Қазақстан Республикасы Білім және ғылым министрлігі

«Алматы энергетика және байланыс университеті»
коммерциялық емес акционерлік қоғам

Г.Д. Мусапирова

АҚПАРАТТЫ ҚОРҒАУ ЖӘНЕ АҚПАРАТТЫҚ ҚАУІПСІЗДІК

Оқу құралы

Алматы
АЭжБУ
2017

ӘОЖ 004(075.8)
М78

Пікір берушілер:
техника ғылымдарының кандидаты, Ресей Жаратылыстану Академиясының
профессоры Ақпараттық технологиялардың халықаралық университеті
Ақпараттық жүйелер кафедрасының меңгерушісі
Сербин В.В.
педагогика ғылымдарының докторы, ҚазҰПУ профессоры
С.Д.Сыдықов
техника ғылымдарының кандидаты, АЭжБУ
көпарналы телекоммуникациялық жүйелер кафедрасының доценті
Байкенов А.С.
Алматы энергетика және байланыс университетінің Ғылыми кеңесі
басуға ұсынды (хаттама №2 27.12.2016ж.). АЭжБУ 2017ж.
Ведомостік әдебиеттер басылымдар шығарудың тақырыптық
қосымша жоспары бойынша басылады, реті 1.

МусапироваГ.Д.
М78

Ақпаратты қорғау және ақпараттық қауіпсіздік: Оқу құралы (жоғары оқу орындарының студенттеріне арналған)/ Г.Д. Мусапирова. –Алматы:АЭжБУ, 2017. – 71б.; кесте –4 , ил. – 19, әдеб.көрсеткіші – 5 атау.

ISBN 978-601-7889-20-3

Бұл оқу құралында қарастырылған теориялық және практикалық материалдар ақпаратты қорғау мен ақпараттық қауіпсіздікті қамтамасыз етуге арналған.

Оқу құралы жоғары оқу орындарының «Есептеу техникасы және бағдарламалық қамтамасыз ету», «Ақпараттық жүйелер», «Математикалық және компьютерлік модельдеу» мамандықтары бойынша білім алатын студенттерге арналған.

ӘОЖ 004(075.8)

ISBN 978-601-7436-84-1

Мазмұны

Кіріспе

Соңғы кезде ақпаратты қорғауға байланысты мәселелер компьютерлік қауіпсіздік жөніндегі мамандар мен көптеген дербес қолданылушыларды ойландырды. Бұл компьютерлік технологияның біздің өмірге әкелген терең өзгерістеріне байланысты. «Ақпарат» түсінігін өзін ұғыну өзгерді. Бұл термин қазір көбінесе арнайы тауарды сату, сатып алу, басқаға айырбастауды белгілеуде қолданылады. Ал осындай тауардың құны он, кейде жүз есе есептеу техникасының құнынан артады. Әрине ақпаратты заңсыз пайдаланудан, ұрлық жасаудан, жоюдан және басқа қылмыстық істерден қорғауға қажеттілік туады. Бірақ қолданышулардың көбісі өзінің қауіпсіздігі мен жеке құпияларына қатер төнуін түсінбейді. Аз ғана адамдар өз мағлұматтарын қорғау тәсілдерін біледі. Компьютерді қолданушылар көбінесе мынадай мағлұматтарды – салықтық және банктік ақпарат, іскери хат алмасу, электрондық кестелер қорғалмай қалады.

Жүйелік администраторлар қорғануды үздіксіз көбейте бере алады, бірақ одан өту тәсілі әрқашан табылады. Бірақ көп адамның ойлауы мен істі жүзеге асыруы бірдей. Адамның бір нәрсеге ақылы жетсе, оған басқа адамның да ақылы жетеді, біреуі жасырғанды екіншісі ашады. Батыс әдебиеті бізден хакер (haker) заңсыз істерге қатыспайтын, жоғарғы дәрежедегі компьютерлік маман, терминімен белгіленетін және крэкер (craker), яғни өзінің қабілетін компьютерлік жүйені бұзу үшін қолданылатын хакер терминдерін айыруды талап етеді.

Ақпараттық технология облысындағы заманауи маман ақпараттық қауіпсіздікпен қамтамасыз ету білімі мен дағдыларына ие болуы керек. Бұл кәсіпорын мен ұйымдардың ақпараттық жүйелерінде өте маңызды ақпарат сақталатындықтан және өңделетіндіктен, құпиялылықтың, бүтіндіктің немесе қолайлылықтың бұзылуы жағымсыз әрекеттерге әкелуі мүмкін. Сондықтан ақпараттық қауіпсіздікті қамтамасыз етудің сұрақтарына ақпараттық жүйелерді құру мен эксплуатацияның барлық сатыларында назар аударылу керек.

Берілген оқу құралында «Ақпаратты қорғау және ақпараттық қауіпсіздік» пәнінде берілетін материалдар жазылған, оны оқу барысында студенттер ақпаратты қорғау теориясын, ақпараттық қауіпсіздікті қамтамасыз ету әдістері мен құралдары туралы базалық білім, сондай-ақ ақпараттық жүйелерді қорғауды ұйымдастырудың тәжірибелік дағдыларын алады. Оқу құралы үш бөлімнен тұрады.

Бірінші бөлімде ақпараттық қауіпсіздікті қамтамасыз етуге байланысты басты түсініктер енгізілген, қауіпсіздіктің негізгі қауіптері мен оларға қарсы шаралар қарастырылған.

Екінші бөлімде криптографияның негізгі түсініктері сипатталды. Сондай-ақ симметриялық және ассиметриялық шифрлеудің кең таралған алгоритмдері, хэш-функция көмегімен дайджестердің қалыптасуы, ашық кілттер инфрақұрылымының құрылу үрдісі қарастырылды.

Үшінші бөлімде телекоммуникациялық желілер бойынша берілетін деректердің криптографиялық қорғау хаттамалары, желілерді қорғауға арналған желіаралық экрандарды пайдалану қарастырылды.

Тез жетілетін компьютерлік ақпараттық технологиялар біздің өмірімізге айрықша өзгерістер енгізуде. Қазіргі кезде ақпаратты зат ретінде қолданады, оны сатуға, ауыстыруға, алуға болады. Ақпараттық технологиялардың дамуы компьютерлік қылмыстар және солармен байланысты ақпараттың ұрлануының өсуімен қосарланып отырады. "Ақпаратқа шабуыл" дегеніміз не? Бұл сұраққа анықтама беру өте қиын, себебі ақпарат, әсіресе ол электронды түрде, жүздеген әртүрлі мағынаны білдіруі мүмкін. Келесі бөлімдерде осы сұраққа жауап ала аласыздар.

Ақпараттық қауіпсіздік сөзінің астында ақпараттық ақпаратты қолданушылар мен иелеріне зиян келетін жүйенің кездейсоқ немесе әдейілеп араласудан қорғау жатыр.

Осы оқу құралы ақпаратпен жұмыс істейтін студенттерге арналған.

1 Ақпараттық қауіпсіздіктің теориялық негіздері

1.1 Негізгі түсініктер

Бұл бөлімді меңгеруді басты түсініктер қатарын анықтаудан бастайық.

Ақпарат – ”information” латын сөзінен шыққан, түсіндіру, баяндау, мәлімет беру дегенді білдіреді.

Ақпараттық жүйе (АЖ) – объектіні басқаруға қажетті ақпаратты беру мен жаңарту, сақтау, жинақтау жүйесі.

АЖ компоненттері:

- аппараттық құралдар: ЭЕМ және құрама бөліктер (процестер, мониторлар, терминалдар, периферийлік құрылғылар, принтерлер, контроллерлер, кабельдер, байланыс линиялары) және т.б.;
- бағдарламалық қамтама: алынған бағдарламалар, негізгі, объектілі, жүктелетін модульдер, операциялық жүйелер және жүйелік бағдарламалар (компиляторлар, құрастырушылар және басқалар), утилиттер, диагностикалық бағдарламалар;
- мәліметтер – магниттік тасымалдаушылардағы тұрақты және уақытша сақталатындар, баспа архивтері, жүйелік журналдар және т.б.;
- персонал – қызмет етуші персонал және қолданушылар.

Ақпараттық жүйелерді қорғаудың мақсаты (ақпаратты өңдеу жүйесі) – қауіп-қатерге қарсы әрекеттер:

- өңделген ақпараттың жасырын бұзылу қатері;
- өңделген ақпараттың бүтіндігінің бұзылу қатері;
- жүйенің жұмыс істеуінің бұзылу қатері.

Қауіп (ақпараттық қауіпсіздік) – ақпараттық қауіпсіздіктің бұзылуының потенциалды немесе шынайы бар қаупін құратын шарттар мен факторлар жиынтығы.

Ақпараттық қауіпсіздік қаупінің қайнар көзі – ақпараттық қауіпсіздіктің қаупі туындауының басты мәселесі болып табылатын субъект (жеке тұлға, материалды объект немесе жеке құбылыс). Қауіптің қайнар көзінің типі бойынша адам қызметіне байланысты және байланысты емес болып бөледі. Мысал ретінде пайдаланушымен маңызды ақпараттың жойылуы және сәйкесінше ғимаратта өрт болуы мүмкін. Адам қызметіне байланысты қауіптер кездейсоқ және әдейі сипаттағы қауіптерге бөледі. Соңғы жағдайда қауіптің қайнар көзін тәртіп бұзушы немесе қаскүнем деп атайды.

Осалдылық (ақпараттық жүйенің) – қауіпсіздік қаупін онда өңделетін ақпаратпен қалыптасу мүмкіндігімен берілетін ақпараттық жүйенің қасиеті. Мысалы, ақпаратты электрмен қоректендіру желісінде ақаулар үшін жоғалту қаупі бар. Егер ақпараттық ресурс туралы айтсақ, онда қауіпті жүзеге асыру ақпаратты жіберу кезінде оған арналмаған адамдарға беру, ақпаратты жою немесе өзгерту, пайдаланушылар үшін ресурстардың қолжетімсіздігі сияқты келеңсіз жағдайларға әкелуі мүмкін. Демек, қауіпсіздіктің үш негізгі қауіп анықтамаларына келдік.

- әзірлік (қол жетерлік), яғни тиімді уақыт аралығында қажетті ақпараттық қызметті алу;

Құпиялық (жасырын) қаупі – құпия немесе жасырын ақпарат тұлғаға, тұлғалар тобына немесе қандайда бір мекемеге қолжетімді болып жүзеге асырылу нәтижесіндегі қауіп. Мұнда жасырын және құпия ақпарат арасындағы айырмашылықты түсіндіру керек. Көбінесе «жасырын» мемлекеттік құпиялар қатарына, ал «құпия» жеке деректер, коммерциялық құпия және т.с.с. жататын ақпаратты атайды.

Тұтастық (бүтіндік) қаупі - ақпараттың қайшылықсыз және лездік, оны құрту мен рұқсат етілмеген өзгерістерден қорғау. Автоматтандырылған жүйенің дұрыс жұмыс істеу режимінде деректер өзгеруі немесе жойылуы мүмкін екендігін атап өту керек. Бұл әрекет заңды немесе жоқ болып табылатындығы қауіпсіздік саясатымен анықталуы тиіс.

Қауіпсіздік саясаты – ақпарат қауіпсіздігі облысында құжаттандырылған ережелер, процедуралар, тәжірибелік қолданыстар немесе басқарушы принциптер жиынтығы, онымен мекеме өз қызметінде басшылық етеді. Қызмет көрсетуден бес тарту қаупі (қол жетімділік қаупі) – автоматтандырылған жүйе клиенттеріне қызмет көрсетуден бас тартуға, зиянкестердің өз қалауы бойынша ресурстарын заңсыз қолдануына әкелетін қауіп. Кейбір авторлар [3] автоматтандырылған жүйе параметрлерін ашу қаупін енгізе отырып, келтірілген жіктеуді толықтырады. Егер зиянкес жүйені заңсыз зерттеу барысында оның барлық осал жерлерін анықтаған болса, қауіп жүзеге асырылған деп есептеледі. Берілген қауіпті жанама разрядына жатқызуға болады: оны жүзеге асыру нәтижесі өңделетін ақпаратқа ешқандай зиян келтірмейді, бірақ алғашқы қауіпті жүзеге асыру үшін мүмкіндік береді. Демек, ақпарат қауіпсіздігі – бұл ақпараттық қорғалу жағдайы, сонымен қатар оның құпиялығы, қол жетімдігі мен бүтіндігі қамтамасыз етілген. Ал ақпаратты қорғау қорғалған ақпараттың сыртқа жайылып кетуін алдын алуға, қорғалатын ақпаратқа заңсыз және байқаусыз әсер етуге бағытталған қызмет ретінде анықталуы мүмкін. Ақпаратты қорғаудың келесі бағыттары ерекшеленеді:

— ақпаратты құқықтық қорғау – ақпаратты қорғау бойынша субъектілердің қатынасын реттейтін заңнамалық және нормативті құқықтық құжаттарды (акт) құрастыруды қосатын құқықтық әдістермен ақпаратты қорғау, бұл құжаттарды қолдану (акт), сондай-ақ олардың орындалуын қадағалау және бақылау;

— ақпаратты техникалық қорғау – техникалық, бағдарламалық және бағдарламалық-техникалық құралдарды қолданумен, қолданыстағы заңнамаға сәйкес қорғауға жататын ақпаратты (деректер) қауіпсіздіктің криптографиялық емес әдістерімен қамтамасыз етуден тұратын ақпаратты қорғау;

— ақпаратты криптографиялық қорғау – ақпаратты оның криптографиялық түрлендірулері көмегімен қорғау;

— Ақпаратты физикалық қорғау – қорғау объектісіне уәкілетті емес жеке тұлғалардың кіруі немесе енуі үшін кедергі келтіретін құралдар жиынтығы және ұйымдастырушылық шараларды қолдану жолымен ақпаратты қорғау.

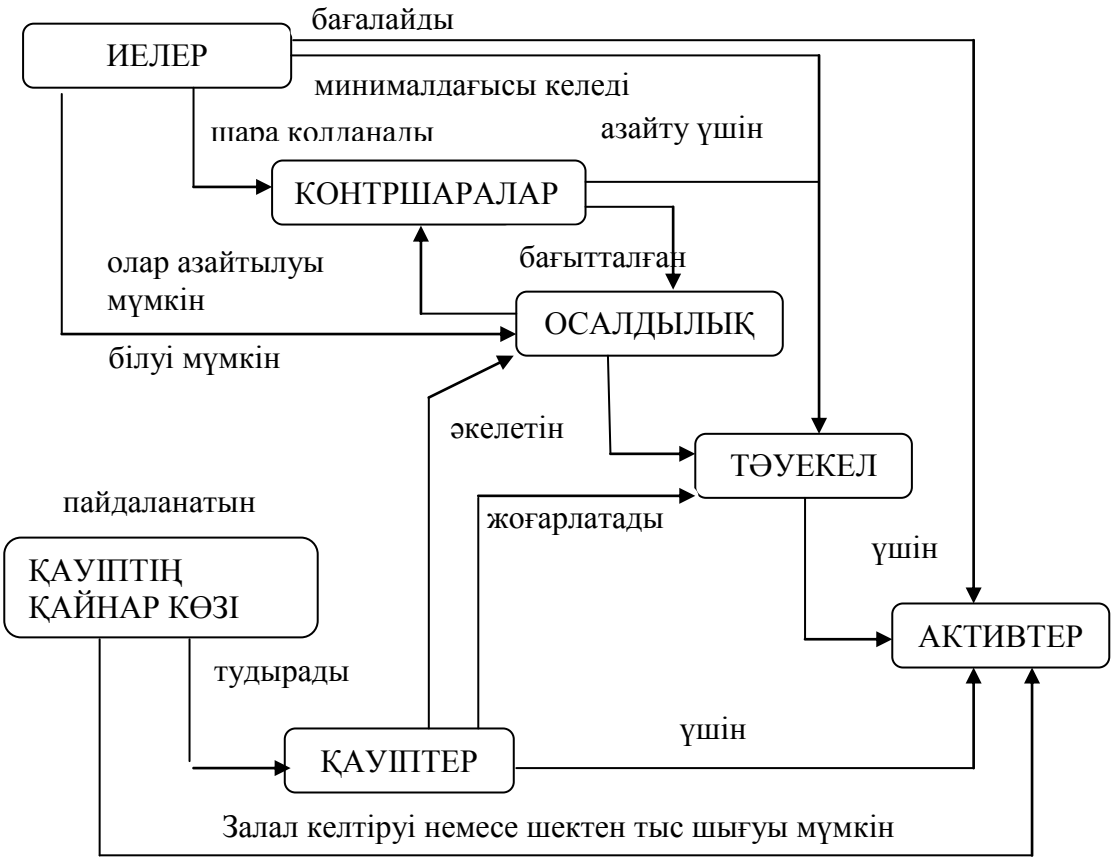
Ақпаратты қорғау қорғау тәсілдері мен құралдарын пайдаланумен жүзеге асырылады. Ақпаратты қорғау тәсілі – ақпаратты қорғаудың анықталған принциптері мен құралдарын қолдану реті мен ережелері. Ақпаратты қорғау құралдары – ақпаратты қорғауға арналған немесе қолданылатын техникалық, бағдарламалық, бағдарламалық-техникалық құралдар, зат немесе материал. Жеке бөлінетіні:

— ақпаратты қорғау тиімділігін бағалау құралдары;
— ақпаратты физикалық қорғау құралдары;
— ақпаратты қорғаудың криптографиялық құралдары.

1.2 Қауіпсіздікті қамтамасыз ету үрдісінің жалпы сұлбалары

ISO/IEC-15408 халықаралық стандартында ұсынылған қауіпсіздікті қамтамасыз етудің негізгі субъектілері мен объектілері арасындағы байланысты қарастырайық.

Қауіпсіздік активтерді қауіптен қорғаумен байланысты. Стандартты құрастырушылар қауіптің барлық түрлерін қарастыру керек деп атап өтуде, бірақ қауіпсіздік сферасында үлкен назар олардың ішінде адам қызметімен байланыстыларына арналған. 1.1-суретте қауіпсіздіктің жоғары деңгейлі түсініктері арасында өзара байланыс көрсетілген. Активтердің сақталуына олардың иелері жауап береді, олар үшін ол құнды болып табылады. Бар немесе болжанған заң бұзушылар бұл активтерге мән беруі және олардың иелерінің мүдделеріне қарсы қолдануға ұмтылуы мүмкін. Заң бұзушылардың әрекеттері қауіптің пайда болуына әкеледі. Жоғарыда айтылғандай, қауіптер жүйедегі бар осалдылық арқылы жүзеге асырылады. Активтердің иелері қарастырылып отырған жүйеге қатысты олардың қайсысы жүзеге асырылуы мүмкін екендігін анықтау үшін мүмкін қауіптерді талдайды. Талдау нәтижесінде тәуекел анықталады (яғни залал болу мүмкіндігін болжайтын құбылыс немесе жағдай) және олардың талдауы жүргізіледі.



1.1 сурет - Қауіпсіздік түсінігі және олардың өзара байланысы

Активтің иелері осалдылықты азайту үшін контршаралар қолданады және қауіпсіздік саясатын орындайды. Бірақ осы контршараларды орындаған соң да қалдық осалдылықтар және сәйкесінше – қалдық тәуекел сақталуы мүмкін.

1.3 Идентификация, аутентификация, кірумен басқару. Рұқсатсыз кіруден қорғау

Бұл бөлімде ақпаратты рұқсатсыз кіруден қорғауға байланысты сұрақтар қарастырылады.

Ақпаратты рұқсатсыз кіруден қорғау – мүдделі субъектілердің орнаған нормативті және құқықтық құжаттардың бұзылуымен қорғалған ақпаратты алуды болдырмас үшін бағытталған ақпаратты қорғау. Рұқсатсыз кіруден қорғау үшін идентификация, аутентификация және кірумен басқару қолданылады. Қосымша басқа әдістер де қолданылуы мүмкін.

Идентификация – пайдаланушыларға идентификаторларды меншіктеу (әмбебап атау немесе белгі). Сондай-ақ пайдаланушылар идентификаторынан басқа пайдаланушылар тобы идентификациясы, автоматтандырылған жүйелер ресурстары және т.с.с. жүргізілуі мүмкін. Идентификация басқа жүйелік есептер үшін қажет, мысалы, оқиғалар журналын жүргізу үшін. Көптеген жағдайда идентификация аутентификациямен бірге жүреді. Аутентификация –

түпнұсқалықты орнату – пайдаланушыға оның жария еткен идентификаторының дұрыстығын тексеру. Мысалы, автоматтандырылған жүйеде жұмыс сеансының басында пайдаланушы атауы мен парольді енгізеді. Осы деректерге сәйкес жүйе идентификация (пайдаланушы атауымен) және аутентификация (пайдаланушы атауы мен енгізілген парольді сәйкестендіріп) жүргізеді.

Кірумен басқару – жүйенің барлық ресурстарын пайдалануды реттеу жолымен ақпаратты қорғау әдісі. Идентификация мен аутентификация жүйелері кез келген ақпараттық жүйенің рұқсатсыз кіруден қорғау инфрақұрылымының кілттік элементтерінің бірі болып табылады. Көбінесе аутентификация әдістерінің 3 тобын ерекшелейді:

1) Пайдаланушыда берілген типтің әмбебап объектісінің бар болуы бойынша аутентификация. Кейде аутентификация әдісінің бұл класын ағылшын тілінде I have («менде бар») деп атайды. Мысал ретінде аутентификацияны смарт-карта немесе электронды USB-кілттер көмегімен келтіруге болады.

2) Пайдаланушыға қандайда бір құпия ақпарат белгілі болған жағдайға негізделген аутентификация - I know («мен білемін»). Мысалы, пароль бойынша аутентификация.

3) Пайдаланушының өзінің меншік әмбебап сипаттамалары бойынша аутентификация - I am («мен бармын»). Бұл әдістер сондай-ақ биометрикалық деп аталады. Аутентификацияның биометрикалық әдістері статикалық және динамикалық болып бөлінеді.

Статикалық белгілер бойынша аутентификация мысалдары – бұл саусақ ізін тексеру, көздің қарашығы, қол геометриясы, фотосуретпен салыстыру және т.с.с. Бұл әдістердің артықшылықтары жеткілікті жоғары дәлдігі болып табылады. Бірақ мұндай әдістер арнайы құрылғылардың бар болуын қажет ететінін (мысалы, арнайы сканерлер) және қолданудың шектеулі облысы бар (мысалы, саусақ ізі бойынша аутентификация кезінде, қолдың кір болғаны үшін адам аутентификацияны өте алмауы мүмкін, яғни мұндай әдістер құрылыста және көптеген кәсіпорындарда қолданылмайды) екендігін атап өту керек.

Динамикалық аутентификация мысалы – дауыс бойынша аутентификация (алдын ала анықталған сөйлем немесе дербес мәтінді айту бойынша), «пернетақталық қол жазу» бойынша аутентификация (пайдаланушының пернетақтада жұмыс істеу ерекшеліктері анықталады, мысалы, пернелерді әртүрлі үйлесімде басу кезіндегі тоқтаулар уақыты) және т.с.с. Әртүрлі кластар әдістерін біріктіретін аутентификацияның аралас схемалары қолданылады. Мысалы, екіфакторлы аутентификация – пайдаланушы жүйеге смарт-картаны береді және оны белсендіру үшін пин-код енгізеді.

Аутентификация *біржақты*, бір тарап басқасын аутентификациялағанда (мысалы, сервер клиенттің шынайылығын тексереді), және тараптар шынайылықты өзара тексеру жүргізгенде *екіжақты* болуы мүмкін. Сондай-ақ

аутентификация *тікелей*, яғни аутентификация процедурасында екі тарап ғана қатысқанда немесе *сенім білдіретін тараппен* қатысу болып бөлінеді. Соңғы жағдайды аутентификация үрдісінде бір бірінің шынайылығын тексеретін тараптар ғана қатысады. Осы үшінші тарапты кейде аутентификация сервері (ағылшын тілінен «authentication server») немесе арбитр (ағылшын тілінен «arbitrator») деп те атайды.

1.3.1 Аутентификацияның парольдік жүйесі.

Қазіргі кезде ең таралған болып аутентификацияның парольдік жүйесі табылады. Мұндай жүйелерді сипаттау кезінде қолданылатын түсініктер қатарын анықтайық.

Пайдаланушы идентификаторы – парольдік жүйенің жеке пайдаланушыларын ерекшелеуге мүмкіндік беретін әмбебап ақпарат (идентификация жүргізу). Бұл жүйеде пайдаланушының есептік жазба атауы немесе генерацияланатын әмбебап сандық идентификатор болуы мүмкін.

Пайдаланушы паролі – аутентификациядан өту үшін қолданылатын, пайдаланушыға ғана белгілі жасырын ақпарат. Жүйенің жүзеге асырылуына байланысты пароль бір реттік немесе көп реттік болуы мүмкін. Бір реттік парольдермен жүйелер аса сенімді болып табылады. Оларда парольді алып алумен байланысты кейбір тәуекелдер алып тасталады, яғни пароль бір ғана сессияға жарамды, ал егер заңды пайдаланушы оны іске қосса, зиянкес мұндай парольді қайта пайдалана алмайды. Бірақ көп реттік парольдермен жүйелерді жүзеге асыру оңай және қолдауда арзан, сондықтан олар кең таралған.

Пайдаланушының есептік жазбасы – пайдаланушыны сипаттау үшін арналған идентификатор, пароль және қосымша ақпарат жиынтығы. Есептік жазбалар парольдік жүйенің деректер базасында сақталады.

Парольдік жүйе – бұл парольді тексеру жолымен компьютерлік жүйе пайдаланушысының идентификация және аутентификация функцияларын іске асыратын бағдарламалық немесе бағдарламалық-аппараттық кешен. Жеке жағдайда мұндай жүйелер қосымша функцияларды орындай алады, яғни криптографиялық кілттерді генерациялау және үлестіру және т.с.с. Демек, парольдік жүйе өзіне пайдаланушы интерфейсін, басқару интерфейсін, есептік жазба базасын, қауіпсіздіктің ішкі жүйелерінің басқа компоненттермен түйісу модульдерін қосады.

Көп реттік парольдерді қолданатын парольдік жүйелерді басқару бойынша кейбір нұсқауларды қарастырайық:

1) Парольдер жүйесінде қолданылатын минималды ұзындықты беру. Бұл парольдерді таңдау жолымен шабуылды қиындатады. Яғни 6-8 символдан тұратын минималды ұзындықты орнату ұсынылады.

2) Парольде символдардың әртүрлі топтарын пайдалану талаптары қойылады, яғни кіші және үлкен әріптер, сандар, арнайы символдар. Бұл жай таңдауды қиындатады.

3) «Сөздік бойынша» парольдерді (яғни «1234» сияқты символдардың табиғи тіл сөздері мен қарапайым комбинацияларды пароль ретінде қолдануға тексеру) таңдау сияқты шабуылдарды имитациялау жолымен қолданылатын парольдердің сапасын қауіпсіздік басқарушысымен мезгіл сайын тексеру.

