UNIVERSITÉ DE TOULON

UFR Sciences et Techniques
Licence Renforcée de Physique-Chimie

Rapport du projet personnel de recherche

La Cryptologie

Provost Mathis L2PC
2017-2019

Tuteur : M.Zanotti
Laboratoire : IMATH

Je souhaite avant tout remercier Mr Jean-Pierre Zanotti, du laboratoire iMath, pour son implication, son aide, son temps et ses précieux conseils tout au long de l'élaboration de mon projet de recherche personnel sur la cryptologie.

Table des matières

Mathis Provost
UNIVERSITÉ DE TOULON

Partie I
Introduction

La création de la cryptologie vient d'un très vieux besoin des Hommes, celui de pouvoir communiquer discrètement et facilement. Les débuts de la cryptologie remontent à l'antiquité, au XV^{ème} av. J-C. La cryptologie était à l'origine créée par des mécanismes physiques, des jeux de lumières et d'écriture. Avec l'évolution des technologies et l'apparition de nos guerres modernes, les enjeux ont évolué et ont nécessité de nouvelles méthodes de communication.

C'est à ce moment que les mathématiques se sont mises au service de l'Homme, pour créer la cryptologie telle que nous la connaissons actuellement. La numérisation de toutes nos données requièrent une grande sécurité pour le stockage et le transfert de ces dernières sur Internet. Cette sécurité est l'un des enjeux principaux des nouvelles méthodes de chiffrement .

Bien qu'il existe de nombreuses méthodes de chiffrement reposant sur des principes différents, le concept reste le même. Il faut un texte en clair, lisible, une méthode de chiffrement que l'on va appliquer au texte en clair et une, ou plusieurs, clés pour passer du texte clair au texte chiffré et inversement.

La cryptologie se décompose en deux domaines d'études :
- La cryptographie
- La cryptanalyse

La cryptographie c'est l'art de crypter ou décrypter un message en un message secret illisible tel quel.
La cryptanalyse, en revanche, c'est l'art de trouver le code secret afin de pouvoir décrypter des messages et accéder au contenu censé être privé.

Désormais la cryptologie est appliquée à la sécurisation de données sur Internet et aux transferts d'argent virtuels, entre autres. Arithmétique, algèbre et algorithmes œuvrent ensemble au service de la cryptologie pour l'aider à faire face au renouvellement incessant des défis qu'elle doit relever.

Nous allons voir différentes méthodes de chiffrement et divers moyens pour les décrypter. Nous verrons l'évolution de l'ingéniosité de ces méthodes de chiffrements qui ont un rôle capital dans notre société numérique.

Partie II
Codes à clés symétriques

Un chiffrement à clé symétrique utilise la même clé pour crypter et décrypter les messages. Ce chiffrement n'est pas très sécurisé car si une personne parvient à subtiliser la clé il aura un total accès aux messages cryptés et pourra également envoyer des messages cryptés et donc se faire passer pour quelqu'un d'autre.
Parmi les chiffrements à clés symétriques les plus anciens, on retrouve le code de César ainsi que le code Vigenère.
Bien qu'ils soient très âgés et peu utilisés, ils restent de très bon exemples pour comprendre les ficelles de la cryptologie.

1 Le code de César

1.1 Chiffrement et déchiffrement

Le chiffrement de César, aussi connu sous le nom de chiffrement par décalage, consiste en une permutation circulaire des lettres de l'alphabet de k lettres, c'est une substitution mono-alphabétique.
Ici la lettre k représente la clé du code. Le fonctionnement de ce code est très simple. On dispose d'un texte en clair, soit n une lettre du texte en clair ; on associe chacune des lettres de ce mot à sa valeur dans l'alphabet (A=1, B=2, C=3, ..., Z=26) et on leur rajoute la valeur k modulo 26, c'est-à-dire que si la valeur d'une lettre dépasse 26, elle repart de la valeur 1. Ainsi on a x qui représente la lettre n une fois cryptée :

$$\boxed{x \equiv n + k \pmod{26}} \tag{1}$$

On dispose donc de 26 possibilités de clés, dont la clé neutre qui ne modifie pas le texte, car il y 26 lettres dans l'alphabet français. C'est ici que réside la plus grande faiblesse de sécurité de ce code.

