Дәріс 2. Негізгі қол шифрлары

Дәріс жоспары:

1. Цезарь шифры
2. Тритемий шифры
3. Виженер шаршысы
4. Плейфер шифры
5. «Қос шаршы» әдісі

Цезарь шифры

Цезарь шифры – ашық мәтіннің әр әрпін алфавиттегі позициялардың белгіленген санына ауыстырылған басқа әріппен ауыстыру үшін қолданылатын шифрдың оқулық мысалы [12]. Ол келесідей анықталады: берілген ауысым (кілт) үшін бастапқы мәтіннің әр әрпі алфавит бойынша берілген позициялар санына сәйкес келетін әріппен ауыстырылады. А ашық мәтіннің әріп нөмірін, n алфавиттегі әріптер санын, $k, k < n$ кейбір сандарды көрсетеді. Содан кейін ашық мәтіннің А әрпінің нөмірі (1.1), (1.2) формулалары бойынша шифрланған мәтіннің әрпін (кодын) анықтайды:

$$\text{егер } c \leq n, c = a + k, \quad (1.1)$$

$$\text{егер } c > n, c = a + k - n. \quad (1.2)$$

Мұндағы k саны криптографиялық жүйенің кілті деп аталады.

Цезарь шифрінің мағынасы ашық мәтіннің кез келген әрпі өзіне қатысты k әріппен ауыстырылады.

Мысал. k кілті 7–ге тең болсын, сонда *алфавит* сөзі Цезарь шифры арқылы *зжзж* сөзіне айналады. *б* әрпінің коды 2, ал *а* әрпінің коды 1, *з* және *ж* әріптері *б* және *а*–ға қатысты жеті позицияға жылжытылады. Содан кейін шифрланған жазбаның әріптік кодтары келесідей анықталады:

б+k = 2+7 = 9 саны *з* әрпіне, ал $a + k$ = 1+7 = 8 саны *ж* әрпіне сәйкес келеді.

Кері шифрлау $a = c - k$ формуласы бойынша жүретінін ескеріңіз.

Цезарь шифры қарапайым алмастыру шифрлары деп аталатын шифрлар класының мүшесі. Цезарь шифры үшін ыңғайлырақ кестелік пішінді пайдалануға болады. Егер n мәні алфавиттегі әріптер саны, ал k мәні кілт болса, онда әліпбиді k баған және $t = n/k$ жолдармен төртбұрышты кестеге жазамыз. Қажет болса, n/k бүтін сан болмаса, жолдар санын көбейтуге болады. Жолдар саны артқан сайын пайда болатын кестенің бос квадраттары, мысалы, тыныс белгілерімен немесе латын әріптерімен немесе басқа әліпбимен толтырылуы мүмкін.

Бұл жағдайда шифрлау алгоритмі өте қарапайым. Ашық мәтіндік әріп сол бағандағы таңбамен ауыстырылады, бірақ ол әріптен төмен. Ашық мәтіндік әріп соңғы жолда болса, ол сол бағанның жоғарғы әрпімен ауыстырылады (1.2–кесте).

1.2 – кесте. ASCI символ кестесі

А	Б	В	Г	Д
Е	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	,	.

Содан кейін *Я мыл раму.* келесі шифрлау алынады: *В с,р хесшд*

Бұл жағдайда кілт кестенің өлшемі және ондағы әріптердің орналасуы екенін ескеріңіз.

Жалпы жағдайда кестедегі әріптер кездейсоқ орналасуы мүмкін. Кестені қолдана отырып ұсынылған шифрлау схемасын келесідей сипаттауға болады. Егер ашық мәтіндік әріптің (i, j) кестесінде координаталары болса, мұндағы i – жол нөмірі және j – баған нөмірі, онда ол координаталы әріпке $(i + 1, j)$, егер i соңғы жол нөміріне сәйкес келсе координаттары $(1, j)$ әріпке айналады.

