Қазақстан Республикасының білім және ғылым министрлігі

С. Торайғыров атындағы Павлодар мемлекеттік университеті

Есептеу техникасы және бағдарламау кафедрасы

АҚПАРАТТЫҚ ҚАУІПСІЗДІК НЕГІЗДЕРІ

Зертханалық сабақтарға арналған
Әдістемелік нұсқау

Павлодар

ФСО ПОУ 7.18.1/05

БЕКІТЕМІН

ФМжАТ Деканы

_____С.К.Тлеукенов

_____8_____200_7_ж.

Құрастырған: аға оқытушы Кишубаева Алтынай Тулпаровна _____
(қолы)

Есептеу техникасы және бағдарламау кафедрасы

Әдістемелік нұсқау

Зертханалық сабақтарға арналған
"Ақпараттық қауіпсіздік негіздері" пәні бойынша «050704» «Есептеу техника және бағдарламалық камтама» мамандығының күндізгі оқу формасы бойынша жалпы орта білім негізінде окитын студенттер үшін

Кафедра мәжілісінде ұсынылған № _1_ хаттама 200_7_ж "_30_" _08_

Кафедра меңгерушісі _____ О. Г. Потапенко
(қолы)

"Физика, математика және ақпараттық технологиялар" факультетінің оқу әдістемелік кеңесінде макұлданды
"_31_" _08_ 200_7_ ж. хаттама №_1_

ӘК төрағасы _____ А.З. Даутова
(қолы)

ТҮПНҰСҚА
ПОДЛИННИК

1. Криптография: негізгі ұғымдар

Компьютерлер мен автоматтандырылған ақпарат құралдарының пайда болуы және дамуына байланысты файлдар мен компьютерлер сақтайтын басқа да ақпараттарды қорғайтын автоматтандырылған құрылғылар қажет бола бастады. Қорғау құрылғылары, әсіресе, коптұтынушы жүйелерде, мысалы, уақытты бөлу жүйелері, сонымен қатар, қарапайым телефон желілері мен ашық компьютерлер буындарына жол ашатын жүйелерде аса қажет. Сондықтан мәліметтерді сақтау және хакерлерге қарсы бағытталған құрылғылар мен әдістер жиынтығына ***компьютерлік қауіпсіздік*** термині қолданыла бастады.

Желілер мен коммуникацияларды сақтау құралдарының автоматтандырылған түрінін ен маныздысы – шифрлау болып саналады.

Конфиденциалды жеткізілу керек болатын хабарламаны ***ашық мәтін*** деп атайды. Ашык мәтінді бөтенге түсініксіз етіп ыкшамдау үрдісін ***шифрлау*** деп атаймыз. Шифрлау арқылы хабарламадан ***шифрмәтін*** шығады. Шифрмәтінге қарама-қарсы үрдісті ***дешифрлау*** дейміз.

Ақпаратты сақтау максатымен ыкшамдау әдістері зерттейтін ғылым «Криптография» деп аталады.

1- сурет арқылы шифрлау сүлбесінің элементтерін карастырайык. Акпарат көзі хабарламаны

ашық мәтін $X=[X_1,X_2,\ldots, X_M]$ түрінде шығарады. X ашық мәтіннің X_i элементтері әліпби соңы түрінде болады. Шифрлау үшін $K=[K_1,K_2,\ldots, K_d]$ түріндегі кілт қолданылады. Алғашқы берілген X және шифрлау кілті K арқылы $Y=[Y_1,Y_2,\ldots, Y_N]$ шифрлық мәтін құрылады. Мұны

$$Y=E_K(X)$$

формуласы аркылы жазуға болады.

Бұдан Y шифрлау алгоритмі E_K-ны X ашық мәтініне K кілті арқылы қолданғаннан шығады.

Кез-келген хабарламаны алушы K кілтті қолданып, кері ықшамдау

$$X=D_K(Y)$$

жасай алуы тиіс.

