Лекция 1 КРИПТОГРАФИЯНЫҢ НЕГІЗГІ ҰҒЫМДАРЫ

Оқытудың техникалық құралдары: интерактивті тақта

Лекция оқудың тәртібі, оқыту әдістері мен түрлері: кіріспе лекция

Бұл бөлімде криптографияның пәні мен міндеттері анықталады, курс негізін салушы анықтамалар және ақпаратты қорғау криптографиялық жүйелерге қойылатын талаптар тұжырымдалынады, криптография ғылымының негізгі даму кезеңдері туралы тарихи анықтама беріледі. Және де тұжырымдалған ұғымдар мен тезистер қарапайым шифрдің мысалы арқылы түсіндіріледі.

Бөлім мақсаты: студентті криптографияның негізгі ұғымдарымен таныстыру.

1.1 Криптографияның пәні мен міндеттері

Абонент арасында ақпаратты беру кезіндегі оны қорғау проблемасын адамдар бұрыннан шешуге тырысатын. Адамзат берілетін хабардың мағынасын жаудан жасыруға мүмкіндік беретін көп тәсілдерді ойлап тапқан. Тәжірибеде құпиялы хабарды қорғайтын бірнеше қорғау әдістер тобы жасалынған. Кейбіреуін, криптографиялық сияқты баяғыдан пайдаланатын, атап кетейік.

Бірінші тәсіл ақпараттың материалдық тасушысын жаудан ***физикалық қорғау***. Мәліметтерді тасушы ретінде қағаз, компьютерлік тасушы (DVD-диск, флэш-карта, магнитті диск, қатқыл диск және т.б.) болу мүмкін. Осы тәсілді жүзеге асыру үшін сенімді байланыс арнасы қажет. Бұрыңғы заманда ол үшін пошта көгершіндері, арнайы курьерлер, құпиялы жиілікте радиохабарлар пайдаланылатын. Ақпараттың физикалық қорғау әдістері қәзіргі мәліметтерді өңдеу автоматтандырылған жүйелерде де пайдалынады. Мысалы, ақпаратты қорғау құрама жүйелерге қоршау жүйелер мен физикалық оқшаулау кіреді және күзет жүйелері.

Ақпаратты қорғаудың бұрыннан белгілі екінші тәсілі – ***стеганографиялық қорғау***. Бұл қорғаудың негізінде қарсыласқа керекті ақпаратты жасыру әрекеті. Стеганографиялық қорғау әдісте жаудан мәліметтердің физикалық тасушысын жасырады немесе құпиялы хабарды құпиялы емес, ашық ақпараттын арасында бүркейді. Осындай тәсілдерге жатады, мысалы, құпиялы ақпараты бар микрофотоларды құпиясыз жерде «тығу»: пошта конвертінің маркасының астында, кітаптың тыс астында және т.б.

Стеганографияға және белгілі тәсілдерде жатады: құпиялы хабарды түймеге, аяқ киімнің өкшесіне, тіс пломбасына және т.б. «тығып жасыру». Ежелгі заманда, мысалы, гректер құлдың бас шашін қырып алып хабарды басқа жазатың. Сосын шаші қайтадан өскеннен кейін оны хабарды жеткізуге жіберетін. Алушы құлдың басын шаштан босатып, хабарды оқитын. Бірақ, осы тісілге ұзақ уақыт кетеді. Кейіннен химиялық сиялар кең пайдаланатын болатын. Құпиясыз хабардың жолдарының арасында осындай сиямен жазылған мәтін көрінбейді. Оны оқу үшін арнайы технология қолдану керек, мысалы қағазды қыздыру.

Қазір жаңа стеганографиялық тәсілдер пайда болады. Мысалы, құпиялы хабар графикалық файлдың ішінде жасырылады. Осы тәсілді пайдаланғанда бейненің әрбір пикселінің кіші байты хабардың битімен ауыстырылады. Бастапқы хабарды биттерге бөліп және осы биттерді бүкіл графикалық файл бойынша орналастырып, біз бүркемеленген хабары бар бейнені алушыға жібереміз. Бұл кезде графикалық бейне аса қатты өзгермейді, әсіресе егер көп түсті тәртіп (мысалы, түстің тереңдігі 24 бит бір пикселге) пайдаланатын болса. Себебі, адамның көзі сондай көп түстерді айыра алмайды. Сонымен, 32х32 нүктесі бар суретке ұзындығы 1024 бит (128 байт) құпиялы хабарды сыйғызуға болады.

Ақпаратты қорғаудың үшінші тәсілі – ең берікті және қәзіргі уақытта кеңінен таралған – ***криптографиялық***. Бұл әдісте жаудан (қаскүнемнен) ақпараттың мағынасын жасыру үшін оны түрлендіру қажет. **Криптография** грек тілінен «құпия жазу» деп аударылады. Қазір криптография ақпаратты түрлендірудің математикалық әдістерін іздеп зерттейді.

Криптографиямен қатар дамиды және жетілдіріледі **криптоталдау** – бұл ақпараттың криптографиялық қорғауын жеңіп өту туралы ғылым. Криптоталдаушылар кілттерді білмей ақпараттың шифрын ашу мүмкінідігін зерттейді. Табысты өткізілген криптоталдау шифрлау кілтті, немесе ашық мәтінді, немесе екеуінде бірге алуға мүмкіндік береді. Кейде криптографиямен криптоталдауды бір ғылымға біріктіреді – **криптология** (kryptos - құпиялы, logos - ғылым). Оның негізгі міндеттері – рұқсатсыз қатынаудан ақпаратты қорғау үшін ақпаратты қайтымды түрлендіру сұрақтары, шифрлау жүйелердің сенімділігін бағалау және шифрдың беріктігін талдау.

Қазіргі ақпараттандырылған қоғамда криптографияның кейбір қолдану салаларын келтірейік:

- ашық байланыс арна арқылы берген кезде деректерді шифрлау (мысалы, Интернетте сатып алу кезіндегі мекен жайы, телефон, кредит картанын нөмірі сияқты мағлұматтар шифрланады);
- банк пластикалық карточкаларға қызмет көрсету;
- желі ішінде пайдаланушылардың парольдерін сақтау және өңдеу; алысталған
- байланыс арна арқылы бухгалтерлік есептерді өткізу; жергілікті және
- ғаламдық желі арқылы кәсіпорындарға банктік қызмет ету;
- рұқсат етілмеген қатынаудан деректерді компьютердің қатқыл дискісінде (мысалы, Windows операциялық жүйеде арнайы термин бар – файлдық шифрланған жүйе EFS) қауіпсіз сақтау.

