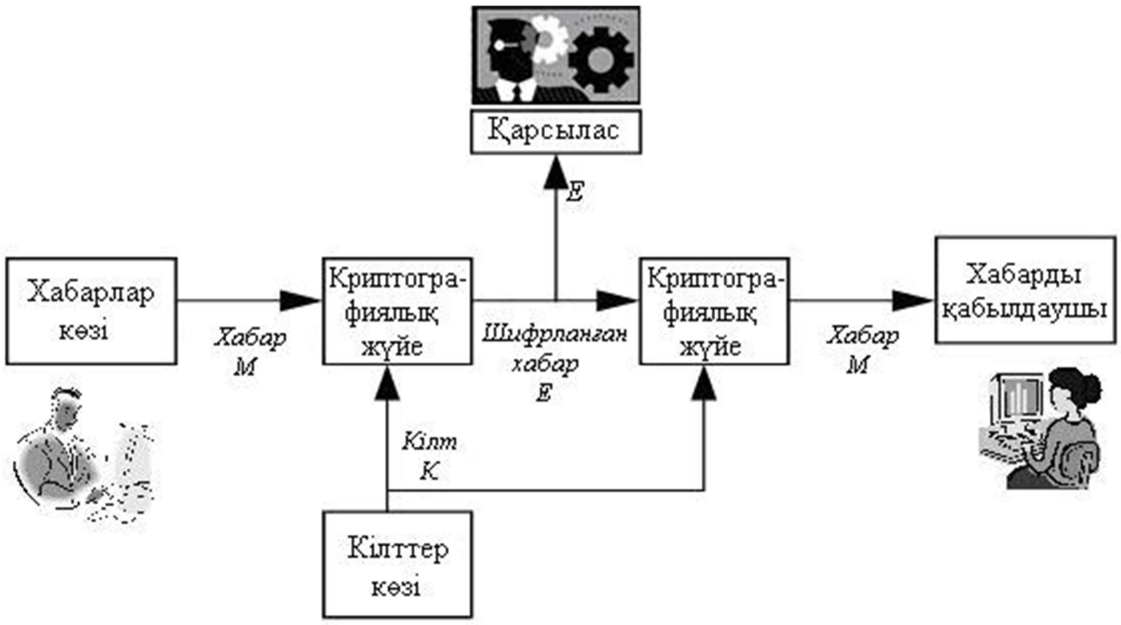
Лекция 2 ЖАБЫҚ КІЛТІ БАР ШИФРЛАУДЫҢ ҚАРАПАЙЫМ ӘДІСТЕРІ

2.1 Симметриялық шифрлаудың жалпы схемасы

Классикалық, немесе біркілтті криптография **шифрлаудың симметриялық алгоритмдерінің** пайдалануына сүйенеді. Бұл алгоритмдер бір ғана құпиялы элемент (кілт) пайдаланады, ал шифрды ашу шифрлаудың жай айналуы болып табылады. Сондықтан, әдетте алмасудың қатысушылары хабарды шифрлау мен дешифрлай алады. Осындай жүйенің схемалық құрылымы 2.1 суретте көрсетілген.



Сурет 2.1. Симметриялық шифрлауды пайдаланатын құпиялы жүйенің жалпы құрылымы

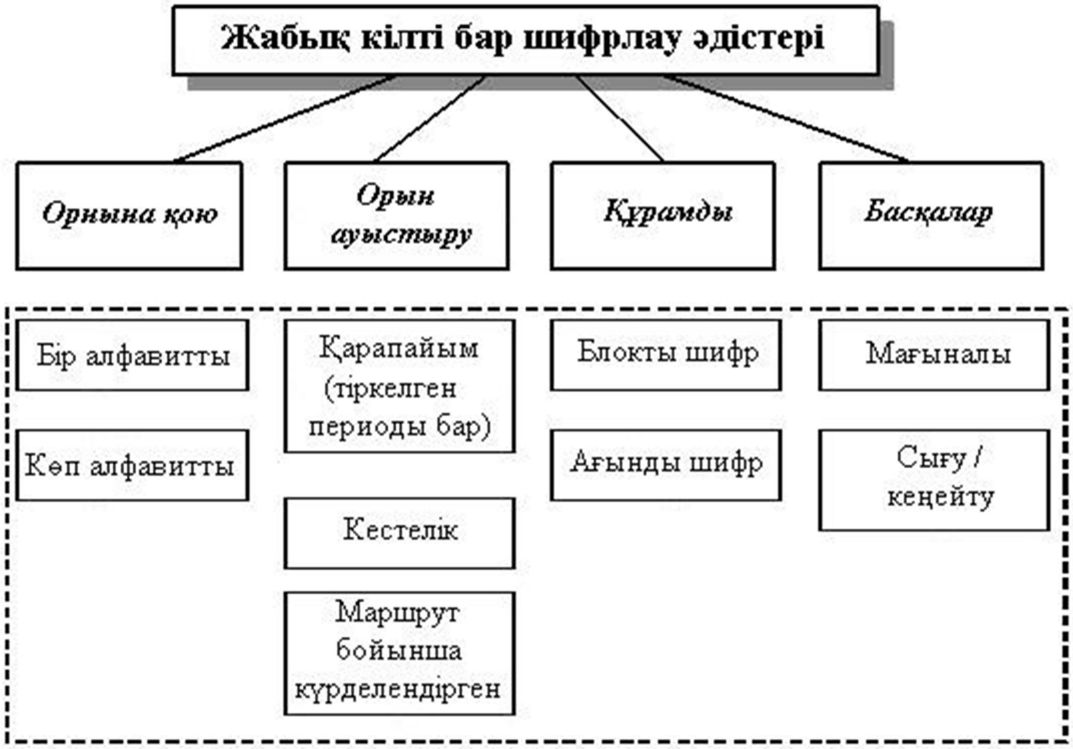
Беретін жақта хабардың көзі мен кілттер көзі бар. Кілттер көзі осы жүйенің барлық мүмкін болатын кілттерінен нақты кілтті ***K*** таңдайды. Бұл кілт ***K*** кейбір тәсіл көмегімен қабылдау жаққа беріледі, кілт басқа қолға түспеу үшін арнайы курьермен жеткізіледі (сондықтан, симметриялық шифрлау жабық кілті бар шифрлау да деп аталады). Хабарлар көзі кейбір хабарды ***M*** жасайды, сосын бұл хабар таңдалған кілт көмегімен шифрланады. Шифрлау нәтижесінде шифрланған хабар ***E*** (криптограмма деп аталатын) алынады. Сосын криптограмма ***E*** байланыс арна арқылы жіберіледі. Байланыс арна ашық және қорғалмаған болғандықтан, мысалы радиоарна немесе компьютерлік желі, онда берілетін хабарды қарсылас қолына ұстап түсіру мүмкін. Қабылдау жақта ***E*** криптограмманы кілт көмегімен ашады және бастапқы ***M*** хабарды алады.

