Module Description, available in: EN, FR

Cryptography and Coding Theory

General Information

Number of ECTS Credits

3

Module code

FTP_CryptCod

Valid for academic year

2024-25

Last modification

2018-11-01

Coordinator of the module

Alexandre Duc (HES-SO, alexandre.duc@heig-vd.ch)

Explanations regarding the language definitions for each location:

- Instruction is given in the language defined below for each location/each time the module is held.
- Documentation is available in the languages defined below. Where documents are in several languages, the percentage distribution is shown (100% = all the documentation).
- The examination is available 100% in the languages shown for each location/each time it is held.

	Lausanne			Lugano	Zurich		
Instruction		**X** F 100%			**X** E 100%		
Documentation		**X** F 70-80%	**X** E 20-30%		**X** E 100%		
Examination		**X** F 100%			**X** E 100%		

Module Category

FTP Fundamental theoretical principles

Profile Recommendations

This module is recommended for the following profiles:

	Lausanne	Zurich
Profile	CS	CS, ICS

Lessons

2 lecture periods and 1 tutorial period per week

Entry level competences

Prerequisites, previous knowledge

No particular prerequisites are required, but fundamental interest in practical applications of mathematics!

Brief course description of module objectives and content

This course provides the mathematical fundamentals of cryptography and coding theory and illustrates them with numerous practical examples.

Aims, content, methods

Learning objectives and competencies to be acquired

This course provides advanced methods of applied algebra and number theory and concentrates on their practical applications in cryptography and coding theory.

Module content with weighting of different components

- Algebra: algebraic structures (proups, fields), modular arithmetic, Chinesise remainder theorem, constuction and fundamental properties of finite fields (Galois fields GF (pm)), applications to cryptography and coding theory
- Algorithms in number theory (primality tests, integer factorization methods, elliptic curves), applications to cryptography and coding theory
- Use of a development environment (Java, C, C++, Python, Sage)

Week	Contents (Order and weighting may be adapted)
1	Algebraic basics: modular arithmetic, Euclidean algorithm, extended Euclidean algorithm, Bezout theorem, Fermat Euler theorem, Chinese Remainder theorem
2	
3	Asymmetric (public key) cryptography: Diffie Hellman key exchange, RSA algorithm, digital signatures
4	
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, Data Encryption Standard (DES), Advanced Encryption Standard (AES), Chacha20, modes of operation, authenticated encryption
8	Elliptic Curve Diffie Hellman (ECDH), digital signatures
9	
10	One-time pad (OTP), Modern Topics in Cryptography, TLS and X509v3
11	Error-correcting codes: Cyclic codes, Reed-Solomon, BCH, Convolutional Codes, Turbo Codes
12	
13	
14	

Teaching and learning methods

- Lectures with practical application examples
- Exercices with solutions allowing knowledge application and deepening

Literature

- 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

Assessment

Certification requirements

Module uses certification requirements

Certification requirements for final examinations (conditions for attestation)

Presence is required during at least 10 exercice sessions

Basic principle for exams

As a rule, all standard final exams are conducted in written form. For resit exams, lecturers will communicate the exam format (written/oral) together with the exam schedule.

Standard final exam for a module and written resit exam

Kind of exam

Written exam

Duration of exam

120 minutes

Permissible aids

Aids permitted as specified below:

Permissible electronic aids

Nonprogrammable pocket calculator

Other permissible aids

Copies of the slides
Course notes (but no former exams, exercices, or solutions!)

Copies of the slides and course notes may be supplemented by any amount of handwritten notes. Books and former exams, exercices, and solutions are prohibited in print form and as complete copies.

Special case: Resit exam as oral exam

Kind of exam

Oral exam

Duration of exam

30 minutes

Permissible aids

Aids permitted as specified below:

Permissible electronic aids

As for the written examination, but only during preparation

Other permissible aids

As for the written examination, but only during preparation

Description du module, disponible en: EN, FR

Cryptographie et théorie du codage

Informations générales

Nombre de crédits ECTS

3

Code du module

FTP_CryptCod

Valable pour l'année académique

2024-25

Dernière modification

2018-11-01

Coordinateur/coordinatrice du module

Alexandre Duc (HES-SO, alexandre.duc@heig-vd.ch)

Explications concernant les langues d'enseignement par site :

- Les cours se dérouleront dans la langue définie ci-dessous par lieu/exécution.
- Les documents sont disponibles dans les langues définies ci-dessous. Pour le multilinguisme, voir la répartition en pourcentage (100% = documents complets)
- L'examen est disponible à 100% dans chaque langue sélectionnée pour chaque lieu/exécution.

	Lausanne			Lugano	Zurich		
Leçons		**X** F 100%			**X** E 100%		
Documentation		**X** F 70-80%	**X** E 20-30%		**X** E 100%		
Examen		**X** F 100%			**X** E 100%		

Catégorie de module

FTP bases théoriques élargies

Recommandations de profil

Ce module est recommandé pour les profils suivants :

	Lausanne	Zurich
Profil	CS	CS, ICS

Leçons

2 leçons et 1 leçon de pratique par semaine

Compétences préalables

Connaissances préalables, compétences initiales

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

Brève description du contenu et des objectifs

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

Objectifs, contenus, méthodes

Objectifs d'apprentissage, compétences à acquérir

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 des modules avec pondération du contenu des cours

- Algèbre : structures algébriques (groupes, corps), arithmétique modulaire, théorème chinois, construction et propriétés de base des corps de Galois GF (pm), 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++, Python, Sage)

Semaine	Contenu du cours (l'ordre des thèmes et leur pondération peuvent varier)
1	Algebraic basics: modular arithmetic, Euclidean algorithm, extended Euclidean algorithm, Bezout theorem, Fermat Euler theorem, Chinese Remainder theorem
2	
3	Asymmetric (public key) cryptography: Diffie Hellman key exchange, RSA algorithm, digital signatures
4	
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, Data Encryption Standard (DES), Advanced Encryption Standard (AES), Chacha20, modes of operation, authenticated encryption
8	Elliptic Curve Diffie Hellman (ECDH), digital signatures
9	
10	One-time pad (OTP), Modern Topics in Cryptography, TLS and X509v3
11	Error-correcting codes: Cyclic codes, Reed-Solomon, BCH, Convolutional Codes, Turbo Codes
12	
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

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

Evaluation

Conditions d'admission

Le module utilise les conditions d'admission

Conditions d'admission à l'examen de fin de module (exigences du certificat)

Présence à 10 séances d'exercices au minimum

Principe pour les examens

En règle générale, tous les examens réguliers de fin de module se déroulent sous forme écrite. Concernant les examens de répétition, leur format (écrit ou oral) sera communiqué par l'enseignant-e en même temps que le calendrier des examens.

Examen de fin de module régulier et examen écrit de répétition

Type de l'examen

Examen écrit

Durée de l'examen

120 minutes

Aides autorisées

Les aides suivantes sont autorisées:

Aides électroniques autorisées

Calculatrice de poche non programmable

Autres aides autorisées

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.

Cas spécial: examen de répétition oral

Type de l'examen

Examen oral

Durée de l'examen

30 minutes

Aides autorisées

Les aides suivantes sont autorisées:

Aides électroniques autorisées

Comme pour l'examen écrit, mais seulement durant la préparation

Autres aides

Comme pour l'examen écrit, mais seulement durant la préparation