XX ғасырға дейін криптографиялық әдістер тек рұқсатсыз қатынаудан қорғау үшін деректерді шифрлауға ғана қолданылатын. XX ғасырда жаңа криптографиялық әдістерін жасағандықтан криптографияның міндеттерінің спектрі де кеңейді. Қазіргі уақытта криптография келесі міндеттерді шешуге арналған:

- рұқсатсыз қатынаудан қорғау үшін деректерді шифрлау;
- хабарлардың дұрысын (тап өзін) тексеру: хабарды алушы оның шығу көзін тексере алады;
- берілетін деректердің бүтіндігін тексеру: жіберу барысында хабар өзгерді ме не ауыстырылды ма алушы тексере алады;
- бас тартудан мүмкін еместігін қамтамасыз ету, яғни алушыға да берушіге де жіберуден бас тартудын мүмкін еместігі.

Шифрлау жүйелері өте қарапайымнан өте күрделіге дейін болу мүмкін. Біріншілері ешқандай математикалық танымдарды талап етпейді, ал соңғыларында математика және информатика салаларынан аса белгілі емес арнайы ұғымдар пайдаланылады. Криптографиялық әдістерді пайдалану кезінде ақпаратты қорғауға және шабуыл әдістерді жүзеге асыруға жұмсалған шығындар еске алыну керек. Тәжірибеде шифрлаудың бағасы мен қауіпсіздіктің қажетті деңгейінің арасындағы ымыраға жетуіне тырысады.

Біздің оқу құралымызда «компьютерге дейін» бұрыннан танымалы қарапайым және XXI ғасырда ойлап тапқан осы заманғы шифрлау жүйелер қарастырылады.

1.2 Негізгі анықтамалар

Енді, криптографияның міндетін білгеннен кейін, негізгі терминдермен танысайық.

Шифр – бастапқы құпиялы хабарды қорғау үшін оның алдын ала айтылған түрлендіру тәсілдерінің жиынтығы.

Бастапқы хабарлар әдетте **ашық мәтін** деп аталады. Шетел әдебиетте ашық мәтін үшін пайдаланады термин ***plaintext***.

Символ – кез келген белгі, соның ішінде әріп, цифр немесе тыныс белгілері.

Әліпби (алфавит) – ақпаратты кодпен жазу (кодтау) үшін пайдаланылатың символдардың шектілік көптігі.

Мысалы, орыс әліпбиі А-дан Я-ға дейін 33 әріптен тұрады. Бірақ, бұл отыз үш белгі хабарды жазу үшін жеткіліксіз, сондықтан оны тақыр, нүкте, үтір және басқа символдармен толтырады. Араб цифрлердің әліпбиі – бұл 0, 1, 2, 3, 4, 5, 6, 7, 8, 9

символдар. Бұл алфавитте 10 белгі бар және оның көмегімен кез келген натурал санды жазуға болады. Кез келген хабар екілік әліпби көмегімен де жазылу мүмкін, яғни тек ноль мен бірді пайдалана отырып.

Кез келген шифрды пайдаланып түрлендіруден кейінгі алынған хабар **шифрланған хабар** (***жабық мәтін***, ***криптограмма***) деп аталады. Шетел әдебиетте жабық мәтін үшін пайдаланады термин ***ciphertext***.

Ашық мәтіннің криптограммаға түрлендіруі **шифрлау** (шифрлану) деп аталады. Кері іс-әрекет **шифрды ашу** (***дешифрлау***) деп аталады. Ағылшын тілде бұл терминдерге сәйкес «***enciphering*** / ***deciphering***».

Кілт – хабарларды шифрлау мен дешифрлау үшін қажетті ақпарат.

Шифрді ашу және дешифрлау терминдері бір біріне синоним, бірақ әдетте екінші термин көбінесе қаскүнем (яғни кілтті білмейтін адам) үшін пайдаланады.

Шифрлау жүйесі немесе **шифржүйесі** – бұл хабар мәтінің қайтымды өзгерту үшін (жолданған адамнан басқа барлықтарға мәтін түсініксіз болсын оймен) пайдаланатын кез келген жүйе.

Кілтті білмегенде шифрды ашуға беріктікті анықтайтын шифр сипаттамасы (яғни криптоталдауға қарсы тұру қабілеті) **криптоберіктік** деп аталады.

Сонымен, берілген анықтамаларды еске ала отырып, «криптография» ғылымының дәл анықтамасын берейік. **Криптография** шифрлау жүйелерінің құруы мен пайдалануын зерттейді, соның ішінде олардың беріктігін, осал жерін және ашу әдістер жөнінде осалдық дәрежесін.

Рұқсатсыз қатынаудан қорғау үшін ақпаратты түрлендірудің барлық әдістері екі үлкен топқа бөлінеді: жабық кілті бар шифрлау әдісі және ашық кілті бар шифрлау әдісі.

Жабық кілті бар шифрлауды (құпиялы кілті бар шифрлау немесе симметриялық шифрлану) адам бұрыннан пайдаланып келе жатыр. Бұл әдісте деректерді шифрлау және дешифрлау үшін бір кілт ғана пайдаланады, оны екі жағы да жаудан жасырып сақтайды.

Ашық кілті бар шифрлаудың (ассимметриялық шифрлау) пайдаланауы XX ғасырдың екінші жартысында ғана басталды. Бұл топқа жатады деректерді шифрлау және дешифрлау үшін екі әртүрлі кілтті пайдаланатың шифрлау әдістері. Мұнда кілттердің біреуі (ашық кілт) ашық (қорғалмаған) арна арқылы берілу мүмкін.

Электронды (**цифрлық**) **қол** (***қолтаңба***) бұл әдетте хабарға қосылатың, криптографиялық түрлендіру көмегімен алынған, деректер блогы.

Мәтінді алған кезде электронды қол хабардың авторлығы мен нақтылығын тексеруге мүмкіндік береді.

Ақпаратты қорғаудың криптографиялық жүйесі – бұл деректерді шифрлау үшін криптографиялық әдістерді пайдаланатын ақпаратты қорғау жүйесі.

