Sommaire

- **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-knoweldge 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