Введение в компьютерную науку

Introduction to cryptography

Salymbekov University

Miss Aliia Beishenalieva

aliya.beiwenalieva@gmail.com

29.10.2024

Recap

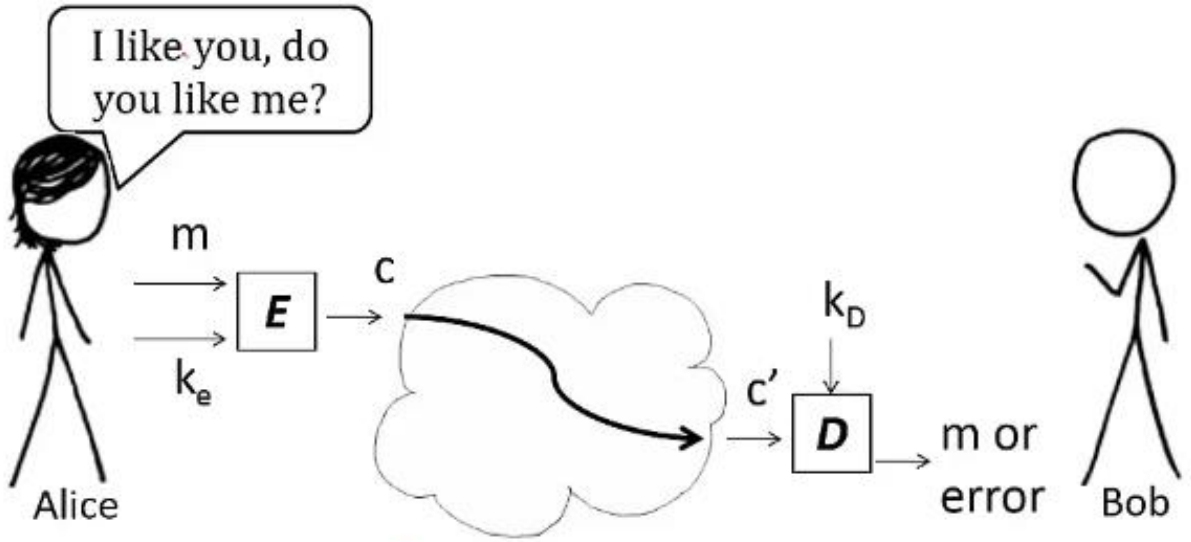
- Что мы прошли на прошлом уроке?

What is the cryptography?

Криптография — это наука о методах шифрования информации, чтобы сделать ее недоступной для несанкционированного доступа. Она обеспечивает защиту данных, передаваемых через каналы связи.

- **Конфиденциальность**: Только авторизованные пользователи могут читать сообщения.
- **Целостность данных**: Обеспечивает защиту данных от изменения.

What is the cryptography?



Cryptosystem

m: Plaintext ***c***: Ciphertext

k_e: Encryption Key ***E***: Encryption Program

k_d: Decryption Key ***D***: Decryption Program

Основные термины

Шифрование и дешифрование:

Шифрование — процесс преобразования текста в зашифрованную форму (шифртекст).

Дешифрование — процесс обратного преобразования зашифрованного текста в исходный.

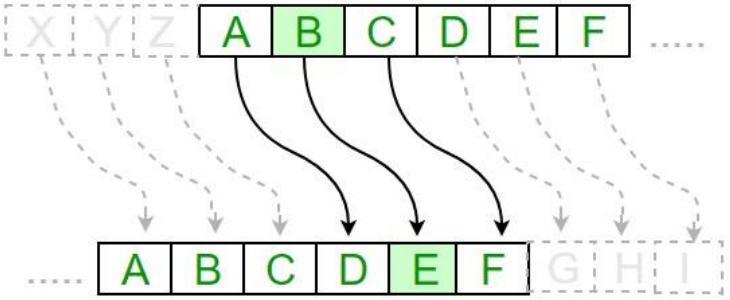
Открытый и закрытый ключи:

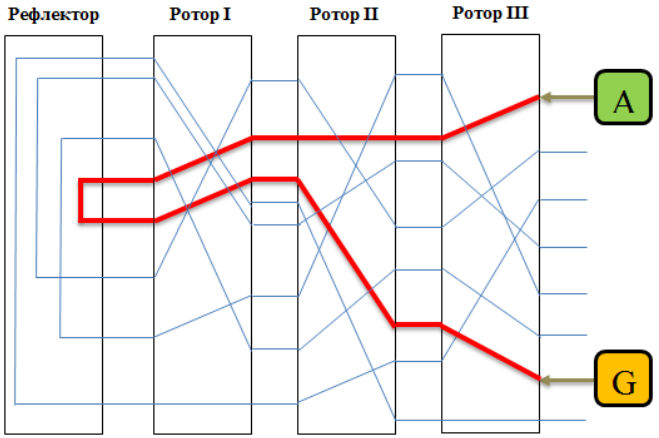
Симметричное шифрование: один ключ используется для шифрования и дешифрования.

Асимметричное шифрование: используется пара ключей — открытый (для шифрования) и закрытый (для дешифрования).

Ранние методы

Шифр Цезаря - простой способ замены букв, использовавшийся Юлием Цезарем. Каждая буква текста сдвигается на определенное количество позиций в алфавите.

