Symmetric Encryption: Building secure Encryption Schemes

Raphael Pertler

October 20, 2025

Stream Chiphers

Definition

We know that a Vernam Key is secure if we use the key only once.
What if the Vernam key is infinite?

Definition

A Block Cipher is a tuple
$(X = \{0,1\}^l\ ; K = \{0,1\}^s ; E ; D)$
where:

- E deterministic encryption algorithm.
- D deterministic decryption algorithm.

It has to satisfy:

$$\forall x \in \{0,1\}^l,\ k \in \{0,1\}^s\ :\ D(E(x,k)k) = x$$