1.3 Ақпаратты қорғаудың криптографиялық жүйесіне қойылатын талаптар

Қазіргі уақытта жасалынып жатқан ақпаратты қорғаудың криптографиялық жүйелеріне келесі талаптар тұжырымдалған:

- шифрланған хабар тек кілт болғанда ғана оқылу керек;
- шифрлау алгоритмды білу қорғаудың сенімділігіне әсер етпеу керек;
- мүмкін болатын көптіктегі кез келген кілт ақпараттың сенімді қорғауын қамтамасыз ету керек;
- шифрлау алгоритмы бағдарламалық та, аппараттық та жүзеге асыруға мүмкіндік беру керек.

Айтылған талаптар шифрлау алгоритмдердің бәріне толық орындалмайды. Мысалы, осал кілттердің болмау талабы (қаскүнемге шифрланған хабарды оңай ашуға мүмкіндік беретін кілттер) кейбір «ескі» блокты шифрлер үшін орындалмайды. Бірақ, жаңадан жасалынған барлық жүйелер айтылған талаптарға қанағаттандырылады.

1.4 Криптографиялық әдістерді жүзеге асыру

«Компьютерге дейін» заманда деректердің шифрлауы қолмен істелінетін. Шифрлаушы бастапқы хабарды символ бойынша өңдей отырып және осылай шифрланған мәтін алынатын. Бұл жұмыс бірнеше рет тексерілседе қателіктер бәрі бір кездесетін. Механикалық шифрлау машиналарды жасағаннан кейін шифрлау кезіндегі деректердің өңдеу процесі автоматтандырылып тездетілді. Және де шифрлау техниканың қолдауы шифрлау мен дешифрлау барысындағы қателіктер ықтималдығын азайтты. Техниканың онан әрі дамуы алдымен электрмеханикалық, сосын электронды криптографиялық құрылғылардың пайда болуына әкелді.

Егер шифрлау мен дешифрлаудың барлық процедуралары белгілі логикалық ережелер бойынша арнайы электронды сызба арқылы орындалса, онда криптографиялық әдістің жүзеге асыруының осындай тәсілі **аппаратты** деп аталады. Криптографиялық әдістің аппараттық жүзеге асыруы жоғары өнімділікпен, пайдалану кезіндегі қарапайымдықпен, қорғалғандықпен ерекшеленеді.

Есептеуіш техниканың, әсіресе дербес компьютерлердің енгізуі, шифрлау алгоритмның **бағдарламалық** жүзеге асырудың пайда болуына әкелді. Қорғаудың бағдарламалық жүзеге асыру әдістерінің негізгі артықшылығы олардың икемділігі, яғни шифрлау алгоритмның немесе оның күйге келтіруінің тез өзгерту мүмкіндігі. Одан басқа криптографиялық әдістердің бағдарламалық жүзеге асыруының бағасы төмен. Ал негізгі кемшілігі аппараттық тәсілдерге қарағанда кіші жылдамдығы (оңдаған есе аз).

Қазіргі уақытта құрамалы да шифрлау модульдер шығарылады, олар **бағдарламалы-аппараттық** деп аталады. Бұл жағдайда компьютерге «криптографиялық сопроцессор» қосылады – арнайы криптографиялық операцияларды орындауға бағытталған аппараттық есептеуіш блогы. Осындай құрылғыда бағдарламалық қамтамасыз етуді ауыстырып, сол не басқа біреу шифрлау әдісті таңдауға болады.

1.5 Криптография тарихынан мәліметтер

Түрлі шифрлардың саясатта және әскери істе қолдануын қыруар көп тарихи құжаттардан табуға болады.

Криптографиялық әдістер Ежелгі Мысырда, Үндістанда, Месопотамияда қолданылатың. Мысалы, мысыр абыздарының жазбаларында шифрланған жолдау хатты құрастырудың жүйелері мен тәсілдері туралы мәлімет табуға болады.

Ежелгі гректер (көбінесе спарталықтар) соғыс кезінде Сцитал деген шифрлау құрылығыны пайдаланатын. ***Сцитал*** – бұл белгілі диаметрі бар цилиндрлық жезл (асатаяқ). Сциталаға енсіз папирус (немесе белдік) тілім-тілімі айналым оралатын. Оралған таспаға жезлдің осі бойынша ашық хабар жазылатың. Сосын таспаны тарқатып алып (сонда хабардың әріптері ретсіз жазылған сияқты болады) жолданған адамға жіберетің. Егер папирус жаудың қолына түссе, ол құпиялы хабарды оқиялмайды. Себебі хабарды оқу үшін дәл сондай диаметрі бар Сцитала қажет болатын – оған алынған папирус таспасы қайтадан оралатың, сонда хабардың жолдары беттесіп құпиялы хабар ашылады. Бұл шифрлау әдістің кілті - Сциталаның диаметрі. Дешифрлау «құрылғыны» Аристотель ойлап тапты деп есептеледі, ол конус тәріздес «найзаны» пайдалануға ұсыныс берді. Ұстап алынған таспаны найзаға орап, оны конустың осі бойынша мағыналы мәтін шыққанша жылжытып отыратын.

Ежелгі Грецияда басқа шифрлер де пайадаланатын. Мысалы, «***Полибий шаршысы***» деп аталатын шифр. Осы шифры бойынша, хабардың әріптері сандарға ауыстырылатын. Бұл сандар 5х5 шаршыға жазылған әліпби символдарының координаталары.

Араб мемлекеттерінде хабардың шифрлауы әскери мен саяси мақсатпен ғана емес, сауда серіктестерінің арасында да пайдаланатын. Айтпақшы, «шифр» мен «цифр» сөздері араб тілінен келген. VIII–XV ғасырларда криптография мен криптоталдау туралы мәліметтері бар ғылыми жұмыстар пайда болды. Мысалы көптомды энциклопедияда «Шауба аль-Аша» жиіліктік криптоталдау (яғни ашық және шифрланған хабарда

әріптердің кездесу жиілігіне негізделген талдау) туралы айтылған. Осы энциклопедияда араб тілі әріптерінің жиілік сипаттамасының кестесі келтірілген.

