№1 Лекцияның тақырыбы: Криптография негіздері. Қарапайым орын алмастыру және ауыстыру. «Сцитала» алмастыру әдісі. Шифрлау кестелері

Лекцияның оқыту нәтижелері: Криптография ұғымын, оның тарихын, негізгі әдістерін және ақпараттық қауіпсіздікті қамтамасыз етудегі маңызын түсіндіру. Қарапайым орын алмастыру мен ауыстыру шифрларының жұмыс принципін, «Сцитала» әдісін және шифрлау кестелерін тәжірибелік мысалдармен көрсету.

Лекция мазмұны:

1. Криптографияның мәні, мақсаттары және қолданылу салалары
2. Криптографияның даму тарихы
3. Қарапайым алмастыру (substitution) және орын ауыстыру (transposition) әдістері
4. «Сцитала» шифрлау әдісі
5. Шифрлау кестелері және олардың түрлері

1. Криптографияның мәні мен мақсаттары

Криптография - ақпаратты қорғаудың ғылымы және өнері. Ол хабарламаларды шифрлау (жасыру) және дешифрлау (қалпына келтіру) әдістерін зерттейді.

*Криптографияның **негізгі міндеттері:***

- Ақпараттың **құпиялылығын** сақтау (Confidentiality);
- Ақпараттың **тұтастығын** қамтамасыз ету (Integrity);
- Ақпарат көзі мен пайдаланушының **аутентификациясын** растау (Authentication);
- Ақпаратты қайта пайдалануға жол бермеу (Non-repudiation).

Криптографияның қолданылу салалары:

- Банктік жүйелер (интернет-төлемдер, транзакциялар);
- Электрондық үкімет және цифрлық қолтаңба;
- Виртуалды жеке желілер (VPN);
- Электрондық пошталар мен мессенджерлер;
- Бұлттық технологиялар мен деректер сақтау орталықтары.

2. Криптографияның даму тарихы

Криптография грек тілінен аударғанда «құпия жазу» дегенді білдіреді. Қазіргі уақытта криптография ақпаратты түрлендірудің математикалық әдістерін іздеумен және зерттеумен айналысады.

Криптографиямен қатар ***криптографиялық талдау*** дамып, жетілдірілуде Криптоталдау – ақпаратты криптографиялық қорғаудан айыру туралы ғылым. Криптоаналитиктер кілттерді білмей-ақ ақпаратты дешифрлау мүмкіндіктерін зерттейді. Сәтті жасалған криптоталдау шифрлау кілтін, немесе ашық мәтінді, немесе екеуін бірге алуға мүмкіндік береді. Кейде криптография мен криптоталдау бір ғылымға біріктіріледі – ***криптология*** (kryptos – құпия, logos – ғылым). Ол ақпаратты қорғау мақсатында оны қайтымды түрлендіру мәселелерімен айналысады, шифрлау

жүйелерінің сенімділігін бағалайды және шифрлардың беріктігін талдайды.

Қазіргі уақытта криптография біздің өмірімізге мықтап енді. Қазіргі ақпараттандырылған қоғамда криптографияны қолданудың кейбір салаларын ғана көрсетейікші:

• ашық байланыс арналары бойынша тасымалдау кезінде деректерді шифрлау (мысалы, Интернетте сатып алу кезінде, мекенжай, телефон нөмірі, несие картасының нөмірі сияқты деректер әдетте қауіпсіздік мақсатында шифрланады);

• банктік пластикалық карталарға қызмет көрсету;

• желіде пайдаланушы құпия сөздерін сақтау және өңдеу;

• қашықтан байланыс арналары арқылы бухгалтерлік және басқа есептерді жеткізу;

• жергілікті (локальді) немесе ғаламдық (глобальді) желі арқылы кәсіпорындарға банктік қызмет көрсету;

• компьютердің қатты дискісіндегі деректерді рұқсатсыз кіруден қауіпсіз сақтау (Windows операциялық жүйесінде тіпті арнайы термин бар – шифрлау файлдық жүйесі (EFS)).

Криптология туралы жалпы мәліметтер

Криптология – құпия жазбаны (*криптографияны*) және оны ашу әдістерін (*криптологиялық талдауды*) зерттейтін білім аймағы, *RSA* әйгілі криптографиялық жүйенің авторларының бірі *Рональд Ривесттің* (Массачусетстің технологиялық институтының профессоры – *MIT*) айтуы бойынша криптология «барлық *computer science* кіндік шешесі». Криптологияның аты грек тілінен (*криптос* – құпия, *логос* – ғылым немесе сөз) пайда болды.