4) Парольдер өмірінің максималды және минималды мерзімдерін орнату, ескі парольдерді міндетті ауыстыру механизмін қолдану. Бұл шараны ендіру кезінде пайдаланушының төмен біліктілігін есепке алу керек, басқарушыдан «жүйе одан не қажет ететінін» пайдаланушыға түсіндіру бойынша қосымша күш қажет етеді.

5) Парольді енгізудің сәтсіз әрекеттерінің санын шектеу (жүйеге кіруде есептік жазбаны сәтсіз әрекеттердің берілген санынан кейін блокқа түсіру). Берілген шара парольдерді таңдау жолымен шабуылдан қорғауға мүмкіндік береді. Бірақ ойланбай кіру кезінде қосымша мәселелерге әкелуі де мүмкін, заңды пайдаланушылар немқұрайлығынан парольді енгізуде қате кетіргені үшін өзінің есептік жазбаларын блокқа түсіруі мүмкін, бұл басқарушыдан қосымша күшті қажет етеді.

6) Парольдердің тарих журналын жүргізу, яғни пайдаланушы парольді мәжбүрлі ауыстырған соң өзіне ескі, мүмкін шынайы емес парольді қайта таңдап алмауы үшін керек.

1.4 Қауіпсіздік модельдері

Алдыңғы бөлімде айтылғандай, автоматтандырылған жүйелердің қауіпсіздігін қамтамасыз ету үрдісіндегі маңызды саты қауіпсіздік саясатын құру болып табылады. Егер қауіпсіздік саясаты жоқ болса, ақпаратқа кірудің заңды және заңсыз кіру арасында ажыратуларды нақты жүргізу мүмкін емес. Қауіпсіздік саясаты формальді немесе формальді емес сипатталуы мүмкін. Қауіпсіздік саясатын формальді сипаттау қауіпсіздік модельдері аясында жүргізіледі. Қауіпсіздік моделін жүйенің бүкіл класының мінезін абстрактті сипаттау сияқты анықтауға болады. Қауіпсіздіктің көптеген модельдері «мән», «субъект», «объект» терминдерімен беріледі.

Мән – қорғалатын автоматтандырылған жүйенің кез келген аталған құрамы.

Субъект – ресурстар сұранысын негіздеуге және оларды қандайда бір есептеу операцияларын орындау үшін қолдануға мүмкіндік беретін белсенді мән. Субъект ретінде жүйеде орындалатын бағдарлама немесе «пайдаланушы» (шынайы емес адам, ал мән ол автоматтандырылған жүйе) болуы мүмкін.

Объект – ақпаратты сақтау немесе алу үшін қолданылатын белсенді емес мән. Объект ретінде мысалы, деректермен файл қарастырылуы мүмкін. Көбінесе объект пен субъектті айырудың қатесіз әдісі бар деп болжанады.

Қол жеткізу – субъект пен объект арасындағы өзара әрекет, оның нәтижесінде олардың арасында ақпаратты ауыстыру жүргізіледі. Қол жеткізудің екі негізгі типі: оқу – нәтижесі объекттен субъектке ақпаратты

ауыстыру болып табылатын операция; жазба - нәтижесі субъекттен объектке ақпаратты ауыстыру болып табылатын операция.

Сондай-ақ объектілер қауіпсіздігінің мониторы бар деп болжанады, яғни объектке кез келген қатынау кезінде белсендірілетін субъект, заңды және заңсыз қатынауды ажырата алады (белгілі бір ережелер негізінде) және заңды кіруге ғана рұқсат етеді.

Әдебиетте қауіпсіздік саясаты моделінің үш негізгі класын ерекшелейді: дискрециялық, мандаттық және рольдік.

Қауіпсіздік саясатының дискрециялық (таңдаулы) негізін қол жеткізуді дискрециялық басқаруды құрайды, ол келесі қасиеттермен сипатталады [3]:

— барлық субъектілер мен объектілер идетификацияланған болуы керек;

— жүйенің субъекттен объектке кіру құқығы жүйеге қатысты қандайда бір сыртқы ережесі негізінде анықталады.

Қол жеткізудің дискрециялық басқару ережесі жиі қол жеткізу матрицасымен беріледі. Мұндай матрицада жолдар жүйенің субъектілеріне, бағандар – объектілеріне сәйкес келеді, матрицаның элементтері «субъект-объект» сәйкес жұбы үшін қол жеткізу құқығын сипаттайды.

Белгілі дискрециялық модельдердің бірі Харрисон–Рузо–Ульманның моделі болып табылады, жиі матрицалық модель деп атайды.

Қол жеткізуді басқарудың бұл типі көбінесе операциялық жүйелерді қолданылады, өйткені жүзеге асыруда өте қарапайым. Бұл жағдайда қол жеткізуді басқару ережесі қол жеткізуді басқару тізімі (ағылшын тілінен «Access Control List», қысқаша ACL) арқылы жиі сипатталады. Тізім қорғалатын объектпен байланысты және субъектілер тізімін, олардың берілген объектке рұқсатын сақтайды. Мысал ретінде Windows NT жанұясының операциялық жүйелерінде NTFS файлдық жүйесінде файлға пайдаланушылар мен топтардың кіру құқықтарын сипаттау үшін ACL қолдануды келтіруге болады.

Қауіпсіздік саясатының мандатты негізін қол жеткізуді мандатты басқару құрайды, ол мынаны білдіреді:

— барлық субъектілер мен объектілер идетификацияланған болуы керек;

— жасырындылық белгісінің сызықты реттелген жиыны берілген;

— жүйенің әрбір объектісіне жасырындылық белгісі меншіктелген, ол ондағы бар ақпараттың құндылығын, яғни жасырындылық деңгейін анықтайды;

— жүйенің әрбір объектісіне жасырындылық белгісі меншіктелген, ол оған сенімділіктің деңгейін, яғни қол жеткізу деңгейін анықтайды;

— субъектінің объектіге қол жеткізу рұқсаты туралы шешімді қол жеткізу типі және субъект пен объект белгілерін салыстырудан қабылданады. Қауіпсіздіктің мандатты саясатын көбінесе Белла–ЛаПадула моделінің терминдерінде сипаттайды.

Рольдерге негізделген қол жеткізуді басқару «роль», «пайдаланушы», «операция» терминдерінде қолданылады. Барлық ақпарат тиесілі (пайдаланушыға емес, ал оның құрастырушысына) мекеме ретінде қарастырылады. Қол жеткізуге рұқсат беру немесе бас тарту туралы шешім пайдаланушы мекемеде орындайтын функция туралы ақпарат негізінде қабылданады. Рольді әрекеттер жиыны ретінде түсінуге болады, ол оның қызметтік міндеттерін орындау үшін пайдаланушыға рұқсат етілген. Басқарушы рольді сипаттайды және пайдаланушыларды берілген рольді орындауға жарғылық (авторизация) етеді. Демек, рольдік модельдер мандаттық белгілер, сондай-ақ таңдамалы модель белгілерінен тұрады.

Бақылау сұрақтары.

1. Ұлттық қауіпсіздендірудің негізгі түсініктерін атаңыз.
2. Қауіпсіздендірудің түрлеріне: мемлекеттік, экономикалық, қоғамдық, әскери, ақпараттық, экологиялық түсініктеме беріңіз.
3. Ақпараттық қауіптер және олармен күресу жолдары.
4. Ақпаратты қорғау жүйелерінің сипаттамалық қасиеттері.
5. Ақпаратты қорғау әдістері және құрал-жабдықтары.
6. Ақпараттық қауіпсіздікті қолдаудың мақсаттары.
7. Ақпараттық қауіпсіздіктің аспектілері.
8. Ақпараттық қауіпсіздіктің негізгі қауіптерін атаңыз.

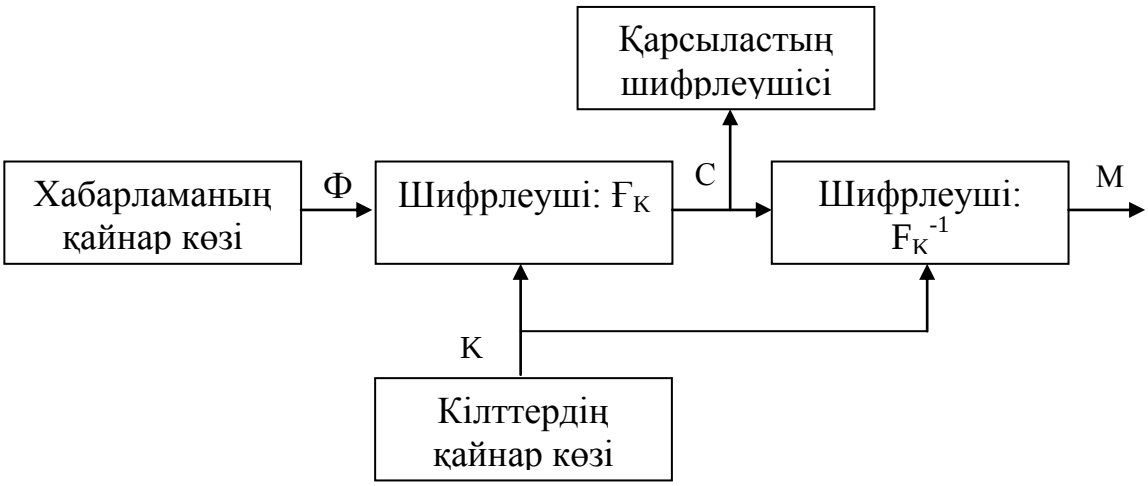
2 Криптография негіздері

2.1 Негізгі түсініктер. Шифрлердің жіктелуі

Ертеде криптография (грек тілінен аударғанда «құпия жазба») хабарламаны жасырын жіберу әдісі ретінде туындады. Бұл мақсатта қандайда бір жалпы қабылданған тілді қолдану арқылы жазылған хабарлама кілт деп аталатын қосымша ақпаратты басқарумен түрлендірілді. Криптограмма деп аталатын түрлендіру нәтижесі толық көлемде алғашқы ақпараттан тұрады, бірақ ондағы белгілер тізбегі сырт көзге кездейсоқ көрсетіледі және кілтті білмесе алғашқы ақпаратты қалпына келтіру мүмкіндігі болмайды. Түрлендіру процедурасы шифрлеу, кері түрлендіру – шифрден алу деп аталады.

Қазір криптографияны ақпараттың құпиялығы және шынайылығын (бүтіндік пен түпнұсқалық) қамтамасыз ететін математикалық әдістер туралы ғылым деп атау қабылданған. Криптографиялық қорғауды еңсеру әдістерін зерттеу мақсатымен криптоталдау айналысады. Криптография мен криптоталдау жиынтығын белгілеу үшін «криптология» термині пайдаланылады. Шифрлер бірдің заманымызға дейін ғылыми бағыт ретінде қолданылса да қазіргі криптография өте жас. Берілген облыста маңызды жұмыстардың бірі Клод Шеннонның «Жасырын жүйелерде байланыс

теориясы» атты 1949 жылы ашық баспада жарияланған мақаласы болып табылады. 2.1-суретте Шеннонмен ұсынылған жасырын жүйелер сұлбасы бейнеленген [7]. Жіберуші тарапында ақпараттың екі қайнар көзі бар, олар хабарламаның қайнар көзі мен кілттің қайнар көзі. Кілттің қайнар көзі барлық мүмкін кілттер жиынының ішінен бір K кілтін таңдайды, ол осы кезде қолданылады. Кілт оны жолдан алып алуға болмайтындай хабарламаны жіберуші мен алушыға жібереді.



2.1 сурет - Жасырын жүйенің сұлбасы

Шифрлеушімен М хабарламаға қолданылған F_K көрсету С криптограммасын береді:

$$C=F_K M. \quad (2.1)$$

Алушы К белгілі кілті кезінде С криптограммасынан М хабарламаны қалпына келтіру мүмкіндігіне ие болу керектігіне байланысты F_K көрінісі F_K^{-1} жалғыз кері көрініске ие болады, яғни:

$$M=F_K^{-1} C. \quad (2.2)$$

Жасырын жүйе (немесе қазіргі терминологияда – шифр) мүмкін хабарламалар жиынын криптограмма жиынына бірмәнді кері көрсету жанұясы ретінде анықталады. К кілтін таңдау қандай F_K элементі қолданылатындығын анықтайды. Қарсыласқа қолданылатын жүйе белгілі деп есептелсін, яғни $\{F_i \mid i=1..N\}$ көрініс жанұясы мен әртүрлі кілттерді таңдау ықтималдығы. Бірақ ол қандай кілт таңдап алынғанын білмейді, қалған мүмкін кілттер ол үшін шынайы кілт сияқты.

Ақпаратты заңды алушы үшін хабарламаны шифрден алу үрдісі шифрлеу кезінде қолданылатын, көрінісіне кері, криптографиялық көріністерін қолданудан тұрады.

Қарсылас үшін шифрден алу үрдісі өзінде тек әртүрлі кілттер мен хабарламалардың криптограммасы мен априорды ықтималдықтары ғана бар хабарламаларды анықтау мүмкіндіктерін көрсетеді.

Шифрлейтін көріністі табу үшін жеткіліксіз кез келген көлемде алынған ақпарат үшін шифрлер бар. Мұндай типтегі шифрлер шартсыз төзімді деп

аталады. Басқа сөзбен айтқанда, шартсыз төзімді болып криптоаналитик белгісіз криптограмма кезіндегі бағамен салыстыру бойынша С криптограммасын білу негізінде М алғашқы хабарламаны бағалауды жақсарта алмайтын шифрлер табылады.

Басқа типтің шифрлері алынған деректердің белгілі бір көлемі кезінде кілтті анықтау теориялық тұрғыда мүмкін екендігімен сипатталады. Криптограмманың минималды көлемі жалғыздықтың интервалы деп аталады. Бірақ шектелген есептеу ресурстарымен ие криптоаналитик үшін ақпараттың құнды болуы кезіндегі уақытта шешімін табу әлдеқайда аз. Мұндай типтегі шифрлер шартты төзімді деп аталады. Олардың төзімділігі шифрлерді «бұзудың» жоғары есептік күрделілігіне негізделген. Қазір қоданылатын көптеген ифрлер осы типке жатады.

Шартсыз төзімді шифрлер бар екендігі дәлелденген. Бірақ оларды тұрғызу үшін хабарламаның ұзындығына тең ұзындығы бар тең ықтималды кездейсоқ кілтті қолдану қажет. Бұл шартты ұстанған кезде түрлендіру процедурасының өзі жеткілікті оңай болуы мүмкін.

Келесі мысалды қарастырайық. Екілік кодтауда көрсетілген М хабарламаны жіберу керек болсын. Хабарламаның келесі символы 1 тең болу ықтималдығы q, 0 – (1 – q) тең. Криптограмма К шексіз, кездейсоқ, тең мөлшерде үлестірілген кілттермен хабарламаны 2 модулі бойынша биттік қосу жолымен алынады:

$$C=M\oplus K. \qquad (2.3)$$

Мұндай түрлендіруді гаммалау деп те, ал К кілтін кілттік гамма деп атайды. Криптограмманың келесі символы 1 тең болатындай ықтималдықты анықтайық. Егер алғашқы хабарламада сәйкес символ 0 тең, ал кілтте – 1 немесе хабарламада – 1, кілтте – 0 тең болғанда болады. Оқиғалардың осы жұбы қарама-қарсы, сондықтан ықтималдықтарды қосу формуласын қолдану керек:

$$p(C=1)=(1-q)x0,5+qx0,5=0,5. \qquad (2.4)$$

Сонымен, криптограммада бірліктің пайда болу ықтималдығы алғашқы хабарламаның статистикалық қасиетіне байланысты емес. Криптограмманы талдай отырып, қаскүнем алғашқы хабарлама туралы қосымша ақпаратты ала алмайды. Мұндай қасиеттермен тек кездейсоқ шексіз тең мөлшерлі үлестірілген кілттер ғана ие екендігін атап өту керек. Егер кілтте бірліктің пайда болу ықтималдығы 0,5 ерекшеленсе, онда (2.4) формуладағы q нәтижеден алып тастау мүмкін емес.

Жақсы шифр қандай қасиеттерге ие болу керектігін қарастырайық. Біріншіден, шифрлеу мен шифрден алу шифр қолданатын шарттарда ғана жеткілікті тез жүзеге асырылуы керек (ЭЕМ пайдалану арқылы, қолмен шифрлеу кезінде және т.с.с.). Екіншіден, шифр хабарламаны сенімді қолғау керек, яғни ашуға төзімді болуы керек.

Криптотөзімділік – криптоталдау әдістерімен ашуға шифрдің төзімділігі. Ол шифрге шабуыл үшін қолданылатын алгоритмдердің есептеу күрделігімен анықталады. Есептеу күрделігі уақытша және біршама

күрделілікпен сыйымдылық өлшенеді. Алгоритмнің күрделілігін анықтау үшін нақты есеппен есептің өлшемі деп аталатын сан байланысады, ол енгізілетін деректер санымен сипатталады. Мысалы, сандарды көбейту есептері үшін өлшем жиындардың ең үлкенінің ұзындығы болуы керек.

Уақытша күрделілік (немесе қарапайым күрделілік) – бұл есептің өлшемімен функция ретінде қарастырылатын есептің шешімі үшін алгоритммен жұмсалатын уақыт. Күрделілікті қандайда бір элементарлы операциялар санымен өлшейді. Сыйымдылықты күрделілік – есептің өлшемінен функция ретінде деректердің жұмысы барысында алынған, сақтау үшін қажет жады көлемі.

Төзімді шифрге өте маңызды талап голландық криптограф Огюст Керкгоффспен (Auguste Kerckhoffs) XIX ғасырда қалыптастырылған. Осыған сәйкес шифрлеудің сенімділігін бағалау кезінде қарсылас қолданылатын кілттен басқа шифрлеудің қолданылатын жүйесі туралы барлығын білетіндігін болжау қажет. Берілген ереже ақпаратты қорғауды ұйымдастырудың маңызды принципін көрсетеді: жүйенің қорғалуы ұзақ мерзімді элементтер жасырындылығына тәуелді болуы қажет емес (яғни жасырын ақпараттың ұрлануы кезінде тез өзгертуге мүмкін емес болатын элементтер).

Криптоталдау есептерінің бірнеше жалпыланған қойылымдары бар. Олардың барлығы криптоаналитикке шифрлеудің қолданылған алгоритмі мен алынған криптограммасы белгілі деген болжамнан қалыптасады. Мыналар қарастырылуы мүмкін:

— белгілі криптограмма ғана бар болған кездегі шабуыл;

— ашық мәтінінің белгілі фрагменті бар болған кездегі шабуыл. Бұл жағдайды криптоаналитик криптограммаға, сондай-ақ олардың сәйкес алғашқы хабарламаларының кейбіреуіне кіру құқығына ие. Мақсаты – шифрлеу кезінде қолданылатын кілтті анықтау немесе барлық қалған хабарламаны шифрден алу. Шабуылдың берілген класының түрлілігі – ашық мәтінді таңдау мүмкіндігімен шабуыл (криптоаналитик шифрлеу үшін мәтінді қосып және оған сәйкес криптограмманы алу мүмкіндігі);

— аппараттық шифраторларды жүзеге асыру ерекшеліктерін қолданатын шабуылдар. Жеке жағдайда, құрылғыдан жылу және электрмагниттік сәулелер талдануы, аппаратураға бір рет әсер етуден кейін қатенің таралуы (электр көзінің сымы бойынша немесе басқаша түрде) және т.с.с.;

— мүмкін кілттердің жиынын толық таңдау әдісімен шабуыл. Берілген шабуыл «қатаң күшпен әдіс шабуылы» деп те аталады (ағылшын тілінде «brute force»).

2.1.1 Шифрлердің түрлері.

Шифрлердің әртүрлі белгілері бойынша жіктелуін қарастырайық. Түрлендіру типі бойынша шифрлерді мына топтарға бөлуге болады:

- алмастыру шифрі (орнына қою);
- орын ауыстыру шифрі;
- гаммалау шифрі;
- аналитикалық түрлендіру негізіндегі шифрлер.

Кейбір қазіргі шифрлер түрлендірудің әртүрлі типтерін бірге қолданатынын ескеру керек.

Алмастыру шифрі: түрлендіру шифрленетін мәтін символы алмастырудың алдын ала келісілген сұлбасына сәйкес белгілі бір алфавиттің символдарымен (криптограмма алфавиті) алмастырылатындығынан тұрады.

Алмастыру біралфавитті және көпалфавитті болып бөлінеді. Бірінші жағдайда, алғашқы хабарламаның алфавитінің белгілі бір символына әрдайым криптограмма алфавитінің бір символы сәйкесінше қойылады. Берілген кластың ең белгілі шифрінің бірі Цезарь шифрі. Онда алфавиттің әрбір әрпі одан кейінгі келесі екінші символмен алмастырылды. Орыс алфавиті жағдайында, «а» әрпі «в» әрпіне, «б» әрпі «г» әрпіне және т.с.с. алмасады. Алфавит шегіне жеткенде «я» әрпі «б» әрпіне алмастырылды. Берілген жағдайда кілт ретінде алфавит символын «шегеретін» сан болды, біздің жағдайда – 2. Мұндай шифрлердің артықшылығына түрлендіру қарапайымдылығын жатқызуға болады. Бірақ олар табиғи тілде және криптограммада әртүрлі символдардың пайда болу жиілігін салыстыру жолымен тез шешілетін.

Көпалфавитті қойылымды қолданған кезде қосымша параметрлер есепке алынады (мысалы, түрленетін символдың мәтіндегі орны) және оларға сәйкес алғашқы алфавит символы шифрмәтін алфавитінің бірнеше символдарының біріне алмастырылады. Мысалы, хабарламаның тақ символдары бір ереже бойынша, оң символдары басқаша алмастырылады.

Орын ауыстыру шифрі: шифрлеу алғашқы мәтін символдары осы мәтін блогының шегінде белгілі бір ереже бойынша орын ауыстыратындығынан тұрады. Блоктың жеткілікті ұзындығы кезінде және орын ауыстырудың қайталанбайтын ретінің күрделілігімен шифрдің жеткілікті төзімділігіне жетуге болады.

Гаммалау шифрі шифрленетін мәтін символдары шифрдің гаммасы немесе кілттік гамма деп аталатын белгілі

Гаммалау шифрі шифрленетін мәтін символдары шифрдің гаммасы немесе кілттік гамма деп аталатын белгілі бір кездейсоқ тізбек символдарымен қосылатындығынан тұрады. Шифрлеу төзімділігі шифр гаммасының қайталанбайтын бөлігінің ұзындығымен (периоды), сондай-ақ гамманың келесі элементтерін алдыңғысы бойынша табу күрделілігімен анықталады.

Аналитикалық түрлендірумен шифрлеу мәтін түрленетін аналитикалық ережелерді (формулалар) қолдану түсіндіріледі.

Кілттерді қолдану типі бойынша шифрлер мыналарға бөлінеді:

- симметриялық, ақпаратты шифрлеу және шифрлеуден алу үшін бір кілтті қолданатын;

- асимметриялық, шифрлеу және шифрден алу үшін екі әртүрлі кілтті қолданатын әдіс.

Түрленетін блок өлшемі бойынша шифрлер блоктық және ағымдық болып бөлінеді.

Блоктық шифрлер тіркелген ұзындықты блоктармен ақпаратты түрлендіруді жүзеге асырады. Егер шифрленетін хабарлама ұзындығы блоктың өлшеміне тең емес болса, онда оны арнайы түр тізбегінің қажет ұзындығына дейін қосады. Мысалы, ол 100…0 тізбегі болуы мүмкін. Шифрден алған соң соңғы блокты оң жақтан сол жаққа қарай қарайды және «құйрығын» бірінші бірлікке дейін лақтырады. Мұндай қосымша барлық жағдайларда қолданбалы болу үшін, егер хабарлама блок ұзындығына тең болса, оның соңына көрсетілген түрдің бүкіл блогын қосу керек.

Ағымдық шифрлер хабарламаны элемент бойынша түрлендіруге арналған (элемент бит, символ және т.с.с. болуы мүмкін). Мұндай шифр түрінің мысалы гаммалау шифрі болып табылады.

2.2 Симметриялық шифрлер

2.2.1Фейстель сұлбасы.

Қазіргі блоктық шифрлер жиі шифрлеу раунды деп аталатын түрлендіру операциясының қандай да бір жиынының бірнеше рет қайталануы негізінде құрылады.

Әрбір раундта кілттің раунды деп аталатын кілттің қандайда бір бөлігі қолданылады. Раундтық кілттің генерациялау реті мен қолданылуы шифрлеу кілтің пайдалану кестесі деп аталады.

Мұндай итеративті түрленудің жалпы түрі келесі формуламен сипатталуы мүмкін:

$$B_i=E(B_{i-1}, K_i), \qquad (2.5)$$

мұнда E – шифрлеудің раундтық функциясы;

B_i – кіру блогы;

B_{i-1} – і-ші раунд үшін кіру блогы;

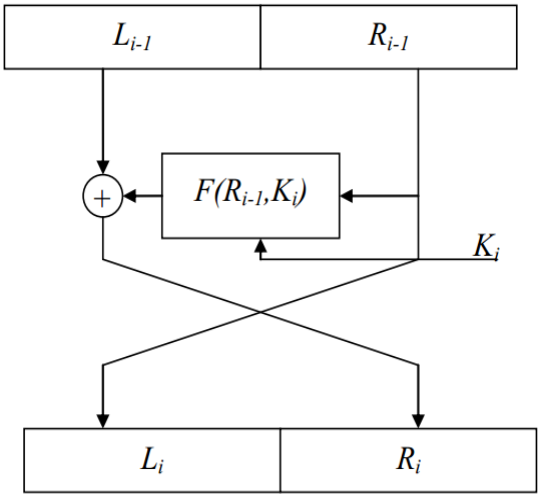
K_i – і-ші раундта қолданылатын кілт; i=1,.., N, мұнда N – раундтар саны. E түрленуі кері қайтарылмалы болуы керек. D – дешифрлеудің раундтық функциясы болсын. Сонда кері түрлендірудің раунды мына формуламен сипатталады:

$$B_i=D(B_{i-1}, K_{N-i+1}). \qquad (2.6)$$

Мұнда түзу және кері түрлендіру жағдайында кілттердің қолданылу кестесіне назар аудару керек. Мұндай шифрлеуде, бірінші раунта бірінші раундтық кілт, шифрден алу кезіндегі бірінші раундта соңғысы қолданылатын болады.

Итерациялық блоктық шифрлерді құрастыру үшін Хорст Фейстельмен (Horst Feistel) 1970 жылдардың басында ұсынылған сұлба кең қолданылады. Бұл сұлба Фейстель желісі деп те аталатын 2.2-суретте келтірілген. Оның артықшылығы ол кері айналатын шифрлейтін түрлендірулерді жүзеге асыру

үшін Ғ кез келген функциясын қолдануға мүмкіндік беретіндігі болып табылады.



2.2 сурет - Фейстель сұлбасы бойынша түзу түрлендіру

Хабарламаның кіру блогы ұзындығы бойынша екі теңжартылай блокқа бөлінеді: сол жағы – L, оң жағы– R.

