

## Modul: Angewandte Kryptographie

<b>Niveau</b>	Bachelor	<b>Stundenplankürzel</b>	AKrypto
<b>Modulname englisch</b>	Applied Cryptography		
<b>Modulverantwortliche</b>	Werth, Sören		
<b>Fachbereich</b>	Elektrotechnik und Informatik		
<b>Studiengang</b>	Informatik/Softwaretechnik, Bachelor		
<b>Verpflichtungsgrad</b>	Wahlpflicht	<b>ECTS-Leistungspunkte</b>	5
<b>Fachsemester</b>	(Nicht festgelegt)	<b>Semesterwochenstunden</b>	4
<b>Dauer in Semestern</b>	1	<b>Arbeitsaufwand in Stunden</b>	150
<b>Angebotshäufigkeit</b>	(Flexibel)	<b>Präsenzstunden</b>	47
<b>Lehrsprache</b>	Deutsch	<b>Selbststudiumsstunden</b>	103

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

<b>Prüfungsleistung</b>	Portfolio-Prüfung	<b>Prüfungsprache</b>	Deutsch
<b>Dauer PL in Minuten</b>		<b>Bewertungssystem PL</b>	Drittelnoten
<b>Lernergebnisse</b>	Die Studierenden <ul style="list-style-type: none"> <li>• beherrschen grundlegende sowie fortgeschrittene kryptographische Primitive und Protokolle.</li> <li>• können verschiedene Verschlüsselungsverfahren vergleichend bewerten.</li> <li>• können Sicherheitsprobleme in der Praxis identifizieren.</li> <li>• Können kryptographische Verfahren, wie z.B. Authentisierung, Signatur oder Verschlüsselung, in der Praxis einsetzen.</li> </ul>		
<b>Teilnahmevoraussetzungen</b>			

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

<b>Berücksichtigung von Gender- und Diversity-Aspekten</b>	<ul style="list-style-type: none"> <li>✓ Verwendung geschlechtergerechter Sprache (THL-Standard)</li> <li>✓ Zielgruppengerechte Anpassung der didaktischen Methoden</li> <li>✗ Sichtbarmachen von Vielfalt im Fach (Forscherinnen, Kulturen etc.)</li> </ul>
<b>Verwendbarkeit</b>	Studiengänge des Fachbereichs Elektrotechnik und Informatik
<b>Bemerkungen</b>	

## Lehrveranstaltung: Angewandte Kryptographie (Vorlesung)

(zu Modul: Angewandte Kryptographie)

<b>Lehrveranstaltungsart</b>	Vorlesung	<b>Lernform</b>	Präsenz
<b>LV-Name englisch</b>	Applied Cryptography (lecture)		
<b>Anwesenheitspflicht</b>	nein	<b>ECTS-Leistungspunkte</b>	3
<b>Teilnahmebeschränkung</b>		<b>Semesterwochenstunden</b>	3
<b>Gruppengröße</b>		<b>Arbeitsaufwand in Stunden</b>	90
<b>Lehrsprache</b>	Deutsch	<b>Präsenzstunden</b>	35
<b>Studienleistung</b>		<b>Selbststudiumsstunden</b>	55
<b>Dauer SL in Minuten</b>		<b>Bewertungssystem SL</b>	

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

<b>Prüfungsleistung</b>		<b>Prüfsprache</b>	
<b>Dauer PL in Minuten</b>		<b>Bewertungssystem PL</b>	
<b>Lernergebnisse</b>			
<b>Teilnahmevoraussetzungen</b>			

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

<b>Lehrinhalte</b>	<ul style="list-style-type: none"> <li>• Zahlentheorie, Kongruenzen, Restklassenringe</li> <li>• Historische und symmetrische Verschlüsselungsverfahren (Caesar, Vigenere, One-Time-Pad, Moderne Blockchiffren)</li> <li>• Sicherheitsmodelle (perfekte Geheimhaltung)</li> <li>• Secure Multiparty Computations</li> <li>• Hashfunktionen und Message Authentication Codes</li> <li>• Asymmetrische Verschlüsselungs- und Signaturverfahren (RSA, Diffe-Hellman, ElGamal)</li> <li>• Public-Key-Infrastrukturen</li> <li>• Kryptographische Protokolle und Anwendungen in der Praxis, insbesondere TLS 1.3</li> </ul>
<b>Literatur</b>	<p>Albrecht Beutelspacher, Jörg Schwenk und Klaus-Dieter Wolfenstetter. <i>Moderne Verfahren der Kryptographie</i>. Springer Spektrum, 2015.</p> <p>Johannes Buchmann. <i>Einführung in die Kryptographie</i>. Springer-Verlag Berlin Heidelberg, 2016.</p> <p>Christoph Paar und Jan Pelzl. <i>Kryptographie verständlich</i>. Springer-Verlag Berlin Heidelberg, 2016.</p>
<b>Bemerkungen</b>	

## Lehrveranstaltung: Kryptographie (Praktikum)

(zu Modul: Angewandte Kryptographie)

<b>Lehrveranstaltungsart</b>	Praktikum	<b>Lernform</b>	Präsenz
<b>LV-Name englisch</b>	Applied Cryptography (practical training)		
<b>Anwesenheitspflicht</b>	nein	<b>ECTS-Leistungspunkte</b>	2
<b>Teilnahmebeschränkung</b>		<b>Semesterwochenstunden</b>	1
<b>Gruppengröße</b>	12	<b>Arbeitsaufwand in Stunden</b>	60
<b>Lehrsprache</b>	Deutsch	<b>Präsenzstunden</b>	12
<b>Studienleistung</b>		<b>Selbststudiumsstunden</b>	48
<b>Dauer SL in Minuten</b>		<b>Bewertungssystem SL</b>	Drittelnoten

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

<b>Prüfungsleistung</b>		<b>Prüfsprache</b>	
<b>Dauer PL in Minuten</b>		<b>Bewertungssystem PL</b>	
<b>Lernergebnisse</b>			
<b>Teilnahmevoraussetzungen</b>			

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

<b>Lehrinhalte</b>	<ul style="list-style-type: none"> <li>Aufgaben und praktische Übungen zum Verständnis der Verschlüsselungsverfahren</li> </ul>
<b>Literatur</b>	
<b>Bemerkungen</b>	