



- UNIVERSITÉ DE BOURGOGNE FRANCHE-COMTÉ -
3ÈME ANNÉE DE LICENCE
UFR SCIENCES ET TECHNIQUES



Tests de primalité
Tests de factorisation d'entiers

RAPPORT

Rédigé par PIARD Arthur, ROBINO Justine, PANTALEON Olivia.

Table des matières

1	Histoire du chiffrement RSA.	2
1.1	Comment le chiffrement RSA a été créé?	2
1.2	Et pourquoi?	3
2	Fonctionnement du chiffrement RSA.	3
2.1	Principes mathématiques	3
3	« Breaking » du chiffrement RSA et difficultés liées à sa casse.	8
3.1	Notre méthode pour les « petits » nombres.	8
3.2	Autre point de vue avec des méthodes plus puissantes.	11
3.2.1	Analyse	16
4	Une autre méthode de chiffrement	17
4.1	L'AES	17
4.1.1	Un peu d'histoire	17
4.1.2	Comment fonctionne-t-il?	17
4.1.3	Explications diverses	18
4.1.4	Analyse	20
4.2	Conclusion	21

1 Histoire du chiffrement RSA.



FIGURE 1 – Ron Rivest, Adi Shamir, Len Adleman

1.1 Comment le chiffrement RSA a été créé?

Le chiffrement RSA tient son nom de ses trois inventeurs : Ronald Rivest, Adi Shamir et Leonard Adleman. Il a été créé en 1977, breveté en 1983. Le RSA a comme spécificité générale son chiffrement asymétrique. En effet, le chiffrement RSA utilise une clé publique qui permet le chiffrement et une clé privée qui permet le déchiffrement. Si l'on modélise le chiffrement RSA à deux individus qui s'échangent des mails : La personne X transmet la clé publique à d'autres personnes qui l'utiliseront afin de chiffrer leurs messages. La personne X utilisera la clé privée afin de décrypter les messages cryptés pour en connaître le contenu. La clé privée peut-être elle aussi utilisée afin de vérifier l'identité de quelqu'un via une donnée cryptée que l'on peut vérifier par la clé publique.

Fonctionnement général :

Le chiffrement RSA est l'exemple le plus courant de cryptographie asymétrique. L'idée générale était de trouver deux fonctions f et g sur les entiers, telles que $f \circ g = Id$, et telles que l'on ne puisse pas trouver f , la fonction de décryptage, à partir de g , la fonction de cryptage. L'on peut alors rendre publique la fonction g (ou clé), qui permettra aux autres de crypter le message à envoyer, tout en étant les seuls à connaître f , donc à pouvoir décrypter.

1.2 Et pourquoi?

Le chiffrement RSA a été créé afin de permettre de crypter des informations de tous type (signature de mails, identifications bancaires, transmissions sécurisées d'informations confidentielles ...) dans le but de garantir la confidentialité d'une information pendant un laps de temps conséquent (plusieurs dizaines d'années dans certains type de chiffrement RSA).

2 Fonctionnement du chiffrement RSA.

2.1 Principes mathématiques

Le chiffrement RSA repose globalement sur les congruences, il utilise de nombreux théorèmes d'arithmétique, en particulier le petit théorème de Fermat, le théorème d'Euler. Nous allons d'abord rappeler quelques résultats d'arithmétique élémentaires très utiles et importants.

Définition 2.1. Un nombre $p \in \mathbb{N}$ est premier si ses seuls diviseurs sont 1 et lui même p .

Théorème 2.1. Soit $n \in \mathbb{N}^*$. Si $n = ab$ alors n est premier $\Leftrightarrow a = 1$ ou $b = 1$.

Théorème 2.2. *Tout entier n supérieur à 2 possède au moins un diviseur premier.*

Démonstration. Soit n un entier naturel différent de 1. L'ensemble des diviseurs de n strictement supérieur à 1 n'est pas vide, il contient n , donc cet ensemble possède un plus petit élément que l'on note d . Si a est un diviseur de d strictement supérieur à 1 alors $a \leq d$. Mais puisque a divise d et que d divise n alors par transitivité de la relation d'équivalence \mathcal{R} : "divise" on a a divise n . Donc $d \geq a$ d'où on a finalement $a = d$ et les seuls diviseurs positifs de a sont 1 et d . \square

Théorème 2.3. *Un nombre premier n est premier avec tout nombre qu'il ne divise pas.*

Démonstration. Si p premier ne divise pas n , l'ensemble des diviseurs de p dans \mathbb{N} est $\{1, p\}$ hors le seul diviseur commun à p et n ne peut être que 1. \square

Théorème 2.4. (Égalité de Bézout) *Soit a et b deux entiers naturels non nuls et $D = \text{pgcd}(a, b)$. Il existe alors un couple (u, v) d'entiers relatifs tels que : $au + bv = D$.*

Démonstration. On note G l'ensemble formé par les entiers naturels strictement positifs de la forme $ma + nb$ où m et n sont des entiers relatifs. G est une partie non vide de \mathbb{N} , en effet on vérifie aisément que $|a| \in G$ donc G admet un plus petit élément d tel que $d = au + bv$.

