Tutorial 2:	**RSA & PGP**
Responsible Lecturers:	**Prof. Dr. rer. nat. habil. Andreas Ahrens** Prof. Dr. rer. nat. Clemens H. Cap Prof. Dr.-Ing. habil. Dennis Pfisterer
Language:	English
Teaching Method:	Practical exercise / Lab
Attendance requirements:	Students are invited to bring their own laptop and to preinstall PGP as well as PGP-enabled email systems, if possible.
Goals / Skill:	Getting familiar with RSA encryption and decryption as well as PGP for signing, encrypting and decrypting texts, e-mails, files and directories
Detailed Content:	RSA is one of the core encryption algorithms currently used. PGP provides an open source implementation and takes a different approach to key management than OpenSSL. In this tutorial the students will as well learn how to manage mail and file encryption using PGP. Particular attention will be on the security of the private key and on the trustworthyness of public keys received from other persons.
Media Used:	Practical Demonstrations, Lab Exercises by the students
Assigned Lectures:	• Concepts in Cryptography • Network Forensics • Network Security