Université Mohammed Premier

Ecole Nationale des Sciences Appliquées

Al Hoceima

Rapport du projet de Fin d'année

Titre :

Cryptographie : méthode de chiffrement RSA

Réalisé par :

- Diongue Mamadou Moustapha
- El Ghaouth Mohamed

Encadrés par :

Pr. BOUJRAF Ahmed

SOUTENU LE 25/06/2019 DEVANT LE JURY :

- Pr. BOUJRAF Ahmed
- Pr. BADI Imad
- Pr. KOLALI Sara

Année universitaire

2018-2019

Sommaire

Table des matières

Résumé

Ce rapport est le fruit du travail que nous avons réalisé dans le cadre de notre projet de fin d'année. L'objectif de ce projet était dans un premier temps d'étudier et de comprendre la méthode de cryptographie RSA et ensuite de réaliser une implémentation de cette dernière.

La réalisation de ce projet s'est déroulé en trois étapes : tout d'abord, nous avons commencé par une documentation assez générale sur la cryptographie dans son ensemble, ensuite nous sommes passé à une étude plus approfondie sur les méthodes de chiffrement asymétriques et nous nous sommes focalisé sur la méthode RSA, à la suite de celui-ci, nous avons effectué une étude conceptuelle de la façon dont on va implémenter cette méthode puis finalement nous sommes passé à l'implémentation proprement dit de la méthode de chiffrement RSA.

Abstract

This report is the result of the work we did as part of our year-end project. The aim of this project was to study and understand the RSA cryptography method and then implement it.

The realization of this project essentially took place in three steps : firstly, we started with a rather general research on the cryptography as a whole, then we went to a more in-depth study on the methods of asymmetric encryption and we focused on the RSA method, following that, we did a conceptual study of how we will implement this method and finally, we moved to the actual implementation of the RSA encryption method.

Introduction générale :

La communication est l'une des caractéristiques intrinsèques à la nature humaine. L'avènement de l'écriture des siècles avant Jésus-Christ pour répondre à certains besoins de l'époque à renforcer et faciliter la communication en permettant de pouvoir garder une trace écrite de tout ce qui est jugé nécessaire mais aussi de pouvoir correspondre à distance ; ce qui était très utile à l'époque car les moyens de transport étaient rudimentaires et le besoin de communiquer avec un interlocuteur qui se trouve à plusieurs jours de voyage à cheval ou à chameau était nécessaire. La seule alternative était donc de lui envoyer le message sous forme écrite.

Dans certains cas, il arrivait que les correspondants voulaient garder secret leurs échanges pour des raisons diverses. C'est le cas par exemple pour des services de renseignements gouvernementaux, de l'armée et plus récemment avec l'essor des nouvelles technologies de l'information et de la communication (NTIC) et plus précisément l'expansion d'internet qui mets en jeu un flux de données important où transitent des millions d'informations qui pour la grande majorité des cas sont vulnérables et sensibles.

D'où la nécessité de trouver un moyen pour répondre à toutes ces contraintes. Des moyens existaient déjà à l'époque pour répondre à quelques-unes de ces problèmes : il s'agit entre autres de la sténographie, et de la cryptographie. Cette dernière est étymologiquement formée par la composition de deux mots du grec ancien : **Kruptos** qui veut dire cachée et **graphein** qui signifie écrire. La sténographie elle, consiste à dissimuler un message dans un autre message afin de la faire passer inaperçu aux yeux du grand public.

La cryptographie désigne l'ensemble des techniques permettant de transformer un message en clair en un autre message codé de telle sorte qu'il soit impossible ou très difficile de retrouver le message initial sans disposer du mécanisme approprié qui permette de faire cette liaison. La cryptographie permet donc de protéger les informations contre les différentes menaces présentent dans leurs environnements qu'elles soient intentionnelles ou accidentelles mais aussi de la vulnérabilité des protocoles d'échanges utilisés.

Elle vise donc à protéger les données conformément à la plupart des modèles de sécurité comme par exemple le Triangle Confidentiality Integrity Availability (C.I.A) des grands axes de la sécurité qui vise à ce que :

L'information ne soit connue que des entités communicantes (Confidentialité),

L'information reste inchangée de sa création à sa livraison (Intégrité)

L'information soit disponible, autrement dit qu'il ne puisse pas se perdre ou se bloquer (Disponibilité).

De nombreux algorithmes de cryptographie ont été développé et n'ont cessé d'être amélioré jusqu'à nos jours. On distingue principalement trois familles :
Les algorithmes de chiffrement faible qui sont assez vulnérables ;
Les algorithmes de cryptographie symétrique et les algorithmes de cryptographie asymétrique dont fait partie la méthode R.S.A.
La méthode RSA est la première mise en œuvre concrète d'un algorithme de cryptographie asymétrique. En effet le concept où l'idée derrière cette dernière avait été présenté par **Martin Hellman** et son collaborateur **Ralph Merkle** considérés comme les pères de la cryptographie asymétrique à la *National Computer Conférence* de *1976* mais ce n'est qu'en 1978 qu'apparaît sa première implémentation baptisée R.S.A. qu'on doit aux chercheurs **Ronald Rivest**, **Adi Shamir** et **Leonard Adleman**. Le terme asymétrique fait référence au fait qu'on a des clefs distinctes pour le chiffrement et le déchiffrement. La clef de chiffrement qui est publique est généralement utilisée pour coder le message et l'envoyer au destinataire qui par la suite la décode grâce à sa clef privée ou bien l'inverse, c'est-à-dire la clef privée utilisée par l'expéditeur pour coder le message et la clef publique pour décoder le message. La première approche permet de garantir la confidentialité du message alors que la deuxième vise à assurer l'authenticité de l'expéditeur.

