

SOMMAIRE

Partie 1: Théorie de l'information et compression

- Codage par blocs et par flots: Présentation des bases du codage, notamment les codes par blocs et les codes par flots, ainsi que les concepts de probabilités et d'algèbre qui leur sont liés.
- Théorie de l'information et compression: Introduction à la théorie de l'information et à son rôle dans la compression des données.
- Exploration des concepts d'entropie et des différentes méthodes de réduction d'entropie.
- Codes compresseurs usuels: Examen de différents codes de compression couramment utilisés, tels que les codes de Huffman et les codes LZW.
- Compression audio/vidéo avec perte: Étude des techniques de compression avec perte, notamment pour les formats audio et vidéo, en abordant les compromis entre la qualité et la taille du fichier.

Partie 2: Cryptologie Principes généraux et terminologie:

- Définition des concepts clés de la cryptographie, tels que le chiffrement, le déchiffrement, les clefs, etc.
- Attaques sur les systèmes cryptographiques: Examen des différentes méthodes d'attaque sur les systèmes de chiffrement, incluant les attaques par force brute, les attaques par dictionnaire, etc.
- Systèmes cryptographiques à clef secrète: Explication des systèmes de chiffrement symétriques, tels que DES et AES, et de leurs mécanismes.
- Systèmes cryptographiques à clef publique: Présentation des systèmes de chiffrement asymétriques, tels que RSA, et de leurs applications.
- Authentification, intégrité, non-répudiation et signatures électroniques: Étude des mécanismes d'authentification, de vérification de l'intégrité des données et de signatures électroniques.
- Protocoles usuels de gestion de clefs: Exploration des protocoles utilisés pour la gestion et l'échange des clés dans les systèmes cryptographiques.

Partie 3: Détection et correction d'erreurs Détection d'erreurs par parité:

- Présentation de la méthode de détection d'erreurs basée sur la parité, et ses limites.
- Distance d'un code: Explication du concept de distance de Hamming et son rôle dans la détection et la correction d'erreurs.
- Codes linéaires et codes cycliques: Étude des codes linéaires et cycliques, ainsi que de leurs propriétés et applications.
- Paquets d'erreurs et entrelacement: Examen des techniques de gestion des paquets d'erreurs et de l'entrelacement pour améliorer la fiabilité de la transmission.
- Codes convolutifs et turbo-codes: Présentation des codes convolutifs et des turbo-codes, des techniques avancées de correction d'erreurs.