Дәріс №1

Тақырыбы: **Курстың мақсаты мен міндеттері. Кіріспе. Ақпараттық жүйелерде ақпаратты қорғаудың жалпы талдау мәселесі.**

Пән: Криптография және криптоталдау1

Аға оқытушы, Phd: Хомпыш А.

Ақпараттық қауіпсіздік

- **Ақпараттық қауіпсіздік** деп ақпаратқа рұқсат етілмеген қол жетімділіктің, пайдаланудың, ашудың, бұрмалаудың, өзгертудің, зерттедің, жазудың немесе жоюдың алдын алу практикасы.
- **Қауіпсіздіктің ұйымдастырушылық саясаты** (Политика безопасности организации) дегеніміз құнды ақпаратты басқаруды, қорғауды және таратуды басқаратын қауіпсіздікке қатысты құжатталған нұсқаулар, ережелер, процедуралар мен практикалық кепілдемелер жиынтығы.
- **Ақпараттық технологиялар қауіпсіздігі** - ақпаратты басқаруға қажетті барлық ресурстардың (компьютерлердің, бағдарламалық жасақтаманың, желілердің) қауіпсіздігі.
- ? Ақпараттық қауіпсіздік ⊃ Киберқаусіздік ⊃ Ақпараттық технологиялар қауіпсіздігі
- ⊇ Компьютерлік қауіпсіздік;

Ақпараттық қауіпсіздіктің негізгі міндеті

- Деректердің **құпиялылығы** (конфиденциальности данных) - ақпаратқа оны алуға құқығы бар адамдарға ғана қол жетімділікті қамтамасыз ету;
- Деректердің **тұтастығы** (целостности данных) - ақпараттың дәлдігі мен толықтығын және өңдеу әдістерін қорғау;
- Деректердің **қол жетімділігі** (доступности данных) - қажет болған жағдайда авторизацияланған пайдаланушыларға ақпарат пен байланысты ресурстарға қол жетімділікті қамтамасыз ету;
- Шектік жағдайда кез-келген ымыраға жол бермеу (табиғи, техногендік және әлеуметтік апаттар, компьютердегі ақаулар, физикалық ұрлау және тағы сол сияқтылар);

Корпоративтік ақпараттық жүйе (КАЖ) ресурстарының сенімді қорғалуын қамтамасыз ету үшін ақпараттық қауіпсіздік жүйеде (АҚЖ) ақпаратты қорғаудың ең озық және перспективалы технологиялары енгізілуі керек:

- ақпараттың құпиялылығын, тұтастығын және растығын қамтамасыз ететін криптографиялық деректерді қорғау;
- пайдаланушылар мен желілік объектілерді аутентификациялауға арналған аутентификация технологиялары;
- жалпыға ортақ байланыс желілеріне қосылған кезде корпоративтік желіні сыртқы қауіптерден қорғауға арналған брандмауэр технологиялары;
- ашық байланыс арналары арқылы берілетін ақпаратты қорғауға арналған виртуалды қорғалған арналар мен VPN желілерінің технологиялары;
- жетондарды (смарт-карталар, сенсорлық жад, USB порттары үшін кілттер және т.б.) және басқа аутентификация құралдарын қолдану арқылы пайдаланушының кепілдендірілген кепілдемесі;
- пайдаланушы деңгейіндегі қол жетімділікті бақылау және ақпаратқа рұқсатсыз қол жеткізуден қорғау;
- PKI ашық кілттерін басқару инфрақұрылымын қолдау;
- ақпараттық ресурстардың қауіпсіздігін белсенді зерттеу үшін енуді анықтау технологиялары;
- антивирустық профилактиканың және қорғаудың мамандандырылған кешендерін қолданатын вирустардан қорғау технологиялары;
- кәсіпорынның бірыңғай қауіпсіздік саясатына негізделген АҚЖ-ны орталықтандырылған басқару;
- технологиялар мен ақпараттық қауіпсіздік құралдарының ұтымды үйлесімін қамтамасыз ететін ақпараттық қауіпсіздікке кешенді тәсіл.

