La méthode RSA

I. Généralités

1°) Origine et historique

Voir article Wikipedia

2°) Principe

Alice :
- donne à tout le monde un moyen de lui coder des messages → clef publique ;
- connaît le moyen de décrypter les messages (et seulement elle) → clef privée.

II. Cryptage

1°) La clef publique

Alice choisit deux nombres premiers distincts p et q. Elle va calculer leur produit $n = pq$.
Elle choisit aussi un entier naturel e qui est premier avec $(p-1)(q-1)$.
La clef publique est le couple (n, e).
Elle la communique à tout le monde, de sorte que tout le monde puisse lui envoyer des messages.
Attention, elle donne la valeur de n mais elle ne donne pas les valeurs de p et q ! Nous verrons dans la suite que cela a une très grande importance pour la sécurité de la méthode.

2°) Exemple

Alice choisit les nombres premiers $p = 13$ et $q = 17$.
Elle calcule alors $n = pq = 221$.
Elle calcule aussi $(p-1)(q-1) = 192$ et elle décide de choisir $e = 5$.
La clef publique sera $(221; 5)$.

3°) Méthode de cryptage

Pour coder un nombre b, on calcule le reste a de la division euclidienne de b^e par n (on a donc $a \equiv b^e \pmod{n}$).

b correspond à un nombre que Bob veut envoyer à Alice ; a correspond au nombre codé que reçoit Alice.

III. Décryptage

1°) Lemme (admis sans démonstration)

p et q sont deux nombres premiers distincts.
On pose $n = pq$.
e est un entier tel que $1 < e < (p-1)(q-1)$ premier avec $(p-1)(q-1)$.
Il existe un unique entier naturel d tel que $1 < d < (p-1)(q-1)$ et $ed \equiv 1 \pmod{(p-1)(q-1)}$.

Avec ces notations, $a \equiv b^e \pmod{n} \Leftrightarrow b \equiv a^d \pmod{n}$.

2°) La clef privée

La clef privée est le couple (n, d). Elle est seulement connue d'Alice : elle lui permet de décrypter les messages qu'on lui envoie.

3°) Méthode de décryptage

Avec les notations précédentes, b est le reste de la division euclidienne de a^d par n.

4°) Exemple

On reprend la clef publique constituée de $n = 221$ (qui correspond à $p = 13$ et $q = 17$) et de $e = 5$.

On peut alors démontrer que $d = 77$. Nous expliquerons dans la suite comment trouver d.

La clef privée est $(221, 77)$.

IV. Commentaires

1°) Bilan (pour mieux comprendre)

$$b \xrightarrow{\text{codage } (n,e)} a : \text{reste de la DE de } b^e \text{ par } n$$

$$b : \text{reste de la DE de } a^d \text{ par } n \xleftarrow[\text{décodage } (n,d)]{} a$$

2°) Le choix des nombres premiers

3°) Il s'agit d'un chiffrement asymétrique.

4°) On notera aussi qu'il s'agit d'un chiffrement par exponentiation.

V. Algorithme et programme utiles

On veut rédiger un algorithme opérationnel qui permette de calculer la division euclidienne de la puissance d'un entier naturel sur calculatrice.

Algorithme du calcul du reste de la division euclidienne de a^p par n où a, p, n sont des entiers naturels avec $p \geqslant 1$

Algorithme 1 :

L'algorithme affiche en sortie le reste de la division euclidienne de a^n par p.

Entrées :
Saisir a
Saisir p $(p \geqslant 1)$
Saisir n

Initialisation :
b prend la valeur 1

Traitement :
Pour i allant de 1 à p **Faire**
    b prend la valeur du reste de la division euclidienne de ab par n
FinPour

Sortie :
Afficher b

Algorithme 2 :

On utilise l'exponentiation rapide qui s'appuie sur la décomposition en base 2 (système binaire).
L'algorithme affiche en sortie le reste de la division euclidienne de a^n par p.

TI (modèle moins élaboré)

```
: Prompt A, P, N
: A → X
: 1 → Y
: P → Q
: While Q≠1
: If PartDéc(Q/2)≠0
: Then
: X*Y–partEnt(X*Y/N)*N → Y
: End
: X²–partEnt(X²/N)*N → X
: partEnt(Q/2) → Q
: End
: X*Y–partEnt(X*Y/N)*N → R
: Disp R
```

TI (modèle plus élaboré)

```
: Prompt A, P, N
: A→ X
: 1→ Y
: P → Q
: While Q≠1
: If reste(Q,2)≠0
: Then
: remainder(X*Y,N) → Y
: End
: reste( X²,N) → X
: partEnt(Q/2) → Q
: End
: reste(X*Y,N) → R
: Disp R
```

Site à consulter :

http://therese.eveilleau.pagesperso-orange.fr/pages/truc_mat/textes/RSA.htm