900 және 1800 МГц), ал кейбіреулері — барлық үш аралықты да қолдайды [22]. 1800/1900 МГц аралықтары көбіне негізгі қалаларда қолданылады, мұндағы базалық станциялар арасындағы арақашықтық үлкен емес. Стандартта 124 жиіліктік канал қолданылады, олардың әрқайысысында TDMA технологиясы арқылы бір мезетте 8 абонентке дейін жұмыс істей алады. Эфир арқылы жіберілетін ақпарат ашық кілттік код арқылы кодталады. Сөйлеуді кодтау үшін RPE / LTP кодегі қолданылады (Residual Pulse Excitation / Long Term Prediction — қалдық импульстік қозу/ұзақ мерзімді болжау), бұл кодек жақсы сапаны сақтау кезінде кодталған сөйлеудің жіберу жылдамдығын салыстырмалы түрде төмен етуге мүмкіндік береді — 13 кбит/с. GSM стандарттың ұялы телефондары өзінің қуатын базалық станцияға дейінгі арақатынасқа қатысты реттей алады, әдетте қуат 900 МГц диапазоны кезінде екі ватт деңгейінде тұрады, ал 1800 МГц аралығы кезінде бір ватт деңгейінде тұрақталады. Осының бәрі базалық станциядан максималды 35 км-ге дейінгі арақатынаста болатын байланысты сақтауға мүмкіндік береді.
Стандарттың маңызды қасиеттерінің бірі SIM-карта болып табылады (Subscriber Identity Module — абонентті идентификациялау модулі) [23]. SIM-карта контроллері болатын флэш-жад микросұлбасы болып табылады, оған абонент жайлы ақпарат, телефон кітабы, телефон баптауы сақталады. DAMPS немесе NMT стандарттарына қарағанда GSM телефоны SIM-карта болмаса жұмыс істемейді. Ерекшелік ақысыз қызмет болып табылады — құтқару қызметін шақыру. SIM-картадағы контроллер PIN-код (Personal Identification Number — жеке идентифицирленген номір) белгісіз болса, телефонмен жұмыс істеуге рұқсат бермейді. PIN-кодты үш сәтсіз теруден кейін SIM-карта автоматты түрде блокталады. Ұмытшақ абоненттер үшін PUK-код болады (Personal Unblocking Key — жеке блоктаудан шығару кілті), оның енгізілуі PIN-кодты блоктан шығарады. Бірақ та егер де PUK-код он рет қате терілсе, онда SIM-карта толығымен жұмыстан шығарылады.

Ұялы байланыстан басқа GSM стандарты қосымша да қызметтер ұсынады: мәліметтерді тасымалдау жылдамдығы 9600 кбит/с-ке дейін жетеді, дыбыстық пошта, қысқа хаттамалар қызметі (SMS — short message system) және WAP (Wireless Application Protocol — сымсыз қосымшалардың протоколы). SMS — бұл екі жақты пейджер, ол абоненттерге 160 символ ұзындығындағы хаттамаларды жіберуге мүмкіндік береді. SMS-хаттаманы жіберген кезінде жүйе оны адресатқа жіберетін кезеңді де көрсетуге болады. Әрекет жүзеге асырылғаннан кейін жіберуші хаттаманың табысты жеткізілуі туралы хабарлама алады, қарама-қарсы жағдайда кезең аяқталғасын хаттаманың жетпегені жайлы хабарлама түседі. Көбіне келетін SMS хаттамалары тегін болады. WAP-

технология ұялы телефонның экранында кейбір арнаулы Интернет ресурстарын көретін мүмкіндіктер береді. Бірақ салыстырмалы түрде WAP-протоколының қымбаттылығы кезінде ол қолдану жеңілдігімен және Интернет программаларының сәйкес келуімен ерекшелінбейді. 2001 жылы GSM стандаты әлем бойынша кең таралған стандарттардың бірі болып табылады [30]. HSCSD (High Speed Circuit Switched Data) жаңа технологиясы Интернетке қатысты қолжетімділікті 57,6 кбит/с жылдамдығымен жүзеге асыруға мүмкіндік береді, бұл технология кезінде стандарттың әлсіз жерін реттеуге мүмкіндік туғызады — мәліметтерді тасымалдаудың төмен жылдамдығы.

*GSM стандартында хабар алмасу.*GSM стандарты екі қызмет класына ие: негізгі қызметтер және телеқызметтер. Негзгі қызметтер хабар алмасуды дуплексті режимде (асинхронды) жалпы қолданыстағы телефондық линия арқылы 300, 600, 1200, 2400, 4800 және 9600 бит/с жылдамдықпен жіберуді; хабар алмасуды дуплексті режимде (синхронды) телефондық линия, жалпы қолданыстағы (CSPDN) және ISDN коммутацияланған желі арқылы 1200, 2400, 4800 және 9600 бит/с жылдамдықпен жіберуді; жалпы қолданыстағы (PSPDN) коммутацияланған желі арқылы адаптердің көмегімен 300 – 9600 бит/с жылдамдықпен жіберетін асинхронды мәліметтер пакетіне қол жетімділік; 2400 – 9600 бит/с жылдамдықпен хабар алмасатын пакеттерге синхронды дуплексті қол жетімділікті қамтаамасыз етеді [23].

Ақпаратты 9,6 кбит/с жылдамдықпен жіберген кезде әр уақытта толық жылдамдығы бар канал қолданылады. 9,6 кбит/с жылдамдығынан аз жылдамдықпен ақпарат жіберілетін болса, жартылай жылдамдықта каналдар қолданылуы мүмкін. Аталған каналдардың функциялары терминалды қызмет ететін құралдар үшін қарастырылған, оларда МККТТ интерфейстері бар, V.24 немесе X.21 сериялары қолданылады. Бұл спецификациялар әдеттегі телефондық линиялар каналының өткізгіштік қабілетін анықтайды.

Телеқызметтер келесідей қызметтерді көрсетеді:

- Телефондық байланыс (пәтерлер қорғанысы, қауіп сигналы және т.б.);
- Қысқа хабарламаларды жіберу;
- Видеотекс, Телетекст қызметтеріне рұқсат;
- Телефакс қызметі.

Қосымша ерекше қызметтер (шақыртуды жіберу, тарифтік шығын туралы хабарлама, қолдаушылардың жабық топқа кіруі) спектрі қарастырылған. Абоненттердің көбі GSM-ді іскерлік мақсатта қолданады деген болжам болғандықтан, қаупсіздік аспектілеріне және көрсетілетін қызметтің сапасына ерекше назар аударылған. Хабарламаны жіберуге GSM-нің келесі жаңа қызметі де жатады, ол қысқа хабарламаларды (қолданушылардың белгілі бір тобына арналған қызметтік әріптік-сандық хабарламалар жіберу) жіберу.

Қысқа хаттамаларды тасымалдау кезінде сигнализация каналдарының өткізгіштік қабілеті қолданылады. Хаттамалар қозғалмалы станциямен жіберіле алады немесе қабылдана алады. Қысқа хаттамаларды тасымалдау үшін басқарудың ортақ каналдары қолданыла алуға мүмкіндік беріледі. Хаттама мөлшері 160 символмен шектеледі, олар ағымдағы шақыру немесе жұмыс жасамайтын цикл кезінде де қабылдана береді. Радиоканалдарды басқаруда ондағы қателерден қорғану, кодтау – сөйлеудің декодталуы, ағымдағы бақылау және қолданушы, шақыру мәліметтерінің реттелуі, радиоканал мен мәліметтер арасында тасымалдау жылдамдығының адаптациясы, жүктемелердің (терминалдар) параллельді жұмысының қамтамасыз етілуі, қозғалыс процесі кезінде үздіксіз жұмыстың қамтылуы.