Y-пен танысуға мүмкіндігі бар, бірақ K және X-ті қолдана алмайтын қарсылас, X және K-ны қайта құруға тырысуға мүмкін. Бұнда қарсылас шифрлау алгоритмі (E) және дешифрлау алгоритмін (D) білетіні көзделген. Егер қарсылас бір ғана белгілі хабарламаны білуге тырысса, онда оған бір ғана бар күшін X-ті X' ашық мәтіні арқылыкайта құруға кажет. Бірақ көбіне қарсылас барлықтиісті хабарламаларды оқуға тырысады. Бұл үшін оған K-ны оған ұксас K' алғашқы кілті арқылы қайта құру кажет.

X немесе K, не болмаса, екеуінің де қайта құрылу үрдісін *криптоанализ* дейміз. Криптоанализбен айналысатын адамды *криптоаналитик* деп атайды.

2. Криптографикалық жүйелер классификациясы

Криптографикалық жүйелер классификациясы келесі үш тәуелсіз мінездемелер негізінде құрылады:

1. **Ашық мәтінді шифрланған мәтінге ықшамдау операциясының типі**. Барлық шифрлау алгоритмдері екі операцияға негізделеді: айырбастау, яғни ашық мәтіннің (бит, әріп, биттер тобы немесе әріптер тобы) әрбір элементін қайсыбір баска элементпен ауыстыру, және орынауыстыру, яғни ашық мәтіннің элементтер тәртібінің өзгерісі. Сондағы басты сұраныс ақпаратты жоғалтуының жоқтығында (яғни барлық үрдістердің қайтарымдылығы). Шифрлау жүйелерінің көпшілігінде бір емес бірнеше айырбастау мен орынауыстыру операцияларының комбинациясы қолданылады. Тиісті шифрлар өнімді деп аталады.
2. **Қолданылатын кілттер саны.** Егер жіберуші мен алушы бір ғана кілт қолданса, онда жүйе симметриялы, бір кілтті жүйе, құпия кілтті немесе әдеттегі шифрлау сүлбесі деп аталады. Егер жіберуші мен алушы әртүрлі кілттер қолданса, онда жүйс симметриялы емес, екі кілтті жүйс немесс ашық кілтті шифрлау сүлбесі деп аталады.
3. **Ашық мәтінді өңдеу әдісі.** *Блокты шифрлау* ашық мәтінді блоктармен өңдеуді көздейді, яғни өңдеу нәтижесінде әр блоктан шифрланған мәтін пайда болады. *Ағымды шифрлау* (Поточное шифрование) ашық мәтіннің барлық элементтерін шифрлауды айтады. Нәтижесінде әр деңгейде шифрланған мәтіннің бір элементі пайда болады.

3. Шифрлаудың классикалық техникасы

3.1. Ауыстырудың қолданылуы

Ауыстыру кезінде ашық мәтіннің жеке әріптері басқа әріптер, сандар немесе баска таңбалармен айырбасталады. Егер ашық мәтін биттер тізбегі ретінде қарастырылса, онда ауыстыру ашық мәтіннің биттер тізбегін шифрланған мәтіннің биттер тізбегіне айырбастауға сәйкес келеді.

Цезарь шифрі

Ең ежелгі және ең карапайым ауыстыру шифрі болып, Юлий Цезарь колданған шифр табылады. Цезарь шифрінде әліпбидің әрбір әрпі осы әліпбидің үш орынға кері орналасқан әрпіне айырбасталады. Сонда әліпби «циклді» болып табылады, яғни Я әрпінен кейін А әрпі келеді. Мысалы:

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

Ашық мәтін:	К Р И П Т О Г Р А Ф И Я
Шифрланған мәтін:	Н У Л Т Х С Ж У Г Ч Л В

Ықшамдауды барлық нұсқаларды қарастыру арқылы анықтауға болады.

