

Sommaire

1. Introduction à l'arithmétique et à la cryptologie

- Rôle de l'arithmétique en cryptologie
- Notions de base en cryptographie
- Importance de la cryptologie moderne dans la sécurité des communications

2. Arithmétique modulaire

- **Calcul modulaire**
 - Définition et propriétés de l'arithmétique modulaire
 - Opérations sur les entiers modulo n
- **Théorème de Fermat et théorème de Wilson**
 - Applications aux tests de primalité
- **Algorithmes de division et de calcul des inverses**
 - Algorithme d'Euclide et extension pour les inverses
 - Application à la cryptographie symétrique et asymétrique
- **Exponentiation rapide**
 - Méthodes de calcul rapide en cryptographie
 - Applications dans les protocoles de chiffrement

3. Théorie des nombres et cryptographie

- **Nombres premiers et leurs propriétés**
 - Primalité et tests de primalité (méthodes de recherche)
- **Factorisation des grands entiers**
 - Difficulté de la factorisation dans les systèmes de chiffrement à clé publique
- **Crible d'Ératosthène et algorithmes de factorisation**
 - Applications à la sécurité des systèmes cryptographiques
- **Fonctions à sens unique et leurs applications**
 - Hachage cryptographique et fonctions de hachage

4. Cryptographie symétrique

- **Chiffrement de César et chiffrement par substitution**
 - Introduction aux méthodes classiques
- **Chiffrement de Vigenère et ses variantes**
 - Méthodes de cryptage simples et faibles
- **Algorithmes modernes de chiffrement symétrique**
 - AES, DES, et autres systèmes de chiffrement par blocs
- **Modes de chiffrement (CBC, CTR, etc.)**
 - Sécurisation des communications avec des modes de chiffrement

5. Cryptographie asymétrique (clé publique)

- **Le problème du logarithme discret**
 - Fondements mathématiques des systèmes à clé publique
- **RSA (Rivest-Shamir-Adleman)**
 - Construction, fonctionnement et sécurité du RSA
 - Attaques potentielles et méthodes de sécurisation
- **Algorithme de Diffie-Hellman pour l'échange de clés**
 - Principe, utilisation dans les protocoles sécurisés
- **Courbes elliptiques et leur application en cryptographie**
 - Cryptographie elliptique et avantages en termes de sécurité et d'efficacité

6. Protocoles cryptographiques et applications

- **Signature numérique et authentification**
 - Modèles de signature et protocole de vérification
- **Protocoles de chiffrement à clé publique et partage de clé**
 - SSL/TLS, HTTPS, et autres applications sécurisées

- **Certificats numériques et infrastructures à clé publique (PKI)**
 - Rôle des autorités de certification et gestion des clés
- **Cryptographie dans les transactions financières**
 - Blockchain, Bitcoin et autres applications de la cryptographie

7. Attaques et sécurité des systèmes cryptographiques

- **Analyse des vulnérabilités des algorithmes cryptographiques**
 - Attaques par force brute, par cryptanalyse, et autres techniques
- **Attaques par canaux auxiliaires**
 - Protection contre les attaques physiques et les fuites d'information
- **Cryptanalyse des systèmes modernes**
 - Évaluation de la sécurité des algorithmes récents
- **Protection des clés et gestion de la sécurité des données**

8. Applications avancées de la cryptographie

- **Cryptographie post-quantique**
 - Risques associés à l'arrivée de l'informatique quantique
 - Recherche sur les algorithmes résistants aux ordinateurs quantiques
- **Homomorphisme et cryptographie sur les données chiffrées**
 - Utilisation de la cryptographie pour le calcul sur des données chiffrées
- **Protocole de zéro-knowledge et confidentialité**
 - Applications à la vérification de données sans révéler l'information

9. Conclusion et perspectives

- Résumé des concepts clés
- État actuel de la cryptologie et de la sécurité informatique
- Défis futurs et évolutions possibles dans le domaine

Annexes (si présents) :

- Tableaux des valeurs de petites puissances modulaire
- Exercices et solutions détaillées
- Références bibliographiques et ressources complémentaires