Notre projet consiste à étudier, comprendre puis implémenter la méthode de cryptographie asymétrique RSA. Le présent rapport est structuré comme suit :

Chapitre 1 : Historique des méthodes de cryptographie
Chapitre 2 : La gestion du projet
Chapitre 3 : Outils de base et chiffrement par la méthode RSA
Chapitre 4 : Application

Chapitre 1 : Historique des méthodes de cryptographie

Introduction :

Ce qui est connu aujourd'hui comme étant la cryptographie, qu'on définit comme étant une discipline scientifique branche de la cryptologie dédiée à l'étude, à l'élaboration et à la mise au point de procédés permettant de protéger des informations en les transformant à l'aide d'un ensemble de techniques en vue de les rendre incompréhensibles aux yeux du grand public a vu le jour il y'a de cela des centaines d'années. Si donner une date exacte à la naissance de celle-ci n'est pas une mince affaire, beaucoup d'historiens s'accordent à situer les débuts de la cryptographie vers **l'antiquité**, et pour certains d'entre eux, au XVIème siècle avant Jésus-Christ. En effet, on atteste que le plus ancien document cryptographique serait une recette secrète de poterie découverte dans l'actuel Irak pendant cette période. Il a été chiffré en supprimant des consonnes et en modifiant l'orthographe de certains mots.

De nombreuses techniques de cryptographie ont été développées au fil des siècles durant lesquels la cryptographie était considérée comme un art avec très peu de règles ou de restrictions. Ce n'est que très récemment avec le développement de l'informatique (au XXIème siècle) qu'elle est devenue une science à part entière.

Historiquement, il y a eu deux grandes familles de méthodes de cryptographie à savoir **les codes à répertoires** et les **codes à clefs secrètes** qui englobent les méthodes à transposition ou à permutation, et les codes à substitutions.

1-1 Terminologie :

***Cryptologie :** signifie étymologiquement "science du secret" et englobe la cryptographie d'une part et d'autre part l'étude de l'ensemble des moyens possibles pour retrouver l'information codée sans en posséder la clef de déchiffrement appelée cryptanalyse.

***Clef de chiffrement :** il s'agit de l'élément essentiel de toute méthode de cryptographie. C'est le paramètre permettant de chiffrer les données dans un sens et de les déchiffrer dans le sens contraire.

***Chiffrement :** procédé par lequel une donnée ou une information en clair est transformée en un message codé à l'aide d'une clef de chiffrement.

***Déchiffrement :** récupération du message original à partir du message chiffré en utilisant une clef appelée clef de déchiffrement.

***Analyse de fréquence :** méthode de cryptanalyse qui vise à déduire le message clair en se basant sur le fait que pour chaque langue, il existe une fréquence à laquelle apparaît chaque lettre dans un texte. Il est utilisé en général pour casser les méthode basées sur la substitution alphabétique.

***Cryptosystème :** désigne l'ensemble des clefs possibles ou espace de clefs, des données claires et des données chiffrées possibles associés à un algorithme donné.

1-2 Méthode à répertoire :

Le principe de ces méthodes repose sur la mise en œuvre d'un document écrit sous forme de **dictionnaire de correspondance** faisant correspondre un mot ou une expression à un code alphanumérique. Le chiffrement et le déchiffrement se font en effectuant la bonne association entre le code et le mot qui lui correspond. On distingue des codes ordonnés et des codes désordonnés. Pour les codes ordonnés, on a un ordre alphabétique dans la partie chiffrée et dans la partie en claire : ça veut dire que si on utilise par exemple des valeurs numériques pour coder les messages, le dictionnaire se présentera sous la forme d'associations des chiffres dans l'ordre croissant d'un côté et des différents mots dans l'ordre alphabétique de l'autre côté.
Ce qui n'est pas le cas pour les codes désordonnés qui ne respectent l'ordre que dans un seul côté.

Pour les codes ordonnés, le même document est utilisé pour coder et décoder le message alors que pour les codes désordonnés, il y a un document pour chiffrer et un autre pour décoder.

Cette méthode est apparue vers la fin du **XVIIIème** siècle et a même été utilisé par le gouvernement américain à des fins diplomatiques. Son utilisation a connu un essor fulgurant dans la seconde moitié du XIXème siècle notamment avec l'avènement de la télégraphie. En effet, elle permettait de diminuer la facturation sur les télégrammes dans la mesure où on pouvait coder tout une phrase en quelques chiffres mais aussi de ne pas s'exposer à la concurrence lorsqu'il s'agissait de correspondances d'ordre financières, commerciales ou militaires.

L'avantage majeur de cette méthode est le fait qu'il soit pratiquement impossible de décrypter un message intercepté par analyse de fréquence ou tout autre approche d'attaque par le fait qu'il y'a un très grand nombre de combinaisons possibles pour déduire le message en clair.
Le point faible de ces systèmes est le fait qu'il repose sur un support physique qui peut être très volumineux et qui doit être envoyer à toutes les parties communicantes.

