

# Module Handbook

for the

Master Programme “Cyber Security”

at

Rheinischen Friedrich-Wilhelms-Universität Bonn

revised version: March 28, 2026

## Contents

<b>1</b>	<b>Example study plans</b>	<b>2</b>
<b>2</b>	<b>Structure of the curriculum</b>	<b>4</b>
<b>3</b>	<b>Recommended prior modules including all labs and seminars</b>	<b>6</b>
<b>4</b>	<b>Module Descriptions</b>	<b>9</b>
4.1	Cyber Security Compulsory Modules . . . . .	9
4.2	Cyber Security Elective Modules . . . . .	16
4.3	Computer Science Elective Modules – Algorithms . . . . .	27
4.4	Computer Science Elective Modules – Graphics, Vision, Audio . . . . .	45
4.5	Computer Science Elective Modules – Security, Information and Communication Management . . . . .	62
4.6	Computer Science Elective Modules – Intelligent Systems . . . . .	76

## 1 Example study plans

Full-time, starting in the winter semester		
<b>1st semester</b>	<b>30 CP</b>	(winter)
compulsory	6 CP	3236 <b>IT-SECURITY</b>
cyber security elective	6 CP	3108 <b>Secure Software Engineering</b>
cyber security elective	6 CP	3239 <b>Malware Analysis</b>
computer science elective	6 CP	3310 Introduction to Sensor Data Fusion
computer science elective	6 CP	4204 Technical Neural Nets
<b>2nd semester</b>	<b>30 CP</b>	(summer)
cyber security elective	6 CP	3322 <b>Applied Binary Exploitation</b>
cyber security elective	6 CP	3241 <b>Practical Challenges in Human Factors of Security &amp; Privacy</b>
cyber security elective	6 CP	3242 <b>Security of Distributed and Resource-constrained Systems</b>
computer science elective	6 CP	3237 Array Signal and Multi-channel Processing
computer science elective	6 CP	4201 Artificial Life
<b>3rd semester</b>	<b>28 CP</b>	(winter)
compulsory	4 CP	3244 <b>SEMINAR CYBER SECURITY</b>
compulsory	9 CP	3245 <b>LAB CYBER SECURITY</b>
cyber security elective	9 CP	3243 <b>Tutorenpraktikum Cyber Security</b>
computer science elective	6 CP	4112 Algorithms for Data Science
<b>4th semester</b>	<b>32 CP</b>	(summer)
compulsory	30 CP	0401 <b>MASTER THESIS</b>
compulsory	2 CP	0402 <b>MASTER SEMINAR</b>

Full-time, starting in the summer semester		
<b>1st semester</b>	<b>30 CP</b>	(summer)
cyber security elective	6 CP	3241 <b>Practical Challenges in Human Factors of Security and Privacy</b>
cyber security elective	6 CP	3242 <b>Security of Distributed and Resource-constrained Systems</b>
computer science elective	6 CP	3237 Array Signal and Multi-channel Processing
computer science elective	6 CP	4114 Robot Learning
computer science elective	6 CP	4201 Artificial Life
<b>2nd semester</b>	<b>30 CP</b>	(winter)
compulsory	6 CP	3236 <b>IT-SECURITY</b>
cyber security elective	6 CP	3108 <b>Secure Software Engineering</b>
cyber security elective	6 CP	3239 <b>Malware Analysis</b>
computer science elective	6 CP	3310 Introduction to Sensor Data Fusion
computer science elective	6 CP	4204 Technical Neural Nets
<b>3rd semester</b>	<b>28 CP</b>	(summer)
compulsory	4 CP	3244 <b>SEMINAR CYBER SECURITY</b>
compulsory	9 CP	3245 <b>LAB CYBER SECURITY</b>
cyber security elective	6 CP	3322 <b>Applied Binary Exploitation</b>
cyber security elective	9 CP	3243 <b>Tutorenpraktikum Cyber Security</b>
<b>4th semester</b>	<b>32 CP</b>	(winter)
compulsory	30 CP	0401 <b>MASTER THESIS</b>
compulsory	2 CP	0402 <b>MASTER SEMINAR</b>

Part-time, starting in the winter semester		
<b>1st semester</b>	<b>18 CP</b>	(winter)
compulsory	6 CP	3236 <b>IT-SECURITY</b>
computer science elective	6 CP	3310 Introduction to Sensor Data Fusion
computer science elective	6 CP	4204 Technical Neural Nets
<b>2nd semester</b>	<b>18 CP</b>	(summer)
cyber security elective	6 CP	3241 <b>Practical Challenges in Human Factors of Security</b>
computer science elective	6 CP	3237 Array Signal and Multi-channel Processing
computer science elective	6 CP	4201 Artificial Life
<b>3rd semester</b>	<b>22 CP</b>	(winter)
compulsory	4 CP	3244 <b>SEMINAR CYBER SECURITY</b>
cyber security elective	6 CP	3108 <b>Secure Software Engineering</b>
cyber security elective	6 CP	3239 <b>Malware Analysis</b>
computer science elective	6 CP	4112 Algorithms for Data Science
<b>4th semester</b>	<b>21 CP</b>	(summer)
compulsory	9 CP	3245 <b>LAB CYBER SECURITY</b>
cyber security elective	6 CP	3322 <b>Applied Binary Exploitation</b>
cyber security elective	6 CP	3242 <b>Security of Distributed and Resource-constrained Systems</b>
<b>5th semester</b>	<b>21 CP</b>	(winter)
cyber security elective	9 CP	3243 <b>Tutorenpraktikum Cyber Security</b>
compulsory	(12 CP)	0401 <b>MASTER THESIS</b> , partially
<b>6th semester</b>	<b>20 CP</b>	(summer)
compulsory	(18 CP)	0401 <b>MASTER THESIS</b> , completion
compulsory	2 CP	0402 <b>MASTER SEMINAR</b>

Part-time, starting in the summer semester		
<b>1st semester</b>	<b>18 CP</b>	(summer)
cyber security elective	6 CP	3241 <b>Practical Challenges in Human Factors of Security</b>
computer science elective	6 CP	3237 Array Signal and Multi-channel Processing
computer science elective	6 CP	4201 Artificial Life
<b>2nd semester</b>	<b>18 CP</b>	(winter)
compulsory	6 CP	3236 <b>IT-SECURITY</b>
cyber security elective	6 CP	3239 <b>Malware Analysis</b>
computer science elective	6 CP	3310 Introduction to Sensor Data Fusion
<b>3rd semester</b>	<b>22 CP</b>	(summer)
compulsory	4 CP	3244 <b>SEMINAR CYBER SECURITY</b>
cyber security elective	6 CP	3322 <b>Applied Binary Exploitation</b>
cyber security elective	6 CP	3242 <b>Security of Distributed and Resource-constrained Systems</b>
computer science elective	6 CP	4114 Robot Learning
<b>4th semester</b>	<b>21 CP</b>	(winter)
compulsory	9 CP	3245 <b>LAB CYBER SECURITY</b>
cyber security elective	6 CP	3108 <b>Secure Software Engineering</b>
computer science elective	6 CP	4113 Cognitive Robotics
<b>5th semester</b>	<b>21 CP</b>	(summer)
cyber security elective	9 CP	3243 <b>Tutorenpraktikum Cyber Security</b>
compulsory	(12 CP)	0401 <b>MASTER THESIS</b> , partially
<b>6th semester</b>	<b>20 CP</b>	(winter)
compulsory	(18 CP)	0401 <b>MASTER THESIS</b> , completion
compulsory	2 CP	0402 <b>MASTER SEMINAR</b>

## 2 Structure of the curriculum

The curriculum of the Master's programme in Cyber Security consists of:

- **COMPULSORY MODULES**, described in Section 4.1 of this document;
- **cyber security electives**, described in Section 4.2 of this document;
- computer science electives, described in Sections 4.3 to 4.6 of this document, among which we can distinguish lectures, *labs* and *seminars*;
- (optionally) modules outside cyber security and computer science, which can be approved on request.

The following table shows the minimum number of credits that must be obtained in each category:

module type	minimum credits required		
<b>3236 IT-SECURITY</b>	6		
<b>3244 SEMINAR CYBER SECURITY</b>	4		
<b>3245 LAB CYBER SECURITY</b>	9		
<b>cyber security electives</b>	24		69
computer science elective lectures	0	54	
<i>computer science seminar</i> (at most one)	0		
<i>computer science lab</i> (at most one)	0		
other modules (can be approved on request)	0		
<b>0401 MASTER THESIS</b>	30		
<b>0402 MASTER SEMINAR</b> (final presentation)	2		

At least 69 credits in non-compulsory modules are required, of which at least 54 credits must come from cyber security and computer science electives, labs and seminars. Out of those 54 credits, at least 24 must come from cyber security electives and at least 12 must come from computer science electives; the remaining credits can be distributed freely between cyber security and computer science. In total, at least 120 credits must be achieved. Some example study plans can be found in Section 1.

When you compose your own study plan, please note the following.

The Master's thesis project ought to be done at the end of your studies and must be completed within six months in the full-time programme, or within nine months in the part-time programme. At least 60 credits must be acquired before the start of the Master's thesis project.

For some modules it is strongly recommended (and sometimes required) to first complete one or two other modules in a previous semester, as indicated in the following tables. In these tables, for each module, the number of credits is indicated in brackets. Most modules are offered yearly. Exceptions are indicated as follows:

- (+) this module is offered in the winter and in the summer semester
- (-) this module is not offered every year

All Modules are offered (at least) in English.

recommended in the winter semester	before taking in the summer semester
[6] <b>3236 IT-SECURITY</b> and [6] 4204 Technical Neural Nets	[6] <b>3246 Security in Digital Supply Chains</b>
[6] <b>3236 IT-SECURITY</b>	[9] <b>3243 Tutorenpraktikum Cyber Security</b> (+) or [4] <b>3244 SEMINAR CYBER SECURITY</b> (+) or [9] <b>3245 LAB CYBER SECURITY</b> (+)
[6] <b>3239 Malware Analysis</b>	[6] <b>3322 Applied Binary Exploitation</b>
[9] 1103 Cryptography	[9] 1223 Privacy Enhancing Technologies
[6] 2113 Audio Signal Processing	[6] 2212 Pattern Matching and ML for Audio Signal Processing
[9] 2201 Computer Vision	[6] 2213 Advanced Computer Vision or [6] 2218 Video Analytics(-)
[6] 3310 Sensor Data Fusion	[6] 3233 Advanced Sensor Data Fusion in Distributed Systems
[6] 4111 Machine Learning(-)	[6] 4242 Self-Supervised Learning

recommended in the winter semester	before taking in the next winter semester
[9] 2201 Computer Vision or [6] 4111 Machine Learning(-)	[6] 4333 Geometric Deep Learning
[6] 4113 Cognitive Robotics	[6] 4334 Computational Neuroscience

modules in the winter semester that are independent of other modules  
(apart from computer science labs and seminars):

- [6] **3108 Secure Software Engineering**
- [6] **3238 Side Channel Attacks**
- [6] 1108 Introduction to High Performance Computing
- [6] 1110 Elliptic Curves and their Applications in Cryptography
- [6] 2317 Numerical Algorithms for Visual Computing and Machine Learning
- [6] 4112 Algorithms for Data Science
- [6] 4326 Explainable AI and Applications
- [6] 4328 Spatio-Temporal Data Analytics

recommended in the summer semester	before taking in the winter semester:
[9] 2222 Visual Data Analysis	[6] 4333 Geometric Deep Learning
[6] 4114 Robot Learning	[6] 4334 Computational Neuroscience

modules in the summer semester that are independent of other modules  
(apart from computer science labs and seminars):

- [6] **3202 Mobile Communication**
- [6] **3241 Practical Challenges in Human Factors of Security and Privacy**
- [6] **3242 Security of Distributed and Resource-constrained Systems**
- [6] 1105 Algorithms for Data Analysis(-)
- [9] 2202 Computer Animation
- [6] 2225 Discrete Models for Visual Computing
- [6] 3237 Array Signal and Multi-channel Processing
- [6] 4201 Artificial Life
- [6] 4215 Humanoid Robotics(-)
- [9] 4228 Foundations of Data Science
- [6] 4230 Advanced Methods of Information Retrieval(-)
- [4] 4236 Advanced Methods for Text Mining(-)

Please check the module descriptions in this handbook for details. This handbook also lists about 40 computer science labs and seminars that are open to cyber security students. You may include one computer science seminar and one computer science lab in your programme. Tables that include recommended prior modules for labs and seminars can be found in Section 3.

When you compose your own study plan, please check whether the modules' weekly schedules are compatible before putting them in your final plan. In any case, the schedules of the compulsory and the cyber security elective modules are always compatible with each other, and the schedules of the computer science lectures are always compatible with **3236 IT-SECURITY**.

**3243 Tutorenpraktikum Cyber Security**, **3244 SEMINAR CYBER SECURITY**, and **3245 LAB CYBER SECURITY** can only be taken in the Master's programme in Cyber Security. All other modules can also be included as electives in the Master's programme in Computer Science.

### 3 Recommended prior modules including all labs and seminars

The following tables show recommended prior modules for all modules, including about 40 computer science labs and seminars that are open to cyber security students. A more concise overview that only lists cyber security modules and computer science lectures (without the labs and the seminars) can be found in Section 2.

Labs and seminars marked (@) may sometimes be offered in the winter semester, sometimes in the summer semester, possibly depending on demand; please check with the instructors early.

recommended in the winter semester	before taking in the summer semester
[6] <b>3236 IT-SECURITY</b> and [6] 4204 Technical Neural Nets	[6] <b>3246 Security in Digital Supply Chains</b>
[6] <b>3236 IT-SECURITY</b>	[9] <b>3243 Tutorenpraktikum Cyber Security(+)</b> or [4] <b>3244 SEMINAR CYBER SECURITY(+)</b> or [9] <b>3245 LAB CYBER SECURITY(+)</b> or [4] <i>3209 Seminar Communication Management(+)</i> or [4] <i>3317 Seminar IT Security(+)</i> or [9] <i>3229 Lab IT-Security(+)</i> or [9] <i>3304 Lab Communication and Communicating Devices(+)</i>
[6] <b>3239 Malware Analysis</b>	[6] <b>3322 Applied Binary Exploitation</b>
[9] 1103 Cryptography	[9] 1223 Privacy Enhancing Technologies or [4] <i>1209 Seminar Cryptography(+)</i> or [9] <i>1316 Lab Cryptography</i>
[6] 4112 Algorithms for Data Science	[9] <i>1221 Lab Computational Analytics</i>
[9] 1103 Cryptography or [6] 1108 High Performance Computing	[9] <i>1309 Lab Efficient Algorithms(@)</i>
[6] 1108 High Performance Computing	[4] <i>1322 Seminar High Performance Computing</i> or [9] <i>2308 Lab Graphics(+)</i>
[6] 2113 Audio Signal Processing	[6] 2212 Pattern Matching & ML for Audio Signal Pr. or [9] <i>2309 Lab Audio</i>
[9] 2201 Computer Vision	[6] 2213 Advanced Computer Vision or [6] 2218 Video Analytics(-)
[6] 2317 Num. Alg. for Visual Comp. and ML	[9] <i>2216 Lab Visual Computing(+)</i>
[6] 3310 Sensor Data Fusion	[6] <b>3233 Adv. Sensor Data Fusion in Distrib. Syst.</b> or [9] <i>3312 Lab Sensor Data Fusion</i>
[9] 2201 Computer Vision or [6] 4111 Machine Learning(-) or [6] 4204 Technical Neural Nets	[4] <i>4208 Seminar Vision Systems(+)</i> or [9] <i>4308 Lab Vision Systems(+)</i>
[6] 4111 Machine Learning(-)	[6] <b>4242 Self-Supervised Learning</b>
[6] 4111 Machine Learning(-) or [6] 4112 Algorithms for Data Science	[4] <i>4209 Seminar Data Mining and Learning Algorithms</i> or [9] <i>4306 Lab Dev. &amp; Appl. of Data Mining and Learning Systems(+)</i>
[6] 4113 Cognitive Robotics	[4] <i>4211 Seminar Cognitive Robotics(+)</i> or [4] <i>4213 Seminar Humanoid Robotics(+)</i> or [9] <i>4214 Lab Humanoid Robotics(+)</i> or [9] <i>4241 Lab Cognitive Modelling of Biological Agents(+)</i> or [9] <i>4304 Lab Cognitive Robotics(+)</i>
[6] 4328 Spatio-Temporal Data Analytics(-)	[4] <i>4324 Seminar Data Science(-)</i> or [9] <i>4325 Lab Data Science in Practice</i>
[9] 2201 Computer Vision and [6] 4113 Cognitive Robotics	[9] <i>4331 Lab Perception and Learning for Robotics(@)</i>

recommended in the winter semester	before taking in the next winter semester
[6] 1108 High Performance Computing	[9] <i>1222 Lab High Performance Optimization</i>
[6] 1108 High Performance Computing	[9] <i>1225 Lab Exploring HPC Technologies (@)</i>
[6] 2113 Audio Signal Processing	[4] <i>2208 Seminar Audio</i>
[6] 3310 Sensor Data Fusion	[4] <i>3216 Seminar Sensor Data Fusion</i>
[9] 1103 Cryptography	[9] <i>4322 Lab Machine Learning on Encrypted Data</i>
[9] 2201 Computer Vision or [6] 4111 Machine Learning(-)	[6] 4333 Geometric Deep Learning
[6] 4113 Cognitive Robotics	[6] 4334 Computational Neuroscience

modules in the winter semester that are independent of other modules

[6] **3108 Secure Software Engineering**  
 [6] **3238 Side Channel Attacks**  
 [6] 1110 Elliptic Curves and their Applications in Cryptography  
 [6] 4326 Explainable AI and Applications  
 [4] *3321 Seminar Usable Security and Privacy(+)*  
 [9] *2226 Lab Geometry Processing (@)*  
 [9] *2227 Lab 3D Animation(+)*

recommended in the summer semester	before taking in the winter semester
[6] 2225 Discrete Models for Visual Computing	[9] <i>2216 Lab Visual Computing(+)</i>
[9] 2222 Visual Data Analysis	[4] <i>2219 Sem. Visualization &amp; Medical Image Anal.(-) or</i> [9] <i>2220 Lab Visualization &amp; Medical Image Analysis(+)</i>
[9] 2202 Computer Animation or [9] 2222 Visual Data Analysis	[9] <i>2308 Lab Graphics(+)</i>
[6] <b>3202 Mobile Communication</b>	[4] <i>3209 Seminar Communication Management(+)</i> or [9] <i>3304 Lab Communication and Communic. Devices(+)</i>
[6] <b>3241 Human Factors of Security &amp; Privacy</b>	[9] <i>3319 Lab Usable Security and Privacy(+)</i>
[6] <b>3242 Security of Distr. &amp; Res.-constr. Syst.</b>	[9] <i>3320 Lab Security in Distributed Systems(+)</i>
[6] 4114 Robot Learning	[4] <i>4211 Seminar Cognitive Robotics(+)</i> or [9] <i>4304 Lab Cognitive Robotics(+)</i> or [6] 4334 Computational Neuroscience
[6] 4215 Humanoid Robotics(-)	[4] <i>4213 Seminar Humanoid Robotics(+)</i> or [9] <i>4214 Lab Humanoid Robotics(+)</i>
[6] 4230 Adv. Methods of Information Retrieval(-)	[4] <i>4231 Seminar Information Retrieval(-)or</i> [9] <i>4232 Lab Information Retrieval in Practice</i>
[6] 4114 Robot Learning or [6] 4215 Humanoid Robotics(-)	[9] <i>4241 Lab Cognitive Modelling of Biological Agents(+)</i>
[9] 2222 Visual Data Analysis	[6] 4333 Geometric Deep Learning

modules in the summer semester that are independent of other modules
--

- |   |
|---|
| <ul style="list-style-type: none"><li>[6] 1105 Algorithms for Data Analysis(-)</li><li>[6] 3237 Array Signal and Multi-channel Processing</li><li>[6] 4201 Artificial Life</li><li>[9] 4228 Foundations of Data Science</li><li>[4] 4236 Advanced Methods for Text Mining(-)</li><li>[4] 3321 Seminar Usable Security and Privacy(+)</li><li>[9] 2216 Lab Visual Computing(+)</li><li>[9] 2226 Lab Geometry Processing (@)</li><li>[9] 2227 Lab 3D Animation(+)</li></ul> |
|---|

Please check the module descriptions in this handbook for details. Note that the module descriptions sometimes recommend alternative modules as prior knowledge that are not open to cyber security students or that may be difficult to complete in advance due to chain dependencies. Please check carefully. There is always at least one viable option for cyber security students, as indicated above.

## 4 Module Descriptions

### 4.1 Cyber Security Compulsory Modules

MA-INF 0401	30 CP	Master Thesis .....	10
MA-INF 0402	2 CP	Master Seminar .....	11
MA-INF 3236	L2E2 6 CP	IT Security .....	12
MA-INF 3244	Sem2 4 CP	Seminar Cyber Security .....	14
MA-INF 3245	Lab4 9 CP	Lab Cyber Security .....	15

---

**MA-INF 0401 Master Thesis**


---

Workload	Credit points	Duration	Frequency
900 h	30 CP	1 semester	every semester

Module coordinator	Lecturer(s)
The Examination Board	All lecturers of computer science

Programme	Mode	Semester
M. Sc. Cyber Security	Compulsory	4.

**Learning goals: technical skills**

Ability to solve a well-defined, significant research problem under supervision, but in principle independently

**Learning goals: soft skills**

Ability to write a scientific documentation of considerable length according to established scientific principles of form and style, in particular reflecting solid knowledge about the state-of-the-art in the field

**Contents**

Topics of the thesis may be chosen from any of the areas of computer science represented in the curriculum

**Prerequisites**
**Required:**

By the examination regulations of 2023, the Master's thesis project can only commence after 60 credits in other modules of the programme have been obtained. Before you start on the project, you must obtain the approval of the exam committee and register the starting date of the project. Please check the website of the examination office for forms and procedures.

**Course meetings**

Teaching format	Group size	h/week	Workload[h]	CP	
Independent preparation of a scientific thesis with individual coaching		0	900 S	30	T = face-to-face teaching S = independent study

**Graded exams**

Master Thesis

**Ungraded coursework (required for admission to the exam)**

None

**Literature**

Individual bibliographic research required for identifying relevant literature (depending on the topic of the thesis)

---

---

**MA-INF 0402 Master Seminar**


---

Workload	Credit points	Duration	Frequency
60 h	2 CP	1 semester	every semester
Module coordinator	Lecturer(s)		
The Examination Board	All lecturers of computer science		
Programme	Mode	Semester	
M. Sc. Cyber Security	Compulsory	4.	

**Learning goals: technical skills**

Knowledge of the state-of-the-art in research in the respective area and how the thesis results relate to that.

**Learning goals: soft skills**

Ability to identify the most relevant content for a knowledgeable scientific audience; ability to present and defend one's work in a presentation with visual media in a way that adheres to academic standards; ability to anticipate, accept and answer critical questions.

**Contents**

Topic, scientific context, and results of the master thesis

**Prerequisites****Required:**

The Master Seminar accompanies the Master Thesis project, see MA-INF 0401 for prerequisites.

