Intitulé : Sécurité informatique
Niveau : 5ème Année
V.H.H: 03H00
Coefficient: 03
A/S : Semestriel

Objectifs : Ce module permet à l'étudiant de s'initier aux concepts fondamentaux de la sécurité informatique et en particulier, aux méthodes de la cryptographie

Contenu :

CHAPITRE I : ASPECTS GENERAUX DE LA SECURITE

1. Les menaces
2. Vulnerabilités applicatives
3. Sécurite des systemes
4. Les outils d'attaque/defense
5. La politique de sécurité
6. Conseils

CHAPITRE II : LES SERVICES DE SECURITE

1. Clef secrète : chiffrement à flot
2. Clef secrète : chiffrement par bloc
3. Clef publique : RSA, log discret

CHAPITRE III : LA CRYPTOGRAPHIE

1. Introduction à la cryptographie
2. Sensibilisation à la cryptographie
3. La terminologie et les concepts de base

CHAPITRE IV : LES DIFFERENTS MECANISMES CRYPTOGRAPHIQUES

1. Probabilité
2. Théorie de l'information
3. Complexité
4. Arithmétique modulaire

CHAPITRE V : DE LA CLE PUBLIQUE AU CERTIFICAT

IV.1 Introduction : Clef SSH, clef SSH, clef PGP
IV.2 En pratique : Panorama des certificats inclus dans Windows 2000
Sécurisation des échanges avec SSL/TLS ;

Références bibliographiques :

1. Johannes Buchmann, Introduction à la cryptographie : Cours et exercices corrigés, Editeur : Dunod Édt. , 2ème édition (juin 2006).
2. Douglas Stinson, Cryptographie - Théorie et Pratique - 2ème édition – Vuibert Edt.
3. Bruce Schneier - Cryptographie Appliquée - Algorithmes, protocoles et codes source en C - 2ème Édition – Vuibert Edt.
4. Schneier B., Cryptographie Appliquée, Vuibert, Wiley and International Thomson Publishing, NY, 2nd edition, 1997.