

# 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)

## **Monoalphabetic cipher**

A specific letter in the plaintext is consistently substituted with another letter in the cipher text

# Definitions

## **Polyalphabetic Cipher**

A specific letter in the plaintext may be substituted with different letters in the cipher text

## **Cryptography**

The art and science of securing messages

## **Cryptanalysis**

The art and science of breaking secured messages to reveal the hidden message

## **Cryptography**

The art and science of secure messaging which encompasses cryptography and cryptanalysis