Sécurité

Niveau du cours : Master (M2) **Parcours(s) :** DSC

Crédits ECTS : 3

Enseignants : **Cayrel Pierre-Louis** (UJM, Saint-Étienne)

Période d'enseignement : 3ème semestre **Langue d'enseignement :** Français

Pré-requis : Connaissance en algorithmie et en mathématiques (algèbre linéaire, un peu de théorie des nombres).

Objectifs : Connaitre les menaces et attaques sur un système d'information, les principes de la cryptographie, les standards de chiffrement.

Mots clés : chiffrement, déchiffrement, RSA, signature numérique, cryptanalyse, hachage, AES, génération de pseudo aléa.

Syllabus :
1. Introduction aux menaces et attaques sur un système d'information
2. Terminologie - Premiers principes de cryptographie (César, Vigénère)
3. Cryptographie moderne – Théorie de l'information de Shannon – Sécurité pratique
4. Cryptographie symétrique – Chiffrement par flot – Chiffrement par blocs – ECB, CBC
5. Standard de chiffrement symétrique: DES, évaluation de sécurité, AES
6. Introduction à la cryptographie asymétrique, rappels d'arithmétique modulaire.
7. Fonctions à sens unique – Problème du logarithme discret - Diffie-Hellmann.
8. Fonctions à sens unique avec trappe – Problème de factorisation – RSA.
9. Risques d'utilisation de RSA: attaque par module commun, par exposant commun.
10. Intégrité - Fonction de Hachage
11. Authentification – Signatures électroniques

Volume horaire : CM (5h), TD (15h).

Contrôle des connaissances : Un contrôle théorique (coefficient 3, durée 1h30), un projet (coefficient 2).

Bibliographie et ressources : http://cayrel.net/Cryptographie

Informations complémentaires/contacts :

Nom : Cayrel Pierre-Louis
Adresse : 18 rue du professeur Benoît Lauras 42000 Saint-Etienne
E-mail: pierre.louis.cayrel@univ-st-etienne.fr
Web : http://cayrel.net/