Crypto-système RSA

Chiffrement et déchiffrement

- On note un message $m \in \mathbb{Z}_n$ et un cryptogramme $c \in \mathbb{Z}_n$

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

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

$$Dec(Enc(m)) = m^{ed} = m^{1+k\varphi(n)} = m \mod n$$

Crypto-système RSA
Sécurité

- La sécurité du système repose sur la difficulté présumée du problème RSA
  - C'est-à-dire trouver la e-ième racine d'un entier modulo n
- Une manière de faire est de factoriser n en p et q
  - Permet de retrouver $\varphi(n)$ et puis d
  - On pense que c'est la meilleure manière
- Considéré comme difficile, pour un n assez grand