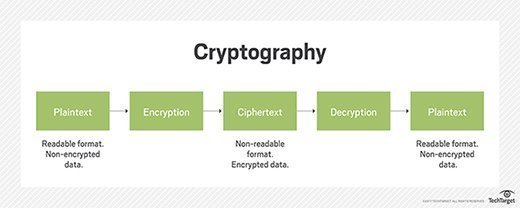


**Cryptography**

Cryptography is the process of hiding or coding information so that only the person a message was intended for can read it. In simple terms converting plain text into a cipher text which is in unreadable format for someone who try to steal the message.



**Cryptography Importance**

Cryptography remains important to protecting data and users, ensuring confidentiality, and preventing cyber criminals from intercepting sensitive corporate information. Common uses and examples of cryptography include the following:

* Privacy and Confidentiality
* Authentication (Integrity, Non-repudiation)
* Key exchange

**Types of Cryptography**

1. **Secret key Cryptography**

Secret key cryptography, also known as symmetric encryption, uses a single key to encrypt and decrypt a message. The sender encrypts the plaintext message using the key and sends it to the recipient who then uses the same key to decrypt it and unlock the original plaintext message.

Example: Advanced Encryption Standard (AES)

1. **Public key Cryptography**

Public key cryptography (PKC), or asymmetric cryptography, uses mathematical functions to create codes that are exceptionally difficult to crack. It enables people to communicate securely over a nonsecure communications channel without the need for a secret key.

Example: Rivest, Shamir, and Adleman (RSA alogorithm)

As you all know that Cryptography is primarily used to ensure **confidentiality** by encrypting data, so only authorized parties can access it. **Hashing**, on the other hand, ensures integrity by creating a unique fixed-size output (hash) for a set of data.

**Hash Function**

Hashing is like creating a unique "fingerprint" for a piece of data.Hash function, a special formula that takes any data (like password) and turns it into a short, fixed-size string of characters called a hash value (or just "hash").

**Cryptographic Key Attacks and Risks**

However, as more entities rely on cryptography to protect communications and data, it is vital to keep keys secure. One compromised key could result in regulatory action, fines and punishments, reputational damage, and the loss of customers and investors.

Organizations and individuals can minimize and mitigate cryptography-related threats with a dedicated electronic key management system from a reputable provider. The solution must use a [**hardware security module**](https://www.fortinet.com/resources/cyberglossary/hardware-security-module) to generate and protect keys, and underpin the entire system’s security.

Cryptography is essential for protecting data and communications by converting plain text into ciphertext using various techniques. It maintains confidentiality, integrity, authenticity, and non-repudiation.