Modulbezeichnung:	Advanced Cryptography
Studiensemester:	3rd
Modulverantwortlicher:	Professor Dr. Joachim von zur Gathen
Dozent(in):	Professor Dr. Joachim von zur Gathen, Dr. Michael Nüsken
Sprache:	English
Zuordnung zum Curriculum:	Media Informatics
Lehrform/SWS: *(und Gruppengrößen)*	V4Ü2 or V3Ü2
Arbeitsaufwand:	240h or 180h
Kreditpunkte:	8 or 6
Voraussetzungen nach Prüfungsordnung:	
Empfohlene Voraussetzungen:	Cryptography and one further course in cryptography like The Art of Cryptography or eSecurity
Angestrebte Lernergebnisse:	<u>Knowledge:</u> On successful completion of this module, students should have gained deeper understanding in a special area of cryptography close to current research. They should be able to • define the relevant terms, • recall the basic facts and • describe the major problems and solutions. The course may treat a theoretical or an applied topic. <u>Skills:</u> Course and tutorial include oral presentation (in tutorial groups), written presentation (of exercise solutions), team collaboration in solving homework problems, critical assessment. Thus on completion of this module, students should be able to • use the standard terms, • apply the appropriate techniques. • They should have acquired soft skills like the ability to communicate problems, techniques and results, creativity, reliability, team collaboration, time management. <u>Competences:</u> Based on the knowledge and skills acquired they should be able to • discuss up-to-date cryptographic applications or techniques, • identify and fix problems in cryptographical applications, • and to propose and examine new solutions for security.
Inhalt:	One varying, advanced topic related to current research in cryptography which may be practical or theoretical, e.g. - elliptic curve cryptography, or - design and analysis of hash functions.
Studien-/Prüfungsleistungen:	Written exam (oral exam in exceptional cases)
Medienformen:	None
Literatur:	Research articles