

№7 Лекция тақырыбы: Өртүрлі ауыстырулармен шифрлау әдістері. Маршрутты, блоктық, тігінен орын ауыстырулар

Лекцияның оқыту нәтижелері: Ауыстыру шифрларының мәнін және түрлерін түсінеді. Маршрутты, блоктық және тігінен орын ауыстыру әдістерін қолдана алады. Берілген мәтінді осы әдістермен шифрлап және дешифрлап орындай алады.

Лекция мазмұны:

Блоктық шифрлер.

Ашық текст ұзындығы шектелмеген болғандықтан текст белгілі бір ұзындықтағы блоктарға бөлінеді. Ол блоктың тексттері бір-бірінен тәуелсіз түрде шифрленеді. Бір кілттік блоктық шифрлер 3 топқа бөлінеді:

- 1) Орын ауыстыру;
- 2) Ауыстыру;
- 3) Құрылымды шифрлау.

Қарапайым орын ауыстыру шифрі

Мысал: «Бүгін кешкі сағат онда паркте кездесеміз» деген хабарды шифрлеу үшін, мысалы хабарды 6 қатар 6 бағаннан құралған кесте түрінде жазу керек.

Б	Е	Ғ	А	Е	С
Ү	Ш	А	П	К	Е
Г	К	Т	А	Е	М
І	І	О	Р	З	І
Н	С	Н	К	Д	З
К	А	Д	Т	Е	Ю

Егер соңғы ұяшықтар толмай қалса кез келген әріптер жазып қойылады шифрленген хабар алу үшін ашық текст қатарлар бойынша оқылады (солдан оңға қарай) және топталған түрде жазылады. Мұнда шифрлеу және қайта шифрлеу процесін түрліше ашық текстті кестеге жазу және кестеден мәтінді оқу бағытына қарай орындауға болады. Ашық текстті кестеге жазу және кестеден оқу бағыттарына мысалдар:

қайта шифрлеу үшін кілт бойынша жоғарыдағы әрекеттер кері бағытта орындалады. Сол хабарды кесте көмегінде шифрлеуге болады. Ашық хабар қатарлар бойынша жазылады. Кілт бағандар орын ауыстыру тәртібін береді.

Ашық текст 

2	4	5	1	3	6
И	М	А	М	А	К
Н	А	М	А	Ф	А
Ф	Т	А	Т	И	Ъ
О	И	Т	И	З	В
Р	К	Е	К	И	Х



Ауыстырудан кейін

1	2	3	4	5	6
М	И	А	М	А	К
А	Н	Ф	А	М	А
Т	Ф	И	Т	А	Ъ
И	О	З	И	Т	В
К	Р	И	К	Е	Х

Шифрленген тексттің беріктігін арттыру үшін тағы да бір рет шифрлеуге болады. Шифрлеудің бұл әдісі 2 рет орын ауыстыру шифрі деп аталады. Әдісінің мағынасы мынада шифрлеу негізінде пайда болған кестені қатарлар бойынша орын ауыстыру.

Күрделі орын ауыстыру шифрлері

Қарапайым орын ауыстыру шифрлерінен басқа кестедегі хабарды жол және баған бойынша орын ауыстыру шифрлері де бар. Шифрлеу бірнеше вариант бойынша жүргізілуі мүмкін. Күрделі орын ауыстыру шифрлерінде ашық тексттің символдар тобы тек жолдар бойынша емес бағандар бойынша да ауыстырылады. Төмендегі қадамдар орындалуы тиіс:

- 1) Кестеге ашық текс жазылады. (бірнеше жолмен жазуға болады);
- 2) Кестенің горизонталь және вертикаліне кілтті жазып шығамыз;
- 3) Кілтке сол сияқты кестенің бағандарын кілт цифрлары өсу тәртібі бойынша орын ауыстырылады;
- 4) Сол заң бойынша жолдар да ауыстырылады. Шифрленген хабар кестені қатар бойынша оқудан келіп шығады.