Le code télégraphique de Sittler est un exemple de méthode de codage appartenant à cette famille. Il utilise en entré une numérotation allant de 00 à 99 sur chaque page du document à laquelle elle fait correspondre des mots. Les règles d'encodages sont à fixer entre les correspondants.
Exemple d'un extrait d'une page du Code de Sittler :

50	Casquette
51	Cassation
52	Se pourvoir en cassation
53	Casser
54	Catastrophe
55	Catégorie
56	Catégorique,Catégoriquement
57	Cathédrale
58	Catherine
59	Catholicisme,Catholique

Figure 1 : *Extrait d'une page du code Sittler*

1-3 Méthodes à clefs secrètes :

" La clef doit pouvoir en être communiquée et retenue sans le secours de notes écrites et être changée ou modifiée au gré des correspondants " disait **Auguste Kerckhoffs** dans son article intitulé la *cryptographie militaire* publié en 1883 dans le journal des sciences militaires. Cet article composé de six principes pose les bases de la sécurité d'un cryptosystème et en même temps celle de la cryptographie moderne. En effet, il marque une rupture par rapport à ce qui se faisait précédemment notamment avec les codes à répertoires qui déjà présentaient l'inconvénient d'être très coûteux à mettre en place et aussi d'être vulnérable à de multiples attaques (interception du dictionnaire...).
Ce principe suggère que la sécurité d'une méthode cryptographique ne doit pas reposer sur le secret absolu ou sur le secret de la clef du fait que le facteur secret est en elle-même une cause première de fragilité car il pourra être divulguer un jour ou l'autre et dans ce cas, c'est le système tout entier qui

s’effondrera. Il sous-entend de garder secret ce qui est moins coûteux à changer si jamais le besoin se présente.

Il est clair que le principe de Kerckhoff n'exclut pas le facteur secret d’autant plus que tout système qui se réclame sécurisé dépend du fait de garder au moins un paramètre secret. Au contraire, un système sera d’autant plus résistant et sûr s’il a été conçu et mis au point avec la plus grande transparence et de ce fait, soumis à une large étude de la communauté cryptographique pour détecter d'éventuelles failles ou possibilités d’attaques du système.
Les méthodes à clefs se caractérisent par leur facilité d’utilisation et leurs applicabilités dans plusieurs domaines pour répondre à des besoins différents. On distingue les méthodes à clef privée et les méthodes à clef publique.

1-4 Les méthodes à clef privée :

Ces méthodes se basent sur l’utilisation d’une unique clef pour le chiffrement et le déchiffrement. Sans cette clef, il est impossible de retrouver les données en claires. Elle regroupe deux sous-groupes qui sont les méthodes à transposition et les méthodes de chiffrement par substitutions alphabétiques qui peuvent être monoalphabétiques ou polyalphabétiques.

1-4-1 Les chiffrements par transposition :

Appelés aussi chiffrement par permutation, elles consistent à subdiviser les données en clair en blocs de mêmes tailles et à effectuer un changement de l’ordre des caractères dans chaque bloc. La clef de chiffrement est alors ce changement d’ordre. C’est une méthode relativement sécurisée pour des blocs de grandes tailles qui augmentent le nombre de possibilités et donc diminue la vulnérabilité aux attaques. Ce système était utilisé depuis l'antiquité en générale dans le domaine militaire pour faire passer un message. **La Scytale spartiate** est considérée comme le plus ancien procédé de cryptographie de cette famille, son fonctionnement était comme suit :
On choisit un bâton avec des dimensions bien déterminés (le diamètre en particulier) sur lequel on enroule une bande qui est en générale une ceinture en cuir et on inscrit le message sur cette dernière. Ainsi, on a une juxtaposition de

caractères sur la ceinture qu'on ne pourra lire que si on possède un bâton avec les mêmes dimensions que celui utilisé initialement.
Il est clair que ce dispositif n'est pas très sécurisé vu qu'avec un peu de bon sens et quelques tentatives, le message pourra facilement être déchiffrer

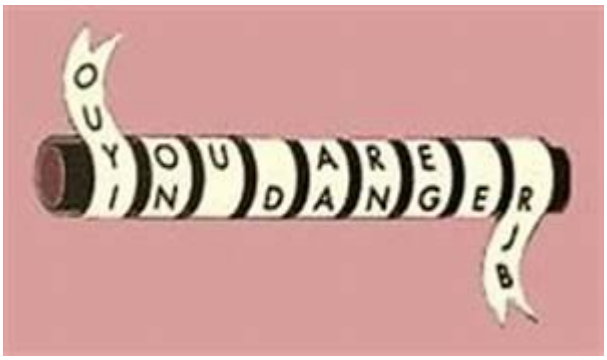


Figure 2 : *Scytale enroule d'un message*

.

1-4-2 Les chiffrements par substitution :

C'est des techniques qui opèrent sur les caractères d'un texte en clair en les changeant avec d'autres caractères du même alphabet ou d'un autre. Ils comprennent deux variantes : les méthodes à substitution monoalphabétique et ceux à substitution polyalphabétique.