Заманауи криптологияны ғылым ретінде құру математиканың, физиканың, ақпарат теориясының және табиғы қыйын күрделі есептеулердің фундаменталды түсініктері мен фактілер жинағында негізделген. Бірақ, оған тән қыйындыққа қарамастан криптологияның көптеген теориялық жетістіктері біздің ақпараттық технологиялармен нығайтылған өмірде кең қолданысқа ие, мысалы: пластикалық *smart*-карталарда, электрондық пошталарда, банктік төлем жүйелерінде, *Internet* арқылы электронды саудада, электронды құжатайналым жүйелерінде, дерекқорларды жүргізу кезінде, электронды дауыс беру жүйелерінде және т.б. Осындай жалпы ішкі қыйындық пен тәжірибелік қолданушылық қатынасы теориялық ғылым үшін бірегей.

Криптография - ақпараттың мазмұнын жасыру, өзгертуді немесе рұқсатсыз қолдануды болдырмау мақсатымен ақпаратты түрлендірудің (шифрлаудың) бағдарламалық және аппараттық құралдарын, әдістерді, алгоритмдерді, үлгілерді зерттейтін қолданбалы математика тарауы. Басқа сөзбен айтқанда, криптограф хабарлардың құпиялығын және/немесе шынайлығын қамтамасыз ету әдістерін іздейді.

Ашық электронды байланыс арналар бойынша жіберілетін деректерді қорғау кезінде, электрондық ақпараттың тұтастығын растау кезінде немесе оның авторлығын дәлелдеу кезінде криптографиясыз болмайды.

Криптографиялық талдау кілтті білусіз ақпараттың конфиденциалдығын және шынайлығын бұзудың математикалық әдістерін біріктіреді.

Криптологияға кірмейтін, бірқатар ұқсас білім салалары бар. Ақпараттық массивтерде ақпаратты жасыруды қамтамасыз етумен *стеганография* айналысады. Кездейсоқ әсер ету кезінде ақпараттың тұтастығын қамтамасыз ету *кедергіге төземді кодтау теориясына* жатады. Сонымен қатар, криптологияға жанама аймақ болып ақпаратты қысудың математикалық әдістері есептеледі.

Криптологияда пайдаланатын негізгі анықтамалар

Заңсыз пайдаланушылардан (рұқсатсыз қатынас құрудан) қорғау мақсатымен ақпаратты түрлендіру (шифрлау) әдістері мен тәсілдері *шифр* деп аталады.

Шифрлау – қорғалатын ақпаратқа шифрды қордану процессі, яғни шифрда анықталған ережелер көмегімен қорғалатын ақпаратты (ашық ақпаратты, деректерді) шифрланған хабарға (шифрланған деректер) түрлендіру.

Керішифрлау – шифрлауға қарсы процесс, яғни шифрда анықталған ережелер көмегімен шифрланған хабарды қорғалатын ақпаратқа түрлендіру.

Кілт – нақты хабарды шифрлау үшін қолданатын түрлендіруге жауап беретін шифрдың маңызды компоненті. Әдетте кілт болып әріптік немесе сендық тізбегі табылады. Бұл тізбек шифрлау алгоритміне «баптайтын» сияқты.

Хаттама – есепті бірігіп шешу үшін екі немесе одан көп жақ орындайтын қадамдар реті. Барлық қадамдар қатаң ретпен орындалады, олардың біреуіде алдынғысы бітпей орындалмау керек. Сонымен қоса, әр хаттамаға аз дегенде екі жақ қатысу керек. Ең соңғысы, хаттама міндетті түрде кейбір мақсатқа жету үшін тағайындалған.

Негізінде криптографиялық алгоритм жатқан хаттама *криптографиялық хаттама* деп аталады. Алайда криптографиялық хаттаманың мақсаты ақпаратты басқалардан құпия сақтау ғана болмайды. Криптографиялық хаттаманың қатысушылары бір бірінен құпиялары жоқ жақын дос болу мүмкін, бірақ бір біріне ештеңе айтпайтын бітіспес душпан да болу мүмкін. Соған қарамастан, оларға бірлестік келісімге қол қою немесе өзін куәландыру қажет болу мүмкін. Бұл жағдайда криптография хаттаманың қатысушылары емес басқа адамдармен тыңдауды табу немесе болдырмау үшін, аялақтықты болдырмау үшін қажет. Сондықтан, криптографиялық хаттама келесіні қамтамасыз етуі жиі талап етіледі: оның қатысушылары хаттамамен анықталғаннан басқа ештеңе білмеу және жасамау керек.

