Dev Systèmes de cryptage

RSA

Soient p et q deux nombres premiers ($p \neq 2$, $q \neq 2$). On pose $n = pq$

soit e un entier tel que $\begin{cases} 1 < e < (p-1)(q-1) \text{ et} \\ e \wedge (p-1)(q-1) = 1 \end{cases}$

1°/ Montrer que $\exists ! d$ tel que $1 \leq d < (p-1)(q-1)$

et $ed \equiv 1 \ [(p-1)(q-1)]$

2°/ Prouver que $\forall m \in \mathbb{N} \quad m^{ed} = m \ (n)$

Lemme Soient a et b deux entiers premiers entre eux ($a > 1$ et $b > 1$)

alors $\exists ! \ u_0 \in \mathbb{N}$ tq $\begin{cases} 1 \leq u_0 \leq b-1 \\ a u_0 \equiv 1 \ [b] \end{cases}$

Existence : d'après le théorème de Bezout $\exists \ u, v$ tq $au + bv = 1$

on effectue la division euclidienne de u par b

$u = bq + u_0$ avec $0 < u_0 < b$ i.e $1 \leq u_0 \leq b-1$

donc $a(bq + u_0) + bv = 1 \Rightarrow abq + au_0 + bv = 1$

$au_0 = 1 + b(-aq - v)$

$au_0 \equiv 1 \ (b)$.

Unicité : a, b premiers entre eux avec $a > 1$ et $b > 1$

on suppose qu'il existe $u_0 \in \mathbb{N}$ $1 \leq u_0 \leq b-1$, $au_0 \equiv 1 \ (b)$

$u_1 \in \mathbb{N}$ $1 \leq u_1 \leq b-1$, $au_1 \equiv 1 \ (b)$

$a(u_0 - u_1) \equiv 0 \ (b)$ donc $b \mid a(u_0 - u_1)$

$a \wedge b = 1$ donc

$b \mid (u_0 - u_1)$

soit $\exists k \in \mathbb{Z}$ $\quad u_0 - u_1 = kb$

la condition $\begin{cases} 1 \le u_0 \le b-1 \\ 1 \le u_1 \le b-1 \end{cases} \Rightarrow \quad 2-b \le u_0 - u_1 \le b-2$

donc $\quad -b < u_0 - u_1 < b$

$\quad -b < kb < b$

$\Rightarrow \quad -1 < k < 1 \Rightarrow k = 0$ d'où $u_0 = u_1$

1) Soient p, q deux nombres premiers distincts $(p \neq 2,\ q \neq 2)$

$n = pq$ et $e \in \mathbb{N}$ tq $\begin{cases} 1 < e < (p-1)(q-1) \\ e \wedge (p-1)(q-1) \end{cases}$

On applique le lemme $\begin{cases} d \to u_0 \\ e \to a \\ (p-1)(q-1) \to b \end{cases}$

Les hypothèses sont vérifiés $e \wedge (p-1)(q-1)$, $e > 1 \Rightarrow \begin{cases} p > 2 \\ p > 2 \end{cases}$

$\Rightarrow (p-1)(q-1) > 1$

donc $\exists ! d \in \mathbb{N} \quad 1 \le d \le (p-1)(q-1) - 1$

$\Rightarrow 1 \le d < (p-1)(q-1)$

et $ed \equiv 1 \ (p-1)(q-1)$

2°/ On forme la clé privée (n, d)

clé publique (n, e) $\quad p, q, d$ sont gardés secret.

Problème : retrouver d à partir de e !

Montrons que $M^{ed} \equiv M \ (n)$

On code le message m : $n = m^e \ (n)$

$ed \equiv 1 \ (p-1)(q-1)$ donc $\exists k \in \mathbb{Z}$ tel que $ed = 1 + k(p-1)(q-1)$ (1)

- Montrons que $m^{ed} \equiv m \ (p)$
  - Si m n'est pas premier avec p alors $p \mid m$ et $p \mid m^{ed}$
    donc $m^{ed} \equiv 0 \ (n) \equiv m \ (p)$
  - Si $m \wedge p = 1$
    d'après le petit théorème de Fermat
    $m^{p-1} \equiv 1 \ (p)$
    $m^{ed} = m^{1 + k(p-1)(q-1)} = m \cdot \underbrace{\left(m^{p-1}\right)^{k(q-1)}}_{\equiv 1 \ (p)} \equiv m \ (p)$ (1)

    donc $m^{ed} \equiv m \ (p)$

Par symétrie de p et q, $m^{ed} \equiv m \ (q)$

$p \wedge q = 1$, d'après le théorème chinois

$m^{ed} \equiv m \ (pq)$

$m^{ed} \equiv m \ (n)$

On a retrouvé le message.