**Recommended:**

None

**Course meetings**

Teaching format	Group size	h/week	Workload[h]	CP	
Seminar		2	30 T / 30 S	2	T = face-to-face teaching S = independent study

**Graded exams**

Oral presentation of final results

**Ungraded coursework (required for admission to the exam)**

None

**Literature**

Individual bibliographic research required for identifying relevant literature (depending on the topic of the thesis)

---

# MA-INF 3236 IT Security

Workload	Credit points	Duration	Frequency
180 h	6 CP	1 semester	every year
Module coordinator	Lecturer(s)		
Prof. Dr. Michael Meier	Prof. Dr. Michael Meier		
Programme	Mode	Semester	
M. Sc. Cyber Security	Compulsory	1. or 2.	

**Learning goals: technical skills**

Knowledge of a variety of active research fields in IT security including motivation, challenges and objectives in these fields as well as selected fundamental knowledge and methods helping students to deepen their knowledge in their upcoming studies. In detail, participants will know

- advanced cryptographic constructions and low-level programming in offensive and defensive scenarios;
- how to apply program analysis techniques to IT security;
- how to achieve security by and security of methods from the area of machine learning.

**Learning goals: soft skills**

Working in small groups on exercises, critical discussion of own and others' results, time management, transferring theoretical knowledge to practical scenarios

**Contents**

The contents vary but usually include

- Privacy
- Cryptographic Protocols
- Network Security
- Supply Chain Attacks
- Management of Identity Data
- Low-level software analysis
- Software testing
- Side Channel Attacks
- Anomaly Detection
- Human Factor in Security

**Prerequisites**

**Recommended:**

Foundational knowledge in

- IT security: security terminology, authentication, access control, applied cryptography (symmetric encryption, asymmetric encryption, hashing, key management)
- Low-level/OS-level programming: x86 assembly, C programming, OS-level programming for Linux, buffer overflows, sockets
- Networking: OSI model, modulation, addressing, routing, udp, tcp

You find useful information on these topics in the following books (available through library search portal bonnus):

- M. Bishop: Computer Security: Art and Science, Pearson Education, 2018.
- J. Streib: Guide to Assembly Language: A Concise Introduction. Springer, 2020.
- W. Stevens: UNIX Network Programming – The Sockets Networking API, Prentice Hall International, 3rd Edition, 2003
- Tanenbaum: Computer Networks, Pearson Education, 4th Edition, 2002

**Course meetings**

Teaching format	Group size	h/week	Workload[h]	CP	
Lecture		2	30 T / 45 S	2.5	T = face-to-face teaching S = independent study
Exercises		2	30 T / 75 S	3.5	

**Graded exams**

Written exam (120 minutes)

**Ungraded coursework (required for admission to the exam)**

The completion of regularly provided exercise sheets. The work can be done in groups of up to three students. For 70% of the exercise sheets, 50% of the points must be achieved for each sheet.

---

## MA-INF 3244 Seminar Cyber Security

Workload	Credit points	Duration	Frequency
120 h	4 CP	1 semester	every semester

Module coordinator	Lecturer(s)
Prof. Dr. Michael Meier	Prof. Dr. Matthew Smith, Prof. Dr. Peter Martini, Prof. Dr. Michael Meier, Dr. Felix Boes, Dr. Matthias Wübbeling, Dr. Christian Tiefenau, Dr. Matthias Frank, Dr. Marc Ohm

Programme	Mode	Semester
M. Sc. Cyber Security	Compulsory	2. or 3.

### Learning goals: technical skills

Enhanced and in-depth knowledge in specialized topics in the area of Cyber Security

### Learning goals: soft skills

Acquire the competence to independently search for and study state-of-the-art scientific literature in depth, read critically, identify the most relevant content, and assess research results in the context of the corresponding research area; to discuss research results with a knowledgeable scientific audience; to present prior work by others in writing and in presentations with visual media in a way that adheres to academic standards, that is well-structured and didactically effective, and that motivates the audience to participate; to formulate and accept criticism; to manage one's time with relatively open assignments and long-ranging deadlines.

### Contents

Recent research topics in Cyber Security based on current journal and conference publications. In addition the seminar group analyses and discusses current societal and political developments related to Cyber Security. Participation in discussion events that are announced in the seminar.

### Prerequisites

#### Recommended:

Foundational knowledge in

- IT security: security terminology, authentication, access control, applied cryptography (symmetric encryption, asymmetric encryption, hashing, key management)
- Usable Security and Privacy: ethics, usability measures, evaluation methods, statistics
- Networks: OSI model, modulation, addressing, routing, udp, tcp

It is recommended to take MA-INF 3236 IT-Security first and to check the material of BA-INF 145 Usable Security and Privacy (available in English).

### Course meetings

Teaching format	Group size	h/week	Workload[h]	CP
Seminar	10	2	30 T / 90 S	4

T = face-to-face teaching  
S = independent study

### Graded exams

Oral presentation, written report

### Ungraded coursework (required for admission to the exam)

Attendance in course sessions in accordance with the exam regulations of 2023, § 12(6).

## MA-INF 3245 Lab Cyber Security

Workload	Credit points	Duration	Frequency
270 h	9 CP	1 semester	every semester
Module coordinator	Lecturer(s)		
Prof. Dr. Michael Meier	Prof. Dr. Michael Meier, Prof. Dr. Matthew Smith, Prof. Dr. Peter Martini, Dr. Felix Boes, Dr. Matthias Wübbeling, Dr. Christian Tiefenau, Dr. Matthias Frank, Dr. Marc Ohm		
Programme	Mode	Semester	
M. Sc. Cyber Security	Compulsory	2. or 3.	

### Learning goals: technical skills

After completion of the lab module students have completed a practical task in the context of cyber security. The students will have gained experience in the typical technical skills like the design and implementation of software, test and documentation of the software, and performance evaluation (e.g. by measurements, simulation, analysis) and presentation of performance results.

### Learning goals: soft skills

Ability to analyze problems theoretically and to find creative and practical solutions; to examine one's solutions and results critically; to classify one's own results into the state-of-the-art of the respective area; to prepare readable documentation of software and research results; to present, defend and discuss design decisions and results in the team/group and to other students clearly and in accordance with academic standards; to collaborate constructively with others in small teams over a longer period of time; to aim at long-range goals under limited resources; to work under pressure.

### Contents

- Selected topics close to current research in the area of cyber security.
- Participation in discussion events that are announced in the lab.

### Prerequisites

#### Recommended:

Foundational knowledge in

- IT security: security terminology, authentication, access control, applied cryptography (symmetric encryption, asymmetric encryption, hashing, key management)
- Usable Security and Privacy: ethics, usability measures, evaluation methods, statistics
- Networks: OSI model, modulation, addressing, routing, udp, tcp

It is recommended to take MA-INF 3236 IT-Security first and to check the material of BA-INF 145 Usable Security and Privacy (available in English).

### Course meetings

Teaching format	Group size	h/week	Workload[h]	CP	
Lab	8	4	60 T / 210 S	9	T = face-to-face teaching S = independent study

### Graded exams

Oral presentation, written report

### Ungraded coursework (required for admission to the exam)

Project work; attendance in course sessions in accordance with the exam regulations of 2023, § 12(6).

## 4.2 Cyber Security Elective Modules

MA-INF 3108	L2E2	6 CP	Secure Software Engineering	17
MA-INF 3202	L2E2	6 CP	Mobile Communication	18
MA-INF 3238	L2E2	6 CP	Side Channel Attacks	19
MA-INF 3239	L2E2	6 CP	Malware Analysis	20
MA-INF 3241	L3E1	6 CP	Practical Challenges in Human Factors of Security and Privacy	22
MA-INF 3242	L2E2	6 CP	Security of Distributed and Resource-constrained Systems	23
MA-INF 3243	Sem2P3	9 CP	Tutorenpraktikum Cyber Security	24
MA-INF 3246	L2E2	6 CP	Security in Digital Supply Chains	25
MA-INF 3322	L2E2	6 CP	Applied Binary Exploitation	26

# MA-INF 3108 Secure Software Engineering

Workload	Credit points	Duration	Frequency
180 h	6 CP	1 semester	every year
Module coordinator	Lecturer(s)		
Dr. Christian Tiefenau	Dr. Christian Tiefenau		
Programme	Mode	Semester	
M. Sc. Cyber Security	Optional	1-3.	

**Learning goals: technical skills**

The students will learn how to integrate security aspects into the phases of a Software Development Lifecycle. They will learn:

- Methods for identifying threats and vulnerabilities (threat modeling and risk analysis).
- How to design secure architectures using fundamental design principles (e.g., STRIDE).
- Secure coding practices and common vulnerability types.
- Key considerations when using cryptographic methods in software.
- How to assess the severity of a vulnerability.
- Best practices for system configuration, deployment, and maintenance.

**Learning goals: soft skills**

In the exercises, the students will conduct practical tasks to strengthen the understanding of the methods within the secure software engineering lifecycle. Through this, the abilities teamwork, organization and critical discussion of their own and others' results are strengthened.

**Contents**

- Threat modeling
- Risk analysis
- Architectural security
- Secure coding
- Applied Cryptography
- Secure configuration and deployment
- Updates and maintenance

**Prerequisites**

**Recommended:**

Basic knowledge of software engineering and IT Security-concepts is advantageous but not mandatory.

**Course meetings**

Teaching format	Group size	h/week	Workload[h]	CP	
Lecture		2	30 T / 45 S	2.5	T = face-to-face teaching S = independent study
Exercises		2	30 T / 75 S	3.5	

**Graded exams**

Written exam (90 minutes)

**Ungraded coursework (required for admission to the exam)**

none

**Literature**

Software Security: Building Security In by Gary McGraw

## MA-INF 3202 Mobile Communication

Workload	Credit points	Duration	Frequency
180 h	6 CP	1 semester	every year
Module coordinator	Lecturer(s)		
Prof. Dr. Peter Martini	Prof. Dr. Peter Martini, Dr. Matthias Frank		
Programme	Mode	Semester	
M. Sc. Cyber Security	Optional	1. or 2.	

### Learning goals: technical skills

After completion of the module students will be able to cope with challenges and problems arising in design and operation of wireless and mobile communication systems. They can choose suitable protocols or design new ones. They are able to select mechanisms from different architectural layers, integrate them into a new complete architecture and justify their selection and integration decisions.

### Learning goals: soft skills

Theoretical exercises support in-depth understanding of lecture topics and stimulate discussions; practical exercises in teamwork support time management, targeted organisation of practical work and critical discussion of own and others' results

### Contents

Mobility Management in the Internet, Wireless Communication Basics, Wireless Networking Technologies (like Bluetooth, Wireless LAN, LoRa/LoRaWAN, focus on system architecture and medium access), Cellular/Mobile Communication Networks (voice and data communication, 2G, 4G, ...).

### Prerequisites

#### Recommended:

Bachelor level knowledge of basics of communication systems and Internet protocols. Students may receive access to lecture slides in English language of our Bachelor module BA-INF 101 "Kommunikation in Verteilten Systemen" as a reference. Contact the lecturer in advance of the course, and information will also be given in the first lecture.

### Course meetings

Teaching format	Group size	h/week	Workload[h]	CP	
Lecture		2	30 T / 45 S	2.5	T = face-to-face teaching
Exercises		2	30 T / 75 S	3.5	S = independent study

### Graded exams

Written exam (90 minutes)

### Ungraded coursework (required for admission to the exam)

The completion of regularly provided exercise sheets. The work can be done in groups of up to three students. A total of 50% of the points must be achieved. For 70% of the exercise sheets, 20% of the points must be achieved for each sheet.

### Literature

- Jochen Schiller: Mobile Communications, Addison-Wesley, 2003
- William Stallings: Wireless Communications and Networking, Prentice Hall, 2002
- Further up-to-date literature will be announced in due course before the beginning of the lecture

---

**MA-INF 3238 Side Channel Attacks**


---

Workload	Credit points	Duration	Frequency
180 h	6 CP	1 semester	every year
Module coordinator	Lecturer(s)		
Dr. Felix Boes	Dr. Felix Boes		
Programme	Mode	Semester	
M. Sc. Cyber Security	Optional	1-3.	

**Learning goals: technical skills**

- Students are introduced to theoretical and practical side channel effects of modern hardware.
- Students learn techniques to utilize these effects to circumvent security mechanisms.
- This includes covert channels as well as side channel attacks and microarchitectural attacks on modern CPUs.

**Learning goals: soft skills**

Theoretical exercises to support in-depth understanding of lecture topics and to stimulate discussions, practical exercises in teamwork to support time management, targeted organization of practical work and critical discussion of own and others' results.

**Contents**

- Theoretical foundations of side channel effects and attacks as well as
- covert channels,
- differential power analysis,
- padding oracle,
- RSA timing attacks,
- cache based side channel effects,
- microarchitectural attacks (Spectre)

**Prerequisites****Recommended:**

Fundamental knowledge about IT Security, operating systems and statistics is advantageous but not mandatory.

**Course meetings**

Teaching format	Group size	h/week	Workload[h]	CP	
Lecture		2	30 T / 45 S	2.5	T = face-to-face teaching S = independent study
Exercises		2	30 T / 75 S	3.5	

**Graded exams**

Oral exam

**Ungraded coursework (required for admission to the exam)**

Participation in two achievement tests. In total, at least 50% of the points must be achieved on these tests.

---

# MA-INF 3239 Malware Analysis

Workload	Credit points	Duration	Frequency
180 h	6 CP	1 semester	every year
Module coordinator	Lecturer(s)		
Prof. Dr. Peter Martini	Prof. Dr. Elmar Padilla		
Programme	Mode	Semester	
M. Sc. Cyber Security	Optional	1. or 2.	

**Learning goals: technical skills**

The students should be able to analyze the functional scope of a binary file independently and to describe its damage potential. In addition, the students should be able to carry out detailed analyzes of given aspects and to partially automate these with the help of scripts.

**Learning goals: soft skills**

Presentation of solutions and methods, critical discussion of applied methods and techniques.

**Contents**

In the course, the skills acquired so far in binary analysis will first be deepened and adapted to the peculiarities of malware analysis. Different malware samples are used to explain the techniques used by malware authors. These priorities include:

- Characteristics of malware
- Persistence
- Network communication
- Encryption
- Dynamic malware analysis
- Debugging
- Behavioral obfuscation
- Virtual analysis environments
- Static malware analysis
- Control flow obfuscation
- Automation of common analysis steps
- Reconstruction of binary algorithms

The event begins with several lectures that provide the basics for the students to work independently later. In the course of this, the students will work on practical topics from the field of malware analysis during the semester. Since these subject areas can turn out to be very specific, it is necessary to be willing to deal with the subject outside of the lecture and exercise times.

**Prerequisites**

**Recommended:**

Basic knowledge of operating systems (kernel, threads, virtual memory), network communication (protocols, architectures), binary analysis (assembler, endianness, semantic gap, coding), software development (programming, semantics, scripting in Python)

**Course meetings**

Teaching format	Group size	h/week	Workload[h]	CP	
Lecture		2	30 T / 45 S	2.5	T = face-to-face teaching
Exercises		2	30 T / 75 S	3.5	S = independent study

**Graded exams**

Oral exam (30 minutes)

**Ungraded coursework (required for admission to the exam)**

The completion of regularly provided exercise sheets. The work can be done in groups of up to two students. A total of 50% of the points must be achieved.

---

**Literature**

The relevant literature will be announced at the beginning of the lecture

---

# MA-INF 3241 Practical Challenges in Human Factors of Security and Privacy

Workload	Credit points	Duration	Frequency
180 h	6 CP	1 semester	every year
Module coordinator	Lecturer(s)		
Prof. Dr. Matthew Smith	Prof. Dr. Matthew Smith		
Programme	Mode	Semester	
M. Sc. Cyber Security	Optional	1-3.	

**Learning goals: technical skills**

Students are introduced to a variety of current challenges in security and privacy which contain human aspects and have societal relevance. Students learn about the motivation, challenges and objectives in these areas and select one for the semester topic. They then learn how to design, conduct and evaluate user studies to tackle the selected challenge. Additionally, they get to know selected fundamental knowledge and methods helping them to deepen their knowledge on human factors research.

**Learning goals: soft skills**

Breaking down complex topics into manageable components, critical discussion of own and others' results, time management, transferring theoretical knowledge to practical scenarios

**Contents**

The course begins with several lectures that provide an overview and discussion of current societal challenges in the area of human factors in security and privacy. The students will select a semester topic and together with the lecturer explore this topic using user studies. Since these subject areas can turn out to be very specific, it is beneficial to be willing to deal with the subject outside of the lecture and exercise times. Topics can include surveillance, age verification, anonymity, online abuse, fake news, etc.

**Prerequisites**

**Recommended:**

It is recommended that students have experience with designing and evaluating survey and interview-based user studies. It is recommended to check the material of BA-INF 145 Usable Security and Privacy (available in English).

**Course meetings**

Teaching format	Group size	h/week	Workload[h]	CP	
Lecture		1	15 T / 45 S	2	T = face-to-face teaching S = independent study
Exercises		3	45 T / 75 S	4	

**Graded exams**

electronic exam (90 minutes, pass/fail)

**Ungraded coursework (required for admission to the exam)**

The participation in at least 80% of regularly provided exercises.

## MA-INF 3242 Security of Distributed and Resource-constrained Systems

Workload	Credit points	Duration	Frequency
180 h	6 CP	1 semester	every year
Module coordinator	Lecturer(s)		
Prof. Dr. Michael Meier	Dr. Thorsten Aurisch		
Programme	Mode	Semester	
M. Sc. Cyber Security	Optional	1. or 2.	

### Learning goals: technical skills

Ability to understand and analyse theoretical and practical cyber security challenges of distributed and resource-constrained systems, as well as the ability to select and apply appropriate solutions.

### Learning goals: soft skills

Working in small groups on exercises, critical discussion of own and others' results, time management, transferring theoretical knowledge to practical scenarios.

### Contents

- Group communication with IP multicast
- Group key management
- Broadcast encryption
- Public key infrastructure
- Web of trust
- Multicast infrastructure protection
- Distributed security mechanisms
- Cyber resilience in groups
- Distributed ledger technology
- Cyber security in software-defined networks
- Artificial intelligence in cyber security
- Security for IoT

### Prerequisites

#### Recommended:

Foundational knowledge in

- IT security: security terminology, authentication, access control, applied cryptography (symmetric encryption, asymmetric encryption, hashing, key management)
- Low-level/OS-level programming: x86 assembly, C programming, OS-level programming for Linux, buffer overflows, sockets
- Networking: OSI model, modulation, addressing, routing, udp, tcp

You find useful information on these topics in the following books (available through library search portal bonnus):

- M. Bishop: Computer Security: Art and Science, Pearson Education, 2018.
- J. Streib: Guide to Assembly Language: A Concise Introduction. Springer, 2020.
- W. Stevens: UNIX Network Programming – The Sockets Networking API, Prentice Hall International, 3rd Edition, 2003
- Tanenbaum: Computer Networks, Pearson Education, 4th Edition, 2002

### Course meetings

Teaching format	Group size	h/week	Workload[h]	CP	
Lecture		2	30 T / 45 S	2.5	T = face-to-face teaching
Exercises		2	30 T / 75 S	3.5	S = independent study

### Graded exams

Written exam (120 minutes)

### Ungraded coursework (required for admission to the exam)

Participation in an achievement test. At least 50% of the points must be achieved on this test.

## MA-INF 3243 Tutorenpraktikum Cyber Security

Workload	Credit points	Duration	Frequency
270 h	9 CP	1 semester	every year

Module coordinator	Lecturer(s)
Prof. Dr. Michael Meier	Prof. Dr. Matthew Smith, Prof. Dr. Michael Meier, Prof. Dr. Peter Martini, Dr. Felix Boes, Dr. Matthias Wübbeling, Dr. Marc Ohm, Prof. Dr. Michael Meier, Dr. Christian Tiefenau, Dr. Matthias Frank

Programme	Mode	Semester
M. Sc. Cyber Security	Optional	3.

### Learning goals: technical skills

Ability to and experience in

- evaluating and assessing exercise solutions and argumentations,
- development, implementation and application of teaching and learning tools.

### Learning goals: soft skills

Ability to and experience in

- conveying knowledge to students,
- presenting technical, conceptual and scientific content.

### Contents

Varying practical tutoring tasks in the context of cyber security are carried out. This can include tutoring of exercise sessions for a cyber security course (bachelor or master level), correction of homework, evaluation of students' progress, participation in the regular tutor meetings, development of teaching material (e.g. exercise tasks) and demonstrations to illustrate and convey technical as well as scientific correlations.

This module can be completed in German or in English.

### Prerequisites

#### Recommended:

Foundational knowledge in

- IT security: security terminology, authentication, access control, applied cryptography (symmetric encryption, asymmetric encryption, hashing, key management)
- Usable Security and Privacy: ethics, usability measures, evaluation methods, statistics
- Networks: OSI model, modulation, addressing, routing, udp, tcp

It is recommended to take MA-INF 3236 IT-Security first and to check the material of BA-INF 145 Usable Security and Privacy (available in English).

### Course meetings

Teaching format	Group size	h/week	Workload[h]	CP	
Seminar	8	1	15 T / 45 S	2	T = face-to-face teaching S = independent study
Practical Work	8	5	75 T / 135 S	7	

### Graded exams

Project work

### Ungraded coursework (required for admission to the exam)

None

---

**MA-INF 3246 Security in Digital Supply Chains**


---

Workload	Credit points	Duration	Frequency
180 h	6 CP	1 semester	every year
Module coordinator	Lecturer(s)		
Dr. Marc Ohm	Dr. Marc Ohm		
Programme	Mode	Semester	
M. Sc. Cyber Security	Optional	2-3.	

**Learning goals: technical skills**

This module introduces the challenges and risks of digital supply chains in the context of cybersecurity. It focuses on recent developments in the software supply chain and the artificial intelligence supply chain. Additionally, it will present threat intelligence methodologies.

**Learning goals: soft skills**

Presentation of solutions and methods, critical discussion of own and others' results.

**Contents**

- Threat Actors
- Threat Intelligence
- Attack vector of Software Supply Chains
- Adversarial Machine Learning
- Prevention and mitigation strategies
- Regulations and compliance

**Prerequisites****Recommended:**

- MA-INF 3236 IT-Security
- MA-INF 4204 Technical Neural Nets

An understanding of the basic concepts of software development, artificial intelligence and IT security.

**Course meetings**

Teaching format	Group size	h/week	Workload[h]	CP	
Lecture		2	30 T / 45 S	2.5	T = face-to-face teaching S = independent study
Exercises		2	30 T / 75 S	3.5	

**Graded exams**

Written exam

**Ungraded coursework (required for admission to the exam)**

Participation in a performance test. At least 50% of the points must be achieved on this test.

---

## MA-INF 3322 Applied Binary Exploitation

Workload	Credit points	Duration	Frequency
180 h	6 CP	1 semester	every year
Module coordinator	Lecturer(s)		
Prof. Dr. Peter Martini	Prof. Dr. Elmar Padilla		
Programme	Mode	Semester	
M. Sc. Cyber Security	Optional	1-3.	

