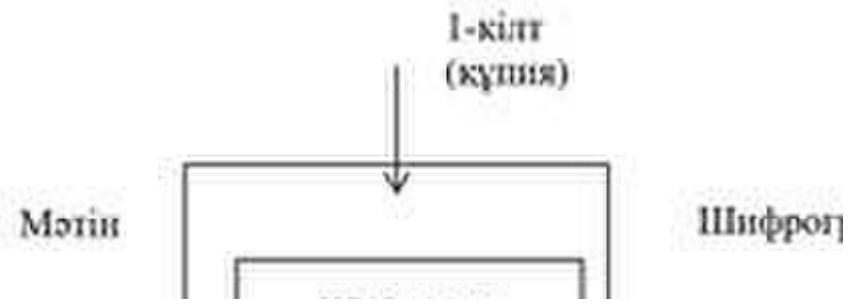
Практикалық жұмыс №8

Тақырыбы: Кілттерді генерациялау үшін аппараттық-бағдарламалық құралдарды пайдалану. E-mail-мен хабарлар алмасу кезінде ЭЦҚ-ны және шифрлауды қолдану
Мақсаты: Ақпаратты қорғаудың криптографиялық әдістерінменгеру.

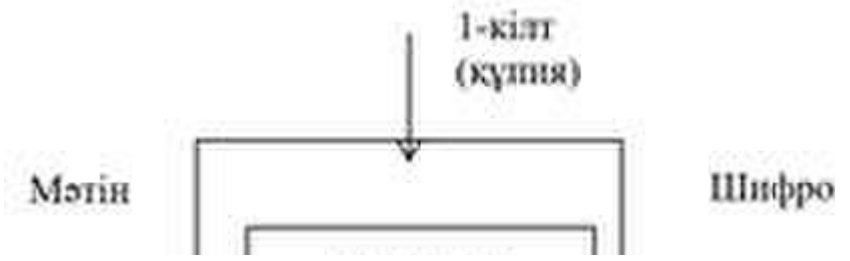
Сипаты бойынша шифрлеу алгаритімінің кілтін қолдану екі түрге бөлінеді: симметриялық (бір кілтпен, басқаша-құпия кілтпен) және симметриялық емес. Шифрлеудің және дешифрлеудің симметриялық емес алгоритмдерін әдетте ассиметриялы деп атайды.

Бірінші жағдайда, жіберуші шифраторы мен алушы дешифраторында тек бір кілт қана қолданылады. Шифратор ашық мәтіннің функциясы болып табылатын шифрограмманы құрады. Түрлендіру (шифрлеу) функциясының нақты түрі құпия кілтпен анықталады. Хабарды алушы дешифраторы, шифраторда орындалған түрлендіру қатынасы бойынша кері түрлендіруді орындайды. Құпия кілт құпия сақталады және хабарлама жіберуші қарсыластың криптоаналитиктің немесе комерциялық бәсекелестің кілтін ұстап алумен шектелетін канал бойынша алушыға беріледі.



1 – сурет – Симметриялы шифрлеу

Екінші жағдайда (ассиметриялы алгоритмді қолданғанда) хабар алушы алғашында ашық канал бойымен, ақпаратты штфрлейтін ашық кілтті хабар берушіге береді. Ақпаратты алған уақытта хабар алушы оны екінші құпия кілт көмегімен де шифрлейді. Қарсыластың криптоаналиктігінің ашық кілтті ұстап алуы жабық хабарламаны дешифрлеуге мүмкіндік бермейді, себебі ол тек екінші құпия кілтпен құпияланады. Сонымен бірге, құпия кілтті практика түрінде ашық кілт көмегімен есептеу мумкін емес.



2 – сурет – Симметриялы емес шифрлеу

Криптожүйелік әдістер

Цезарьдың алмастырып қою әдісі

Цезарьдың алмастырып қою әдісі өте қарапайым әдіс болып табылады. Олар *моно алфавиттік алмастырып қою тобына жатады*.

Цезарьдың алмастырып қоюы рим императоры Гай Члий Цезарь есімімен байланысты, ол Марк Туллий Цицеронға C_3 алмастырып қоюды пайдаланып жолдау хат құруды тапсырған.

Алмастырып қою сәйкесінше "***бастапқы мәтін → шифрленген мәтін***" әріптер жұбынан тұратын орнына қою кестесі бойынша анықталады. C_3 үшін алмастырып қою 1-кестеде берілген. Бағыттауыш (→) бастапқы мәтін әріптері (сол жақтағы) C_3 көмегімен шифрленген мәтін (оң жақтағы) әріптерімен шифреленетіндігін білдіреді.