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

Егер әрбір әріпке сандық мән берсек (А = 1, Б = 2 және т.с.с.), онда шифрлау алгоритмін келесі формула арқылы көрсетуге болады. *P* ашық мәтіннің әрбір әрпі, шифрленген *C* мәтіннің әрпіне айырбасталады:

$$C = E(P) = (P+3) \bmod (26).$$

Жалпы түрде ауысу кез-келген болуы мүмкін, сол себепті Цезарь алгоритмі

$$C = E(P) = (P+k) \bmod (26),$$

формуласы арқылы жазылады. Мұндағы *k* 1-ден 31 аралығындағы санды қамтиды. Дешифрлау алгоритмі де өте карапайым:

$$P = D(C) = (C-k) \bmod (26).$$

Егер бір мәтін Цезарь шифрі арқылы шифрленгені белгілі болса, онда оны карапайым барлық нұсқаларды тексеру арқылы онай табуға болады. Тек 31 мүмкін нұсқаны тексеру қажет.

Барлық нұсқаларды тізбектей тексеру әдісі үш маңызды мінездемемен анықталады:

1. Шифрлеу және дешифрлеу алгоритмдері белгілі.

2. Тек 31 нұсқаны тексеру керек.

3. Ашық мәтіннің тілі белгілі және оңай танымал.

Компьютерлі акпаратты қорғау туралы сөз болған көп жағдайда, алгоритм белгілі деп ойлауға болады. Тізбектеп тексеру әдісі негізіндегі криптоанализді мүмкін етпейтін жалғыз жай, ол – аса көп кілттерді тексеруге тиіс алгоритм.

Моноалфавитті шифр

31 нұсқасы бар Цезарь шифрін қорғалған деп айтуға болмайды. Кілттер кеңістігін кеңейтілуін, кез-келген ауыстыруды рұқсат ету арқылы қамтамасыз етуге болады.

Мысалы: егер Цезарь шифрінде кез-келген 31 таңбаның ауысуын *k* таңбасының көшуін ғана емес қолдансақ, онда біз 31! аламыз. Мысалы:

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

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

Осындай кілтті қолдану арқылы шифрлаудың мысалы:

Ашық мәтін:	К	Р	И	П	Т	О	Г	Р	А	Ф	И	Я
Шифрленген мәтін:	Ф	Ю	В	Ч	Ц	С	Ь	Ю	Й	Э	В	З

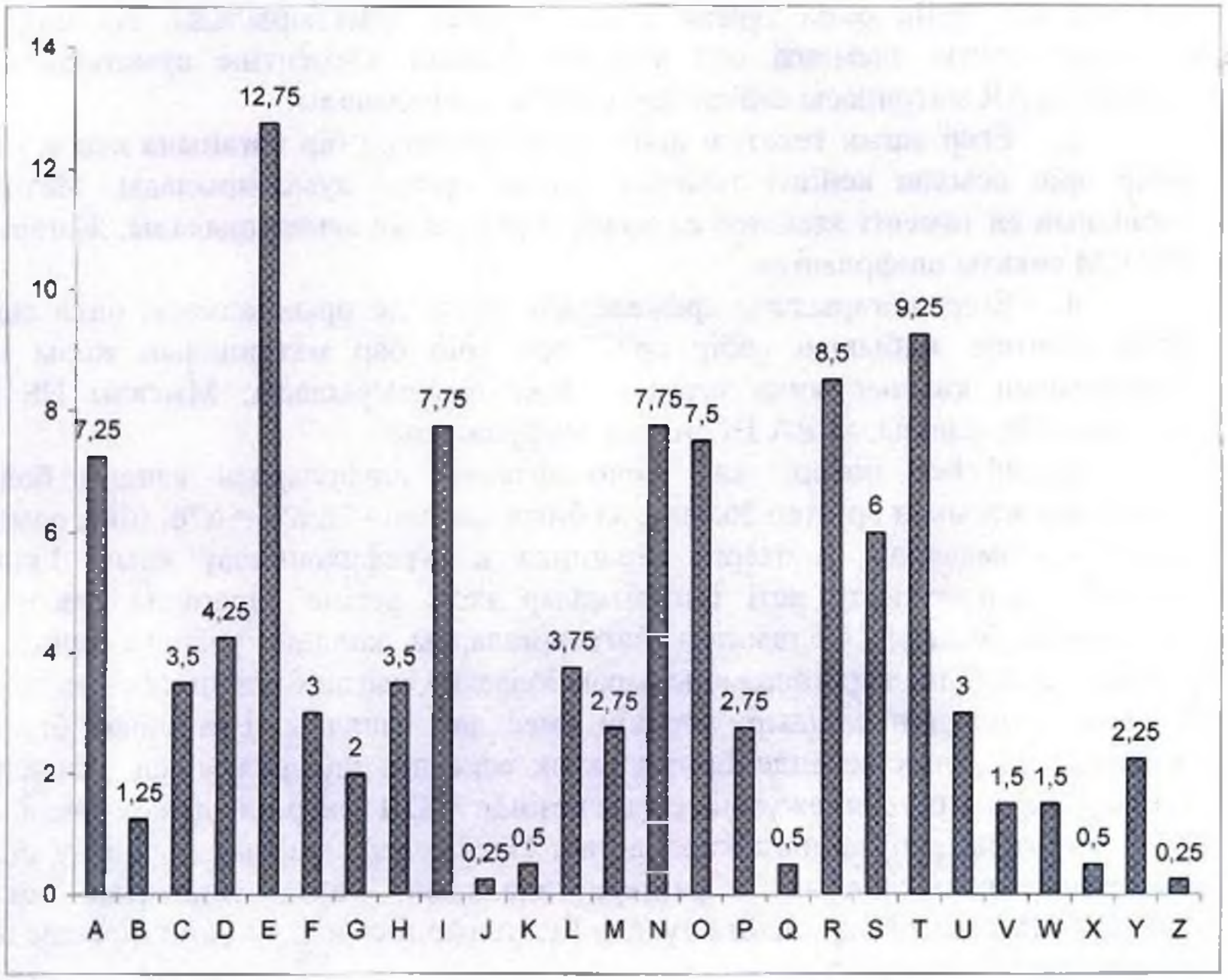
31! Кілт екен деп ойлауға болады (бұл $8x10^{33}$ артық), оны тез тексеріп көруге болады. Бірақ криптоаналитиктер басқа да жолдар бар. Егер криптоаналитик ашық мәтіннің шығу табиғатын (мысалы, мәтін ағылшын тілінде) білсе, онда тиісті тілдерге қолданылатын танымал ерекшеліктері туралы ақпаратты колдануға болады.

2-суретте ағылышын тіліндегі мәтінде әріптерді қолдану жиілігі көрсетілген. Ашық мәтіндегі әрбір әріп, кілттегі әрбір әріпке сәйкес келетіндіктен, криптоаналитик бірінші сатыда шифрланған мәтінде қолданылған әріптердің жиілігін және әліпби мен шифрмәтін арасындағы сәйкестіктерді анықтайды (Мысалы, 2-суреттің диаграммасына сәйкес, шифрмәтінде жиі қолданылатын әріп Е). Әрі қарай ағылшын тілінде жиі қолданылатын триграмма the, яғни бұл ашық мәтіннің бөлігін қайта құруға және қолдану кілтін тексеруге мүмкіндік береді. Нақты мәтіннің мазмұнын анализді жалғастыру арқылы алуға болады.