### Learning goals: technical skills

recognition of vulnerabilities in binary programs, static reverse engineering of binary programs (Ghidra, IDA Free, Linux command line tools), debugging of binary programs with gdb/pwndbg, Python programming with pwntools, application of exploit strategies such as overwriting return addresses/function pointers, return-oriented programming (ROP, SROP, ret2csu), shellcoding, glibc heap exploitation techniques (Use-After-Free, Unlink Exploit, House of Orange), understanding a complex real-world exploit, usage of git/GitLab and Docker for the exercises.

### Learning goals: soft skills

Frustration tolerance when working with binary representations and trying to apply taught techniques, focused working on technically challenging problems, simultaneously applying knowledge from different areas of computer science.

### Contents

This university course covers various topics related to software security and exploitation techniques. It starts with an introduction to finding vulnerabilities in C programs and binaries. The course then delves into stack-based buffer overflows and the mitigations used to prevent them. Students will also learn about circumventing these mitigations and explore return-oriented programming. The course continues with a focus on manual crafting of shellcode and understanding the internals of the glibc heap. Students will gain knowledge about heap exploitation techniques, including use-after-free exploits, heap unlink exploits, and the house of orange exploit. The course concludes with a complex case study on the Exim RCE exploit, providing students with a practical understanding of real-world vulnerabilities. Additionally, guest lectures will be held to provide further insights into the field of software security. Please note that basic skills in static and dynamic binary analysis (e. g. read disassembled/decompiled code or debug a binary program with gdb) are required to successfully participate in this lecture.

### Prerequisites

#### Recommended:

- Binary Analysis skills (as taught in the Bachelor's module BA-INF 155 Angewandte Binäranalyse; English slides available)
- Basic knowledge of the Linux operating system
- System Programming skills in C
- Basic Python programming skills

This module is best taken after or together with MA-INF 3239 Malware Analysis.

### Course meetings

Teaching format	Group size	h/week	Workload[h]	CP	
Lecture		2	30 T / 45 S	2.5	T = face-to-face teaching
Exercises		2	30 T / 75 S	3.5	S = independent study

### Graded exams

Oral Examination (30 minutes)

### Ungraded coursework (required for admission to the exam)

The completion of regularly provided exercise sheets. The work can be done in groups of up to three students. The exercises are divided into group tasks and tasks to be completed individually. For each category of tasks, at least 50% of the points must be achieved.

### Literature

The relevant literature will be announced at the beginning of the lecture

### 4.3 Computer Science Elective Modules – Algorithms

MA-INF 1103	L4E2	9 CP	Cryptography .....	28
MA-INF 1105	L2E2	6 CP	Algorithms for Data Analysis .....	29
MA-INF 1108	L2E2	6 CP	Introduction to High Performance Computing: Architecture Features and Practical Parallel Programming .....	30
MA-INF 1110	L2E2	6 CP	Elliptic Curves and their Applications in Cryptography .....	31
MA-INF 1209	Sem2	4 CP	Seminar Advanced Topics in Cryptography .....	33
MA-INF 1221	Lab4	9 CP	Lab Computational Analytics .....	34
MA-INF 1222	Lab4	9 CP	Lab High Performance Optimization .....	36
MA-INF 1223	L4E2	9 CP	Privacy Enhancing Technologies .....	38
MA-INF 1225	Lab4	9 CP	Lab Exploring HPC technologies .....	39
MA-INF 1309	Lab4	9 CP	Lab Efficient Algorithms: Design, Analysis and Implementation .....	41
MA-INF 1316	Lab4	9 CP	Lab Cryptography .....	43
MA-INF 1322	Sem2	4 CP	Seminar Focus Topics in High Performance Computing .....	44

## MA-INF 1103 Cryptography

Workload	Credit points	Duration	Frequency
270 h	9 CP	1 semester	every year
Module coordinator	Lecturer(s)		
Dr. Michael Nüsken	Dr. Michael Nüsken		
Programme	Mode	Semester	
M. Sc. Cyber Security	Optional	1. or 2.	

### Learning goals: technical skills

Understanding of security concerns and measures, and of the interplay between computing power and security requirements. Mastery of the basic techniques for cryptosystems and cryptanalysis, including modelling security and reducing security to basic assumptions.

### Learning goals: soft skills

Competences: Ability to assess, present and explain schemes and their use in applications, orally and written. Critical assessment of applications in terms of security, social and ethical context and more.

### Contents

Basic private-key and public-key cryptosystems: AES, RSA, group-based. Security reductions. Key exchange, cryptographic hash functions, signatures, identification; factoring integers and discrete logarithms; lower bounds in structured models.

### Prerequisites

#### Recommended:

Basics in elementary number theory, groups and complexity theory -in particular, reductions- are helpful.

### Course meetings

Teaching format	Group size	h/week	Workload[h]	CP	
Lecture		4	60 T / 105 S	5.5	T = face-to-face teaching
Exercises		2	30 T / 75 S	3.5	S = independent study

### Graded exams

Written exam (120 minutes)

### Ungraded coursework (required for admission to the exam)

The completion of regularly provided exercise sheets. Each student must present a solution to an exercise in the exercise sessions twice.

### Literature

- Jonathan Katz & Yehuda Lindell (2015/2008). Introduction to Modern Cryptography, CRC Press.
- Course notes

## MA-INF 1105 Algorithms for Data Analysis

Workload	Credit points	Duration	Frequency
180 h	6 CP	1 semester	at least every 2 years
Module coordinator	Lecturer(s)		
Prof. Dr. Petra Mutzel	Prof. Dr. Petra Mutzel		
Programme	Mode	Semester	
M. Sc. Cyber Security	Optional	1. or 2.	

### Learning goals: technical skills

Ability to independently design and analyze efficient algorithms and data structures, in particular using methods and techniques of modern algorithmics with respect to big data and/or analytics tasks;

### Learning goals: soft skills

Presentation of solutions and methods; critical discussion of applied methods and techniques clearly and in accordance with academic standards; ability to analyze problems theoretically and to find efficient as well as practical solutions; to examine one's solutions and results critically; to classify new problems into the state-of-the-art of the respective area;

### Contents

Advanced algorithmic techniques and data structures relevant to analytic tasks for big data, i.e., algorithms for efficiently computing centrality indices for networks, theoretical and practical approaches to graph similarity, parallel algorithms, external data structures, and streaming algorithms.

### Prerequisites

#### Recommended:

Essential is knowledge of:

- fundamental algorithms and algorithmic paradigms (e.g., graph algorithms, greedy algorithms, divide and conquer, dynamic programming), data structures (e.g., balanced search trees, hash tables)
- mathematical foundations of algorithm analysis (e.g., Big O notation, recurrence relations, proof techniques, running-time analysis)
- computational complexity (e.g., NP-hardness, reductions)

### Course meetings

Teaching format	Group size	h/week	Workload[h]	CP	
Lecture		2	30 T / 45 S	2.5	T = face-to-face teaching
Exercises		2	30 T / 75 S	3.5	S = independent study

### Graded exams

Oral exam (30 minutes)

### Ungraded coursework (required for admission to the exam)

It is necessary to pass one of two written tests during the semester. Moreover, the completion of regularly provided exercise sheets is required. The work can be done in groups. A total of 50% of the points must be achieved. Each student must present a solution to an exercise in the exercise sessions twice. At the beginning of each exercise session, all participants mark on a list which (sub)exercises they have completed successfully and for which they wish to receive credit. The tutor then selects, for each (sub)exercise, one participant to present it. For more complex exercises, a written solution is required, which can be uploaded during the presentation.

## MA-INF 1108 Introduction to High Performance Computing: Architecture Features and Practical Parallel Programming

Workload	Credit points	Duration	Frequency
180 h	6 CP	1 semester	every year
Module coordinator	Lecturer(s)		
Prof. Dr. Estela Suarez	Prof. Dr. Estela Suarez		
Programme	Mode	Semester	
M. Sc. Cyber Security	Optional	1. or 2.	

### Learning goals: technical skills

Understanding principles of computer architecture of modern HPC systems at component (processor, accelerators) and system level (system architecture, network, memory hierarchy) and their implication for application programming. Ability to program parallel computers, employing multi-core and multi-node features. Programming CPU and GPUs. Understanding the quality of performance and scaling behaviour, and applying the measures needed to improve them.

### Learning goals: soft skills

Critical assessment of hardware and applications in terms of performance and efficiency.

### Contents

- Computer architectures, system components (CPU, memory, network) and their interrelation.
- Software environment
- Access to HPC compute resources at the Jülich Supercomputing Centre
- Practical use of parallel programming paradigms (MPI, OpenMP, CUDA)
- Performance of applications and scaling behavior, understanding and strategies for improvement
- Current challenges in HPC

### Prerequisites

#### Required:

MA-INF 1108 replaces MA-INF 1106 and cannot be taken after completing MA-INF 1106.

#### Recommended:

Knowledge of a modern programming language (ideally C/C++ and Python) is required.

### Course meetings

Teaching format	Group size	h/week	Workload[h]	CP	
Lecture		2	30 T / 45 S	2.5	T = face-to-face teaching
Exercises		2	30 T / 75 S	3.5	S = independent study

### Graded exams

Written exam (90 minutes)

### Ungraded coursework (required for admission to the exam)

The completion of regularly provided exercise sheets. A total of 50% of the points must be achieved. Each student must present a solution to an exercise in the exercise sessions once.

### Forms of media

Laptop and projector

### Literature

- John L. Hennessy, David A. Patterson: Computer Architecture - A Quantitative Approach. Morgan Kaufmann Publishers, 2012
- David A. Patterson, John L. Hennessy: Computer Organization and Design - The Hardware / Software Interface. Morgan Kaufmann Publishers, 2013
- Message Passing Interface Forum: MPI: A Message-Passing Interface Standard, Version 3.1
- OpenMP Application Programming Interface, Version 4.5, November 2015

---

**MA-INF 1110 Elliptic Curves and their Applications in Cryptography**


---

Workload	Credit points	Duration	Frequency
180 h	6 CP	1 semester	every year
Module coordinator	Lecturer(s)		
Prof. Dr. Michael Meier	Dr. Gerhard Schabhüser		
Programme	Mode	Semester	
M. Sc. Cyber Security	Optional	1-3.	

**Learning goals: technical skills**

After completion of the modul students will understand the theory of elliptic Curves and their applications in cryptography. The students will learn, why elliptic curves have useful properties in Cryptography (at least as long as there are no powerful Quantum-Computers in place).

The relevant mathematical background will be developed and specific applications like ECC-Pseudo-Random-Number-Generators, ECC-Public-KC-Protocols and-Algorithms or Algorithms used in Cryptoanalysis will be presented.

In addition to the mathematical perspective the implementation-perspective especially concerning secure implementation will be addressed.

**Learning goals: soft skills**

Students will get the competence of understanding the mathematical background of elliptic curves, they will be sensible for the need of secure implementation of cryptographic algorithms and -protocols. They will be aware, that understanding the mathematics of cryptography has the capability to support secure implementation in cryptography their knowledge for secure implementation.

## Contents

### Algebraic Background

- algebraic Structures
- Introduction to Number theory
- Finite Fields

### Basic Arithmetic Algorithms.

- Exponentiation.
- Integer arithmetic.
- Finite fields arithmetic.

### Geometry und arithmetic of algebraic curves.

- Affine space.
- Projective space.

### Elliptic Curves.

- Arithmetic.
- Points of finite order.
- Group of rational points.

### Cubic curves over finite fields.

- Arithmetic.
- Rational points.
- A theorem of Gauß.
- Points of finite order (revisor).

### Elliptic curve cryptography.

- Factorisation of integers.
- Discrete logarithm.
- Diffie-Hellman-protocol.
- El-Gamal-signatures.
- EC-DSA.

### Implementing ECC-arithmetic.

- Timing attacks.
- Power consumption attacks.
- Secure implementations using Mathematics.

## Prerequisites

### Recommended:

Recommended : linear algebra, basic knowledge in algebra.

## Course meetings

Teaching format	Group size	h/week	Workload[h]	CP	
Lecture		2	30 T / 45 S	2.5	T = face-to-face teaching
Exercises		2	30 T / 75 S	3.5	S = independent study

## Graded exams

Oral exam (30 min).

## Ungraded coursework (required for admission to the exam)

Participation in one written achievement test. At least 50% of the points must be achieved.

## Literature

- Henri Cohen, Gerhard Frey et. al. (2005). Handbook of Elliptic and hyperelliptic Curve Cryptography.
- Joseph Silverman and John Tate. Rational Points on Elliptic Curves.
- Joseph Silverman. The Arithmetic of Elliptic Curves. 2nd Edition.

---

**MA-INF 1209 Seminar Advanced Topics in Cryptography**


---

Workload	Credit points	Duration	Frequency
120 h	4 CP	1 semester	every semester
Module coordinator	Lecturer(s)		
Dr. Michael Nüsken	Dr. Michael Nüsken		
Programme	Mode	Semester	
M. Sc. Cyber Security	Optional	2. or 3.	

**Learning goals: technical skills**

Enhanced and in-depth knowledge in specialized topics in the area of cryptography.

**Learning goals: soft skills**

Acquire the competence to independently search for and study state-of-the-art scientific literature in depth, read critically, identify the most relevant content, and assess research results in the context of cryptography; to discuss research results with a knowledgeable scientific audience; to present prior work by others in writing and in presentations with visual media at academic standards, well-structured and didactically effective, and motivate the audience to participate; to formulate and accept criticism; to manage one's time with relatively open assignments and long-ranging deadlines.

**Contents**

We discuss cutting-edge papers from current cryptographic research literature.

**Prerequisites**
**Recommended:**

Basic knowledge in cryptography is highly recommended, eg. by MA-INF 1103 – Cryptography.

**Course meetings**

Teaching format	Group size	h/week	Workload[h]	CP	
Seminar	10	2	30 T / 90 S	4	T = face-to-face teaching S = independent study

**Graded exams**

Oral presentation, written report

**Ungraded coursework (required for admission to the exam)**

Attendance in course sessions in accordance with the exam regulations of 2023, § 12(6).

**Literature**

Current cryptographic literature.

---

## MA-INF 1221 Lab Computational Analytics

Workload	Credit points	Duration	Frequency
270 h	9 CP	1 semester	every year
Module coordinator	Lecturer(s)		
Prof. Dr. Petra Mutzel	Prof. Dr. Petra Mutzel		
Programme	Mode	Semester	
M. Sc. Cyber Security	Optional	2. or 3.	

### Learning goals: technical skills

Ability to independently design, theoretically analyze, implement, and experimentally evaluate algorithms and efficient data structures for computational analytics problems; gain experience with software development techniques, tools and standards and the scientifically clean documentation of the students own work (including the written report and software).

### Learning goals: soft skills

- Knowledge of scientific approach to problem solving;
- ability to scientifically present solutions and methods;
- critical discussion of applied methods and techniques clearly and in accordance with academic standards;
- ability to analyze problems theoretically and to find efficient as well as practical solutions;
- to examine one's solutions and results critically;
- to classify new problems into the state-of-the-art of the respective area.

### Contents

We will design efficient exact and approximate algorithms and data structures for computational analytics problems. We study a (set of) selected combinatorial optimization problem(s) with the goal to design new algorithmic approaches. Often, we focus on solving (graph) problems for selected applications (e.g., in cartography, geodesy, neurosciences, chemistry, or others). Typically, we start with a literature search on State-of-the-Art approaches; based on that, we adapt selected approaches

to our studied problem(s) or we design new approaches. We then theoretically analyze and implement our adapted/new algorithms. This is followed by an extensive experimental evaluation including a discussion of the results on benchmark instances. Often, the analysis triggers improvements of the algorithms. This is also called the Algorithm Engineering cycle.

### Prerequisites

#### Recommended:

Essential are knowledge of:

- fundamental algorithms and algorithmic paradigms (e.g., graph algorithms, greedy algorithms, divide and conquer, dynamic programming), data structures (e.g., balanced search trees, hash tables)
- mathematical foundations of algorithm analysis (e.g., Big O notation, recurrence relations, proof techniques, running-time analysis)
- computational complexity (e.g., NP-hardness, reductions).

It is recommended to first complete at least one of the following modules:

- MA-INF 1105 Algorithms for Data Analysis
- MA-INF 1201 Approximation Algorithms
- MA-INF 1203 Discrete and Computational Geometry
- MA-INF 1213 Randomized Algorithms and Probabilistic Analysis
- MA-INF 1218 Algorithms and Uncertainty
- MA-INF 1301 Algorithmic Game Theory
- MA-INF 4112 Algorithms for Data Science

### Course meetings

Teaching format	Group size	h/week	Workload[h]	CP
Lab	8	4	60 T / 210 S	9

T = face-to-face teaching  
S = independent study

### Graded exams

Oral presentation, written report

**Ungraded coursework (required for admission to the exam)**

Project work; attendance in course sessions in accordance with the exam regulations of 2023, § 12(6).

**Literature**

The relevant literature will be announced in time.

---

## MA-INF 1222 Lab High Performance Optimization

Workload	Credit points	Duration	Frequency
270 h	9 CP	1 semester	every year
Module coordinator	Lecturer(s)		
Prof. Dr. Petra Mutzel	Prof. Dr. Petra Mutzel, Gayatri Manda		
Programme	Mode	Semester	
M. Sc. Cyber Security	Optional	2. or 3.	

### Learning goals: technical skills

- Ability to independently design, theoretically analyze, implement, and experimentally evaluate algorithms and efficient data structures for computational analytics problems;
- understanding and using parallel programming paradigms and high-level programming languages;
- using performance analysis tools, understanding performance bottlenecks and measures to improve them;
- acquisition of knowledge about software development and standards;
- gain experience with the documentation of the students own work (including the written report and software);

### Learning goals: soft skills

- Knowledge of scientific approach to problem solving;
- ability to scientifically present solutions and methods;
- critical discussion of applied methods and techniques clearly and in accordance with academic standards;
- ability to analyze problems theoretically and to find efficient as well as practical solutions;
- to examine one's solutions and results critically;
- to classify new problems into the state-of-the-art of the respective area;

### Contents

We will design efficient exact and approximate algorithms and data structures for optimization problems on big data with the focus of using high performance computing (HPC) systems (like, e.g. the HPC clusters Marvin or Bender). We study a (set of) selected optimization problem(s) with the goal to design new parallel algorithms that scale well on HPC systems. Often, we focus on solving (graph) problems for selected applications (e.g., physics, chemistry, neurosciences, geodesy, or others).

Typically, we start with an introduction into parallel algorithms and an introduction into the relevant API for developing parallel programs. A literature search yields State-of-the-Art techniques; based on that, we adapt selected approaches to our studied problem(s) or we design new approaches with the goal that they scale well on HPC systems. We then theoretically analyze and implement our adapted/new parallel algorithms using parallel programming paradigms and high-level programming languages. This is followed by an extensive experimental evaluation using performance analysis tools and understanding performance bottlenecks. Often, this triggers improvements of the parallel algorithms and/or the implementation.

### Prerequisites

#### Recommended:

Essential are knowledge of:

- fundamental algorithms and algorithmic paradigms (e.g., graph algorithms, greedy algorithms, divide and conquer, dynamic programming), data structures (e.g., balanced search trees, hash tables)
- mathematical foundations of algorithm analysis (e.g., Big O notation, recurrence relations, proof techniques, running-time analysis)
- computational complexity (e.g., NP-hardness, reductions)

It is recommended to complete at least one the following modules first:

- MA-INF 1105 Algorithms for Data Analysis
- MA-INF 1108 Introduction to High Performance Computing: Architecture Features and Practical Parallel Programming
- MA-INF 1201 Approximation Algorithms
- MA-INF 1203 Discrete and Computational Geometry
- MA-INF 1213 Randomized Algorithms and Probabilistic Analysis
- MA-INF 1218 Algorithms and Uncertainty
- MA-INF 1301 Algorithmic Game Theory

**Course meetings**

Teaching format	Group size	h/week	Workload[h]	CP
Lab	8	4	60 T / 210 S	9

T = face-to-face teaching  
S = independent study

**Graded exams**

Oral presentation, written report

**Ungraded coursework (required for admission to the exam)**

Project work; attendance in course sessions in accordance with the exam regulations of 2023, § 12(6).

**Literature**

The relevant literature will be announced in time.

---

# MA-INF 1223 Privacy Enhancing Technologies

Workload	Credit points	Duration	Frequency
270 h	9 CP	1 semester	every year
Module coordinator	Lecturer(s)		
Dr. Michael Nüsken	Dr. Michael Nüsken		
Programme	Mode	Semester	
M. Sc. Cyber Security	Optional	2. or 3.	

**Learning goals: technical skills**

Knowledge: Cryptographic schemes for enhancing privacy, underlying security notions, applications and restrictions.  
 Skills: Secure application of sophisticated cryptographic schemes. Evaluation of their correctness, efficiency and security in an application setting.

**Learning goals: soft skills**

Competences: Ability to assess, present and explain schemes and their use in applications, orally and written.  
 Critical assessment of applications in terms of security, social and ethical context and more.

**Contents**

With more and more data available a clear separation of sensitive data is necessary and needs to be protected. Some of that data must stay within strict environments, for examples hospitals must store certain highly sensitive medical information about patients but they are not allowed to store it outside its own facilities. Some of that data is stored or collected in a cloud environment in encrypted form, say data from a medical device or a smart home. But it shall still be possible to derive important conclusions from it, for example to send immediate help to a patient suffering a heart attack.

Innovative solutions are needed in this area of tension. The research in cryptography provides some highly sophisticated tools for solving the like problems.

- Fully homomorphic encryption (FHE).
- Zero-Knowledge techniques, in particular: Non-interactive zero-knowledge proof (NIZKs).
- Secure multi-party computations (MPC).
- Anonymisation, TOR. Pseudonymization. Blinding.
- Weaker privacy notions, like differential privacy.

**Prerequisites**

**Recommended:**

Basic knowledge in cryptography (for example from MA-INF 1103) is highly recommended.

A profound mathematical background does help. In particular, precise mathematical formulation and reasoning are important, but also topics like elementary number theory and discrete mathematics, especially lattices, are interesting.

**Course meetings**

Teaching format	Group size	h/week	Workload[h]	CP	
Lecture		4	60 T / 105 S	5.5	T = face-to-face teaching S = independent study
Exercises		2	30 T / 75 S	3.5	

**Graded exams**

Written exam (120 minutes)

**Ungraded coursework (required for admission to the exam)**

The completion of regularly provided exercise sheets. Each student must present twice in the tutorial.

## MA-INF 1225 Lab Exploring HPC technologies

Workload	Credit points	Duration	Frequency
270 h	9 CP	1 semester	at least every 2 years
Module coordinator	Lecturer(s)		
Prof. Dr. Estela Suarez	Prof. Dr. Estela Suarez		
Programme	Mode	Semester	
M. Sc. Cyber Security	Optional	2. or 3.	

### Learning goals: technical skills

Understanding a use case from complex code developed. Adapting and running applications to different kinds of processing units, taking into account their specific architecture characteristic and programming environments. Understanding and using parallel programming paradigms and high-level programming languages. Designing and executing a benchmarking campaign. Using performance analysis tools, understanding performance bottlenecks and measures to improve them. Software development skills and standards.