Premièrement, $D = \text{pgcd}(a, b)$ divise a et b donc D divise $d = au + bv$ donc $D \leq d$. De plus, si on divise a par d alors $a = d + r$ avec $0 \leq r \leq d$. D'où $r = a - dq = a - auq - bvq = a(1 - uq) + b(1 - vq)$, de plus si $r \neq 0$ alors on aurait $r \in G$, or $r \leq d$ et d est le plus petit élément de G ce qui est absurde, donc $r = 0$. Puisque $r = 0$ alors d divise a . Par un raisonnement **strictement** analogue on montre que d divise b . D'où d divise a et b donc $d \leq D$. On a alors $d = D$, donc tout diviseur commun à a et b divise leur pgcd. \square

Théorème 2.5. (de Gauss) *Soient a, b, c trois entiers naturels. Si a divise le produit bc et si a est premier avec b alors a divise c .*

Démonstration. On a $\text{pgcd}(a, b) = 1$ alors, par le Théorème de Bézout, on a : $au + bv = 1$ avec $(u, v) \in \mathbb{Z}^2$. De plus si a divise bc alors $bc = aq$ avec $q \in \mathbb{Z}$. D'où :

$$\begin{aligned} au + bv = 1 &\Rightarrow auc + bvc = c \\ &\Rightarrow auc + aqv = c \\ &\Rightarrow a(uc + vq) = c \end{aligned}$$

Donc a divise c . □

Théorème 2.6. Si un nombre premier divise un produit de facteurs premiers, alors il est égal à l'un d'eux.

Théorème 2.7. Si p est premier, alors p divise ab implique p divise a ou p divise b .

Démonstration. Si p ne divise pas a , alors p est premier avec a , donc divise b d'après le théorème de Gauss. □

Théorème 2.8. (Fondamental)

Soit n un entier naturel strictement supérieur à 1. Alors :

- il existe k nombres premiers naturels p_1, p_2, \dots, p_k deux à deux distincts et des entiers naturels non nuls $\alpha_1, \alpha_2, \dots, \alpha_k$ tels que :
 $n = p_1^{\alpha_1} \cdot \dots \cdot p_k^{\alpha_k}$.
- Cette décomposition est unique à l'ordre des facteurs près, i.e :

$$n = p_1^{\alpha_1} \cdot \dots \cdot p_k^{\alpha_k}$$

entraîne $k = m$ et l'existence d'une permutation σ de $\mathbb{N}_k = \{1, \dots, k\}$ telle que $q_i = p_{\sigma(i)}$ et $\beta_i = \alpha_{\sigma(i)}$ pour tout i .

Démonstration. L'existence et l'unicité se montrent par récurrence sur n . **Existence :** Si $n = 2$, $(p_1, \alpha_1) = (2, 1)$, n possède au moins un diviseur premier p d'après le **Théorème 2.2**, on peut écrire $n = pm$ avec $m \leq n$. Si $m = 1$, on a le résultat. Sinon on applique l'hypothèse de récurrence à m pour obtenir une décomposition de m et donc de n .

Unicité : Elle est acquise si $n = 2$ puisque $2 = q_1^{\beta_1} \dots q_m^{\beta_m}$ montre que q_i divise 2 pour tout i , autrement dit, $m = 1$, $q_1 = 2$ et $\beta_1 = 1$. Supposons que l'unicité soit démontrée jusqu'au rang n et considérons :

$$n + 1 = p_1^{\alpha_1} \cdot \dots \cdot p_k^{\alpha_k} = q_1^{\beta_1} \cdot \dots \cdot q_m^{\beta_m}; 546, 1, 1000; q_m^{\beta_m}$$

avec $\alpha_1, \dots, \alpha_k, \beta_1, \dots, \beta_m \in \mathbb{N}^*$, et où les $p_1, \dots, p_k, q_1, \dots, q_m \in \mathbb{N}$ sont premiers p_k divise $q_1^{\beta_1} \dots q_m^{\beta_m}$, donc divisera l'un des q_i d'après le **Théorème 2.6**, par exemple, p_k divise q_m . Comme p_k est premier alors $p_k = q_m$ et

$$\frac{n+1}{p_k} = p_1^{\alpha_1} \cdot \dots \cdot (p_k^{\alpha_k})^{-1} = q_1^{\beta_1} \cdot \dots \cdot (q_m^{\beta_m})^{-1}.$$

On applique l'hypothèse de récurrence à cette décomposition en distinguant deux cas pour que les exposants soient tous strictement positifs :

- Si $\alpha_k = 1$ alors $\beta_m = 1$, autrement q_m diviserait l'un des p_i avec $i \neq k$ ce qui serait absurde.
- Si $\alpha_k \geq 1$ alors $\beta_m \geq 1$, autrement p_k diviserait l'un des q_i avec $i \neq m$ ce qui serait absurde.