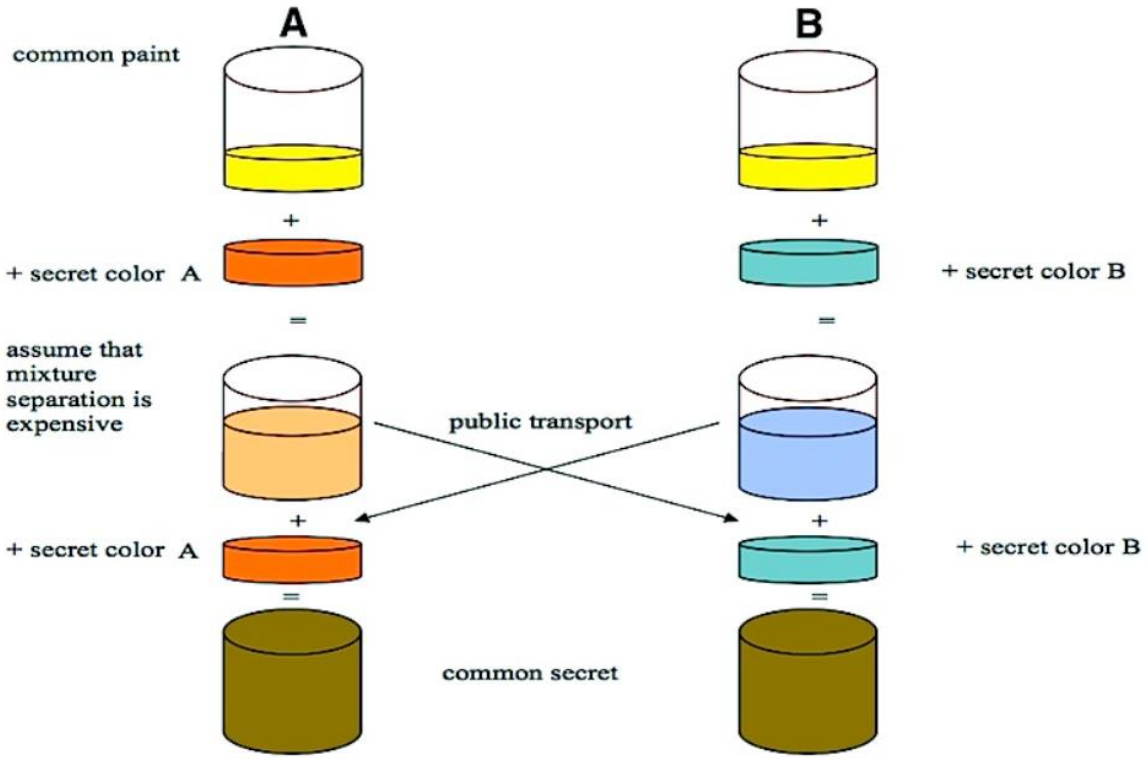




Машина «Энигма» - (Enigma — загадка) — переносная шифровальная машина, использовавшаяся для шифрования и расшифрования секретных сообщений. Использовался во время 2-мировой.

Обмен ключами

- **Mixed color**



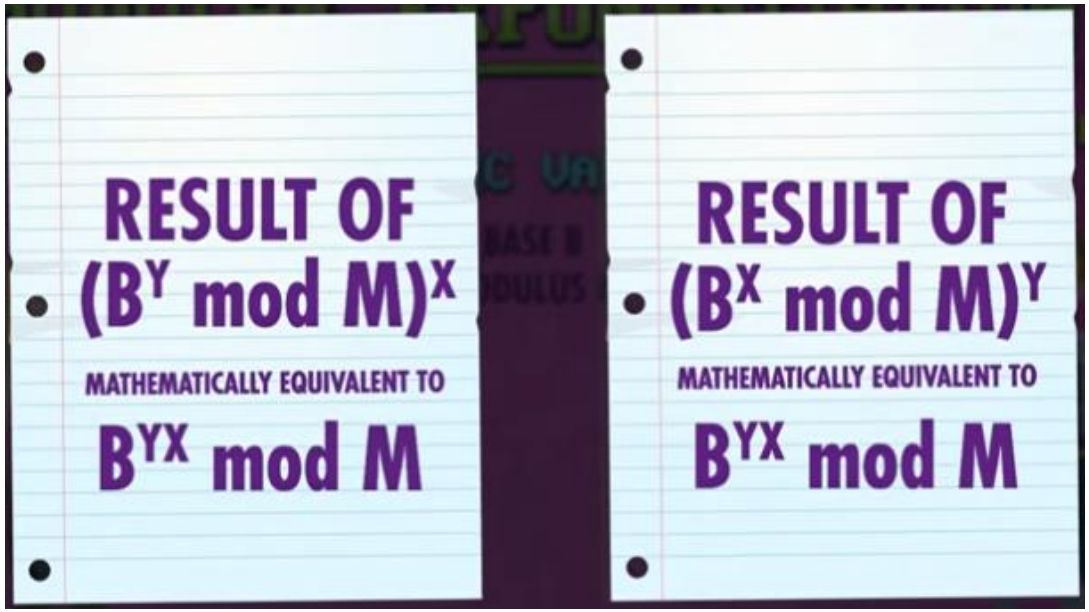
Обмен ключами

- **Math formula**

Y

B, M are known

X



Practice

- Шифрование и дешифрование по алгоритму Цезаря (ключ неизвестный)

Thank you for your attention

Introduction to cryptography

Salymbekov University

Miss Aliia Beishenalieva

aliya.beiwenalieva@gmail.com

29.10.2024