Қауіпсіздіктің бұзылу көздерінің диаграммысы

Криптография

Криптография (ежелгі грек тілінен аударғанда «жасырын» + «жазамын») – **құпиялылықты** (бейтаныс адамдардың ақпаратты оқудың мүмкін еместігі), **мәліметтердің тұтастығын** (ақпараттың сезілмейтін өзгерісінің мүмкін еместігі), **шынайылығын** (аутентификацияны – авторлықтың немесе объектінің басқа қасиеттерінің растығын) қамтамасыз ету әдістері туралы ғылым.

Криптография - бұл деректерді заңсыз пайдаланушыларға пайдасыз ету арқылы қорғауға арналған деректерді түрлендіру әдістерінің жиынтығы негізінде төмендегі үш проблеманы шешуге мүмкіндік береді:

• жадта тасымалданатын немесе сақталатын мәліметтердің құпиялылығын қорғау;

• деректердің тұтастығы мен шынайылығын растау;

• жүйеге кіру кезінде және байланыс орнатқанда абоненттердің аутентификациясы;

Криптографияның мақсаты

ақпараттың құпиялылығын, шынайылығын және тұтастығын қорғауды жүзеге асыру үшін шифрлаудың, цифрлық қолтаңбаның және аутентификацияның криптографиялық технологиялары қолданылады.

Құпиялылық симметриялық және асимметриялық шифрлау әдістерін қолдану арқылы, сондай-ақ абоненттердің қайта пайдаланылатын және бір реттік парольдер, сандық сертификаттар, смарт-карталар және т.б. негізінде өзара аутентификациясы арқылы қамтамасыз етіледі.

Берілген деректердің **тұтастығы мен шынайлығы**, әдетте, бір жақты функциялар мен шифрлаудың асимметриялық әдістеріне негізделген электронды қолтаңба технологиясының түрлі нұсқаларын қолдану арқылы қол жеткізіледі.

Аутентификация тек заңды пайдаланушылар арасында байланыс орнатуға мүмкіндік береді және қалаусыз адамдардың желі құралдарына кіруіне жол бермейді. Заңдылығын (шынайылығын) дәлелдеген абоненттерге желілік қызметтердің рұқсат етілген түрлері ұсынылады.

Криптографиялық түрлендірулер туралы түсінік

Шифр деп ақпаратты шифрлау кілтін пайдаланып шифрлау және шифрын ашу үшін қолданылатын криптографиялық түрлендірулерге арналған процедуралар мен ережелер жиынтығымен түсіндіріледі.

Ақпаратты **шифрлау** деп ашық ақпаратты (түпнұсқа мәтінді) шифрлық мәтінге (шифрмәтінге) түрлендіру процесін жатқызамыз.

Шифрлау кілтінің көмегімен криптограммадан бастапқы мәтінді қалпына келтіру процесі **дешифрлау** деп аталады.

Қазіргі заманауи криптографиялық алгоритмдердің (криптографиялық түрлендірулер) мақсаты әрбір ашық мәтінді қандайда бір кездейсоқ тізбектен тұратын шифр мәтінге айналдыру:

- егер ашық мәтіннің қандайда бір битті өзгерсе, онда сәйкесінше алынған шифрмәтіндер бір-біріне мүлдем құсамайтын кездейсоқ тізбектер алынуы керек;
- егер түрлендіруде кілт болса, онда кілттің бір биттің өзгерсек, онда сәйкесінше алынған шифрмәтіндер бір-біріне мүлдем құсамайтын кездейсоқ тізбектер алынуы керек;

Шифрлау синтаксисі

Жеке кілтпен шифрлау схемасы немесе шифр үш алгоритмнен тұрады: біріншісі - кілттерді құру процедурасы, екіншісі - шифрлау процедурасы, үшіншісі - шифрды ашу (дешифрлау) процедурасы. Бұл алгоритмдердің келесі функциялары бар:

1. *G* генерациялау алгоритмі - бұл схемамен анықталған кейбір үлестірімге сәйкес таңдалған *k* кілтін шығаратын ықтимал алгоритм.

