CS 127/CSCI E-127: Introduction to Cryptography

Definition 1 *A Block Cipher is a family:*

$$\mathcal{F} = \left\{ f_k : \{0,1\}^l \to \{0,1\}^l \right\}_{k \in \{0,1\}^n}$$

Such that:

1. f_k is a permutation.
2. Given k, f_k, and $f_k' \mathcal{F}$ it is easy to compute.
3. For $k \xleftarrow{R} \{0,1\}^n$, f_k is indistinguishable from a truly random permutation.

Definition 2 *AES is a variant of a "substitution permutation network".*

1. $l = 128$
2. $n = 128, 192, 256$