Crypto-système RSA

Génération de clés

- On génère p, q de grands nombres premiers
- On calcule $n = pq$, et $\varphi(n) = (p-1)(q-1)$
- On choisi $e, d \in \mathbb{Z}^{\times}_{\varphi(n)}$ tels que $ed \equiv 1 \pmod{\varphi(n)}$
  - Algorithme d'Euclide étendu trouve d tel que $1 = ed + k\varphi(n)$
- (n, e) est la clé de chiffrement et (n, d) la clé de déchiffrement

Crypto-système RSA

Chiffrement et déchiffrement

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

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

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

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