Лекция 9 АШЫҚ КІЛТІ БАР КРИПТОГРАФИЯҒА КІРІСПЕ

1 Ашық кілті бар шифрлау әдістерінің жасау алғышарттары және негізгі анықтамалар

Жабық кілті бар шифрлауды пайдалану кезінде екі салмақты проблема пайда болады. Бірінші проблема – құпиялы кілттерді жасау және оларды ақпараттық алмасуға қатысатын абоненттерге жеткізу. Жалпы арнаулы байланыс арна (мысалы, әдеттегі пошта немесе электронды пошта) арқылы жіберген кезде осындай кілттің жеткізу қауіпсіздігіне және оның дұрыстығына кепілдік беру өте қиын. Екінші проблема – электронды қатынаста серіктестердің дәл өзіндігін (дұрыстығын) қамтамасыз ету. Корреспонденцияны алушыда құжаттың дұрыстығын растауына мүмкіндігі болу керек, ал электронды хабарды жасаушыда өз авторлығын дәлдеуге мүмкіндігі болу керек. Сондықтан, электронды құжаттарда әдеттегі қол қоюдың аналогы болу керек.

Осы проблемаларды шешуге мүмкіндік берді **ассиметриялық криптоалгоритмдер**. Оларда тура және кері криптотүрлендірудің процедуралары әртүрлі кілттерде орындалады және олардың арасында оңай табылатын байланыстар жоқ болады. Ассиметриялық криптоалгоритмдер көбінесе математикалық функциялардың қасиеттеріне негізделген, ал симметриялық шифрлаудың алгоритмдері көбінесе орын ауыстыру мен орнына қою операцияларды пайдаланады. Осындай зерттеуге үлкен үлес қосты американ ғалымдары қосты У.Диффи (W.Diffie), Э.Хеллман (M.Hellman), Р.Меркль (R.Merkle). Олар бірнші екі есепті шешуге жаңа ұсыныстар берді.

Ассиметриялық шифрлау алгоритмдер тағы да **ашық кілті бар алгоритмдер** деп аталады. Бірдей кілт пайдаланатын симетриялық шифрлау алгоритмге (жабық кілті бар шифрлау алгоритмы) қарағанда ассиметриялық шифрлау алгоритмде бір кілт шифрлау үшін, ал одан өзгеше басқасы – ашып оқу үшін пайдаланады. Алгоритм ассиметриялық деп аталады, өйткені шифрлау және дешифрлау кілттері әртүрлі, сондықтан негізгі криптографиялық процестін симметриясы жоқ. Екі кілттің біреуі **ашық** (public key) болып табылады және бәріне жариялану мүмкін, ал екіншісі – **жабық** (private key) және құпиялы түрде сақталынады. Кілттердің қайсысы, ашық немесе жабық, шифрлау үшін, ал қайсысы дешифрлау үшін пайдаланатыны криптографиялық жүйенің міндетімен анықталады.

Қазіргі уақытта ассиметриялық алгоритмдер тәжірибеде кең қолданылады, мысалы, телекоммуникациялық желілердің ақпараттық қауіпсіздігін қамтамасыз ету үшін; Internet ғаламдық желінің ақпараттық қауіпсіздігін қамтамасыз ету үшін; әртүрлі банктік және төлем жүйелердің қауіпсіздігін қамтамасыз ету үшін.

Ашық кілті бар шифрлау алгоритмды ең азы үш есепті шешу үшін пайдалануға болады:

1. Рұқсатсыз қатынаудан деректерді қорғау үшін берілетің және сақталатын деректерді шифрлау үшін.
2. Электронды құжаттарға цифрлық қол қоюды жасау үшін.
3. Құпиялы кілттерді үлестіру үшін, сосын оларды құжаттарды симметриялық әдістермен шифрлауда пайдаланады.

