# Symmetric Encryption

Raphael Pertler

October 14, 2025

## Encryption Schemes

**Definition**

An Encryption Scheme is a tuple $(X, K, E, D)$ with:

- $X \subseteq \{0,1\}^*$ Plaintexts
- $K \subseteq \{0,1\}^*$ the finite Set of keys
- $E$ is a probabilistic encryption algorithm with $x \in X; k \in K$ as inputs, so that $E(x,k) = y \in \{0,1\}^*$
- $D$ is a deterministic decryption algo. with $y \in \{0,1\}^*; k \in K$ as inputs and returns $x \in X$

The Scheme has to satisfy the
"perfect correctness" property:
$\forall x \in X; k \in K : D(E(x,k)k) = x$

$y := E(x,k)$ is called a cyphertext.
$Y$ is the set of all possible cyphertexts.
$Y \subseteq \{0,1\}^*$

**Definition**

Let $X, K, E, D$ be an encryption scheme with deterministic encryption.
For $k\ in K$ the function:

$$E(\cdot,k) : X \to Y; x \to E(x,k)$$

Is called a Cipher.