Advanced Cryptography: ICT-6115

Introduction to Cryptography

Most. Jebun Nahar Juthy (IT23612)

Dept. of ICT, MBSTU, Tangail-1902

Mawlana Bhashani
Science and Technology University

30 Nov 2024, MBSTU, Tangail

OUTLINE

- What is Cryptography?
- Key Concepts in Cryptography
- Private Key Cryptography
- Public Key Cryptography

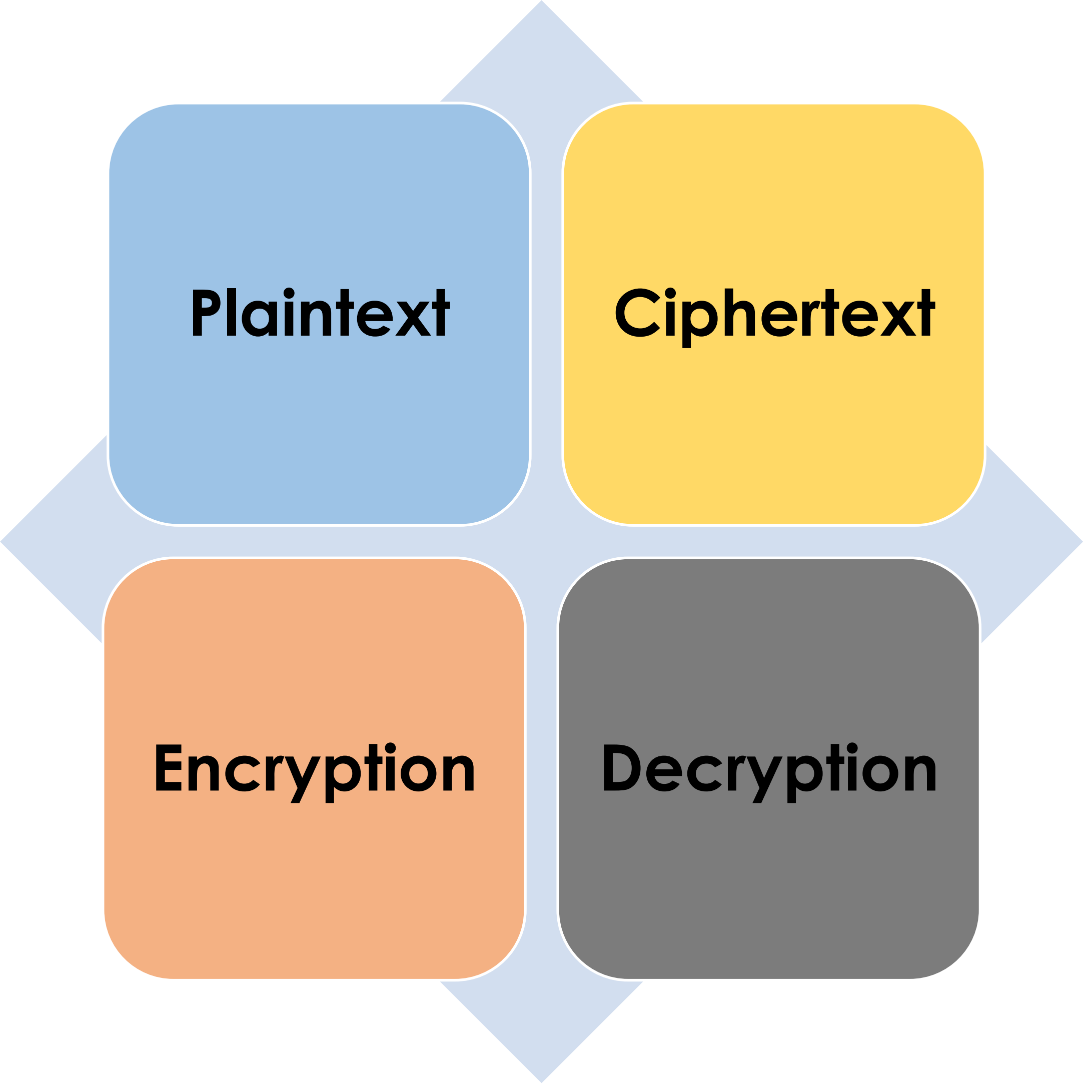
Cryptography

Confidentiality

Integrity

Availability

Key Concepts in Cryptography



Plaintext

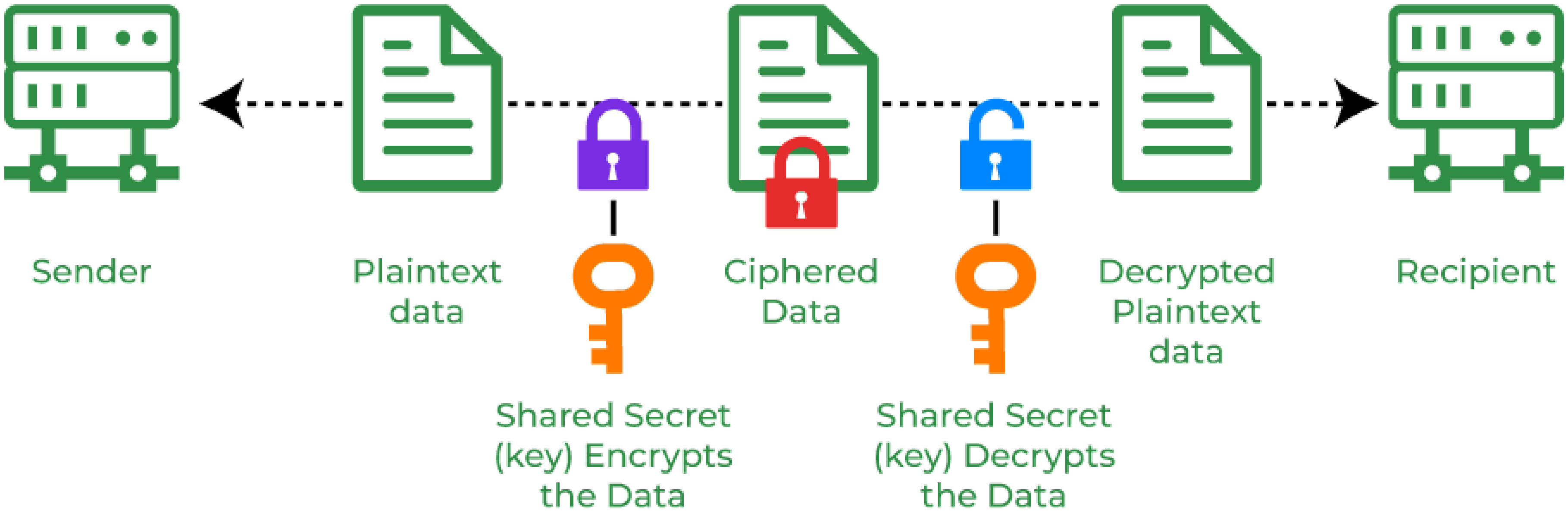
Ciphertext

Encryption

Decryption

Types of Cryptography

Private key Cryptography


Sender
Plaintext data
Shared Secret (key) Encrypts the Data
Ciphered Data
Shared Secret (key) Decrypts the Data
Decrypted Plaintext data
Recipient

Private key Cryptography

❑ Example 7.1

- ➢ One of the first and most famous private key cryptosystems was the shift code used by **Julius Caesar**.
- ➢ We first digitize the alphabet by letting A = 00, B = 01, . . . , Z = 25.
  The encoding function will be,

$$f(p) = p + 3\ mod\ 26$$

that is, A → D, B → E, . . . , Z → C.

The decoding function is then,

$$\begin{aligned} f^{-1}(p) &= p - 3 \bmod 26 \\ &= p + 23 \bmod 26 \end{aligned}$$

Private key Cryptography

- ❑ **Example 7.1 continued..**
- ❑Suppose we receive the encoded message **CRYPTO**.

To decode this message, we first digitize it:

2, 17,24,15,19,14.

Next, we apply the inverse transformation:

25, 14, 21, 12, 16,11.

and get **ZOUMQL**

Private key Cryptography

Affine Cryptosystem

- ❑ A type of substitution cipher in cryptography that combines two mathematical operations: multiplication and addition, to encrypt and decrypt messages.
- ❑ It uses modular arithmetic to ensure the transformations stay within the alphabet range.

The encryption process uses the formula:

