Université Gaston Berger
UFR SAT
Séction Mathématiques appliquées

Projet Cryptography *à* clef public

15 Mai 2021

Membres : Seyni KANE
Ramatoulaye DIALLO

Table de matiere

Introduction

La cryptographie *à* clef public asymétrique est un domaine de la cryptography *ò*u il existe une distinction entre des données *public* et *privées*. Le calcule de ces d'onnées fait appel a des conceptes mathématiques plus précisement arythémetique tels que les conceptes de primalités, et aussi des conceptes algorithmiques.
Ici nous allons essayer de traiter les exercices qui sont proposer.

<u>Exercice 6.1 :</u> Factorisation d'un module RSA

Soit $n = p * q \in \mathbb{R}$, avec p, q des nombres premiers.

1) Determination de p et q connaissant $n = p * q$ et $\phi(n) = (p-1) * (q-1)$

On a :

$$\left\{ \begin{array}{r} n = p * q \\ \phi(n) = (p-1) * (q-1) \end{array} \right.$$

Donc

$$\left\{ \begin{array}{r} n = p * q \\ \phi(n) = p * q - p - q + 1 \end{array} \right.$$

Donc

$$\left\{ \begin{array}{r} n = p * q \\ \phi(n) = p * q - (p + q) + 1 \end{array} \right.$$

Ce qui nous donne

$$\left\{ \begin{array}{r} n = p * q \\ p + q = n - \phi(n) + 1 \end{array} \right.$$

Posons $S = p + q$ et $P = p * q$

Connaissat n et $\phi(n)$ la resolution de l'équation $X^2 - SX + P = 0$, nous permet de rerouver p et q.

D'ou le resultat.

Exercice 6.2 : Ensemble reconnaissable, echantillonable de maniere efficace

Soient p et q deux nombre premiers superieurs à 2 tels que $p|q-1$. Soit $G =< g >$ un sous-groupe de $\mathbb{Z}^*{}_p$ d'orde p.

1)Montrons que G est reconnaissable de maniere efficace.

Il suffit de trouver un algorithme efficace $\mathcal{A}$ qui etant donnée $x \in \mathbb{Z}^*{}_p$ nous renvoie 1 si $x \in G$ et 0 sinon.

Soit l'algorithme $\mathcal{A}$ défini comme suit :

Algorithm 1: L'algorithme $\mathcal{A}$

input : $g, p, x \in \mathbb{Z}^*{}_p$

output: 0 ou 1

```
x ←_R Z*_p;
for i = 0 to p − 1 do
    if x == g^i then return 1 ;
return 0
```

Ainsi , on constate que l'algorithme $\mathcal{A}$ definie ci-dessus test de maniére éfficace si un element $x \in \mathbb{Z}^*{}_p$ appartient a ou non a $G =< g >$ d'ou G est reconnaissable de maniere efficace.

D'ou le resultat.

2)Montrons que G est echantillonable de maniére éfficace
Pour ce la il suffit de trouver un algorithme éfficace $\mathcal{B}$ qui renvoie $x \in G$, tels que x soit uniformement distribuée sur G.
Soit l'algorithme $\mathcal{B}$ défini comme suit :

Algorithm 2: L'algorithme $\mathcal{B}$

output: $x \in G$

$x \leftarrow_R G$;
return x;

L'algorithme $\mathcal{B}$ definie ci-dessus tire un élement de G de maniére uniformément aléatoire, de maniére éfficace d'ou G est échantillonable de maniere efficace.
D'ou le resultat.

3)Montrons que si G' est un groupe d'ordre p telque :
-G' est reconnaissable de maniére éfficace. C'est a dire il existe un algorithme efficace $\mathcal{A}$ qui étant donnée $x \in \mathbb{Z}^*{}_p$ nous renvoie 1 si $x \in G$ et 0 sinon.
-Il existe un algorithme efficace $\mathcal{B}$ qui étant donnée $(a, b) \in G'^2$ renvoie $a.b$.
Alors G' est échantillonnable de maniére éfficace
Pour ce la il suffit de trouver un algorithme éfficace $\mathcal{C}$ qui renvoie $x \in G'$, tels que x soit uniformement distribuée sur G'.
Soit l'algorithme $\mathcal{C}$ défini comme suit :