Моноалфавитті шифрлер тез ашылады, себебі түпнұсқа әліпбидің әріптерін жиілігін иемденеді. Берілген жағдай үшін контрөлшем болып, бір әріп үшін бірнеше ауыстырғыш (омофон) қолданылады. Егер ауыстырғыш таңба саны, осы әрінтің шығу жиілігіне пропорционалды таңдалған болса, онда әріпті қолдану жиілігін шифрленген мәтінде санау мүмкін болмайды. Омофондарды қолдансақ та, әрбір ашық мәтіннің элементіне, тек бір ғана шифрленген мәтіннің элементі сәйкес келеді, сондықтан соңғысында бірнеше әріптің

кайталану жиілігі көріну керек. Нәтижесінде криптоанализ мақсаты қарапайым болып қалады.

Айырбастау әдісі арқылы шифрленген мәтінде, алғашқы мәтін құрылысы аз көрінуі үшін екі бір-біріне ұқсас емес жол таңдауға болады. Бірінші жолда ашық мәтіннің жеке таңбаларын ауыстыру емес, ал бірнеше танбалар комбинациясын қолдану қолдану қажет. Ал екінші жол бірнеше әліпбиді қолдануды көздейді.



Плейфейер шифры

Ең белгілі шифрлардың бірі. Көп әріпті шифрлар тәсілі негізінде салынған. Плейфейер шифрында ашық текстті блограммалар шифрлы текстті блограммаларға келтірілген бірліктер ретінде қарастырылады.

Плейфейер алгоритмі кілтті сөз негізінде құрылған, 5х5 көлемді әріптер матрицасын қолдану негізінде құрылған. Матрица кілтті сөзде қолданылатын әріптердің орналасу жолымен құрылады. Бұл әріптер реті солдан оңға қарай және биіктен төменге қарай. Одан кейін алфавиттің калған әріптері нақты ретпен калған матрицаның жолдары мен бағандарында орналасады. I мен J

әріптері бір әріп болып саналады. Төменде monarchy (монархия) кілтті сөзінің матрицасы мысал ретінде келтірілген.

Ашық текст 2 әріпті порциямен келесі ережеге сәйкес шифрланады.

1. Егер ашық тексттің бірдей әріптері шифрлау үшін бір жұп құрса, онда бұл әріптердің арасына әдейі әріп-толықтаушы қойылады. Мысалы X. Мысалы balloon сөзі ba lx lo on.

2. Егер ашық текст әріптері матрицаның бір жолына келсе, онда әрбір әріп осыдан кейін онда тұрған келесі әріппен ауыстырылады. Ал матрица жолының соңғы элементі сол жолдың бірінші элементіне ауыстырылады. Жоғарыда AR матрицасы сәйкес RM сияқты шифрланады.

3. Егер ашық тексттің әріптері матрицаның бір бағанына келсе, онда әрбір әріп осыдан кейінгі төменде тұрған әріпке ауыстырылады. Матрица бағананың ең төменгі элементі ең жоғары элементке ауыстырылады. Жоғарыда MU CM сияқты шифрланған.

4. Егер жоғарыдағы ережелердің біреуі де орындалмаса, онда ашық мәтін әріптері жұбының әрбір әріпі осы әріп бар матрицаның жолы мен бағанасының қиылысуында тұрған әріпке ауыстырылады. Мысалы HS BP сияқты шифрланады, ал EA JN сияқты шифрланады.

Плейфейер шифрі жай моноалфавитті шифрлардан сапалы болып келеді. Бір жағынан әріптер 26 ғана, ал биграммалар - 26x26 = 676, міне, осыдан ғана биграммаларды әріптерге қарағанда идентификациялау киын. Екінші жағынан әріптер келу реті биграммалар келу ретіне қарағанда үлкенірек диапазонда болады. Сондықтан биграммаларды қолдану анализі әріптерді қолдану анализына қарағанда қиынырақ болады. Осыған байланысты көп уақыт Плейфейер шифрін сындыру мүмкін емес деп саналды. Бұл шифр бірінші дүниежүзілік соғыс кезінде Британиялық әскердің шифрлауының стандарты болды және екінші дүниежүзілік соғыс кезінде АҚШ әскерінде де қолданды.