9.2 Бір жақты функциялар

Барлық ашық кілті бар шифрлау алгоритмдер бір жақты деп аталатын функциялардың пайдалануына негізделген. Бір жақты функциялар (one-way function) деп оңай есептейтің, бірақ функция мәні бойынша сәйкес аргумент мәнің қиын табатын математикалық функцияны атайды. Яғни, берілген x мәнінде $f(x)$ мәнің есептеуге қиын емес, бірақ $y=f(x)$ болғанда, x мәнің есептеуге оңай жол табылмайды. «Оңай жол табылмайды» дегеніміз ЭЕМ-ды пайдалана отырып көз жетерлік уқытта кері мәнің есептеудің мүмкін еместігі. Бір жақты функциялар криптографияда хеш-функция ретінде де қолданылады. Хабарды шифрлау үшін бір жақты функцияларды пайдалану мағынасыз, себебі шифрланған хабарды қайта ашуға келмейді. Шифрлау үшін арнайы бір жақты функциялар пайдаланады – люкы (немесе құпиясы) бар бір жақты функциялар. Бұл бір жақты функциялардың ерекше түрі, олардың кейбір құпиясы (люк) функцияның кері мәнің тез есептеуге мүмкіндік береді.

Люкы бар бір жақты f функция үшін келесі бекітулер орын алады:

1. x біліп $f(x)$–ты есептеуге оңай;
2. $f(x)$–ты біле отырып x–ты табу қиын;
3. кейбір құпиялы ақпаратты қосымша біле отырып x–ты есептеуге оңай.

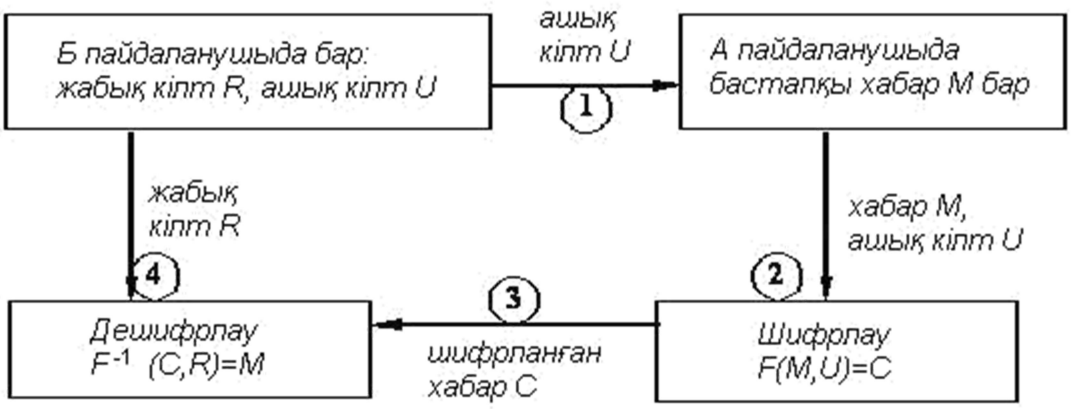
9.3 Ассиметриялық алгоритмдерді шифрлау үшін пайдалану

XX ғасырдың 70-ші жылдары Диффи мен Хеллман екі кілтті пайдалануға негізделген шифрлау принципті ұсынды. Бұл кілттер өзара байланыста болса да, біреуінен (ашықтан) басқаны (жабықты) есептеу мүмкін емес. Бұл принципті пайдаланушыларды шифрлау/дешифрлау кілттерімен қамтамасыз ету проблеманы шешу үшін пайдалануға болады, дәл айтқанда – бұл проблеманы жою үшін. Диффи мен Хеллман айтқандай, алдын ала үлестірілген кілттер деректерді шифрлау үшін пайдаланбау керек (өйткені бір адамға белгілі құпия – бұл енді құпия емес). Жабық кілт тек бір адамға ғана белгілі болу керек – оның иесіне. Ассиметриялық алгоритмның осындай пайдалану принципі ***ашық шифрлау*** немесе ***ашық кілті бар шифрлау*** деп аталады.

Осы принципке сәйкес кез келген адам хабарды ашық кілтпен шифрлау мүмкін. Хабарды ашып оқуға тек жабық кілттің иесі ғана істей алады. Мысалы, пайдаланушылар *А* мен *Б* ашық шифрлау схемасын пайдалансын. Пайдаланушы *А* құпиялы хабарды тек пайдаланушы *Б*-ға жібергісі келсін. Ол үшін келесі істерді орындау қажет:

1. Пайдаланушы *Б* пайдаланушы *А*-ға өзінің ашық кілтің U кез келген байланыс арна арқылы жібереді, мысалы электронды пошта бойынша.
2. Пайдаланушы *А* өзінің хабарын M алынған ашық U кілтімен шифрлап шифрланған C хабарды алады.
3. Шифрланған хабар C пайдаланушы *Б*-ға жіберіледі.
4. Пайдаланушы *Б* алынған хабарды C өзінің жабық кілтімен R ашып оқиды.

