1. ДӘСТҮРЛІ СИММЕТРИЯЛЫҚ КРИПТОЖҮЙЕЛЕР

Мақсаты: студенттерге дәстүрлі симметриялық криптожүйелердің негізгі ұғымдарын, шифрлау және дешифрлау әдістерін, алмастыру және орналастыру шифрларының ерекшеліктерін түсіндіру.

Негізгі сұрақтар:

1. Криптология, криптография және криптоанализ ұғымдары
2. Симметриялық және ассиметриялық криптожүйелер
3. Алмастыру және орналастыру шифрлары
4. Цезарь және Полибиан квадрат шифрлары
5. Магиялық квадраттар және қосарланған орналастыру әдісі

Қысқаша мазмұны:

Криптологияның негізгі ұғымдары: Криптология — хабарламаларды құпиялау мен ашу ғылымы. Ол криптография және криптоанализ бөлімдерінен тұрады.Симметриялық және ассиметриялық криптожүйелер: Симметриялық жүйелерде шифрлау мен дешифрлауға бір кілт қолданылады. Ашық кілтті жүйелерде екі кілт бар: ашық және жабық.Алмастыру шифрлары: Әрбір таңба белгілі ереже бойынша басқа таңбамен алмастырылады. Мысалы, 'Сцитала' және кестелік шифрлар.Қосарланған орналастыру: Хабарды екі рет — баған және жол бойынша орналастыру әдісімен шифрлау.

1.1. Анықтамалар мен түсініктемелер

Криптология грек сөздерінен шыққан: "cryptos" (құпия) және "logos" (хабар). Ол екі бөлімге бөлінеді: криптография (шифрлау) және криптоанализ (криптоталдау). Криптография хабарламаны бөгде адамдардан қорғау үшін шифрлау әдістерін қолданады, ал криптоталдаушы шифрланған мәтінді кілтсіз бұзып ашуды іздейді. Ашық мәтін бастапқы хабарлама, ал шифрланған мәтін – криптограмма деп аталады. Шифрлау процесі ашық мәтінді шифрмәтінге айналдыруды білдіреді, және криптограф шифрлау үшін құпия кілт қолданады. Шифрдың беріктілігі оның бұзып ашылуына қарсы тұра алу қабілетімен өлшенеді.

Алфавит – ақпараттағы белгілерді кодтауға қолданылатын шектеулі жиын.

Мәтін – алфавит элементтерінің реттелген жиынтығы.

Қазіргі заманға сай криптография АЖ-де қолданылады. Осы жағдайларға байланысты:

- алфавит Z_{42} – қазақ алфавитінің 42 әрпі және бос орын;
- алфавит Z_{32} – орыс алфавитінің 32 әрпі және бос орын;
- алфавит Z_{256} – ASC-II және КОИ-8;
- бинарлық алфавит $Z_2 = \{0;1\}$;
- сегіздік және он алтылық алфавит.

Криптожүйелер симметриялық және ассиметриялық (ашық кілтті) болып екіге бөлінеді [1-22]. Симметриялық криптожүйелерде шифрлауда және шифрды ашуда бір кілт қолданылады [2, 3, 7-9, 13,

16, 18, 21].

Ашық кілтті жүйелерде екі кілт қолданылады – ашық және жабық, олар бір-бірімен математикалық байланыста болады [1, 4-7, 10-14, 16, 17]. Ақпарат барлық тұтынушылар қолдана алатындай ашық кілт арқылы шифрланады, ал шифрды ашу тек қана қабылдаушы адамға белгілі жабық кілт арқылы орындалады.

1.2. Алмастыру шифрлары

Алмастыру шифрымен шифрлау кезінде мәтіннің әрбір символы осы мәтін аумағында белгілі бір ереже бойынша ауыстырылады [2, 3, 8, 13]. Алмастыру шифрлары ең қарапайым және ең көне шифрлар болып табылады.

1.2.1.«Сцитала» алмастыру шифры

Б.э.д. V ғасырда Спарттық әскерлерде жақсы жабдықтылған құпиялы әскери байланыс болды. Олар өздерінің хабарларын сцитала шифры көмегімен құпияланды.Шифрлау іс жүзінде былай жасалынды. Цилиндрлік пішіндегі стерженьге спираль түрінде қағаз қиындысы оралады және оған стержень бойымен хабар мәтіні жазылды (1-кесте).