Жоғары репутацияға қарамастан, Плейфейер шифрын сындыру оңай. Көптеген статистикалық характеристикаларын сақтайтындықтан, онын шифрланған текстін оку оңайға түседі. Бұл шифрді сындыру үшін бірнеше жүз әріптен тұратын текст керек.

Хилл шифрі

1929 жылы математик Лестер Хиллмен (Lester Hill) ұсынылған көп әріпті шифр да қызык болды. Ол мына алгоритммен өтеді: әрбір m ретті ашык мәтін әріптері шифрланған тексттін m әріптерімен ауыстырылады. Әрбір символға цифрлық мән берілетін m сызыкты өрнектермен бұл шифр анықталады (A=0, B=1,..., Z=25). Мысалы m=3 болғанда келесі өрнектер жүйесін аламыз:

$$C_1 = (k_{11}p_1 + k_{12}p_2 + k_{13}p_3) \bmod 26.$$
$$C_2 = (k_{21}p_1 + k_{22}p_2 + k_{23}p_3) \bmod 26.$$
$$C_3 = (k_{31}p_1 + k_{32}p_2 + k_{33}p_3) \bmod 26.$$

Бұл жүйсні вектор мсн матрицаның көбейтіндісі ретінде келесідей жазуға болады:

$$\begin{pmatrix} C_1 \\ C_2 \\ C_3 \end{pmatrix} = \begin{pmatrix} k_{11} & k_{12} & k_{13} \\ k_{21} & k_{22} & k_{23} \\ k_{31} & k_{32} & k_{33} \end{pmatrix} \times \begin{pmatrix} p_1 \\ p_2 \\ p_3 \end{pmatrix}$$

немесе мына түрде

$$\mathbf{C = K \times P},$$

мұндағы **C** мен **P** - 3 ұзындық векторлары, бұлар ашық және шифрлы мәтінді қарастырады, ал **K** - бұл шифрлаудың кілті болатын 3x3 көлемді матрица. Бұл операциялар 26 модулі арқылы іске асырылады.

Мысалы

«PAYMOREMONEY» мәтіні шифрланған делік. Мұның кілті

$$K = \begin{pmatrix} 17 & 17 & 5 \\ 21 & 18 & 21 \\ 2 & 2 & 19 \end{pmatrix}.$$

Ашық мәтіннің алғаш 3 әрпі (15 0 24)векторы ретінде берілген. Сонымен, **K**(15 0 24) = (275 819 486) mod 26 = (11 13 18) = LNS. Есептеулерді жалғастыра отырып осы мысалға LNSHDLEWMTRW шифрланған текстін аламыз.

Шифрді анықтау үшін **K**-ға кері матрицаны қолдану керек. **K**-ға қатысты кері матрица $\mathbf{K}^{-1}$ матрицасы болады. Бұл матрицада $\mathbf{K} \times \mathbf{K}^{-1} = \mathbf{K}^{-1} \times \mathbf{K} = \mathbf{I}$ тендігі орындалу керек. Мұндағы **I** – бірлік матрица (бұл матрицада бастапқы диагоналінің элементтері 1 цифрынан құралады, ал баска элементтері 0-ге тең). Әрбір матрицанын кері матрицасы бола бермейді, бірақ кері матрица болса, онда ол үшін жоғарыдағы теңдік орындалу қажет. Біздің мысалда кері матрица

$$K^{-1} = \begin{pmatrix} 4 & 9 & 15 \\ 15 & 17 & 6 \\ 24 & 0 & 17 \end{pmatrix}$$

Бұл келесі ссептсулермен анықталады:

$$\begin{pmatrix} 17 & 17 & 5 \\ 21 & 18 & 21 \\ 2 & 2 & 19 \end{pmatrix} \times \begin{pmatrix} 4 & 9 & 15 \\ 15 & 17 & 6 \\ 24 & 0 & 17 \end{pmatrix} = \begin{pmatrix} 443 & 442 & 442 \\ 858 & 495 & 780 \\ 494 & 52 & 365 \end{pmatrix} \bmod 26 = \begin{pmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix}$$

Шифрланған мәтінге $\mathbf{K}^{-1}$ матрицасын қолданған кезде ашық мәтін болатынын оңай тексеруге болады.