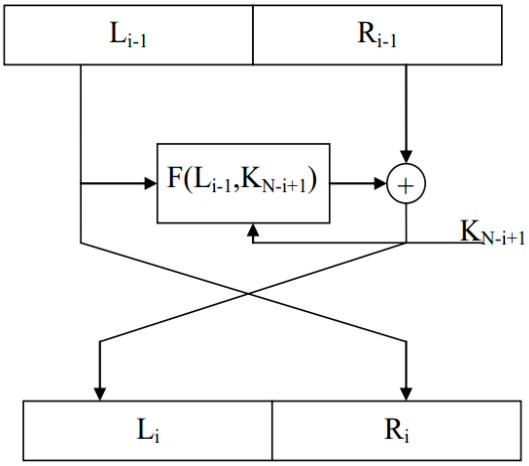
Түзу түрлендіру келесі қатынастарға сәйкес жүзеге асырылады:

$$L_i=R_{i-1};$$
$$R_i=L_{i-1}\oplus F(R_{i-1}, K_i), \qquad (2.7)$$

мұнда $\oplus$ - 2 модулі бойынша биттік қосу операциясы (2.1-кестеде оның анықтамасы келтірілген). Онда деректердің алғашқы блогы – бұл $L_0|R_0$, ал $L_N|R_N$–деректердің шығу блогы.

2.1 кесте - 2 модулі бойынша қосу операциясы

X	Y	X⊕Y
0	0	0
0	1	1
1	0	1
1	1	0



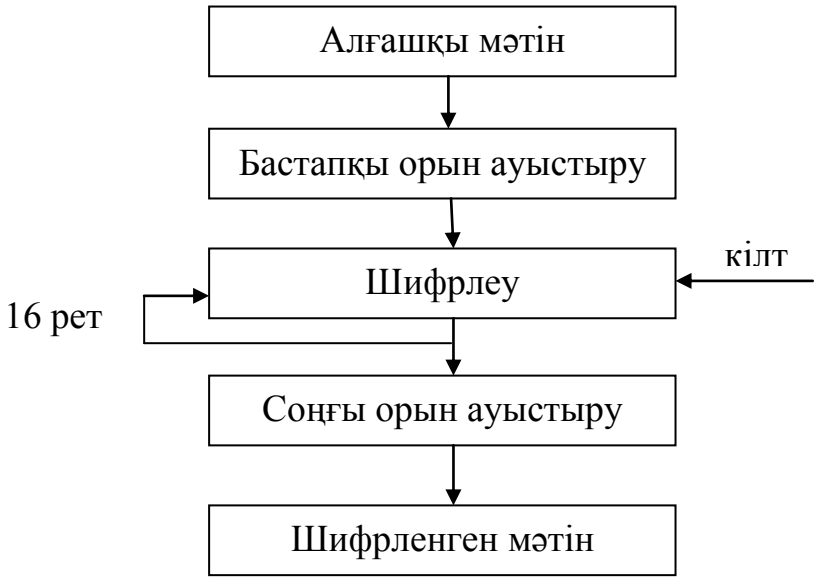
2.3 сурет - Фейстель сұлбасы бойынша кері түрлендіру

2.1-кестеде көріп отырғандай, операндтардың барлық мүмкін мәндері үшін мына қатынас орындалады: $(X \oplus Y) \oplus Y = X$. Түрлену кезінде осы қасиеттің өзі Ғ басқа қайтарылмайтын функциялар санында қолдануға және оған қарамастан кері түрлендіру жүргізуге мүмкіндік береді. Фейстель бойынша кері түрлендіру 2.3-суретте көрсетілген және мына формулалармен сипатталады:

$$R_i = L_{i-1};$$
$$L_i = R_{i-1} \oplus F(L_{i-1}, K_{N-i+1}). \quad (2.8)$$

2.2.2 DES шифрі.

DES (Data Encryption Standard) 1978 жылы қабылданған, деректерді криптографиялық жабудың американдық стандарты блоктық шифрлердің бірі болып табылады. Фейстель әдісіне негізделген DES 56-биттік кілт көмегімен деректердің 64-биттік блоктарын шифрлеуді жүзеге асырады. DES-те дешифрлеу шифрлеуге кері операция болып табылады және шифрлеу операциясын кері тізбекте қайталау жолымен орындалады. Шифрлеу процесі 64-биттік блок биттерін бастапқы орынға қою, шифрлеудің 16 циклін және биттерді кері орын ауыстырудан тұрады (2.4 сурет).



2.4 сурет - DES шифраторы

Бастапқы орын ауыстырудың Р матрицасы мына түрге ие

58	50	42	34	26	18	10	02
60	52	44	36	28	20	12	04
62	54	46	38	30	22	14	06
64	56	48	40	32	24	16	08
57	49	41	33	25	17	09	01
59	51	43	35	27	19	11	03

61	53	45	37	29	21	13	05
63	55	47	39	31	23	15	07

Файлдан кезекті 8-байттық Т блогы оқылады, ол бастапқы орын ауыстырудың Р матрицасы көмегімен түрленеді, яғни Т блогының 58 номері бар биті 1 номері бар бит, 50 номері бар бит – 2 номері бар бит және т.с.с. болады, нәтижесінде: T(0)=P(T). Бастапқы орын ауыстырудың криптотөзімділікке әсері туралы ештеңе белгісіз. Ол деректерді байт бойынша жүктеу үшін DES аппараттық қалыптасуында пайдаланылды деп есептеледі. Орын ауыстыру деректердің әрбір байтының алдымен оң биттерін (2,4,6,8), содан теріс биттерін таңдауға сәйкес келеді (1,3,5,7). Бірақ, бастапқы орын ауыстыруды орындау DES стандартымен сәйкестікті қамтамасыз ету үшін қажет.

Содан соң алынған T(0) биттер тізбегі екі тізбекке, әрбіреуі 32 бит бойынша бөлінеді: L(0) – сол немесе үлкен биттер, R(0) – оң немесе кіші биттер. Содан 16 итерациясымен 2.5-суретте көрсетілгендей Фейстель әдісі бойынша шифрлеу орындалады, і –ші итерация келесі түрде сипатталады:

— L(i)=R(i−1)

— R(i)=L(i-1)⊕F(R(i-1),K(i)),

Мұнда L(i)и R(i) – бұл і-ші тактте сол және оң ішкі тізбектер, K(i)- 64 биттік кілттен алынған 48 биттік кілт. 16-шы итерацияда R(16) мен L(16) (орын ауыстырусыз) тізбектерін алады, олар (R(16), L(16)) ні 64-биттік тізбекке біріктіреді. Содан осы тізбектің биттерін P-1 кері орын ауыстыру матрицасымен сәйкес орын ауыстырады.

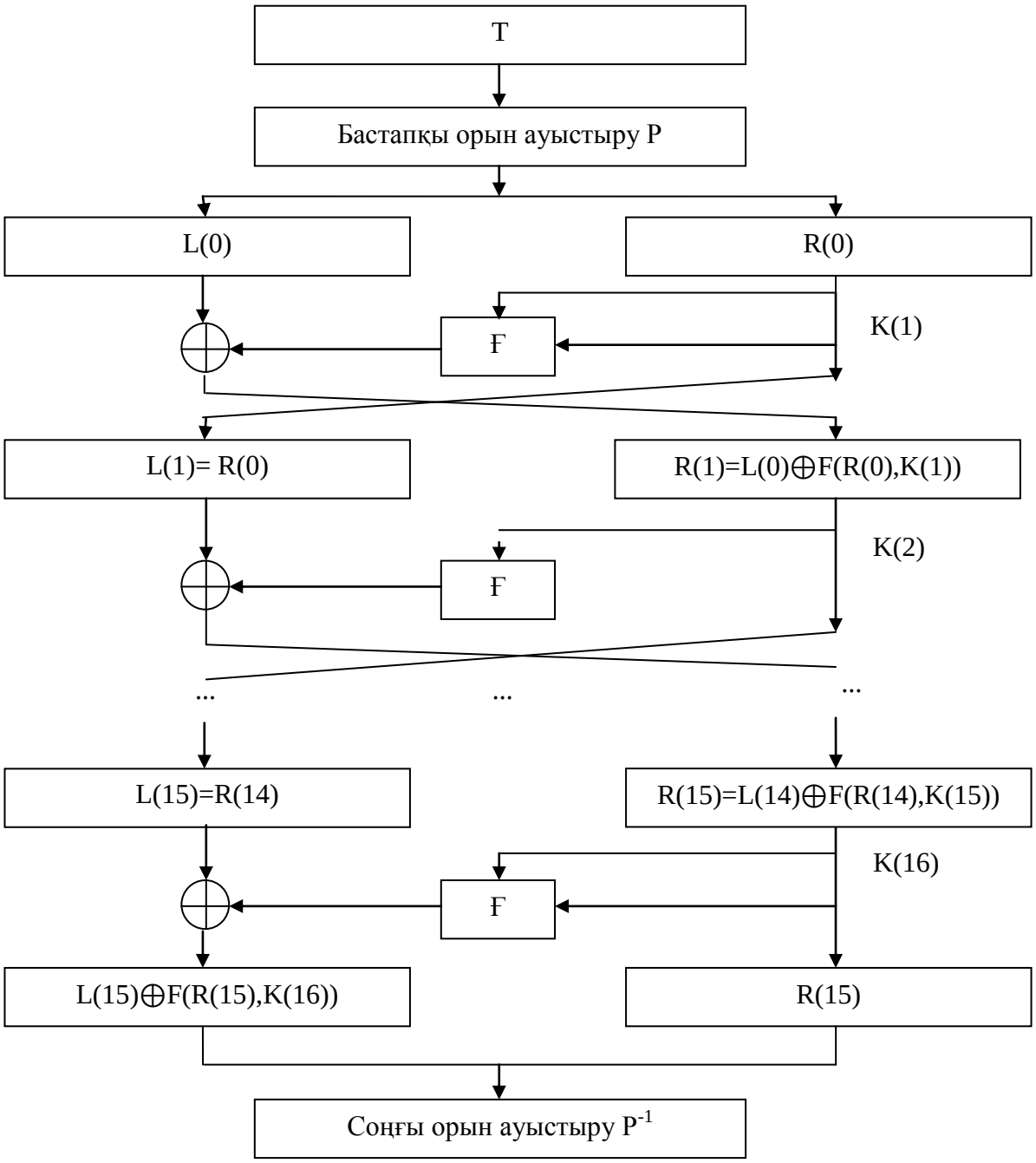
40	08	48	34	26	18	10	02
60	52	44	36	28	20	12	04
62	54	46	38	30	22	14	06
64	56	48	40	32	24	16	08
57	49	41	33	25	17	09	01
59	51	43	35	27	19	11	03
61	53	45	37	29	21	13	05
63	55	47	39	31	23	15	07

— P^{-1} мен Р матрицалары келесі түрде қатынасады: P^{-1} матрицасының 1-ші элементінің мәні 40 тең, ал Р матрицасының 40-шы элементінің мәні 1 тең, P^{-1} матрицасының 2-ші элементінің мәні 8 тең, ал Р матрицасының 8 элементінің мәні 2 тең және т.с.с.

— і-ші итерацияда K(i) – бұл 64 биттік алғашқы кілттен келесі түрде алынған 48 биттік кілт: итерацияның алдында 64 биттік кілттен 56 биттік кілтті әрбір сегізінші битті лақтыру жолымен алынады, яғни 8, 16, 24, 32, 40, 48, 56, 64 позицияларында тұрған биттер. Бұл биттер таңба ауысуын бақылау биттері ретінде қалыптастырылған және кілттің бүтіндігін бақылау үшін

қолданылады. Содан G кестесімен сәйкес 56 биттік кілттің бастапқы орын ауысуы жүргізіледі.

57	49	41	33	25	17	9	1	58	50	42	34	26	18
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
14	6	61	53	45	37	29	21	13	5	28	20	12	4



2.5 сурет - DES шифраторының схемасы

Осылай алынған 56 биттік кілт екі 28 биттік блокқа бөлінеді: C(0) – сол және D(0) – оң. C(1) және D(1) блоктарында КР орын ауыстыру көмегімен 48 разряд таңдап алынады:

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

Бұл разрядтар бірінші итерацияда қолданылады. і-ші итерацияда C(i), D(i) блоктарын алу үшін C(i-1), D(i-1) блоктарын s(i) позицияға циклдік жылжыту жүргізіледі, мұнда s(i) кесте бойынша таңдалынады.

2.2 кесте - 16 итерация үшін циклдік жылжыту

i	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16
s	1	1	2	2	2	2	2	2	1	2	2	2	2	2	2	1

Ары қарай қайта КР орын ауыстыру көмегімен 48 разрядты кілтті таңдаймыз.

Кілтті есептеу алгоритмінің блок-схемасы 2.6-суретте келтірілген.

Енді DES стандартында F(R(i-l),K(i)) шифрлеу функциясын қарастырайық. Ол 3-суретте схема түрінде көрсетілген.

Ғ функциясын есептеу үшін келесі функция-матрица қолданылады:

– E - 32 битті тізбектің 48-биттікке кеңейтілімі,

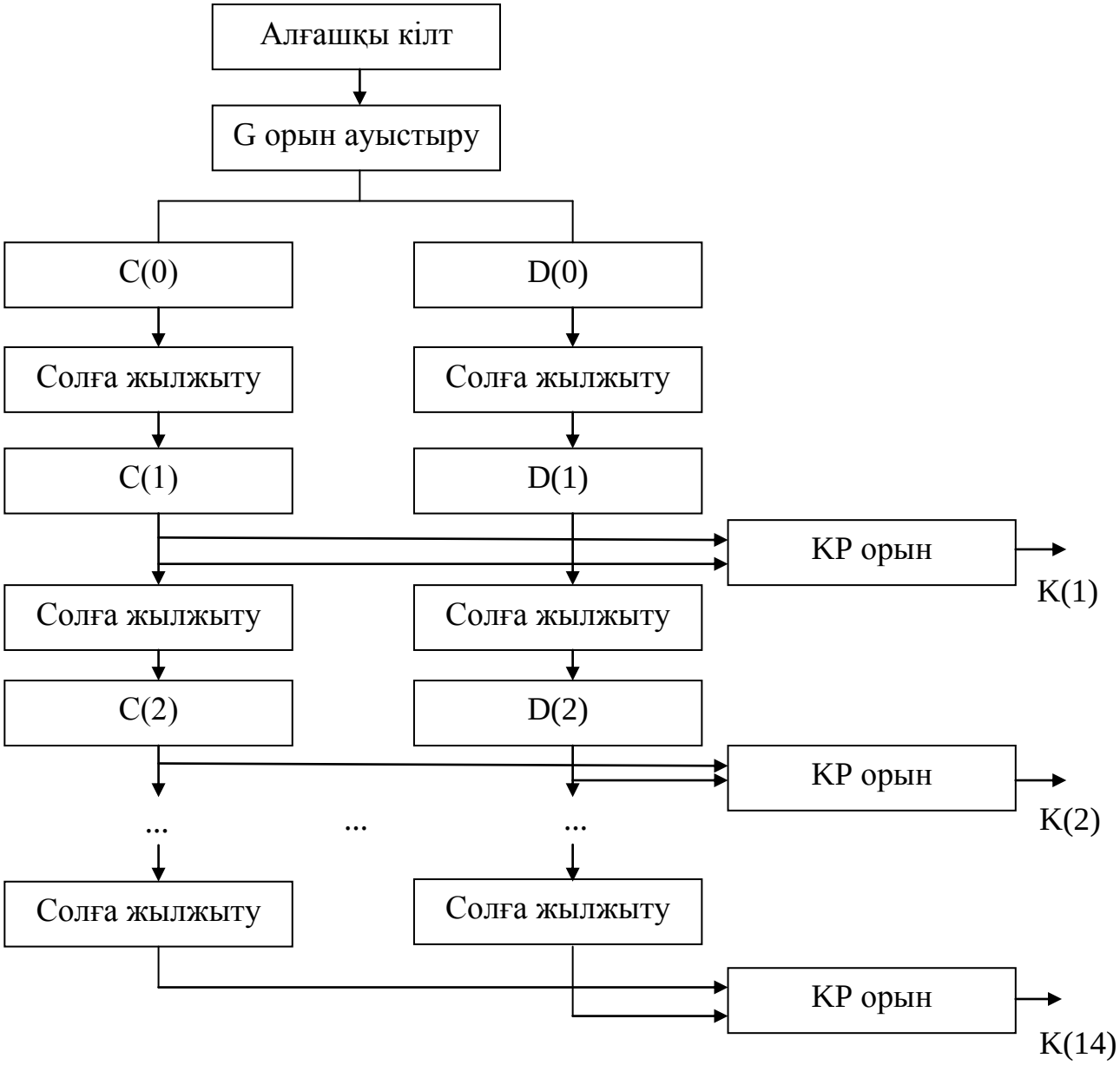
– SI, S2, ..., S8- 6-биттік блоктың 4-биттікке сызықты емес түрленуі,

– P2 – 32-биттік тізбекте биттің орын ауысуы.

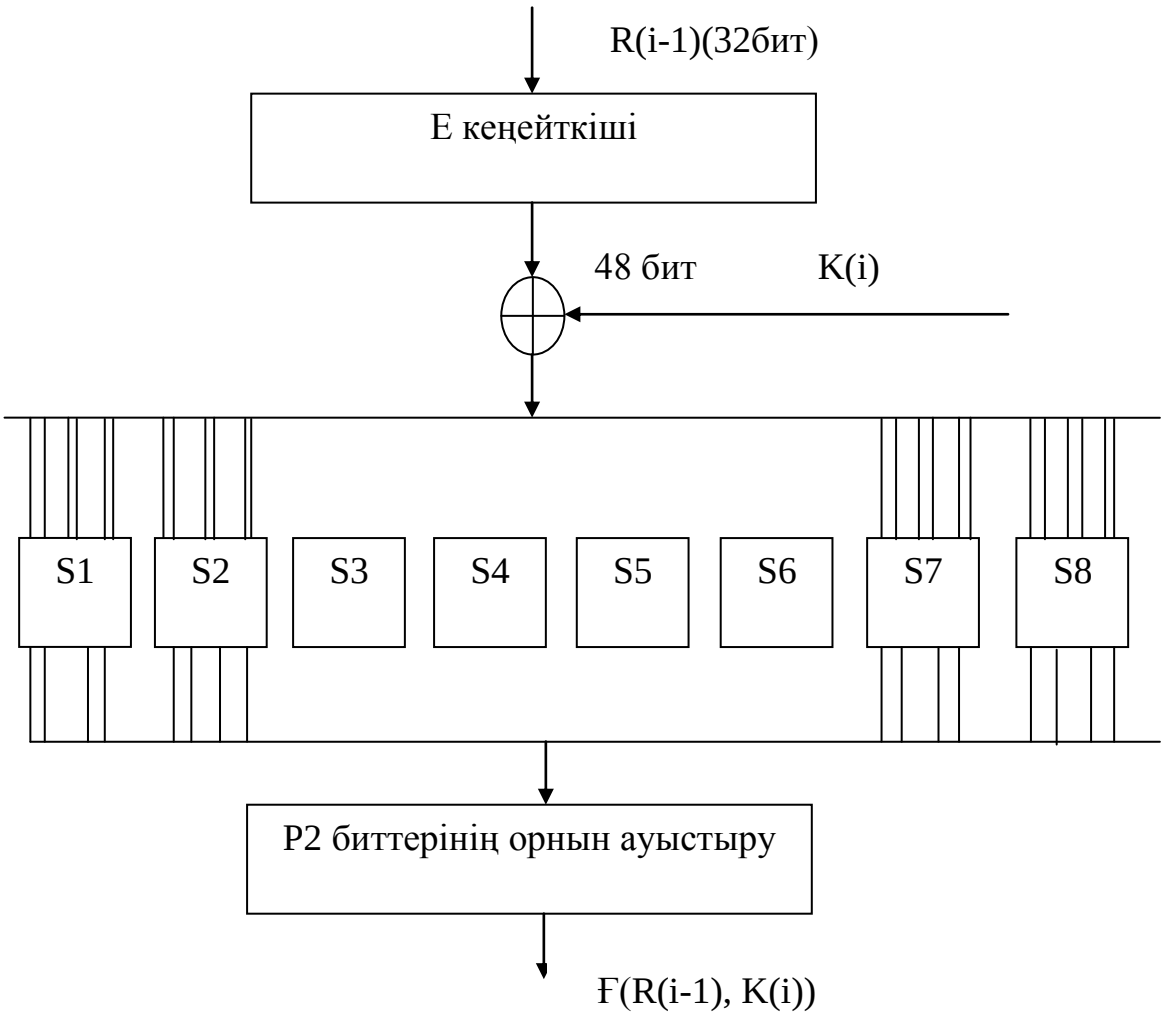
E кеңейтілім функциясы келесі кестемен анықталады

32	01	02	03	04	05
04	05	06	07	08	09
08	09	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	01

E(R(i-l)) кеңейтілім нәтижесі 48-биттік тізбекті көрсетеді, ол 2 модулі бойынша K(i) 48-биттік кілттікпен қосындыланады. Нәтижелі 48-биттік тізбек 8 блокқа B(1), B(2), …, B(8) әрбіреуі 6 бит бойынша бөлінеді, яғни E(R(i-1)) xor K(i) = B(1)B(2)...B(8). Sj функция-матрица кірісіне 6-биттік блок $B(j)=(b_1,b_2,b_3,b_4,b_5,b_6)$ түседі делік. Сонда (b_1,b_6) биттер Sj сипаттайтын матрицадағы жол номерін анықтайды, ал (b2, b3, b4, b5) биттер осы матрицадағы баған номерін анықтайды. S_j блогының шығысы сәйкес жол мен баған қиылысында тұратын 4-биттік элемент болады.



2.6 сурет - Кілтті қалыптастыру схемасы



2.7 сурет - Шифрлеу функциясы

Мысалы, B(1)=(010111) болсын, онда жол номері 1 тең, ал баған номері 11, яғни S1 матрицасында 1-ші жол мен 11-ші баған қиылысында тұрған элементті табамыз. Бұл 11 блок шығысында 1011 түріне ие.

Әрбір 6 биттік блоктың сегізіне түрлендіруді қолдана отырып, 32-биттік шығыс тізбекті аламыз және оған Р2 орын ауыстыруды қолданамыз.

16	07	20	21
29	12	28	17
01	15	23	26
05	18	31	10
02	08	24	14
32	27	03	09
19	13	30	06
22	11	04	25

Нәтижесінде F(R(i-l), K(i)) = P2(S1(B(1)),...S8(B(8))) аламыз.

2.3 кесте - S1, S2,…, S8 түрлендіру функциялары

		Баған номері																
		0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	
Жол номері	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	
	2	4	1	14	8	13	6	2	11	15	12	9	7	3	10	5	0	S1
	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	S2
	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	S3
	2	13	6	4	9	8	15	3	0	11	1	2	13	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	S4
	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	S5
	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	
	0	12	1	10	15	9	2	6	8	0	13	3	4	14	7	5	11	
	1	10	15	4	2	7	12	9	5	6	1	13	14	0	11	3	8	S6
	2	9	14	15	5	2	8	12	3	7	0	4	10	1	13	11	6	
	3	4	3	2	12	9	5	15	10	11	14	1	7	6	0	8	13	
	0	4	11	2	14	15	0	8	13	3	12	9	7	5	10	6	1	
	1	13	0	11	7	4	9	1	10	14	3	5	12	2	15	8	6	S7
	2	1	4	11	13	12	3	7	14	10	15	6	8	0	5	9	2	
	3	6	11	13	8	1	4	10	7	9	5	0	15	14	2	3	12	
	0	13	2	8	4	6	15	11	1	10	9	3	14	5	0	12	7	
	1	1	15	13	8	10	3	7	4	12	5	6	11	0	14	9	2	S8
	2	8	11	4	1	9	12	14	2	0	6	10	13	15	3	5	8	
	3	2	1	14	7	4	10	8	13	15	12	9	0	3	5	6	11	

2.2.3 ГОСТ 28147-89 шифрі.

Бұл шифр 64-биттік блоктармен хабарламаларды түрлендіреді, түрлендіру 32 раундта Фейстель сұлбасымен сәйкес жүзеге асырылады, кілттік өлшемі - 256 бит. Алгоритм жұмыстың 4 режимін қарастырады:

- қарапайым алмастыру режимінде деректерді шифрлеу (DES шифрі үшін ECB режимінің аналогы);

- гаммалау режимінде деректерді шифрлеу (DESшифрі үшін OFB режимінің аналогы);

- кері байланыспен гаммалау режимінде деректерді шифрлеу;

- имитоқойылымды құрастыру.

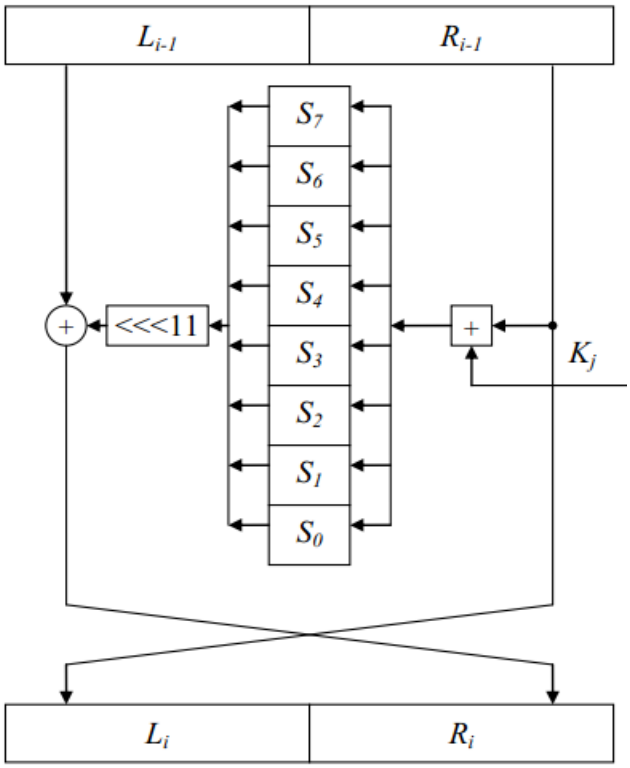
Басқа режимдерді тұрғызу үшін негіз болып табылатын қарапайым алмастыру режимін төменде қарастырамыз. Шифрлеу раундының сұлбасы 2.8-суретте келтірілген.

Түрлендіру келесі ретте жүргізіледі. R_{i-1} оң жартылай блогы K_j раундық кілтпен 2^{32} модулі бойынша қосылады. Ары қарай S_0, ..., S_7 кестесімен берілген қойылым орындалады және циклдік жылжыту көмегімен сол жаққа 11 позицияға түрленеді. Содан кейін 2 модулі бойынша L_{i-1} сол жақ жартылай блокпен биттік қосу және жартылай блоктармен орын ауыстыру орындалады.

Раундық кілттерді қолдану кестесі келесі түрде қалыптасады. K 256-биттік құпия кілт K=K7|K6|K5|K4|K3|K2|K1|K0 32- биттік ішкі кілттердің 8-мен қосарласу түрінде көрсетіледі.

