<table>
<tr><td>Module
MA-INF 1103</td><td colspan="5">Cryptography</td></tr>
<tr><td>Workload
270 h</td><td>Credit points
9 CP</td><td>Duration
1 semester</td><td colspan="3">Frequency
every year</td></tr>
<tr><td>Module coordinator</td><td colspan="5">Prof. Dr. Joachim von zur Gathen</td></tr>
<tr><td>Lecturer(s)</td><td colspan="5">Prof. Dr. Joachim von zur Gathen, Dr. Michael Nüsken</td></tr>
<tr><td>Classification</td><td colspan="2">Programme
M. Sc. Computer Science</td><td>Mode
Optional</td><td colspan="2">Semester
1. or 2.</td></tr>
<tr><td>Technical skills</td><td colspan="5">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</td></tr>
<tr><td>Soft skills</td><td colspan="5">Oral presentation (in tutorial groups), written presentation (of exercise solutions), team collaboration in solving homework problems, critical assessment</td></tr>
<tr><td>Contents</td><td colspan="5">Basic private-key and public-key cryptosystems: AES, RSA, group-based. Security reductions. Key exchange, cryptographic hash functions, signatures, identification; factoring integers and discrete logarithms; lower bounds in structured models.</td></tr>
<tr><td>Prerequisites</td><td colspan="5">none</td></tr>
<tr><td>Format</td><td colspan="5"><table><tr><th>Teaching format</th><th>Group size</th><th>h/week</th><th>Workload[h]</th><th>CP</th></tr><tr><td>Lecture</td><td>60</td><td>4</td><td>60 T / 105 S</td><td>5.5</td></tr><tr><td>Exercises</td><td>30</td><td>2</td><td>30 T / 75 S</td><td>3.5</td></tr></table>T = face-to-face teaching; S = independent study</td></tr>
<tr><td>Exam achievements</td><td colspan="5">Written exam (graded)</td></tr>
<tr><td>Study achievements</td><td colspan="5">Successful exercise participation (not graded)</td></tr>
<tr><td>Forms of media</td><td colspan="5"></td></tr>
<tr><td>Literature</td><td colspan="5">• Stinson, Cryptography: Theory and Practice, 2nd edition
• Course notes</td></tr>
</table>