UCLouvain

lmat2450

2023

Cryptography

5.00 crédits	30.0 h + 15.0 h	Q1

Enseignants	Pereira Olivier ;Peters Thomas (supplée Pereira Olivier) ;
Langue d'enseignement	Anglais > Facilités pour suivre le cours en français
Lieu du cours	Louvain-la-Neuve
Préalables	Il est recommandé que l'étudiant·e ait des notions élémentaires d'algèbre comme couvertes dans les cours LMAT1131 ou LEPL1101 et de probabilités comme couverte dans les cours LMAT1271 ou LEPL1108.
Thèmes abordés	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 notions de sécurité et algorithmes les plus utilisés aujourd'hui, ainsi qu'à la justification de leur sécurité.
Acquis d'apprentissage	**A la fin de cette unité d'enseignement, l'étudiant est capable de :** Contribution du cours aux acquis d'apprentissage du programme de master en mathématique. **A la fin de cette activité, l'étudiant aura progressé dans sa capacité à :** - Connaître et comprendre un socle fondamental des mathématiques. Il aura notamment développé sa capacité à : -- Reconnaître les concepts fondamentaux d'importantes théories mathématiques actuelles. - Faire preuve d'abstraction, de raisonnement et d'esprit critique. Il aura notamment développé sa capacité à : -- Dégager les aspects unificateurs de situations et expériences différentes. -- Raisonner dans le cadre de la méthode axiomatique. -- Construire et rédiger une démonstration de façon autonome, claire et rigoureuse. Acquis d'apprentissage spécifiques au cours. **A la fin de cette activité, l'étudiant sera capable de :** 1 - Décrire, de manière rigoureuse, la fonction et les propriétés de sécurité des principales primitives utilisées en cryptographie. - Construire des attaques ou des preuves de la sécurité d'algorithmes. - Reconnaître et articuler les principales techniques de cryptographie mises en oeuvre pour sécuriser l'information. - Déterminer l'existence d'algorithmes offrant certaines garanties de sécurité dans différents contextes, notamment sur base de résultats d'impossibilité. **Modes d'évaluation des acquis des étudiants :** L'évaluation se fait sur base d'un examen écrit. La possibilité est offerte aux étudiants, durant l'examen, de présenter oralement leurs solutions aux questions proposées. On teste la connaissance et la compréhension des notions, des exemples et des principaux algorithmes introduits durant le cours, ainsi que la capacité à évaluer la sécurité d'algorithmes cryptographiques, que ce soit de manière constructive (rédaction de preuves de sécurité) ou destructive (description d'attaques). L'étudiant peut choisir la langue de l'examen (anglais ou français).
Modes d'évaluation des acquis des étudiants	L'évaluation se fait sur base d'un examen écrit. Des devoirs proposés pendant l'année pourront intervenir dans la note finale, pour un pourcentage maximum de 20%, et ce seulement si c'est au bénéfice de l'étudiant.
Méthodes d'enseignement	Le cours est donné sous forme de cours magistral et de séances de travaux pratiques. Des devoirs pourront aussi être proposés. Une attention particulière est consacrée à l'analyse des liens entre les concepts théoriques introduits dans le cours et les applications pratiques de la cryptographie.
Contenu	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 notions de sécurité et algorithmes les plus utilisés aujourd'hui, ainsi qu'à la justification de leur sécurité. - Éléments de théorie de l'information, chiffrement parfait.

	- Algorithmes probabilistes, sécurité calculatoire, modèles d'attaquants, élaboration et usage de preuves de sécurité en cryptographie. - Chiffrement symétrique: notions de sécurité, constructions élémentaires, DES, AES, cryptanalyse, modes opératoires. - Codes d'authentification, fonctions de hachage. - Cryptographie asymétrique: protocole de Diffie-Hellman, chiffrement (RSA, ElGamal, ...), signature (RSA, hash-and-sign, DSS, ...), infrastructure à clé publique. - Éléments de théorie algorithmique des nombres (arithmétique modulaire, test de primalité, courbes elliptiques). - Protocoles : challenge-response, identification, authentification, protocoles à divulgation nulle. - Standards et normes : élaboration et précautions à prendre en pratique. L'équilibre entre les différentes parties est susceptible de varier d'année en année.
Ressources en ligne	Site Moodle.
Bibliographie	J. Katz et Y. Lindell, Introduction to Modern Cryptography, 3rd edition. (Chapman and Hall/CRC Press). More references are available on Moodle.
Faculté ou entité en charge:	MATH

Programmes / formations proposant cette unité d'enseignement (UE)

Intitulé du programme	Sigle	Crédits	Prérequis	Acquis d'apprentissage
Approfondissement en sciences mathématiques	APPMATH	5		
Master [120] en sciences mathématiques	MATH2M	5		
Master [120] : ingénieur civil électricien	ELEC2M	5		
Master [120] : ingénieur civil en informatique	INFO2M	5		
Master [120] en sciences informatiques	SINF2M	5		
Master [120] : ingénieur civil en mathématiques appliquées	MAP2M	5		
Master [120] : ingénieur civil en science des données	DATE2M	5		
Master [120] en science des données, orientation technologies de l'information	DATI2M	5		