Data field	Explanation
Module number	WP03
German title / English title	Network Sicherheit und Kryptografie / Network Security and Cryptography
Credits	5 ECTS
Workload	68 Contact hours (4 SWS Ü), 82 Hours of independent study
Subject coverage	Subject-specific specialization
Learning outcomes	Students understand the mathematical properties of secure algorithms and protocols. This includes modular arithmetic, finite-field arithmetic and properties of Euler's totient function. They are able to evaluate properties of current encryption methods and hash-functions. They know about network protection mechanisms such as firewalls, Virtual Private Networks and have practical experience in implementing security mechanisms in IP-networks. They can evaluate the security thread-level of networked environments and are able to assess and implement necessary protection measures.
Requirements	-
Level	1./2. Semester
Type of module	Seminar, Laboratory Training
Status	Required-elective module
Semesters when offered	Every semester
Method of assessment / Type of examination	The method of assessment / type of examination must be defined by the lecturer within the deadline determined in §19 (2) RSPO. Should the deadline pass without determination of the form of assessment in the module, the following method of assessment / type of examination applies: Written examination (120 minutes)
Grade assessment	See study and examination regulations
Content	• Properties of historical and modern crypto-systems • Mathematical foundations of cryptographic methods • Symmetric and asymmetric encryption algorithms • Approaches for the generation of random-numbers • Hash-functions and Message Authentication Codes (HMAC) • Digital Signatures • Cryptographic protocols for key-exchange and authentication • Denial of Service Attacks(DoS) and Distributed Denial of Service (DDoS) • Modelling and properties of security protocols (using TLS as an example) • Protecting Data and Privacy: authentication and access control • Firewalls: packet-filter und application-level-gateways • Virtual Private Networks based on Layer-3 encryption (IPsec) • Exemplary use of RSA, AES and Diffie-Hellman Key-Exchange • Introduction to firewalls (packet-filter) • Classroom discussion and presentations of scientific papers/methods relevant to the field
Reading list	W. Stallings: Cryptography and Network Security, Prentice Hall Bruce Schneier: Applied Cryptography, Pearson-Studium
Further information	Language employed in the module: English
Required Room type	Ü-Sem, Ü-Lab