CS387 - Applied Cryptography

Ángel Sola Orbaiceta

December 2021

1 Concepts

Given a message $m \in M$, where M is the set of all possible messages, and a key $k \in K$, where K is the set of all possible keys, an encryption function E can be defined as:

$$E : M \times K \to C$$

where $c \in C$ is the *ciperthext* (being C the set of all possible ciphertexts). Conversely, a decryption function D can be defined as:

$$D : C \times K \to M$$

The **correctness property** states that, for all messages and keys, decrypting the result of encrypting a message must result in the message itself. Mathematically:

$$\forall m, k : D_k(E_k(m)) = m$$

The **security property** states that the ciphertext reveals nothing about the key or original message.

1.1 One-Time Pad

The one-time pad is based in the XOR ($\oplus$) function. The XOR function satisfies the property that any value XOR-ed with itself equals zero: $x \oplus x = 0$. The one-time pad uses this property so that, by using a key that's the same size as the ciphertext, we can do:

$$c = m \oplus k$$

$$m = c \oplus k$$