A квадраттық матрицаның кері матрицасы $[A^{-1}]_{ij} = (-1)^{i-j}\ (\mathbf{D}_{ij})/\det(A)$ сиякты есептеледі, мұндағы $(\mathbf{D}_{ij})$ – матрицанын анықтауышы, $\det(A)$ – *A* матрицаның өзінің анықтауышы. Біздің жағдайда барлық есептеулер 26 модулімен өткізіледі.

Хилл жүйесін жалпы түрде былай жазуға болады:

$$\mathbf{C} = E_K(\mathbf{P}) = \mathbf{KP},$$
$$\mathbf{P} = D_K(\mathbf{C}) = \mathbf{K}^{-1}\mathbf{C}=\mathbf{P}.$$

Плейфейер шифрі сияқты, Хилл шифрі да әрбір әріптің кіруін көрсетиейтінімен белгілі. Хилл шифрі үшін шифрдағы матрицаның көлемі қандай үлкен болса, символдардың баска комбинацияларының жиілігінің ерекшеліктері туралы ақпарат көп болады. Осылай 3x3 матрицалы Хилл шифрі әрбір әріптің көріну жиіліктерін көрсетпей қоймай, сонымен катар екі әріпті комбинациялардың көрінуін де көрсетпейді.

Полиалфавитті шифрлар. Виженер шифрі

Моноалфавитті шрифтті дамытудың ашык текстті шифрлау жолында қолданылатын бірнеше моноалфавитті құрылғыларды қолдану болады. Шифрлау тәсілдерін колдану негізіндегі құрылған шрифттар отбасы – **полиалфавитті шрифттар** деп аталады. Осындай шифрлау тәсілдері келесі касеиттерге ие болады.

1. Бір-бірімен байланысты моноалфавитті құрылғылар қолданылады.

2. Белгілі бір этаптағы шифрлауға кандай келтірулер қолданылатынын анықтайтын кілт болады.

Осындай шифрлауға сәйкес келетін және ең карапайым алгоритмі бар шифрлау бұл – Виженер шифрі (Vigenure). Бұл шифр моноалфавитті құрылғылардың ережелері пегізінде салынған. Бұл ережелер Цезарьдің 26 шифрлармен берілген. Осындай әрбір шифрді шифрланған мәтіннің әрпі болатын кілтті әріппен белгілеуге болады. Ал шифрланған мәтіннің әрпі ашық мәтіннін А әрпіне сәйкес келу керек.

Бұл сызбаны тез ұғып қолдану үшін «Виженер таблосы» атты матрица берілген (Кесте.1 қара). Барлык 26 шифр жазықтық бойынша орналастырылған және әрбір шифр үшін сол жактағы соңғы бағанада берілген кілтті әріп сәйкес келеді. Ашық мәтін әріптеріне сәйкес келетін алфавит кестенің ең бірінші бағанында орналаскан. Шифрлау процессі өте карапайым – x кілтті әрпімен y ашық мәтін әрпі аркылы x жол мен y бағананың қиылысуында орналасқан шифрлаған текстгің әрпін табу керек. Берілген жағдайда бұл әріп V әрпі болып табылады.

