

Sommaire

1. Introduction à la cryptographie

- Histoire de la cryptographie
- Objectifs de sécurité
- Confidentialité, intégrité et authentification

2. Outils mathématiques

- Arithmétique modulaire
- Nombres premiers
- Congruences
- Théorie des groupes et des corps finis

3. Cryptographie à clé secrète

- Principes du chiffrement symétrique
- Chiffrement par blocs
- Chiffrement par flot
- DES et AES

4. Fonctions de hachage

- Propriétés des fonctions de hachage
- MD5, SHA
- Contrôle d'intégrité

5. Authentification

- Codes d'authentification de message (MAC)
- Protocoles d'authentification
- Gestion des identités

6. Cryptographie à clé publique

- Principe des clés publiques
- Algorithme RSA
- Échange de clés Diffie-Hellman
- Cryptosystèmes à courbes elliptiques

7. Signature électronique

- Signature numérique
- Certificats électroniques
- Infrastructure à clés publiques (PKI)

8. Protocoles cryptographiques

- Distribution des clés

- Protocoles d'authentification
- Protocoles sécurisés sur Internet

9. Sécurité des réseaux

- SSL/TLS
- Courrier électronique sécurisé
- Commerce électronique

10. Attaques cryptographiques

- Cryptanalyse
- Attaques par force brute
- Attaques statistiques
- Attaques sur les protocoles

11. Preuves de sécurité

- Modèles de sécurité
- Sécurité calculatoire
- Validation des protocoles

12. Applications de la cryptographie

- Cartes à puce
- Paiement électronique
-