Орта ғасырда криптографиялық әдістер ең алдымен әскери істе, тыңшылықта, дипломатияда пайдаланатын. Дін қызметшілері, ғалымдар және дипломаттар шифрлерді зерттейтің. Криптография туралы алғашқы жұмыстарды XIV–XVI ғасырда Чикко Симоннети (папасының кеңсе қызметкері), Габлиэль де Лавинда (Клементий XII папаның хатшысы), Леон Баттиста Альберти (атақты итальян архитекторы және философы), Германияда өмір сүрген аббат Иоганнес Тритемий жазды. Леон Альберти полиалфавитты шифрды бірінші ұсынды деп саналады. Және де ол бірінші автоматты машинаны (шифрлайтың диск) ойлап тапты деп есептеледі.

XVII-XVIII ғасырда Еуропаның мемлекеттерінде арнайы шифрлау қызметтер пайда болды. Ресейде криптографиялық қызмет 1549 жылдан басталады, сонда ашылған «елші бұйрықтың» құрамына «цифрлық» бөлімше кіретін. Петр I заманында криптографиялық қызмет «Елші кеңсеге» қайта құрылды.

Криптографиямен көп саясатшылар мен ғалымдар айналысатын. Солардың ішінде Пифагор, Аристотель, Платон, Галилей, Д. Порта, Д.Кардано, Л. да Винчи, Ф.Виет, Д.Валлис, Б.Паскаль, И.Ньютон, Ф.Бекон, Х.Гольбах, Ф.Эпинус, Л.Эйлер, П.Ф.Шиллинг, Ч.Беббидж және басқалар.

Криптографияның дамуына ғылым мен техниканың жетістіктері үлкен әсер етеді. Мысалы, XIX ғасырдың ортасында телеграфты ойлап тапқаннан кейін оны қолданатың бірнеше дипломатиялық және сауда шифрлері пайда болды. XIX ғасырдың аяғында механикалық Т.Джефферсон мен Ч.Уитстонның шифрлаторлары пайда болды. XX ғасырда ақпаратты үлкен қашықтыққа үлкен жылдамдықпен беруге жаңа мүмкіндіктер пайда болды. Алдымен криптография электрмеханикалық болып, сосын электронға ауысты. XX ғасырдың 20-ші жылдары шифрлау процесін автоматтандыру үшін көп механикалық құрылғылар пайда болды. Сол қатарда роторлы шифрлау машиналар кең қолданылатын. Оларда символдарды ауыстыру үшін механикалық дөңгелектер – роторлар пайдалынатын.

XX ғасырдың ортасында криптографиялық алгоритмдерді кәсіби математиктер мен информатика мамандары жасайтын болды. Криптографияның дамуына елеулі әсер етті американ инженер-математик К.Шеннонның жұмысы «Құпиялы жүйелерде байланыс теориясы» («Теория связи в секретных системах»), онда шифрлердің «ашылмайтын» шарттары тұжырымдалып математикалық дәлелденді.

XX ғасырдың 50-ші жылдарынан криптографияда электронды есептеуіш техника пайдаланады. Блокты деп аталатын шифрлар жасалына басталды, олар ақпаратты бүтін фрагмент немесе блок бойынша өңдеуге мүмкіндік береді. Криптографиялық бағдарламалық және аппараттық құралдар азаматтық мақсат үшін пайдалана басталды, мысалы, ақпаратты беру сауда жүйелерде.

Ежелгі заманда шифрланған хабармен алмасу процесіне тек екі жақ ғана қатысатын, сондықтан шифрлау кілті осы екеуіне ғана керек болатын. Қазіргі ақпараттық жүйелерде ақпаратты беру процесіне көп абоненттер қатысады, оларға әрине шифрлау кілттерді алу үшін сенімді және ыңғайлы арналар қажет. Кілттерді үлестіру проблемасы XX ғасырда шешілді. Ол үшін жаңа шифрлау принципі ойлап табылды – ассиметриялық шифрлау немесе ашық кілті бар шифрлау (XX ғасырдың 70-ші жылдары).

Осы шифрлау әдісті ойлап тапқандар У.Диффи мен М.Хеллман. Ассиметриялық шифрлау алгоритмде арнайы математикалық функциялар пайдалынады – бір жақты функциялар. Ассиметриялық криптожүйелердің ашылуы криптографияның қолдау саласын одан әрі кеңейтті. Ашық кілті бар шифрлау цифрлық қолды құрастырудың және нақтылықты тексерудің негізінде жатыр. Басқа сөзбен айтқанда, банк пластикалық карталардың жұмыс принципі, «электронды» ақша және басқа жаңа технологиялардың негізінде жатыр.

1.6 Криптографиялық шабуылдар

Сақтау, беру және түрлендіру барысында ақпарат әртүрлі шабуылға душар болады. Шабуылды қарсыластар (жаулар, қаскүнемдер және т.б.) жүзеге асырады. Қауіпсіздіктін негізгі бұзулары: ақпараттық құндылықты ашу (конфиденциалдықты жоғалту), автордан рұқсатсыз модификациялау (тұтастықты жоғалту) немесе осы құндылықтарға авторлықсыз қол жетерлікті жоғалту (қол жетімділікті жоғалту).

Шабуылдар пассивті (дәртсіз) және белсенді болу мүмкін. Егер қарсыластар берілетін хабарларды өзгерте алмаса, онда осындай шабуылды **пассивті** деп атайды. Пассивті шабуыл кезінде берілетін хабарларды тек тыңдауға, дешифрлауға және трафикті талдауға болады. **Белсенді** шабуылда қарсылас берілген хабарды өзгерте алады және өзінің хабарларын да қосу мүмкін.

Түрлі шифрдың криптоталдауы хабар мәтінің ерекшелерін еске алмай мүмкін емес.

Криптоталдауда қолданатын мәтіннің ең қарапайым сипаттамалары мұндай: әріптердің, қос әріптердің (биграмма) және жалпы n-граммалардың қайталанғыштығы, дауысты және дауыссыз дыбыстардың кезектесі және кейбір басқалар. Осындай сипаттамалар жеткілікті ұзын мәтіндерді байқаған кезде зерттеледі.

Криптографиялық шабуылдарды қарсыластың криптоталдауы үшін жетімді ақпараттың саны және типі бойынша жіктеуге болады. осы жіктеу бойынша келесі шабуыл түрлерін ажыратады.