Егер шифрлау операцияны F деп белгілесек, ал дешифрлау операцияны F^{-1}, онда пайдаланушылар арасындағы ақпаратпен алмасу протоколының схемасын 9.1 суреттегідей көрсетуге болады.



Сурет 9.1. Ашық шифрлаудың схемасы

Ашық шифрлауды пайдалану кілттерді үлестіру проблемасын шешеді. Бұрын шифрланған деректермен алмасудың алдында пайдаланушылар қандай да болса түрімен жабық байланыс арна арқылы пайдаланатын құпиялы кілтті жеткізу керек болатын. Ол үшін бір бірімен кездесетін немесе курьерді жіберетін. Егер пайдаланушының біреуі кілтті өзгертетің болса, онда жаңа кілтті қайтадан өзінің абонентіне жеткізу керек болатын. Ашық кілті бар криптографияда бәрі оңай. Байланыс жүйесінің пайдаланушылары ашық кілттермен және олармен шифрланған хабарлармен еркін айырбаса алады. Егер пайдаланушы өз құпиялы кілтің сенімді сақтаса, онда берілетін хабарларды ешкім оқи алмайды.

Хабарларды беру желіде алмасу процедурасын оңайлату үшін әдетте деректер базасы пайдаланады, оның ішінде барлық пайдаланушылардың ашық кілттері сақталынады. Керек кезінде жүйенің пайдаланушысы базадан басқа адамның ашық кілтің сұрап алып оны хабарды шифрлау үшін пайдаланады.

9.4 Ашық кілті бар алгоритмның негізінде цифрлық қол қою

Кейбір адамдар бөтен хабарларды өзгерту мүмкін, өз авторлығынан бас тарту мүмкін немесе басқа адам деп өзін-өзі атау мүмкін. Бұл өте актуалды электронды коммерцияның дамуымен және Интернет арқылы қызметтік төлем жасауда. Сондықтан, корреспонденцияны алушыда құжаттың дұрыстығын растауына мүмкіндігі болу керек, ал электронды хабарды жасаушыда өз авторлығын дәлдеуге мүмкіндігі болу керек. Сондықтан, электронды құжаттарда әдеттегі физикалық қол қоюдың аналогы болу керек. Бұл кезде қол қоюдың келесі қасиеттері болу керек:

1. қолды тек бір адам ғана қоялады, ал дұрыстығын көбі тексеру мүмкін;
2. қол қою берілген хабармен үздіксіз байланыста болу керек және басқа құжатқа көшірілмейді;
3. құжатқа қол қойғаннан кейін, оны өзгертуге болмайды;
4. қойылған қолдан бас тарту мүмкін емес, яғни құжатқа қол қойған адам кейін мен қоймадым деп айталмайды.

Ассиметриялық шифрлау алгоритмдер цифрлық (электронды) қол қоюды құрастыру үшін пайдалану мүмкін. **Цифрлық (электронды) қол қою** (digital signature) – бұл берілетің ақпараттың авторлығын тексеруге мүмкіндік беретің оның бірегей сандық қосымшасы. Электронды (цифрлық) қол қою (ЭЦҚ) тіркелген ұзындығы бар биттер тізбегі болып табылады, ол белгілі бір түрде ақпараттың ішіндегісі мен құпиялы кілт көмегімен есептеледі.