Algorithm 3: L'algorithme $\mathcal{C}$

input : $a \in G'$
output: $x \in G'$

$b \leftarrow_R \mathbb{Z}^*{}_p$;
while $\mathcal{A}(b) \neq 1$ **do**
  $b \leftarrow_R \mathbb{Z}^*{}_p$;
$x \leftarrow \mathcal{B}(a, b)$;
return x;

L'algorithme $\mathcal{C}$ definie ci-dessus retourne un élement de G' tiré de maniére uniformément aléatoire, de maniére éfficace, car vue que G' est un groupe, donc on a $\forall(a,b) \in G'^2$,$a.b \in G'$. Et comme que b est tiré de maniére uniformément aléatoire dans G', $a.b$ aussi est tiré de maniére uniformément aléatoire dans G'. De plus on a $\mathcal{A}$ et $\mathcal{B}$ des algorithmes efficaces, alors notre algorithme $\mathcal{C}$ est effice.
D'ou G' est échantillonable de maniere efficace.
D'ou le resultat.

Exercice 6.2 : Nombre de Carmichael

Un entier n impair est dit Carmichael s'il est :
i)sans facteur carré
ii)si p_i est un d ses facteurs premier, ona $(p_i - 1)|(n-1)$
1)Montrons que si n est un nombre de Carmichael pour tout b appartenant à $\mathbb{Z}, b^{\text{n}} \equiv b(modn)$. Soit p un des entiers de la décomposition de n en facteur premier -Si $p \nmid n$ d'apres le theoréme de Fermat $b^{\text{phi(p)}} \equiv 1(modn) \Rightarrow b^{\text{p-1}} \equiv 1(modp)$
or on a
$(p-1)|(n-1) \Rightarrow$ il $\exists k \in \mathbb{Z}/(n-1) = k(p-1)doncb^{\text{n-1}} \equiv b^{\text{k(p-1)}}(modp) \equiv 1(modp)$ (*)
En multipliant (*) par b, on obtient
$b^{\text{n-1}} \equiv b(modp)(1)$ -Si $p|n$, alors $b^{\text{p-1}} \equiv 0(modp) \Rightarrow b^{\text{n-1}} \equiv 0(modp)$
(1) et (2) $\Rightarrow \forall p$ de la décomposition de n en produit de facteur premier on a $b^{\text{n}} \equiv b(modp)$ or $\mathbb{Z}_n = \mathbb{Z}_{p_1}\mathbb{Z}_{p_2} * ...\mathbb{Z}_{p_k}$, avec $n = p_1 * p_2 * ...p_k$, p_i premier $\forall i = 1, ..., k$.
Donc $b^{\text{n}} \equiv (bmodn)$
D'ou pour tout $b \in \mathbb{Z}, b^{\text{n}} \equiv (bmodn)$. 2)Montrons que tout nombre de Carmichael n s'ecrit sous la forme $p_1 * p_2 * ...p_k$, oú les p_i distincts, $k >= 3$ et $(p_i - 1)|(n-1)$ pour tout $i = 1, ..., k$

Supposons par absurde il existe $k < 3$ tel que n soit un nombre de Carmichael et $n = p_1 * p_2$ avec les p_i distincts pour tout $i = 1, 2$ -Pour $k = 1, n = p_1$ n'est pas un nombre de Carmichael -Pour $k = 2, n = p_1 * p_2$ Puisque $p1$ et $p2$ sont distinct alors ona :$p_1 < p_2$ oú $p_2 < p_1$ On prend $p2 < p1$ ona $(p_1 - 1)|(n-1) or n - 1 = p_1 * p_2 - 1 + p_1 - p_1 = p_1(p_2 - 1) + p_1 - 1$ Donc $(p_1 - 1)|(n - 1) \Rightarrow (p_1 - 1)|p_1(p_2 - 1) + p_1 - 1 or pgcd(p_1 - 1, p_1) = 1$ d'oú $(p_1 - 1)|(p_2 - 1) \Rightarrow p_1 - 1 < p_2 - 1 \Rightarrow p_1 < p_2$ ce qui est absurde. d'oú tout nombre de Carmichael s'ecrit sous la forme $p_1 * p_2 * ...p_k$, oú les p_i distincts, $k >= 3$ et $(p_i - 1)|(n - 1)$ pour tout $i = 1, ..., k$, oú les p_i distincts, $k >= 3$ et $(p_i - 1)|(n - 1)$ pour tout $i = 1, ..., k$. 3)Le test de Fermat ne saurait etre utilisé comme test de primalité .En effet,pour le test de Fermat l'algorithme teste si un nombre donneé en entré s'il est *"composite"* ou *"peut etre premier"*

