



# Дәстүрлі Симметриялық Криптожүйелер

Бұл презентация дәстүрлі симметриялық криптожүйелердің негізгі ұғымдарын, шифрлау және дешифрлау әдістерін, алмастыру және орналастыру шифрларының ерекшеліктерін түсіндіруге арналған.

# Криптологияның Негізгі Ұғымдары

1

## Криптология

Хабарламаларды құпиялау мен ашу ғылымы. Ол криптография (шифрлау) және криптоанализ (криптоталдау) бөлімдерінен тұрады.

2

## Криптография

Хабарламаны бөгде адамдардан қорғау үшін шифрлау әдістерін қолданады. Ашық мәтінді шифрмәтінге айналдыру процесі.

3

## Криптоанализ

Шифрланған мәтінді кілтсіз бұзып ашуды іздейді. Шифрдың беріктілігі оның бұзып ашылуына қарсы тұра алу қабілетімен өлшенеді.



# Симметриялық және Асимметриялық Криптожүйелер

## Симметриялық Криптожүйелер

Шифрлауда және шифрды ашуда бір кілт қолданылады. Бұл жүйелер қарапайымдылығымен және жылдамдығымен ерекшеленеді.



## Асимметриялық Криптожүйелер (Ашық Кілтті)

Екі кілт қолданылады – ашық және жабық. Ашық кілт арқылы шифрланады, ал жабық кілт арқылы шифрды ашу орындалады. Олар бір-бірімен математикалық байланыста болады.





# Алмастыру Шифрлары

Алмастыру шифрларында мәтіннің әрбір символы белгілі бір ереже бойынша басқа таңбамен ауыстырылады. Бұл ең қарапайым және ең көне шифрлау әдістерінің бірі.



## «Сцитала» Шифры

Б.э.д. V ғасырда Спарттық әскерлер қолданған. Цилиндрлік стерженьге қағаз оралып, мәтін жазылады. Кілт – стерженьнің диаметрі.



## Кестелік Шифрлау

Хабарды кестеге баған бойынша жазып, жол бойынша оқу арқылы шифрлау. Кілт ретінде кесте өлшемі немесе кілттік сөз қолданылады.



## Қосарланған Орналастыру

Құпиялықты арттыру үшін мәтінді екі рет – баған және жол бойынша орналастыру әдісімен шифрлау.

# «Сцитала» Алмастыру Шифры

«Сцитала» шифры б.э.д. **V** ғасырда Спарттық әскерлерде құпиялы әскери байланыс үшін қолданылған. Шифрлау үшін цилиндрлік стерженьге спираль түрінде қағаз қиындысы оралып, оған стержень бойымен хабар мәтіні жазылады.

|   |   |   |   |   |
|---|---|---|---|---|
| х | а | б | а | р |
| м | ә | т | і | н |

Стерженнен оралған мәтін жазылған қағазды алғанда, әріптер ретсіз орналасқан хаостық түрде болады. Шифр мәтінді шешу үшін шифрлау әдісімен қатар, стерженнің диаметрін білу қажет, себебі ол құпиялы кілт болып табылады.

# Кестелік Шифрлау Әдістері

Криптограмма қайта өрлеу заманында саяси, дипломатиялық және әскери жұмыстарда кеңінен қолданылған. Кестелік шифрлау — танымал әдіс, мұнда кілт ретінде кесте өлшемі немесе кілттік сөз пайдаланылады.

## Мысал: 5x7 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 |

Хабарды баған бойынша жазып, шифрлы мәтінді алу үшін кестедегі мәтінді жол бойынша оқимыз: **ТНТСБ ҰЕЕАА АЕШЛР ТҢҒСЫ ЕМОҒА ТПДИР ЫТЕКІ.**

# Қосарланған Орналастыру Әдісі

Құпияның мықтылығын арттыру үшін шифрланған мәтінді қайта шифрлау әдісі — қосарланған орналастыру. Бұл әдісте кесте бағаны мен жолы жеке-жеке орналастырылады.

Бастапқы кесте

|   |   |   |   |
|---|---|---|---|
| Е | К | І | Н |
| Ш | І | К | Ү |
| Н | І | Ұ | Ш |
| А | М | Ы | Н |

Баған бойынша орналастыру

|   |   |   |   |
|---|---|---|---|
| К | Н | І | Е |
| І | Ү | К | Ш |
| І | Ш | Ұ | Н |
| М | Н | Ы | А |

Қосарланған орналастыру әдісінде кілт ретінде баған және жолдың бойында кез келген ретпен орналастырылған сандар алынады. Шифрлау кезінде алдымен баған элементтерін ретімен қоямыз, содан кейін жол элементтерін ретімен қоямыз. Соңғы кестені жол бойынша оқып, шифрлы мәтінді аламыз: **ІҮКШ МНЫІА КНІЕ ІШҰН.**

# Магиялық Квадраттардың Қолданылуы

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

|   |   |   |   |
|---|---|---|---|
| Н | І | К | А |
| Ш | І | Ұ | Ү |
| Н | І | К | Ш |
| Н | Ы | М | Е |

Хабар мәтінін квадраттық кесте торларына сандар ретімен жазамыз. Жол бойынша оқылған шифрмәтін түсініксіз күйге енеді: **НІҚА ШІҰҮ НІКШ ҰЫМЕ.**

Магиялық квадраттар саны квадрат өлшемі өскен сайын артады, бұл орта ғасырларда өте тиімді шифрлау әдісі болды.



# Жай Алмастыру Шифрлары

Жай алмастыру шифрында әр таңба барлық мәтінде бірдей алмастырылады. Мұндай шифрлар біралфавитті қойылым шифрлары деп аталады.

## Полибиан Квадраты

Б.д.д. II ғасырда грек жазушысы Полибий ойлап тапқан **5x5** өлшемді кесте. Шифрлау кезінде ашық мәтіннің әрпін кесте ішінен тауып алып, шифрмәтінге сол әріптен төмен тұрған әріп жазылады.

## Цезарь Шифрлау Жүйесі

Рим императоры Цезарь қолданған алмастыру шифры. Әріптер белгілі бір орынға (мысалы, **3** орынға) ауыстырылады. Мысалы, "**A**" әрпі "**D**" болады.

# Цезарь Шифрының Мысалы

Цезарь шифры — алмастыру шифрының бір түрі. Әріптер үш орынға ауыстырылады (**K = 3**). Мысалы, "A" әрпі "D" болады.

|   |   |
|---|---|
| A | B |
| E | З |
| Қ | Н |
| П | Т |
| Ф | Ц |
| Ь | Ъ |

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

## **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).