Бірінші раундта 0-ші ішкі кілт, екіншісінде – 1-ші және т.с.с., 9-шы раундта тағы да 0-ші ішкі кілт, 24-де – 7-ші алынады, ал 25-ші раундта түрлендіру тағы 7-ші кілт қолданылады және ары қарай кілттер кері ретте қолданылады. Басқаша айтқанда, j раундтық кілт номері і раунд номеріне келесі түрде тәуелді:

$$1 \le i \le 24 \text{ үшін } j=(i-1) \bmod 8;$$
$$25 \le i \le 32 \text{үшін } j=(32-i) \bmod 8. \qquad (2.9)$$



2.8 сурет - ГОСТ 28147-89 алгоритмінің раунд сұлбасы

Қойылым 4-биттік ішкі блоктарға енгізу мәндерін бөлген соң жүргізіледі. Оң жартылай блок R раундтық кілтпен қосылған соң ол 8 бөлікке R=R7|R6|R5|R4|R3|R2|R|R01 бөлінеді. S_i кестелер қойылымы 4-биттік 16 элементтері бар векторды көрсетеді. Одан R_i мәнімен сәйкес келетін номері бар элемент алынады. Қойылым кестесінің мәні стандартпен анықталмағандығын атап өту керек, бұл мысалы, DES шифрінде жасалған. Сонымен қатар, алгоритм төзімділігі оларды дұрыс таңдауға да байланысты.

Бұл кестелердің нақты мәндері жасырын сақталуы керек деп есептеледі және олар өзіндік кілттік элементтер, олар барлық мекеме немесе бөлімшелер үшін ортақ және сирек өзгереді.

DES шифрімен салыстырғанда ГОСТ 28147-89 келесі артықшылықтары бар:

- аса ұзын кілт (256 бит DES шифріндегі 56 битке қарсы), кілттік жиынды толық таңдау жолында шабуыл қазіргі уақытта орындалмаған болып келеді;
- кілтті қолданудың қарапайым күнтізбесі, алгоритмді жүзеге асыруды жеңілдетеді және есептеу жылдамдығын жоғарлатады.

2.2.4 Blowfish шифрі.

Blowfish шифрі 1993 жылы белгілі американдық криптограф Брюс Шнейермен (Bruce Schneier) құрастырылды. Алгоритм 32-разрядты микропроцессорларға бағдарламалық жүзеге асуына негізделген. Оны жоғары жылдамдық пен криптотөзімділік ерекшелейді. Сондай-ақ негізгі ерекшелігі ретінде кіттің айнымалы ұзындығын қолдану мүмкіндігі деп атауға болады. Шифр блоктық, кіру блогының өлшемі 64 битке тең. Блокты түрлендіру 16 раундпен орындалады (111-ші раундпен версиясы бар). Айнымалы ұзындықты кілт максималды 448 бит.

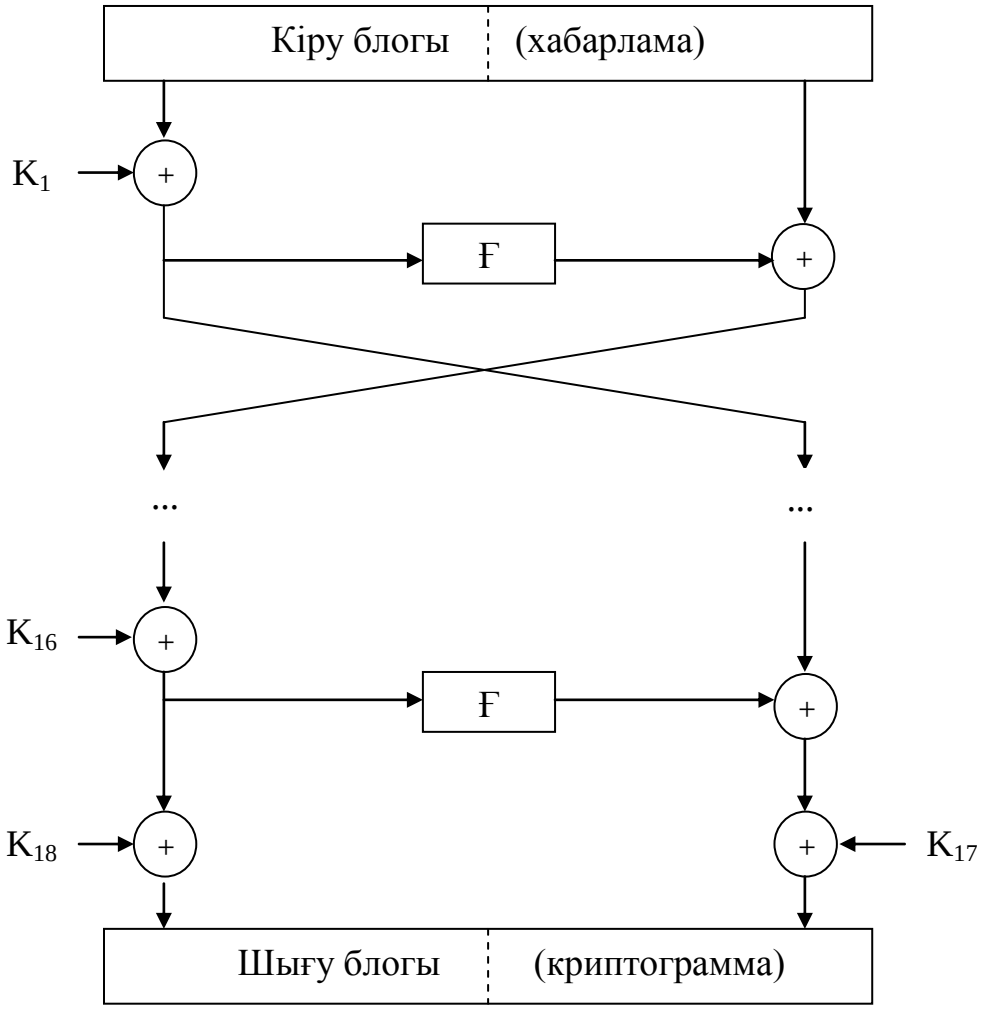
Деректерді шифрлеу мен шифрден алуға дейін кілттің кеңейтілімі жүргізіледі. Нәтижесінде, жасырын кілт негізінде кеңейтілімді алады, ол K_1,…, K_{18} (K_i өлшемділігі – 32 бит) 18 раундтық кілттерден және 4 жолмен, 256 бағанмен және 32-биттік элементтермен Q қойылым матрицасынан тұратын массивті көрсетеді.

$$Q = \begin{vmatrix} Q_0^{(1)} \dots Q_{25_5}^{(1)} \\ Q_0^{(2)} \dots Q_{25_5}^{(2)} \\ Q_0^{(3)} \dots Q_{25_5}^{(3)} \\ Q_0^{(4)} \dots Q_{25_5}^{(4)} \end{vmatrix}. \quad (2.10)$$

Берілген матрица F(X) шифрлейтін түрлендірудің сызықты емес функциясын беру үшін қолданылады, мұнда X – 32-биттік аргумент. X 8-биттік сөздің X=X3|X2|X1|X0 4-ші қысу түрінде көрсетіледі, ал функцияның өзі мына формуламен беріледі (мұнда + 232 модулі бойынша қосу, $\oplus$ - 2 модулі бойынша қосуды білдіреді):

$$F(X) = \left(\left(Q_{X_3}^{(1)} + Q_{X_2}^{(2)}\right) \oplus Q_{X_1}^{(3)}\right) + Q_{X_0}^{(4)}. \quad (2.11)$$

Шифрлейтін түрлендіру сұлбасы 2.9-суретте көрсетілген. KS жасырын кілт кеңейтілімі келесі түрде жүргізіледі.



2.9 сурет - Blowfish шифрі

1) K_i раундтық кілттердің және Q элементтерінің бастапқы массиві тіркелген мәндермен инициалданады. Мысалы, оналтылық көрсетілімде K_1=243F6A88 және т.с.с.

2) K_1KS жасырын кілттің бірінші 32 битімен, K_2 – келесі 32 битпен және т.с.с. 2 модулі бойынша қосындыланады. KS кілті аяқталған соң, оны бастапқыдан қайта қолдана бастайды. Тек K_i (Q-сыз) қосындылады.

3) Нольдің 64-биттік блоктары 0=(0…0)Blowfish көмегімен 1) және 2): C_0=Blowfish(0) қадамдарда алынған кілттерде шифрленеді.

4) Раундтық ішкі кілттер K_1мен K_2 3 қадамда алынған C_0 мәнімен алмастырылады.

5) C_0модификацияланған кілттерде C_1=Blowfish(C0) шифрленеді.

6) K_3пен K_4 раундтық кілттерді C_1 мәнімен алмастырады.

7) Үрдіс раундтық кілттердің барлық жұптары (9 жұп), содан кейін Q матрицасы элементтерінің барлық жұптары (512 жұп) басынан алынбағанға дейін жалғаса береді.

Демек, кілттің кеңейтілімі деректерлің 521 блогын шифрлеуді қажет етеді. Бұл процедура кілттік жиынды таңдау жолымен шабуылды қосымша қиындатады, яғни заң бұзушы әрбір мүмкін кілт үшін кеңейтілім процедурасын жүргізуі керек болады.

2.3 Симметриялық шифрлер үшін криптографиялық кілттермен басқару

Кілттік ақпарат ретінде жүйеде әрекет ететін барлық кілттердің жиынтығы түсіндіріледі. Егер кілттік ақпаратпен жеткілікті сенімді және қауіпсіз басқару қамтамасыз етілмесе, онда деректерді криптографиялық қорғауды қолданғаннан әсер нольге тең болуы мүмкін: заң бұзушы кілтке ие болған соң қорғалатын ақпаратқа кіру құқығын алады. Кілттермен басқару үрдісі өзіне үш негізгі функцияны жүзеге асыруды қосады:

- кілттерді генерациялау;
- кілттерді сақтау;
- кілттерді үлестіру.

Кілттердің генерациясы кілттің мәнін алдын ала табу (қалай ол генерацияланатын болса да) мүмкін болмайтындай етіп жүргізілуі тиіс. Қол жетімді жиындарда нақты кілтті таңдау ықтималдығы 1/N тең, мұнда N – кілттік жиынның (оның элементтерінің саны) күштілігі.

Кілттерді алу үшін кездейсоқ мәндер генерациясының аппараттық және бағдарламалық құралдары қолданылады. Қауіпсіздіктің деңгейіне жоғары талаптармен жүйелер үшін кездейсоқ физикалық үрдістерге негізделген аппараттық датчиктер қолайлы деп саналады. Бірақ өзінің арзандығы мен таратудың шексіз мүмкіндіктері үшін бағдарламалық жүзеге асыру ең кең таралған болып табылады. Бірақ бұл жағдайда алынған тізбек псевдокездейсоқ болатынын ескеру керек, егер бағдарламалық генераторды қайта сондай бастапқы мәндермен жүктесе, онда сол тізбекті шығарады.

Кілттердің бағдарламалық генераторларында генерация есептері үшін арнайы резервтелген шифрлеу алгоритмі мен кілттер қолданылады. Бастапқы мәндер ретінде, мысалы, есептеу жүйесінің таймер мәні алынуы мүмкін.

Жүйеде қолданылатын кілттердің ауысуын жиі жүргізіп тұру ұсынылды. Кейбір жағдайларда ауыстыру орнына модификация процедурасын қолдануға болады. Кілттің модификациясы – біржақты функция көмегімен алдыңғы мәннен жаңа кілт генерациясы. Бірақ бұл жағдайда жаңа кілт алдыңғысы сияқты сол шамада қауіпсіз, яғни қарсылас модификацияның барлық тізбегін қайталауы мүмкін.

Симметриялық шифрлеудің кілттерін сақтауды ұйымдастыру үшін жасырын кілттер анық түрде ешқашан тасымалдағышқа жазылмауы үшін жұмыс шартын қамтамасыз ету керек. Мысалы, бұл талапты кілттердің иерархиясын құра отырып орындауға болады. Үш деңгейлі иерархия кілттерді мыналарға бөлуді білдіреді:

- басты кілт;

- кілттерді шифрлеу кілті;

- деректерді шифрлеу кілті (сеанстық кілт).

Сеанстық кілттер – иерархияның төменгі деңгейі – деректерді шифрлеу және хабарлама аутентификациясы үшін қолданылады. Жіберу немесе сақтау кезінде осы кілттерді қорғау үшін кілттерді шифрлеу кілті қолданылады, олар ешқашан сеанстық сияқты қолданылмауы тиіс. Иерархияның жоғары деңгейінде басты кілт орналасқан (немесе мастер-кілт). Ол екінші деңгейдегі кілттерді қорғау үшін қолданылады. Симметриялық шифрлерді ғана пайдаланатын жүйелерде басты кілтті қорғау үшін криптографиялық емес құралдарды қолдану керек болады, мысалы, деректері физикалық қорғау құралдары (кілт тасымалдағышқа жазылады, ол жұмыс аяқталған соң жүйеден алынып, сейфте сақталады және т.с.с.) кішігірім ақпараттық жүйелерде кілттердің екі деңгейлі иерархиясы қолданылуы мүмкін (басты және сеанстық кілттер). Кілттерді үлестіру кезінде келесі талаптарды орындау керек:

- кілттерді үлестірудің оперативтілігі мен нақтылығын қамтамасыз ету;

- кілттерді үлестірудің құпиялығын қамтамасыз ету.

Кілттерді үлестіру мыналарды орындау арқылы жүргізілуі мүмкін:

- кілттерді үлестірудің бір немесе бірнеше орталықтарын қолданумен (орталықтандырылған үлестіру);

- желі пайдаланушылары арасында сеанстық кілттермен тікелей алмасу (кілттерді деорталықтандырыла үлестіру).

Симметриялық шифрлеудің кілттерін деорталықтандыра үлестіру әрбір пайдаланушыда кілттердің үлкен саны (жүйенің әрбір абоненттерімен байланысуы үшін) бар болуы қажет, ол алдымен қауіпсіз үлестіреді, ал содан соң сақтау үрдісінде олардың құпиялығын қамтамасыз етеді.

Симметриялық шифрлеудің кілттерін орталықтандыра үлестіру әрбір пайдаланушыда кілтті үлестіру орталығымен өзара байланыс үшін тек бір негізгі кілт ғана бар. Деректермен басқа абонентпен алмасу үшін пайдаланушы кілттер серверіне хабарласады, ол бұл пайдаланушыға және сәйкесінше абонентке сеанстық симметриялық кілт тағайындайды. Кілттерді орталықтандыра үлестірудің белгілі жүйелерінің бірі Kerberos болып табылады.

2.3.1 Kerberos хаттамасы.

Kerberosхаттамасы 1980 жылдың ортасында Массачусетстің технологиялық институтында құрастырылған және қазір орталықтандырылған аутентификация мен симметриялық шифрлеудің кілттерін үлестіру жүйесінің нақты стандарты болып табылады. Unix, Windows (Windows’2000 бастап) операциялық жүйелермен қолдау алған, Mac OS үшін жүзеге асырылуы бар.

Kerberos хаттамасы симметриялық шифрлеудің кілттерін үлестіруді және қорғалмаған желіде жұмыс істейтін пайдаланушылардың шынайылығын тексеруді қамтамасыз етеді. Kerberos жүзеге асыру – бұл «клиент-сервер» архитектурасы бойынша құрылған бағдарламалық жүйе.

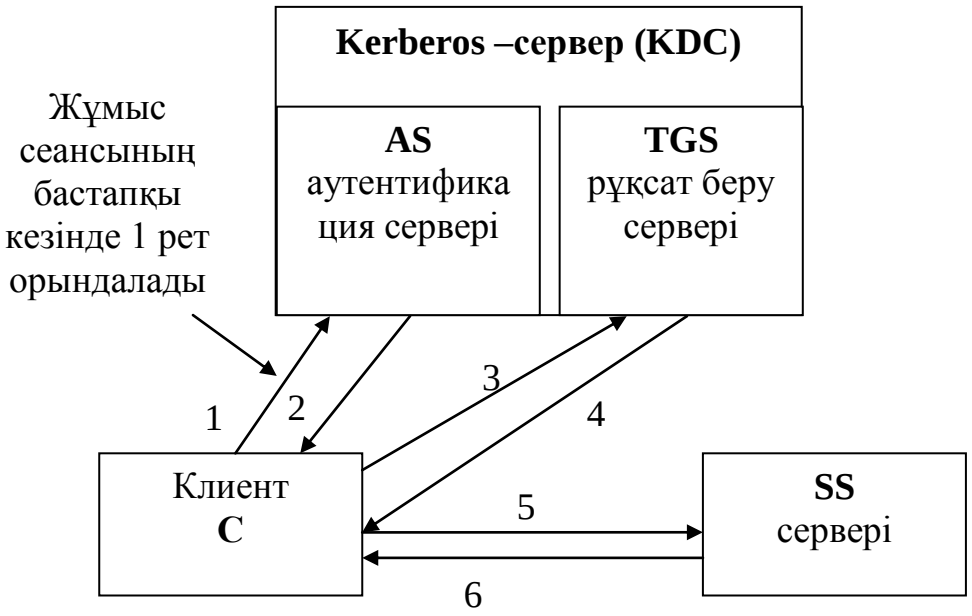
Клиенттік бөлігі Kerberos серверінің компоненттерін орнатудан басқа қорғалатын желінің барлық компьютерлеріне орнатылады. Kerberos клиентінің рөлінде, жеке жағдайда, желілік серверлер (файлдық серверлер, баспа серверлері және т.б.) де шығуы мүмкін.

Kerberos серверлік бөлігі кілттерді үлестіру орталығы (ағылшын тілінде «Key Distribution Center», қысқаша KDC) деп аталады және екі компоненттен тұрады:

- аутентификация сервері (ағылшын тілінде «Authentication Server», қысқаша AS);

- рұқсат беру сервері ((ағылшын тілінде «Ticket Granting Server»,қысқашаTGS).

Желінің әрбір субъектісіне Kerberos сервері симметриялық шифрлеудің онымен бөлісетін кілтін тағайындайды және субъектілердің деректер базасы мен олардық жасырын кілттерін қолдайды. Kerberos хаттамасының жұмыс істеу сұлбасы 2.10-суретте көрсетілген.



2.10 сурет - Kerberos хаттамасы

С клиенті SS (ағылшын тілінде «Service Server» – желілік сервистер беретін сервер) серверімен өзара іс-әрекет бастауға дайындалсын делік. Бірнеше жеңілдетілген түрде хаттама келесі қадамдарды ұсынады [10,11].

1) C->AS: {c}.

С клиенті AS аутентификация серверіне өзінің идентификаторын жібереді (идентификатор ашық мәтінмен беріледі).

2)AS->C: {{TGT}KAS_TGS, KC_TGS}KC,

мұнда KC – С негізгі кілті;

KC_TGS –TGS рұқсатын беретін серверге кіру үшін С беретін кілт;

{TGT}– рұқсат беру серверіне кіру билеті (ағылшын тілінде «Ticket

Granting Ticket»);{TGT}={c,tgs,t1,p1, KC_TGS}, мұнда tgs – рұқсат беру серверінің идентификаторы, t1 – уақыт белгішесі, p1 – билеттің әрекет ету кезеңі. {…}KX жазбасы осы жерді және ары қарай фигуралық жақшаның ішіндегісі KX кілтінде шифрленген дегенді білдіреді.

Бұл қадамда AS аутентификация сервері C клиенті оның базасында бар екендігін тексеріп, рұқсат беру серверіне кіру үшін оған билетті және рұқсат беру серверімен өзара әрекет ету үшін кілтті қайтарады. Барлық жіберілетін хабарламалар C клиентінің кілтінде шифрленеді. Демек, егер өзара әрекеттесудің бірінші қадамында c идентификаторын C клиент емес, ал X заңбұзушы жіберген болса да, онда AS алған X хабарламаны шифрден ала алмайды.

TGT билетінің ішіне кіру құқығын заңбұзушы ғана емес, сондай-ақ C клиенті де ала алмайды, өйткені билет аутентификация сервері мен рұқсат беру сервері өзара үлестірген кілтте шифрленген.

3)C->TGS: {TGT}KAS_TGS, {Aut1} KC_TGS, {ID},

мұнда {Aut1} – аутентификациялық блок – Aut1 = {c,t2}, t2 – уақыт белгісі; ID – сұралатын сервис идентификаторы (жеке жағдайда, бұл SS серверінің идентификаторы болуы мүмкін).

C клиенті TGS рұқсат беру серверіне қатынассын делік. Ол AS алынған KAS_TGS кілтінде шифрленген билетті және хабарлама қашан құрылғандығын көрсететін c идентификаторы мен уақыт белгішесінен тұратын аутентификациялық блокты жібереді.

Рұқсат беру сервері TGT билетін шифрден алады және одан билет кімге, қашан және қай мерзімге берілгендігі, C клиенті мен TGS сервері арасында өзара әрекет үшін AS серверімен генерацияланған шифрлеу кілті туралы ақпаратты алады. Осы кілт көмегімен аутентификациялық блок шифрден алынады. Егер блоктағы белгі билеттегі белгімен сәйкес келсе, хабарламаны шын мәнінде C генерациялағандығын дәлелдейді (өйткені ол ғана KC_TGS кілтін білді және өзінің идентификаторын дұрыс шифрлей алады). Ары қарай билеттің әрекет ету уақыты және 3 хабарламаны жіберу уақыты тексеріледі. Егер тексеру жүрген болса және жүйеде іске асатын саясат C клиентіне SS клиентіне қатынасуға мүмкіндік беретін болса, онда 4 қадам орындалады.

4)TGS->C: {{TGS}KTGS_SS,KC_SS}KC_TGS,

мұнда KC_SS –C мен SS өзара әрекеттесуіне арналған кілт,{TGS} – ағылшын тілінде «TicketGranting Service» –SS кіруге арналған билет (осындай аббревиатура хаттаманы сипаттауда рұқсат беру сервері де белгіленетіндігіне назар аударыңыз). {TGS} ={c,ss,t3,p2, KC_SS }.

Қазір TGS рұқсат беру сервері C клиентіне шифрлеу кілті мен SS серверіне кіру үшін қажет билетті жібереді. Билеттің құрылымы 2 қадамдағыдай: билетті кімге бергендегі идентификатор; билетті кім үшін бергендегі идентификатор; уақыт белгісі; жүзеге асу периоды; шифрлеу кілті.

5) C->SS: {TGS}KTGS_SS, {Aut2} KC_SS ,

мұнда Aut2={c,t4}.

С клиенті рұқсат беру серверінен алынған билетті және қорғалған өзара әрекеттесу сеансын орнатқысы келетін өзінің SS серверіне аутентификациялық блогын жібереді. SS жүйеде тіркелген және TGS серверімен KTGS_SS шифрлеу кілтін үлестіргендігі болжанады. Осы кілтке ие бола отырып, ол билетті шифрлеуі, KC_SS шифрлеу кілтін алуы және хабарламаны жіберу түпнұсқалығын тексеруі мүмкін.

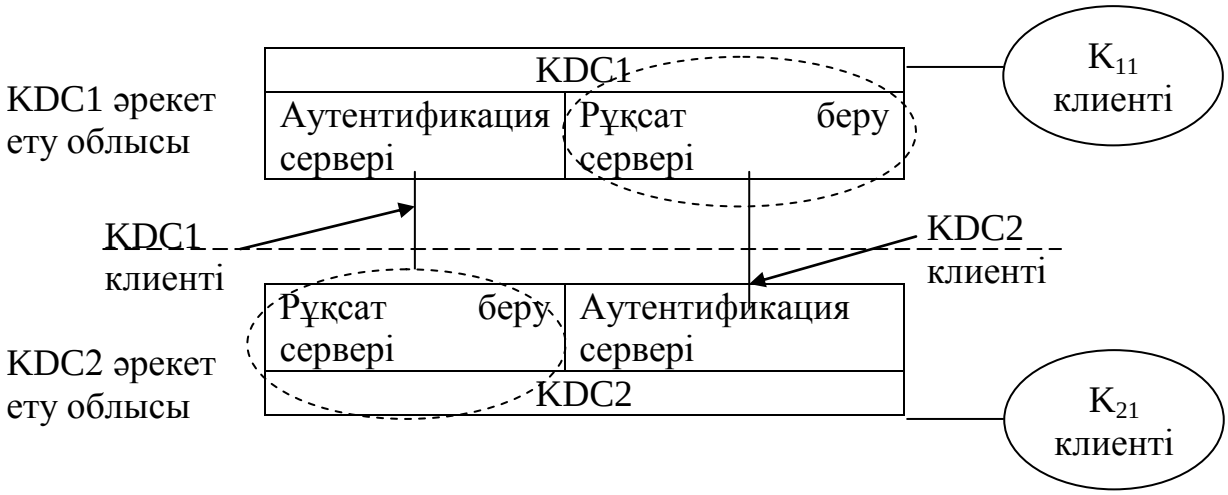
6) SS->C: {t4+1}KC_SS

Соңғы қадамның мәні SS енді С өзінің шынайылығын дәлелдеуі керектігінен тұрады. Ол алдыңғы хабарламаларды дұрыс шифрден алғанын көрсете отырып жасай алады. Сондықтан SS С аутентификациядық блоктан уақыт белгісін алады, алдын ала анықталған нұсқамен оны өзгертеді 1-ге ұлғайтады), KC_SS кілтінде шифрлейді және С қайтарады.

Егер барлық қадамдар дұрыс орындалып және барлық тексерістер табысты аяқталса, онда С мен SS өзара әрекеттесу жақтары, біріншіден, бір бірінің шынайылығына көз жеткізді, ал екіншіден, байланыс сеансын қорғау үшін шифрлеу кілтін –KC_SS кілтін алды.

Жұмыс сеансының үрдісінде клиент 1 мен 2 қадамдарды тек бір рет ғана өтетіндігін атып өту керек. Басқа серверге кіруде билет алу қажет болғанда (оны SS1 деп атайық), С клиенті TGS рұқсат беру серверіне ондағы бар билетпен қатынасады, яғни хаттама 3 қадамнан бастап орындалады.

Kerberos хаттамасын қолданған кезде компьютерлік желі Kerberos серверлердің әрекет ету облыстарына бөлінеді. Kerberos облысы – бұл пайдаланушылар мен серверлер Kerberos бір серверінің деректер базасында (немесе бірнеше серверлермен бөлінген бір базада) тіркелген желі облысы. Бір облыс локальді желі сегментін, барлық локальді желіні қамти немесе бірнеше байланысқан локальді желілерді біріктіре алады. Kerberos-облыстар арасындағы өзара әрекеттің сұлбасы 2.11-суретте көрсетілген.



2.11 сурет - Kerberos-облыстары арасындағы өзара әрекет

Облыстар арасында өзара әрекет үшін Kerberos серверлерін өзара тіркеу жүзеге асырылған, бұл үрдісте бір облыстың рұқсат беру сервері басқа облыста клиент ретінде тіркеледі (яғни аутентификация серверінің базасына енгізіледі және онымен кілтті бөліседі).

