

№3 Лекцияның тақырыбы: Сиқырлы квадрат (Магиялық квадрат) әдісінің қолданылуы.

Лекцияның оқыту нәтижелері: Шифрлеу әдістерінің теориялық негізін, олардың практикалық қолданылу принциптерін және ақпараттық қауіпсіздік жүйесіндегі рөлін терең түсінеді.

Лекция мазмұны

Блоктық шифрлер, қарапайым орын ауыстыру шифрі, кесте бойынша орын ауыстыру шифрі, сондай-ақ *күрделі орын ауыстыру шифрлері* қарастырылады. Сонымен қатар, шифрлеу процесін жетілдірудің ерекше тәсілі ретінде **Сиқырлы квадрат (Магиялық квадрат)** әдісінің қолданылуы түсіндіріледі.

1. Блоктық шифрлер

Блоктық шифрлеу — ашық мәтінді белгілі ұзындықтағы блоктарға бөліп, әр блокты жеке шифрлеу әдісі. Бұл тәсіл ақпараттың үлкен көлемін жүйелі түрде өңдеуге және әр бөлікті тәуелсіз түрде қорғауға мүмкіндік береді.

Блоктық шифрлер үш топқа бөлінеді:

1. **Орын ауыстыру шифрлері** – мәтін ішіндегі символдардың орналасу ретін өзгертеді;

2. **Ауыстыру шифрлері** – мәтіндегі әр символды басқа символмен немесе белгілермен алмастырады;

3. **Құрылымды шифрлер** – екі немесе одан да көп шифрлеу әдістерінің біріктірілген нұсқасы болып табылады.

Мұндай тәсілдер қазіргі замандағы ақпараттық қауіпсіздік жүйелерінде, соның ішінде деректерді қорғау, хабар алмасу және құпия кодтау салаларында кеңінен қолданылады.

2. Қарапайым орын ауыстыру шифрі

Қарапайым орын ауыстыру шифрі — ең көне және түсінікті әдістердің бірі. Мұнда ашық хабар **кесте түрінде жазылып**, белгілі бір бағытта оқылады. Мәтін жолдар мен бағандар бойынша қайта реттеліп, шифрленген хабар пайда болады.

Мысал:

Хабар: *«Бүгін кешкі сағат онда паркте кездесеміз»*

Мәтін 6×6 кестеге жазылады, ал шифрленген мәтін жол бойынша оқылады.

Осы әдістің басты артықшылығы - қарапайымдылығы мен тез орындалуы. Дегенмен, мұндай шифрлер жиілік талдау әдістері арқылы оңай шешіледі, сондықтан тек оқыту немесе негізгі логиканы түсіндіру мақсатында пайдаланылады.

3. Кесте бойынша орын ауыстыру шифрі

Бұл әдіс қарапайым орын ауыстыруға қарағанда күрделірек. Мұнда кестенің бағандары кілт арқылы орын ауыстырылады. Ашық мәтін белгілі бір ұзындықтағы топтарға (блоктарға) бөлінеді және әр блок кілтке сәйкес қайта орналастырылады.

Кілт - бұл бағандар ретін анықтайтын сандық немесе әріптік комбинация. Мысалы, кілт «245136» болса, мәтін бағандары осы ретпен шифрленеді. Осы әдіс нәтижесінде мәтіннің бастапқы құрылымы бұзылып, оны түсіну мүмкін болмай қалады.

Кесте бойынша орын ауыстыру шифрлері қазіргі таңда да өзекті. Мысалы, олар деректерді сақтау мен жіберу кезінде бастапқы хабардың мазмұнын жасыру үшін қолданылады.

4. Күрделі орын ауыстыру шифрлері

Күрделі орын ауыстыру шифрі — шифрлеудің бірнеше деңгейін қамтитын жетілдірілген әдіс. Мұнда мәтіннің жолдары мен бағандары **бірнеше кілт бойынша** ауыстырылады. Алдымен ашық мәтін кестеге жазылады, содан кейін бағандар мен жолдар кілттің өсу реті бойынша ауыстырылады. Бұл тәсілде мәтіннің логикалық құрылымы толық өзгеріп, оны кері шифрлеу үшін дәл сол кілт қажет болады.

