Cryptographie

Système de chiffrement RSA

Yoann Morel

http://xymaths.free.fr/index.php?subdir=Signal

"La mathématique est la reine des Sciences, mais la théorie des nombres est la reine des sciences mathématiques."

Carl-Friedrich GAUSS
(1777 / 1855)

"J'ai trouvé une merveilleuse démonstration de cette proposition, mais la marge est trop étroite pour la contenir."

Pierre de Fermat
(1601-1665)

Propriété (Division Euclidienne)

Soient a et b deux entiers naturels. Il existe un unique couple (q, r) d'entiers tel que :

$$a = bq + r \quad \textit{avec, } 0 \leq r \leq b - 1$$

Ex. $a = 20$, $b = 3$, alors $20 = 3 \times 6 + 2$
$a = 33$, $b = 6$, alors $32 = 6 \times 5 + 3$

Définition

On dit que deux entiers x et y sont congrus modulo p, si il existe un entier q avec $x = pq + y$, i.e. si le reste de la divison euclidienne de x par p est y.
On le note $x \equiv y[p]$.

Ex. $20 \equiv 2\ [6]$
$33 \equiv 3\ [5]$

Théorème ((petit) Théorème de Fermat)

Soit $p \geq 2$ un nombre premier, alors, pour tout entier relatif a,

$$a^p \equiv a \ [p]$$

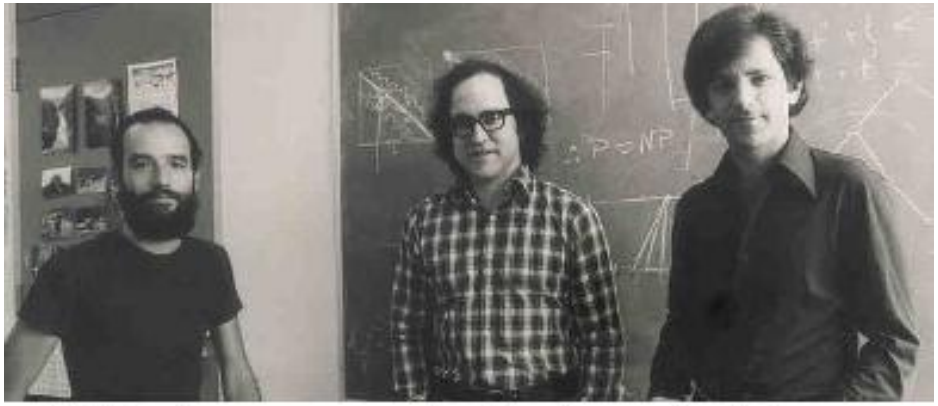
et, pour tout entier relatif a, tel que p ne divise pas a,

$$a^{p-1} \equiv 1 \ [p]$$

Ex. $p = 3$, $a = 5$, alors $a^p = 5^3 = 125 \equiv 5 \ [3]$
et $a^{p-1} = a^2 \equiv 1 \ [3]$

$p = 5$, $a = 3$, alors $a^p = 3^5 = 243 \equiv 3 \ [5]$
et $a^{p-1} = 3^4 = 81 \equiv 1 \ [5]$

La méthode de cryptographie RSA a été inventée en 1977 par Ron **R**ivest, Adi **S**hamir et Len **A**dleman, à la suite de la découverte de la cryptographie à clé publique par Diffie et Hellman.



Le RSA est encore le système cryptographique à clé publique le plus utilisé de nos jours.

Il est intéressant de remarquer que son invention est fortuite : au départ, Rivest, Shamir et Adleman voulaient prouver que tout système à clé publique possède une faille.

On considère un message M à transmettre.

Ce message M est un nombre entier, par exemple un texte codé à l'aide du code ASCII (**A**merican **S**tandard **C**ode for **I**nformation **I**nterchange).

La personne qui veut recevoir un message “privé”, Bob, génére quatre nombres de la façon suivante :

- deux nombres p et q premiers et distincts
- deux nombres c et d tels que $cd \equiv 1 \ [(p-1)(q-1)]$

On caclule alors le nombre $n = p\,q$.

Le couple (n, c) constitue la **clé publique**. Bob la diffuse publiquement à toute personne qui souhaite communiquer avec lui.

Alice souhaite communiquer avec Bob.
Elle a connaissance (comme tout le monde) de la clé publique (n, c).
Une fois son message numérisé, sous la forme d'un entier M, elle calcule et envoie :

$$E = M^c \ [n]$$

E est le message **chiffré** ou **crypté**.

Bob reçoit E. Il peut alors le déchiffré en calculant grâce à sa clé privée :

$$M' = E^d \ [n]$$

Bob a alors le message $M' = E^d = M^{cd} \equiv M \ [n]$.

Démonstration :

Il faut montrer que pour un entier M, $M^{cd} \equiv M\ [n]$.
Avec $n = pq$ et p et q premiers (donc premiers entre eux), il suffit alors de montrer que $M^{cd} \equiv M\ [p]$ et $M^{cd} \equiv M\ [q]$.

On a $cd \equiv 1\ [(p-1)(q-1)]$; soit k tel que $cd = 1 + k(p-1)(q-1)$.

- Si M et p sont premiers entre eux, alors $M^{p-1} \equiv 1\ [p]$, d'après le théorème de Fermat.
  Donc,
  $$M^{cd} = M^{1+k(p-1)(q-1)} = M.\left(M^{p-1}\right)^{k(q-1)} \equiv M\ [p]$$
- Si M et p ne sont pas premiers entre eux, alors p divise M (car p est un nombre premier), et donc, $M^{cd} \equiv M \equiv 0\ [p]$

Le calcul modulo q est identique.

La sécurité de ce système repose sur le fait que connaissant la clé publique (n, c), il est très difficile de déterminer le nombre d, nécéssaire au décryptage.

Il faudrait par exemple factoriser n pour trouver p et q, ce qui encore impossible à réaliser de nos jours lorsque p et q sont grands, de l'ordre de 100 chiffres (on ne sait pas factoriser aujourd'hui des entiers de plus de 120 chiffres).

En résumé, tout le monde connaît la clé publique, donc tout le monde peut chiffrer un message, mais seuls ceux connaissant la clé privée peuvent déchiffrer.

Temps de calcul pour factoriser un nombre de N chiffres :