Цифрлық қол қоюды құрастыру барысында арнайы түрімен барлық хабар толық шифрланады немесе хабардан хеш-функциясының есептеу нәтижесі. Көбінесе соңғы әдіс

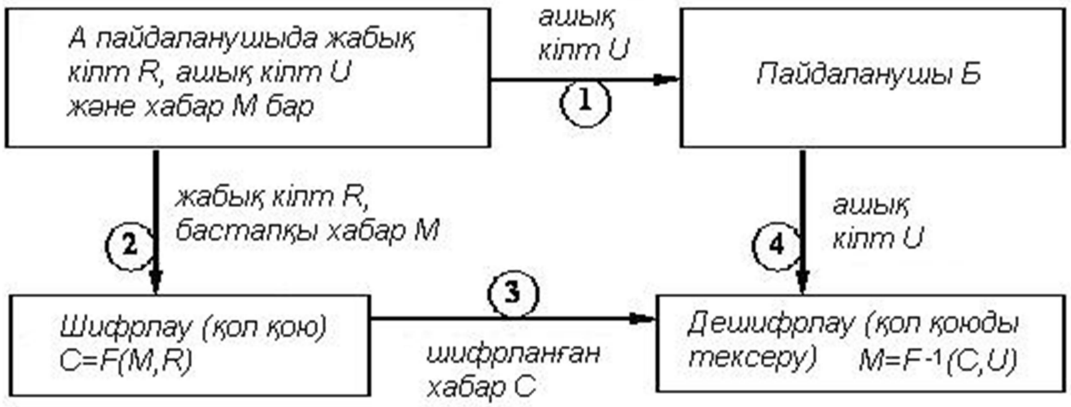
пайдалынады, себебі хабардың мөлшері әртүрлі болу мүмкін, кейде өте үлкен, ал хеш-кодының ұзындығы тұрақты және аса үлкен емес. Екі вариантын да қарап шығайық.

Ең қарапайым әдіс өзара байланысқан екі кілтті (ашық және жабық) пайдалану. Бірақ жабық пен ашық кілттің рольдері ауысады – қол қою кілті құпиялы болады, ал тексеру кілті – ашық. Егер ашық кілті бойынша жабық кілтті табалмау қасиеті сақталатын болса, онда қол ретінде құпиялы кілтпен шифрланған хабардың өзі болу мүмкін. Сонымен, хабарға қол қояды тек жабық кілттің иесі, ал ашық кілті бар әрбіреулер қол қоюды тексере алады.

Мысалы, пайдаланушы *А* пайдаланушы *Б*-ға қол қойылған хабар жібергісі келеді. Қол қоюды жасау және тексеру процедурасы келесі қадамнан тұрады:

1. Пайдаланушы *А* пайдаланушы *Б*-ға өзінің ашық кілтің *U* кез келген байланыс арна арқылы жібереді, мысалы электронды поштамен.
2. Пайдаланушы *А* хабарды *M* өзінің жабық *R* кілтімен шифрлап шифрланған *С* хабарды алады.
3. Шифрланған хабар *С* пайдаланушы *Б*-ға жіберіледі.
4. Пайдаланушы *Б* пайдаланушы *А*-ның ашық кілтің пайдаланып алынған хабарды С ашып оқиды. Егер хабар ашылса, онда оған пайдаланушы *А* қол қойды.

Бұл протоколды схема түрінде көрсетуге болады (сур. 9.2).



Сурет 9.2. Цифрлық қол қоюды жасау және тексеру схеманың бірінші варианты

Пайдаланушы *А* өз жабық кілтің сенімді сақтап отырғанша, оның қол қоюы дұрыс болады. Одан басқа, абонент *А*-ның жабық кілтіне рұқсат алмай, хабарады өзгерту мүмкін емес; осымен аутентификация және деректер бүтіндігі қамтамасыз етіледі.

Қос кілттің физикалық ұсынуы ЭЦҚ пайдаланатың нақты жүйеге тәуелді. Көбінесе кілт файлға жазылады, онда кілттен басқа пайдаланушы – кілт иесі туралы ақпарат, кілттің қызмет ету мерзімі, және нақты жүйенің жұмысына қажетті деректер жиынтығы болу мүмкін. Кілт иесі туралы деректер авторлықты анықтауға мүмкіндік береді, себебі қолды тексеру кезінде анық шығады - кім хабарға қол қойды. Әдетте ЭЦҚ тексергенде нәтижесі ыңғайлы түрде қол қойған пайдаланушыны көрсетіп экранға шығады, мысалы былай:

```
"Подпись файла приказ.doc верна (Автор: Соколов А.И.)"
```

9.2 суретте көрестілген схема – бұл **құжатты қалпына келтіруімен цифрлық қол қою** схемасы. Құжатты қалпына келтіруімен цифрлық қолдың құрамына құжаттың өзі де кіреді: қолды тексеру барысында автоматты түрде құжат денесі де есептеледі. Егер ашып оқыған кезде хабар дұрыс қалпына келсе, онда қойылған қол да дұрыс деп саналады. Құжатты қалпына келтіруімен цифрлық қол қою, мысалы RSA алгоритмы көмегімен жүзеге асырылу мүмкін.

