

**REPUBLIQUE ALGERIENNE DEMOCRATIQUE ET POPULAIRE**

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

**Centre de Recherche sur l'Information Scientifique et Technique**

Mémoire de fin d'étude

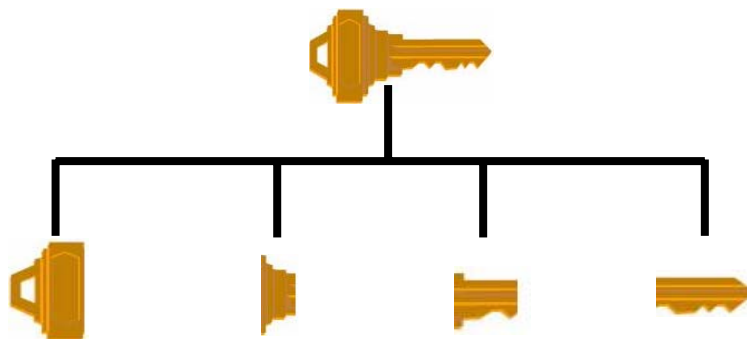
Pour l'obtention du Diplôme de Post Graduation Spécialisé en

**SECURITE INFORMATIQUE**

**Présenté par : Riad KOUAH**

**Thème**

**CRYPTOGRAPHIE A SEUIL**



**Devant le Jury :**

**Mme S. BENMEZIANE**

**Présidente**

**Mme N. NOUALI**

**Membre**

**Mme F. BESSAI**

**Membre**

**Dr. O. NOUALI**

**Encadreur**

**PGS/CERIST : 2006-2007**

# SOMMAIRE

<b>Introduction Générale.....</b>	<b>01</b>
<b>CHAPITRE I : Cryptographie Moderne .....</b>	<b>00</b>
1. Introduction .....	03
2. Objectifs de la sécurité .....	00
3. La cryptographie et la vie réelle .....	00
4. Description d'un schéma de chiffrement .....	00
5. Rappel mathématique (corps fini).....	00
6. Description d'un schéma de chiffrement RSA.....	00
7. Description d'un schéma de chiffrement El Gamal .....	00
8. Attaques contre les systèmes de chiffrement .....	00
<b>CHAPITRE II : Cryptographie partagée .....</b>	<b>00</b>
1. Le but de la cryptographie partagée .....	00
2. Introduction à la cryptographie partagée .....	00
3. Partage de secret ( $n, n$ )-Threshold .....	00
4. Problèmes relatifs à l'utilisation de la cryptographie à seuil .....	00
4.1. Problème de distribution du secret .....	00
4.2. Choix de $t$ et $n$ .....	00
5. Outils de cryptographie partagée .....	00
5.1. Partage additif .....	00
5.2. Partage polynomiale .....	00
5.3. Partage de secret « Schéma de partage de secret à la Shamir » .....	00
5.4. RSA avec ( $k, n$ ) .....	00
5.5. Partage des secret publiquement vérifiable .....	00
6. Partage de fonction .....	00
6.1. Propriété des schémas cryptographiques de partage de fonction .....	00
6.2. Sécurité d'un crypto-système de chiffrement partagé .....	00
6.3. Sécurité d'un schéma de signature .....	00
7. Partage proactif .....	00
<b>CHAPITRE III : Cryptographie à seuil .....</b>	<b>00</b>
1. Introduction .....	00
2. Partage du crypto-système RSA .....	00
3. Signature RSA partagée .....	00
Historique .....	00
Schéma de signature RSA à seuil de Shoup .....	00
Algorithme de génération partagée de clés RSA de Boneh-Franklin .....	00
Schéma complètement distribué de signature RSA à seuil .....	00
4. Partage du crypto-système de Paillier .....	00
Rappels sur les algorithmes de chiffrement homomorphique .....	00
Crypto-système de Paillier .....	00
Description du crypto-système de Paillier distribué	
Fonction RSA homomorphique .....	00
5. Cryptographie à seuil avec El Gamal .....	00
<b>CHAPITRE IV : Crypto-systèmes partagés sûrs contre les attaques à chiffrés choisis ..</b>	<b>00</b>

1. Introduction .....	00
2. Partage du crypto-système IND-CCA .....	00
3. Proposition de schémas IND-CCA à seuil .....	00
Système de chiffrement à seuil .....	00
Conversion générique .....	00
4. Exemples .....	00
Version IND-CPA à seuil du crypto-système El Gamal .....	00
Version IND-CCA à seuil du crypto-système El Gamal .....	00
Version IND-CCA à seuil du crypto-système de Paillier .....	00
5. Conclusion .....	00
<b>CHAPITRE V : Applications de la cryptographie à seuil .....</b>	<b>00</b>
1. Introduction .....	00
2. Schéma de loterie électronique .....	00
Principe .....	00
Exemple de réalisation .....	00
Nécessité d'un chiffrement IND-CCA .....	00
3. Schéma de vote électronique .....	00
Exigences de sécurité .....	00
Techniques générales .....	00
4. Nouveau système de vote électronique .....	00
Organisation de l'élection .....	00
Schéma de vote .....	00
Améliorations du Schéma .....	00
5. Conclusion .....	00
<b>Conclusion Générale.....</b>	<b>01</b>

## **Bibliographie**

## **Annexe**