### Learning goals: soft skills

Ability to analyze computational problems and to find creative and practical solutions; to examine one's solutions and results critically; to classify one's own results into the state-of-the-art of the respective area; to produce good quality software, prepare readable documentation of software and research results; to present, defend and discuss design decisions and results in the team/group and to other students clearly and in accordance with academic standards; to aim at long-range goals under limited resources; to work under pressure.

### Contents

The students carry out a practical task (project) in High Performance Computing (HPC), including test of different hardware architectures and software tools, documentation of the implemented software/system. Contents might be adapted to a specific topic focus on different semesters. Example areas of work are: HPC systems: access/use of compute resources; Use or simulation of different processor architectures; Software environment, performance analysis tools; Parallel programming; Benchmarking tools/procedures; Performance of applications and scaling behavior, strategies for improvement; Studying relation between architecture and application performance. Detailed information on semester-specific focus topics will be given over the course website.

### Prerequisites

#### Recommended:

- Knowledge of modern programming languages (C/C++, Python).
- Willingness to stay for at least 2 days per week during 4 weeks at the Jülich Supercomputing Centre, dates to be discussed.
- Interest in High Performance Computing
- Recommended: Passed the exam of MA-INF 1108 Introduction to High Performance Computing: Architecture Features and Practical Parallel Programming (or its precursor MA-INF 1106).

### Remarks

Registration first via direct mail communication with the lecturer, in order to identify level of previous knowledge and suitable dates for the stay at JSC.

### Course meetings

Teaching format	Group size	h/week	Workload[h]	CP	
Lab	2	4	60 T / 210 S	9	T = face-to-face teaching S = independent study

### Graded exams

Oral presentation, written report

### Ungraded coursework (required for admission to the exam)

Project work; attendance in course sessions in accordance with the exam regulations of 2023, § 12(6).

**Forms of media**

Own laptop to connect and program on workstation or supercomputers.

**Literature**

- John L. Hennessy, David A. Patterson: Computer Architecture - A Quantitative Approach. Morgan Kaufmann Publishers, 2012
  - David A. Patterson, John L. Hennessy: Computer Organization and Design - The Hardware / Software Interface. Morgan Kaufmann Publishers, 2013
  - Message Passing Interface Forum: MPI: A Message-Passing Interface Standard, Version 3.1
  - OpenMP Application Programming Interface, Version 4.5, November 2015
  - Further semester-specific literature will be announced in the lab website.
-

## MA-INF 1309 Lab Efficient Algorithms: Design, Analysis and Implementation

Workload	Credit points	Duration	Frequency
270 h	9 CP	1 semester	at least every year

Module coordinator	Lecturer(s)
Prof. Dr. Heiko Röglin	Prof. Dr. Anne Driemel, Prof. Dr. Thomas Kesselheim, Prof. Dr. Heiko Röglin, PD Dr. Elmar Langetepe, Dr. Herman Haverkort

Programme	Mode	Semester
M. Sc. Cyber Security	Optional	1-3.

### Learning goals: technical skills

Ability to independently design, analyze and implement efficient algorithms and data structures for selected computational problems

### Learning goals: soft skills

Ability to analyze problems theoretically and to find creative and practical solutions; to examine one's solutions and results critically; to classify one's own results into the state-of-the-art of the respective area; to prepare readable documentation of software and research results; to present, defend and discuss design decisions and results in the team/group and to other students clearly and in accordance with academic standards; to collaborate constructively with others in small teams over a longer period of time; to aim at long-range goals under limited resources; to work under pressure.

### Contents

Design of efficient exact and approximate algorithms and data structures for selected computational problems.

### Prerequisites

#### Recommended:

Knowledge of:

- fundamental algorithms and algorithmic paradigms (e.g., graph algorithms, greedy algorithms, divide and conquer, dynamic programming), data structures (e.g., balanced search trees, hash tables)
- mathematical foundations of algorithm analysis (e.g., Big O notation, recurrence relations, proof techniques, running-time analysis)
- computational complexity (e.g., NP-hardness, reductions)

It is recommended to take at least one of the following modules first:

- MA-INF 1102 Combinatorial Optimization
- MA-INF 1103 Cryptography
- MA-INF 1105 Algorithms for Data Analysis
- MA-INF 1107 Foundations of Quantum Computing
- MA-INF 1108 Introduction to High-Performance Computing: Architecture Features and Practical Parallel Programming
- MA-INF 1201 Approximation Algorithms
- MA-INF 1202 Chip Design
- MA-INF 1203 Discrete and Computational Geometry
- MA-INF 1213 Randomized Algorithms and Probabilistic Analysis
- MA-INF 1218 Algorithms and Uncertainty
- MA-INF 1227 Hardness of Approximation
- MA-INF 1301 Algorithmic Game Theory
- MA-INF 1314 Online Motion Planning
- MA-INF 1323 Computational Topology

### Course meetings

Teaching format	Group size	h/week	Workload[h]	CP
Lab	8	4	60 T / 210 S	9

T = face-to-face teaching  
S = independent study

---

**Graded exams**

Oral presentation, written report

---

**Ungraded coursework (required for admission to the exam)**

Project work; attendance in course sessions in accordance with the exam regulations of 2023, § 12(6).

---

**Literature**

The relevant literature will be announced in time.

---

## MA-INF 1316 Lab Cryptography

Workload	Credit points	Duration	Frequency
270 h	9 CP	1 semester	every year
Module coordinator	Lecturer(s)		
Dr. Michael Nüsken	Dr. Michael Nüsken		
Programme	Mode	Semester	
M. Sc. Cyber Security	Optional	2. or 3.	

### Learning goals: technical skills

The students will carry out a practical task (project) in the context of Cryptography, including test and documentation of the implemented software/system.

### Learning goals: soft skills

Ability to properly present and defend design decisions, to prepare readable documentation of software; skills in constructively collaborating with others in small teams over a longer period of time; ability to classify ones own results into the state-of-the-art of the resp. area.

### Contents

Front of research topics in cryptography, in particular, related to fully homomorphic encryption, multi-party computation, automated security verification.

The target of the lab is to understand how cryptography may work in one particular application that we are choosing together. Ideally, we can come up with a novel solution for performing an unconsidered algorithm. We study the tasks and tools, select algorithms, find a protocol, prototype an implementation, perform a security analysis, present an evaluation.

### Prerequisites

#### Recommended:

Good knowledge in cryptography is vital, eg. by

- MA-INF 1103 - Cryptography
- MA-INF 1223 - Privacy Enhancing Technologies
- MA-INF 1209 - Seminar Advanced Topics in Cryptography.

### Course meetings

Teaching format	Group size	h/week	Workload[h]	CP	
Lab	8	4	60 T / 210 S	9	T = face-to-face teaching S = independent study

### Graded exams

Oral presentation, written report

### Ungraded coursework (required for admission to the exam)

Project work; attendance in course sessions in accordance with the exam regulations of 2023, § 12(6).

## MA-INF 1322 Seminar Focus Topics in High Performance Computing

Workload	Credit points	Duration	Frequency
120 h	4 CP	1 semester	every year
Module coordinator	Lecturer(s)		
Prof. Dr. Estela Suarez	Prof. Dr. Estela Suarez		
Programme	Mode	Semester	
M. Sc. Cyber Security	Optional	2. or 3.	

### Learning goals: technical skills

Enhanced and in-depth knowledge on topics and trends in the area of high performance computing.

### Learning goals: soft skills

Acquire the competence to independently search for and study state-of-the-art scientific literature in depth, read critically, identify the most relevant content, and assess research results in the context of the corresponding research area; to execute peer-review processes, both to review work from others and to write rebuttal letters to reply reviewer reports; to discuss research results with a knowledgeable scientific audience; to present prior work by others in writing and in presentations with visual media in a way that adheres to academic standards, that is well-structured and didactically effective, and that motivates the audience to participate; to formulate and accept criticism; to manage one's time with relatively open assignments and long-ranging deadlines.

### Contents

General topics and trends in high performance computing, based on recent review and research literature

### Prerequisites

#### Recommended:

MA-INF 1108 Introduction to High Performance Computing: Architecture Features and Practical Parallel Programming

### Course meetings

Teaching format	Group size	h/week	Workload[h]	CP	
Seminar	10	2	30 T / 90 S	4	T = face-to-face teaching S = independent study

### Graded exams

Oral presentation, written report

### Ungraded coursework (required for admission to the exam)

Attendance in course sessions in accordance with the exam regulations of 2023, § 12(6).

### Literature

Literature and further information about this seminar will be announced in time in the website of lecturer.

## 4.4 Computer Science Elective Modules – Graphics, Vision, Audio

MA-INF 2113	L2E2	6 CP	Foundations of Audio Signal Processing .....	46
MA-INF 2201	L4E2	9 CP	Computer Vision .....	47
MA-INF 2202	L4E2	9 CP	Computer Animation .....	48
MA-INF 2208	Sem2	4 CP	Seminar Audio .....	49
MA-INF 2212	L2E2	6 CP	Pattern Matching and Machine Learning for Audio Signal Processing ....	50
MA-INF 2213	L3E1	6 CP	Advanced Computer Vision .....	51
MA-INF 2216	Lab4	9 CP	Lab Visual Computing .....	52
MA-INF 2219	Sem2	4 CP	Seminar Visualization and Medical Image Analysis .....	53
MA-INF 2220	Lab4	9 CP	Lab Visualization and Medical Image Analysis .....	54
MA-INF 2222	L4E2	9 CP	Visual Data Analysis .....	55
MA-INF 2225	L2E2	6 CP	Discrete Models for Visual Computing .....	56
MA-INF 2226	Lab4	9 CP	Lab Geometry Processing .....	57
MA-INF 2227	Lab4	9 CP	Lab 3D Animation .....	58
MA-INF 2308	Lab4	9 CP	Lab Graphics .....	59
MA-INF 2309	Lab4	9 CP	Lab Audio .....	60
MA-INF 2317	L2E2	6 CP	Numerical Algorithms for Visual Computing and Machine Learning .....	61

## MA-INF 2113 Foundations of Audio Signal Processing

Workload	Credit points	Duration	Frequency
180 h	6 CP	1 semester	every year
Module coordinator	Lecturer(s)		
apl. Prof. Dr. Frank Kurth	apl. Prof. Dr. Frank Kurth, Prof. Dr. Michael Clausen		
Programme	Mode	Semester	
M. Sc. Cyber Security	Optional	1. or 2.	

### Learning goals: technical skills

- Introduction to basic concepts of analog and digital signal processing: Acquire basic knowledge on modeling and representing audio content; learn fundamental concepts of analog and digital signal processing, in particular mathematical models of signal spaces and apply them to the audio domain; learn methods for analog to digital conversion, frequency analysis, time-frequency analysis and digital filtering.
- Applications in the field of Audio Signal Processing: Learn typical application domains of audio signal processing techniques and how to apply the acquired methods in solving applications problems from those domains. Important examples are basic signal manipulation and filtering.
- Solving basic Signal Processing Problems: Learn basic signal processing algorithms for performing the Fourier Transform and a time-frequency analysis, as well as for performing filter operations and fundamental types of signal manipulations.
- Implementing basic Signal Processing Algorithms using state-of-the-art software frameworks: In the exercises, the introduced methods and algorithms have to be implemented and applied to basic applications problems. Hence knowledge in the practical implementation of digital signal processing methods in standard programming environments such as Python, Matlab or Octave is acquired.

### Learning goals: soft skills

Capability to analyze; Time management; Presentation skills; Discussing own solutions and solutions of others, and working in groups.

### Contents

Theoretical introduction to analog and digital Signal Processing; Fourier Transforms; Analog to digital Conversion; Digital Filters; Audio Signal Processing Applications; Filter banks; Windowed Fourier Transform; 2D-Signal Processing

### Prerequisites

#### Recommended:

Solid basic knowledge on Linear Algebra and Analysis on the level acquired in Bachelor in Computer Science programmes, including proficiency in using complex numbers.

### Course meetings

Teaching format	Group size	h/week	Workload[h]	CP	
Lecture		2	30 T / 45 S	2.5	T = face-to-face teaching S = independent study
Exercises		2	30 T / 75 S	3.5	

### Graded exams

Written exam (120 minutes)

### Ungraded coursework (required for admission to the exam)

The completion of regularly provided exercise sheets. The work can be done in groups of two to four students. A total of 50% of the points must be achieved.

### Forms of media

Slides, Blackboard, Whiteboard

## MA-INF 2201 Computer Vision

Workload	Credit points	Duration	Frequency
270 h	9 CP	1 semester	every year
Module coordinator	Lecturer(s)		
Prof. Dr. Jürgen Gall	Prof. Dr. Jürgen Gall		
Programme	Mode	Semester	
M. Sc. Cyber Security	Optional	1. or 2.	

### Learning goals: technical skills

Students will be able to understand and explain mathematical descriptions of methods in publications from Computer Vision. Students will be able to implement the discussed Computer Vision algorithms, apply them, and choose the right approach and hyper-parameters for a given problem.

### Learning goals: soft skills

Productive work in small teams, development and realization of individual approaches and solutions, critical reflection of competing methods, discussion in groups.

### Contents

The class will cover a number of mathematical methods and their applications in computer vision. For example, linear filters, edges, derivatives, Hough transform, segmentation, graph cuts, mean shift, active contours, level sets, MRFs, expectation maximization, background subtraction, temporal filtering, active appearance models, shapes, optical flow, 2d tracking, cameras, 2d/3d features, stereo, 3d reconstruction, 3d pose estimation, articulated pose estimation, deformable meshes, RGBD vision.

### Prerequisites

#### Recommended:

Basic knowledge of linear algebra, analysis, probability theory, Python programming

### Course meetings

Teaching format	Group size	h/week	Workload[h]	CP	
Lecture		4	60 T / 105 S	5.5	T = face-to-face teaching S = independent study
Exercises		2	30 T / 75 S	3.5	

### Graded exams

Written exam (120 minutes)

### Ungraded coursework (required for admission to the exam)

The completion of regularly provided exercise sheets. The work can be done in groups of up to two students. A total of 50% of the points must be achieved.

### Literature

- R. Hartley, A. Zisserman: Multiple View Geometry in Computer Vision
- R. Szeliski: Computer Vision: Algorithms and Applications
- S. Prince: Computer Vision: Models, Learning, and Inference

## MA-INF 2202 Computer Animation

Workload	Credit points	Duration	Frequency
270 h	9 CP	1 semester	every year
Module coordinator	Lecturer(s)		
Prof. Dr. Björn Krüger	Prof. Dr. Björn Krüger		
Programme	Mode	Semester	
M. Sc. Cyber Security	Optional	1-3.	

### Learning goals: technical skills

Students will learn fundamental paradigms used in computer animation. They will learn the mathematical foundations and basic algorithms to solve problems in the areas of motion capturing, motion synthesis, and motion analysis.

### Learning goals: soft skills

Social competences (work in groups), communicative skills (written and oral presentation)

### Contents

Fundamentals of computer animation; kinematics; representations of motions; motion capturing; motion editing; motion synthesis; facial animations

### Prerequisites

#### Recommended:

Basic knowledge of linear algebra, analysis, Matlab and Python

### Course meetings

Teaching format	Group size	h/week	Workload[h]	CP	
Lecture		4	60 T / 105 S	5.5	T = face-to-face teaching
Exercises		2	30 T / 75 S	3.5	S = independent study

### Graded exams

Oral exam (30 minutes)

### Ungraded coursework (required for admission to the exam)

The completion of regularly provided exercise sheets. The work can be done in groups of up to three students. A total of 50% of the points must be achieved.

### Literature

- Dietmar Jackel, Stephan Neunreither, Friedrich Wagner: Methoden der Computeranimation, Springer 2006
- Rick Parent: Computer Animation: Algorithms and Techniques, Morgan Kaufman Publishers 2002
- Frederic I. Parke, Keith Waters: Computer Facial Animation. A K Peters, Ltd. 199
- Grünvogel Stefan, Einführung in die Computer Animation, Springer 2024

---

**MA-INF 2208 Seminar Audio**


---

Workload	Credit points	Duration	Frequency
120 h	4 CP	1 semester	every year

Module coordinator	Lecturer(s)
apl. Prof. Dr. Frank Kurth	apl. Prof. Dr. Frank Kurth, Dr. Michael Clausen

Programme	Mode	Semester
M. Sc. Cyber Security	Optional	2. or 3.

**Learning goals: technical skills**

Ability to understand new research results presented in original scientific papers.

**Learning goals: soft skills**

Ability to present and to critically discuss these results in the framework of the corresponding area.

**Contents**

Current conference and journal papers in the area of audio signal processing.

**Prerequisites**
**Recommended:**

MA-INF 2113 - Audio Signal Processing

**Course meetings**

Teaching format	Group size	h/week	Workload[h]	CP	
Seminar	10	2	30 T / 90 S	4	T = face-to-face teaching S = independent study

**Graded exams**

Oral presentation, written report

**Ungraded coursework (required for admission to the exam)**

Attendance in course sessions in accordance with the exam regulations of 2023, § 12(6).

---

# MA-INF 2212 Pattern Matching and Machine Learning for Audio Signal Processing

<b>Workload</b>	<b>Credit points</b>	<b>Duration</b>	<b>Frequency</b>
180 h	6 CP	1 semester	every year
<b>Module coordinator</b>	<b>Lecturer(s)</b>		
apl. Prof. Dr. Frank Kurth	apl. Prof. Dr. Frank Kurth		
<b>Programme</b>	<b>Mode</b>	<b>Semester</b>	
M. Sc. Cyber Security	Optional	2. or 3.	

**Learning goals: technical skills**

- Introduction into selected topics of digital signal processing: Acquire basic knowledge on representing and manipulating 1D-time series. Learn basic methods for time-frequency analysis and signal processing methods for feature extraction.
- Applications in the field of Audio Signal Processing: Learn typical application domains of audio signal processing techniques and how to apply the acquired methods in solving applications problems. Important examples are filtering, signal/object detection and classification tasks.
- Methods of Automatic Pattern Recognition and Machine Learning: Learn methods for Feature Extraction, Automatic Pattern Recognition and Machine Learning for the context of Audio Signal Processing. Be able to apply those fundamental methods (method list: see "Contents" section) in particular for solving applications tasks.

**Learning goals: soft skills**

Audio Signal Processing Applications; Extended programming skills for signal processing applications; Capability to analyze; Time management; Presentation skills; Discussing own solutions and solutions of others, and working in groups.

**Contents**

The lecture is presented in modular form, where each module is motivated from the application side. The presented topics are: Windowed Fourier transforms; Audio Identification; Audio Matching; Signal Classification; Applications of ML/DL concepts, in particular HMMs, SVMs and Neural Networks to Audio Signal processing tasks.

**Prerequisites**

**Recommended:**

Solid basic knowledge on Linear Algebra, Analysis and Stochastics, including proficiency in using complex numbers. Having attended MA-INF 2113 Foundations of Audio Signal Processing is highly recommended, as fundamental material from (Digital) Signal Processing and Audio Processing are introduced there in depth. Basic knowledge in time series data analysis is helpful but not mandatory.

**Course meetings**

Teaching format	Group size	h/week	Workload[h]	CP	
Lecture		2	30 T / 45 S	2.5	T = face-to-face teaching S = independent study
Exercises		2	30 T / 75 S	3.5	

**Graded exams**

Written exam (120 minutes)

**Ungraded coursework (required for admission to the exam)**

The completion of regularly provided exercise sheets. The work can be done in groups of two to four students. A total of 50% of the points must be achieved.

**Forms of media**

Slides, Blackboard, Whiteboard

---

**MA-INF 2213 Advanced Computer Vision**


---

Workload	Credit points	Duration	Frequency
180 h	6 CP	1 semester	every year
Module coordinator	Lecturer(s)		
Prof. Dr. Jürgen Gall	Prof. Dr. Jürgen Gall		
Programme	Mode	Semester	
M. Sc. Cyber Security	Optional	2. or 3.	

**Learning goals: technical skills**

Students will be able to implement the discussed machine learning algorithms for Computer Vision, apply them, and choose the right approach and hyper-parameters for a given problem.

**Learning goals: soft skills**

Productive work in small teams, development and realization of individual approaches and solutions, critical reflection of competing methods, discussion in groups.

**Contents**

The class will cover a number of computer vision applications. For example, image classification, object detection, action recognition, pose estimation, face analysis, tracking, image synthesis, vision-language models.

**Prerequisites**
**Recommended:**

MA-INF 2201 – Computer Vision

**Course meetings**

Teaching format	Group size	h/week	Workload[h]	CP	
Lecture		3	45 T / 45 S	3	T = face-to-face teaching S = independent study
Exercises		1	15 T / 75 S	3	

**Graded exams**

Oral exam (20 minutes)

**Ungraded coursework (required for admission to the exam)**

The completion of regularly provided exercise sheets. The work can be done in groups of up to two students. A total of 50% of the points must be achieved.

---

## MA-INF 2216 Lab Visual Computing

Workload	Credit points	Duration	Frequency
270 h	9 CP	1 semester	every year
Module coordinator	Lecturer(s)		
Prof. Dr. Florian Bernard	Prof. Dr. Florian Bernard		
Programme	Mode	Semester	
M. Sc. Cyber Security	Optional	2. or 3.	

### Learning goals: technical skills

- Getting into a selected topic of visual computing
- Implementation and practical application of current visual computing methods
- Experimental evaluation and visualisation of results
- Scientific research and writing

### Learning goals: soft skills

- self-organisation
- ability to analyze problems theoretically and to find creative and practical solutions
- critical thinking: examine one's solutions and results critically
- to classify own results into the state-of-the-art of the respective area
- to prepare readable documentation of software and research results
- to present, defend and discuss design decisions and results in the team/group and to other students clearly and in accordance with academic standards

### Contents

This lab introduces visual computing methods and applications. You will get a chance to study the methods in depth by implementing them and running experiments. At the end of the semester, you will present the method, give a short demonstration and hand in a report describing the method and experimental outcomes. Potential topics include deep learning (e.g. graph neural networks, unsupervised learning, 3D deep learning), mathematical optimization (e.g. linear/convex/non-convex programming, graph-based algorithms) and other methods involving mathematical modeling of visual computing problems.

### Prerequisites

#### Recommended:

Basic knowledge in mathematics (e.g. linear algebra, calculus, optimization) and programming (e.g. python, in particular pytorch or tensorflow, C++, or Matlab). In addition:

- MA-INF 2317: Numerical Algorithms for Visual Computing and Machine Learning, or
- MA-INF 2225: Discrete Models for Visual Computing

### Course meetings

Teaching format	Group size	h/week	Workload[h]	CP	
Lab	8	4	60 T / 210 S	9	T = face-to-face teaching S = independent study

### Graded exams

Oral presentation, written report

### Ungraded coursework (required for admission to the exam)

Project work; attendance in course sessions in accordance with the exam regulations of 2023, § 12(6).

## MA-INF 2219 Seminar Visualization and Medical Image Analysis

Workload	Credit points	Duration	Frequency
120 h	4 CP	1 semester	at least every 2 years
Module coordinator	Lecturer(s)		
Prof. Dr. Thomas Schultz	Prof. Dr. Thomas Schultz		
Programme	Mode	Semester	
M. Sc. Cyber Security	Optional	2. or 3.	

### Learning goals: technical skills

Enhanced and in-depth knowledge in specialized topics in the area of visualization and medical image analysis.

