# Network Security

**Unit 1** — Security Approaches, the CIA Triad, Security Services, Cryptography & Classical Encryption Techniques

NETWORK SECURITY | UNIT 1

# Three Security Approaches

Security is not a single action — it is a layered strategy spanning three phases of threat response.

### Prevention

Act **before** a threat occurs. Identify root causes, define the threat, and adopt mechanisms or programs to eliminate it.

### Protection

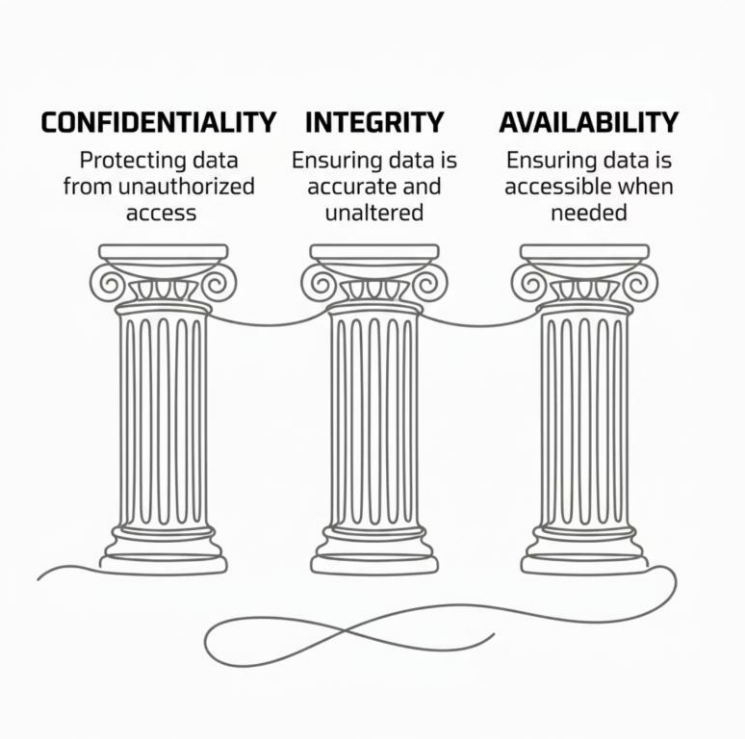
Threats are **imminent**. Deploy controls and safeguards to minimize damage and reduce the attack surface.

### Resilience

Threats have **already occurred**. Focus on recovery, continuity, and restoring normal operations.

# The CIA Triad

The foundational model guiding all information security strategies — every control maps back to these three principles.




### Confidentiality

Information is accessible **only to authorized parties**. No third-party disclosure.

### Integrity

Data remains **trustworthy, complete, and unmodified** by unauthorized users.

### Availability

Data is **accessible when needed** — readable, writable, executable, and modifiable by authorized users.

# Security Services

## Data Confidentiality

Information accessible only for reading by authorized parties — covers printing, display, and all forms of disclosure.

## Data Integrity

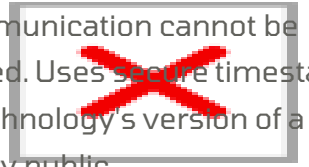
Only authorized parties may modify data. Covers writing, changing status, deleting, and replaying messages.

## Authentication

**Peer entity:** confirms identities during connection. **Data origin:** corroborates the source of a data unit.

## Non-Repudiation

Communication cannot be denied. Uses secure timestamps — technology's version of a notary public.



## Access Control

Determines **who has access** to what resources, and under what conditions.

# Security Mechanisms

Mechanisms are the technical tools that **implement** security services.

## Encipherment

Hides data using algorithms, making it unreadable without the key.

## Data Integrity

Appends a verification value checked before and after transmission.

## Digital Signature

Electronic signature verifying sender identity.

## Authentication Exchange

Two-way handshake confirming identity at the TCP/IP layer.

## Routing Control

Changes routes to prevent eavesdropping on a single path.

## Notarization

Trusted third party stores requests to prevent denial.

# A Model for Network Security


The **Trusted Third Party** oversees both ends. An **Opponent** may attempt to intercept the message in transit.

### Design an Algorithm

Create encryption/decryption algorithms for sender and receiver.

### Generate Secret Info

Produce plaintext and key — larger keys mean stronger security.