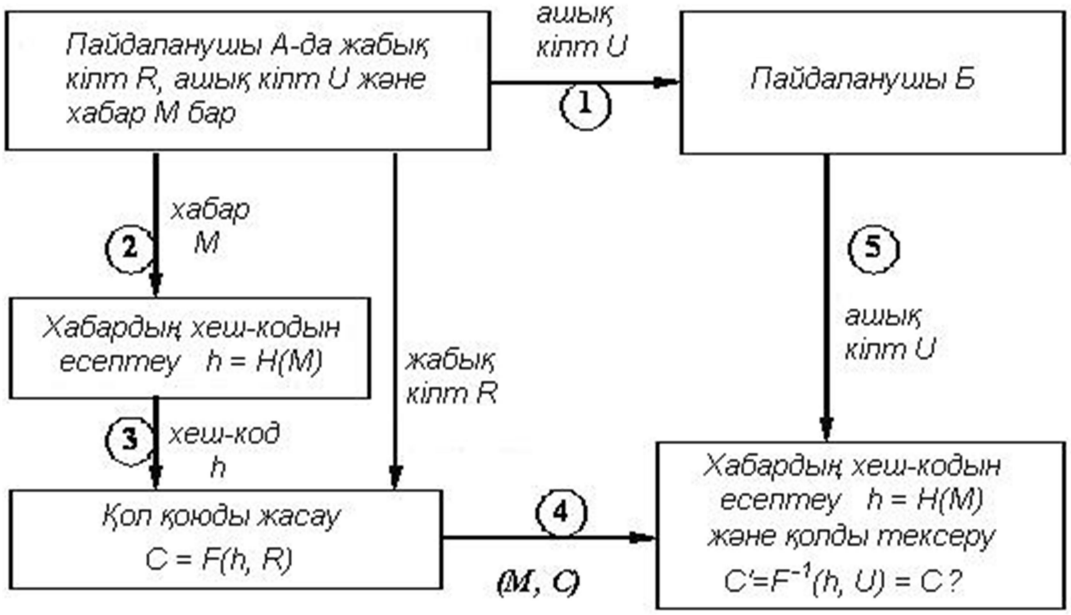
Құжатты қалпына келтіруімен цифрлық қол қоюды пайдаланғанда барлық хабарға қол қойылады, яғни ол шифрланады. Бірақ, қазір тәжірибеде олай істемейді. Ашық кілті бар шифрлау алгоритмдер баяу, одан әрі хабардың бүтіндігін растау үшін көп жад көлемі қажет болады. Және де ЭЦҚ есептейтің алгоритмдердің барлығы есеп үшін алдын ала стандартты ұзындығы берілген хабарларды пайдаланады. Мысалы, ресей ГОСТ Р34.10-94 алгоритмда бұл мөлшері 32 байтқа тең. Сондықтан, уақытты және есептеу ресурстарды үнемдеу үшін, ассиметриялық алгоритм әдетте бір бағытталған хеш-функциямен бірге пайдаланады. Мұнда басында хеш-функция көмегімен кез келген ұзындығы бар хабардан керекті мөлшері бар хеш-код есептеледі, сосын ЭЦҚ есептеу үшін алдында алынған хеш-код шифрланады.

Құжаттын хеш-коды бойынша есептелген ЭЦҚ **қосылатын цифрлық қол қоюлар** деп аталады. Осындай цифрлық қолдар кейбір сандық коды болып табылады және оны қол қойылатын құжатқа тіркеу қажет. Хабардың өзі бұл жағдайда шифрланбайды және ашық түрде цифрлық қолмен бірге жіберіледі.