1-кесте

«Сцитала шифры»

	х	а	б	а	
	р	м	ә	т	
	і	н			

Бұдан соң стерженнен оралған мәтін жазылған қағазды аламыз. Бұл қағазға жазылған әріптер ретсіз орналасқан хаостық түрде болады. Мұндай шифр мәтінді шешу үшін тек қана шифрлау әдісі емес, сонымен қатар стерженнің диаметрін білу қажет. Себебі стерженнің диаметрі құпиялы кілт болады.

1.2.2. Шифрлау кестелері

Криптограмма қайта өрлеу заманында саяси, дипломатиялық, әскери жұмыстарда және қарақшылардан қорғану үшін қолданылды. Танымал әдіс — кестелік шифрлау, мұнда кілт ретінде кесте өлшемі пайдаланылады.

ТЕРМИНАТОР ТАҢҒЫ САҒАТ БЕСТЕ ҰШЫП КЕЛЕДІ

2-кестеде көрсетілгендей 5х7 өлшемді кестеге хабарды баған бойынша жазамыз.

2-кесте.

5х7 өлшемді кесте

Т	Н	Т	С	Б	Ұ	Е
Е	А	А	А	Е	Ш	Л
Р	Т	Ң	Ғ	С	Ы	Е
М	О	Ғ	А	Т	П	Д
И	Р	Ы	Т	Е	К	І

Ал шифрлы мәтінді алу үшін кестедегі мәтінді жол бойынша оқимыз. Егер шифрлы мәтінді бес әріппен топтап жазсақ, онда мынадай мәтін шығады:

ТНТСБ ҰЕЕАА АЕШЛР ТҢҒСЫ ЕМОҒА ТПДИР ЫТЕКІ

Бұл жағдайда хабарды жіберуші және қабылдаушы алдын ала кілтті, яғни кесте өлшемін белгілеуі керек. Шифрлы мәтіннің бес әріппен жазылуы шифрлау процесіне кірмейді, ол тек мәтінді қолайлы жазу үшін қолданылады. Шифрмәтінді ашып оқу үшін процесті кері қарай жүргіземіз.

Келесі шифрлау әдісі алдыңғыларға қарағанда тиімдірек. Себебі, мұнда кілт ретінде кесте ұзындығына тең кілттік сөзді аламыз. Мұндай әдісті кілт бойынша орналастыру деп атаймыз.

Мысал ретінде кілттік сөзді ЖҰБАНОВ деп алайық, ал хабар мәтінін өткен мысалдан алайық.

ТЕРМИНАТОР ТАҢҒЫ САҒАТ БЕСТЕ ҰШЫП КЕЛЕДІ

3-кесте.

Хабарлама мәтін мен кілттік сөздер

9	26	3	1	17	19	4
Ж	Ұ	Б	А	Н	О	В
Т	Н	Т	С	Б	Ұ	Е
Е	А	А	А	Е	Ш	Л

Р	Т	Ң	Ғ	С	Ы	Е
М	О	Ғ	А	Т	П	Д
И	Р	Ы	Т	Е	К	І

Орналастыруға дейін

А	Б	В	Ж	Н	О	Ұ
1	3	4	9	17	19	26
С	Т	Е	Т	Б	Ұ	Н
А	А	Л	Е	Е	Ш	А
Ғ	Ң	Е	Р	С	Ы	Т
А	Ғ	Д	М	Т	П	О
Т	Ы	І	И	Е	К	Р

Орналастырудан кейін 3-кестенің бірінші жолында кілттік сөз жазылған. Ал кейінгі жолдағы сандар кілттік сөздегі әріптердің алфавиттік ретімен қойылған. Келесі кестеде сандар реттік нөмірмен жазылған. Шыққан кестені жол бойынша оқысақ, шифрмәтінді аламыз. Оны бес әріппен топтап жазсақ ыңғайлы болады.