Тритемий шифры

Бекітілген кілт үшін қарапайым ауыстыру шифрында k алфавиттің кез-келген әрпі, ашық мәтінде қай жерде кездессе де, әрқашан сол немесе басқа алфавиттің бірдей әрпіне айналады. Шын мәнінде, алфавит әріптерінің қарапайым түрленуі орын алады [13]. Сондықтан қарапайым ауыстыру шифрын шифрланған мәтіндегі таңбалардың пайда болу жиілігін есептеу арқылы бұзу оңай. Кез-келген тілде әр түрлі әріптер әр түрлі жиілікте кездеседі. А таңбасын түрлендіру (1.3) формуласы бойынша жүзеге асырылады.

$$\gamma = \alpha + k \qquad (1.3)$$

Бұл формула α әрпінің пайда болу жиілігін γ белгісінің пайда болу жиілігіне автоматты түрде «тасымалдайды». Нәтижесінде, шифрланған мәтінді талдау кезінде үлгілер мен жиілік сипаттамаларын анықтауға болады, бұл қарапайым ауыстыру шифрын криптоанализге осал етеді.

XVI ғасырда Аббат Йоханнес Тритемиус көп алфавиттік ауыстыру шифрларының класына негіз болатын шифрлау әдісін ұсынды. Тритемия «Тритемия кестесі» деп аталатын кесте құрды. Орыс алфавиті үшін ол келесідей (Ү және е әріптері жоқ):

АБВ Г Д Е Ж З И К Л М Н О П Р С Т У Ф Х Ц Ч Ш Щ Ъ Ы Ь Э Ю Я
БВ Г Д Е Ж З И К Л М Н О П Р С Т У Ф Х Ц Ч Ш Щ Ъ Ы Ь Э Ю Я А
ВГД Е Ж З И К Л М Н О П Р С Т У Ф Х Ц Ч Ш Щ Ъ Ы Ь Э Ю Я А Б
ГДЕ Ж З И 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
ДЕЖ З И 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 Г
ЕЖЗИ 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 Г Д
ЖЗ И 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 Г Д Е
ЗИК Л М Н О П Р С Т У Ф Х Ц Ч Ш Щ Ъ Ы Ь Э Ю Я А Б В Г Д Е Ж
ИКЛ М Н О П Р С Т У Ф Х Ц Ч Ш Щ Ъ Ы Ь Э Ю Я А Б В Г Д Е Ж З
КЛМ Н О П Р С Т У Ф Х Ц Ч Ш Щ Ъ Ы Ь Э Ю Я А Б В Г Д Е Ж З И
ЛМНО П Р С Т У Ф Х Ц Ч Ш Щ Ъ Ы Ь Э Ю Я А Б В Г Д Е Ж З И К
МНОПР С Т У Ф Х Ц Ч ШЩ Ъ Ы Ь Э Ю Я АБ В Г Д Е Ж З И К Л
НОП Р С Т У Ф Х Ц Ч Ш Щ Ъ Ы Ь Э Ю Я А Б В Г Д Е Ж З И К Л М
ОП Р С Т У Ф Х Ц Ч Ш Щ Ъ Ы Ь Э Ю Я А БВ Г Д Е Ж З И К Л М Н
ПРС Т У Ф Х Ц Ч Ш Щ Ъ Ы Ь Э Ю Я А Б В Г Д Е Ж З И К Л М Н О
РСТ У Ф Х Ц Ч Ш Щ Ъ Ы Ь Э Ю Я А Б В Г Д Е Ж З И К Л М Н О П
СТУ Ф Х Ц Ч Ш Щ Ъ Ы Ь Э Ю Я А Б В Г Д Е Ж З И К Л М Н О П Р
ТУФ Х Ц Ч Ш Щ Ъ Ы Ь Э Ю Я А Б В Г Д Е Ж З И К Л М Н О П Р С
УФХ Ц Ч Ш Щ Ъ Ы Ь Э Ю Я А Б В Г Д Е Ж З И К Л М Н О П Р С Т
ФХЦ Ч Ш Щ Ъ Ы Ь Э Ю Я А Б В Г Д Е Ж З И К Л М Н О П Р С Т У
ХЦЧ Ш Щ Ъ Ы Ь Э Ю Я А Б В Г Д Е Ж З И К Л М Н О П Р С Т У Ф
ЦЧШ Щ Ъ Ы Ь Э Ю Я А Б В Г Д Е Ж З И К Л М Н О П Р С Т У Ф Х
ЧШЩЪ Ы Ь Э Ю Я А Б В Г Д Е Ж З И К Л М Н О П Р С Т У Ф Х Ц
ШЩЪЫ Ь Э Ю Я А Б В Г Д Е Ж З И К Л М Н О П Р С Т У Ф Х Ц Ч
ЩЪЫ Ь Э Ю Я А Б В Г Д Е Ж З И К Л М Н О П Р С Т У Ф Х Ц Ч Ш
ЪЫЬЭ Ю Я А Б В Г Д Е Ж З И К Л М Н О П Р С Т У Ф Х Ц Ч Ш Щ
ЫЬЭ Ю Я А Б В Г Д Е Ж З И К Л М Н О П Р С Т У Ф Х Ц Ч Ш Щ Ъ
ЬЭЮ Я А Б В Г Д Е Ж З И К Л М Н О П Р С Т У Ф Х Ц Ч Ш Щ Ъ Ы
ЭЮЯА Б В Г Д Е Ж З И К Л М Н О П Р С Т У Ф Х Ц Ч Ш Щ Ъ Ы Ь
ЮЯА Б В Г Д Е Ж З И К Л М Н О П Р С Т У Ф Х Ц Ч Ш Щ Ъ Ы Ь Э
Я АБ ВГ Д ЕЖЗ И КЛМ НОПРСТУФХЦЧШЩЪЫЬ ЭЮ