Кез келген криптографиялық хаттаманың негізі *криптографиялық алгоримдер.* Әр түрлендіру *кілтпен* бірмәнді анықталады және кейбір *криптографиялық алгоритммен* сипатталады. Бір криптографиялық алгоритм әртүрлі режимдерде шифрлау үшін қолдану мүмкін. Солай шифрлаудың әртүрлі тәсілдері жүзеге асырылады. Шифрлаудың әр

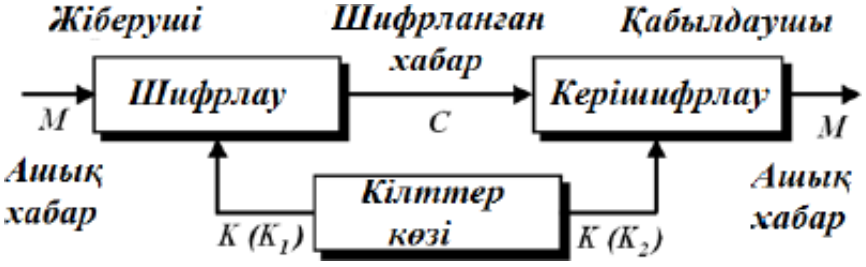
режимінің артықшылықтары және кемшіліктері бар. Сондықтан режимді таңдау нақты жағдайдан тәуелді. Керішифрлау кезінде хабарды шифрлауға қолданған алгоритмнен жалпы жағдайда айырмашылы бар болу мүмкін алгоритмі қолданылады. Осыған сәйкес *шифрлау* және *керішифрлау кілттерінің* айырмашылығы болу мүмкін. Шифрлау және керішифрлау алгоримдердің жұбын *криптографиялық жүйе* деп атайды, ал оларды жүзеге асыратын құрылғыларды – шифрлаушы құрылғылар деп атайды.

Криптографиялық жүйенің жалпылама сұлбасы

Криптографиялық жүйе – ақпаратты қорғау мақсатымен криптографиялық түрлендіруді орындайтын бағдарламалық, аппаратты немесе бағдарламалық-аппаратты түрде жүзеге асырылған жүйе.

Жіберуші қабылдаушыға хабар жібергісі келді дейік. Осыған қоса, жіберуші өз хабарын қауіпсіз жібергісі келеді: ол тасымалдаушыны жолай ұстаған қасқой хабардың мазмұнын біле алмайтынына сенімді болғысы келеді. Жіберілетін хабар *ашық хабар (мәтін, деректер)* деп аталады. Хабардың түрін, оның мәнін жасыру мақсатымен өзгерту *шифрлау* деп аталады. Шифрланған хабар *шифрмәтін (деректер, криптограмма)* деп аталады. Шифрланған мәтінді ашық хабарға түрлендіру процессі *керішифрлау* (криптографиялық талдау кезінде керішифрлау) деп аталады.

Жіберілетін ақпаратты (хабарды, мәтінді, деректерді) шифрлауды және керішифрлауды қамтамасыз ететін криптографиялық түрлендірудің жалпылама сұлбасы 2.1 суретінде көрсетілген.



2.1 сурет - Криптографиялық түрлендірудің жалпылама сұлбасы

Ашық мәтінді *M* (*message* – хабар) немесе *P* (*plaintext* – ашық мәтін) деп белгілейміз. Бұл биттер ағыны, мәтіндік файл, биттік бейне, цифрланған дыбыс, цифрлық бейнекөрініс және басқа болу мүмкін.

Шифрмәтінді *C* (*ciphertext – шифрланған мәтін*) деп белгілейміз. Бұл да екілік деректер, кей кезде *M* бірдей көлемді, кей кезде үлкенрек. Егер шифрлау қысумен болса, онда *C* кішірек болу мүмкін. Бірақ шифрлаудың өзі ақпаратты қысуды қамтамасыз етпейді. *E шифрлау функциясы* ашық мәтінге шифрланған мәтінді құрып әсер етеді:

$$C = E(M). \quad (1.1)$$

Ашық мәтінді шифрланған мәтін бойынша қалпына келтіру *керішифрлау* деп аталады және D керішифрлау функциясы көмегімен орындалады:

$$M = D(C). \quad (1.2)$$

Хабарды шифрлау және ары қарай керішифрлаудың мағынасы ашық мәтінді қалпына келтіру болғандықтан, келесі теңдік орындалады:

$$M = D(E(M)).$$

Шифр деп аталатын криптографиялық алгоритм шифрлауға және керішифрлауға қолданатын математикалық функция (мысалы, (1.1) және (1.2) өрнектерінде E және D функциялары) болады.