2. *E* шифрлау алгоритмі *k* кілт пен m ашық мәтінін қабылдайды және *c* шифрмәтінін шығарады. *k* кілтін пайдаланып m ашық мәтіннің шифрлануын $c = E_k(m)$ арқылы белгілейміз.

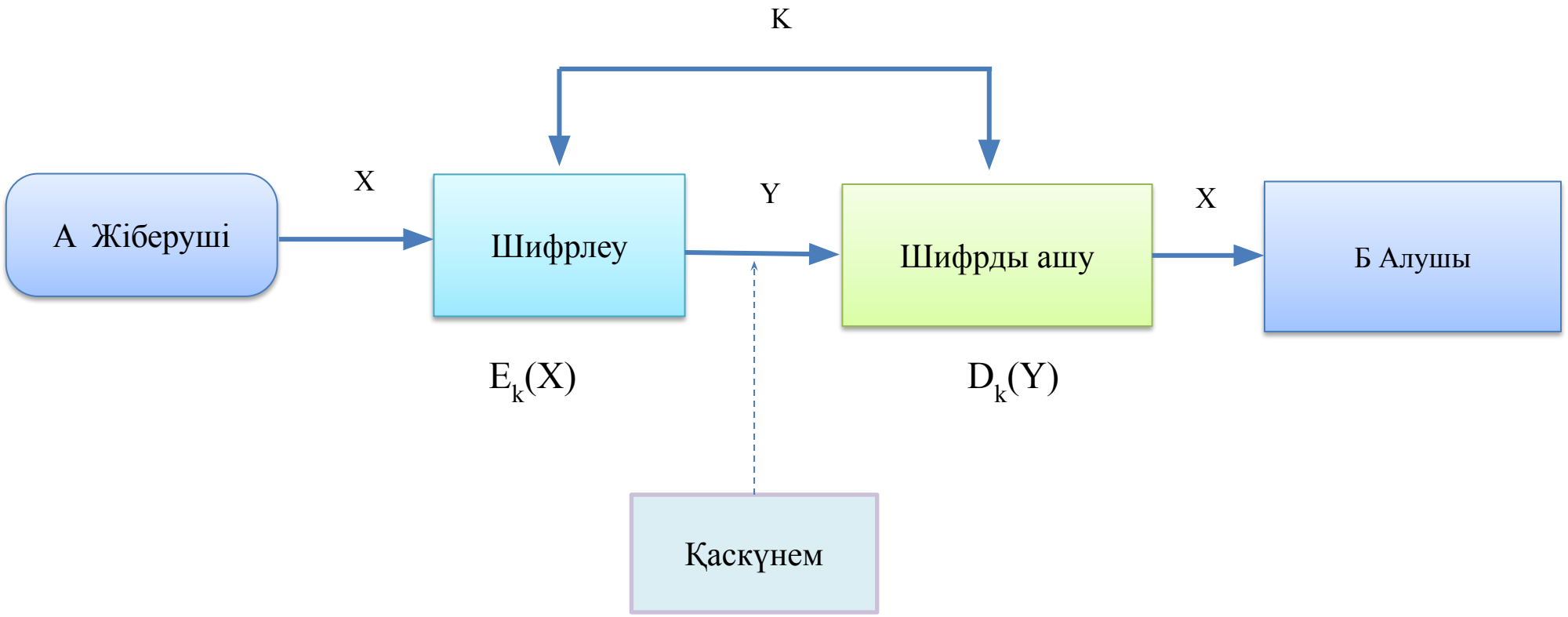
3. *D* дешифрлау алгоритмі *k* кілт пен *c* шифрмәтінін қабылдап, m мәтінін шығарады. *k* кілтін пайдаланып *c* шифрленген мәтіннің шифрын шешуді $m = D_k(c)$ арқылы белгілейміз.

