# PRINCIPLES OF CYBERSECURITY:

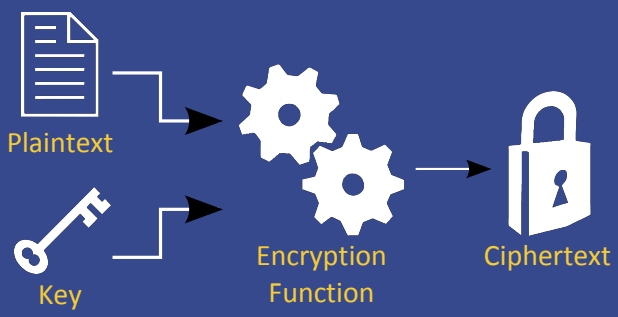
# Encryption

Encryption is the process of transforming an original intelligible message (plaintext) into its secure unintelligible form (ciphertext) for storage or transmission. Once encrypted, information cannot be read by unauthorized third parties.

## The Encryption Process

There are four main components that are part of the encryption process:

1. **Plaintext** - The original intelligible message
2. **Encryption/Decryption Function**- The method used to transform the original intelligible message into its secure unintelligible form (encryption) or vice-versa (decryption).
3. **Key(s)**- Secret code(s) used by the function to encrypt or decrypt.
4. **Ciphertext**- The unintelligible encrypted message





### Symmetric Key

In a symmetric key cryptosystem, the same key is used to encrypt the plaintext and decrypt the ciphertext. This symmetric key is a shared secret known by both the sender and receiver of the message. Only those with the symmetric key can decrypt the ciphertext.


### Asymmetric Key

In an asymmetric key cryptosystem each user has two keys, a public key and a private key. The user's public key is known to all other users of the system. The private key is known only to the person who will receive the encrypted message.

The message is encrypted by the sender using the recipient's public key. The recipient of the encrypted message can then decrypt it using the corresponding private key. The encrypted message can only be decrypted using the private key, not even the sender can decrypt the message once it has been encrypted using the recipients public key.