Ашық текст

	2	4	5	1	3	6
2	И	М	А	М	А	К
4	Н	А	М	А	Ф	А
5	Ф	Т	А	Т	И	Ъ
1	О	К	Т	К	З	В
3	Р	К	Е	К	И	Х
6						

Бағандар бойынша ауыстырудан кейін

	1	2	3	4	5	6
2	М	И	А	М	А	К
4	А	Н	Ф	А	М	А
5	Т	Ф	И	Т	А	Ъ
1	И	О	З	И	Т	В
3	К	Р	И	К	Е	Х
6						

Жолдар бойынша ауыстырудан кейін

	1	2	3	4	5	6
1	И	О	З	И	Т	В
2	М	И	А	М	А	К
3	К	Р	И	К	Е	Х
4	А	Н	Ф	А	М	А
5	Т	Ф	И	Т	А	Ъ
6						

Жоғарыдағы хабарды басқа орын ауыстыру шифрімен шифрлейміз. Мұнда шифрлеу тізбектелінбеген ашық текст жолдарлардың кілт бойынша оқудан пайда болады. Жолдар шифртекст жанындағы вертикаль бойынша орналасқан кілт бойынша оқылады.

Оқытудың техникалық құралдары: Компьютер, проектор, интерактивті тақта, презентация слайдтары, шифрлау бағдарламалары (мысалы, Excel немесе Python), оқу-әдістемелік материалдар.

Лекция оқудың тәртібі, оқыту әдістері мен түрлері:

Оқудың тәртібі:

- Лекция түрінде түсіндіру, мысалдар арқылы көрсету;
- Шифрлау тәсілдерін кезең-кезеңмен талдау және тәжірибе жүзінде орындау;

Оқыту әдістері мен түрлері:

- Түсіндірмелі-баяндамалық әдіс;
- Практикалық тапсырмалар орындау;
- Интерактивті сұрақ-жауап және топтық талқылау.

БӨЖ және ОБӨЖ тапсырмалары, олардың түрлері мен орындалуына қойылатын ұпайлардың үлестері:

1. Теориялық сұрақтарға жауап дайындау;
 2. Маршрутты, блоктық және тігінен шифрлау мысалдарын орындау;
- Қысқаша конспект немесе реферат жазу.. Бұл жұмыс жалпы бағалаудың

60-баллды құрайды.

БӨЖ бағалау критерийлері:

- Теориялық материалды түсіну және қолдану -20 балл
- Бағдарламаны дұрыс жазу немесе есепті шешу -25 балл
- Нәтижелердің дәлдігі мен түсіндіру сапасы -15 балл

Барлығы: 60 балл

ОБӨЖ: Маршрутты, блоктық, тігінен орын ауыстырулар шифрының алгоритмін қолданып мәтінді шифрлау және әдістердің айырмашылығын талдау бойынша қысқаша есеп дайындау. Бұл жұмыс жалпы бағалауда 40-баллды құрайды.

ОБӨЖ бағалау критерийлері:

- Тапсырманың толық және уақытылы орындалуы -15 балл
- Теориялық және практикалық түсіндіру сапасы -15 балл
- Топтық жұмысқа белсенді қатысу, сұрақтарға жауап беру-10 балл

Барлығы: 40 балл

Жалпы бағалау үлесі:

- БӨЖ — 60% (60 балл)
- ОБӨЖ — 40% (40 балл)

Пайдалынатын әдебиеттер тізімі:

Негізгі:

1. Г. Камалова, А. Х. Касимова, Л. Б. Диярова. «Ақпараттық қауіпсіздікті басқару». Оқу құралы. /- Алматы: Альманахъ, 2020. - 128 с.
2. Бояринова Л.А. Криптография және ақпаратты қорғау негіздері. – Алматы: Қазақ университеті, 2020.
3. Столлинс У. Криптография және желілік қауіпсіздік. – Алматы: Дәуір, 2018.
4. Нечаев В.И. Элементы криптографии основы теории защиты информации. / В. И. Нечаев. - М.: Высшая школа, 1999. - 109 с.

Қосымша:

1. Ахметова, С. Бағдарламалау технологиясы : Лекция жинағы. / ЮКГУ им. М.О. Ауезова. - Шымкент: ОҚМУ, 2007. - 51 б. <https://rmebrk.kz/book/50006>
2. Ж.З. Сатмаганбетова. Бағдарламалау тілдері және технологиясы: Оқу-әдістемелік куралы. / Қостанай: А. Байтұрсынов атындағы ҚМУ, 2014. - 64 б. <http://rmebrk.kz>