School of **Business**
Department of **Business Information Systems**

Theoretical Computer Science
(W3WI_SE301)

FORMAL INFORMATION ON THE MODULE

MODULE #	LOCATION IN THE COURSE OF STUDY	MODULE DURATION (SEMESTER)	SEMESTER	LANGUAGE
W3WI_SE301	2nd academic year	1	Fall Term	English

FORMS OF TEACHING USED

Lecture, exercise, laboratory exercise

FORMS OF EXAMINATION USED

EXAM PERFORMANCE	EXAM DURATION (IN MINUTES)	GRADING
Written or oral exam	120	yes

WORKLOAD AND ECTS CREDITS

TOTAL WORKLOAD (IN H)	OF WHICH ATTENDANCE TIME (IN H)	OF WHICH SELF-STUDY (IN H)	ECTS CREDIT POINTS
150	55	95	5

QUALIFICATION OBJECTIVES AND COMPETENCIES

PROFESSIONAL COMPETENCE

Students know basic concepts, terms and relationships from the sub-areas of formal languages, automata, computability and complexity. They have basic knowledge in the areas of IT security and cryptography, encryption techniques and network security.

METHODOLOGICAL COMPETENCE

Students can deal with formal languages, create and apply regular expressions, understand and program automata, determine and calculate the complexity of problems. They can also assess IT security scenarios and select and apply suitable protective measures.

PERSONAL AND SOCIAL COMPETENCE

Students recognize the strengths and limitations of the formalizations presented and can independently analyse and evaluate problems. They are familiar with the basic principles of IT security and are able to argue for the use of suitable security procedures against attacks.

LEARNING UNITS AND CONTENT

TEACHING AND LEARNING UNITS	PRESENCE TIME	SELF-STUDY
Introduction to theoretical computer science	28	47

Formal languages: language and grammar (regular, context-free, context-sensitive languages), regular expressions
Automata: finite automata, basement automata, automata and regular languages
Computability: computational models (e.g. Turing machines), computable and non-computable functions, primitive-recursive functions.
Complexity theory: complexity of problems, decision problems, NP-complete problems.

LEARNING UNITS AND CONTENT

TEACHING AND LEARNING UNITS	PRESENCE TIME	SELF-STUDY
IT security and cryptography	27	48

Basic concepts of IT security: protection goals, attackers and attacks, economic aspects

Network and software security, security models

Basic cryptographic procedures

Hash functions, digital signatures and certificates

Key management and key exchange

Authentication, digital identity, access control

SPECIAL FEATURES

-

PREREQUISITES

-

LITERATURE

- Eckert, C.: IT-Sicherheit: Konzepte -Verfahren -Protokolle, De Gruyter Oldenbourg, Munich.
- Hoffmann, D. W.: Theoretische Informatik, Hanser, Munich.
- Hromkovic, J.: Theoretische Informatik, Springer-Vieweg, Vienna.
- Kappes, M.: Netzwerk-und Datensicherheit, Springer, Vienna.
- Schöning, U.: Theoretische Informatik - kurzgefasst, Spektrum, Heidelberg.
- Schwenk, J.: Sicherheit und Kryptographie im Internet, Springer-Vieweg, Vienna.
- Stallings, W.: Network Security Essentials, Pearson, London.