Module Handbook

Master Program
Computer Science in IT-Security
60 ECTS

Master of Science (M.Sc.)
Distance Learning

Modulhandbuch_FS-FI_MACSIS_Computer Science in IT-Security 60_KSa_19.09.2019
This module handbook contains information about the topical issues and the organisation of the Master Program “Master Computer Science in IT-Security (60 ECTS)”. In particular, it contains

- **Administrative facts**
  - module-/course number
  - module-/course titles
  - duration of modules/courses
  - ECTS-credits
  - Module director

- **Academic approaches**
  - type of lecture
  - prerequisites, topical links to other modules
  - language of instruction
  - course objectives
  - course content, course literature, instructional methods

- **Student affairs**
  - course outcomes
  - workload structured by contact hours and individual studies

- **Examination issues**
  - number and type of assessments
  - requirements for participation in final assessments
  - modular weightings within the final master mark
Contents

Module DLMCSA Algorithmics ................................................................. 4
  Module Description ................................................................. 5
  Algorithmics ............................................................................. 7

Module DLMCSITSDP IT Security and Data Protection ......................... 10
  Module Description ................................................................. 11
  IT Security and Data Protection ................................................... 13

Module DLMCSSAITS Seminar: Advanced IT Security ......................... 16
  Module Description ................................................................. 17
  Seminar: Advanced IT Security .................................................. 19

Module DLMCSC Cryptology ................................................................. 21
  Module Description ................................................................. 22
  Cryptology ............................................................................... 24

Module DLMCSBC Blockchain ............................................................ 27
  Module Description ................................................................. 28
  Blockchain ............................................................................... 30

Module DLMCSSCSAS Seminar: Computer Science and Society ........... 33
  Module Description ................................................................. 34
  Seminar: Computer Science and Society .................................... 36

Module DLMCSQC Quantum Computing .............................................. 38
  Module Description ................................................................. 39
  Quantum Computing ............................................................... 41

Module DLMCSITPM IT Project Management ....................................... 44
  Module Description ................................................................. 45
  IT Project Management ............................................................ 47

Module DLMMTHE Master Thesis ....................................................... 50
  Module Description ................................................................. 51
  Master Thesis ........................................................................... 53
  Thesis Defense ........................................................................ 55
Module DLMCSA

Algorithmics

5 ECTS

Minimum duration of the module: 1 semester

Admission requirements: Advanced Mathematics (DLMDSAM01), Advanced Statistics (DLMDSAS01)
## Module Description

<table>
<thead>
<tr>
<th>Module Title:</th>
<th>Algorithmics</th>
</tr>
</thead>
<tbody>
<tr>
<td>Module No.:</td>
<td>DLMCSA</td>
</tr>
<tr>
<td>Semester / Term:</td>
<td>1&lt;sup&gt;st&lt;/sup&gt; semester</td>
</tr>
<tr>
<td>Duration:</td>
<td>Minimum 1 semester</td>
</tr>
<tr>
<td>Module Type(s):</td>
<td>Compulsory</td>
</tr>
<tr>
<td>Regularly Offered in:</td>
<td>WS / SS</td>
</tr>
<tr>
<td>Workload:</td>
<td>150 h</td>
</tr>
<tr>
<td>Credit Points:</td>
<td>5</td>
</tr>
</tbody>
</table>
| Admission Requirements: | Advanced Mathematics (DLMDSAM01)  
|                  | Advanced Statistics (DLMDSAS01) |
| Language of Instruction: | English |
| Contributing Courses to Module: | Algorithmics (DLBCSA01) |
| Workload:    | Self-study: 90 h  
|              | Self-examination: 30 h  
|              | Tutorials: 30 h |
| Course Coordinator(s) / Tutor(s): | Please see the current list of tutors on the Learning Management System. |
| Module Director: | Dr. Leonardo Riccardi |
| References to Other Degree Programs: | none |
| References to Other Modules in this Degree Program: | Cryptology  
|                  | Blockchain  
|                  | Quantum Computing |
### Qualification and Educational Objectives of the Module:

On successful completion of this module, students will be able to:

- explain the concept of algorithms and its relevance in computing.
- evaluate the correctness of software programs.
- discuss the theoretical and practical limits of software programs.
- select algorithms to solve specific application problems.
- design new algorithms based on standard methods to solve simple application problems.
- analyze and compare algorithms and outline their strengths and weaknesses.

### Learning Content of the Module:

- Algorithm design
- Introduction to important classes of algorithms
- Correctness and completeness of algorithms
- Computability and the theoretical limits of algorithms
- Efficiency of algorithms

### Teaching Methods:

See the contributing course outline

### Literature:

See the contributing course outline

### Percentage of the Module Grade Relative to the Final Grade for the Program:

5 ECTS of 60 ECTS = 8.33%

### Prerequisites to Qualify for Assessment:

See course outline

### Assessment:

- **DLMCSA01:**
  - Exam, 90 min. (100%)
Course No.: DLMCSA01
Course Title: Algorithmics

Hours Total: 150
Credit Points: 5

Course Type: Compulsory
Course Availability: In each semester
Course Duration: Minimum 1 semester

Course Coordinator / Instructor:
See current list of tutors in the Learning Management System.

Admission Requirements:
Please see module description.

References to Other Modules:
Please see module description.

Course Description:
A core activity of computer science and related disciplines is the design, use, and application of algorithms to solve problems. This course introduces common approaches to the design of algorithms, as well as important classes of algorithms that can be used to solve common problems.

Performing these tasks successfully requires a thorough understanding of the quality characteristics of algorithms: (partial and total) correctness, accuracy, completeness, and efficiency. At the same time, there are limits to what an algorithm can and should achieve, in theory and in practice, and it is important to realize these limits and take them into account.

Apart from algorithms based on standard programming paradigms, there are also various other programming paradigms that lead to other types of algorithms; therefore, this course also provides a short introduction to algorithms for parallel computing, probabilistic algorithms, and quantum algorithms.

Course Objectives and Outcome:
On successful completion of this course, students will be able to:

- explain the concept of algorithms and its relevance in computing.
- evaluate the correctness of software programs.
- discuss the theoretical and practical limits of software programs.
- select algorithms to solve specific application problems.
- design new algorithms based on standard methods to solve simple application problems.
- analyze and compare algorithms and outline their strengths and weaknesses.

Teaching Methods:
The learning materials include printed and online course books, vodcasts, online knowledge tests, podcasts, online tutorials, and case studies. This range of learning materials is offered to students so they can study at a time, place, and pace that best suits their circumstances and individual learning style.
Course Content:

1. Introduction to Algorithms
   1.1. Basic Concepts and Historical Overview
   1.2. Algorithms, Programming Languages and Data Structures
   1.3. Quality Algorithms: Correctness, Accuracy, Completeness, Efficiency
   1.4. The Role of Algorithms in Society

2. Algorithm Design
   2.1. Data Structures
   2.2. Recursion and Iteration
   2.3. Divide-and-Conquer
   2.4. Balancing, Greedy Algorithms, and Dynamic Programming

3. Some Important Algorithms
   3.1. Sorting and Searching
   3.2. Pattern-Matching
   3.3. The RSA Algorithm
   3.4. The k-Means Algorithm for Data Clustering

4. Correctness, Accuracy, and Completeness of Algorithms
   4.1. Partial Correctness
   4.2. Total Correctness
   4.3. Ensuring Correctness in Day-to-Day Programming
   4.4. Accuracy, Approximation, and Error Analysis

5. Computability
   5.1. Models of Computation
   5.2. The Halting Problem
   5.3. Undecidable Problems

6. Efficiency of Algorithms: Complexity Theory
   6.1. Models of Complexity
   6.2. NP-Completeness
   6.3. P=NP?

7. Advanced Algorithmics
   7.1. Parallel Computing
   7.2. Probabilistic Algorithms
   7.3. Quantum Computing and the Shor Algorithm

Literature:

A current list with course-specific compulsory reading, as well as references to further literature, is stored in the Learning Management System.
<table>
<thead>
<tr>
<th>Prerequisites to Qualify for Assessment:</th>
<th>Depending on the course: Completion of online knowledge tests (approx. 15 minutes per unit, pass / not pass)</th>
</tr>
</thead>
<tbody>
<tr>
<td>Assessment:</td>
<td>Exam, 90 min.</td>
</tr>
<tr>
<td>Student Workload (in hours): 150</td>
<td>Self-study: 90</td>
</tr>
<tr>
<td></td>
<td>Self-testing: 30</td>
</tr>
<tr>
<td></td>
<td>Tutorials: 30</td>
</tr>
</tbody>
</table>
Module DLMCSITSDP
IT Security and Data Protection
5 ECTS

Minimum duration of the module: 1 semester

Admission requirements: Advanced Mathematics (DLMDSAM01)
## Module Description

<table>
<thead>
<tr>
<th><strong>Module Title:</strong></th>
<th>IT Security and Data Protection</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Module No.:</strong></td>
<td>DLMCSITSDP</td>
</tr>
<tr>
<td><strong>Semester / Term:</strong></td>
<td>1&lt;sup&gt;st&lt;/sup&gt; semester</td>
</tr>
<tr>
<td><strong>Duration:</strong></td>
<td>Minimum 1 semester</td>
</tr>
<tr>
<td><strong>Module Type(s):</strong></td>
<td>Compulsory</td>
</tr>
<tr>
<td><strong>Regularly Offered in:</strong></td>
<td>WS / SS</td>
</tr>
<tr>
<td><strong>Workload:</strong></td>
<td>150 h</td>
</tr>
<tr>
<td><strong>Credit Points:</strong></td>
<td>5</td>
</tr>
<tr>
<td><strong>Admission Requirements:</strong></td>
<td>Advanced Mathematics (DLMDSAM01)</td>
</tr>
<tr>
<td><strong>Language of Instruction:</strong></td>
<td>English</td>
</tr>
<tr>
<td><strong>Contributing Courses to Module:</strong></td>
<td>IT Security and Data Protection (DLMCSITSDP01)</td>
</tr>
<tr>
<td><strong>Workload:</strong></td>
<td>Self-study: 110 h, Self-examination: 20 h, Tutorials: 20 h</td>
</tr>
<tr>
<td><strong>Course Coordinator(s) / Tutor(s):</strong></td>
<td>Please see the current list of tutors on the Learning Management System.</td>
</tr>
<tr>
<td><strong>Module Director:</strong></td>
<td>Prof. Dr. Ralf Kneuper</td>
</tr>
<tr>
<td><strong>References to Other Degree Programs:</strong></td>
<td>Master Data Science (120)</td>
</tr>
<tr>
<td><strong>References to Other Modules in this Degree Program:</strong></td>
<td>Seminar: Advanced IT Security, IT Project Management</td>
</tr>
</tbody>
</table>
Qualification and Educational Objectives of the Module:

On successful completion of this module, students will be able to:

- explain the core concepts of IT security, data protection, and cryptography including their differences and relationships.
- compare the approaches to data protection within in different legal systems.
- apply data protection concepts to data science and other application scenarios.
- analyze application scenarios to identify the adequate IT security management measures that should be implemented.
- scrutinize application scenarios to identify the appropriate cryptographic concepts to be applied.

Learning Content of the Module:

- Data protection and privacy
- IT security building blocks
- IT security management
- Cryptography concepts
- Cryptography applications

Teaching Methods: See the contributing course outline

Literature: See the contributing course outline

Percentage of the Module Grade Relative to the Final Grade for the Program:

5 ECTS of 60 ECTS = 8.33%

Prerequisites to Qualify for Assessment: See course outline

Assessment:

DLMCSITSDP01: Oral Assessment: Oral Assignment (100%)
<table>
<thead>
<tr>
<th>Course No.:</th>
<th>Course Title:</th>
<th>Hours Total: 150</th>
</tr>
</thead>
<tbody>
<tr>
<td>DLMCSITSDP01</td>
<td>IT Security and Data Protection</td>
<td>Credit Points: 5</td>
</tr>
</tbody>
</table>

**Course Type:** Compulsory  
**Course Availability:** In each semester  
**Course Duration:** Minimum 1 semester  

**Admission Requirements:**  
Please see module description.

**Course Coordinator / Instructor:**  
See current list of tutors in the Learning Management System.

**References to Other Modules:**  
Please see module description.

**Course Description:**

With the increasing digitization and networking of IT systems, the need for safeguarding systems and the data processed by these systems has grown. The aim of this module is to provide an understanding of security measures needed, IT security including cryptography, and data protection.  

While the need for IT security is similar around the world, different cultures have different expectations regarding data protection and privacy. Nevertheless, personal data are often processed outside the country where the affected individuals live. Hence, the cultural aspects of data protection need to be taken into account wherever the data are processed.  

This course provides an overview of the main IT security measures in different application scenarios, as well as their integration into an Information Security Management System, with particular focus on the relevant ISO/IEC 270xx family of standards.  

Cryptography provides an important tool set for IT security and is used in many different application scenarios such as secure Internet protocols and block chain.

**Course Objectives and Outcome:**

On successful completion of this course, students will be able to:  

- explain the core concepts of IT security, data protection, and cryptography including their differences and relationships.  
- compare the approaches to data protection within in different legal systems.  
- apply data protection concepts to data science and other application scenarios.  
- analyze application scenarios to identify the adequate IT security management measures that should be implemented.  
- scrutinize application scenarios to identify the appropriate cryptographic concepts to be applied.

**Teaching Methods:**

The learning materials include printed and online course books, vodcasts, online knowledge tests, podcasts, online tutorials, and case studies. This range of learning materials is offered to students so they can study at a time, place, and pace that best suits their circumstances and individual learning style.
Course Content:

1. Foundations of Data Protection and IT Security
   1.3 Terminology and Risk Management
   1.4 Core Concepts of IT Security
   1.5 Core Concepts of Data Protection and Privacy
   1.6 Core Concepts of Cryptography
   1.7 Legal Aspects

2. Data Protection
   2.3 Basic Concepts of Data Protection (ISO/IEC 29100, Privacy by Design)
   2.4 Data Protection in Europe: the GDPR
   2.5 Data Protection in the USA
   2.6 Data Protection in Asia

3. Applying Data Protection
   3.3 Anonymity and Pseudonyms (k-Anonymity, i-Diversity, Differential Privacy)
   3.4 Data Protection in Data Science and Big Data
   3.5 User Tracking in Online Marketing
   3.6 Cloud Computing

4. Building Blocks of IT Security
   4.3 Authentication, Access Management and Control
   4.4 IT Security in Networks
   4.5 Developing Secure IT Systems (OWASP, etc.)

5. IT Security Management
   5.3 Security Policy
   5.4 Security and Risk Analysis
   5.5 The ISO 270xx Series
   5.6 IT Security and IT Governance
   5.7 Example: IT Security for Credit Cards (PCI DSS)

6. Cryptography
   6.3 Symmetric Cryptography
   6.4 Asymmetric Cryptography
   6.5 Hash Functions
   6.6 Secure Data Exchange (Diffie-Hellman, Perfect Forward Secrecy, etc.)

7. Cryptographic Applications
   7.3 Digital Signatures
   7.4 Electronic Money
   7.5 Secure Internet Protocols (TLS, IPSec, etc.)
   7.6 Block Chain
A current list with course-specific compulsory reading, as well as references to further literature, is stored in the Learning Management System.

