

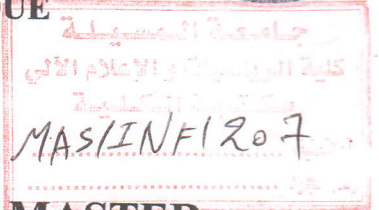
REPUBLIQUE ALGERIENNE DEMOCRATIQUE ET POPULAIRE
MINISTERE DE L'ENSEIGNEMENT SUPERIEUR ET DE LA RECHERCHE SCIENTIFIQUE



UNIVERSITE MOHAMED BOUDIAF - M'SILA
FACULTE DES MATHÉMATIQUES ET
DE L'INFORMATIQUE



DEPARTEMENT D'INFORMATIQUE



MEMOIRE de fin d'étude

Présenté pour l'obtention du diplôme de **MASTER**

Domaine : Mathématiques et Informatique

Filière : Informatique

Spécialité : Technologie de l'Information et de Communication

Par : Mahdi Hamza

SUJET

**étude et comparaison des principaux systèmes de cryptage
et les technique y afférentes**

Soutenu publiquement le : / /2016 devant le jury composé de :

M. El khier DEHMECHE

Université de M'sila

Encadreur

.....

Université de M'sila

Président

.....

Université de M'sila

Rapporteur

.....

Université de M'sila

Examineur

Promotion : 2015/20 16

Table des matières

CHAPITRE 1 GÉNÉRALITÉS SUR LA SÉCURITÉ INFORMATIQUE

1	Introduction	4
2	Introduction à la sécurité	4
2.1	Terminologie de la sécurité informatique	4
2.2	L'objectif de la sécurité	5
3	Les attaques	6
3.1	Types d'attaques	6
3.2	Les différentes étapes d'une attaque	6
4	Domaines d'application de la sécurité	6
5	aspects techniques de la sécurité informatique	7
6	Mécanismes de sécurité	7
6.1	Cryptage	7
6.2	pare-feu	8
6.3	Antivirus	9
7	Détection et prévention d'intrusions	9
8	Conclusion	10

CHAPITRE 2 INTRODUCTION A LA CRYPTOLOGIE

1	Introduction	12
2	Définitions et mots clés	12
2.1	Vocabulaire de base	12
2.2	Les objectifs de la cryptographie	15
3	Histoire de la cryptologie	17
4	Techniques classiques de chiffrement	18
4.1	Historique de cryptographie	18
4.2	La cryptographie classique	20
5	Quelques algorithmes classiques	21
5.1	Les scytales des Spartiates	21
5.2	chiffrement de César	21

5.3	Le chiffre de Hill	22
5.4	Chiffrement de VIGENERE (1523-1596)	23
6	chiffrement mécanisé (La machine ENIGMA)	24
7	Conclusion	26

CHAPITRE 3 LA CRYPTOGRAPHIE MODERNE

1	Introduction	28
2	Techniques de cryptographie.....	28
2.1	La cryptographie à clé secrète (symétrique)	28
2.1.1	Le chiffrement par bloc (block cipher).....	29
2.1.2	Chiffrements de flot (Stream Cipher).....	30
2.1.3	Quelque algorithmes de La cryptographie à clé secrète (symétrique)	31
2.2	La cryptographie à clé publique.....	34
2.2.1	Les avantages de la cryptographie asymétrique sont :	34
3	La signature numérique (ou digitale).....	36
3.1	Les principaux algorithmes de signature	37
3.1.1	Digital Signature Standard (DSS).....	37
3.1.2	La signature RSA	37
4	Fonctions de hachage.....	38
4.1	Algorithmes de hachage :	38
4.1.1	Algorithme de hachage sécurisé SHA :	38
4.1.2	L'algorithme MD5 (Message Digest version 5).....	39
5	Code d'authentification de message MAC	40
6	Conclusion.....	41

CHAPITRE 4 IMPLÉMENTATION ET RÉALISATION

1.	Introduction	29
2.	L'environnement de développement	29
3.	Les applets de simulation	43
4.	L'architecture de notre système.....	43
5.	Implémentation et résultat :	44
1.1.	5.1 Calcul de l'exécution de temps et l'espace mémoire	44
	5.2 Comparaison et performance des tests des algorithmes	47
	5.2.1 Le temps d'exécution.....	47
6.	Quelque interface de notre projet	50

7 conclusion.....	51
CONCLUSION GÉNÉRALE.....	52

Liste des Figures :

