Cryptographie

Algorithme RSA

Un message est assimilé à une suite de nombres entiers : par exemple chaque bloc de 8 caractères (octets) est assimilé à un entier représenté par 64 chiffres binaires.

- Le message est brouillé, pour en assurer la confidentialité, en remplaçant chaque nombre a par a^e (**mod** n) ; voir exponentiation rapide.
- Le message original (dit message *clair*) est reconstitué en remplaçant chaque nombre a du message brouillé par a^d (**mod** n).

Bien entendu la fonction de décodage doit être l'inverse de celle de brouillage, soit :

pour tout a : $a^{de} = a$ (**mod** n).

Si n est le produit pq de deux nombres premiers distincts, le petit théorème de Fermat implique que cette condition est équivalente à :

$d\ e = 1$ (**mod** $(p\text{-}1)\ (q\text{-}1)$).

Soit $m = (p\text{-}1)\ (q\text{-}1)$; connaissant e, on peut calculer d si et seulement si e est premier avec m ; si c'est le cas, en calculant le pgcd de e et m par l'algorithme d'Euclide étendu on obtient des coefficients u et v tels que $1 = eu + mv$ (formule de Bézout), et il suffit donc de prendre $d = u$. Comme l'algorithme d'Euclide est linéaire, le calcul du coefficient d de décodage est très rapide, à condition de connaître m, c'est à dire p et q.

Cette méthode constitue l'algorithme cryptographique RSA, du nom de ses inventeurs *Rivest, Shamir* et *Adelman*. Comme il est impossible de factoriser rapidement un grand nombre, on peut rendre publics e et n, et donc la méthode de codage, sans qu'il soit possible de calculer d, et donc de décoder, sauf pour le destinataire du message qui est seul à connaître les facteurs premiers secrets p et q tels que $n = pq$.