Math

Génération probabiliste de nombre premiers (Miller-Rabin)

- Tire n aléatoirement tant que
  - Aucun de k nombres aléatoires $a \in \mathbb{Z}_n^\times$ (i.e. tels que $a \perp n$) ne témoigne contre n
- On dit qu'un nombre a **témoigne contre** n si pour $n - 1 = 2^s d$ on a aucune des relations

$$a^d \equiv 1 \pmod{n}$$

$$a^{2^r d} \equiv -1 \pmod{n} \qquad 0 \leq r < s$$

- Plus k est grand, plus on est confiant (pas sur) que n est premier

RSA