

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

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

Lehrveranstaltung <span>(18.)</span>	Dozent/in <span>(19.)</span>	Art <span>(20.)</span>	Teilnehmer (maximal) <span>(21.)</span>	Anzahl Gruppen <span>(22.)</span>	SWS <span>(23.)</span>	Workload	
						Präsenz <span>(24.)</span>	Selbst-studium <span>(25.)</span>
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>Workload für das Modul</b>						<b>(26.)</b>	<b>125</b>

<b>Qualifikationsziele</b>	<p>(27.)</p> <p>Die Studierenden...</p> <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>	<p>(28.)</p> <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>	<p>(29.)</p> <p>Vorleistungen:</p> <ul style="list-style-type: none"> <li>• keine</li> </ul> <p>Modulprüfung:</p> <ul style="list-style-type: none"> <li>• 100% Klausur über 90 min im Prüfungszeitraum</li> </ul>
<b>Literatur</b>	<p>(30.)</p> <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>