Rapport TIPE

AZZOUZI Hamza

2021/2022

1 Introduction

Mon TIPE se base essentiellement sur l'étude de quelques systèmes cryptographiques. La cryptographie est une science essentielle de nos jours, elle assure la protection des données mondiales. Bien que ce soit une science apparue a l'Antiquité, ce sont les mathématiques modernes qui l'ont révolutionnée. Je vais commencer dans une premier temps par présenter quelques techniques de cryptographie. Dans un second temps je vais étudier quelques tests de primalité ainsi que leurs preuves.

2 Premières techniques de cryptographie

2.1 La méthode par substitution

Une des méthodes les plus anciennes de cryptographie connue est la méthode César. Cette méthode était utilisée par l'empereur romain afin de pouvoir communiquer en toute sécurité. Elle consiste à créer un décalage de 3 lettres.

Une manière inspirée de la méthode César consiste à réaliser une bijection entre les lettres. En français par exemple, il y a 26! possibilités de chiffrage ($= Card(S_{26})$). Malgré le grand nombre de possibilités les ordinateurs peuvent déchiffrer des messages de ce genre. Pour cela il suffit de connaître la fréquence d'utilisation des lettres dans la langue chiffrée.

2.2 La méthode XOR

Le chiffrement en utilisant la méthode XOR utilise l'écriture binaire pour chiffrer. Pour chiffrer un texte normal on peut alors utiliser **ASCII** qui transforme chaque caractère en un nombre de 8bits.
Le principe du XOR (ou exclusif) est le suivant : *Pour* x,y $\in \{0,1\}^2$

$$x \oplus y = \begin{cases} 0 \text{ si x=y} \\ 1 \text{ sinon} \end{cases}$$

On peut alors crypter un message en utilisant comme clé un nombre de bits. Ainsi on aura :

$$E_k(m) = k \oplus m$$

La fonction de décryptage sera alors :

$$D_k(c) = k \oplus c$$

3 Cryptage asymétrique

Les méthodes citées dans le paragraphe d'avant demandent l'échange d'une clé secrète pour pouvoir échanger les messages.

L'article de Diffie-Hellmann *"New Directions in Cryptography"* publié en 1976 a été révolutionnaire au monde de la cryptographie. Ils introduisent dans cet article l'idée de la clé publique.

Description de l'échange :

1. Alice et Bob se mettent d'accord sur un très grand nombre premier p et une racine primitive de l'unité g. Cela représente le clé publique
2. Alice choisit un nombre a qu'elle garde secret. De même Bob choisit un nombre b secret
3. Alice(resp. Bob) calcule alors $A = g^a \, mod \, p$ (resp $B = g^b \, mod \, p$)
4. Enfin Alice(resp. Bob) calcule le nombre $A' = B^a \, mod \, p$ (resp $B' = A^b \, mod \, p$) et on a alors $A' = B'$ qui va constituer la clé secrète commune.

On remarque que l'échange suivant postule l'existence d'une racine primitive dans $\mathbf{F}_p^*$ *ie* un élément d'ordre $p-1$. On va alors démontrer le théorème suivant :

Théorème 3.1. $\mathbf{F}_p^*$ *est cyclique*

3.1 Méthode RSA

La fonction indicatrice d'Euler est la base de la cryptographie par la méthode de RSA dont le principe est le suivant :

— Le choix d'un grand entier $n = pq$(où p et q sont deux grands nombres premiers), et un nombre r
— L'application de chiffrement est :

$$c = E(m) = m^r \, mod \, n$$

— L'application de déchiffrement est :

$$D(m) = c^s \, mod \, n$$

De sorte que : $rs \equiv 1 \, [\varphi(n)]$

Le calcul des fonctions E et D se fait rapidement si on connaît r et s grâce à l'algorithme des calcul rapides des puissances. Le nombre s n'est connu que par le propriétaire. La connaissance de s demande alors celle de $\varphi(n)$. Or pour calculer $\varphi(n)$ il faut essentiellement décomposer n en facteurs premiers. Cependant il n'existe pas d'algorithme rapide pour le faire. La RSA permet d'autant plus de signer le message puisque le nombre s caractérise la personne qui a chiffré le message.

