№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 көбеюімен 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≤К<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 C 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.