Егер ***M*** – хабар, ***K*** - кілт, ***E*** - шифрланған хабар, онда жазуға болады:

$$E = f(M,K),$$

яғни шифрланған хабар ***E*** бастапқы хабар ***M*** мен кілттің ***K*** кейбір функциясы болып табылады. Криптографиялық жүйеде пайдаланатын әдіс немесе шифрлау алгоритмы ***f*** функцияны анықтайды.

Жабық кілті бар шифрлаудың әртүрлі әдістері белігілі (сур. 2.2). Тәжірибеде жиі қолданады орын ауыстыру, орнына қою (ауыстыру) алгоритмдер және құрамды әдістер.



Сурет 2.2. Жабық кілті бар шифрлау әдістері

Орын ауыстыру әдістерінде бастапқы мәтіннің символдары белгілі ереже бойынша бір-бірімен орнымен ауыстырылады. ***Орнына қою*** (немесе ***ауыстыру***) әдістерінде ашық мәтіннің символдары шифрланған мәтіннің кейбір баламаларымен ауыстырылады. Шифрлаудың сенімділігін өсіру үшін, бір әдіс көмегімен шифрланған мәтінді басқа әдіспен тағы бір рет шифрлауға болады. бұл жағдайда ***құрамды*** немесе ***композициялы*** шифр пайда болады. Қазіргі уақытта пайдаланатын блокты немесе тасқынды (ағынды) симметриялық шифрлар да құрамды шифрларға жатады, өйткені оларда хабарларды шифрлау үшін бірнеше операциялар пайдаланылады.

Бұрынғы криптографиялық алгоритмдер табиғи тілдердің символдары мен, мысалы ағылшын немесе орыс әліпбидің әріптерімен жұмыс істейтің. Бұл әріптер белгілі ереже бойынша орындарымен немесе басқа әріптермен ауыстырылатың. Қәзіргі криптографиялық алгоритмде екілік белгелір (яғни нольмен бір) арқылы операциялар жүргізіледі.

Қазіргі заманның блокты шифрлардың негізінде орнына қою және орын ауыстыру процедуралар жатыр.

2.2 Орнына қою әдістер

Орнына қою (ауыстыру) шифрлау әдістері былай негізделеді: әдетте блоктарға бөлінген және бір алфавитта жазылған бастапқы мәтіннің символдары басқа әліппенің бір не бірнеше символдары мен, қабылданған түрлендіру ережеге сәйкес, ауыстырылады.

Біралфавитты орнына қою

Орнына қою әдістерінің бағыныңқы класстарының маңызды біреуі ***біралфавитты*** (немесе ***моноалфавитты***) орнына қоюлар, мұнда ***A*** хабардың бастапқы алфавитінің әрбір a_i белгінің және шифрланаған ***E*** мәтіннің сәйкес e_i белгінің арасында бірмәнді сәйкестік

орындалады. Біралфавитты орнына қою кейде ***қарапайым орнына қою*** деп аталады, себебі бұл ең қарапайым шифр.

Біралфавитты орнына қоюдың мысалы Цезарь шифры. Жоғарыда қарастырылған мысалда бірінші жол бастапқы алфавит, екінші (*k*–ға солға қарай циклдық ығыстыру) – *орнына қою векторы* болып табылады.

Жалпы жағдайда біралфавитты орнына қоюда бастапқы символдар олардың орнына қою вектордағы (немесе ауыстыру кестесі) баламаларымен бір мәнді ауыстырылады. Осындай шифрлау әдісте кілт болып пайдаланатын ауыстыру кестесі болады.

Орнына қою кесте көмегімен берілу мүмкін (мысалы 2.1 кесте).

Кесте 2.1. Екі шифр үшін ауыстыру кестесінің мысалы

Ашық мәтін	**Шифр 1**	**Шифр 2**	**Ашық мәтін**	**Шифр 1**	**Шифр 2**	**Ашық мәтін**	**Шифр 1**	**Шифр 2**
А	В	^	М	Т	№	Ч	М	∑
Б	И	@	Н	Ц	#	Ш	У	∇
В	О	)	О	.	-	Щ	Д	ϒ
Г	А	+	П	Ж	=	Ъ	Э	ℵ
Д	Щ	<	Р	Г	(	Ы	Н	⊕
Е	П	>	С	Л	?	Ь	Ю	×
Ж	К	∀	Т	Х	%	Э	Ы	ω
З	Б	♦	У	С	⊗	Ю	Ш	$
И	Ъ	*	Ф	Ь	!	Я	Е	Δ
К	Бос орын	♥	Х	Ч	©	Бос орын	Ф	∞
Л	Р	♠	Ц	З	®	.	Я	♣

Негізінде бұл кестеде екі кесте бірлескен. Біреуі (шифр 1) бастапқы мәтіннің орыс әріптерін басқа орыс әріптеріне ауыстыруын анықтайды, ал екіншісі (шифр 2) - әріптерді арнайы символдарға ауыстыру. Екі шифры үшін бастапқы алфавит орыс бас әріптері («Ё» мен «Й» әріптерінен басқа), ақ жері (тақыр) және нүкте болып табылады. Қазақ алфавитын мысалға алмай ақ қояйық, себебі кейбір әріптерден басқа қалғандары бірдей.

Моноалфавитты орнына қоюдың түрлі шифрының пайдалануымен шифрланған хабар келесі түрде алынады. Бастапқы хабардан келесі белгі алынады. Оның орыны ауыстыру кестедегі «Ашық мәтін» бағанадан анықталады. Шифрланған хабарға осы жолдағы шифрланған символ қойылады.

Осы екі шифрды пайдаланып «ВЫШЛИТЕ ПОДКРЕПЛЕНИЕ» хабарды шифрлап көрейік (2.3 сур.). Ол үшін бастапқы хабардың бірінші «В» әрпін аламыз. 2.1 кестеде «Шифр 1» бағанда «В» әріп үшін орнына қойылатын символды табамыз. Бұл әріп «О». Оны «В» астына жазамыз. Сосын бастапқы хабардың екінші символын қараймыз - әріп «Ы». «Ашық мәтін» бағанында бұл әріпті табамыз және «Шифр 1» бағаннан сол жолда тұратын әріпті аламыз - әріп «Н». Осы жолмен бастапқы хабарды толық шифрлаймыз (2.3 сур.).