4 Tests de primalités

On a vu que les cryptosystèmes asymétrique reposent essentiellement sur la disposition de grands nombres premiers, d'où l'importance des test de primalités.

4.1 Test de Fermat

Un nombre n n'est pas premier ssi $\exists a \in (\mathbf{Z}/n\mathbf{Z})^*, a^{n-1} \not\equiv 1[n]$

4.2 Test de Miller Rabin

Le test de Fermat n'est pas très utilisé car il demande plusieurs opérations. Le test de Miller Rabin est un test probabiliste qui vérifie si un nombre est premier. Ce test ne permet pas d'assurer la primalité des nombres. Mais il s'avèrent que ce soit suffisant dans le domaine de la cryptographie.

Soit $p \in \mathbf{Z}^*$ un nombre premier impair et soit $a \in \mathbf{Z}/p\mathbf{Z}$ notons $p - 1 = 2^s t$ où t est impair et $o(a)$ l'ordre de a. Par le théorème de Fermat $o(a)|p-1$

— si $o(a) = t$ alors $a^t = 1(modp)$
— sinon il existe i et k impair divisant t tq $0 < i \leq s$ et $(a^k)^{2^i} = 1 \, mod \, p$ On a alors $(a^k)^{2^{i-1}} = -1 \, mod \, p$

Definition 4.1. *Témoin de Miller* Si un nombre $a \in \mathbf{Z}^*$ ne vérifie pas les conditions précédentes il est appelé témoin de Miller.

Le test de Miller Rabin repose sur la recherche des témoins de Miller. Il repose sur le théorème suivant qui affirment que si un nombre n'est pas premier, il y a "beaucoup" de témoins de Miller.

Théorème 4.1. *Théorème de Miller Rabin : Si n est un entier composé au moins 3 quarts des nombres entre 2 et n-2 sont des témoins de Miller.*

4.2.1 Démonstration du théorème de Miller Rabin

Si W est le nombre de témoins de Miller dans $\{1, 2, ..., n-1\}$ on va montrer que $\frac{W}{n-1} > \frac{3}{4}$ et donc dans $\{2, 3, , .., n-2\}$ est $\frac{W}{n-3} > \frac{W}{n-1} > \frac{3}{4}$

Théorème 4.2. *Si $n = p^\alpha$ pour p et α supérieurs à 2, Les nombres qui ne sont pas témoins de Miller Rabin sont solutions de $a^{p-1} = 1\,(mod\, n)$ et forment un groupe multiplicatif dans $(\mathbf{Z}/n\mathbf{Z})^*$*

Démonstration. Soit $a \in \{1, \dots, n\}$ un nombre qui n'est pas témoin de Miller. Puisque a est premier avec n on a alors $a^{\varphi(n)} = 1\,(mod\, n)$. Or a n'est pas un témoin de Miller donc on a alors $a^{n-1} = 1\, mod\, n$. Ainsi on $o(a)|(\varphi(n) \wedge (n-1)) = (p^\alpha(p-1) \wedge (p^\alpha - 1)) = p - 1$. On a alors $o(a)|p-1$ ie $a^{p-1} = \, mod\, n$.

Réciproquement si $a^{p-1} = 1\, mod\, n$ alors on écrit $p - 1 = 2^f l$ et $f \geq 1$ et l est impair. Or $p-1$ divise $p^\alpha - 1$ donc $n = 2^e k$ avec $e \geq f$ et $l|k$. On a de plus $a^{2^f l} = \, mod\, n$ donc $o(a^l) = 2^j$ où $j \in \{0, \dots f\}$

