Department	VII – Electronics – Mechatronics - Optometry / *Elektrotechnik - Mechatronik – Optometrie*
Degree level	Master's
Degree program	Information and Communications Engineering / *Information and Communications Engineering*
Type of instruction	Seminar plus laboratory training
Credits	5
Availability	Every semester
Hours/week	4

Module Number	WP03
English/German Title	**Network Security and Cryptography / *Network Sicherheit und Kryptografie***
Credit Points	5 credits
Workload	150 hours: • Class attendance 4 h/w during the semester lecture period: 68 hours • Independent study: 82 hours
Subject Coverage	Subject-specific specialization
Learning Objectives / 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 and 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.
Prerequisites	Recommendation: Principles of computer and data networks (e.g. IP technology)
Level	1st/2nd semester
Type of Module	Seminar, Laboratory Training
Status	Required-elective module
Semester when Offered	Every semester
Method of Assessment / Type(s) 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 100%.
Determination of the Grade	See study and examination regulations
Equivalent Modules	Modules with comparable contents
Contents	• 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 filters) • 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	This module is offered in English.