


Master

Module name eSecurity		 universität bonn			
Module No. t.b.a.	Workload 240h or 180h	Credit points 8 or 6		Frequency every year	
Module coordinator	Professor Dr. Joachim von zur Gathen				
Lecturer(s)	Professor Dr. Joachim von zur Gathen, Dr. Michael Nüsken				
Classification	Programme	Compulsory/optional		Semester	
	Media Informatics (M.Sc.), Computer Science (M.Sc.)	optional		2 nd	
Targeted learning outcomes	<p><u>Technical skills:</u> Understanding of security concerns and measures, and of the interplay between computing power, and security requirements in the realm of real-world applications, in particular internet-based ones. Mastery of advanced techniques for the design of cryptosystems and practical cryptanalysis.</p> <p><u>Soft skills:</u> Oral presentation (in tutorial groups), written presentation (of exercise solutions), team collaboration in solving homework problems, critical assessment.</p>				
Contents	<p>First focus: security on the internet and secure protocols. Furthermore: at least one real world application, for example</p> <ul style="list-style-type: none"> - electronic health cards, - electronic elections, or - electronic passports. 				
Prerequisites	Cryptography (Ma-INF 1103)				
Format/workload/credits	Teaching format	Group size		SWS	Workload [h]
	Lecture	60		4	60T / 90S
	Tutorials	30		2	30T / 60S
	For students who only want 6 credit points, on request a breakpoint at about $\frac{3}{4}$ of the teaching time will be defined, and only the course material up to that point will be relevant for their exams and grades.				
Exam achievements (graded)	Exam(s)				
	Written exam (oral exam in exceptional cases)				
Study achievements (not graded)	Successful tutorial participation				
Forms of media	None				
Literature	Varying according to the selected topic				