Ces récurrences terminent la démonstration. □

A la base de l'arithmétique et du chiffrement se loge le **Petit Théorème de Fermat**. Il a de grandes applications autant en cryptographie qu'en arithmétique et est aussi puissant qu'il est élégant. Mais avant de définir ce théorème nous allons définir la base même de l'arithmétique dans \mathbb{Z} , les congruences.

Définition 2.2. Soient a, b deux entiers relatifs et n un entier strictement plus grand que 2. On dit que " a est congru à b modulo n " si a et b ont le même reste dans la division euclidienne par n .

On note alors : $a \equiv b \pmod{n}$ ou $a \equiv b \pmod{n}$.

Théorème 2.9. Soient a, b deux entiers relatifs et n un entier naturel strictement plus grand que 1. On a : $a \equiv b \pmod{n} \Leftrightarrow n$ divise $(a - b)$.

Démonstration. Sens direct : Soient a et b congrus modulo n . Il existe alors q et r entiers relatifs tels que : $a = n \cdot q + r$ avec $0 \leq r < n$. b ayant le même reste il existe q' entier relatif tel que $b = n \cdot q' + r$. D'où $a - b = n \cdot q - n \cdot q' = n \cdot (q - q')$. Donc n divise $(a - b)$.

Sens réciproque : Supposons que n divise $(a - b)$. Alors il existe k entier relatif tel que $a - b = nk$. Soit r le reste de la division euclidienne de a par n : $a = n \cdot q + r$ avec $0 \leq r < n$. Alors $b = a - nk = n \cdot (q - k) + r$ avec $0 \leq r < n$ et $q - k$ entier relatif. Donc r est le reste de la division de b par n . Puisque a et b ont le même reste, alors $a \equiv b \pmod{n}$. □

Théorème 2.10. (Petit Théorème de Fermat)

Soit $a \in \mathbb{N}$, p un nombre premier, on a alors : $a^p - a \equiv 0 \pmod{p}$

Démonstration. On note l'hypothèse de récurrence $H_a : a^p - a \equiv 0 \pmod{p}$.

Initialisation :

Pour $a = 0$ on a, $0^p - 0 = 0 \equiv 0 \pmod{p}$, donc H_0 est vraie.

Hérédité, pour $a + 1$:

$$(a + 1)^p - (a + 1) = \sum_{k=0}^p \binom{p}{k} a^k - (a + 1) = \left(\sum_{k=1}^{p-1} \binom{p}{k} a^k \right) + a^p - a.$$

Or $\binom{p}{k} = \frac{p!}{k!(p-k)!}$ avec $k \in \llbracket 1; p-1 \rrbracket$, ainsi que : $k < p$ et $p-k < p$. D'où puisque p est premier, il n'est pas divisible par les diviseurs de $k!$ ou $(p-k)!$. On en déduit alors que $\binom{p}{k}$ mais aussi $\sum_{k=1}^{p-1} \binom{p}{k} a^k$ sont divisibles par p .

En outre on a aussi que, par hypothèse, $a^p - a$ est aussi divisible par p . On a alors : $(a + 1)^p - (a + 1)$ est divisible par p . D'où $H_a \implies H_{a+1}$, c'est à dire que $\forall a \in \mathbb{N}$, H_a est vraie. \square

Le chiffrement utilise des calculs modulo un entier n qui est le produit de deux nombres premiers. Le message crypté et non crypté sont des entiers inférieurs à l'entier n précédent. Les différentes opérations de chiffrement consistent à de l'exponentiation modulaire, on élève le message à une certaine puissance modulo n . En effet :

Les problèmes d'exponentiation modulaires reviennent à résoudre, pour une base b donnée, un exposant e et un entier m , on souhaite calculer c tel que : $c \equiv b^e \pmod{m}$. Si b, e, m sont tous positifs ou nuls avec $b \leq m$, alors il existe une unique solution notée c tel que : $0 \leq c \leq m$. En effet, prenons le cas simple suivant avec $b = 5, e = 3$ et $m = 13$. On cherche c tel que $c \equiv 5^3 \equiv 125 \equiv 8 \pmod{13}$. D'où $c = 8$. Concernant le petit théorème de Fermat, il donne une condition nécessaire pour qu'un nombre soit premier. Il faut en effet que, pour

tout a plus petit que p , a^p soit congru à a modulo p . Ce principe est la première approche du test de primalité de Fermat, d'autres méthodes pour tester la primalité d'un nombre existent (certaines découlent directement de celle de Fermat) mais c'est celle-ci qui est utilisée pour le chiffrement RSA.

3 « Breaking » du chiffrement RSA et difficultés liées à sa casse.

3.1 Notre méthode pour les « petits » nombres.

Nous allons traiter ici un exemple avec des "petits" nombres :

On se donne une clé publique : (10142789312725007, 5) ainsi que la clé privée : (10142789312725007, 8114231289041741).

On pose $n = 10142789312725007$ et $e = 5$, avec n le module et e publique. De plus on définit $d = 8114231289041741$ qui est l'exposant de décryptage.