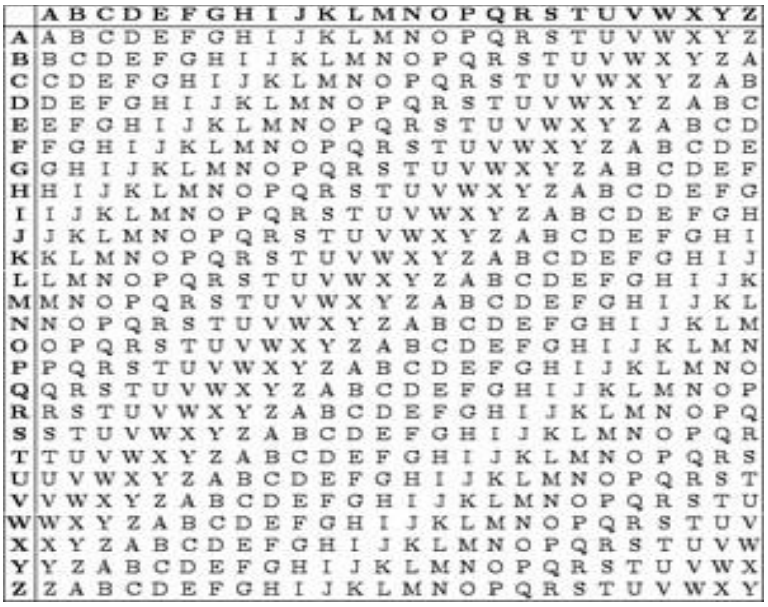
Dans les procédés de chiffrement par substitution monoalphabétique, un caractère du texte en clair sera toujours substitué avec le même caractère. Autrement dit, à un caractère en clair correspond une unique possibilité de chiffrement et vice-versa : à un caractère codé ne peut correspondre qu'un seul caractère clair. **Le chiffre de César** et **le Carré de Polybe** utilisent ce principe. Le chiffre de César, appelle aussi chiffrement par décalage consiste à remplacer

dans le même alphabet une lettre par la lettre située trois positions plus loin. Exemple, **a** sera substitué par **d, b** par **e,** et ainsi de suite...
Les chiffrements par substitutions polyalphabétiques quant à elles se basent sur un remplacement dynamique des caractères à chiffrer. En fait, les substitutions sont réalisées à l'aide d'une clef qui définit le décalage adéquat à observer. Les plus célèbres chiffres de cette famille sont **la machine Enigma** qui était activement utilisée aux environs de la seconde guerre mondiale et **le chiffre de Vigenère**. Cette dernière est une amélioration du chiffre de César qui présentait l'inconvénient d'être facilement décrypter par analyse de fréquence dans la mesure où un caractère donné était toujours codé de la même façon. L'amélioration dans ce système consiste à l'ajout d'une clef qui représente le décalage à observer pour chaque caractère du message en clair. On utilise pour cela **la table de Vigenère** qui fait la correspondance entre chaque caractère en clair et le caractère de la clef qui lui est associé pour faire la substitution avec le code approprié(caractère) ; la clef est répétée si besoin pour être de la même longueur que le texte en clair. Ainsi, avec une clef suffisamment longue et irrégulière, la sécurité du chiffrement est considérablement renforcée.

Exemple : soit à chiffrer le message suivant : **ESSAI DE CHIFFREMENT** avec la clef ***STATUT***

donnée en clair	E	S	S	A	I	D	E	C	H	I	F	F	R	E	M	E	N	T
Clef	S	T	A	T	U	T	S	T	A	T	U	T	S	T	A	T	U	T
décalage	18	7	0	19	6	19	18	19	0	7	20	19	8	19	0	19	6	7
donnée chiffrée	W	L	S	T	C	W	W	V	H	B	Z	Y	J	X	M	X	H	M

Figure 3 : *application du chiffrement de Vigenère sur un texte*



	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z
A	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z
B	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A
C	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B
D	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C
E	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D
F	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E
G	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F
H	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G
I	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H
J	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I
K	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J
L	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K
M	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L
N	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M
O	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N
P	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O
Q	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P
R	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q
S	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R
T	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S
U	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T
V	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U
W	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V
X	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W
Y	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X
Z	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y

Figure 4 : *table de Vigenère*

1-5 Méthodes à clefs publiques :

La force des méthodes de chiffrement à clef privée repose sur leurs rapidités de mise en œuvre et d'utilisation, en plus du fait que tant que la clef reste secrète, il est théoriquement impossible de déchiffrer des données cryptées par ces méthodes. Par ailleurs, il n'en est pas de même dans la réalité des choses. En effet, une fois que l'algorithme utilisé pour coder des données avec ces méthodes est découvert, il est possible de parvenir à les décrypter en procédant à une recherche exhaustive sur l'ensemble des clefs possibles et avec suffisamment de temps, parvenir à retrouver la clef privée de chiffrement. D'autre part, la clef privée en question nécessite d'être transmise ou communiquer vers le côté destination, ce qui représente une faiblesse supplémentaire des

méthodes symétriques car la clef peut être intercepté en cours de transmission.

La publication des travaux de **Diffle** et **Hellman** en 1976 apporte une solution au problème d'échange des clefs ; ce qui réduit les problèmes des approches symétriques de chiffrement et pose les bases de la cryptographie asymétrique encore appelée méthodes à clef publique.

