

№1 зертханалық жұмыс

Сабак тақырыбы: Ақпаратты қоғаудың криптографиялық принциптері. Орын ауыстыру шифрлары

Сабак мақсаты: Ақпаратты қоғаудың криптографиялық принциптерін дағдыларын қалыптастыру, өзіндік тапсырмаларды орындау.

Қарастырылатын негізгі мәселелер:

1. Негізгі ұғымдар
2. Орын ауыстыру шифрлары
3. Шифрлайтын кестелер

Әдістемелік нұсқаулық.

Шифрланатын мәтіннің символдарын орын ауыстырумен шифрлаған кезде бұл мәтіннің блогының шегінде анықталған ереже бойынша орындары ауыстырылады. Орын ауыстыру шифрлары ең қарапайым, сондай-ақ ең ежелгі шифрлар болып табылады.

Шифрлайтын кестелер

Шифрлайтын кестелерде кілт ретінде мыналар қолданылады:

- кестенің өлшемі;
- орын ауыстыруды беретін сөз немесе сөздер тіркесі;
- кестенің құрылымының ерекшеліктері.

Орын ауыстыру кестелік шифрларының ең үнемдісі кестенің өлшемі қызмет ететін жай орын ауыстыру болып табылады. Мысалы, КОМПЬЮТЕРЛІК ЖҮЙЕЛЕРДІ ҚОРҒАУ хабар кестеге баған бойынша кезектесіп жазылады. Кестенің 4 қатардан және 7 бағаннан тұратын толтыру нәтижесі 1-суретте көрсетілген.

Шифрмәтінді қалыптастыру үшін хабар мәтінін баған бойынша кестені толтырудан кейін қатар бойынша кестенің құрамын есептейді. Егер шифрмәтінді жеті әріп бойынша тобымен жазып отырса мынадай шифрланған хабар алынады:

ҚЫРЖЛІГ ОЮЛҮЕҚА МТІЙРОУ ПЕКЕДР.

Шифрды ашу кезінде іс-әрекеттер кері ретпен орындалады.

К	Ь	Р	Ж	Л	І	±
О	Р	Л	Ү	Е	Қ	А
М	Т	І	Й	Р	О	У
П	Е	К	Е	Д	Р	.

3.1-сурет. Кестенің 4 қатардан және
7 бағаннан тұратын толтырылуы

Кілт бойынша орын ауыстыру әдісі. Алдыңғы тәсілден бұл тәсіл кестенің бағандары кілттік сөз, сөздер тіркесі немесе кестенің қатарына теру ұзындығының саны бойынша орын ауыстырылады.

Мысалы, кілт ретінде ТЕХНИКА сөзін қолданайық, ал хабардың мәтінін алдыңғы мысалдан алайық. 3.2-суретте хабардың мәтінімен кілттік сөзбен толтырылған екі кесте көрсетілген, бұл кезде сол жақ кесте орнын ауыстыруға дейінгі толтыруға, ал оң жақ кесте – орнын ауыстырудан кейінгі толтыруға сәйкес.

Кілт →	Т	Е	Х	Н	И	К	А	А	Е	И	К	Н	Т	Х
	6	2	7	5	3	4	1	1	2	3	4	5	6	7
	К	Ь	Р	Ж	Л	І	Ғ	Ғ	Ь	Л	І	Ж	К	Р
	О	Ю	Л	Ү	Е	Қ	А	А	Ю	Е	Қ	Ү	О	Л
	М	Т	І	Й	Р	О	У	У	Т	Р	О	Й	М	І
	П	Е	К	Е	Д	Р	.	.	Е	Д	Р	Е	П	Қ
а) Орын ауыстыруға дейін								б) Орын ауыстырудан кейін						

3.2-сурет. Хабардың мәтіні мен кілттік сөзбен толтырылған кесте

Сол жақ кестенің жоғарғы қатарында кілт, ал кілттің әріптерінің астындағы нөмірлер алфавитте кілттің әріптерінің ретімен сәйкес анықталған. Егер кілтте бірдей әріптер кездессе, олар солдан оңға қарай нөмірленетін еді. Оң жақ кестенің бағандары кілттің әріптерінің реттелген нөмірімен сәйкес орындары ауыстырылған.

Оң жақ кестенің құрамындағы қатар бойынша және жеті әріп бойынша шифрмәтіннің тобының жазбасын есептеу кезінде шифрланған хабарды аламыз:

ҒЫЛЖКР АЮЕҚУОЛ УТРОЙМІ .ЕДРЕПК

Қосымша жасыруды қамтамасыз ету үшін шифрланудан өткен хабарды қайта шифрлауға болады. Шифрлаудың мұндай тәсілі **екі рет орын ауыстыру** деп аталады. Бұл әдісте орын ауыстыру кестелері жеке баған үшін және жеке қатар үшін анықталады. Кестеге алдымен хабардың мәтіні жазылады, ал содан кейін кезекпен бағандар, сосын қатарлар ауыстырылады. Шифрды ашу кезінде ауыстырулар кері ретте жүргізіледі.

3.3-суретте екі рет орын ауыстыру әдісін іске асыр мысалы көрсетілген.

	2	3	1
3	А	Қ	П
1	А	Р	А
5	Т	Т	Ы
2	Қ	О	Р
4	Ғ	А	У
Бастапқы кесте			
	1	2	3
3	П	А	Қ
1	А	А	Р
5	Ы	Т	Т
2	Р	Қ	О
4	У	Ғ	А
Бағандардың орнын ауыстыру			
	1	2	3
1	А	А	Р
2	Р	Қ	О
3	П	А	Қ
4	У	Ғ	А
5	Ы	Т	Т
Қатарлардың орнын ауыстыру			

3.3-сурет. Екі рет орын ауыстыру әдісінің мысалы

Бастапқы кестенің бағандарының нөмірлері мен қатарларының нөмірлерінің тізбегі қосарлы алмастыру шифрының кілтіне қызмет етеді. (Біздің мысалымызда 231 және 31524 тізбектері сәйкес).

Егер шифрмәтінді оң жақ кестеден 5 әріп бойынша блок қатарымен оқыса, онда келесі шығады: ААРРҚ ОПАҚУ ҒАЫТТ

Сиқырлы квадраттар

Сиқырлы квадрат деп әрбір бағаны, әрбір қатары және әрбір диагональдарының қосындысы бірдей сан беретін, оның клеткаларына бірден басталатын натурал сандардың тізбегі жазылған квадраттық кестені атайды.

Шифрланатын мәтін сиқырлы квадратқа оның клеткаларының нөмірленуіне сәйкес жазылады. Егер содан кейін қатар бойынша осындай кестенің құрамын жазып алса, онда бастапқы хабардың әріптерін орнын ауыстыру арқасында жинақталған шифрмәтін алынады.

3.4-суретте АҚПАРАТТЫ ҚОРҒАУ мәтінін сиқырлы квадраттың көмегімен шифрлау мысалы көрсетілген. Қатар бойынша оң жақ кестенің құрамын оқу кезінде алған шифрмәтіннің жұмбақты түрі бар: .ПҚҒ РҚОТ ЫАТР АУАА

1	3	2	13
6			
5	10	11	8
9	6	7	12
4	15	14	1

.	П	Қ	Ғ
Р	Қ	О	Т
Ы	А	Т	Р
А	У	А	А

3.4-сурет. АҚПАРАТТЫ ҚОРҒАУ хабарымен толтырылған 4x4 сиқырлы квадраттың мысалы