Егер алгоритмнің қауіпсіздігі алгоритмнің өзін құпия сақтауда негізделсе, онда бұл *шектелген алгоритм.* Шектелген алгоритмдер тек тарихи қызығушылықты тұдырады, бірақ олар бүгінгі стандарттарға мүлдем сәйкес келмейді. Үлкен немесе өзгеретін пайдаланушылар тобы бұндай алгоритмдерді қолдана алмайды, себебі пайдаланушы топтан шыққан сайын оның мүшелері басқа алгоритмді қолдану керек. Егер сырттан біреу құпияны кездейсоқ біліп қойса, алгоритмді ауыстыру керек.

Заманауи криптография бұл проблемаларды K кілт көмегімен шешеді. *Кілт* - берілген алгоритм үшін барлық мүмкінді нұсқалардан біреуін таңдауды қамтамасыз ететін, деректерді криптографиялық түрлендіру алгоритмнің кейбір параметрлерінің нақты құпия күйі. Мүмкінді кілттер көптігін *кілттер кеңістігі* деп атайды.

Кілтті қолдануды есептеумен шифрлау (1.1) және керішифрлау (1.2) функциялары келесідей жазылады:

$$C = E_K(M) \qquad (1.3)$$

және

$$M = D_K(C), \qquad (1.4)$$

келесі орындалу керек:

$$M = D_K(E_K(M)). \qquad (1.5)$$

Шифрлау және керішифрлау кезінде кейбір алгоритмдер үшін әртүрлі кілттер қолданылады. Бұл жағдайда (1.3) және (1.4) келесі түрде жазылады:

$$C = E_{K_1}(M), \quad M = D_{K_2}(C), \qquad (1.6)$$

ал теңдік (1.5):

$$M = D_{K_2}(E_{K_1}(M)).$$

Шифрлауға және керішифрлауға арналған ақпарат ретінде кейбір *алфавитте* құрылған мәтіндер (хабарлар) қарастырылады. Бұл терминдер астында келесіні түсінеді. *Алфавит* – ақпаратты кодтау үшін қолданатын белгілердің ақырлы (шектеулі) жиыны. *Мәтін (хабар, деректер)* – алфавит элементтерінің реттелген жинағы.

Заманауи ақпараттық жүйелерде қолданатын алфавиттер мысалы ретінде келесілерді келтіруге болады:

- алфавит Z_{26} – ағылшын алфавитының *26* әріпі (бос орынсыз);
- алфавит Z_{33} – орыс тілінің *32* әріпі ("è" әріпісіз) және бос орын;
- алфавит Z_{256} – *ASCII* стандартты кодтарына кіретін *256* символ;
- алфавит Z_{16} – он алтылық алфавиттың *{0,1,…,f} 16* символы;
- алфавит Z_2 – екілік алфавиттың *2* символы *{0,1}*.

Хабарларды шифрлау әдістерін жіктеу

Классикалық немесе біркілтті криптография симметриялық шифрлау алгоритмдерін қолдануға сүйенеді, бұл жерде шифрлаудың және керішифрлаудың тек орындау ретінде және кейбір қадамдар бағытында айырмашылығы болады. Бұл алгоритмдер сол құпия элементті (кілтті) қолданады, және екінші әрекет (керішифрлау) біріншінің (шифрлаудың) қарапайым айналысы болады. Сондықтан, алмасудың әр қатысушысы хабарды шифрлай және керішифрлай алады. Сондай жүйенің сұлбалық құрылымы 2.1 суретінде көрсетілген.

Жіберуші жағында *M* хабар көзі және *K* кілт көзі бар. Кілт көзі берілген жүйенің барлық мүмкін кілттерінен нақты *K* кілтін таңдайды. Ол кілт *K* кейбір тәсілмен қабылдаушы жаққа жіберіледі, және де оны жолай ұстауға болмайды деп есептеледі, мысалы, кілт арнайы курьер арқылы жіберіледі (сондықтан симметриялық шифрлау *жабық кілтті шифрлау* деп аталады).

