# 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
  - On calcule $s, d$ tels que $n - 1 = 2^s \times d$ pour un $d$ impair et $x = a^d \mod n$
  - Aucun des $s$ répétitions de $x \leftarrow x^2 \mod n$ ne sont égal à $1$ ou $n - 1$
- Plus $k$ est grand, plus on est confiant (pas sur) que $n$ est premier

# RSA