Ашық мәтін																			
В	Ы	Ш	Л	И	Т	Е		П	О	Д	К	Р	Е	П	Л	Е	Н	И	Е
Шифр 1 көмегімен шифрланған хабар																			
О	Н	У	Р	Ъ	Х	П	Ф	Ж	.	Щ		Г	П	Ж	Р	П	Ц	Ъ	П

Шифр 2 көмегімен шифрланған хабар																			
)	⊕	∇	♠	*	%	>	∞	=	-	<	♥	(	>	=	♠	>	#	*	>

Сурет 2.3. Тура орнына қою әдіспен шифрлау мысалы

Осылай алынған мәтіннің қорғау деңгейі аса үлкен емес, өйткені бастапқы мен шифрланған мәтіндерде бірдей статистикалық заңдылығы бар. Мұнда қандай символдар (әрептер немесе белгілер) ауыстыру үшін пайдаланғаны маңызды емес.

Шифрланған хабарды жиілік криптоталдау көмегімен ашуға болады. Ол үшін хабарды жазған тілдің кейбір статистикалық мәліметтерін пайдалануға болады.

Бізге белгілі, орыс тіліндегі мәтіндерде ең жиі кездесетін символдар О, И. Одан сирек кездеседі Е, А әріптері. Дауыссыз әріптерден ең жиі кездесетіні Т, Н, Р, С символдары. Криптоталдаушының қолында түрлі типті мәтіндер (ғылыми, көркем және т.б.) үшін символдардың кездесу жиілігінің арнайы кестелері бар.

Криптоталдаушы алынған криптограмманы ықыласпен зерттейді және қандай символдар неше рет кездесетінің санайды. Алдымен шифрланған хабардың ең жиі кездесетін белгілерін ауыстырады, мысалы О әрпімен. Сосын И, Е, А әріптер үшін орындарын іздеп тырысады. Сонан соң ең жиі кездесетін дауыссыздар қойылады. Әрбір кезеңде сол не басқа біреу әріптерінің «сай келу» мүмкіндігі бағаланады. Мысалы, орыс сөздерінде қатар жазылатын төрт дауысты әріптерді табу қиын, орыс тілінде сөздер Ы әріптен басталмайды және т.б. Шынында, әрбір табиғи тілі (қазақ, орыс, ағылшын және т.б.) үшін көп заңдылықтар бар, олар маманға шифрланған хабарды ашуға көмектеседі.

Бірмәнді криптоталдаудын мүмкіндігі ұстап алынған хабардың ұзындығына тікелей тәуелді. Мысалы, криптоталдаушының қолына кейбір біралфавитты орнына қою шифры көмегімен шифрланған хабар түссін:

ТНФЖ.ИПЩЪРЪ

Бұл хабар 11 символдан тұрады. Осы символдар үлкен мәтіннің фрагменты емес бүтін хабар құрайтыны белгілі болсын. Бұл жағдайда біздің шифрланған хабар бір не бірнеше бүтін сөзден тұрады. Шифрланған хабарда символ Ъ екі рет кездеседі. Ашық мәтінде шифрланған Ъ белгінің орнында дауысты әріп О, А, И немесе Е тұр деп болжайық. Ъ орнына осы әріптерді қойып әрі қарай талдаудың мүмкіндігін бағалайық (2.2 кесте).

Кесте 2.2. Криптоталдаудың бірінші кезеңнің варианттары

Шифрланған хабар										
Т	Н	Ф	Ж	.	И	П	Щ	Ъ	Р	Ъ
Ъ -ны О -ға ауыстырғаннан кейін										
								О		О
Ъ -ны А -ға ауыстырғаннан кейін										
								А		А
Ъ -ны И -ға ауыстырғаннан кейін										
								И		И
Ъ -ны Е -ға ауыстырғаннан кейін										
								Е		Е

Барлық келтірілген ауыстыру варианттары тәжірибеде кездесу мүмкін. Криптограммада басқа символдар бір рет кездесетінің еске алып, қандай болмасын хабардың варианттарын таңдап алайық (2.3 кесте).

Кесте 2.3. Криптоталдаудың екінші кезеңнің вариантты

Шифрланған хабар										
Т	Н	Ф	Ж	.	И	П	Щ	Ъ	Р	Ъ Дешифрланған таңдап
алынған хабарлардың варианттары										
Ж	Д	И		С	У	М	Р	А	К	А
Д	Ж	О	Н	А		У	Б	И	Л	И
В	С	Е	Х		П	О	Б	И	Л	И
М	Ы		П	О	Б	Е	Д	И	Л	И

2.3 кестеде келтіргеннен басқа хабарлардан одан да артық сай келетін сөйлемдерді таңдап алуға болады. Сонымен, егер бізге ұстап алынған хабардың мазмұны туралы еш нәрсе алдын ала белгілі болмаса, онда оны бірмәнде ашалмаймыз.

Егер де криптоталдаушының қолына қарапайым орнына қою әдіспен шифрланған жеткілікті ұзын хабар түссе, онда әдетте оны ойдағыдай ашып оқуға болады. Шифрланған хабар неғұрлым ұзын болса, соғұрлым оны бірмәнді дешифрлауға болады.

Егер ашық мәтіннің статистикалық сипаттамаларын жасыратын болсақ, онда қарапайым орнына қою шифрдың ашуы бірталай күрделі болады. Мысалы, осы оймен шифрлаудың алдында ашық мәтінді архиватор программа көмегімен «сығуға» болады.

Орнына қою ережелерінің күрделендіруімен шифрлаудың сенімділігі өседі. Жеке символдарды емес, ал мысалы, екі әріпті тіркестерді – *биграммаларды* ауыстыруға болады. Осындай шифр үшін ауыстыру кестесі 2.4 кестеде берілген.

Кесте 2.4. Екі әріпті тіркестерді ауыстыру кестесінің мысалы

Ашық мәтін	**Шифрланған мәтін**	**Ашық мәтін**	**Шифрланған мәтін**
аа	кх	бб	пш
аб	пу	бв	вь
ав	жа	...	...
...	...	яэ	сы
ая	ис	яю	ек
ба	цу	яя	рт

Осындай ауыстыру кестесінің мөлшерін бағалайық. Егер бастапқы алфавитта N символ болса, онда биграммалық шифры үшін ауыстыру векторында N^2 «ашық мәтін - шифрланған мәтін» жұптар болу керек. Осындай шифры үшін ауыстыру кестесін басқа түрде де жазуға болады: бағандардың атаулары биграмманың бірінші әрпіне сәйкес, ал жолдардың атаулары – екіншіге, мұнда кестенің ұяшықтары орнына қойылатын символдармен толтырылған. Бұл кестеде N жол және N баған болады (2.5 кесте).

Кесте 2.5. Биграммалық шифры үшін ауыстыру кестесінің басқа варианты

	а	**б**	**...**	**я**
а	кх	цу	...	...
б	пу	пш	...	...
в	жа	вь	...	...
...	...	...	...	...

ю	...	...	...	ек
я	ис	...	...	рт

Үшграммалы және *n*–граммалы шифрдың пайдалану варианттары да мүмкін. Сондай шифрлардың криптоберіктігі үлкенірек болады, бірақ олар жүзеге асыру үшін күрделі және кілтті ақпараттың (ауыстыру кестенің үлкен көлемін) көп саның талап етеді. Барлық *n*–граммалы шифрлар жиілік криптоталдау көмегімен ашылу мүмкін, тек кездесу статистикасы жеке символдардың емес, *n* символдан тұратын тіркестерден пайдаланады.