Қозғалмалы станцияның шеттелген құрылғының үш түрі қолданылады, олар: МТО (Mobile Termination 0) — құрамына мәліметті және сөзді қабылдау және жіберу мүмкінідігі бар: МТ1 (Mobile Termination 1) — ISDN терминалы арқылы байланыс орнатылатын қозғалмалы станция; МТ2 (Mobile Termination 2) — V немесе X сериялы МККТТ хаттамасының байланыс терминалы арқылы қосылу мүмкіндігі бар қозғалмалы станция. Терминалды құрылғы бір немесе бірнеше типті құрылғылардан құрылуы мүмкін. Мысалы, нөмір тергіші бар телефондық тұтқа, мәліметті жіберу құрылғысы, телекс және т.б. Терминалдардың келесідей түрлері бар:

- (Terminal Equipment 1) — ISDN-мен байланысты орнататын терминалдық құрылғы;
- ТЕ2 (Terminal Equipment 2) — V немесе X сериялы МККТТ хаттамасы арқылы кез-келген құрылғымен байланыс орнататын терминалдық құрылғы (ISDN-мен байланыс орнатпайды). ТЕ2 терминалы МТ1-ге (ISDN-мен байланыс орнату мүмкіндігі бар қозғалмалы станция) ТА адаптері арқылы жүктеме ретінде қосыла алады. GSM стандартының сипаттамасы хабарламаны жіберудегі жоғары пааметрлерді, қолда бар және болашақтағы ақпараттық желілермен сәйкестілікті қамтамасыз тетеді, абоненттерге сандық қызметтердің кең спектрін ұсынады.

GSM-900 стандартының модификациясы салыстырмалы түрде жас болып саналады, сондықтан әлем бойынша әлі кең таралмаған. Цифрлік стандарт, жиіліктер аралығы — 1710 – 1880 МГц [20].

GSM-1800 бен GSM-900 айырмашылығы. Көбіне тек жұмыс жиіліктері негізінде ерекшелінеді. Ұсынылатын сервис көбіне диапазонға емес, операторға тәуелді болады.

Бірақ та мұнда көп қызықты жағдайлар бар:

- Салыстырмалы түрде жоғары жиілік үшін сотының максималды мүмкін радиусы азаяды, яғни – базалық станциядан максималды арақашықтығы. GSM-900 диапазонында бұл арақашықтық 35 км шамасына дейін жетеді. GSM-1800 үшін

— шамамен 10 км.

- 1800 – 2000 МГц жиіліктерінің радиотолқындарында басқа енетін қасиеттер болады [19].

Маңызды артықшылық — салыстырмалы түрде үлкен жиілікті ресурс, себебі бұл жиілікті диапазон баяғыда «биліктегі» мүшелерді жаулап үлгермеген. Осыдан басқа 1800 және 1900 жиілік аралығындағы жиіліктік жобалау каналдардың көп санына қатысты және сот радиустарының аз шамасына қатысты икемдірек орындалады.

Ерекшеліктері. GSM-1800 стандартының ұялы телефонның шағылатын максималды қуаты — 1Вт, салыстыру үшін GSM-900 — 2Вт. Аккумуляторға зарядка бермей үздіксіз жұмыстың көп мәнді уақыты және радиошағылу деңгейінің төмендеуі, бірақ та ең жоғары жиілігін ескерсек, онда «микротолқынды пештің эффектісі сіздің ағзаңызға теріс әсер етеді» деген жоғарлауды болжауға болады.

GSM-900 және GSM-1800 стандарттарында жұмыс жасайтын ұялы аппараттардың қолданылу мүмкіндігі бірдей болып табылады. Мұндай аппарат GSM-900 желісінде функционалдайды, бірақ та GSM-1800 аймағына түскенде бұл аппарат қайта қосылады — қолмен немесе автоматты түрде қосылады. Бұл операторға жиіліктік ресурсты рационалды түрде қолдануға мүмкіндік береді, ал клиенттерге – төмен тарифтер арқылы ақшаны үнемдеуге мүмкіндік туғызады. Екі желіде де абонент бір номерді қолданады. Бірақ та екі желіде аппараттың қолданылуы тек мына жағдайда ғана мүмкін: бұл екі желі бір компанияға тиісті болса немесе әр түрлі диапазонда жұмыс жасайтын компаниялар арасында роуминг туралы келісімшарт жасалса.

Күрделі мәселе болып саналатыны базалық станцияның ұстау аймағы GSM-900, AMPS/DAMPS-800, NMT-450 стандарттарына қарағанда кішірек болады [19]. Сондықтан базалық станциялардың саны көбірек болуы керек. Жиіліктер аралығы қаншалықты жоғары болған сайын, радиотолқындардың өткізгіштік қабілеті соншалықты көбірек болып, оның шағылу және тосқауылдарды айналу қабілеті төменірек болады. Осының бәрі жобалау мәселесіне және басқа стандарттағы желілермен қатынасқа жаңа жағдайларды енгізеді, бірақ та бұл жобалау принциптерінде кқрсетілмейді және оған еш әсер етпейді де, олар GSM-900 стандарты сияқты қала береді. Ал өзара қатынас мәселелері көбіне өз желісін құруға қолданатын операторға тәуелді болады.

GSM Қазақстанда.«FinTur Holding B.V.» холдингінің құрамына, ірі скандинавиялық оператор TeliaSonera құрамына кіреді, 49% «Казахтелеком» АҚ компаниясына тиесілі.

Бүгінгі таңда GSM Қазақстанда ұялы байланыстың озаты болып келеді, ол GSM-900 стандартымен қызмет көрсетеді. Компанияның мақсаты ұялы байланысты Қазақстанның барлық тұрғындарына қол жетімді ету және өзінің абоненттеріне максималды түрде пайда әкеліп, жоғары сапалы қызмет көрсету. «GSM Қазақстан» компаниясы 1998 жылы құрылды және 1999 жылдың қаңтар айында K’cell сауда маркасы атымен ұялы байланыс

қызметін көрсетіп бастады. Сол жылдың қыркүйек айында Activ ұялы бредін шығарды. Алдын-ала ойластырылған маркетингтік жоспары бар компания, 2000 жылдың басына қарай абоненттік базасы 100 000-нан асты және сол жылдың аяғына қарай олардың саны екі есе өсті. Бүгінгі таңда абоненттік база 7,5 милионнан астам адамды құрайды.

Жұмыстың алғашқы күндерінен бастап GSM Қазақстан тредсеттер ретінде шығып жүр, ол Қазақстанның ұялы байланыс нарығында даму бағытын және болашақты анықтайды. Компанияның белсенд түрде жұмыс жасауы нәтижесінде қазақстандық мобильдік нарығында алғашқы GPRS/EDGE жаңа технологиялар пайда болды және миллиондаған абоненттер барлық ел масштабында Мобильді Интернет, WAP, MMS сияқты өызметтерді пайдалана алды. Қазіргі таңда компания ұялы байланыстың жаңа буынын — 3G моделін енгізумен айналысуда, ол абоненттерге видеоқоңырау шалу және мобильді телефидение сияқты жабдықтарды қолдануға мүмкіндік береді [19]. Бұл үшін арнайы құралдың ауыстырылуы мен орнатылуы, компания қызметкерлерінің дайындығы жүріп жатыр.

Нарықта GSM Қазақстан 9 жыл жұмыс жасау барысында әр уақытта сигнал желісі қамтитын аймақты кеңейтуде. 2008 жылдың маусым айының қорытындысы бойынша, компания ұсынатын ұялы байланыс 1449 қаласында қол жетімді. 2008 жылдың аяғында базалық станциялардың саны 50%-ға артты. Болашақта компания алдында алдағы уақытта тұрғындардың саны 2000-нан асатын барлық аймақты ұялы баланыспен қамту мақсаты тұр.