Le déchiffrement est sensiblement pareil ; la seule différence réside dans le fait que pour retrouver les lettres initiales du texte en clair il faut enlever à chacune des lettres du texte crypté la valeur k de la clé. Pour retrouver n il faut donc faire le calcul suivant :

$$\boxed{n \equiv x - k \pmod{26}} \tag{2}$$

1.2 Décryptage

1.2.1 La méthode "Force Brute"

Comme énoncé précédemment, la clé du chiffrement de César n'est en effet pas très dure à trouver. La première méthode de décryptage appelée *Force Brute* consiste à essayer toutes les clés possibles, comme il n'y en a que 25, plus la clé neutre, l'opération est plutôt rapide et ne nécessite pas de traduire l'intégralité d'un texte, mais seulement les premiers mots pour s'assurer que ces mots soient lisibles. Bien que peu raffinée, elle marche parfaitement pour ce type de chiffrement et reste relativement rapide.

1.2.2 Analyse fréquentielle

Cette seconde méthode, déjà plus raffinée nécessite un texte assez long pour pouvoir se prêter à une analyse fréquentielle. En effet, dans chacune des langues, une lettre est plus utilisée que les autres. En France et dans les pays anglo-saxons c'est la lettre e qui est la plus représentée dans les textes. En France, la lettre e constitue en moyenne 12% des lettres d'un texte.
Cette analyse fréquentielle consiste donc à compter l'apparition de chaque lettre tout au long du texte crypté. Si l'on repère une lettre y qui apparait beaucoup plus souvent que les autres il y a de fortes chances qu'il s'agisse de la lettre e cryptée. Il suffit ensuite de noter le rang dans l'alphabet qu'occupe cette lettre y et d'y soustraire le rang de la lettre e pour obtenir la clé k :

$$\boxed{k = rang_{alphabet}(y) - rang_{alphabet}(e)} \tag{3}$$

Il suffit ensuite de se référer à l'étape (2) indiquée dans la partie *Déchiffrement* pour retrouver le texte déchiffré une fois que nous sommes en possession de cette clé. En cas d'échec, il faut prendre la lettre suivante apparaissant le plus souvent dans le texte réessayer jusqu'à la réussite.

Le chiffrement de César est une étape clé dans l'histoire de la cryptologie mais il reste néanmoins basique et facilement décryptable ; de nombreux chiffrements plus élaborés vont lui succéder tel que DES ou AES, pour parler de chiffrements relativement récents.

2 Le code de Vigenère

2.1 Chiffrement et déchiffrement

Le chiffrement de Vigenère s'inspire grandement du chiffrement de César et repose sur le même principe, à l'exception près qu'il contrecarre sa plus grande faiblesse ; le fait que toutes les lettres du texte soient décalés dans l'alphabet par la même clé k. C'est ainsi que Vigenère imagine ce chiffrement à substitution poly-alphabétique. La clé k n'est plus un nombre compris entre 1 et 26, dont la clé neutre, mais peut être un nombre extrêmement grand ou bien un mot, une phrase ou encore un texte.

Soit n_i la valeur de la $i^{\text{ème}}$ lettre du texte clair et k_i la valeur de la $i^{\text{ème}}$ $\mod (m)$ lettre de la clé, avec m la longueur de la clé . La première lettre chiffrée x_1 sera égale à la somme de n_1+k_1, de la même façon on a $x_2 = n_2 + k_2$, ...

Par extension on a : $\boxed{x_i = n_i + k_i}$

Texte →	U	N	E	P	L	A	N	C	H	E	A	V	O	I	L	E
Clé →	S	U	R	F	S	U	R	F	S	U	R	F	S	U	R	F
Chiffré →	M	H	V	U	D	U	E	H	Z	Y	R	A	G	C	C	J

Texte →	21	14	5	16	12	1	14	3	8	5	1	22	15	9	12	5
Clé →	19	21	18	6	19	21	18	6	19	21	18	6	19	21	18	6
(Texte + clé) modulo 26 →	14	9	23	22	5	22	6	9	1	26	19	2	8	4	4	11

FIGURE 1 – Chiffrement de Vigenère

Pour le chiffrement de César le nombre de clés possible était 25, avec cette méthode de chiffrement il s'élève à 25^n, n étant la longueur de la clé sans répétitions. On comprend relativement vite, que pour un texte assez long, plus la clé est grande plus il semble compliquer de pouvoir essayer toutes les possibilités manuellement comme précédemment.

Bien évidemment, le déchiffrement du texte chiffré consiste à faire l'opération inverse. Cette méthode de chiffrement, plus complexe que le chiffrement de César, est restée près de 300 ans après sa création sans aucune méthode pour pouvoir la décrypter. C'est le mathématicien Charles Babbage qui rédige la cryptanalyse en 1854 sans la dévoiler. C'est Friedrich Kasiski, qui 9 ans plus tard, arrive à cette même cryptanalyse et la rend publique.