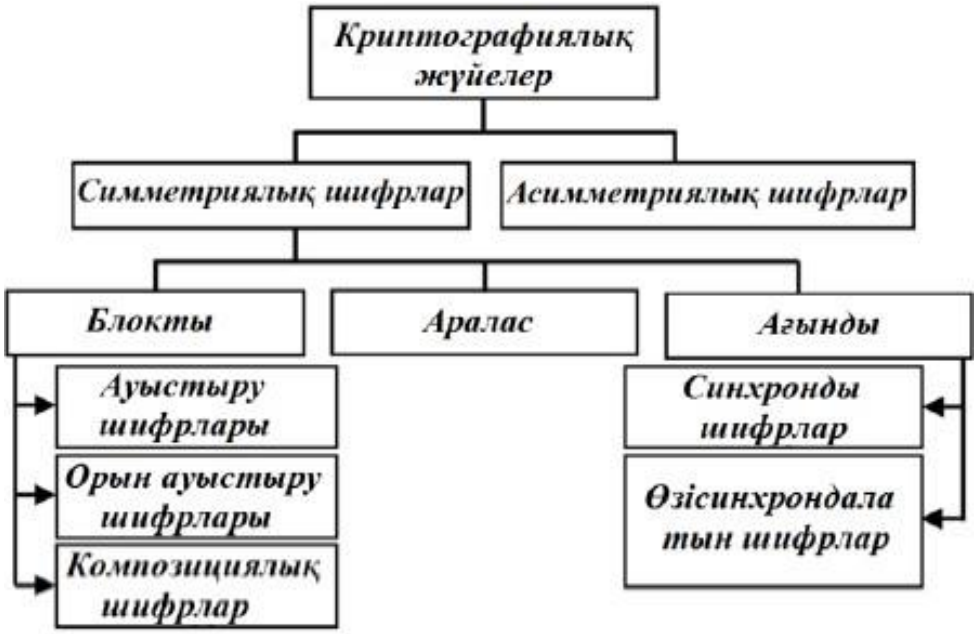
Хабар көзі кейбір *M* хабарын қалыптастырады, ол содан кейін таңдалған кілт *K* арқылы шифрланады. Шифрлау процедурасы нәижесінде *C* шифрланған мәтін алынады (*криптограмма* деп аталады). Ары қарай криптограмма *C* байланыс арнасымен жіберіледі. Байланыс арнасы ашық (қорғалмаған) болғандықтан, мысалы, радиоарна немесе компьютерлік желі, жіберілген хабарды қарсылас жолай ұстау мүмкін. Қабылдайтын жақта *C* криптограммасы *K* кілт көмегімен керішифрланады және *M* кіріс хабары алынады.

Әртүрлі шифрлау әдістері белгілі (2.2 сурет).

Тәжірибеде ауыстыру, орын ауыстыру алгоритмдері және аралас (комбинацияланған) әдістері жиі қолданылады.

Криптографиялық әдістер шифрлау алгоритмі типі бойынша екі үлкен топқа бөлінеді (2.2 сурет): *симметриялық* және *асимметриялық.* Осыған қоса, алгоритмдер түрлендіру типі, ақпаратты өңдеу тәсілі бойынша бөлінеді.

Симметриялық криптографиялық жүйелерде шифрлау және керішифрлау бір кілт арқылы орындалады. Және осыған сәйкес кілтті құпия сақтау керек (бұл жерден симметриялық криптографиялық жүйелердің басқа аты – *құпия кілті бар криптографиялық жүйелер*).



2.2 сурет – Хабарды шифрлау әдістерінің жіктелуі

Асимметриялық криптографиялық жүйелерде екі әртүрлі кілт бар: біреуі шифрлау үшін қолданылады және *ашық* деп аталады, басқасы – керішифрлау үшін, *жабық* деп аталады. Асимметриялық криптожүйелердің басты айырмашылығы келесіде: ашық кілтпен шифрлаған адам да хабарды құпия кілтсіз керішифрлай алмайды. Сондықтан бұл жүйелер *ассимметриялық* немесе *ашық кілтті жүйелер* деп аталады.