Осылайша, GSM Қазақстан абоненттердің саны бойынша, қамту аймағы бойынша, инновация мен технологиясы бойынша алдыңғы орынға ие болып отыр. Бірақ компания озат орын деген ұғымға ерекше мағына береді, яғни тек сапалы қызмет көрсету емес. GSM Қазақстан үшін алдыңғы орын деген еліміздің жалпы қоғамдық дамыту процесстеріне қатысып, әлеуметтік-жауапкершілікті бизнесте блсенді орынға ие болу дегенді білдіреді. Сондықтан да компания көптеген жалпы маңызды проекттерге қатысуда.

Жыл сайын GSM Қазақстан алпыстан астам әлеуметтік бағдарламаларды іске асырады, әлеуметтік сфераға жалпы инвестиция көлемі 2007 жылы 1,5 миллион доллардан асты [31].

*NMT-450.*Ұялы байланыстың аналогты алдыңғы стандарты NMT450 (Nordic Mobile Telephone System), HMT 450. NMT 450i стандартында қауіпсіздік мәселесін шешу. NMT900 стандарты және оның сипаттамасы. NMT450 (Nordic Mobile Telephone System) – ұялы байланыстың алғашқы стандарттарының бірі. 1978 жылы төрт елдің – Дания, Финляндия, Норвегия және Швецияның қатысумен тұрғындар саны көп болмайтын елді мекендерде қолдану үшін жасалған. Бұл стандарт негізінде жұмыс жасайтын алғашқы жүйелер 1981 жылы жасалды. Стандарт толығымен аналогты, NMT450 нұсқасы 450 МГц

жиіліктегі диапазонда жұмыс жасайды. Барлығы 180 дуплексті 10 МГц жиілігі бар диапазонды каналдар қолданылады. NMT стандарты бөліп таратылған (FDMA, Frequency Division Multiple Access — бөліп таратылған көпшіліктік рұқсат) рұқсатты пайдаланады. TDMA (Time Division Multiple Access — уақытша бөлінген көпшіліктік рұқсат) немесе CDMA (Code Division Multiple Access — код бойынша бөлінген көпшіліктік рұқсат) технологияларын пайдаланатын сандық байланыс жүйелерімен салыстырғанда аналогты жүйелер мобильді телефон мен базалық станция аралығындағы қашықтық – 70 шақырым болған кезде де байланыс орната алады [24]. GSM 900 Мгц (TDMA) стандартында бұл қашықтық 35 шақырымнан көп емес, ал 1800 МГц (GSM1800) нұсқасында одан да аз болады. NMT450 базалық станциялары ретінде өзара біріккен ретрансляторлар алынады, олар бір ортақ коммутатормен басқарылады (MSC, Mobile Switching Center — ұялы байланыстың комутация орталығы). Осындай түрдегі әрбір құрылым traffic area (байланыс аймағы) деп аталады. Әрекет аймағына түскен кезде байланыс аймақтары, телефон қызметтік канал арқылы осы аймақта тіркеледі де, базалық станцияардың сигналы телефонның қалыпты жұмыс жасауына дейін жеткілікті болғанша дейін қайта тіркелу әрекеттеріне тырыспайды. Тіркелуден кейін коммутатор телефонның онымен қамтамасыз етілетін базалық станция аймағында орналасатынын ескереді: телефон қолжетімді саналып, оған звондауға болады. Телефон нақты қабылдау аймағынан шыққан кезінде қайта тіркелу әрекеті жүзеге асырылады, бұл кезде телефон алдымен бірінші аймақтан сөндіріледі де, көршілес базалық станцияның аймағына қосылуға тырысады. Сонымен қатар бұл кезде байланыс жоғалуы мүмкін —GSM стандартына қарағанда, онда бір базалық станциядан екінші базалық станцияға ауысуы көбіне бір мезетте байқалмай өтеді.

Байланыс сапасы 4 кГц жиілігіндегі қызметтік сигнал бойынша анықталады, бұл сигнал сөйлеу кезінде бір базалық станциядан канал арқылы тасымалданады. Сигнал ұялы телефон арқылы қабылданады да, базалық станцияға қайтадан жіберіледі. Сигналдың сапасын сараптаудан кейін коммутатор ұялы телефонмен жақсы қабылдауды қамтамасыз ету үшін байланыс аймағында нақты базалық станцияны таңдайды. NMT стандартының кемшілігі ретінде оның әлсіз ақпараттық қауіпсіздігі болып саналады. Ұқсас стандарт ретінде ол кез келген радиостанция арқылы тыңдауды қамтамасыз етеді, бұл радиостанция 450 МГц аралығында жұмыс жасайды. Нақты NMT450 стандартында егіздерден сақтану әрекеті табыссыз орындалды: нақты телефонның кодын телефонның ППЗУ-нан (программалайтын тұрақты еске сақтайтын құрылғы) немесе тікелей эфирден жазуға болады. Осылайша, бірінші телефонның толық егізі жасалды.Соңыра бұл мәселе де өз шешімін тапты. Стандартың жаңа нұсқасы NMT450i деп аталады және SiS технологиясын қолданады (Subscriber Identification Security — қолданушы идентификациясының қауіпсіздігі). Бұл стандарт есептелетін кодтардың негізінде қорғау жүйелері ретінде алынады. Телефон эфирге кодты емес, базалық станциялардың жағынан жіберілетін аргументтер негізінде кейбір математикалық

әрекеттердің нәтижесін шығарады. Аргументтер алуан түрлі болғасын, эфир арқылы кодты есептеу мүмкін емес әрекет болып саналады. Абонентті идентификациялау жүйесін жетілдіру қажеттілігі NMT стандартын Ресей мемлекетінде қолданыла бастағасын мәнді түрге айналды. NMT стандарты ұқсас болғасын және аз қоныстанған территориялар үшін әзірленгесін үлкен көлемді қалалардағы байланыс сапасы жақсыны талап етеді. 450 МГц диапазоны алуан түрлі бөгеуілдерге қатты ұшырайды және цифрлік байланыс NMT450 жүйесіне қарағанда сөйлеу тарктатында сигнал/шумның жақсы қатынасын құра алмайды. NMT стандартын жетілдіру мақсатында NMT900 стандарты жасалды, бұл стандарт 900 МГц диапазонындағы жиіліктерді қолданды және 5-10 есе көп каналдар санына, сонымен қатар ұялы телефонның төмендетілген қуатына ие болды [23].

- **Ұялы байланыстың криптографиялық қорғау**

жүйесінің программалық іске асырылуы

- **Шифрлеу алгоритмінің таңдау негізі**

Шифр немесе шифрлеу алгоритмі деп аталатын криптографиялық алгоритм шифрлеу немесе дешифрлеу үшін қолданылатын математикалық функция болып табылады.

Шифрлеу алгоритмі шектелген деп аталады, егер де криптографиялық алгоритмнің сенімділігі алгоритмнің мәнін жасыру арқылы қамтамасыз етілсе.

Шектелген алгоритмдер шифрлеуге қойылатын заманауи талаптар кезінде жарамсыз болады, себебі:

- құпия хаттамалармен алмасқысы келетін қолданушылардың әрбір тобы шифрлеудің әмбебап алгоритмін әзірлеулері қажет;
- дайын құралды немесе стандартты программаларды жасау мүмкін емес әрекет;
- топтың құрамындағы қолданушылардың бірі программадан шыққысы келетін жағдай үшін немесе алгоритм бөлшектері кездейсоқта бөтен адамдарға белгілі болған жағдай үшін міндетті криптографиялық алгоритм әзірлеу қажет.

Қарастырылған мәселелер криптографияда кілт қолдану арқылы шешіледі, ол кілт әрпімен белгіленеді (ағылшын тілінен key сөзінен алынған). Кілт жиынға тиісті мәндерден алынуы керек, бұл жиын кілттік кеңістік деп аталады. Шифрлеу функциясы әрпімен, ал дешифрлеу функциясы әрпімен белгіленіп, осы екі функция да кілтке тәуелді болады. Бұл қасиет және функцияларында индексі ретінде көрсетіледі.