Анықтама. *Цезарь жүйесі* деп, бастапқы $(x_0, x_1, .., x_{n-1})$ мәтіннің *n*-граммын шифрленген $(y_0, y_1, ..., y_{n-1})$ мәтінінің *n*-граммына, $y_i=C_k(x_i)$, $0i<n$ ережесіне сәйкес түрлендіретін моно алфавиттік алмастырып қоюды айтады.
Мысалы, «ВЫШЛИТЕ_НОВЫЕ_УКАЗАНИЯ» C_3 алмастырып қою көмегімен «еюыолхиврсеюивцнгкгрлб» түрленеді.
Кесте 1.

А→г	Й→м	Т→х	Ы→ю
Б→д	К→н	У→ц	Ь→я
В→е	Л→о	Ф→ч	Э→_
Г→ж	М→п	Х→ш	Ч→а
Д→з	Н→р	Ц→щ	Я→б
Е→и	О→с	х→ъ	_→в
Ж→й	П→т	Ш→ы	
З→к	Р→у	Щ→ь	
И→л	С→ф	Ъ→э	

Көп алфавиттік жүйелер. Бір рет қолданылатын жүйелер.

Моно алфавиттік алмастырып қоюдың әлсіз криптотұрақтылығы көп алфавитті алмастырып қоюды қолданумен игеріледі.

Көп алфавитті алмастырып қою екіден көп әр түрлі алмастырып қоюдан тұратын $=(_1, _2, ...)$ кілтпен анықталады.

Бір рет қолданылатын жүйе $X=(X_0, x_1, ..., x_{n-1})$ бастапқы мәтінін шифрленген $Y=(Y_0, y_1, ..., y_{n-1})$ мәтініне түрлендіреді.

Шексіз кілтпен шифрлеу мысалын қарастырайық. Кілт ретінде "**БЕСКОНЕЧНЫЙ_КЛЮЧ....**" мәтінін алайық.
Оның көмегімен "**ШИФР_НЕРАСКРЫВАЕМ**" мәтінін шифрлейміз. Шифрлеуді кесте түрінде дайындаймыз:
ШИФРУЕМЫЙ_ТЕКСТ 24 8 20 16 19 5 12 27 9 32 18 5 10 17 18

БЕСКОНЕЧНЫЙ_КЛЮЧ 1 5 17 10 14 13 5 23 13 27 9 32 10 11 30
ЩРДЪАТТССЦЪЫДФЫП 25 13 4 26 0 18 17 17 22 26 27 4 20 28 15

Вижинер алмастырып қою әдісі

Қолданушы кілті деп аталатын кілттің $k = (k_0, k_1, ..., k_n)$ соңғы тізбегінен бастайық, және оны тізбекті қайталай отырып, шексіз тізбелікке дейін созайық. Осылайша, $k = (k_0, k_1, ..., k_n)$, $k_j = k_{(j \bmod r)}$, 0 j жұмыс кілтін аламыз.
Мысалы, $r =$ и болғанда қолданушының 15 8 2 10 11 4 18 кілтінде жұмыс кілті келесі периодтық тізбек болады:

15 8 2 10 11 4 18 15 8 2 10 11 4 18 15 8 2 10 11 4 18 ...

Анықтама. Вижинер алмастырып қою әдісі $VIG_k : (x_0, x_1, ..., x_{n-1})$ $(y_0, y_1, ..., y_{n-1}) = (x_0+k, x_1+k, .., x_{n-1}+k)$ ретінде анықталады.
Ендеше:
1) x бастапқы мәтін r *фрагменттеріне* $x_i = (x_i, x_{i+r}, ..., x_{i+r(n-1)})$, 0 i $< r$ бөлінеді;
2) бастапқы мәтіннің і-ші фрагменті x_i Цезарь алмастырып қою көмегімен шифрленеді $C_k : (x_i, x_{i+r}, ..., x_{i+r(n-1)})$ $(y_i, y_{i+r}, ..., y_{i+r(n-1)})$,
Мысал. Вижинера алмастырып қою көмегімен мәтінді түрлендіру (r=4)
Бастапқы мәтін (БМ1):
НЕ_СЛЕДУЕТ_ВЫБИРАТЬ_НЕСЛУЧАЙНЫЙ_КЛЮЧ
Кілт: КЛЮЧ
Бастапқы мәтінді 4 символдар бойынша блоктарға бөлеміз:
НЕ_С ЛЕДУ ЕТ_В ЫБИР АТЬ_ НЕСЛ УЧАЙ НЫЙ_ КЛЮЧ
Және оларға кілтті қолданамыз (Вижинер кестесін қолданып): Н+К=Ч, Е+Л=Р және т.б..
Шифрленген мәтінді (ШМ1) аламыз:
ЧРЭЗ ХРБЙ ПЭЭЩ ДМЕЖ КЭЩЦ ЧРОБ ЭБЧ_ ЧЕЖЦ ФЦЫН