si j=0 alors $a^l = 1, mod\, n$ et donc $a^k = 1 \wedge, mod\, n$

On suppose alors $j \geq 1$ et notons $x = a^{2^{j-1} l}$ on a alors n divise $x^2 - 1$ mais ne divise pas $x - 1$ de sorte à ce que $n|(x-1)(x+1)$. Supposons que p divise $x-1$ et $x+1$ alors p divise leur différence et donc p divise 2 ce qui est exclu. Si on suppose de plus que p est premier avec $x+1$ on aura que n divise $x-1$ ce qui est aussi exclu . Donc p est premier avec $x-1$ et alors n divise $x+1$. On a alors $a^{2^{j-1} l} = -1\, mod\, n$, or $l|k$ donc $a^{2^{j-1} k} = -1\, mod\, n$. □

Au lieu de montrer que la proportion des témoins de Miller est supérieur à $\frac{3}{4}$, on va montrer que la proportion des "non témoins" de Miller est inférieure à $\frac{1}{4}$.

On commence par le cas où $n = p^\alpha$. D'après le théorème ci dessus les "non témoins" sont solutions de $a^{p-1} = -1\, mod\, n$.

Lemme 4.3. *Cette équation admet p-1 solution*

Il existe alors p-1 "non témoin" de Miller-Rabin pour p^α dans $\{1, \dots p^\alpha - 1\}$. Leur proportion est donc de :

$$\frac{p-1}{p^\alpha - 1} = \frac{1}{1 + p + \cdot + p^{\alpha-1}} \tag{1}$$

Comme $\alpha \geq 2$ la proportion est au plus $1/(1+p)$ qui est inférieure à $1/(1+3) = 1/4$

On suppose désormais que n a au moins deux facteurs premier et on écrit alors $n - 1 = 2^e k$ avec $e \geq 1$ et k impair. On note i_0 le plus grand entier dans $\{0, \dots, e-1\}$ tel qu'il existe un entier a_0 tel que $a \wedge n = 1$ et $a_0^{2^{i_0}} = -1\, mod\, n$. On montre alors le lemme suivant :

Lemme 4.4. *$G_n = \{1 \leq b \leq n - 1 / b^{2^{i_0} k} = \mp 1\, mod\, n\}$ est un groupe multiplicatif modulo n qui contient tous les "non témoins" de Miller Rabin et c'est un sous groupe strict des groupe des inversibles modulo n.*

Démonstration. On peut facilement montrer que G_n est un sous groupe des inversibles modulo n.
Soit a un nombre qui n'est pas témoin de Miller.
Premier cas : $a^k = 1\, mod\, n$. On a alors que $a^{2^{i_0} k} = 1\, mod\, n$ donc $a \in G_n$
Deuxième cas : On dispose de i tel que $a^{2^i k} = -1\, mod\, n$. Or par maximalité de i on a $i \leq i_0$. Si $i = i_0$ alors $a^{2^{i_0} k} = -1\, mod\, n$. Sinon en mettant les deux termes de l'égalité au carré le nombre suffisant de fois on obtient $a^{2^{i_0} k} = 1\, mod\, n$. et donc $a \in G_n$.

On montre alors que G_n est un sous groupe strict du groupe des inversibles modulo n. Soit p un nombre premier tel que $n = p^\alpha n'$, $\alpha \geq 1$ et p premier avec n' et $n' > 1$.

D'après le théorème des restes chinois, on dispose de $a \in \{1, \dots, n\}$ tel que

$$a = a_0\, mod n, p^\alpha\,,\ a = 1\, mod n \tag{2}$$

Comme $a_0 \wedge n = 1$ on a $a \wedge n = 1$. En regardant successivement modulo p^α puis modulo n', on a

$$a^{2^{i_0} k} = a_0^{2^{i_0} k} = (-1)^k = -1\, mod\, p^\alpha$$

et donc on a

$$a^{2^{i_0}k} \neq 1 \, mod \, n$$

on a de plus $a^{2^{i_0}k} = 1 \, mod \, n'$ donc $a^{2^{i_0}k} \neq -1 \, mod \, n$.
Ainsi $a \wedge 1 = 1$ t $a \notin G_n$. □

On peut alors démontrer le théorème de Miller Rabin :

Théorème 4.5. *théorème de Miller Rabin*
Si n est un entier composé, alors au moins 3 quarts des nombres entre 2 et n-2 sont des témoins de Miller.

