№1 ЗЕРТХАНАЛЫҚ ЖҰМЫС

САБАҚ ТАҚЫРЫБЫ: Ақпаратты қорғаудың криптографиялық принциптері. Орын ауыстыру шифрлары

САБАҚ МАҚСАТЫ: Ақпаратты қоғаудың криптографиялық принциптерін дағдыларын қалыптастыру, өзіндік тапсырмаларды орындау.

ҚАРАСТЫРЫЛАТЫН НЕГІЗГІ МӘСЕЛЕЛЕР:

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

НЕГІЗГІ МАҒЛҰМАТТАР:

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:

КЬРЖЛІҒ ОЮЛҮЕҚА МТІЙРОУ ПЕКЕДР.

Шифрды ашу кезінде іс-әрекеттер кері ретпен орындалады.

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

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
6	2	7	5	3	4	1
К	Ь	Р	Ж	Л	І	Ғ
О	Ю	Л	Ү	Е	Қ	А
М	Т	І	Й	Р	О	У
П	Е	К	Е	Д	Р	.

а) Орын ауыстыруға дейін

А	Е	И	К	Н	Т	Х
1	2	3	4	5	6	7
Ғ	Ь	Л	І	Ж	К	Р
А	Ю	Е	Қ	Ү	О	Л
У	Т	Р	О	Й	М	І
.	Е	Д	Р	Е	П	К

б) Орын ауыстырудан кейін

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:

ҒЬЛІЖКР АЮЕҚҮОЛ 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 орын ауыстыру

	1	2	3
1	А	А	Р
2	Р	Қ	О
3	П	А	Қ
4	У	Ғ	А
5	Ы	Т	Т

Қатарладың орын ауыстыру

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.

Кестеде 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

16	3	2	13
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

Қолданылған әдебиеттер:

1. К.С.Дүйсенбекова Ақпараттық қауіпсіздік және ақпаратты қорғау. Әл-Фараби атындағы ҚазҰУ .
2. Тұрым А.Ш., Мұстафина Б.М., Ақпарат қорғау және қауіпсіздендіру негіздері. – Алматы: Алматы энергетика және байланыс институты, 2002ж.
3. Романец Ю.В., Тимофеев П.А., Шаньгин В.Ф. Защита информации в компьютерных системах и сетях. –М.: РАДИО И СВЯЗЬ, 1999.

№ 2 ЗЕРТХАНАЛЫҚ ЖҰМЫС

САБАҚ ТАҚЫРЫБЫ: Классикалық симметриялы криптожүйелер. Вижинер шифрлау жүйесі

САБАҚ МАҚСАТЫ: Классикалық симметриялы криптожүйелерін, дағдыларын қалыптастыру, өзіндік тапсырмаларды орындау.

ҚАРАСТЫРЫЛАТЫН НЕГІЗГІ МӘСЕЛЕЛЕР:

1. Негізгі ұғымдар
2. Вижинер жүйесі
3. Шифрлайтын кестелер

НЕГІЗГІ МАҒЛҰМАТТАР:

Вижинер жүйесі Цезарь шифрлау жүйесіне ұқсайды**.**

Бұл көпалфавитті ауыстыру шифрын шифрлау кестесімен жазуға болады. Бұл шифрлау кестесі Вижинер кестесі деп аталады. 4-кестеде қазақ тіліне арналған Вижинер кестесі көрсетілген.

Қазақ әліпбиіне арналған Вижинер кестесі

а	ә	б	в	г	ғ	д	е	ж	з	и	й	к	қ	л	м	н	ң	о	ө	п	р	с	т	у	ұ	ү	ф	х	һ	ц	ч	ш	щ	ъ	ы	і	ь	э	ю	я
ә	б	в	г	ғ	д	е	ж	з	и	й	к	қ	л	м	н	ң	о	ө	п	р	с	т	у	ұ	ү	ф	х	һ	ц	ч	ш	щ	ъ	ы	і	ь	э	ю	я	а
б	в	г	ғ	д	е	ж	з	и	й	к	қ	л	м	н	ң	о	ө	п	р	с	т	у	ұ	ү	ф	х	һ	ц	ч	ш	щ	ъ	ы	і	ь	э	ю	я	а	ә
в	г	ғ	д	е	ж	з	и	й	к	қ	л	м	н	ң	о	ө	п	р	с	т	у	ұ	ү	ф	х	һ	ц	ч	ш	щ	ъ	ы	і	ь	э	ю	я	а	ә	б
г	ғ	д	е	ж	з	и	й	к	қ	л	м	н	ң	о	ө	п	р	с	т	у	ұ	ү	ф	х	һ	ц	ч	ш	щ	ъ	ы	і	ь	э	ю	я	а	ә	б	в
ғ	д	е	ж	з	и	й	к	қ	л	м	н	ң	о	ө	п	р	с	т	у	ұ	ү	ф	х	һ	ц	ч	ш	щ	ъ	ы	і	ь	э	ю	я	а	ә	б	в	г
д	е	ж	з	и	й	к	қ	л	м	н	ң	о	ө	п	р	с	т	у	ұ	ү	ф	х	һ	ц	ч	ш	щ	ъ	ы	і	ь	э	ю	я	а	ә	б	в	г	ғ
е	ж	з	и	й	к	қ	л	м	н	ң	о	ө	п	р	с	т	у	ұ	ү	ф	х	һ	ц	ч	ш	щ	ъ	ы	і	ь	э	ю	я	а	ә	б	в	г	ғ	д
ж	з	и	й	к	қ	л	м	н	ң	о	ө	п	р	с	т	у	ұ	ү	ф	х	һ	ц	ч	ш	щ	ъ	ы	і	ь	э	ю	я	а	ә	б	в	г	ғ	д	е
з	и	й	к	қ	л	м	н	ң	о	ө	п	р	с	т	у	ұ	ү	ф	х	һ	ц	ч	ш	щ	ъ	ы	і	ь	э	ю	я	а	ә	б	в	г	ғ	д	е	ж
и	й	к	қ	л	м	н	ң	о	ө	п	р	с	т	у	ұ	ү	ф	х	һ	ц	ч	ш	щ	ъ	ы	і	ь	э	ю	я	а	ә	б	в	г	ғ	д	е	ж	з
й	к	қ	л	м	н	ң	о	ө	п	р	с	т	у	ұ	ү	ф	х	һ	ц	ч	ш	щ	ъ	ы	і	ь	э	ю	я	а	ә	б	в	г	ғ	д	е	ж	з	и
к	қ	л	м	н	ң	о	ө	п	р	с	т	у	ұ	ү	ф	х	һ	ц	ч	ш	щ	ъ	ы	і	ь	э	ю	я	а	ә	б	в	г	ғ	д	е	ж	з	и	й
қ	л	м	н	ң	о	ө	п	р	с	т	у	ұ	ү	ф	х	һ	ц	ч	ш	щ	ъ	ы	і	ь	э	ю	я	а	ә	б	в	г	ғ	д	е	ж	з	и	й	к
л	м	н	ң	о	ө	п	р	с	т	у	ұ	ү	ф	х	һ	ц	ч	ш	щ	ъ	ы	і	ь	э	ю	я	а	ә	б	в	г	ғ	д	е	ж	з	и	й	к	қ
м	н	ң	о	ө	п	р	с	т	у	ұ	ү	ф	х	һ	ц	ч	ш	щ	ъ	ы	і	ь	э	ю	я	а	ә	б	в	г	ғ	д	е	ж	з	и	й	к	қ	л
н	ң	о	ө	п	р	с	т	у	ұ	ү	ф	х	һ	ц	ч	ш	щ	ъ	ы	і	ь	э	ю	я	а	ә	б	в	г	ғ	д	е	ж	з	и	й	к	қ	л	м
ң	о	ө	п	р	с	т	у	ұ	ү	ф	х	һ	ц	ч	ш	щ	ъ	ы	і	ь	э	ю	я	а	ә	б	в	г	ғ	д	е	ж	з	и	й	к	қ	л	м	н
о	ө	п	р	с	т	у	ұ	ү	ф	х	һ	ц	ч	ш	щ	ъ	ы	і	ь	э	ю	я	а	ә	б	в	г	ғ	д	е	ж	з	и	й	к	қ	л	м	н	ң
ө	п	р	с	т	у	ұ	ү	ф	х	һ	ц	ч	ш	щ	ъ	ы	і	ь	э	ю	я	а	ә	б	в	г	ғ	д	е	ж	з	и	й	к	қ	л	м	н	ң	о
п	р	с	т	у	ұ	ү	ф	х	һ	ц	ч	ш	щ	ъ	ы	і	ь	э	ю	я	а	ә	б	в	г	ғ	д	е	ж	з	и	й	к	қ	л	м	н	ң	о	ө
р	с	т	у	ұ	ү	ф	х	һ	ц	ч	ш	щ	ъ	ы	і	ь	э	ю	я	а	ә	б	в	г	ғ	д	е	ж	з	и	й	к	қ	л	м	н	ң	о	ө	п
с	т	у	ұ	ү	ф	х	һ	ц	ч	ш	щ	ъ	ы	і	ь	э	ю	я	а	ә	б	в	г	ғ	д	е	ж	з	и	й	к	қ	л	м	н	ң	о	ө	п	р
т	у	ұ	ү	ф	х	һ	ц	ч	ш	щ	ъ	ы	і	ь	э	ю	я	а	ә	б	в	г	ғ	д	е	ж	з	и	й	к	қ	л	м	н	ң	о	ө	п	р	с
у	ұ	ү	ф	х	һ	ц	ч	ш	щ	ъ	ы	і	ь	э	ю	я	а	ә	б	в	г	ғ	д	е	ж	з	и	й	к	қ	л	м	н	ң	о	ө	п	р	с	т
ұ	ү	ф	х	һ	ц	ч	ш	щ	ъ	ы	і	ь	э	ю	я	а	ә	б	в	г	ғ	д	е	ж	з	и	й	к	қ	л	м	н	ң	о	ө	п	р	с	т	у
ү	ф	х	һ	ц	ч	ш	щ	ъ	ы	і	ь	э	ю	я	а	ә	б	в	г	ғ	д	е	ж	з	и	й	к	қ	л	м	н	ң	о	ө	п	р	с	т	у	ұ
ф	х	һ	ц	ч	ш	щ	ъ	ы	і	ь	э	ю	я	а	ә	б	в	г	ғ	д	е	ж	з	и	й	к	қ	л	м	н	ң	о	ө	п	р	с	т	у	ұ	ү
х	һ	ц	ч	ш	щ	ъ	ы	і	ь	э	ю	я	а	ә	б	в	г	ғ	д	е	ж	з	и	й	к	қ	л	м	н	ң	о	ө	п	р	с	т	у	ұ	ү	ф
һ	ц	ч	ш	щ	ъ	ы	і	ь	э	ю	я	а	ә	б	в	г	ғ	д	е	ж	з	и	й	к	қ	л	м	н	ң	о	ө	п	р	с	т	у	ұ	ү	ф	х
ц	ч	ш	щ	ъ	ы	і	ь	э	ю	я	а	ә	б	в	г	ғ	д	е	ж	з	и	й	к	қ	л	м	н	ң	о	ө	п	р	с	т	у	ұ	ү	ф	х	һ
ч	ш	щ	ъ	ы	і	ь	э	ю	я	а	ә	б	в	г	ғ	д	е	ж	з	и	й	к	қ	л	м	н	ң	о	ө	п	р	с	т	у	ұ	ү	ф	х	һ	ц
ш	щ	ъ	ы	і	ь	э	ю	я	а	ә	б	в	г	ғ	д	е	ж	з	и	й	к	қ	л	м	н	ң	о	ө	п	р	с	т	у	ұ	ү	ф	х	һ	ц	ч
щ	ъ	ы	і	ь	э	ю	я	а	ә	б	в	г	ғ	д	е	ж	з	и	й	к	қ	л	м	н	ң	о	ө	п	р	с	т	у	ұ	ү	ф	х	һ	ц	ч	ш
ъ	ы	і	ь	э	ю	я	а	ә	б	в	г	ғ	д	е	ж	з	и	й	к	қ	л	м	н	ң	о	ө	п	р	с	т	у	ұ	ү	ф	х	һ	ц	ч	ш	щ
ы	і	ь	э	ю	я	а	ә	б	в	г	ғ	д	е	ж	з	и	й	к	қ	л	м	н	ң	о	ө	п	р	с	т	у	ұ	ү	ф	х	һ	ц	ч	ш	щ	ъ
і	ь	э	ю	я	а	ә	б	в	г	ғ	д	е	ж	з	и	й	к	қ	л	м	н	ң	о	ө	п	р	с	т	у	ұ	ү	ф	х	һ	ц	ч	ш	щ	ъ	ы
ь	э	ю	я	а	ә	б	в	г	ғ	д	е	ж	з	и	й	к	қ	л	м	н	ң	о	ө	п	р	с	т	у	ұ	ү	ф	х	һ	ц	ч	ш	щ	ъ	ы	і
э	ю	я	а	ә	б	в	г	ғ	д	е	ж	з	и	й	к	қ	л	м	н	ң	о	ө	п	р	с	т	у	ұ	ү	ф	х	һ	ц	ч	ш	щ	ъ	ы	і	ь
ю	я	а	ә	б	в	г	ғ	д	е	ж	з	и	й	к	қ	л	м	н	ң	о	ө	п	р	с	т	у	ұ	ү	ф	х	һ	ц	ч	ш	щ	ъ	ы	і	ь	э
я	а	ә	б	в	г	ғ	д	е	ж	з	и	й	к	қ	л	м	н	ң	о	ө	п	р	с	т	у	ұ	ү	ф	х	һ	ц	ч	ш	щ	ъ	ы	і	ь	э	ю

