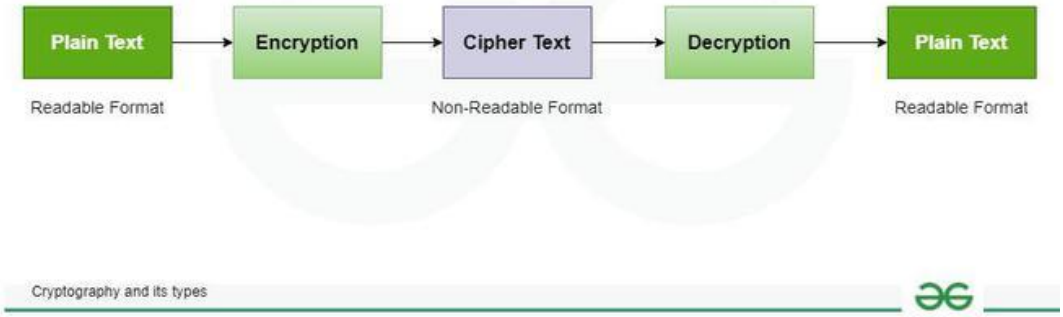
Cryptography and its Types

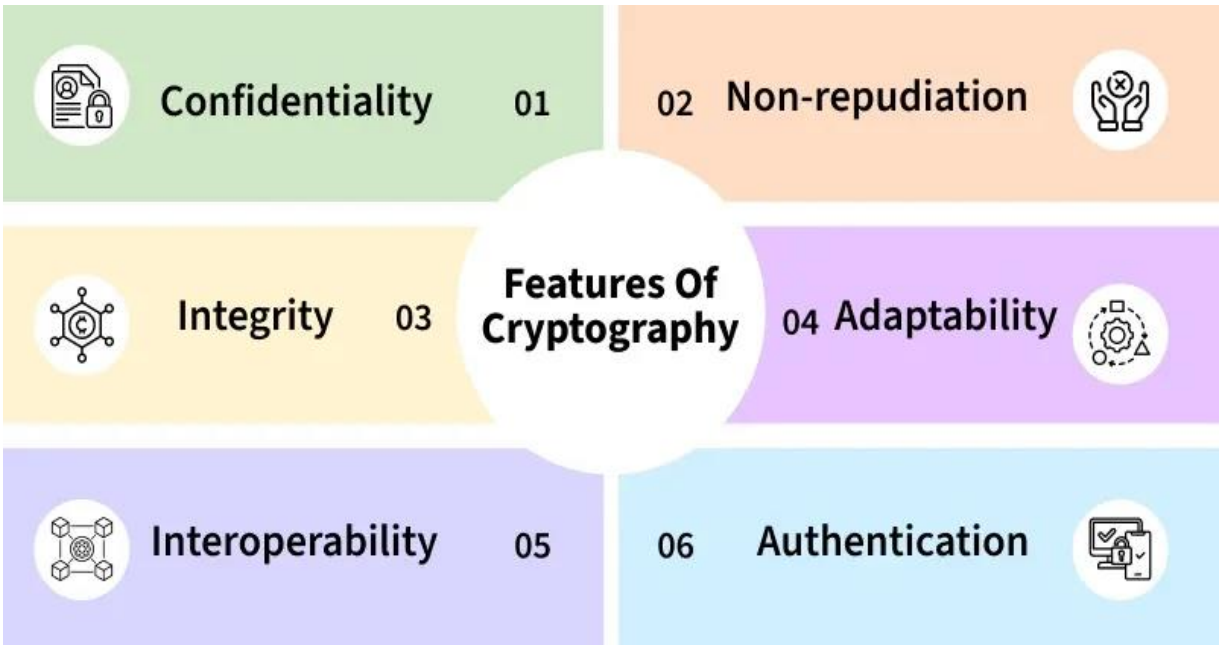
Cryptography is a technique of securing information and communications using codes to ensure confidentiality, integrity and authentication. Thus, preventing unauthorized access to information. The prefix "crypt" means "hidden" and the suffix "graphy" means "writing". In Cryptography, the techniques that are used to protect information are obtained from mathematical concepts and a set of rule-based calculations known as algorithms to convert messages in ways that make it hard to decode them.



These algorithms are used for cryptographic key generation, digital signing, and verification to protect data privacy, web browsing on the internet and to protect confidential transactions such as credit card and debit card transactions.