Numéro	Titre	page
1.1	Fonctionnement de chiffrement	8
1.2	Fonctionnement d'un pare-feu	9
2.1	Protocole de chiffrement	12
2.2	histoire de la cryptologie	17
2.3	Le Scytale Spartiate	21
2.4	Chiffrement de César	22
2.5	La table de Vigenère	24
3.1	La cryptographies à clé secrète	29
3.2	Le chiffrement par bloc	30
3.3	algorithme DES	32
3.4	La cryptographies à clé publique	35
3.5	La signature numérique	37
3.6	Fonctions de hachage	38
3.7	Algorithm SHA	39
3.8	L'algorithme MD5	40
4.1	NetBeans	42
4.2	l'architecture de système	43
4.3	Comparaison RSA vs EL-GAMMAL et ECC	47
4.4	Comparaison d'AES vs RC4	48
4.5	Comparaison de RSA vs ECC	49

4.6	interface générale	50
4.7	méthode de hachage	50
4.8	chiffrement symétrique	51
4.9	cryptage en web	51

Liste des tableaux

Numéro	Titre	Page
2.1	l'objectifs de la cryptographies	15
2.1	Historique de cryptographies	18
4.1	Sélection des paramètres	44
4.2	RSA	44
4.3	EL-Gamal	45
4.4	ECC	45
4.5	AES	45
4.6	RC4	46
4.7	RSA dans le web	46
4.8	ECC dans le web	46
4.9	techniques de hachage	47
4.10	Comparaison RSA vs EL-GAMMAL et ECC	47
4.11	Comparaison d'AES vs RC4	48
4.12	Comparaison de RSA vs ECC	49

INTRODUCTION GENERALE

Tout au long l'histoire, l'être humain a essayé d'envoyer ou bien de transmettre des informations de manière sécurisée, c'est à dire confidentielle. le chiffrement d'information a été utilisé comme instrument de sécurisation pour des stratégies militaires et des changes de données secrètes au cours de la seconde guerre mondiale, ou encore de nos jours où les banques recherchent des techniques fiables pour assurer à leurs clients des moyens de régler leurs achats sans risque de fraude, la cryptographie s'est imposée comme passage incontournable dans le transit des informations sensibles.

Utilisée sous diverses formes, sans cesse en progrès, la cryptographie reste une science peu connue quant à son fonctionnement. Si ses formes primitives (remplacement d'un alphabet par un autre, usage de pseudo-langues, de dessins...) sont connues du grand public, les applications modernes, avec usage des mathématiques, de la physique quantique, et des technologies les plus avancées, le sont beaucoup moins. Les utilisateurs de logiciels de cryptage destinés au grand public comme RSA, AES, PGP..., sont certes nombreux, mais ignorent le principe de fonctionnement du programme qu'ils utilisent. Le but de cette étude n'est pas d'être exhaustive quant aux différents algorithmes de cryptage existant, bien trop nombreux pour être seulement cités dans le cadre d'un mémoire de master, mais bien de servir d'introduction à la découverte d'un univers en plein essor, riche en innovations et problèmes irrésolus, en défis humains et informatiques.

Un survol de la méthode des classiques ou à algorithme secret sera effectué dans la première partie du mémoire. La base de la cryptographie et aussi sa plus ancienne application à savoir la cryptographie à clé secrète ainsi que la cryptographie à clé publique, plus récente, et sur laquelle sont fondés beaucoup d'espairs, seront toutes les deux abordées dans la deuxième partie. Les activités annexes telles que les fonctions de hachage, la signature électronique. Le point qui sera abordé en dernier concerne le côté pratique du mémoire où sera menée une étude comparative de plusieurs algorithmes cryptographique pour ce qui concerne le chiffrement, le déchiffrement et le hachage. Les plans détaillés de chaque partie ainsi qu'une brève introduction seront présentés au début de chacune.

L'objectif de ce mémoire :

Dans ce mémoire, nous allons répondre aux questions souvent posées par ceux qui veulent avoir un aperçu sur la cryptographie, ses méthodes, ses forces et ses faiblesses ainsi que sur son utilisation pratique :

- Quelles sont les différentes formes qu'a prises la cryptographie à travers le temps ?
- Quel est l'intérêt de la cryptographie moderne et de son utilisation pratique ?
- Quels sont les avantages de la cryptographie à clé secrète et celle à clé publique ? Et quel est le moyen pratique pour combiner les deux méthodes afin de tirer profit des avantages de chacune des deux méthodes ?
- Quels sont les algorithmes cryptographiques fiables par rapports aux autres et quels sont les ordres de grandeur de vitesse, de tailles des clés ?

