

№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.