On peut « casser » le chiffrement RSA en cherchant comment factoriser n avec ses p^{ieme} et q^{ieme} facteurs premiers, i.e, on veut écrire $n = p * q$. On prend ensuite la racine carré de n , ce qui nous donne 100711415. On cherche le premier nombre impair suivant telle que n soit congru à ce nombre :

$$10142789312725007 \equiv 100711367 \pmod{100711415}$$

$$10142789312725007 \equiv 100711373 \pmod{100711413}$$

$$10142789312725007 \equiv 100711387 \pmod{100711411}$$

$$10142789312725007 \equiv 0 \pmod{100711409}$$

On a alors $p = 100711409$. D'où :

$$\begin{aligned}
q &= \frac{n}{p} \\
&= \frac{10142789312725007}{100711409} \\
&= 100711423
\end{aligned}$$

d est un nombre spécial, en effet il doit vérifier :

$$d \equiv \frac{1}{e} \pmod{\phi(n)}$$

Où $\phi(n)$ est l'indicatrice d'Euler. Ce nombre existe bien en effet :

Théorème 3.1. (Euler)

Pour tout entier naturel $n \in \mathbb{N}^*$ et tout entier naturel a premier avec n , autrement dit, inversible modulo n , on a : $a^{\phi(n)} \equiv 1 \pmod{n}$

Démonstration. Nous travaillerons modulo n dans cette preuve et ne différencierons donc pas deux nombres qui sont égaux modulo n .

On note $\mathbf{A} = \{a_1, a_2, \dots, a_k\}$ l'ensemble des entiers de $\{0, 1, \dots, n-1\}$ qui sont premiers avec n . On a donc $\#\mathbf{A} = \phi(n)$ par définition de la fonction indicatrice d'Euler, d'où $k = \phi(n)$. On remarque que si l'on multiplie par l'élément a (de l'énoncé du théorème) les éléments de \mathbf{A} , les éléments de \mathbf{A} sont simplement permutés. On a alors : $\mathbf{A} = \{aa_1, aa_2, \dots, aa_k\}$. En effet, si $a_j \equiv 1 \pmod{n}$ alors $aa_j \equiv 1 \pmod{n}$ puisque a est premier avec n . On remarque de plus que deux éléments a_i et a_j distincts, lorsqu'ils sont multipliés par a restent distincts, en effet : par l'absurde, on aurait : $aa_i = aa_j$ ce qui donnerait $a_i = a_j$ en multipliant par a^{-1} des deux côtés, ce qui est contradictoire. Les éléments de \mathbf{A} étant exactement les mêmes que ceux de $\{aa_1, aa_2, \dots, aa_k\}$, multiplier les éléments de \mathbf{A} entre eux revient à multiplier ceux de $\{aa_1, aa_2, \dots, aa_k\}$ entre eux.

On a donc :

$$\begin{aligned}
a_1 \cdot a_2 \cdot \dots \cdot a_k &\equiv aa_1 \cdot aa_2 \cdot \dots \cdot aa_k \pmod{n} \\
&\equiv a^k \cdot a_1 \cdot \dots \cdot a_k \pmod{n}
\end{aligned}$$

De plus les éléments, a_1, \dots, a_k étant tous inversibles on peut multiplier les deux membres de cette égalité par $a_1^{-1} \cdot \dots \cdot a_k^{-1}$ pour obtenir : $1 \equiv a^k \pmod{n}$.
On a donc le résultat attendu, puisque $k = \phi(n)$. \square

D'où, en reprenant notre raisonnement nous avons :

$$\begin{aligned} d &= \frac{1}{e} \pmod{\phi(n)} \\ &= \frac{1}{e} \pmod{(p-1) \cdot (q-1)} \end{aligned}$$

Théorème 3.2. Soient p et q deux nombres premiers distincts.
Alors $\phi(n) := \phi(pq) = (p-1) \cdot (q-1)$.

Démonstration. Pour calculer $\phi(pq)$, il nous suffit de calculer le nombre d'entiers compris entre 1 et pq qui ne sont pas premiers à pq . Ce sont les multiples respectifs de p et q . Or il y a exactement q multiples de p dans l'intervalle $\llbracket 1 ; pq \rrbracket$, ainsi que p multiples de q . A noter que l'entier pq a donc été compté 2 fois, il faut donc le retirer. Le nombre d'entiers non premiers à pq dans l'intervalle $\llbracket 1 ; pq \rrbracket$ est donc $p + q - 1$. D'où il vient : $\phi(pq) = pq - (p + q - 1) = (p-1) \cdot (q-1)$. \square

On vérifie alors que : $d \cdot e = 40571156445208705 \equiv 1 \pmod{10142789111302176}$
Ceci est important, en effet, si vous avez un message crypté, noté m , le message décrypté vérifie : $c \equiv m^e \pmod{n}$, où c est le message crypté. D'où :

$$\begin{aligned} c &\equiv m^e \pmod{n} \\ &\equiv (123456789)^5 \pmod{10142789312725007} \\ &= 7487844069764171 \end{aligned}$$

Maintenant il nous est possible d'échanger c et d , en effet :

$$\begin{aligned} m &\equiv c^d \pmod{n} \\ &\equiv (7487844069764171)^{8114231289041741} \pmod{10142789312725007} \\ &= 123456789 \end{aligned}$$

Nous trouvons finalement le message décodé qui est $m = 123456789$.