Вижинер кестесі шифрлау және шифрды ашу үшін қолданылады. Кестенің екі кірісі бар:

- негізгі ашық мәтіннің әрпін анықтайтын жоғарғы қатардың сызылған символдары;
- кілттің шеткі сол бағанасы.

Шифрлау процесі кезінде кестенің жоғарғы қатарында негізгі мәтіннің кезекті әрпін және сол бағанада кезекті кілттің мәнін табады. Осы екі әрпін байланыстыратын сызықтардың қиылысқан жерінде шифрмәтіннің әрпі алынады. Вижинер кестесі көмегімен алынған шифрмәтіннің мысалын қарастырайық. РЕСПУБЛИКА кілттік сөз таңдап алынсын. КОМПЬЮТЕРЛІК ЖҮЙЕЛЕРДІ ҚОРҒАУ деген хабарды шифрлау керек.

Негізгі хабарды қатарға көшіреміз және оның астына қайта қайталанатын кілттік сөзді жазамыз. Үшінші қатарға Вижинер кестесінен анықталған шифрмәтін әріптерін көшіреміз.

Хабар	КОМПЬЮТЕРЛІК	ЖҮЙЕЛЕРДІ	ҚОРҒАУ
Кілт	РЕСПУБЛИКАРЕ	СПУБЛИКАР	ЕСПУБЛ
Шифрмәтін	ЩҰЬЯПАЬҢЩЛНӨ	ҢҒЫЗХҢЩДН	ПЯАРБЭ

Қолданылған әдебиеттер:

4. К.С.Дүйсенбекова Ақпараттық қауіпсіздік және ақпаратты қорғау. Әл-Фараби атындағы ҚазҰУ .
5. Тұрым А.Ш., Мұстафина Б.М., Ақпарат қорғау және қауіпсіздендіру негіздері. – Алматы: Алматы энергетика және байланыс институты, 2002ж.
6. Романец Ю.В., Тимофеев П.А., Шаньгин В.Ф. Защита информации в компьютерных системах и сетях. –М.: РАДИО И СВЯЗЬ, 1999.

№3 ЗЕРТХАНАЛЫҚ ЖҰМЫС

САБАҚ ТАҚЫРЫБЫ: Гамма тәсілі арқылы шарт белгілеу. Қазіргі симметриялы криптожүйелер. Полибий квадраты. Цезарь шифрлау жүйесі

САБАҚ МАҚСАТЫ: Студенттерге гамма тәсілі арқылы шарт белгілеу, қазіргі симметриялы криптожүйелер мен Полибий квадраты және Цезарь шифрлау жүйесі туралы мәліметтер беріп, алған білімдерін Зертханалық сабақтар орындауда қолдану дағдыларын қалыптастыру.

ҚАРАСТЫРЫЛАТЫН НЕГІЗГІ МӘСЕЛЕЛЕР:

- Гамма тәсілі арқылы шарт белгілеу
- Қазіргі симметриялы криптожүйелер
- Полибий квадраты
- Цезарь шифрлау жүйесі

НЕГІЗГІ МАҒЛҰМАТТАР:

Полибий квадраты қарапайым ауыстырудың алғашқы шифрларының бірі болып есептеледі. Полибий шифрлау мақсатында грек алфавитінің әріптерімен кездейсоқ ретпен толтырылған, өлшемі 5х5 болып келетін квадраттық кестені жасапты.

Бұл полибий квадратта шифрлау кезінде ашық мәтіннің кезекті әрпін тауып, сол бағанда одан төмен орналасқан әріпті шифрмәтінге жазған. Егер мәтіннің әрпі кестенің төменгі қатарында болса, онда шифрмәтін үшін сол бағаннан ең жоғарғы әрпін алады.