Кез-келген шифрлау схемасының негізгі дәлдігі мынада: *G* шығарған әрбір *k* кілті және $m \in M$ ашық мәтіндік хабарламасы үшін

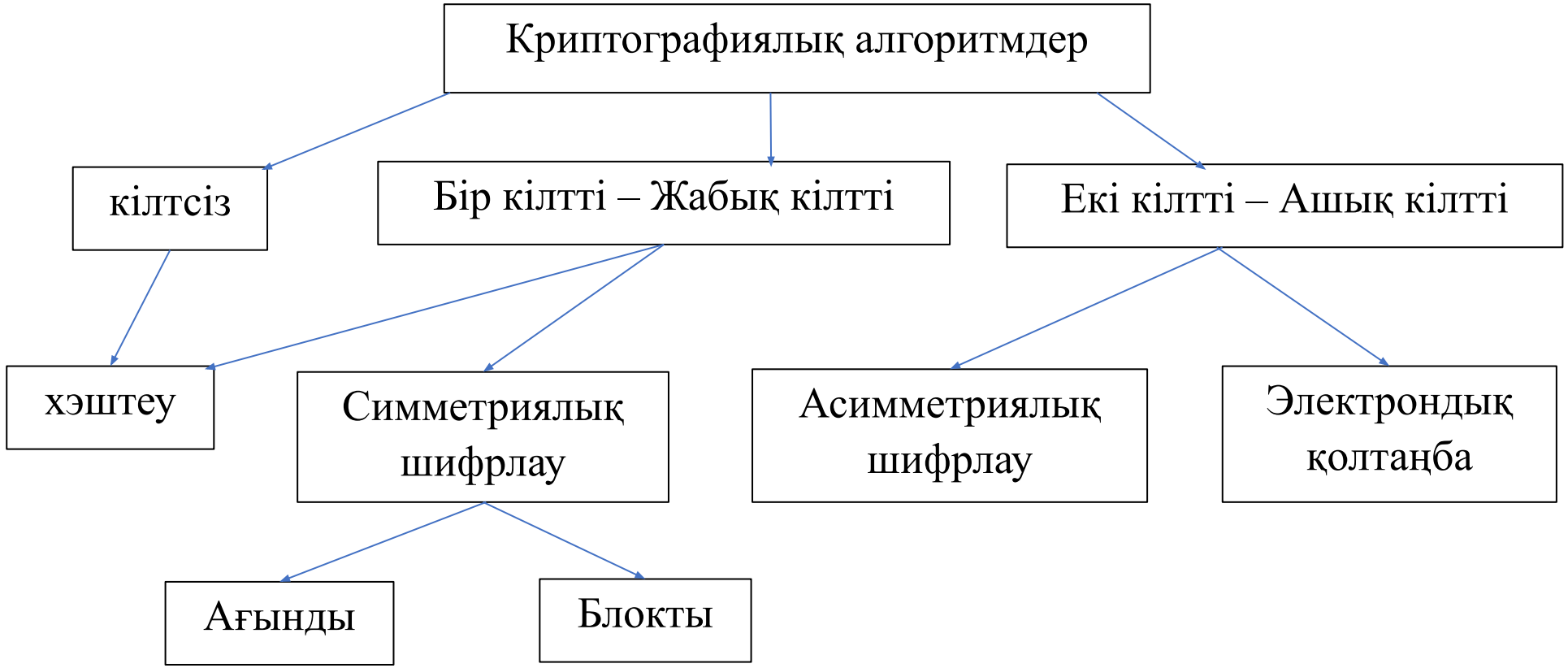
$$D_k\big(E_k(m)\big) = m$$

Ескерту: $c = E_k(m)$ немесе $c = E(k, m)$.