СТЕТБ ҰНААЛ ЕЕШАҒ ҢЕРСЫ ТАҒДМ ТПОТЫ ІИЕКР

Құпияның мықтылығын арттыру үшін шифрланған мәтінді қайта шифрлау әдісі — қосарланған орналастыру. Бұл әдісте кесте бағаны мен жолы жеке-жеке орналастырылады. Алдымен мәтін кестеге жазылып, кейін баған және жол бойынша орналастырылады. Шифрмәтінді оқығанда процесті кері жүргіземіз.

Мысал ретінде көрсетілген кестелерді қарастырайық. Хабар мәтіні былай берілсін:

ЕКІНШІ КҮНІ ҰШАМЫН

4-кесте.

Бастапқы берілген кесте

	4	1	3	2
3	Е	К	І	Н
1	Ш	І	К	Ү
4	Н	І	Ұ	Ш
2	А	М	Ы	Н

5-кесте.

Баған бойынша орналастыру

	1	2	3	4
3	К	Н	І	Е
1	І	**Ү**	К	Ш
4	І	Ш	Ұ	Н
2	М	Н	Ы	А

Қосарланған орналастыру әдісінде кілт ретінде баған және жолдың бойында кез келген ретпен орналастырылған сандар алынады. Шифрлау кезінде алдымен баған элементтерін (сандарын) ретімен қоямыз. Енді шыққан кестенің жолының элементтерін ретімен қоямыз.

6- кесте.

Жол бойынша орналастыру

	1	2	3	4
1	І	Ү	К	Ш
2	М	Н	Ы	А
3	К	Н	І	Е
4	І	Ш	Ұ	Н

Соңғы кестені жол бойынша оқып, төрт әріптен топтап жазсақ, шифрлы мәтінді аламыз.

ІҮКШ МНЫА КНІЕ ШШҰН

Қосарланған орналастыру әдісінде қолайлы нұсқалар саны кесте өлшеміне байланысты

өседі.

- 3х3 өлшемді кесте үшін 36 нұсқа.
- 4х4 өлшемді кесте үшін 576 нұсқа.
- 5х5 өлшемді кесте үшін 14 400 нұсқа.

Бірақ қосарланған орналастыру әдісі кез келген кесте өлшеміне байланыссыз оңай шешіледі.

1.2.3. Магиялық квадраттардың қолданылуы

Орта ғасырда шифрлауға магиялық квадраттар да қолданылды. Магиялық квадрат дегеніміз – кесте торларына бірден басталатын натурал сандар жазылған және ол сандардың жол бойынша, баған бойынша және диагональдары бойынша қосындылары тең болатын квадраттық кестелерді айтамыз.

Хабар мәтінін квадраттық кесте торларына сандар ретімен жазамыз. Егер шыққан кестені жол бойынша оқысақ, шифрмәтінді аламыз. Орта ғасырда бұл әдіспен жазылған құпияны кілт қана емес, магиялық күш те жасырады деп түсінген.Мысал келтірейік. Хабар мәтіні.

ЕКІНШІ КҮНІ ҰШАМЫН

7- кесте.

Магиялық квадраттың қолданылуы

16	3	2	13
5	10	11	8
9	6	7	12
4	15	14	1

Н	І	К	А
Ш	І	Ұ	Ү
Н	І	К	Ш
Н	Ы	М	Е

Жол бойынша оқылған шифрмәтін түсініксіз күйге енеді.

НІҚА ШІҰҮ НІКШ ҚЫМЕ

Магиялық квадраттар саны квадрат өлшемі өскен сайын артады. Тек 3х3 өлшемді жалғыз квадрат бар. 4х4 өлшемді квадраттар саны 880, ал 5х5 өлшемді квадраттар саны 250000.Магиялық квадраттар орта ғасырларда өте тиімді шифрлау әдісі болып табылды. Себебі, ол кезде барлық нұсқаларды қолмен есептеу мүмкін емес еді.

1.3. Жай алмастыру шифрлары

Шифрлау кезінде таңбалар алдын ала дайындалған ереже бойынша алмастырылады. Жай алмастыру шифрында әр таңба барлық мәтінде бірдей алмастырылады. Мұндай шифрлар біралфавитті қойылым шифрлары деп аталады.