On a si n est un nombre premier,

alors pour tout $\alpha \in \mathbb{Z}_n{}^*$ $\quad pgcd(\alpha, n) = 1 \Rightarrow \alpha^{\mathrm{phi(n)}} \equiv 1(modn)$

$\Rightarrow \alpha^{(\mathrm{n\text{-}1})} \equiv 1(modn)$

or si $\beta = alphat^{(\mathrm{n\text{-}1})} \neq 1 \Rightarrow n$ nént pas premier sinon, le test revoie peut étre premier,

or si n est un nombre de Carmichael, on pour tout $b \in \mathbb{Z}, b^{(\mathrm{n\text{-}1})} \equiv 1(modn)$

Donc d'apres le test n peut etre prenmier,or il exist $p_1, p_2, ..., p_k, k >= 3$ pour tout $i = 1, ..., k$,telque :

$n = p_1 * p_2 * ...p_k \Rightarrow \forall i = 1, ..., k \quad p_i | n$ donc n ne peut pas etre premier et etant donnée que les nombres de Carmichael sont infinis.
Alors le test de Fermat ne saurait etre utilisé comme test de primalité.
4)Modifions l'alorithmede maniere á renvoyer une preuve de non primalité de n verifiable en temps polynomiale. On sait que s'il existe alpha dans ${\mathbb{Z}_n}^* / \alpha^{(\text{n-1})} \neq 1$, on peut affirmer avec certitude que n n'est pas premier.
soit l'algorithme suivant :

Algorithm 4: L'algorithme $\mathcal{A}$

input : n, k

output: 0 ou 1

```
for i = 0 to k − 1 do
    α ←_R Z*_n; β = α^(n-1)
    if β ≠ 0 then return α ;
return α = 0
```

Sortie : α

$$\begin{cases} \text{si } \alpha \neq 0 \text{ alors } \alpha \text{est un certificat de non primalité} \\ \textbf{Sinon aucun certificat de non primalté} \end{cases}$$

<u>*Exercice 6.5 :*</u> *Test de primalité*

Soit n $\in \mathbb{N}^* \setminus 2\mathbb{N}$. On note $\mathbb{Z}_n \setminus \{0\}$ par $\mathbb{Z}_n^+$ et on définit :

$l_n = \{\alpha \in \mathbb{Z}_n^+, \alpha^{n-1} = 1\}$

1. Montrons que $l_n \subseteq \mathbb{Z}_n^*$.

$$\text{soit} \in l_n \Longrightarrow \alpha_n^{n-1} = 1$$
$$\Longrightarrow \alpha = 1 \bmod n.$$

D'après le théorème de Fermet $\alpha \wedge n = 1$ on a $\alpha \wedge = 1 \Leftrightarrow \bar{\alpha}$est un génerateur de $(\mathbb{Z}/\mathbb{Z}_n)$

$\Leftrightarrow \bar{\alpha}$ est un élement inversible de l'anneau $(\mathbb{Z}_n, +, .\ )$.
D'où $\bar{\alpha} \in (\mathbb{Z}/\mathbb{Z}_n)^*$.

Par conséquent $l_n \subseteq \mathbb{Z}_n$. (1)

2. Montrons que si n est premier alors $L_n = \mathbb{Z}_n^*$

n est premier $\Longrightarrow \mathbb{Z}_n^*$ est cyclique d'ordre $\varphi(n) = n - 1$

$$\Longrightarrow \forall x \in x_n^*, \quad x_n^{n-1} = 1$$
$$\Longrightarrow \forall x \in x_n^*, \quad x \in l_n$$
$$\Longrightarrow x_n \subseteq l_n$$