Пропорционал шифрлар

Біралфавитты орнына қою әдістеріне **пропорционал** немесе **монофониялық** шифрлар жатады, оларда жиілік талдау көмегімен ашудан қорғау үшін шифрланған белгілердің кездесу жиілігі теңестіріледі. Жиі кездесетін белгілер үшін мүмкін болатын баламалар пайдаланады. Аса көп пайдаланбайтың бастапқы белгілер үшін бір не екі балама жеткілікті. Шифрлау кезінде ашық мәтіннің символы үшін орнына қою кездейсоқ немесе белгілі түрде (мысалы, рет-ретімен) таңдалады. Символдарды ауыстыру үшін пропорционал шифрды пайдалану кезінде әдетте сандар таңдап алынады. Мысалы, 2.6 кестеде көрсетілгендей орыс тілдің әріптеріне үштаңбалы сандарды қояйық.

Кесте 2.6. Пропорционал шифры үшін ауыстыру кестесі

Символ	Ауыстыру варианты					Символ	Ауыстыру варианты					
А	760	128	350	201		С	800	767	105			
Б	101					Т	759	135	214			
В	210	106				У	544					
Г	351					Ф	560					
Д	129					Х	768					
Е	761	130	802	352		Ц	545					
Ж	102					Ч	215					
З	753					Ш	103					
И	762	211	131			Щ	752					
К	754	764				Ъ	561					
Л	132	354				Ы	136					
М	755	742				Ь	562					
Н	763	756	212			Э	750					
О	757	213	765	133	353	Ю	570					
П	743	766				Я	216	104				
Р	134	532				Бос орын	751	769	758	801	849	035…

Бұл жағдайда хабар

БОЛЬШОЙ СЕКРЕТ

келесі түрде шифрлану мүмкін:

101757132562103213762751800761754134130759

Берілген мысалда қайталанатын әріптер үшін (мысалы, «О») ауыстыру варианттары рет-ретімен таңдалды.

Пропорционал шифрлар қарапайым біралфавитты орнына қою шифрларға қарағанда ашу үшін күрделірек. Бірақ, «ашық мәтін – шифрланған мәтін» бір жұбы ғана

бар болса, ашуы қиын емес. Егер де тек шифрланған мәтіндер қолда болса, онда кілтті ашу, яғни ауыстыру кестесін табу, күрделі болса да, бірақ сонда да жүзеге асырылу мүмкін.

Көп алфавитты орнына қоюлар

Бастапқы тілдің табиғи жиілік статистикасын жасыру үшін көп алфавитты орнына қою қолданады, ол да бірнеше түрлі болады. ***Көп алфавитты орнына қоюларда*** бастапқы мәтіннің символдарын ауыстыру үшін бір емес, бірнеше әліпби пайдаланады. Әдетте ауыстыру үшін алфавиттер бастапқы алфавиттың басқа ретімен жазылған символынан жасалынады.

Көп алфавитты орнына қоюдың мысалы ***Вижинер*** кестесін пайдалануына негізделген схемасы болып табылады. Бұл әдісті француз Блез Вижинер 1585 жылы шыққан «Шифрлар туралы трактатта» жазып шығарған.

Осы әдісте шифрлау үшін *N*x*N* элементі бар квадратты матрица тәріздес кесте пайдаланады, мұнда *N* – алфавиттағы символдар саны (2.7 кесте). Матрицаның бірінші жолында бастапқы алфавиттегідей рет-ретімен әріптер жазылады, екінші жолында – сол әріптердің тізбегі, бірақ сол жаққа бір орынға циклдық ығысумен, үшінші жолда – екі орынға ығысуымен және т.б.

Кесте 2.7. Шифрлау кестені дайындау

АБВГДЕ.....	.....ЭЮЯ
БВГДЕЖ.....	.....ЮЯА
ВГДЕЖЗ.....	.....ЯАБ
ГДЕЖЗИ.....	.....АБВ
ДЕЖЭИК.....	.....БВГ
ЕЖЗИКЛ.....	.....ВГД
.....	.....
ЯАБВГД.....	.....ЬЭЮ

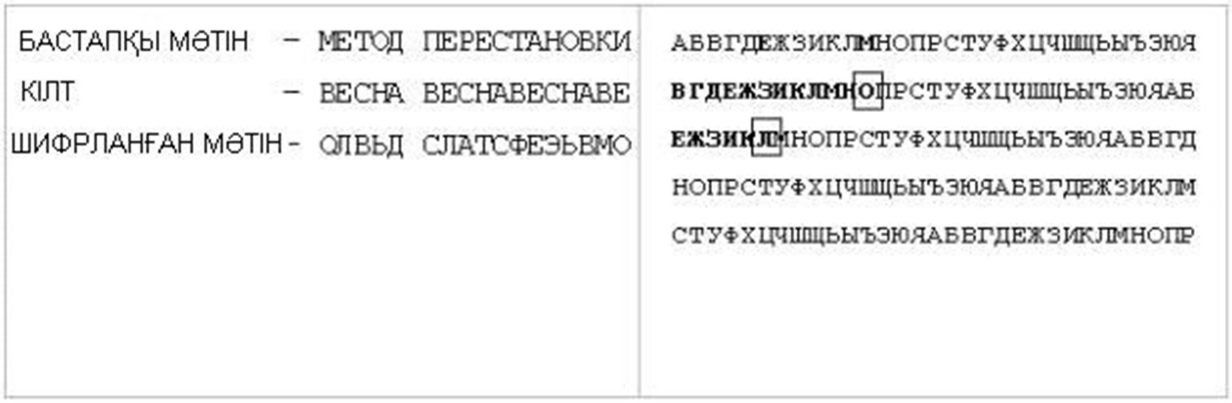
Мәтінді шифрлау үшін бастапқы алфавиттың кейбір сөзі немесе символдар жиынтығы болатын кілтті таңдайды. Сосын толық матрицадан бірінші жолынан және бастапқы әріптері рет-ретімен кілт әріптері болатын жолдарынан бағыныңқы шифрлау матрицаны жазып шығарады (мысалы, егер «весна» кілтті таңдасақ, онда шифрлау кестесі 2.8 кестегідей болады).

