TECHNISCHE HOCHSCHULE LÜBECK

Modul: Kryptoanalyse

Niveau		**Stundenplankürzel**	KryptoA
Modulname englisch	Cryptanalysis		
Modulverantwortliche	Werth, Sören		
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**	60
Lehrsprache	Deutsch	**Selbststudiumsstunden**	90

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 • kennen wichtige symmetrische und Public-Key Kryptosysteme. • sind mit der Sicherheitsanalyse solcher Systeme vertraut und können die Sicherheit solcher Verfahren beurteilen. • haben die elementaren mathematischen Analysemethoden durchdrungen und können diese auf verwandte Problemstellungen anwenden. • können einfache Seitenkanalangriffe durchführen. • 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: Kryptoanalyse (Vorlesung)

(zu Modul: Kryptoanalyse)

Lehrveranstaltungsart	Vorlesung	**Lernform**	Präsenz
LV-Name englisch	Cryptanalysis (lecture)		
Anwesenheitspflicht	nein	**ECTS-Leistungspunkte**	3
Teilnahmebeschränkung		**Semesterwochenstunden**	3
Gruppengröße		**Arbeitsaufwand in Stunden**	90
Lehrsprache	Deutsch	**Präsenzstunden**	45
Studienleistung		**Selbststudiumsstunden**	45
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	• Symmetrische Verschlüsselungsverfahren und deren Kryptoanalyse
	  • Differentielle Analyse
	  • Lineare Analyse
	• Asymmetrische Verfahren und deren Kryptoanalyse
	  • RSA
	  • Diskrete Logarithmen
	• Seitenkanalanalysen und deren stochastische Grundlagen
	  • Poweranalysen		

Literatur	J. Buchmann. *Einführung in die Kryptographie*. Springer-Verlag Berlin Heidelberg. J. Katz, Y. Lindell. *Introduction to Modern Cryptography* (*2nd Edition).* Chapman & Hall. S. Mangard, E. Oswald, T. Popp. *Power Analysis Attacks - Revealing the Secrets of Smart Cards*. Springer, Berlin. C. Swenson. *Modern Cryptanalysis,* Wiley. M. Stamp, R.M. Low. *Applied Cryptanalysis,* Wiley.		
Bemerkungen			

TECHNISCHE HOCHSCHULE LÜBECK

Lehrveranstaltung: Kryptoanalyse (Praktikum)

(zu Modul: Kryptoanalyse)

Lehrveranstaltungsart	Praktikum	**Lernform**	Präsenz
LV-Name englisch	Cryptoanalysis (practical training)		
Anwesenheitspflicht	ja	**ECTS-Leistungspunkte**	2
Teilnahmebeschränkung		**Semesterwochenstunden**	1
Gruppengröße	12	**Arbeitsaufwand in Stunden**	60
Lehrsprache	Deutsch	**Präsenzstunden**	15
Studienleistung	Praktikum	**Selbststudiumsstunden**	45
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	• Übungen zum Verständnis der Verschlüsselungs- und Analyseverfahren • Praktische Durchführung von Seitenkanalanalysen im Labor		
Literatur			
Bemerkungen			