

Sommaire

Sommaire	1
Liste des figures	5
Liste des tableaux	6
Introduction générale.....	7
Chapitre 1 : Généralité sur la cryptographie :	
1.1 Introduction	9
1.2. Définition de cryptologie	9
1.3. Définition de la cryptographie.....	10
1.4. L'usage de la cryptographie.....	10
• La confidentialité	10
• L'intégrité.....	10
• L'authentification.....	10
• La non répudiation	10
1.5. Mécanisme de la cryptographie.....	10
1.6. Confidentialité et algorithme de chiffrement	11
1.6.1. Les avantages et inconvénients de la cryptographie à clé publique comparé à la cryptographie à clé privée	12
1.7. Différence entre chiffrement et codage.....	13
1.8. Définition de la cryptanalyse.....	13
• Cassage complet	14
• Obtention globale	14
• Obtention locale	14
• Obtention d'information	14
1.8.1 Les niveaux d'attaque.....	14
• L'attaque par cryptogramme.....	14
• L'attaque à message en clair connu	14
• L'attaque à message en clair choisi	15
• L'attaque à message chiffré choisi	15
1.10. Conclusion	15
Chapitre2 : Histoire du cryptage Arabe :	

2.1. Introduction.....	16
2.2 La cryptographie Andalouse Marocaine.....	17
2.2.1 Historique	17
2.2.2 L'exemple du Roi Cryptographe Al Moetamid	18
2.3. La cryptographie Numérique Arabe.....	19
2.3.1 Codage numérique Arabe	19
2.3.2 Calcul Arabe « Hissab Al-Joummal ».....	19
2.3.3. Substitution Affine et le Codage numérique Arabe.....	20
2.4 La cryptographie d'Or : période de la dynastie Saàdienne.....	20
2.5 Exemple de cryptogrammes publiés d'El Mansour.....	21
• Cryptogramme numérique	23
• Cryptogramme d'Inversion.....	24
2.5.1. Le Cryptogramme d'Or.....	24
2.5.2. Le Cryptogramme d'Or et la plume de Fès.....	26
2.6 Signature.....	28
2.7 Conclusion	29
 Chapitre3 : Les crypto-systèmes :	
3.1 Introduction	30
3.2 Description de systèmes cryptographiques classiques.....	30
3.2.1. Algorithme de substitution.....	30
• Substitution monoalphabétiques.....	30
• Substitution polyalphabétique	30
• Substitution homophonique	30
• Substitution de polygrammes.....	31
3.2.2. Le chiffre de césar.....	31
3.2.3. Le chiffre de VIGENERE ou de BEAUFORT.....	32
• Fonctionnement	32

• Principe mathématique.....	33
3.2.4. Le chiffre de transposition	34
3.2.5. Le OU exclusif.....	35
3.3 Système cryptographiques modernes.....	35
3.3.1 Systèmes symétriques à clé secrètes.....	35
• Principe de base	36
1) L'algorithme DES (Data Encryption Standard).....	37
1.1 Génération du DES.....	37
1.2 Principe du DES.....	38
1.3 Les grandes lignes de l'algorithme.....	38
2) Description du DES	38
✓ Les avantages	39
✓ Les faiblesses	40
3.4 Systèmes asymétriques à clé publique.....	40
3.4.1 Définition et fonctionnement.....	41
3.4.2. l'algorithme RSA.....	42
• Le principe.....	42
• L'algorithme de chiffrement.....	42
• Exemple.....	42
3.4.3. Le protocole de Diffie et Hellman.....	43
✓ Les avantages	44
✓ Inconvénients	44
3.4 Conclusion.....	45
Chapitre 4 : Présentation de l'application :	
4.1. Introduction.....	46

4.2. Objectif	46
4.3. Logiciel utilisé.....	46
4.3.1 Description de l'interface et composantes.....	46
4.4. Le contenu du menu « ملف ».....	47
4.5. Le contenu du menu « طبعة ».....	48
4.6. Exemple de quelque opérateur.....	48
4.6.1 Exemple de chiffrement à clé secrète (DES).....	48
• Introduction de la clé.....	49
• Le texte chiffré	50
• Le déchiffrage.....	50
4.6.2 Exemple de chiffrement à clé publique (RSA).....	51
• Les clefs RSA.....	52
• Introduction de la clé	53
• Le texte chiffré.....	53
• Le déchiffrage	54
4.7. Lettre Arabe	55
4.7.1. Table des caractères ASCII	56
4.8. Code source de différentes implémentations.....	61
4.8. 1. Code source de l'algorithme DES	62
4.8.2. Code source de l'algorithme RSA.....	67
4.9. Conclusion.....	73
Conclusion générale.....	74
Référence Bibliographique.....	75
Webographie.....	76