Өзара келісімдер орнатқан соң 1 облыстан клиент (бұл К11 болсын делік) 2 облыстан клиентпен өзара әрекеттесу сеансын орнатуы мүмкін (мысалы, К21). Ол үшін К11 өзінің рұқсат беру серверінен ол өзара әрекеттесуді орнатқысы келетін клиентпен Kerberos-серверге кіруіне билет алуы керек (суретте бұл KDC2 сервер). Алынған билет қай облыста билеттің иесі тіркелгендігі туралы белгішеден тұрады. Билет KDC1 мен KDC2 серверлері арасында бөлінген кілтте шифрленеді. Билетті табысты шифрден алған кезде қашықтағы Kerberos-сервер билет сенімді қатынас орнатылған Kerberos-облыс клиентіне берілгендігіне сенімді болуы мүмкін. Ары қарай хаттама жұмысын жалғастырады.

Қарастырылғандардан басқа, Kerberos қосымша мүмкіндіктер қатарын береді. Мысалы, билеттің құрылымында көрсетілген p параметрі (уақыт периоды) «әрекеттің басталу уақыты» - «әрекеттің аяқталу уақыты» мәндер жұбымен беріледі, бұл кейінге қалдырылған әрекет билетін алуға мүмкіндік береді.

«Беру құқығымен» билет типі бар, ол, мысалы, серверге оған қатынас жасаған клиенттің атынан әрекетті орындауға мүмкіндік береді.

2.4 Ассиметриялық шифрлер

2.4.1 Негізгі түсініктер.

Симметриялық криптография облысында жетістікке жеткендігіне қарамастан 1970 жылдың соңында есептердің бүкіл қатарын шешу үшін берілген әдістердің қолданылмайтындығы мәселесі біліне бастады.

Біріншіден, симметриялық шифрлерді қолданған кезде жиі кілттерді үлестірудің тривиальды емес есептерін жеке шешу қажет. Кілттер иерархиясы

мен үлестіру орталықтарын пайдаланғандығына қарамастан қандай да бір бастапқы мезетте кілт (немесе шебер-кілт) қауіпсіз арнамен жіберілуі керек. Бірақ мұндай арнаның болмауы да немесе ол жеткілікті қымбат болуы да мүмкін.

Екіншіден, симметриялық шифрлеудің әдістерін пайдаланған кезде өзара әрекетке қатысатын жақтардың өзара сенімі түсіндіріледі. Егер олай болмаса, сол бір жасырын кілтті бірге қолдану жағымсыз болуы мүмкін.

Үшінші мәселе ақпарат аутентификациясын жүргізу мен жіберушінің (алушының) хабарламаны жіберу (алу) фактісінен бас тартуымен байланысты қауіптерден қорғау қажеттілігімен байланысты.

Қарастырылған мәселелер өте маңызды болып табылады және оларды шешу жұмысы ассиметриялық криптографияның пайда болуына әкелді, оны ашық кілті бар криптография деп те атайды [4].

Анықтамалар қатарын қарастырайық.

Біржақты (бір жаққа бағытталған) функция деп екі қасиетке ие $F: X \to Y$ функциясы аталады:

а) $F(x)$ мәнін есептеудің полиномиальді алгоритмі бар;

б) F функциясын инверттаудың полиномиальді алгоритмі жоқ (яғни x қатысты $F(x)=y$ теңдеуін шешу, $x \in X$, $y \in Y$.

k құпиясы бар функция (функция-ловушка) деп үш қасиетке ие және k параметріне тәуелді $F_k: X \to Y$ функция аталады:

а) кез келген k мен x үшін $F_k(x)$ мәнін есептеудің полиномиальді алгоритмі бар;

б) белгісіз k үшін F_k инверттаудың полиномиальді алгоритмі бар;

в) белгілі k үшін F_k инверттаудың полиномиальді алгоритмі бар.

Криптографияда біржақты функцияларды қолдану мыналарға мүкіндік береді:

- шифрленген хабарлармен байланыстың тек ашық арналарын қолдану арқылы алмасуды ұйымдастыру, яғни кілтпен алмасу үшін байланыстың құпия арналарынан бас тарту;
- шифрді ашу есебіне күрделі математикалық есепті қосу және шифрдің төзімділігін негіздеу;
- шифрлеуден ерекше жаңа криптографиялық есептерді шешу (электронды цифрлік қолтаңба және т.б.).

Ашық кілті бар криптография облысында бірінші мақаланы Уитфилд Диффи (Whitfield Diffie) мен Мартин Хеллманның (Martin Hellman) 1976 жылы жарық көрген «Криптографиядағы жаңа бағыттар» атты мақаласын айтуға болады.

Симметриялықтан қарағанда ассиметриялық алгоритмдерде кілттер жұптармен – ашық кілт (ағылшынша «public key») және құпия кілт немесе жабық (ағылшынша «private key») қолданылады.

Хаттама екі жаққа алдын ала жеке кездесусіз байланыстың ашық каналы бойынша құпия кілт туралы келісімге жетуге мүмкіндік береді. Оның

төзімділігі А абелевті топта дискретті логарифмдеудің қиын шешілетін мәселелеріне негізделеді.

Өз жұмыстарында авторлар A = GF(p) тобын қолдануды ұсынған, бірақ қазіргі таңда бұл хаттаманың көптеген тиімді версиялары эллипстік қисықтар тобын негізге алады. Мұндай версиялар EC-DH аббревиатурасымен белгіленеді, ағылшын тілінен қысқартылғанда: Elliptic Curve және Diffie-Hellman.

Кілттерді ашық үлестіру идеясы

$$F(x) = \alpha^x \bmod p, \tag{2.12}$$

p – үлкен жай сан;

x – дербес натурал сан;

α - GF(p) өрісінің белгілі бір примитивті элементі (p мен α сандары бәріне қол жетімді болып есептеледі).

$\alpha^x \bmod p$ функциясын инверттау екендігі белгілі, яғни дискретті логарифмдеу қиын математикалық есеп болып табылады.

Ортақ кілтті алу хаттамасы.

Дана мен Димаш бір біріне тәуелсіз кездейсоқ бір-бір натурал санды таңдайды – мысалы a мен b. Бұл элементтерді олар құпияда сақтайды. Ары қарай олардың әрбіреуі жаңа элементті есептейді:

$$u = \alpha^a \bmod p \text{ және } v = \alpha^b \bmod p.$$

Содан кейін олар осы элементтермен байланыс арнасы бойынша алмасады. Енді Дана v алып және өзінің a құпия элементін біле отырып, жаңа элементті есептейді:

$$k = v^a = (\alpha^b)^a = \alpha^{ab} \bmod p.$$

Димашта солай істейді: $k = u^b = (\alpha^a)^b = \alpha^{ab} \bmod p$

Дана		*Димаш*
a, α^a	$\rightarrow$	α^a
α^b	$\leftarrow$	b, α^b

Дана есептейді: $k = (\alpha^b)^a = \alpha^{ab} \bmod p.$

Димаш есептейді: $k = (\alpha^a)^b = \alpha^{ab} \bmod p.$

Кілттерді ашық үлестіру идеясы (пассивті қарсыласушыға қарсы төзімділік)

Арай ол хабарды жолдан қағып алуы мүмкін, яғни Арайда $\alpha, \alpha^a, \alpha^b$ бар.

Кілтті бұзу үшін Арайға мынаны есептеу қажет: α^{ab}. Сондықтан *a немесе b* білу қажет, ал ол үшін α^a *немесе* α^b логарифмдеу керек.

«Адам ортасында» шабуылы

Дана	*Арай*	*Димаш*
a	$\rightarrow \quad \alpha^a$	
α^m	$\leftarrow \quad m$	
α^{am}	α^{am}	
	$n \quad \rightarrow$	α^n
	$\alpha^b \quad \leftarrow$	b
	α^{bn}	α^{bn}

Ашық кілтпен шифрлеу идеясы.

Дана шифрленген хабарды алғысы келеді, сондықтан ол k құпиясымен F_k қандайда бір функция-ловушканы таңдап алады, барлық қызыққан адамдарға шифрлеудің өз алгоритмі ретінде F_k функцияның сипаттамасын хабарлайды (мысалы, жариялайды), бірақ k (жабық кілт) құпия мәнін ол ешкімге хабарламайды және құпияда ұстайды.

Енді егер пайдаланушы Димаш Данаға m қорғалатын ақпаратты жібергісі келсе, онда ол $c = F_k(m)$ есептейді және Данаға ашық канал бойынша c жібереді.

Цифрлік қолтаңба идеясы.

Данаға m хабарламаға қол қою керек. Ол k құпияны біле отырып, s табады, ол $m = F_k(s)$ және m хабарламасымен бірге Димашқа өзінің цифрлік қолтаңбасы ретінде s жібереді. Қол қойылған хабарлама –(m,s) жұбы.

Димаш s –ті Дана m хабарламаға қол қойды деген дәлел ретінде сақтайды.

Цифрлік қолтаңбамен қол қойылған хабарламаны (m, s) жұбы ретінде көрсетуге болады, мұнда m—хабарлама, s— теңдеу шешімі, мұнда $F_k : M \rightarrow S$ - құпиясы бар функция.

Цифрлік қолтаңба қасиеті

1) Бәсекенің туындауы кезінде қолтаңбадан бас тарту мүмкін емес, өйткені оны қолдан жасауға болмайды.

2) (m,s) қол қойылған хабарламаны байланыстың кез келген арнасы бойынша жіберуге болады.

Кемшіліктері:

1) Жоғары есептеу шығындары:

– шешімі: симметриялық шифрлеу алгоритмін қолдану.

2) Кілттік алмасу аутентификациясының түзу мүмкіндігінің жоқтығы:

– «Man in the Middle» шабуылы.

2.4.2 Диффи-Хеллман сұлбасы бойынша кілттерді үлестіру.

Жоғарыда қарастырылғандай, ассиметриялық криптография негізі американдық зерттеушілерУ.Диффи және М.Хеллманмен қаланған. Олармен екі абонентке байланыстың қауіпсіз арнасы арқылы хабарламамен алмаса

отырып, шифрлеудің құпия кілтін өзара үлестіруге мүмкіндік беретін алгоритм ұсынылды.

Берілген алгоритмнің ерекшеліктерімен жақсы танысу үшін сандар теориясынан бірнеше анықтамаларды қарастырайық. Екі бүтін сандар n мен n’m модулі бойынша салыстырмалы деп аталады, егер m бөлу кезінде олар бірдей қалдық берсе: n≡n’ (mod m), m – салыстыру модулі. Демек, Z бүтін сандар жиынын m модулі бойынша өзара салыстырмалы сандар класына бөлуге болады және m модулі бойынша алып тастау класы деп аталады. Әрбір алып тастау класы мына түрге ие:

$$\{r\}_m=\{r+ mk \mid k\in Z\}. \quad (2.13)$$

Алып тастаудың барлық кластарының жиыны m модулі бойынша Z_m или Z/mZ ретінде белгіленеді. Әрбір екі класқа $\{k\}_m$ және $\{l\}_m$ олардың қосындысы мен көбейтіндісі болып табылатын класты қоюға болады, бірмәнді қосу мен көбейту операциялары анықталады. $\{Z_m, +, \times\}$ жиыны бірлігі бар коммутативті сақина болып табылады, ал егер m – жай болса, онда соңғы өріс. Мультипликативті топ $\{Z_m , \times\}$m=1,2,4,p^k,2p^k кезінде (мұнда k∈ N,p – тақ жай сан) циклдік [12] болып табылады, яғни a∈Z_m түзетуші элемент бар, ол белгілі ретте a дәрежесін 0-ден m-1 дейін барлық мәндерді береді. Элемент a сондай-ақ m модулі бойынша түпкі түбір деп аталады. Диффи-Хеллман алгоритмінде біржақты функция ретінде жай сан модулі бойынша дережеге шығару қолданылады:

$$y=a^x \bmod p. \quad (2.14)$$

мұнда p – үлкен жай сан (қазір 2^{1024} немесе одан асатын модульді қолдану қауіпсіз деп саналады), a – p модулі бойынша түпкі түбір. Кері мәнді табу есебі, яғни y белгісіз бойынша x есептеу дискретті логарифмдеу есебі деп аталады және есептеу үшін күрделі болып табылады. Басқаша айтқанда, модульдің жеткілікті үлкен мәндері кезінде (2.13) функциясының көрсеткіштері мен дәреже негізі кері қайтарылмайтын болып есептеледі.

p – жай сан, p>2, p-1 қарапайым көбейткіштерге орналастыру белгілі болсын: $p-1=\prod_{j=i}^{k} q_j{}^{\propto_j}$. a саны p модулі бойынша түпкі түбір болып табылады, егер келесі шарт [12] орындалса:

$$НОД(a, p)=1;\ a^{(p-1)/qj}\neq 1 \ (\text{mod})p,\ j=1, ..., k, \quad (2.15)$$

мұнда НОД(x, y) – x және y сандарының ең үлкен ортақ бөлгіші.

Диффи-Хеллман алгоритмін енді қадам бойынша қарастырайық. Желі абоненттері Дана мен Димаш (2.13) формуладан a мен p мәндерін алдын ала келісіп алған делік. (p-1) санының бөлінуі үлкен жай жиыннан тұрсын делік, мысалы, (p-1)=2t, мұнда t – жай.

1) Дана құпия кілт X_A таңдайды және оған сәйкес келетін ашық кілтті $Y_A = a^{X_A} \bmod p$ есептейді.

2) Димаш өз кезегінде X_B анықтайды және есептейді.

3) Абоненттер ашық кілттерімен Y_A мен Y_B алмасады.

4) Абоненттер ортақ құпия кілтті есептейді. Дана келесі қатынаспен қолданады: $K_{AB} = (Y_B)^{X_A} \bmod p$. Димаш мына формуланы қолданады:

$K_{BA} = (Y_A)^{X_B} \bmod p$. Соңғы өрісте көбейту операциясының ассоциативтілік қасиетін қолдана отырып, $K_{AB}=K_{BA}$ екендігін көрсетейік:

$$K_{AB} = (Y_B)^{X_A} \bmod p = (a^{X_B})^{X_A} \bmod p = (a^{X_A})^{X_B} \bmod p = K_{BA.} \quad (2.16)$$

Демек, жақтар ортақ құпия кілтті K_{B_A} үлестіру алды. Y_A мен Y_B жіберілетін ашық кілттерді алып алатын заңбұзушы онымен абоненттердің құпия кілттерін білмей-ақ ортақ құпия кілтті есептеуі мүмкін. Қазіргі кезде берілген есепті шешудің жақсы жолы табылмаған, тек дискретті логарифмдеу, ол алгоритмнің криптографиялық төзімділігін қамтамасыз етеді.

2.4.3 RSA криптографиялық жүйесі.

Ашық кілтпен криптожүйеде симметриялыққа қарағанда екі кілт қолданылады: ашық және жабық (жабық құпияда сақталады). Ашық кілт ЭЦҚ тексеру үшін және хабарламаны шифрлеу үшін қолданылады. Жабық кілт ЭЦҚ генерациялау үшін және хабарламаны дешифрлеу үшін қолданылады.

ЭЦҚ (Электронды цифрлік қолтаңба) – электронды құжат атрибуты, деректердің белгілі бір криптографиялық түрленуі нәтижесінде алынады. ЭЦҚ құжаттардың бүтіндігін, құжаттардың конфиденциалдылығын тексеруге, сондай-ақ құжат иесін идентификациялауға мүмкіндік береді. Қарапайым қолтаңба аналогы [4].

2.4 кесте - Ашық кілті бар криптожүйе кестесі

Кілттер	ЭЦҚ құру	Шифрлеу	ЭЦҚ тексеру	Шифрден алу
	Жабық кілт	Ашық кілт	Ашық кілт	Жабық кілт

Ашық кілтпен криптографиялық жүйелер негізінде біржақты функциялар жатқанын атап өту керек, олар келесі қасиеттерге ие:

1) x мәні белгілі болсын, онда F(x) есептеу айтарлықтай оңай.

2) y=F(x) белгілі болсын, бірақ x есептеу қиын.

Ашық кілті бар криптожүйелер симметриялық криптожүйелерді алмастыра алмайтындығын атап өту керек, бұл мынамен байланысты:

- ашық кілтпен алгоритмдердің жұмыс істеу жылдамдығы симметриялық алгоритм жұмысының жылдамдығына қарағанда әлдеқайда төмен. Сондықтан ассиметриялық шифрлер өлшемі бойынша кіші деректерді шифрлеу үшін қолданылады, мысалы, кілттер;

- кілттер ұзындығы симметриялық криптожүйеге қарағанда әлдеқайда үлкен.

Әрине, жақсы жақтары да бар, мысалы:

- ашық кілттерді ыңғайды үлестіру, құпиялықты қажет етпейді;

- үлкен желілерде кілттер саны симметриялық криптожүйеге қарағанда әлдеқайда аз.

RSA негізінде екі жай үлкен сандардың көбейтіндісін факторизациялау есептері жатыр. Шифрлеу үшін N модулі бойынша дәрежеге шығарудың қарапайым операциясы қолданылады. Шифрден шешу үшін N санынан Эйлер

функциясын есептеу қажет, ол үшін n санын жай көбейткіштерге тізбектеуді білу керек (Факторизация есебі осыдан тұрады).

RSAда ашық және жабық кілт жұп бүтін саннан тұрады. Жабық кілт құпияда сақталады, ал ашық кілт басқа адамға хабарланады немесе бір жерге жарияланады.

RSA кілттерін генерациялау.

Барлығы кілттік жұпты генерациялаудан басталады (ашық, жабық кілт). RSA-да кілттерді генерациялау келесі түрде жүзеге асады:

1) p мен q екі жай сан таңдап алынады (p q-ге тең емес).

2) $N=p*q$ модулі есептеледі.

3) N: $\varphi(N)=(p-1)(q-1)$ модулінен Эйлер функциясының мәні есептеледі.

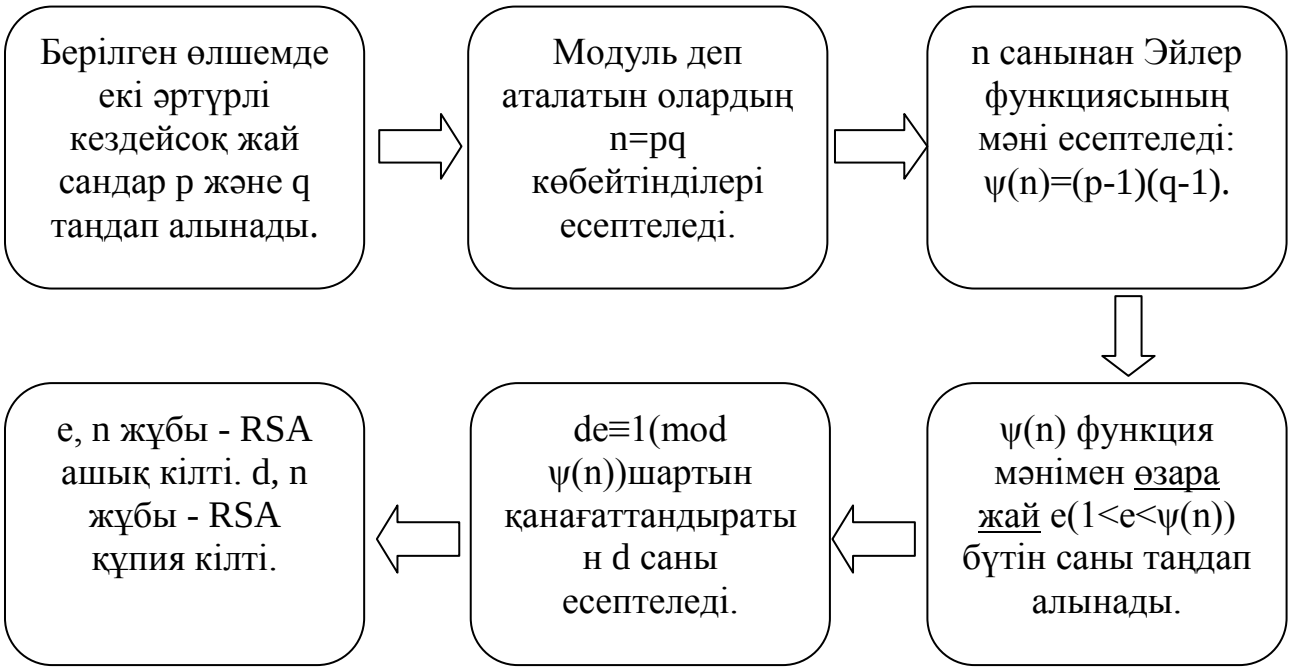
4) e саны таңдап алынады, ол ашық экспонента деп аталады, e саны $1<e<\varphi(n)$ интервалында жатуы керек, сондай-ақ $\varphi(N)$ функция мәнімен өзара жай сан болуы керек.

5) d саны есептеледі, ол құпиялы экспонента деп аталады, $d*e=1(\mathrm{mod}\varphi(N))$, яғни $\varphi(N)$ модулі бойынша e санына мультипликативті кері болып табылады.

Сонымен, біз кілттер жұбын аламыз:

(e,N) жұбы - ашық кілт.

(d,N) жұбы – жабық кілт.



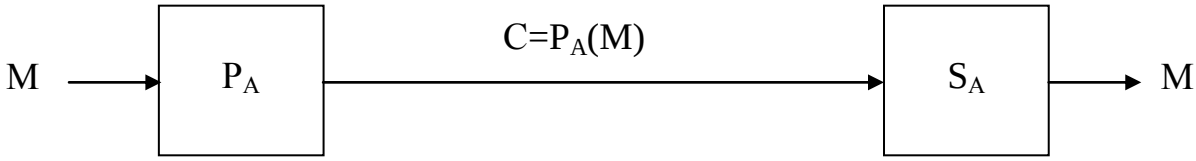
2.12 сурет - RSA кілттерін генерациялау сұлбасы

Алгоритм сипаттамасы. Шифрлеу және дешифрлеу.

B A

Шифрлеу Дешифрлеу

Коммуникациялық арна



Алгоритм:

1) А жағының (e, n) ашық кілтін алу.
2) М ашық мәтінін алу.
3) Шифрленген хабарламаны жіберу:

$$P_a(M)=M^e \bmod n.$$

Алгоритм:

1) С шифрленген хабарламаны қабылдау.
2) Шифрден шешу үшін өзінің (d, n) құпия кілтін қолдану:

$$S_a(C)=C^d \bmod n.$$

RSA шифрлеу мысалы.

1. Жай сандарды таңдап аламыз (кішкентай, есептеуді жеңілдету үшін): p=3 және q=11.

2. n=p•q=3•11=33 модулін есептейміз.

3. n модулі бойынша Эйлер функциясын есептейміз:

$\varphi(N)=(p-1)\bullet(q-1)=2\bullet10=20.$

4. e=7 ашық экспонентаны таңдаймыз.

5. d жабық экспонентаны анықтаймыз: $d\bullet e=1(\text{mod } \varphi(N)) \Rightarrow d=3.$

CAB хабарламасын шифрлейміз, шифрленетін хабарламаны 0-ден 32 дейінгі диапазондағы сандар тізбегімен көрсетейік.

A =1, B=2, C=3.

Ашық кілт: (e,n)=(7,33);

C1 = (3^7) mod 33 = 2187 mod 33 = 9;

C2 = (1^7) mod 33 = 1 mod 33 = 1;

C3=(2^7)mod33=128 mod 33=29;

C(“CAB")=9129.

RSA шифрден алу мысалы.

Жабық кілтті қолданамыз: (d,n)=(3,33);

M1=(9^3) mod 33 =729 mod 33 = 3(C);

M2=(1^3) mod 33 =1 mod 33 = 1(A);

M3=(29^3) mod 33 = 24389 mod 33 = 2(B);

3=C; 1=A; 2=B.

Алғашқы мәтінді аламыз - CAB.

RSA неге қарапайым емес?

Берілген алгоритм ассиметриялық криптожүйелерге талаптарды қанағаттандырады ма екендігін тексеру керек.

Шарт 1. Шифрлеудің ассиметриялық алгоритмі төзімді болып табылады, егер шабуылшы екі ашық мәтінге M1 мен M2, сондай-ақ Ci шифрленген мәтінге ие болса.

Шарт 1 дәлелдеу. RSA қайтып келіп 1 шартты тексерейік. Дана мен Димаш жағдайын еске түсірейік. Мысалы, Арай байланыс арнасын тыңдады делік. Димаш Данадан: «Дана, бүгін киноға барамыз ба?» деп сұрады. Дана Димашқа жауап береді, бірақ оны ешкім білмегенін қалайды, сондықтан өзінің

жауабын Димаштың ашық кілтінде шифрлейді де Димашқа шифрмәтінді жібереді. Арай шифрленген хабарламаны алып, Дана «Иә» немесе «Жоқ» деген жауап бергенін біледі. Арай Димаштың ашық кілтін біледі, сондықтан «Иә» мен «Жоқ» хабарын тізбектей шифрлейді, сәйкесінше олардың бірі Дананың шифрленген хабарымен сәйкес келеді және Арай Дананың бүгін киноға барады не бармайтынын біліп қояды.

RSA алгоритмінің жеңілдетілген сипаттамасы практикалық қолдануда келмейтіндігін көреміз. Практикада бұл мәселе қалай шешіледі? Бұл мәселе жеткілікті қарапайым шешіледі: хабарламаға қандайда бір кездейсоқ шама қосылады, содан соң алынған мәтін шифрленеді. Демек, егер Арай C1=E(«ИәA1B2") хабарламасын алса, ол «Иә» мен «Жоқ»:C2=E(«Жоқ"), C3=E(«Иә") шифрлеп, C1 мен C3 сәйкес келмейтінін көреді.

Демек, RSA алгоритмінде хабарламаны шифрлемес бұрын мәтінге қандайда бір кездейсоқ шама қосылады, содан соң мәтін шифрлеу процедурасынан өтеді. Сондықтан шифрлеу функциясы мына түрге ие болады:

C=(M||random)^emod (N), орнына C=M^emod (N)

Шарт 2. Арайда екі функция бар делік, біріншісі Ғ1 хабарламаны шифрлейді, екіншісі Ғ2 шифрмәтінді шифрден шешеді. Содан соң Арай екі хабарламаны M1 мен M2 генерациялайды. Содан хабарламаның бірі наугад Ғ1 функциясымен, функция шығуында –шифрмәтін Сі шифрленеді. Сі Арайға қайтып оралады, оның мәндеті Сі хабарламаның M1 мен M2 қайсысына жататындығын анықтау. Сондай-ақ Арай Сі басқа кез келген хабарламаны шифрден шеше алады. Ашық кілтпен криптожүйе төзімді болып есептеледі, егер қаскүнем шифрмәтін хабарламаның қайсысына сәйкес келетінін білмесе.

Шарт 2 дәлелдеу. Арайда екі ашық хабарлама M1 мен M2 және бір шифрмәтін Сі=M1^e mod (N) бар болсын. Арай не істейді? Ол ашық кілтті (e,N) : C^∗=2^e Ci mod(N) пайдаланып хабарлама құрады, содан соң Ғ2 функциясын пайдалана отырып бұл хабарламаны мына түрде шифрден шешеді: M∗=C^∗d mod(N) =2^ed∗M1^ed mod(N) =2 M1 mod(N), M^∗/2 есептей отырып, Арай M1 хабарламаны алады.

