RSA

Génération de clé

- Chiffrement asymétrique, on génère deux clés
  - Une **publique** (n, e) pour chiffrer / Une **privée** d pour déchiffrer
- On choisi deux grands nombres premiers $p, q \in \mathbb{Z}$ (par Miller-Rabin)
  - On calcule $n = pq$ et $\varphi(n) = (p-1)(q-1)$
  - On choisi un $e \in \mathbb{Z}^{\times}_{\varphi(n)}$ (i.e. $e \perp \varphi(n)$) et calcule son inverse $d \in \mathbb{Z}^{\times}_{\varphi(n)}$ (par Euclide)
- La sécurité dépend de la difficulté de retrouver $p, q, \varphi(n)$ étant donné seulement n, e

RSA

Chiffrement et déchiffrement

$$n = pq$$

$$ed \equiv 1 \pmod{\varphi(n)}$$

$$Enc(m) = m^e \mod n$$

$$Dec(c) = c^d \mod n$$

$$\begin{aligned} Dec(Enc(m)) &= m^{ed} \mod n \\ &= m^{k\varphi(n)+1} \mod n \\ &= m \mod n \end{aligned}$$