(2) (1) et (2) si n est premier alors $L_n = \mathbb{Z}_n^*$

3. Montrons que si n est composite et si $L_n \subsetneq \mathbb{Z}_n^*$, alors $|L_n| \leq (n-1)/2$

Soit $\psi : \mathbb{Z}_n^* \longrightarrow \mathbb{Z}_n^*$
$$x \longmapsto \quad x^{n-1}$$

i)ψ est un morphisme. En effet $\forall x, y \in \mathbb{Z}_n^*$
$\psi(xy) = \quad xy^{n-1} \quad = \quad x^{n-1}y^{n-1} = \quad \psi(x)\psi(y)$
On a $L_n = ker\psi.$ En effet $L_n \subset ker\psi$ et $ker\psi \subset L_n$ par définition. D'oú le résultat
Or $L_n = ker\psi \subset \mathbb{Z}_n^*$
$\Longrightarrow \mid L_n \mid \Bigg| \mid \mathbb{Z}_n \mid$ et l_n n'est pas un sous-groupe trivial de $\mathbb{Z}_n^*$ D'oú
$\frac{|\mathbb{Z}_n^*|}{|L_n|} \geq 2 \Longrightarrow \quad \mid l_n \mid \leq \quad \frac{1}{2} \mid \mathbb{Z}_n^* \mid$
$\Longrightarrow \mid L_n \leq \frac{1}{2}\psi(n)$
or n est un composite donc $\psi(n) \leq n - 1$
d'oú $\mid L_n \mid \leq \frac{1}{2}(n-1)$
4. Montrons que pour tout nombre Carmichael n $l_n = \mathbb{Z}_n^*$
$\rightarrow$ D'après la question 1 $L_n \subseteq \mathbb{Z}_n^* \forall n \in \mathbb{N}^*/2\mathbb{N}$ (*)
$\rightarrow$ on a n est un nombre de Carmichael donc
$\exists P_1, ..., P_k$ avec P_i premier $i \in \{1, ..., k\}$
Soit x $\in \mathbb{Z}_n^*$, montrons que x $\in L_n$ ie $x^{n-1} = 1$
On a $\mathbb{Z}_n^* \cong \mathbb{Z}_{p_1}^* \quad * \mathbb{Z}_{p_2}^* * \quad ... * \quad \mathbb{Z}_{p_1}^*$
Soit $\varphi \quad \mathbb{Z}_n^* \longrightarrow \quad \mathbb{Z}_{p_1}^* \quad * \mathbb{Z}_{P_2}^* * \quad ... * \quad \mathbb{Z}_{P_1}^*$

x $\mapsto$ $(x_1, ..., x_k)$
un isomorphisme de $\mathbb{Z}_n^*$ $dans$ $\mathbb{Z}_{P_1}^*$ $* \mathbb{Z}_{P_2}^* *$ $... *$ $\mathbb{Z}_{P_1}^*$
soit x $\in \mathbb{Z}_n^*$, alors $\forall$ $i \in \{1, ..., k\}$, $x_i \in$ $\mathbb{Z}_{P_i}^*$
$\Longrightarrow x_i^{P_i - 1} = 1$, $\forall i \in \{1, ..., k\}$
$\Longrightarrow x_i^{P_i - 1} = 1$, $\forall i \in \{1, ..., k\}$ car $Pi - 1 | (n - 1)$, $\forall i \in \{1, ..., k\}$
Donc $for x \in \mathbb{Z}_n^*$ $(\varphi(x))^{n-1}$ $=$ $(x_1^{n-1}, x_2^{n-1}, ..., x_k^{n-1})$
$= (1, 1, ...1) \Longrightarrow x \in \mathbb{Z}_n^*, \ x^{n-1} = 1$
$\Longrightarrow x \in \mathbb{Z}_n^*, \ x \in L_n \Longrightarrow \mathbb{Z}_n^* \subseteq L_n$ (**)
D'après (*) et (**) sin n est un nombre Carmichael alors
$L_n = \mathbb{Z}_n^*$
5. On pose $n - 1 = t_2$ avec t_2 et on définit

$$l_n^{'} = \{\alpha \in \mathbb{Z}_n^* : \alpha^{n-1} = 1 \quad \forall j \in \{0, ..., k-1\}, \alpha^{t_2 j+1} = 1, \quad \alpha^{t_2 j} = \pm 1\}$$

a. Montrons que si n est premier impair alors $L_n^{'} = \mathbb{Z}_n^*$
On a comme n est premier impair alors $\mathbb{Z}_n^* \varphi(n) = n - 1$
Donc $\forall x \in \mathbb{Z}_n^*, \ x^{n-1} = 1$
Supposons $x^{t_2 j+1} = 1$ montrons $x^{t_2 j} = \pm 1$
on a $t2^{j+1} = t2^j * 2$
$x^{t2^{j+1}} = 1 \Longrightarrow x^{t2^j * 2} = 1$