2.2 Décryptage

2.2.1 Le test de Kasiski

Toute la difficulté de décrypter un message chiffré par le chiffrement de Vigenère repose sur la longueur de la clé k et la longueur du texte à analyser, car plus le texte est long plus la méthode sera précise.

Le test de Kasiski, très méthodique, est composé de 5 étapes. La première étape consiste à analyser le texte, et plus particulièrement les séquences d'au moins 3 lettres qui se répètent dans le texte et partir du principe que ces répétitions ne sont pas le fruit du hasard. On notera l la distance entre deux séquences de lettres qui se répètent.
Une langue, quelle qu'elle soit, présente souvent les mêmes enchainements de lettres dans les mots. Kasiski part du principe que les séquences de 3 lettres répétées, sont à chaque fois les 3 mêmes lettres du texte initial, chiffrées par la même séquence de 3 lettres de la clé.
Soit m la longueur de la clé k, pour que les deux séquences répétées soient codées avec les mêmes lettres de la clé k, il vient que m doit diviser l. Si la clé est très petite devant la longueur du texte, elle se répète (*cf. Figure 1*), donc dans la distance l, la clé de longueur m se répète n fois ; ainsi on prendra m comme étant égal au pgcd des distances l des différentes séquences répétées.

CS AZZMEQM CO XRWF CS DZRM GFMJECV. X'IMOQJ JC LB NLFMK CC LBM
WCCZBM KFIMSZJSZ CS URQIUOU. CS ZLPIE ECZ RMWWTV SB KCCJ QMJ
FCSOVJ GCI ZI ICCKS MK QMLL YL'CV ECCJ OKTFWTVM JIZ CO XFWBIWVV IV
ACCI CC C'OCKFM JINWWB U'OBKSVUFM

Séquence	Position	Distance	Décomposition
COX	11-140	129	3.43
FCS	16-99	83	83
ZRM	20-83	63	3.3.7
FMJ	24-162	138	2.2.3.3
CLB	37-46	9	3.3
KCC	44-92	48	2.2.2.3
WTV	87-133	46	2.23
CCJ	93-126	33	3.11
ICC	110-155	45	3.3.5
MJI	136-163	27	3.3.3

On voit clairement que le nombre prédominant est 3, donc m=3.

FIGURE 2 – Test de Kasiski

Maintenant que l'on a une hypothèse sur la longueur de la clé m, tous les caractères du texte chiffré distants de m caractères devraient être codés par la même lettre de la clé k. On sépare le texte alors en m sous-textes dans lesquels on ajoute toutes les lettres chiffrées par la même lettre de la clé. Comme chacune des lettres de chaque sous-texte est chiffré par la même lettre de la clé, on se retrouve face à un simple chiffrement de César, on peut alors trouver quelle lettre a chiffré chaque sous-texte par une *Analyse fréquentielle (1.2.2)*.
On ré-assemble ensuite les sous-textes décryptés dans le bon ordre pour avoir le texte final entièrement décrypté.

Le seul cas ou ce test ne marchera jamais est le *Cas de Vernam* où la clé est aussi longue que le texte, sans aucune répétition et à usage unique. Dans ce cas aucune séquence ne sera répétée, hormis le hasard, et l'on ne pourra extraire aucune information du texte pour en déduire la clé. Ce cas est réputé inviolable mais il n'est toutefois que très rarement utilisé car le chiffre de Vernam exige des clés extrêmement longues, et une parfaite synchronisation des clés. L'échange des clés, qui doit être sécurisé, est donc difficile à réaliser. Enfin, les clés utilisées doivent être parfaitement aléatoires, ce qui n'est pas facile à garantir.

2.2.2 Indice de coïncidence

La méthode de Kasiski bien que révolutionnaire n'était pas toujours des plus précises ni des plus rapides, de nouvelles méthodes plus récentes et plus performantes ont été mise au point comme la méthode de *l'indice de coïncidence*

On appelle indice de coïncidence d'un texte la probabilité pour que, si on tire simultanément deux lettres au hasard dans ce texte, ce soient les mêmes. Si un texte est composé de n lettres choisies parmi l'alphabet $A, \ldots, Z$ alors son indice de coïncidence I_c vaut :

$$\boxed{I_c = \frac{n_A(n_A-1)}{n(n-1)} + \ldots + \frac{n_Z(n_Z-1)}{n(n-1)}} \tag{4}$$

Cette formule s'explique par le fait qu'il y est une probabilité égale à $\frac{n_A}{n}$ pour que la première lettre choisie soit un A. Il reste alors $(n-1)$ lettres et (n_A-1) lettres A. La probabilité que l'on ait tiré encore un A pour deuxième lettre est donc $\frac{(n_A-1)}{(n-1)}$. La probabilité que l'on ait tiré deux fois la lettre A vaut donc exactement $\frac{n_A(n_A-1)}{n(n-1)}$. Lorsque l'on fait la somme pour toutes les lettres on obtient bien I_c.