Егер пайдаланушы *А* пайдаланушы *Б*-ға қосылған цифрлық қолмен толықтырылған хабар *M* жібергісі келсе, онда қол қоюды жасау және тексеру процедурасы келесі қадамнан тұрады:

1. Пайдаланушы *А* пайдаланушы *Б*-ға өзінің ашық кілтің *U* кез келген байланыс арна арқылы жібереді, мысалы электронды поштамен.
2. Пайдаланушы *А* сенімді хеш-функциясы *H* көмегімен өз хабарының хеш-кодын $h = H(M)$ есептейді.
3. Сосын пайдаланушы *А* хабардың хеш-кодын *h* өзінің жабық *R* кілтімен шифрлайды және цифрлық қолды *C* алады.
4. Бастапқы хабар *M* цифрлық қолмен *C* бірге пайдаланушы *Б*-ға жіберіледі.
5. Пайдаланушы *Б* алынған хабардың *M* хеш-кодын *h* есептейді, сосын пайдаланушы *А*-ның ашық кілтің пайдаланып цифрлық қолды *C* тексереді.

Бұл протоколды схема түрінде көрсетуге болады (сур. 9.3).



Сурет 9.3. Цифрлық қол қоюды жасау және тексеру схеманың екінші варианты

Хеш-функция ЭЦҚ-ң алгоритмнын құрамына кірмейді, сондықтан схемада кез келген сенімді хеш-функция пайдалану мүмкін.

Суреттелген қол қоюды жасау процесі конфиденциалдықты қамтамасыз етпейді. Яғни осы тәсілмен жіберілген хабарды өзгертуге болмайды, бірақ жіберушінің ашық кілтің пайдаланып оқуға болады.

Көп жағдайда келтірілген цифрлық қолды жасау және пайдалану схемасы әбден жеткілікті. Бірақ пайдаланушы *Б* алаяқтық жасау жағдайлары да болады. Мысалы, жіберілген құжат *А* пайдаланушының чегі болсын (қызмет еткен үшін). Пайдаланушы *Б* цифрлық қолдың дұрыстығын анықтап оны ақша алу үшін пайдаланды. Бірақ, пайдаланушы *Б* қол қойылған құжаттан бір не бірнеше көшірме жасап алып, анда-санда банкіге барып ақша алу мүмкін.

Осындай алаяқтықты болдырмау үшін цифрлық қолдарға жиі қосады уақыт белгісін. Құжатқа қол қойлған дата мен уақытты хабарға қосып құжатпен бірге қол қояды. Чек арқылы төлем жасағанда уақыт белгісін банк байқап деректер қорына енгізу мүмкін. Енді чекты қайтадан пайдаланатын болса, бұл көрініп қалады.

Цифрлық қол қоюдын өзге түрі *мойындамайтың* цифрлық қол. ЭЦҚ-дан оның айырмашылығы – қол қойған адам рұқсат бермесе қолды тексеруге болмайды. Сонымен, құжатты алушы хабарға қол қойған адамның рұқсатын алмай қол қоюды көрсете алмайды (немесе қолдың дұрыстығын дәлелдей алмайды).

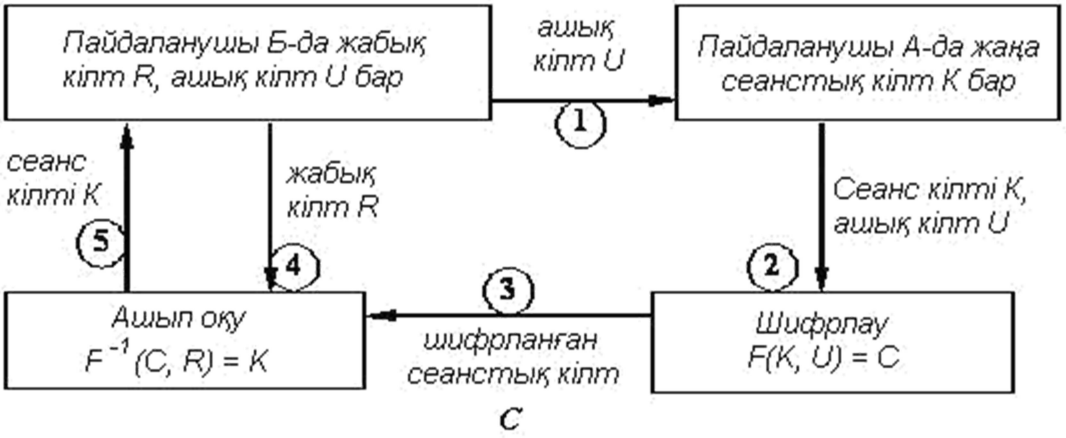
9.5 Ассиметриялық алгоритмдерді пайдаланып құпиялы кілтті құрастыру

