№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.