Кесте 2.8. Шифрлаудың бірінші кезеңі – шифрлаудың бағыныңқы матрицасын құру

АБВГДЕЖЗИКЛМНОПРСТУФХЦЧШЩЪЫЬЭЮЯ
ВГДЕЖЗИКЛМНОПРСТУФХЦЧШЩЪЫЬЭЮЯАБ
ЕЖЗИКЛМНОПРСТУФХЦЧШЩЪЫЬЭЮЯАБВГД
НОПРСТУФХЦЧШЩЪЫЬЭЮЯАБВГДЕЖЗИКЛМ
СТУФХЦЧШЩЪЫЬЭЮЯАБВГДЕЖЗИКЛМНОПР

Шифрлау барысында (сур. 2.4) шифрланатын мәтіннің әрбір әріптерінің астында, кілтті қажетті рет қайталайтын, кілттің әріптерін жазады, сосын шифрланатын мәтінді шифрлау кестесі (2.8 кесте) арқылы ауыстырады. Ол үшін кестенінің бірінші жолындағы әріптерді және оның астында тұратын кілт әріптерінің сызықтар қиылысында тұратын әріптермен ауыстырады.

Мысалы, бастапқы мәтіннің бірінші «М» әріптің астында кілттің «В» әрпі жазылған. Кодтау кестеде «М»-нан басталатын бағанды және «В»-нан басталатын жолды табамыз. Олардың қиылысында «О» әрпі тұр. Бұл әріп шифрланған хабардың бірінші символы болады (2.4 суретте бұл әріп төртбұрышпен белгіленген). Бастапқы хабардың келесі әрпі – «Е», кілт символы – «Е». «Е» дан басталатын жол мен бағанның қиылысын табамыз. Бұл әріп «Л» - шифрланған хабардың екінші символы.



Сурет 2.4. Көп алфавитты орнына қою шифрлаудың механизмы

Вижинер әдісі бойынша хабарды ашып оқу мысалын қарастырайық. ВЕСНА кілт көмегімен шифрланған КЕКХТВОЭЦОТССВИЛ хабар болсын (шифрлау кезінде ақ жерлері еске алынбаған). Мәтіннің дешифрлауы келесі ретпен орындалады (2.9 кесте):

- шифрланған мәтін әріптерінің үстінен рет-ретімен кілттің әріптері жазылады және қажетті рет кілт қайталанады;
- Вижинер кестесінің бағыныңқы матрица жолында әрбір кілт әрпі үшін шифрланған мәтін белгісіне сәйкес әріп іздеп табылады. Оның үстінде тұратын бірінші жолдын әрпі ашылған мәтіннің белгісі болып табылады; алынған мәтін мағынасы бойынша
- топтастырылады.

Кесте 2.9. Дешифрлау механизмы

КІЛТ	ВЕСНАВЕСНАВЕСНАВ
ШИФРЛАНҒАН МӘТІН	КЕКХТВОЭЦОТССВИЛ
АШЫП АЛЫНҒАН МӘТІН	ЗАЩИТАИНФОРМАЦИИ
БАСТАПҚЫ МӘТІН	ЗАЩИТА ИНФОРМАЦИИ

Бір алфавитты орнына қою әдісі сияқты Вижинер шифрын ашуға мүмкін емес, өйткені ашық мәтіннің бірдей символдары шифрланған мәтіннің әртүрлі символдарымен ауыстырылу мүмкін. Басқа жақтан, ашық мәтіннің әртүрлі әріптерінің орнына шифрланған мәтіннің бірдей белгілері қойылу мүмкін.

Берілген көп алфавитты орнына қою әдістің ерекшелігі мұндай – кілт символдарының әрбіреуі бастапқы хабардың бір символын шифрлау үшін пайдаланады. Кілт символдарының барлығын пайдаланғаннан кейін, олар сол ретімен қайталанады. Егер он әріптен тұратын кілт пайдаланса, онда хабардың әрбір оныншы әрпі кілттің бірдей символымен шифрланады. Осы параметр ***шифр периоды*** деп аталады. Егер шифрлау кілті бір символдан тұрса, онда шифрлау кезінде Вижинер кестесінің бір жолы пайдаланылады, сондықтан бұл жағдайда біз моноалфавитты орнына қоюды аламыз, яғни Цезарь шифрын.

Мәтін шифрлауның сенімділігін күшейту үшін екі немесе одан көп Вижинер әдісі бойынша (әртүрлі кілтпен) қатар шифрлауды пайдалануға болады (Вижинер құрама шифры).

Тәжірибеде Вижинер әдісінен басқа оның әртүрлі өзгертулері пайдаланған. Мысалы, бір рет араластырылған Вижинер шифры. Бұл жағдайда хабарды ашып оқу үшін алушы кілтті білгеннен басқа, шифрлау кестедегі символдардың ретін білу қажет.

Көп алфавитты орнына қоюдың тағы бір мысалы – *жүгіру кілті бар шифр* немесе *кітап шифры*. Бұл әдісте мәтінді шифрлау үшін басқа мәтін кілт ретінде пайдаланады.

«Компьютерге» дейін заманда криптографияда жүгіру кілті бар шифры үшін жуан кітапты таңдап алатын (осыдан шифрдың екінші атауы шықты). Осындай шифрлау әдістің периоды - кілт ретінде таңдап алынған шығарманың ұзындығы болып табылады.

Көп алфавитты орнына қою әдістері, соның қатарында Вижинер әдісі, «қол» криптоталдауға қиын беріледі. Көп алфавитты орнына қою әдістерді ашу үшін арнайы, күрделі алгоритмдер жасалынған. Компьютердің пайдалануымен көп алфавитты орнына қою әдістердің ашуын тез уақытта жүзеге асыруға болады.

XX ғасырдың бірінші жартысында көп алфавитты орнына қою процесті автоматтандыру үшін роторлық шифрлау машиналарды кең қолдана бастады. Осындай құрылғыдағы басты элементі роторлар – орнына қоюды орындау үшін пайдаланатын механикалық дөңгелектер. Роторлық шифрлау машинада әдетте пернетақтасы мен ротор жиынтығы болатын. Әрбір роторда символдар жиынтығы (алфавиттегі саны бойынша) болатын, олар кез келген ретімен орналасатын және ротор қарапайым орнына қоюды орындайтын. Бірінші ауыстыруды орындағаннан кейін хабар символдары екінші ротормен өңделетін және әрі қарай. Роторларды ығыстырып шифрлау кілтті тапсыруға болатын. Кейбір роторлық машиналар шифрлау барысында символдардың орнын да ауыстыра алатын. Осындай типке жататын ең танымал құрылғы неміс шифрлау роторлық машина Энигма (лат. enigma — жұмбақ), ол Екінші Дүниежүзілік соғыс кезінде пайдаланған еді. Энигманың түрлі роторлар саны бар бірнеше моделі шығарылған болатын. Үш роторы бар Энигма шифрлау машинада 16900 әртүрлі алфавитты пайдалануға болатын.

Гаммалау әдісі

Көп алфавитты орнына қоюдың тағы бір жиі кездесетін жағдайы **гаммалау**. Бұл әдісте шифрлау бастапқы мәтіннің символдарын және модулі бойынша алфавиттың әріптер санына тең кілтпен қосу арқылы орындалады. Егер бастапқы алфавитте, мысалы, 33 символ, онда қосы 33 модулі бойынша орындалады. Осындай бастапқы мәтіннің және кілттің қосу процесі криптографияда ***гамманы салу*** деп аталады.

