Introduction to cryptography

Titulaires
Christophe PETIT (Coordonnateur) et Gilles VAN ASSCHE

Mnémonique du cours
INFO-F405

Crédits ECTS
5 crédits

Langue(s) d'enseignement
Anglais

Période du cours
Premier quadrimestre

Campus
Plaine

Contenu du cours

Éléments d'histoire de la cryptographie et de la sécurité informatique. Le chiffrement symétrique et asymétrique, l'authentification, le hachage, les signatures digitales et la gestion des clés. Définitions des notions de confidentialité et authenticité. Fonctionnement interne et externe des algorithmes cryptographiques.

Objectifs (et/ou acquis d'apprentissages spécifiques)

Comprendre les différents concepts de la sécurité informatique et de la cryptographie. Comprendre les algorithmes et protocoles cryptographiques usuels. Connaître les limites d'usage et d'inter-opérabilité de ces différents mécanismes.

Pré-requis et co-requis

Cours ayant celui-ci comme co-requis

MEMO-H504 | Mémoire de fin d'études en Informatique | 20 crédits

Méthodes d'enseignement et activités d'apprentissages

Cours et exercices

Contribution au profil d'enseignement

Acquérir des connaissances pointues dans son domaine, agir en acteur expert scientifique dans des résolutions de problèmes, communiquer dans un langage adapté au contexte et à son public, se développer professionnellement dans un souci du respect des questions éthiques liées à son domaine d'expertise.

Références, bibliographie et lectures recommandées

- Paar et Pelzl, *Understanding Cryptography*, Springer 2011 (ISBN 978-3642041006)
- Katz et Lindell, *Introduction to Modern Cryptography (third edition)*, CRC Press, 2021 (ISBN 978-0815354369)
- Alfred J. Menezes, Paul C. van Oorschot et Scott A. Vanstone, *Handbook of Applied Cryptography*, CRC Press, 1997

Support(s) de cours

Université virtuelle

Autres renseignements

Lieu(x) d'enseignement

Plaine

Contact(s)

- Gilles Van Assche, gilles.van.assche@ulb.be
- Abel Laval, Département d'Informatique - CP212 Campus Plaine - Bâtiment N/O, 8ème étage, abel.laval@ulb.be
- Christhope Petit, Département d'Informatique - CP212 Campus Plaine - Bâtiment N/O, 8ème étage, christophe.petit@ulb.be

Méthode(s) d'évaluation

Examen écrit

Méthode(s) d'évaluation (complément)

Important : l'assiduité aux travaux pratiques est un critère nécessaire de réussite

Construction de la note (en ce compris, la pondération des notes partielles)

Examen de fin de quadrimestre

Langue(s) d'évaluation principale(s)

Anglais

Programmes

Programmes proposant ce cours à la faculté des Sciences

MA-INFO | Master en sciences informatiques | finalité Spécialisée/bloc 1 et MA-SECU | Master en cybersécurité | finalité Conception et Analyse de Systèmes/bloc 1 et finalité Stratégies en entreprise/bloc 1

Programmes proposant ce cours à l'école polytechnique de Bruxelles

MA-IRIF | Master : ingénieur civil en informatique | finalité Spécialisée/bloc 1