$\Longrightarrow x^{(t2^j)2} = 1$
Posons $\beta = x^{2^j t}$, on a $\beta^2 = 1$
$\Longrightarrow \beta^2 - 1 = 0 \quad \Longrightarrow \beta = \pm 1$
$\Longrightarrow x \in L_n^{'}$
$\Longrightarrow \mathbb{Z}_n^* \subset L_n^{'}$ en plus $L_n^{'} \subset \mathbb{Z}_n^*$
Si n est premier impair alors $L_n^{'} = \mathbb{Z}_n^*$
b. On suppose que $n = p^e$ avec p premier et $e > 1$
Soit l'endomorphisme de $\mathbb{Z}_n^*$ définit par
$f(x) = x^(n-1)$
i)Montrons que $L_n^{'} \subset kerf$
Soit x $\in L_n^{'} \Longrightarrow x^{n-1} = 1 \quad (1)$
$kerf = \{x \in \mathbb{Z}_n^* \quad : x^{n-1} = 1\}$
On a x $\in L_n^{'} \Longrightarrow \quad : x^{n-1} = 1 \Longrightarrow \quad xx^{n-2} = 1$
Posons $x^{'} = x^{n-2} \quad \Longrightarrow \quad x^{'}x = 1$
D'où $x \in \mathbb{Z}_n^* \quad (2)$
(1)et (2) $\Longrightarrow \quad x \in kerf$
D'où $L_n^{'} \subset kerf$
On a $kerf = \{x \in \mathbb{Z}_n^* \quad : x^{n-1} = 1\}$ avec
f : $\mathbb{Z}_n^* \longrightarrow \mathbb{Z}_n^*$
x$\longmapsto x^{n-1}$
Posons $n = p^e$, $\mathbb{Z}_n^*$ est cyclique d'ordre $\varphi(n)$

$\Longrightarrow$ il est isomorphe à $\mathbb{Z}_{\varphi(n)}$.
soit $\theta : \mathbb{Z}_n^* \longrightarrow \mathbb{Z}_{\varphi(n)}$

$$x \longmapsto \theta(x) = yx$$

$(n-1)yx = O_{\mathbb{Z}_{\varphi(n)}}$ (*)
le nombre de solution (*) est le $pgcd(n-1, \varphi(n))$
Donc $\mid ker f \mid = pgcd(n-1, \varphi(n))$
$= pgcd(p^e - 1, p^{e-1}(1-\frac{1}{p})$
5-b ii) $\mid ker f \mid = p - 1 = \frac{p^e}{p^e + \ldots + 1}$
$= \frac{n-1}{\beta}$ avec $\beta \geq 4$
D'où $\mid ker f \mid \leq \frac{n-1}{4}$
or $l_n^{'} \subset ker f \Longrightarrow \mid l_n^{'} \mid \leq \mid ker f \mid$
$\Longrightarrow \mid l_n^{'} \mid \leq \dfrac{n-1}{4}$
5.c) i) montrons que pour tout $x \in L_n^{'}$, $\alpha^{t2^g} = 1$ Si $x \in L_n^{'}$ alors $\alpha \in \mathbb{Z}_n^*$
$\varphi(\alpha) = (\alpha_1, .., \alpha_r)$
$\varphi(\alpha^{t2^g}) = (\alpha_1^{t2^g}, ..., \alpha_r^{t2^g})$
Supposons par l'absurde qu'il existe $\alpha \in L_n^{'} \neq 1$
On a nécessairement $g \neq h$ car si $g = h$ on a
$t2^g = t2^h = n - 1$, or par défaut $L_n^{'}$, $\forall \alpha \in L_n^{'}$ $n^{n-1} = 1$

