



*République Algérienne Démocratique et Populaire*  
*Ministère de l'Enseignement Supérieure et de la Recherche Scientifique*  
Université des Sciences et de la Technologie Houari Boumediene

**USTHB**

***Faculté d'Electronique et d'Informatique***  
***Département d'Informatique***

Mémoire du projet de fin d'études

Pour l'obtention du diplôme  
D'ingénieur d'état en informatique

**SUJET:**

**Conception d'un système de sécurité des  
données pour réseau inter laboratoires de  
cytogénétique**

Thème proposé et encadré par:

**M<sup>me</sup> L. HAMAMI**  
**M<sup>r</sup> D. HADJARI**

Etudié par:

**Radia GANA**  
**Sabrina ADDI**

Membres de jury composé de :

**M<sup>r</sup> BELKHIR** ..... **Président**  
**M<sup>r</sup> BERBER** ..... **Examineur**  
**M<sup>r</sup> AMANI** ..... **Examineur**

**PROMOTION: 2002-2003**

### Résumé:

Dans le cadre d'élaboration d'un système de sécurisation des transactions entre les médecins des différents laboratoires de cytogénétique, nous étudions dans ce mémoire les différentes méthodes utilisées dans la sécurité.

Après une introduction à la notion des réseaux informatiques, qui consiste à prendre en considération les différents protocoles de communication et topologies les plus citées dans la littérature. Elle intègre la notion de la sécurité informatique et ces différentes techniques.

Notre travail est basé sur l'architecture Client/Serveur. Les informations envoyées du client au serveur seront stockées dans une base de données en utilisant l'API JDBC. Nous avons appliqué deux méthodes pour la sécurité des messages échangés: la méthode de cryptage RSA pour le texte et la méthode de watermarking étalement du spectre pour les images. Les éléments nécessaires à la compréhension et la justification de ces approches sont ainsi présentés.

**Mots Clés:** Réseau informatique, Architecture Client/Serveur, Sécurité informatique, base de données, API JDBC, Cryptage, Watermarking.

### Abstract:

Within the framework of the development of a system reassuring the transactions between the doctors of the various laboratories of cytogenetics, we study in this memory the various methods used in safety.

After an introduction to the notion of the networks data-processing, this consists in taking into account the different protocols of communication and topologies the most quoted in the literature. All of them integrate the notion of the computer security and these various techniques.

Our work is based on Client/Server architecture. The information sent of the customer to the server will be stored in a data base by using the API JDBC. We have applied two methods for safety of the exchanged messages: method of encoding RSA for the text and the method of watermarking spreading out of the spectrum for the images. The elements necessary to comprehension and the justification of these approaches are thus presented.

**Key Words:** Data-processing network, Client/Server Architecture, Computer security, data base, API JDBC, Encoding, Watermarking.

# TABLE DES MATIERES

<b>Introduction générale</b> .....	1
------------------------------------	---

## Chapitre I: Généralités sur les réseaux informatiques

Introduction .....	4
I-1 Les réseaux informatiques .....	4
I-1-1 Historique .....	4
I-1-2 Les réseaux locaux .....	5
I-1-3 Les réseaux étendus .....	5
I-1-4 Objectifs des réseaux .....	5
I-1-5 Structure des réseaux .....	6
I-1-6 Topologies des réseaux .....	6
I-1-6-1 Topologie en étoile .....	7
I-1-6-2 Topologie en bus .....	8
I-1-6-3 Topologie en anneau .....	8
I-1-7 Les supports de transmission .....	9
I-2 Architectures des réseaux .....	10
I-3 Protocoles de communication .....	10
I-3-1 Le modèle OSI .....	11
I-3-2 Le modèle DoD .....	13
I-4 Protocole TCP/IP .....	14
I-4-1 L'adressage IP .....	14
I-4-2 Classes d'adresse IP .....	15
Conclusion .....	15

## Chapitre II : Architecture Client/Serveur

Introduction .....	16
II-1 Modèle Client/Serveur .....	16
II-1-1 Présentation de l'architecture d'un système Client/Serveur .....	16
II-1-2 Fonctionnement d'un système Client/Serveur .....	17
II-1-3 Avantage de l'architecture Client/Serveur .....	17
II-1-4 Inconvénients du modèle Client/Serveur .....	18
II-2 Les niveaux du Client/Serveur .....	18
II-3 Caractéristiques du Client/Serveur .....	18
II-3-1 Attribut client .....	18
II-3-2 Attribut serveur .....	18
II-3-3 Attribut de communication .....	19
II-4 Types d'architecture Client/Serveur .....	20
II-4-1 L'architecture à deux niveaux .....	20
II-4-2 L'architecture à trois niveaux .....	20
II-4-3 L'architecture multi niveaux .....	21
II-5 Classification du modèle Client/Serveur .....	22
II-5-1 Le Client/Serveur de présentation .....	23
II-5-2 Le Client/Serveur de traitement .....	23
II-5-3 Le Client/Serveur de données .....	23
II-6 L'interaction Client/Serveur .....	24
II-7 Les interfaces applicatives .....	24

