## Module

**MA-INF 3311**  
**Topics in Applied Cryptography**

<table>
<thead>
<tr>
<th>Workload</th>
<th>Credit points</th>
<th>Duration</th>
<th>Frequency</th>
</tr>
</thead>
<tbody>
<tr>
<td>270 h</td>
<td>9 CP</td>
<td>1 semester</td>
<td>every year</td>
</tr>
</tbody>
</table>

**Module coordinator**  
Prof. Dr. Joachim von zur Gathen

**Lecturer(s)**  
Prof. Dr. Joachim von zur Gathen, Dr. Michael Nüsken

**Classification**  

<table>
<thead>
<tr>
<th>Programme</th>
<th>Mode</th>
<th>Semester</th>
</tr>
</thead>
<tbody>
<tr>
<td>M. Sc. Computer Science</td>
<td>Optional</td>
<td>3.</td>
</tr>
</tbody>
</table>

**Technical skills**  
Gain deeper understanding in a special area of cryptography close to current research.

**Soft skills**  
Oral presentation (in tutorial groups), written presentation (of exercise solutions), team collaboration in solving homework problems, critical assessment.

**Contents**  
One varying, advanced topic related to current research in applied cryptography, e.g.
- mobile security, or
- design and analysis of hash functions.

**Prerequisites**  
Required:
MA-INF 1103 – Cryptography
and one further course in cryptography like The Art of Cryptography or eSecurity.

**Format**  

<table>
<thead>
<tr>
<th>Teaching format</th>
<th>Group size</th>
<th>h/week</th>
<th>Workload[h]</th>
<th>CP</th>
</tr>
</thead>
<tbody>
<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>
</tbody>
</table>

T = face-to-face teaching; S = independent study

**Exam achievements**  
Written exam (graded)

**Study achievements**  
Successful exercise participation (not graded)

**Forms of media**

**Literature**