Fonctionnement

Alice veut transmettre un message à Bob.

Bob choisit p, q premiers distincts
et vérifiant $1 < e < (p-1)(q-1)$
et $e \wedge (p-1)(q-1)$

[ex $p = 41$ et $q = 53$
$n = pq = 2173$ et $(p-1)(q-1) = 2080$

on prend par exemple $e = 1427$ premier avec 2080 (Voir algo d'Euclide)

B calcule l'unique entier d tel que

$$1 \leq d < (p-1)(q-1) \quad \text{et} \quad ed \equiv 1 \ [(p-1)(q-1)]$$

$$\text{ou} \quad (p-1)(q-1)\cdot v + e\cdot u = 1$$

Par l'algo d'Euclide en remontant $d = -937$ soit $d = 1083$

$$(e\cdot u + (p-1)(q-1)\cdot v = 1$$

(u, v) puis $\longrightarrow$ ~~et~~ d reste de la division euclidienne de u par $(p-1)(q-1)$

B diffuse $n = pq$ et e (p, q, d restent secrets)

Pour envoyer un message à B

A convertit ce message en suite de nombres $m < n$

A chiffre chaque nombre en calculant $c \in [\![1, n]\!]$ tq

$$m^e \equiv c \ (n)$$

Ex $\quad n = 356\,453\,213$

découpage en 3 blocs $m_3 = 356$, $m_2 = 453$ et $m_1 = 213$

(en partant de la droite)

Avec $e = 1427$ $\quad m_1^e \equiv 1273 \ (n)$

$m_2^e = 507 \ (n) \longrightarrow 0507$ (pour respecter la position)

$m_3^e = 1297 \ (n)$

A transmet chaque nombre à B.

B décrypte en faisant $c^d = m^{ed} \equiv m \ (n)$

Message transmis $1273, 0507, 1897$

Découpage et on retrouve c_1, c_2, c_3

compléments RSA

Soit (p,q) deux nombres premiers distincts $(p \neq 2,\ q \neq 2)$

On pose $n = pq$

Soit e tq $1 < e < (p-1)(q-1)$ et $e \wedge (p-1)(q-1) = 1$

Lemme Soient a et b premiers entre eux $(a>1$ et $b>1)$

alors $\exists!\ u_0 \in \mathbb{N}$ tq $\begin{cases} 1 \leq u_0 \leq b-1 \\ a u_0 = 1\ (b) \end{cases}$

(Elts clés. $\exists u, v \in \mathbb{Z}$ $au + bv = 1$

$u = bq + u_0$ avec $0 < u_0 < b$ ie $1 \leq u_0 \leq b-1$

Donc $a(bq+u_0) + bv = 1 \Rightarrow a u_0 = 1\ (b)$

1) Mq $\exists!\ d$ tq $1 \leq d < (p-1)(q-1)$ et $ed = 1\ [(p-1)(q-1)]$

Elts clés. Lemme $e = a$ / $d = u_0$ / $(p-1)(q-1) = b$.

Par le lemme, on vérifie les hyp.

2°/ Prouver que $\forall m \in \mathbb{N}$ $m^{ed} = m\ (n)$

Elts clés. Il faut mq $n \mid m^{ed} - m$ et $n = pq$ avec $p \wedge q = 1$

* Si $p \mid m^{ed} - m$

d'après 1) $\exists k \in \mathbb{Z}^*$ tq $ed = 1 + k(p-1)(q-1)$ par la condition d'existence de d.

Si $p \mid m \rightarrow$ ok

$p \nmid m \rightarrow$ petit TH de Fermat

$m^{p-1} = 1\ (p)$

calcul de $m^{ed} = m(p)$

puis $m^{ed} = m(q)$ $\Big\}$ $p \wedge q = 1 \Rightarrow m^{ed} = m(n)$

th. des Restes chinois

Applications

$A \longrightarrow B$

1) choix de p et q premiers

et e tq $1 < e < (p-1)(q-1)$

$e \wedge (p-1)(q-1) = 1$

2) calcul de d. tq

$1 \leq d < (p-1)(q-1)$

$ed = 1 [(p-1)(q-1)]$ (+)

(*) algo d'euclide après choix de e

$eu + (p-1)(q-1)v = 1$

↳ calcul de d tq $(p-1)(q-1) = ku + d$

3) Diffusion de (n, e)

$\longleftarrow$

(n, d)

$M =$ 

$m_1^e(n)$ e_1

$m_2^e(n) \Rightarrow e_2$ $\longrightarrow$ $e_1 e_2 e_3$

$m_3^e(n)$ e_3

déchiffrer et e_1^d, e_2^d, e_3^d.