3.2 Autre point de vue avec des méthodes plus puissantes.

La méthode de Fermat

Tout d'abord nous allons définir les nombres friables :

Définition 3.1. Soit $n \in \mathbb{N}$, n est qualifié de p -friable ou p -lisse si n est un produit d'entiers inférieurs ou égaux à n .

Fermat a, habilement, remarqué que pour trouver un facteur non trivial d'un entier n il suffit de l'écrire comme une différence de deux carrés.

On pose alors $n = x^2 - y^2 = (x - y)(x + y)$. S'il est possible d'écrire un multiple de n comme différence de deux carrés, il est alors possible de trouver un facteur non trivial de n . En effet, si $x^2 \equiv y^2 \pmod{n}$ alors on peut penser que le pgcd de n et $x - y$ est non trivial. Afin de trouver des solutions non triviales à la congruence suivante :

$$x^2 - y^2 \equiv 0 \pmod{n}$$

on ne peut pas faire mieux que de chercher des congruences entre des nombres friables à carrés près, i.e :

$$\prod_i p_i \equiv x^2 \pmod{n}.$$

où x est un entier et les p_i sont des nombres premiers plus petits qu'une borne B prédéfinie. Une fois muni de nombreuses relations telles que ci-dessus, on peut, par élimination linéaire (système d'équations modulaire), obtenir une congruence entre deux carrés. Le crible linéaire de Dixon et le crible quadratique, que nous allons présenter plus bas, sont eux-même basés sur la méthode de Fermat.

Le crible linéaire de Dixon

Définition 3.2. Un entier naturel q est appelé résidu (quadratique) modulo p s'il existe un entier x tel que :

$$x^2 \equiv q \pmod{p}$$

Nous allons maintenant expliquer cette méthode au travers d'un exemple.

Principe général :

On choisit arbitrairement un résidu x modulo n et on calcule y , le reste de la division euclidienne de x^2 par n . On a alors $x^2 \equiv y \pmod{n}$. Soit alors B une borne quelconque donnée. On aimerait que y soit B -friable, si c'est le cas on obtient alors une congruence entre un carré et un entier B -friable. Sinon on collecte suffisamment de telles relations et on termine selon le principe général exposé ci-dessus.

Application :

On suppose que l'on veut factoriser $n = 7081$. On choisit $B = 3$. Les nombres B -friables sont alors les entiers de type $\pm 2^a 3^b$. Après quelques essais nous trouvons :

$$4486^2 \equiv -2 \cdot 3 \pmod{n},$$

$$1857^2 \equiv 2 \pmod{n},$$

$$2645^2 \equiv -3 \pmod{n}.$$

On associe alors à ces trois congruences la matrice de $\mathcal{M}_3(\mathbb{F}_2)$ suivante :

$$\begin{array}{c|ccc} & -1 & 2 & 3 \\ \hline 4486 & 1 & 1 & 1 \\ 1857 & 0 & 1 & 0 \\ 2645 & 1 & 0 & 1 \end{array}$$

ce qui nous donne la matrice suivante :

$$\mathcal{E} = \begin{pmatrix} 1 & 1 & 1 \\ 0 & 1 & 0 \\ 1 & 0 & 1 \end{pmatrix}$$

On vérifie aisément que la ligne $[1, 1, 1] \in \mathbb{F}_2^3$ est annulée par la matrice. On en déduit alors la congruence entre les deux carrés suivant :

$$(4486.1857.1645)^2 \equiv (-2.3)^2 \pmod{n}.$$

De plus le pgcd de n et $4486.1857.2645 + 6$ est 73. On a alors trouvé un facteur non trivial.

Le crible quadratique

Principe général :

Il s'agit d'un raffinement de la méthode du Crible de Dixon, cet algorithme est dû à Carl Pomerance. Le but est d'établir une congruence de carrés modulo n qui est l'entier à factoriser, et qui, bien souvent conduit à une factorisation de n . Il y a deux étapes, la première qui est une collecte de différentes congruences qui peuvent conduire à une congruence de carrés. Puis enfin on place tous nos résultats dans une matrice et on la résout afin d'obtenir une congruence de carrés.