Шифрлеудің кейбір алгоритмдері шифрлеу мен дешифрлеу үшін алуан түрлі кілттерді қолданады. Яғни, шифрлеу кілті шифрлеу кілтінен ерекше болады.

Кілттерді қолданатын шифрлеу алгоритмдерінің сенімділігі кілттерді таңдау әрекетіне және олардың құпияда сақталу әрекеттеріне тәуелді болады. Яғни, мұндай алгоритмдерді жасырын сақтап қоюдың қажеттілігі болмайды. Зиянкес криптографиялық алгоритмді білсе де, ол хаттамаларды шифрлеу үшін қолданылған құпия кілтті білмегесін жасырынып тұрған хаттамаларды ашып, оқи алмайды.

Криптожүйесі ретінде шифрлеу алгоритмі алынады, сонымен қатар алуан түрлі кілттер, ашық және шифрленген мәтіндер алынады.

Шифрлеу алгоритмін таңдау. Жасалатын криптожүйеде қолданылатын шифрлеу алгоритмін таңдаған кезінде ең алдымен алгоритмдердің мынадай қасиеттеріне назар аудару керек.

Криптотөзімділік. Алгоритм ұзақ уақыт бойында әлемдік криптографиялық ұйымның тиянақты сарапталануынан өтуі қажет (бес жылдан кем емес) және көптеген шабуылдарға қарсы криптотөзімді болуы керек.

Кілт ұзындығы. Шифрлеу алгоритінде қолданылатын кілт симметриялық шифрлеу үшін 56 биттен кем болмауы керек және ашық кілтті алгоритмдер үшін 2048 бит болуы керек. Бұл қасиет XXI ғасырда шифрді тікелей іріктеп алу тәсілі арқылы ашу мүмкін емес болу үшін жасалған.

Шифрлеу жылдамдығы. Компьютер арқылы толық жылдамдықты интерфейс USB2.0.(12 Мбит/сек) арқылы байланыс құру мүмкіндігі ойлап табылу жолында. Сондықтан таңдалған алгоритм көмегімен мәліметтерді шифрлеу жылдамдығы максималды жылдамдық кезінде деректерді жіберу кезінде үзілістер туындамайтындай ғып жоғары болуы керек [1].

Ресурс көлемі. Алгоритм аппаратты жүзеге асыру үшін оптимизациялануы керек. Оперативті жад мөлшері мен микропроцессордың қажетті өнімділігі ортақ қолданыстағы микроконтроллермен шектелетін деңгейде болуы қажет.

- **DES, Data Encryption Standard**

DES (Data Encryption Standard) — IBM фирмасымен жасалған және 1977 жылы АҚШ-пен ресми стандарт (FIPS 46-3) ретінде танылған симметриялы шифрлеу алгоритмі. DES 64 биттен тұратын блоктар мен Фейстель желісінің 16 циклды құрылымынан тұрады, шифрлеу кезінде ұзындығы 56 бит болатын кілтті қолданады. Алгоритм сызықты емес (S-блоктары) және сызықты (E қайта орнатуы, IP, IP^{-1})түрлендірулерінен тұрады. DES алгоритмінде төрт жұмыс жасау режимі бар [9]:

- Электронды кодтау кітабының режимі (ECB — Electronic Code Book);
- Блоктарды біріктіру режимі (CBC — Cipher Block Chaining);
- Шифромәтін бойынша кері байланыс режимі (CFB — Cipher Feed Back);
- Шығыс бойынша кері байланыс режимі (OFB — Output Feed Back).
- Бастапқы мәтін – 64 биттен тұратын блок.

Шифрлеу процесі бастапқы орналастыруынан, шифрлеудің 16 циклінен (алмастыру) және соңғы қайта орнатуынан тұрады.

*Бастапқы орналастыру.*Алғашқы T мәтіні (64 биттен тұратын блок) бастапқы IP орналастыру арқылы түрленеді, ол 1 кестемен анықталады:

Кесте 1. Бастапқы IP орналастыру

58	50	42	34	26	18	10	2	60	52	44	36	28	20	12	4
62	54	46	38	30	22	14	6	64	56	48	40	32	24	16	8
57	49	41	33	25	17	9	1	59	51	43	35	27	19	11	3
61	53	45	37	29	21	13	5	63	55	47	39	31	23	15	7

Мағынасы 256, әр 8-ші бит алынады (жұптылықты тексеру үшін).

Кесте арқылы нәтижелі блогының алғашқы 3 биті Т кіріс блогының 58, 50, 42 биттері болады, ал оның соңғы биттері ретінде кіріс блогының 23, 15, 7 биттері алынады.

*Шифрлеу циклдары.*Бастапқы орналастырудан кейін алынған 64-биттік IP(T) блогы Фейстель түрленуінің 16-циклына қатысады.

Фейстель түрленуінің 16 циклы:

блогын екі бөліктеріне бөлеміз, мұндағы — сәйкесінше блогының 32 үлкен биттері және 32 кіші биттері.

итерацияның нәтижесі болсын, онда і-ші итерацияның нәтижесі мына түрде анықталады:

(3.2)

(3.2.1)

сол жағы алдыңғы векторының оң жағына тең. Ал оң жағы модуль бойынша және биттік қосындысына тең.

Сурет 6. DES алгоритмнің шифрлеу сұлбасы.

Шифрлеудің негізгі функциясы (Фейстель функциясы).

функциясының аргументтері ретінде 32-биттіквекторы және 48-биттік k_i кілті алынады, кілт 56-биттік бастапқы кілтке жасалған түрлендіру нәтижесі болып табылады.

функциясын есептеу үшін кеңейту функциясы, 8 түрленуден тұратын түрлендіруі

және ауыстыруы қолданылады.

функциясы векторынан кейбір биттерді көшіру арқылы 32-биттік R_{i-1} векторын 48-биттік векторына дейін кеңейтеді;

бұл әрекет кезіндегі векторының тізбегі 2 кестеде көрсетілген.

Кесте 2. кеңейту функциясы

32	1	2	3	4	5
4	5	6	7	8	9
8	9	10	11	12	13
12	13	14	15	16	17
16	17	18	19	20	21
20	21	22	23	24	25
24	25	26	27	28	29
28	29	30	31	32	1

векторының алғашқы үш биті векторының биттері болып табылады.

2 кесте бойынша биттері қайта көшірілгені айқын көрінеді.

векторының соңғы үш биті — векторының биттері . Алмастырудан кейін алынғанблогы модуль бойынша кілттерімен шығады да, кейін сегіз тізбектей орналасқан блоктары ретінде саналады.

(3.2.2)

Әрбір блогы 6-биттік болып табылады.

Содан кейін әрбір блогы түрленуі негізінде 4-биттік блогына айналады. түрлендіруі 3 кесте арқылы анықталады.

Сурет 7. fфункциясыныңжұмысістеусұлбасы.

