§2. RSA.

(2.1) Chiffrement et déchiffrement

Un message clair x et son chiffré y appartiennent à $\mathbb{Z}_n$.

Algorithme RSA1.

Cryptage RSA. clé publique $k_{pub} = (n, e)$

$$y = e_{k_{pub}}(x) = x^e \bmod n.$$

où $x, y \in \mathbb{Z}_n$.

Décryptage RSA. clé privée $k_{pr} = d$

$$x = d_{k_{pr}}(y) = y^d \bmod n.$$

Génération de clés pour RSA. **Algorithme RSA2**

sortie : clé publique $k_{pub} = (n, e)$ et une clé privée $k_{pr} = (d)$

1. Choisir deux entiers premiers assez grand p et q
2. $n = p \cdot q$
3. $\phi(n) = (p-1)(q-1)$
4. Choisir l'exposant public $e \in \{1, 2, \dots, \phi(n)-1\}$ tq $\operatorname{pgcd}(e, \phi(n)) = 1$
5. calculer la clé privée d telle que $d \cdot e \equiv 1 \bmod \phi(n)$.

Ainsi B publie $k_{pub} = (n, e)$ et privatise $d = k_{pr}$.