№4 Лекцияның тақырыбы: Цезарь шифрлау жүйесі. Цезарь ауыстыруының аффиндік жүйесі

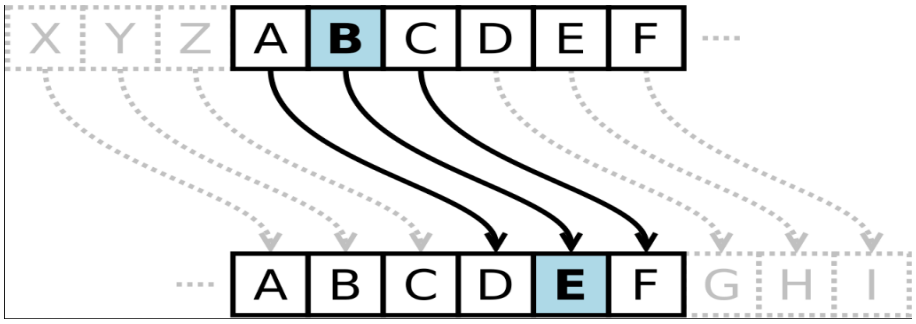
Лекцияның оқыту нәтижелері: Цезарь шифрлау жүйесінің және аффиндік ауыстыру жүйесінің математикалық және логикалық принциптерін толық меңгереді. Цезарь шифрының пайда болу тарихы, оның Рим империясындағы қолданылуы және қазіргі заманғы ақпараттық қауіпсіздік саласында атқаратын қызметі жан-жақты түсіндіріледі. Сондай-ақ, аффиндік шифрдың негізінде жатқан сызықтық функциялар мен олардың математикалық тәуелділіктерін түсінеді.

Лекция мазмұны:

Цезарь шифры - ең жеңіл және кеңінен тараған шифр әдісі. Оны Цезарь коды, Цезарь жылжытуы немесе жылжыту шифры деп те атайды.

Шифр орнына қоюдың бір түрі деп те атауға болады. Шифрде әрбір таңба ашық мәтінде әліпби бойынша тұрақты көлемде оңға немесе солға жылжытылып отырады.Мысалы, жылжыту саны 3 болатын шифрде А әрібі В, Ә әрібі Г ауыстырылады.

Шифр рим императоры **Гай Юлий Цезарь** атымен аталған. Ол осы шифрды өзінің генералдарымен қолданған.



Бұл шифрование көбінесе көптеген күрделі шифрдің бөлігі ретінде қолданады, мысалы, Виженер шифры. Цезарь шифры әлі де ROT13 системасында қолданыс табуда. Барлық монолитті шифрлер секілді Цезарь шифрі де тез сындырылады, практикада мүлдем қолданыс көрмейді.

Аффиндік шифр - Цезарь шифрының жалғасы және кеңейтілген түрі. Мұнда әріптерді шифрлау үшін сызықтық түрлендіру формуласы қолданылады:

E(x)=(a×x+b)mod mE(x) = (a \times x + b) \mod mE(x)=(a×x+b)modm Ал кері түрлендіру:D(x)=a−1(x−b)mod mD(x) = a^{-1}(x - b) \mod mD(x)=a−1(x−b)modm Бұл жерде *a* мен *b* — шифрдың кілттері, ал *a* мен *m* өзара жай сандар болуы шарт.

Аффиндік шифрдың жұмыс істеу принципі және мысалдары Мәтінді шифрлау және дешифрлау қадамдары көрсетіледі, әрбір таңбаның сандық мәні есептеліп, формулаға сәйкес түрлендіріледі. Практикалық мысалдар арқылы студенттер аффиндік функцияның ақпаратты түрлендіру логикасын нақты түсінеді.

Математикалық моделі

Егер әліпбидегі әрбір әріпке өз санын қойып шықса (0 бастап), онда шифрлау мен шифрын анықтауды модульдік арифметиканы қолдана отырып мынадай формуламен табамыз: : $y = (x + k) \ mod \ n$

$$x = (y - k) \ mod \ n,$$

мұндағы x — ашық мәтіннің таңбасы, y — шифрланған мәтіннің таңбасы, n — әліпби күші, ал k — кілт.

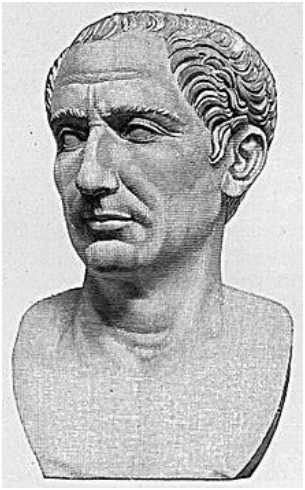
Математикалық тұрғыда Цезарь шифры Афин шифрының өзгертілген түрі болып табылады.

Мысалы:

Шифр кілті $k = 3$ болған жағдайда әр таңба үш орынға жылжиды.Мысалы А Вге,Б Fға айналады

- Негізгі әліпби:А-Ә-Б-В-Г-Ғ-Д--Е-Ё-Ж-З-И-Й-К-Қ--Л-М-Н-Ң-О-Ө-П-Р-С-Т-У-Ұ-Ү-Ф-Х--Һ-Ц-Ч-Ш-Щ-Ъ-Ы--І--Ь-Э--Ю
- Шифрланған: В-Г-Ғ-Д-Е-Ё-Ж-З-И-Й--К-Қ-Л-М-Н-Ң-О-Ө-П-Р-С-Т-У--Ұ-Ү-Ф-Х-Һ-Ц-Ч-Ш-Щ-Ъ-Ы--І--Ь-Э-Ю-А--Ә--Б
- Негізгі мәтін: Мына тұрған бауырсақты жеп қой.
- Шифрленген мәтін үш орынға жылжу арқылы пайда болады:Оэөв үхуёвө ғвфэуұвнүэ йзт нрл.

