Démonstration de la Proposition fondamentale du cryptage RSA.

Hélène Arnaud, Caroline Pintoux

La compréhension de ce qui suit nécessite des connaissances en théorie des groupes. Commençons par un petit lemme qui se révèlera très utile :

Lemme 0.1. *Soient G un groupe fini d'ordre n et d, e deux entiers tels que $ed \equiv 1 \mod (n)$. Alors les applications*

$$\begin{array}{ccc} G & \to & G \\ x & \mapsto & x^e \end{array} \quad et \quad \begin{array}{ccc} G & \to & G \\ x & \mapsto & x^d \end{array}$$

sont inverses l'une de l'autre.

Démonstration : Il s'agit de vérifier que $x^{ed} = x \ \forall x \in G$. Comme $ed \equiv 1 \mod (n)$, il existe $k \in \mathbb{N}$ tel que $ed = 1 + kn$. Ainsi

$$x^{ed} = x^{1+kn} = x.x^{kn} = x.\left(x^n\right)^k = x,$$

car d'après le théorème de Lagrange, $x^n = 1$. On a donc le résultat voulu. □

Notations : Nous disposons de deux nombres premiers p et p. On note

$$m = pq.$$

Soit $G = \mathcal{U}(\mathbb{Z}/m\mathbb{Z})$ le groupe des inversibles de $\mathbb{Z}/m\mathbb{Z}$. On sait que le cardinal de G est $\sharp G = \varphi(m) = (p-1)(q-1)$, où φ est l'indicateur d'Euler. On pose donc

$$n = (p-1)(q-1).$$

On choisit enfin e et d tels que

$$ed \equiv 1 \mod (n).$$

Proposition 0.2. *Les applications*

$$\begin{array}{ccc} \mathbb{Z}/m\mathbb{Z} & \to & \mathbb{Z}/m\mathbb{Z} \\ x & \mapsto & x^e \end{array} \quad et \quad \begin{array}{ccc} \mathbb{Z}/m\mathbb{Z} & \to & \mathbb{Z}/m\mathbb{Z} \\ x & \mapsto & x^d \end{array}$$

sont réciproques l'une de l'autre.

Démonstration : Nous devons vérifier que

$$x^{ed} = x \ \forall x \in \mathbb{Z}/m\mathbb{Z} \qquad (\star).$$

Soit donc $x \in \mathbb{Z}/m\mathbb{Z}$. Nous allons procéder par étapes :

1. Si $x = \bar{p}$ dans $\mathbb{Z}/m\mathbb{Z}$. Il faut montrer que $(\bar{p})^{ed} = \bar{p}$, c'est à dire que $p^{ed} \equiv p \mod (pq)$.
   • Il est clair que $p^{ed} \equiv p \mod p$ (car $p^{ed} - p$ est divisibe par p).
   • Soit $\tilde{p}$ la classe de p dans $\mathbb{Z}/q\mathbb{Z}$. Comme p et q sont premiers entre eux, $\tilde{p} \in \mathcal{U}(\mathbb{Z}/q\mathbb{Z})$. Or $ed \equiv 1 \mod ((p-1)(q-1))$, donc a fortiori $ed \equiv 1 \mod (q-1)$. On peut donc appliquer le lemme à $G = \mathcal{U}(\mathbb{Z}/q\mathbb{Z})$, ce qui donne que $(\tilde{p})^{ed} = \tilde{p}$, c'est à dire que $p^{ed} \equiv p \mod q$.

   On a donc montré que $p^{ed} \equiv p \mod p$ et $p^{ed} \equiv p \mod q$. Or p et q étant premiers entre eux, cela implique (conséquence du théorème de Gauss) que $p^{ed} \equiv p \mod (pq)$, ce qu'il fallait démontrer.
2. Si $x = \bar{q}$ dans $\mathbb{Z}/m\mathbb{Z}$, alors $q^{ed} \equiv p \mod (pq)$ par symétrie des rôles de p et q, c'est à dire $x^{ed} = x$.
3. Si x et y vérifient $(\star)$, alors xy également. En effet, comme $x^{ed} = x$ et $y^{ed} = y$,
   $$(xy)^{ed} = x^{ed}y^{ed} = xy$$
   (tout est commutatif).
4. D'après le lemme, $(\star)$ est vérifiée pour tout $x \in \mathcal{U}(\mathbb{Z}/m\mathbb{Z}) \subset (\mathbb{Z}/m\mathbb{Z})$ (puisque ce groupe est d'ordre n).

Montrons maintenant que $(\star)$ est vérifiée pour tout $x \in \mathbb{Z}/m\mathbb{Z}$. Soient $x \in \mathbb{Z}/m\mathbb{Z}$ et $a \in \mathbb{Z}$ tel que $x = \bar{a}$ (dans $\mathbb{Z}/m\mathbb{Z}$). Alors a se décompose sous la forme

$$a = p^\alpha q^\beta b, \ \alpha, \beta \in \mathbb{N}, \ b \wedge (pq) = 1.$$

Alors

$$x = \bar{a} = (\bar{p})^\alpha (\bar{q})^\beta \bar{b}.$$

- On a vu que $\bar{p}$ vérifie $(\star)$ et donc, d'après ce qui a été dit concernant le produit d'éléments vérifiant $(\star)$, $(\bar{p})^\alpha$ vérifie $(\star)$.
- De même, $(\bar{q})^\beta$ vérifie $(\star)$.
- Enfin, comme $b \wedge (pq) = 1$, $\bar{b} \in \mathcal{U}(\mathbb{Z}/m\mathbb{Z})$, et $\bar{b}$ vérifie $(\star)$.

Conclusion : x s'écrit comme produit d'éléments vérifiant $(\star)$, ce qui prouve que x vérifie lui même cette relation, c'est à dire que $x^{ed} = x$ dans $\mathbb{Z}/m\mathbb{Z}$. □