Кесте 3. S_i, i=1...8 түрленуі

	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	
0	14	4	13	1	2	15	11	8	3	10	6	12	5	9	0	7	
1	0	15	7	4	14	2	13	1	10	6	12	11	9	5	3	8	S_1
2	4	1	14	8	13	6	2	11	15	12	9	7	3	10	5	0	
3	15	12	8	2	4	9	1	7	5	11	3	14	10	0	6	13	
0	15	1	8	14	6	11	3	4	9	7	2	13	12	0	5	10	
1	3	13	4	7	15	2	8	14	12	0	1	10	6	9	11	5	S_2
2	0	14	7	11	10	4	13	1	5	8	12	6	9	3	2	15	
3	13	8	10	1	3	15	4	2	11	6	7	12	0	5	14	9	
0	10	0	9	14	6	3	15	5	1	13	12	7	11	4	2	8	
1	13	7	0	9	3	4	6	10	2	8	5	14	12	11	15	1	S_3
2	13	6	4	9	8	15	3	0	11	1	2	12	5	10	14	7	
3	1	10	13	0	6	9	8	7	4	15	14	3	11	5	2	12	
0	7	13	14	3	0	6	9	10	1	2	8	5	11	12	4	15	
1	13	8	11	5	6	15	0	3	4	7	2	12	1	10	14	9	S_4
2	10	6	9	0	12	11	7	13	15	1	3	14	5	2	8	4	
3	3	15	0	6	10	1	13	8	9	4	5	11	12	7	2	14	
0	2	12	4	1	7	10	11	6	8	5	3	15	13	0	14	9	
1	14	11	2	12	4	7	13	1	5	0	15	10	3	9	8	6	S_5
2	4	2	1	11	10	13	7	8	15	9	12	5	6	3	0	14	
3	11	8	12	7	1	14	2	13	6	15	0	9	10	4	5	3	

тең деп алайық та бізге тауып алу керек. бастапқы және соңғы разрядтары санының екілік жазбасы болып табылады,, ортаңғы 4 разряд санын көрсетеді, . кестесінің

жолдары ден 3-ке дейін нөмірленеді, ал кестенің бағандары ден -ке дейін жазылады. Сандар жұбы жолы мен бағанының қиылысында орналасқан санды анықтайды. Осы санның екілік түрленуі -ті береді. Біздің жағдайда, ал жұбымен анықталатын сан -ге тең. Оның екілік түрленуі. функциясының мәні 32-биттік блогына қолданылатын P алмасу көмегімен алынады.

P алмастыруы 4 кестемен анықталады.

Кесте 4. P алмастыруы

16	7	20	21	29	12	28	17
1	15	23	26	5	18	31	10
2	8	24	14	32	27	3	9
19	13	30	6	22	11	4	25

(3.2.3)

4 кесте бойынша функциясының әсерінен шығатын нәтижелі векторының алғашқы төрт биті — бұл векторыныңбиттері.

*k_i кілтінің генерациялануы.*кілттері бастапқы кілтінен алынады (немесе ASCII кодындағы 8 символ). 8, 16, 24, 32, 40, 48, 56, 64 позициясында орналасқан сегіз бит k кілтіне қосылады, қосылу механизмі: әрбір байт бірліктердің тақ санына тең болуы керек.

Осындай түрде қолданылу себебі: кілттерді сақтау мен алмастыру кезіндегі қателерді анықтау үшін. Одан кейін кеңейтілген кілт үшін алмастыруды жасайды (қосылатын 8, 16, 24, 32, 40, 48, 56, 64 биттерінен басқа). Мұндай алмастыру 5 кестеде анықталған.

Кесте 5. Алмастыру

57	49	41	33	25	17	9	1	58	50	42	34	26	18	C_0
10	2	59	51	43	35	27	19	11	3	60	52	44	36	
63	55	47	39	31	23	15	7	62	54	46	38	30	22	D_0
14	6	61	53	45	37	29	21	13	5	28	20	12	4	

Бұл алмастыру әрқайсысы 28 бит болатын екі C_0 және D_0 блоктарымен жүзеге асырылады.

C_0 блогының алғашқы үш биті кеңейтілген кілттің биттері болып табылады — 57, 49, 41. Ал D_0 блогының алғашқы үш биті кеңейтілген кілттің биттері болып табылады — 63,55,47. C_i,D_i i=1,2,3... мәндері C_{i-1},D_{i-1} блоктарынан 6 кесте бойынша бір немесе екі сол циклды ығысу көмегімен алынады.

Кесте 6. Ығыстыру

I	*1*	*2*	*3*	*4*	*5*	*6*	*7*	*8*	*9*	*10*	*11*	*12*	*13*	*14*	*15*	*16*
Ығысу саны	1	1	2	2	2	2	2	2	1	2	2	2	2	2	2	1

кілті 48 биттен тұрады, олар(56 бит) векторынан 7 кесте бойынша анықталады. кілтінің бірінші және екінші биттері векторының 14, 17 биттері болып табылады.

Кесте 7.Биттер

14	17	11	24	1	5	3	28	15	6	21	10	23	19	12	4
26	8	16	7	27	20	13	2	41	52	31	37	47	55	30	40
51	45	33	48	44	49	39	56	34	53	46	42	50	36	29	32

_

Соңғы қайта орнату.

Соңғы қайта орнатуы блогына әсер етеді және позицияны бастапқы күйге келтіру үшін қолданылады.

Ол орнатуына кері болып табылады. Соңғы қайта орнатуы кесте 8 арқылы анықталады.

Кесте 8. Соңғы қайта орнатуы

40	8	48	16	56	24	64	32	39	7	47	15	55	23	63	31
38	6	46	14	54	22	62	30	37	5	45	13	53	21	61	29
36	4	44	12	52	20	60	28	35	3	43	11	51	19	59	27
34	2	42	10	50	18	58	26	33	1	41	9	49	17	57	25

_

*DES алгоритмнің қолданылу режимдары.*DES төрт режимде қолданыла алады.

1. Электронды кодтау кітабының режимі (*ECB*— Electronic Code Book): DES алгоритмінің блокты шифр ретінде қарапайым қолданылуы. Шифрленетін мәтін блоктарға бөлінеді және де әр блок бір-бірімен әсерлеспей, жекелеп шифрленеді (сурет 8).

Сурет 8. Электронды кодтау кітабының режимі — ECB.

2. Блоктарды біріктіру режимі (*CBC*— Cipher Block Chaining). Әрбір блогы шифрлау алдында модуль бойынша келесі ашық мәтін блогына қосылады. векторы — бастапқы вектор, ол жиі ауысып тұрады және құпияда сақталады.

Сурет 9. Блоктарды біріктіру режимі — CBC.

3. Шифромәтін бойынша кері байланыс режимі (ағылш.*CFB*— Cipher Feed Back). CFB режиміндеблокты «гаммасы» түзіледі. бастапқы векторы синхронды тасымалдау болып табылады және деректердің әр түрлі жинақтарының бір құпия кілт негізінде шифрлеу мүмкіндігін қамтамасыз ету әрекетінде қолданылады.

Синхро тасымалдау қабылдаушыға шифрленген мәтінмен бірге ашық түрде жіберіледі.

Сурет 10. Шифромәтін бойынша кері байланыс режимі — CFB.

4. Шығыс бойынша кері байланыс режимі (OFB— Output Feed Back). OFB режиміндеблокты гаммасы түзіледі.

Сурет 11. Шығыс бойынша кері байланыс режимі — OFB.

Режимдердің артықшылықтары мен кемшіліктері:

- ECB және OFB режимдерінде шифр мәтінінің бір 64-биттік блогын тасымалдау кезіндегі бұрмалану дешифрлеу өткеннен кейін тек бір Mi ашық блогының белгілі бір бөлігінің ғана бұрмалануына әкеледі, сондықтан бұл режимдарды бұрмалану саны үлкен деректер каналы үшін қолданылады [32].

*DES алгоритмнің криптоберіктілігін ұлғайту.*DES алгоритмнің криптоберіктілігін ұлғайту үшін бірнеше нұсқалар пайда болған: double DES (2DES), triple DES (3DES), DESX, G-DES.

- 2DES және 3DES әдістері DES алгоритміне негізделген, бірақ та олар кілттің ұзындығын ұлғайтады(2DES — 112 бит, 3DES — 168 бит), сондықтан криптоберіктілікті ұлғайтады.

