Chiffrement & Blockchain

Volume horaire : 16h

Objectifs pédagogiques

- Comprendre le besoin de chiffrer les données
- Comprendre et savoir différencier les algorithmes de chiffrement
- Être capable de choisir et mettre en œuvre un processus de chiffrement en fonction d'un problème donné
- Comprendre les principes généraux liés à la blockchain et être capable d'identifier les problèmes où elle peut être une solution pertinente

Programme

1. Introduction aux concepts de la cryptographie

- Historique et but de la cryptographie
- Chiffrement de transposition, substitution
- Chiffrement monoalphabétique, polyalphabétique, polygrammique
- Chiffrement symétrique, asymétrique
- Principe de signature numérique et fonctions de hachage
- Présentation et comparatif des différents algorithmes

TP : Confection et utilisation de différents algorithmes de chiffrement

2. Introduction aux concepts de la cryptanalyse

- Historique et but de la cryptanalyse
- Attaque à chiffré seul & choisi
- Attaque à clair connu & choisi
- Cryptanalyse linéaire, différentielle
- Exemples : attaque par dictionnaire, recherche statistique

TP : Application des principes de la cryptanalyse sur un exemple simple

3. Introduction aux concepts de la blockchain

- Historique de la blockchain : exemple du bitcoin
- Principe de block, chain, header, nounce
- Algorithmes de chiffrement asymétrique & signature
- Principe et algorithme de POW (Proof Of Work)
- Principe du minage de block et rôle des miners

TP : Création d'une blockchain réduite

Moyens et outils pédagogique

Cours théorique & TP de mise en situation

Évaluation

Devoir sur table & Épreuve pratiques

Bibliographie

- *The handbook of applied cryptography* – **Menezes, Oorschot et Vanstone**
- *Initiation à la cryptographie* - **Dubertret**
- *Blockchain et cryptomonnaies* – **Primavera De Filippi**
- *Bitcoin: A Peer-to-Peer Electronic Cash System* **- Satoshi Nakamoto**