

№ 8 Лекция тақырыбы: Кардано криптографиялық шифрлау жүйесі, Қарапайым ауыстыру және Кардано торлары

Лекцияның оқыту нәтижелері: Кардано шифрлау жүйесінің мәнін және жұмыс принциптерін, Қарапайым ауыстыру (жай орын ауыстыру) әдісінің ерекшеліктерін сипаттауды түсіндіреді. Кардано торларын пайдаланып мәтінді шифрлау және дешифрлауды орындайды.

Лекция мазмұны:

1. Кардано шифрлау жүйесі.

Кардано шифрлау жүйесі, қарапайым ауыстыру әдісі және Кардано торлары - бұл классикалық криптографиялық әдістердің ең танымал мысалдары. Джероламо Кардано (1501- 1576) - итальяндық математик, дәрігер және криптограф, ол шифрлау саласына зор үлес қосты. Оның енгізген шифрлау әдістері қазіргі заманғы криптографиялық жүйелерге негіз болды.

Кардано шифрының негізгі принциптері

Кардано шифры - бұл торлы шифрлау жүйесі. Оның негізінде арнайы тор қолданылады, ол әдетте картоннан немесе металдан жасалады. Торда бос орындар болып, олар арқылы шифрланбаған әріптер өтеді. Шифрлау процесі келесідей:

1. Торды мәтіннің үстіне қояды.
2. Бос орындар арқылы көрінетін әріптерді жазады.
3. Торды алып тастап, қалған орындарға кездейсоқ әріптерді қосады.

Кардано шифрының қолданылуы: мысалдар мен алгоритмдер

Кардано шифрын қолдану үшін арнайы тор қажет. Тордың бос орындары арқылы шифрланған мәтін жазылады. Мысалы, тордың бос орындары келесідей болуы мүмкін:

S - - E - -
- C - - R -
E - - T - -

Шифрланған мәтін: "S E C R E T".

Шифрды ашу үшін торды дұрыс орналастыру керек. Тордың орналасуын білсеңіз, шифрды ашу оңай.

Кардано шифрының артықшылықтары мен кемшіліктері

Кардано шифрының артықшылықтары:

- Қарапайымдылығы: шифрлау процесі оңай және түсінікті.
- Механикалық құрылғыларды қолдану: шифрлауды жеңілдетеді.
- Тарихи маңызы: криптографияның дамуына үлкен әсер етті.

Кардано шифрының кемшіліктері:

- Төмен қауіпсіздік: тордың орналасуын білсеңіз, шифрды ашу оңай.
- Шифрды бұзу оңай: тордың құрылымын білсеңіз, шифрды ашу қиын емес.

Кардано шифрының қазіргі замандағы қолданылуы

Кардано шифры қазіргі кезде негізінен тарихи маңызы бар әдіс ретінде қарастырылады. Ол қазіргі криптографиялық жүйелерге үлгі ретінде қызмет етеді. Дегенмен, оның қауіпсіздігі төмен болғандықтан, қазіргі заманғы криптографиялық жүйелерде қолданылмайды.

2. Қарапайым ауыстыру әдісі

Қарапайым ауыстыру әдісі - бұл криптографияның ең ежелгі және ең қарапайым әдістерінің бірі. Оның негізгі принципі - мәтіндегі әріптерді басқа әріптермен ауыстыру. Бұл әдіс ежелгі замандардан бері қолданылып келеді және оның ең танымал мысалы - Цезарь шифры. Қарапайым ауыстыру әдісінің артықшылығы - оның қарапайымдылығы және түсініктілігі. Дегенмен, бұл әдістің кемшіліктері де бар, мысалы, шифрды бұзу оңай, өйткені әріптердің жиілігін талдау арқылы шифрды ашуға болады.

3. Қарапайым ауыстыру әдісі.

Қарапайым ауыстырудың анықтамасы және тарихы

Қарапайым ауыстыру - бұл мәтіндегі әріптерді басқа әріптермен ауыстыру арқылы шифрлау әдісі. Бұл әдістің тарихы ежелгі замандарға дейін созылады. Мысалы, ежелгі Римде Цезарь шифры қолданылды. Цезарь шифры - бұл ауыстыру әдісінің бір түрі, ол әріптерді белгілі бір орынға ығыстыру арқылы жүзеге асырылады.

Қарапайым ауыстыру әдісі орта ғасырларда да кеңінен қолданылды. Ол әскери және дипломатиялық хабарламаларды қорғау үшін пайдаланылды. Дегенмен, бұл әдістің қауіпсіздігі төмен болғандықтан, оны бұзу оңай болды.

Ауыстыру әдісінің негізгі түрлері

Ауыстыру әдісінің бірнеше түрі бар:

1. Цезарь шифры: әріптерді белгілі бір орынға ығыстыру арқылы шифрлау. Мысалы,

әріптерді 3 орынға ығыстыру:

A -> D

B -> E

C -> F

...