Цезарь шифрлау жүйесі

Цезарь шифры қарапайым ауыстыру (біралфавиттік ауыстыруы) шифрының меншікті жағдайы болып табылады. Бастапқы мәтінді шифрлау кезінде әрбір әріп келесі ереже бойынша сол алфавиттің әрпіне ауыстырылады. Ауыстырылған әріп бастапқы әріптен К әріпке алфавит бойынша ығысқан жолмен анықталады. Алфавиттің соңына жеткен кезде оның басына циклдық өту орындалған. Цезарь К=3 ығысуы кезінде ауыстыру шифрын қолданған. Осындай ауыстыру шифрының құрамында ашық мәтіннің және шифрмәтіннің жұп әріптері сәйкес келетін ауыстыруы кестесімен беруге болады. К=3 үшін мүмкін болатын ауыстырудың жиынтығы 3.1-кестеде көрсетілген.

1 кесте

Біралфавиттік ауыстыру

A→D	J→M	S→V
B→E	K→N	T→W
C→F	L→O	U→X
D→G	M→P	V→Y
E→H	N→Q	W→Z
F→I	O→R	X→A
G→J	P→S	Y→B
H→K	Q→T	Z→C
I→L	R→U	

Мысалы, Цезарьдің жолдауы VENI VIDI VICI (қазақшаға аударғанда “Келді, Көрді, Жеңді” дегенді білдіреді), Митридаттың ұлы понтийлік патша Фарнакты жеңгеннен кейін өзінің досы Аминтийге жіберілген, шифрды ашқан кезде мына түрде болған:

YHQL YLGL YLFL

Біралфавиттік ауыстыруы жүйесіне қарсы криптоаналитикалық шабуыл, символдардың пайда болу жиілігін есептеумен басталады: шифрмәтінде әрбір әріптің пайда болуы санмен анықталады. Содан әріптердің алынған бөлу жиіліктері шифрмәтінде бастапқы хабарламаның, мысалға ағылшынша, алфавиттегі әріптердің бөлу жиілігімен салыстырылады. Шифрмәтінде жоғарғы жиілікті пайда болған әріп ағылшын және т.б.

тілдердегі жоғарғы жиілікпен пайда болған әріпке ауыстырылады. Шифрлау жүйесінің табысты ашылу мүмкіндігі шифрмәтіннің ұзындығының көбеřімен жоғарылайды.

Кілттік сөзі бар Цезарь жүйесі

Кілттік сөзі бар Цезарь жүйесі ауыстырудың біралфавиттік жүйесі болып табылады. Бұл жүйенің ерекшелігі - ауыстыру алфавитіндегі символдардың ығысқан және өзгертілген реті үшін кілттік сөз қолданылуы.

Кілттік сөз ретінде К санын, 0≤K<25 және сөз немесе қысқа сөздер тіркестігі таңдап алынады. Кілттік сөздің барлық әріптері әртүрлі болғаны жақсы. Мысалы, кілттік сөз ретінде DIPLOMAT сөзін және К=5 саны таңдалсын.

Кілттік сөз сандық коды таңдалған К санымен сәйкес келетін әріптен басталатын алфавиттің әріптерінің астына жазылады:

0 1 2 3 4 5 10 15 20 25

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
D I P L O M A T

Ауыстыруы алфавитінің қалған әріптері алфавиттік ретпен кілттік сөзден кейін жазылады:

5

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

Енді бізде кез келген хабарламаның әрбір әрпі үшін ауыстыруы бар.

Бастапқы хабарлама SEND MORE MONEY

былай шифрланады HZBY TCGZ TCBZS

Кілттік сөздің барлық әріптері әр түрлі болуы тиісті деген талаптың міндетті емес екенін ескеру керек. Кілттік сөзді (немесе сөздер тіркестігін) жай ғана бірдей әріптерді қайталамай жазу керек. Мысалы, кілттік сөйлем АУЫЛДЫҢ ЖАНЫ ТЕРЕҢ САЙ және К=3 саны ауыстырудан келесі кестесі туындайды:

	0			3										
1	А	Ә	Б	В	Г	Ғ	Д	Е	Ж	З	И	Й	К	Қ
2	Э	Ю	Я	А	У	Ы	Л	Д	Ң	Ж	Н	Т	Е	Р
1	Л	М	Н	Ң	О	Ө	П	Р	С	Т	У	Ұ	Ү	Ф
2	С	Й	Ә	Б	В	Г	Ғ	З	И	К	Қ	М	О	Ө
1	Х	Һ	Ц	Ч	Ш	Щ	Ь	Ы	І	Ъ	Э	Ю	Я	
2	П	Ұ	Ү	Ф	Х	Һ	Ц	Ч	Ш	Щ	Ь	І	Ъ	

Кілттік сөзі бар Цезарь жүйесінің жетістігі мүмкін болатын кілттік сөздердің саны тәжірибе түрінде өшірілмейтін болып табылады. Бұл жүйенің кемшілігі пайда болатын әріптердің жиіліктерін талдау негізіндегі шифрмәтіннің бұзылу мүмкіндігі болып табылады.

Қолданылған әдебиеттер:

7. К.С.Дүйсенбекова Ақпараттық қауіпсіздік және ақпаратты қорғау. Әл-Фараби атындағы ҚазҰУ .
8. Тұрым А.Ш., Мұстафина Б.М., Ақпарат қорғау және қауіпсіздендіру негіздері. – Алматы: Алматы энергетика және байланыс институты, 2002ж.
9. Романец Ю.В., Тимофеев П.А., Шаньгин В.Ф. Защита информации в компьютерных системах и сетях. –М.: РАДИО И СВЯЗЬ, 1999.

№4 ЗЕРТХАНАЛЫҚ ЖҰМЫС

САБАҚТЫҢ ТАҚЫРЫБЫ: Ағымды шифрлар. Трисемустың шифрлайтын кестесі

САБАҚТЫҢ МАҚСАТЫ: Студенттерге ағымды шифрлар мен Трисемустың шифрлайтын кестесі туралы түсіндіріп, сабақ барысында алған білімдерін тапсырмалар орындауда қолдана білу дағдыларын қалыптастыру.

ҚАРАСТЫРЫЛАТЫН МӘСЕЛЕЛЕР:

- Ағымды шифрлар
- Трисемустың шифрлайтын кестесі

НЕГІЗГІ МАҒЛҰМАТТАР:

Осындай ауыстыруы шифрын алу үшін әдетте алфавиттің әріптері мен кілттік сөз (немесе сөздер тіркестігі) жазбасына арналған кесте қолданылған. Кестеге алдымен кілттік сөзі жазылып, қайталанатын әріптері алынып тасталады. Содан бұл кесте алфавиттің кілтке кірмей қалған әріптермен реттелген түрде толықтырылады. Кілттік сөз немесе сөздер тіркестігі жадыда оңай сақталатындықтан, мұндай жағдай шифрлау немесе шифрды ашу процестерін жеңілдеткен.

Бұл шифрлау тәсілін мысалда анықтайық. Қазақ алфавиті үшін шифрлайтын кестенің өлшемі 6х7 болады. Кілт ретінде АЛГОРИТМ сөзін алайық. Осындай кілтпен шифрлайтын кесте 1-суретте көрсетілген.

А	Л	Г	О	Р	И	Т
М	Ә	Б	В	Ғ	Д	Е
Ж	З	Й	К	Қ	Н	Ң
Ө	П	С	У	Ұ	Ү	Ф
Х	Һ	Ц	Ч	Ш	Щ	Ъ
Ы	І	Ь	Э	Ю	Я	

1-сурет. АЛГОРИТМ кілттік сөзімен шифрлайтын кесте

Шифрлау кезінде Полибий квадратындағы сияқты осы кестеден ашық мәтіннің кезекті әрпін тауып, одан төменгі бағанда орналасқан әріпті шифрмәтінге жазады. Егер бастапқы мәтіннің әрпі кестенің төменгі қатарында болса, онда шифрмәтін үшін сол бағандағы ең жоғарғы әрпін алады.

Мысалы, осы кестенің көмегімен АҚПАРАТТЫ ҚОРҒАУ хабарды шифрлаған кезде МҰҺМҒМЕЕАТҰВҒҚМЧ шифрмәтінді аламыз.

Мұндай кестелік шифрларда шифрлау бір әріп бойынша орындалатындықтан монограммды деп аталады. Трисемус шифрлайтын кестелердің екі әріптері бойынша шифрлауға болатынын байқаған. Мұндай шифрлар ***биграммалық*** деп аталады.

Плейфердің биграммалық шифры

Плейфер жүйесінің шифрлайтын кестесінің құрылымы Трисемустың шифрлайтын кестесінің құрылымына ұқсас болады. Сондықтан Плейфер жүйесінде шифрлау және шифрды ашу процедураларын түсіну үшін өткен тараудан (3.6-суретті қара) Трисемустың шифрлайтын кестесін қолданамыз.