Démonstration. Puisque n n'est pas premier on a $\varphi(n) < n-1$. Et d'après le lemme ci-dessus on aussi que $G_n | \varphi(n)$. On va essayer de montrer que $\varphi(n)/G_n \geq 4$. Et ainsi on aura que :

$$\frac{|\{Nombres \, qui \, ne \, sont \, pas \, temoins \, de \, Miller\}|}{n-1} = \frac{Card(G_n)}{n-1} < \frac{Card(G_n)}{\varphi(n)} \leq 1/4$$

J'admets qu'un nombre de Carmichael a au moins trois facteurs premiers. Ainsi soit n n'est pas un nombre de Carmichael, ou bien il admet au moins trois diviseurs premiers distincts.
Premier cas ; n n'est pas un nombre de Carmichael.
Posons

$$F_n = \{1 \leq a \leq n-1 \, / a^{n-1} = 1 \, mod \, n\}$$

On a alors F_n est sous groupe strict des inversibles modulo n. Donc d'après le théorème de Lagrange $Card(F_n) | \varphi(n)$ et alors $Card(F_n) \leq \varphi(n)/2$. De même on a que G_n est sous groupe de F_n. Il reste à montrer qu'il s'agit d'un sous groupe stricte. Pour cela on utilise le nombre dans (2). On a alors que $a \notin G_n$ et $a^{2^{i_0}k} = -1 \, mod \, p^\alpha$ et $a^{2^{i_0}k} = 1 \, mod \, n'$ donc $a^{2^{i_0+1}k} = 1 \, mod \, p^\alpha$ et alors $a^{2^{i_0}k} = 1 \, mod \, n$, ainsi $a \in F_n$. Donc $F_n \neq G_n$. On alors que :

$$Card(G_n) \leq card(F_n)/2 \leq \varphi(n)/4$$

Deuxième cas : n a au moins trois nombres premiers disctincts.
On écrit alors $n = p_1^{m_1} ... p_r^{m_r}$ sa décompositions en nombres premiers avec $r \geq 3$. Notons *

$$H_n = \{1 \leq a \leq n-1 / \, a^{2^{i_0}k} = \mp 1 \, mod p_l^{m_l} \, pour \, l \in \{1, ... \, r\}\}$$

On a que G_n est un sous groupe de H_n qui est un sous groupe du groupe des inversibles modulo n. On va alors montrer que $card(H_n) | card(G_n) \geq 4$ de sorte à ce que $\frac{\varphi(n)}{Card(G_n)} \geq \frac{Card(H_n)}{Card(G_n)} \geq 4$ On définit alors l'application $f : H_n \longrightarrow \prod_{l=1}^{r} \{\mp 1 \, mod p_l^{m_l}\}$ définie par :

$$f(a mod n) = (a^{2^{i_0}k} \, mod \, p_1^{m_1}, ... \, a^{2^{i_0}k} \, mod \, p_r^{m_r})$$

est un morphisme. Soit $K_n = ker f$ on a alors $K_n \subset G_n \subset H_n$. L'ensemble d'arrivée est de cardinal 2^r. Montrons que f est surjective. Comme f est un morphisme il suffit de montrer que les r-tuples $(1, ... \, 1, -1, 1, ... \, , 1)$ admettent des antécédents. Par symétrique il suffit de le prouver pour le r-tuple $(-1, 1, 1, ... \, , 1)$.