**Prerequisites to Qualify for Assessment:**
- Depending on the course: Completion of online knowledge tests (approx. 15 minutes per unit, pass / not pass)

**Assessment:**
- Oral Assessment: Oral Assignment

**Student Workload (in hours):**
- Self-study: 110
- Self-testing: 20
- Tutorials: 20
Module DLMCSSAITS
Seminar: Advanced IT Security

5 ECTS

Minimum duration of the module: 1 semester

Admission requirements: IT Security and Data Protection (DLMCSITSDP01)
Advanced Mathematics (DLMDSAM01)
## Module Description

<table>
<thead>
<tr>
<th>Module Title:</th>
<th>Seminar: Advanced IT Security</th>
</tr>
</thead>
<tbody>
<tr>
<td>Module No.:</td>
<td>DLMCSSAITS</td>
</tr>
<tr>
<td>Semester / Term:</td>
<td>1st semester</td>
</tr>
<tr>
<td>Duration:</td>
<td>Minimum 1 semester</td>
</tr>
<tr>
<td>Module Type(s):</td>
<td>Compulsory</td>
</tr>
<tr>
<td>Regularly Offered in:</td>
<td>WS / SS</td>
</tr>
<tr>
<td>Workload:</td>
<td>150 h</td>
</tr>
<tr>
<td>Credit Points:</td>
<td>5</td>
</tr>
<tr>
<td>Admission Requirements:</td>
<td></td>
</tr>
<tr>
<td></td>
<td>IT Security and Data Protection (DLMCSITSDP01)</td>
</tr>
<tr>
<td></td>
<td>Advanced Mathematics (DLMDSAM01)</td>
</tr>
<tr>
<td>Language of Instruction:</td>
<td></td>
</tr>
<tr>
<td></td>
<td>English</td>
</tr>
<tr>
<td>Contributing Courses to Module:</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Seminar: Advanced IT Security (DLMCAITSC01)</td>
</tr>
<tr>
<td>Workload:</td>
<td>Self-study: 120 h</td>
</tr>
<tr>
<td></td>
<td>Self-examination: -- h</td>
</tr>
<tr>
<td></td>
<td>Tutorials: 30 h</td>
</tr>
<tr>
<td>Course Coordinator(s) / Tutor(s):</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Please see the current list of tutors on the Learning Management System.</td>
</tr>
<tr>
<td>Module Director:</td>
<td>N.N. Professur für Cyber Security</td>
</tr>
<tr>
<td>References to Other Degree Programs:</td>
<td></td>
</tr>
<tr>
<td></td>
<td>none</td>
</tr>
<tr>
<td>References to Other Modules in this Degree Program:</td>
<td></td>
</tr>
<tr>
<td></td>
<td>IT Security and Data Protection</td>
</tr>
<tr>
<td></td>
<td>Algorithmics</td>
</tr>
</tbody>
</table>
Qualification and Educational Objectives of the Module:

On successful completion of this module, students will be able to:

- analyze and describe one aspect of IT security in detail.
- independently analyze selected topics in IT security and link them with well-known concepts, as well as critically question and discuss them.
- transfer theoretically-acquired knowledge to a specific context.
- write and edit a scientific essay on a relevant select topic.

Learning Content of the Module:

This course covers selected advanced topics in IT security, including the closely related topics of data protection and cryptology, and discusses them in detail. Based on a list of topics updated regularly, students select or are assigned a specific topic about which they write a scientific research essay.

A current list of topics is located in the Learning Management System.

Teaching Methods:

See the contributing course outline

Literature:

See the contributing course outline

<table>
<thead>
<tr>
<th>Percentage of the Module Grade Relative to the Final Grade for the Program:</th>
</tr>
</thead>
<tbody>
<tr>
<td>5 ECTS of 60 ECTS = 8.33%</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Prerequisites to Qualify for Assessment:</th>
</tr>
</thead>
<tbody>
<tr>
<td>See course outline</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Assessment:</th>
</tr>
</thead>
<tbody>
<tr>
<td>DLMCSEAITSC01:</td>
</tr>
<tr>
<td>Written Assessment:</td>
</tr>
<tr>
<td>Research Essay (100%)</td>
</tr>
<tr>
<td>Course No.:</td>
</tr>
<tr>
<td>----------------</td>
</tr>
<tr>
<td>Credit Points:</td>
</tr>
<tr>
<td>Course Type:</td>
</tr>
<tr>
<td>Course Availability:</td>
</tr>
<tr>
<td>Course Duration:</td>
</tr>
<tr>
<td>Admission Requirements:</td>
</tr>
</tbody>
</table>

**Course Coordinator / Instructor:**
See current list of tutors in the Learning Management System.

**References to Other Modules:**
Please see module description.

**Course Description:**
This seminar covers advanced topics in IT security. With the growth of the internet and digitization, IT security has become an increasingly important topic and needs to be taken into account in the development and setup of software and IT systems.

Typical topics that may be addressed include the analysis of selected aspects of information security management systems according to the ISO 27000 series; the use of IT security to support data protection; and the detailed analysis and description of certain algorithms or cryptosystems.

**Course Objectives and Outcome:**
On successful completion of this course, students will be able to:

- analyze and describe one aspect of IT security in detail.
- independently analyze selected topics in IT security and link them with well-known concepts, as well as critically question and discuss them.
- transfer theoretically-acquired knowledge to a specific context.
- write and edit a scientific essay on a relevant select topic.

**Teaching Methods:**
The learning materials include printed and online course books, vodcasts, online knowledge tests, podcasts, online tutorials, and case studies. This range of learning materials is offered to students so they can study at a time, place, and pace that best suits their circumstances and individual learning style.
Course Content:
The seminar covers different advanced topics regarding IT security. Each participant must prepare a research essay on a topic assigned to him/her.

Literature:

A current list with course-specific compulsory reading, as well as references to further literature, is stored in the Learning Management System.

<table>
<thead>
<tr>
<th>Prerequisites to Qualify for Assessment:</th>
<th>Depending on the course: Completion of online knowledge tests (approx. 15 minutes per unit, pass / not pass)</th>
</tr>
</thead>
<tbody>
<tr>
<td>Assessment:</td>
<td>Written Assessment: Research Essay</td>
</tr>
<tr>
<td>Student Workload (in hours): 150</td>
<td>Self-study: 120</td>
</tr>
<tr>
<td></td>
<td>Self-testing: --</td>
</tr>
<tr>
<td></td>
<td>Tutorials: 30</td>
</tr>
</tbody>
</table>
Module DLMCSC

Cryptology

5 ECTS

Minimum duration of the module: 1 semester

Admission requirements: Seminar: Advanced IT Security (DLMCSEAITSC01), IT Security and Data Protection (DLMCSITSDP01), Advanced Mathematics (DLMDSAM01)
## Module Description

<table>
<thead>
<tr>
<th>Module Title:</th>
<th>Cryptology</th>
</tr>
</thead>
<tbody>
<tr>
<td>Module No.:</td>
<td>DLMCSC</td>
</tr>
<tr>
<td>Semester / Term:</td>
<td>1st semester</td>
</tr>
<tr>
<td>Duration:</td>
<td>Minimum 1 semester</td>
</tr>
<tr>
<td>Module Type(s):</td>
<td>Compulsory</td>
</tr>
<tr>
<td>Regularly Offered in:</td>
<td>WS / SS</td>
</tr>
<tr>
<td>Workload:</td>
<td>150 h</td>
</tr>
<tr>
<td>Credit Points:</td>
<td>5</td>
</tr>
<tr>
<td>Admission Requirements:</td>
<td>Seminar: Advanced IT Security (DLMCSEAITSC01) IT Security and Data Protection (DLMCSITSDP01) Advanced Mathematics (DLMDSAM01)</td>
</tr>
<tr>
<td>Language of Instruction:</td>
<td>English</td>
</tr>
</tbody>
</table>

### Contributing Courses to Module:

- Cryptology (DLMCSEAITSC02)

### Course Coordinator(s) / Tutor(s):

Please see the current list of tutors on the Learning Management System.