Application :

On définit

$$n = 21311 = 101.211$$

le nombre que l'on souhaite factoriser. On choisit m un entier proche de la racine carrée de n , par exemple :

$$m = \mathbf{E}(n^{\frac{1}{2}}) = 146, \text{ où } \mathbf{E}(x) \text{ désigne la fonction partie entière de } x.$$

On forme alors des congruences modulo n en remarquant que, quelque soit l'entier a ,

$$(m + a)^2 \equiv (m^2 - n) + a^2 + 2am \pmod{n} \equiv 5 + a^2 + 292a \pmod{21311},$$

où l'on remarque de plus que $m^2 - n$ est de l'ordre de \sqrt{n} . On se donne alors une borne $B = 13$ et l'on va chercher de petits entiers a tels que $5 + a^2 + 292a$ soit B -friable. Par exemple pour $-60 \leq a \leq 60$ on trouve :

a	$5 + 292a + a^2$
-27	$-2.5^2.11.13$
-5	$-2.5.11.13$
-1	$-2.11.13$
0	5
60	$5^3.13^2$

On porte alors dans une matrice la parité des valuations, ce qui nous donne :

	-1	2	5	11	13
-27	1	1	0	1	1
-5	1	1	1	1	1
-1	1	1	0	1	1
0	0	0	1	0	0
60	0	0	1	0	0

On forme alors des carrés à partir des lignes annulées par cette matrice (exactement comme pour la méthode de Dixon). L'ensemble de ces lignes est un espace vectoriel dont une base est donnée par les trois lignes de la matrice suivante :

-27	-5	-1	0	60
1	0	1	0	0
1	1	0	1	0
1	1	0	0	1

La première ligne du tableau nous donne la congruence suivante :

$$(2.5.11.13)^2 \equiv (146 - 27)^2 \cdot (146 - 1)^2 \pmod{21311}.$$

On calcule alors le pgcd de $2.5.11.13 \cdot (146 - 27) \cdot (146 - 1) = -15825$ et 21311. On trouve alors le facteur non trivial $p = 211$ de $n = 21311$ et son cofacteur est 101. Il est évident que p et q sont premiers.

3.2.1 Analyse

La différence à noter avec la méthode de Dixon réside dans la manière de trouver les relations de congruences. En effet, dans le crible de Dixon, le résidu x^2 modulo n est un entier entre 1 et $n - 1$, il faut espérer que cet entier est friable. Tandis que dans le crible quadratique le nombre supposé friable est de l'ordre de \sqrt{n} . La probabilité de succès est donc plus forte. Nous avons donc vu trois méthodes, toutes différentes, mais qui permettent de répondre à notre problématique, **la factorisation d'entiers**, à noter que le crible quadratique, comme le crible de Dixon, même si leurs utilisations sont laborieuses, sont efficaces pour trouver les facteurs d'un nombre entiers. Ces méthodes là mènent au crible algébrique (en anglais Number Field Sieve) qui est une méthode redoutablement puissante qui a d'ailleurs fait ses preuves, en effet, le système de chiffrement RSA-768, a été brisé par une méthode de factorisation de nombre de 1061-bits grâce justement à la méthode du crible algébrique. Son explication mathématique, précise et rigoureuse sort très rapidement du cadre et serait bien trop longue à expliquer ici.

4 Une autre méthode de chiffrement

4.1 L’AES

Nous allons maintenant définir et décrire dans les grandes lignes une méthode de chiffrement symétrique :

Le chiffrement AES-256

4.1.1 Un peu d’histoire

Le chiffrement AES (Advanced Encryption Standard) est l’algorithme de chiffrement le plus utilisé et le plus sûr disponible aujourd’hui. Lors de son arrivée dans le monde public il a suscité beaucoup d’intérêts en particulier pour la NSA, qui l’utilise encore aujourd’hui pour chiffrer des documents portant mention **secret défense**. La première version de chiffrement AES a débuté en 1997 lorsque le N.I.S.T (National Institute of Standards and Technology, agence du département du Commerce des États-Unis) a décidé de trouver un successeur à un algorithme plus ancien, le DES (Data Encryption Standard). Ce premier algorithme se fera nommé **Rijndael** en l’honneur de ses créateurs : les chercheurs Belges Daemen et Rijmen. Après plusieurs évolutions du **Rijndael**, l’**AES** va voir le jour. En effet, l’algorithme **Rijndael** va devenir officiellement la norme de cryptage **AES** après une victoire écrasante sur ses concurrents lors d’une compétition internationale organisée en 2001.

4.1.2 Comment fonctionne-t-il ?

L’algorithme prend en entrée un bloc de 128 bits (16 octets), la clé fait 128, 192 ou 256 bits. Les 16 octets en entrée sont permutés selon une table définie au préalable. Ces octets sont ensuite placés dans une matrice de taille 4x4 et ses lignes subissent une rotation vers la droite. L’incrément pour la rotation varie selon le numéro de la ligne. Une transformation linéaire est ensuite appliquée sur la matrice, elle consiste en la multiplication binaire de chaque élément de la matrice avec des polynômes issus d’une matrice auxiliaire, cette multiplication est soumise à des règles spéciales selon $\mathcal{GF}(2^8)$ (groupe de Galois ou corps fini). La transformation linéaire garantit une meilleure diffusion (propagation des bits

dans la structure) sur plusieurs tours. Finalement, un OU exclusif (XOR) entre la matrice et une autre matrice permet d'obtenir une matrice intermédiaire. Ces différentes opérations sont répétées plusieurs fois et définissent un « tour ». Pour une clé de 128, 192 ou 256, l'AES nécessite respectivement 10, 12 ou 14 tours. A chaque tour, une clé unique est calculée à partir de la clé de cryptage et incorporée dans les calculs. L'algorithme prend en entrée un bloc de 128 bits (16 octets), la clé fait donc entre 128, 192 ou 256 bits.