Криптографиялық түрлендірудің жалпылама сұлбасы



криптоалгоритмдердің жіктелуі



Криптографияның қысқаша тарихы (Википедия)

Криптографияны периодтаудың негізгі критерийі ретінде қолданылатын шифрлау әдістерінің технологиялық сипаттамалары бойынша:

Бірінші кезең (шамамен б.з.д. 3 мыңжылдықтан бастап) моно-алфавиттік шифрлардың үстемдігімен сипатталады (негізгі принцип - әріптердің орнын басқа әріптермен немесе белгілермен ауыстыру арқылы бастапқы мәтіннің алфавитін басқа алфавитке ауыстыру).

Екінші кезең (хронологиялық шеңбер - 9 ғасырдан бастап Таяу Шығыста (Аль-Кинди) және 15 ғасырдан бастап Еуропада (Леон Баттиста Альберти) - 20 ғасырдың басына дейін) полиалфавиттік шифрлардың енгізілуімен ерекшеленді.

Үшінші кезең (20 ғасырдың басынан бастап ортасына дейін) электромеханикалық құрылғыларды шифрлағыштардың жұмысына енгізумен сипатталады. Сонымен қатар полиалфавиттік шифрларды қолдану жалғасты.

Төртінші кезең - XX ғасырдың ортасынан бастап 70-ші жылдарына дейін - математикалық криптографияға көшу кезеңі. Шеннонның жұмысында ақпарат көлемін, деректерді беру, энтропия және шифрлау функцияларын қатаң математикалық анықтамалар пайда болады. Шифр құрудың міндетті кезеңі оның әртүрлі белгілі шабуылдарға - сызықтық және дифференциалды криптанализге осалдығын зерттеу болып табылады.

Криптологияның даму тарихы (А.Ж. Асамбаев)

Криптография тарихында шартты түрде төрт кезеңді белгілеуге болады: аңғырт, формалды, ғылыми, компьютерлік.

Аңғырт криптология (XVI ғ. басына дейін) үшін хабар мазмұнын жасыру үшін қарсыласты шатастырудың кез келген қарапайым тәсілдері қолданды (Цезарь шифры, полибиандық төртбұрыш, сиқырлы квадрат және т.б.).

Формалды криптология кезеңі (XV ғ. соңы - XX ғ. басы) формалданған және қолымен жасалатын криптографиялық талдауына берік шифрлардың пайда болуымен байланысты (полиалфавитті шифрлар, роторлық машиналар).

Ғылыми криптологияның (1930 - 1960 жж.) басты айырмашылығы – криптографиялық беріктілікті қатал математикалық негіздеумен криптографиялық жүйелердің пайда болуы.

Компьютерлік критография (1970 жылдардан бастап) өзінің пайда болумен қолдан жасалған және механикалық шифрларға қарағанда, шифрлаудың жоғары жылдамдығы бар кезде бірнеше деңгейге жоғары криптографиялық беріктілікті қамтамасыз ететін криптографиялық жүйелерді жүзеге асыру үшін жеткілікті өнімділікпен есептеу құралдарының пайда болуына міндетті.

Криптографиялық терминология

Ашық (бастапқы) мәтін - криптографияны қолданбай берілетін мәліметтер (міндетті түрде мәтін емес) немесе басқаша айтқанда, шифрланбаған деректер.

Шифрлық мәтін, шифр (жабық) мәтін - криптожүйені қолданғаннан кейін алынған мәліметтер (әдетте - белгілі бір кілтпен). Басқа атауы: криптограмма.

Шифр, криптожүйе - қарапайым мәтіннің шифрмәтінге айналдыратын қайтымды түрлендірулерінің тобы.

Кілт - бұл берілген мәтіннің нақты түрленуін таңдауды анықтайтын шифрлық параметр. Қазіргі шифрларда шифрдың криптографиялық беріктігі толығымен кілт құпиялылығымен анықталады (Керхофс принципі). Сондай-ақ, шифрлау кілті мен дешифрлеу кілті ажыратылады.