Кестенің бірінші жолы ашық мәтінге арналған әріптер тізбегі болып табылады. Әрі қарай, ашық мәтіннің бірінші әрпі кестенің бірінші жолының көмегімен, екінші әрпі екінші жолдың көмегімен, үшінші әрпі үшінші жолдың көмегімен және т.б. Егер ашық мәтіндік әріптің бірінші жолда координаттары болса $(1, j)$, онда i жолда ол координаттары (i, j) әріпімен ауыстырылады. Басқаша айтқанда, бірінші жолдағы j саны бар әріп i жолдағы j саны бар әріппен ауыстырылады. Соңғы жол қолданылғаннан кейін ол бірінші жолға оралады. Бұл шифрлау әдісімен бірдей ашық мәтін әрпін әртүрлі әріптерге түрлендіруге болады. Осылайша, осы шифрлау схемасы бар «*мама*» сөзі «*мбог*» сөзіне түрлендіріледі.

Сипатталған шифрлау опциясында кілт жоқ екенін ескеріңіз. Кейіннен шифр бастапқы алфавиттің әріптерінің ерікті реті мен шифрлау кезінде жолдардың ретін таңдаудың күрделілігіне негізделген күрделірек болды.

Виженер шаршысы

Виженер шаршысы Тритемиялық кесте сияқты циклдік ауысқан алфавиттерден тұрады. Бірінші жол әліпбидің жолы болып табылады, ал i-ші жол бір таңбаны солға циклдік жылжыту арқылы $(i-1)$ жолдан алынады. Бірінші жол оны құрайтын әріптердің кез келген реті бар алфавит болуы мүмкін. Бірінші жол ашық мәтін әріптері үшін, ал осы кестенің бірінші бағанасы кілт алфавиті үшін пайдаланылады.

Шифрлау ережесі келесідей. Егер ашық мәтіндік әріптің координатасы $(1, j)$, ал негізгі әріптің координаты $(i, 1)$, болса, онда шифр белгісі i-ші жол мен j қиылысында орналасқан әріп болады. Мұнда ашық мәтіннің әрбір әрпі кілттің белгілі бір әрпіне сәйкес келеді деп есептеледі. Әрине, әліпби әртүрлі тілдердің кез келген бар таңбалары мен әріптерінен тұруы мүмкін.