### Module Director:

N.N. Online Dozent für Cryptology

### References to Other Degree Programs:

- none

### References to Other Modules in this Degree Program:

- IT Security and Data Protection
- Algorithmics
Qualification and Educational Objectives of the Module:

On successful completion of this module, students will be able to:

- discuss the main cryptographic systems and algorithms and their relevance in IT today.
- discuss the security of Internet-based applications.
- evaluate different cryptographic systems and algorithms to select an appropriate solution for real-world problems in IT.
- apply standard cryptographic systems and algorithms to solve real-world problems in IT.
- appraise existing cryptographic solutions to real-world problems and identify major weaknesses where relevant.

Learning Content of the Module:

- Symmetric and asymmetric cryptosystems
- Authentication
- Cryptanalysis
- Cryptology in the internet
- Applications

Teaching Methods: See the contributing course outline

Literature: See the contributing course outline

Percentage of the Module Grade Relative to the Final Grade for the Program:

5 ECTS of 60 ECTS = 8.33%

Prerequisites to Qualify for Assessment: See course outline

Assessment:

DLMCSEAITSC02:
Oral Assessment: Oral Assignment (100%)
Course No.: DLMCSEAITSC02  
Course Title: Cryptology  
Hours Total: 150  
Credit Points: 5

<table>
<thead>
<tr>
<th>Course Type:</th>
<th>Compulsory</th>
</tr>
</thead>
<tbody>
<tr>
<td>Course Availability:</td>
<td>In each semester</td>
</tr>
<tr>
<td>Course Duration:</td>
<td>Minimum 1 semester</td>
</tr>
</tbody>
</table>

Admission Requirements:  
Please see module description.

References to Other Modules:  
Please see module description.

Course Description:  
The focus of this course is to provide a thorough introduction to cryptology and its main sub-disciplines cryptography and cryptanalysis. Particular emphasis is put on the use of cryptology to support the security of IT systems.

In the first part of the courses, students gain a solid understanding of the basic concepts of cryptology, in particular symmetric and asymmetric cryptosystems, authentication, and common approaches to break these cryptosystems using cryptanalysis.

Based on this foundational understanding, the course goes on to cover the practical use of cryptology, starting with an introduction to the standard protocols and techniques used to ensure the security of communication via the internet. Next, practical aspects of applying cryptographic techniques and algorithms are covered, such as their long-term security. Finally, some application examples show how the concepts of cryptology are commonly used and can be used to solve challenges such as online banking.

Course Objectives and Outcome:  
On successful completion of this course, students will be able to:

- discuss the main cryptographic systems and algorithms and their relevance in IT today.
- discuss the security of internet-based applications.
- evaluate different cryptographic systems and algorithms to select an appropriate solution for real-world problems in IT.
- apply standard cryptographic systems and algorithms to solve real-world problems in IT.
- appraise existing cryptographic solutions to real-world problems and identify major weaknesses where relevant.

Teaching Methods:  
The learning materials include printed and online course books, vodcasts, online knowledge tests, podcasts, online tutorials, and case studies. This range of learning materials is offered to students so they can study at a time, place, and pace that best suits their circumstances and individual learning style.
Course Content:

1. Basic concepts of cryptology
   1.1. Introduction and terminology
   1.2. IT security, threats and common attacks
   1.3. Historical overview
   1.4. Kerckhoffs’s principle

2. Symmetric cryptosystems
   2.1. Substitution and transposition
   2.2. Stream and block ciphers
   2.3. Digital encryption standard (DES)
   2.4. Advanced encryption standard (AES)

3. Asymmetric cryptosystems
   3.1. The RSA algorithm
   3.2. Elliptic curves
   3.3. Cryptographic hash functions
   3.4. Signatures and MACs
   3.5. Key exchange and public key infrastructures

4. Authentication
   4.1. Passwords
   4.2. Challenge-response and zero-knowledge
   4.3. Biometrics-based authentication
   4.4. Authentication in distributed systems
   4.5. Smartcards
   4.6. Identity and anonymity

5. Cryptanalysis – how to break encryption
   5.1. Frequency analysis
   5.2. Brute-force attacks
   5.3. Rainbow tables
   5.4. Known/chosen plaintext
   5.5. Side-channel attacks

6. Cryptology and the internet
   6.1. Basic setup of the Internet and its protocols
   6.2. IPSec
   6.3. Transport Layer Security
   6.4. Secure E-Mail (TLS, S/MIME and PGP)
   6.5. Secure DNS

7. Practical aspects of cryptology
   7.1. Random number generation
   7.2. Long-term security (key lengths, perfect forward security, quantum computing)
   7.3. Incorporating cryptography into application development
   7.4. Legal and regulatory aspects

8. Applications
   8.1. Online banking
   8.2. Blockchain
   8.3. Voting
   8.4. Steganography and watermarks
   8.5. The Tor Project
Literature:


A current list with course-specific compulsory reading, as well as references to further literature, is stored in the Learning Management System.

**Prerequisites to Qualify for Assessment:**
- Depending on the course: Completion of online knowledge tests (approx. 15 minutes per unit, pass / not pass)

**Assessment:**
- Oral Assessment: Oral Assignment

**Student Workload (in hours):** 150
- Self-study: 110
- Self-testing: 20
- Tutorials: 20
Module DLMCSBC
Blockchain
5 ECTS

Minimum duration of the module:  1 semester

Admission requirements:   None
## Module Description

<table>
<thead>
<tr>
<th>Module Title:</th>
<th>Blockchain</th>
</tr>
</thead>
<tbody>
<tr>
<td>Module No.:</td>
<td>DLMCSBC</td>
</tr>
<tr>
<td>Semester / Term:</td>
<td>1&lt;sup&gt;st&lt;/sup&gt; semester</td>
</tr>
<tr>
<td>Duration:</td>
<td>Minimum 1 semester</td>
</tr>
<tr>
<td>Module Type(s):</td>
<td>Compulsory</td>
</tr>
<tr>
<td>Regularly Offered in:</td>
<td>WS / SS</td>
</tr>
<tr>
<td>Workload:</td>
<td>150 h</td>
</tr>
<tr>
<td>Credit Points:</td>
<td>5</td>
</tr>
<tr>
<td>Admission Requirements:</td>
<td>None</td>
</tr>
<tr>
<td>Language of Instruction:</td>
<td>English</td>
</tr>
<tr>
<td>Contributing Courses to Module:</td>
<td>Blockchain (DLMCSEBCQC01)</td>
</tr>
<tr>
<td>Workload:</td>
<td>Self-study: 110 h</td>
</tr>
<tr>
<td></td>
<td>Self-examination: 20 h</td>
</tr>
<tr>
<td></td>
<td>Tutorials: 20 h</td>
</tr>
<tr>
<td>Course Coordinator(s) / Tutor(s):</td>
<td>Please see the current list of tutors on the Learning Management System.</td>
</tr>
<tr>
<td>Module Director:</td>
<td>N.N. Professur für Cyber Security</td>
</tr>
<tr>
<td>References to Other Degree Programs:</td>
<td>none</td>
</tr>
<tr>
<td>References to Other Modules in this Degree Program:</td>
<td>IT Security and Data Protection</td>
</tr>
<tr>
<td></td>
<td>Algorithmics</td>
</tr>
</tbody>
</table>
Qualification and Educational Objectives of the Module:

On successful completion of this module, students will be able to:

- outline the functions provided by and the technology used in blockchains.
- explain important applications of blockchains, in particular BitCoin.
- demonstrate the technical architecture of blockchain applications.
- appraise the benefits and challenges of suggested blockchain applications.
- discuss the social and legal aspects of blockchain technology.

