

## Basics of Cryptography

### 1. What is Cryptography?

Cryptography is the science of securing information so that only the intended person can read or use it.

It protects confidentiality, integrity, authentication, and non-repudiation.


---

### 2. Core Principles (CIA + AN)

- Confidentiality → Data is secret (encryption).
  - Integrity → Data is not altered (hashing).
  - Authentication → Verify identity (digital signatures, certificates).
  - Non-repudiation → Sender cannot deny sending (signatures, logs).
- 

### 3. Types of Cryptography

#### ◆ 1. Symmetric Encryption

- Same key for encryption & decryption.
- Fast, used for bulk data encryption.
- Examples: AES, DES, 3DES, Blowfish.
-  Problem → Key distribution (how to share securely).

#### ◆ 2. Asymmetric Encryption

- Uses a public key (encrypt) and a private key (decrypt).
- Slower but more secure for communication.
- Examples: RSA, ECC, Diffie-Hellman.
- Used in: SSL/TLS, digital certificates, email encryption.

#### ◆ 3. Hash Functions

- One-way cryptographic functions.

- No decryption possible.
- Used for password storage, integrity checks.
- Examples: MD5, SHA-1, SHA-256.

#### ◆ 4. Digital Signatures

- Provide authentication, integrity, non-repudiation.
  - Example: RSA signatures, ECDSA.
- 

#### 4. Cryptographic Attacks

- Brute Force Attack → Trying all possible keys.
  - Dictionary Attack → Using wordlists to crack hashes.
  - Man-in-the-Middle (MITM) → Intercepting communication.
  - Replay Attack → Reusing valid data packets.
  - Quantum Threat → Future quantum computers breaking RSA, ECC.
- 

#### 5. Applications in Cybersecurity

- Secure Communication → HTTPS, VPNs.
- Data Protection → Disk encryption (BitLocker, VeraCrypt).
- User Authentication → Password hashing, MFA.
- Blockchain & Cryptocurrency → Hashing + public key cryptography.
- Digital Forensics & Evidence → Digital signatures.