République Algérienne Démocratique et Populaire

Ministère de l'Enseignement Supérieur et de la Recherche Scientifique

Centre de Recherche sur l'Information Scientifique et Technique

Mémoire pour l'obtention du diplôme de

Post-Graduation Spécialisée en Sécurité Informatique

Thème

Réalisation d'une boite à outils cryptographiques

Réalisé et présenté par :

BELMEBARKI Mohamed.

CHIKHI Miloud.

Thème proposé et encadré par :

Dr. NOUALI Omar.

Co-encadreur

Mme CHALAL Zakia

Devant le jury:

Dr. BESSAI Fatma Zohra	**MRB**	**Présidente**
Dr. TABOUDJEMAT NOUALI Nadia	**DR**	**Examinatrice**
Mr. SEBA Abderazek	**AR**	**Examinateur**

Promotion 2011 / 2012

Sommaire

Introduction générale ……..... 01
Partie 1 : Etat de l'art
Chapitre 1: Généralités sur la sécurité informatique
1. Introduction ……..... 03
2. Termes et définitions ……..…. 04
3. Niveaux de sécurité …..…….. 04
4. Objectifs la de Sécurité ….……..…….. 06
4.1. Confidentialité ……..……..…….…….... 06
4.2. Intégrité ……......06
4.3. Disponibilité des services ……..…..…..…..…..... 06
4.4. Authentification ……..... 07
4.5. Non-répudiation ……..…… 07
5. Les menaces ……..… 07
5.1. Menaces accidentelles ….……..… 08
5.2. Menaces intentionnelles …….. 08
5.2.1 Menaces passives ……..... 08
5.2.2 Menaces actives .. …… 08
6. Mécanismes de sécurité …… 08
6.1.1. Mécanismes de contrôle d'accès …… 09
6.1.2. Mécanismes de cryptographie …… 09
7. Quelques protocoles de sécurité ……... 09
7.1 IPSec ..…… 09
7.2 SSL ...……...……10
8. Conclusion ...……. 12
Chapitre 2: La Cryptographie
1. Introduction …… 13
2. Définitions ……... 13
3. Historique …… 14
4. Objectifs de la cryptographie ……... 16
5. Méthodes cryptographiques ……..…… 17
5.1 Chiffrement symétrique (à clé secrète) ……..……..……..... 17
5.1.1. Principe …….. ……..……... 17
5.1.2. Algorithmes de chiffrement symétrique …….. 17
5.1.3. Modes de chiffrement symétrique ……..……. 18
5.1.4. Problèmes de chiffrement à clé secrète ……... 23
5.2 Le chiffrement asymétrique (à clé publique) …….. 23
5.2.1. Principe …….. 23
5.2.2. Quelques algorithmes de chiffrement à clé publique ……. 24
5.2.3. Certificat numérique et autorité de certification …… 24
5.2.4. Problèmes de la cryptographie à clé publique ……. 26
5.3 Chiffrement hybride (Asymétrique et Symétrique) ……..…… 26
6. Hachage …… 27
6.1 Principe de hachage …… 27
6.2 Types de hachage ……. 28
7. Signature numérique ……... 29
7.1 Définition …… 29
7.2 Caractéristiques d'une signature numérique ...…….. 29
7.3 Processus de création d'une signature …….. 29
7.4 Processus de vérification d'une signature ……..…… 30

8. Quelques outils de chiffrement …….. 31
9. Cadre juridique de la signature numérique ……35
9.1. Chiffrement ……35
9.2. Signature numérique …….. 35
10. Conclusion …….. 37
Partie 2 : Conception et réalisation
Chapitre 3: Conception de la boite à outils
1. Introduction ……. 38
2. Spécification des besoins ……..…... 39
3. Identification des acteurs ……. 39
4. Identification des fonctionnalités …… 39
5. Architecture et fonctionnement de la boite à outils …… 40
5.1.Chiffrement/Déchiffrement …… …… 41
5.1.1 Données à transférer ……... 41
5.1.2.Données stockées en local ……..... 42
5.2.Signature/Vérification d'une signature des documents …….. 43
5.2.1. Signature des documents …… 43
5.2.2. Vérification d'une signature ……... 44
6. Conclusion ……... 44
Chapitre 4: Réalisation de la boite à outils
1. Introduction ……..…..…..…… 45
2. Environnement de développement ……..…..…… 45
2.1. Langage Java ……..…..…..... 45
2.2. Bibliothèque OpenSSL ……..…..…..…... 46
3. Description de l'application ……..…..…..…… 47
3.1. Fenêtre d'accueil ……..…..…..…….. 47
3.2. Configuration ……..…..…..…….. 47
3.3. Génération des clés ……..…..…..……. 48
3.4. Chiffrement /Déchiffrement des données locales ……..…..…….. 49
3.5. Chiffrement/signature des données à transférer ……..…..……..…….. 50
3.6. Déchiffrement/vérification des données transférées ……..…. 52
4. Conclusion ……..…..…..…..…… 53
Conclusion générale et perspectives ……... 54
Références……..…… 55
Annexe ……...……... 57