


Master

Module name Cryptography		 universität bonn			
Module No. Ma-INF 1103	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	1 st		
Targeted learning outcomes	<p><u>Technical skills:</u> Understanding of security concerns and measures, and of the interplay between computing power and security requirements. Mastery of the basic techniques for cryptosystems and 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	Basic private-key and public-key cryptosystems: AES, RSA, group-based. Security reductions. Key exchange, cryptographic hash functions, signatures, identification; Factoring integers and discrete logging; Lower bounds in structured models.				
Prerequisites	None				
Format/workload/credits	Teaching format	Group size	SWS	Workload [h]	Credits
	Lecture Tutorials	60 30	4 2	60T / 90S 30T / 60S	8
	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	Stinson, Cryptography: Theory and Practice, 2 nd edition				