UCL Faculté des sciences

SC

MATH2350 Cryptographie

[22.5h] 2.5 crédits

Cette activité se déroule pendant le 2ème semestre

Enseignant(s): Jean-Jacques Quisquater
Langue d'enseignement : français
Niveau : cours de 2ème cycle

Objectifs (en terme de compétences)

Donner une formation aux outils fondamentaux de la cryptographie

Objet de l'activité (principaux thèmes à aborder)

Le cours abordera des éléments de la théorie du codage et présentera des algorithmes et des exemples de protocoles cyptographiques.

Résumé : Contenu et Méthodes

1. Eléments de théorie de l'information, clés secrètes et clés publiques.
2. Algorithmes probabilistes et schémas probabilistes.
3. Quelques algorithmes cryptographiques : chiffrement DES, autres algorithmes de chiffrement, chiffrement et signature RSA, chiffrement et signature El Gamal, échange de clés Diffle-Hellman et examen des hypothèses cryptographiques utilisées.
4. Opposant passif et actif et ses objectifs : recherche exhaustive, attaque existentielle, fausse signature, cryptanalyse différentielle et linéaire.
5. Fonctions liées au codage.
6. Théorie du zéro-knowledge (ZK) et applications.
7. Standards et normes : précautions à prendre en pratique.
8. Exemples de protocoles cryptographiques : promesse, certificat, protocole CQ.

Autres informations (Pré-requis, Evaluation, Support, ...)

Références :
A. Menezes, P. Van Oorschot, S. Vanstone : Handbook of applied cryptography, CRS Press, 1996.
S. Stinson, Cryptography, theory and pratice, CRC Press, 1995
N. Koblitz, A course in number theory and cryptography, Springer-Verlag, Graduate Texts in Mathematics, 1994 (2e édition).

Autres crédits de l'activité dans les programmes

ELEC22	Deuxième année du programme conduisant au grade d'ingénieur civil électricien	(2.5 crédits)
ELEC23	Troisième année du programme conduisant au grade d'ingénieur civil électricien	(2.5 crédits)
INFO21	Première année du programme conduisant au grade d'ingénieur civil informaticien	(2.5 crédits)
INFO22	Deuxième année du programme conduisant au grade d'ingénieur civil informaticien	(2.5 crédits)
INFO23	Troisième année du programme conduisant au grade d'ingénieur civil informaticien	(2.5 crédits)
MAP21	Première année du programme conduisant au grade d'ingénieur civil en mathématiques appliquées	(2.5 crédits)
MAP22	Deuxième année du programme conduisant au grade d'ingénieur civil en mathématiques appliquées	(2.5 crédits)
MAP23	Troisième année du programme conduisant au grade d'ingénieur civil en mathématiques appliquées	(2.5 crédits)
MATH22/E	Deuxième licence en sciences mathématiques (Economie mathématique)	(2.5 crédits)
MATH22/G	Deuxième licence en sciences mathématiques	(2.5 crédits)
MATH22/S	Deuxième licence en sciences mathématiques (Statistique)	(2.5 crédits)