Dans une langue usuelle, les lettres n'apparaissent pas toutes avec la même fréquence. C'est pourquoi l'indice de coïncidence d'un texte écrit en français I_f est très supérieur à l'indice de coïncidence d'un texte aléatoire I_a où les lettres ont une fréquence d'apparition identiques. Ainsi une analyse statistique sur de nombreux textes a donné $I_f = 0,074$, tandis qu'un petit calcul donne $I_a = \frac{1}{26} \approx 0.038$.

On suppose qu'on dispose d'un texte de n lettres chiffré par Vigenère avec une clé k inconnue composée de m lettres , et n très grand devant m. On cherche à exprimer la valeur théorique de l'indice de coïncidence du texte codé Ic. Les paires de 2 lettres du texte peuvent être partagées en 2 groupes :

- Ou bien elles sont codées avec la même lettre de la clé et il y a donc $\frac{n(n-m)}{2m}$ paires de la sorte.
- Ou bien elles sont codées avec une lettre différente de la clé et il y a $\frac{n^2(n\text{-}m)}{2}$ paires de la sorte.

Il vient alors que le nombre de paires de 2 lettres identiques dans le texte sera égal à $\frac{n(n\text{-}m)}{2m} I_f + \frac{n^2(m-1)}{2} I_a$. Comme il y a $\frac{n(n\text{-}1)}{2}$ paires de deux lettres dans le texte, on peut approximer I_c comme étant égal à :

$$\boxed{I_c = \frac{(I_f - I_a)n + m(n \times I_a - I_f)}{m(n-1)}} \tag{5}$$

On isole ensuite la constante m, représente la longueur de la clé k.

$$\boxed{m = \frac{(I_f - I_a)n}{(n-1)I_c - n \times I_a + I_f}} \tag{6}$$

Il suffit de calculer I_c avec la formule *(4)*, d'en déduire m et comme précédemment, diviser le texte en sous-textes et procéder à une *Analyse fréquentielle (1.2.2)*.

Bien évidemment l'usage d'ordinateurs permet de réaliser beaucoup plus facilement tous ces calculs et donc d'automatiser cette méthode, plus la clé est longue plus le travail de calcul de l'ordinateur sera important. Néanmoins le décryptage de ce type de chiffrement se fait très aisément de nos jours avec la technologie dont nous disposons. Le chiffrement de Vigenère ne représente plus un chiffrement sécurisé et n'est donc plus utilisé.

On sait que l'on se trouve dans le cas de Vernam lorsque l'indice de coïncidence I_c a une valeur proche de l'indice de coïncidence d'un texte aléatoire $I_a = 0.033$. Il est donc inutile de poursuivre les calculs car il ne sera pas possible de déterminer la clé k.

Partie III
Codes à clés asymétriques

Le chiffrement à clé asymétrique, à l'inverse du chiffrement à clé symétrique, n'utilise pas la même clé pour chiffrer un message que pour le déchiffrer. Ce type de chiffrement utilise deux clés, une clé publique connue de tous pouvant chiffrer des messages, et une clé secrète censée n'être connue que par le créateur qui veut pouvoir déchiffrer les messages qu'il reçoit.
Le chiffrement à clé asymétrique résout l'un des plus gros problèmes des chiffrements à clé symétrique, celui de devoir communiquer l'unique clé avec une autre personne pour pouvoir communiquer secrètement, au risque qu'elle se fasse intercepter par des personnes malveillantes. Le chiffrement a clé asymétrique le plus connu et le plus utilisé mondialement actuellement est le chiffrement RSA.

3 Le code RSA

3.1 Préparation des clés

Avant de procéder au chiffrement ou au déchiffrement, il faut préparer les deux clés, publique et privée. La préparation de ces deux clés, intimement liées, repose essentiellement sur les propriétés des nombres premiers et de théorèmes mathématiques.

- La première étape, et la plus importante, consiste à créer la clé publique n grâce à deux nombres premiers distincts p et q, tel que :

$$\boxed{n = p \times q} \tag{7}$$

Définition 1 *Soit $a \in N$, a est dit premier s'il admet exactement deux diviseurs : 1 et lui-même.*

Toute la sécurité de ce chiffrement repose sur la grandeur des nombres p et q et leur caractère aléatoire vis-à-vis de l'autre.