Шифрлама (шифрланған мәтін) негізіндегі шабуыл – қарсыластың қолында талдау үшін бір кілтпен шифрланған әртүрлі белгісіз ашық мәтіндердің шифрламасы болғанда. Криптоталдаушының міндеті көбірек хабарлардың ашық мәтіндерін немесе шифрлау кезіндегі пайдаланған кілтті алу. Алынған кілт кейін басқа хабарларды дешифрлауға пайдаланады.

Белгілі ашық мәтін негізіндегі шабуыл – криптоталдаушының қолына бұрын берілген шифрланған хабарларға сәйкес қандай да болса ашық мәтіндер түссе. «Мәтін-шифрлама» қостарды салыстырып, қарсылас құпиялы кілтті білуге тырысады, сосын оның көмегімен келесі барлық хабарларды ашу үшін.

Таңдап алынған ашық мәтін негізіндегі шабуыл – бұл жағдайда криптоталдаушы оған берілген «мәтін-шифрлама» қостардан басқа, өзі де керек мәтіндерді жасай алады және білгісі келген кілт көмегімен оларды шифрлай алады.

Екінші дүниежүзілік соғыс кезінде американдар жапон елшілігінен шифрлау машинаны екі күнге ұрлап әкеткен, сонда олар оның кіреберісіне әртүрлі мәтіндерді жіберіп оған сәйкес шифрлама алатын болатын (бірақ құпиялы кілтті анықтау үшін американдар машинаны бұзбады, әйтпесе оны жапондар байқап барлық кілттерді ауыстырар еді).

Криптография саласындағы мамандар бұрыннан мұндай болжау шығарған болатын – шифрлау алгоритмның құпиялығы оны бұзып ашудан кепілдік бермейді. Онан әрі түсінікті болды: қарсылас шифрлау алгоритмды білсе де шын мәнінде сенімді шифрлау жүйесі қорғалған болып қалу керек. Бұзу әрекетіне беріктікті сақтау үшін жақсы шифрдың кілттін құпиялығы жеткілікті болу керек. Бұл іргелі принципті 1883 жылы алғаш тұжырымдаған Керкхоффс (A.Kerckhoffs) және әдетте **Керкхоффс** принципі деп аталады.

Қазіргі криптографиялық жүйелердің жасаушылары таңдап алынған ашық мәтін бойынша шабуылды болжап тура осы жолды пайдаланады.

1.7 Шифр мысалы

Енді негізгі анықтамаларды бергеннен кейін, бір өте қарапайым шифрлау жүйесін қарастырайық, оның аты «***Юлий Цезарь шифры***». Біздің заманымызға дейінгі I ғасырда өмір сүрген атақты рим императоры бұл шифрды хат алмасу кезінде қолданатын деп есептеледі.

Цезарь шифры қазақ тіліне қатысты мұндай (мысал 1.1). Хабардың әрбір әріптері қазақ әліпбиде бастапқы орыннан үш позицияға әрі тұратын басқа әріппен ауыстырылады.

Сонымен, А әрпі В мен ауыстырылады, Б - Ғ-ға және т.с.с. Ь әріпке дейін. Оны Я мен ауыстырады, сосын Э-ны А-ға, Ю-ны Ә-ға және Я-ны Б-ға.

А **Ә Б В Г Ғ Д Е Ё Ж З И Й К Қ Л М Н Ң О Ө П Р С Т У Ұ Ү Ф Х Һ Ц Ч Ш Щ Ъ Ы І Ь Э Ю Я**

Сурет 1.1. Бастапқы әліпби

Мысалы АУЫСТЫР деген сөз Цезарь әдісімен шифрлағаннан кейін ВФЭҰҮЭУ –ға айналып кетеді.

Бұл әдіс аса күрделі емес, оның үстіне бірнеше сөзден тұратын хабарды шифрлаған кезде бастапқы мәтінде неше сөз болғаны бірден түсінікті болады. Одан басқа, шифрланған хабарда қайталанатың әріптер бойынша талдау жүргізіп тағы бір ақпарат алуға болады. Мысалы, шифрланған ВФЭҰҮЭУ –де бір әріп екі рет кездеседі. Оған қарамастан, Цезарь криптография тарихына кірді, ал оның шифры шифрлау жүйесінің алғашқы мысалы деп саналады.

ВФЭҰҮЭУ хабарды ашып оқу үшін шифрлау алгоритмды ғана білу керек. Шифрлау тәсілді білетін адам құпиялы хабарды оңай ашалады. Сонымен, бұл әдістің кілті алгоритмның өзі болып шығады.

Цезарь шифрын қалай жақсартуға болады? Тыныс белгілерін және тақырды (сөз арасындағы ақ жері) қосып әліпбиді 42 ден 45 символға дейін кеңейтуге болады. Сонда әрбір жеке сөздің ұзындығы жасырылар еді.

Керкхоффс ережесін пайдаланып Цезарь шифрын жақсартайық. Болжамдайық, әріптер оңға қарай үш белгіге емес n ($0<n<33$) белгіге жылжытылсын. Бұл жағдайда шифрлау жүйеде пайда болады кілт – n саны – жылжыту параметрі. Беруші мен алушы бір бірімен келісіп, кілт мәнін кейде өзгерте алады. n мәні әртүрлі болғандықтан, тек алгоритмды білгені қарсыласқа құпиялы хабарды дешифрлауға мүмкіндік бермейді.

Хабардың мазмұнын білу үшін қаскүнем не істеу керек? Мысалы, орыс тіліндегі құпиялы хабар ЧСЮЭЮЪ қолға түссін. Қарсыласқа белгілі болсын - кілт (жылжыту параметрі n) 1 ден 32-ге дейін мән алай алады. Құпиялы кілттің мәнін табу үшін біз шифрлама бойынша шабуыл жүргіземіз. Барлық мүмкін болатын кілттерді кезек-кезек таңдау тәсілін қарастырайық (бұл «дөрекі күш» деп аталатын әдіс). Әрбір әріпті 1, 2, 3,..., 32 позицияға сәйкес жылжытумен алынатын варианттарды 32 жолға жазайық. Бұл операцияны қолмен де жазуға болады, немесе n параметрдің барлық таңдау варианттарын файлға жазатын қарапайым программа құруға болады. Осы 32 жолдарынын біреуінде бастапқы хабар табылады (кесте 1.1).