### Learning goals: soft skills

Acquire the competence to independently search for and study state-of-the-art scientific literature in depth, read critically, identify the most relevant content, and assess research results in the context of the corresponding research area; to discuss research results with a knowledgeable scientific audience; to present prior work by others in writing and in presentations with visual media in a way that adheres to academic standards, that is well-structured and didactically effective, and that motivates the audience to participate; to formulate and accept criticism; to manage one's time with relatively open assignments and long-ranging deadlines.

### Contents

Recent research topics in visualization and medical image analysis based on journal and conference publications. Relevant journals include Medical Image Analysis, IEEE Transactions on Medical Imaging, IEEE Transactions on Visualization and Computer Graphics; relevant conferences include Medical Image Computing and Computer-Assisted Intervention (MICCAI), IEEE/CVF Computer Vision and Pattern Recognition (CVPR) IEEE VIS, EuroVis.

### Prerequisites

#### Recommended:

At least one of the following:

- MA-INF 2222 – Visual Data Analysis
- MA-INF 2312 – Image Acquisition and Analysis in Neuroscience

### Course meetings

Teaching format	Group size	h/week	Workload[h]	CP	
Seminar	10	2	30 T / 90 S	4	T = face-to-face teaching S = independent study

### Graded exams

Oral presentation, written report

### Ungraded coursework (required for admission to the exam)

Attendance in course sessions in accordance with the exam regulations of 2023, § 12(6).

## MA-INF 2220 Lab Visualization and Medical Image Analysis

Workload	Credit points	Duration	Frequency
270 h	9 CP	1 semester	every year
Module coordinator	Lecturer(s)		
Prof. Dr. Thomas Schultz	Prof. Dr. Thomas Schultz		
Programme	Mode	Semester	
M. Sc. Cyber Security	Optional	2. or 3.	

### Learning goals: technical skills

Students acquire a deep understanding of a specific problem in visualization and medical image analysis, and technical knowledge about state-of-the-art algorithmic approaches to solving it. This involves problem identification; data processing; selection, design, implementation, and application of suitable algorithms; communication of results.

### Learning goals: soft skills

Ability to analyze problems theoretically and to find creative and practical solutions; to examine one's solutions and results critically; to classify one's own results into the state-of-the-art of the respective area; to prepare readable documentation of software and research results; to present, defend and discuss design decisions and results in the team/group and to other students clearly and in accordance with academic standards; to collaborate constructively with others in small teams over a longer period of time; to aim at long-range goals under limited resources.

### Contents

The students will carry out a practical task (project) in the context of data visualization and visual analytics or medical image analysis, including test and documentation of the implemented software/system. Projects are often based on journal and conference publications. Relevant journals include Medical Image Analysis, IEEE Transactions on Medical Imaging, IEEE Transactions on Visualization and Computer Graphics; relevant conferences include Medical Image Computing and Computer-Assisted Intervention (MICCAI), IEEE/CVF Computer Vision and Pattern Recognition (CVPR) IEEE VIS, EuroVis.

### Prerequisites

#### Recommended:

At least one of the following:

- MA-INF 2222 – Visual Data Analysis
- MA-INF 2312 – Image Acquisition and Analysis in Neuroscience.

A solid background in programming is required, preferably in Python. Most projects also require basic knowledge in linear algebra, calculus, probability theory, and/or numerical algorithms.

### Course meetings

Teaching format	Group size	h/week	Workload[h]	CP	
Lab	8	4	60 T / 210 S	9	T = face-to-face teaching S = independent study

### Graded exams

Oral presentation, written report

### Ungraded coursework (required for admission to the exam)

Project work; attendance in course sessions in accordance with the exam regulations of 2023, § 12(6).

## MA-INF 2222 Visual Data Analysis

Workload	Credit points	Duration	Frequency
270 h	9 CP	1 semester	every year
Module coordinator	Lecturer(s)		
Prof. Dr. Thomas Schultz	Prof. Dr. Thomas Schultz		
Programme	Mode	Semester	
M. Sc. Cyber Security	Optional	1. or 2.	

### Learning goals: technical skills

Ability to design, implement, and make proper use of systems for visual data analysis. Knowledge of algorithms and techniques for the visualization of multi-dimensional data, graphs, as well as scalar, vector, and tensor fields.

### Learning goals: soft skills

Productive work in small teams, self-dependent solution of practical problems in the area of visual data analysis, critical reflection on visualization design, presentation of solution strategies and implementations, self management

### Contents

This class provides a broad overview of principles and algorithms for data analysis via interactive visualization. Specific topics include perceptual principles, color spaces, visualization analysis and design, integration of visual with statistical data analysis and machine learning, as well as specific algorithms and techniques for the display of multidimensional data, dimensionality reduction, graphs, geospatial data, neural networks, as well as scalar, vector and tensor fields.

### Prerequisites

#### Recommended:

Students are recommended to have a basic knowledge in linear algebra and calculus, as well as proficiency in programming.

### Course meetings

Teaching format	Group size	h/week	Workload[h]	CP	
Lecture		4	60 T / 105 S	5.5	T = face-to-face teaching
Exercises		2	30 T / 75 S	3.5	S = independent study

### Graded exams

Written exam (120 minutes)

### Ungraded coursework (required for admission to the exam)

The completion of regularly provided exercise sheets. The work can be done in groups of up to three students. A total of 50% of the points must be achieved. Each student must present a solution to an exercise in the exercise sessions once.

### Literature

- A.C. Telea, Data Visualization: Principles and Practice. CRC Press, Second Edition, 2015
- M. Ward et al., Interactive Data Visualization: Foundations, Techniques, and Applications. CRC Press, 2010
- T. Munzner, Visualization Analysis and Design, A K Peters, 2015

## MA-INF 2225 Discrete Models for Visual Computing

Workload	Credit points	Duration	Frequency
180 h	6 CP	1 semester	at least every 2 years
Module coordinator	Lecturer(s)		
Prof. Dr. Florian Bernard	Prof. Dr. Florian Bernard		
Programme	Mode	Semester	
M. Sc. Cyber Security	Optional	1. or 2.	

### Learning goals: technical skills

- Ability to implement basic visual computing algorithms, understanding their strengths and shortcomings
- Mathematical modelling of computational problems in visual computing
- Gain an intuition which algorithm is best applied for which problem in visual computing, so that practical problems in these areas can be solved

### Learning goals: soft skills

- Problem solving skills: ability to identify and utilise analogies between new problems and previously seen ones
- Analytical and abstract thinking: develop a general intuition of computational problems, being able to adopt different perspectives of particular concepts

### Contents

This module focuses on discrete models that frequently occur in the field of visual computing (VC). In addition to algorithms, this module will also cover modelling aspects that are relevant for solving practical problems in VC. The contents include:

- Graph-based models (e.g. linear and quadratic assignment, network flows, product graph formalisms, dynamic programming and their application)
- Continuous algorithms for discrete problems (e.g. convex & spectral relaxations, projection methods, path-following and their application)
- Deep Learning for discrete domains (e.g. differentiable programming, graph neural networks, deep learning on meshes)

### Prerequisites

#### Recommended:

Participants are expected to have a high level of mathematical maturity (in particular, a good working knowledge of linear algebra and calculus/analysis is essential). A basic understanding of graph theory is advantageous.

### Course meetings

Teaching format	Group size	h/week	Workload[h]	CP	
Lecture		2	30 T / 45 S	2.5	T = face-to-face teaching
Exercises		2	30 T / 75 S	3.5	S = independent study

### Graded exams

Written exam

### Ungraded coursework (required for admission to the exam)

The completion of regularly provided exercise sheets. The work can be done in groups of up to two students. A total of 50% of the points must be achieved.

## MA-INF 2226 Lab Geometry Processing

Workload	Credit points	Duration	Frequency
270 h	9 CP	1 semester	at least every 2 years
Module coordinator	Lecturer(s)		
Jun. Prof. Dr. Zorah Lähner	Prof. Dr. Zorah Lähner		
Programme	Mode	Semester	
M. Sc. Cyber Security	Optional	1-3.	

### Learning goals: technical skills

Ability to handle complex geometric data types; to extract implementation details from research publications; to implement and visualize geometric data.

### Learning goals: soft skills

Ability to analyze problems theoretically and to find creative and practical solutions; to examine one's solutions and results critically; to classify one's own results into the state-of-the-art of the respective area; to prepare readable documentation of software and research results; to present, defend and discuss design decisions and results in the team/group and to other students clearly and in accordance with academic standards; to collaborate constructively with others in small teams over a longer period of time.

### Contents

Mesh deformation, point cloud meshing, pytorch3D, shape correspondence, reconstruction, 2D-to-3D transfer. This lab introduces methods and applications in the field of geometry processing. You will get a chance to study the methods in depth by implementing them and running experiments. At the end of the semester, you will present the method, give a short demonstration and hand in a report describing the method and experimental outcomes.

### Prerequisites

none

### Course meetings

Teaching format	Group size	h/week	Workload[h]	CP
Lab	8	4	60 T / 210 S	9

T = face-to-face teaching  
S = independent study

### Graded exams

Oral presentation, written report

### Ungraded coursework (required for admission to the exam)

Project work; attendance in course sessions in accordance with the exam regulations of 2023, § 12(6).

---

**MA-INF 2227 Lab 3D Animation**


---

Workload	Credit points	Duration	Frequency
270 h	9 CP	1 semester	every semester
Module coordinator	Lecturer(s)		
Prof. Dr. Ina Prinz	Prof. Dr. Ina Prinz		
Programme	Mode	Semester	
M. Sc. Cyber Security	Optional	1-3.	

**Learning goals: technical skills**

The students will learn to carry out a practical task (project) in the context of 3D animation, containing modelling, preparing a screenplay, realizing an animation related to real physical laws, rendering and creating a video.

**Learning goals: soft skills**

Ability to properly present and defend design decisions, to prepare readable documentation of software; skills in constructively collaborating with others in small teams over a longer period of time; ability to classify ones own results into the state-of-the-art of the resp. area.

**Contents**

Varying selected topics close to current research in the area of the history of computing and the mechanization of computing as well as deep understanding of mechanical and technical functions and its presentation in a representative 3D animation video, contains technical visualization and didactic skills.

**Prerequisites**
**Recommended:**

For students who did not take BA-INF 108 Geschichte des maschinellen Rechnens I and BA-INF 126 Geschichte des maschinellen Rechnens II in their Bachelor's studies, recommended reading includes:

- Aspray, W.: Computing before Computers. Ames, 1990.
- Bauer, Friedrich L.: Origins and Foundations of Computing. Berlin 2010.
- Ceruzzi, Paul E.: A History of Modern Computing. Cambridge, 2003.
- Goldstine, H.: The Computer from Pascal to von Neumann. Princeton, 1972.

**Course meetings**

Teaching format	Group size	h/week	Workload[h]	CP	
Lab	8	4	60 T / 210 S	9	T = face-to-face teaching S = independent study

**Graded exams**

Oral presentation, written report, presentation of the video

**Ungraded coursework (required for admission to the exam)**

Project work; attendance in course sessions in accordance with the exam regulations of 2023, § 12(6).

---

---

## MA-INF 2308 Lab Graphics

---

Workload	Credit points	Duration	Frequency
270 h	9 CP	1 semester	every semester
Module coordinator	Lecturer(s)		
Prof. Dr. Reinhard Klein	Prof. Dr. Reinhard Klein		
Programme	Mode	Semester	
M. Sc. Cyber Security	Optional	2. or 3.	

### Learning goals: technical skills

The students will learn to carry out a practical task (project) in the context of geometry processing, rendering, scientific visualization or human computer interaction, including test and documentation of the implemented software/system.

### Learning goals: soft skills

Ability to properly present and defend design decisions, to prepare readable documentation of software; skills in constructively collaborating with others in small teams over a longer period of time; ability to classify ones own results into the state-of-the-art of the resp. area

### Contents

Varying selected topics close to current research in the area of geometry processing, rendering, scientific visualization or human computer interaction.

### Prerequisites

#### Recommended:

At least one of the following:

- MA-INF 1108 Introduction to High Performance Computing
- MA-INF 2202 Computer Animation
- MA-INF 2222 Visual Data Analysis

### Course meetings

Teaching format	Group size	h/week	Workload[h]	CP
Lab	8	4	60 T / 210 S	9

T = face-to-face teaching  
S = independent study

### Graded exams

Oral presentation, written report

### Ungraded coursework (required for admission to the exam)

Project work; attendance in course sessions in accordance with the exam regulations of 2023, § 12(6).

---

## MA-INF 2309 Lab Audio

Workload	Credit points	Duration	Frequency
270 h	9 CP	1 semester	every year
Module coordinator	Lecturer(s)		
apl. Prof. Dr. Frank Kurth	apl. Prof. Dr. Frank Kurth, Prof. Dr. Michael Clausen		
Programme	Mode	Semester	
M. Sc. Cyber Security	Optional	2. or 3.	

### Learning goals: technical skills

Proficiency in implementing signal processing concepts introduced in selected scientific publications or research reports. Proficiency in collecting and maintaining data sets, in particular signals and corresponding metadata, and performing scientific evaluations of signal processing methods based on data sets and implemented algorithms.

### Learning goals: soft skills

Ability to analyze problems theoretically and to find creative and practical solutions; to examine one's solutions and results critically; to classify one's own results into the state-of-the-art of the respective area; to prepare readable documentation of software and research results; to present, defend and discuss design decisions and results in the team/group and to other students clearly and in accordance with academic standards; to collaborate constructively with others in small teams over a longer period of time; to pursue long-range goals under a given resource budget.

### Contents

In the lab a medium-sized programming project related to digital audio signal processing has to be solved during the period of one semester. For this, initial literature, usually in form of one or two scientific papers or reports, will be provided at the beginning of the lab. Also, resources regarding the audio signal data to be used, are given. Typical programming tasks consist of implementing either general signal processing algorithms such as fundamental frequency estimation or of implementing algorithms for solving application problems such as speaker detection or classification. For participants with interest in topics of pattern recognition, machine and deep learning, programming projects from those areas, with application to audio processing, can be selected.

### Prerequisites

#### Recommended:

Solid basic proficiency in imperative programming (e.g. knowledge of C/C++, Java, Python). Knowledge of the material from MA-INF 2113 Foundations of Audio Signal Processing is highly recommended. Knowledge of material from MA-INF 2212 Pattern Matching and Machine Learning for Audio is helpful but not necessary.

### Course meetings

Teaching format	Group size	h/week	Workload[h]	CP	
Lab	8	4	60 T / 210 S	9	T = face-to-face teaching S = independent study

### Graded exams

Oral presentation, written report

### Ungraded coursework (required for admission to the exam)

Project work; attendance in course sessions in accordance with the exam regulations of 2023, § 12(6).

# MA-INF 2317 Numerical Algorithms for Visual Computing and Machine Learning

Workload	Credit points	Duration	Frequency
180 h	6 CP	1 semester	at least every 2 years
Module coordinator	Lecturer(s)		
Prof. Dr. Florian Bernard	Prof. Dr. Florian Bernard		
Programme	Mode	Semester	
M. Sc. Cyber Security	Optional	1. or 2.	

### Learning goals: technical skills

- ability to implement basic numerical algorithms, understanding their strengths and shortcomings
- mathematical modelling of computational problems in visual computing and machine learning
- gain an intuition which algorithm is best applied for which problem in visual computing and machine learning, so that practical problems in these areas can be solved

### Learning goals: soft skills

- problem solving skills: ability to identify and utilise analogies between new problems and previously seen ones
- analytical and abstract thinking: develop a general intuition of computational problems, being able to adopt different perspectives of particular concepts

### Contents

This module focuses on numerical methods that frequently occur in the fields visual computing (VC) and machine learning (ML). In addition to algorithms, this module will also cover modelling aspects that are relevant for solving practical problems in VC and ML. The contents include:

- Error analysis and conditioning of problems
- Linear systems (solvability, algorithms, stability, regularisation), and applications and modelling in VC and ML (e.g. linear regression, image alignment, deconvolution)
- Spectral methods (eigenvalue decomposition, singular value decomposition, respective algorithms), and their applications and modelling in VC and ML (e.g. clustering, Procrustes analysis, point-cloud alignment, principal components analysis)
- Numerical optimisation (gradient-based methods, second-order methods, large-scale optimisation) and applications and modelling in VC and ML.

### Prerequisites

#### Recommended:

Participants are expected to have a high level of mathematical maturity (in particular, a good working knowledge of linear algebra and calculus/analysis is essential). A basic understanding of mathematical optimisation is advantageous.

### Course meetings

Teaching format	Group size	h/week	Workload[h]	CP	
Lecture		2	30 T / 45 S	2.5	T = face-to-face teaching
Exercises		2	30 T / 75 S	3.5	S = independent study

### Graded exams

Written exam (120 minutes)

### Ungraded coursework (required for admission to the exam)

The completion of regularly provided exercise sheets. The work can be done in groups of up to two students. A total of 50% of the points must be achieved.

#### 4.5 Computer Science Elective Modules – Security, Information and Communication Management

MA-INF 3110	Lab4	9 CP	Lab Basics of iOS-Development	63
MA-INF 3209	Sem2	4 CP	Seminar Selected Topics in Communication Management	64
MA-INF 3216	Sem2	4 CP	Seminar Sensor Data Fusion	65
MA-INF 3229	Lab4	9 CP	Lab IT-Security	66
MA-INF 3233	L2E2	6 CP	Advanced Sensor Data Fusion in Distributed Systems	67
MA-INF 3237	L2E2	6 CP	Array Signal and Multi-channel Processing	68
MA-INF 3304	Lab4	9 CP	Lab Communication and Communicating Devices	69
MA-INF 3310	L2E2	6 CP	Introduction to Sensor Data Fusion - Methods and Applications	70
MA-INF 3312	Lab4	9 CP	Lab Sensor Data Fusion	71
MA-INF 3317	Sem2	4 CP	Seminar Selected Topics in IT Security	72
MA-INF 3319	Lab4	9 CP	Lab Usable Security and Privacy	73
MA-INF 3320	Lab4	9 CP	Lab Security in Distributed Systems	74
MA-INF 3321	Sem2	4 CP	Seminar Usable Security and Privacy	75

## MA-INF 3110 Lab Basics of iOS-Development

Workload	Credit points	Duration	Frequency
270 h	9 CP	1 semester	every year
Module coordinator	Lecturer(s)		
Prof. Dr. Stephan Jonas	Prof. Dr. Stephan Jonas		
Programme	Mode	Semester	
M. Sc. Cyber Security	Optional	1-3.	

### Learning goals: technical skills

Students acquire the ability to design and develop iOS applications while critically evaluating current research and best practices in mobile computing. They learn to compare different frameworks and architectural approaches, justify their decisions based on literature, and reflect on the advantages and limitations of various solutions. In addition to implementation, emphasis is placed on critical analysis and integration of current research findings, e.g., in the areas of usability, accessibility, performance, and security.

Students learn how to conduct literature research related to digital medicine application development and to critically evaluate scientific sources in mobile app development and human-computer interaction. They learn to document and justify design and development decisions with reference to scientific findings and empirical evidence. Furthermore, students learn to communicate results in a scientifically grounded project report and oral presentation.

### Learning goals: soft skills

- Self-competences: Work and time management, handling feedback, and adapting to changing requirements.
- Develop scientific thinking and research literacy by critically evaluating sources, documenting decisions, and reflecting on the app development process in an evidence-based manner.

### Contents

- Usage of Xcode
- Basic understanding of the programming language Swift.
- UI development with SwiftUI.
- Design of User Interfaces and Prototyping.
- Local data persistence on the devices.
- Git: Branches, Pull Requests, Code Review.

### Prerequisites

#### Recommended:

Experience in object-oriented programming

### Course meetings

Teaching format	Group size	h/week	Workload[h]	CP	
Lab	8	4	60 T / 210 S	9	T = face-to-face teaching S = independent study

### Graded exams

Oral presentation (individually graded), written project documentation / report.

### Ungraded coursework (required for admission to the exam)

Project work; attendance in course sessions in accordance with the exam regulations of 2023, § 12(6).

### Forms of media

Projection, videos, interactive exercises.

The lectures and exercises are based on interaction. We expect active participation! To take part in the exercises, a MacBook (with macOS 15 or later) is required. Please bring your own device or contact us in advance if you need to borrow one.

### Literature

- Human Interface Guidelines (<https://developer.apple.com/design/human-interface-guidelines>).
- SwiftUI Dokumentation (<https://developer.apple.com/documentation/swiftui/>).

## MA-INF 3209 Seminar Selected Topics in Communication Management

Workload	Credit points	Duration	Frequency
120 h	4 CP	1 semester	every semester
Module coordinator	Lecturer(s)		
Prof. Dr. Peter Martini	Prof. Dr. Peter Martini, Prof. Dr. Michael Meier, Dr. Matthias Frank		
Programme	Mode	Semester	
M. Sc. Cyber Security	Optional	2. or 3.	

### Learning goals: technical skills

Enhanced and in-depth knowledge in specialized topics in the area of communication systems and Internet protocols.

### Learning goals: soft skills

Acquire the competence to independently search for and study state-of-the-art scientific literature in depth, read critically, identify the most relevant content, and assess research results in the context of the corresponding research area; to discuss research results with a knowledgeable scientific audience; to present prior work by others in writing and in presentations with visual media in a way that adheres to academic standards, that is well-structured and didactically effective, and that motivates the audience to participate; to formulate and accept criticism; to manage one's time with relatively open assignments and long-ranging deadlines.

### Contents

Current research topics in communication systems and Internet protocols based on conference and journal papers.

### Prerequisites

#### Recommended:

Successful completion of at least one of the following lectures:

- MA-INF 3202 Mobile Communication
- MA-INF 3236 IT Security
- MA-INF 3239 Malware Analysis

Bachelor level knowledge of basics of communication systems and Internet protocols, e.g. OSI model, medium access of wired and wireless LAN technologies, IP addressing and routing, transport protocols UDP and TCP.

### Course meetings

Teaching format	Group size	h/week	Workload[h]	CP	
Seminar	10	2	30 T / 90 S	4	T = face-to-face teaching S = independent study

### Graded exams

Oral presentation, written report

### Ungraded coursework (required for admission to the exam)

Attendance in course sessions in accordance with the exam regulations of 2023, § 12(6).

### Literature

The relevant literature will be announced towards the end of the previous semester

## MA-INF 3216 Seminar Sensor Data Fusion

Workload	Credit points	Duration	Frequency
120 h	4 CP	1 semester	every year
Module coordinator	Lecturer(s)		
Prof. Dr. Wolfgang Koch	Prof. Dr. Wolfgang Koch, Dr. Felix Govaers		
Programme	Mode	Semester	
M. Sc. Cyber Security	Optional	3.	

### Learning goals: technical skills

Enhanced and in-depth knowledge in specialized topics in state estimation and object tracking.

### Learning goals: soft skills

Acquire the competence to independently search for and study state-of-the-art scientific literature in depth, read critically, identify the most relevant content, and assess research results in the context of the corresponding research area; to discuss research results with a knowledgeable scientific audience; to present prior work by others in writing and in presentations with visual media in a way that adheres to academic standards, that is well-structured and didactically effective, and that motivates the audience to participate; to formulate and accept criticism; to manage one's time with relatively open assignments and long-ranging deadlines.