- 3DES сұлбасының жалпы көрінісі: мұндағы DES шифрінің кілттері болып табылады. Сонымен қатар бұл нұсқа түрінде де белгілі, себебі DES алгоритмінің үш операциясы шифрлеу болып табылады. 3DES алгоритмінің үш типі анықталған:
- DES-EEE3: 3 рет үш әр түрлі кілтпен шифрленеді.
- DES-EDE3: 3DES операциялары шифрлеу-дешифрлеу- шифрлеу үш әр түрлі кілтпен өтеді.
- DES-EEE2 және DES-EDE2: алдыңғы типтер сияқты, бірақ та айырмашылығы – бірінші және үшінші операция бірдей кілтті пайдаланады.
- DESX тәсілі Рональд Ривестпен жасалған және ресми түрде Killian және Rogaway фирмаларымен көрсетілген. DESX алгоритмін RSA Data Security әзірледі. Ол 1986 жылы MailSafe электронды поштаның қауіпсіздігін қамтамасыз ету үшін жасалып, 1987 жылы BSAFE жинағына енді. DESX тәсілі DES алгоритмінің кірістері мен шығыстарын жасыру мақсатында ағарту деп аталатын әдісті қолданады. Бұл тәсіл — DES алгоритмінің жетілдірілген нұсқасы, ол RSA Security құралдарымен қамтамасыз етіледі. DESX алгоритмі DES алгоритмінен ашық мәтіннің әрбір битінің модуль бойынша қосымша кілттің 64 битімен логикалық қосу әрекеті бойынша ерекшелінеді. Нәтиженің әрбір биті логикалық түрде модуль бойынша кілттің кез келген басқа да 64 биттерімен қосылады. DESX алгоритмін қолданудың негізгі себебі DES алгоритмін шабуылдардан қорғау болып табылады, бұл әрине есептеу жағынан қарапайым әрекет болып табылады. DES алгоритмінде қолданылатын 56-биттік кілтінен басқа DESX алгоритмінде ағарту әрекетінің қосымша 64-биттік кілті қолданылады. Осы 64-биттер DES алгоритмінің алдында ашық мәтін блогына жасалатын XOR операциясы үшін пайдаланылады. DESX алгоритмінінің толық 120-биттік кілтіне қолданылатын бір бағытты функцияның нәтижесінде алынатын қосымша 64-биттер соңғы этапта алынған шифр мәтініне XOR операциясын қолдану үшін пайдаланылады. Ағарту әрекеті DES алгоритмін шабуылдардан қорғау үшін қолданылады. Сонымен қатар бұл әрекет алгоритмінің криптологияға деген тұрақтылығын жоғарылату үшін де қолданыла береді.
- G-DES әдісі DES алгоритмінің өнімділігін ұлғайту үшін шифрленген блоктың мөлшерін үлкейту арқылы Schaumuller-Bichl компаниясымен әзірленген. Олар G-DES DES алгоритмі сияқты әр түрлі шабуылдардан қорғалған деп айтты. Бірақ та Biham және Shamir ұсынылатын параметрлері бар G-DES алгоритмінінің жеңіл бұзылатынын көрсетті және оның параметрлерінің кез келген өзгерісі кезінде шифр DES-ке қарағанда да әлсіз болып қалады [9].

DES алгоритмінің басқа нұсқасы тәуелсіз суб-кілттерді пайдаланады. DES алгоритміне

қарағанда қолданушы 56 бит негізіндегі құпия кілттен 16 раундта қолдануға болатын он алты 48-биттік суб-кілттерді алады. Осы нұсқада 16 тәуелді 48-биттік кілттердің орнына 768-биттік кілт (16 48-биттік ішкі кілттер) қолданылады. Бірақ та тәуелсіз суб-кілттерді қолдану кілттің толық іздеуін күрделіндірсе де, дифференциалды және сызықтық криптосараптамадан туындайтын шабуылдарға төзімділігі жоғарылайды. Берілген Biham бағасы бойынша DES алгоритмінің дифференциалды криптосараптамасы үшін 2^{61} ашық мәтіндер керек, ал сызықтық криптосараптама үшін 2^{60} әйгілі ашық мәтіндер қажет.

- **Java тілі, қолдану аясы**

Java тілі бұл Internet желісінде жұмыс істейтін объектілі-бағытталған, платформалы – тәуелсіз, желі ішінде жұмыс істейтін тармақталған қосымшалардың өңдеуіне қолданылатын программалау тілі.

Java тілі C++ тілінің синтаксисын қолданады, бірақ объектілік үлгі Smalltalk тілінен алынған. Осыдан Java тілінің C++ тілімен ұқсастықтары тек қана сыртқы түрде екенін көруге болады. Басқа программалау тілдерімен салыстырып қарағандағы негізгі айырмашылығы — программалар мөлшерінің азаюын қажет етуі мен желіде жұмыс істейтін тасымалданатын қосымшалардың қауіпсіздігі шарттарының ұлғаюы. Java көрсеткіштерді (C++, Pascal және тағы да басқа тілдердің ең қауіпті құралы) қолдамайды, себебі, жадтың жанама адрестерімен типі көрсетілмеген көрсеткіштер арқылы жұмыс істеу мүмкіндігі жадтың қорғанышын елемеуге рұқсат береді. Java тілінде айнымалы арифметикамен есептеудің тәсілдері өзгерген, сондықтан да тіл түрлерінің арасында аралық код шыдамдылығын қамтамасыздандыру үшін strictfp кілттік сөзі енгізілді. Ол компиляторға айнымалы үтірі бар сандар үшін арифметикалық әрекеттерді алдыңғы түрдегі есептеулерге сәйкес орындау керек екендігін көрсетіп, жаздырады.

Тіл кластарының жүйелік кітапханасы кластар және пакеттерден тұрады, олар тілдің әртүрлі базалық мүмкіншіліктерін жүзеге асырады. Бұл кітапханаларға қосылған кластардың әдістері JVM-нан Java – бағдарламаның интерпретациясы кезінде шақырылады. Java-да бағдарламаның барлық объектілері динамикалық жадта орналасқан (heap) және стектерде сақталынатын объекті сілтемелер арқылы қолжетімді. Бұл шешім жадқа тікелей қолжетімсіздікке мүмкіндік берді, бірақ массив элементтерімен жұмыс істеуді қиындатып жіберді. Java тіліндегі объектілі сілтемелер өздері бағытталып тұрған объектілердің класы туралы хабардан тұрады. Сондықтан да

объектілі сілтемелер дегеніміз, көрсеткіштер емес, олар объектілердің дескрипторлары. Дескрипторлардың болуы JVM-ге код интерпретациясы фазасында типтердің сәйкес келуін тексеруге мүмкіндік береді. Java-да жадты динамикалық бөлу концепциясы да қайта қарастырылған: динамикалық бөлінген жадты босату тәсілдері жоқ болады. Оның орнына new (қоқыс жинаушысы) операторының көмегі арқылы көрсетілген жадты автоматты түрде босату жүйесі іске асырылған [25].

Java — бағдарламаларда класс спецификациясы мен оның жүзеге асырылуы әрқашан да тек қана бір файлда болады.

Java тілі операторларды қайта жүктеуді және typedef, белгісіз бүтіндерді (егер ол ретінде char- ды есептемесек) қолдамайды. Java-да көптік мұрагерлік жоқ, тек құрастырушылар бар, бірақ деструкторлар жоқ (қоқысты автоматты түрде жинастыру қолданылады), тілдің кейінге сақталған сөздері бола тұрса да, goto операторы және const сөзі қолданылмайды.

Java тілінде пайда болған маңызды мүмкіндіктер интерфейстер мен кең ағымдылық (бағдарлама бөлімдерінің бір уақытта орындалу мүмкіншілігі).

Виртуалды Java — машина, байт — код , JIT — компиляциясы. Java тілінде жазылған бағдарламалардың категориялары.

Java тілінде жазылған программалар кластар жиынтықтарынан тұрады және .java кеңейтілімі бар мәтіндік файлдарда сақталынады. Компиляциялау барысында программа мәтіні .class кеңейтілімі бар екілік файлдарға аударылады. Мұндай файлдар байт-кодтардан тұрады. Ол дегеніміз абстрактілі Java — процессорға арналған процессордың командаларын және оларға арналған мәліметтердің тізбектілігін байттық битте көрсету.

