UCL Université catholique de Louvain

LMAT2450

2010-2011

Cryptography

5.0 crédits	30.0 h	1q

Enseignants:	Pereira Olivier ;
Langue d'enseignement:	Anglais
Lieu du cours	Louvain-la-Neuve
Thèmes abordés :	Le cours abordera des éléments de la théorie de la cryptographie et présentera des algorithmes et des exemples de protocoles cryptographies, avec un point de vue mathématique. Les aspects historiques seront abordés.1. Eléments de théorie de l'information, clés secrètes et clés publiques.2. Algorithmes probabilistes et schémas probabilistes. Preuves en cryptographie. 3. Quelques algorithmes cryptographiques : chiffrement DES, autres algorithmes de chiffrement, chiffrement et signature RSA ; chiffrement et signature El-Gamal, échanges de clés Diffle-Hellman et examen des hypothèses cryptographiques utilisées. Analyse de la complexité. 4. Opposant passif et actif et ses objectifs : recherche exhaustive, attaque existentielle, fausse signature, cryptananalyse différentielle et linéaire.5. Théorie du zéro-knowledge (ZK) et applications.6. Les courbes elliptiques en cryptographie.7. Standards et normes : précautions à prendre en pratique .8. Exemples de protocoles cryptographiques : promesse, certificat, protocole GQ.9. Un exemple détaillé de preuve formelle en cryptographie.L'équilibre entre les différentes parties et les détails du programme ci-dessus sont susceptibles de varier d'année en année.10. Méthode : exposés théoriques.
Acquis d'apprentissage	On introduira les concepts fondamentaux de la cryptographie moderne, en accordant une attention particulière aux aspects mathématiques et algorithmiques. Des problèmes et constructions historiques seront abordés, qui serviront de base à la présentation des algorithmes les plus utilisés de nos jours. Les aspects suivants seront abordés: 1. Éléments de théorie de l'information, chiffrement parfait 2. Algorithmes probabilistes, sécurité calculatoire, modèles d'attaquants, élaboration et usage de preuves en cryptographie 3. Chiffrement symétrique: notions de sécurité, constructions élémentaires, DES, AES, cryptanalyse, modes opératoires 4. Codes d'authentification, fonctions de hachage 5. Cryptographie asymétrique: protocole de Diffie-Hellman, chiffrement (RSA, El Gamal, ...), signature (RSA, hash-and-sign, DSS, ...), infrastructure à clé publique 6. Éléments de théorie algorithmique des nombres (tests de primalité, factorisation, extraction du logarithme discret, ...), cryptographie basée sur les courbes elliptiques 7. Protocoles : challenge-response, identification, authentification, protocoles à divulgation nulle, protocole GQ 8. Standards et normes : élaboration et précautions à prendre en pratique L'équilibre entre les différentes parties et les détails du programme ci-dessus sont susceptibles de varier d'année en année. *La contribution de cette UE au développement et à la maîtrise des compétences et acquis du (des) programme(s) est accessible à la fin de cette fiche, dans la partie « Programmes/formations proposant cette unité d'enseignement (UE) ».*
Autres infos :	Pré-requis: Éléments d'algèbre linéaire et d'arithmétique modulaire du niveau baccalauréat. Exposés oraux en français, avec support écrit en anglais Evaluation: Examen oral. Références: Le livre de Jonathan Katz et Yehuda Lindell: Introduction to Modern Cryptography (Chapman & Hall/CRC Press, 2007) peut servir de support pour la plupart des questions abordées dans le cours. Autres références utiles: - N. Koblitz : A course in number theory and cryptography, Springer-Verlag, Graduate Texts in Mathematics, 1994 (2e édition) - W. Mao: Modern Cryptography - Theory and Practice, Prentice Hall PTR, 2003 - A. Menezes, P. Van Oorschot, S. Vanstone : Handbook of applied cryptography (CRC press, 1996) (disponible librement sur le WEB à) - S. Stinson : Cryptography, theory and practice, CRC Press, 2005 (3e édition)

Cycle et année d'étude: :	> Master [120] en sciences mathématiques > Master [60] en sciences mathématiques > Master [120] : ingénieur civil en mathématiques appliquées > Master [120] : ingénieur civil en informatique > Master [120] en sciences informatiques > Master [120] : ingénieur civil électricien > Master [120] : ingénieur civil électromécanicien
Faculté ou entité en charge:	MATH