Тәжірибеде ашық кілті бар алгоритмдер хабарларды тікелей шифрлау үшін сирек пайдаланады. Бұған әсер етеді үлкен дерекетер көлемін шифрлау мен дешифрлау кезінде ассиметриялық алгоритмдердің аса үлкен емес жылдамдығы. Өйткені, ашық кілті бар жүйелерде негізгі операция 500-1000 битты сандарды үлкен модулі бойынша дәрежеге көтеру. Бірақ, қысқа деректер блогын өңдегенде, мысалы белгілі ұзындығы бар кілттер, бұл алгоритмдер жеткілікті тиімді болу мүмкін. Сондықтан, келесі құрамды схеманы жиі пайдаланады: ассиметриялық алгоритм сессияның кілтің келісілу үшін қолданылады, ал сосын бұл кілт хабарларды симетриялық алгоритмымен шифрлау үшін құпиялы кілт ретінде шығады.

Сессияның құпиялы кілтті құрастырудың қарапайым протоколы келесі түрде болу мүмкін (егер кейбір байланыс жүйенің пайдаланушылары кілттерді үлестіру орталығындағы ашық кілттер деректер базасына рұқсат алып отырса, олар одан бір бірінің ашық кілттерің алып отырар еді):

1. Пайдаланушы *А* пайдаланушы *Б*-ның ашық кілтің кілттерді үлестіру орталығынан алады немесе тура пайдаланушы *Б*-ның өзінен.
2. Пайдаланушы *А* кездейсоқ сеанстық кілтті генерациялайды және алынған ашық кілтпен оны шифрлайды.
3. Шифрланған сеанстық кілт пайдаланушы *Б*-ға жіберіледі.
4. Пайдаланушы *Б* алынған пакетті өзінің жабық кілтімен ашып оқиды.
5. Пайдаланушылар *А* және *Б* келісілген сеанстық кілтті шифрланған хабарлармен алмасу үшін пайдаланады.

А және *Б* қос пайдаланушылардың шифрлау – дешифрлау үшін ортақ құпиялы кілтті *К* құрастыру схемасын келесі түрде көрсетуге болады (сур. 9.4).



Сурет 9.4. Ортақ құпиялы кілтті құрастыру схемасы

Бұл схема 9.1 суреттегі схемаға ұқсайды, өйткені онда да ашық кілтпен шифрлау тәртібі пайдаланады. Айырмашылығы тек нені шифрлауда. 9.4 суреттегі схемада аса үлкен емес сеанстық кілт шифрланады, ол әрі қарай симметриялық шифрлауда құпиялы кілт ретінде пайдаланады. Үлкен емес деректер блоктың шифрлауы жеткілікті тез орындалады және мындаған пайдаланушылары бар жүйедегі телекоммуникациялық процестерді тежелемейді.

9.6 Ашық кілті бар шифрлау алгоритмге қойылатын талаптар

Ашық кілті бар шифрлау алгоритмның негізгі қолданылу тәсілдерін қарастырып, Диффи мен Хеллманның пікір бойынша ашық кілті бар шифрлау алгоритмы қанағаттандырылатын талаптарды зерттейік. Бұл талаптар келесі:

1. Есептеу жағынан оңай қостарды (ашық кілт, жабық кілт) жасау.
2. Есептеу жағынан оңай ашық кілтпен хабарды шифрлау.
3. Жабық кілтті пайдаланып есептеу жағынан хабарды оңай дешифрлау.
4. Ашық кілтті біліп сәйкес жабық кілтті есептеу жағынан анықтау мүмкін емес.
5. Ашық кілтті және шифрланған хабарды ғана біле тұрып бастапқы хабарды есептеу жағынан қалпына келтіру мүмкін емес.

Осы жалпы талаптардан көрініп тұр, ашық кілті бар нақты алгоритмды жүзеге асыруы сәйкес бір жақты функцияға тәуелді.