Puisque $g = min\{h_1, h_1, ..., h_1\}, g = h$ pour un certain i
Soit j le plus petit entier tel que $\alpha^{t2^j} = 1$ on a $\alpha^{t2^{j-1}} \neq 1$
Par ailleurs $j - 1 \geq g = h_i$
Ainsi $\alpha^{t2^j} = 1 \quad et \quad \alpha^{t2^{j-1}} \neq 1$. On en déduit que $2^j | ord(\alpha_i^t) \quad (*)$
Si $\alpha_i^t)$ appartient à un groupe cyclique d'ordre $t_i 2^{h_i} \quad avec \quad t_i \quad impair$
$(*) \Longrightarrow 2^i | 2^{h_i}$ absurde car $j - 1 \geq h_i$. Donc $\forall n \quad \alpha \in L_n^{'}, \quad \alpha^{t2^g} = 1$.
iia <u>Montrons que si $\alpha \in L_n^{'} \quad alors \quad \alpha^{t2^{g-1}} \neq 1$</u>
soit $\alpha \in L_n^{'} \Longrightarrow \forall j \in \{i, ..., h_i\} \alpha^{t2^{j+1}} = 1 \quad \Longrightarrow \quad \alpha^{t2^j} = \pm 1$ et on a :
$\forall \alpha \in L_n^{'}, \alpha^{t2^g} = 1 h \geq g = 1 g - 1 \in \{0, ..., h\}$
Donc $\alpha^{t2^{g-1}+1} = 1 \quad \Longrightarrow \alpha^{t2^{g-1}} = \pm 1$
iii) Déduisons en que $| L_n^{'} | \leq 2 \quad | ker f_{g-1} |$
$f_{g-1} : \quad c \longrightarrow \quad \mathbb{Z}_n^*$
$\alpha \longmapsto \quad \alpha^{t2^g}$
$ker f_{g-1} = \{\alpha \in \mathbb{Z}_n^* \quad : f_{g-1}(\alpha) = 1\}$
$= \{\alpha \in \mathbb{Z}_n^* \quad : \alpha^{t2^{g-1}} = 1\}$
On a $\alpha^{t2^{g-1}} = 1$
si $\alpha \in L_n^{'} \alpha^{t2^{g-1}} = \pm 1$
$\Longrightarrow L_n^{'} \subseteq \{\alpha \in \mathbb{Z}_n^* \quad : \alpha^{t2^{g-1}} = \pm 1\}$
On a $f_{g-1} = \alpha^{t2^{g-1}} = \pm 1$

$\Longrightarrow L_n^{'} \subseteq f_{g-1}^{-1}(\{-1\}) \cup f_{g-1}^{-1}(\{1\})$
$\Longrightarrow |L_n^{'}| \leq |f_{g-1}^{-1}(\{-1\})| + |f_{g-1}^{-1}(\{1\})|$
or $|f_{g-1}^{-1}(\{-1\})| = keerf_{g-1} \quad et \quad |f_{g-1}^{-1}(\{1\})| = kerf_{g-1}$
Donc $|L_n^{'}| \leq 2|kerf_{g-1}|$

iii.c) Montrons que $|kerf_j| = \prod_{i=1}^{r} pgcd(t_i 2^{h_i}, t2^j)$

$$f(\alpha) = 1 f(\alpha_i) = 1 \qquad \forall i \in \{1...r\}\{\alpha_i \in \mathbb{Z}_p \alpha^{t^{2^j}} = 1\} = pgcd(t_i 2^{h_i}, t2^j)$$

donc $\{\alpha \in \mathbb{Z}_n^* \quad f_g(\alpha) = 1\}$

$= \prod_{i=1}^{r} |\{\alpha_i \in \mathbb{Z}_{pi}^{e^* i}, \alpha^{t2^j} = 1\}$

$= \prod_{i=1}^{r} pgcd(t_i 2^{h_i}, t2^j)$

iii.d) Montrons que $2^r|kerf_{g-1} |=| kerf_g |\leq |kerf_r|$
$g = min\{h_1, ...h_r\} \Longrightarrow g \leq h$
$kerf_g = \{\alpha \in \mathbb{Z}_n^* : f_g(\alpha) = 1\}$
$= \{\alpha \in \mathbb{Z}_n^* : \alpha^{t2^g} = 1\}$
$= \{\alpha \in \mathbb{Z}_n^* : \alpha^{t2^h} = 1\}$