Мәтіннің шифры келесі схема бойынша шешіледі. Кілт координатасы $(i,1)$ жол нөмірін анықтайды, ал осы жолдан (i,j) шифрлық әріп координатасы $(1,j)$ координатасы бар ашық мәтін әріпі анықталатын баған нөмірін анықтайды.

Шифрлау кестелері

Сциталь шифрын, бұрын айтылғандай, сәл басқаша түсіндіруге болады, $n \times m$ саны ашық мәтіндік әріптер санына тең болатындай n жол және m бағаннан тұратын кестені алайық. Кестеден мәтінді оқудың белгілі бір ретін анықтасақ, шифрленген мәтін аламыз. Бұл шифрлау схемасында кілт-кестенің құрылымы, яғни оның өлшемі және «оқу бағыты». Сциталь шифры мәтінді баған бойынша оқу әдісіне сәйкес келеді (1.3 кестені қараңыз).

1.3 – кесте. 4 жол мен 4 бағаннан тұратын кестені қарастырайық

	1	**2**	**3**	**4**
1	П	Р	И	Е
2	З	Ж	А	Ю
3	α	Ш	Е	С
4	Т	О	Г	О

α таңбасы бос орын үшін пайдаланылады. Бұл кестеде мәтін кірістірілген

Приезжаю шестого

Бірінші оқу маршруты баған нөмірлері бойынша жүзеге асырылады. Бағандар ретімен нөмірленеді. Бұл жағдайда сіз келесі мәтінді аласыз

Пзатржшоиаегеюсо

Заңды пайдаланушы алынған мәтінді бағандарға жазады және хабарламаны жолдар бойынша оқиды.

Екінші есептеу бағыты баған нөмірлері бойынша жүзеге асырылады. Бағандар кездейсоқ нөмірленеді, яғни баған нөмірлері ауыстырудың қандай да бір түрін құрайды. Бұл жағдайда 1.4 – кесте келесідей болады:

1.4 – кесте. Баған номері бойынша екінші есептеу бағыты

	3	**1**	**4**	**2**
1	П	Р	И	Е
2	З	Ж	А	Ю
3	α	Ш	Е	С
4	Т	О	Г	О

Нәтиже келесі шифрлық мәтін болып табылады

Ржшоеюсопзαтиаег

Үшінші оқу жолы кездейсоқ нөмірленетін жол нөмірлерімен, содан кейін кездейсоқ нөмірленетін баған нөмірлерімен анықталады. Бұл жағдайда 1.4 – кесте келесідей болады:

1.5 – кесте. Баған номері бойынша үшінші есептеу бағыты

	3	**1**	**4**	**2**
1	П	Р	И	Е
2	З	Ж	А	Ю
3	α	Ш	Е	С
4	Т	О	Г	О

Бұл жағдайда жолдар алдымен сандық ретпен орналасады. Нәтижесінде біз келесі кестені аламыз.

1.6 – кесте. Баған номері бойынша төртінші есептеу бағыты

	3	**1**	**4**	**2**
1	Т	О	Г	О
2	П	Р	И	Е
3	З	Ж	А	Ю
4	α	Ш	Е	С

Содан кейін мәтінді нөмірлеу тәртібімен бағандарға жазамыз. Біз келесі мәтінді аламыз

Оржшоеюстпзαгиае

Төртінші оқу маршрутын бұрын берілген кестелердің кез келгені үшін орнатуға болады. Ол келесідей: оқу матрицаның диагональдары бойынша кез келген бұрыштық әріптен жасалады. Шындығында, оқу маршруттарының әртүрлі нұсқалары мүмкін және біз олардың бірнешеуін ғана тізімдедік. Барлық жағдайларда түрлендірілген мәтінді декодтау кері тәртіпте орындалады. Бұл әдістердің барлығы ауыстыру шифрларына қатысты.