Кесте 1.1. Цезарь әдісін пайдалану кезінде кілтті іздеу үшін варианттарды таңдау Ұстап

алынған криптограмма ЧСЮЭЮЪ			
1	ШТЯЮЯЫ	17	ЗВОНОК
2	ЩУАЯАЬ	18	ИГПОПЛ
3	ЪФБАБЭ	19	ЙДРПРМ
4	ЫХВБВЮ	20	КЕСРСН
5	ЬЦГВГЯ	21	ЛЁТСТО
6	ЭЧДГДА	22	МЖУТУП
7	ЮШЕДЕБ	23	НЗФУФР
8	ЯЩЁЕЁВ	24	ОИХФХС
9	АЪЖЁЖГ	25	ПЙЦХЦТ
10	БЫЗЖЗД	26	РКЧЦЧУ

11	ВЬИЗИЕ	27	СЛШЧШФ
12	ГЭЙИЙЁ	28	ТМЩШЩХ
13	ДЮКЙКЖ	29	УНЪЩЪЦ
14	ЕЯЛКЛЗ	30	ФОЫЪЫЧ
15	ЁАМЛМИ	31	ХПЬЫЬШ
16	ЖБНМНЙ	32	ЦРЭЬЭЩ

Кестеден көрініп тұр мағыналы бір сөз ғана бар – ЗВОНОК. Бұл сөз 17 орында. Сондықтан, шифрланған мәтінді 17 позицияға алға жылжытса ашық мәтін алынады. Демек, шифрланған мәтінді алу үшін ашық мәтінді (33-17)=16 позицияға жылжыту керек. Сонымен, табылған кілт n=16.

Басқа жолдарда мағыналы хабар болмағандықтан, біз бұл хабарды дұрыс аштық. Бірақ, ол үшін бастапқы хабар табиғи тілде (біздің мысалда – орыс тілі) құрастырылу керек және белгілер саны бес-алтыдан артық болу керек. Егер де хабар өте қысқа болса, мүмкін шешімдері бірнеше болу мүмкін. Бір ғана шешімді табуға өте қиын, егер бастапқы хабар цифрден тұратын болса.

Мысалы, бастапқы әліпби араб цифрлерден тұрсын, яғни 0

1 2 3 4 5 6 7 8 9.

Абоненттің біреуі басқаға бес цифрден тұратын және 12345 -ке тең құлыптын құпиялы кодын бергісі келді. Жіберуші мен алушы алдын ала келісті – шифрлау кілті n=3 болсын. Жіберуші осы кілтпен бастапқы хабарды 12345 шифрлап алады 45678 және алынған мәнді абонентке жібереді. Қаскүнем криптограмманы ұрлап алып кезек-кезек таңдау әдісті пайдалансын. Бастапқы әліпби 10 символдан тұрғандықтан, кілт мәні 1-ден 9 аралығында жатады. Бұрынғыдай, әрбір белгіні 1, 2, 3,..., 9 позицияға жылжытып, барлық варианттарды жазайық (кесте 1.2).

Кесте 1.2. Құлыптын шифрланған кодын ашу үшін варианттарды таңдау

Ұстап алынған криптограмма 45678	
1	56789
2	67890
3	78901
4	89012
5	90123
6	01234
7	12345
8	23456
9	34567

Көрініп тұр, барлық алынған варианттардың маңызы бірдей және қаскүнем түсіне алмайды – қай комбинация дұрыс. Шифрламаны талдап, ол құпиялы кілт мәнің табалмайды.

Бірінші мысалда хабар – орыс тілінде, сондықтан ол көпшілік ережелерге бағынады, әртүрлі әріптердің және олардың тіркестерінің түрлі ықтималдығы бар, және кейбір әріптерге жалпы тыйым салынған (бұл қасиет мәтіннің артықшылығы деп аталады). Сондықтан кілтті табуға және хабарды ашуға оңай болды, яғни артықшылық шифрды «бұзуға» мүмкіндік берді. Ал екінші мысалда цифрлердің барлық комбинациясы орын алу мүмкін. Кодты құлыптың «тілінде» артықшылық жоқ. Сондықтан, шифр қарапайым болса да, шифрлама бойынша шабуыл кезінде ол ашылмайтын болады. Егер

біз шабуылды ашық мәтін бойынша да жүргізе алсақ, яғни қолымызда «ашық хабар» - «шифрланған хабар» жұбы болса, онда ашуы әбден оңай болады.

Келтірілген қарапайым мысалдар көрсетіп отыр - табысты криптоталдаудың ықтималдығы көп факторларға тәуелді: шифрлау жүйесіне, ұстап алынған хабардың ұзындығына, бастапқы хабардың тілі мен алфавитіне.

1.8 Криптографиялық протокол

Қазіргі криптографияда шифрлерді жасаудан және зерттеуден басқа көп назар аударылады криптографиялық протоколдарды әзірлеуге.

Криптографиялық протокол – криптографиялық құралдарды пайдаланып екі немесе одан көп абоненттердің өзара әрекеттесу процедурасы, оның нәтижесінде абоненттер өзінің мақсатына жетеді, ал олардың қарсыластары – жетпейді. Протоколдың негізінде ақпараттық процестердегі криптографиялық өзгерістер мен алгоритмдердің пайдалануын регламенттейтің ережелер жиынтығы жатыр. Әрбір криптографиялық протокол белгілі бір есепті шешуге арналған.

Кез келген протоколдың келесі қасиеттері бар:

- протоколды орындаған кезде іс-әрекеттің реті маңызды; әрбір іс-әрекет алдағы аяқталғаннан кейін өзінің ретімен орындалу керек;
- протокол қайшы болмау керек;
- протокол толық болу керек, яғни әрбір мүмкін болатын жағдайы үшін сәйкес іс-әрекет ескерілу керек.