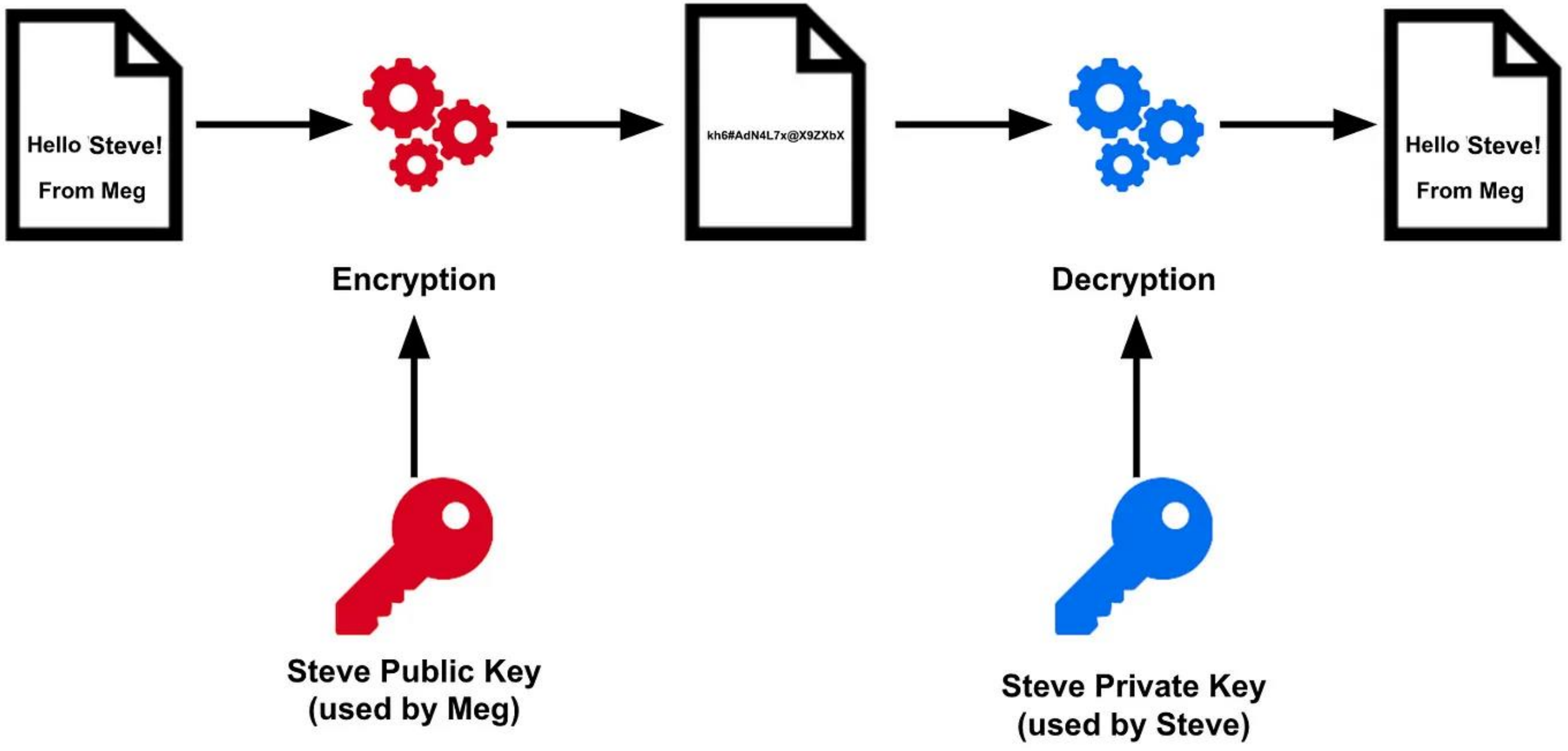
$$f(p) = (a \cdot p + b) \bmod m$$

The decryption process reverses the encryption using the formula:

$$f^{-1}(p) = a^{-1}p - a^{-1}b \bmod 26$$

Types of Cryptography

Public key Cryptography



Public Key Cryptography: RSA

- **Developed by:** R. Rivest, A. Shamir, and L. Adleman (1978).
- **Based on:** RSA is an asymmetric encryption algorithm that uses a public key and a private key to encrypt and decrypt data.
- RSA works by creating a public key that's the product of two large prime numbers, along with an auxiliary value. The prime factors are kept secret. Anyone can use the public key to encrypt a message, but only someone with the prime factors can decode it.

How RSA Works: Key Generation

1. Choose two large prime numbers **p** and **q**.

2. Compute :

$$\rightarrow n = p \times q$$
$$\rightarrow \phi(n) = (p-1)(q-1)(Euler's\ \phi - function)$$

3. Find a number EEE (public key) such that:

$$gcd\big(E, \phi(n)\big) = 1$$

4. Use the **Euclidean Algorithm** to find D (private key) such that:

$$D \times E \equiv 1(\mathrm{mod}\,\phi(n))$$

How RSA Works

Encryption

1. Convert the message into integers using a scheme (**e.g., A = 00, Z = 25**).

2. Break the message into pieces ***x*** such that ***x* < *n***.

3. Compute: $\boldsymbol{y = x^E \pmod{n}}$

4. Send y (ciphertext) to the receiver.

Decryption

1. Receiver computes:

$$\boldsymbol{x = y^D \pmod{n}}$$

2. Recover original message ***x***

Thank You