Introduction

Chiffrement asymétrique

- Qu'est-ce que le chiffrement **asymétrique**? (Par opposition au chiffrement symétrique)
- Qu'est-ce que le problème **d'établissement de clé**?
- Qu'est-ce qu'une **signature** cryptographique?
  - En quoi cela diffère d'un **CAM** (Code d'Authentification de Message)?
- Est-ce que le destinataire doit nécessairement **déchiffrer** notre message pour qu'il soit utile?

Introduction

Objectif: RSA

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

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

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

$$n = pq$$

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