L'échange des clefs Diffle-Hellman utilise un ensemble de propriétés et de principes de l'arithmétique modulaire pour mettre en place un protocole sécurisé d'échange de la clef privée. Cependant, cet échange nécessite la synchronisation des deux entités communicantes durant la phase d'élaboration des clefs. C’est ainsi que prennent naissance les méthodes de chiffrement à clef publique qui mettent en jeu une clef publique et une clef privée qui n’est jamais diffusée. On distingue plusieurs systèmes de chiffrement dans cette famille : El Gamal, les méthodes utilisant les courbes elliptiques, la méthode RSA etc.

Chapitre 2 : La gestion du projet

Introduction :

Ce chapitre décrit la conduite du projet. Il s'agira dans un premier temps de procéder à la spécification des besoins puis par la suite nous passerons à la planification du projet.

2-1 Spécification des besoins :

La spécification des besoins est la première phase du cycle de vie d'une application. Elle permet de bien comprendre le travail à réaliser et ainsi de mieux répondre aux exigences. Il s'agit d'une part de répondre aux besoins fonctionnels qui correspondent aux fonctionnalités que l'application doit offrir, c'est-à-dire ceux pourquoi elle a été développée et d'autre part, aux besoins non fonctionnels. Les besoins non fonctionnels ne sont pas intrinsèquement liés à la finalité de l'application, mais participent à sa bonne marche et caractérisent le système.
Dans notre cas, les besoins fonctionnels sont :
-Chiffrer un message en clair
-Déchiffrer un message crypté
-Authentifier un message donné.

Les besoins non fonctionnels sont :
-L'application doit être disponible et opérationnelle à tout moment
-L'application doit supporter les messages de grand taille
-L'application doit être facile à utiliser.

2-1 Planification du projet :

Le projet s'étale sur six mois durant lesquels on va procéder de la façon suivante :

- Documentation et compréhension du projet : un projet ne peut pas être entrepris sans connaitre son environnement et dans quel contexte il s'inscrit. Il faut donc faire une étude approfondie et détaillée du sujet afin de bien saisir le travail demandé.
- Spécification des besoins fonctionnels et non fonctionnels : afin de décrire la façon la plus précise possible les besoins auxquels le système doit répondre.

- Rédaction du rapport : consigner chaque avancement convenablement dans le rapport pour mieux organiser le travail et mesurer son avancement. La rédaction commence dés le début du projet et se complète au fur et à mesure de l'avancement de ce dernier.
- Conception et implémentation de la solution proposée : il s'agit de définir l'architecture et le fonctionnement de l'application et ensuite passer à sa réalisation avec le langage et les technologies adaptées enfin procéder à des tests.

Conclusion :

Dans ce chapitre, nous avons effectué une spécification des différents besoins qui va nous permettre de mieux aborder la solution à réalisé et nous avons établit un planning des différentes étapes à suivre pour concrétiser le projet.

Chapitre 2 : Outils de base et Chiffrement par la méthode RSA

Introduction (Quelques notions mathématiques utiles) :

Le succès de l'algorithme RSA et sa longévité en tant que référence en matière de chiffrement asymétrique sont dues entre autres au fait qu'il repose fortement sur un ensemble de fondement et d'outils mathématiques qui en garantissent la sécurité. Il est donc nécessaire de jeter un coup d'œil sur quelques-unes de ces principes avant d'entamer l'étude proprement dite de la méthode RSA.
Cette section est donc dédiée à la présentation de ces propriétés mathématiques. Nous allons parler de la congruence sur les entiers, du petit théorème de Fermat et de d'autres concepts et théorèmes en rapport avec l'arithmétique.

3-1 Congruence sur les entiers :

Définition : deux entiers **a** et **b** sont dits **congrus modulo n** s'ils ont le même reste par la division par n. Autrement dit, a et b sont congrus modulo n s'il existe un entier k tel que :

b - a = k * n

On note **a ≡ b mod n** (notation de **Gauss)** et on lit : **a est congru à b modulo n.**

Exemple : 26 et 12 sont congrus modulo 7. En effet,

26 - 12 = 14 = 2 * 7

On peut également voir que :

26 = 3 * 7 + **5** et que 12 = 1 * 7 + **5**

D'où **26 ≡ 12 mod 7**

3-2 Le petit théorème de Fermat :

Enoncé : Si **p** est un **nombre premier** et si **a** est un entier non divisible par p, alors $a^{p-1} - 1$ est un **multiple de p.** Autrement dit, a^{p-1} est **congru à 1 modulo p.**

On peut aussi le formuler de cette façon : Si **p** est un nombre premier et si **a** est un **entier quelconque,** alors $a^{p} - a$ est un **multiple de p.**

Exemple : pour a=5 et p=3 , 3 est premier et 5 n'est pas divisible par 3. Donc d'après **Fermat,** $5^2 - 1 = 24$ est un multiple de 3

3-3 L'exponentiation modulaire :

Définition : l'exponentiation modulaire consiste au fait qu'étant donné trois entiers **e , b** et **m** de trouver un nombre **c** tel que :

$$c \equiv b^{e} \bmod m$$

Si e,b et m sont **positifs ou nuls** et b < m**,** alors c est **unique** et vérifie la condition $0 \leq c < m$,

c peut être trouver de façon naïve en effectuant l'opération $b^{e} \bmod m$; c est le reste de cette opération.

