Chap 1. Introduction* (Durée 1h).

§1. Contenu, description et objectifs du cours.

§2. Notions d'arithmétique et Eléments d'informatique théorique. (compléments algorithmiques)

* : optionnel. Durée totale ≈ 30 h.

Références

1) • Paar §.

2) • B. Martin. Codes, cryptographie

3) • D. R. Stinson. Cryptography : Theory and Practice. 1995.

4) Buchmann. Intro to cryptography.

---

§1 • L'objectif du cours est d'avoir une bonne compréhension des mécanismes cryptographiques, sans trop exiger de l'auditoire, en vue d'implémenter des applications par le futur ingénieur. L'un des choix est d'adapter l'aspect mathématique en introduisant les notions nécessaires par besoin.

• Le chap 2. décrit la cryptographie symétrique, à bloc variable et fixe. L'étude des DES (et AES)