

Sommaire:

1. Introduction à la cryptographie

- Histoire et importance de la cryptographie
- Concepts de base

2. Algorithmes de chiffrement symétrique

- Chiffrement par bloc (ex. DES, AES)
- Modes de fonctionnement (CBC, ECB, etc.)
- Analyse de la sécurité

3. Algorithmes de chiffrement asymétrique

- RSA
- Diffie-Hellman
- DSA et variantes

4. Fonctions de hachage

- Principes des fonctions de hachage
- Hachage sécurisé (SHA-1, SHA-2, etc.)
- Applications et sécurité

5. Protocoles cryptographiques

- Protocoles d'échange de clés
- Protocoles d'authentification
- SSL/TLS et autres protocoles sécurisés

6. Cryptographie dans les systèmes modernes

- Applications de la cryptographie dans le stockage et la transmission de données
- Cryptographie dans les réseaux sans fil

7. Questions de sécurité et de mise en œuvre

- Erreurs courantes en cryptographie
- Attaques et défenses

8. Exemples de code en C

- Implémentations de divers algorithmes cryptographiques
- Exemples pratiques d'utilisation de la cryptographie en C

9. Perspectives futures

- Cryptographie quantique
- Évolution des menaces et des technologies