

SOMMAIRE

LISTE DES FIGURES

LISTE DES TABLEAUX

INTRODUCTION GENERAL	01
CHAPITRE I : La cryptographie	
1. Introduction.....	04
2. Définitions.....	04
3. Terminologie.....	04
4. Propriétés de sécurité.....	05
4.1. Confidentialité.....	05
4.2. Authentification.....	05
4.3. Non-répudiation.....	06
4.4. Intégrité.....	06
5. Les primitives cryptographiques.....	06
5.1. Chiffrement symétrique.....	06
5.2. Chiffrement asymétrique.....	07
6. PRNG.....	08
6.1. Historique du développement des générateurs pseudo-aléatoires.....	08
6.2. Qu'est-ce qu'une variable aléatoire.....	09
6.3. Quelle est leur utilité.....	09
6.4. Comment les générer.....	10
6.5. Les méthodes de générateur pseudo-aléatoire.....	10
6.5.1. La méthode de Von Neumann.....	10
6.5.2. Méthode de Fibonacci.....	11
6.5.3. Générateurs congruentiels linéaires.....	11
6.5.4. Générateurs pseudo-aléatoires cryptographiques.....	12
7. Fonction de hachage.....	13
7.1. Principe.....	13
7.2. MD5.....	13
7.3. SHA-1.....	15
8. Opérateur ou-exclusif.....	15
9. Concaténation.....	16

10. Protocoles cryptographiques.....	16
10.1. Protocoles d'authentification.....	17
10.2. Protocoles d'échange de clé.....	17

CHAPITRE II : Protocoles d'authentification RFID

I. Les systèmes RFID	20
1. Définitions.....	20
2. Historique.....	20
3. Fonctionnement.....	22
4. Le format des tags.....	22
5. La sécurité.....	23
6. Les Applications de RFID.....	23
6.1. Le paiement.....	24
6.2. Transport.....	24
6.3. Bibliothèques.....	24
6.4. Control d'accès.....	24
6.5. La santé.....	24
6.6. Le RFID et la logique.....	25
II. Protocoles d'authentification RFID	25
1. Protocole RHLS	25
2. Protocole HMNB	26
3. Protocole CRAP.....	27
4. Protocole LAK.....	28
5. Protocole PAP	30

CHAPITRE III : Spécification des besoins et conception du simulateur

Introduction.....	34
1. Simulation.....	34
1.1. Méthodes de simulation.....	35
1.1.1. La simulation des événements	35
1.1.2. Le temps en simulation discrète.....	35
1.1.3. Les arrivées dans le système.....	35
1.1.4. Simulation orientée clients	36
1.2. Evaluation des performances.....	36
1.3. La simulation pour l'évaluation des performances.....	36
1.4. La performance des protocoles RFID	36

1.5. Les hypothèses de simulation	37
2. Modélisation avec UML	37
2.1. Définition.....	37
2.2. Les objectifs d'UML	37
2.3. Présentation générale des diagrammes d'UML	38
3. Conception de simulation des protocoles d'Authentification RFID	39
3.1 Spécification des besoins du simulateur	39
3.2 Diagramme de classe du simulateur	40
3.3 Diagramme de séquence des protocoles étudiés.....	43
3.3.1 Protocole LAK	43
3.3.1 Protocole LAK (Attaque).....	45
3.3.1 Protocole RHLS	46
3.3.1 Protocole HMNB	47
3.3.1 Protocole CRAP	49
3.3.1 Protocole PAP	51
CHAPITRE IV: Implémentation du simulateur	
Introduction	54
1. Outils et langages utilisés.....	54
1.1. Java	54
1.2. EDI NetBeans	54
1.3. JCE (Java Cryptography Extension)	54
1.4. Système de gestion de base de données (SGBD)	55
1.5. MySQL-Connector-java-3.1.12.....	55
2. Pseudo-code principal.....	56
2.1 Fonction de hachage	56
2.2 Nonce (Générateur de nombre pseudo aléatoire.....	57
2.3 Concaténation.....	57
2.4 Opérateur ou-exclusif	57
3. Algorithme de simulation des activités (ex. protocole LAK.....	58
3.1. Algorithme.....	58
3.2. Programme.....	58
4. Algorithme de simulation des événements pour plusieurs clients (protocole CRAP)	59
5. Implémentation d'application SimRF-Auth.....	61
5.1. Structure du programme	61

5.2. Quelques interfaces des modules du système implémenté SimRF-Auth	62
6. Résultats expérimentaux	68
Conclusion et perspectives	70
Notes et Références	72