Conclusion.....	25
<b>Chapitre III : La sécurité informatique</b>	<b>26</b>
III-1 La terminologie de la sécurité .....	26
III-2 La politique de sécurité .....	27
III-2-1 Définition .....	27
III-3 Aspects de la sécurité .....	27
III-3-1 Intégrité .....	27
III-3-2 Confidentialité .....	28
III-3-3 Disponibilité de service .....	28
III-3-4 La non répudiation.....	28
III-3-5 L'authentification.....	28
III-4 Les formes de la sécurité.....	29
III-4-1 - La sécurité matérielle .....	29
a)- Sécurité physique .....	29
b)- Sécurité d'émanation .....	30
III-4-2 Sécurité de l'information .....	30
a)- Sécurité des machines .....	30
b)- Sécurité des communications .....	30
III-4-3 Sécurité organisationnelle .....	30
a)- La sécurité du personnel .....	30
b)- La sécurité des opérations .....	31
III-5 Les mécanismes de la sécurité .....	31
III-5-1 L'authentification et l'identification .....	31
III-5-2 Mécanismes de contrôle d'accès .....	32
a)- Le contrôle d'accès discriminatoire .....	32
b)- Le contrôle d'accès mandataire .....	33
III-5-3 Sécurité de communication .....	33
a)Le contrôle de routage et de bourrage des informations.....	33
b)- Le chiffrement .....	33
c)- Protocoles sûrs .....	34
III-6 Les menaces.....	34
III-6-1 Les menaces accidentelles .....	35
III-6-2 Les menaces intentionnelles (ou attaques) .....	35
III-6-3 Quelques types d'attaques spécifiques .....	36
Conclusion .....	40
<b>Chapitre IV : La cryptographie</b>	<b>41</b>
IV-1 La cryptographie .....	41
IV-1-1 Définition.....	41
IV-1-2 La cryptographie classique.....	42
IV-1-2-1 Substitution et transposition .....	43
IV-1-2-2. Machine à tambours .....	44
IV-1-2-3 Ou exclusif simple .....	45
IV-1-2-4 Masque jetable .....	45
IV-1-3 Les techniques de la cryptographie .....	46
IV-1-3-1 Les algorithmes à clé secrète .....	46
IV-1-3-2 Chiffrement à clé publique .....	47

IV-1-3-3 La signature digitale .....	49
IV-1-3-4 Les fonctions de scellement .....	50
IV-1-3-5 Notion de certificat.....	50
IV-1-4 Algorithmes de la cryptographie .....	51
a) L'algorithme RSA .....	51
b) L'algorithme DES .....	53
c) Le DSA .....	54
IV-1-5 Exemple de cryptosystème.....	54
Conclusion.....	55

## Chapitre V: La stéganographie et le watermarking 56

V-1 La stéganographie .....	56
V-1-1 A quoi sert la Stéganographie ? .....	56
a) Filigrane.....	56
b) Canal de communication secrète .....	57
V-1-2 Où et comment cacher l'information secrète ?.....	57
V-1-2-1 Texte.....	57
V-1-2-2 Son.....	57
V-1-2-3 Image.....	58
V-1-2-4 Autres.....	58
V-2 Le watermarking.....	58
V-2-1 Définitions.....	58
V-2-2 Qu'est ce que le watermarking?.....	59
V-2-3 Les modèles de marquage.....	61
V-3 Les champs d'application du watermarking .....	63
V-3-1 Le texte .....	63
V-3-2 L'image .....	66
V-3-3 Audio .....	70
V-4 Attaques sur les marques .....	71
V-4-1 Selon le but de l'attaque .....	71
V-4-2 Selon le type d'attaque.....	74
V-4-3 D'autres attaques.....	75
Conclusion.....	75

## Chapitre VI: La partie conception 78

Introduction.....	78
VI-1 Problématique.....	78
VI-2 Solutions au problème posé.....	78
VI-2-1 Le stockage et la gestion des informations.....	78
VI-2-2 La communication (échange des informations).....	80
VI-2-3 La sécurisation des données.....	80
VI-3 Les outils utilisés.....	81
VI-3-1 Choix du langage de programmation .....	81
VI-3-2 Choix d'un SGBD.....	81
VI-3-3 Solution de communication.....	81

VI-3-4 Solution de sécurisation.....	82
VI-4 Principe de fonctionnement du système.....	83
VI-5 Spécification du système à mettre en place.....	83
VI-6 Avantages du système.....	84
VI-7 La conception des bases de données.....	84
VI-7-1 Les requêtes émises par le client.....	84
VI-7-1-1 La requête pour la demande d'inscription.....	85
VI-7-1-2 La requête pour le cryptage.....	85
VI-7-1-3 La requête pour la lecture des messages.....	85
VI-8 Conception de la passerelle entre le client et le serveur .....	85
VI-9 La méthode d'interfaçage à implémenter.....	86
VI-10 Les connexions concurrentes des clients.....	86
VI-11 L'interface client.....	86
L'interface graphique développée .....	87

<b>Conclusion générale</b> .....	95
----------------------------------	----

## **Annexe**

### **Références bibliographiques**