

№ 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

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.

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	КОМПЬЮТЕ	ЖҮЙЕЛЕ	ҚОРҒАУ
	РЛІК	РДІ	
Кілт	РЕСПУБЛИК	СПУБЛИ	ЕСПУБЛ
	АРЕ	КАР	
Шифрмәтін	ЩҰЪЯПАЬҢ	ҢҒЫЗХҢ	ПЯАРБЭ
	ЩЛНӨ	ЩДН	

3.4-кесте

Қазақ әліпбиіне арналған Вижинер кестесі