


Master

<b>Module name</b> Advanced Cryptography		 universität <b>bonn</b>			
<b>Module No.</b> t.b.a.	<b>Workload</b> 240h or 180h	<b>Credit points</b> 8 or 6	<b>Frequency</b> every year		
<b>Module coordinator</b>	Professor Dr. Joachim von zur Gathen				
<b>Lecturer(s)</b>	Professor Dr. Joachim von zur Gathen, Dr. Michael Nüsken				
<b>Classification</b>	<b>Programme</b>	<b>Compulsory/optional</b>	<b>Semester</b>		
	Media Informatics (M.Sc.), Computer Science (M.Sc.)	optional	3 <sup>rd</sup>		
<b>Targeted learning outcomes</b>	<p><u>Technical skills:</u> Gain deeper understanding in a special area of cryptography close to current research. This may be a theoretical or applied topic.</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>				
<b>Contents</b>	<p>One varying, advanced topic related to current research in cryptography which may be practical or theoretical, e.g.</p> <ul style="list-style-type: none"> <li>- elliptic curve cryptography, or</li> <li>- design and analysis of hash functions.</li> </ul>				
<b>Prerequisites</b>	Required: Cryptography (Ma-INF 1103) and one further course in cryptography like The Art of Cryptography or eSecurity.				
<b>Format/workload/credits</b>	<b>Teaching format</b>	<b>Group size</b>	<b>SWS</b>	<b>Workload [h]</b>	<b>Credits</b>
	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.				
<b>Exam achievements (graded)</b>	<b>Exam(s)</b>				
	Written exam (oral exam in exceptional cases)				
<b>Study achievements (not graded)</b>	Successful tutorial participation				
<b>Forms of media</b>	none				
<b>Literature</b>	Research articles				