Жоғарыда айтылған тағы да RSA жеңілдетілген алгоритмін практикада пайдалануға болмайтынын көрсетеді. Бұл мәселе шарт 1 жағдайдағыдай шешіледі, яғни хабарламаға абсолютті кездейсоқ және болжанбайтын ақпарат қосылады, содан соң мәтінді шифрледік. Енді тағы бір талапты қосамыз: қосымша блоктар шифрмәтін шифрлейтін функция нәтижесінде немесе ол қаскүнеммен модельдеу нәтижесінде алынды ма екендігін анықтауға көмектесуі қажет. Түпнұсқалыққа шифрден шешілген деректерді тексеру үшін барлығына белгілі хеш-функция қолданылады.

Мұндай схема RSA шифрлеуде *RSA-OAEP(Optimal asymmetric encryption padding)* деген атауға ие, OAEP мысалда толығырақ қарастырайық.

RSA-OAEP.

Шифрлеу. Мәтінді RSA-OAEP шифрлеу үшін келесі жасалады:

1) Екі хеш-функциялар H(x) мен G(x) таңдап алынады, хеш-функция нәтижесінің суммарлы ұзындығы RSA кілті ұзындығынан үлкен болмауы керек.

2) L биттер жолы генерацияланады. Сондай-ақ тізбек кездейсоқ болуы керек, ал ұзындығы H(x) хеш-функция нәтижесі ұзындығынан аспауы керек.

3) M ашық мәтін k-бит бойынша блоктарға бөлінеді. Әрбір mi блокқа (p−k) нольдер қосылып жазылады, мұнда p - G(x) хеш-функция ұзындығының саны.

4) (m||0^(p−k)⊕G(L))||(L⊕H(p||0^(p−k)⊕G(L)) бит жиынын анықтау.

5) 4 қадамда алынған биттер M1 бүтін саны түрінде алынады.

6) Шифрмәтін анықталады:C=M1^e mod (N).

Ширфден алу. Хабарламаны шифрден шешу үшін келесі орындалады:

1) M1анықталады: M1=C^d mod (N).

2) биттердің алынған тізбегінен сол жақ бөлігін алып тастайды (M1 санының p сол жақ биті, p - G(x) хеш-функциясының ұзындығы). Бұл T биттер: T=(m||0^(n−k)⊕G(L)).

3) H(T)=H(m||0^(n−k)⊕G(L)) анықталады.

4) Осыдан H(T) белгілі, яғни L⊕H(T) білгендіктен (блоктың оң жақ бөлігі), L аламыз.

5) T⊕G(L) шартынан m табамыз, ал T өз кезегінде: T=(m||0^(n−k)⊕G(L)).

6) Бұл қадамда алынған m тексеру керек, егер ол (p−k)-нольдермен аяқталса, онда хабарлама дұрыс шифрленген, кері жағдайда шифрмәтін дұрыс емес болса, онда ол қаскүнеммен жасалған.

2.4.4 Электронды қол қою.

Мәліметтерді түп нұсқалау мәселесі неден тұрады? Қарапайым хат немесе құжат соңына орындаушы не жауапты тұлға әдетте өз қолын қояды. Мұндай әрекет әдетте екі мақсатты көздейді. Біріншіден, алушы өзіндегі үлгімен қойылған қолды салыстырып, хаттың ақиқаттығына көз жеткізеді. Екіншіден, жеке адамның қолы құжаттың автордікі екендігіне заңды кепіл болып табылады. Соңғы аспект әртүрлі сауда-саттық, бітім-шарттарын бекіткенде, сенім хат, міндеттемелер құрғанда ерекше маңызды. Егер қағазға адамның қолын қою мүлде оңай іс емес, ал қазір қылмыстық әдіспен қолдың автордікі екені жасау – техникалық бөлшек болса, онда электронды қолдың ісі басқаша. Оны көшіре отырып қолды жасау немесе құжатқа заңсыз түзетулер енгізуді кез келген пайдаланушы істей алады. Қазіргі дүние жүзінде құжаттардың электронды формалары мен олардың өңделу құралдары кең таралуымен қағазсыз құжаттарды автордікі етіп жасау ерекше өзекті мәселе болады. Ашық кілтті криптографиялық жүйелердің бөлімінде шифрлеудің қазіргі жүйелерінің барлық артықшылығында олар мәліметтердің түпнұсқалануын қамтамассыз етуге жол бермейді. Сондықтан түпнұсқалау құралдары комплексте және криптографиялық алгоритмдермен пайдаланылулары тиіс.

Кілтпен басқару. Нақты пайдаланылатын жүйеге қолайлы криптографиялық жүйені таңдаудан басқа маңызды мәселе – кілттермен басқару. Криптожүйенің өзі қанша қиын әрі сенімді болғанымен ол кілттердің қолданылуына негізделген. Егер ақпараттармен жасырын алмасуды екі пайдаланушы арасында қамтамассыз ету үшін кілттермен алмасу езбе процесс болса, онда кілттермен басқаруды пайдаланушылар саны ондап, жүздеп болатын пайдаланылатын жүйеде – қиын мәселе. Кілтті ақпараттың астарында пайдаланылатын барлық жұмыс істейтін кілттердің жиынтығы деген түсінік жатыр. Егер кілтті ақпараттың сенімді басқаруы айтарлықтай қамтамассыздандырылмаған болса, онда оны қолға түсіріп алып, қара ниетті барлық ақпаратқа шектеусіз ене береді. Кілтпен басқару – ақпаратты процесс, оған мына үш элемент кіреді:

- кілт генерациясы;
- кілттердің жинақталуы;
- кілттердің таралуы.

Пайдаланылатын жүйеде олар кілтті ақпараттың қауіпсіздігін қамтамассыздандыру үшін қалай жүзеге асуы тиістігін қарастырайық.

Кілттердің генерациясы. Криптографиялық әдістер туралы ең бастапқы әңгімеде-ақ жеңіл есте сақтау мақсатымен кездейсоқ кілттерді пайдаланудың қажеті жоқ екені айтылған болатын. Шынайы пайдаланылатын жүйелерде кездейсоқ кілттер генерациясының арнайы аппаратты және бағдарламалық әдістері пайдаланылады. Тәртіп бойынша ПСЧ көрсеткіштерін қолданады. Алайда олардың генерацияларының кездейсоқтық дәрежесі айтарлықтай жоғары болуы тиіс. «Табиғи» кездейсоқ процестер негізіндегі құрылғылар тамаша генераторлар болып табылады. Мысалы, кездейсоқ математикалық объект стандартты математикалық әдістердің көмегімен есептелетін ирроционалдық сандардың ондық таңбалары болып табылады.

Кілттердің жиналуы. Кілттердің жиналуы сөзінің астарында олардың сақталу, саналу және жойылуының ұйымдастырылу түсінігі жатыр. Кілт қаскүнем үшін жасырын ақпаратқа жол ашатын объект болғандықтан кілттер жинақталуы мәселесіне ерекше көңіл бөлген жөн. Құпия кілттер ешқашан саналуы немесе көшірілуі мүмкін таратушыға жаңа түрде жазылмауы тиіс. Айтарлықтай қиын ПЖ (пайдаланылатын жүйеде) қолданушы кілтті ақпараттың үлкен көлемімен жұмыс істеуі мүмкін, кейде тіпті кілтті ақпарат бойынша мәліметтердің мини-базалары ұйымдастырылу қажеттілігі туындайды. Мәліметтердің мұндай базалары пайдаланылатын кілттердің қабылдануы, сақталуы, есептелуі мен жойылуына жауап береді. Сонымен, қолданылатын кілттер туралы әрбір ақпарат шифрленген түрде сақталуы тиіс. Кілтті ақпаратты шифрлайтын кілттер шебер – кілттер деп аталады. Шебер кілттерді әр қолданушы жатқа білуі және оларды жалпы қандайда бір материалдық таратушыларда сақталмаған дұрыс. Ақпараттар қауіпсіздігінің өте маңызды шарты – ПЖ кілттің ақпараттың мезгіл сайын жаңартып отыруы болып табылады. Оның үстіне қарапайым кілттер сияқты шебер кілттер де қайта белгіленіп отыруы тиіс. Ерекше жауапты ПЖ кілтті ақпараттардың

жаңарып отыруын күнделікті жасаған дұрыс. Кілтті ақпараттың жаңару мәселесі кілтпен басқарудың үшінші элементі – кілттің таратылуымен де байланысты.

Кілттердің таратылуы. Кілттердің таратылуы – кілттермен басқарудағы ең жауапты процесс. Оған екі талап қойылады:

1) Таратылудың шапшаңдығы мен дәлдігі.
2) Таратылатын кілттердің құпиялылығы.

Соңғы уақыттарда кілттердің таратылу мәселесі жоқ болатын ашық кілтті криптожүйелердің қолданылу жағына жылжу байқалады. Алайда ПЖ кілтті ақпараттың таратылуы жаңа тиімді шешімдерді талап етеді. Қолданушылар арасында кілт таратылуы екі түрлі жолмен жүзеге асырылады:

1) Бір не бірнеше кілттер таралу орталығын құру жолымен. Мұндай әрекеттің кемтігі таралу орталығында кімге қандай кілттер белгіленгені белгілі және бұл ПЖ айналып жататын барлық хабарламаларды оқуға жол беретіндігінде. Мүмкін теріс пайдаланушылық қолданысқа едәуір ықпал етеді.

2) Ақпараттық жүйелерді қолданушылар арасында кілтті тікелей алмастырумен. Бұл жағдайда мәселе субъектілердің түп нұсқа екендігі сенімді куәландыруда. Кілттермен алмасу үшін сол RSA алгоритмін пайдалана отырып, ашық кілтті криптожүйелерді қолдануға болады.

Кілттердің таралуы туралы айтылғандардың талданған қорытындысы ретінде мыналарды айтқан дұрыс:

Кілттермен басқару міндеті кілттерді тарату орталығынан бас тарту мүмкіндігін, сеансқа қатысушылар түпнұсқалығын, өзара растауды, сұраныс – жауап механизмімен сеанстың нақтылығын растауды, бұл үшін бағдарламалық немесе аппараттық құралдарды пайдалануды, кілттермен алмасуда хабарламалардың азын пайдалануды қамтамассыздандыратындай кілттердің таралуының осындай протоколын іздеуге саяды.

2.4.5 Эль–Гамаль криптографиялық жүйесі.

Ашық кілті бар криптожүйенің тағы бір мысалы – бұл Эль-Гамаль жүйесі. Бұл жүйеде p жай саны таңдап алынады және СҒ(p) өрісі тұрғызылады. Осы өрістің α примитивті элементі, кездейсоқ сан $1< a<p-2$ таңдап алынады және $y = \alpha^a \bmod p$ есептеледі. Ары қарай (α, p, y) ашық кілт, ал кездейсоқ a – құпия кілт ретінде қолданылады.

Шифрлеу келесі түрде орындалады. Хабарлама сандар жиыны түрінде көрсетіледі, мұнда $1<M_i<p-1$. Кездейсоқ $1<k<p-2$ таңдап алынады және $\gamma=\alpha^к \bmod p$, содан кейін $\delta=M_i y^к \bmod p$ есептеледі. Криптограмма (γ,δ) жұбын көрсетеді.

Дешифрлеу. Құпия кілтті $1<a<p-2$ қолдана отырып, $\gamma^{-a} \bmod p$ есептейміз, содан соң $\delta\gamma^{-a} \bmod p=M_i\alpha^{ak}\alpha^{-ak}=M_i$ есептейміз.

Эль-Гамаль жүйесінің ерекшелігі ол рандомизациялық шифрлеу жүйесіне жататындығы болып табылады, яғни шифрлеу кезінде k кездейсоқ саны қолданылады. Рандомизациялық шифрлеу криптоталдаудың кейбір әдістеріне қатысты төзімді болып есептеледі. Жүйенің кемшілігі

криптограмма ұзындығы хабарлама ұзындығынан 2 есе үлкен болғандығында. Эль-Гамаль жүйесі дискретті логарифмдеудің NP-күрделі есебіне негізделген. M_i хабарламаның әрбір бөліктерін шифрлеу кезінде әртүрлі k таңдау қажет екендігін атап өту керек, өйткені белгілі M_i кезінде $\frac{\delta_1}{\delta_2} = \frac{M_i}{M_j}$ қатынасынан M_j есептеу оңай.

Электронды цифрлік қолтаңбалар.

Желі бойынша электронды құжаттарды жіберу кезінде құжат авторының және құжаттың өзінің аутентификациясы мәселесі туындайды, яғни автордың түпнұсқалығын орнату және алынған құжатта өзгерістердің жоқтығы. Аутентификация мақсаты қаскүнем әрекеттерінен қорғау болып табылады, оларға мыналар жатады:

1) Бас тарту (ренегатство) – жіберуші соңынан жіберілетін хабарламадан бас тартады.

2) Маскировка – заңбұзушы басқа пайдаланушы болып маскіленеді.

3) Қайталау – заңбұзушы алдында А абоненті В абонентіне жіберген құжатты қайталайды.

4) Алмастыру – алушы құжатты өзгертеді немесе алмастырады және оны жіберушіден алдым деп хабарлайды.

Электронды цифрлік қолтаңба қарапайым қол қоюмен теңбе тең және оның негізгі ерекшеліктеріне ие:

– қол қойылған мәтін қол қойған адамнан келді дегенді растайды;

– осы адамның өзіне қол қойылған мәтінмен байланысты міндеттерінен бас тарту мүмкіндігін бермейді;

– қол қойған мәтін бүтіндігін кепіл етеді.

Ассиметриялық криптожүйелерге негізделген цифрлік қолтаңба алгоритмі.

Ассиметриялық криптожүйелерге негізделген цифрлік қолтаңбаны қалыптастыру алгоритмі негізінде белгілі NP-күрделі есептеу есептері жатыр:

- үлкен бүтін сандардың факторизация есептері (жиындарға бөлу);
- дискретті логарифмдеу есептері.

Цифрлік қолтаңбаны қалыптастыру үшін RSA жүйесін пайдалануға болады. Бұл жүйеде цифрлік қолтаңба құру құпия кілтте құжатты шифрлеумен теңбе тең. Бұл жағдайда әрбір адам ашық кілтпен қолдануы мүмкін және қолтаңба түпнұсқалығын тексере алады. Демек, қолтаңба мына формула арқылы алынады:

$$SIG(X) = X^d \bmod n, \qquad (2.17)$$

мұнда d – X ашық хабарға қол қойған пайдаланушының құпия кілті. Қалған пайдаланушылар осы пайдаланушының ашық кілті көмегімен верификацияны жүзеге асырады, яғни:

$$(SIG(X))^e \bmod n = X^{de} \bmod n = X. \qquad (2.18)$$

Мұндай шарттың кемшілігі ассиметриялық алгоритммен оларды шифрлеу арқылы үлкен құжаттарға қол қою шифрлеудің төмен жылдамдығына байланысты тиімді емес. Шешімі хеш-функция немесе

хэштеу функциясы деп аталатын арнайы тиімді есептеу функциясын қолдануды пайдалану болып табылады. Бұл функция кірісі X хабарлама, ал шығысы m=h(X) сөзі болып табылады. Цифрлік қолтаңба осы схема бойынша алынады, бірақ хабарламаның өзі емес, ал одан хеш-функция мәні қолданылады. Басқаша айтқанда, цифрлік қолтаңбаны мына түрде есептейді:

$$SIG(X) = m^d \bmod n.$$

Ары қарай (X, SIG(X)) жұбы SIG (X) цифрлік қолтаңбамен қол қойылған X электронды құжат ретінде алушыға жіберіледі. (X, SIG(X)) жұбын алған соң алушы X хабарламаның хэш-мәнін екі әдіспен есептейді. Біріншісі, ол е ашық кілтте қолтаңбаны шифрлеуді қолдана отырып, m хэш-мәнін қалпына келтіреді

$$m= (SIG(X))^e \bmod n.$$

Сондай-ақ, ол m=h(X) хэш-функция көмегімен X қабылданған хабарламаны хэштеу нәтижесін табады. Егер алынған мәндер тең болса, онда қабылдаушы (X, SIG(X)) жұбын түпнұсқа екендігін мойындайды. Құпия кілті d бар адам ғана X құжаты бойынша цифрлік қолтаңбаны қалыптастыруы мүмкін екендігі дәлелденген және ашық кілт бойынша құпия кілтті анықтау жиындарға n модулін қоюға қарағанда оңай емес.

RSAжүйесі негізінде цифрлік қолтаңба жүйесінің кемшіліктеріне мыналарды жатқызуға болады:

1) DES шифрлеу стандарты деңгейінде RSA цифрлік қолтаңбаның криптотөзімділігін қамтамасыз ету үшін есептеу кезінде әрбіреуі 2^{512}ретте n, e, d сандарын қолдану керек, бұл үлкен есептеу шығындарын қажет етеді.

2) RSA цифрлік қолтаңба мултипликативті шабуыл деп аталатын шабуылға төзімді емес. Басқаша айтқанда, алгоритм құпия кілтті білмей-ақ қаскүнемге хэштеу нәтижесін қол қойылған құжаттарды хэштеу нәтижесін көбейту ретінде есептеуге болатын құжаттар етіп қолды қалыптастыру мүмкіндігін береді.

Мысалы, үш X_1, X_2 мен Xз хэш-функциясымен хабарлама бар:

$m_1=h(X_1)$, $m_2=h(X_2)$, $m_3=h(X_3)$, яғни $m_3 = m_1m_2 \bmod n$.

Енді X_1 мен X_2 екі хабарлама үшін заңды цифрлік қолтаңба алынды делік

$$SIG(X_1)=m_1^d \bmod n$$
$$SIG(X_2)=m_2^d \bmod n.$$

Оны қаскүнем d құпия кілтті білмей-ақ X_3 құжаты үшін $SIG(X_3)$ қолтаңбаны оңай есептей алады:

$$SIG(X_3)= SIG(X_1)\, SIG(X_2) \bmod n.$$

Шынында да,

$$SIG(X_1)\, SIG(X_2) \bmod n= m_1^d m_2^d \bmod n=(m_1m_2)^d \bmod n=m_3^d \bmod n= SIG(X_3).$$

3) Хабарлама қайталанған кезде қолтаңба өзгермейді.

Дербес компьютерлерде жүзеге асуы үшін ең сенімді және ыңғайлы цифрлік қолтаңба алгоритмі 1984 ж. Тахер Эль-Гамалмен құрастырылған. Цифрлік қолтаңба фальсификациясының практика жүзінде болмауын негіздеу

үшін дискретті логарифмдеу есептеріне қарағанда күрделі есептеу есептері қолданылған. Сондай-ақ, Эль Гамальға құпия кілтті анықтаусыз қандайда бір хабарламамен цифрлік қолтаңбаны ұқсатып жасау мүмкіндігімен байланысты RSA цифрлік қолтаңба алгоритмінің анық әлсіздігінен құтыла алды.

Цифрлік қолтаңба, егер бір хабарлама екі рет қол қойылған жағдайда әртүрлі болуы үшін Эль-Гамальмен келесі алгоритм ұсынылды. α - СҒ(p) өрісінің примитивті элементі, мұндай – жайсан. Өріс жіберуші мен алушыға белгілі. Жіберуші өзінің 1≤z≤p-2 құпия кілтін пайдалана отырып, ашық кілтті есептейді

$$y = \alpha^z \bmod p$$

және оны ашық анықтамаға орналастырады. Содан соң, X хабарламаға қол қою үшін ол оның хеш-функциясын есептейді

$$m=h(X), \qquad (2.19)$$

мұнда 1<m<p-1.

Ары қарай, ол p-1-мен өзара жай 1≤k≤p-2 кездейсоқ санды таңдайды және мынаны есептейді

$$r=\alpha^k \bmod p. \qquad (2.20)$$

Содан соң Евклидтің кеңейтілген алгоритмі көмегімен жіберуші k^{-1} табады, яғни $k^{-1}k=1 \bmod (p-1)$ шешеді. k элементі p -1 модулі бойынша элемент сақинасында кері элементке ие, өйткені k p -1-мен өзара жай.

Содан ол s есептейді:

$$s=k^{-1}(m-zr) \bmod (p-1)$$

немесе

$$m=zr+ks \bmod (p-1). \qquad (2.21)$$

(r, s) жұбы қолтаңба ретінде қолданылады. Өңдеуден кейін k қолы жойылады.

Алушы y ашық кілтін біледі. m=h(X) хабарламадан хеш-функцияны есептейді. (r, s) қолын алған соң $y^r r^s=\alpha^m \bmod p$ екендігін тексереді. Бұл теңдеудің дұрыстығы $y^r r^s=\alpha^{zr}\alpha^{ks}=\alpha^m \bmod p$ көрініп тұр.

Мысал. Хабарламаға қол қою.

M=baaqab хабарламасына қол қою керек делік. Кілттер генерациясын жүргізейік: p=23, α=5 айнымалылар делік, олар белгілі бір қоғамға белгілі. Құпия кілт z=7 – кездейсоқ бүтін сан, ол 1<x<p.

y ашық кілтті есептейміз: $y=\alpha^z \bmod p$.

$y=5^7 \bmod 23=17$.

Демек, ашық кілт үштік (α, p, y) болып табылады (5, 23, 17).

Енді хэш-функцияны есептейік: h(M)=h(baaqab)=m=3; k кездейсоқ санды таңдайық, ол 1<k<p-1 шартын орындау керек.

k =5 делік. $r=\alpha^k \bmod p=5^5 \bmod 23=20$ есептейміз.

$s=k^{-1}(m-zr) \bmod (p-1)$ санын табамыз. Мұндай s бар, өйткені НОД(k,p-1)=1. s=21 аламыз.

Демек, біз хабарламаға қол қойдық: <baaqab, 20, 21>.

Алынған хабарлама түпнұсқалығын тексеру.

Хэш-функцияны есептейміз: h(M)=h(baaqab)=m=3. Салыстыруды $y^r r^s=\alpha^m \bmod p$ тексереміз.23 модулі бойынша сол жағын есептейміз: $17^{20} \cdot 20^{21} \bmod 23=16 \cdot 15 \bmod 23=10$.

23 модулі бойынша оң жақ бөлігін есептейміз: $5^3 \bmod 23=10$.

Оң және сол жақ бөліктері тең болғандықтан, қол дұрыс екендігін білдіреді.

Цифрлік қолтаңба төзімділігінің берілген деңгейінде есептеуге қатысатын бүтін сандар екілік көрсетілуінің RSA негізіндегі жүйеге қарағанда 25% кем ұзындығына ие, бұл есептеу қиындығын екі есе төмендетеді. Бірақ, цифрлік қолтаңба ұзындығы RSA негізіндегі жүйелерге қарағанда 1,5 есе үлкен, бұл оның есептеу уақытын ұлғайтады. Демек, RSA негізіндегі жүйеде және Эль-Гамаль жүйесінде цифрлік қолтаңбаны есептеу уақыты бірдей.

2.4.6 Шноррдің цифрлік қолтаңба жүйесі.

Шноррдің цифрлік қолтаңба жүйесі Эль-Гамаль цифрлік жүйесіне ұқсас.

p – жай сан, q - (p-1) жай бөлгіші, ал g –СҒ(p)-де q реттегі элемент (p модулі бойынша бұл элементтің дәрежесі q өрістің әртүрлі элементтерін тудырады) делік, $0 < k < q$- кездейсоқ сан, $0 < z < q$ – құпия кілт, $y = g^z \bmod p$ – ашық кілт. Қолтаңбаны алу теңдеуі мына түрге ие

$$r= g^k \bmod p,\ e = h(X, r),\ s=(ze +k) \bmod q.$$

Қолтаңба (e, s) болып табылады. Бұл жағдайда алушы $g^s y^{-e} \bmod p$ және $e^{/} = h(X, g^s y^{-e} \bmod p)$ хэш-функцияны есептейді. Егер $e^{/} = e$, онда қолтаңба дұрыс деп есептеледі.

Шнорр жүйесі бойынша құрылған цифрлік қолтаңба Эль- Гамаль немесе RSA жүйесіне қарағанда қысқа.

DSS (Digital Signature Standard) стандарты АҚШ-та 2000 ж. қабылданды. Бұл стандартқа сәйкес үш алгоритмнің біреуі қалыптасуы мүмкін:

1) DSA (Digital Signature Algorithm), соңғы өрісте логарифмдерді есептеу мәселесіне негізделген.

2) ANSI X9.31 (RSA DSA).

3) ANSI X9.63, соңғы өріспен эллипстік қисықтың нүктесі тобында логарифмдерді есептеу мәселесіне негізделген.

DSA алгоритмі келесі сатылардан тұрады:

1) Алдын ала сатысы- параметрлерді таңдау

Келесі параметрлер таңдап алынады: $p - 2l-1 < p < 2l$ диапазонындағы жай сандар, g - СҒ(p) өрісінде q ретті элемент, $\alpha(p-1)/q$ түрінде таңдап алынады, мұнда α – примитивті элемент.

$0 < z < q$ құпия кілт таңдап алынады және $y = gz \bmod p$ қолтаңбаны тексеру үшін ашық кілт есептеледі.

2) Цифрлік қолтаңбаны қалыптастыру

h(X) хабарламадан хэш-функция мәні есептеледі. Сондай-ақ SHA-1 (Secure Hashing Algorithm) қауіпсіз хэштеу алгоритмі қолданылады. h(X) мәні 160 бит ұзындыққа ие. Ары қарай жіберуші кездейсоқ мәнді $0 < k < q$ таңдап алады және k-1 mod q есептейді. Содан соң мәндер жұбы есептеледі

$$r = gk \pmod p \pmod q;$$
$$s = k\text{-}1\ (h(X) + zr) \pmod q.$$

(r, s) мәндер жұбы X хабарламаның цифрлік қолтаңбасы болып табылады. Қолтаңбаны алған соң k мәні жойылады.

3) Цифрлік қолтаңба верификациясы

Алушы $g^{h(X)s^{-1}} y^{rs^{-1}} (\mathrm{mod}\ p)(\mathrm{mod}\ q)$ есептейді және алынған мәнді r-мен салыстырады. Қолтаңба дұрыс болып есептеледі, егер алынған нәтиже r-мен сәйкес келсе.

Есептелетін мәнді қарастырайық

$$g^{h(X)s^{-1}y^{rs^{-1}}} y^{rs^{-1}} (\mathrm{mod}\ p)(\mathrm{mod}\ q) = g^{h(X)s^{-1}} g^{zrs^{-1}} (\mathrm{mod}\ p)(\mathrm{mod}\ q) =$$
$$= g^{s^{-1}(h(X)+zr)} (\mathrm{mod}\ p)(\mathrm{mod}\ q) = g^{k^{-1}(h(X)+zr))^{-1}(h(X)+zr)} (\mathrm{mod}\ p)(\mathrm{mod}\ q) =$$
$$= g^{(k^{-1}(h(X)+zr))^{-1}(h(X)+zr)} (\mathrm{mod}\ p)(\mathrm{mod}\ q) =$$
$$= g^{k} (\mathrm{mod}\ p)(\mathrm{mod}\ q) = r.$$

Төзімділіктің кез келген деңгейінде z, q, r, s сандары 160 бит ұзындыққа ие, бұл цифрлік қолтаңба ұзындығын 320 битке дейін қысқартады [4].