Шифрлау процедурасы келесі қадамдардан тұрады:

1. Бастапқы хабарламаның ашықмәтіні әріптер жұбына (биграммаларға) бөлінеді. Мәтінде әріптердің саны жұп болу керек және онда құрамында екі бірдей әріп, биграммалар, болмау керек. Егер бұл талаптар орындалмаса, онда мәтін мәні жоқ орфографиялық кестелердің арқасында түрлендіріледі.
2. Ашық мәтіннің биграммалар тізбегі шифрлайтын кестенің көмегімен келесі ережелер бойынша түрленеді:

а) егер ашық мәтіннің биграммасының екі әрпі де бір қатарға немесе бағанға (мысалы, 6 суреттегі кестедей М және П әріптері сияқты) түспесе, онда берілген

әріптердің жұбымен анықталатын тікбұрыштың бұрышындағы әріптер ізделінеді. (Біздің мысалда бұл МП°´ әріптері. МП әріптер жұбы °´ жұбына бейнеленеді. Шифрмәтіндегі биграммаларда әріптердің тізбегі ашық мәтіннің биграммасындағы әріптер тізбегінің қатынасы бойынша айнадай орналасу керек);

б) егер ашық мәтіннің биграммасының екі әріптері де кестенің бір бағанында орналасса, онда шифрмәтіннің әріптері болып оның астында жатқан әріптер есептелінеді. (Мысалы, КО биграммасы УВ шифрмәтіннің биграммасын береді). Егер ашық мәтіннің әрпі төменгі қатарда орналасса, онда шифрмәтін үшін сол бағанның жоғарғы қатарындағы сәйкес келетін әріп алынады;

в) егер ашық мәтіннің биграммасының екі әрпі де кестенің бір қатарына орналасса, онда шифрмәтіннің әріптері болып олардың оң жағында жатқан әріптер есептелінеді. (Мысалы, ЬЮ биграммасы °ß шифрмәтіннің биграммасын береді). Егер ашық мәтіннің әрпі соңғы оң жақ бағанда орналасса, онда шифр үшін сол қатардағы сол жақ бағаннан сәйкес келетін әріпті алады.

КОМПЬЮТЕРЛЕР сөзін шифрлайық. Бұл мәтіннің биграммаларға бөлуі мынаны береді: КО М П ЬЮ ТЕ РЛ ЕР.

Ашық мәтіннің берілген биграммалар тізбегі келесі шифр мәтіннің биграммалар тізбегіне шифрлайтын кестенің (6 суретті қара) көмегімен түрленеді: УВ ӘӨ ЭЯ ЕҢ ИГ ҒТ.

Шифрды ашу кезінде әрекеттердің кері реті қолданылады.

Қолданылған әдебиеттер:

10. К.С.Дүйсенбекова Ақпараттық қауіпсіздік және ақпаратты қорғау. Әл-Фараби атындағы ҚазҰУ .
11. Тұрым А.Ш., Мұстафина Б.М., Ақпарат қорғау және қауіпсіздендіру негіздері. – Алматы: Алматы энергетика және байланыс институты, 2002ж.
12. Романец Ю.В., Тимофеев П.А., Шаньгин В.Ф. Защита информации в компьютерных системах и сетях. –М.: РАДИО И СВЯЗЬ, 1999.

№5 ЗЕРТХАНАЛЫҚ ЖҰМЫС

САБАҚТЫҢ ТАҚЫРЫБЫ: Криптографияда қолданатын сандар теориясының элементтері. Асимметриялық криптожүйелер. Уитстонның “қос квадрат” шифры

САБАҚТЫҢ МАҚСАТЫ: Студенттерге криптографияда қолданатын сандар теориясының элементтері мен асимметриялық криптожүйелер, Уитстонның “қос квадрат” шифры туралы ақпарат беріп, алған білімдерін тапсырмалар орындау барысында қолдану тағдыларын қалыптастыру.

ҚАРАСТЫРЫЛАТЫН МӘСЕЛЕЛЕР:

- Криптографияда қолданатын сандар теориясының элементтері
- Асимметриялық криптожүйелер
- Уитстонның “қос квадрат” шифры

НЕГІЗГІ МАҒЛҰМАТТАР:

1894 жылы Чарльз Уитстон ағылшыны “қос квадрат” деп аталатын биграммалармен шифрланатын жаңа әдіс тапты. “Қос квадрат” шифры Плейфейр шифрындағы сияқты биграммалармен шифрлау жүргізілетін екі кестені бірден қолданады.

Осы шифрмен шифрлауға мысал келтірейік. Қазақ алфавитінің кездейсоқ орналасқан символдары бар екі кесте берілсін.

Шифрлау алдында негізгі хабарды биграммаларға бөледі. Әрбір биграмма бөлек шифрланады. Биграмманың бірінші әрпі сол жақтағы кестеден, ал екінші әрпі – оң жақ кестеден алынады. Содан кейін қарсы төбелерінде жатқан биграмма әріптері бар тіктөртбұрышты ойдағыдай құрастырады.

Бұл тіктөртбұрыштың басқа екі төбесі шифрмәтіннің биграмма әріптерін береді.

1	2	3	4	5		1	2	3	4	5
Р	А	М	,	Һ	1	Л	.	Н	Ы	П
Ү	Ш	Ж	П	Қ	2	Ә	М	У	Б	Ұ
З	Й	.	У	Н	3	С	К	З	:	Ф
І	С	Э	Ұ	Ы	4	Ч	Ш	А	Һ	О
Ң	Л	Ө	Х	Ч	5	Х	,	Ү	И	Ң
В	Ь	К	Я	:	6	Ъ	Щ	Д	Ц	Э
Ә	Ф	О	И	Б	7	Ғ	Й	І	Т	Ж
Щ	_	Д	Ю	Е	8	_	Р	Ь	Ө	Я
Т	Г	Ц	Ъ	Ғ	9	Қ	Ю	Е	Г	В

1-сурет. “Қос квадрат” шифрына арналған қазақ алфавиттің кездейсоқ орналасқан символдары бар екі кесте

БҮ негізгі мәтіннің биграммасы шифрлансын дейік. Б әрпі сол кестенің 5-ші бағаны мен 7-ші қатарында орналасқан. Ү әрпі оң кестенің 3-ші бағаны мен 5-ші қатарында орналасқан. Бұл тіктөртбұрыштың 5 және 3 қатарлары, сонымен бірге сол кестенің 7 және оң кестенің 5 бағаналары бойынша пайда болғанын білдіреді. Сондықтан, шифрмәтіннің биграммасына оң кестесіндегі 3-ші баған мен 7 қатарда орналасқан І әрпі және сол кестедегі 5 баған мен 5 қатарда орналасқан Ч әрпі кіреді. ІЧ шифрмәтін биграммасы алынады.

Егер хабар биграмманың екі әріпі де бір қатарда жатса, онда шифрмәтін әріптері де осы қатардан алынады. Хабар биграмманың екінші әрпіне сәйкес келетін шифрмәтін биграмманың бірінші әрпі сол кестедегі қатардан алынады.

Бастапқы хабар	БҮ	ГІ	Н_	ЖА	ҢБ	ЫР	ЛЫ	_К	ҮН
Шифрмәтін	ІЧ	ЕФ	СЕ	УЭ	ИУ	ШЕ	ИА	РЙ	УР

Қолданылған әдебиеттер:

13. К.С.Дүйсенбекова Ақпараттық қауіпсіздік және ақпаратты қорғау. Әл-Фараби атындағы ҚазҰУ .
14. Тұрым А.Ш., Мұстафина Б.М., Ақпарат қорғау және қауіпсіздендіру негіздері. – Алматы: Алматы энергетика және байланыс институты, 2002ж.
15. Романец Ю.В., Тимофеев П.А., Шаньгин В.Ф. Защита информации в компьютерных системах и сетях. –М.: РАДИО И СВЯЗЬ, 1999.

№6 ЗЕРТХАНАЛЫҚ ЖҰМЫС

САБАҚ ТАҚЫРЫБЫ: Ақпаратты қорғау әдістері. Цезарь шифрі

САБАҚ МАҚСАТЫ: Excel ортасында Цезарь шифрін пайдалана мәтінді шифрлеу және кері шифрлеу технологиясын үйрену

ҚАРАСТЫРЫЛАТЫН НЕГІЗГІ МӘСЕЛЕЛЕР:

- Ақпаратты қорғау әдістері
- Цезарь шифрі

НЕГІЗГІ МАҒЛҰМАТТАР:

Цезарь шифрі қарапайым ауыстыру әдісіне жатады. Рим императоры Гай Юлий Цезарь осы әдісті пайдаланғандықтан әдіс осылай аталады. Бастапқы мәтінді шифрлеу үшін мәтіннің әр әріпі алфавиттың басқа арпіне келесі ережемен аустырылады.

Мысалы: айталық, A - қолданылатын алфавит:

$A=\{a1, a_2,\ldots,a_m,\ldots,a_N\}$, мұнда $a_1,a_2,\ldots,a_m,\ldots,a_N$ - алфавит символдары; N алфавит ұзындығы.

