Introduction

Objectif: RSA

$$Gen(1^\lambda) = (n, e, d)$$

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

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

$$n = pq$$

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

Introduction

Plan

- Math
  - Arithmétique, inverse modulaire, primalité, théorème d'Euler
  - Algorithme d'Euclide étendu, d'exponentiation rapide et de Miller-Rabin
- RSA
  - Génération de clé
  - Chiffrement et déchiffrement
- Mot de la fin sur les "privacy homomorphisms"