PKCS#1

RSA Cryptography Standard

RSA (Rivest Shamir Adleman) est un algorithme asymétrique.

Génération des clés

Pour calculer une paire de clé privée/publique RSA, l'algorithme s'appuie sur 2 nombres premiers, p et q. Une fois ces 2 nombres déterminés, on obtient 2 nombres :

n = p x q

z = (p - 1) x (q - 1)

On calcul ensuite l'indicatrice d'Euler e de z (inférieur à z), qui doit nécessairement être premier avec z :

d = e-1 mod((p - 1)(q - 1))

le couple (**n,e**) est la clé publique, le couple (**n,d**) est la clé privée. Une fois **e**, **d** et **n** caclulés, il faut détruire **p**, **q**, et **z** pour des raisons évidentes de sécurité. La clé privée est généralement chiffrée avec un algorithme symmetrique pour la conserver de façon sûre.

Chiffrement et déchiffrement

Pour chiffrer un nombre, il faut le mettre à la puissance de e. Le reste modulo n représente le nombre chiffré :

$c = t^e \bmod n$

pour déchiffrer, on utilise la même opération, mais à la puissance d :

$t = c^d \bmod n$

exemple simple utilisant de petits nombres :

pour chiffrer le texte suivant : "Hello World", on choisis p = 37 et q = 43.

on déduit :

n = 37 x 43 = 1591

z = 36 x 42 = 1512

on choisit e = 19, premier avec 1512. L'inverse de 19 modulo 1512 est d = 955.

pour chiffrer chaque caractère :

Hello World = 72 101 108 108 111 32 87 111 114 108 100

```
H___e___l___l___o___ ___W___o___r___l___d
72__101_108_108_111_32__87__111_114_108_100
```

on caclule chaque caractère avec :

7219 [1591] = 335 ; 10119 [1591] = 1174 ; etc…

```
72____101____108____108____111___32____87____111___114___108____100
335___1174___1329___1329___703___930___431___703___632___1329___396
```

On déchiffre avec :

335955 [1591] = 72 ; 1174955 [1591] = 101 ; etc…

Notes

Plusieurs techniques permettent de déchiffrer ou déduire la clé privée :

- si **p** et **q** sont trop petits, un brute force ne prend que très peu de temps à déterminer la clé privée. il faut donc choisir des valeures très grandes (minimum 1024 bits)
- Le chiffrement par caractère comme dans l'exemple ci-dessus, peut être cassé en déterminant la fréquence des octets (analyse fréquentielle). Il est préférable de chiffrer un bloc d'octets.
- **n** ne doit pas être inférieur au bloc d'octets à chiffrer, sinon plusieurs valeurs initiales peuvent donner le même nombre chiffré, donnant des erreurs au déchiffrement.
- on peut déterminer la taille d'une clé privée en déterminant le temps que prend le déchiffrement d'un message. Toute la sécurité RSA repose sur le temp nécessaire pour calculer **p** et **q** à partir de **n**.