

Schéma de chiffrement

Définition

- Un schéma de chiffrement Π est défini par un tuple $(\mathcal{P}, \mathcal{C}, \mathcal{K}, \mathcal{E}, \mathcal{D})$ où
 - \mathcal{P} l'espace des messages clairs
 - \mathcal{C} l'espace des cryptogrammes
 - \mathcal{K} l'espace des clés
 - $\mathcal{E} = \{E_k \mid k \in \mathcal{K}\}$ avec $E_k : \mathcal{P} \rightarrow \mathcal{C}$ fonctions de chiffrement
 - $\mathcal{D} = \{D_k \mid k \in \mathcal{K}\}$ avec $D_k : \mathcal{C} \rightarrow \mathcal{P}$ fonctions de déchiffrement
- On demande que $\forall k \in \mathcal{K}, \forall m \in \mathcal{M} : D_k(E_k(m)) = m$

Schéma de chiffrement

Symétrique vs Asymétrique

- Symétrique
 - 1 clé secrète, doit être connues des deux parties
 - Sert à chiffrer et déchiffrer les messages
- Asymétrique
 - 1 clé publique: sert à chiffrer des messages
 - 1 clé secrète: sert à déchiffrer des cryptogrammes