Шифрлау - бұл алгоритм мен кілт негізінде ашық мәтінді криптографиялық түрлендіруді қолданудың қалыпты процесі, нәтижесінде шифрлық мәтін пайда болады.

Шифрды шешу (дешифрлау) - шифрленген мәтінді криптографиялық түрлендіруді қарапайым мәтінге қолданудың қалыпты процесі.

Криптографиялық терминология

Асимметриялық шифр, екі кілтті шифр, ашық кілт шифры - шифрлау және шифрды ашу екі кілтті қолданатын шифр. Сонымен қатар, тек шифрлау кілтін біле отырып, хабарламаның шифрын ашу мүмкін емес, керісінше.

Ашық кілт - ассиметриялық жүйенің екі кілтінің бірі - еркін таратылатыны. Электрондық қолтаңба үшін құпия хат-хабарларды шифрлау және шифрын ашу.

Құпия кілт, жабық кілт - асимметриялық жүйенің екі кілтінің бірі - құпия сақталатыны.

Криптанализ - бұл ақпараттың құпиялылығы мен тұтастығын бұзудың математикалық әдістерін зерттейтін ғылым.

Криптаналист - криптоанализ әдістерін жасаушы және қолданушы ғалым.

Криптография және криптоанализ **криптология**ны шифрларды жасау мен бұзудың біртұтас ғылымы ретінде құрайды (мұндай бөлу батыстан енгізілген, оған дейін КСРО мен Ресейде арнайы бөлім қолданылмаған).

Криптографиялық терминология

Криптографиялық шабуыл дегеніміз - криптоаналитиктің шабуылға ұшыраған қауіпсіз ақпарат алмасу жүйесінде ауытқулар жасау әрекеті. Табысты криптографиялық шабуыл хак немесе шабуыл деп аталады.

Шифрды ашу (дешифрды шешу) - белгілі шифрланған криптографиялық кілтті білмей, қарапайым мәтінді шығару процесі. Шифрды ашу термині, әдетте, шифрленген мәтінді криптоанализ процесіне қатысты қолданылады (криптоанализдің өзі, жалпы айтқанда, шифрланған ашық хабарлама ғана емес, криптожүйені талдаудан да тұруы мүмкін). **Криптографиялық беріктік** - криптографиялық алгоритмнің криптоанализге қарсы тұру қабілеті.

Имитациялық қорғаныс (орысша Имитозащита) - жалған ақпаратты таңудан қорғау. Басқаша айтқанда, мәтін ашық болып қалады, бірақ оның кездейсоқ немесе әдейі өзгертілмегендігін тексеру мүмкіндігі туады. Имитациялық қорғанысқа, әдетте, имитацияланған кірістіруді мәліметтер пакетіне қосу арқылы қол жеткізіледі.

Криптографиялық терминология

имитациялық кірістіру (орысша имитовставка) - бұл кілтке және деректерге байланысты қорғауды имитациялау үшін қолданылатын ақпарат блогы.

Электрондық цифрлық қолтаңба немесе электронды қолтаңба - асимметриялық имитация (қауіпсіздік кілті тексеру кілтінен өзгеше). Басқаша айтқанда, емтихан жасанды жасай алмайтын имитациялық кірістіру.

Сертификаттау Орталығы - бұл тұтастығы даусыз және ашық кілт кеңінен танымал жақ. Куәландырушы орталықтың ЭЦҚ-сы ашық кілттің дұрыстығын тексереді.

Хэш-функция - бұл ерікті ұзындықтағы хабарламаны белгіленген ұзындықтағы санға («бүктеуге») түрлендіретін функция. Криптографиялық хэш-функция үшін (жалпы мақсаттағы хэш-функциядан айырмашылығы), кері инженер жасау, тіпті жалпы хэш-функциясы бар екі хабарламаны табу қиын.

Гибридті криптожүйе - бұл ашық кілттік жүйенің артықшылықтарын симметриялы криптожүйелердің өнімділігімен біріктіретін шифрлау жүйесі.

Назар аударғандарыңызға рахмет!