« Initiation à la cryptographie»
L3 – UEO – S5 ou S6 ?

ECTS : 4

Nombre d'Heures : CM/TD/TP : 20h/ 10h/ 10h

Equipe pédagogique :
Sandrine Julia, Enrico Formenti, Bruno Martin

Objectif : Découverte et mise en oeuvre des principes de bases de la cryptographie moderne

Programme :

Ce cours commence par relater l'histoire de la cryptologie, avant qu'elle devienne la discipline scientifique de pointe qu'elle est aujourd'hui, entre informatique et mathématiques.
Le cours présente des méthodes chiffrement à clé secrète (DES, AES) et des méthodes de chiffrement à clé publique (protocole de Diffie-Hellman, RSA). On ne fera qu'évoquer les dernières avancées dans le domaine. La cryptographie ne se limite pas au chiffrement des messages, d'autres notions seront présentées comme la signature, l'identification, l'authentification, l'intégrité des données, les certificats.
On recensera aussi les usages quotidiens de la cryptographie : connexion à un système informatique, commerce électronique, carte bleue, envoi de données sécurisé, one-time password ...
Enfin, on analysera les évolutions qu'a entraîné la cryptographie moderne (lois, autorités de certification, e-commerce, etc).
Les TP mettront en oeuvre les protocoles classiques de chiffrement ou de signature. Ils permettront aussi de fouiller les applications informatiques pour comprendre où s'y loge la cryptographie.

-

Ressources BU ou ouvrages conseillés :

- Codage, cryptologie et applications, B. Martin, Presses Universitaires Romandes, 2004.

Ressources numériques :

- http://fr.wikipedia.org/wiki/Cryptologie

Supports TICE/ENT : *cours, TP, annales sur le web et/ou sur j@lon*

Compétences : (I = initiation, U = utilisation, M = maîtrise)

- scientifiques
Faire preuve de capacité d'abstraction (U),
Comprendre la différence entre cryptographie à clé secrète et à clé publique (U)
Programmer différentes méthodes de cryptographie (I)

-transversales
Effectuer une recherche d'information (U),
Utiliser des outils mathématiques (U).

Modalités de contrôle des connaissances :

1 CC intermédiaire (1/3 de la note finale), 1 TP noté (1/3 de la note finale), 1 CC terminal (1/3 de la note finale).