

Module:	<b>Concepts in Cryptography</b>
Lecturer:	Privatdoz. Dr. rer. nat. Peter Wagner
Language:	English
Teaching Method:	Lecture and practical exercise
Credit Points:	1 ECTS
Attendance requirements:	Basics in mathematics and computer science
Goals / Skill:	<p>This lecture gives an introduction in the most sophisticated cryptography schemes used in today's communication systems. Starting with cryptography concepts, the most sophisticated cryptography schemes used in today's communication systems and networks are introduced and analysed.</p> <p>The <b>focus</b> of the module is on understanding the concepts and mechanisms in cryptography.</p>
Detailed Content:	<ol style="list-style-type: none"> <li>1. Introduction</li> <li>2. Cryptography concepts</li> <li>3. Elliptic Curve Cryptography</li> <li>4. Cryptography in today's networks</li> <li>5. Applications</li> </ol>
Media Used:	Electronic Presentation, Blackboard Illustrations, Practical Demonstrations, Lab Exercises by the students.
Literature:	<ul style="list-style-type: none"> <li>• Mollin, R.A.: RSA and Public-Key Cryptography. Boca Raton, London, New York: CRC Press, 2003.</li> <li>• Paar, C.; Pelzl, J.: Understanding Cryptography: A Textbook for Students and Practitioners. Berlin, Heidelberg: Springer, 2009.</li> <li>• Delfs, H., Knebl, H.: Introduction to Cryptography. Principles and Applications. Berlin, Heidelberg: Springer, 2002.</li> </ul>
Assigned Tutorial:	<p>RSA</p> <ul style="list-style-type: none"> <li>• Getting familiar with RSA encryption and decryption for encrypting and decrypting texts, e-mails, files and directories</li> </ul>
Suggested Reading before the start of the summer school:	<ul style="list-style-type: none"> <li>• Paar, C.; Pelzl, J.: Understanding Cryptography: A Textbook for Students and Practitioners. Berlin, Heidelberg: Springer, 2009.</li> </ul>