

Le codage arithmétique à clés publiques

Retour sur le fonctionnement du système RSA

- Choix de deux nombres premiers p et q
- Calcul de $m = p \cdot q$ et $\phi(m) = (p - 1) \cdot (q - 1)$
- Choix de r tel que $PGCD(r, \phi(n)) = 1$
- calcul de $S \equiv r^{-1} \pmod{\phi(n)}$
- Publication de (m, r) , clé publique
- (S, m) : Clé privée

Exercice 1

On dit que m est composite s'il possède un facteur *inférieur* \sqrt{m} .

Testons un algorithme qui essaie successivement la division exacte de m par les entiers de 1 à \sqrt{m} .

Texte de l'algorithme

```
Pour i de 2 à SQRT(m) Faire
  Si (m Mod i = 0) Alors
    m est composite
  Fin
Finsi
FinPour
```

Complexité

La complexité de cet algorithme est en $\Theta(\sqrt{m}/2) = \Theta(\sqrt{m})$

Si m est composé de n bits, alors $n = \log_2(m + 1)$

$$\Rightarrow n \cdot \log(2) = \log(m + 1)$$

$$\Rightarrow \log(2^n) = \log(m + 1)$$

$$\Rightarrow 2^n = m + 1$$

$$\Rightarrow m = 2^n - 1$$

La complexité est alors en $\Theta(\sqrt{2^n}) = \Theta(2^{n/2})$. La complexité est donc exponentielle.

Théorème de Fermat

“Si m est premier, alors $a^{m-1} \equiv 1 \pmod{m}$, pour $1 < a < m$.”

Pour prouver qu'un nombre est composite, il suffit donc de trouver a , tel que $a^{m-1} \not\equiv 1 \pmod{m}$.

Texte de l'algorithme

```

Pour i de 2 à m-1 Faire
  Si  $i^{m-1} \neq 1 \pmod{m}$  Faire
    m est Composite
  Fin
Finsi
Finpour

```

Complexité

Si $m = (m_0, \dots, m_{n-1})$, $m_i \in \{0, 1\}$, alors $m = \sum_{i=0}^{n-1} m_i \cdot 2^i$.

$$a^m = a^{\sum_{i=0}^{n-1} m_i \cdot 2^i} = \prod_{i=0}^{n-1} a^{m_i \cdot 2^i} = \prod_{i=0}^{n-1} (a^{2^i})^{m_i}$$

La complexité est en $\Theta(n^3)$. Elle est donc polynômiale.

Exercice 3

Expliquez pourquoi RSA fonctionne !

Soit :

(m, r) clé publique

(s, n) clé privée

$s = (r^{-1}) \pmod{\varphi(n)}$, avec $s = p \cdot q$. La complexité pour décomposer s en p et q est exponentielle.

Montrons que $d(c(x)) = x$.

$$\begin{aligned} d(c(x)) &= (c^r[m])^s[m] \\ &= x^{r \cdot s}[m]^s[m] \end{aligned}$$

$$\begin{aligned} &= x^{rs}[m] \\ &= x^{k(p-1)(q-1)+1}[m] \\ &= x^{(p-1)(q-1)} \cdot x[m] \\ &= x[m] \end{aligned}$$