### Contents

The seminar focuses on specific research papers in the field of sensor data fusion, which may include topics like non-linear state estimation, deep learning for sensor perception, or multi object tracking.

### Prerequisites

#### Recommended:

- MA-INF 3310 Introduction to Sensor Data Fusion – Methods and Applications.
- It is assumed that the participants know linear algebra and have basic knowledge in probability theory.

### Course meetings

Teaching format	Group size	h/week	Workload[h]	CP	
Seminar	10	2	30 T / 90 S	4	T = face-to-face teaching S = independent study

### Graded exams

Oral presentation, written report

### Ungraded coursework (required for admission to the exam)

Attendance in course sessions in accordance with the exam regulations of 2023, § 12(6).

### Literature

The relevant literature will be announced at the beginning of the seminar.

---

**MA-INF 3229 Lab IT-Security**


---

Workload	Credit points	Duration	Frequency
270 h	9 CP	1 semester	every semester
Module coordinator	Lecturer(s)		
Prof. Dr. Michael Meier	Prof. Dr. Michael Meier		
Programme	Mode	Semester	
M. Sc. Cyber Security	Optional	2. or 3.	

**Learning goals: technical skills**

After completion of the lab module students have completed a practical task in the context of IT security. The students will have gained experience in the typical technical skills like the design and implementation of software, test and documentation of the software, and performance evaluation (e.g. by measurements, simulation, analysis) and presentation of performance results.

**Learning goals: soft skills**

Ability to analyze problems theoretically and to find creative and practical solutions; to examine one's solutions and results critically; to classify one's own results into the state-of-the-art of the respective area; to prepare readable documentation of software and research results; to present, defend and discuss design decisions and results in the team/group and to other students clearly and in accordance with academic standards; to collaborate constructively with others in small teams over a longer period of time; to aim at long-range goals under limited resources; to work under pressure.

**Contents**

Selected topics close to current research in the area of IT security.

**Prerequisites**
**Recommended:**

Foundational knowledge in

- IT security: security terminology, authentication, access control, applied cryptography (symmetric encryption, asymmetric encryption, hashing, key management)
- Networks: OSI model, addressing, routing, protocols.

It is recommended to take MA-INF 3236 IT Security first.

**Course meetings**

Teaching format	Group size	h/week	Workload[h]	CP	
Lab	8	4	60 T / 210 S	9	T = face-to-face teaching S = independent study

**Graded exams**

Oral presentation, written report

**Ungraded coursework (required for admission to the exam)**

Project work; attendance in course sessions in accordance with the exam regulations of 2023, § 12(6).

---

## MA-INF 3233 Advanced Sensor Data Fusion in Distributed Systems

Workload	Credit points	Duration	Frequency
180 h	6 CP	1 semester	every year
Module coordinator	Lecturer(s)		
Prof. Dr. Wolfgang Koch	Dr. Felix Govaers		
Programme	Mode	Semester	
M. Sc. Cyber Security	Optional	2. or 3.	

### Learning goals: technical skills

Students will be able to describe the advanced principles of sensor data fusion for state estimation and object tracking based on tracks from multiple sensors in distributed systems. They will be aware of the correlation problem in track-to-track fusion and know several algorithms to cope with it. They will know the assumptions, advantages and disadvantages of different algorithms and be able to select and apply suitable candidates in practical applications.

### Learning goals: soft skills

Mathematical derivation of algorithms, application of mathematical results on estimation theory.

### Contents

Tracklet fusion, the Bar-Shalom-Campo formula, the Federated Kalman Filter, naive fusion, the distributed Kalman filter and the least squares estimate, Accumulated State Densities, Decorrelated fusion, product representation.

For challenging state estimation tasks, algorithms which enhance the situational awareness by fusing sensor information are inevitable. Nowadays it has become very popular to improve the performance of systems by linking multiple sensors. This implies some challenges to the sensor data fusion methodologies such as sensor registration, communication delays, and correlations of estimation errors. In particular, if the communication links have limited bandwidth, data reduction techniques have to be applied at the sensor sites, that is local tracks have to be computed. Once received at a fusion center (FC), the tracks then are fused to reconstruct a global estimate.

### Prerequisites

#### Recommended:

Basic knowledge about the Kalman filter is required (see also recommended literature).

Students who did not take BA-INF 137 – Einführung in die Sensordatenfusion in their Bachelor's are advised to first take MA-INF 3310 – Introduction to Sensor Data Fusion - Methods and Applications.

### Course meetings

Teaching format	Group size	h/week	Workload[h]	CP	
Lecture		2	30 T / 45 S	2.5	T = face-to-face teaching
Exercises		2	30 T / 75 S	3.5	S = independent study

### Graded exams

Oral exam (30 minutes)

### Ungraded coursework (required for admission to the exam)

50% of the maximum achievable points in the practical programming exercises are required. There is one practical exercise, which is a workload of about 15h. The delivery of the programmed solution is done individually or in group work of up to three students. A total of 10 points will be awarded, 50% of which will have been achieved if the Distributed Kalman filter has been programmed in an executable and consistent manner.

### Forms of media

Power Point

### Literature

W. Koch: "Tracking and Sensor Data Fusion: Methodological Framework and Selected Applications", Springer, 2014.  
 D. Hall, C.-Y. Chong, J. Llinas, and M. L. II: "Distributed Data Fusion for Network-Centric Operations", CRC Press, 2014.

---

**MA-INF 3237 Array Signal and Multi-channel Processing**


---

Workload	Credit points	Duration	Frequency
180 h	6 CP	1 semester	every year
Module coordinator	Lecturer(s)		
Prof. Dr. Wolfgang Koch	Dr. Marc Oispuu		
Programme	Mode	Semester	
M. Sc. Cyber Security	Optional	1-3.	

**Learning goals: technical skills**

Students will be able to describe the central principles of array signal and multi-channel processing and to name their advantages and disadvantages as well as to illustrate their relevance in application examples such as wireless communication, acoustics, radar, sonar or seismology. Furthermore, they will be able to implement suitable methods of direction finding, spatial filtering and bearings-only localization and to apply them to electromagnetic or acoustic signals and to evaluate the achieved results in terms of their performance.

**Learning goals: soft skills**

Mathematical derivation of algorithms, applications of mathematical results on estimation theory

**Contents**

Estimation theory, Sensor model, Cramér-Rao analysis, conventional beamforming, Multiple Signal Classification (MUSIC), sensor calibration, Bearings-only localization, Direct Position Determination (DPD), Applications

**Prerequisites**

none

**Course meetings**

Teaching format	Group size	h/week	Workload[h]	CP	
Lecture		2	30 T / 45 S	2.5	T = face-to-face teaching
Exercises		2	30 T / 75 S	3.5	S = independent study

**Graded exams**

Oral Exam (30 minutes)

**Ungraded coursework (required for admission to the exam)**

50% of the maximum achievable points in the practical programming exercises are required. There is one practical exercise, which is a workload of about 10h. The delivery of the programmed solution is done individually or in group work of up to three students. A total of 10 points will be awarded, 50% of which will have been achieved if the basic signal processing algorithms for array sensors have been implemented.

**Forms of media**

Power Point

**Literature**

H. L. van Trees, Optimum Array Processing. Part IV of Detection, Estimation, and Modulation Theory. New York: Wiley-Interscience, 2002.

---

## MA-INF 3304 Lab Communication and Communicating Devices

Workload	Credit points	Duration	Frequency
270 h	9 CP	1 semester	every semester
Module coordinator	Lecturer(s)		
Prof. Dr. Peter Martini	Prof. Dr. Peter Martini, Prof. Dr. Michael Meier, Dr. Matthias Frank		
Programme	Mode	Semester	
M. Sc. Cyber Security	Optional	2. or 3.	

### Learning goals: technical skills

After completion of the lab module students have completed a practical task in the context of communication and networked systems. The students will have gained experience in the typical technical skills like the design and implementation of communication software/networked systems, test and documentation of the software, and performance evaluation (e.g. by measurements, simulation, analysis) and presentation of performance results.

### Learning goals: soft skills

Ability to analyze problems theoretically and to find creative and practical solutions; to examine one's solutions and results critically; to classify one's own results into the state-of-the-art of the respective area; to prepare readable documentation of software and research results; to present, defend and discuss design decisions and results in the team/group and to other students clearly and in accordance with academic standards; to collaborate constructively with others in small teams over a longer period of time; to aim at long-range goals under limited resources; to work under pressure.

### Contents

Selected topics close to current research in the area of communication systems, network security, mobile communication and communicating devices.

### Prerequisites

#### Recommended:

Foundational knowledge in networks: OSI model, addressing, routing, protocols;

Successful completion of at least one of the following lectures:

- MA-INF 3202 Mobile Communication
- MA-INF 3236 IT Security
- MA-INF 3239 Malware Analysis

### Course meetings

Teaching format	Group size	h/week	Workload[h]	CP	
Lab	8	4	60 T / 210 S	9	T = face-to-face teaching S = independent study

### Graded exams

Oral presentation, written report

### Ungraded coursework (required for admission to the exam)

Project work; attendance in course sessions in accordance with the exam regulations of 2023, § 12(6).

### Literature

The relevant literature will be announced towards the end of the previous semester.

# MA-INF 3310 Introduction to Sensor Data Fusion - Methods and Applications

<b>Workload</b>	<b>Credit points</b>	<b>Duration</b>	<b>Frequency</b>
180 h	6 CP	1 semester	every year
<b>Module coordinator</b>	<b>Lecturer(s)</b>		
Prof. Dr. Wolfgang Koch	Prof. Dr. Wolfgang Koch		
<b>Programme</b>	<b>Mode</b>	<b>Semester</b>	
M. Sc. Cyber Security	Optional	1. or 2.	

**Learning goals: technical skills**

Students will be able to describe the central principles of sensor data fusion for state estimation and object tracking based on error-prone and ambiguous measurements. They will be able to apply the Kalman filter and to formulate sensor and dynamics models for different kind of sensors and objects. Furthermore, they will know the concept of probabilistic data association and a computationally feasible approximation using Gaussian mixture densities.

**Learning goals: soft skills**

Mathematical derivation of algorithms, application of mathematical results on estimation theory.

**Contents**

Gaussian probability density functions, Kalman filter, Unscented Kalman Filter, Extended Kalman Filter, Particle Filter, Multi-Hypothesis-Tracker, Extended Target Tracking, Road Tracking, Interacting Multiple Model Filter, Retrodiction, Smoothing, Maneuver Modeling.

The lecture starts with preliminaries on how to handle uncertain data and knowledge within analytical calculus. Then, the fundamental and well-known Kalman filter is derived. Based on this tracking scheme, further approaches to a wide spectrum of applications will be shown. All algorithms will be motivated by examples from ongoing research projects, industrial cooperations, and impressions of current demonstration hardware.

Because of inherent practical issues, every sensor measures certain properties up to an error. This lecture shows how to model and overcome this error by an application of theoretical tools such as Bayes' rule and further derivations. Moreover, solutions to possible false-alarms, miss-detections, maneuvering phases, and much more will be presented.

**Prerequisites**

**Recommended:**

It is assumed that the participants know linear algebra and have basic knowledge in probability theory.

**Course meetings**

Teaching format	Group size	h/week	Workload[h]	CP	
Lecture		2	30 T / 45 S	2.5	T = face-to-face teaching
Exercises		2	30 T / 75 S	3.5	S = independent study

**Graded exams**

Oral exam

**Ungraded coursework (required for admission to the exam)**

50% of the possible points for the exercises. The points are acquired by a small programming exercise with a workload of about 15 hours and some theoretical exercises with a workload of 10 hours. The solution has to be submitted individually or in groups of up to three students and will be rated by points.

**Literature**

- W. Koch: "Tracking and Sensor Data Fusion: Methodological Framework and Selected Applications", Springer, 2014.
- Y. Bar-Shalom: "Estimation with Applications to Tracking and Navigation", Wiley-Interscience, 2001.

## MA-INF 3312 Lab Sensor Data Fusion

Workload	Credit points	Duration	Frequency
270 h	9 CP	1 semester	every year
Module coordinator	Lecturer(s)		
Prof. Dr. Wolfgang Koch	Prof. Dr. Wolfgang Koch		
Programme	Mode	Semester	
M. Sc. Cyber Security	Optional	2. or 3.	

### Learning goals: technical skills

Enhanced and in-depth knowledge in specialized topics in state estimation and object tracking.

### Learning goals: soft skills

Ability to analyze problems theoretically and to find creative and practical solutions; to examine one's solutions and results critically; to classify one's own results into the state-of-the-art of the respective area; to prepare readable documentation of software and research results; to present, defend and discuss design decisions and results in the team/group and to other students clearly and in accordance with academic standards; to collaborate constructively with others in small teams over a longer period of time; to aim at long-range goals under limited resources; to work under pressure.

### Contents

In the lab, the students apply methods from the sensor data fusion and state estimation theory to practical examples in order to get experience in the application and implementation. The exemplary scenarios and application examples vary each year but may be for instance on a simulated radar network for multi object tracking, camera image processing, heterogeneous sensor fusion, or array sensor bearing processing.

The students shall work together in a team. Everyone is responsible for a specific part in the context of a main goal. Results will be exchanged and integrated via software interfaces.

### Prerequisites

#### Recommended:

- MA-INF 3310 Introduction to Sensor Data Fusion – Methods and Applications;
- knowledge of linear algebra and basic knowledge in probability theory.

### Course meetings

Teaching format	Group size	h/week	Workload[h]	CP	
Lab	8	4	60 T / 210 S	9	T = face-to-face teaching S = independent study

### Graded exams

Oral presentation, written report

### Ungraded coursework (required for admission to the exam)

Project work; attendance in course sessions in accordance with the exam regulations of 2023, § 12(6).

### Literature

The relevant literature will be announced at the beginning of the lab.

## MA-INF 3317 Seminar Selected Topics in IT Security

Workload	Credit points	Duration	Frequency
120 h	4 CP	1 semester	every semester
Module coordinator	Lecturer(s)		
Prof. Dr. Michael Meier	Prof. Dr. Michael Meier, Prof. Dr. Peter Martini		
Programme	Mode	Semester	
M. Sc. Cyber Security	Optional	2. or 3.	

### Learning goals: technical skills

Enhanced and in-depth knowledge in specialized topics in the area of IT Security.

### Learning goals: soft skills

Acquire the competence to independently search for and study state-of-the-art scientific literature in depth, read critically, identify the most relevant content, and assess research results in the context of the corresponding research area; to discuss research results with a knowledgeable scientific audience; to present prior work by others in writing and in presentations with visual media in a way that adheres to academic standards, that is well-structured and didactically effective, and that motivates the audience to participate; to formulate and accept criticism; to manage one's time with relatively open assignments and long-ranging deadlines.

### Contents

Current research topics in IT security based on conference and journal papers.

### Prerequisites

#### Recommended:

Foundational knowledge in

- IT security: security terminology, authentication, access control, applied cryptography (symmetric encryption, asymmetric encryption, hashing, key management)
- Networks: OSI model, addressing, routing, protocols.

It is recommended to take MA-INF 3236 IT Security first.

### Course meetings

Teaching format	Group size	h/week	Workload[h]	CP
Seminar	10	2	30 T / 90 S	4

T = face-to-face teaching  
S = independent study

### Graded exams

Oral presentation, written report

### Ungraded coursework (required for admission to the exam)

Attendance in course sessions in accordance with the exam regulations of 2023, § 12(6).

## MA-INF 3319 Lab Usable Security and Privacy

Workload	Credit points	Duration	Frequency
270 h	9 CP	1 semester	every semester
Module coordinator	Lecturer(s)		
Prof. Dr. Matthew Smith	Prof. Dr. Matthew Smith		
Programme	Mode	Semester	
M. Sc. Cyber Security	Optional	2. or 3.	

### Learning goals: technical skills

Ability to carry out a practical task (project) in the context of human factors of security and privacy, including user studies and their evaluation. This includes selecting variables of interest, designing measurement instruments, such as interviews, surveys or prototypes, recruiting participants, executing and evaluating the user-study.

### Learning goals: soft skills

Ability to work in small teams and cooperate with other teams in a group; ability to make design decisions in a practical task; present and discuss (interim and final) results in the team/group and to other students; prepare written documentation of the work carried out

### Contents

The students will select and carry out a practical task (project) in the context of human factors of security and privacy, including user studies and their evaluation. Topics for the project are close to current research in the area of human aspects of security and privacy. Focus topics include but are not limited to: Attitudes towards Surveillance, S&P Ethics, Privacy technology, Authentication, Encryption, Gamification, Age verification, etc.

### Prerequisites

#### Recommended:

Knowledge on how to run and evaluate user studies is required. It is recommended to check the material of the Bachelor’s course BA-INF 145 Usable Security and Privacy (available in English) and to take:

- MA-INF 3241 Practical Challenges in Human Factors of Security and Privacy.

### Course meetings

Teaching format	Group size	h/week	Workload[h]	CP
Lab	8	4	60 T / 210 S	9

T = face-to-face teaching  
S = independent study

### Graded exams

Oral presentation, written report

### Ungraded coursework (required for admission to the exam)

Project work; attendance in course sessions in accordance with the exam regulations of 2023, § 12(6).

---

**MA-INF 3320 Lab Security in Distributed Systems**


---

Workload	Credit points	Duration	Frequency
270 h	9 CP	1 semester	every semester
Module coordinator	Lecturer(s)		
Prof. Dr. Matthew Smith	Prof. Dr. Matthew Smith		
Programme	Mode	Semester	
M. Sc. Cyber Security	Optional	2. or 3.	

**Learning goals: technical skills**

Ability to carry out a practical task (project) in the context of distributed security using modern software engineering processes, including testing and documentation of the implemented software/system.

**Learning goals: soft skills**

Ability to work in small teams and cooperate with other teams in a group; ability to make design decisions in a practical task; present and discuss (interim and final) results in the team/group and to other students; prepare written documentation of the work carried out.

**Contents**

The students will carry out a practical task (project) in the context of distributed security, including documentation of the implemented software/system. Topics are selected topics close to current research in the area of distributed systems security and privacy. Focus topics include but are not limited to: Authentication, Encryption, Gamification, Age verification, Data management, Study platforms, etc. The students will build software systems using modern software engineering processes. They will test them either programmatically or with a small user studies. They will document their software.

**Prerequisites**
**Recommended:**

Strong programming skills are required. It is recommended to take MA-INF 3242 Security of Distributed and Resource-constrained Systems first.

**Course meetings**

Teaching format	Group size	h/week	Workload[h]	CP	
Lab	8	4	60 T / 210 S	9	T = face-to-face teaching S = independent study

**Graded exams**

Oral presentation, written report

**Ungraded coursework (required for admission to the exam)**

Project work; attendance in course sessions in accordance with the exam regulations of 2023, § 12(6).

---

---

**MA-INF 3321 Seminar Usable Security and Privacy**


---

Workload	Credit points	Duration	Frequency
120 h	4 CP	1 semester	every semester
Module coordinator	Lecturer(s)		
Prof. Dr. Matthew Smith	Prof. Dr. Matthew Smith		
Programme	Mode	Semester	
M. Sc. Cyber Security	Optional	1-3.	

**Learning goals: technical skills**

Enhanced and in-depth knowledge in specialized topics in the area of human aspects of security and privacy.

**Learning goals: soft skills**

Acquire the competence to independently search for and study state-of-the-art scientific literature in depth, read critically, identify the most relevant content, and assess research results in the context of the corresponding research area; to discuss research results with a knowledgeable scientific audience; to present prior work by others in writing and in presentations with visual media in a way that adheres to academic standards, that is well-structured and didactically effective, and that motivates the audience to participate; to formulate and accept criticism; to manage one's time with relatively open assignments and long-ranging deadlines.

**Contents**

Current conference and journal papers in the area of human aspects of security and privacy. This includes but is not limited to: Attitudes towards Surveillance, S&P Ethics, Privacy technology, Authentication, Encryption, Gamification, Age verification, etc.

**Prerequisites**

none

**Course meetings**

Teaching format	Group size	h/week	Workload[h]	CP	
Seminar	10	2	30 T / 90 S	4	T = face-to-face teaching S = independent study

**Graded exams**

Oral presentation, written report

**Ungraded coursework (required for admission to the exam)**

Attendance in course sessions in accordance with the exam regulations of 2023, § 12(6).

---

## 4.6 Computer Science Elective Modules – Intelligent Systems

MA-INF 4111	L2E2	6 CP	Principles of Machine Learning	77
MA-INF 4112	L2E2	6 CP	Algorithms for Data Science	79
MA-INF 4113	L2E2	6 CP	Cognitive Robotics	80
MA-INF 4114	L2E2	6 CP	Robot Learning	81
MA-INF 4115	L3E1	6 CP	Introduction to Natural Language Processing	82
MA-INF 4117	L2E1	4 CP	Mining Media Data I	84
MA-INF 4201	L2E2	6 CP	Artificial Life	85
MA-INF 4204	L2E2	6 CP	Technical Neural Nets	86
MA-INF 4208	Sem2	4 CP	Seminar Vision Systems	88
MA-INF 4209	Sem2	4 CP	Seminar Principles of Data Mining and Learning Algorithms	89
MA-INF 4211	Sem2	4 CP	Seminar Cognitive Robotics	90
MA-INF 4213	Sem2	4 CP	Seminar Humanoid Robots	91
MA-INF 4214	Lab4	9 CP	Lab Humanoid Robots	92
MA-INF 4215	L2E2	6 CP	Humanoid Robotics	93
MA-INF 4228	L4E2	9 CP	Foundations of Data Science	94
MA-INF 4230	L2E2	6 CP	Advanced Methods of Information Retrieval	95
MA-INF 4231	Sem2	4 CP	Seminar Advanced Topics in Information Retrieval	97
MA-INF 4232	Lab4	9 CP	Lab Information Retrieval in Practice	98
MA-INF 4241	Lab4	9 CP	Lab Cognitive Modelling of Biological Agents	99
MA-INF 4242	L2E2	6 CP	Self-supervised Learning	100
MA-INF 4243	L2E1	4 CP	Mining Media Data II	101
MA-INF 4304	Lab4	9 CP	Lab Cognitive Robotics	102
MA-INF 4306	Lab4	9 CP	Lab Development and Application of Data Mining and Learning Systems	103
MA-INF 4308	Lab4	9 CP	Lab Vision Systems	104
MA-INF 4322	Lab4	9 CP	Lab Machine Learning on Encrypted Data	105
MA-INF 4324	Sem2	4 CP	Seminar Advanced Topics in Data Science	106
MA-INF 4325	Lab4	9 CP	Lab Data Science in Practice	107
MA-INF 4326	L2E2	6 CP	Explainable AI and Applications	108
MA-INF 4328	L2E2	6 CP	Spatio-Temporal Data Analytics	110
MA-INF 4331	Lab4	9 CP	Lab Perception and Learning for Robotics	111
MA-INF 4333	L2E2	6 CP	Geometric Deep Learning	112
MA-INF 4334	L2E2	6 CP	Computational neuroscience: cognition and behaviour	113
MA-INF 4335	Lab4	9 CP	Lab AI Alignment	114
MA-INF 4336	Sem2	4 CP	Seminar Selected Topics in Natural Language Processing	116

# MA-INF 4111 Principles of Machine Learning

<b>Workload</b>	<b>Credit points</b>	<b>Duration</b>	<b>Frequency</b>
180 h	6 CP	1 semester	every year
<b>Module coordinator</b>	<b>Lecturer(s)</b>		
Prof. Dr.-Ing. Christian Bauckhage	Prof. Dr.-Ing. Christian Bauckhage		
<b>Programme</b>	<b>Mode</b>	<b>Semester</b>	
M. Sc. Cyber Security	Optional	1-2.	

