Cryptographie : méthode RSA [1]

Dans la cryptographie à clé publique, l'algorithme de codage est connu de tout le monde. L'algorithme de décodage, connu uniquement du destinataire, ne peut pas se déduire de l'algorithme de codage.

Méthode de cryptographie RSA
– On choisit p et q sont 2 nombres premiers différents (très grands).
– On pose $n = pq$ et $m = (p-1)(q-1)$.
– On choisit un entier positif e premier avec m.
– On détermine un entier positif d tel que $ed \equiv 1\ (m)$ (on trouve d grâce à une relation de Bézout entre e et m).

Le couple (n, e) est la **clé publique** : on la communique à tout le monde.
Les entiers p, q et d sont gardés secrets par le destinataire.

Codage
Le message est un entier M avec $0 \leq M \leq n-1$.
L'expéditeur calcule l'entier $C \equiv M^e\ (n)$ avec $0 \leq C \leq n-1$. Il envoie le message codé C.

Décodage
Le destinataire calcule $M' \equiv C^d\ (n)$ avec $0 \leq M' \leq n-1$.

Propriété : $M' = M$ (autrement dit, on retrouve bien le message de départ).

Preuve. On montre d'abord le lemme suivant :

Lemme. *Soit p et q deux nombres premiers différents et $k \in \mathbb{N}$ tel que $k \equiv 1\ ((p-1)(q-1))$. Alors, pour tout entier $x \in \mathbb{Z}$, $x^k \equiv x\ (pq)$.*

Preuve du lemme. On écrit $k = i(p-1)(q-1)+1$. L'entier i est positif car $p-1 \geq 1$, $q-1 \geq 1$ et $k \geq 1$ (car k est positif et $k \neq 0$ car 0 n'est pas congru à 1 modulo $(p-1)(q-1)$). Montrons d'abord que $x^k \equiv x\ (p)$.
• *Si p divise x, alors $x \equiv 0\ (p)$ donc $x^k \equiv 0\ (p) \equiv x\ (p)$.*
• *Si p ne divise pas x, alors $x^{p-1} \equiv 1\ (p)$ par le petit théorème de Fermat.*
$x^k = x^{i(p-1)(q-1)+1} = (x^{p-1})^{i(q-1)} \cdot x$ donc $x^k \equiv 1^{i(q-1)} \cdot x\ (p) \equiv x\ (p)$.
Pour tout $x \in \mathbb{Z}$, on a donc $x^k \equiv x\ (p)$.
Le même argument montre que

$$\forall x \in \mathbb{Z},\ x^k \equiv x\ (q).$$

Ceci montre que, pour tout entier x, p et q divisent $x^k - x$. Comme p et q sont premiers entre eux, le produit pq divise $x^k - x$, autrement dit $x^k \equiv x\ (pq)$. □

Maintenant montrons la propriété permettant le décodage de RSA.
Par définition, $M' \equiv C^d\ (pq) \equiv M^{ed}\ (pq)$, et $ed \equiv 1\ ((p-1)(q-1))$. Par le lemme (appliqué à $x = M$ et $k = ed$), $M^{ed} \equiv M\ (pq)$. Par conséquent, $M' \equiv M\ (pq)$. Or $0 \leq M < pq$ et $0 \leq M' < pq$, donc nécessairement $M' = M$. □

Pourquoi ne peut-on pas décrypter le cryptage RSA ?
Pour retrouver le message initial M à partir du message codé C, on a besoin de connaître d. L'entier d se calcule facilement à partir de e si on connaît p et q. Tout le monde connaît les entiers n et e, donc, en théorie, on peut retrouver p et q en décomposant n en facteurs premiers. En pratique, la décomposition en facteurs premiers est très difficile et prend énormément de temps quand les entiers sont grands. À l'inverse, multiplier les entiers p et q pour obtenir n est très facile. De plus, on dispose d'algorithmes assez rapides pour trouver de grand nombres premiers.

1. La méthode RSA date de 1978, son nom vient des initiales de ses trois auteurs : Rivest, Shamir, Adleman.