Java – машина нақ осылармен айналысады. Алдымен байт-код әрқашан да түсіндіріледі: қандай да бір Java-процессор нұсқаулары кездескен жағдайда ол компьютердің процессоры нұсқауларының тізбектілігіне айналдырылады. Сондықтан бұл Java қосымшасының жұмысын әлдеқайда бәсеңдеткен болатын.

Операциялық жүйе қосымшасы операциялық жүйе құралдарының арқасында орындауға жіберіледі. Ал Java қосымшасы болса, операциялық жүйе қосымшасы болып табылатын виртуалды Java — машинасының арқасында орындауға жіберіледі. Сондықтан да ең алдымен Java — машина орындауға жіберіледі. Ол параметр сапасы ретінде кластың компиляцияланған коды бар файлдың атын алады. Осы класта main деген атпен ішкі программа орындалуға жіберіледі.

Java қосымшалары тек жақсы төзімділік қана көрсетіп қоймай, жұмысты жылдам орындауға мүмкіндік береді. Бірақ олар JIT-компиляциясы бола тұрса да C немесе C++ тілінде жазылған программаларға қарағанда жұмыс істеу жылдамдығы азырақ. Бұл мынаған байланысты: JIT-компиляциясы программаның құрылымын іздеуге көп ресурс

пен өте үлкен уақыт жібере алатын C/C++ көп өткізгішті компиляторының үйлесімді коды секілді код құра алмайды. JIT-компиляциясы белгіленген шартты уақыт және ресурстар аралығында “тез арада” жүзеге асады. Осы мәселенінің шешімін табу үшін нақты программалы-аппараттық платформалар (native code – “өзінің” коды) кодына айналдыратын Java программаларының компиляторы жасалынды. Мысалы, GNU қорымен тәуелсіз таратылатын gjc компиляторы. Бірақ Sun-ның Java-машиналарды дамыту барысындағы жетістіктері кейбір жағдайлармен салыстырғанда басқа тілдерде жазылған программалардың жылдамдығынан артық болу мүмкіндігін берді. Жекелеп алғанда, жадты босату және орын берумен айналысатын Java қосымшалары C/C++ тілінде жазылған өзінің аналогтарына қарағанда, жадтың программалық слоттарының (slot – “паз, бір нәрсені қоюға арналған тесік”) арнайы механизміне байланысты жылдамырақ жұмыс істеуге мүмкіндік береді. Виртуалды Java-машина тек қана байт-кодты орындап қоймай (оны интерпретациялайды, JIT-компиляциясымен айналысады және JIT-компиляцияланған кодты орындайды), сонымен қатар, басқа да әртүрлі функцияларды орындайды. Мысалы, файлдар немесе графиканы қолдауға қолжетімділікті қамтамасыз ету үшін операциялық жүйемен қарым-қатынас жасайды. Сонымен қатар, қоқыс жинау (garbage collection) деп аталатын қажетсіз объектілермен толып тұрған жадты автоматты түрде босатумен айналысады.

Java программаларын бірнеше негізгі категорияларға бөлуге болады:

- Қосымша (application) – «қарапайым» қолданбалы программаның аналогы;
- Апплет (applet) – WWW-құжат терезесінде браузердің басқаруымен жұмыс атқаратын мүмкіндіктері шектелген арнайы программа;
- Сервлет (servlet) – WWW-да сервер жағынан жұмыс істейтін мүмкіндіктері шектелген арнайы программа. WWW-құжаттарды сервер жағынан программалау үшін JSP технологиясы (Java Server Pages – Java Серверлік Беттері) шеңберінде қолданылады.
- Серверлік қосымша (Enterprise application) – сервер жағынан көп еселі қолдануға арналған.
- Кітапхана (Java Class Library – кластар кітапханасы, немесе NetBeans Module – NetBeans платформасының модулі) – Java программасын көп еселі қолдануға арналған [25].

Кесте 9. Қосымшаны өңдеу құралдары

Утилита	Қолданылуы

javac	Java тілінде жазылған командылық жол режимінде жазылған компилятор
java	Командалық жол режимінде программаның қосымшасын іске қосуға арналған утилита
appletviewer	Браузерсіз апплеттерді орындауға іске қосу мен жөндеуге арналған утилита. Бұл жағдайда браузердегі жөнделген апплеттін жұмысқа жарамдылығына кепілдік берілмейді
jdb	Java тілінде жазылған жөндеуші программалар
javadoc	с /** басталатын түсініктемелер негізінде құжаттарды класқа бөлу генераторы
jar	jar архивы арқылы Java басқару және құру
javah	JNI интерфейсы негізінде C/C++ сыртқы кітапханаларын Java тіліне C/C++ файлдарын қосу генераторы

Жалпы Java қосымшасында программа жасау үшін мен бірінші JavaWorkShop жасанды интерпретаторын орнаттым. Бұл интерпретатор автономды қосымшаларды жасау үшін қолданылады. Java WorkShop интерпретаторын жүктегесін, экранға оның бірінші терезесі шығады.

Сурет 12. Java WorkShop интегралданған әзірлеу жүйесінің негізгі терезесі.

Қосымшаға алуан түрлі элементтерді қосып көрейік. Мысалға, менің бағдарламалық программамда батырмалар, панельдер, өрістер және жолдар және т.б элементтер бар. Бұл элементтердің барлығы класстар объектілері түрінде Component дейтін үлкен кластан туындайды [26].

Сурет 13. Java қосымшасындағы басқару элементтерінің өзара байланысы.

Button класы стандартты батырмаларды жасауға мүмкіндік береді. Ал егер де стандартты батырма емес, мысалға, графикалық батырма қажет болатын болса, онда оны Canvas класы негізінде жасауға болады.

Тәуелсіз немесе тәуелді фиксациясы бар қосқыштарды жасау үшін CheckBox класы қолданылады.

Label класы арқылы қосымша бетінде мәтіндік жолдарды жасауға болады, мысалға, басқа компонент үшін алуан түрлі атаулар. Бұл жолдарды қолданушы өзгерте алмайды.

List тізімдерді жасау үшін қолданылады.

Scrollbar класы арқылы көру жолақтарын жасауға болады, көбіне ұзын мәтіндерді оқыған кезде пайдалы.

TextComponent класы басқа екі класс үшін негіз болып саналады — TextField және TextArea. Оның біріншісі мәтіннің бір жолдық редакторлерін жасау үшін арналған, ал екіншісі мәтіннің көп жолды редкаторларын жасауға арналған.

Осы компоненттер кез келген қосымшада қалай орналасатынын түсіну үшін келесі байланысты ескеру керек.

Сурет 14. Компоненттер мен контейнерлер.

Component класы Container класы үшін негіз болып қолданылады. Бұл кластың объектілері Component және Container класының объектілерінен тұруы мүмкін.

Бұл интепретаторда жаңа жоба жасау үшін Java WorkShop Project Manager терезесінен File менюінен New жолын таңдадым. Нәтижесінде жобаларды жасау шебері жүктелді, оның бірінші диалог терезесі келесі суретте көрсетілген [25].

Сурет 15. Жобаларды жасау шеберінің терезесі.

Мысалға, кез келген бастапқы программа жазу шаблонын көрсетсем:System.out.println(«Hello, Java!»);

Содан кейін Java WorkShop негізгі терезеден Build жалпы мәзірінен Build All жолын таңдап, Project менюінен Run жолын бассақ, нәтижесінде консольға «Hello, Java!» хаттамасы жазылған қосымша шығады.

Сурет 16. Hello, Java! қосымшасымен жұмыс.

Осы қосымшалар мен компоненттерді қолданып, ұялы байланыс жүйесі үшін криптографиялық қорғай бағдарламасын жасауға кірістім.

- **Криптографиялық қорғаудың іске асуы**

Қорғау алгоритмі ретінде DES стандарты қолданылып, java тілінде іске асырылды.