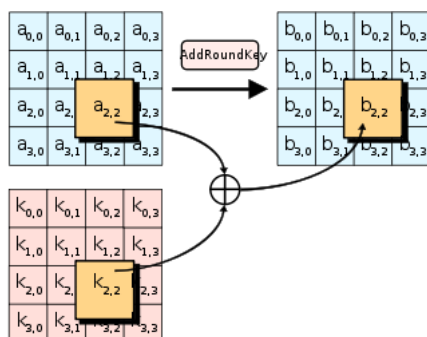
4.1.3 Explications diverses

L'explication rigoureuse serait très longue c'est pourquoi nous allons expliquer le fonctionnement le plus simplement possible des différentes étapes.

1^{ère} étape « Key Expansion » : préparation des clés

Le but de cette étape est d'utiliser la clé secrète d'origine afin de dériver une série de nouvelles clés appelés "round keys" à l'aide de l'algorithme de Rijndael pour la préparation des clefs. Le chiffrement AES nécessite un block de "round keys" de 128 bits pour chaque tour.

2^{ème} étape « AddRoundKey » : Ajout de la clé au premier tour



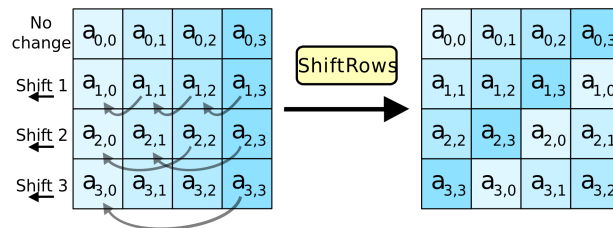
Un premier mélange. Chaque "round key" est combinée avec le texte à crypter à l'aide de l'opérateur **XOR** (ou exclusif).

3^{ème} étape « SubBytes » : Substitution

Une étape de substitution non linéaire où chaque octet est remplacé par un autre selon une table de correspondance prédéfinie. Chaque octet $a_{i,j}$ dans la matrice est remplacé par un SubByte $S(a_{i,j})$ en utilisant une substitution sur 8 bits. Cette opération fournit la non-linéarité du chiffre. La S-box utilisée est dérivée de l'inverse multiplicatif sur $\mathcal{GF}(2^8)$, connu pour avoir de bonnes propriétés de non-linéarité.

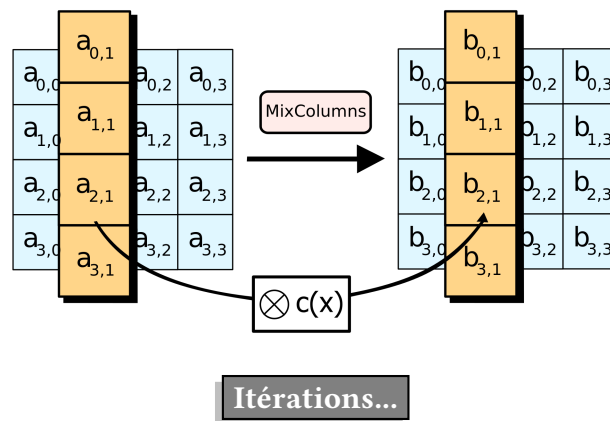
4^{ème} étape « ShiftRows » : Décallage cyclique

Dans cette étape, on effectue des transpositions. Les trois dernières lignes de la matrice sont déplacées cycliquement un certain nombre de fois.



5^{ème} étape « MixColumns » : Mélange par colonnes

On effectue une opération linéaire de mélange sur les colonnes de la matrice. Les quatre octets de chaque colonne de la matrice sont combinés à l'aide d'une transformation linéaire inversible. Chaque colonne est multiplié par une matrice fixée. Plus précisément, chaque colonne de la matrice est vue comme un polynôme de $\mathcal{GF}(2^8)$ et on le multiplie modulo $01_{16} \cdot X^4 + 01_{16}$ par un polynôme de $\mathcal{GF}(2^8)$ bien précis.



On effectue à nouveau l'étape 2), et on répète l'étape 3), l'étape 4), l'étape 5) puis l'étape 2) un certain nombre de fois (9, 11 ou 13 fois suivant le nombre d'octets que l'on a au départ). Puis dernière étape, on effectue une dernière fois l'étape 3), l'étape 4) puis l'étape 2) et notre message est enfin chiffré.