1 Кесте. Виженер таблосы

	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
a	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
b	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	A
c	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B
d	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C
e	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D
f	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E

g	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F
h	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G
i	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H
j	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I
k	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J
l	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K
m	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L
n	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M
o	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N
p	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O
q	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P
r	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q
s	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R
t	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S
u	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T
v	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U
w	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V
x	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W
y	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X
z	Z	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

Хабарламаны шифрлау үшін, сол хабарламаның ұзындығы сиякты кілт керек. Керекті ұзындығы бар жолды алу үшін, кілт керекті рет кілтті сөзді кайталайды. Мысалы: deceptive кілтті сөз болса, онда «we are discovered save yourself» хабарламасы келесідей шифрланады:

Ашық мәтін: D E C E P T I V E D E C E P T I V E D E C E P T I V E
Кілт: W E A R E D I S C O V E R E D S A V E Y O U R S E L F
Шифрланған мәтін: Z I C V T W Q N G R Z G V T W A V Z H C Q Y G L M G J

Мәтіннің шифрін аныктау онай – кілттің әрпі жолды анықтайды, ал шифрланған мәтіннің әрпі бағанды аныктайды. Бұл бағаннын кестенің бірінші жолында ашық мәтіннің сәйкес әрпі орналасады.

Осы шифрдің басқа шифрларға карағанда ерекшелігі бұл ашық мәтіннін бір әрпінің шифрлапған мәтінде берілгенінің көп тәсілдері бар – бұл кілтті сөздің әрбір кайталанбайтын әрпіне бір-бір әріптен. Сонымен әріптердің қолдануының жиілігін сипаттайтын ақпарат көрсетілмейді. Бірақ бұл тәсілмен ашык мәтіннің құрылымы шифрланған мәтіннің құрылымына ықпалын толығымен жоюға мүмкін емес. Шифрдің сапасын көтеру үшін хабарламаның ұзындығымен сәйкес келетін кілтті қолдану керек.

3.2. Орынауыстыруды қолдану

Жогарыда көрсетілген барлық тәсілдер ашык мәтін символдарымен шифрланған мәтін символдарына ауыстыру негізінде салынған. Орынауыстыру көмегімен құрылған шифрлар ***орынауыстырулы*** шифрлар деп аталады.

"Ақпараттық кауіпсіздік негіздері"
пәні бойынша
«050704» «Есептеу техника және бағдарламалық қамтама» мамандығының күндізгі оқу формасы бойынша жалпы орта білім негізінде окитын студенттер үшін

Әдебиетпен камтамасыздандыру картасы

Негізгі және қосымша әдебиеттер тізімі	семестр	Кітаптар саны	
		С. Бейсембаев ат. ҒК	керектігі
Негізгі әдебиет			
Батурин Ю. М., Жодзишский А.М. Компьютерная преступность и компьютерная безопасность.- М.,1991	**5**	1	20
Безопасность. Криптографические алгоритмы (CD),2003-Прилож.к ж-лу"Компьютер-пресс"	**5**	1	1
Криптография шаг за шагом:CD.- M.:Delta-MM Corp.,2002	**5**	1	1
Левин, М. Криптография без секретов: Руководство пользователя/ Максим Левин.- М.:Новый издательский дом,2005.- 315 с.	**5**	10	20
Штребе М. и др. Безопасность сетей NT 4:В 2 т.: Пер. с англ.Штрее М., Перкинс Ч., Монкур М.-М.:Мир. Т. 1.-1999.- 367с.+ CD-ROM.	**5**	1	1
Ярочкин. В. И. Информационная безопасность: учебник для студ. вузов, обучающихся по гуманит. и соц.-экон. спец./В. И. Ярочкин.-М :Трикста: Академический Проект,2005.-543 с.-(Учебник для вузов)	**5**	10	20
Қосымша әдебиет			
Защита от хакеров Web - приложений/Форристал Д. [и др.]; пер. с англ. В. Зорина.- М.:Академия АйТи: ДМК,2004	5	1	20
Информатика: Базовый курс:Учеб.пособие для вузов/Под ред. Симоновича.2003.	5	67	67
Чирилло, Д. Защита от хакеров/Джон Чирилло; пер. с англ. Л. Серебрякова.- СПб. : Питер,2003.-472 с.-(Для профессионалов)	5	3	5