

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.)	Selbst- studium (25.)
1 Kryptographie	Haußen	V	25	1	2	30	25
2 Kryptographie	Haußen	Ü	25	1	2	30	40
Summe					4	60	65
Workload für das Modul (26.)						125	

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