4.1.4 Analyse

Le chiffrement AES repose sur des algorithmes d'un niveau assez avancé, pas à la portée de personnes n'ayant pas un bagage mathématique conséquent. Le fait que l'AES utilise, une série d'étapes qu'il répète et qu'à chaque boucle le message en cours de chiffrement deviens de plus en plus sécurisé, le rend particulièrement fiable. Il n'est certes pas asymétrique et donc nous avons besoin d'une seule clef pour chiffrer et déchiffrer un message. Mais la seule méthode que nous pourrions qualifier d'optimale pour casser les clés AES serait la méthode **brute-force**. En d'autres termes, un ordinateur, aussi puissant soit-il, va essayer toutes les combinaisons possibles de clé d'une taille prédéfinie.

4.2 Conclusion

Le chiffrement RSA et le chiffrement AES sont fondamentalement opposés, ils ne fonctionnent pas de la même façon et ne suivent pas les mêmes codes. L'un est asymétrique, nécessitant deux clés, l'autre est symétrique, nécessitant qu'une seule clé. Si l'on se restreint à cet aspect, le chiffrement RSA est plus sécurisé que le chiffrement AES. Si l'on va un peu plus loin, le principe mathématique. Le chiffrement RSA a besoin de deux clés, l'une et l'autre étroitement liées qui permettent le chiffrement ou le déchiffrement après diverses opérations arithmétiques. Sa sécurité repose sur le problème de factorisation d'entiers. Il faut choisir des entiers très grand pour une grande sécurité et nous sommes jamais réellement à l'abri que par l'usage de méthodes comme le crible algébrique (extrêmement puissant pour des grands nombres) nous puissions casser le chiffrement RSA en décomposant le nombre en question comme produit de deux nombres premiers et alors à ce moment là il suffira de faire l'opération inverse pour trouver le message non chiffré. Alors même si le temps nécessaire à cela est long, que c'est très aléatoire, laborieux et que les cas de casse de chiffrement RSA ne sont pas des événements fréquents, les risques sont bien présents et réels. Tandis qu'avec le chiffrement AES son fonctionnement est tout autre et sa sécurité repose sur des arguments plus concrets. Des chercheurs pour Microsoft ont publié une méthode permettant de casser une clé AES en seulement 2^{126} opérations au lieu de 2^{128} pour une attaque de type brute-force. On peut donc naturellement se dire que le système a des faiblesses, ce qui est vrai puisque la simplicité algébrique du chiffrement AES peut être vue comme une potentielle faiblesse, mais en réalité ces attaques ne sont pas réalisables. Pour une clé de 128 bits, il y a $3,4 \times 10^{38}$ combinaisons possibles, donc même les super calculateurs les plus puissants du monde mettraient plus de 13 milliards d'années (âge de l'univers) pour briser ces clefs en effectuant toutes les combinaisons possible. L'AES a alors lui aussi une faiblesse qui existe, mais qui contrairement au chiffrement RSA, n'est pas une menace car aucun matériel aujourd'hui (ni pour les décennies à venir) ne permet de casser une clé AES. De plus, l'algorithme AES reste la norme de cryptage préférée pour les gouvernements, les banques et de nombreux systèmes de sécurité dans le monde.

Références

- [1] Wikipédia, Cryptographie, <https://fr.wikipedia.org/wiki/Cryptographie>.
- [2] Lucas Willems, Arithmétique, <https://www.lucaswillems.com>.
- [3] Wikipédia, Chiffrement RSA, https://fr.wikipedia.org/wiki/Chiffrement_RSA.
- [4] Wikipédia, Factorisation de Dixon, https://fr.wikipedia.org/wiki/Factorisation_de_Dixon.
- [5] Wikipédia, Crible Quadratique https://fr.wikipedia.org/wiki/Crible_quadratique.
- [6] Wikipédia, Crible Algébrique, https://fr.wikipedia.org/wiki/Crible_algébrique.
- [7] Daniel Perrin, Université Paris Saclay, Cours n° 6 : Arithmétique et cryptographie <https://www.imo.universite-paris-saclay.fr/~perrin/interdisciplines/Cours6cryptographie.pdf>.
- [8] Charles Bouillaget, Arithmétique pour la cryptographie, Chapitre 7 <https://www.fil.univ-lille1.fr/~bouillaget/PAC/poly/ch7.pdf>.
- [9] Exo7, Cryptographie http://exo7.emath.fr/cours/ch_crypto.pdf
- [10] BoxCryptor, Le Chiffrement AES et RSA, <https://www.boxcryptor.com/fr/encryption/>.
- [11] SecuriteInfo, Les chiffrements cassés, <https://www.securiteinfo.com/cryptographie/cracked.shtml>.
- [12] SecuriteInfo, L'AES : Advanced Encryption Standard, <https://www.securiteinfo.com/cryptographie/aes.shtml>.
- [13] Wikipédia, AES, https://fr.wikipedia.org/wiki/Advanced_Encryption_Standard.
- [14] Pierre-Alain Fouque, Cours ENS, Algorithmes de chiffrement symétrique par bloc (DES et AES), <https://www.di.ens.fr/~fouque/mpri/des-aes.pdf>.
- [15] Acrypta, Fonctionnement d'AES, http://www.acrypta.com/telechargements/fgc/annexes/fgc_annexe_1.pdf.