TECHNISCHE HOCHSCHULE LÜBECK

Modul: Kryptographie

Niveau		**Stundenplankürzel**	Krypto
Modulname englisch	Cryptography		
Modulverantwortliche	Werth		
Fachbereich	Elektrotechnik und Informatik		
Studiengang	Informatik/Softwaretechnik für verteilte Systeme, Master		
Verpflichtungsgrad	Wahlpflicht	**ECTS-Leistungspunkte**	5
Fachsemester	(Nicht festgelegt)	**Semesterwochenstunden**	4
Dauer in Semestern	1	**Arbeitsaufwand in Stunden**	150
Angebotshäufigkeit	(Flexibel)	**Präsenzstunden**	47
Lehrsprache	Deutsch	**Selbststudiumsstunden**	103

Der folgende Abschnitt ist nur ausgefüllt, wenn es **genau eine** modulabschließende Prüfung gibt.

Prüfungsleistung	Portfolio-Prüfung	**Prüfsprache**	Deutsch
Dauer PL in Minuten		**Bewertungssystem PL**	Drittelnoten

Lernergebnisse	Die Studierenden • beherrschen grundlegende sowie fortgeschrittene kryptographische Primitive und Protokolle. • können verschiedene Verschlüsselungsverfahren vergleichend bewerten • können kryptographische Verfahren, wie z.B. Authentisierung, Signatur oder Verschlüsselung, in der Praxis einsetzen. • können bei der Bewertung und Auswahl der Verfahren zukünftige Verfahren der Kryptoanalyse berücksichtigen. • besitzen die Voraussetzungen, um neue Verfahren aus der aktuellen Fachliteratur zu verstehen.
Teilnahmevoraussetzungen	

Der vorige Abschnitt ist nur ausgefüllt, wenn es **genau eine** modulabschließende Prüfung gibt.

Berücksichtigung von Gender- und Diversity-Aspekten	✔ Verwendung geschlechtergerechter Sprache (THL-Standard) ✔ Zielgruppengerechte Anpassung der didaktischen Methoden ✘ Sichtbarmachen von Vielfalt im Fach (Forscherinnen, Kulturen etc.)
Verwendbarkeit	
Bemerkungen	

TECHNISCHE HOCHSCHULE LÜBECK

Lehrveranstaltung: Kryptographie (Vorlesung)

(zu Modul: Kryptographie)

Lehrveranstaltungsart	Vorlesung	**Lernform**	Präsenz
LV-Name englisch	Cryptography (lecture)		
Anwesenheitspflicht	nein	**ECTS-Leistungspunkte**	3
Teilnahmebeschränkung		**Semesterwochenstunden**	3
Gruppengröße		**Arbeitsaufwand in Stunden**	90
Lehrsprache	Deutsch	**Präsenzstunden**	35
Studienleistung		**Selbststudiumsstunden**	55
Dauer SL in Minuten		**Bewertungssystem SL**	
Der folgende Abschnitt ist nur ausgefüllt, wenn es eine lehrveranstaltungsspezifische Prüfung gibt.			
Prüfungsleistung		**Prüfsprache**	
Dauer PL in Minuten		**Bewertungssystem PL**	
Lernergebnisse	Beispiel: Die Studierenden können die Verfahren der deskriptiven Statistik selbstständig anwenden.		
Teilnahmevoraussetzungen			
Der vorige Abschnitt ist nur ausgefüllt, wenn es eine lehrveranstaltungsspezifische Prüfung gibt.			
Lehrinhalte	• Blockchiffren • Asymmetrische Verschlüsselungs- und Signaturverfahren (RSA, Diffe-Hellman, ElGamal, …) • Hashfunktionen, Message Authentication Codes und Schlüsselableitungsfunktionen • Postquantum sichere Verfahren (Gitterbasierte Kryptographie, …) • Kryptographische Protokolle (Zero Knowledge, Secret Sharing ,..) • Aktuelle Forschungsergebnisse zu den Themen		
Literatur	Albrecht Beutelspacher, Jörg Schwenk und Klaus-Dieter Wolfenstetter. *Moderne Verfahren der Kryptographie.* Springer Spektrum, 2015. Johannes Buchmann. *Einführung in die Kryptographie*. Springer-Verlag Berlin Heidelberg, 2016. Christoph Paar und Jan Pelzl. *Kryptographie verständlich*. Springer-Verlag Berlin Heidelberg, 2016. J. Katz, Y. Lindell. *Introduction to Modern Cryptography* (*2nd Edition).* Chapman & Hall. R. Cramer, I. Damgard, J.B. Nielsen, *Secure Multiparty Computation and Secret Sharing*, Cambridge.		
Bemerkungen			

Lehrveranstaltung: Kryptographie (Praktikum)

(zu Modul: Kryptographie)

Lehrveranstaltungsart	Praktikum	**Lernform**	Präsenz
LV-Name englisch	Cryptography (practical training)		
Anwesenheitspflicht	nein	**ECTS-Leistungspunkte**	2
Teilnahmebeschränkung		**Semesterwochenstunden**	1
Gruppengröße	12	**Arbeitsaufwand in Stunden**	60
Lehrsprache	Deutsch	**Präsenzstunden**	12
Studienleistung		**Selbststudiumsstunden**	48
Dauer SL in Minuten		**Bewertungssystem SL**	
Der folgende Abschnitt ist nur ausgefüllt, wenn es eine lehrveranstaltungsspezifische Prüfung gibt.			
Prüfungsleistung		**Prüfsprache**	
Dauer PL in Minuten		**Bewertungssystem PL**	
Lernergebnisse			
Teilnahmevoraussetzungen			
Der vorige Abschnitt ist nur ausgefüllt, wenn es eine lehrveranstaltungsspezifische Prüfung gibt.			
Lehrinhalte	• Aufgaben und praktische Übungen zum Verständnis der Verschlüsselungs- und Analyseverfahren		
Literatur			
Bemerkungen			