Titel des Moduls: Grundzüge der Kryptologie	**LP (nach ECTS): 3**	**Kurzbezeichnung:** BINF-AktThemAlgo.W12
Verantwortliche/-r für das Modul: Prof. Rolf Niedermeier	**Sekr.:** TEL 5-1	**Email:** rolf.niedermeier@tu-berlin.de

Modulbeschreibung

1. Qualifikationsziele

Absolventinnen und Absolventen dieses Moduls verfügen über Kenntnisse zu wichtigen Ideen der Kryptologie, sowohl von theoretischer als auch von anwendungsbezogener Seite. Sie sind in der Lage, sich ein neues Thema eigenständig zu erarbeiten und dieses in einem klar strukturierten Vortrag samt schriftlicher Ausarbeitung Nichtexperten verständlich zu vermitteln.

Die Veranstaltung vermittelt überwiegend:
Fachkompetenz 40% Methodenkompetenz 40% Systemkompetenz 10% Sozialkompetenz 10%

2. Inhalte

In diesem Seminar werden elementare Methoden zum Verschlüsseln von Nachrichten/Informationen besprochen. Dabei soll insbesondere auch die praktische Anwendbarkeit der theoretischen Protokolle/Algorithmen vorgestellt werden. Die Themen umfassen unter anderen:

- Public-Key Verschlüsselungsverfahren
- symmetrische Verschlüsselungsverfahren
- Fingerabdrucksfunktionen
- Authentifizieren
- Elektronisches Geld
- Hashing
- Zero-Knowledge-Beweise
- Pokern am Telefon

3. Modulbestandteile

LV-Titel	LV-Art	SWS	LP (nach ECTS)	Pflicht(P) / Wahl(W) Wahlpflicht(WP)	Semester (WiSe / SoSe)
Aktuelle Themen der Algorithmik	SE	2	3	P	WiSe

4. Beschreibung der Lehr- und Lernformen

Klassische Seminarform mit Vorträgen (ca. 45min) durch die Teilnehmer und der Ausarbeitung begleitender Schriftstücke (3-6 Seiten), die die wesentlichen Inhalte des jeweiligen Vortrags wiedergeben. Direktes Feedback durch die Veranstalter und die anderen Teilnehmer.

5. Voraussetzungen für die Teilnahme

6. Verwendbarkeit

Wahlpflicht im Bachelor Informatik im Studienschwerpunkt Softwaretechnik und im Bachelor Technische Informatik im Studienschwerpunkt Informatik.
Bei ausreichenden Kapazitäten auch als Wahlpflichtmodul in anderen Studiengängen wählbar.

7. Arbeitsaufwand und Leistungspunkte

LV-Art	Berechnung	Stunden

Präsenzzeiten:	15x2	30
Selbststudium: (Nachbereitung, eigenständige Erarbeitung, Erstellung des Vortrags und der Ausarbeitung)		60
	Gesamt:	90

8. Prüfung und Benotung des Moduls

Prüfungsäquivalente Studienleistungen (PÄS):
60% Vortrag, 30% Ausarbeitung, 10% Mitarbeit

9. Dauer des Moduls

Das Modul kann in 1 Semester abgeschlossen werden.

10. Teilnehmer(innen)zahl

Max. 15

11. Anmeldeformalitäten

http://www.akt.tu-berlin.de

12. Literaturhinweise, Skripte

Skripte in Papierform vorhanden	ja	nein **X**
Wenn ja, wo kann das Skript gekauft werden?		
Skripte in elektronischer Form vorhanden	ja	nein **X**

Literatur:

- Dietmar Wätjen: Kryptographie: Grundlagen, Algorithmen, Protokolle (Spektrum Lehrbuch 2003)
- Albrecht Beutelspacher: Kryptologie: Eine Einführung in die Wissenschaft vom Verschlüsseln, Verbergen und Verheimlichen (Vieweg 2005)
- Berthold Vöcking et al. (Hrsg.) : Taschenbuch der Algorithmen (Springer 2008)

13. Sonstiges