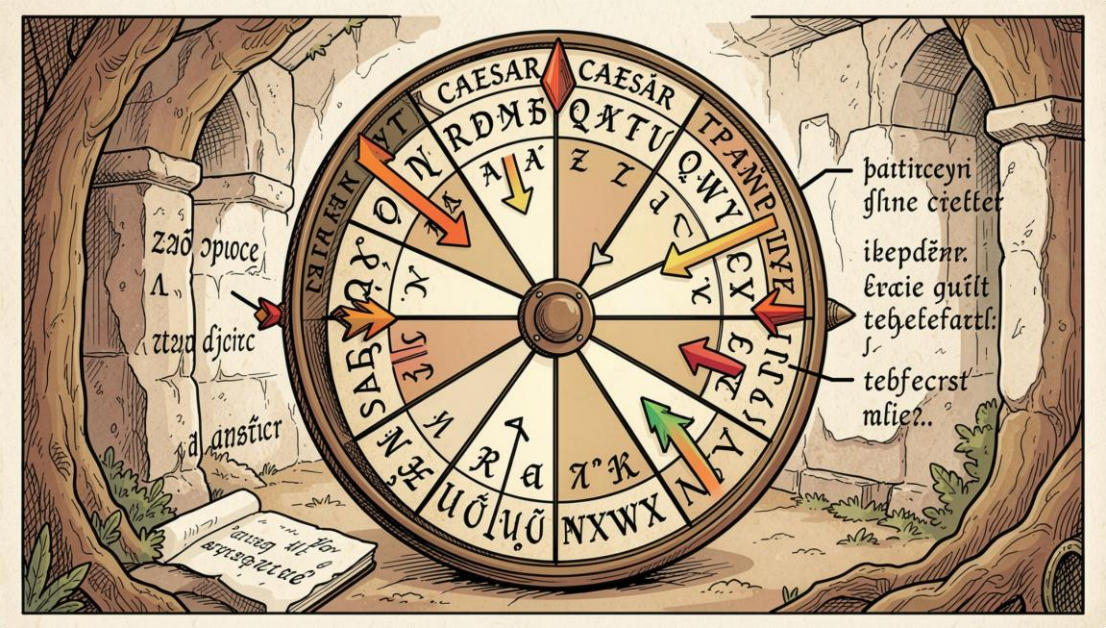
### Key Distribution

Develop methods for securely sharing keys between parties.

### Specify a Protocol

Define rules both parties follow, embedding security essentials in packets.

# Cryptography Fundamentals




## Core Concepts

**Plaintext** — Human-readable input. **Ciphertext** — Encrypted, unreadable output. **Encryption** converts plaintext to ciphertext; **decryption** reverses it.

**Caesar Cipher (k=7):** "This is a plaintext" → "Aopz pz h wshpualea"

## Types of Cryptography

- **Symmetric:** Single shared key (DES, AES) — fast but requires secure key exchange
- **Hash Function:** No key; fixed-length output; passwords cannot be reversed
- **Asymmetric:** Public key encrypts, private key decrypts — no shared secret needed

# Classical Encryption: Substitution Ciphers

1

### Caesar Cipher

Shift each letter by *k* positions: $E_k(p) = (p + k) \bmod 26$. "Cyber Security" (k=3) → "FBEHUVHFXULWB"

2

### Monoalphabetic Cipher

Any permutation of 26 letters. Each plaintext letter maps to one fixed ciphertext letter.

3

### Playfair Cipher

5×5 matrix using a keyword. Encrypts letter pairs via row, column, or rectangle rules.

4

### Hill Cipher

Matrix-based: $C = P \times K \bmod 26$. Encrypts groups of letters using linear algebra.

# Advanced Classical Techniques

## Polyalphabetic — Vigenère Cipher

Uses a repeating keyword, applying a different shift to each letter.

$C_i = (P_i + k_i) \bmod 26$

## One-Time Pad — Vernam Cipher

Random key as long as the message, used once then discarded. **Provably unbreakable.** Each extra bit doubles cracking time — a 128-bit key is considered safe.

## Transposition Techniques

**Rail Fence:** Write diagonally, read by rows.
**Row-Column:** Write in a rectangle, read columns in key order.

## Steganography

Hide data *within* ordinary files — text, images, audio, video, or network protocols — without encrypting.

# Cryptographic Attacks

## 1 Brute Force

Try every possible key until the correct one is found. An 8-bit key has 256 possibilities.

## 2 Ciphertext-Only

Attacker has only ciphertext and attempts to deduce the key or plaintext.

## 3 Chosen Plaintext

Attacker selects plaintexts to obtain ciphertexts, simplifying key recovery.

## 4 Chosen Ciphertext

Attacker analyzes chosen ciphertexts against their plaintexts to guess the key. Older RSA versions were vulnerable.

## 5 Known Plaintext

Attacker knows some plaintext-ciphertext pairs and uses them to recover the key.

## 6 Key & Algorithm

Attacker analyzes the cryptographic algorithm itself to recover the key.