Айталық, k – шифрлеу кезіндегі алфавит символдарының ығыстыру позициясының саны, $0<k<N$. Шифрлеу кезінде алфавиттың кодталатын мәтіннің әр нөмері m символы осы алфавиттың $m+k$ символына ауыстырылады. Егер $m+k>N$, онда A алфавиттегі символ нөмері $m+k-N$ өрнек арқылы анықталады.

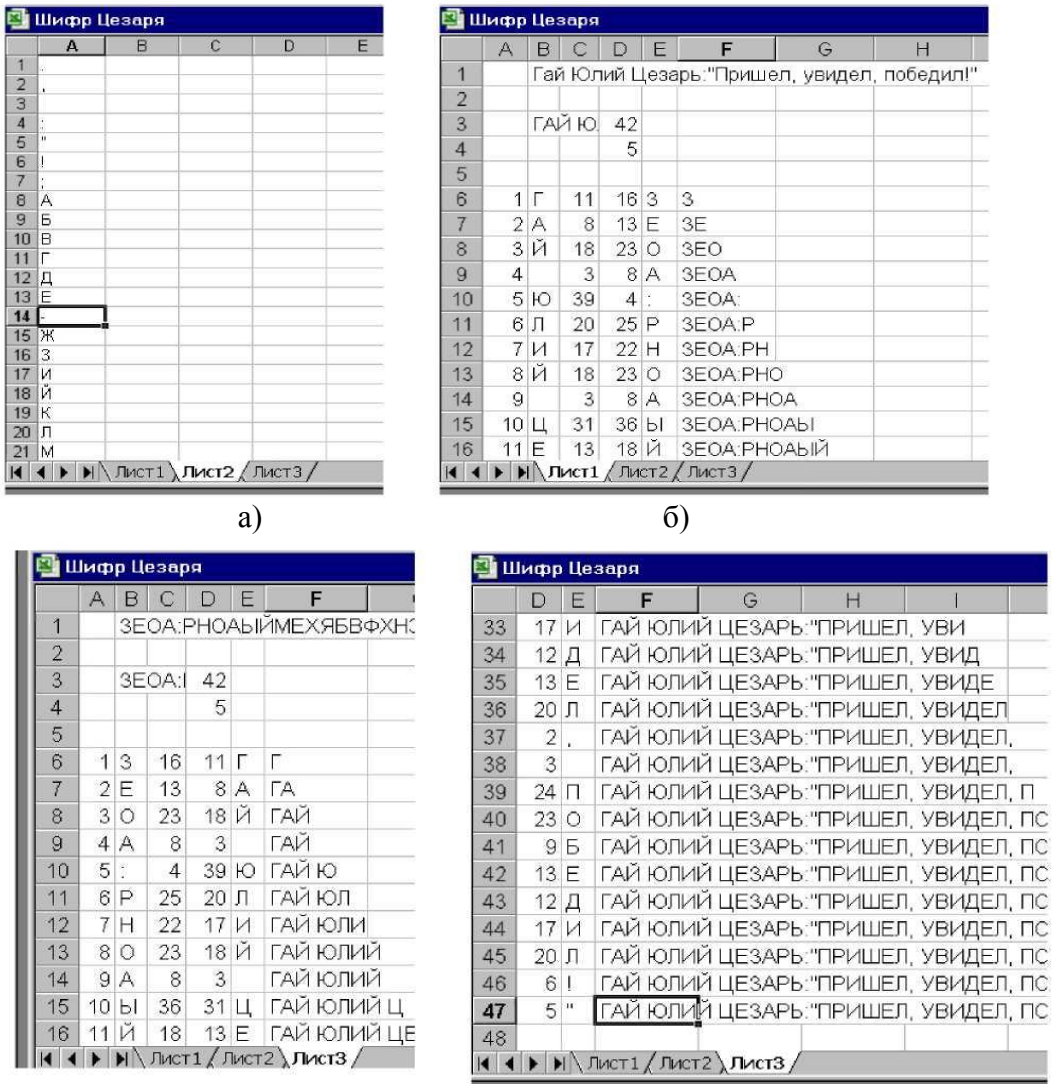
ЖҰМЫСТЫ ОРЫНДАУҒА ӘДІСТЕМЕЛІК НҰСҚАУЛАР:

1. Excelді қосыңыз. Жаңа құжатты құрып, екінші бетіне өтіңіз. A1 бастап A40 дейін 1"а" суреттегідей алфавитті теріңіз. Алфавит диапазонын ерекшелеп оған «ЗЕРТ1» атты меншіктеңіз.
2. Құжаттың бірінші бетіне B1 ұяшығына шифрленетін мәтінді теріңіз, мысалы: **Гай Юлий Цезарь:"Пришел, увидел, победил!"** Мәтінді теру барысында тек қана алфатитте бар символдарды пайдалану қажет.
3. B3 ұяшығына B1 ұяшығындағы мәлеметтерді көшіріп, символдарды үлкен әріптерге аустырыңыз.
4. D3 ұяшығына =ДЛСТР(B3) формуласын енгізіңіз, ДЛСТР функциясы шифрленетін символдар санын есептейді.
5. D4 ұяшығына k мәнін енгізіңіз, *мысалы*, 5-ті.
6. A бағанасының, A6 ұяшығынан бастап 1 ден Nге дейін нөмірлеңіз, мұнда N – мәтіндегі символдар саны (пробелді қосқанда).
N мәні D3 ұяшығында есептелген.
7. B6 ұяшығына =ПСТР(B$3;A6;1) формуласын енгізіңіз, бұл формула шифрленетін мәтінді жеке символдарға бөледі. Бұл формуланы B7- B47 ұяшықтарға көшіріңіз.
8. C6 ұяшығына =ПОИСКПОЗ(B6; ЗЕРТ1;0)" формуласын енгізіңіз. ПОИСКПОЗ функциясы ЗЕРТ1 массивтегі символдың индексін 2 – беттен іздейді. C6 ұяшығының мәнін C7-C47 ұяшықтарға көшіріңіз.
9. ЗЕРТ1 алфавитінен символ нөмерін алып кодталатын мәтіннің символдарын ығыстырыңыз. Ол үшін D6 ұяшығына келесі формуланы енгізіңіз:
=ЕСЛИ(ПОИСКПОЗ(B6; ЗЕРТ1;0)+$D$4>38;ПОИСКПОЗ(B6; ЗЕРТ1;0)+$D$4-40;ПОИСКПОЗ(B6; ЗЕРТ1;0)+$D$4) (1)

   Бұл формулаға тұсініктеме беріңіз. D6 ұшығының мазмұнын D7-D47 ұяшықтар диапазонына көшіріңіз.
10. ЗЕРТ1 алфавитінен жаңа нөмерлеріне сәйкес символдарды таңдап алу. E6 ұяшығына =ИНДЕКС(ЗЕРТ1;D6) формуласын еңгізіңіз. E6 ұшығының мазмұнын E7-E47 ұяшықтар диапазонына көшіріңіз.
11. Кодталған мәтінді алу үшін F6 ұяшығына =E6 формуланы, ал F7 ұяшығына =F6&E7 формуланы енгізіңіз. F7 ұшығының мазмұнын F8-F47 ұяшықтар диапазонына көшіріңіз. F47 ұшығынан шифрленген мәтінді оқи аласыз.
12. Шифрлеуді тексеру үшін шифирленген мәтінді (F47 ұшығында) кері шифрлеу керек

және оларды салыстыру қажет. 3 – бетте зертханалық жұмыстың 2-11пунктерін орындау керек. Мұнда келесіні ескеру қажет:
2 – пункті орындағанда шифрленген мәтінді теру қажет; ал 9 – пункті орындағанда D6 ұяшығына мына формуланы енгізіңіз:

=ЕСЛИ(ПОИСКПОЗ(B6; ЗЕРТ1;0)-$D$4<0;ПОИСКПОЗ(B6; ЗЕРТ1;0)-$D$4+40; ПОИСКПОЗ (B6; ЗЕРТ1;0)-$D$4). (2)



сурет.1. – № 6 зертханалық жұмыстың Excelдегі құжаттардың фрагменттері:
а) Цезарь шифрінің символдар алфавиті; б) шифрлеу құжаттың бастапқы бөлігі; в) және г) кері шифрленген құжаттың бастапқы және соңғы бөлігі

Тапсырмалар:

1. Осы мысалды пайдалана отырып қазақ алфавитін құрастырып, өздеріңіз қазақ тіліндегі тақпақтардан, мақалдардан немесе мәтелдерден алынған мәтіндерді шифрлеу және кері шифрлеуді орындаңыз.

Максималды бал зертханалық жұмыстарды уақытысында орындаған және қорғау барысында қойылған сұрақтарға толық жауап берген студентке қойылады.

