Chiffrement affine

Schéma symétrique

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

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

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

Crypto-système RSA

Génération de clés

- On génère p, q de grands nombres premiers
- On calcule $n = pq$, et $\varphi(n) = (p-1)(q-1)$
- On choisi $e, d \in \mathbb{Z}^{\times}_{\varphi(n)}$ tels que $ed \equiv 1 \pmod{\varphi(n)}$
  - Algorithme d'Euclide étendu trouve d tel que $1 = ed + k\varphi(n)$
- (n, e) est la clé de chiffrement et (n, d) la clé de déchiffrement