

**Modulbeschreibung**

# Kryptographie und Codierungstheorie

**Allgemeine Informationen**
**Anzahl ECTS-Credits**

3

**Modulkürzel**

FTP\_CryptCod

**Version**

30. August 2009

**Modulverantwortliche/r**

Grégoire Nicollier, HES-SO

**Sprache**

	Lausanne	Bern	Zürich
Unterricht	<input type="checkbox"/> E <input checked="" type="checkbox"/> F	<input type="checkbox"/> D <input type="checkbox"/> E <input type="checkbox"/> F	<input checked="" type="checkbox"/> D <input type="checkbox"/> E
Unterlagen	<input checked="" type="checkbox"/> E <input checked="" type="checkbox"/> F	<input type="checkbox"/> D <input type="checkbox"/> E <input type="checkbox"/> F	<input type="checkbox"/> D <input checked="" type="checkbox"/> E
Prüfung	<input type="checkbox"/> E <input checked="" type="checkbox"/> F	<input type="checkbox"/> D <input type="checkbox"/> E <input type="checkbox"/> F	<input type="checkbox"/> D <input checked="" type="checkbox"/> E

**Modulkategorie**

- Erweiterte theoretische Grundlagen
- Technisch-wissenschaftliche Vertiefung
- Kontextmodule

**Lektionen**

- x 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 (Die Themenreihenfolge kann variieren)
1	Algebraische Grundlagen: Modulare Arithmetik, euklidischer Algorithmus, erweiterter euklidischer Algorithmus, Satz von Bezout, Satz von Fermat-Euler, Chinesischer Restsatz
2	
3	Asymmetrische Kryptographie: Diffie-Hellman-Schlüsselaustausch, RSA-System, digitale Signaturen
4	
5	Algebraische Grundlagen: Polynome und endliche Körper
6	Symmetrische Kryptographie: Beispiele aus der Geschichte der Kryptographie (Verschlüsselung durch Substitution oder Permutation, Produktverschlüsselung, Blockverschlüsselung u.a.)
7	Symmetrische Kryptographie: Hash-Funktionen, IDEA, DES-Verfahren, AES-Verfahren
8	Elliptische Kurven und Diffie-Hellman-Schlüsselaustausch, digitale Signaturen
9	
10	One-Time-Pad-Verfahren, Sicherheit, Authentifizierung
11	Fehlerkorrekturverfahren, linear rückgekoppeltes Schieberegister (LFSR), zyklische Codes
12	

13	
14	Quantenkryptographie

**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: Zusammenfassung (10 A4-Seiten), Taschenrechner