SEMESTRE 8 **UE-IRM 82**

EE-IRM825

Codage et Cryptographie

Système d'évaluation	Crédits
Examen	1 ECTS

Liste des compétences visées : CG2, CG3, CG6, CS1, CS4, CS6.

Pré-requis: Mathématiques pour l'ingénieur (EE-IRM522), Algorithmiques numériques (EE- IRM524), Réseaux de communication (EE-IRM733).

Mots clés: cryptographie, chiffrement.

Objectifs de l'enseignement : Ce cours permet à l'étudiant de :

- Connaître les enjeux techniques, méthodologiques et réglementaires liées à la protec- tion des réseaux et le rôle de la cryptographie dans la mise en place des services de sécurité.
- Maîtriser les caractéristiques des algorithmes de chiffrement pour être en mesure de choisir le type d'algorithme en fonction des services de sécurité à mettre en place, selon des critères techniques et juridiques.
- Etendre ces connaissances aux nouvelles techniques avancées de chiffrement et à leur mise en oeuvre dans les réseaux.

Contenu de l'enseignement :

1. Leçon 1 : Sécurité de l'information dans les réseaux
   - (a) Section 1 : Cybercriminalité et besoins de protection des réseaux
   - (b) Section 2 : Audit et Conseil : analyse des risques et test d'intrusion
   - (c) Section 3 : Méthodologies d'analyse des risques
2. Leçon 2 : Cryptographie
   - (a) Section 1 : Introduction à la cryptographie
   - (b) Section 2 : Codes de permutation ou de transposition
   - (c) Section 3 : Codes de substitution
   - (d) Section 4 : Masques jetables (one-time-pad) et cryptographie quantique
   - (e) Section 5 : Principes fondamentaux de la cryptographie
3. Leçon 3 : Algorithmes de chiffrement à clé symétrique
   - (a) Section 1 : DES
   - (b) Section 2 : AES
   - (c) Section 3 : Modes de chiffrement
   - (d) Section 4 : Cryptanalyse
4. Leçon 4 : Algorithmes de chiffrement à clé publique

    (a) Section 1 : Principes des codes à clé publique
    (b) Section 2 : Le cryptosystème Merkle-Hellman
    (c) Section 3 : RSA
    (d) Section 4 : Le cryptosystème El Gamal
5. Leçon 5 : Signatures numériques
    (a) Principe et définitions
    (b) Signatures à clé symétrique
    (c) Signatures à clé publique
    (d) Condensats de messages et fonctions de hachage
    (e) Attaque de l'anniversaire
6. Leçon 6 : Gestion des clés publiques
    (a) Section 1 : Certificats
    (b) Section 2 : X.509
    (c) Section 3 : Infrastructures de clés publiques