1.3.1. Полибиан квадраты

Полибиан квадраты – жай алмастыру шифрлауының алғашқыларының бірі болып табылады. Біздің дәуірімізге дейін II ғасырда грек жазушысы және тарихшы Полибий, шифрлау мақсатында 5х5 өлшемді кез келген ретте орналастырылған грек алфавиттерінен тұратын кесте ойлап шығарды (8-кесте).

6- кесте.

Полибиан квадраты

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

Шифрлау кезінде ашық мәтіннің әрпін кесте ішінен тауып алып, шифрмәтінге сол әріптен

төмен тұрған әріп жазылады. Егер әріп кестенің соңғы жолында тұрса, онда сол әріп тұрған бағанның ең бірінші әрпі алынады.

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

χφδμτξ

1.3.2. Цезарь шифрлау жүйесі

Цезарь шифры — алмастыру шифрының бір түрі. Бұл шифрды Рим императоры Цезарь қолданған. Әріптер үш орынға ауыстырылады (K = 3). Мысалы, "A" әрпі "D" болады. Шифрлау кестесі ашық және шифрланған мәтіннен тұрады.Мысалы, егер бастапқы мәтін "ABCD" болса, онда шифрланған мәтін "DEFG" болады.

7- кестеде $K=3$ болғанда мүмкін болатын ауыстыру $(K=3, m=42)$ көрсетілген:

9-кесте.

Алфавиттерді алмастыру

А → В	Е → З	Қ → Н	П → Т	Ф → Ц	Ь → Ъ
Ә → Г	Е → И	Л → Ң	Р → У	Х → Ч	Ы → Э
Б → Ғ	Ж → Й	М → О	С → Ұ	Һ → Ш	І → Ю
В → Д Г → Е	З → К И → Қ	Н → Ө Ң → П	Т → Ү У → Ф	Ц → Щ Ч → Ь	Ъ → Я Э → А
Ғ → Е	Й → Л	О → Р	Ұ → Х	Ш → Ы	Ю → Ә
Д → Ж	К → М	Ө → С	Ү → Һ	Щ → І	Я → Б

Мысалы, Цезарьдің КЕЛДІМ КӨРДІМ ЖЕҢДІМ жолдауы шифрланған кезде мына түрде болар еді: МЗҢЖЮО МСУЖЮО ЙЗПЖЮО.

Бөлімнің басында енгізілген түсініктер бойынша қарапайым ауыстыру шифрына математикалық талдау жасайық.

$\overline{Z_m}$ алфавитіндегі ауыстыру $\overline{Z_m}$ -нен $\overline{Z_m}$ -ге өзара бірмәнді бейнелеуі болады:

$$\pi : t \to \pi(t),$$

ол ашық мәтіннің t әрпін шифрланған мәтіннің $\pi(t)$ әрпіне ауыстырады. Z_m -дегі барлық ауыстырулар жиынын Z_m -нің симметриялық тобы деп атайды және келесі түрде белгіленеді: $SYM(Z_m)$.

$SYM(Z_m)$ симметриялық тобының келесідей қасиеттері бар:

1. Тұйықтығы. $\pi_1\pi_2$ ауыстыруларының көбейтіндісі

$$\pi : \underline{Z}_m \xrightarrow{\pi_2} \underline{Z}_m \xrightarrow{\pi_1} \underline{Z}_m, \quad \pi : t \to \pi_1(\pi_2(t))$$

ауыстыруы болады.

2. Ассоциативтік. $\pi_1\pi_2\pi_3$ ауыстыруларының көбейтіндісін жақшаға алудың екі әдісі де: $(\pi_1\pi_2\pi_3) = (\pi_1\pi_2)\pi_3$ бірдей нәтиже береді.

