

REPUBLIQUE ALGERIENNE DEMOCRATIQUE ET POPULAIRE  
MINISTERE DE L'ENSEIGNEMENT SUPERIEUR ET DE LA RECHERCHE SCIENTIFIQUE  
CENTRE DE RECHERCHE SUR L'INFORMATION SCIENTIFIQUE ET TECHNIQUE



**Mémoire**  
**Pour l'obtention du diplôme de**  
**Post Graduation Spécialisée**  
**Sécurité Informatique**

# Cryptographie Dans les cartes à puce

Présenté par  
**BELHADJ Nedjma**

**Jury**

M<sup>r</sup>. TANDJAOUI Djamel  
M<sup>r</sup>. NOUALI Omar  
M<sup>me</sup>. NOUALI Nadia  
M<sup>me</sup>. BENMEZIANE SOUAD

Président  
Encadreur  
Examineur  
Examineur

2006-2007

# TABLE DES MATIERES

TABLE DES FIGURES.....	1
LISTE DES TABLEAUX.....	4
TERMINOLOGIE.....	5
INTRODUCTION.....	6
<b>CHAPITRE I</b>	
<b>PRESENTATION DES CARTES A PUCE .....</b>	<b>7</b>
1- HISTORIQUE .....	8
2- DEFINITION D'UNE CARTE A PUCE .....	9
3- TYPES DE CARTES A PUCE.....	9
3.1- CARTES AVEC CONTACTS .....	9
3.1.1- Caractéristiques physiques.....	10
3.1.2- Caractéristiques mécaniques .....	11
3.1.3- Position des contacts.....	12
3.1.4- Brochage des contacts .....	13
3.1.5- Caractéristiques électriques et logiques .....	14
3.1.6- Insertion et retrait des cartes dans les lecteurs.....	15
3.1.7- Description de l'opération de rese.....	16
3.2- CARTES SANS CONTACTS.....	18
3.2.1- Principe de fonctionnement d'un composant RFID .....	19
3.2.2- Catégories des cartes à puce sans contact .....	21
3.2.3- Caractéristiques physiques et mécaniques .....	21
3.2.4- Caractéristiques électriques.....	22
4- FAMILLES DE CARTES A PUCE (AVEC OU SANS CONTACT).....	22
4.1- CARTES A MEMOIRE OU CARTES SYNCHRONES.....	23
4.2- CARTES A MICROCONTROLEUR OU CARTES ASYNCHRONES.....	24
5- FABRICATION ET CYCLE DE VIE D'UNE CARTE A PUCE .....	25
5.1- ACTEURS .....	25
5.2- FABRICATION .....	26
5.3- CYCLE DE VIE DE LA CARTE .....	26
6- NORMES ET STANDARDS .....	28
7- SYSTEMES D'EXPLOITATION DES CARTES A PUCE .....	30

7.1- SYSTEMES D'EXPLOITATION FERMES .....	31
7.1.1- Principe.....	33
7.1.2- Exemples .....	33
7.2- SYSTEMES D'EXPLOITATION OUVERTS .....	34
7.2.1- Téléchargement du code natif .....	34
7.2.2- Systèmes d'exploitation à interpréteur .....	34
8- FICHIERS DES CARTES A PUCE.....	35
8.1- ARBORESCENCE DES FICHIERS.....	35
8.2- STRUCTURE DES FICHIERS .....	36
9- PROTOCOLES D'ECHANGES.....	39
9.1- PROTOCOLE D'ECHANGES PAR CARACTERE .....	39
9.2- PROTOCOLE D'ECHANGES PAR BLOCS.....	40
10- STRUCTURE DES COMMANDES.....	41
11- CONCLUSION.....	43

## CHAPITRE II

### NOTIONS CRYPTOGRAPHIQUES..... 44

1- VOCABULAIRE SUR LA CRYPTOGRAPHIE .....	45
1.1- ALGORITHMES RESTREINTS ET ALGORITHMES PUBLICS .....	45
1.1.1- Algorithme symétrique ou à clé secrète .....	46
1.1.2- Algorithme asymétrique ou à clé public .....	46
1.2- FONCTION DE HACHAGE .....	47
1.3- CRYPTANALYSE ET CARTES A PUCES .....	47
2- METHODES CRYPTOGRAPHIQUES SIMPLES.....	48
3- METHODES CRYPTOGRAPHIQUES COMPLEXES A CLE SECRETE.....	49
3.1- CHIFFREMENT PAR FLOT.....	49
3.2- CHIFFREMENT PAR BLOC .....	49
3.3- DES.....	51
3.3.1- Présentation.....	51
3.3.2- Principe de l'algorithme .....	51
3.4- TRIPLE DES .....	53
3.5-AES.....	54
3.5.1- Présentation .....	55
3.5.2- Principe de l'algorithme .....	56
4- ALGORITHMES CRYPTOGRAPHIQUES COMPLEXES A CLE PUBLIQUE.....	57
4.1- RSA.....	57

4.1.1- Fonctionnement.....	57
4.1.2-Utilisation.....	58
4.2- CRYPTOGRAPHIE ELLIPTIQUE .....	59
4.2.1- Définition d'une courbe elliptique.....	59
4.2.2- Chiffrement par courbe elliptique.....	60
4.2.3- Utilisation des courbes elliptiques.....	61
5- MECANISMES CRYPTOGRAPHIQUES DANS LES CARTES A PUCES.....	61
6- CONCLUSION .....	64

### **CHAPITRE III**

<b>PROBLEMES DE SECURITE DES CARTES A PUCE.....</b>	<b>65</b>
1-ATTAQUES PUREMENT LOGICIELLES.....	66
2- ATTAQUES MATERIELLES DESTRUCTRICES.....	66
3- ATTAQUES MATERIELLES NON DESTRUCTRICES .....	68
4- ATTAQUES EXTERNES.....	68
4.1- SIMPLE POWER ANALYSIS OU SPA .....	68
4.1.1- Quelques exemples de signaux .....	69
4.1.2- Extraction d'une clé RSA avec une attaque de type SPA .....	71
4.1.3- Exemple de protection .....	73
4.2- DIFFERENTIAL POWER ANALYSIS OU DPA .....	73
4.3- ELECTRO MAGNETIC ANALYSIS OU EMA .....	75
5- CONCLUSION.....	75

### **CHAPITRE IV**

<b>DEVELOPPEMENT ET APPLICATION .....</b>	<b>76</b>
1-LECTEURS ET/OU PROGRAMMATEUR.....	77
1.1- PRESENTATION .....	77
1.2- INSTALLATION D'UN LECTEUR .....	78
2- BASIC CARD .....	79
3- KIT DE DEVELOPPEMENT .....	80
4-DESCRIPTION DE L'APPLICATION .....	82
5- REALISATION PRATIQUE .....	86
<b>CONCLUSION .....</b>	<b>91</b>
<b>BIBLIOGRAPHIE .....</b>	<b>92</b>
<b>ANNEXE.....</b>	<b>94</b>