

Republique Algérienne Democratique et Populaire  
Ministère de l'Enseignement Supérieur et de la Recherche Scientifique

Université des Sciences et de la Technologie HOUARI BOUMEDIENE

**INSTITUT D'INFORMATIQUE**

Mémoire du projet de fin d'études  
Pour l'obtention du diplôme d'ingénieur d'état en informatique

Option : **Reseau**

Sujet :

**LE PAIEMENT ELECTRONIQUE  
SECURISE**

Proposé par :

M. NOUALI Omar  
M<sup>me</sup> NOUALI Nadia

Realise par :

ALIOUANE Lynda  
CHENAÏT Manel

Soutenu le :

Devant le jury comuose de :

M<sup>me</sup> MOUSSAOUI Présidente  
M. BENCHAIBA Membre

**Organisme d'accueil : Dept. IA et logiciel de base/ C.E.R.I.S.T**

PROMOTION : 62/2000

# RESUME

L'enthousiasme avec lequel entreprises et consommateurs ont adopté le World Wide Web (WWW) offre une chance inouïe au développement du commerce électronique ou e-commerce.

Aujourd'hui, les sites de vente mettent en ligne une description détaillée et claire du produit et des photos (comme une vitrine), et propose une commande en ligne avec plusieurs moyens de paiement et c'est justement l'aspect paiement qui est le point sensible de l'échange. Les clients sont encore très frileux pour la consommation sur Internet, car ils ne savent pas ce qu'on fait, de leur numéro de carte de crédit lorsqu'ils le donnent. et ont peur que quelqu'un d'autre ne le récupère.

Les risques sont multiples : Le commerçant peut modifier le montant à débiter ou vendre un produit qui n'existe pas et que le client ne recevra jamais. Le client, lui, peut utiliser une carte qui n'est pas la sienne, contester avoir passé une commande ou avoir un découvert à la banque. Enfin, une tierce personne peut récupérer les informations sur la carte de crédit et les utiliser.

Dans ce mémoire, nous nous sommes intéressées à l'utilisation de moyens cryptographiques afin de sécuriser les échanges en s'assurant qu'ils sont chiffrés (confidentialité), que ceux qui y participent sont bien ceux qu'ils disent être (authentification), que les données n'ont pas été modifiées (intégrité). Il faut également pouvoir certifier que les échanges ont bien eu lieu (non-repudiation) et que le client peut payer

Mots clés :

Systèmes de paiement électronique, commerce électronique, cryptographie, sécurité, Internet et protocoles, transactions sécurisées, carte à puce, monnaie électronique, SET, SSL, C-SET.

# SOMMAIRE

## CHAPITRE I : INITIATION AUX PROBLEMES DE SÉCURITÉ SUR INTERNET

1.1	INTRODUCTION.....	3
1.2	LES PROBLÈMES DE SÉCURITÉ .....	4
1.2.1	<i>Types d'attaques</i> .....	4
1.2.2	<i>Exemples d'attaques</i> .....	4
1.3	LES MÉCANISMES DE BASE DE LA SÉCURITÉ SUR INTERNET : "LES OIJTILS CRYPTOGRAPHIQUES".....	7
1.3.1	<i>Définitions</i> .....	7
1.3.2	<i>Les techniques de la cryptographie</i> .....	7
1.3.3	<i>La notion de certificat</i> .....	11
1.4	LES MÉCANISMES DE SÉCURITÉ .....	12
1.4.1	<i>L'authentification et l'identification</i> .....	12
1.4.2	<i>Le contrôle d'accès</i> .....	12
1.4.3	<i>La sécurité des communications</i> .....	13
1.5	CONCLUSION.....	13

## CHAPITRE II : LES SYSTÈMES DE PAIEMENT SUR INTERNET

2.1	INTRODUCTION.....	16
2.2	LE COMMERCE SUR INTERNET .....	16
2.2.1	<i>Le commerce électronique (ou e-commerce)</i> .....	16
2.2.2	<i>Les transactions du paiement électronique</i> .....	18
2.3	LES MOYENS DE PAIEMENT .....	23
2.3.1	<i>Les moyem waditionnels</i> .....	23
2.3.2	<i>Les moyens modernes</i> .....	24
2.4	CONCLUSION.....	32

