



SYLLABUS

Semestre : 06

Unité d'Enseignement : UEF1 (fondamentale)

Matière : Sécurité Informatique

Domaine / Filière : Licence Informatique **Parcours :** SI / ISIL

Crédit : 05 **Coefficient :** 03

Langue d'enseignement : Français

Enseignant responsable de la matière : Mr Bourbia Riad

Bureau : E8.3 **E-mail :** Bourbia.riad@univ-guelma.dz

Objectifs de l'enseignement

Cette matière permet aux étudiants d'acquérir des compétences pour assurer la sécurité et le bon fonctionnement des systèmes informatiques.

Connaissances préalables recommandées : fondement algorithmique, technique de programmation

Contenu de la matière

Chapitre I : Introduction à la sécurité Informatique

I.1 - Définitions : Sécurité, Sureté de fonctionnement, ...

I.2 - Principaux concepts de sécurité informatique : vulnérabilité, menace, contre-mesure, risque, ...

I.3 - Objectifs de la sécurité informatique : La confidentialité, L'intégrité, La disponibilité, La non-répudiation, L'authentification, ...

I.4 - Nécessité d'une approche globale

I.5 - Mise en place d'une politique de sécurité

Chapitre II : Les attaques Informatiques et les systèmes de détection des intrusions

II.1 - Qu'est-ce qu'une attaque ?

II.2 - Définitions : Virus - Ver - Cheval de Troie - Logiciel espion

II.3 - Origine des attaques

II.4 - Qui peut être visé ?

II.5 - Les étapes d'une attaque

II.6 - Les différents types d'attaques

- Les attaques réseaux
- Les attaques de système
- Les attaques de mots de passe
- Les attaques de site web
- Les attaques d'applications.

II.7 - Méthodes de défense : Anti-virus, Pare-feu, Réseaux privés, Détection d'intrusion, ...

Chapitre III : Initiation à la cryptographie

III.1- Vocabulaire et définitions : Cryptologie, Cryptographie, Cryptogramme, Cryptanalyse, etc...

III.2- Histoire de la cryptographie

III.3- Cryptographie Classique

- Algorithme de Substitution : Chiffre de César, chiffre de VIGENERE.
- Algorithme de Transposition : la technique assyrienne.

III.4- Cryptographie Moderne

- Cryptographie symétrique : Principe, Algorithmes DES et AES
- Cryptographie Asymétrique : Principe, Algorithme RSA

III.5- Fonctions de Hachage

- Principe
- Les algorithmes MD5 et SHA-1.

III.6- La signature électronique

III.7- Les certificats numériques

Mode d'évaluation

- **Examen (60%),**
- **Contrôle continu (40%)**

- **Note travaux dirigés :**
 - Micro interrogation : **50%**
 - Travail continu + assiduité : **50%**

Références

1. Laurent Bloch, Christophe Wolfhugel, Ary Kokos, G r me Billois, Arnaud Soulli , Alexandre Anzala-Yamajako, Thomas Debize, **S curit  informatique pour les DSI, RSSI et administrateurs**,  ditions Eyrolles, 5   dition, Collection Blanche, 2016.
2. Jean-Fran ois Pillou, Jean-Philippe Bay, **Tout sur la s curit  informatique**, Dunod, 4  Edition, 2016.
3. Gilles Dubertret, **L'univers secret de la cryptographie**, Vuibert, 2015.
4. Damien Vergnaud, **Exercices et probl mes de cryptographie**, Collection : *Sciences Sup, Dunod*, 2015

Le responsable du Module
R. Bourbia