Si $h = g$ alors $f_g = f_h \implies |kerf_g| = |kerf_h|$
Sinon si $h > g$ alors $h = g * u$ avec u $\in \mathbb{N}$
Ainsi $\forall a \in kerf_g, f_h(\alpha) = \alpha^{t2^{gu}} = (\alpha^{t2^g})^{2u} = 1^{2u}$
donc $\forall \alpha \in kerf_g \subset, kerf_h$ d'où $|kerf_g| \leq |kerf_h|$
Ce qui montre $|l_n^{'}| \leq 2^{r+1}|kerf_h|$
$|l_n^{'}| \leq 2|kerf_{g-1}|$
$|kerf_{g-1}| \leq |kerf_h| avec |kerf_g| = 2^r|kerf_{g-1}|$
$2^r|kerf_{g-1}| \leq |kerf_h| \quad (a)$
or $|L_n^{'} \leq 2|kerf_{g-1}| \quad (b)$
$|kerf_{g-1} \leq 2^r|kerf_h|$
$2|kerf_{g-1} \leq 2^{1-r}|kerf_h|$

$$\boxed{|l_n^{'}| \leq 2|kerf_{g-1}| \leq 2^{1-r}|kerf_h|}$$

iii.e) Montrons que si $r \geq 3$ alors $|l_n^{'}| \neq |\mathbb{Z}_n^*|/4 \neq (n-1)/4$

On a $|l_n^{'}| \leq 2^{1-r}|kerf_h|$
$r \geq 3 \implies |l_n^{'}| \leq 2^{1-3}|kerf_h|$

$$\implies |l_n^{'}| \leq \frac{|kerf_h|}{4} or kerf_h \subseteq \mathbb{Z}_n^*$$

$$\implies |l_n^{'}| \leq \frac{|\mathbb{Z}_n^*|}{4}$$

6) Montrons que l'algorithme teste la validité de l'assertion $\alpha \in \mathbb{Z}_n^*$

$\longrightarrow Si\beta = \alpha^j = 1 \quad \forall \in \{0, ...h-1\}$ on a $\alpha^{t2^{j+1}} = (\alpha^t)^{2^{j+1}} = 1 \qquad \alpha \in L_n^{'}$

$\alpha^{t2^j} = (\alpha^t)^{2^j} l = 1 \qquad \alpha \in L_n^{'}$

$\Longrightarrow$ Si l'algorithme s'arrête á la ligne 11 on a $\alpha \in L_n^{'}$

$\Longrightarrow$ ai l'algorithme s'arrête á la ligne 15, on a :

$\forall i_1 < i, \alpha^{t2^{i_1}} \neq pm$

$\alpha^{t2^i} = -1 et \alpha^{t2^{i+1}} = 1 \forall j$

Il est vérifié que

$\alpha^{n-1} = \alpha^{t2^j} = 1$

$\forall j \in \{0, ..., h\} si \alpha^{t_i 2^{j+1}} = 1 alors \alpha^{t_i 2^j} = \pm 1 \qquad \forall \alpha \in L^{'} n$

$\Longrightarrow$ Si l'algorithme s'arrête à la ligne 18

on a $\forall i_2 \subset i, \alpha^{t2^{i+1}} \neq \pm 1, deplus \forall j$

$\alpha^{n-1} = \alpha^{t2^i} = 1$

$\forall j \in \{0, ..., h-1\} si \alpha^{t2j+1} = 1 alors \alpha^{t2^j} = \pm 1 \qquad \forall \alpha \in L_n^{'}$

$\longrightarrow$ Si l'algorithme s'arrête à la ligne 22

On a $\forall i \leq h-1, \alpha^{t2^i} \neq \pm 1 \Longrightarrow \alpha \in L_n^{'}$

Conclusion : l'analyse que nous venons de faire nous fait remarquer que l'algorithme revoie vrai uniquement lorsque $\alpha \in L_n^{'}$ et faux dans le cas contraire. Donc on peut affirmer que cette algorithme, pour un n donné et un $\alpha \in L_n^{'}$, teste efficacement la validit2 de l'insertion.

7) $\Longrightarrow$ si l'algorithme s'arrête à la ligne 24
On a n=2 qui est en effet un nombre premier
$\Longrightarrow$ si l'algorithme s'arrête à la ligne 27
On a $n \neq 2et2/n$
Donc $n \neq 2etnestpaire$
Or le seul nombre premier pair que l'on connait est 2
Donc on peut affirmer avec certitude que n 'est pas premier
$\Longrightarrow$ Si l'algorithme s'arrête à la ligne 32
On a $n \neq 2et2 \nmid ndoncn \neq 2etnestimapair$ à la ième itération on a tiré un $\alpha \in \mathbb{Z}_n^* et\alpha \notin L_n^{'}$
Ce qui implique que $\mathbb{Z}_n^* \neq L_n^{'}$
Si n est premier on a $\mathbb{Z}_* = L_n^{'}$
Donc on peut affirmé avec certitude que n n'est pas premier.
$\Longrightarrow$ Si l'algorithme s'arrête à la ligne 35
On a $n \neq 2$ donc n impair. De plus on tire k fois de manir̂e uniformÃ©ment et aléatoire un élément de $\alpha \in \mathbb{Z}_n^*$ et à chaque fois on a $\alpha \in L_n^{'}$, donc on peut affirmer avec une probabilité d'erreur très faible que n est premier.