Exemple : Trouvons c pour b=4, e=13 et m=497

On a : $4^{13} = 67108864 \% 497 = 445$ alors c = 445.

3-4 L'indicateur d'Euler :

Définition : On appelle indicateur d'Euler, fonction Phi d'Euler ou fonction Phi la fonction φ définie telle que :

$\varphi : \mathbb{N}^* \rightarrow \mathbb{N}^*$
$n \rightarrow \text{card}(\{m \in \mathbb{N}^* \mid m \leqslant n \text{ et } m \text{ premier avec } n\})$.

Exemple : $\varphi(8) = 4$,en effet, sur [1;8] seul les nombres 1,3,5 et 7 sont premiers avec 8 d'où $\varphi(8) = 4$

3-5 Algorithme d'Euclide étendu :

Description : Cet algorithme est comme son nom l'indique une extension de l'algorithme classique d'Euclide qui permet étant donné deux nombres **a** et **b** de trouver leur plus grand diviseur commun(pgcd). L'extension consiste à trouver en plus du **pgcd, les coefficients de Bézout** des deux nombres qui sont définie comme suit :

si **d** est le pgcd de **a** et **b,** alors il existe des entiers **u** et **v** tels que:

au + bv = d

Pour ce faire, on applique l'algorithme d'Euclide pour trouver le pgcd de a et b et pour chaque reste trouver, on l'exprime en fonction de a et b.

Exemple : appliquons cet algorithme pour a=255 et b=141

255 = 1*141+114	|	r1=114=1*255 - 1*141
141 = 1*114 + 27	|	r2=27= 1*141 - 1*114 r2 = 1*141 - 1*(255 - 141) r2 = 2*141 - 1*255
114 = 4*27 + 6	|	r3= 6 = 1*114 - 4*27 r3= 1*114 - 4*(141- 114) r3= 5*114 - 4*141 r3= 5*(255 - 141) - 4*141 r3=5*255 -9*141
27 = 4*6 + 3	|	r4= 3 = 1*27 - 4*6 r4=3=2*141-255 - 4*(5*255 -9*141) r4=3=38*141-21*255
6 = 2*3 + 0	|	r5=0;

On a donc d=3 (dernier reste non nul) et 3=38*141 - 21*255

d'où d= au +bv = 38*141 - 21* 255

38 et 21 sont les coefficient de **Bezout** de a et b.

4 La méthode de chiffrement RSA :

4-1 Présentation de la méthode :

En 1976, **Whitfield Diffie** et **Martin Hellman**, deux cryptologues américains publient ***New Directions in Cryptography,*** un article qui va révolutionner le monde de la cryptographie. Ils traitent dans cet article des problèmes que rencontrait la discipline à l'époque et plus précisément celui de la distribution des clefs dans un cryptosystème. En effet, le Data Encryption Standard (**D.E.S.**) d'IBM qui était à l'époque le standard en matière de cryptographie souffrait de ce problème. D'ailleurs, ils affirment dans l'article que " *Le problème le plus connu en cryptographie est celui de la confidentialité : prévenir les interceptions indésirées d'informations provenant d'une communication à travers un canal non sécurisé."*

Ils soutiennent que les systèmes de distribution de clefs publiques offrent une approche différente pour éliminer le besoin d'un canal(sécurisé) de distribution des clefs. Cet article décrit un cryptosystème à clef publique d'une façon assez théorique ; sachant que ce n'est qu'en Avril 1977 que deux chercheurs américains du Massachusetts Institute of technology (**M.I.T.**) **Ronald Rivest** et **Leonard Adleman** avec la collaboration du mathématicien Israélien **Adi Shamir** fournissent pour la première fois une implémentation de ce type de cryptosystème. Leur article montrait comment préserver la confidentialité et comment authentifier des messages dans le cadre d'une transmission. Ils décrivent leur processus à travers un algorithme nommé **RSA (R**ivest **S**hamir **A**dleman). La grande sûreté de cette méthode ainsi que sa difficulté à être casser le rend rapidement très populaire. Son utilisation s'est rapidement répandue avec l'avènement des nouvelles technologies et s'étend dans presque tous les secteurs du numérique, notamment celui du commerce en ligne de nos jours.

4-2 Description et fonctionnement de la méthode RSA:

Dans leur article *New Direction in Cryptography,* Diffie et Hellman définissent la cryptographie comme l'étude des systèmes “mathématiques” pour résoudre deux types de problèmes : la confidentialité et l’authentification. La méthode RSA fournit des solutions à ces problèmes.

La confidentialité consiste à rendre une communication privée, c’est-à-dire la rendre accessible uniquement aux parties prenantes. L’émetteur chiffre son message et l’envoi au récepteur qui dispose des moyens nécessaires pour retrouver le texte original à partir du cryptogramme reçu. Il est important de signaler qu’il n’est pas nécessaire que les échanges de messages passent par des canaux sécurisés.
L’authentification(signature) est une autre application de la cryptographie visant à certifier l'identité de l'émetteur, c’est-à-dire que pour une donnée reçue d’un supposé émetteur X, comment prouver qu’il provient effectivement de lui, d’une part. D’autre part, garantir que la donnée reçue ne puisse pas être modifiée par le récepteur pour diverses raisons que ce soit et qu’il soit toujours associé à l'émetteur initial. Cela veut dire que la signature doit avoir une dépendance absolue avec son auteur ou bien avec le message auquel il est associé.