Features Of Cryptography

The features of cryptography that makes it a popular choice in various applications could be listed down as



1. **Confidentiality:** Information can only be accessed by the person for whom it is intended and no other person except him can access it.

2. **Non-repudiation:** The creator/sender of information cannot deny his intention to send information at a later stage.

3. **Integrity:** Information cannot be modified in storage or transition between sender and intended receiver without any addition to information being detected.

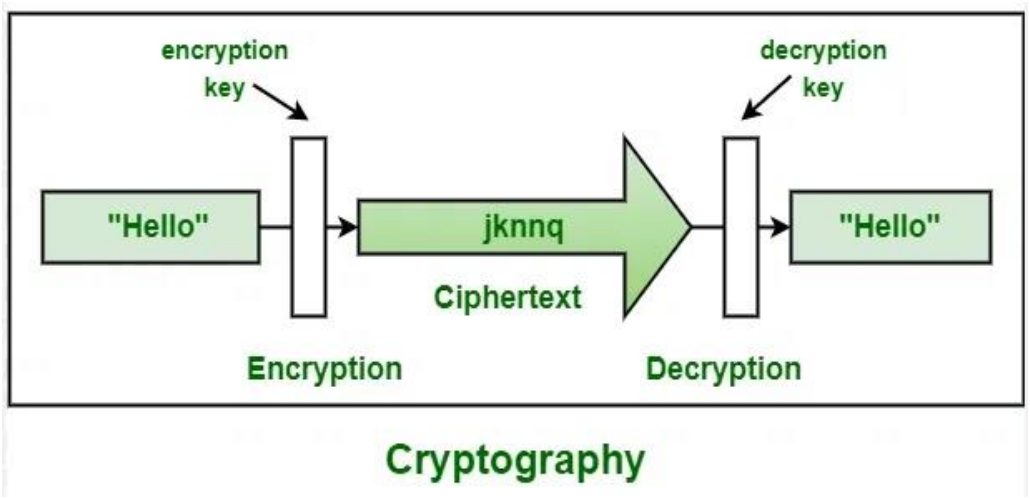
4. **Adaptability:** Cryptography continuously evolves to stay ahead of security threats and technological advancements.

5. **Interoperability:** Cryptography allows for secure communication between different systems and platforms.

6. **Authentication:** The identities of the sender and receiver are confirmed. As well destination/origin of the information is confirmed.

Working of Cryptography

As we all know, cryptography technique is use to convert plain text into ciphertext. This technique is done by cryptographic key. Basically, cryptographic key is a string of characters which is used to encrypts the data and decrypt the data.

