Math

Exponentiation rapide

- Naïf 7 mul: $2^8 = 2 \times 2 \times 2 \times 2 \times 2 \times 2 \times 2 \times 2$

$$a^n = \begin{cases} 1 & \text{si n = 0} \\ a \times a^{n-1} & \text{sinon} \end{cases}$$

$$a^n = \begin{cases} 1 & \text{si } n = 0 \\ \left(a^{\frac{n}{2}}\right)^2 & \text{si } n \text{ est pair} \\ a \times a^{n-1} & \text{sinon} \end{cases}$$

- $2^8 = 2^{2^{2^2}}$ multiplie par lui-même 3 fois

- $\Longrightarrow$ exponentiation par ~1000 nécessite une dizaine de multiplications plutôt qu'un millier

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