Par construction de i_0, on dispose de a_0 tel que $a^{2^{i_0}k} = -1 \, mod \, n$. D'après le théorème des restes chinois on dispose de $a \in \{1, ... \, n-1\}$ tel que :

$$a = a_0 \, mod \, p_1^{m_1}, \;\; a = 1 \, mod p_l^{m_l} \, pour \, l \geq 2$$

On a alors que $a^{2^{i_0}k} = a_0^{2^{i_0}k} = (-1)^k = -1 \, mod p_1^{m_1}$ et $a^{2^{i_0}k} = 1 \, mod p_l^{m_l} \, pour \, l \geq 2$. Ainsi $f(a \, mod \, n) = (-1, 1, ... \, , 1)$ et donc f est surjective.

On a que $card(H_n) = Card(K_n) Card(f(H_n))$ et f est surjective, donc $\frac{card(H_n)}{card(K_n)} = 2^r$ et de même $\frac{card(G_n)}{card(K_n)} = 2$ (car $Im(G) = \{(1, 1, ... \, 1), (-1, -1, ... \, , -1)\}$)
Ainsi $\frac{card(H_n)}{card(G_n)} = 2^{r-1}$. Or $r \geq 3$ donc $2^{r-1} > 4$ □

On vient de prouver le théorème de Miller Rabin.

4.2.2 Test de Miller Rabin

D'après le théorème ci dessus on peut énoncer les étapes du test de Miller-Rabin :

1. On choisit un nombre t qui représentera le nombre de test à effectuer
2. on choisit aléatoirement un nombre entre 2 et $n-2$
3. si a n'est pas un témoin de Miller on réitère l'opération
4. Si après t test le test n'est pas terminé on retourne *"n est premier avec une probabilité supérieure à* $1-\frac{1}{4^t}$ *"*

4.3 Test de Lucas-Lehmer

Si le test de Miller Rabin permet de tester si un nombre est premier de manière probabiliste. Le test de Lucas-Lehmer permet quant à lui de générer de grands nombres premiers. Ce test repose sur la primalité des nombres de Mersenne.

Definition 4.2. *Nombre de Mersenne* Un nombre de Mersenne est un terme de la suite $M_n = 2^n - 1$

Je vais commencer par énoncer des lemmes importants.

Lemme 4.6. *Si M_q est un nombre premier, alors q est premier.*

Démonstration. Par contraposée, si q n'est pas premier on écrit $q = mn0$ avec $m, n \geq 2$. On a alors $2^n - 1 | M_q$.

□

Lemme 4.7. *Pour tout entier k non nul, $M_{2k+1} = 7 \, mod \, 12$*

Lemme 4.8. *Morphisme de Frobenius Si p est un nombre premier alors $\forall a \in \mathbf{N}$*

$$(X+a)^p = X^p + a \quad mod(p)$$

Definition 4.3. *Symbole de Legendre*
Soit p premier.
Pour tout $a \in \mathbf{Z}$ non divisible par p le symbole de Legendre de a modulo p, noté $\left(\frac{a}{p}\right)$ est défini par :

$$\left(\frac{a}{p}\right) = \begin{matrix} \text{-1 si a n'est pas un carré modulo p} \\ 1 \qquad\qquad\qquad\qquad\quad \text{sinon} \end{matrix}$$

Si p divise a on pose $\left(\frac{a}{p}\right) = 0$

Lemme 4.9. *Critère d'Euler Soit p un nombre premier. Pour tout $a \in \mathbf{F}_p^*$ On a*

$$\left(\frac{a}{p}\right) = a^{(p-1)/2} \, mod \, p$$

Démonstration. Si $a = b^2$ dans $\mathbf{F}_p^*$, d'après le théorème de Fermat, on a donc $a^{(p-1)/2} = b^{p-1} = 1$.
Réciproquement, le polynôme $X^{(p-1)/2} - 1$, de degré $(p-1)/2$, a pour racines les $(p-1)/2$ carrés de $\mathbf{F}_p^*$ donc ce sont les seules, de sorte que pour tout a non carré dans $\mathbf{F}_p^*$, $a^{(p-1)/2} \neq 1$ mais son carré vaut 1. C'est donc -1.
On vient alors de démontrer le critère d'Euler □

Je vais admettre le résultat suivant qui sera utile dans ma démonstration.