À travers la réponse sue ces questions on a :

- Comprendre comment la cryptographie permet d'atteindre les différents objectifs (confidentialité, intégrité, authentification, etc.) reliés à la sécurité informatique.
- Comprendre comment la cryptographie est mise en œuvre dans certaines applications réelles (courrier électronique, commerce électronique, etc...).
- Réaliser un logiciel regroupant plusieurs algorithmes de chiffrement, déchiffrement et de hachage puis l'exécuter afin d'obtenir quelques résultats qui vont servir à mener une étude comparative entre ces algorithmes.
- Développer des simulateurs en applets Java afin de vulgariser l'utilisation pratique des différentes méthodes citées à travers ce mémoire.

L'organisation de mémoire :

Pour le plan méthodologique de ce mémoire, nous allons diviser en quatre chapitres :

- Le premier chapitre présente une vue générale sur la sécurité informatique
- Le deuxième chapitre présenté la cryptographie classique tel que l'histoire de la cryptographie et sa l'objectifs et l'étude de quelque algorithmes classique.
- La troisième chapitre étudie la cryptographie moderne (La cryptographie à clé secrète et à clé publique, la signature numérique, fonctions de hachage) et l'analyse de quelque algorithmes.
- Le quatrième chapitre traite l'implémentation d'un certain algorithme (classique, symétrique, asymétrique) sur différents plateforme (Windows, exploiteur), et ensuite tester la performance de chaque algorithme, et à la fin la comparaison des résultats avec une discutassions.

CONCLUSION GÉNÉRALE

[01] Ce projet a été réalisé dans le cadre de projet de fin d'étude niveaux master au sein de
[02] département des MI (mathématique et informatique) d'université de M'SILA. Dans lequel nous
[03] avons appliqué toutes les compétences et connaissances acquises durant les années d'étude.

[04] Notre travail se résumé en étude et comparaison des principaux systèmes de cryptage et les
[05] technique y afférentes.

[06] A travers notre étude, nous avons vu un panel de méthodes de chiffrement de l'antiquité à
[07] nos jours, les attaques existantes sur les cryptosystèmes actuels les plus utilisées et les moyens
[08] inventés pour s'assurer de l'intégrité, de l'authentification de l'expéditeur et du destinataire
[09] d'un message.

[10] Ainsi, la cryptographie est une science en perpétuelle évolution, la cryptanalyse l'aidant à
[11] trouver les failles d'un système pour toujours avancer. Cette évolution est importante car la
[12] cryptographie joue un grand rôle dans la sécurité internationale, tout étant aujourd'hui
[13] informatisé.

[14] Dans notre projet, nous avons utilisé le JAVA-NetBeanse comme environnement de
[15] programmation.

[16] En effet, malgré les grosses difficultés qu'on a rencontré, des quelles la non organisation et
[17] moins de l'expérience, le peu de temps consacré à cette étude, l'implémentation de notre projet
[18] fut l'une des majeures difficultés que nous avons rencontré, choix du langage de programmation
[19] plus efficace. Nous pouvons dire qu'on a très bien tiré profit de ce travail et qu'en toutes
[20] circonstances, on a appris beaucoup de choses : le travail en groupe, les technique et les
[21] compétences acquises dans le domaine du la cryptographie, la maîtrise et le savoir-faire dans
[22] les domaines de l'analyse et la conception, ainsi que beaucoup d'autres connaissances
[23] concernant le milieu de la sécurité.

[12] SecurityInfo.com, L'AES : Advanced Encryption Standard

<http://www.securityinfo.com/cryptographie/aes.html>

[13] Bayart, Frederic. La sage du DSS. <http://www.himath.net/crypt>

[14] Jason Wehrbridge . Walter Nyland "NetBeans Platform for Beginners", Lean Publishing

31-08-2014

[15] STANDARDS FOR EFFICIENT CRYPTOGRAPHY, SEC 2: Recommended Elliptic
Curve Domain Parameters, Certicom Research