Définition 2 *Soit $n \in N$. L'indicateur d'Euler de n noté $\phi(n)$ est le nombre d'éléments inversibles dans $\mathbb{Z}/n\mathbb{Z}$. Ce nombre d'éléments correspond également au nombre d'entiers a inférieurs à n et tels que $PGCD(a, n) = 1$.*

- La seconde étape consiste à calculer l'indicateur d'Euler de n noté $\phi(n)$, qui est défini de la sorte :

$$\boxed{\phi(n) = (p-1) \times (q-1)} \tag{8}$$

- La troisième étape est le calcul de l'exposant public e grâce à l'algorithme d'Euclide, ou de Fermat-Euler.

  Lemme 1 *Soient a,b* $\in \mathbb{N}^*$ *et a* $>$ *b, alors :*

  $$\boxed{(a,b) = (b, a \mod n)}$$

  L'exposant public e doit répondre à la condition suivante afin que e et $\phi(n)$ soient premiers entre eux :

  $$\boxed{(e, \phi(n)) = 1 \Leftrightarrow e^{\phi(n)} \equiv 1 \pmod n} \quad (9)$$

- Finalement, on utilise le théorème d'Euclide étendu pour déterminer les coefficients de Bezout :

  Théorème 1 *Soient a,b* $\in \mathbb{N}^*$ *premiers entre eux, avec a* $>$ *b et k=PGCD(a,b). Alors il existe un couple* (u, v) *tel que :*

  $$\boxed{au + bv = PGCD(a,b) = k}$$

  Dans notre cas, comme e est premier avec $\phi(n)$, d'après le théorème de *Bachet-Bézout* il existe deux entiers d et k tel que :

  $$\boxed{de + k\phi(n) = 1 \Leftrightarrow ed \equiv 1 \mod (\phi(n)) \Leftrightarrow d \equiv \frac{1}{e} \mod (\phi(n))} \quad (10)$$

  Nous sommes maintenant en possession de la clé publique (e, n) et de la clé privée (e, d) et pouvons chiffrer ou déchiffrer les messages.

3.2 Chiffrement et déchiffrement

Afin de pouvoir procéder au chiffrement du texte en clair, il faut attribuer à chaque lettre du texte une valeur numérique, cette valeur peut être le rang de la lettre dans l'alphabet ou de façon plus répandue sa valeur ASCII.

- Soit M l'entier naturel strictement inférieur à n qui représente successivement chaque lettre du texte, et X représentant la lettre chiffrée alors :

  $$\boxed{X \equiv M^e \pmod n} \quad (11)$$

- Pour déchiffrer X, on utilise d, l'inverse de e $modulo(\phi(n))$, et l'on retrouve le message clair M en inversant l'équation précédente grâce au théorème d'Euler :

  $$\boxed{M \equiv X^d \pmod n} \quad (12)$$

3.3 Décryptage

3.3.1 Un système infaillible ?

Le chiffrement du système RSA repose sur une chose toute simple, notre incapacité à décomposer n en ses facteurs premiers afin de pouvoir recalculer la clé privée d. Bien qu'en apparence il ne semble pas compliquer de tester toutes les combinaisons possibles, surtout avec l'aide d'ordinateurs toujours plus puissants, il en est autrement. Si par exemple, la clé publique n vaut 85, alors il ne prendra pas très longtemps à trouver que $n = 5 \times 17$, mais si n prend une valeur astronomique à plusieurs dizaines de chiffres, il est beaucoup moins aisé de déterminer p et q, même pour un ordinateur, qui peut y passer des mois comme des années. Cette solution n'est que peu rentable car il suffirait de changer la clé régulièrement pour anéantir des mois de calculs informatiques.

Actuellement le système RSA est réputé comme inviolable, mais ce n'est pas pour autant qu'il n'existe pas des moyens d'en venir à bout. En effet bien que ce chiffrement soit très perfectionné, il restera toujours une faille majeure qui est l'Homme. Comme la clé semble impossible à décrypter, il est alors plus facile de pirater un ordinateur pour y soutirer des informations ou encore d'intercepter des informations secrètes échangées. En effet, bien que n soit rendu publique, il ne faut pas pour autant penser que partager $\phi(n)$ est anodin ! La connaissance de l'indicateur d'Euler $\phi(n)$ est un précieux atout car :

$$\begin{aligned}
&\phi(n) = (p-1)(q-1)\\
\Leftrightarrow &\phi(n) = pq - p - q + 1\\
\Leftrightarrow &\phi(n) = (n+1) - (p+q)\\
\Leftrightarrow &q = (n+1) - \phi(n) - p\\
&n = p \times q\\
\Leftrightarrow &n = p(n+1-\phi(n)-p)\\
\Leftrightarrow &n = -p^2 + (n+1-\phi(n)) \times p\\
\Leftrightarrow &p^2 - (n+1-\phi(n)) \times p + n = 0
\end{aligned}$$