Бастапқы алфавиттың символдарына 0 (А) ден 32 (Я) дейін сандар сәйкес болсын. Егер бастапқы символға сәйкес санды x деп, ал кілт символын - k деп белгілесек, онда гаммалау ережесін былай жазуға болады:

$$z = x + k \pmod N,$$

мұнда z – кодталған символ; N - алфавиттың әріптер саны, ал N модулі бойынша қосу – кәдімгі қосуға сәйкес операция (оның айырмашылығы – кәдімгі қосудың нәтижесі N–ға тең немесе одан артық, ал модулі бойынша қосудың нәтижесі N–ға бөлудін қалдығы). Мысалы, 33 модулі бойынша Г (3) мен Ю (31) символдарды қосайық:

$$3 + 31 \pmod{33} = 1,$$

яғни нәтижесінде аламыз 1 санға сәйкес Б символын.

Тәжірибеде ең жиі кездеседі *екілік гаммалау*. Мұнда екілік алфавит пайдаланады, ал қосу 2 модулі бойынша орындалады. 2 модулі бойынша қосу операцияны көбінесе $\oplus$ деп белгілейді, сонда жазуға болады:

$$z = x + k \pmod 2 = x \oplus k.$$

Екі модулі бойынша қосу операциясы логика алгебрасында «шығарып тастайтын ИЛИ» немесе ағылшынша XOR деп аталады.

Мысал қарастырайық. Бізге 14 ондық санды 12 кілтті пайдаланып гаммалау әдіспен шифрлау керек. Ол үшін алдымен бастапқы санды және кілтті (гамманы) екілік түрге түрлендіру керек:

$$14_{(10)} = 1110_{(2)}, \qquad 12_{(10)} = 1100_{(2)}.$$

Сосын алынған екілік сандарды бір бірінің астында жазу керек және әрбір қос символдарды екі модулі бойынша қосу керек. Екі екілік белгіні қосқан кезде 0 аламыз, егер бастапқы екілік символдар бірдей болса, және 1 аламыз, егер цифрлар әртүрлі:

$$0 \oplus 0 = 0;$$
$$0 \oplus 1 = 1;$$

$$1 \oplus 0 = 1;$$
$$1 \oplus 1 = 0.$$

Екі модулі бойынша екі екілік санды 1110 және 1100 қосайық:

Бастапқы сан	1 1 1 0
Гамма	1 1 0 0
Нәтижесі	0 0 1 0

Қосу нәтижесінде біз алдық екілік сан 0010. Егер оны ондық түрге ауыстырсақ, аламыз 2. Сонымен, 14 санға 12 кілті бар гаммалауды қолдап, нәтижесінде алдық 2 санды.

Дешифрлауды қалай орындаймыз? Шифрланған сан 2 екілік түрде жазылады және қайтадан екі модулі бойынша кілтпен қосу жүргізіледі:

Шифрланған сан	0 0 1 0
Гамма	1 1 0 0
Нәтижесі	1 1 1 0

Алынған екілік мәнінің 1110 ондық түрге ауыстырамыз және аламыз 14, яғни бұл бастапқы сан.

Сонымен, 2 модулі бойынша гаммалау кезінде шифрлау үшін да дешифрлау үшін да бірдей операцияны пайдалану керек. Бұл бірдей алгоритмды және оған сәйкес программалық жүзеге асыруда бірдей программаны пайдалануға мүмкіндік береді.

Екі модулі бойынша қосу операциясы компьютерде өте тез орындалады (басқа арифметикалық операцияларға қарағанда), сондықтан тіпті үлкен ашық мәтінге гамманың салуы лезде жасалынады. Сол себептен, қазіргі техникалық жүйелерде гаммалау әдісі кең қолданылады.

Жалпы жағдайда екі модулі бойынша гаммалау қалай орындалатының тұжырымдайық:

- бастапқы мәтіннің символдары мен гамма екілік кодта беріледі және бір бірінің астында орналасады, бұл кезде кілт (гамма) неше рет қажет болса сол рет жазылады;
- екілік белгілердің әрбір жұбы екі модулі бойынша қосылады;
- алынған екілік белгілердің тізбегі таңдалған коды бойынша алфавит символдарымен кодталады.

2.5 суретте орыс символдарынан тұратын мәтінге гаммалаудың қолдануы көрсетілген. Қабылданған кодтауға сәйкес символдар кодталады, ал сосын екі модулі бойынша қосу орындалады.

Гаммалау әдісті пайдаланғанда қосуды орындайтын тізбек - гамма кілт болып табылады. Егер гамма шифрлауға арналған хабардан қысқа болса, онда гамма қажетті рет қайталанады. Мысалы, 2.5 суретте бастапқы хабардың ұзындығы 12 байтқа тең, ал кілт ұзындығы – 5 байт. Сондықтан, шифрлау үшін гамма екі рет толық қайталану керек және бір рет жартылай.

Кілт негұрлым ұзын болса, соғұрлым гаммалау шифрлау әдісінің сенімділігі жоғары. Тәжірибеде кілт ұзындығы деректер алмасу аппаратураның және есептеуіш техниканың мүмкіндігімен шектелген. Яғни кілтке бөлінген жад көлемімен, хабарды өңдеу уақытымен, және кілттер тізбегін дайындау мен жазу аппаратураның мүмкіншілігімен. Одан басқа, кілтті пайдалану үшін, алдымен кейбір сенімді жолмен оны хабарлармен алмасатын екі жаққа жеткізу қажет. Бұл кілттерді үлестіру проблемасына әкеледі, оның шешу күрделігі кілттің ұзындығының және абонентер санының өсуімен көбейеді.

Бастапқы мәтін: *Гаммирование*

Бастапқы мәтін он алтылық түрде:

83 A0 AC AC A8 E0 AE A2 A0 AD A8 A5

Гамма (Кілт): *Весна (82 A5 E1 AD A0)*

Гаммирование

Баст. биттер	1000	0011	1010	0000	1010	1100
Гамма	1000	0010	1010	0101	1110	0001
Нәтиже	0000	0001	0000	0101	0100	1101
Баст. биттер	1010	1100	1010	1000	1110	0000
Гамма	1010	1101	1010	0000	1000	0010
Нәтиже	0000	0001	0000	1000	0110	0010
Баст. биттер	1010	1110	1010	0010	1010	0000
Гамма	1010	0101	1110	0001	1010	1101
Нәтиже	0000	1011	0100	0011	0000	1101
Баст. биттер	1010	1101	1010	1000	1010	0101
Гамма	1000	0010	1010	0101	1110	0001
Нәтиже	0010	1111	0000	1101	0100	0101

Он алтылық түрде кодталған мәтін:

01 05 4D 01 08 62 0B 43 0D 2F 0D 45

Сурет 2.5. Гаммалау механизмы

2.3 Орын ауыстыру әдістер

Орын ауыстыру шифрларын пайдалану кезінде бастапқы мәтіннің кіріс ағыны блоктарға бөлінеді, олардың әрбіреуінде символдардың орын ауыстыруы орындалады. Классикалық «компьютерге» дейін криптографияда, орын ауыстыру геометриялық пішіннің түрлі жолдары бойынша бастапқы мәтінді жазу және шифрланған мәтінді оқу нәтижесінде алынатын.