Полибий квадраты.

Шифрлеу үшін 1-ден 5-ке дейін нөмірленетін алты бағаннан және алты жолдан тұратын квадратты беретін кестені қолданамыз. Әр торға бір әріп жазылады. Нәтижесінде әр әріпке сандар жұбы сәйкес келу керек және шифрлеу әріпті сандар жұбымен алмастыруға алып келу керек. Полибий квадратында символдарды орналастыру реті құпия кілт болып табылады.

	1	2	3	4	5	6
1	А	Б	В	Г	Д	Е
2	Ё	Ж	З	И	Й	К
3	Л	М	Н	О	П	Р
4	С	Т	У	Ф	Х	Ц
5	Ч	Ш	Щ	Ъ	Ы	Ь
6	Э	Ю	Я	.	,	_

Полибий квадратының көмегімен «КРИПТОГРАФИЯ» сөзін жасырайық.

Нәтижесінде алатынымыз:

26 36 24 35 42 34 14 36 11 44 24 63

Мысалдан криптожүйедегі бірінші сан жол нөмірін, ал екінші сан баған нөмірін беретінін көруге болады.

Қайта қою әдісі.

Криптографияның осы әдісін ойлап табу, ашылған мәтінді жазу және шифровканы әрі қарай санау кейбір геометриялық фигураның (мыслы, шаршының) ішінде әр түрлі жолдармен жүргізілуімен беріледі

Ойды түсіндіру үшін 8*8 өлшемді шаршылық кестені (матрицаны) аламыз, мәтінді жоғарыдан төменге жол бойынша тізбектеп жазамыз, ал – санауды солдан оңға қарай бағана бойынша жүргіземіз.

Келесі хабарды шифрлеу керек болсын дейік:

НА ПЕРВОМ КУРСЕ ТЯЖЕЛО УЧИТЬСЯ ТОЛЬКО ПЕРВЫЕ ЧЕТЫРЕ ГОДА ДЕКАНАТ.

Мұны матрица түрінде жазайық:

Н	А	_	П	Е	Р	В	О
М	_	К	У	Р	С	Е	_
Т	Я	Ж	Е	Л	О	_	У
Ч	И	Т	Ь	С	Я	_	Т
О	Л	Ь	К	О	_	П	Е
Р	В	Ы	Е	_	Ч	Е	Т
Ы	Р	Е	_	Г	О	Д	А
_	Д	Е	К	А	Н	А	Т

Матрицада ”_” символымен бос орын белгіленеді.

Түрлендіру нәтижесінде келесі шифрлеу алынады:
НМТЧРЫ_А_ЯИЛВРД_КЖТЬЫЕЕПУЕЬКЕ_КЕРЛСО_ГАРСОЯ_ЧОНВЕ_ПЕДАО_УТЕТАТ.

Берілген жағдайға матрица өлшемі, ашық мәтінді жазу тәртібі және шифрограмманы санау кілт болып табылады. Нақты алғанды кілт басқа болуы мүмкін. Мысалы: жас бойынша ашық мәтіннің жазылуы: 48127653 жолдар нөмірлері ретімен жүргізілуі мүмкін, ал криптограмманы сану 81357642 ретімен бағана бойынша жүргізілуі мүмкін.

Матрицаның жолдармен жазылу ретін жазылу кілті деп, ал шифрограмманың бағана бойынша санау ретін – санау кілті деп атаймыз.

n*n өлшемді матрица көмегімен алынған криптограмманы әрбір топта n-символдар бойынша символдар тобына болу керек. Сол жақтағы шеткі топты, нөмірі санау кілтінің бірінші цифрымен сәйкес келетіндей, жоғарыдан төменге бағанамен жазу керек. Символдардың екінші тобын, нөмірі санау кілтінің цифрымен сәйкес келетіндей, бағанамен жазу керек, және т.с.с.

