Le Cryptosystème RSA

Ronald Rivest, Adi Shamir et Leonard Adleman ont publié leur chiffrement en 1978 dans A Method for Obtaining Digital Signatures and Public-key Cryptosystems. Ils utilisent les congruences sur les entiers et le petit théorème de Fermat, pour obtenir des fonctions à sens unique, avec brèche secrète (ou porte dérobée).

Tous les calculs se font modulo un nombre entier n qui est le produit de deux nombres premiers. Le petit théorème de Fermat joue un rôle important dans la conception du chiffrement.

Les messages clairs et chiffrés sont des entiers inférieurs à l'entier n (tout message peut être codé par un entier). Les opérations de chiffrement et de déchiffrement consistent à élever le message à une certaine puissance modulo n (c'est l'opération d'exponentiation modulaire).

Création des clés

L'étape de création des clés est à la charge d'Alice. Elle n'intervient pas à chaque chiffrement car les clés peuvent être réutilisées, la difficulté première, que ne règle pas le chiffrement, est que Bob soit bien certain que la clé publique qu'il détient est celle d'Alice. Le renouvellement des clés n'intervient que si la clé privée est compromise, ou par précaution au bout d'un certain temps (qui peut se compter en années).

1-Choisir p et q, deux nombres premiers distincts ;

2-calculer leur produit n = pq, appelé module de chiffrement ;

3-calculer $\varphi(n) = (p - 1)(q -1)$ (c'est la valeur de l'indicatrice d'Euler en n) ;

4-choisir un entier naturel e premier avec $\varphi(n)$ et strictement inférieur à $\varphi(n)$, appelé exposant de chiffrement ;

5-calculer l'entier naturel d, inverse de e modulo $\varphi(n)$, et strictement inférieur à $\varphi(n)$, appelé exposant de déchiffrement ; d peut se calculer efficacement par l'algorithme d'Euclide étendu.

Comme e est premier avec $\varphi(n)$, d'après le théorème de Bachet-Bézout il existe deux entiers d et k tels que $ed + k\varphi(n) = 1$, c'est-à-dire que $ed \equiv 1 \pmod{\varphi(n)}$: e est bien inversible modulo $\varphi(n)$.

Le couple (n,e) est la clé publique du chiffrement, alors que le couple (n,d) est sa clé privée.

Chiffrement du message

Si M est un entier naturel strictement inférieur à n représentant un message, alors le message chiffré sera représenté par $C = M^e \bmod n$

Déchiffrement du message

Pour déchiffrer C, on utilise d, l'inverse de e modulo (p-1)(q-1), et on retrouve le message clair M par $M = C^d \bmod n$.

Exemple

Un exemple avec de petits nombres premiers (en pratique il faut de très grands nombres premiers) :

on choisit deux nombres premiers p = 3, q = 11 ;

leur produit n = 3 x 11 = 33 est le module de chiffrement ;

$\varphi(n) = (3-1) \times (11-1) = 2 \times 10 = 20$;

on choisit e= 3 (premier avec 20) comme exposant de chiffrement ;

l'inverse de 3 modulo 20 est d =7 ($ed = 3 \times 7 = 1 \bmod 20$), l'exposant de déchiffrement.

La clé publique est (n,e) = (33,3), et la clé privée est (n,d) = (33,7).

Chiffrement de M = 4 par avec la clé publique: $4^3 = 31 \bmod 33 = 31$, le chiffré est C = 31;

Déchiffrement de C = 31 par avec la clé privée : $31^7 = 4 \bmod 33$, on retrouve le message intial M = 4.