Lemme 4.10. *Loi de réciprocité quadratique Pour tous nombre premiers impairs p, q distincts on a :*

$$\left(\frac{q}{p}\right)\left(\frac{p}{q}\right) = (-1)^{\frac{p-1}{2}\frac{q-1}{2}}$$

On peut alors énoncer une caractérisation de primalité des nombres de Mersenne.

Théorème 4.11. *Pour tout nombre premier impair q :*

$$M_q \, est \, premier \iff (2+\sqrt{3})^{2^{q-1}} = -1 \, mod \, M_q$$

On remarque qu'il faut se placer dans un corps où 3 admet une racine carrée. *On commence par prouver le sens direct*

Lemme 4.12. *3 est résidu quadratique modulo un entier premier p ssi* $p = \pm 1 \, mod \, 12$

Démonstration. Comme M_q n'est congru ni à 1 ni à -1 modulo 12, 3 n'est pas résidu quadratique modulo M_q. X^2-3 est donc irreductible sur $\mathbf{F}_{M_q}$, et donc $A = \mathbf{F}_{M_q}/(X^2-3)$ est un corps. On note $\sqrt{3}$ la classe de X dans A. On remarque de plus que $2^{q+1} = 2 \, mod \, M_q$, et donc 2 admet une racine carrée $\sqrt{2} = 2^{(q+1)/2}$ On définit les quantité

$$a = \frac{1+\sqrt{3}}{\sqrt{2}} \, et \, b == \frac{1-\sqrt{3}}{\sqrt{2}}$$

On montre facilement que $a^2 = 2+\sqrt{3}$ et $ab = -1$ De plus comme 3 n'est pas un résidu quadratique modulo M_q, par le critère d'Euler :

$$(\sqrt{3})^{M_q} = 3^{\frac{M_q-1}{2}}\sqrt{3} = -\sqrt{3}$$

Par le morphisme de Frobénius :

$$(1+\sqrt{3})^{M_q} = 1-\sqrt{3}$$

Comme $\sqrt{2}^{M_q} = \sqrt{2}$ on a $a^{M_q} = b$.
Ainsi on a :

$$(2+\sqrt{3})^{2^{q-1}} = (2+\sqrt{3})^{\frac{M_q+1}{2}} = (a^2)^{\frac{M_q+1}{2}} = ab = -1$$

□

Démonstration. du sens réciproque Je vais noter dans la suite $\mathbf{Z}_n$ l'anneau $\mathbf{Z}/n\mathbf{Z}$ Si $\mathbf{Z}_{M_q}$ contient une racine de 3 on note $A = \mathbf{Z}_{M_q}$, sinon on prend $A = \mathbf{Z}_{M_q}/(X^2-3)$ On suppose M_q est non premier, et on appelle p un de ses diviseurs premiers. p est donc un diviseur de 0 dans A, et a fortiori n'est pas inversible. Il est donc contenu dans un idéal maximal I par le théorème de Krull (admis). Alors A/I est un corps de caractéristique p. On appelle a (resp. b) la classe de $2+\sqrt{3}$ (resp. de $2-\sqrt{3}$) dans A/I On pose $Q = (X-a)(X-b) = X^2-4X+1$. C'est un polynôme à coefficient dans le corps premier de $A/I, \mathbf{F}_p$(Le plus petit sous corps de ce dernier).
Comme a est racine de Q d'après le lemme de Frobénius a^p l'est aussi, et donc $a^p = a$ ou $a^p = b$.
Notre hypothèse s'écrit $a^{2^{q-1}} = -1 \, mod \, M_q$ est on déduit que a est d'ordre 2^q dans A/I
Dans le premier cas, comme a est d'ordre 2^q, on a donc $2^q|(p-1)$ donc $p > 2^q$.D'où une contradiction.
Dans le second cas, $a^p = b = a^{-1} = a^{M_q}$ On a alors $p = 2^q - 1 \, mod \, 2^q$ ce qui impose que $p = M_q$. Ce qui est encore une contradiction. □