Ашық мәтінді матрицадан жазу кілтінің цифрларымен сәйкес жол бойынша санау керек.

Орын ауыстыру әдісімен алынған криптограмманы дешифрлеу мысалын қарастырайық. Шифрленгенде 6*6 өлшемді матрицасы қолданылғаны, жазу кілті-352146 және санау кілті-425316 екені белгілі, шифрограмма мәтіні келесідегідей болады:

ДКАГЧЬОВА_РУААКОЕБЗЕРЕ_ДСОХТЕСЕ_Т_ЛУ

Шифрограмманы 6 символ бойынша топтарға бөлеміз:

ДКАЧЬ ОВА_РУ ААКОЕБ ЗЕРЕ_Д СОХТЕС Е_Т_ЛУ

Символдардың бірінші тобын матрицаның 4 бағанын жазамыз, себебі санау кілтінің алғашқы цифрларын 6 символдың ішіндегі екінші топты 2-ші бағанаға, символдардың 3-ші тобын 5-ші бағанаға және т.с.с. жазамыз. Ашық мәнінде санауды жазба кілтіне сәйкес 3 жолдан бастаймыз, одан соң 5 жолды және т.с.с. санаймыз.

Дешифрлеу нәтидесінде келесі ашық мәтінді аламыз:

ХАРАКТЕР ЧЕЛОВЕКА СОЗДАЕТ ЕГО СУДЬБУ

Осы сипатталған криптограмманы дешифрлеу процедурасын, алдын ала өңдеген бағдарлама көмегімен компьерде автоматты түрде орындауға болады.

	1	2	3	4	5	6
1	С	О	З	Д	А	Е
2	О	В	Е	К	А	_
3	Х	А	Р	А	К	Т
4	Т	_	Е	Г	О	_
5	Е	Р	_	Ч	Е	Л
6	С	У	Д	Ь	Б	У

Тапсырма.

Шифрлеу әдістері*:*

1 –Цезарь әдісі;

2 – Көпалфавитті жүйе;

3 – Вижинер әдісі;

4 – Полибий квадраты ;

5 – Алмастырып қою әдісі (1 әдіс);

6 – Алмастырып қою әдісі (2 әдіс).

Тапсырма нұсқалары:

№	Шифрлеу әдісі	Шифрленетін мәтін
1.	1	Отан оттан да ыстық
2.	2	Ел құлағы елу
3.	3	Көш жүре түзеледі
4.	4	Бейбіт елде сән болар
5.	5	Ағасыз ел жағасыз
6.	6	Адамына қарай сәлемі
7.	1	Ақ жүрек адам азбас
8.	2	Ханын сыйламаған ел азады

9.	3	Ата балаға сыншы
10.	4	Әке тірегің, ана жүрегің
11.	5	Ана тілін алмаған арсыз
12.	6	Жолдасты жол айырады
13.	1	Құс қанатымен, ер жолдасымен
14.	2	Жығылсаң нардан жығыл
15.	3	Жығылғанға жұдырық
16.	4	Батырлық айқаста танылар
17.	5	Ерлікте қорлық жоқ
18.	6	Шын батыр сын үстінде танылар
19.	1	Жақсы өтіріктен жаман шындық артық
20.	2	Кішіпейілділік кісі көркі
21.	3	Ақыл жастан, асыл тастан
22.	4	Ердің атын еңбек шығарар
23.	5	Алтынды тот баспайды
24.	6	Байлыққа жомарттық жарасады
25.	1	Жақсылық еткен алғыс алады

Бақылау сұрақтары

1. Ақпаратты қорғау термині қандай түсініктен тұрады?
2. Ақпараттық қауіпсіздіктің маңызды аспектілерін атап шығыңыз.
3. Ақпараттық қауіпсіздіктің проблемаларын шешу деңгейлерін атап шығыңыз.
4. Ақпаратты қорғау деңгейлерін атап шығыңыз.
5. Компьютерлік қылмыстардың себептері немен түсіндірілуі мүмкін.
6. Компьютерлік қылмыстарды қалай табуға болады?
7. Ақпараттық қауіпсіздікті қорғау шараларын атап шығыңыз.
8. Ақпаратты қорғау мақсатымен жұмыс жасау барысындағы сақтық шараларды атап шығыңыз.
9. Интернеттен орынсыз ақпараттарға жетуді қалай шектеуге болады?
10. Компьютерлік вирустар қандай болады, олардың таралу жолдары қандай?