Криптографиялық жүйелердің екі типін де біріктіретін криптографиялық жүйелерді *гибридті* деп атайды. Оларда, ереже сияқты, хабар мәтіні симметриялық криптографиялық жүйені қолданумен

шифрланады, ал симметриялық криптографиялық жүйемен қолданылған құпия кілт асимметриялық криптографиялық жүйені қолданумен шифрланады.

Кіріс ақпарат тізбегін өңдеу типі бойынша жүйелер *ағындыға* және *блоктыға* бөлінеді. Ағынды жүйелерде ашық мәтіннің әр символы немесе биті шифрланған мәтін символына ағынмен шифрланады. Блокты жүйелерде хабарлар анықталған ұзындығы бар блоктармен түрлендіріледі.

Орын ауыстыру әдістерінде кіріс мәтіннің символдары анықталған ереже бойынша бір бірімен орын ауыстырады. *Ауыстыру әдістерінде* ашық мәтін символдары шифрланған мәтіннің эквиваленттерімен ауыстырылады.

Шифрлау сенімділігін жоғарлату мақсатымен бір әдіспен шифрланған мәтін басқа шифрмен тағы шифрлану мүмкін. Бұл жағдайда *құрамдас* немесе *композициялық шифр* болады. Кәзіргі уақытта тәжірибеде қолданылатын блокты немесе симметриялық ағынды шифрлар құрамдас шифрларға жатады, олар хабарды шифрлау үшін бірнеше операцияны қолданады.

3. Қарапайым алмастыру және орын ауыстыру әдістері

Ауыстыру шифры (Substitution cipher): Ашық мәтіндегі әр символ басқа бір символмен ауыстырылады.

Мысал:

Ашық мәтін: ҚАУІП

Кілт: әр әріпті +3 орынға жылжыту

Шифрланған мәтін: ТВЦЛС

Артықшылықтары: Қарапайым және тез.

Кемшіліктері: Жиілік талдау арқылы оңай бұзылады.

Түрлері:

1. *Моноалфавиттік шифр:* бір әріп әрдайым бір символмен алмастырылады.

2. *Полиалфавиттік шифр:* әр әріп бірнеше түрлі сәйкестікте шифрланады (мысалы, Виженер шифры).

Орын алмастыру шифры (Transposition cipher):

Мәтіндегі әріптер өз орнын өзгертеді, бірақ өздері өзгермейді.

Мысал:

Ашық мәтін: **ҚАУІПСІЗДІК**

Топтарға бөлу: 3 баған

Қ	А	У
І	П	С
І	З	Д
І	К	*

Шифрланған мәтін: **ҚІІ АПЗК УСД***

Артықшылықтары: Құрылым күрделірек, жиілік талдау көмектеспейді.
Кемшілігі: Ұзақ мәтіндерді қолмен шифрлау қиын.

4. «Сцитала» алмастыру әдісі

Б.э.д. V ғасырда Спарттық әскерлерде жақсы жабдықтылған құпиялы әскери байланыс болды. Олар өздерінің хабарларын сцитала шифры көмегімен құпияланды.Шифрлау іс жүзінде былай жасалынды. Цилиндрлік пішіндегі стерженьге спираль түрінде қағаз қиындысы оралады және оған стержень бойымен хабар мәтіні жазылды (1-кесте).

1-кесте

«Сцитала шифры»

	х	а	б	а	
	р	м	ә	т	
	і	н			

Бұдан соң стерженнен оралған мәтін жазылған қағазды аламыз. Бұл қағазға жазылған әріптер ретсіз орналасқан хаостық түрде болады.

Жұмыс принципі:

1. Белгілі диаметрлі стерженге таспа немесе тері жолақ оралады. Себебі стерженнің диаметрі құпиялы кілт болады.
2. Хабар таспаға көлденең жазылады.
3. Таспаны шешкенде әріптер ретсіз болып шығады.
4. Дәл сондай стерженге қайта оралғанда ғана хабар қалпына келеді.

Маңызы:

Бұл әдіс ақпаратты физикалық құрал арқылы қорғаудың алғашқы түрі. Ол шифрлау мен дешифрлаудың тек белгілі бір құралға тәуелді болатынын көрсетті.

5. Шифрлау кестелері және олардың қолданылуы

Шифрлау кестелері — әріптерді немесе сандарды жүйелі түрде алмастыру үшін қолданылатын құрал.

