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

Chiffrement affine

Schéma symétrique

- On pose $\mathscr{M} = \mathscr{C} = \mathbb{Z}_n$ et $\mathscr{K} = \mathbb{Z}_n^\times \times \mathbb{Z}_n$

$$Enc_{(a,b)}(m) = ma + b \mod n$$

$$Dec_{(a,b)}(c) = (c - b)a^{-1} \mod n$$