Біз қарастырамыз ашық кілті бар төрт алгоритмды, олардың үшеуі тәжірибеде бұрынғыдан қолданылады, ал төртіншісі ақпаратты қорғау жүйелерде жақында ғана пайдалана басталды. Бұл алгоритмдер әдетте түрлі мақсаттар үшін пайдаланады (9.1 кестені қараңыз).

Кесте 9.1. Ашық кілті бар алгоритмдер

Алгоритмның аты	**Пайдалану мүмкіндігі**		
	Деректерді шифрлау / дешифрлау	Цифрлық қол қою	Кілтті келісу немесе құрастыру
RSA	Иә	Иә	Иә
Диффи-Хеллман алгоритмы	Жоқ	Жоқ	Иә
Эль-Гамаль алгоритмы	Иә	Иә	Иә
Эллиптикалық қисықтарды пайдаланатын алгоритмдер	Иә	Иә	Иә

Тағы айта кетейік, барлық ассиметриялық алгоритмдер белгілі бір математикалық функцияларға негізделген. Олардың жұмыс істеуінің дәлелдеуі күрделі болу мүмкін, сондықтан біз тек жұмысының негізгі принциптерін ғана зерттейміз. Криптографиялық алгоритмдердің көбі классикалық сандар теориясына негізделеді. Бұл теорияның негіздерімен біз төменірек таңысамыз.

Негізгі терминдер

Ашық кілті бар шифрлау алгоритмы (немесе **ассиметриялық криптоалгоритмы**) – шифрлау мен ашып оқу үшін әртүрлі кілттерді пайдаланатын криптографиялық алгоритм.

Жабық кілт - ассиметриялық криптографиялық алгоритмдерде пайдаланатын кілт, ол жасырыну түрде сақталыну керек.

Бір жақты функция – есептеуге оңай, бірақ функцияның мәні бойынша оған сәйкес аргументты табуы қиын математикалық функция. Яғни x біле отырып $f(x)$-ты есептеуге оңай, бірақ белгілі $f(x)$ бойынша сәйкес келетін x мәнің табу қиын.

Люкы бар (немесе **құпиясы бар**) **бір жақты функция** – бұл кейбір құпиясы (люк) бар бір жақты функциялардың ерекше түрі, ол функцияның кері мәнің жеткілікті тез есептеуге мүмкіндік береді.

Ашық кілт - ассиметриялық криптографиялық алгоритмдерде пайдаланатын кілт, оны жасырыну түрде сақтамасада болады.

Қосылатын цифрлық қол қоюлар – құжаттың хеш-коды бойынша есептелген қол қоюлар. Осындай қол қоюлар кейбір сандық коды түрінде болады және оны қол қоятың құжатқа тіркеу керек. Мұнда хабардың өзі шифрланбайды және ашық түрде цифрлық қолмен бірге жіберіледі.

Цифрлық (электронды) қол қою (digital signature) – берілетің ақпараттың авторлығын тексере алатын, оған бірегей сандық қосымшасы. Электронды (цифрлық) қол қою (ЭЦҚ) тіркелген ұзындығы бар биттер тізбегі болып табылады, ол белгілі бір түрде ақпараттың ішіндегісі мен және құпиялы кілт көмегімен есептеледі.

Құжатты қалпына келтіруімен цифрлық қол қою – мұнда құжат қолдың құрамына кіретіндей болады: қолды тексеру барысында автоматты түрде құжат денесі де есептеледі. Егер ашып оқыған кезде хабар дұрыс қалпына келсе, онда қойылған қол да дұрыс деп саналады.

Сұрақтар

1. Ассиметриялық шифрлау алгоритмның симметриялықтан айырмашылығы неде?
2. Ашық кілті бар шифрлау алгоритмдер тәжірибеде қандай есептерді шешуге қолданылу мүмкін?
3. Қандай математикалық функциялар бір жақты деп аталады? Криптографияда олар не үшін қолданылу мүмкін?
4. Цифрлық қол қою деген не?
5. Ашық кілті бар шифрлау алгоритмдерді пайдаланғанда цифрлық қол қоюды құрастыру алгоритмы қандай болады?
6. Пайдаланушылар тобында ортақ құпиялы кілтті құрастыру үшін ашық кілті бар шифрлау алгоритмдер қай түрде пайдалану мүмкін?
7. Ассиметриялық алгоритмдерге қойылатын талаптар қандай?