Шифрлау модулінің негізгі шифрлану листингінің бір бөлігі төменде келтірілген:

```
public  String encrypt(String s)
{
String enc_hello=»»;
try{
DESKeySpec desKeySpec = new DESKeySpec(«klaradiplom».getBytes());
SecretKeyFactory keyFactory = SecretKeyFactory.getInstance(«DES»);
SecretKey secretKey = keyFactory.generateSecret(desKeySpec);
Cipher desCipher = Cipher.getInstance(«DES»);
desCipher.init(Cipher.ENCRYPT_MODE, secretKey);
enc_hello = new String(desCipher.doFinal(s.getBytes()));
}catch(Exception e)
{
}
return enc_hello;
}
public  String decrypt(String s)
{
String dec_hello=»»;
try{
DESKeySpec desKeySpec = new DESKeySpec(«klaradiplom».getBytes());
SecretKeyFactory keyFactory = SecretKeyFactory.getInstance(«DES»);
```

```
SecretKey secretKey = keyFactory.generateSecret(desKeySpec);
Cipher desCipher = Cipher.getInstance(«DES»);
desCipher.init(Cipher.DECRYPT_MODE, secretKey);
dec_hello = new String(desCipher.doFinal(s.getBytes()));
}catch(Exception e)
{
}
return dec_hello;
}
}
```

Қорытынды

«Ұялы байланыс жүйелерінде криптографиялық қорғау аппараттық жүйесін жобалау» ғылыми жұмыстың негізгі нәтижесі болып ұялы байланыс үшін криптографияда қолданылатын алгоритмдер мен тәсілдердің зерттелуі.

Бұл жұмыста криптографияның және ұялы байланыс жүйесінің түрлері, олардың артықшылықтары мен кемшіліктері, салыстыру анализі нәтижесінде алгоритм таңдалып, сымсыз байланыс арқылы екі құрылғы арасында ақпаратты жіберу кезіндегі шифрлеу бағдарламасы құрылды.

Жасап шығарылған өнім кауіпсіздікті және ақпараттың бүтіндігіне байланысты маңызды тапсырмаларды шешеді:

Хабарламаны жіберуде DES алгоритмі арқылы шифрлеу;

Осы алгоритм арқылы хабарламаны дешифрлеу.

Программалық өнім жоғары дәрежелі JAVA тілінде жазылды.

Қосымшаны әзірлеу аяқталған соң жан-жақты рефакторинг өткізілді, код толығымен нақты түрде комментарияланды, бұл жүзеге асыру процесін толығымен еске түсіру әрекетін жеңілдетеді және қажеттілік туындаған кезінде кез-келген бөлшектерге оралуға мүмкіндік береді және қосымшаны баптап, дұрыстауға болады. Код жеке қосымшада берілген (Қосымша А, Қосымша Ә).

Осылайша жасалған өнім тәуелсіз бағдарлама болып табылады. Маңызды ақпараттың таңдалған алгоритм негізінде шифрлеу тәсілі арқылы қауіпсіздікті қамтамасыз етеді. Бағдарлама қолданушыға түсінікті және қарапайым интерфейстен тұрады. Екі құрылғы арасында хабарлама жіберуде қажет болады.

Бірақ кез-келген бағдарламалы-аппараттық қамтама жетілген болмайды, сондықтан да ақаулар болады. Реалды уақытта маңызды ақпаратты рұқсаты жоқ қолданушылардан құпия түрле сақтау практикалық түрде мүмкін емес. Осы себептен көптеген қолданушылар өзінің ақпаратын сақтау үшін арнайы бағдарламаларға ие болуды қалайды. Қазіргі уақытта шифрлейтін бағдарлалардың көптеген түрлері бар, бірақ олар шартты түрде ғана ақысыз немесе ақылы болады, көптеген қолданушылар бұған ие бола алмайды. Мен жасаған өнім толығымен ақысыз болып табылады.

Қойылған мәселелердің толық шешімін бағалау. Алға қойылған мақсат орындалды.

Қолданылған әдебиеттертізімі

1. Зуйкова О.Л. 392 Основы криптографической защиты информации. Учебное пособие. — Московский государственный институт электроники и математики. М., 2005. — 207 б.
2. М.Г. Адигеев, Введение в криптографию. Методические указания для студентов. —Ростовский государственный университет Механико — математического факультета, Часть 1 Основные понятия, задачи и методы криптографии, Ростов–на–Дону — 103 б.
3. Подред. В.В. Ященко.Введение в криптографию. — 2-еизд., испр. — М.: МЦНМО: ЧеРо, 1999. — 272 б.
4. Молдовян А.А, МолдовянН.А., СоветовБ.Я. Криптография. — СПб.: Лань, 2000.— 218 б.
5. Алферов А.П.,Зубов А.Ю.,Кузьмин А.С.,Черемушкин А.В. Основы криптографии: Учебное пособие. — М.: Гелиос АРВ, 2001. — 205 б.
6. Ф ЕҰУ 703-02-11. Қолданбалы криптография. Пәннің оқу-әдістемелік кешені. Екінші басылым. Астана 2011.— 108 б.
7. Венбо Мао. Современная криптография: теория и практика. – М.: Издательский дом Вильямс, 2005. — 768 б.
8. Дж. Л. Месси. Введение в современную криптологию. ТИИЭР, т.76, №5, Май 88 – М, Мир, 1988.— 24-42 б.
9. Н. Фергюсон, Б.Шнайдер. Практическая криптография. – М.: Издательский дом Вильямс, 2005.— 625 б.

10. У. Диффи. Первые десять лет криптографии с открытым ключом. ТИИЭР, т.76, №5, Май 88 – М, Мир, 1988.—155 б.
11. Расин Вадим, Клочков Павел. Криптографические протоколы. Курсовая работа. — Московский Государственный Институт Электроники и Математики. Москва, 2000.—35-45 б.
12. В. Жельников. Криптография от папируса до компьютера. – М., ABF, 1996.— 335 б.
13. Мёрлинг Дж. , Дженс Р. История сотовой связи, Мир связи CONNECT 1997. №3.— 99 б.
14. Мерлинг Дж., Джинс Р. История сотовой (продолжение), Мир связи CONNECT. 1997. №5.—65 б.
15. Ратынский М.В. Основы сотовой связи,Под ред. Д.Б. Зимина. М.: Радио и связь, 1988.— 248 б.
16. Wireless ’98: достижения и тенденции развития сотовой связи ComputerWeekly. 1998. №38.— 80 б.
17. Волков И. Сотовая связь в условиях кризиса, Экспресс-электроника. 1998. №11.— 125 б.
18. Долгая дорога к рынку, Мир связи Connect. 1999. №1.— 89 б.
19. Афанасьев В., Грабк. Что ждет абонентов сетей GSM завтра? Компьютерная неделя. 1998. №18. — 142 б.
20. Ковалева Н. Сотовая связь сегодня и завтра, Монитор. 1998. №93.— 163б.
21. Ю.А. Громаков. Сотовые системы подвижной радиосвязи. Технологии электронных коммуникаций. Том 48. Эко-Трендз. Москва. 1994. —311 б.
22. GPRS пакетная передача данных в сетях GSM, Электросвязь, 2000. №5.—130 б.
23. Ю.А. Громаков. Структура TDMA кадров и формирование сигналов в стандарте GSM. Электросвязь. N 10. 1993. — 9-12 б.
24. Томас М., Пател П., Хадсон А. Секреты программирования для Internet на Java Перев.с англ. — СПб: Питер,1997.—640 б.
25. Мильвидский А. М. Введение в Java. –1998.—250 б.
26. http://www.enlight.ru/ib/tech/crypto/
27. http://www.gfs-team.ru/articles/read/49
28. http://www.boosters.ru/article5.htm
29. http://byt-pyt.ru/standarti-sotovoi-svyazi.php
30. http://www.region.kz/c502
31. http://protect.htmlweb.ru/des.htm