Протокол қасиеттері информатикадан белгілі алгоритм қасиеттеріне ұқсайды. Шынында да, протокол – бұл белгілі жағдайда бірнеше тараптардың іс-әрекеттесу алгоритмы. Протокол қатысушылары протоколды білу керек және оның барлық кезеңдерін толық орындау керек. Криптографиялық протоколдың қатысушылары әдетте кейбір байланыс жүйенің абоненттері. Протокол қатысушылары бір біріне сенбеу мүмкін, сондықтан криптографиялық протоколдар оның қатысушыларын сыртқы жаудан ғана емес, серіктестердің арамдық іс-әрекетінен де қорғау керек

Криптографиялық протоколдардың типтерін шартты екі топқа бөлуге болады: қолданбалы және қарадүрсін протоколдары. Қолданбалы протокол тәжірибеде кездесетін нақты есепті шешуге арналған. Қарадүрсін протоколдар қолданбалы протоколдарды әзірлеген кезде «құрылыс блоктар» сияқты пайдаланады. Біз оқу құралында тек қарадүрсін протоколдарды қарастырамыз.

Кейбір протокол түрлерінің міндетін қарап шығайық.

1. ***Хабарларды конфиденциал беру протоколы***. Хабарларды конфиденциал берудің міндеті келесі. Байланыс желінің абоненты болатын протоколдың екі қатысушысы бар. Қатысушылар кейбір байланыс жолымен қосылған, ол бойынша хабарды екі жаққа жіберуге болады. Байланыс жолды қарсылас бақылау мүмкін. Абоненттің біреуінде конфиденциал хабар *m* бар, осы хабарды конфиденциал түрде екінші абонентке беру керек. Осындай протокол типі бірінші пайда болған.
2. ***Аутентификация және идентификация протоколдары***. Олар кейбір ақпаратқа рұқсатсыз қатынауды және пайдаланушылардың өкілеттігі жоқ қорларға қатынауды болдырмауға арналған. Кәдімгі қолдану саласы – кейбір үлкен ақпараттық жүйенің қорларына пайдаланушылардың қол жетімділігін ұйымдастыру.
3. ***Кілттерді үлестіру протоколы*** – шифрланған хабарлармен алмасудағы қатысушыларды құпиялы кілттермен қамтамасыз ету үшін қажетті.
4. ***Электронды цифрлық қол протоколы*** – қағаз құжаттардағы кәдімгі қол сияқты электронды құжаттарға қол қоюға мүмкіндік береді. Протокол орындалу нәтижесінде, берілетің ақпараттың авторлық тексеруін қамтамасыз ететің, оған бірегей сандық қосымша қосылады.

5. ***Қадағалмауды қамтамасыз ететін протоколы*** («Электронды ақша»).

Криптографияда электронды ақша деген қадағалмауды қамтамасыз ететін (яғни ақпаратты тасымалдау көзін қарап жүруге мүмкін еместігі) электронды төлем құралдарды айтады.

Екі тараптын арасында конфиденциал хабарлармен алмасудың қарапайым протоколын қарастырайық, тараптарды абонент №1 және абонент №2 деп атайық. Абонент №1 шифрланған хабарды абонент №2 –ге бергісі келсін. Бұл жағдайда олардың іс-әрекет тізбегі мұндай болу керек.

1. Абоненттер шифрлау жүйесін таңдайды (мысалы, *n* позицияға жылжытуы бар Цезарь шифры).
2. Абоненттер шифрлау кілті туралы келіседі.
3. Абонент №1 бастапқы хабарды таңдалған әдіс арқылы кілт көмегімен шифрлайды және шифрланған хабарды алады.
4. Шифрланған хабар абонент №2 –ге жіберіледі.
5. Абонент №2 шифрланған хабарды кілт көмегімен ашады және ашық хабарды алады.

Бұл протокол оңай, бірақ ол шынында тәжірибеде пайдалану мүмкін. Криптографиялық протоколдар міндетіне байланысты қарапайым да күрделі де болу мүмкін.

Алдында біз криптографиялық шабуыл анықтамасын енгіздік және криптографиялық алгоритмге шабуылдар типтерін қарап шықтық. Көп жағдайда шабуыл шифрлау алгоритмге емес протоколға бағытталу мүмкін. Сондықтан, абсолют сенімді шифрлау алгоритмының бар болуы байланыс жүйенің абоненттеріне толық қауіпсіздікті кепілдей алмайды. Сол себептен қазіргі уақытта мамандар криптографиялық протоколдарды ұқыпты талдайды.

Негізгі терминдер

Ciphertext – шифрланған хабар (жабық мәтін, криптограмма).

Deciphering – шифрды ашу (дешифрлау).

Enciphering – ашық мәтінді криптограммаға түрлендіру (шифрлау).

Plaintext – бастапқы хабар немесе ашық мәтін.

Белсенді криптографиялық шабуыл – осындай шабуылда қарсылас берілген хабарларды өзгерте алады және өзінің хабарларын қосу мүмкін.

Әліпби (алфавит) – ақпаратты кодтау үшін пайдаланатын символдардың шекті көптігі.

Кілт – хабарларды шифрлауға және дешифрлауға қажетті ақпарат.

Криптоталдау – ақпараттың криптографиялық қорғауын жеңіп алу туралы ғылым.

Ақпаратты қорғаудың криптографиялық жүйесі – деректерді шифрлау үшін криптографиялық әдістерді пайдаланатын ақпаратты қорғау жүйесі.

Криптографиялық протокол – криптографиялық құралдарды пайдаланып екі немесе одан көп абоненттердің өзара әрекеттесу алгоритмы, оның нәтижесінде абоненттер өзінің мақсатына жетеді, ал олардың қарсыластары – жетпейді.

Криптография шифрлау жүйелерінің құруын және пайдалануын зерттейді, соның ішінде түрлі ашу әдістер жөнінде олардың беріктігін, осал жерін және осалдық дәрежесін.

Криптоберіктік – кілтті білмегенде дешифрлауға беріктікті анықтайтын шифр сипаттамасы (яғни криптоталдауға қарсы тұру қабілеті).

Пассивті криптографиялық шабуыл - қарсыластар берілетін хабарларды өзгертуге мүмкіндігі болмағандағы шабулы. Пассивті шабуыл кезінде берілетін хабарларды тек тыңдауға, дешифрлауға және трафикті талдауға болады.

Керкхоффс принципы – криптографиялық жүйелерді құрастыру ережесі, оған сәйкес құпиялы түрде шифрлау кілті сақталынады, ал шифрлау жүйесінің басқа параметрлері, алгоритмның беріктігін төмендетпей, ашық та болу мүмкін. Басқа сөзбен,

шифрлаудың сенімділігін бағалаған кезде қарсылас пайдаланатын шифрлау жүйесі туралы, қолданылатын кілттерден басқа, бәрін біледі деп ойлаймыз. Бұл принципті XIX ғасырда алғаш тұжырымдаған голланд криптографы Огюст Керкхоффс.