Тарихы



Цезарь шифры Гай Юлий Цезарь атымен аталған. Ол шифрды солға үш орын жылжыту арқылы қолданған.

Он екі Цезарь өміріне сенсек Гай Светоний Транквилл оны үш орынға жылжыту арқылы әскери ақпарат жіберуде қолданған. Цезарь алғашқы шифр өолданушы ретінде тарихта қалғанымен,алдында басқа шифрлеу әдістері де қолданғанын білеміз.*Егер онда конфидициеалды жіберу болса, ол осы шифрды қолданған,мәселен, әліпби ретін ауыстырған.Сонда ешқандай сөзді түсінуге мүмкіншілік болмаған.Егер мәтінді түсінгісі келсе төртінші әріпті қою міндетті еді. Мысалы, А әрпі В.*

Оның жиені, Август, қолданыста осы шифрлеу әдісін ұстанған. Бірақ ол оңға қарай бір орын жылжытуды ұстанған.*Шифрлеген кезде А орнына Ә, Ә орнына Б қойған.*

Юлий Цезарьдің қиынырақ схемалар қолданғанына дәлелдер табылуда.

Цезарьдің шифрлеу әдісі қаншалықты тиімді болғаны белгісіз. Бірақ Цезарьдің көптеген жаулары сауатсыз болғандықтан, шифр басқа тілде жазылған деп ойлағандықтан шифр айтарлықтай қауіпсіз болған. Шифрды сындыру жайлы ешқандай деректер жоқ. Ең алғашқы дерек 9-ғасырда өмір сүрген әл Кинди жазбаларында кездеседі. Цезарь шифры бір орынға жылжыту кері жылжыту Мезузада Құдай аттарын шифрлеу үшін

қолданады.Бұл алғашқы кездегі жағдай болуы мүмкін, еврей халқына Мезузаға сенуге рұқсат берілмеген. 19 ғасырда газеттегі жарнама бөлігінде жеңіл шифрды ақпарат алмастыру үшін қолданған. Кан Дэвид Таймс газетінде бұқара халық құпиялы коммуникацияларда өз кезегін бермегені туралы сипаттап жазды. 1915 жылы Цезарь шифры өз қолданысын тапты. Ресей әскері бұл шифрды қиын шифрлер орнына қолданды.Өйткені қиын шифрлер әскерлерге қиындай болды,бірақ неміс, австрия әскерлеріне бұл шифрды табу қиынға соқпады.

Он үш орынға жылжытылып шифр ROT13 алгоритмінде қолданылады, қарапайым мәтін шатастыру тәсілінде Usenet кеңінен қолданады. Көбінесе спойлерді тығу үшін қолданады. 2006 жылы мафия бастығы Бернардо Провенцано Сицилияда Цезарь шифрын өзінің хабарламаларының криптоанализінде қолданғаны үшін ұсталды. Провенцано шифрды "А" әріпі 4 орында "Ә" әріпі 5 орында тұрған бойында қолданған.

Цезарь шифрын жеңіл қолдану үшін ортақ оське кіргізілген 2 диаметрлері әр түрлі шеттерінде әліпби жазылған дисктерді қолданады. Алғашында дисктер әр дисктегі әріптері сәйкестендіріліп тұрғызады, сосын қанша орынға жылжыту арқылы Цезарь шифры шығады.

Цезарь мен аффиндік шифрлардың салыстырмалы талдауы
Бұл бөлімде екі жүйенің ұқсастықтары мен айырмашылықтары салыстырылады. Цезарь шифры — аффиндік шифрдың жеке жағдайы екені түсіндіріледі. Сонымен қатар, шифрлардың қауіпсіздік деңгейі мен есептеу күрделілігі талданады.

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. Цезарь шифрлау алгоритмін Python, C++ немесе басқа бағдарламалау тілінде жүзеге асыру.
2. Берілген мәтінді Цезарь әдісімен шифрлау және дешифрлау процесін көрсету.
3. Аффиндік шифрдың формуласы бойынша өз мысалын құрастырып, нәтижесін есептеу.
4. Цезарь және аффиндік шифрлардың айырмашылығын талдайтын қысқаша есеп немесе эссе жазу.
5. Криптографиялық әдістердің қауіпсіздік деңгейін салыстыру бойынша кесте жасау.

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 тапсырмалары

1. Оқытушының басшылығымен Цезарь және аффиндік шифрларды тәжірибе жүзінде орындау.
2. Аффиндік функцияның жұмыс принципін тақтада немесе презентация түрінде түсіндіру.
3. Топтық жұмыс ретінде шифрлау және дешифрлау процестерін модельдеу.
4. Криптографиялық әдістердің артықшылықтары мен әлсіз тұстарын талқылау.

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)*

Негізгі әдебиеттер:

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

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

4. 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