Modulbeschrieb

Kryptographie und Codierungstheorie

Allgemeine Informationen

Anzahl ECTS-Credits

3

Modulkürzel

FTP_CryptCod

Version

10.10.2015

Modulverantwortliche/r

Grégoire Nicollier, HES-SO

Sprache

	Lausanne	Bern	Zürich
Unterricht	☐ E ☑ F	☐ D ☐ E ☐ F	☑ D ☐ E
Unterlagen	☑ E ☑ F	☐ D ☐ E ☐ F	☐ D ☑ E
Prüfung	☐ E ☑ F	☐ D ☐ E ☐ F	☐ D ☑ E

Modulkategorie

☑ Erweiterte theoretische Grundlagen
☐ Technisch-wissenschaftliche Vertiefung
☐ Kontextmodule

Lektionen

☑ 2 Vorlesungslektionen und 1 Übungslektion pro Woche
☐ 2 Vorlesungslektionen pro Woche

Kurzbeschreibung /Absicht und Inhalt des Moduls in einigen Sätzen erklären

Der Kurs vermittelt die mathematischen Grundlagen von Kryptographie und Codierungstheorie und illustriert diese an zahlreichen Beispielen aus der Praxis.

Ziele, Inhalt und Methoden

Lernziele, zu erwerbende Kompetenzen

Diese Vorlesung vermittelt weiterführende Methoden der angewandten Algebra und der Zahlentheorie, und konzentriert sich auf deren praktische Anwendung in der Kryptographie und der Codierungstheorie.

Modulinhalt mit Gewichtung der Lehrinhalte

- Algebra: algebraische Strukturen (Gruppen, Körper), modulare Arithmetik, Chinesischer Restsatz, Konstruktion und grundlegende Eigenschaften endlicher Körper (Galois-Körper GF (p^m)), Anwendungen in der Codierungstheorie und Kryptographie
- Algorithmen der Zahlentheorie (Primzahltest, Faktorisierungsverfahren, elliptische Kurvenmethode), Anwendungen in der Codierungstheorie und Kryptographie
- Anwendung einer Programmierumgebung (Java, C, C++)

Woche	Thema (Reihenfolge und Gewichtung kann angepasst werden)
	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, 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: Cyclic codes, Reed-Solomon, BCH, Convolutional Codes, Turbo Codes
12	
13	
14	

Lehr- und Lernmethoden

- Vorlesungen mit praktischen Anwendungsbeispielen
- Übungen mit Lösungen zur Umsetzung und Vertiefung des Gelernten

Voraussetzungen, Vorkenntnisse, Eingangskompetenzen

- Es sind keine besonderen Vorkenntnisse erforderlich. Ein grundsätzliches Interesse an den praktischen Anwendungsmöglichkeiten der Mathematik wird jedoch vorausgesetzt.

Bibliografie

- 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

Leistungsbewertung

Zulassungsbedingungen für die Modulschlussprüfung (Testatbedingungen)

Präsenz an mindestens 10 Übungsveranstaltungen

Schriftliche Modulschlussprüfung

Prüfungsdauer :	120 Minuten
Erlaubte Hilfsmittel:	Nicht-programmierbarer Taschenrechner Kopien der Folien Skripte der Vorlesung (aber **keine** alten Prüfungen, Übungen, Musterlösungen!) Kopien der Folien und Skripte dürfen durch handschriftliche Notizen in beliebigem Umfang ergänzt werden. Bücher, alte Prüfungen, Übungen und dazugehörige Musterlösungen sind weder als Ausdrucke noch als vollständige Abschriften zugelassen.