2.4.7 Симметриялық және ассиметриялық шифрлерді бірге қолдану.

Ашық кілті бар криптографиялық алгоритмдердің негізгі артықшылығы қауіпсіз емес арна бойынша кілттерді үлестіру, хабарлама мен жіберуші аутентификациясы және т.с.с. есептерді шешу мүмкіндігі болып табылады. Сондай-ақ, ассиметриялық шифрлер симметриялыққа қарағанда әлдеқайда ақырын жұмыс істейді. Бұл өте үлкен сандармен операцияларды жүргізу қажеттілігімен байланысты. Сондықтан симметриялық және ассиметриялық алгоритмдер жиі бірге қолданылады – кілттерді үлестіру үшін және ЭЦҚ ашық кілті бар криптографияны пайдаланады, деректер симметриялық алгоритмдер көмегімен шифрленеді.

Бірнеше алгоритмдер бірге қолданылатын жүйені талдау кезінде ең әлсіз буынды бұзу күрделілігі бойынша оны бұзу қиындығы бағалану қабылданған. Әдебиетте [9] симметриялық шифрлеу алгоритмі мен сәйкес төзімділігін қамтамасыз ететін RSA алгоритмі үшін сәйкесінше мысал ретінде кілттер ұзындығы келтірілген. Мысалы, симметриялық шифрлеудің 64-биттік кілтіне RSA 512-биттік кілті, ал 128 биттікке – RSA 2300 биттен асатын ұзындығы бар кілті сәйкес келеді.

2.5 Хэш-функциялар

Хэш-функция айнымалы ұзындықты X енгізу хабарламасының H тіркелген ұзындықты m жолына m = h(X) бейнелеуді көрсетеді. Hash ұсақ етіп бөлу және араластыру дегенді білдіреді. Көбінесе m X-ке қарағанда қысқа және енгізу хабарламасының қысылған екілік көрінісі болып табылады.

Хэштеу функциясы келесі шарттарды қанағаттандыруы керек:

1) Хэш-функция кез келген өлшемді аргументке қолданылуы мүмкін.

2) Шығару мәні тіркелген өлшемге ие.

3) Хэш-функцияны есептеу жылдамдығы хэш-функцияны пайдалану кезінде цифрлік қолтаңбаны қалыптастыру жылдамдығы хабарламаның өзін қолдану кезінде цифрлік қолтаңбаны қалыптастыру жылдамдығынан асатындай болуы керек.

4) Хэш-функция біржақты функция болып табылады. Ашық кілтпен криптожүйенің төзімділігі ашық түрлендіру лазейкасы бар біржақты функция болып табылатындығына байланысты. Бұл функциялардан ерекшелігі хэш-функция лазейкасы жоқ біржақты функция болып табылады. Демек, кез келген m үшін есептеу тұрғысынан қарағанда X, h(X) = m ашық мәтінін табу мүмкін емес.

5) Екі әртүрлі құжаттардың хэш-функциясы мәні (олардың ұзындығына байланысты емес) сәйкес болу ықтималдығы аз болуы керек.

Коллизияның екі түрін ерекшелейді. Бірінші түрдегі коллизия келесіден тұрады. X_1 қандайда бір мәтін $m_1 = h(X_1)$ хэш-функцияның шығару мәніне ие болсын. Егер X_2 қандайда бір басқа мәтін табылып, ол да сондай-ақ $h(X_2) = m_1$ ие болса, коллизия болады. Екінші түрдегі коллизия екі әртүрлі мәтін үшін хэш-функцияның мәні сәйкес келуінен тұрады. Хэш-функциялардың бірінші түрдегі коллизияға төзімділігі ашық мәтінді таңдау үшін криптоаналитикке қажет амалдар санымен бағаланады. Бұл амалдар саны 2^n ретке ие, мұнда n-хэш-функцияның шығару мәнін биттік көрсету ұзындығы. Екінші түрдегі коллизияға хэш-функцияның төзімділігін ықтималдықтар теориясында белгілі «туған күн парадоксын» пайдаланумен бағаланады.

Туған күннің сәйкес түсуі туралы есеп келесі түрде қалыптасады:

Бөлмеде r адам бар болсын. Екеуі немесе одан да көп адамның туған күні бірдей болу ықтималдығын бағалау қажет. Сәйкес келмеу ықтималдығы мынаған тең $P_{сәйкескелмеу} \approx \left(1-\frac{1}{365}\right)\left(1-\frac{2}{365}\right)\ldots\left(1-\frac{r-1}{365}\right)$.

Бұл ықтималдықты $P_{сәйкескелмеу} \approx 1-\frac{r^2}{365}$ бағалауға болады.

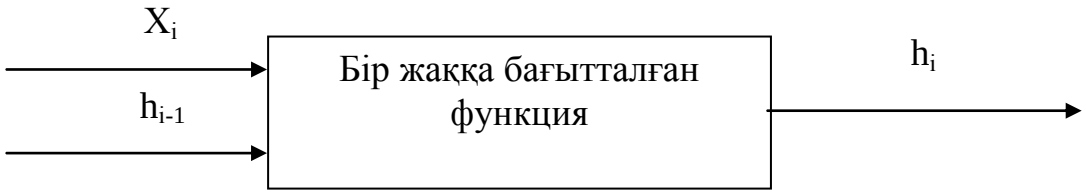
Біздің есепке сәйкес $P_{сәйкескелмеу} \approx 1-\frac{r^2}{N}$ аламыз, мұнда r – криптоаналитиктің амалдар саны, N –хэш-функция мәнінің жалпы саны. Онда егер $1 - P_{сәйкескелмеу} = C$ болса, мұнда $0 < C < 1$ – қандайда бір константа, онда хэш-функцияның екі бірдей мәнімен екі мәтінді табу үшін амалдар санын былайша бағалауға болады

$$r \approx \sqrt{CN} \approx \sqrt{C2^n} \approx 2^{\frac{n}{2}}.$$

Есеп туған күн парадоксы атауын алынатын нәтиженің сәйкес келмеуінен және ол туралы интуитивті ойлауынан алды. Бөлмеде 23 адам болған жеткілікті екен, өйткені екі немесе одан да көп адамның туған күні сәйкес келуі ықтималдығы 0,5 көп болуы үшін. Белгілі күнде r-ден екі немесе одан да көп адамның туылуы ықтималдығы келесі формула бойынша есептеледі $1-\left(1-\frac{1}{365}\right)^r$ және r= 23 болғанда 0,06 тең.

Көптеген хэш-функциялар f(•) біржақты функция негізінде құрылады, олар екі енгізу мәнін берген кезде H ұзындықты шығару мәнін

қалыптастырады, ұзындық қосындысы k битке тең, мұнда k ≥ H. Бұл шығарулар k-H бит ұзындықты X алғашқы мәтін блогы болып табылады және мәтіннің алдыңғы блогының h_{i-1} хэш-мәні 2.13-суретте көрсетілген.

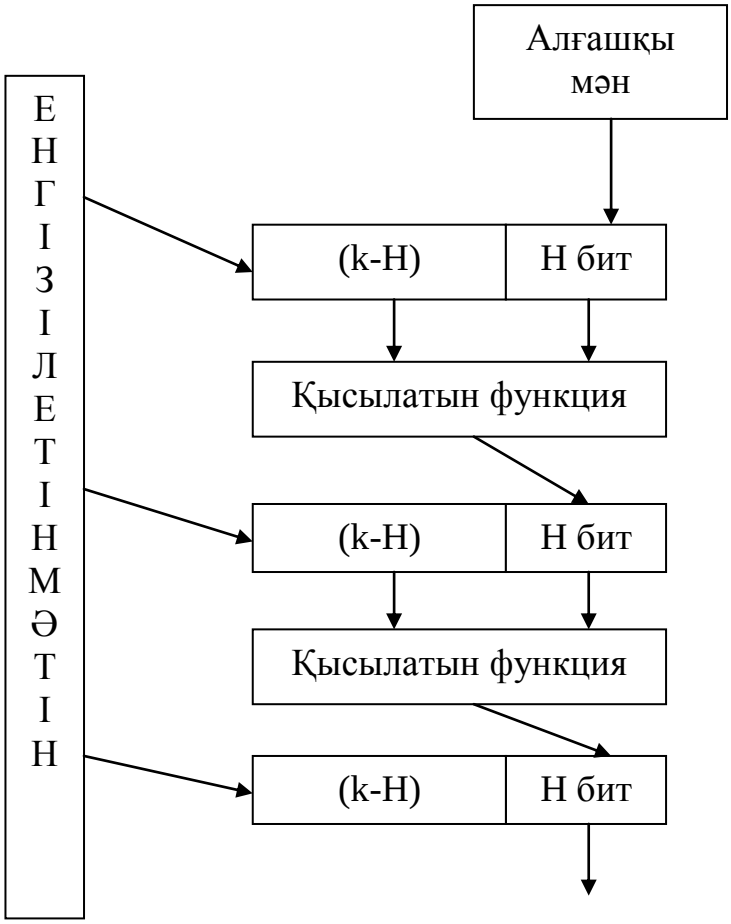


2.13 сурет - Біржаққа бағытталған $h_1=f(X, h_{i-1})$ хэш-функциясын тұрғызу

Мәтіннің соңғы блогын енгізу кезінде есептелетін хэш-мән барлық X хабарламаның хэш-мәні болады. Нәтижесінде біржақты хэш-функция әрдайым H тіркелген ұзындықты шығаруды қалыптастырады (енгізілетін мәтін ұзындығына тәуелсіз).

Басқа сөзбен айтқанда, хэш-функцияны тұрғызудың жалпықабылданған принципі итеративті тізбектелген схема болып табылады. Алгоритм ядросы k биттің H битке түрленуі болып табылады, мұнда H – хэш-функцияның шығу разрядтылығы, ал k – H үлкен немесе тең дербес сан. Базалық түрлендіру хэш-функцияның барлық қасиеттеріне ие болуы керек. Хэштеу H бит разрядты аралық көмекші айнымалы көмегімен жүргізіледі. Оның бастапқы мәні ретінде дербес белгілі мәні таңдап алынады, мысалы, 0.

Енгізілетін мәндер (k -H) бит бойынша блоктарға бөлінеді. Хэштеудің әрбір итерациясында алдыңғы итерацияда алынған аралық шама мәнімен енгізілетін деректердің (k -H) битінен кезекті блок біріктіріледі және алынған k-биттік блокпен базалық түрлендіру жүргізіледі. Нәтижесінде барлық енгізілген мәтін қосалқы шаманың бастапқы мәнімен «араласқан» болып кетеді. Түрлендіру сипатына қарай базалық біржақты функцияны жиі қысатын деп атайды. Қосалқы шама мәні соңғы итерациядан кейін хэш-функцияның шығарылу жеріне келіп түседі (2.14 сурет). Кейде алынған мәнмен қосымша түрлендірулер жүргізеді.



2.14 сурет - Итеративті хэш-функция

Криптографияда хэш-функцияның 2 класы қолданылады:

1) Кілтсіз хэш-функциялар.

2) Кілтпен хэш-функциялар.

2.5.1 Кілтсіз хэш-функциялар.

Кілтсіз хэш-функциялар әлсіз және күшті болып бөлінеді. Әлсіз хэш-функция деп келесі шарттарды қанағаттандыратын H(x) біржақты функциясы аталады:

- аргумент кездейсоқ ұзындықтағы бит жолы болуы мүмкін;
- H(x) функциясының мәні белгіленген ұзындықтағы бит жолы болуы мүмкін;
- H(x) мәнін есептеу оңай;
- кез келген белгіленген аргумент x үшін басқа x’≠ x табу есептеу тұрғысынан мүмкін емес, олар H(x’)=H(x).

x’≠ x: H(x’)=H(x) мәндер жұбы хэш-функцияның коллизиясы деп аталады.

Күшті хэш-функция деп 1-3 шарттарын және келесі тұжырымдауда соңғы шартты қанағаттандыратын H(x) біржақты функциясы аталады:

- x’≠ x мәндерінің кез келген жұбын табу есептеу тұрғысынан мүмкін емес, олар H(x’)=H(x).

Кез келген күшті хэш-функция әлсіз үшін талаптарға сәйкес келеді. Әлсіз және күшті хэш-функция коллизиясын іздеу күрделілігінде айырмашылықты көрсету үшін «туған күн парадоксын» пайдаланумен шабуылды қарастыруға болады. Аргумент x мәнін белгілеп, кездейсоқ түрде x’≠ x іріктейміз, мұнда H(x’)=H(x). Егер хэш-функция мәні тең үлестірілген, ал H(x) мүмкін мәндер саны N тең деп болжасақ, онда орташа N/2 нұсқаны іріктеу қажет болады. Егер де біз қандайда бір коллизияны толықтай тапқымыз келсе, онда есеп оңайырақ болады: 0,63 ықтималдығымен мәндердің қажет жұбын анықтау үшін N нұсқаны сынау қажет. Криптографиялық хэш-функцияны құру құнын минималдау үшін құрастырушылар жиі шифрлеудің бар алгоритмдерінің бірін қолданады. E(m,k)k кілтінде m хабарламасын шифрлеу, ал v_0 – старттық вектор белгіленсін делік. Хэштелетін M хабарламасын блоктар тізбегі m_1, …, m_tтүрінде көрсетейік және оларды раундтық кілттер ретінде қолданайық. Сонда H(m) келесі түрде есептеледі:

$$h_0=v_0;$$
$$h_i=E(h_{i-1},m_i);\ i = 1...t; \qquad (2.22)$$
$$H(m)=h_t.$$

Бірақ DES алгоритмінің E(m,k) ретінде пайдалануымен нұсқасында «туған күн парадоксына» негізделген шабуылдарды дәлелдеуден соң жеткіліксіз төзімді болып шықты. Бұл сұлбаны жақсарту ұсынылды, мысалы, келесі түрде:

$$h_0=v_0;$$
$$h_i=E(h_{i-1},m_i) \oplus h_{i-1};\ i=1...t; \qquad (2.23)$$
$$H(m)=h_t.$$

Хэштеу алгоритмдерінің арнайы құрастырылған қатары бар, олардың бірі - SHA-1

2.5.2 SHA-1 алгоритмі.

SHA (Secure Hash Algorithm) қауіпсіз хэштеу алгоритмі АҚШ стандарты ретінде 1993 жылы қабылданды және DSS стандартында анықталған цифрлік қолтаңба алгоритмімен бірге пайдалануға арналған. Ашық мәтінді енгізген кезде алгоритм цифрлік қолтаңбаны шығару кезінде қолданылатын 160-биттік шығарылатын хабарламаны өңдейді (digest (қысқаша айту), «дайджест» деп атайды). SHA хэштеу алгоритмі қауіпсіз деп аталған, өйткені ол берілген дайджестке сәйкес хабарламаны қалпына келтіру есептеу тұрғысынан мүмкін емес болатындай жобаланған. Жіберу кезінде хабарламаның кез келген өзгерісі жоғары ықтималдықпен дайджесттің өзгеруін шақырады және қабылданған цифрлік қолтаңба тексерістен өтпейді. Мысалы, егер хабарламаның 800 бит ұзындығы бар болса, онда 801-ші бит=1, содан 960 битке дейін нольдер қосамыз, одан кейін қалған 64-разрядтарда «800» санын жазамыз, соңында 1024-биттік хабарламаны хэштейміз. Түрлендірудің жалпы

сұлбасы 2.15-суретте көрсетілген. Түрлендіруді бастамас бұрын бес 32-биттік айнымалылар инициалданады:

A=0x67452301;

B=0xEFCDAB89;

C=0x98BADCFE;

D=0x10325476;

E=0xC3D2E1F0.

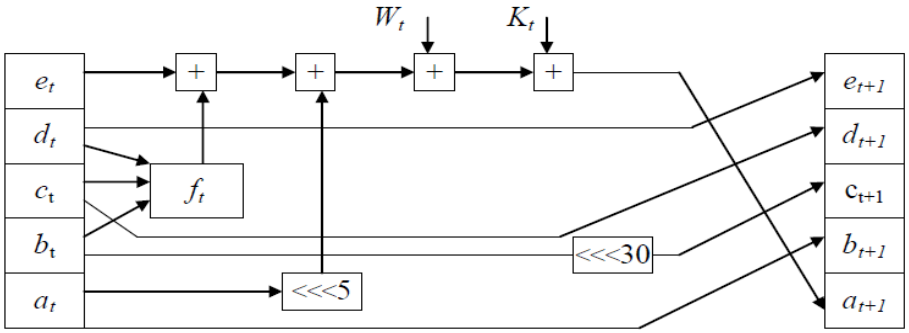
Бұл мәндер сондай-ақ a_0, b_0, c_0, d_0, e_0 айнымалыларға меншіктеледі.

Түрлендіру 80 раундта 512 бит өлшемімен хабарлама блогымен жүргізіледі. Түрлендіру үрдісінде келесі f_t сызықты емес функциясы қолданылады:

t=0…19 үшін $f_t(X,Y,Z)=(X\wedge Y)\vee((\neg X)\wedge Z)$;

t=20…39 және t=60…79үшін $f_t(X,Y,Z)=X\oplus Y\oplus Z$;

t=40…59 үшін $f_t(X,Y,Z)=(X\wedge Y)\vee(X\wedge Z)\vee(Y\wedge Z)$.



2.15 сурет - Схема раунда алгоритма SHA-1 алгоритмінің раундтар сұлбасы

Түрлендіру үрдісінде төрт тұрақты қолданылады:

t=0…19 үшін K_t=0x5A827999;

t=20…39 үшін K_t=0x6ED9EBA1;

t=40…59 үшін K_t=0x8F1BBCDC;

t=60…79 үшін K_t=0xCA62C1D6.

M алғашқы хабарлама блогы M_0, …, M_{15} 16 32-разрядты ішкі блоктар түрінде көрсетіледі, олар Wt мәндерін қалыптастыру үшін қолданылады:

t=0…15 үшін $W_t=M_t$;

t=16…79 үшін $W_t=(W_{t-3}\oplus W_{t-8}\oplus W_{t-14}\oplus W_{t-16})<<<1$.

«<<< X» белгісі – сол жаққа X разрядқа циклдік жылжу,«+» – 232 модулі бойынша қосу.

Кезекті 512-биттік блокты түрлендірген соң, алынған a,b,c,d,e мәндері сәйкесінше A,B,C,D,E мәндерімен қосылады және келесі блоктың өңделуі (немесе егер өңделген блок соңғы болса, a,b,c,d,e тіркесі түрінде алынған мән шығуға әкелінеді) басталады.

Демек, шығуда алғашқы хабарламаның 160-биттік дайджестін аламыз.

2.5.3 Кілтпен хэш-функциялар.

Ашық кілтпен хэш-функция деп келесі қасиеттермен H(k,x) біржақты функциясы аталады:

- H(k,x) функциясының x аргументі дербес ұзындықты бит жолы болуы мүмкін;
- функция мәні белгіленген ұзындықты бит жолы болуы мүмкін;
- кез келген k мен x деректері болғанда H(k,x) есептеу оңай;
- кез келген x үшін k білмей, H(k,x) есептеу іс жүзінде мүмкін емес;
- {x, H(k,x)} белгілі жұптың үлкен саны болғанда k анықтау немесе x’≠ x үшін H(k,x’) ақпарат бойынша есептеу іс жүзінде мүмкін емес.

Жиі мұндай функциялар хабарламаның аутентификация коды (ағылш. «Message Authentication Code», қысқаша MAC) деп аталады. Отандық әдебиеттерде имитоқорғалмалы кірістірме (немесе имитокірістірме).

Кілтпен хэш-функцияны кілтсіз криптографиялық хэш-функция негізінде немесе шифрлеу алгоритмінде тұрғызуға болады.

H(x) – кілтсіз хэш-функция болсын. Кілтті хэштеу үрдісіне ендіруге және H(k,x) кілтімен хэш-функцияны алуға болады. Тұрғызудың мүмкін нұсқалары төменде келтірілген:

$$H(k,x)=H(k|x);$$
$$H(k,x)=H(x|k), \qquad (2.24)$$

$H(k,x)=H(k_1|x|k_2)$, мұнда $k=k_1|k_2$.

| символы аргументтердің жолын біріктіру, конкатенацияны білдіреді.

Басқа мысал – DES шифрі көмегімен хэш-функцияны тұрғызу. m енгізу мәтіні $m_1,...,m_t$ блоктарға 64 бит бойынша бөлінеді, олар келесі түрде түрленеді (k – шифрлеу кілті):

$$c_0=0,$$
$$ci=DESk(mi \oplus ci\text{-}1),\ i=1,...,t, \qquad (2.25)$$
$$H(k,m)= ct.$$

Бақылау сұрақтары.

1. Ақпаратты қорғаудың криптографиялық принциптерін атаңыз.
2. Деректерді қорғаудың криптографиялық құралдарына не жатады?
3. Криптожүйелерге қандай талаптар қойылады?
4. Симметриялық криптографиялық жүйелер дегеніміз не?
5. Шифрлеу әдістерін атаңыз.
6. Құпия кілтпен шифрлеу дегеніміз не?
7. Шабуыл түрлерін атаңыз.
8. Криптошабуыл түсінігі, шабуылдардың жіктелуі, оларды жүзеге асыру кезеңдері.
9. DES стандартына сипаттама беріңіз.
10. DES стандартына шабуыл және DES күшейту нұсқаларын атаңыз.
11. AES стандарты. Rijndael алгоритмдері дегеніміз не?
12. Ағымды шифрлер дегеніміз не?
13. Ағымды шифрдің жалпы схемасын көрсетіңіз.

14. Өзіндік синхрондалатын шифрлер (автокілтпен) дегеніміз не?

15. Синхронды шифрлер дегеніміз не?

16. Ашық кілті бар криптожүйеге сипаттама беріңіз.

17. Біржақты функция дегеніміз не?

18. Диффи-Хеллман – Меркль кілттерін үлестіру.

19. Ашық кілтпен шифрлеу идеясы.

20. Электрондық цифрлық қолтаңба (ЭЦҚ). ЭЦҚ құрылымы және ЭЦҚ қою қағидаттары.

21. Цифрлік қолтаңба идеясы.

22. Цифрлік қолтаңба қасиеттерін атаңыз.

23. RSA криптографиялық алгоритміне сипаттама беріңіз.

24. Ассиметриялық криптожүйелерге негізделген цифрлік қолтаңба алгоритмін сипаттаңыз.

25. Хэштеу функциясы дегеніміз не?

3 Ақпараттық қауіпсіздікті қамтамасыз етудің программалық-техникалық шаралары

3.1 Ақпараттық қауіпсіздіктің программалық-техникалық деңгейінің негізгі түсініктері

Программалық-техникалық шаралар болып ақпараттық жүйелер мен ақпаратты қорғау бойынша есептерді қамтамасыз етуге бағытталған технологиялар жиынтығы түсініледі. Берілген шаралар ақпараттық қауіпсіздікті қамтамасыз ету бойынша көптеген есептерді автоматтандыруға мүмкіндік береді.

Ақпараттық жүйені детализацияның бастапқы деңгейінде қарастыру кезінде ол АЖ негізгі функционалды есептерін орындауды қамтамасыз ететін ақпараттық сервистер жиынтығы ретінде қарастырылуы мүмкін.

Қауіпсіздік сервисі санына мыналарды жатқызуға болады:

1) Идентификация және аутентификация.
2) Кірумен (доступ) басқару.
3) Протоколдау және аудит.
4) Шифрлеу.
5) Бүтіндікті бақылау.
6) Экрандау.
7) Қорғалу анализі.
8) Серпімділікті қамтамасыз ету.
9) Қауіпсіз қалпына келтіруді қамтамасыз ету.

Қауіпсіздік сервистер негізіне қауіпсіздік шараларының жіктелуі және олардың АЖ жалпы архитектурасындағы орны:

1) Превентивті (ескерту).
2) Қатені табу шаралары.

3) Әрекеттесудің локальді зоналары.
4) Қатені табу бойынша шаралар.
5) Қауіпсіздік режимін қалпына келтіру шаралары.

Идентификация мен аутентификация. Идентификация мен аутентификация – АҚ программалық-техникалық құралдарының негізі. Идентификация АЖ-де субъектке өз атын көрсетуге мүмкіндік береді. Аутентификация енгізілген идентификаторды растау шарасы болып табылады.

Аутентификация біржақты (клиент серверге өзінің өзі екендігін дәлелдейді) немесе екіжақты (өзара келісілген) болып бөлінеді.

Парольді аутентификация. Субъект идентификациясы кезінде парольді қолдану. Артықшылығы адам үшін қарапайымдылығы мен ыңғайлығы болып табылады. Кемшілігі әлсіз қорғанысты қамтамасыз етеді.

Парольді қорғау сенімділігін қамтамасыз ету бойынша шаралар:

1) Техникалық шектеулер қою (пароль ұзындығы, пароль әліпбиі).
2) Парольдің жұмыс істеу мерзімімен басқару, оларды периодты ауыстыру.
3) Парольдер файлына кіруді шектеу.
4) Жүйеге кірудің табыссыз әрекеттер санын шектеу.
5) Пайдаланушыларды оқыту.
6) Кілтті генерациялаудың программалық құралдарын қолдану.

Бір реттік парольдер. Парольді схема сенімділігін арттыру жолдарының бірі – бір реттік парольдерді қолдану (мысалы, S/Key жүйесі).

Аутентификация процесінде f біржақты функциясы қолданылады, берілген функция пайдаланушыға және аутентификация серверіне белгілі. K кілті берілген, ол тек пайдаланушыға белгілі. Бастапқы басқару сатысында f функциясы кілтке n рет қолданылады, нәтижесі серверге сақталады.

Аутентификация кезінде сервер пайдаланушылық жүйеге (n-1) санын жібереді. Пайдаланушы құпия санға (n-1) рет f функциясын қолданады және нәтижесін серверге жібереді. Сервер f функциясын пайдаланушыдан алған мәнге қолданады және алдында сақталған шамамен салыстырады. Сәйкес келген кезде түпнұсқалық орнатылды деп есептеледі, сервер жіберілген мәнді есіне сақтайды және санағышты бірлікке азайтады.

Биометриялық деректерді қолдану. Пайдаланушының идентификации/аутентификациясын орындау үшін биометриялық деректер қолданылады. Оларға мыналар жатады:

1) Саусақ таңбасы.
2) Көз торы мен қарашығы.
3) Қол мен бет геометриясы.
4) Дауыс және сөзді тану.
5) Пернетақтамен жұмыс және қол.

Кірумен басқару. Кірумен басқару субъекттің ақпараттық объектпен орындауға құқығы бар әрекеттерін бақылауға мүмкіндік береді.

Есептің дәстүрлі қойылымы S_i субъектілер жиынтығы мен O_j объектілер жиынының бар болуынан тұрады. Логикалық басқару міндеті әрбір (S_i,O_j) жұбы үшін мүмкін операциялар жиынын анықтау және орнатылған ретте орындалуын басқарудан тұрады.

