

# Sommaire

1. Concepts fondamentaux de sécurité
2. Principes du chiffrement moderne
3. Chiffrement symétrique
4. Algorithmes DES et Triple DES
5. Le standard AES
6. Modes opératoires des chiffrements par blocs
7. Fonctions de hachage cryptographique
8. Authentification des messages
9. Signatures électroniques
10. Cryptographie à clé publique
11. RSA et systèmes asymétriques
12. Échange et négociation de clés
13. Gestion sécurisée des clés
14. Génération des nombres aléatoires
15. Infrastructure à clés publiques (PKI)
16. Protocoles cryptographiques
17. Sécurité des réseaux et Internet
18. SSL, TLS et sécurisation des communications
19. Sécurité des mots de passe
20. Protection des données sensibles
21. Attaques cryptographiques courantes
22. Failles d'implémentation
23. Architecture des systèmes sécurisés
24. Cryptographie appliquée aux applications réelles
25. Bonnes pratiques de conception sécurisée
26. Études de cas et exemples pratiques
27. Standards et recommandations internationales
28. Annexes techniques
29. Bibliographie et références