Қолданылған әдебиеттер:

1. К.С.Дүйсенбекова Ақпараттық қауіпсіздік және ақпаратты қорғау. Әл-Фараби атындағы ҚазҰУ .
2. Тұрым А.Ш., Мұстафина Б.М., Ақпарат қорғау және қауіпсіздендіру негіздері. – Алматы: Алматы энергетика және байланыс институты, 2002ж.
3. Романец Ю.В., Тимофеев П.А., Шаньгин В.Ф. Защита информации в компьютерных системах и сетях. –М.: РАДИО И СВЯЗЬ, 1999.

№7 ЗЕРТХАНАЛЫҚ ЖҰМЫС

САБАҚ ТАҚЫРЫБЫ: Атбаш шифрі

САБАҚ МАҚСАТЫ: Атбаш шифірі көмегімен ақпаратты шифирлеу мүмкіндігін үйрету

ҚАРАСТЫРЫЛАТЫН НЕГІЗГІ МӘСЕЛЕЛЕР:

- Атбаш шифріне байланысты ақпаратты шифірлеу
- Атбаш шифріне байланысты ақпаратты кері шифірлеу

Тапсырмалар:

1. «Zadanie_na_shifr-каз» файлындағы тапсырмалардың ішінен Атбаш шифрі әдісіне баланысты тапсырмаларды орындап нәтижелерге талдау жасаңыз.
2. Осы мысалдарды пайдалана отырып, өздеріңіз қазақ тіліндегі тақпақтардан, мақалдардан немесе мәтелдерден алынған мәтіндерді осы екі әдіспен шифрлеу және кері шифрлеуді орындаңыз.

Максималды бал зертханалық жұмыстарды уақытысында орындаған және қорғау барысында қойылған сұрақтарға толық жауап берген студентке қойылады.

Қолданылған әдебиеттер:

1. К.С.Дүйсенбекова Ақпараттық қауіпсіздік және ақпаратты қорғау. Әл-Фараби атындағы ҚазҰУ .
2. Тұрым А.Ш., Мұстафина Б.М., Ақпарат қорғау және қауіпсіздендіру негіздері. – Алматы: Алматы энергетика және байланыс институты, 2002ж.
3. Романец Ю.В., Тимофеев П.А., Шаньгин В.Ф. Защита информации в компьютерных системах и сетях. –М.: РАДИО И СВЯЗЬ, 1999.

№8 ЗЕРТХАНАЛЫҚ ЖҰМЫС

САБАҚ ТАҚЫРЫБЫ: Полибия квадраты

САБАҚ МАҚСАТЫ: Полибия квадраты көмегімен ақпаратты шифирлеу мүмкіндігін үйрету

ҚАРАСТЫРЫЛАТЫН НЕГІЗГІ МӘСЕЛЕЛЕР:

- Полибия квадратының көмегімен ақпаратты шифірлеу
- Полибия квадратының көмегімен ақпаратты кері шифірлеу

Тапсырмалар:

1. «Zadanie_na_shifr-каз» файлындағы тапсырмалардың ішінен Полибия квадраты әдісіне баланысты тапсырмаларды орындап нәтижелерге талдау жасаңыз.
2. Осы мысалдарды пайдалана отырып, өздеріңіз қазақ тіліндегі тақпақтардан, мақалдардан немесе мәтелдерден алынған мәтіндерді осы екі әдіспен шифрлеу және кері шифрлеуді орындаңыз.

Максималды бал зертханалық жұмыстарды уақытысында орындаған және қорғау барысында қойылған сұрақтарға толық жауап берген студентке қойылады.

Қолданылған әдебиеттер:

1. К.С.Дүйсенбекова Ақпараттық қауіпсіздік және ақпаратты қорғау. Әл-Фараби атындағы ҚазҰУ .
2. Тұрым А.Ш., Мұстафина Б.М., Ақпарат қорғау және қауіпсіздендіру негіздері. – Алматы: Алматы энергетика және байланыс институты, 2002ж.
3. Романец Ю.В., Тимофеев П.А., Шаньгин В.Ф. Защита информации в компьютерных системах и сетях. –М.: РАДИО И СВЯЗЬ, 1999.

№9 ЗЕРТХАНАЛЫҚ ЖҰМЫС

САБАҚ ТАҚЫРЫБЫ: Виженер әдісі

САБАҚ МАҚСАТЫ: Виженер әдісін пайдалана мәтінді шифрлеу және кері шифрлеу технологиясын үйрену

ҚАРАСТЫРЫЛАТЫН НЕГІЗГІ МӘСЕЛЕЛЕР:

- Виженер әдісінің көмегімен ақпаратты шифірлеу
- Виженер әдісінің көмегімен ақпаратты кері шифірлеу

Тапсырмалар:

1. «Zadanie_na_shifr-каз» файлындағы тапсырмалардың ішінен ***Виженер*** әдісіне баланысты тапсырмаларды орындап нәтижелерге талдау жасаңыз.
2. Осы мысалдарды пайдалана отырып, өздеріңіз қазақ тіліндегі тақпақтардан, мақалдардан немесе мәтелдерден алынған мәтіндерді осы әдіспен шифрлеу және кері шифрлеуді орындаңыз. Кілт ретінде өз фамилияңызды қолданыңыз.

Максималды бал зертханалық жұмыстарды уақытысында орындаған және қорғау барысында қойылған сұрақтарға толық жауап берген студентке қойылады.

Қолданылған әдебиеттер:

1. К.С.Дүйсенбекова Ақпараттық қауіпсіздік және ақпаратты қорғау. Әл-Фараби атындағы ҚазҰУ .
2. Тұрым А.Ш., Мұстафина Б.М., Ақпарат қорғау және қауіпсіздендіру негіздері. – Алматы: Алматы энергетика және байланыс институты, 2002ж.
3. Романец Ю.В., Тимофеев П.А., Шаньгин В.Ф. Защита информации в компьютерных системах и сетях. –М.: РАДИО И СВЯЗЬ, 1999.

№10 ЗЕРТХАНАЛЫҚ ЖҰМЫС

САБАҚ ТАҚЫРЫБЫ: Ауыстыру әдісі

САБАҚ МАҚСАТЫ: Ауыстыру әдісін пайдалана мәтінді шифрлеу және кері шифрлеу технологиясын үйрену

ҚАРАСТЫРЫЛАТЫН НЕГІЗГІ МӘСЕЛЕЛЕР:

- Ауыстыру әдісінің көмегімен ақпаратты шифірлеу
- Ауыстыру әдісінің көмегімен ақпаратты кері шифірлеу

Тапсырмалар:

1. «Zadanie_na_shifr-каз» файлындағы тапсырмалардың ішінен ***Аустыру әдісі*** әдісіне баланысты тапсырмаларды орындап нәтижелерге талдау жасаңыз.
2. Осы мысалдарды пайдалана отырып, өздеріңіз қазақ тіліндегі тақпақтардан, мақалдардан немесе мәтелдерден алынған мәтіндерді осы әдіспен шифрлеу және кері шифрлеуді орындаңыз.

Максималды бал зертханалық жұмыстарды уақытысында орындаған және қорғау барысында қойылған сұрақтарға толық жауап берген студентке қойылады.

Қолданылған әдебиеттер:

1. К.С.Дүйсенбекова Ақпараттық қауіпсіздік және ақпаратты қорғау. Әл-Фараби атындағы ҚазҰУ .
2. Тұрым А.Ш., Мұстафина Б.М., Ақпарат қорғау және қауіпсіздендіру негіздері. – Алматы: Алматы энергетика және байланыс институты, 2002ж.
3. Романец Ю.В., Тимофеев П.А., Шаньгин В.Ф. Защита информации в компьютерных системах и сетях. –М.: РАДИО И СВЯЗЬ, 1999.

№11 ЗЕРТХАНАЛЫҚ ЖҰМЫС

САБАҚ ТАҚЫРЫБЫ: Символдарды араластыру арқылы шифрлеу

САБАҚ МАҚСАТЫ: Символдарды араластыру арқылы шифрлеу әдісін пайдалана мәтінді шифрлеу және кері шифрлеу технологиясын үйрену

ҚАРАСТЫРЫЛАТЫН НЕГІЗГІ МӘСЕЛЕЛЕР:

- Символдарды араластыру арқылы шифрлеу әдісінің көмегімен ақпаратты шифірлеу
- Символдарды араластыру арқылы шифрлеу әдісінің көмегімен ақпаратты кері шифірлеу

Тапсырмалар:

Төмендегі келтірілген программаға келесілерді орындаңыз:

1. алгоритмның блок – схемасын келтіріңіз;
2. осы программаны Делфи тіліне аударыңыз;
3. программаның нәтижесінде экранда құпиясөзді енгізу терезесі мен құпияланған сөздің терезесі болу қажет.

