

1. Cryptographie classique, concepts cryptographiques, et cryptanalyse

- a. Les définitions d'un cryptosystème, le principe de Kerckhoff, etc.
- b. Les chiffrements à substitution, par transpositions, de Vigenère, et de Hill : leurs définitions et leurs propriétés cryptanalytiques (par rapport à fréquences de lettres et l'invariance de l'indice de coïncidence).
- c. La plupart des cryptosystèmes modernes sont des *chiffrements produits*, qui sont des compositions des composants classiques (mais avec un alphabet des mots binaire). Pourquoi n'est-il pas suffisant utiliser que des chiffrement à substitution et par transposition ?
- d. Les formes d'attaque cryptanalytique (texte chiffré seul, etc.)
- e. Les attaques par force brute et la taille de clés.

2. Les chiffrement par blocs

- a. Cryptosystèmes : DES, 3DES, AES (structure générale)
- b. Modes d'opération : ECB, CBC, CFB, OFB, CTR
- c. Comment est-ce qu'on peut définir un chiffrement à flot avec un chiffrement par bloc ?

3. Arithmétique modulaire

- a. La division euclidienne (+ et \cdot dans $\mathbb{Z}/n\mathbb{Z}$)
- b. ppgcd, ppcm, ppgcd étendu : inversion modulaire et CRT

4. Le chiffrement à clé publique.

- a. RSA, ElGamal, l'échange de clé de Diffie–Hellman
- b. Signatures : RSA, ElGamal.
- c. Pourquoi est-ce que les cryptosystèmes publics doivent etres moins efficaces que les cryptosystèmes symmetriques ?

5. Protocoles et standards cryptographiques : quels sont les rôles des standards cryptographiques pour chiffrement, signatures, autorités de certification, etc.