Қорытындылай келе, жазушылардың айтуынша, күнделікті жұмыс режимінде шағын көлемдегі ақпаратты жедел және сенімді түрде шифрлау үшін пайдалануға болатын сенімді шифрлау кестесінің мысалын келтірейік. Ұсынылған кестеде бағандарды кездейсоқ нөмірлеуден басқа, кейбір ұяшықтар толтырылмаған күйінде қалады. Бұл тәсіл мүмкін кілттердің санын

едәуір арттырады, өйткені кесте өлшемі мен баған нөмірлеу тәртібінен басқа, пайдаланылмаған ұяшықтардың саны мен орналасуы қосымша кілт параметрлеріне айналады. Мұндай кестенің мысалы төменде келтірілген (1.7 кестені қараңыз).

1.7 – кесте. Блоктық шифрлау жүйелері

	3	10	4	2	9	8	1	6	7	5
1	Ф	И	Р	М	♦	А	α	Б	А	♦
2	Р	♦	С	α	С	К	О	♦	Р	О
3	ß	О	Б	О	Н	♦	♦	К	Р	О
4	♦	Т	И	Т	С	Я	ω	α	Н	Е
5	α	В	Ы	♦	Д	А	В	А	♦	Т
6	Т	Е	ß	К	Р	Е	Д	И	Т	А
7	ω	♦	♦	♦	.	Н	О	В	И	♦
8	♦	К	♦	♦	О	В	.	α	ß	♦

Қарастырылған ағындық шифрлардан басқа, блоктық шифрлау жүйелері де бар. Деректерді биттік немесе таңбалық түрде өңдейтін ағындық әдістерден айырмашылығы, блоктық жүйелер белгіленген ұзындықтағы таңбалар блоктарын түрлендіреді. Бұл шабуылға төзімділікке қол жеткізуге мүмкіндік береді, әсіресе әртүрлі жұмыс режимдерін пайдалану кезінде. Қазіргі криптографияда мұндай жіктеу өзектілігін сақтайды және ақпаратты қорғау үшін блоктық Алгоритмдер кеңінен қолданыла береді.

Плейфер шифры

Плейфер шифры үшін $N = n \times m$ өлшемді кесте құрылады. Мұнда n жолдар саны, m бағандар саны. N саны әліпбидегі таңбалар санына сәйкес келуі керек. Кестедегі алфавит таңбалары кездейсоқ реттелген. Кестенің өлшемі және ондағы белгілердің орналасуы осы криптографиялық жүйенің кілті болып табылады.

Әрі қарай, шифрлау алгоритмі келесідей. Ашық мәтін әрқайсысы екі таңбадан тұратын блоктарға бөлінген. Мұндай блок биграмма деп аталады. Егер соңғы блокта бір таңба болса, онда ол жойылады (мүмкіндігінше) немесе ашық мәтіннің мазмұнына әсер етпейтін бір таңба қосылады. ab таңбалары ашық мәтін биграммасы болсын.

Кестедегі a және b символының координаталары анықталған. а символының координаталары сандар (i, j), ал b символының координаталары (t, q) болсын.

Бұл жағдайда, егер:

$i \neq t$ және $j \neq q$ (биграмманың әріптері кестенің әртүрлі жолдарында және әртүрлі бағандарында орналасқан), содан кейін биграмманың a таңбасы координаталары (i, q) бар кесте таңбасына, ал b символы (t, j) координаталарымен символға өтеді;

$i \neq t$ және $j \neq q$ (биграмма әріптері бір жолда, бірақ әртүрлі кесте бағандарында), содан кейін а биграмма таңбасы координаталары бар кесте таңбасына $(i, j+1)$, ал b символы символға өтеді координаталарымен $(t, q+1)$. Егер $j = m$ немесе $q = m$ болса, онда жаңа символдардың координаталары $(i, 1)$ немесе $(t, 1)$ тең болады;