Орындау әдісі

ПРОГРАММА ЛИСТИНГІ:

```
Program transpose;

Type
  str100 = string[100];
  str80 = string[80];

Var
  inf, outf: str80;
  message: str100;
  ch: char;
  t: integer;

Procedure code(inf, outf: str80);

Var
  infile, outfile: file Of char;
  temp: char;
  t, t2: integer;
Begin
  assign(infile, inf);
  reset(infile);
  assign(outfile, outf);
  rewrite(outfile);
  t := 1;
```

```
  while (Not eof(infile)) and (t<=100) Do
  Begin
    Read(infile, message[t]);
    t := t+1;
  End;
  message[t-1] := '#'; {удаление знака конца файла }
{теперь перемешиваются символы }
  For t2 := 0 To 4 Do
    For t := 1 To 4 Do
      Begin
        temp := message[t+t2*20];
        message[t+t2*20] := message[t+10+t2*20];
        message[t+10+t2*20] := temp;
      End;
{ now write it out }
  For t := 1 To 100 Do
    Write(outfile, message[t]);
  WriteLn('файл закодирован');
  close(infile);
  close(outfile);
End;

Procedure decode(inf, outf: str80);

Var
  infile, outfile: file Of char;
  temp: char;
  t, t2: integer;
Begin
  assign(infile, inf);
  reset(infile);
  assign(outfile, outf);
  rewrite(outfile);
  t := 1;
  while (Not eof(infile)) and (t<=100) Do
  Begin
    Read(infile, message[t]);
    t := t+1;
  End;
  message[t-1] := '#'; {удаление знака конца файла }
{теперь перемешиваются символы  }
  For t2 := 0 To 4 Do
    For t := 1 To 4 Do
      Begin
        temp := message[t+t2*20];
        message[t+t2*20] := message[t+10+t2*20];
        message[t+10+t2*20] := temp;
      End;
{теперь осуществляем вывод }
  For t := 1 To 100 Do
    Write(outfile, message[t]);
  WriteLn('файл декодирован');
```

```
  close(infile);
  close(outfile);
End;

Begin
  For t := 1 To 100 Do
    message[t] := '#';
  Write('введите имя входного файла : ');
  ReadLn(inf);
  Write('введите имя выходного файла : ');
  ReadLn(outf);
  Write('кодировать или декодировать (C or D): ');
  ReadLn(ch);
  If upcase(ch)='C' Then code(inf, outf)
  Else If upcase(ch)='D' Then decode(inf, outf);
End.
```

Максималды бал зертханалық жұмыстарды уақытысында орындаған және қорғау барысында қойылған сұрақтарға толық жауап берген студентке қойылады.

Қолданылған әдебиеттер:

1. К.С.Дүйсенбекова Ақпараттық қауіпсіздік және ақпаратты қорғау. Әл-Фараби атындағы ҚазҰУ .
2. Тұрым А.Ш., Мұстафина Б.М., Ақпарат қорғау және қауіпсіздендіру негіздері. – Алматы: Алматы энергетика және байланыс институты, 2002ж.
3. Романец Ю.В., Тимофеев П.А., Шаньгин В.Ф. Защита информации в компьютерных системах и сетях. –М.: РАДИО И СВЯЗЬ, 1999.

№12 ЗЕРТХАНАЛЫҚ ЖҰМЫС

САБАҚ ТАҚЫРЫБЫ: Символдарды ауыстыру арқылы шифрлеу (skytale шифрі)

САБАҚ МАҚСАТЫ: Символдарды араластыру арқылы шифрлеу әдісін пайдалана мәтінді шифрлеу және кері шифрлеу технологиясын үйрену

ҚАРАСТЫРЫЛАТЫН НЕГІЗГІ МӘСЕЛЕЛЕР:

- Символдарды араластыру арқылы шифрлеу әдісінің көмегімен ақпаратты шифірлеу
- Символдарды араластыру арқылы шифрлеу әдісінің көмегімен ақпаратты кері шифірлеу

Тапсырмалар:

Төмендегі келтірілген программаға келесілерді орындаңыз:

1. алгоритмның блок – схемасын келтіріңіз;
2. осы программаны Делфи тіліне аударыңыз;
3. программаның нәтижесінде экранда құпиясөзді енгізу терезесі мен құпияланған сөздің терезесі болу қажет.

Орындау әдісі

ПРОГРАММА ЛИСТИНГІ:

```
Program skytale;

Type
  str100 = string[100];
  str80 = string[80];

Var
  inf, outf: str80;
  sky: str100;
  t: integer;
  ch: char;

Procedure code(inf, outf: str80);

Var
  infile, outfile: file Of char;
  t, t2: integer;
Begin
  assign(infile, inf);
  reset(infile);
  assign(outfile, outf);
  rewrite(outfile);
  t := 1;
{ считывание текстового файла, как одномерной матрицы }
  while (Not eof(infile)) and (t<=100) Do
```

```
  Begin
    Read(infile, sky[t]);
    t := t+1;
  End;
{запись в матрицу размера 5x20}
  For t := 1 To 5 Do
    For t2 := 0 To 19 Do
      Write(outfile, sky[t+(t2*5)]);
  WriteLn('файл закодирован');
  close(infile);
  close(outfile);
End;

Procedure decode(inf, outf: str80);

Var
  infile, outfile: file Of char;
  t, t2: integer;
Begin
  assign(infile, inf);
  reset(infile);
  assign(outfile, outf);
  rewrite(outfile);
{ считывание матрицы размером 5x20  }
  For t := 1 To 5 Do
    For t2 := 0 To 19 Do
      Read(infile, sky[t+(t2*5)]);
{ вывод в качестве строки   }
  For t := 1 To 100 Do
    Write(outfile, sky[t]);
  WriteLn('файл декодирован');
  close(infile);
  close(outfile);
End;

Begin
{ заполнение символов "#"  }
  For t := 1 To 100 Do
    sky[t] := '#';
  Write('введите имя входного файла: ');
  ReadLn(inf);
  Write('введите имя выходного файла: ');
  ReadLn(outf);
  Write('кодировать или декодировать (C or D): ');
  ReadLn(ch);
  If upcase(ch)='C' Then code(inf, outf)
  Else If upcase(ch)='D' Then decode(inf, outf);
End.
```

Максималды бал зертханалық жұмыстарды уақытысында орындаған және қорғау барысында қойылған сұрақтарға толық жауап берген студентке қойылады.

Қолданылған әдебиеттер:

1. К.С.Дүйсенбекова Ақпараттық қауіпсіздік және ақпаратты қорғау. Әл-Фараби атындағы ҚазҰУ .
2. Тұрым А.Ш., Мұстафина Б.М., Ақпарат қорғау және қауіпсіздендіру негіздері. – Алматы: Алматы энергетика және байланыс институты, 2002ж.
3. Романец Ю.В., Тимофеев П.А., Шаньгин В.Ф. Защита информации в компьютерных системах и сетях. –М.: РАДИО И СВЯЗЬ, 1999.

№13 ЗЕРТХАНАЛЫҚ ЖҰМЫС

САБАҚ ТАҚЫРЫБЫ: Символдарды ауыстыру арқылы шифрлеу

САБАҚ МАҚСАТЫ: Символдарды араластыру арқылы шифрлеу әдісін пайдалана мәтінді шифрлеу және кері шифрлеу технологиясын үйрену

ҚАРАСТЫРЫЛАТЫН НЕГІЗГІ МӘСЕЛЕЛЕР:

- Символдарды араластыру арқылы шифрлеу әдісінің көмегімен ақпаратты шифірлеу
- Символдарды араластыру арқылы шифрлеу әдісінің көмегімен ақпаратты кері шифірлеу

Тапсырмалар:

Төмендегі келтірілген программаға келесілерді орындаңыз:

1. алгоритмның блок – схемасын келтіріңіз;
2. осы программаны Делфи тіліне аударыңыз;
3. программаның нәтижесінде экранда құпиясөзді енгізу терезесі мен құпияланған сөздің терезесі болу қажет.

