**[CS309] Introduction to Cryptography and Network Security**

Course Instructor: Dr. Dibyendu Roy
Scribed by: Tanuj Saini (202251141)

Autumn 2024-2025
Lecture (Week 1,2)

# 1. Introduction to Cryptography

## 1.1 Cryptography and Cryptanalysis

**Cryptography** is the practice of securing information by transforming it into an unreadable format, only reversible with a secret key. On the other hand, **Cryptanalysis** involves studying and breaking these cryptographic algorithms to test their strength.

**Cryptology** combines both Cryptography and Cryptanalysis.

## 1.2 NIST Standards

The **National Institute of Standards and Technology (NIST)** standardizes cryptographic algorithms and ensures their design and implementation meet high standards of security.

# 2. Example: ATM Security

Consider two ATMs:

- ATM1: `pin1 + x = y1`
- ATM2: `pin2 + x = y2`

Here, $x$ is a secret key. The value $y1$ is stored on the card, and to access the original PIN, $x$ is subtracted from $y1$.

# 3. Encryption and Decryption

## 3.1 Encryption Process

Encryption converts readable text (plaintext) into unreadable text (ciphertext) using an encryption algorithm. This can be mathematically represented as:

$$E(P, K) = C$$

where $P$ is the plaintext, $K$ is the key, and $C$ is the ciphertext.

## 3.2 Decryption Process

Decryption is the reverse process where ciphertext is transformed back into readable plaintext using a decryption algorithm:

$$D(C, K) = P$$

In the ATM example, `pin1` is the plaintext, $x$ is the secret key, and $y1$ is the ciphertext.

# 4. Types of Cryptography

## 4.1 Symmetric Key Cryptography

This technique uses the same secret key for both encryption and decryption.

## 4.2 Public Key Cryptography

This method employs two different keys: a public key for encryption and a private key for decryption. These keys are mathematically related but different.

# 5. Security Services Provided by Cryptography

## 5.1 Confidentiality

Ensures that information is accessible only to those authorized to have access, often achieved through encryption.

## 5.2 Integrity

Guarantees that the information cannot be altered without detection.

## 5.3 Authentication

Verifies the identity of the source of the information.

## 5.4 Non-repudiation

Prevents the sender from denying the transmission of a message.

# 6. Classical Cipher Techniques

## 6.1 Caesar Cipher

The Caesar Cipher shifts the alphabet in the plaintext by a fixed number of positions. For example:

$$E(x, 3) = (x + 3) \mod 26$$

$$D(c, 3) = (c + 26 - 3) \mod 26$$

## 6.2 Transposition Cipher

In this method, the characters of the plaintext are rearranged according to a predefined system to form the ciphertext. For example:

$$M = m_1, m_2, m_3, \ldots, m_t$$

$$C = m_{e(1)}, m_{e(2)}, \ldots, m_{e(t)}$$

$$M = c_{e^{-1}(1)}, c_{e^{-1}(2)}, \ldots, c_{e^{-1}(t)}$$

## 6.3 Substitution Cipher

In substitution ciphers, each letter in the plaintext is replaced by another letter. The function can be expressed as:

$$C = e_{m1}, e_{m2}, \ldots, e_{mt}$$

where $e$ represents the substitution rule.

## 6.4 Affine Cipher

An advanced substitution cipher where each letter in the alphabet is mapped to its numeric equivalent, encrypted using a mathematical function, and then converted back to a letter. The encryption function is:

$$e(x, k) = (a \cdot x + b) \mod 26$$

The decryption function is:

$$d(c, k) = ((c - b) \cdot a^{-1}) \mod 26$$

## 6.5 Playfair Cipher

This method uses a 5x5 matrix generated from a keyword. Pairs of letters from the plaintext are encrypted as follows:

1. If both letters are in the same row, replace them with the letters to their immediate right.
2. If both letters are in the same column, replace them with the letters immediately below.
3. If neither of the above applies, the letters form a rectangle, and each letter is replaced by the one in the same row but in the column of the other letter.

**Example:**
*Secret Key: PLAYFAIR EXAMPLE*

| | | | | |
|---|---|---|---|---|
| $P$ | $L$ | $A$ | $Y$ | $F$ |
| $I$ | $R$ | $E$ | $X$ | $M$ |
| $B$ | $C$ | $D$ | $G$ | $H$ |
| $S$ | $T$ | $U$ | $V$ | $W$ |
| $K$ | $N$ | $O$ | $Q$ | $Z$ |

*Plaintext: HIDE*
*Ciphertext: BMOD*