

Modul: Angewandte Kryptographie

Niveau	Bachelor	Kürzel	AKrypto
Modulname englisch	Applied Cryptography		
Modulverantwortliche	Berndt, Sebastian		
Fachbereich	Elektrotechnik und Informatik		
Studiengang	Informationstechnologie und Design, Bachelor		
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	Prüfungsprache	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 Sicherheitsprobleme in der Praxis identifizieren. • Können kryptographische Verfahren, wie z.B. Authentisierung, Signatur oder Verschlüsselung, in der Praxis einsetzen.		
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	Studiengänge des Fachbereichs Elektrotechnik und Informatik
Bemerkungen	

Lehrveranstaltung: Angewandte Kryptographie (Vorlesung)

(zu Modul: Angewandte Kryptographie)

Lehrveranstaltungsart	Vorlesung	Lernform	Präsenz
LV-Name englisch	Applied 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		Prüfungsprache	
Dauer PL in Minuten		Bewertungssystem PL	
Lernergebnisse			
Teilnahmevoraussetzungen			

Der vorige Abschnitt ist nur ausgefüllt, wenn es eine lehrveranstaltungsspezifische Prüfung gibt.

Lehrinhalte	• Sicherheitsmodellierung (perfekte Sicherheit und Komplexitätstheoretische Sicherheit) • Moderne symmetrische Verschlüsselungsverfahren (Stromchiffren und Blockchiffren) • Hashfunktionen und Message Authentication Codes • Schlüsselaustausch • Asymmetrische Verschlüsselungs- und Signaturverfahren • Kryptographische Protokolle und Anwendungen in der Praxis, insbesondere TLS 1.3
Literatur	Albrecht Beutelspacher, Jörg Schwenk und Klaus-Dieter Wolfenstetter. <i>Moderne Verfahren der Kryptographie</i>. Springer Spektrum, 2015. Johannes Buchmann. <i>Einführung in die Kryptographie</i>. Springer-Verlag Berlin Heidelberg, 2016. Christoph Paar und Jan Pelzl. <i>Kryptographie verständlich</i>. Springer-Verlag Berlin Heidelberg, 2016.
Bemerkungen	

Lehrveranstaltung: Angewandte Kryptographie (Praktikum)

(zu Modul: Angewandte Kryptographie)

Lehrveranstaltungsart	Praktikum	Lernform	Präsenz
LV-Name englisch	Applied 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	Drittelnoten

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 Verfahren
Literatur	
Bemerkungen	