## CHAPITRE III : LA CRYPTOGRAPHE

3.1	INTRODUCTION.....	35
3.2	CRYPTOGRAPHIE CLASSIQUE.....	36
3.2.1	<i>Chiffre a substitution</i> .....	36
3.2.2	<i>Chiffre a transposition</i> .....	36
3.2.3	<i>Le chiffrement par ou exclusif (Xoring)</i> .....	37
3.3	CRYPTOGRAPHIE .....	37
3.3.1	<i>Les techniques cryptographiques</i> .....	37
3.3.2	<i>La securite des cryptosystèmes</i> .....	40
3.3.3	<i>Description des algorithmes</i> .....	42
3.3.4	<i>Application cryptographique complete : PGP (Pretty Good Privacy)</i> .....	52
3.4	CONCLUSION.....	53

**CHAPITRE IV : LES PROTOCOLES DE PAIEMENT ÉLECTRONIQUE**

4.1 INTRODUCTION.....	55
4.2 LE PROTOCOLE S-HTTP (SECURE HYPER TEXT TRANSFER PROTOCOL) .....	55
4.2.1 <i>Présentation du protocole S-HTTP</i> .....	55
4.2.2 <i>La communication sécurisée spontanée pour le service Web S-HTTP</i> .....	56
4.3 LE PROTOCOLE SSL (SECURE SOCKET LAYER).....	58
4.3.1 <i>Présentation du protocole SSL</i> .....	58
4.3.2 <i>SSL et les logiciels de communication</i> .....	58
4.3.3 <i>A avantages et limites du SSL</i> .....	58
4.4 iKP (INTERNET KEYED PROTOCOL).....	59
4.4.1 <i>Présentation du protocole iKP</i> .....	59
4.4.2 <i>Les transactions au moyen du protocole iKP (description mathématique)</i> .....	59
4.5 LE PROTOCOLE SET (SECURE ELECTRONIC TRANSACTION) .....	60
4.5.1 <i>Présentation du protocole SET</i> .....	60
4.5.2 <i>Messages de paiement électronique par SET</i> .....	60
4.6 LE PROTOCOLE C-SET (CHIP-SECURE ELECTRONIC TRANSACTION).....	61
4.6.1 <i>Présentation du protocole C-SET</i> .....	62
4.7 PROTOCOLES CRYPTOGRAPHIQUES :AVANTAGES ET INCONVÉNIENTS.....	62
4.8 CONCLUSION.....	63

**CHAPITRE V : IMPLEMENTATION****PARTIE I : CONCEPTION D'UN SYSTÈME DE PAIEMENT SÉCURISÉ .....66**

5.1 INTRODUCTION.....	66
5.2 LES RISQUES ET LES BESOINS POUR UN PAIEMENT SÉCURISÉ .....	66
5.3 SOLUTIONS.....	67
5.4 UNE APPLICATION DE PAIEMENT SÉCURISÉ .....	68
5.4.1 <i>Les acteurs</i> .....	69
5.4.2 <i>Les phases du processus de paiement</i> .....	69

**PARTIE II : RÉALISATION .....75**

5.5 OUTILS DE MISE EN ŒUVRE .....	75
5.6 LA COMMUNICATION .....	76
5.7 LA SÉCURITÉ.....	76
5.7.1 <i>Les algorithmes cryptographiques utilisés</i> .....	76
5.7.2 <i>La generation de clés</i> .....	76
5.8 DESCRIPTION DU LOGICIEL.....	76
5.8.1 <i>Interface client</i> .....	77
5.8.2 <i>Interface marchand</i> .....	78
5.8.3 <i>Interface banque</i> .....	79
5.9 DÉROULEMENT DU LOGICIEL.....	79
5.10 CONCLUSION.....	81

CONCLUSION GÉNÉRALE.....	82
GLOSSAIRE.....	84
BIBLIOGRAPHIE.....	88