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

UNIVERSITE MOHAMED BOUDIAF - M'SILA
FACULTE DES MATHEMATIQUES 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**	**Examinateur**

Promotion : 2015/20 16

Table des matières

CHAPITRE 3 LA CRYPTOGRAPHIE MODERNE

CHAPITRE 4 IMPLÉMENTATION ET RÉALISATION

Liste des Figures :

Liste des tableaux

INTRODUCTION GENERALE

Tout au long l'histoire, l'être humain a essayé d'envoyer où 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 dis 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'espoirs, 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 étude 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 GÉNERALE

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

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

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

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

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

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

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, diplome 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] Sitegénéralistesur lesréseaux. 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 stady cryptography science, and Evolved with the times. as well find a better and efficient cryptography algorithemn that use on information techology, frome memory usage and safty degrees, whitout ingrowibg Development environment during act analy stady a defferent symtric crytography 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.