**Learning goals: technical skills**

Upon successful completion of this module, students should be able to describe fundamental methods, algorithms, and use cases of machine learning. Students acquire knowledge about supervised and unsupervised learning; based on the knowledge and skills acquired, students should be able to

- Implement, algorithms for optimization and parameter estimation in model training and machine learning tasks.
- Adopt the fundamental methods they learned about to a wide range of problems in automated intelligent data analysis.

**Learning goals: soft skills**

In the exercises, students can put their knowledge about theoretical concepts, mathematical methods, and algorithmic approaches into practice and realize small projects involving the implementation and evaluation of machine learning algorithms. This requires teamwork; upon successful completion of the module, students should be able to

- draft and implement basic machine learning algorithms for various practical problem settings
- prepare and give oral presentations about their work in front of an audience

**Contents**

Fundamental machine learning models for classification and clustering, model training via minimization of loss functions, fundamental optimization algorithms, model regularization, kernel methods for supervised and unsupervised learning, probabilistic modeling and inference, dimensionality reduction and latent factor models, the basic theory behind neural networks and neural network training; This course is intended to lay the foundation for more advanced courses on modern deep learning and reinforcement learning.

**Prerequisites**

**Recommended:**

Linear algebra, statistics, probability theory, calculus, python programming

**Remarks**

At most 150 participants.

**Course meetings**

Teaching format	Group size	h/week	Workload[h]	CP	
Lecture	150	2	30 T / 45 S	2.5	T = face-to-face teaching
Exercises		2	30 T / 75 S	3.5	S = independent study

**Graded exams**

Written exam (120 minutes)

**Ungraded coursework (required for admission to the exam)**

The completion of regularly provided exercise sheets. The work can be done in groups of up to five students. A total of 50% of the points must be achieved. Each student must present a solution to an exercise in the exercise sessions once.

**Forms of media**

- lecture slides / lecture notes are made available online
- notebooks with programming examples are made available online

### Literature

- D.J.C MacKay: Information Theory, Inference and Learning Algorithms, Cambridge University Press, 2003
  - C.M. Bishop: Pattern Recognition and Machine Learning, Springer, 2006
  - S. Haykin: Neural Networks and Learning Machines, Pearson, 2008
-

## MA-INF 4112 Algorithms for Data Science

Workload	Credit points	Duration	Frequency
180 h	6 CP	1 semester	every year
Module coordinator	Lecturer(s)		
Prof. Dr. Stefan Wrobel	Dr. Tamas Horvath, Prof. Dr. Stefan Wrobel		
Programme	Mode	Semester	
M. Sc. Cyber Security	Optional	1. or 2.	

### Learning goals: technical skills

In this module the students will learn algorithms for data science as well as implement and practice selected algorithms from this field. The module concentrates on basic algorithms in association rule mining, graph mining, and data streams. At the end of the module, students will be capable of analyzing formal properties of this kind of algorithms and choosing appropriate pattern discovery and data stream algorithms.

### Learning goals: soft skills

Communicative skills (oral and written presentation of solutions, discussions in teams), self-competences (ability to accept and formulate criticism, ability to analyse, creativity in the context of an "open end" task), social skills (effective team work and project planning).

### Contents

The module is offered every year, each time concentrating on one or more specific issues, such as frequent, closed and maximal frequent itemset mining, frequent subgraph mining algorithms for forests and for other graph classes beyond forests, frequent items and frequency moments in data streams, and graph stream algorithms.

### Prerequisites

#### Recommended:

Knowledge of standard notions and results from complexity theory, propositional logic, hashing, probability theory, and calculus, all on the bachelor level, are required.

### Course meetings

Teaching format	Group size	h/week	Workload[h]	CP	
Lecture		2	30 T / 45 S	2.5	T = face-to-face teaching
Exercises		2	30 T / 75 S	3.5	S = independent study

### Graded exams

Written exam (120 minutes)

### Ungraded coursework (required for admission to the exam)

The completion of regularly provided exercise sheets. The work can be done in groups of up to five students. A total of 50% of the points must be achieved. Each student must present a solution to an exercise in the exercise sessions once.

### Forms of media

lectures, exercises

### Literature

- Avrim Blum, John Hopcroft, Ravindran Kannan: Foundations of Data Science. Cambridge University Press, 2020.
- Jiawei Han, Micheline Kamber, Jian Pei: Data Mining: Concepts and Techniques. Morgan Kaufmann Publishers, 2012.
- David J. Hand, Heikki Mannila and Padhraic Smyth: Principles of Data Mining. The MIT Press, 2001.

---

**MA-INF 4113 Cognitive Robotics**


---

Workload	Credit points	Duration	Frequency
180 h	6 CP	1 semester	every year
Module coordinator	Lecturer(s)		
Prof. Dr. Sven Behnke	Prof. Dr. Sven Behnke, Prof. Dr. Maren Bennewitz		
Programme	Mode	Semester	
M. Sc. Cyber Security	Optional	1. or 2.	

**Learning goals: technical skills**

This lecture is one of two introductory lectures on Robotics of the intelligent systems track. The lecture covers cognitive capabilities of robots, like self-localization, mapping, object perception, and action-planning in complex environments.

This module complements MA-INF 4114 and can be taken before or after that module.

**Learning goals: soft skills**

Communicative skills (oral and written presentation of solutions, discussions in small teams), self competences (ability to accept and formulate criticism, ability to analyze problems)

**Contents**

Probabilistic approaches to state estimation (Bayes Filters, Kalman Filter, Particle Filter), motion models, sensor models, self-localization, mapping with known poses, simultaneous mapping and localization (SLAM), iterated closest-point matching, path planning, place- and person recognition, object recognition.

**Prerequisites**

none

**Course meetings**

Teaching format	Group size	h/week	Workload[h]	CP	
Lecture		2	30 T / 45 S	2.5	T = face-to-face teaching S = independent study
Exercises		2	30 T / 75 S	3.5	

**Graded exams**

Written exam (120 minutes)

**Ungraded coursework (required for admission to the exam)**

The completion of regularly provided exercise sheets. The work can be done in groups of up to two students. A total of 50% of the points must be achieved.

**Literature**

- S. Thrun, W. Burgard and D. Fox: Probabilistic Robotics. MIT Press, 2005.
  - B. Siciliano, O. Khatib (Eds.): Springer Handbook of Robotics, 2008.
  - R. Szeliski: Computer Vision: Algorithms and Applications, Springer 2010.
-

## MA-INF 4114 Robot Learning

Workload	Credit points	Duration	Frequency
180 h	6 CP	1 semester	every year
Module coordinator	Lecturer(s)		
Prof. Dr. Sven Behnke	Prof. Dr. Sven Behnke, Dr. Nils Goerke		
Programme	Mode	Semester	
M. Sc. Cyber Security	Optional	1. or 2.	

### Learning goals: technical skills

This lecture is one of two introductory lectures on Robotics of the intelligent systems track. Creating autonomous robots that can learn to assist humans in situations of daily life is a fascinating challenge for machine learning. The lecture covers key ingredients for a general robot learning approach to get closer towards human-like performance in robotics, such as reinforcement learning, learning models for control, learning motor primitives, learning from demonstrations and imitation learning, and interactive learning.

This module complements MA-INF 4113 and can be taken before or after that module.

### Learning goals: soft skills

Communicative skills (oral and written presentation of solutions, discussions in small teams), self competences (ability to accept and formulate criticism, ability to analyze problems)

### Contents

Reinforcement learning, Markov decision processes, dynamic programming, Monte Carlo methods, temporal-difference methods, function approximation, linear quadratic regulation, differential dynamic programming, partially observable MDPs, policy gradient methods, inverse reinforcement learning, imitation learning, learning kinematic models, perceiving and handling of objects.

### Prerequisites

none

### Course meetings

Teaching format	Group size	h/week	Workload[h]	CP	
Lecture		2	30 T / 45 S	2.5	T = face-to-face teaching
Exercises		2	30 T / 75 S	3.5	S = independent study

### Graded exams

Written exam (120 minutes)

### Ungraded coursework (required for admission to the exam)

The completion of regularly provided exercise sheets. The work can be done in groups of up to two students. A total of 50% of the points must be achieved.

### Literature

- R. Sutton and A. Barto: Reinforcement Learning, MIT-Press, 1998.
- O. Sigaud and J. Peters (Eds.): From Motor Learning to Interaction Learning in Robots. Springer, 2010.

# MA-INF 4115 Introduction to Natural Language Processing

Workload	Credit points	Duration	Frequency
180 h	6 CP	1 semester	every year
Module coordinator	Lecturer(s)		
Prof. Dr. Lucie Flek	Prof. Dr. Lucie Flek		
Programme	Mode	Semester	
M. Sc. Cyber Security	Optional	1. or 2.	

### Learning goals: technical skills

This class provides a technical perspective on NLP methods for building computer software that understands and manipulates human language. Contemporary data-driven approaches are emphasized, focusing on machine learning techniques. The covered applications vary in complexity, including for example Entity Recognition, Argument Mining, or Emotion Analysis.

### Learning goals: soft skills

Group work during programming exercises will allow students to work on real-world NLP application projects. The final project offers you the chance to apply your newly acquired skills towards an in-depth application using different frameworks such as PyTorch and spaCy and present it in a poster session.

### Contents

Through lectures, exercises, and a final project, you will gain a thorough introduction to cutting-edge research in NLP, from the linguistic basis of computational language methods to recent advances in deep learning and large language models. This course provides:

- An overview of NLP goals, challenges, and applications
- Text representation (Words, sentences, paragraphs, documents), word embeddings, word2vec, BERT, word similarity
- Machine learning / deep learning algorithms for text classification, Transformers
- Basics of neural language modeling
- Basics of computational linguistics
- Transforming words to their base forms (tokenization, stemming, lemmatization)
- Syntactic analysis (part of speech tagging, chunking, and parsing)
- Techniques for extracting meaning from text (semantic analysis), use of lexical resources in NLP
- NLP applications and projects (e.g., Sentiment Analysis, Named Entity Recognition, Question Answering, Summarization, Fake news detection, Plagiarism detection, Abusive language detection, Opinion mining...)

### Prerequisites

#### Recommended:

- Basics of statistics recommended.
- Basic programming knowledge in Python is of advantage.
- Basics of machine learning are of advantage.

### Course meetings

Teaching format	Group size	h/week	Workload[h]	CP	
Lecture		3	45 T / 45 S	3	T = face-to-face teaching S = independent study
Exercises		1	15 T / 75 S	3	

### Graded exams

Written exam (60 %); Project work (40 %)

### Ungraded coursework (required for admission to the exam)

The completion of regularly provided exercise sheets. The work must be done individually. A total of 50% of the points must be achieved.

**Forms of media**

- Lecture slides
- Exercise slides
- Notebooks with programming examples

**Literature**

- J. Eisenstein: Introduction to Natural Language Processing
  - Jurafsky, Daniel, and James H. Martin. "Speech and Language Processing: An Introduction to Natural Language Processing, Computational Linguistics, and Speech Recognition."
  - S. Bird, E. Klein, E. Loper; Natural Language Processing with Python
-

## MA-INF 4117 Mining Media Data I

Workload	Credit points	Duration	Frequency
120 h	4 CP	1 semester	every year
Module coordinator	Lecturer(s)		
Prof. Dr. Rafet Sifa	Prof. Dr. Rafet Sifa, Dr. Lorenz Sparrenberg		
Programme	Mode	Semester	
M. Sc. Cyber Security	Optional	1. or 2.	

### Learning goals: technical skills

By the end of this course, students will be able to:

- Analyze and extract meaningful relationships from large-scale media datasets using advanced data mining techniques.
- Develop and implement predictive and descriptive models for applications such as recommender systems, trend analysis, and outlier detection.
- Apply mathematical optimization methods to create interpretable and efficient machine learning models.
- Integrate theoretical concepts with practical tools to address challenges in digital forensics, behavioral profiling, and marketing strategy design.

### Learning goals: soft skills

### Contents

This course provides a comprehensive exploration of advanced data mining techniques tailored for media data analysis. Students will delve into methods like affinity mining, latent pattern mining, neural networks, and archetypal analysis to uncover insights in behavioral profiling, recommender systems, and outlier detection. Emphasis is placed on theoretical understanding and practical application through mathematical optimization, interpretable models, and real-world case studies, enabling participants to harness data for impactful digital marketing, fraud detection, and content personalization.

### Prerequisites

#### Recommended:

Basic knowledge of data science, machine learning, and pattern recognition; programming skills; linear algebra.

### Course meetings

Teaching format	Group size	h/week	Workload[h]	CP	
Lecture		2	30 T / 45 S	2.5	T = face-to-face teaching
Exercises		1	15 T / 30 S	1.5	S = independent study

### Graded exams

Written exam (120 minutes) or oral exam.

### Ungraded coursework (required for admission to the exam)

(i) The completion of regularly provided exercise sheets. The work can be done in groups of up to five students. A total of 50% of the points must be achieved. (ii) The completion of a programming project. The work is done in groups of up to five students. The results of the programming project must be presented in class.

### Literature

- Rafet Sifa (2019). Matrix and Tensor Factorization for Profiling Player Behaviour. Independently pressed.
- Jiawei Han, Jian Pei, Micheline Kamber (2012). Data Mining: Concepts and Techniques. 3rd Ed., Elsevier Inc.
- Christopher Manning, Prabhakar Raghavan, Hinrich Schütze (2008). Introduction to Information Retrieval. Cambridge University Press.
- Michael Negnevitsky (2019), Artificial Intelligence: A Guide to Intelligent Systems. 3rd Ed., Pearson.
- Ian Goodfellow, Yoshua Bengio, Aaron Courville (2016). Deep Learning. MIT Press..
- Lecture notes of the instructors.

## MA-INF 4201 Artificial Life

<b>Workload</b>	<b>Credit points</b>	<b>Duration</b>	<b>Frequency</b>
180 h	6 CP	1 semester	every year
<b>Module coordinator</b>	<b>Lecturer(s)</b>		
Prof. Dr. Sven Behnke	Dr. Nils Goerke		
<b>Programme</b>	<b>Mode</b>	<b>Semester</b>	
M. Sc. Cyber Security	Optional	1-3.	

### Learning goals: technical skills

Detailed understanding of the most important approaches and principles of artificial life. Knowledge and understanding of the current state of research in the field of artificial life. The students can judge and explain if an Artificial Life approach is feasible for a given class of problems. They can estimate the necessary effort to implement and shape the Artificial Life paradigm w.r.t. the task, and can give an educated estimation of the possible outcome and foreseeable limitations of the approach. They can implement the basic fundamental Artificial Life paradigms.

### Learning goals: soft skills

Capability to identify the state of the art in artificial life, and to present and defend the found solutions within the exercises in front of a group of students. Critical discussion of the results of the homework.

### Contents

Foundations of artificial life, cellular automata, Conway's "Game of Life"; mechanisms for structural development; foundations of nonlinear dynamical systems, Lindenmeyer-systems, evolutionary methods and genetic algorithms, reinforcement learning, artificial immune systems, adaptive behaviour, self-organising criticality, multi-agent systems, and swarm intelligence, particle swarm optimization.

### Prerequisites

#### Recommended:

Basic knowledge of linear algebra, analysis, logic, automata, and complexity analysis of deterministic and randomised algorithms.

### Course meetings

Teaching format	Group size	h/week	Workload[h]	CP	
Lecture		2	30 T / 45 S	2.5	T = face-to-face teaching
Exercises		2	30 T / 75 S	3.5	S = independent study

### Graded exams

Written exam (100 minutes)

### Ungraded coursework (required for admission to the exam)

The completion of regularly provided exercise sheets. The work can be done in groups of up to four students. A total of 50% of the points must be achieved. Each student must present a solution to an exercise in the exercise sessions twice.

### Forms of media

Pencil and paper work, explain solutions in front of the exercise group, implementation of small programs, use of simple simulation tools.

### Literature

- Christoph Adami: Introduction to Artificial Life, The Electronic Library of Science, TELOS, Springer-Verlag
- Eric Bonabeau, Marco Dorigo, Guy Theraulaz: Swarm Intelligence: From Natural to Artificial Systems, Oxford University Press, Santa Fe Institute Studies in the Science of Complexity.
- Andrzej Osyczka: Evolutionary Algorithms for Single and Multicriteria Design Optimization, Studies in Fuzzyness and Soft Computing, Physica-Verlag, A Springer-Verlag Company, Heidelberg

## MA-INF 4204 Technical Neural Nets

<b>Workload</b>	<b>Credit points</b>	<b>Duration</b>	<b>Frequency</b>
180 h	6 CP	1 semester	every year
<b>Module coordinator</b>	<b>Lecturer(s)</b>		
Dr. Nils Goerke	Dr. Nils Goerke		
<b>Programme</b>	<b>Mode</b>	<b>Semester</b>	
M. Sc. Cyber Security	Optional	1. or 2.	

### Learning goals: technical skills

Detailed knowledge of the most important neural network approaches and learning algorithms and its fields of application. Knowledge and understanding of technical neural networks as Non-Von Neumann computer architectures similar to concepts of brain functions at different stages of development. The students can judge and explain if a neural network approach is feasible for a given class of problems. They can estimate the necessary effort to implement and shape the neural approach for a given task and can give an educated estimation of the possible outcome and foreseeable limitations of that approach. They can implement the basic neural network approaches and neural learning paradigms.

### Learning goals: soft skills

The students will be capable to propose several paradigms from neural networks that are capable to solve a given task. They can discuss the pro and cons with respect to efficiency and risk. They will be capable to plan and implement a small project with state of the art neural network solutions. Capability to identify the state of the art in neural network research. Capability to present and defend the found solutions within the exercises in front of a group of students. Critical discussion of the results of the homework.

### Contents

Multi-layer perceptron, radial-basis function nets, Hopfield nets, self organizing maps (Kohonen), adaptive resonance theory, learning vector quantization, recurrent networks, back-propagation of error, reinforcement learning, Q-learning, support vector machines, pulse processing neural networks. Exemplary applications of neural nets: function approximation, prediction, quality control, image processing, speech processing, action planning, control of technical processes and robots. Implementation of neural networks in hardware and software: tools, simulators, analog and digital neural hardware.

### Prerequisites

#### Recommended:

Basic knowledge of linear algebra, analysis, logic, automata, complexity analysis of deterministic and randomised algorithms, and practical and theoretical foundations of machine learning.

### Course meetings

Teaching format	Group size	h/week	Workload[h]	CP	
Lecture		2	30 T / 45 S	2.5	T = face-to-face teaching
Exercises		2	30 T / 75 S	3.5	S = independent study

### Graded exams

Written exam (100 minutes)

### Ungraded coursework (required for admission to the exam)

The completion of regularly provided exercise sheets. The work can be done in groups of up to four students. A total of 50% of the points must be achieved. Each student must present a solution to an exercise in the exercise sessions twice.

### Forms of media

Pencil and paper work, explaining solutions in front of the exercise group, implementation of small programs, use of simple simulation tools

**Literature**

- Christopher M. Bishop: Neural Networks for Pattern Recognition, Oxford University Press, ISBN-10: 0198538642, ISBN-13: 978-0198538646
  - Ian T. Nabney: NETLAB. Algorithms for Pattern Recognition, Springer, ISBN-10: 1852334401, ISBN-13: 978-1852334406
  - David Kriesel: A brief Introduction on Neural Networks, [http://www.dkriesel.com/en/science/neural\\_networks](http://www.dkriesel.com/en/science/neural_networks)
  - David Kriesel: Ein kleiner Überblick über Neuronale Netze, [http://www.dkriesel.com/science/neural\\_networks](http://www.dkriesel.com/science/neural_networks)
  - Simon Haykin: Neural Networks, and Learning Machines, 3rd Edition, Prentice Hall International Editions.
-

## MA-INF 4208 Seminar Vision Systems

Workload	Credit points	Duration	Frequency
120 h	4 CP	1 semester	every semester
Module coordinator	Lecturer(s)		
Prof. Dr. Sven Behnke	Prof. Dr. Sven Behnke, Dr. Nils Goerke		
Programme	Mode	Semester	
M. Sc. Cyber Security	Optional	2. or 3.	

### Learning goals: technical skills

- Knowledge in advanced topics in the area of technical vision systems, such as image segmentation, feature extraction, and object recognition.
- Ability to understand new research results presented in original scientific papers and to present them in a research talk as well as in a seminar report.

### Learning goals: soft skills

Self-competences (time management, literature search, self-study), communication skills (preparation and clear didactic presentation of research talk, scientific discussion, structured writing of seminar report), social skills (ability to formulate and accept criticism, critical examination of research results).

### Contents

Current research papers from conferences and journals in the field of vision systems covering fundamental techniques and applications.

### Prerequisites

#### Recommended:

At least one of the following:

- MA-INF 2201 - Computer Vision
- MA-INF 4111 – Principles of Machine Learning
- MA-INF 4204 – Technical Neural Nets

### Course meetings

Teaching format	Group size	h/week	Workload[h]	CP	
Seminar	10	2	30 T / 90 S	4	T = face-to-face teaching S = independent study

### Graded exams

Oral presentation, written report

### Ungraded coursework (required for admission to the exam)

Attendance in course sessions in accordance with the exam regulations of 2023, § 12(6).

### Literature

- R. Szeliski: Computer Vision: Algorithms and Applications, Springer 2010.
- C. M. Bishop: Pattern Recognition and Machine Learning, Springer 2006.
- D. A. Forsyth and J. Ponce: Computer Vision: A Modern Approach, Prentice Hall, 2003.

## MA-INF 4209 Seminar Principles of Data Mining and Learning Algorithms

Workload	Credit points	Duration	Frequency
120 h	4 CP	1 semester	every year
Module coordinator	Lecturer(s)		
Prof. Dr. Stefan Wrobel	Prof. Dr. Stefan Wrobel, PD Dr. Michael Mock, Dr. Florian Seiffarth, Dr. Tamas Horvath		
Programme	Mode	Semester	
M. Sc. Cyber Security	Optional	2. or 3.	

### Learning goals: technical skills

Enhanced and in-depth knowledge in specialized topics in the area of machine learning and data mining.

### Learning goals: soft skills

Acquire the competence to independently search for and study state-of-the-art scientific literature in depth, read critically, identify the most relevant content, and assess research results in the context of the corresponding research area; to discuss research results with a knowledgeable scientific audience; to present prior work by others in writing and in presentations with visual media in a way that adheres to academic standards, that is well-structured and didactically effective, and that motivates the audience to participate; to formulate and accept criticism; to manage one's time with relatively open assignments and long-ranging deadlines.

### Contents

Theoretical, statistical and algorithmical principles of data mining and learning algorithms. Search and optimization algorithms. Specialized learning algorithms from the frontier of research. Fundamental results from neighbouring areas.

