Cryptography is the art and science of securing communication. It is an essential component of modern cybersecurity, as it provides a robust shield against malicious attacks.

How Cryptography Works

At its core, cryptography involves converting plain text (readable information) into ciphertext (unintelligible data) through encryption. This transformation is achieved using complex algorithms and cryptographic keys. Only individuals with the correct decryption key can revert the ciphertext back to its original form.

The Pillars of Cryptographic Security

Cryptography ensures the following security properties:

- **Confidentiality:** Only authorized parties can access and understand the information.
- **Integrity:** Data remains unaltered during transmission or storage.

- **Authentication:** Verifies the identity of the sender and receiver.
- **Non-repudiation:** Prevents the sender from denying having sent the message.

Types of Cryptography

There are three main types of cryptography:

- **Symmetric Key Cryptography:** Uses a single key for both encryption and decryption.
- **Asymmetric Key Cryptography:** Employs a pair of keys: a public key for encryption and a private key for decryption.
- **Hash Functions:** Creates a fixed-size digital fingerprint of data.