Learning Content of the Module:

- Basic concepts of blockchain and related technologies
- Applications of blockchain and DLT
- Security
- Development of blockchain and DLT applications
- Social and legal aspects

Teaching Methods: See the contributing course outline

Literature: See the contributing course outline

Percentage of the Module Grade Relative to the Final Grade for the Program:

5 ECTS of 60 ECTS = 8.33%

Prerequisites to Qualify for Assessment: See course outline

Assessment:

DLMCSEBCQC01:
Written Assessment: Written Assignment (100%)
Course No.: DLMCSEBCQC01
Course Title: Blockchain

Hours Total: 150
Credit Points: 5

Course Type: Compulsory
Course Availability: In each semester
Course Duration: Minimum 1 semester

Admission Requirements:
None

Course Coordinator / Instructor:
See current list of tutors in the Learning Management System.

References to Other Modules:
Please see module description.

Course Description:
Started by the cryptocurrency BitCoin, blockchain and related topics such as distributed ledger technologies and smart contracts have become increasingly important over the last few years and are claimed to be a major disruptive technologies. As BitCoin shows, systems that today need a trustworthy central coordinating body may become genuinely distributed systems without the need for such a body in the future.

While blockchain has the potential for completely new types of applications, these suggested applications do not always make use of the strengths of the technology; rather, they simply provide a different approach to solving problems that could be solved more easily and efficiently using standard technologies such as database systems. Furthermore, blockchain applications have led to new social challenges and legal questions, such as the legal status of “smart contracts”.

Different infrastructures such as Ethereum and Hyperledger have been developed to form the basis for blockchain applications.

The goal of this course is to provide an understanding of the technical, as well as social and legal, aspects of blockchain and related technologies.

Course Objectives and Outcome:
On successful completion of this course, students will be able to:
- outline the functions provided by and the technology used in blockchains.
- explain important applications of block chains, in particular BitCoin.
- demonstrate the technical architecture of blockchain applications.
- appraise the benefits and challenges of suggested blockchain applications.
- discuss the social and legal aspects of blockchain technology.

Teaching Methods:
The learning materials include printed and online course books, vodcasts, online knowledge tests, podcasts, online tutorials, and case studies. This range of learning materials is offered to students so they can study at a time, place, and pace that best suits their circumstances and individual learning style.
Course Content:

1. Basic Concepts
   1.1. The Functional View: Distributed Ledger Technologies
   1.2. The Technical View: Blockchain
   1.3. History of Blockchain and DLT
   1.4. Consense Mechanisms

2. BitCoin
   2.1. The BitCoin Payment System
   2.2. The Technology Behind BitCoin
   2.3. Security of BitCoin
   2.4. Scalability and Other Limitations of BitCoin
   2.5. BitCoin Derivatives and Alternatives

3. Smart Contracts and Decentralized Apps
   3.1. Smart Contracts
   3.2. Decentralized Apps (DApps)
   3.3. Ethereum
   3.4. Hyperledger
   3.5. Alternative Platforms for Smart Contracts and DApps

4. Security of Block Chain and DLT
   4.1. Cryptology Used
   4.2. Attacks on Blockchain and DLT
   4.3. Resolving Bugs and Security Holes
   4.4. Long-Term Security

5. Block Chain and DLT Application Scenarios
   5.1. Benefits and Limits of Applying Blockchain and DLT
   5.2. Registers for Land and Other Property
   5.3. Applications in the Supply Chain
   5.4. Applications in Insurance
   5.5. Initial Coin Offerings for Sourcing Capital
   5.6. Examples of Further Applications

6. Development of Blockchain and DLT Applications
   6.1. Architecture of Blockchain and DLT Applications
   6.2. Platform Selection
   6.3. Design of Blockchain and DLT Applications

7. Blockchain and Society
   7.1. (Mis-)Trust in Institutions
   7.2. Blockchain and the Environment
   7.3. Cyber-Currencies in the Darknet
   7.4. ICO Fraud

8. Legal Aspects
   8.1. DLT and Smart Contracts as Legal Contracts
   8.2. Cryptocurrencies as Legal Currencies
   8.3. Regulation of ICOs
   8.4. Data Protection / Privacy in Blockchains
Literature:


A current list with course-specific compulsory reading, as well as references to further literature, is stored in the Learning Management System.

Prerequisites to Qualify for Assessment:

- Depending on the course: Completion of online knowledge tests (approx. 15 minutes per unit, pass / not pass)

Assessment:

- Written Assessment: Written Assignment

Student Workload (in hours): 150

- Self-study: 110
- Self-testing: 20
- Tutorials: 20
Module DLMCSSCSAS
Seminar: Computer Science and Society

5 ECTS

Minimum duration of the module: 1 semester

Admission requirements: None
## Module Description

<table>
<thead>
<tr>
<th>Module Title:</th>
<th>Seminar: Computer Science and Society</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Module No.:</strong></td>
<td>DLMCSCSSCSAS</td>
</tr>
<tr>
<td><strong>Semester / Term:</strong></td>
<td>1&lt;sup&gt;st&lt;/sup&gt; semester</td>
</tr>
<tr>
<td><strong>Duration:</strong></td>
<td>Minimum 1 semester</td>
</tr>
<tr>
<td><strong>Module Type(s):</strong></td>
<td>Compulsory</td>
</tr>
<tr>
<td><strong>Regularly Offered in:</strong></td>
<td>WS / SS</td>
</tr>
<tr>
<td><strong>Workload:</strong></td>
<td>150 h</td>
</tr>
<tr>
<td><strong>Credit Points:</strong></td>
<td>5</td>
</tr>
<tr>
<td><strong>Admission Requirements:</strong></td>
<td>None</td>
</tr>
<tr>
<td><strong>Language of Instruction:</strong></td>
<td>English</td>
</tr>
<tr>
<td><strong>Contributing Courses to Module:</strong></td>
<td>Seminar: Computer Science and Society (DLMCSCSSCSAS01)</td>
</tr>
<tr>
<td><strong>Workload:</strong></td>
<td>Self-study: 120 h</td>
</tr>
<tr>
<td></td>
<td>Self-examination: -- h</td>
</tr>
<tr>
<td></td>
<td>Tutorials: 30 h</td>
</tr>
<tr>
<td><strong>Course Coordinator(s) / Tutor(s):</strong></td>
<td>Please see the current list of tutors on the Learning Management System.</td>
</tr>
<tr>
<td><strong>Module Director:</strong></td>
<td>Prof. Dr. Carsten Clauß</td>
</tr>
<tr>
<td><strong>References to Other Degree Programs:</strong></td>
<td>none</td>
</tr>
<tr>
<td><strong>References to Other Modules in this Degree Program:</strong></td>
<td>IT Security and Data Protection</td>
</tr>
</tbody>
</table>
### Qualification and Educational Objectives of the Module:

On successful completion of this module, students will be able to:

- name the main questions regarding the relationship between computer science and society.
- discuss selected topics regarding the relationship between computer science and society.
- analyze one aspect of the relationship between computer science and society in detail.
- take selected topics and case studies and link them with well-known concepts, as well as critically question and discuss them.
- transfer theoretically acquired knowledge to a specific context.
- edit scientifically a select topic.

### Learning Content of the Module:

The seminar covers the relationship between computer science and society, including topics such as the social responsibility of computer scientists and the effects of digitization on society. Based on a list of topics updated regularly, students select or are assigned a specific topic on which to write a scientific report.

A current list of topics is located in the Learning Management System.

### Teaching Methods:

See the contributing course outline

### Literature:

See the contributing course outline

### Percentage of the Module Grade Relative to the Final Grade for the Program:

5 ECTS of 60 ECTS = 8.33%

### Prerequisites to Qualify for Assessment:

See course outline

### Assessment:

**DLMCSSCSAS01:**
- Written Assessment:
  - Research Essay (100%)
Course No.: DLMCSSCSAS01
Course Title: Seminar: Computer Science and Society
Hours Total: 150
Credit Points: 5

Course Type: Compulsory
Course Availability: In each semester
Course Duration: Minimum 1 semester

Course Coordinator / Instructor:
See current list of tutors in the Learning Management System.

Admission Requirements:
None

References to Other Modules:
Please see module description.

