RSA

(e, n) ← public

$n = p \cdot q$

p, q premiers

$e \cdot d \equiv 1 \mod (p-1)(q-1)$

$\varphi(p \cdot q) = \varphi(n)$

p, q secret

$m^e \mod n = c$

$c^d \mod n = m$

RSA p, q, e donnés tq. $\gcd(e, \underbrace{(p-1)(q-1)}_{\varphi(n)}) = 1$

clef publique : (e, n) $\boxed{n = p \cdot q}$

clef privée : (p, q, d)

$e \cdot d \equiv 1 \mod \varphi(n) \iff e \cdot d = 1 + k \cdot \varphi(n)$

$\iff ed - k \cdot \varphi(n) = 1$ ($\varphi(n) = (p-1)(q-1)$)

d se trouve à l'aide de Euclide étendu.

⚠ si $d < 0$: $d = d \bmod \varphi(n)$

Chiffrer : $m \in \mathbb{N}$ $m \leq n$

$$\boxed{c = m^e \bmod n}$$

Déchiffrer : c

$$\boxed{m = c^d \bmod n}$$

$$C^d = (m^e)^d = m^{ed} = m^{(1 + k\,\varphi(n))}$$

$$= m^1 \cdot m^{k \cdot \varphi(n)}$$

$$= m^1 \cdot \left(m^{\varphi(n)}\right)^k \equiv m^1 \cdot 1^k \bmod n$$

$$\underbrace{\quad}_{\equiv 1 \bmod \varphi(n)}$$

$$\equiv m \bmod n$$

$$\Rightarrow C^d \equiv m \bmod n$$

Thm d'Euler :

$m^{\varphi(n)} \equiv 1 \bmod n$

si $\gcd(m, n) = 1$

$$ed \equiv 1 \bmod \varphi(n)$$

$$\Leftrightarrow \quad ed = 1 + k \cdot \varphi(n)$$