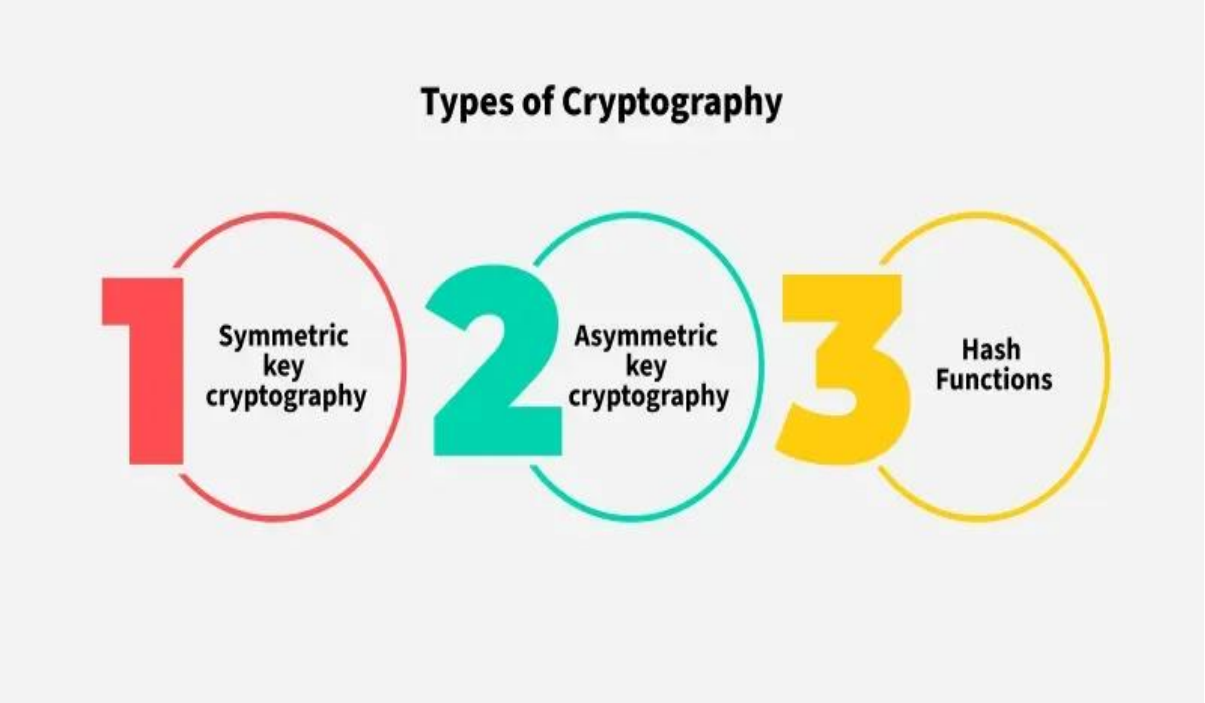


Here,

```
"Hello" is a plaintext and convert into ciphertext "jknnq" with the help of
cryptographic key and then decrypt into "Hello".
```

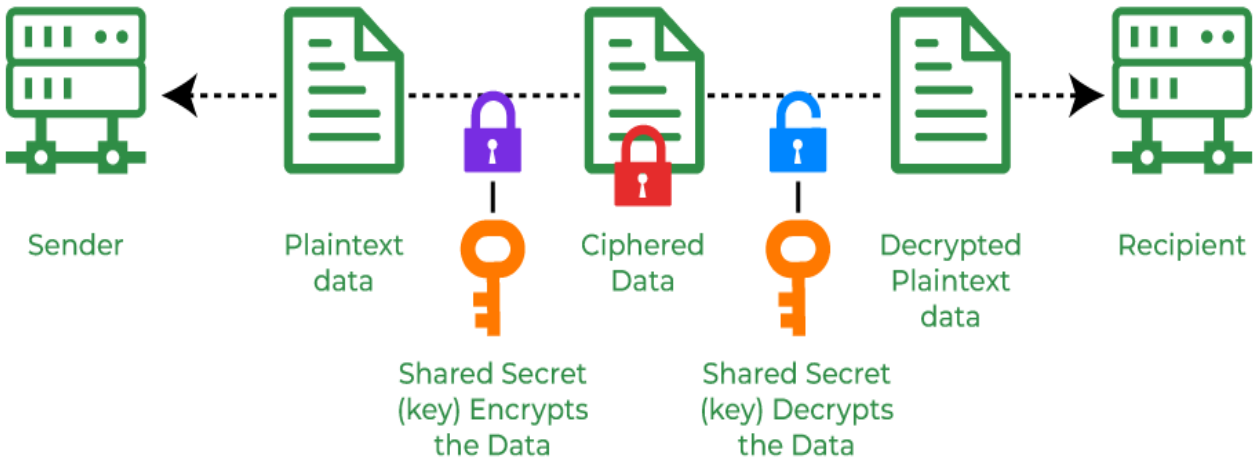
Types Of Cryptography

There are three types of cryptography, namely Symmetric Key Cryptography, Asymmetric Key Cryptography and Hash functions, here's a detailed explanation below:



