Module:	**Concepts in Cryptography**
Lecturer:	Prof. Dr.-Ing. habil. Andreas Ahrens
Language:	English
Teaching Method:	Lecture and practical exercise
Credit Points:	1 ECTS
Attendance requirements:	Basics in mathematics and computer science
Goals / Skill:	This lecture gives an introduction in the most sophisticated cryptography schemes used in today's communication systems. Starting with basic cryptography concepts, the most sophisticated cryptography schemes used in today's communication systems and networks are introduced and analysed. The **focus** of the module is on understanding the basic concepts and mechanisms in cryptography.
Detailed Content:	1. Introduction 2. Basics of Applied Cryptography (Substitution and Transposition ciphers, One-Time-Pad, Feistel Networks, Stream- and Block-Ciphers, One-Way Functions) 3. Cryptography in today's networks 4. Applications
Media Used:	Electronic Presentation, Blackboard Illustrations, Practical Demonstrations, Lab Exercises by the students.
Literature:	Mollin, R.A.: RSA and Public-Key Cryptography. Boca Raton, London, New York: CRC Press, 2003. Paar, C.; Pelzl, J.: Understanding Cryptography: A Textbook for Students and Practitioners. Berlin, Heidelberg: Springer, 2009. Delfs, H., Knebl, H.: Introduction to Cryptography. Principles and Applications. Berlin, Heidelberg: Springer, 2002. Schneier, B.: Applied Cryptography: Protocols, Algorithms, and Source Code in C, New York: Wiley, 1996.
Assigned Tutorial:	RSA • Getting familiar with RSA encryption and decryption for encrypting and decrypting texts, e-mails, files and directories
Suggested Reading before the start of the summer school:	Paar, C.; Pelzl, J.: Understanding Cryptography: A Textbook for Students and Practitioners. Berlin, Heidelberg: Springer, 2009.