Nous avons une équation quadratique de p tel que : $p = \frac{-b \pm \sqrt{b^2-4ac}}{2a}$ avec :

$$a = 1 \qquad b = -(n+1-\phi(n)) \qquad c = n$$

$$\boxed{p = \frac{(n+1-\phi(n)) \pm \sqrt{(n+1-\phi(n))^2 - 4n}}{2}} \tag{13}$$

Par symétrie, l'une des deux solutions de p sera p et l'autre sera q, nous pouvons maintenant recalculer la clé privée et déchiffrer tous les messages.

3.3.2 Les ordinateurs quantiques

Si la solution pour décomposer n en facteurs premiers ne se trouve pas dans nos ordinateurs classiques, incapables de traiter autant d'informations et de trouver une solution dans un laps de temps convenable, peut-être se trouve-t-elle dans les ordinateurs quantiques. Là ou un ordinateur classique effectue une liste d'opérations à la suite, l'ordinateur quantique lui les effectue toutes en même temps et représente un gain de temps important.

Un ordinateur classique traite les informations sous forme de bits, un bit ne peut prendre que la valeur 0 ou la valeur 1, et il traite les bits un par un, à la suite. Un ordinateur quantique, quant à lui traite des bits quantiques appelés q-bits qui obéissent aux lois de la mécanique quantique et plus particulièrement au *Principe de superposition*. Le q-bit peut prendre la valeur 0, 1 ou une superposition de la valeur 0 et 1 :

$$\boxed{qbit = \alpha|0\rangle + \ \beta|1\rangle}$$

Intéressons nous maintenant aux registres de bits, avec par exemple un registre de 4 bits, voici toutes les configurations possibles que nous pouvons faire avec 4 bits :

$$\begin{bmatrix} 0000 & 0001 & 0010 & 0100 \\ 1000 & 0011 & 0101 & 1001 \\ 0110 & 1010 & 1100 & 0111 \\ 1011 & 1101 & 1110 & 1111 \end{bmatrix}$$

Il y a donc 16 combinaisons possibles, soit 16 informations différentes, et donc 16 calculs successifs à réaliser, que l'on peut créer avec un registre de 4 bits.
Si maintenant on a un registre de 4 q-bits :

$$\begin{bmatrix} \alpha|0000\rangle + & \beta|0001\rangle + & \gamma|0010\rangle + & \delta|0100\rangle + \\ \epsilon|1000\rangle + & \zeta|0011\rangle + & \eta|0101\rangle + & \theta|1001\rangle + \\ \iota|0110\rangle + & \kappa|1010\rangle + & \lambda|1100\rangle + & \mu|0111\rangle + \\ \nu|1011\rangle + & \xi|1101\rangle + & \sigma|1110\rangle + & \chi|1111\rangle \end{bmatrix}$$

Avec un registre de 4 q-bits on peut maintenant avoir une superposition de ces 16 états, en pratique on peut même en avoir plus que 16 grâce aux coefficients, et donc effectuer ces 16 calculs en même temps, c'est 16 fois plus rapide qu'avec un registre de 4 bits. De manière générale, pour un registre de N q-bits :

$$\boxed{N \ \ qbits = 2^N \ \ etats}$$

Donc avec N q-bits on va 2^N fois plus vite qu'avec N bits.

En moyenne un ordinateur quantique de 20 q-bits serait l'équivalent d'un ordinateur classique vendu dans le commerce et un de 40 q-bits correspondrait a l'ordinateur classique le plus puissant qui existe, la courbe de puissance évolue ainsi exponentiellement.

C'est en 2001, dans les laboratoires d'IBM, qu'un algorithme quantique, *l'algorithme de Shor* : qui effectue des décompositions en nombres premiers bien plus rapidement que n'importe quel algorithme classique , fut enfin testé et permis de décomposer 15 en ses facteurs premiers : $15 = 3 \times 5$ avec un ordinateur quantique de 7 q-bits. En 2005 l'ordinateur quantique le plus puissant dépassait les 8 q-bits et plus de 12 q-bits l'année suivante. En 2014, un ordinateur quantique a réussi à décomposer le nombre 56153 et le dernier record officiel est le nombre 200 099 en 2016. En novembre 2017, le nombre de q-bits sur un ordinateur quantique atteint 50 q-bits et en mars 2018 il s'élevait à 72 q-bits. On estime ainsi qu'en utilisant 500 ordinateurs classiques d'aujourd'hui, il faudrait un milliard d'années pour craquer une clé de chiffrement RSA de 2048 bits. L'informatique quantique pourrait le faire en une centaine de secondes.

