Syllabus SEC

Crédits : 1	**SEC** Introduction à la sécurité informatique Introduction to IT security	**Coef : 1**
VH Cours : 10.00 **VH TD :** 10.00	**Pré-requis :**	

Ingénierie des Compétences

Familles de Compétences

- **CF7 :** Concevoir, mettre en œuvre et administrer des infrastructures complexes et réparties

Type de compétence: TEC : Technique, **MET :** Méthodologique, **MOD :** Modélisation, **OPE :** Opérationnel,

Niveau de compétence: Base | Intermédiaire | Avancé

Famille de Compétence	Compétence	Elément de Compétence	Type
CF7	**C7.2:** Définir et mettre en œuvre une politique de sécurité	**C72.2:** Sécuriser un système informatique	OPE
		C72.1: Analyser les menaces et les vulnérabilités d'un système	MET
		C72.3: Identifier les mécanismes cryptographiques permettant d'assurer des services de sécurité requis	OPE
		C72.4: Exploiter des outils logiciels pour mettre en oeuvre des mécanismes de sécurité de données	TEC

Description du programme de la matière

Objectifs:	Sensibiliser l'étudiant aux problèmes de sécurité informatique. Présenter les aspects fondamentaux de la sécurité informatique. Savoir réaliser des analyses de risque. Comprendre le rôle et les limites de la cryptographie dans la protection de l'information Familiariser l'étudiant avec les aspects de la cryptographie. Découvrir le fonctionnement des primitives cryptographiques Apprendre à les utiliser correctement et raisonner sur la sécurité (garantir un ou plusieurs services de la sécurité.) Savoir utiliser quelques outils cryptographiques pour réaliser un service de sécurité. Identifier et corriger les failles possibles aussi bien au niveau utilisation d'un système d'exploitation qu'au niveau construction d'un logiciel.
	Concepts de base sur la sécurité informatique I. Les enjeux de la sécurité II. La sécurité dans les Systèmes d'Information. III. Les Menaces IV. Les différents niveaux de sécurité V. Politique de sécurité VI. Les services de la sécurité. Introduction à la cryptographie I. Généralités. I.1 Contexte général. I.2 Définition cryptographie/cryptanalyse I.3 Objectifs de la cryptographie. I.4 Les services de la sécurité. II. Historique de la cryptographie avant l'ère de la technologie II.1 La scytale. II.2 Le cryptogramme de César. II.3 La permutation de lettres. II.4 Le chiffrement de Vigenère. II.5 Le chiffrement de Hill. II.6 Le chiffrement de Vernam III. Cryptographie moderne. III.1 Principes de Kerckhoffs III.2 L'âge de la technique

Contenu:	III.3 Codage de l'information IV. Chiffrement symétrique. IV.1 Chiffrement par flots. IV.2 Chiffrement par blocs. IV.2.1 Le DES (Data Encryption Standard) IV.2.2 L'AES (Advanced Encryption Standard) IV.3 Calcul dans le corps de Galois GF(28) IV.4 Force d'un mot de passe. V. Chiffrement Asymétrique. V.1 Chiffrement RSA. V.2.1 Remarques sur les mathématiques modulaires. V.2.2 Exponentiation modulaire. V.2.3 Calcul des clés du RSA V.4 Chiffrement ECC. V.4.1. La Multiplication Scalaire VI. Chiffrement hybride RSA/AES VII. Principe de gestion de clés. VII.1 Présentation du problème. VII.2 Echange de clé. VII.2.1 Echange de Diffie-Hallman. VII.2.2 Echange d'El Gamal VIII. Autres primitives cryptographiques. VII.1 Hachage cryptographique et intégrité. (MD5, SHA2) VII.2 MAC/HMAC et authentification. VII.3 Signature électronique et Non-répudiation. IX. Notion de certificat IX.1 Norme ISO X509 TD/TP du chapitre II : Atelier OpenSSL pour utiliser la cryptographie au profit de la sécurité des données et des échanges.
Travail Personnel:	Mise en place du protocole HTTPS (serveur web sécurisé) durée ~ 10h Exposé sur des thèmes relatifs à la sécurité informatique. Apprendre à utiliser un logiciel de cryptographie (PGP/ Cryptool) pour réaliser un service de la sécurité
Bibliographie:	L. Bloch, C. Wolfhugel Sécurité Informatique (Principes et méthodes) Eyrolles, 2007 W. Talligs, « Sécurité des réseaux : Applications et Standards », Vuibert, 2002. B. Schneier, « Cryptographie appliquée : Algorithmes, protocoles et codes source en C », Vuibert, 2002. G. Dubertret, « Initiation à la cryptographie », Vuibert 1998. A. J. Menezes, PC. van Oorschot SA. Vanstone HANDBOOK of APPLIED CRYPTOGRAPHY CRC Press; Fifth Printing (August 2001)