<http://www.1024.org/hall/efsec2.html>

BIBLIOGRAPHIE

- [01]: STERN JACQUES, "La science du secret", Editions Edile Jacob, 1998
- [02] BRUCE SCHNEIER: "Applied Cryptography, Second Edition: Protocols, Algorithms, and Source Code in C", John Wiley & Sons, Inc., 01/01/96
- [03] A. MENEZES, P. VAN OORSCHOT, AND S. VANSTONE: "Handbook of Applied Cryptography", CRC Press, 1996 .
- [04]: DAVID KAHN, "The Codebreakers: The Story of Secret Writing", New York: Macmillan Publishing Co., 1967.
- [05]:Hacini Souleyman Boumedyen, "Implémentation d'algorithmes de Cryptographie", Université Abou Bakr Belkaid- Tlemcen Faculté des Sciences Département d'Informatique, 2013-2014
- [06]: HILL LESTER S., "Cryptography in an Algebraic Alphabet", American Mathematical Monthly-N36-P306à312, 1929
- [07]: Mahammedi Nadjiba, Mahdadi Houda, "Implémentation de benchmark d'opérations crypto basées ECC pour l'étude et comparaison de courbes elliptiques, Mémoire MASTER ACADEMIQUE, UNIVERSITE KASDI MERBAH OUARGLA, 2012 /2013
- [08] National Institute of Standards and Technology (NIST), Secure Hash Standard. Federal Information Processing Standards Publication 180-2, 2002, en ligne
<http://csrc.nist.gov/publications/fips/fips180-2/fips180-2.pdf>.
- [09] Niels Ferguson, Bruce Schneier. Practical Cryptography. Indiana: Wiley Publishing, Inc. : s.n., 2003
- [10] T. El Gamal, A public key cryptosystem and signature scheme based on discrete logarithms. IEEE Transactions on Information Theory IT-31, 496-473,1976.
- [11] El Khier DEHMECHE, ETUDE ET COMPARAISON DES PRINCIPAUX SYSTEMES DE CRYPTAGE, diplôme de magister en informatique, université M'sila, 2006.
- [12] SecuriteInfo.com, L'AES : Advanced Encryption Standard
<http://www.securiteinfo.com/cryptographie/aes.shtml>.
- [13] Bayart, Frederic. La saga du DES. <http://www.bibmath.net/crypto>.
- [14] Jason Wexbridge , Walter Nyland, "NetBeans Platform for Beginners", Lean Publishing, 31-08-2014
- [15] STANDARDS FOR EFFICIENT CRYPTOGRAPHY, SEC 2: Recommended Elliptic Curve Domain Parameters, Certicom Research
http://www.secg.org/collateral/sec2_final.pdf.

[16] JeF Hoffstein, Nicholas Howgrave-Graham, Jill Pipher, Joseph H. Silverman, William Whyte, Performance Improvements and a Baseline Parameter Generation Algorithm for NTRUSign, 5 Burlington Woods, MA 01803.

<https://www.securityinnovation.com/uploads/Crypto/NTRUSignParams-2005-08.pdf>.

[17] Site généraliste sur les réseaux. <http://www.orbytes.fr>

[18]: FEDERAL INFORMATION PROCESSING STANDARDS PUBLICATION, "Digital Signature Standard (DSS)", FIPS PUB 186, 19 Mai 1994

[19]: Santa Clara, An Introduction to Cryptography, Copyright © 1990-1999 Network Associates, Inc. and its Affiliated Companies, pages 11, 15.

الملخص:

ان الهدف من هذه المذكرة هو دراسة علم التشفير وتطوره مع مرور الزمن، و إيجاد افضل أنظمة التشفير الفعالة في مجال تكنولوجيا المعلومات، من حيث، السرعة واستهلاك سعة الذاكرة ودرجة الأمان مع الاخذ بعين الاعتبار بيئة التطوير، وذلك بإجراء دراسة تحليلية لمختلف خوارزميات التشفير، المتماثل مثل (AES, RC4...) والغير المتماثل (RSA, ECC...).

كلمات دلالية: تشفير، خوارزمية، سرعة التشفير، AES, RSA, hachage, ECC,

Abstract:

The purpose of this research paper is study cryptography science, and Evolved with the times. as well find a better and efficient cryptography algorithmn that use on information techology, frome memory usage and safty degrees, whitout ingrowibg Development environment during act analy stady a defferent symtric cryptography algorithms as RC4 , AES, and asymtric cryptography as RSA, ECC .

Keys words: cryptography, algorithms, hachage, ECC, performance.

Résume:

L'objectif de ce mémoire est L'étude de la cryptographie et son développement avec le temps de trouver des systèmes de cryptage plus efficaces (en fonction de la vitesse et l'aspect de sécurité), dans le domaine des technologies informatique et adaptés pour les différents environnements de programmation, en fait une étude et comparaison chiffrement/déchiffrement : soit symétrique (AES, RC4...), asymétrique (RSA, ECC...).

Mottes clés : cryptage, algorithme, hachage, ECC, performance.