Полибиан квадраты (Polybius square)

Тік бұрышты кесте алфавит әріптерімен кездейсоқ тәртіпте толтырылады. Ашық хабардың әрбір әрібі сол бағанда бір қатар төменде орналасқан әріппен ауыстырылады. Егер әріп ең соңғы қатарда орналасқан болса, онда шифрленетін символ бағандағы бірінші әріп болады. Мысалы, «АЛФАВИТ» хабары шифрленгеннен кейін «УЫ_УТСЗ» көрінісіне келеді:

У	К	В	Ъ	М	Ю	Ь	Д
И	Б	Т	Л	Э	Г	Щ	Н
С	Ф	З	Ы	П	Ц	Е	Я
А		Р	Х	Ж	Ш	О	Ч

Полибий квадраты қарапайым ауыстырудың алғашқы шифрларының бірі болып есептеледі. 5х5 квадраттың әрбір орнына кездейсоқ түрде алынған бір әріп жазылады (1-сурет). Грек алфавитінің әріптерімен толтырғанда бір орын

бос қалған, ал латын алфавитінің әріптерімен толтырғанда бір орынға екі әріп (i және j) жазылған.

Мысал:

A	B	C	D	E
F	G	H	I,J	K
L	M	N	O	P
Q	R	S	T	U
V	W	X	Y	Z

Артықшылығы:

- Қарапайым алмастыруға қарағанда әлдеқайда қауіпсіз.
- Кілт ұзындығы өскен сайын бұзу қиындайды.

6. Қазіргі заманғы криптография және оның бағыттары

Қазіргі криптография – математикалық логикаға және есептеу күрделілігіне сүйенетін ғылым.

Негізгі бағыттар:

1. Симметриялық шифрлау: бір кілт қолданылады. (AES, DES, Blowfish)
2. Асимметриялық шифрлау**:** ашық және жабық кілттер пайдаланылады. (RSA, ECC)
3. Хэш функциялар: ақпараттың тұтастығын тексереді. (MD5, SHA256)
4. Сандық қолтаңба: хабардың түпнұсқалығын дәлелдейді. (DSA, ECDSA)
5. Кванттық криптография: болашақта жарық фотондары арқылы абсолютті қауіпсіз байланыс жасауға бағытталған.

Қолданылуы:

- Электрондық үкімет жүйелері;
- Интернет банкинг және онлайн төлем жүйелері;
- Бұлттық сақтау жүйелері (Google Drive, iCloud);
- Блокчейн және криптовалюта жүйелері (Bitcoin, Ethereum).

7. Криптографиялық қауіпсіздік принциптері

Ақпараттық қауіпсіздік келесі үш негізгі қасиетке негізделеді:

- Құпиялылық (Confidentiality) – ақпаратқа тек уәкілетті тұлға ғана қол жеткізе алады.
- Тұтастық (Integrity) – ақпарат өзгеріссіз сақталады.
- Қолжетімділік (Availability) – ақпарат қажет уақытта қолжетімді болуы керек.

БӨЖ және ОБӨЖ тапсырмалары

БӨЖ: «Криптографияның даму тарихы мен қазіргі заманғы әдістері» тақырыбында 2 бет конспект жазыңыз (10 ұпай).

ОБӨЖ: Python тілінде қарапайым орын ауыстыру шифрын бағдарламалау (мәтінді шифрлап, қайта ашу). Нәтижені кестемен көрсетіңіз (15 ұпай).

Пайдаланылған әдебиеттер

Негізгі әдебиеттер:

1. Г. Камалова, А. Х. Касымова, Л. Б. Диярова. «Ақпараттық қауіпсіздікті басқару». Оқу құралы. /- Алматы: Альманахъ, 2020. - 128 с.

2. Дүйсебекова, К.С. Ақпараттық қауіпсіздік және ақпараттарды қорғау: Оқу құралы. - Стер. бас - Алматы: Қазақ университеті, 2020. - 156 б. http://rmebrk.kz

3. Камалова Г.А., Диярова, Л.Б. Ақпараттық қауіпсіздік және ақпаратты қорғау: Оқу құралы. / Жәңгір хан атындағы Батыс Қазақстан аграрлық-техникалық университеті. - Алматы: Альманах, 2020. - 116б. http://rmebrk.kz

Қосымша әдебиеттер:

1. Ж.З. Сатмаганбетова. Бағдарламалау тілдері және технологиясы: Оқу-әдістемелік куралы. / Қостанай: А. Байтурсынов атындағы ҚМУ, 2014. - 64 б. http://rmebrk.kz