Күрделі орын ауыстыру шифрлері көбінесе **екі реттік шифрлеу** әдісін қамтиды, яғни бір хабар екі рет кесте арқылы кодталады. Бұл шифрдің беріктігін айтарлықтай арттырады.

5. Сиқырлы квадрат (Магиялық квадрат) әдісінің қолданылуы

Магиялық квадрат - бұл сандар немесе белгілер арнайы математикалық заңдылыққа сәйкес орналасқан квадрат түріндегі кесте.

Ол шифрлеу кезінде мәтінді квадрат ұяшықтарына жазып, белгілі бір бағытта (мысалы, диагональ, спираль немесе сандардың реттік мәні бойынша) оқу арқылы хабарды түрлендіреді.

Бұл әдіс кесте арқылы орын ауыстыру шифрлерінің логикалық жалғасы болып табылады. Ол ақпаратты шифрлеу кезінде қосымша кездейсоқтық енгізіп, хабардың құрылымын танылмайтындай етеді.

Сиқырлы квадрат әдісі әсіресе оқыту және зерттеу мақсатында, сондай-ақ қарапайым криптографиялық жүйелерде қолдануға қолайлы.

Нәтижесінде студенттер орын ауыстыру шифрлерінің барлық түрлерін түсініп, *Сиқырлы квадрат әдісі арқылы шифрлеудің ерекшеліктерін* іс жүзінде қолдануды үйренеді.

Оқытудың техникалық құралдары: Компьютер, ноутбук, мультимедиялық проектор және экран. Интерактивті тақта. Презентация материалдары (PowerPoint, Google Slides). Бағдарламалық құралдар.

Қосымша құралдар мен материалдар.

✓ Флипчарт немесе маркерлік тақта – формулалар мен шифрлеу кестелерін қолмен көрсету үшін.

✓ Үлестірме материалдар – шифрлеу мысалдары, тапсырмалар мен алгоритмдердің қысқаша сипаттамалары.

✓ Интернет желісіне қосылу – қосымша ақпарат алу және интерактивті тапсырмалар орындау үшін.

Лекция оқудың тәртібі, оқыту әдістері мен түрлері:

Бұл лекцияны оқыту барысында негізгі мақсат – студенттерге шифрлеудің түрлері мен олардың қолдану принциптерін теориялық және практикалық тұрғыда меңгерту. Сол себепті дәріс мазмұны құрылымдық түрде, бірізділікпен және интерактивті әдістермен өтеді.

1. Лекцияны оқудың тәртібі:

Лекция үш негізгі бөлімнен тұрады:

Кіріспе бөлім. Мұнда оқытушы студенттерге ақпаратты қорғау ұғымы мен оның маңызын түсіндіреді. Шифрлеудің пайда болу тарихы мен алғашқы орын ауыстыру әдістері жайлы қысқаша мағлұмат беріледі. Мақсат – студенттерді тақырыпқа қызықтыру және шифрлеудің өмірдегі нақты мысалдарын көрсету (мысалы, банктік жүйелерде немесе мессенджерлерде деректерді қорғау).

Негізгі бөлім. Бұл бөлімде шифрлеудің нақты түрлері: блоктық, қарапайым орын ауыстыру, кестелік және күрделі шифрлер егжей-тегжейлі талданады. Әр әдіс бойынша теориямен қатар мысалдар мен визуалды схемалар қолданылады. Студенттерге шифрлеу және дешифрлеу бойынша шағын тапсырмалар беріледі.

Қорытынды бөлім. Лекция соңында тақырып бойынша қорытынды жасалады, сұрақ-жауап түрінде кері байланыс орнатылады. Студенттер алған білімдерін қысқаша талдап, шифрлеудің заманауи жүйелердегі рөлін түсіндіреді.