Course Description:
The seminar covers the relationship between computer science and society. Over the past several decades, computer science has greatly changed society, and it is important that prospective computer scientists think about the effects of computer science on society and take these influences into account in their work.

Typical topics to be addressed include, for example, the effects of ethics and professionalism in computing, the responsibility of computer scientists, the effects of data science and social networks on society, surveillance, and dual use of IT.

Course Objectives and Outcome:
On successful completion of this course, students will be able to:

- name the main questions regarding the relationship between computer science and society.
- discuss selected topics regarding the relationship between computer science and society.
- analyze one aspect of the relationship between computer science and society in detail.
- take selected topics and case studies and link them with well-known concepts, as well as critically question and discuss them.
- transfer theoretically acquired knowledge to a specific context.
- edit scientifically a select topic.

Teaching Methods:
The learning materials include printed and online course books, vodcasts, online knowledge tests, podcasts, online tutorials, and case studies. This range of learning materials is offered to students so they can study at a time, place, and pace that best suits their circumstances and individual learning style.
**Course Content:**
The seminar covers different topics regarding the relationship between computer science and society. Each participant must create a seminar paper on a topic assigned to him/her and present the contents of the written paper.

**Literature:**

A current list with course-specific compulsory reading, as well as references to further literature, is stored in the Learning Management System.

**Prerequisites to Qualify for Assessment:**
- Depending on the course: Completion of online knowledge tests (approx. 15 minutes per unit, pass / not pass)

**Assessment:**
- Written Assessment: Research Essay

**Student Workload (in hours):** 150
- Self-study: 120
- Self-testing: --
- Tutorials: 30
Module DLMCSQC

Quantum Computing

5 ECTS

Minimum duration of the module:  1 semester

Admission requirements:  None
### Module Description

<p>| | |</p>
<table>
<thead>
<tr>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Module Title:</strong></td>
<td>Quantum Computing</td>
</tr>
<tr>
<td><strong>Module No.:</strong></td>
<td>DLMCSQC</td>
</tr>
<tr>
<td><strong>Semester / Term:</strong></td>
<td>2(^{nd}) semester</td>
</tr>
<tr>
<td><strong>Duration:</strong></td>
<td>Minimum 1 semester</td>
</tr>
<tr>
<td><strong>Module Type(s):</strong></td>
<td>Compulsory</td>
</tr>
<tr>
<td><strong>Regularly Offered in:</strong></td>
<td>WS / SS</td>
</tr>
<tr>
<td><strong>Workload:</strong></td>
<td>150 h</td>
</tr>
<tr>
<td><strong>Credit Points:</strong></td>
<td>5</td>
</tr>
<tr>
<td><strong>Admission Requirements:</strong></td>
<td>None</td>
</tr>
<tr>
<td><strong>Language of Instruction:</strong></td>
<td>English</td>
</tr>
<tr>
<td><strong>Contributing Courses to Module:</strong></td>
<td>Quantum Computing (DLMCSEBCQC02)</td>
</tr>
<tr>
<td><strong>Workload:</strong></td>
<td></td>
</tr>
<tr>
<td></td>
<td>Self-study: 110 h</td>
</tr>
<tr>
<td></td>
<td>Self-examination: 20 h</td>
</tr>
<tr>
<td></td>
<td>Tutorials: 20 h</td>
</tr>
<tr>
<td><strong>Course Coordinator(s) / Tutor(s):</strong></td>
<td>Please see the current list of tutors on the Learning Management System.</td>
</tr>
<tr>
<td><strong>Module Director:</strong></td>
<td>N.N. Online Dozent für Quantum Computer</td>
</tr>
<tr>
<td><strong>References to Other Degree Programs:</strong></td>
<td>none</td>
</tr>
<tr>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>IT Security and Data Protection</td>
</tr>
<tr>
<td></td>
<td>Algorithmics</td>
</tr>
</tbody>
</table>
### Qualification and Educational Objectives of the Module:

On successful completion of this module, students will be able to:

- outline the basic concepts of quantum mechanics as they relate to quantum computing.
- describe the computation models used in quantum computing.
- demonstrate the role of quantum computing for cryptography and other application areas.
- compare the theoretical and practical potential of quantum computing to classical computing.
- apply the concepts of quantum computing to develop simple programs within the Qiskit framework.

### Learning Content of the Module:

- Physics of quantum computing
- Quantum computing models
- Quantum algorithms
- Quantum computing with the IBM framework Qiskit
- Applications, potential for and challenges of quantum computing

### Teaching Methods:

See the contributing course outline

### Literature:

See the contributing course outline

<table>
<thead>
<tr>
<th>Percentage of the Module Grade Relative to the Final Grade for the Program:</th>
<th>Prerequisites to Qualify for Assessment:</th>
<th>Assessment:</th>
</tr>
</thead>
<tbody>
<tr>
<td>5 ECTS of 60 ECTS = 8.33%</td>
<td>See course outline</td>
<td>DLMCSEBCQC02: Oral Assessment: Oral Assignment (100%)</td>
</tr>
<tr>
<td><strong>Course No.:</strong></td>
<td>DLMCSEBCQC02</td>
<td></td>
</tr>
<tr>
<td>-----------------</td>
<td>--------------</td>
<td></td>
</tr>
<tr>
<td><strong>Course Title:</strong></td>
<td>Quantum Computing</td>
<td></td>
</tr>
<tr>
<td><strong>Hours Total:</strong></td>
<td>150</td>
<td></td>
</tr>
<tr>
<td><strong>Credit Points:</strong></td>
<td>5</td>
<td></td>
</tr>
<tr>
<td><strong>Course Type:</strong></td>
<td>Compulsory</td>
<td></td>
</tr>
<tr>
<td><strong>Course Availability:</strong></td>
<td>In each semester</td>
<td></td>
</tr>
<tr>
<td><strong>Course Duration:</strong></td>
<td>Minimum 1 semester</td>
<td></td>
</tr>
<tr>
<td><strong>Admission Requirements:</strong></td>
<td>None</td>
<td></td>
</tr>
<tr>
<td><strong>Course Coordinator / Instructor:</strong></td>
<td>See current list of tutors in the Learning Management System.</td>
<td></td>
</tr>
<tr>
<td><strong>References to Other Modules:</strong></td>
<td>Please see module description.</td>
<td></td>
</tr>
</tbody>
</table>

**Course Description:**
Quantum computing is a completely new paradigm for the architecture of computers. It currently is in the early stage of development but has the potential to speed up certain kinds of computations, not just by orders of magnitude but by moving them from exponential to linear growth. One of the issues that will be affected is the prime factorization of large numbers which currently forms the basis for important cryptographic algorithms, in particular the RSA algorithm which would in that case would no longer be secure.

This course gives an introduction to the physics behind quantum computing and the computation models used. Students are familiarized with the most important algorithms for quantum computing and write a few programs for quantum computers. The application potential and challenges of quantum computing are also discussed.

**Course Objectives and Outcome:**
On successful completion of this course, students will be able to:
- outline the basic concepts of quantum mechanics as they relate to quantum computing.
- describe the computation models used in quantum computing.
- demonstrate the role of quantum computing for cryptography and other application areas.
- compare the theoretical and practical potential of quantum computing to classical computing.
- apply the concepts of quantum computing to develop simple programs within the Qiskit framework.