«Субъекттер-объекттер» қатынасы матрица түрінде көрсетілуі мүмкін, оның жолдарында субъекттер, ал бағандарында кіру объектілері көрсетілген. Жолдар мен бағандар қиылысындағы ұяшықта кіру шарты мен құқығы беріледі.

Кіру құқығын бақылау программалық ортаның арнайы компонентімен – операциялық жүйе ядросы, қауіпсіздік сервисі, деректер базасымен басқару жүйесі, аралық қабаттың программалық модульдерімен жүргізіледі.

Қіруге рұқсат берген кезде келесі ақпаратты талдау жүргізіледі:

1) Субъект идентификаторы – дискрецонды (дербес) кіру.

2) Субъект атрибуты (қауіпсіздік меткасы, пайдаланушылар тобы) – мандатты (принудительный) кіру.

Дискрецонды (дербес) кіру кемшіліктері:

1) Кірумен басқару көптеген объектілермен басқаруды қажет етеді, бұл басқару функцияларын көптеген пайдаланушылар арасында бөлуді қажет етеді.

2) Кіру құқығы деректерден бөлек жүреді (ақпаратқа кіру құқығы бар зиянкес файлдарды жазуға және ақпаратты ауыстыруға мүмкіндік береді).

Рольдік басқару. Пайдаланушылар мен олардың кіру құқықтары арасында аралық қатынас – АЖ-де пайдаланушы ролі орнатылады.

Әрбір пайдаланушы үшін бірнеше рольдер белсенді болуы мүмкін, оның әрбіреуі пайдаланушыға белгілі бір құқық береді.

Роль оларды тексеру құқықтары мен тәсілдерінің нақты түрлеріне қатысты нейтралды, пайдаланушылармен басқаруға объектілі-бағытталған әдісті қалыптастырады.

Рольдік басқару мына түсініктермен анықталады:

1) Пайдаланушы.
2) Пайдаланушының жұмыс істеу сеансы.
3) Роль (ұйымдық құрылыммен анықталатын).
4) Объект (қатынас, оған кіру шектелмелі).
5) Операция (объектпен орындалатын).
6) Кіру құқығы.

Протоколдау және аудит. Протоколдау – АЖ оқиғалары туралы ақпаратты жинау мен толықтыру (сыртқы, ішкі, клиенттік).

Аудит – жедел немесе периодты жүргізілетін жинақталған ақпарат анализі.

Олар келесі есептерді шешуге мүмкіндік береді:

1) АЖ пайдаланушылары мен администраторларының ішкі есептерін қамтамасыз етеді.
2) Оқиға тізбегінің реконструкциясын қамтамасыз етеді.
3) Ақпараттық қауіпсіздіктің бұзылуы ретін табу.

4) Мәселені табу және талдау үшін ақпаратты көрсету.

Протоколдау кезінде келесі ақпаратты жазуға ұсыныс береді:

1) Оқиға күні мен уақыты.
2) Субъекттің әмбебап идентификаторы – оқиға инициаторы.
3) Оқиға нәтижесі.
4) Сұраныстың қайнар көзі.
5) Объектілер атауы.
6) Қорғаудың деректер базасына енгізілген өзгерістерін сипаттау.

Активті аудит міндеті күдікті белсенділігін табу және оған автоматты жауап беру құралдарымен басқару.

Қауіпсіздік саясатына қарама-қайшы келетін белсенділікті мыналарға бөледі:

1) Басқару құқығын заңсыз алуға бағытталған шабуылдар.

2) Басқару құқығы негізінде орындалатын әрекеттер, бірақ қауіпсіздік саясатын бұзатын (басқару құқығымен асыра сілтеу).

Активті аудит қателерін бірінші және екінші түрге бөледі. Бірінші түрдегі қателер – шабуылды жіберіп алу. Екінші түрдегі қателер – жалған жауаптар.

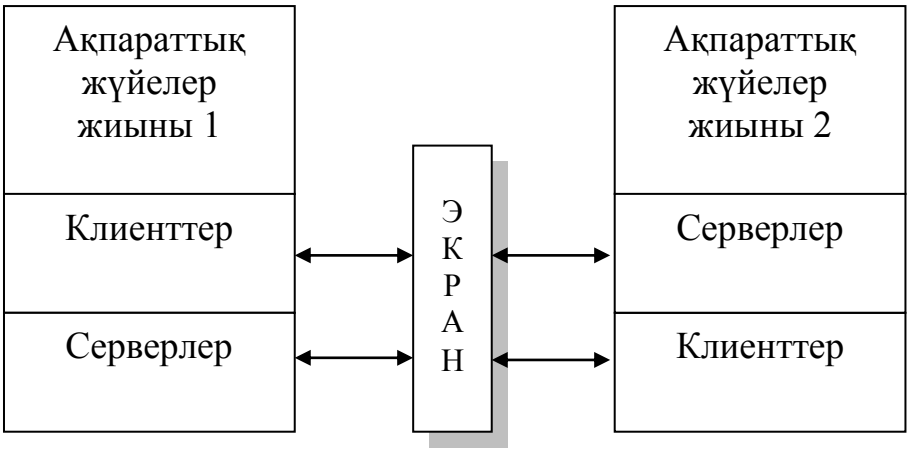
Активті аудит әдістері:

1) Сигнатурлы – шабуыл сигнатурасын анықтау негізінде – бірінші түрдегі қателер үлкен (белгісіз шабуылдарды таба алмауы).

2) Статистикалық – субъектілердің орындайтын әрекеттерін талдау негізінде – екінші түрдегі қателер үлкен.

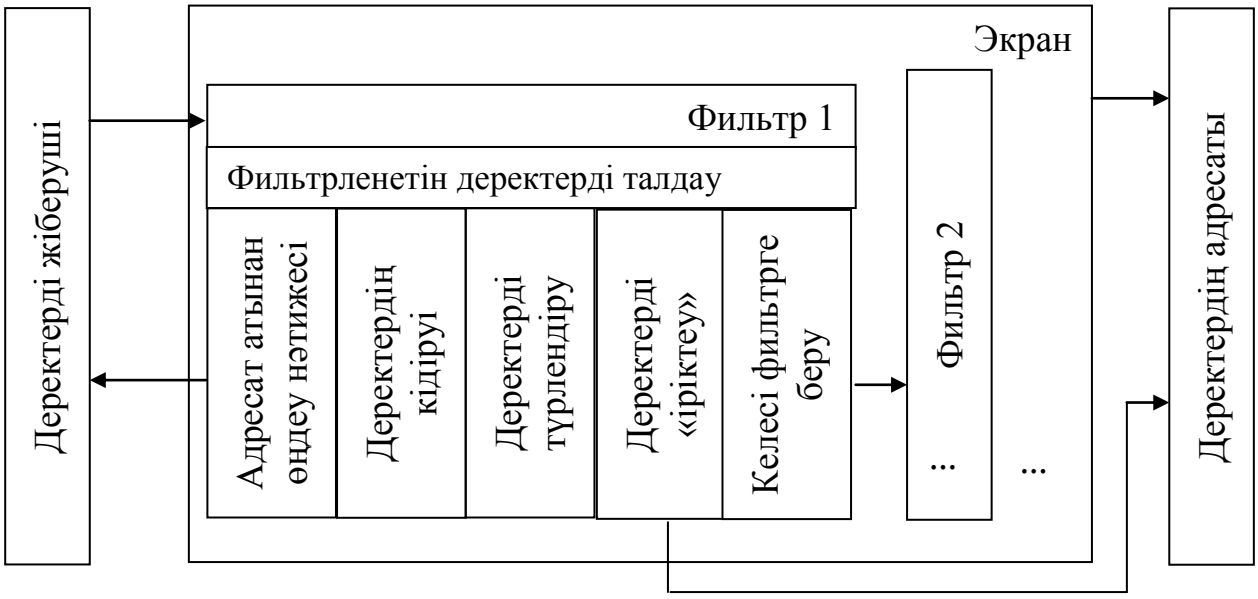
3.2 Экрандау, қорғаныс анализі

Экрандау есебінің формальді қойылымы келесідей. Ақпараттық жүйелердің екі жиыны берілсін делік. Экран – бұл серверге бір жиыннан екінші жиынына клиенттердің кіруін шектеу. Экран жүйенің екі жиыны арасында барлық ақпараттық ағынды басқара отырып, өз функцияларын жүзеге асырады (3.1 сурет). Ағынды бақылау оларды сүзгілеуден тұрады, кейбір түрлендірулер орындаумен болуы мүмкін.



3.1 сурет - Экран кіруді шектеу құралы ретінде

Детализацияның келесі деңгейінде экранды (жартылай өткізгіш мембрана) сүзгі тізбегі ретінде көрсету ыңғайлы. Деректерді талдаған соң сүзгінің әрбіреуі оларды ұстап қалуы (өткізбей) немесе экранға бірден «лақтыруы» мүмкін. Сондай-ақ, деректерді түрлендіруге рұқсат беріледі, адресат атынан деректерді талдау немесе өңдеуді жалғастыру үшін келесі сүзгіге деректер порциясын жіберу және жіберушіге нәтижені қайтару (3.2 сурет).



3.2 сурет - Экран сүзгі тізбегі ретінде

Кіруге құқықты шектеу функциясынан басқа экран ақпаратпен алмасуды протоколдауды жүзеге асырады. Көбінесе экран симметриялық болып табылмайды, оған «ішкі» және «сыртқы» деген түсініктер анықталған. Экрандау міндеті ішкі облысты потенциалды зиян сыртқы факторлардан қорғаныс ретінде қалыптастырылады. Желіаралық экрандар (ағылшын тілінен

аударғанда firewall термині) көбінесе Internet шығатын ұйымның корпоративті желісін қорғау үшін орнатылады.

Экрандау сыртқы белсенділікпен шақырылған жүктемені жоюды азайта отырып, ішкі облыстың сервистеріне кіру құқығын қолдайды. Қауіпсіздіктің ішкі сервистерінің осалдылығы азаяды, өйткені қаскүнем алдымен экранды еңсеруі керек, мұнда қорғаныс механизмдері аса мұқият конфигурацияланған.

Экрандау, сондай-ақ сыртқы ортаға бағытталған ақпараттық ағындарды бақылауға мүмкіндік береді, бұл ұйымның АЖ-де конфиденциалдылық режимін қолдауға көмектеседі. Экрандау қауіпсіздік сервисі ретінде тек желілік емес, сондай-ақ хабарламамен алмасу жүретін кез келген басқа ортада да қолданылуы мүмкін.

Мұндай ортаның маңызды мысалы – объектіге негізделген программалық жүйелер, объектілер әдісін белсендіру үшін хабарлама жіберу орындалған кезде (кем дегенде концептуалды жоспарда). Болашақ объектіге негізделген орталарда экрандау объектіге кіру құқығын шектеудің маңызды құралдарының бірі болуы ықтимал.

Экрандау ішінара болуы мүмкін, белгілі бір ақпараттық сервистерді қорғайтын.

Шектеуші интерфейс, сондай-ақ экрандау түрі ретінде қарастырылуы мүмкін. Көрінбейтін объектке шабуыл жасау қиын, әсіресе құралдардың тұрақты жиыны көмегімен. Бұл жағдайда Web-интерфейс табиғи қорғанысқа ие, әсіресе гипермәтіндік құжаттар динамикалық қалыптасқан жағдайда. Әрбір пайдаланушы оған көру керек нәрсені ғана көреді.

Web-сервистің экрандаушы ролі бұл сервис делдалдылық функцияларын басқа ресурстарға кіру кезінде жүзеге асырғанда ғана көрінеді, мысалы деректер базасының кестелеріне. Мұнда тек сұраныстар ағыны ғана бақыланбайды, сондай-ақ деректерді ұйымдастыру жасырылған.

Архитектурлы аспектілер.

Әмбебап операциялық жүйелер құралдарымен желілік ортаға тиесілі қауіптермен күресу мүмкін болып табылмайды. Әмбебап ОЖ – бұл анық қателерінен басқа кіру құқығын легальді алу үшін қолданылуы мүмкін кейбір ерекшеліктерінен тұратын үлкен программа. Программалаудың қазіргі технологиялары сондай үлкен программаларды қауіпсіз етіп істей алмайды.

Сондай-ақ күрделі жүйемен жұмыс істейтін администратор әрдайым жүргізілетін өзгерістердің барлығын есепке ала алмайды. Жалғыз перспективті жол арнайы қауіпсіздік сервистерін құрумен байланысты, олар өзінің қарапайымдылығымен формальді немесе формальді емес верификацияға рұқсат етеді. Желіаралық экран осындай құралдардың бірі болып табылады. Әртүрлі желілік хаттамаларға қызмет көрсетумен байланысты ары қарай декомпозицияны болдырады.

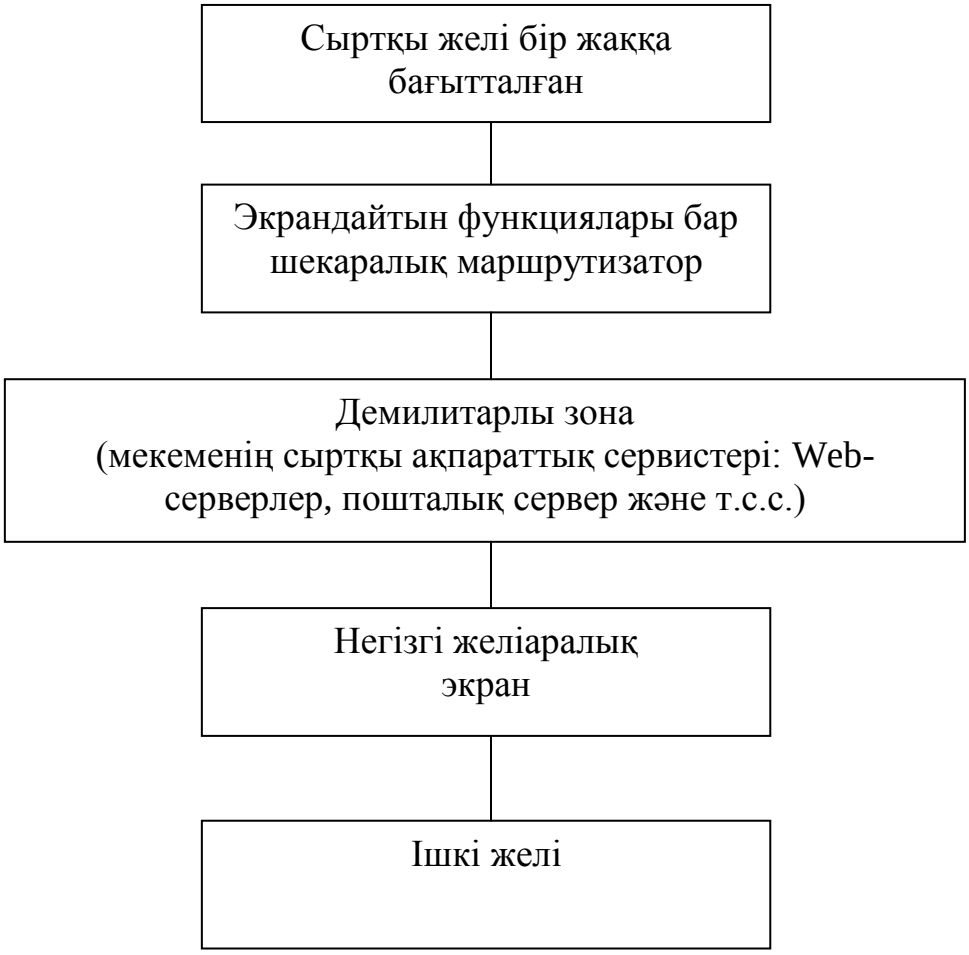
Желіаралық экран қорғалатын (ішкі) желі және сыртқы орта (сыртқы желілер немесе корпоративті желінің басқа сегменттер) арасында орналасады. Бірінші жағдайда сыртқы желіаралық экран туралы айтылады, екінші жағдайда – ішкі туралы. Сыртқы желіаралық экранды қорғаныстың бірінші

немесе соңғы линиясы деп есептеуге болады. Бірінші – егер әлемге сыртқы қаскүнем көзімен қарасақ. Соңғы – егер корпоративті желінің барлық компоненттерінің қорғалуына ұмтылғандағы жағдайды қарастырсақ. Желіаралық экран – активті аудит құралын орнату үшін арнайы орын. Бір жағынан, бірінші және соңғы қорғау белгісінде күдікті белсенділікті табу өзіндік маңызды.

Басқа жағынан алғанда, желіаралық экран күдікті белсенділікке өз бетінше мықты реакция қалыптастыруға қабілетті. Қауіпсіздіктің екі сервисін біріктіру өз кезегінде кемістік құруы мүмкін екендігін білуіміз керек. Желіаралық экранға корпоративті ресурстарға кіруге мұқтаж сыртқы пайдаланушылардың идентификация/аутентификацияны қоюы орынды (желіге бірыңғай кіру концепциясын қолдаумен).

Сыртқы қосылуларды қорғау үшін қорғаныстың эшелондау принципіне сәйкес көбінесе екікомпонентті экрандау қолданылады.

Алғашқы сүзгілеу (фильтрация) (мысалы, SNMP басқарушы хаттамасы пакеттерін немесе анықталған IP-адрестерімен пакеттерін блоктау) шекаралық маршрутизатормен жүзеге асырылады. Онда демилитарлы деп аталатын зона (қауіпсіздіктің қалыпты сенімімен желі, онда ұйымның сыртқы ақпараттық сервистері - Web, электронды пошта және т.с.с. шығарылады) және корпоративті желінің ішкі бөлігін қорғайтын негізгі желіаралық экран орналасқан.



3.3 сурет - Демилитарлы зонамен екі компонентті экрандау

Теориялық жағына алғанда желіаралық экран (әсіресе ішкі) көп хаттамалы болуы керек, бірақ тәжірибеде TCP/IP хаттамасының үстемділігі жоғары болғандықтан басқа хаттамаларды қолдау артық, қауіпсіздік үшін зиян болып табылады (сервис күрделі болғанда ол соншалықты осал).

Ішкі және сыртқы желіаралық экран тар орын болып қалуы мүмкін, өйткені желілік трафик көлемі тез өсу тенденциясына ие. Бұл мәселені шешудің бір жолы желіаралық экранды бірнеше аппараттық бөліктерге бөлу және арнайы сервер-делдалдарды ұйымдастыруды болжайды.

Негізгі желіаралық экран түр бойынша кіріс трафиктің жіктелуін және сәйкес делдардарға сүзгіні қайта сеніп тапсыруы мүмкін (мысалы, HTTP-трафикті талдайтын делдалға). Шығыс трафик алдымен сервер-делдалмен өңделеді, олар функционалды пайдалы әрекеттерді орындауы мүмкін, мысалы, сыртқы Web-сервердің беттерін кэштеу сияқты, бұл желіге және негізгі желіаралық экранға жүктемені төмендетеді.

Желіаралық экрандардың жіктелуі.

Желілік технологияға қатысты кез келген сұрақты қарастыру кезінде ISO/OSI жеті деңгейлі эталонды модель негіз болып келеді. Желіаралық экранды сүзгілеу деңгейіне қарай жіктеуге болады – каналды, желілік, транспорттық немесе қолданбалы. Демек, экрандайтын концентраторлар (мост, коммутатор) (2 деңгей), маршрутизаторлар (3 деңгей), транспорттық экрандау (4 деңгей) және қолданбалы экран (7 деңгей) туралы айтуымызға болады. Ақпаратты бірнеше деңгейлерде талдайтын кешенді экран бар.

Ақпараттық ағындарды сүзгілеу ұйымның қауіпсіздік саясатының желілік аспектілерінің мәні болып табылатын ережелер жиыны негізінде желіаралық экрандармен жүзеге асырылады. Мұндай ережелерде, сүзгіленетін ағындарда бар ақпараттан басқа, айналадан алынған деректер бар болуы мүмкін, мысалы, ағымды уақыт, белсенді қосылу саны, желілік сұраныс келіп түскен порт және т.с.с. Демек, желіаралық экрандарда кіруге шектеу қоюға мықты логикалық тәсіл қолданылады.

Қорғалу анализі.

Қорғалу анализі сервисі осал орындарды оларды оперативті ликвидациялау мақсатымен табуға арналған. Өздігінен бұл сервис ештеңеден қорғамайды, бірақ қаскүнемнен бұрын қорғауда пробелдерді табуға (немесе жою) көмектеседі. Алдымен, архитектуралық емес (оларды ликвидациялау қиын), ал «оперативті» кемістіктер алынады, басқару қатесі нәтижесінде немесе программалық қамтама версиясының жаңаруына көңіл аудармаудан туындаған.

Қорғалу анализі жүйесі (қорғалу сканерлері деп те аталатын) білімді жинау және қолдануға негізделген. Берілген жағдайда қорғауда пробелдер туралы білім алынады: оларды қалай іздеу туралы, олар қаншалықты күрделі және оларды қалай жою туралы.

Бақылау сұрақтары.

1. Ақпараттық қауіпсіздіктің программалық-техникалық деңгейінің негізгі түсініктеріне сипаттама беріңіз.
2. Ақпараттық қауіпсіздікті қамтамасыз етудің программалық-техникалық шараларын атаңыз.
3. Протоколдау және аудит дегеніміз не?
4. Кірумен басқару дегеніміз не?
5. Экрандау, қорғаныс анализі дегеніміз не?
6. Желіаралық экрандардың жіктелуі.
7. Қорғалу анализі дегеніміз не?

Қорытынды

Ақпараттық қауіпсіздікті қамтамасыз ету мәселесі қазақстандық нарықта өте актуалды болып отыр. Бұл сыртқы нарықта бәсекелестікпен күресу және компаниялардың халықаралық деңгейге шығуымен байланысты. Олардың көбі өз күштерімен коммерциялық ақпаратты қорғауды қамтамасыз ете алмайды және кәсіби IT-кеңесшілердің қызметтеріне жүгінуі керек.

Ақпараттық қауіпсіздікті қамтамасыз ету қазақстандық ғана емес, әлемдік мәселе болып табылады. Корпоративті жергілікті желіні ендірудің бірінші жылында компаниялардың басты ауруы сыртқы кірулер (хакерлік шабуылдар) жолымен коммерциялық ақпаратқа рұқсатсыз кіру болды. Қазір ақпараттық қауіпсіздік көзқарасымен қарасақ, көптеген компаниялар мықты қабырғалардың бірнеше перимерлерімен – ақпараттық қауіпсіздіктің бағдарламалық және аппараттық платформаларымен оқшауланған зәулім қорған еске түсіреді. Бірақ тәжірибеде ақпарат бәрібір ағып кетеді екендігін көрсетеді. Сондай-ақ ақпараттық ағып кетугенегізгі тұжырымдама компанияларда ақпараттық қауіпсіздікті қамтамасыз етуге бірыңғай жүйелік көзқарастың жоқтығы болып табылады.

Көптеген жылдар бойы компаниялар вирустық эпидемиялармен күресті, периметрлерін және кірудің алдын алу жүйелерін желі аралық экрандармен қоршады, рұқсатсыз кіруге қарсы мықты құралдарды ендірді. Бірақ компаниялар басты қауіпті тыс қалдырды. Ақпараттық қауіпсіздіктің бірыңғай саясатының жоқтығы, сондай-ақ компанияның ақпараттық қорғанысының профилін тұрғызудың бірыңғай концепциясы ақпараттық қауіпсіздіктің бағдарламалық және аппараттық кешендеріне миллиондаған шығындарды жұмсайды. Бірнеше жыл бұрын IT-қызметтер сыртқы қауіптерден қорғауға жауап берді, ал ішкі қауіптермен қауіпсіздік қызметтері айналысты. Қазір ол ақпараттың электронды желі бойынша және тасымалдауыштар көмегімен жүруін физикалық түрде бақылай алмайды. Ол үшін арнайы құрастырылған уақыт тәртібі, арнайы дайындалған қауіпсіздік қызметкерлері және рұқсатсыз кіру әрекеттерін айқындау үшін техникалық құралдар қажет. Барлық шаралар бірыңғай концепция негізінде ақпараттық қауіпсіздік мамандарымен жүзеге асырылуы керек. IT технология мен ақпараттық қауіпсіздік бағытының қарқынды дамуы берілген облыста кәсіби мамандарға сұраныстың өсуіне әкеледі. Бұл ақпараттық қауіпсіздік облысында білім алуды және еңбек нарығында кәсіби білім алуға кең талап етуді белсендіреді.

Бұл оқу құралы IT сферасында болашақ мамандарға беделді компанияларда өте қажет және жоғары төлемақысы бар қызметкерлер болу үшін ақпараттық қауіпсіздік облысында білімнің жалпы жинағын және икемділігін алуға көмектеседі деп үміттенемін.

Әдебиеттер тізімі

Негізгі

1. Шеннон К. Теория связи в секретных системах /Сб.: «Работы по теории информации и кибернетике».- М.: Иностранная литература, 1963.- С. 333-402.
2. Белов Е.Б., Лось В.П., Мещеряков Р.В., Шелупанов А.А. Основы информационной безопасности. – М.: Горячая линия – Телеком, 2006.- 544 с.
3. Галатенко В.А., Основы информационной безопасности. – М.: ИНТУИТ.РУ «Интернет-Университет Информационных Технологий», 2003. – 280 с.
4. Аяжанов Қ.С.Ақпараттық қауіпсіздік және ақпаратты қорғау. -А.: «Дәуір», 2011
5. Шаньгин В.Ф. Защита компьютерной информации. Эффективные методы и средства. – М.: ДМК Пресс, 2008. – 544 с.
6. Корт С.С. Теоретические основы защиты информации: Учебное пособие. – М.: Гелиос АРВ, 2004. – 240 с.
7. Тұрым А.Ш., Мұстафина Б.М., Ақпарат қорғау және қауіпсіздендіру негіздері. – Алматы: Алматы энергетика және байланыс институты, 2002ж.
8. Алферов А.П., Зубов А.Ю., Кузьмин А.С., Черемушкин А.В. Основы криптографии: Учебное пособие. – М.: Гелиос АРВ, 2002. – 480 с.
9. Ященко В.В. Введение в криптографию. Новые математические дисциплины. –М.: МЦНМО Питер, 2001.
10. Глушков С.В., Бабенко М.И., Тесленко Н.С. Секреты хакера: защита и атака. – М.: АСТ: АСТ МОСКВА: ХРАНИТЕЛЬ, 2008. -544 с. (Учебный курс).
11. Герасименко В. А. Защита информации в автоматизированных системах обработки данных. Книга 1,2 М.; Энергоатомиздат, 1994 .-176 с.
12. Касперский К. Фундаментальные основы хакерства (искусство дизассемблирования). –М.: Солон-Р, 2002.
13. Венбо Мао. Современная криптография: теория и практика. – М.: Издательский дом “Вильямс”, 2005.- 768 с.
14. Молдовян Н.А. Практикум по криптосистемам с открытым ключом. – СПб.: БХВ-Петербург, 2007. – 304 с.