Cryptologie et arithmétique

1 Méthode de cryptage « à clé publique »

1.1 Principe

Le problème posé. Supposons qu'un individu A souhaite transmettre à un autre individu B un message **confidentiel** M en utilisant un réseau de communication **public**, par exemple les ondes hertziennes, sur lequel n'importe quel individu peut se mettre à l'écoute et intercepter le message.

Autrement dit :

- le message M doit être inintelligible pour tout individu autre que A et B.
- B doit pouvoir comprendre le message M.
- B doit pouvoir s'assurer que le message M provient bien de A (et non d'un plaisantin quelconque).

L'idée. L'idée est de se doter d'une **méthode de cryptage** public. Cependant les résultats du cryptage d'un même message par différents individus doivent être différents, car chacun d'entre eux emploie une « clé » qui lui est propre.

La **méthode de cryptage** est fondée sur l'existence de fonctions f_K, **dépendant d'un paramètre K (la « clé »)**, **inversibles**, mais pour lesquelles la détermination de l'inverse est **matériellement impossible**, en l'état actuel des connaissances humaines.

→ Soit f_K la fonction de cryptage qui utilise la clé propre à l'individu K.

→ La fonction de cryptage f_K de l'individu K est publique, ainsi n'importe qui est en mesure d'appliquer la fonction f_K à un message M quelconque : on dit que f_K est la clef public de K

→ Par contre, seul l'individu K connaît la fonction inverse f_K^{-1} qui permet de retrouver le message initial.

Revenons à notre à notre problème pour le résoudre :

Solution du problème :

→ Au message M, A applique en fait f_A^{-1}(il est le seul à pouvoir le faire).

→ Puis, à ce message $f_A^{-1}(M)$, il applique la fonction de cryptage de B, soit f_B (il peut le faire, la clé de B est publique), pour obtenir $f_B \circ f_A^{-1}(M)$, incompréhensible car les clés sont évidemment uniques,et donc $f_B \circ f_A^{-1}$ n'est pas l'identité.

→ C'est ce message « doublement » crypté qui est envoyé. B le reçoit et lui applique aussitôt f_B^{-1}, ce qu'il est le seul à pouvoir faire, pour obtenir $f_A^{-1}(M)$, auquel il applique f_A : si le résultat est compréhensible, B est sûr que le message lui était bien destiné, et qu'il a bien été envoyé par A.

1.2 Utilisation de l'indicatrice d'Euler

Définition. (Fonction indicatrice d'Euler) *Soit n un entier strictement positif ; on note $\varphi(n)$ le nombre des entiers inférieurs à n qui sont premiers avec n. L'application φ: $\mathbb{N}^* \longrightarrow \mathbb{N}^*$ ainsi définie est appelée fonction indicatrice d'Euler.*

Proposition 1.

1. *Pour tout nombre premier p, on $\varphi(p) = p - 1$,*
2. *Pour tout nombre premier p et tout $\alpha \in \mathbb{N}^*$,$\varphi(p^\alpha) = p^\alpha - p^{\alpha-1}$*

3. *Pour tout couple de nombres entiers naturels n et m premiers entre eux on a* $\varphi(nm) = \varphi(n)\varphi(m)$.
4. *Pour tout entier a premier avec n, et pour tout entier n dépourvu de facteur carré,* $a^{\varphi(n)} \equiv 1 \bmod n$.

Résultat de base . Diverses fonctions « à inverse difficile à déterminer » ont été proposées. Les plus satisfaisantes sont celles qui utilisent le résultat suivant :

Proposition 2. *s'il est très facile d'obtenir un très grand nombre entier composé par produit de deux nombres premiers eux-mêmes grands, la décomposition en facteurs premiers d'un nombre composé est très difficile.*

Methode de cryptage. La méthode de cryptage est la suivante :