On peut alors citer le test de Lehmer-Lucas :

Théorème 4.13. *Soit la suite* $(s_n)_{n\in\mathbf{N}}$ *définie par récurrence :*

$$\begin{aligned} s_0 &= 4 \\ s_{n+1} &= (s_n)^2 - 2 \end{aligned}$$

Soit p un nombre premier impaire. M_p *est premier ssi* $M_p | s_{p-2}$

Démonstration. Soit A un anneau contenat $\sqrt{3}$. On écrit $a = 2+\sqrt{3}$ et $b = 2-\sqrt{3}$. On remarque de plus que $ab = 1$ On prouve alors par récurrence que $s_k = a^{2^k} + b^{2^k}$ Ainsi

$$M_q | s_{q-2} \iff a^{2^{k-2}} = -b^{2^{k-2}} \, mod \, M_q \iff (a^2)^{2^{k-2}} = -1 \, mod \, M_q \iff (2+\sqrt{3}^{2^{q-1}} = -1 \, mod \, M_q$$

□

4.3.1 Test de Lucas-Lehmer

On peut alors effectuer le test de ce Lucas-Lehmer :

1. choisir un entier naturel p qui est premier et impair
2. Calculer le nombre de Mersenne M_p
3. Calculer s_{p-2}
4. Evaluer le reste de la division euclidienne de s_{p-2} par M_p. S'il vaut 0 alors M_p est un nombre premier

5 Annexes

Sécurité de cet échange : . Il n'y a pas encore d'algorithme qui permet de résoudre le problème de Diffie-Helmann en un temps raisonnable.
Une manière de déchiffrer le problème de Diffie-Helmann est de résoudre le problème du logarithme discret. L'algorithme le plus efficace se fait en $e^{\left(\sqrt{1/2}+o(1)\right)\sqrt{\ln(n)\ln(\ln(n))}}$.
Si on suppose que l'ordinateur effectue chaque opération en une microseconde on obtient les résultats suivants :

Longueur du nombre	Nb d'opérations	Durée
100	$3.9x \times 0^6$	3 secondes
200	9.9×10^9	2.5 heures
500	1.3×10^{17}	3170 années

Sécurité du système RSA Supposons qu'Eve arrive à décrypter le message. Pour cela il faut qu'elle arrive à factoriser le nombre n. Jusqu'à présent l'algorithme le plus rapide pour factoriser un nombre se fait en $\mathcal{O}(e^{\sqrt{\ln(n)\ln(\ln(n))}})$.
En supposant que l'ordinateur prend environ une microseconde à chaque opérations on obtient les résultats suivants :

Longueur	Nb d'opérations	Durée
75	$9.0.10^{12}$	74 années
200	$1.2\ .10^{23}$	$3.8\ .10^9$ années
500	$1.3\ .10^{39}$	$4.2\ .10^{25}$ années

Ainsi en choisissant un nombre n très grand il est quasiment impossible de décrypter le message en un temps raisonnable.

Preuve de 3.1

Soit H un sous groupe de $\mathbf{F}_p^*$ de cardinal d. On a alors d'après le théorème de Lagrange : $\forall x \in H\, x^d = 1$ Ainsi on a : $H \subset$ {racines de $X^d - 1$ }. Or $\mathbf{F}_p$ est un corps alors Card({racines de $X^d - 1$})$\leq d$ Ainsi H= racines de $X^d - 1$ Il existe alors au plus un sous groupe de cardinal d. Notons pour $d|n\, \psi(d)$ le nombre d'éléments d'ordre d. On a alors $\sum_{d|n} \psi(d) = n$ Soit d diviseur de n tq $\psi(d) > 0$, il existe alors x $\in \mathbf{F}_p^*$ tq $ord(x) = d$ notons H le sous groupe engendré par x. H est cyclique et donc admet $\varphi(d)$ générateur. Comme H est l'unique sous groupe d'ordre d alors pour tout élément y d'ordre d ; y génère H. Ainsi $\varphi(d) = \psi(d)$. Dès lors on a pour tout $d|n$ $\psi(d) \leq \varphi(d)$

Comme $\sum_{d|n} \varphi(d) = n$, alors pour tout $d|n$ on a $\psi(d) = \varphi(d)$. En particulier $\psi(n) = \varphi(n)$ donc $\psi(n) > 0$. Ainsi $\mathbf{F}_p^*$ est cyclique

Preuve de 4.3 :

Pour $\alpha = 1$ cela est vrai d'après le théorème de Fermat.