3. Бірлік элементінің бар болуы

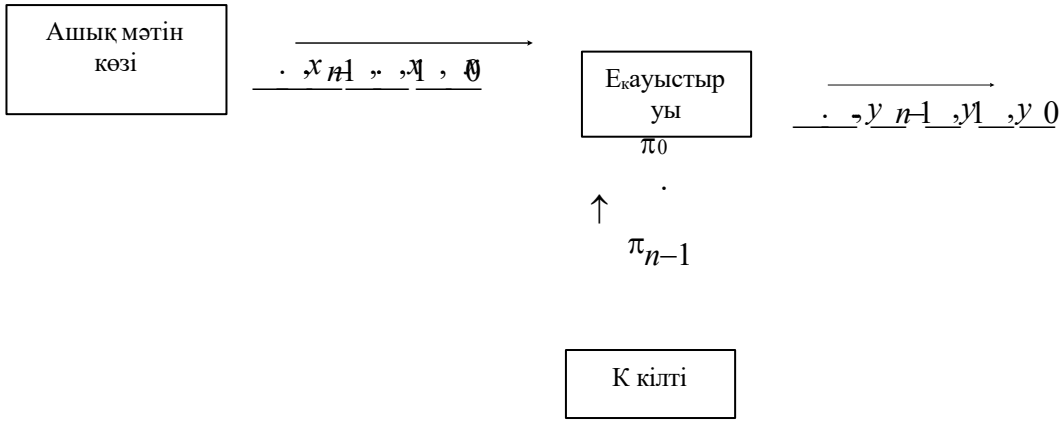
$$\delta(t) = t, \qquad 0 \le t < m$$

арқылы анықталған δ ауыстыруы $\delta\pi = \delta\pi$, мұнда барлық $\pi \in SYM(Z)$ көбейтіндісі бойынша $SYM(Z)$ тобының жалғыз бірлік элементі m болып табылады.

4. Кері элементтерінің бар болуы. Әрбір ауыстыруының π^{-1} арқылы белгіленетін және мына қатысты: $\pi^{-1}\pi = \delta$ қанағаттандыратын өзара бірмәнді анықталған кері ауыстыруы болады.

Көрсетілген қасиеттер топтың аксиомалары болып табылады.

Z_m алфавитінің ауыстыруының K кілті дегеніміз - Z_m-дегі симметриялық топтың элементтерінің тізбегі десек болады:



E_k ауыстыруының жүйесі.

E_k ауыстыруына тән ерекшеліктер:

- ашық мәтін әрбір әріп бойынша шифрланады;
- y_i шифрланған мәтіннің i-ші әрпі дегеніміз – кілтінің π_i компонентінің тек i-ші функциясы және x ашық мәтінінің i-ші әрпі;
- n-грамманың $(x_1, x_2, ..., x_{n-1})$ шифрлануы мына формуламен сәйкес жүргізіледі: $(y_0, y_1, ..., y_{n-1}) = E_k(x_1, x_2, ..., x_{n-1})$.

Цезарь жүйесі біралфавитті ауыстыру, ол ашық мәтіннің n-граммасын $(x_1, x_2, ..., x_{n-1})$ шифрланған мәтіннің n-граммасына $(y_0, y_1, ..., y_{n-1})$ төмендегі ережелер бойынша шифрлайды:

$$y_i = E_k(x_i), \quad 0 \le i < n$$
$$E_k : j \to (j + k) (\mathrm{mod}\, n), \qquad 0 \le K < m$$

мұнда, i-ашық мәтін әрпінің сандық коды, j-шифрланған мәтіннің сәйкес әрпінің сандық коды. Осы бөлімнің басында сипаттал

Бақылау сұрақтары

1. Криптология қандай екі бөлімнен тұрады?
2. Симметриялық және ассиметриялық шифрлар айырмашылығы неде?
3. Алмастыру және орналастыру шифрларының мәні қандай?
4. Цезарь шифрының негізгі принципі қандай?
5. Магиялық квадрат арқылы шифрлау қалай орындалады?

Ұсынылған әдебиеттер тізімі:

1. M. M. Kasianchuk, I. Z. Yakymenko & Ya. M. Nykolaychuk «Symmetric Cryptoalgorithms in the Residue Number System» (2021).
2. G. Nişancı, P. G. F. & T. Y. «Symmetric Cryptography on RISC-V: Standardized Algorithms» (2022).
3. Soto-Cruz, E. Ruiz-Ibarra, J. Vázquez-Castillo и др. «A Survey of Efficient Lightweight Cryptography for Power-Constrained Microcontrollers» (2024).