

Modulcode (1.)	Modulbezeichnung (2.)	Zuordnung (3.)
BAI6520	Kryptographie (KRY)	
	Studiengang (4.)	Bachelor Angewandte Informatik
	Fakultät (5.)	Gebäudetechnik und Informatik

Modulverantwortlich (6.)	Dipl.-Math. Anja Haußen
Modulart (7.)	Wahl
Angebotshäufigkeit (8.)	SS
Regelbelegung / Empf. Semester (9.)	BA6
Credits (ECTS) (10.)	5 CP
Leistungsnachweis (11.)	PL (N)
Unterrichtssprache (12.)	Deutsch
Voraussetzungen für dieses Modul (13.)	
Modul ist Voraussetzung für (14.)	-
Moduldauer (15.)	1 Semester
Notwendige Anmeldung (16.)	-
Verwendbarkeit des Moduls (17.)	-

Lehrveranstaltung (18.)	Dozent/in (19.)	Art (20.)	Teilnehmer (maximal) (21.)	Anzahl Gruppen (22.)	SWS (23.)	Workload	
						Präsenz (24.)	Selbststudium (25.)
1 Kryptographie	Haußen	V	25	1	2	30	25
2 Kryptographie	Haußen	Ü	25	1	2	30	40
<b>Summe</b>					<b>4</b>	<b>60</b>	<b>65</b>
<b>Workload für das Modul (26.)</b>						<b>125</b>	

<b>Qualifikationsziele</b>	Die Studierenden... <ul style="list-style-type: none"> <li>• kennen die verschiedenen Ziele und Methoden der Kryptografie</li> <li>• kennen aktuelle Verfahren</li> <li>• können die Verfahren hinsichtlich ihrer Sicherheit und Einsatzmöglichkeiten beurteilen</li> </ul>
<b>Inhalte</b>	<ul style="list-style-type: none"> <li>• historische Chiffren</li> <li>• zahlentheoretische Grundlagen</li> <li>• symmetrische Algorithmen</li> <li>• asymmetrische Algorithmen</li> <li>• Digitale Signaturen</li> <li>• Protokolle</li> </ul>
<b>Vorleistungen und Modulprüfung</b>	Vorleistungen: <ul style="list-style-type: none"> <li>• keine</li> </ul> Modulprüfung: <ul style="list-style-type: none"> <li>• 100% Klausur über 90 min im Prüfungszeitraum</li> </ul>
<b>Literatur</b>	<ul style="list-style-type: none"> <li>• Schneier, Bruce: Angewandte Kryptographie. Protokolle, Algorithmen und Sourcecode in C." (1996).</li> <li>• Ertel, Wolfgang: Angewandte Kryptographie. Carl Hanser Verlag GmbH Co KG, 2012.</li> <li>• Beutelspacher, Albrecht, Heike B. Neumann, and Thomas Schwarzpaul: Kryptografie in Theorie und Praxis. Springer-Verlag, 2009.</li> </ul>