

# Definitions

## **Plaintext**

The message in its clear form (the original message)

## **Ciphertext**

The message in its ciphered form (the encrypted message)

## **Encryption**

Transform a plaintext into ciphertext

## **Decryption**

Transform a ciphertext into a plaintext

# Definitions

## **Cryptographic algorithm**

The method to do encryption and decryption

## **Cryptographic key**

An input variable used by the algorithm for the transformation

## **N-bit security entropy** (a.k.a. the key space)

The number of bits necessary to encode the number of possible keys (could be different than the key length)