Description du module

Cryptographie et théorie du codage

Généralités

Nombres de crédits ECTS

3

Sigle du module

FTP_CryptCod

Version

10.10.2015

Responsable du module

Grégoire Nicollier, HES-SO

Langue

	Lausanne	Berne	Zurich
Enseignement	☐ E ☑ F	☐ D ☐ E ☐ F	☑ D ☐ E
Documentation	☑ E ☑ F	☐ D ☐ E ☐ F	☐ D ☑ E
Questions d'examen	☐ E ☑ F	☐ D ☐ E ☐ F	☐ D ☑ E

Catégorie du module

☑ Bases théoriques élargies

☐ Approfondissement technique et scientifique

☐ Modules de savoirs contextuels

Périodes

☑ 2 périodes d'enseignement frontal et une période d'exercices par semaine

☐ 2 périodes d'enseignement frontal par semaine

Brève description /Explication des objectifs et du contenu du module en quelques phrases

Ce cours pose les bases mathématiques de la cryptographie et du codage et présente de nombreux exemples pratiques.

Objectifs, contenu et méthodes

Objectifs d'apprentissage et compétences visées

Le but de ce cours est d'enseigner des techniques avancées dans les domaines de l'algèbre appliquée et de la théorie des nombres, en mettant l'accent sur les méthodes utiles en cryptographie et en théorie du codage.

Contenu du module avec pondération des contenus d'enseignement

- Algèbre : structures algébriques (groupes, corps), arithmétique modulaire, théorème chinois, construction et propriétés de base des corps de Galois GF (p^m), applications à la théorie du codage et en cryptographie.
- Algorithmes en théorie des nombres (test de primalité, algorithmes de factorisation, méthode des courbes elliptiques), applications à la théorie du codage et en cryptographie.
- Utilisation d'un environnement de développement (Java, C, C++).

Semaine	Contenu du cours (l'ordre des thèmes et leur pondération peuvent varier)
1	Algebraic basics:
2	modular arithmetic, Euclidean algorithm, extended Euclidean algorithm, Bezout theorem, Fermat Euler theorem, Chinese Remainder theorem
3	Asymmetric (public key) cryptography:
4	Diffie Hellman key exchange, RSA algorithm, digital signatures
5	Algebraic basics: polynomials and finite fields
6	Symmetric (secret key) cryptography: review of important examples (substitution cipher, transposition cipher, product cipher, block cipher,etc.)
7	Symmetric (secret key) cryptography: Hash functions, International Data Encryption Algorithm (IDEA), Data Encryption Standard (DES), Advanced Encryption Standard (AES)
8	Elliptic Curve Diffie Hellman (ECDH), digital signatures
9	
10	One-time pad (OTP), Quantum Cryptography
11	Error-correcting codes:
12	Cyclic codes, Reed-Solomon, BCH, Convolutional Codes, Turbo Codes
13	
14	

Méthodes d'enseignement et d'apprentissage

Enseignement ex cathedra avec exemples concrets et appliqués

Exercices avec corrigé permettant la mise en pratique et l'approfondissement des connaissances acquises

Connaissances et compétences prérequises

Aucune, si ce n'est un intérêt pour les liens entre la théorie mathématique et les applications pratiques

Bibliographie

Buchmann, Johannes: Introduction to Cryptography, 2nd. ed., Springer Verlag, 2004, ISBN: 978-0-387-21156-5

Stinson, Douglas: Cryptography: Theory and Practice, 3rd ed., Chapman & Hall, 2005, ISBN: 978-1-584-88508-5

Zémor, Gilles: Cours de cryptographie, Cassini, 2000, ISBN: 2-84225-020-6

Mode d'évaluation

Conditions d'admission aux examens de fin de module (tests exigés)

Présence à 10 séances d'exercices au minimum

Examen écrit de fin de module

Durée de l'examen:	120 minutes
Moyens autorisés:	Calculatrice de poche non programmable
	Copie des transparents
	Scripts du cours (mais **sans** anciens examens ni exercices ni corrigés !)
	Les copies des transparents et les scripts peuvent être complétés par des notes manuscrites de volume quelconque. Ne sont autorisés ni livres, ni anciens examens, ni exercices, ni corrigés, que ce soit sous forme imprimée ou comme copies.