Символ – кез келген белгі, соның ішінде әріп, цифр немесе тыныс белгісі.

Шифрлау жүйесі немесе **шифржүйесі** – хабардың мәтінің қайтымды өзгерту үшін

(жолданған адамнан басқа барлықтарға мәтін түсініксіз болсын оймен) пайдаланатын кез келген жүйе.

Шифр – бастапқы құпиялы хабарды қорғау үшін оның алдын ала айтылған түрлендіру тәсілдерінің жиынтығы.

Жабық кілті бар шифрлау (симметриялық шифрлау) - деректерді қайтымды түрлендіру әдісі, оларда ақпараттық алмасудың екі жағы да жаудан жасырып сақтайтын бір кілтті ғана пайдаланады. Тарихтан танымал барлық шифрлар, мысалы Цезарь шифры – бұл жабық кілті бар шифрлар.

Ашық кілті бар шифрлау (ассимметриялық шифрлау) - деректерді шифрлау және дешифрлау үшін екі әртүрлі кілтті пайдаланатын шифрлау әдістері. Мұнда кілттердің біреуі (ашық кілт) ашық (қорғалмаған) арна арқылы берілу мүмкін.

Электронды (цифрлық) қол - криптографиялық түрлендіру көмегімен алынған хабарға қосылатың деректер блогы. Мәтінді алған кезде электронды қол хабардың авторлығы мен нақтылығын тексеруге мүмкіндік береді.

ОБМӨЖ тапсырмалары:

Ақырлы өрістердегі келтірілмейтін көпмүшеліктер.

Ақырлы өрістердің примитивті элементтері.

Модулярлық арифметика.

Дискретті логарифмдер

Фурьенің дискретті түрлендірілулері.

МӨЖ тапсырмалары:

Салыстырулар теориясы.

Қалдықтар туралы қытай теоремасы.

Эйлер және Ферма теоремалары.

Ақырлы өрістер.

Ақырлы өрістерді құру.

Сұрақтар

1. Қандай проблемаларды шешу үшін криптографиялық әдістер пайдалану мүмкін?
2. Криптографияның стеганографиядан айырмашылығы неде?
3. Қазіргі криптография қандай міндеттер шешеді?
4. Ақпаратты қорғаудың криптографиялық жүйесіне қойылатын талаптарды айтып

беріңіз.

5. Келесі ұғымдардың анықтамаларын беріңіз: әліпби, криптограмма, криптографиялық жүйе, криптографиялық протокол, символ, шифр, электронды (цифрлық) қол.
6. Цезарь әдісімен шифрлаудың ережесін қандай?
7. Кодты құлып үшін коды бар криптограмманы неге ашуға болмайды?
8. Неге ақпараттық жүйелерде криптографиялық әдістерді пайдалану проблемасы қәзіргі уақытта өте маңызды болды?
9. Криптографиялық шабуыл деген не?
10. Криптографиялық шабуылдардың қандай типтері бар?
11. Криптографиялық протокол деген не?

12. Келесі криптографиялық протоколдардың міндетін
    - түсіндіріңіз: конфиденциал хабарлармен алмасу;
    - электронды цифрлық қолды жасау; кілттерді үлестіру.
    -

Әдебиеттер

1. Бабаш А.В. Информационная безопасность. Лабораторный практикум: Учебное пособие / А.В. Бабаш, Е.К. Баранова, Ю.Н. Мельников. - М.: КноРус, 2013. - 136 с.
2. Гафнер В.В. Информационная безопасность: Учебное пособие / В.В. Гафнер. - Рн/Д: Феникс, 2010. - 324 с.
3. Громов Ю.Ю. Информационная безопасность и защита информации: Учебное пособие / Ю.Ю. Громов, В.О. Драчев, О.Г. Иванова. - Ст. Оскол: ТНТ, 2010. - 384 с.
4. Ефимова Л.Л. Информационная безопасность детей. Российский и зарубежный опыт: Монография / Л.Л. Ефимова, С.А. Кочерга. - М.: ЮНИТИ-ДАНА, 2013. - 239 с.
5. Партыка Т.Л. Информационная безопасность: Учебное пособие / Т.Л. Партыка, И.И. Попов. - М.: Форум, 2012. - 432 с.
6. Петров С.В. Информационная безопасность: Учебное пособие / С.В. Петров, И.П. Слинькова, В.В. Гафнер. - М.: АРТА, 2012. - 296 с.
7. Семененко В.А. Информационная безопасность: Учебное пособие / В.А. Семененко. - М.: МГИУ, 2010. - 277 с.
8. Шаньгин В.Ф. Информационная безопасность компьютерных систем и сетей: Учебное пособие / В.Ф. Шаньгин. - М.: ИД ФОРУМ, НИЦ ИНФРА-М, 2013. - 416 с.
9. Ярочкин В.И. Информационная безопасность: Учебник для вузов / В.И. Ярочкин. - М.: Акад. Проект, 2008. - 544 с.
10. Төкеев У.А., Ахметов Б.Б. Ақпараттық қауіпсіздікті басқару: Оқу қуралы. – Алматы: Қазақ университеті, 2011 – 161б.
11. Тұрым А.Ш., Мұстафина Б.М. Ақпарат қорғау және қауіпсіздендіру негіздері.- Алматы.:АЭжБИ, 2002ж.

Жаттығулар

1. Цезарь шифрдың кілтін анықтандар, егер келесі жұптар «ашық мәтін – шифрлама» белгілі болса (бастапқы әліпби:
АБВГДЕЁЖЗИЙКЛМНОПРСТУФХЦЧШЩЪЫЬЭЮЯ):
    - АПЕЛЬСИН - ТВЧЮОДЫА
    - МАНДАРИН – ТЁУЙЁЦОУ
2. Цезарь шифры көмегімен шифрланған келесі хабарларды ашыңыз және n ($0<n<33$)

кілттіанықтаңыз.Бастапқыхабарлармұндайәліпбиденқұрастырылған
АБВГДЕЁЖЗИЙКЛМНОПРСТУФХЦЧШЩЪЫЬЭЮЯ:

- ЮВПЛШУХ
- СФЫЮБШЯФУ