№4 Лекцияның тақырыбы: Жай алмастыру шифры. Полибиан квадраты.

Лекцияның оқыту нәтижелері: Криптографияның қарапайым әдістерінің бірі болып саналатын **жай алмастыру шифры** мен **Полибиан квадраты әдісінің** теориялық және практикалық негіздерін толық меңгереді. Лекцияның мақсаты – ақпаратты қорғаудың бастауыш деңгейін түсіндіру және тарихи шифрлау тәсілдерінің логикасын ашу арқылы қазіргі заманғы криптографиялық жүйелерге негіз бола алатын білім қалыптастыру.

Лекция мазмұны:

Жай алмастыру шифрының теориялық негізі

Жай алмастыру шифры - шифрлаудың ең қарапайым және интуитивті түсінікті түрі. Оның мәні - әрбір әріпті немесе таңбаны басқа таңбамен ауыстыру. Алмастыру ережесі кілт болып табылады. Егер бір әріп бірдей басқа таңбамен алмастырылса, онда бұл - *моноалфавиттік шифр* деп аталады.

Полибиан квадраты

Қарапайым ауыстыру шифрларының ең алғашқысы полибиан квадраты болып есептеледі. Б.э.д. 2 ғасыр бұрын грек жазушысы және тарихшысы Полибий шифрлау мақсатында 5*5 өлшемді грек алфавиті әріптерімен толтырылған кестені ойлап шығарды.

λ	δ	υ	ω	γ
ρ	ξ	δ	σ	υ
μ	η	β	ξ	τ
ψ	π	θ	α	χ
χ	ν		φ	ι

Полибиан квадраты әйтеуір орналасқан 24 әріптен және бос орыннан (пробел) тұрады. Шифрлау кезінде осы полибиан квадратынан ашық мәтіннің кезекті әріпін тауып және шифрмәтінге осы әріптен төмен тұрған сол бағандағы әріпті жазып отырған. Егер ашық мәтіннің әріпі кестеде ең соңғы жолда тұрған болса, онда шифрмәтін үшін дәл сол бағандағы ең жоғарғы әріп алынған.

Мысалы: ταvρυσ сөзін алсақ, онда шифр мәтін былай болған болар еді:

χφδμτξ

Тік бұрышты кесте алфавит әріптерімен кездейсоқ тәртіпте толтырылады. Ашық хабардың әрбір әрібі сол бағанда бір қатар төменде орналасқан әріппен ауыстырылады. Егер әріп ең соңғы қатарда орналасқан болса, онда шифрленетін символ бағандағы бірінші әріп болады. Мысалы, «АЛФАВИТ» хабары шифрленгеннен кейін «УЫ_УТСЗ» көрінісіне келеді:

У	К	В	Ъ	М	Ю	Ь	Д
И	Б	Т	Л	Э	Г	Щ	Н
С	Ф	З	Ы	П	Ц	Е	Я
А		Р	Х	Ж	Ш	О	Ч

Полибий квадраты қарапайым ауыстырудың алғашқы шифрларының бірі болып есептеледі. 5x5 квадраттың әрбір орнына кездейсоқ түрде алынған бір әріп жазылады (1-сурет). Грек алфавитінің әріптерімен толтырғанда бір орын бос қалған, ал латын алфавитінің әріптерімен толтырғанда бір орынға екі әріп (i және j) жазылған

A B C D E

F G H IJ K

L M N O P

Q R S T U

V W X Y Z

1-сурет

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.

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.

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. Жай алмастыру шифры ұғымын зерттеу және оның тарихи дамуын талдау. *Орындау тәсілі:* әдебиеттер мен интернет-дереккөздер арқылы теориялық мәлімет жинау, конспект жазу. *Ұпай үлесі:* **30%**

2. Полибиан квадраты әдісін *қазіргі ақпараттық технологияда қолдану мысалдары. Орындау тәсілі:* шағын баяндама немесе презентация дайындау. *Ұпай үлесі:* **70%**

ОБӨЖ тапсырмалары:

1. Полибиан квадраты әдісінің алгоритмін талқылау және код түрінде орындау (Python). *Ұпай үлесі:* **50%**

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

3. Қорытынды жоба «Полибиан квадраты әдісінің практикалық маңызы» атты мини-зерттеу жұмысы. *Орындау тәсілі:* жазбаша баяндама + ауызша қорғау.
Ұпай үлесі: **30%**

1. Теориялық сұрақтарға жазбаша жауап дайындау.
2. Блоктық және орын ауыстыру шифрлерінің айырмашылығын талдау.
3. Шифрлеу әдістерінің тарихи дамуын зерттеу.
4. Белгілі бір мәтінді шифрлеп, нәтижесін талдау.
5. Реферат немесе қысқаша баяндама жазу.
6. Тесттік тапсырмаларды өз бетімен орындау.
7. Ақпаратты қорғау тақырыбы бойынша эссе жазу.

ОБӨЖ тапсырмаларының түрлері:

1. Оқытушының жетекшілігімен шифрлеу және дешифрлеу алгоритмдерін орындау.
2. Python бағдарламасында қарапайым шифр моделін жасау.
3. Блоктық шифрлердің схемасын құрастыру және түсіндіру.

4. Кесте бойынша шифрлеу әдісін тәжірибеде қолдану.
5. Топтық мини-жоба дайындау (мысалы, шифрлеу жүйесінің үлгісі).
6. Практикалық тапсырмалар мен талдау сұрақтарын орындау.
7. Тақырып бойынша презентация немесе қорғау жұмысын өткізу.

Негізгі әдебиеттер:

1. Г. Камалова, А. Х. Касымова, Л. Б. Диярова. «Ақпараттық қауіпсіздікті басқару». Оқу құралы. /- Алматы: Альманахъ, 2020. - 128 с.

2. Дүйсебекова, К. С. Ақпараттық қауіпсіздік және ақпараттарды қорғау. Оқу құралы /- Алматы: Қазақ университеті, 2013. - 156 с.

3. Нечаев В.И. Элементы криптографии основы теории защиты информации. / В. И. Нечаев. - М.: Высшая школа, 1999. - 109 с.

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

5. 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. 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. Байтурсынов атындағы ҚМУ, 2014. - 64 б. http://rmebrk.kz