



République Algérienne Démocratique et Populaire

Ministère de l'Enseignement Supérieur et de la Recherche Scientifique

Université des Sciences et de la Technologie HOUARI

BOUMEDIENE

FACULTE DE GENIE ELECTRIQUE ET D'INFORMATIQUE

DEPARTEMENT D'INFORMATIQUE

Mémoire du projet de fin d'études

Pour l'obtention du diplôme

d'ingénieur d'état en informatique

Option : Software

SUJET:

Sécurité de la transmission des fichiers_malades sur une plate forme
de logiciel de communication entre laboratoires de cytologie

Thème proposé par : Mlle N. Lassouaoui - CERIST -

Encadré par : Mlle N. Lassouaoui

Mr D. Hadjari

Etudié par :

Djedjig Nabil

Hadj Arab Samir

Soutenu le 04/10/2004

Devant le jury composé de :

Mme Zaouèche

Mr Ferguène

Mme Benbaziz

Président

Examineur

Examinatrice

PROMOTION : 121/2004

SOMMAIRE

Résumé	1
Introduction Générale	3
Chapitre 1: Généralités sur la cryptographie	
1. Introduction.....	5
2. La cryptographie	5
2.1. Définitions	5
2.2. Les fonctions de la cryptographie	7
3. Historique	7
3.1. Les balbutiements de la cryptographie	8
3.2. La technique assyrienne	8
3.3. Le carré de Polybe	9
3.4. Le chiffrement par substitution	10
3.4.1. Le chiffrement de César	10
3.4.2. La substitution monoalphabétique	10
3.5. Le chiffrement de Vigenère	11
3.6. Transposition à base matricielle	12
4. Les méthodes de cryptage modernes	12
4.1. La cryptographie symétrique	13
4.2. La cryptographie asymétrique	14
5. Les différents algorithmes de cryptage	15
5.1. DES	15
5.2. IDEA	17
5.3. RSA	17
5.4. PGP	18
6. Conclusions	18

Chapitre 2: Techniques de cryptage d'images

1. Introduction	20
2. Quelques algorithmes de cryptage d'image	20
2.1. Cryptage des images par dissimulation	21
2.2. Chiffrement d'image basé sur les cartes chaotiques	22
2.3. L'algorithme chaotique hiérarchique de chiffrement d'image	23
2.3.1. Algorithme chaotique hiérarchique du chiffrement d'image (HCIE)	25
2.3.2. Algorithme de Sub-HCIE	27
2.4. L'algorithme chaotique basé sur la clé (CKBA)	29
3. Conclusion	30

Chapitre 3: Conception

1. Introduction	32
2. Chiffrement Continu des Données par un Registre à Décalage à Rétroaction Linéaire (RDRL)	32
2.1 Protocole de cryptage	33
2.2 Générateur de codons	34
2.3. Registres à Décalage à Rétroaction Linéaire	35
2.4. Analyse d'algorithme	38
2.5. Résultats et interprétations	38
2.5.1. Cryptage d'image	39
2.5.1.1. Critiques	42
2.5.1.2. Amélioration	43
2.5.2. Applications à d'autres images	46
2.6. Cryptage du texte	48
3. Conclusion	49

Chapitre 4: Présentation du logiciel conçu

1. Introduction	51
2. Environnement de développement	51
2.1. Langage de programmation	51
2.2. Plateforme : (Windows)	52
2.3. Architecture utilisée	53
2.3.1. Les communications dans le réseau	53

3. Solution proposée et adoptées	54
3.1. Procédures du cryptage	54
4. Description du logiciel	55
4.1. Description de l'interface graphique	56
5. Conclusion	59
Conclusion générale	60
Bibliographie	61