Blog 2: Cryptography – The Art of Securing Secrets

"Those who can imagine anything, can create the impossible." – Alan Turing

Cryptography is the backbone of secure digital communication. It's the art and science of converting information into an unreadable format that can only be deciphered by the intended recipient.

Cryptography is essential for protecting everything from emails and passwords to financial transactions and national secrets. It ensures confidentiality, integrity, authenticity, and non-repudiation in digital communication.

Types of Cryptography

- **Symmetric Cryptography**: Uses the same key for encryption and decryption (e.g., AES).
- **Asymmetric Cryptography**: Uses a public and private key pair (e.g., RSA).
- **Hash Functions**: One-way functions used to verify data integrity (e.g., SHA-256).

Real-world Applications

- **End-to-End Encrypted Messaging Apps** like Signal and WhatsApp
- **SSL/TLS** for secure browsing
- **Blockchain** – Cryptographic algorithms ensure transaction security

Common Algorithms

- **AES** – Advanced Encryption Standard
- **RSA** – Rivest–Shamir–Adleman algorithm
- **Elliptic Curve Cryptography (ECC)** – Used for secure mobile communication

Future of Cryptography

With the emergence of quantum computing, current cryptographic systems may become obsolete. Post-quantum cryptography is already being explored by researchers worldwide.

References:

- NIST Cryptographic Standards
- Crypto101: Introduction to Cryptography