Орын ауыстырудың қарапайым мысалы - тіркелген *d* периоды бар орын ауыстыру. Бұл әдісте хабар *d* символы бар блоктарға бөлінеді және әрбір блокта бірдей орын ауыстыру жүргізіледі. Орын ауыстыруды орындайтын ереже кілт болып табылады және бірінші *d* натурал сандардың кейбір орын ауыстыруымен берілу мүмкін. Нәтижесінде хабардың әріптері өзгермейді, бірақ басқа ретімен беріледі.

Мысалы, *d*=6 үшін орын ауыстыру кілтін 436215 деп алуға болады. Бұл көрсетеді: 6 символдан тұратын әрбір блокта төртінші символ бірінші орынға қойылады, үшінші символ – екінші орынға, алтыншы – үшіншіге және т.с.с. Мынадай мәтінді шифрлау керек болсын:

ЭТО_ТЕКСТ_ДЛЯ_ШИФРОВАНИЯ

Бастапқы хабарда символдар саны 24, сондықтан хабарды 4 блокқа бөлу керек. Орын ауыстыру 436215 көмегімен шифрлаудың нәтижесі мұндай хабар болады

_ОЕТЭТ_ТЛСКДИШР_ЯФНАЯВОИ

Теорияда, егер блок *d* символдан тұратын болса, онда мүмкін болатын орын ауыстырулар саны

$$d! = 1*2*...*(d-1)*d.$$

Соңғы мысалда d=6, сондықтан орын ауыстырудың

саны 6! = 1*2*3*4*5*6 = 720.

Сонымен, егер қарсылас шифрланған хабарды қолына ұстап алса, онда оған бастапқы хабарды (блок мөлшері белгілі болса) ашып оқу үшін 720 артық емес әрекет қажет болады.

Криптоберіктікті күшейту үшін шифрланатын хабарға екі не одан көп түрлі периоды бар орын ауыстыруларды қолдауға болады.

Орын ауыстырулардың басқа мысалы - кесте бойынша орын ауыстыру. Бұл әдісте бастапқы мәтін кейбір кестенің жолдары бойынша жазылады және ол сол кестенің бағандары бойынша оқылады. Жолдарды толтыру және бағандарды оқу реті әртүрлі болу мүмкін және кілт арқылы беріледі.

Мысал қарастырайық. Кодтау кестеде 4 баған мен 3 жолы болсын (блок мөлшері тең 3*4=12 символ). Мына мәтінді шифрлайық:

ЭТО ТЕКСТ ДЛЯ ШИФРОВАНИЯ

Бастапқы хабарда символдар саны 24, сондықтан хабарды 2 блокқа бөлу керек. Әрбір блокты өзінің кестесіне жолдар бойынша жазайық (2.10 кесте).

Кесте 2.10. Кесте бойынша орын ауыстыру әдісімен шифрлау

1 блок			
Э	Т	О	
Т	Е	К	С
Т		Д	Л
2 блок			
Я		Ш	И
Ф	Р	О	В
А	Н	И	Я

Сосын әрбір блокты кестеден бағандар бойынша оқып отырамыз:

ЭТТТЕ ОКД СЛЯФА РНШОИИВЯ

Бағандарды рет-ретімен емес те оқуға болады, мысалы былай: үшінші, екінші, бірінші, төртінші:

ОКДТЕ ЭТТ СЛШОИ РНЯФАИВЯ

Бұл жағдайда бағандарды оқу реті кілт болып табылады.

Егер хабар ұзындығы блок мөлшеріне еселі болмаса, онда хабарды мағынасын бұзбайтын кейбір символдармен толтыруға болады, мысалы ақ жерілермен. Бірақ, былай істеуге болмайды, өйткені қарсылас криптограмманы ұстап алса, онда пайдаланатың орын ауыстыру кестенің мөлшерін (блок ұзындығын) біліп қояды. Блок ұзындығын анықтағаннан кейін қарсылас блок ұзындығының бөлгіштерінің арасында кілт ұзындығын да (кестенің бағандар санын) табалады.

Орын ауыстыру кестенің мөлшеріне ұзындығы еселі емес хабарды қалай шифрлап дешифрлауға болатының қарап шығайық. Мына сөзді шифрлайық

ПЕРЕМЕНКА

Бастапқы хабарда символдар саны 9. Хабарды кестеге жолдар бойынша жазайық (2.11 кесте), ал соңғы үш ұяшықты бос қалдырамыз.

Кесте 2.11. Кесте бойынша орын ауыстыру әдісімен толық емес блокты шифрлау

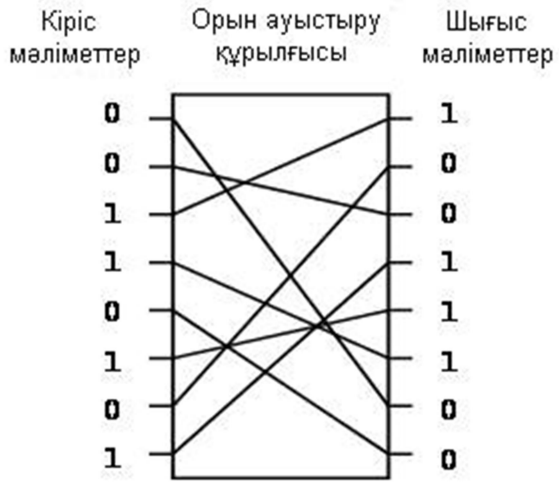
П	Е	Р	Е
М	Е	Н	К
А			

Сосын кестеден баған бойынша рет-ретімен оқып отырамыз:

ПМАЕЕРНЕК

Ашып оқу үшін алдымен толық бағандар санын анықтайды, яғни соңғы жолдағы символдар саның. Ол үшін хабар мөлшерін (біздің мысалда - 9) бағандар санына немесе кілт мөлшеріне (мысалда - 4) бөледі. Бөлудің қалдығы толық бағандар санына тең болады: 9 mod 4 = 1. Сондықтан, біздің мысалымызда бір толық баған және үш қысқа болатын. Енді хабар әріптерің өзінің орнына қоюға және хабарды ашып оқуға болады. Шифрлау кезінде кілт болып 1234 саны болғандықтан (бағандар рет-ретімен оқылды), онда дешифрлау кезінде алғашқы үш символ (ПМА) ауыстыру кестенің бірінші бағанына жазылады, келесі екеуі (ЕЕ) – екінші бағанға, келесі екеуі (РН) – үшіншіге, және соңғы екеуі (ЕК) – төртіншіге. Кестені толтырғаннан кейін жолдарды оқыймыз және бастапқы хабарды ПЕРЕМЕНКА аламыз.