$i \neq t$ және $j \neq q$ (биграмманың әріптері әртүрлі жолдарда, бірақ кестенің бір бағанында), содан кейін биграмманың a таңбасы координаталары бар кесте таңбасына $(i+1, j)$ өтеді және b символын координаталары бар таңбаға $(t+1, q)$. Егер $i = n$ немесе $t = n$ болса, онда жаңа символдардың координаталары сәйкесінше $(1, j)$ немесе $(1, q)$ тең болады. (i, j) координаталары бар екі бірдей әріптер $(i+1, j)$ координаталары бар екі бірдей әріптерге түрлендіріледі;

Мәтінді кері шифрлау дәл осылай жүреді. Түрлендірілген мәтін екі таңбадан тұратын блоктарға бөлінген. Содан кейін шифрланған таңбалардың координаталары арқылы ашық мәтіндік таңбалар бірдей реттілікпен анықталады.

«Қос шаршы» әдісі

«Қос шаршы» әдісі үшін $N = n \times m$ өлшемді екі кесте құрылады, мұндағы n жолдар саны, m бағандар саны. N кестелеріндегі элементтер саны алфавиттегі таңбалар санына сәйкес келуі керек. Кестелердегі алфавит таңбалары кездейсоқ орналасады және олардың реті алфавитке сәйкес келмеуі керек. Кестелердің өлшемдері және олардағы таңбалардың орналасуы берілген криптографиялық жүйенің кілті болып табылады. Бір кесте сол (нөмір 1), екіншісі оң (нөмір 2) деп аталады.

Әрі қарай, шифрлау алгоритмі келесідей. Ашық мәтін әрқайсысы екі таңбадан тұратын блоктарға бөлінген. Мұндай блок биграмма деп аталады. Егер соңғы блокта бір таңба болса, онда ол жойылады (мүмкіндігінше) немесе ашық мәтіннің мазмұнына әсер етпейтін бір таңба қосылады. ab таңбалары ашық мәтін биграммасы болсын.

Бірінші кестеде a биграммасының бірінші таңбасы орналастырылған. Бірінші кестедегі осы таңбаның координаталары (i, j) сандар жұбы болсын. Екінші биграмма b символы екінші кестеде орналастырылған. Бірінші кестедегі осы таңбаның координатасы сандар жұбы (t, j) болсын.

Бұл жағдайда, егер:

$i \neq t$ (биграмма әріптерінің жол нөмірлері сәйкес келмейді, ал биграмма әріптері орналасқан бағандардың нөмірлері ерікті), содан кейін биграмма таңбасы координаталары бар екінші кестенің символына өтеді (i, q), ал b символы координаталары (t, j) бірінші кестенің символына түседі;

$i = t$ және $j \neq q$ (биграмманың әріптері бірдей сандары бар жолдарда, бірақ кесте бағандарының саны әртүрлі), содан кейін биграмманың а таңбасы координаталары бар екінші кестенің символына өтеді (i, j), ал b символы координаталары (t, q) бірінші кестенің символына.

$i = t$ және $j = q$ (биграмманың әріптері сандары бірдей жолдар мен бағандарда орналасқан), содан кейін биграмманың a және b таңбалары қайта реттеледі. Мәтіннің шифры бірдей ережелер бойынша шешіледі, оның жалғыз айырмашылығы шифрлық мәтіннің биграммасының бірінші әрпі оң (екінші) кестеде, ал биграмманың екінші әрпі бірінші (сол) кестеде орналасқан.

«Қос шаршы» криптографиялық жүйе бұзуға өте төзімді. Оны компьютерде бағдарлама ретінде орындау оңай. Бұл жағдайда барлық пернетақта таңбаларын алфавит таңбаларына қосуға болады.

Қолданылған әдебиеттер тізімі

1. Кац Дж., Линделл Ю. Введение в современную криптографию. / Кац Дж. – М.: Триумф, 2018. – 342 с.

2. Бонех Д., Шуп В. Аспирантура по прикладной криптографии. / Бонех Д. – Спрингер, 2020. – 514 с.

3. Менезес А., Ван О., Ванстон С.А. Справочник по прикладной криптографии. / Менезес А. – ЦРК: Пресс, 2018. – 516 с.