UCLouvain

ldacs1310

2026

Introduction to Applied Cryptography

5.00 crédits	30.0 h + 30.0 h	Q1

Enseignants	Peters Thomas ;Standaert François-Xavier ;
Langue d'enseignement	Anglais > Facilités pour suivre le cours en français
Lieu du cours	Louvain-la-Neuve
Préalables	· Discrete mathematics (as in LEPL1108 or LINFO1114) · Notions of probability (as in LBIR1212 or LEPL1108) · Computer programming (Python) and computational complexity (as in LEPL1401 or LINFO1101 and in LEPL1402) · Linear algebra (as in LEPL1101 or LINFO1112)
Thèmes abordés	Le cours abordera différents thèmes introductifs à la cryptographie et des éléments calculatoires pour son usage en pratique : notions de cryptographie symétrique (fonctions pseudo-aléatoires, chiffrement par bloc et fonctions booléennes), notions de cryptographie à clé publique (signature digitale, chiffrement asymétrique et calcul dans des corps simples et des groupes cycliques) et notions de protocoles d'échange de clés tels que présents dans les standards. Différentes applications courantes seront aussi abordées.
Acquis d'apprentissage	**A la fin de cette unité d'enseignement, l'étudiant est capable de :** Au terme de cette unité d'enseignement, l'étudiant sera capable de: · Comprendre les fonctionnalités offertes par les différentes primitives cryptographiques utilisées dans des protocoles d'authentification et pour construire des canaux de communication sûrs. · Comprendre comment la sécurité des mécanismes de cryptographie est établie. · Comprendre l'impact du choix de l'usage de différents types de mécanismes cryptographiques, en termes de sécurité et de performance (en temps et en énergie). Ce cours contribuera notamment aux axes suivants du référentiel d'acquis d'apprentissage du programme de bachelier en sciences informatiques: S1.L1, S1.L3, S1.L8, S1.G1, S.2.1, S.2.2, S.2.3, S.2.4, S.4.4, S5.2, S5.4, S5.5.
Modes d'évaluation des acquis des étudiants	L'évaluation se fait sur base d'un examen écrit.
Méthodes d'enseignement	Le cours est donné sous forme de cours magistral et de séances de travaux pratiques. Des devoirs pourront aussi être proposés.
Contenu	Le cours aborde les concepts fondamentaux de la cryptographie appliquée. - Sécurité : parfaite ou calculatoire, asymptotique ou conrète. - Base de cryptographie symétrique : générateur/fonction pseudo-aléatoire, chiffrement à clé secrète (bloc et mode), code d'authentification et fonction de hachage. - Base de cryptographie asymétrique : chiffrement à clé publique, schéma de signature. - Notion de chiffrement authentifié et application. - Standards et normes : élaboration et précautions à prendre en pratique. - Aperçu de cryptographie post-quantique. L'équilibre entre les différentes parties est susceptible de varier d'année en année.
Bibliographie	See on Moodle .
Faculté ou entité en charge:	DACS