

*République Algérienne Démocratique et Populaire*

*Ministère de L'Enseignement Supérieur et de la  
Recherche Scientifique*

*Université des Sciences et de la Technologie  
Houari Boumediene  
(U.S.T.H.B)*

*Institut d'Informatique*

**Mémoire de Fin d'Étude Pour l'Obtention du Diplôme d'Ingénieur  
d'État en Informatique**

**Thème:**

**Protection de la Messagerie  
Electronique par des Méthodes  
Cryptographiques**

**Réalisé par:**

**Mr BERBAR Ahmed**

**Mr SAADI Rachid**

**Dirigé par:**

**Mr O. Nouali**

**Mme N. Nouali (Taboudjemat)**

**Soutenu devant le jury:**

**A. Belkheir.....Président**

**S. Maazouz .....Examineur**

**Organisme d'accueil : Dept. LA et logiciel de base/ C.E.R.S.T**

**N° d'ordre 71/00**

## Résumé

La messagerie électronique est l'un des services les plus répandus sur Internet (et les réseaux en général). De ce fait elle est la cible de plusieurs attaques contre sa sécurité, d'autant plus qu'elle intervient dans tout les domaines qu'ils soient privés, politiques, commerciales ou autres. D'où l'importance de sa sécurisation qui a motivé le travail réalisé dans ce mémoire consistant en la réalisation d'un outil cryptographique permettant d'assurer la confidentialité, l'intégrité, l'authentification et la non répudiation des messages électroniques (e-mails).

**SOMMAIRE**

<b>INTRODUCTION GENERALE</b>	<b>1</b>
<b>CHAPITRE I : LA SÉCURITÉ INFORMATIQUE</b>	<b>3</b>
INTRODUCTION	4
1. LA SÉCURITÉ DE NOS JOURS	5
2. L'ÉTUDE DE LA SÉCURITÉ	8
2.1. LES DIFFÉRENTS SERVICES QU'IL DOIT OFFRIR LA SÉCURITÉ	8
2.2. LES MENACES CONTRE LA SÉCURITÉ	9
2.3. QUELQUES EXEMPLES D'ATTAQUES	11
3. LES MÉCANISMES ET LES SOLUTIONS DE SÉCURITÉ	18
3.1. LES FIRE WALLS	18
3.2. LA PROTECTION DES MOTS DE PASSE ET LA CRÉATION DE MOTS DE PASSE SÛRS	19
3.3. LA CRYPTOGRAPHIE	20
3.4. LA SÉCURITÉ À TRAVERS L'OBSCURITÉ	26
3.5. L'ÉDUCATION ET LA PRISE DE CONSCIENCE	26
CONCLUSION	28
<b>CHAPITRE II : LA MESSAGERIE ÉLECTRONIQUE</b>	<b>29</b>
INTRODUCTION	30
1. COMMENT FONCTIONNE UN SYSTÈME DE MESSAGERIE	31
2. LES DIFFÉRENTS FORMATS D'ADRESSES	32
3. LES DIFFÉRENTS MODES DE LA MESSAGERIE	33
4. FONCTIONS DE BASE DE LA MESSAGERIE ÉLECTRONIQUE	33
5. ARCHITECTURE ET NORME DE LA MESSAGERIE ÉLECTRONIQUE SOUS LE MODÈLE TCP/IP	34
5.1. LES PROTOCOLES D'ÉCHANGE	34
5.2. ANATOMIE D'UN MESSAGE ÉLECTRONIQUE	40
6. QUELQUES LOGICIELS DE GESTION DE LA MESSAGERIE ÉLECTRONIQUE	42
7. PROBLÈMES POTENTIELS DU E-MAIL	43
7.1. LES ACCIDENTS	43
7.2. LES MENACES SUR LE COURRIER	43
CONCLUSION	46
<b>CHAPITRE III : LA CRYPTOGRAPHIE</b>	<b>47</b>
INTRODUCTION	48
1. DÉFINITIONS	49
2. CRYPTOGRAPHIE CONVENTIONNELLE (À CLÉ SECRÈTE OU SYMÉTRIQUE)	50
3. CRYPTOGRAPHIE À CLÉ PUBLIQUE	51
3.1. LES SIGNATURES NUMÉRIQUES	53
3.2. FONCTION DE HACHAGE	53
3.3. LES CERTIFICATS NUMÉRIQUES	54
4. LA CRYPTOGRAPHIE QUANTIQUE	56

## **Sommaire**

---

<b>5. LES RESTRICTIONS IMPOSÉES À LA PROPAGATION DE LA CRYPTOGRAPHIE</b>	<b>57</b>
5.1. LES LOIS CRYPTOGRAPHIQUES EN FRANCE	57
5.2. LA LOI CRYPTOGRAPHIQUE AUX ETATS-UNIS	58
<b>6. LA CRYPTANALYSE</b>	<b>61</b>
6.1. MESURE DE LA COMPLEXITÉ D'UNE ATTAQUE	61
6.2. LES PRINCIPAUX TYPES D'ATTAQUES	61
<b>7. ETUDES DES DIFFÉRENTS ALGORITHMES DE CHIFFREMENT</b>	<b>63</b>
7.1. LES MODES OPÉRATIONNELS UTILISÉS DANS LES ALGORITHMES À CLÉS SYMÉTRIQUES	63
7.2. ALGORITHMES À CLÉ SYMÉTRIQUE	65
7.3. ALGORITHMES À CLÉ PUBLIQUE	79
<b>8. LES GÉNÉRATEURS DE NOMBRES ALÉATOIRES</b>	<b>84</b>
<b>9. LE SYSTÈME PGP</b>	<b>85</b>
<b>CONCLUSION</b>	<b>90</b>

## **CHAPITRE IV :L'IMPLÉMENTATION**

---

**91**

<b>INTRODUCTION</b>	<b>92</b>
<b>1. LE MODÈLE PROPOSÉ POUR LE MESSAGE SÉCURISÉ</b>	<b>93</b>
<b>3. GESTION ET ORGANISATIONS DES DONNÉES</b>	<b>95</b>
<b>4. FONCTIONNEMENT DU LOGICIEL'</b>	<b>97</b>
4.1. LE CONTRÔLE D'ACCÈS	97
4.2. EDITION ET TRANSMISSION DES MESSAGES	99
4.3. LE CHIFFREMENT	100
4.4. LE DÉCHIFFREMENT	112
4.5. LA GESTION DES CLÉ	113
<b>5. LE LANGAGE CHOISI</b>	<b>114</b>
<b>CONCLUSION</b>	<b>115</b>

## **CONCLUSION GÉNÉRALE**

---

**116**

## **BIBLIOGRAPHIES**

---

**118**

## **ANNEXE**

---

**ERREUR! SIGNET NON DÉFINI.**