Plus de détails sur RSA

1 Solution d'exercice sur RSA

$x = ?$
y = x^e mod n

$$\begin{tikzcd} \text{Alice} \arrow[r, bend right, "y = 4"'] & \text{Bob} \arrow[l, bend right, "k_{pub} = (n, e) = (14, 5)"'] \end{tikzcd}$$

$n = p \cdot q$
$14 = 2 \cdot 7$

$\phi(14) = (p-1)(q-1)$
$\phi = (p_1^{e_1} - p_1^{e_1 - 1}) \Rightarrow \phi(14) = (7^1 - 7^0)(2^1 - 2^0) = 6 \cdot 1 = 6$

$d = e^{-1} \bmod \phi(n) = e^{-1} \bmod 6$
$d = 5$

$4^5 \bmod 14 = 2$

Autre numéro: $\emptyset$ (35 ne consiste pas de 2 nombres premiers)

2 Devoir 1: Masque jetable

$c_1 \oplus c_2 = m_1 \oplus m_2$ (où c_1, c_2 donnés)

Soit S un ensemble de mots.
Pour chaque $m_1 \in S$, on peut obtenir un m_2.

Mini-preuve voulu dans le devoir:
$m_1 \oplus (c_1 \oplus c_2) = m_1 \oplus (m_1 \oplus m_2) = m$
$m_2 \in S$?

Au ce moment-là, on a deux solutions:

- $m_1 = squeamish$, $m_2 = ossifrage$
- $m_1 = ossifrage$, $m_2 = squeamish$

Donc, il faut préciser qu'il peut y avoir deux clés

3 RSA

3.1 Encryption rapide

y = $ENC_{k_{pub}}(x) = x^e$ mod n
x = $DEC_{k_{pr}}(y) = y^d$ mod n

$\phi^{(n)} \rightarrow e^{-1}$

e: 1024-3072 bits $\Rightarrow 2^{1024}$ multiplications

Méthode naïve: $x^n = x \cdot x \rightarrow x^2 \cdot x \rightarrow x^3 \cdot x \rightarrow ... \rightarrow x^n$
(par comparaison: 2^{300} atomes dans l'universe)

3.2 Exponentiation rapide

Ex: x^8

$x \underset{\text{SQ}}{\longrightarrow} x^2 \underset{\text{SQ}}{\longrightarrow} x^4 \underset{\text{SQ}}{\longrightarrow} x^8 \quad || \quad x \cdot c \rightarrow x^2 \cdot x \rightarrow x^3 \rightarrow ... \rightarrow x^8$

On peut faire ça avec des exposants e, d = 2^i

Il est possible de mélanger les multiplications avec mises en carré:

Ex: x^{26}

$x \underset{\text{SQ}}{\longrightarrow} x^2 \cdot x \underset{\text{MULT}}{\longrightarrow} x^3 \underset{\text{SQ}}{\longrightarrow} x^6 \underset{\text{SQ}}{\longrightarrow} x^{12} \cdot x \underset{\text{MULT}}{\longrightarrow} x^{13} \underset{\text{SQ}}{\longrightarrow} x^{26}$

3.3 Algorithme: Square and multiply

On "scan" la valeure binaire de notre exposant de gauche à droite. Pour chaque bit, on met au carré et si le bit est de 1, on multiplie après de mettre qu carré.

Ex: x^{26}=$x^{11010_2} = x^{(b_4 b_3 b_2 b_1 b_0)_2}$
Initialisation:

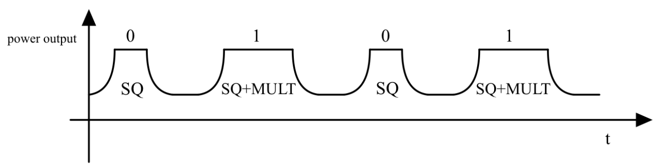
$$\begin{array}{ll}
x^{1_2} & \rightarrow b_3 = 1 \\
\left.\begin{array}{l} (x)^2 = x^2 = x^{10_2} \\ x^2 \cdot x = x^3 = x^{11_2} \end{array}\right\} & \rightarrow b_4 = 1 \\
(x^3)^2 = x^6 = x^{110_2} & \rightarrow b_2 = 0 \\
\left.\begin{array}{l} (x^6)^2 = x^{12} = x^{1100_2} \\ x^{12} \cdot x = x^{13} = x^{1101_2} \end{array}\right\} & \rightarrow b_1 = 1 \\
(x^{13})^2 = x^{26} = x^{11010_2} & \rightarrow b_0 = 0
\end{array}$$

SQ $\rightarrow$ left shift de l'exposant;
MULT $\rightarrow$ set 0$\rightarrow$1 le LSB (least significant bit)

3.3.1 Matrice de Fibonacci

$$\begin{pmatrix} 1 & 1 \\ 1 & 0 \end{pmatrix}^n = \begin{pmatrix} f_{n+1} & f_n \\ f_n & f_{n+1} \end{pmatrix}^n$$

3.3.2 Rélation avec l'attaque par canal auxiliaire



3.3.3 Complexité:

$$\begin{aligned} & d \Rightarrow 1024\ bits \\ & d \Rightarrow t\ bits \\ & \quad \Rightarrow t\ SQ \\ & \quad \underline{+0.5t\ MULT}(\longrightarrow Poids\ de\ Hamming\ \Rightarrow nombre\ de\ \text{"}1\text{"}) \\ & \quad\ 1.5t \end{aligned}$$

$1024 \cdot 1.5 = 1536$ opérations/2^{1024}

3.3.4 Encryption rapide:

x^e mod n rapide à faire

Petits exposants:

3	11
17	1 0001
$2^{16}+1$	1 0000 0000 0000 0001

$\rightarrow$ encryption d'un message
$\rightarrow$ vérification d'uni signature RSA

3.3.5 Decryption rapide:

CRT (Chinese remainder Theorem)

$$x^d \; mod \; n \equiv y$$
$$x^d \; mod \; p \cdot q \equiv y$$

$$\begin{array}{lll} x_p \equiv x \; mod \; p & y_p \equiv x_p^{d_p} \; mod \; p & d_p \equiv d \; mod \; (p-1) \\ x_q \equiv x \; mod \; p & y_q \equiv x_p^{d_p} \; mod \; p & d_q \equiv d \; mod \; (q-1) \end{array}$$

CRT:
$y \equiv [q \cdot c_p]y_p + [p \cdot c_q]y_q$ mod n

$c_p \equiv q^{-1}$ mod p
$c_q \equiv p^{-1}$ mod q

Ex: $p = 11, \; q = 13$
$n = p \cdot q = 11 \cdot 13 = 143$
$\phi(143) = (11-1)(13-1) = 10 \cdot 12 = 120$

$e = 7$
$d = e^{-1} \equiv 103$ mod 120
$15 \rightarrow$ message à decrypter

$$\begin{tikzcd} y = x^e \text{ mod n} & \text{Alice} \arrow[r, bend right, "d = e^{-1} \text{ mod } \phi(n)"'] & \text{Bob} \arrow[l, bend right, "k_{pub} = (n, e) = (13, 7)"'] & \begin{array}{l} n = p \cdot q = 11 \cdot 13 \\ e = 7 \end{array} \end{tikzcd}$$

$$y^d \; mod \; n$$

On veut decrypter:
15^{103} mod 143

$x_p \equiv 15 \equiv 4$ mod 11
$x_q \equiv 15 \equiv 2$ mod 13

$d_p \equiv 103 \equiv 3$ mod 10
$d_q \equiv 103 \equiv 7$ mod 12

$y_p \equiv x_p^{d_p} \; mod \; p \equiv 4^3 \equiv 64 \equiv 9$ mod 11
$y_q \equiv x_q^{d_q} \; mod \; q \equiv 2^7 \equiv 128 \equiv 11$ mod 13
$\rightarrow$ (y_p, y_q)

$y \equiv [q \cdot c_p]y_p + [p \cdot c_q]y_q$ mod n

$x \equiv [13 \cdot 6] \cdot 9 + [11 \cdot 6] \cdot 11$ mod 143

Complexité:

- nombre d'opérations reste le même: $\frac{1.5t}{2} \cdot 2 = 1.5t$
- mulitiplication de t/2 bits est x4 plus rapide que pour t bits

Génération de p et q:

$$\begin{tikzcd} & & \tilde{p} \text{ est premier} \quad \leftarrow (\textit{probablement}) \\ \boxed{\text{PRNG}} \arrow[r, "\tilde{p}"] & \boxed{\text{TEST}} \arrow[ur] \arrow[dr] & \\ & & \tilde{p} \text{ est composé} \end{tikzcd}$$

3.3.6 PNT: Prime Number Theorem

P($\tilde{p}$ est premier) $\approx \frac{1}{ln(\tilde{p})}$

en pratique: P($\tilde{p}$ est premier) $\approx \frac{2}{ln(\tilde{p})}$

Ex: $n \rightarrow 1024$ bits; p, q $\rightarrow 512$ bits

P($\tilde{p}$ premier) $= \frac{2}{ln(2^{512})} = \frac{2}{512 ln(2)} \approx \frac{1}{177}$

3.3.7 Miller-Rabin: Algorithme Probabiliste

Théorème decomposé:
$\tilde{p} - 1 = 2^u \cdot r$ (r impair)

Si on peut trouver $a \in \mathbb{Z}$ t.q.:

- 1-$a^r \not\equiv 1$ mod $\hat{p}$
- 2-$a^{r \cdot 2^j} \not\equiv \tilde{p} - 1$ mod $\tilde{p}$ $\forall j \in \{0, 1, ..., u-1\}$ $\mathbb{Z}_{u-1}$

$\tilde{p}$ est composé (100%).
Sinon, $\tilde{p}$ est probablement premier.

3.3.8 Algorithme de Miller-Rabin: *input* : $\hat{p} - 1 = 2^u r$

Pour i = 1 à s $\leftarrow$*s: security parameter*

    choisir aléatoirement a $\in \{2, 3, ..., \tilde{p} - 2\}$

    $z \equiv a^r$ mod $\hat{p}$

    si $z \not\equiv 1$ et $z \not\equiv \tilde{p} - 1$:

        pour j = 1 à u-1:

            $z \equiv z^2$ mod $\hat{p}$

            si z = 1:

                retourne $\hat{p}$ est composé

            si z $\neq \hat{p} - 1$:

                retourne $\hat{p}$ est composé

retourne $\hat{p}$ est probablement premier

Si composé, k est probablement $P(\tilde{p}) = 4^{-k}$

#de bits de p	S donnant une erreur avec P $<2^{-80}$
250	11
300	9
400	6
500	5
600	3

- SCHOOLBOOK RSA -

Padding

RSA est déterministe

x = 0, x = 1, x = -1 $\Rightarrow$ y = 0, y = 1, y= -1

Malléable *si on n'ajoute pas de padding*

Oscar peut transformer un message chiffré en un autre sachant la transformation effectuée au message clair associé à ce nouveau chiffre:

$(S^e y)^d \equiv S^{ed} x^{ed} \equiv Sx$ mod n *(si y est un montant)*