Conclusion : lánalyse que l'on vient de faire, on peut dire que le test de Miller-Rabin teste la validité de l'affirmation "n'est pas premier". En effet si n est premier , elle renvoie toujours vraie car si $n = 2$, elle renvoie vraie, et $n \neq 2$ et n premier, on ne pouvait pas trouver un $\alpha \in L_n^{'}$ tel que $\alpha \notin L_n^{'}$ vu que $\mathbb{Z}_n^n = L_n^{'}$

Exercice 6.6 : Chiffrement RSA

1)Voire le script ci-joint. En effet nous avons pue generer une bi-cléfs, et ajouter a cela nous avons mplémenter la partie cryptage et decriptage RSA.

2)Explication :On utilise le théoréme des restes chinois pour optimiser le calcul.

On notera C le message chiffré reçu et M' le message déchiffré et celui-ci est calculé de la façon suivante :

$M' \equiv C^{\mathrm{d}}(mod n)$, ou d est l'exposent privé RSA et n le module RSA.

Ici nous avons noté le message dechiffré par M' et non M, pour mettre en exergue que nous n'avons pas encore démontré que l'on peut effectivement retrouver le message d'origine.

Donc nous allons effectuer les calcules suivant :

$M' \equiv C^{\mathrm{d}}(mod n)$

En fonction du message original

$M' \equiv M^{\mathrm{ed}}(mod n)$

L'idée est donc de montrer que M' est congru a M modulo n

Comme on a choisit d tel que le produit $ed \equiv 1(mod \phi(n))$, il existe un entier $k \in \mathbb{Z}$ tel que $ed = k\phi(n) + 1$. De plus , $n = pq$ avec p et q premiers, alors $\phi(n) = (p-1)(q-1)$; on peut alors ecrire :

$M' \equiv M^{\mathrm{k(p\text{-}1)(q\text{-}1)+1}}(mod n)$

M,par construction, est un entier naturel strictement plus petit que le module n. $n = pq$, avec p et q premiers. Le raisonnement suivant est effectué avec p, et doit être effectué de maniére symétrique avec q : M et p sont premiers entre eux, alors d'aprés le théoréme de Fermat $M^{(p-1)} \equiv 1(modn)$, donc en élevant la puissance $k(q-1)$ et en multipliant par M, on obtient :
$M^{k(p-1)(q-1)+1} \equiv M(modp)$ en raissonnant de manére symétrique pour q :
$M^{k(p-1)(q-1)+1} \equiv M(modq)$
En appliquant le *théoréeme des restes chinois* p et q premiers entre eux car premiers, et avec $n = pq$, il vient que
$M^{k(p-1)(q-1)+1} \equiv M(modn)$
-Si M et p ne sont pas premier entre eux, alors M est un multiple de p alors $M \equiv 0(modp)$, et en élevant *à* la puissance $k(p-1)(q-1)+1$,
$M^{k(p-1)(q-1)+1} \equiv 0(modp) \equiv M(modp)$
En raissonnant de manére symétrique avec q et en appliquant le *théoréme des restes chinois* on obtient :
$M^{k(p-1)(q-1)+1} \equiv M(modn)$
On a donc bien
$M' \equiv M^{k(p-1)(q-1)+1}(modn)$. Comme on a pris M inferieur *à* n, alors $M \equiv M(modn)$.
Donc le message dechiffré est bien identique au message d'origine.

Conclusion

La realisation des execices ci-dessus de meme que l'élaboration de ce present documents, nous on était trés profitable en terme d'enseignement theorique et pratique avec les programme que l'on a joint au document. La chronologie des exercercice est trés pertinante, les concéptes developper ici sont la continuité des concépte developper dans l'exercice precedant et ainsi de suite .

Sources

`https://fr.wikipedia.org/`

Bibliographie

- *Codage, cryptologie et application*
  Par Bruno Martin
- *Repére-Comprendre RSA*
  nico34-buffer, 13 Avril 2013