On suppose $\alpha \geq 0$. Notons $n = p^{\alpha+1}$ et $m = p^\alpha$ Soit $a \in \mathbf{Z}$ tq $a^{p-1} = 1\, mod\, n$, on a alors $a \in \mathbf{Z}$ tq $a^{p-1} = 1\, mod\, m$. On montre alors que si a vérifie $a^{p-1} = 1\, mod\, m$, il existe un unique $a'\, mod\, n$ tq $a' = a\, mod\, m$ et $a'^{p-1} = 1\, mod\, n$. Pour cela il suffit de montrer qu'il existe un unique $c\, mod\, p$ tq $a' = a + cp^\alpha\, mod\, n$. D'après le binome de Newton on a

$$(a + cp^\alpha)^{p-1} = a^{p-1} + (p-1)a^{p-2}cp^\alpha\, mod\, n$$

on écrit de plus $a^{p-1} = 1 + p^\alpha M$ pour $M \in \mathbf{Z}$. On cherche alors c tel que :

$$(1 + +Mp^\alpha) + (p-1)a^{p-2}cp^{6\alpha} = 1\, mod\, n$$

Ceci est équivalent à

$$M = a^{p-2}c\, mod\, p$$

d'où l'unicité de c car a est premier avec p.

Preuve de 4.7

Démonstration. Par récurrence.

si k =1 le résultat est immédiat.

Soit $k \in \mathbf{N}^*$ .On suppose le résultat au rang k.

On a modulo 12 :

$$2^{2(k+1)+1} - 1 = 4 \times 2^{2k+1} - 1 = (2^{2k+1} - 1) \times 4 + 3 = 7 \times 4 + 3 = 7$$

□

Preuve de 4.12 Par la loi de réciprocité quadratique on a :

$$\left(\frac{3}{p}\right)\left(\frac{p}{3}\right) = (-1)^{\frac{p-1}{2}}$$

Ainsi 3 est un résidu modulo p ssi $\left(\frac{p}{3}\right) = (-1)^{\frac{p-1}{2}}$ On remarque que le seul carré non nul de $\mathbf{F}_3$ est 1, et donc 3 est résidu quadratique modulo p *ssi* l'une des deux conditions est vérifiée :

1. $p = 1\, mod\, 3$ et $(p-1)/2$ est pair.
2. $p = 2\, mod\, 3$ et $(p-1)/2$ est impair.

Dans le premier cas , p est congru à 1 modulo 3 et 4, donc à 1 modulo 12.
Dans le second cas, p est congru à 2 modulo 3, et 3 modulo 4, et donc d'après le théorème chinois, à -1 modulo 12.

Références

[1] Jeffrey hoffstein : An introduction to mathematical cryptography, 2008

[2] Whitfield Diffie and Martin E. Hellman :, New Directions in Cryptography, https ://www.cs.utexas.edu/ shmat/courses/cs380s_fall08/dh.pdf

[3] Evan Dummit,Cryptography (part 3) : Discrete Logarithms in Cryptography , 2016

[4] Pierre Rouchon, Arithmétique et Tests de Primalité, https ://studylibfr.com/doc/658008/arithm%C3%A9tique-et-tests-de-primalit%C3%A6

[5] KEITH CONRAD,The Miller Rabin test T,https ://kconrad.math.uconn.edu/blurbs/ugradnumthy/millerrabin.pdf

[6] Philippe Saux Piccart, Eric Rannou, Primalité des nombres de Mersennes.