Орын ауыстырудың басқа да тәсілдері бар, оларды бағдарламалық және аппараттық жолмен жүзеге асурыға болады. Мысалы, екілік түрде жазылған деректерді беру кезінде, аппараттық блокты қолдануға ыңғайлы. Бұл блок, сәйкес электр схема көмегімен, белгілі бір түрде бастапқы *n*–разрядты хабардың биттерін араластырады. Былай, егер блок мөлшерін сегіз бит деп алсақ, онда, мысалы, осындай ауыстыру блокты 2.6 суретте көрсетілгендей пайдалануға болады.



Сурет 2.6. Аппараттық ауыстыру блогы

Ашып оқу үшін қабылдау жақта, тізбектер ретін қалпына келтіретің, басқа блок орнатылады.

Тәжірибеде аппаратты жүзеге асыралатын ауыстыру қазіргі кейбір шифрлардың құрама бөлігі ретінде кең пайдаланылады.

Қандай да ауыстыру кезінде шифрланған хабарға ашық мәтіндегі символдар кіріп отырады, бірақ басқа ретте. Сондықтан, тілдің статистикалық заңдылықтары өзгеріссіз қалады. Бұл криптоталдаушыға символдардың дұрыс ретін қалпына келтіру үшін түрлі әдістерді пайдалануға мүмкіндік береді.

Егер қарсыласта шифрлау жүйе арқылы арнайы ауыстыру әдісімен таңдап алынған хабарларды өткізуге мүмкіндігі бар болса, онда ол таңдап алынған мәтін бойынша шабуыл жасай алады. Егер бастапқы мәтінде блок ұзындығы *N* символға тең болса, онда кілтті ашу үшін бастапқы мәтіннің *N*-1 блогын (оларда біреуінен басқа, барлық символдар бірдей) шифрлау жүйе арқылы өткізуге жеткілікті.

Егер *N* блогының ұзындығы алфавит символдар санынан кем болса, онда таңдап алынған мәтін бойынша шабуылдың басқа варианты болу мүмкін. Бұл жағдайда алфавиттың әртүрлі әріптерінен бір арнайы хабарды жасауға болады (мысалы, оларды

алфавиттегідей рет-ретімен орналастырып). Осылай дайындалған хабарды шифрлау жүйе арқылы өткізіп, криптоталдаушыға шифрлаудан кейін алфавит символдары қандай позицияда табылғанын ғана көруге қалады, және ауыстыру схемасын салуға ғана қалады.

Сонымен, біз симметриялық шифралудың жалпы схемасын және жабық кілті бар қарапайым шифрлау әдістерінің жіктеуін қарап шықтық.

Негізгі терминдер

Гаммалау – ашық мәтінге гамма тізбегін «салуына» негізделген шифрлау әдісі. Әдетте бұл қандай да шекті алаңда қосындылау (модулі бойынша қосындылау). Мысалы, GF(2) алаңда осындай қосындылау кәдімгі «шығарып тастайтын ИЛИ» түрге келеді. Ашып оқуда операция қайталанады, нәтижесінде ашық мәтін алынады.

Пропорционал немесе **монофониялық шифрлар** – ауыстыру әдістері, оларда шифрланған белгілердің кездесу жиілігі теңестіріледі.

Орнына қою (**ауыстыру**) **шифрлар** әдетте блоктарға бөлінген және бір алфавитта жазылған бастапқы мәтіннің символдары басқа алфавиттың бір не бірнеше символдары мен, қабылданған түрлендіру ережеге сәйкес, ауыстыруға негізделген.

Көп алфавитты орнына қою (не ауыстыру) шифры - бастапқы мәтіннің символдарын белгілі ереже бойынша ауыстыру үшін бір емес, бірнеше әліпби пайдаланатын шифрлау әдістерінің тобы.

Орын ауыстыру шифры – бұл шифрда бастапқы мәтіннің кіріс ағыны блоктарға бөлінеді, олардың әрбіреуінде символдардың орын ауыстыруы орындалады. Осындай шифрдың кілті шифрлауда пайдаланатын және орын ауыстыруды көрсететін орын ауыстыру матрица немесе векторы болып табылады.

Қарапайым (не біралфавитты) орнына қою шифры, моноалфавитты шифр – шифрлау әдістерінің тобы, оларда белгілі алгоритм бойынша шифрлау кестесі жасалынады, бұл кестеде ашық мәтіннің әрбір әрпі үшін оған сәйкес шифрмәтіннің бір ғана әрпі болады. Шифрлауда әріптер кестеге сәйкес ауыстырылады. Ашып оқу үшін сол кестені немесе оны жасайтың алгоритмды білу жеткілікті.

Симметриялық шифрлау (жабық кілті бар шифрлау) – деректерді қайтымды түрлендіру әдістері, оларда бірдей кілт пайдаланады, оны ақпараттық алмасудағы жақтар жаудан құпиялы түрде сақтау керек. Тарихтан белгілі барлық шифрлар, мысалы, Цезарь шифры – бұл жабық кілті бар шифрлар.

Сұрақтар

1. Симметриялық шифрлаудың жалпы схемасын түсіндіріңіз.
2. Жабық кілті бар шифрлау әдістерінің қандай ортағы бар?
3. Жабық кілті бар шифрлау әдістерінің негізгі топтарын айтыңыз.
4. Орын ауыстыру шифрдың мысалдарын көрсетіңіз.
5. Орнына қою шифрлау әдістерінің жалпы принциптерін айтып беріңіз.
6. Көп алфавитты орнына қоюларды қалай түсінесіз.
7. Бір алфавитты орнына қою шифрдың мысалын келтіріңіз.
8. Орын ауыстыру шифрлаудың түрлі алгоритмын бейнелеп беріңіз. Кейбір хабарды осы әдіспен шифрлау мысалын келтіріңіз. Бұл әдісте ашып оқу алгоритмы қандай?
9. Вижинер кестесін пайдалану әдісі қандай жабық кілті бар шифрлау әдістерінің тобына жатады? Бұл әдісте шифрлау және дешифрлау алгоритмы қандай? Кейбір хабарды осы әдіспен шифрлау мысалын келтіріңіз.
10. Кестелік орын ауыстыру әдіспен хабарды қалай шифрлауға және дешифрлауға болады, егер шифрланатын хабардың мөлшері блок көлеміне еселі болмаса?
11. Монофониялық шифр деген не?

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.