Chiffrement RSA
(Rivest Shamir Adleman)

Jusqu'à la fin du XX^e siècle, on utilise des méthodes de chiffrement symétriques (codage affine, Vigenère, Hill, ...) : l'émetteur et le récepteur connaissent la clé qui permet de chiffrer ou d'en déduire le déchiffrement

<u>Problème</u>: il faut transmettre la clé
ex: pour les banques, il fallait envoyer des coursiers à travers le monde pour distribuer les clés aux clients, aux filiales, ...

Chiffrement asymétrique

Il existe deux clés :

- une clé publique : connue par tous qui permet de chiffrer les messages

- une clé secrète : uniquement connue par le destinataire (c'est donc lui qui a créé la clé)

<u>Idée</u> : il faut trouver un chiffrement suffisamment compliqué pour que l'on ne puisse pas le réaliser en sens inverse

Création d'une clé :
* choisir p et q deux nombres premiers distincts
* $n = p \times q$: "module de chiffrement"
* c tel que $PGCD(c; (p-1)(q-1)) = 1$: "exposant de chiffrement"

Le couple $(n; c)$ est la <u>clé publique</u>

* Chiffrement :

le nombre a est chiffré par le nombre b tel que $b \equiv a^c [n]$

* Déchiffrement

le nombre b est déchiffré par le nombre a tel que $a \equiv b^d [n]$ où d est tel que $c \times d \equiv 1 [(p-1)(q-1)]$ (d est l'inverse de c modulo $(p-1)(q-1)$)

<u>Remarque</u>: on connaît n ($= p \times q$) mais on ne connaît pas, ni p, ni q qui doivent être des nombres premiers très grands afin que l'on ne puisse pas les trouver.
La connaissance de p et q permet de connaître $(p-1)\times(q-1)$ et donc de trouver d.

Le couple $(n; d)$ est la <u>clé privée</u>

<u>Remarques</u>: - ici on chiffre des nombres qui peuvent être relativement grand (il suffit que ce nombre soit inférieur à n) on peut donc chiffrer des mots, voire des phrases et pas nécessairement faire du lettre par lettre
- pour RSA 768 bits n est un nombre de 232 chiffres.

Justification (on code a avec $0 \leq a < n$)

* Inverse de c modulo $(p-1)(q-1)$

c et $(p-1)(q-1)$ sont premiers entre eux donc d'après le théorème de Bézout, il existe $(x_0 ; y_0)$ tel que :

$$c x_0 - [(p-1)(q-1)] y_0 = 1$$

Toute solution $(x ; y)$ vérifie $cx - [(p-1)(q-1)]y = c x_0 - [(p-1)(q-1)] y_0$

$$\Leftrightarrow \quad c(x - x_0) = [(p-1)(q-1)](y - y_0)$$

d'après le théorème de Gauss c divise $(y - y_0)$ et $[(p-1)(q-1)]$ divise $(x - x_0)$

donc $y = y_0 + kc$ et $x = x_0 + k'[(p-1)(q-1)]$ $(k, k') \in \mathbb{Z}^2$

Or $c(x_0 + k'[(p-1)(q-1)]) - [(p-1)(q-1)](y_0 + kc) = 1$

donc $ck'[(p-1)(q-1)] - kc[(p-1)(q-1)] = 0$ donc $k = k'$

Donc tout couple solution est de la forme $(x_0 + k[(p-1)(q-1)] ; y_0 + kc)$ $k \in \mathbb{Z}$

Il existe un unique k_1 tel que $0 \leq x_0 + k_1[(p-1)(q-1)] < n$

On note $d = x_0 + k_1[(p-1)(q-1)]$

On a bien $c \times d = 1 + (y_0 + k_1 c)[(p-1)(q-1)]$ donc $cd \equiv 1 \, [(p-1)(q-1)]$

* 1^{er} cas : a n'est pas divisible ni par p ni par q.

D'après le petit théorème de Fermat

p est premier donc $a^{p-1} \equiv 1 \, [p]$ et q est premier donc $a^{q-1} \equiv 1 \, [q]$

donc $a^{(p-1)(q-1)} \equiv 1 \, [p]$ et $a^{(q-1)(p-1)} \equiv 1 \, [q]$

soit $a^{(p-1)(q-1)} = 1 + kp = 1 + k'q$ donc $kp = k'q$ donc p divise k' donc $k' = k''p$

ainsi $a^{(p-1)(q-1)} = 1 + k''pq$ et donc $a^{(p-1)(q-1)} \equiv 1 \, [pq]$ soit $a^{(p-1)(q-1)} \equiv 1 \, [n]$

Par conséquent, lorsque l'on connaît d :

$b \equiv a^c [n] \Rightarrow b^d \equiv a^{cd} [n] \Rightarrow b^d \equiv a^{1 + k(p-1)(q-1)} [n]$ (car $cd \equiv 1 \, [(p-1)(q-1)]$)

$\Rightarrow b^d \equiv a \times (a^{(p-1)(q-1)})^k [n]$

$\Rightarrow b^d \equiv a \times 1^k [n]$ (car $a^{(p-1)(q-1)} \equiv 1 \, [n]$)

$\Rightarrow b^d \equiv a \, [n]$

* 2^{eme} cas : a est un multiple de p ou de q

(a ne peut être multiple de p et de q car $0 \leq a < n$)

par ex, a multiple de p donc $a = p^\alpha m$ avec m non divisible par p

De plus m n'est pas divisible par q sinon a serait divisible par n

On a donc :

$b \equiv a^c [n] \Rightarrow b^d \equiv a^{cd} [n] \Rightarrow b^d \equiv p^{\alpha cd} m^{cd} [n]$

avec $m^{cd} \equiv m \, [n]$ (d'après l'étude de cas précédente)

de plus $p^{\alpha cd} \equiv p^\alpha [p]$ et $p^{cd} \equiv p^{1 + k(p-1)(q-1)} [q] \equiv p \times (p^{q-1})^{k(p-1)} [q]$

or $p^{q-1} \equiv 1 \, [q]$ donc $p^{cd} \equiv p \times 1^{k(p-1)} [q] \equiv p \, [q]$

ainsi $p^{\alpha cd} \equiv p^\alpha [q]$, donc d'après le théorème de Gauss

$$p^{\alpha cd} \equiv p^\alpha [n]$$

Par conséquent,

$$b^d \equiv a^{cd} [n] \equiv p^{\alpha cd} m^{cd} [n] \equiv p^\alpha m \, [n] \equiv a \, [n]$$

* On obtient donc bien, dans tous les cas $b^d \equiv a \, [n]$

(on retrouve ainsi le nombre a initial)

Remarques : - il est donc nécessaire de connaître p et q pour en déduire $(p-1)(q-1)$. On peut alors trouver d tel que $cd \equiv 1 \, [(p-1)(q-1)]$. Il ne reste plus qu'à effectuer $b^d \, [n]$ pour trouver a.

- Dans le cas où $n = p \times q$ avec p et q deux nombres premiers $(p-1) \times (q-1)$ est l'indicatrice d'Euler de n (elle correspond au nombre d'entiers naturels inférieurs ou égaux à n et premiers avec n)