Title of course	**IT Security**
Responsible instructor	*Prof. Ralf C. Staudemeyer, Ph.D.*
Learning objectives	*In this course students will learn how to determine the level of security of a computer system or service, specify vulnerabilities, and to estimate the potential damage resulting from a successful attack. It covers the basic principles and key concepts for the operation of secure and (mostly) distributed systems, which includes partial components from operating systems and computer networks. The focus of this course is to deepen the understanding of network attacks and the cryptographic techniques to ensure integrity and confidentiality of information. Topics include various sub-components like cryptographic key management, biometrics, authentication in distributed systems, and basic security protocols and standards.*
Course contents	*The course starts with a general introduction into IT-Security, Cryptography and Privacy-Enhancing Technologies. The main focus of this course is on cryptographic algorithms and security protocols. Principally this module treats a selection of the following topics:* *• _Selected Attacks (attacks analysis, protection mechanisms)* *• _Cryptographic Algorithms (AES, RSA, ECC, MACs, signatures)* *• _Cryptographic Key Management (Diffie-Hellman key exchange, certificates, public-key infrastructure)* *• _Digital Identity (multi-factor authentication, challenge-response protocols, authentication in distributed systems)* *• _Mobile Security (mobile networks, Internet-of-Things, SmartCities)* *• _Network Security (security protocols, virtual private networks, secure Internet services)* *• _User-tools for IT-Security and Privacy in daily practise (email, web, chat, filesystems)* *This module is under constant development to reflect the most recent developments.*
Teaching methods	*Lecture (2 hours/week), Exercise (2 hours/week)*
Prerequisites	*Decent programming skills and basic knowledge in IT-security*
Suggested reading	*• Eckert, C. (2018). IT-Sicherheit. Berlin, München, Boston. De Gruyter.* *• Stallings, W. (2016). Cryptography and network security, principles and practices (7th edition). Prentice Hall.* *• Paar, C., & Pelzl, J. (2010). Understanding Cryptography. Berlin, Heidelberg: Springer Berlin Heidelberg.* *• Schneier, B. (1996), Applied Cryptography, John Wiley & Sons.* *• Hoglund, G, & McGraw , G. (2004). Exploiting Software, how to break code, Addison Wesley.* *• Selected sources announced in the lecture.*
Applicability	*Master of Applied Computer Science*
Workload	*Total 150 hours. Attendance: 60 hours, Self-Study incl. exam preparation: 90h*

ECTS credit points and weighting factor	*5 CP (Emphasis of the Grade for the final Grade 5/120)*
Basis of student evaluation	• *successfully completed exercises* • *oral exam or written exam (>14 participants)*
Time	*1st Semester*
Frequency	*annually (WS)*
Duration	One semester
Course type	*Obligatory course from the area IT-Security*
Remarks	Teaching language is English.