**Teaching Methods:**
The learning materials include printed and online course books, vodcasts, online knowledge tests, podcasts, online tutorials, and case studies. This range of learning materials is offered to students so they can study at a time, place, and pace that best suits their circumstances and individual learning style.
Course Content:

1. Basic concepts
   1.1. Quantum physics as a basis for computing
   1.2. Types of quantum computers
   1.3. Qbits
   1.4. Linear algebra

2. The physics of quantum computers
   2.1. Basic concepts of quantum mechanics
   2.2. Spin and entanglement
   2.3. Architecture of quantum computers
   2.4. Noise and error correction
   2.5. Current state and outlook

3. Quantum computing models
   3.1. Quantum gates and circuits
   3.2. Single qubit quantum systems
   3.3. Multiple qubit quantum systems

4. Quantum algorithms
   4.1. Computability and complexity in quantum computing
   4.2. Quantum Fourier transform
   4.3. The Shor algorithm
   4.4. The Grover algorithm

5. Quantum computing with the IBM framework Qiskit
   5.1. Overview of Qiskit and the IBM Q Provider
   5.2. Quantum circuits in Qiskit
   5.3. First steps in programming with Qiskit

6. Applications, potential and challenges of quantum computing
   6.1. Applications of quantum computing
   6.2. Quantum cryptography and post-quantum cryptography
   6.3. Quantum supremacy
## Literature:


A current list with course-specific compulsory reading, as well as references to further literature, is stored in the Learning Management System.

### Prerequisites to Qualify for Assessment:

- Depending on the course: Completion of online knowledge tests (approx. 15 minutes per unit, pass / not pass)

### Assessment:

- Oral Assessment: Oral Assignment

### Student Workload (in hours):

<table>
<thead>
<tr>
<th>Task</th>
<th>Hours</th>
</tr>
</thead>
<tbody>
<tr>
<td>Self-study</td>
<td>110</td>
</tr>
<tr>
<td>Self-testing</td>
<td>20</td>
</tr>
<tr>
<td>Tutorials</td>
<td>20</td>
</tr>
</tbody>
</table>

Total: 150 hours
Module DLMCSITPM
IT Project Management
5 ECTS

Minimum duration of the module: 1 semester

Admission requirements: None
## Module Description

<table>
<thead>
<tr>
<th><strong>Module Title:</strong></th>
<th>IT Project Management</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Module No.:</strong></td>
<td>DLMCSITPM</td>
</tr>
<tr>
<td><strong>Semester / Term:</strong></td>
<td>2nd semester</td>
</tr>
<tr>
<td><strong>Duration:</strong></td>
<td>Minimum 1 semester</td>
</tr>
<tr>
<td><strong>Module Type(s):</strong></td>
<td>Compulsory</td>
</tr>
<tr>
<td><strong>Regularly Offered in:</strong></td>
<td>WS / SS</td>
</tr>
<tr>
<td><strong>Workload:</strong></td>
<td>150 h</td>
</tr>
<tr>
<td><strong>Credit Points:</strong></td>
<td>5</td>
</tr>
<tr>
<td><strong>Admission Requirements:</strong></td>
<td>None</td>
</tr>
<tr>
<td><strong>Language of Instruction:</strong></td>
<td>English</td>
</tr>
<tr>
<td><strong>Contributing Courses to Module:</strong></td>
<td>IT Project Management (DLMBITPAM01)</td>
</tr>
<tr>
<td><strong>Workload:</strong></td>
<td>Self-study: 90 h</td>
</tr>
<tr>
<td></td>
<td>Self-examination: 30 h</td>
</tr>
<tr>
<td></td>
<td>Tutorials: 30 h</td>
</tr>
<tr>
<td><strong>Course Coordinator(s) / Tutor(s):</strong></td>
<td>Please see the current list of tutors on the Learning Management System.</td>
</tr>
<tr>
<td><strong>Module Director:</strong></td>
<td>Dr. Damir Ismailović</td>
</tr>
<tr>
<td><strong>References to Other Degree Programs:</strong></td>
<td>Master Artificial Intelligence (120)</td>
</tr>
<tr>
<td></td>
<td>International Business Master of Business Administration (IB-90)</td>
</tr>
<tr>
<td><strong>References to Other Modules in this Degree Program:</strong></td>
<td>IT Security and Data Protection</td>
</tr>
<tr>
<td></td>
<td>Seminar: Computer Science and Society</td>
</tr>
</tbody>
</table>
### Qualification and Educational Objectives of the Module:

On successful completion of this module, students will be able to:

- critically reflect the status of knowledge about IT project management.
- set up different IT project management formats (small, medium and large projects) and know the methods for managing these different IT projects professionally.
- develop an IT management proposal as the fundament of a professional IT project management concept.
- understand and integrate different IT management project plans (e.g., time plan, cost plan, resources plan, risk plan) and use those plans in an integrative IT project planning and controlling scheme.
- organize and lead an IT project team and its core and/or extended team members.

### Learning Content of the Module:

- Organizing the work
- Cost estimation and controlling
- The human factor
- Organizing small and medium projects
- Organizing large projects

### Teaching Methods:

See the contributing course outline

### Literature:

See the contributing course outline

---

### Percentage of the Module Grade Relative to the Final Grade for the Program:

5 ECTS of 60 ECTS = 8.33%

### Prerequisites to Qualify for Assessment:

See course outline

### Assessment:

- **Assessment:** 
  - **DLMBITPAM01:** Exam, 90 min. (100%)
<table>
<thead>
<tr>
<th>Course No.: DLMBITPAM01</th>
<th>Course Title: IT Project Management</th>
<th>Hours Total: 150</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td></td>
<td>Credit Points: 5</td>
</tr>
</tbody>
</table>

**Course Type:** Compulsory  
**Course Availability:** In each semester  
**Course Duration:** Minimum 1 semester  
**Admission Requirements:** None  
**References to Other Modules:** Please see module description.

**Course Description:**

The purpose of this course is to introduce students to the concepts involved in IT project management. This is achieved through the development of an understanding of the fundamental tenets of project management enhancing the students’ ability to apply their knowledge, skills and competencies in analyzing and solving IT project management problems. A special focus is put on the specifics of IT project organization, cost management and the human factor within IT projects.

**Course Objectives and Outcome:**

On successful completion of this course, students will be able to:

- critically reflect the status of knowledge on IT project management.
- set up different IT project management formats (small, medium and large projects) and know the methods for managing these different IT projects professionally.
- develop an IT management proposal as the fundament of a professional IT project management concept.
- understand and integrate different IT management project plans (e.g., time plan, cost plan, resources plan, risk plan) and use those plans in an integrative IT project planning and controlling scheme.
- organize and to lead an IT project team and its core and/or extended team members.

**Teaching Methods:**

The learning materials include printed and online course books, vodcasts, online knowledge tests, podcasts, online tutorials, and case studies. This range of learning materials is offered to students so they can study at a time, place, and pace that best suits their circumstances and individual learning style.
Course Content:

1. **Introduction: Characteristics of IT Projects**
   1.1. Defining IT Projects
   1.2. Overview on Typical Roles and Phases of IT Projects
   1.3. Risks and Challenges of IT Projects
   1.4. Role of an IT Project Manager

2. **Organizing the Work**
   2.1. Project Breakdown Structure, Work Packages
   2.2. Prioritization
   2.3. Time Planning, Milestones, Gantt-Diagram
   2.4. Definition of Done

3. **Cost Estimation and Controlling**
   3.1. Challenges of Cost Estimation in IT Projects
   3.2. Estimation Techniques: 3-Point Estimation, Double Blind Expert Estimation, Function Points
   3.3. Cost Controlling Using Earned Value Analysis
   3.4. Risk Management

4. **The Human Factor**
   4.1. Vision Keeping
   4.2. Stakeholder Management
   4.3. Conflict Management

5. **Organizing Small and Medium Projects**
   5.1. Rational Unified Process (RUP)
   5.2. Agile Software Processes
   5.3. Scrum
   5.4. Plan-driven Project Management in Small Projects

6. **Organizing Large Projects**
   6.1. PMBOK Guide
   6.2. Prince2
   6.3. Multi Project Management
   6.4. Agile Software Processes in Large Projects
   6.5. Selection of the Appropriate Project Management Method
Literature:


A current list with course-specific compulsory reading, as well as references to further literature, is stored in the Learning Management System.

Prerequisites to Qualify for Assessment:

- Depending on the course: Completion of online knowledge tests (approx. 15 minutes per unit, pass / not pass)

Assessment:

- Exam, 90 min.