1. Symmetric Key Cryptography

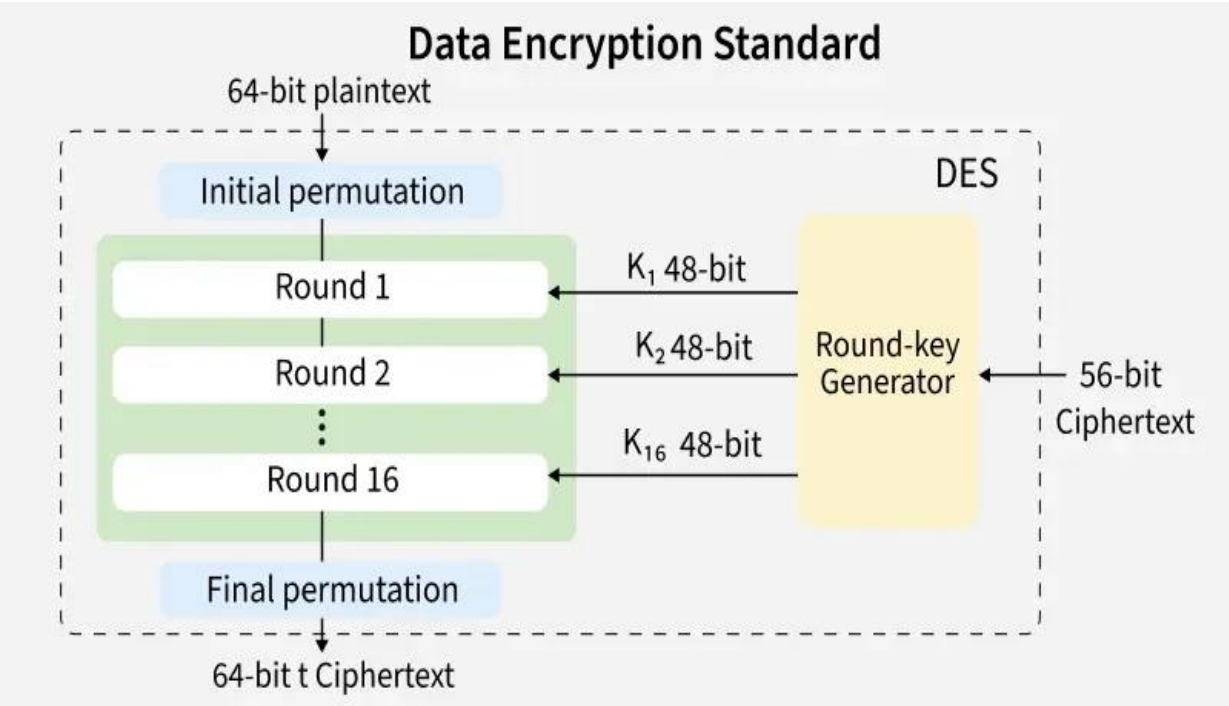
Symmetric Key Cryptography is an encryption system where the sender and receiver of a message use a single common key to encrypt and decrypt messages. Symmetric Key cryptography is faster and simpler but the problem is that the sender and receiver have to somehow exchange keys securely. The most popular symmetric key cryptography systems are Data Encryption Systems (DES) and Advanced Encryption Systems (AES) .



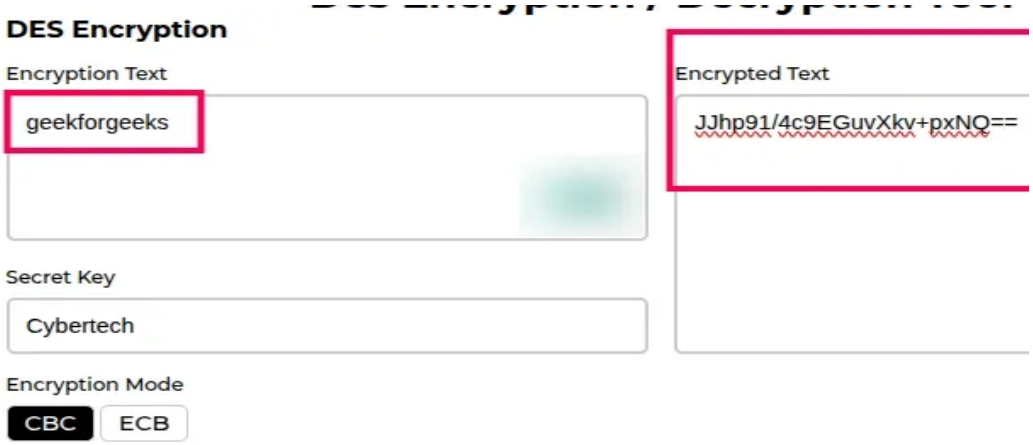
Example:

1. Data Encryption Standard (DES)

DES (Data encryption standard) is an older encryption algorithm that is used to convert 64-bit plaintext data into 48-bit encrypted ciphertext. It uses symmetric keys (which means same key for encryption and decryption). It is kind of old by today's standard but can be used as a basic building block for learning newer encryption algorithms.



example of DES Encryption and Decryption tool:


DES Encryption
Encryption Text
geekforgeeks
Encrypted Text
JJhp91/4c9EGuvXkv+pxNQ==
Secret Key
Cybertech
Encryption Mode
CBC
ECB

Asymmetric Key Cryptography

In Asymmetric Key Cryptography a pair of keys is used to encrypt and decrypt information. A sender's public key is used for encryption and a receiver's private key is used for decryption. Public keys and Private keys are different. Even if the public key is known by everyone the intended receiver can only decode it because he holds his private key. The most popular asymmetric key cryptography algorithm is the RSA algorithm.