Z -> C

2. Полиалфавиттік ауыстыру: бірнеше ауыстыру ережелерін қолдану. Бұл әдіс шифрды

бұзуды қиындатады. Ауыстыру әдісінің қолданылуы: мысалдар мен алгоритмдер

Ауыстыру әдісін қолдану үшін әріптерді белгілі бір ереже бойынша ауыстыру керек.

Мысалы, Цезарь шифрын қолдану үшін әріптерді 1 орынға ығыстыру арқылы шифрлауға болады.

Мысал:

Мәтін: "HELLO"

Шифрлау ережесі: әріптерді 1 орынға ығыстыру

Шифрланған мәтін: "IFMMP"

Ауыстыру әдісінің артықшылықтары мен кемшіліктері

Ауыстыру әдісінің артықшылықтары:

- Қарапайымдылығы: шифрлау процесі оңай және түсінікті.
- Жылдамдығы: шифрлау және шифрды ашу процесі тез жүзеге асырылады.

- Тарихи маңызы: криптографияның дамуына үлкен әсер етті.

Ауыстыру әдісінің кемшіліктері:

- Төмен қауіпсіздік: шифрды бұзу оңай, өйткені әріптердің жиілігін талдау арқылы шифрды ашуға болады.
- Шифрды бұзу оңай: ауыстыру ережесін білсеңіз, шифрды ашу қиын емес.

Қарапайым ауыстыру әдісі мен Кардано шифрлау жүйесінің қазіргі заманғы криптографиядағы орны.

Қарапайым ауыстыру әдісі қазіргі кезде негізінен тарихи маңызы бар әдіс ретінде қарастырылады. Ол қазіргі криптографиялық жүйелерге үлгі ретінде қызмет етеді. Дегенмен, оның қауіпсіздігі төмен болғандықтан, қазіргі заманғы криптографиялық жүйелерде қолданылмайды. Оның орнына күрделірек және қауіпсіздігі жоғары әдістер, мысалы, AES және RSA, қолданылады. Кардано торларының қазіргі замандағы қолданылуы. Кардано торлары қазіргі кезде негізінен тарихи маңызы бар әдіс ретінде қарастырылады.

Ол қазіргі криптографиялық жүйелерге үлгі ретінде қызмет етеді. Дегенмен, оның қауіпсіздігі төмен болғандықтан, қазіргі заманғы криптографиялық жүйелерде қолданылмайды. Оның орнына күрделірек және қауіпсіздігі жоғары әдістер, мысалы, AES және RSA, қолданылады.

1. Тапсырма

Мәтінді блоктарға бөлу: Біз сөздің әріптерін жолдар мен бағаналарға орналастырамыз.

Бұл үшін 5 бағана мен 6 жолды қолданайық. Мәтін ұзын болғандықтан, біз оны осы өлшеммен бөліп орналастырамыз. Кейбір ұяшықтар бос қалады.

Шифрланған мәтін:

Ұылңы
сңыдй
тдәел
аыкйа
зұес_

2. Тапсырма. Шифрланған мәтін: (2, 3), (1, 5), (3, 2), (3, 2), (3, 5).

1 2 3 4 5
A B C D E
F G H I J
K L M N O
P Q R S T
U V W X Y

Оқытудың техникалық құралдары: Компьютер, ноутбук, интернет.

Лекция оқудың тәртібі, оқыту әдістері мен түрлері:

Оқудың тәртібі:

- Лекция түрінде түсіндіру және мысалдар арқылы көрсету
- Шифрлау тәсілдерін кезең-кезеңмен талдау және тәжірибе жүзінде орындау
- Қорытынды сұрақтар мен талқылау

Оқыту әдістері мен түрлері:

- Түсіндірмелі-баяндамалық әдіс
- Көрнекілік және демонстрациялық әдіс
- Практикалық тапсырмалар орындау
- Интерактивті сұрақ-жауап және топтық талқылау

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

БӨЖ: Қарапайым ауыстыру және Кардано торы арқылы шифрлау мысалдарын орындау, берілген мәтінді шифрлап және дешифрлап орындауы қажет. 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: Қарапайым ауыстыру және Кардано торы арқылы шифрлау алгоритмін қолданып мәтінді шифрлау және екі әдістің айырмашылығын талдау бойынша қысқаша есеп дайындау. Бұл жұмыс жалпы бағалаудың 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. Кауфман Ч., Перлман Р., Спеснер М. *Network Security: Private Communication in a Public World*. – Prentice Hall, 2016.
3. Schneier B. *Applied Cryptography*. – Wiley, 2015.

4. Stallings W. *Cryptography and Network Security: Principles and Practice*. – Pearson, 2022. Таненбаум Э. Компьютерлік желілер. – Алматы: Эверо, 2019
5. 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>