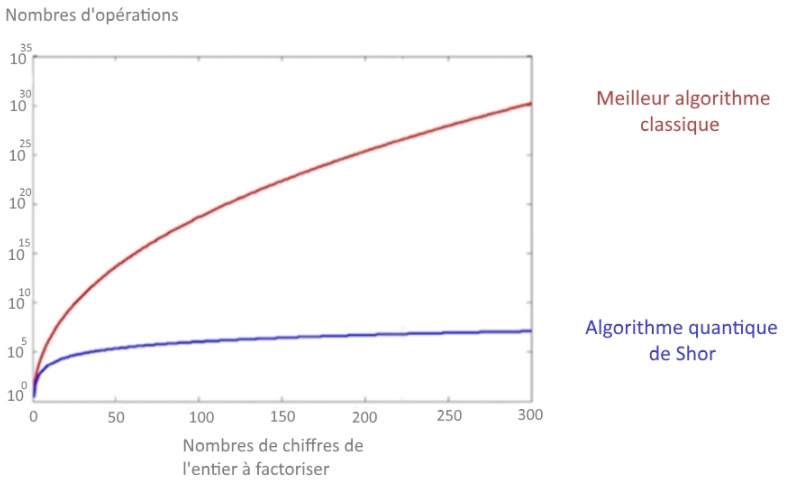

FIGURE 3 – Algorithme de Shor

Malgré cette évolution très rapide et impressionnante nous sommes encore loin de pouvoir décomposer les clés publiques n, servant au chiffrement du code RSA, pouvant s'élever à plusieurs milliards de milliards. Néanmoins, à ce rythme d'évolution il ne pas faut sous-estimer la menace que représente les ordinateurs quantiques. S'il s'avérait qu'un ordinateur quantique serait assez puissant pour décrypter les clés de chiffrement RSA actuelles ce serait une catastrophe mondiale d'un point de vue de la cyber-sécurité, de la sécurité de la vie privée autant que de tout notre système économique qui s'effondrerait.

Partie IV
Conclusion

Alors que l'évolution constante des technologies nous pousse à tout numériser et à beaucoup se reposer sur la fiabilité de nos systèmes de chiffrement, dont le système RSA qui représente un pilier central dans la protection des données en lignes, c'est également cette même évolution qui pourrait porter préjudice au système RSA.

Même s'il est plutôt aisé de comprendre le fonctionnement du système RSA, ce qui est l'une des raisons de sa célébrité, toutefois il se cache derrière cette simplicité un véritable arsenal mathématique très puissant. On devine cependant que comme toute chose, RSA est loin de la perfection. Il est donc normal de se questionner sur la fiabilité de ce système car l'histoire à déjà prouvé maintes fois que les exploits d'hier peuvent vite être éclipsés par les avancées de demain et qu'il ne faut jamais s'arrêter à nos acquis.

On peut penser à *Enigma* qui était à son époque considéré comme incassable et qui trône actuellement avec le statut d'archive de la cryptographie. Depuis quelques années on peut entendre parler de la cryptographie quantique, cette méthode basée sur la superposition d'états des particules, tels des photons, pourrait mettre à mal de nombreux systèmes déclarés fiables, dont le système RSA.

Cette défaillance du système RSA face a la cryptographie quantique soulève de nombreuses questions et enjeux vis-à-vis de la cyber-sécurité et nous oblige à être en recherche perpétuelle de nouvelles méthodes de chiffrement toujours plus performantes et ingénieuses car les avancées technologiques n'ont cessé de s'accélérer ces dernières décennies et permettent de décrypter les systèmes de chiffrement toujours plus rapidement. La question qui se pose alors est celle de l'existence d'un système parfait qui mettrait fin à toutes ces recherches.

Tout laisse penser que la grande histoire de la cryptologie n'a pas fini de nous surprendre, et que quoi qu'il advienne du système RSA dans le futur, il restera à jamais un produit de l'ingéniosité humaine.