4-3 Procédure de chiffrement et de déchiffrement RSA :

La première chose à faire pour chiffrer des données en utilisant la méthode RSA est de générer les clefs.
Tout d'abord, il faut choisir deux nombres premiers relativement grand qu’on va noter **p** et **q** et ensuite calculer **n=p*q.**

On recommande généralement d’effectuer le choix de p et q de façon aléatoire. Le nombre **n** est rendu **public** alors que **p** et **q** doivent rester **secret.**

Ensuite choisir aléatoirement un entier noté **d** premier avec **(p-1)*(q-1)**

c’est-à-dire : pgcd(d,(p-1)(q-1)) = 1

La clef de chiffrement **e** est l’inverse multiplicatif de d modulo (p-1)(q-1),on a:

$$e*d \equiv 1 \ (\mathrm{mod}((p-1)*(q-1)))$$

Pour trouver **e,** on applique l’algorithme d’Euclide étendu sur **(p-1)*(q-1)** et **d** en exprimant chaque reste avec ses coefficients de Bézout. Dès qu’on trouve un reste égal à 1, alors **e** correspond à son coefficient de Bézout **b.**

À la suite de ce processus, on a la clef de **chiffrement** qui est le couple **(e,n)** et celle de **déchiffrement** qui correspond au couple **(d,n).**

Les correspondants mettent chacun leurs clefs de chiffrement publique et gardent celles de déchiffrement privé.

L'étape suivante est celle du chiffrement du message. Pour ce faire, on représente le message ou la donnée qu’on désire transmettre sous forme numérique**.** Pour les messages longs, il peut s'avérer nécessaire de les subdiviser en blocs et de numériser chaque bloc convenablement. La valeur de chaque bloc doit être comprise entre **0** et **n-1.**

Soit **M** le message sous forme numérique, le cryptogramme **C** est obtenu comme suit :

$$C = e(M) \equiv M^{e} \ \mathbf{mod\ (n)}$$

Le message original est donné par :

$$M = d(C) \equiv C^{d} \ \mathbf{mod\ (n)}$$

4-4 Exemple d'application :

On choisit p=31 et q=53, on aura donc n=p*q=1643 et (p-1)*(q-1)=1560

On choisit aussi d=851, on a bien pgcd (851,1560) = 1

Calculons **e :**
Appliquons l'algorithme d'Euclide étendu pour trouver les coefficients de Bézout de **a=1560** et **b=851** :

1560 = 1*851 + **709**	**|**	709 = 1560 - 851
851 = 1*709 + **142**	**|**	142 = 851 - 709 142 = 851 - (1560 - 851) 142 = -1*1560 + 2*851
709 = 4*142 + **141**	**|**	141 = 709 - 4*142 141 =1560-851- 4*(-1560 +2*851) 141 = 5*1560 - 9*851
142 = 1*141 + **1**	**|**	1 = 142 - 141 1= -1560+2*851 - (5*1560 - 9*851) 1 = -6*1560 + 11*851

Donc la clef de chiffrement est **e = 11** et par suite :
La clef publique est le couple (11,1643) et la clef privée est (851,1643).

Soit à chiffrer le texte suivant : **TEST ENCRYPION RSA** en utilisant l'ordre alphabétique des lettres comme méthode de numérisation du message.

Ce qui donne la représentation numérique suivante :

20 05 19 20 05 14 03 18 25 16 09 15 14 18 19 01

Avec n=1643, on peut chiffrer le message ci-dessus en utilisant des blocs de trois chiffres, sachant qu'un caractère est représenté sur deux chiffres, Ce qui donne :

020 051 920 051 403 182 516 091 514 181 901

c1 = 020^{11} mod(1643) = 224
c2 = 051^{11} mod(1643) = 1185
c3 = 920^{11} mod(1643) = 1004
c4 = 051^{11} mod(1643) = 1185
c5 = 403^{11} mod(1643) = 1333
c6 = 182^{11} mod(1643) = 1143
c7 = 516^{11} mod(1643) = 813
c8 = 091^{11} mod(1643) = 587
c9 = 514^{11} mod(1643) = 59
c10 = 181^{11} mod(1643) = 874
c11 = 901^{11} mod(1643) = 901

-Déchiffrement :

d1 = 224^{851} mod(1643) = 20
d2 = 1185^{851} mod(1643) = 51
d3 = 1004^{851} mod(1643) = 920
d4 = 1185^{851} mod(1643) = 51
d5 = 1333^{851} mod(1643) = 403
d6 = 1143^{851} mod(1643) = 182
d7 = 813^{851} mod(1643) = 516
d8 = 587^{851} mod(1643) = 91
d9 = 59^{851} mod(1643) = 514
d10 = 874^{851} mod(1643) = 181
d11 = 901^{851} mod(1643) = 901

Sachant qu'on a utilisé des blocs de trois entiers, il faudra juste compléter les blocs de tailles inférieures à trois par des 0 à gauche.
On retrouve donc après ce procédé :

020 051 920 051 403 182 516 091 514 181 901

Sachant qu'on a utilisé l'ordre alphabétique pour numériser les caractères et que chaque caractère est représenté par deux chiffre, on retrouve le message en clair :

20	05	19	20	05	14	03	18	25	16	09	15	14	18	19	01
T	E	S	T	E	N	C	R	Y	P	I	O	N	R	S	A

On vient ainsi de d'envoyer un message crypté avec l'algorithme RSA. On signale que la méthode de numérisation utilisée ici (position alphabétique des lettres) n'est pas la seule façon de faire, d'autres techniques peuvent être employées du moment que le récepteur en est informé. Par ailleurs, on pouvait aussi choisir de diviser le message en des blocs de quatre en respectant bien sûr la contrainte sur la taille des messages (<n-1).