1. Soit donc $n=pq$ un entier, produit de deux nombres entiers premiers, par exemple tels que $p \equiv q \equiv 2 \bmod 3$.
2. Soit M le message, préalablement chiffré (sans précautions particulières, par exemple en remplaçant les lettres par leurs codes ASCII).
3. Si $M > n$, on décompose M en plusieurs sous-messages, ses « chiffres » en base n, par exemple.
4. Si n est la clé choisie par A, et pour $M < n$, $f_A(M) = C$, avec $C\ C = M^3 \bmod n$. Comme n est connu de tous, n'importe qui peut calculer C très rapidement. Par contre, les facteurs premiers p et q de n sont soigneusement tenus secrets par A.
5. Un résultat (élémentaire) d'arithmétique indique que, comme n n'a pas de facteur carré, si M est premier avec n, alors $M^{\varphi(n)} \equiv 1 \bmod n$ (dans cette expression, $\varphi(n)$ est la fonction indicatrice d'Euler
6. Un autre résultat (élémentaire) d'arithmétique dit que, comme $n=pq$, avec p et q premiers, $\varphi(n) = \varphi(pq) = \varphi(p)\varphi(q) = (p-1)(q-1)$.
7. On a donc, en combinant ces deux résultats, $M^{(p-1)(q-1)} \equiv 1 \bmod n$, donc $M^{2(p-1)(q-1)} \equiv 1 \bmod n$, et finalement $M^{2(p-1)(q-1)+1} \equiv M \bmod n$.
8. Comme on a choisi $p \equiv q \equiv 2 \bmod 3$, $(p-1)(q-1) \equiv 1 \bmod 3$, $2(p-1)(q-1) \equiv 2 \bmod 3$ et $2(p-1)(q-1)+1 \equiv 0 \bmod 3$. Il s'agit donc d'un multiple de 3 on peut poser $2(p-1)(q-1)+1 = 3k$, et on a $M^{3k} \equiv M \bmod n$.
9. Or $M^{3k} = (M^3)^k$, donc, si le message crypté est $C \equiv M^3 \bmod n$, $C^k \equiv M \bmod n$ et la connaissance de :
$$k = \frac{2(p-1)(q-1)+1}{3}$$
permet de retrouver le message original.

Exemple. Avec $p = 5$, $q = 11$, $n = pq = 55$.
Le message à envoyer est chiffré $M = 7$.
Alors $7^2 \equiv 49 \bmod 55$, $7^3 \equiv 13 \bmod 55$.
Le message crypté est $C = 13$.
Ici $k = \frac{2 \times 4 \times 10 + 1}{3} = 27$, donc $M = 13^{27} \bmod 55$.
En effectuant le calcul, on obtient bien $13^{27} \equiv 7 \bmod 55$.

2 Choix d'un nombre n

Dans l'exemple ci-dessus, le cryptage est immédiatement percé, puisque la décomposition de 55 en ses facteurs premiers 5 et 11 est immédiate. On peut en dire autant de tout entier représentable sur 32 bits. Il faut aller chercher bien plus loin pour assurer un minimum de sécurité. Pour fixer les idées, les clés utilisées sont à l'heure actuelle le produit de deux nombres représentable sur 1024 voir 2048 bits.

Cours assuré par : Dr D. N. Diatta(dndiatta@univ-zig.sn)

2.1 Nombres premiers

Pour produire un nombre n utilisable, il faut tout d'abord trouver deux nombres p et q premiers, suffisamment grands. On choisit deux nombres se terminant par 1, 3, 7 ou 9 dans leur représentation décimale et de longueurs comparables (mais pas trop proches : il existe un algorithme de décomposition qui est capable de décomposer rapidement un nombre qui est le produit de deux nombres de longueurs très proches). Il faut vérifier qu'ils sont premiers et, pour cela, disposer d'un critère de primalité. Il existe une technique de génération de nombres premiers consistant à prendre au hasard un entier et s'il n'est n'est pas premier, il suffit de lui ajouter 2, puis encore 2 etc.,jusqu'à obtenir un nombre premier, ce qui interviendra très rapidement.

2.2 Décomposition en facteurs premiers

Théoriquement, bien sûr, la décomposition d'un nombre composé (non premier) est un problème-résolu : il suffit de tenter de le diviser par tous les nombres premiers jusqu'à sa racine carrée.

Pratiquement, cet algorithme est totalement impraticable dès que la longueur du nombre dépasse une vingtaine de chiffres décimaux (durée d'exécution trop élevée).

La durée d'exécution d'un algorithme de décomposition en facteurs premiers dépend, bien sûr, de la longueur du nombre à décomposer. Mais il n'y a pas de proportionnalité stricte : cela dépend aussi de l'algorithme utilisé. Pour prendre un exemple limite, 1000 !, qui est un nombre dont la représentation décimale occupe plus de 4000 chiffres, est décomposé en quelques fractions de seconde par le plus rudimentaire des algorithmes.

Le seul moyen, donc, pour savoir si un nombre n obtenu comme ci-dessus est une « bonne » clé, est de tenter de le décomposer par tous les algorithmes connus. S'il résiste vaillamment, on peut l'adopter, sinon, il faut en changer.

Conclusion. La conclusion de cette présentation est qu'il est donc nécessaire de disposer d'un test de primalité et d'algorithmes de décomposition en facteurs premiers, questions que nous allons aborder dans le chapitre suivant.