Student Workload (in hours): 150

Self-study: 90
Self-testing: 30
Tutorials: 30
Module DLMMTHE

Master Thesis

20 ECTS

Minimum length of the module: 1 semester

Admission requirements: See study and exam regulation (SPO)
## Module Description

<table>
<thead>
<tr>
<th>Module Title:</th>
<th>Master Thesis</th>
</tr>
</thead>
<tbody>
<tr>
<td>Module No.:</td>
<td>DLMMTHE</td>
</tr>
<tr>
<td>Semester / Term:</td>
<td>2nd semester</td>
</tr>
<tr>
<td>Duration:</td>
<td>1 Semester</td>
</tr>
<tr>
<td>Module Type(s):</td>
<td>Compulsory</td>
</tr>
<tr>
<td>Regularly Offered In:</td>
<td>WS / SS</td>
</tr>
<tr>
<td>Workload:</td>
<td>600 h</td>
</tr>
<tr>
<td>Credits:</td>
<td>20</td>
</tr>
<tr>
<td>Admission Requirements:</td>
<td>See current study and exam regulations (SPO)</td>
</tr>
<tr>
<td>Language of Instruction:</td>
<td>English</td>
</tr>
<tr>
<td>Contributing Courses to Module:</td>
<td></td>
</tr>
<tr>
<td>- Master Thesis (DLMMETHE01)</td>
<td></td>
</tr>
<tr>
<td>- Thesis Defense (DLMMETHE02)</td>
<td></td>
</tr>
<tr>
<td>Workload:</td>
<td></td>
</tr>
<tr>
<td>- Research &amp; Writing:</td>
<td>540 h</td>
</tr>
<tr>
<td>- Thesis Defense:</td>
<td>60 h</td>
</tr>
<tr>
<td>Course Coordinator(s) / Tutor(s):</td>
<td></td>
</tr>
<tr>
<td>See the current list of tutors on the Learning Management System.</td>
<td></td>
</tr>
<tr>
<td>Module Director:</td>
<td>Prof. Dr. Holger Sommerfeldt</td>
</tr>
<tr>
<td>References to Other Programs:</td>
<td>none</td>
</tr>
<tr>
<td>- none</td>
<td></td>
</tr>
<tr>
<td>References to Other Modules in the Program:</td>
<td></td>
</tr>
<tr>
<td>- All modules in the master program</td>
<td></td>
</tr>
</tbody>
</table>

51/56
### Qualification and Educational Objectives of the Module:

The module master thesis includes the courses Master Thesis and Thesis Defense. The master thesis is an extensive, scholarly, written composition, where the student seeks to independently examine a topic using scientific methods, and where the arguments, results, and processes are documented.

The thesis defense will take place when the finished thesis has been handed in to the supervisor. The defense consists of a presentation detailing the outcomes of the thesis, and a question-and-answer session led by the examiners.

### Learning Content of the Module:

- Written Master Thesis
- Thesis Defense

### Teaching Methods:

See the course description

### Literature:

See the reading list in the course description

### Percentage of the Module Grade of the Total Final Grade of the Program:

20 ECTS of 60 ECTS = 33.3 %

### Prerequisites to Qualify for Assessments:

See current study and exam regulations (SPO)

### Assessment:

- **DLMMTHE01:**
  - Master Thesis (90 %)
  - (approx. 60 A4 pages)
- **DLMMTHE02:**
  - Thesis Defense (10 %)
  - (45 minutes)
<table>
<thead>
<tr>
<th>Course No.: DLMMTHE01</th>
<th>Course Title: Master Thesis</th>
<th>Total Hours: 540</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td></td>
<td>Credits: 18</td>
</tr>
</tbody>
</table>

**Course Type:** Compulsory  
**Course Availability:** in each semester  
**Course Duration:** 1 Semester  
**Admission Requirements:**  
See current study and exam regulations (SPO)

**Course Coordinator / Instructor:**  
See current list of tutors on the Learning Management System.  
**References to Other Modules:**  
All modules in the master program

**Course Description:**
The aim of the master thesis is to effectively apply the knowledge acquired throughout the master course to an academic paper that has a thematic reference to the master program. The thesis can consist of an empirical study or theoretical research. The thesis is an independent piece of work, that, with the guidance of a supervisor, seeks to scientifically analyze and critically discuss a chosen issue, and suggest possible solutions. The chosen topic from the student’s area of specialization should demonstrate their acquired competence in the functional area, yet also enrich and round out the student’s scientific knowledge. This will optimally prepare the student for the needs of their future career path.

**Course Objectives and Outcome:**
The objective of this module is the completion of a written assignment, in line with scientific methodology, that demonstrates the student’s capabilities through independent investigation of a topic pertaining to the master program’s area of focus.

**Teaching Methods:**
While the students complete the thesis individually, guidance and feedback is provided through an academic supervisor.
**Course Content:**

The master thesis should clearly state the topic and research question, and should, through extensive research, reflect the current state of the field in question. The student should demonstrate their knowledge in the form of an independent and solution oriented paper, using theoretical and/or empirical norms.

**Recommended Literature:**

- Further subject specific literature

An actual list with course-specific mandatory reading as well as references to further literature is available in the Learning Management System.

**Assessment:**

Written assessment: Master Thesis (approx. 60 A4 pages)

Two internal examiners will grade the thesis on the basis of an established grading rubric.

The grading criteria are as follows:

- Extent, structure and objective of the research question
- Structure and development of research
- Analysis of key sources and choice of theoretical framework
- Rationale, presentation and use of the scientific approach and chosen methodology
- Presentation, interpretation and discussion of the theoretical and/or empirical findings
- Originality, creativity and independence of the academic writing
- Citation and use of sources
- Adherence to academic writing standards (citations, list of references, list of figures and tables etc.)

**Student Workload (in hours):** 540

Research / Academic Writing: 540 h
<table>
<thead>
<tr>
<th><strong>Course No.:</strong></th>
<th><strong>Course Title:</strong></th>
<th><strong>Total Hours:</strong></th>
<th><strong>Credits:</strong></th>
</tr>
</thead>
<tbody>
<tr>
<td>DLMMTHE02</td>
<td>Thesis Defense</td>
<td>60</td>
<td>2</td>
</tr>
</tbody>
</table>

**Course Type:** Compulsory  
**Course Availability:** in each semester  
**Course Duration:** 1 Semester  
**Admission Requirements:**  
See current study and exam regulations (SPO)  

**Course Coordinator / Instructor:**  
See current list of tutors on the Learning Management System.  
**References to Other Modules:**  
All modules in the master program  

**Course Description:**

The thesis defense takes place after the written master thesis has been handed in by the student. The examiners (the supervisor and a second examiner) will invite the student to the defense. During the presentation, the student will demonstrate that he/she personally has independently produced the content and the results of their written thesis.

The thesis defense consists of a presentation where the student discusses the most significant research outcomes and the results of their thesis, followed by a question-and-answer session chaired by the examiners.

**Course Objectives and Outcome:**

The main objective of the thesis defense is for the student to prove their competence in research methodology and the specific subject matter. The students should also be able to actively participate in a subject specific discussion at a higher academic level with subject area experts. Additionally, the defense will evaluate the academic presentation skills and overall communication skills of the student.

**Teaching Methods:**

The students will be provided with adequate presentation technologies.

**Course Content:**

The thesis defense consists of a presentation of the results and applied method of the master thesis, followed by a question-and-answer session chaired by the examiners.

**Recommended Literature:**

- Subject specific literature chosen by the student
**Assessment:**
- Presentation (15 minutes)
- Oral examination (30 minutes)

The examiners evaluate the student according to the following grading criteria:
- Understanding and application of appropriate scientific methods
- Structure and content of the presentation
- Capability to academically defend a master thesis
- Quality of answers to the examination questions

**Student Workload (in hours):** 60 h
- Preparation: 59 h
- Oral Exam: 1 h