Chapitre 4 : Application

Exécution de l’application et visualisation des résultats :

Dans cette partie, on a testé le cryptage et le décryptage d’un message avec notre implémentation de la méthode RSA en Java. Cette implémentation consiste en un programme console auquel on fournit les informations de chiffrements ainsi que la chaine à chiffrer et qui procède au chiffrement et ensuite au déchiffrement de ce message en différents étapes.

Le contenu de la fonction principale :

```
String s= "Mohamed el ghaouth";
RSA1 r1=new RSA1(50);
System.out.println("Le message à crypter est : "+s);
System.out.println(" ");
r1.decripter(r1.cripter(r1.split_to_blocs(r1.convert_to_bited(s))));
```

Les informations de chiffrement :

```
|
RSA [n=711995029304633, e=677794963209845, d=99475603209821, taillecle=50, blocsize=7]
```

```
Le message à crypter est : Mohamed el ghaouth
```

Comme indiqué ci-dessus, il s’agit ici de chiffrer le texte « **mohamed el ghaouth** » avec la clé de chiffrement (e,n)

```
convertie le message en code ascii :

77 111 104 97 109 101 100 32 101 108 32 103 104 97 111 117 116 104
```

Ci-dessus, Le texte en clair est numérisé en utilisant le code ascii de chaque caractère. Ce qui nous permet de passer à l'étape suivante qui consiste à subdiviser le message en bloc de même taille :

```
decoupage du message en bloc:

7711110 4971091 0110032 1011083 2103104 9711111 7116104
[7711110, 4971091, 110032, 1011083, 2103104, 9711111, 7116104, 7]
```

Ensuite on applique la procédure de chiffrement sur chaque bloc ; ce qui nous donne de nouveaux blocs de données cryptés :

```
les blocs crypte
[345188857868356, 1925337386524, 657637643428566, 321458390284088, 575551944555169, 66954862022073, 316325663353438, 7]
345188857868356 1925337386524 657637643428566 321458390284088 575551944555169 66954862022073 316325663353438
```

Ces blocs cryptés représentent le message crypté qui correspond à une chaine de caractère quelconque :

```
le message crypté est :
.@B??▯v▯
```

el

On passe maintenant au déchiffrement du message codé. Il s'agit ici de retrouver le message en clair grâce à la clé de déchiffrement (d,n).Tout d'abord on reconstitue les blocs initiales du message :

```
decryptage

les blocs initiales :
[7711110, 4971091, 110032, 1011083, 2103104, 9711111, 7116104, 7]
```

Puis de là, on remet les blocs sous forme de caractères :

```
chaine code ascii initiale:
771111049710910110032101108321031049711111 7116104
```

Et finalement, on retrouve le message initial qu'on avait chiffrer :

```
la chaine de cractere initiale
Mohamed el ghaouth
```

Conclusion générale

La réalisation de ce projet nous a permis de découvrir l'univers passionnant de la cryptographie et de pouvoir saisir toute son importance et les enjeux économiques qu'elle implique.

Dans la première partie du travail, nous nous sommes basés sur des livres, des articles scientifiques et des publications de certains sites internet pour pouvoir bien comprendre la cryptographie depuis ces origines jusqu'à l'état actuel du domaine notamment les derniers standards en vigueur.

L'étude détaillée de la méthode RSA ainsi que l'exemple illustratif que nous avons proposé nous ont permis d'avoir les idées claires sur la façon dont on devrait implémenter cette méthode. D'ailleurs, concernant l'application proprement dit, une présentation lui sera exclusivement dédié afin d'expliquer les détails de sa conception et son fonctionnement ; de l'envoi d'un message à sa réception en passant par les différentes étapes de chiffrement et de déchiffrement.

Références :

-Initiation à la cryptographie(2eme edition) de GILES DUBERTRET

-L'univers secret de la cryptographie de GILES DUBERTRET

-Histoire des codes secrets de SIMON SINGH

-La guerre des codes secrets de DAVID KAHN

-Notes de cours sur la cryptographie du professeur RENAUD DUMONT de la faculté des sciences et techniques de l'université de Liège (Belgique)

-Support de cours du professeur E. THOME de l'INRIA de Nancy

-Manuel de cryptographie des professeurs DANIEL BARSKY et GHISLAIN DARTOIS de l'université Paris 13

-New directions in cryptography de WHITFIELD DIFFIE et MARTIN HELLMAN

-A method for obtaining digital signatures and public key cryptosystems de RON RIVEST, ADI SHAMIR et LEONARD ADLEMAN

-Wikipedia.org

-bibmath.net