2. Оқыту әдістері:

Лекция барысында бірнеше әдістер қолданылады:

- Түсіндіру әдісі. Негізгі теориялық материалды логикалық, жүйелі түрде баяндау арқылы студенттерге ұғымдарды нақты жеткізу.
- Демонстрация әдісі. Оқытушы шифрлеу процесін экранда, интерактивті тақтада немесе бағдарламалық құралдар арқылы көрсетеді. Мысалы, Цезарь шифрін Python тілінде орындау.
- Сұрақ-жауап әдісі. Студенттердің тақырыпты түсіну деңгейін анықтау, ойлануға және талқылауға тарту.
- Практикалық мысалдар әдісі. Нақты мәтінді шифрлеу және шешу арқылы білімді тәжірибемен бекіту.
- Интерактивті талқылау. Студенттер топқа бөлініп, әртүрлі шифр түрлерінің артықшылықтары мен әлсіз жақтарын салыстырады.

3. Оқыту түрлері:

Дәріс (теориялық оқыту). Негізгі ұғымдар, анықтамалар мен мысалдар слайд және тақта арқылы түсіндіріледі.

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

БӨЖ тапсырмалары:

1. Сиқырлы квадрат ұғымын зерттеу және оның тарихи дамуын талдау. *Орындау тәсілі:* әдебиеттер мен интернет-дереккөздер арқылы теориялық мәлімет жинау, конспект жазу. *Ұнай үлесі: 10%*

2. 3×3 және 4×4 сиқырлы квадраттарды қолмен құрастыру. *Орындау тәсілі:* есептеу, диаграмма және кесте түрінде көрсету. *Ұнай үлесі: 15%*

3. Сиқырлы квадраттың қасиеттерін математикалық тұрғыдан дәлелдеу. *Орындау тәсілі:* есептер шығару, формулаларды қолдану. *Ұнай үлесі: 10%*

4. Сиқырлы квадратты қазіргі ақпараттық технологияда қолдану мысалдары. *Орындау тәсілі:* шағын баяндама немесе презентация дайындау. *Ұнай үлесі: 10%*

ОБӨЖ тапсырмалары:

1. Сиқырлы квадрат құрастыру алгоритмін талқылау және код түрінде орындау (Python, Excel).

2. *Орындау тәсілі:* топпен талқылау, код жазу, нәтижесін демонстрациялау. *Ұнай үлесі: 20%*

3. Өртүрлі реттік квадраттарды салыстыру және олардың құрылымдық айырмашылықтарын анықтау. *Орындау тәсілі:* кесте, график және диаграмма арқылы талдау. *Ұнай үлесі: 15%*

4. Қорытынды жоба «Сиқырлы квадраттың практикалық маңызы» атты мини-зерттеу жұмысы. *Орындау тәсілі:* жазбаша баяндама + ауызша қорғау. *Ұнай үлесі: 20%*

Негізгі әдебиеттер:

1. Г.А. Тюлепбердинова. Бағдарламалау технологиясы. Оқу-әдістемелік кешен. - Алматы: Альманахъ, 2021. - 148 с.

2. Дүйсебекова, К.С. Ақпараттық қауіпсіздік және ақпараттарды қорғау: Оқу құралы. - Стер. бас - Алматы: Қазақ университеті, 2020. - 156 б. <http://rmebrk.kz>

6. Камалова Г.А., Диярова, Л.Б. Ақпараттық қауіпсіздік және ақпаратты қорғау: Оқу құралы. /Жәңгір хан атындағы Батыс Қазақстан аграрлық-техникалық университеті. - Алматы: Альманах, 2020. - 116б. <http://rmebrk.kz>

Қосымша әдебиеттер:

1. Ж.З. Сатмаганбетова. Бағдарламалау тілдері және технологиясы: Оқу-әдістемелік құралы. / Қостанай: А. Байтұрсынов атындағы ҚМУ, 2014. - 64 б. <http://rmebrk.kz>