Орындау әдісі

1 – вариант (қарапайым ауыстыру)
ПРОГРАММА ЛИСТИНГІ:

```
Program subst;

Type
  str80 = string[80];

Var
  inf, outf: str80;
  start: integer;
  ch: char;

Procedure code (inf, outf: str80; start: integer);
Var
  infile, outfile: file Of char;
  ch: char;
  t: integer;
Begin
  assign(infile, inf);
  reset(infile);
  assign(outfile, outf);
  rewrite(outfile);
  while not eof(infile) Do
  Begin
    Read(infile, ch);
    ch := upcase(ch);
```

```
    If (ch>='A') And (ch<='Z') Then
      Begin
        t := ord(ch)+start;
        If t>ord('Z') Then t := t-26;
        ch := chr(t);
      End;
    Write(outfile, ch);
  End;
  WriteLn('файл закодирован');
  close(infile);
  close(outfile);
End;

Procedure decode(inf, outf: str80; start: integer);

Var
  infile, outfile: file Of char;
  ch: char;
  t: integer;
Begin
  assign(infile, inf);
  reset(infile);
  assign(outfile, outf);
  rewrite(outfile);
  while not eof(infile) Do
  Begin
    read(infile, ch);
    ch := upcase(ch);
    If (ch>='A') And (ch<='Z') Then
      Begin
        t := ord(ch)-start;
        If t<ord('A') Then t := t+26;
        ch := chr(t);
      End;
    Write(outfile, ch);
  End;
  WriteLn('файл декодирован');
  close(infile);
  close(outfile);
End;
Begin
  Write('введите имя входного файла : ');
  ReadLn(inf);
  Write('введите имя выходного файла : ');
  ReadLn(outf);
  Write('начальная позиция (1-26): ');
  ReadLn(start);
  Write('кодировать или декодировать (C or D): ');
  ReadLn(ch);
  If upcase(ch)='C' Then code(inf, outf, start)
  Else If upcase(ch)='D' Then decode(inf,outf,start);
End.
```

2 – вариант (күрделі ауыстыру)
ПРОГРАММА ЛИСТИНГІ:

```
Program subs1;

Type
  str80 = string[80];

Var
  inf, outf: str80;
  alphabet,sub: str80;
  ch: char;

{данная функция возвращает индекс в алфавите замены }

Function find(alphabet: str80; ch: char): integer;

Var
  t: integer;
Begin
  find := -1; { код ошибки  }
  For t := 1 To 27 Do
    If ch=alphabet[t] Then find := t;
End;

{данная функция возвращает TRUE истина, если с - это буква алфавита }

Function isalpha(ch: char): boolean;
Begin
  isalpha := (upcase(ch)>='A') And (upcase(ch)<='Z');
End;

Procedure code(inf, outf: str80);

Var
  infile, outfile: file Of char;
  ch: char;
Begin
  assign(infile, inf);
  reset(infile);
  assign(outfile, outf);
  rewrite(outfile);
  while not eof(infile) Do
  Begin
    Read(infile, ch);
    ch := upcase(ch);
    If isalpha(ch) Or (ch=' ') Then
      Begin
        ch := sub[find(alphabet, ch)]; { найти замену  }
      End;
    Write(outfile, ch);
  End;
```

```
  WriteLn('файл закодирован');
  close(infile);
  close(outfile);
End;

Procedure decode(inf, outf: str80);

Var
  infile, outfile: file Of char;
  ch: char;
Begin
  assign(infile, inf);
  reset(infile);
  assign(outfile, outf);
  rewrite(outfile);
  while not eof(infile) Do
  Begin
    Read(infile, ch);
    ch := upcase(ch);
    If isalpha(ch) Or (ch=' ') Then ch := alphabet[find(sub,ch)];
    {замена снова на реальный алфавит }
    Write(outfile, ch);
  End;
  WriteLn('файл декодирован');
  close(infile);
  close(outfile);
End;

Begin
  alphabet := 'ABCDEFGHIJKLMNOPQRSTUVWXYZ ';
  sub := 'CAZWSXEDCRFVTGBYHNUJM IKOLP';
  Write('введите имя входного файла : ');
  ReadLn(inf);
  Write('введите имя выходного файла : ');
  ReadLn(outf);
  Write('кодировать или декодировать (C or D): ');
  ReadLn(ch);
  If upcase(ch)='C' Then code(inf, outf)
  Else If upcase(ch)='D' Then decode(inf, outf);
End.
```

Максималды бал зертханалық жұмыстарды уақытысында орындаған және қорғау барысында қойылған сұрақтарға толық жауап берген студентке қойылады.

Қолданылған әдебиеттер:

1. К.С.Дүйсенбекова Ақпараттық қауіпсіздік және ақпаратты қорғау. Әл-Фараби атындағы ҚазҰУ .
2. Тұрым А.Ш., Мұстафина Б.М., Ақпарат қорғау және қауіпсіздендіру негіздері. – Алматы: Алматы энергетика және байланыс институты, 2002ж.
3. Романец Ю.В., Тимофеев П.А., Шаньгин В.Ф. Защита информации в компьютерных системах и сетях. –М.: РАДИО И СВЯЗЬ, 1999.

№14 ЗЕРТХАНАЛЫҚ ЖҰМЫС

САБАҚ ТАҚЫРЫБЫ: XOR операция арқылы шифрлеу

САБАҚ МАҚСАТЫ: XOR операция арқылы шифрлеу әдісін пайдалана мәтінді шифрлеу және кері шифрлеу технологиясын үйрену

ҚАРАСТЫРЫЛАТЫН НЕГІЗГІ МӘСЕЛЕЛЕР:

- XOR операция арқылы шифрлеу әдісінің көмегімен ақпаратты шифірлеу
- XOR операция арқылы шифрлеу әдісінің көмегімен ақпаратты кері шифірлеу

Тапсырмалар:

Төмендегі келтірілген программаға келесілерді орындаңыз:

1. алгоритмның блок – схемасын келтіріңіз;
2. осы программаны Делфи тіліне аударыңыз;
3. программаның нәтижесінде экранда құпиясөзді енгізу терезесі мен құпияланған сөздің терезесі болу қажет.

Орындау әдісі

ПРОГРАММА ЛИСТИНГІ:

шифр на основе операции с ключом

```
Program xor_with_key;

Type
  str80 = string[80];

Var
  inf, outf: str80;
  key: byte;
  ch: char;

Procedure code(inf, outf: str80; key: byte);

Var
  infile, outfile: file Of byte;
  ch: byte;
Begin
  assign(infile, inf);
  reset(infile);
  assign(outfile, outf);
  rewrite(outfile);
  while not eof(infile) Do
  Begin
    Read(infile, ch);
    ch := key xor ch;
    Write(outfile, ch);
  End;
  WriteLn('файл закодирован');
  close(infile);
```

```
  close(outfile);
End;

Procedure decode(inf, outf: str80; key: byte);

Var
  infile, outfile: file Of byte;
  ch: byte;
Begin
  assign(infile, inf);
  reset(infile);
  assign(outfile, outf);
  rewrite(outfile);
  while not eof(infile) Do
  Begin
    Read(infile, ch);
    ch := key xor ch;
    Write(outfile, ch);
  End;
  WriteLn('файл декодирован');
  close(infile);
  close(outfile);
End;

Begin
  Write('введите имя входного файла: ');
  ReadLn(inf);
  Write('введите имя выходного файла; ');
  ReadLn(outf);
  Write(' введите односимвольный ключ : ');
  ReadLn(ch);
  key := ord(ch);
  Write('кодировать или декодировать (C or D): ');
  ReadLn(ch);
  If upcase(ch)='C' Then code(inf, outf, key)
  Else If upcase(ch)='D' Then decode(inf, outf, key);
End.
```

Максималды бал зертханалық жұмыстарды уақытысында орындаған және қорғау барысында қойылған сұрақтарға толық жауап берген студентке қойылады.

Қолданылған әдебиеттер:

1. К.С.Дүйсенбекова Ақпараттық қауіпсіздік және ақпаратты қорғау. Әл-Фараби атындағы ҚазҰУ .
2. Тұрым А.Ш., Мұстафина Б.М., Ақпарат қорғау және қауіпсіздендіру негіздері. – Алматы: Алматы энергетика және байланыс институты, 2002ж.
3. Романец Ю.В., Тимофеев П.А., Шаньгин В.Ф. Защита информации в компьютерных системах и сетях. –М.: РАДИО И СВЯЗЬ, 1999.

№15 ЗЕРТХАНАЛЫҚ ЖҰМЫС

САБАҚ ТАҚЫРЫБЫ: Антивирустық программалар

САБАҚ МАҚСАТЫ: Антивирустық программалар туралы түсінік беріп, өз бетінше жұмыс істеу дағдыларын қалыптастыру.

ҚАРАСТЫРЫЛАТЫН НЕГІЗГІ МӘСЕЛЕЛЕР:

- Антивирустық программалар көмегімен компьютерді вируска тексеру
- Желідегі компьютерлерді вирусқа тексеру

Тапсырмалар:

Антивирус программалармен жұмыс істеу. Компьютерде орнатылған антивирустық программасымен желідегі компьютерлерді вирусқа тексеріп шығу.

Максималды бал зертханалық жұмыстарды уақытысында орындаған және қорғау барысында қойылған сұрақтарға толық жауап берген студентке қойылады.

Қолданылған әдебиеттер:

16. К.С.Дүйсенбекова Ақпараттық қауіпсіздік және ақпаратты қорғау. Әл-Фараби атындағы ҚазҰУ .
17. Тұрым А.Ш., Мұстафина Б.М., Ақпарат қорғау және қауіпсіздендіру негіздері. – Алматы: Алматы энергетика және байланыс институты, 2002ж.
18. Романец Ю.В., Тимофеев П.А., Шаньгин В.Ф. Защита информации в компьютерных системах и сетях. –М.: РАДИО И СВЯЗЬ, 1999.