Partie V
Bibliographie

- Jean-Pierre Zanotti. « Le chiffrement de Vigenère ».
http ://zanotti.univ-tln.fr/crypto/vigenere.html

- Simon Singh «Histoire des codes secrets» (1999)
ISBN Poche : 978-2253150978

- Didier Müller. Edition City «Les Codes secrets Décryptés» (2007)
ISBN : 978-2-35288-544-3

- Philippe Guillot « Cryptologie : l'art des codes secrets »
Futura-sciences.com (23 novembre 2015)
https ://www.futura-sciences.com/sciences/dossiers/mathematiques-cryptologie-art-codes-secrets-1817/

- Lucia Sillig. « La cryptographie, un art toujours perfectible ».
CourrierSciences (12 janvier 2011)
https ://www.courrierinternational.com/article/2011/01/13/la-cryptographie-un-art-toujours-perfectible

- Frédéric Bayart. « Le lexique de la cryptographie ». Bibm@th.net
http ://www.bibmath.net/crypto/index.php ?action=affiche&quoi=moderne/vocabulaire

- ANSSI (agence nationale de la sécurité des systèmes d'information)
http ://www.securiteinformatique.gouv.fr/autoformations/cryptologie/co/-Cryptologie.html

- Didier Müller. « Chiffre de César ». Nymphomath.com (11 juin 2001)
http ://www.nymphomath.ch/crypto/cesar/index.html

- « Chiffre de Vigenère ». Wikipédia, (14 mai 2018)
https ://fr.wikipedia.org/wiki/Chiffre_de_Vigenère

- « Chiffre de Vigenère ». Dcode, 2018
https ://www.dcode.fr/chiffre-vigenere

- Didier-Müller. « Décryptement du chiffre de Vigenère ». Nymphomath.com (4 avril 2001) https ://www.apprendre-en-ligne.net/crypto/vigenere/decodevig.html

- « Test de Kasiski ». Numb3rs-Singularity (6 août 2008) http ://www.numb3rs-singularity.fr/mathematiques/par-nom/test-de-kasiski

- Frédéric Bayart.« Comment vaincre le chiffre de Vigenère ? ». Bibm@th.net http ://www.bibmath.net/crypto/index.php ?action=affiche&quoi=poly/viganalyse

- « L'indice de coïncidence ». Bibm@th.net http ://www.bibmath.net/crypto/index.php ?action=affiche&quoi=complements/indice_coincidence

- Douglas Stinson. « Cryptographie, théorie et pratique, 2nd édition » (6 octobre 2003) ISBN : 978-2-7117-4800-6 Éditeur : Vuibert

Mathis Provost
UNIVERSITÉ DE TOULON

Partie VI
Résumé

À travers ce projet de recherche sur la cryptologie nous avons abordé les différentes méthodes qui ont existé au cours du temps, à chaque fois plus complexe pour remédier aux défauts du précédent. Nous avons traité la méthode de chiffrement et de déchiffrement de chacun des codes abordés, que ce soit le code de César, Vigenère ou RSA, ainsi que leurs failles et comment ces failles ont été utilisées pour créer des algorithmes pour décrypter chacun de ces codes. Ces codes ont tous permis une avancée monumentale dans différents domaines au moment de leur création, que ce soit dans la communication secrète ou plus récemment dans la protection de données sensibles sur Internet. On voit clairement qu'au fil du temps les mathématiques se sont imposées comme maîtres dans l'art de la cryptologie. À chaque fois que nous pensions qu'un système de chiffrement était inviolable, les mathématiques ont prouvé qu'il ne l'était pas. Actuellement c'est le système RSA, utilisé mondialement dans la protection des données bancaires notamment, qui se retrouve menacé avec l'apparition d'ordinateurs quantiques qui dans un futur proche nous donnerons du fil à retordre et nous obligera à mettre au point un nouveau système de chiffrement jusqu'à ce que le futur ne se répète inévitablement.

Through this research project on cryptology, we broached the different methods that existed throughout mankind history, every new method was more complex than the previous in terms of fixing security breaches. Both the encryption and decryption of each code were tackled, namely : Caesar's code, Vigenere's Code and the RSA code. Furthermore, we handled their security breaches and how they were used to develop algorithms in order to decrypt the codes. As a matter of fact, each of them led to a great breakthrough in some distinctive fields of research at the time they were created, whether in secret communications or more recently in data security on the Internet. It is obvious that over time, Mathematics have been defined as masters in the art of cryptology. Every time a code was thought to be unbreakable, Mathematics proved that wrong. It is currently the RSA code, globally used in data protection, including bank secrecy, that is threatened by the appearance of quantum computers that is likely to give us major issues and force us to design a brand new encryption code in a near future, until the story repeats itself ineluctably.