### Prerequisites

#### Recommended:

Knowledge of basic notions and algorithms from machine learning and data mining. It is recommend to first take at least one of the following modules:

- MA-INF 4111 – Principles of Machine Learning
- MA-INF 4112 – Algorithms for Data Science

### Course meetings

Teaching format	Group size	h/week	Workload[h]	CP	
Seminar	10	2	30 T / 90 S	4	T = face-to-face teaching S = independent study

### Graded exams

Oral presentation, written report

### Ungraded coursework (required for admission to the exam)

Attendance in course sessions in accordance with the exam regulations of 2023, § 12(6).

### Forms of media

Scientific papers and websites, interactive presentations.

### Literature

The relevant literature will be announced towards the end of the previous semester.

## MA-INF 4211 Seminar Cognitive Robotics

Workload	Credit points	Duration	Frequency
120 h	4 CP	1 semester	every semester
Module coordinator	Lecturer(s)		
Prof. Dr. Sven Behnke	Prof. Dr. Sven Behnke, Dr. Raphael Memmesheimer		
Programme	Mode	Semester	
M. Sc. Cyber Security	Optional	2. or 3.	

### Learning goals: technical skills

Knowledge in advanced topics in the area of cognitive robotics, such as robot perception, action planning, and robot learning.

Ability to understand new research results presented in original scientific papers and to present them in a research talk as well as in a seminar report.

### Learning goals: soft skills

Self-competences (time management, literature search, self-study), communication skills (preparation and clear didactic presentation of research talk, scientific discussion, structured writing of seminar report), social skills (ability to formulate and accept criticism, critical examination of research results).

### Contents

Current research papers from conferences and journals in the field of cognitive robotics covering fundamental techniques and applications.

### Prerequisites

#### Recommended:

At least 1 of the following:

- MA-INF 4113 – Cognitive Robotics
- MA-INF 4114 – Robot Learning

### Course meetings

Teaching format	Group size	h/week	Workload[h]	CP	
Seminar	10	2	30 T / 90 S	4	T = face-to-face teaching S = independent study

### Graded exams

Oral presentation, written report

### Ungraded coursework (required for admission to the exam)

Attendance in course sessions in accordance with the exam regulations of 2023, § 12(6).

### Literature

- S. Thrun, W. Burgard and D. Fox: Probabilistic Robotics. MIT Press, 2005.
- B. Siciliano, O. Khatib (Eds.): Springer Handbook of Robotics, 2008.
- Selected papers.

## MA-INF 4213 Seminar Humanoid Robots

Workload	Credit points	Duration	Frequency
120 h	4 CP	1 semester	every semester
Module coordinator	Lecturer(s)		
Prof. Dr. Maren Bennewitz	Prof. Dr. Maren Bennewitz		
Programme	Mode	Semester	
M. Sc. Cyber Security	Optional	2. or 3.	

### Learning goals: technical skills

Enhanced and in-depth knowledge in specialized topics in the area of humanoid robotics, such as perception, state estimation, navigation, manipulation, and motion planning.

### Learning goals: soft skills

Self-competences (time management, literature search, self-study), communication skills (preparation of the talk, clear didactic presentation of techniques and experimental results, scientific discussion, structured writing of summary), social skills (ability to formulate and accept criticism, critical examination of algorithms and experimental results).

### Contents

Current research papers from conferences and journals in the field of humanoid robotics covering fundamental techniques and applications.

### Prerequisites

#### Recommended:

At least 1 of the following:

- MA-INF 4215 – Humanoid Robotics
- MA-INF 4113 – Cognitive Robotics

### Course meetings

Teaching format	Group size	h/week	Workload[h]	CP	
Seminar	10	2	30 T / 90 S	4	T = face-to-face teaching S = independent study

### Graded exams

Oral presentation, written report

### Ungraded coursework (required for admission to the exam)

Attendance in course sessions in accordance with the exam regulations of 2023, § 12(6).

### Literature

- S. Thrun, W. Burgard and D. Fox: Probabilistic Robotics. MIT Press
- B. Siciliano, O. Khatib (Eds.): Springer Handbook of Robotics
- K. Harada, E. Yoshida, K. Yokoi (Eds.), Motion Planning for Humanoid Robots, Springer
- Selected papers.

## MA-INF 4214 Lab Humanoid Robots

Workload	Credit points	Duration	Frequency
270 h	9 CP	1 semester	every semester
Module coordinator	Lecturer(s)		
Prof. Dr. Maren Bennewitz	Prof. Dr. Maren Bennewitz		
Programme	Mode	Semester	
M. Sc. Cyber Security	Optional	2. or 3.	

### Learning goals: technical skills

Design and implementation of perception, state estimation, navigation, manipulation, and motion planning techniques for humanoid robots.

### Learning goals: soft skills

Ability to analyze problems theoretically and to find creative and practical solutions; to examine one's solutions and results critically; to prepare readable documentation of software and research results; to present, defend and discuss design decisions and results in the team/group and to other students clearly and in accordance with academic standards; to collaborate constructively with others in small teams over a longer period of time;

### Contents

Robot middleware, perception, state estimation, navigation, manipulation, and motion planning for humanoid robots.

### Prerequisites

#### Recommended:

At least 1 of the following:

- MA-INF 4215 – Humanoid Robotics
- MA-INF 4113 – Cognitive Robotics

### Course meetings

Teaching format	Group size	h/week	Workload[h]	CP	
Lab	8	4	60 T / 210 S	9	T = face-to-face teaching S = independent study

### Graded exams

Oral presentation, written report

### Ungraded coursework (required for admission to the exam)

Project work; attendance in course sessions in accordance with the exam regulations of 2023, § 12(6).

### Literature

- S. Thrun, W. Burgard and D. Fox: Probabilistic Robotics. MIT Press
- B. Siciliano, O. Khatib (Eds.): Springer Handbook of Robotics
- K. Harada, E. Yoshida, K. Yokoi (Eds.), Motion Planning for Humanoid Robots, Springer
- Selected papers.

## MA-INF 4215 Humanoid Robotics

<b>Workload</b>	<b>Credit points</b>	<b>Duration</b>	<b>Frequency</b>
180 h	6 CP	1 semester	at least every 2 years
<b>Module coordinator</b>	<b>Lecturer(s)</b>		
Prof. Dr. Maren Bennewitz	Prof. Dr. Maren Bennewitz		
<b>Programme</b>	<b>Mode</b>	<b>Semester</b>	
M. Sc. Cyber Security	Optional	2. or 3.	

### Learning goals: technical skills

This lecture covers techniques for humanoid robots such as perception, navigation, and motion planning. After the lecture, the students will be able to understand and implement techniques that enable humanoid robots to autonomously navigate in human environments as well as perceive, represent, and manipulate objects.

### Learning goals: soft skills

Communicative skills (oral and written presentation of solutions, discussions in small teams), ability to analyze problems.

### Contents

Sensing and perception, environment representations, active perception, inverse kinematics, motion planning, grasping, balance control, walking, and footstep planning.

### Prerequisites

#### Recommended:

MA-INF 4113 – Cognitive Robotics

### Course meetings

Teaching format	Group size	h/week	Workload[h]	CP	
Lecture		2	30 T / 45 S	2.5	T = face-to-face teaching
Exercises		2	30 T / 75 S	3.5	S = independent study

### Graded exams

Written exam (90 minutes)

### Ungraded coursework (required for admission to the exam)

The completion of regularly provided exercise sheets. The work can be done in groups of up to three students. A total of 50% of the points must be achieved.

### Literature

- S. Thrun, W. Burgard and D. Fox: Probabilistic Robotics. MIT Press, 2005.
- B. Siciliano, O. Khatib (Eds.): Springer Handbook of Robotics
- K. Harada, E. Yoshida, K. Yokoi (Eds.), Motion Planning for Humanoid Robots, Springer
- Selected research papers.

## MA-INF 4228 Foundations of Data Science

Workload	Credit points	Duration	Frequency
270 h	9 CP	1 semester	every year
Module coordinator	Lecturer(s)		
Prof. Dr. Lucie Flek	Prof. Dr. Lucie Flek		
Programme	Mode	Semester	
M. Sc. Cyber Security	Optional	1-3.	

### Learning goals: technical skills

Knowledge: Peculiarities of high dimensional spaces in geometry and probabilities. Singular vector decomposition. Basics in machine learning and clustering.

Skills: Understanding of mathematical tools.

Competences: Application to data science problems and ability to assess similar methods.

### Learning goals: soft skills

Oral presentation (in tutorial groups), written presentation (of exercise solutions), team collaboration in solving homework problems, critical assessment

### Contents

Data science aims at making sense of big data. To that end, various tools have to be understood for helping in analyzing the arising structures.

Often data comes as a collection of vectors with a large number of components. To understand their common structure is the first main objective of understanding the data. The geometry and the linear algebra behind them becomes relevant and enlightning. Yet, the intuition from low-dimensional space turns out to be often misleading. We need to be aware of the particular properties of high-dimensional spaces when working with such data. Fruitful methods for the analysis include singular vector decomposition from linear algebra and supervised and unsupervised machine learning.

### Prerequisites

#### Recommended:

Basic skills in linear algebra and stochastics.

### Course meetings

Teaching format	Group size	h/week	Workload[h]	CP	
Lecture		4	60 T / 105 S	5.5	T = face-to-face teaching S = independent study
Exercises		2	30 T / 75 S	3.5	

### Graded exams

Written exam (120 minutes)

### Ungraded coursework (required for admission to the exam)

The completion of regularly provided exercise sheets. A total of 50% of the points must be achieved. Each student must present a solution to an exercise in the exercise sessions twice.

### Literature

Avrim Blum, John Hopcroft, and Ravindran Kannan (2018+). Foundations of Data Science.

## MA-INF 4230 Advanced Methods of Information Retrieval

Workload	Credit points	Duration	Frequency
180 h	6 CP	1 semester	at least every 2 years
Module coordinator	Lecturer(s)		
Prof. Dr. Elena Demidova	Prof. Dr. Elena Demidova		
Programme	Mode	Semester	
M. Sc. Cyber Security	Optional	1. or 2.	

### Learning goals: technical skills

This module introduces the students to the advanced methods, data structures, and algorithms of information retrieval for structured and semi-structured data (including, for example, knowledge graphs, relational data, and tabular data).

At the end of the module, the students will be capable of choosing appropriate data structures and retrieval algorithms for specific applications and correctly apply relevant statistical and machine learning-based information retrieval procedures.

### Learning goals: soft skills

Communication skills: oral and written presentation and discussion of solutions.

Self-competences: ability to analyse and solve problems.

### Contents

The module topics include data structures, ranking methods, and efficient algorithms that enable end-users to effectively obtain the most relevant search results from structured, heterogeneous, and distributed data sources. Furthermore, we will study the corresponding evaluation techniques as well as novel applications.

### Prerequisites

#### Recommended:

Basic knowledge of data science and machine learning; programming skills. Recommended reading:

- Sarah Boslaugh. Statistics in a Nutshell. A Desktop Quick Reference, O'Reilly Media, Inc., 2nd Edition, (2012).
- Ethem Alpaydin. Machine Learning. The MIT Press (2021).

### Course meetings

Teaching format	Group size	h/week	Workload[h]	CP	
Lecture		2	30 T / 45 S	2.5	T = face-to-face teaching
Exercises		2	30 T / 75 S	3.5	S = independent study

### Graded exams

Written exam (120 minutes)

### Ungraded coursework (required for admission to the exam)

The completion of regularly provided exercise sheets. The work can be done in groups of up to three, four or five students, depending on the total number of students taking the course. A total of 50% of the points must be achieved. For 80% of the exercise sheets, 40% of the points must be achieved for each sheet. Each student must present a solution to an exercise in the exercise sessions once.

**Literature**

Selected chapters from:

- Christopher D. Manning, Prabhakar Raghavan and Hinrich Schütze, Introduction to Information Retrieval, Cambridge University Press. 2008.
- Bhaskar Mitra and Nick Craswell (2018), "An Introduction to Neural Information Retrieval ", Foundations and Trends<sup>so</sup> in Information Retrieval: Vol. 13: No. 1, pp 1-126.
- Ridho Reinanda, Edgar Meij and Maarten de Rijke (2020), "Knowledge Graphs: An Information Retrieval Perspective", Foundations and Trends<sup>so</sup> in Information Retrieval: Vol. 14: No. 4, pp 289-444.
- Jeffrey Xu Yu, Lu Qin, Lijun Chang. Keyword Search in Databases. Synthesis Lectures on Data Management. Morgan & Claypool Publishers. 2009.

Further references to relevant material will be provided during the lecture.

---

## MA-INF 4231 Seminar Advanced Topics in Information Retrieval

Workload	Credit points	Duration	Frequency
120 h	4 CP	1 semester	at least every 2 years
Module coordinator	Lecturer(s)		
Prof. Dr. Elena Demidova	Prof. Dr. Elena Demidova		
Programme	Mode	Semester	
M. Sc. Cyber Security	Optional	2. or 3.	

### Learning goals: technical skills

Enhanced and in-depth knowledge in specialized topics in the area of information retrieval, including understanding of information retrieval process, specialized data representation methods, advanced retrieval methods, evaluation techniques, and domain-specific applications.

### Learning goals: soft skills

Acquire the competence to independently search for and study state-of-the-art scientific literature in depth, read critically, identify the most relevant content, and assess research results in the context of the corresponding research area; to discuss research results with a knowledgeable scientific audience; to present prior work by others in writing and in presentations with visual media in a way that adheres to academic standards, that is well-structured and didactically effective, and that motivates the audience to participate; to formulate and accept criticism; to manage one's time with relatively open assignments and long-ranging deadlines.

### Contents

Statistical and machine learning-based information retrieval methods, including typical steps of the information retrieval process: data collection, feature extraction, indexing, retrieval, ranking, and evaluation. Specialized data representation and retrieval methods for selected data types and applications in specific domains.

### Prerequisites

#### Recommended:

MA-INF 4230 - Advanced Methods of Information Retrieval.

### Course meetings

Teaching format	Group size	h/week	Workload[h]	CP	
Seminar	10	2	30 T / 90 S	4	T = face-to-face teaching S = independent study

### Graded exams

Oral presentation, written report

### Ungraded coursework (required for admission to the exam)

Attendance in course sessions in accordance with the exam regulations of 2023, § 12(6).

### Literature

Selected chapters from:

- Christopher D. Manning, Prabhakar Raghavan and Hinrich Schütze, Introduction to Information Retrieval, Cambridge University Press. 2008.
- Bhaskar Mitra and Nick Craswell (2018), "An Introduction to Neural Information Retrieval ", Foundations and Trends<sup>SM</sup> in Information Retrieval: Vol. 13: No. 1, pp 1-126.

Further relevant literature will be announced at the beginning of the seminar.

---

**MA-INF 4232 Lab Information Retrieval in Practice**


---

Workload	Credit points	Duration	Frequency
270 h	9 CP	1 semester	every year
Module coordinator	Lecturer(s)		
Prof. Dr. Elena Demidova	Dr. Rajjat Dadwal		
Programme	Mode	Semester	
M. Sc. Cyber Security	Optional	2. or 3.	

**Learning goals: technical skills**

This module concentrates on practical experience in information retrieval. Participants acquire basic knowledge and practical experience in designing and implementing information retrieval systems for specific data types and applications.

**Learning goals: soft skills**

Communication skills: the ability to work in teams.

Self-competences: the ability to analyse problems and find practical solutions. Time management, creativity, presentation of results.

**Contents**

Practical application of information retrieval methods to solve retrieval problems on real-world data and evaluate proposed solutions.

**Prerequisites**
**Recommended:**

MA-INF 4230 - Advanced Methods of Information Retrieval

**Course meetings**

Teaching format	Group size	h/week	Workload[h]	CP
Lab	8	4	60 T / 210 S	9

T = face-to-face teaching  
S = independent study

**Graded exams**

Oral presentation, written report

**Ungraded coursework (required for admission to the exam)**

Project work; attendance in course sessions in accordance with the exam regulations of 2023, § 12(6).

**Literature**

Selected chapters from:

- Christopher D. Manning, Prabhakar Raghavan and Hinrich Schütze, Introduction to Information Retrieval, Cambridge University Press. 2008.
- Bhaskar Mitra and Nick Craswell (2018), "An Introduction to Neural Information Retrieval ", Foundations and Trends<sup>o</sup> in Information Retrieval: Vol. 13: No. 1, pp 1-126.

Further references to relevant material will be provided during the lab.

---

## MA-INF 4241 Lab Cognitive Modelling of Biological Agents

Workload	Credit points	Duration	Frequency
270 h	9 CP	1 semester	every semester
Module coordinator	Lecturer(s)		
Prof. Dr. Dr. Dominik Bach	Prof. Dr. Dr. Dominik Bach		
Programme	Mode	Semester	
M. Sc. Cyber Security	Optional	2. or 3.	

### Learning goals: technical skills

- Cognitive modelling workflow in computational neuroscience.
- Analysis of real-life cognitive tasks.
- Reasoning about different problem solutions.
- Understanding constraints of biological systems.

### Learning goals: soft skills

Ability to analyze problems theoretically and to find creative and practical solutions; to examine one's solutions and results critically; to classify one's own results into the state-of-the-art of the respective area; to prepare readable documentation of software and research results; to present, defend and discuss design decisions and results in the team/group and to other students clearly and in accordance with academic standards; to collaborate constructively with others in small teams over a longer period of time; to aim at long-range goals under limited resources; to work under pressure.

### Contents

The goal of cognitive modelling in computational neuroscience is to reverse-engineer how a real neural system solves a given cognitive task, often using reinforcement learning theory as a starting point. This lab covers the entire cognitive modelling workflow as used in computational neuroscience. Students will address an interesting cognitive problem by (a) developing rational solutions drawing on reinforcement learning, or descriptive solutions drawing on cognitive science and mathematical psychology, (b) derive behavioural signatures of this solution by mathematical analysis or computational simulation, (c) design efficient experiments to disambiguate these solutions from real behaviour, and (d) potentially analyse existing data sets. The course emphasises a practical, application-focused approach. Students collaborate in teams of 2, each supervised by a CAIAN researcher.

### Prerequisites

#### Recommended:

One out of:

- MA-INF 4113 Cognitive Robotics
- MA-INF 4114 Robot Learning
- MA-INF 4215 Humanoid Robotics
- MA-INF 4235 Reinforcement Learning

### Course meetings

Teaching format	Group size	h/week	Workload[h]	CP
Lab	8	4	60 T / 210 S	9

T = face-to-face teaching  
S = independent study

### Graded exams

Oral presentation, written report

### Ungraded coursework (required for admission to the exam)

Project work; attendance in course sessions in accordance with the exam regulations of 2023, § 12(6).

## MA-INF 4242 Self-supervised Learning

Workload	Credit points	Duration	Frequency
180 h	6 CP	1 semester	every year
Module coordinator	Lecturer(s)		
JProf. Dr. Hermann Blum	JProf. Dr. Hermann Blum		
Programme	Mode	Semester	
M. Sc. Cyber Security	Optional	2. or 3.	

### Learning goals: technical skills

Students can list and explain different fundamental unsupervised, self-supervised machine learning models and can justify a choice of model for a given problem. Students can list and explain different techniques of self-supervision and semi-supervision. For a given data source and task, they can evaluate if a technique is applicable and implement it based on established software frameworks.

### Learning goals: soft skills

Communicative skills (discussions in small teams), self competences (ability to accept and formulate criticism, ability to analyze problems).

### Contents

The course covers a broad range of methods to learn from unlabelled data with a focus on deep neural networks and hybrid methods.

Models: Nearest Neighbors, Clustering, Autoencoders, (pretrained) Neural Networks, Generative Models

Self-Supervision Techniques: Denoising, Masking, Pre-text Tasks, Distillation, Cycleconsistency, Contrastive Learning, Pseudo-Labeling, System-level Self-Supervision.

### Prerequisites

#### Recommended:

It is recommended that the students have:

- knowledge of foundations of artificial intelligence and deep learning.

It is recommended to first complete the following module:

- MA-INF 4111 Principles of Machine Learning.

### Course meetings

Teaching format	Group size	h/week	Workload[h]	CP	
Lecture		2	30 T / 45 S	2.5	T = face-to-face teaching S = independent study
Exercises		2	30 T / 75 S	3.5	

### Graded exams

Written exam (120 min)

### Ungraded coursework (required for admission to the exam)

none

### Literature

- scikit-learn User Guide.
- I. Goodfellow, Y. Bengio and A. Courville: Deep Learning. MIT Press, 2016.
- Balestriero et al.: A Cookbook of Self-Supervised Learning, 2023.

## MA-INF 4243 Mining Media Data II

Workload	Credit points	Duration	Frequency
120 h	4 CP	1 semester	every year
Module coordinator	Lecturer(s)		
Prof. Dr. Rafet Sifa	Prof. Dr. Rafet Sifa, Dr. Lorenz Sparrenberg		
Programme	Mode	Semester	
M. Sc. Cyber Security	Optional	2. or 3.	

### Learning goals: technical skills

By the end of the course, students will be able to:

- Understand and implement advanced data mining techniques for predictive and prescriptive analytics.
- Employ large language models and transformer-based architectures for tasks like text analysis, classification, and summarization.
- Apply knowledge distillation techniques to optimize and deploy machine learning models in resource-constrained environments.
- Analyze media data effectively to derive insights and support decision-making in real-world applications, including digital marketing and fraud detection.
- Address challenges in media analytics, such as ethical considerations, model interpretability, and efficient resource use.

### Learning goals: soft skills

### Contents

This course explores advanced techniques in data mining, emphasizing predictive and prescriptive methods applied to media data. Students will learn to analyze large and complex datasets using state-of-the-art machine learning methodologies, including behavioral prediction, knowledge distillation, and large language models (LLMs). The curriculum includes foundational concepts, text representation learning, transformer architectures, and practical applications in media analytics, such as recommendation systems and information extraction. The course combines theoretical instruction with hands-on exercises to develop both technical and analytical skills relevant to industry and research.

### Prerequisites

#### Recommended:

Basic knowledge of data science, machine learning, and pattern recognition; programming skills; linear algebra. Completion of MA-INF 4117 - Mining Media Data I is recommended but not mandatory.

### Course meetings

Teaching format	Group size	h/week	Workload[h]	CP	
Lecture		2	30 T / 45 S	2.5	T = face-to-face teaching
Exercises		1	15 T / 30 S	1.5	S = independent study

### Graded exams

Written exam (120 min) or oral exam.

### Ungraded coursework (required for admission to the exam)

(i) The completion of regularly provided exercise sheets. The work can be done in groups of up to five students. A total of 50% of the points must be achieved. (ii) The completion of a programming project. The work is done in groups of up to five students. The results of the programming project must be presented in class.

## MA-INF 4304 Lab Cognitive Robotics

Workload	Credit points	Duration	Frequency
270 h	9 CP	1 semester	every semester
Module coordinator	Lecturer(s)		
Prof. Dr. Sven Behnke	Prof. Dr. Sven Behnke, Dr. Raphael Memmesheimer		
Programme	Mode	Semester	
M. Sc. Cyber Security	Optional	2. or 3.	

### Learning goals: technical skills

Participants acquire practical experience and in-depth knowledge in the design and implementation of perception and control algorithms for complex robotic systems. In a small group, they analyze a problem, realize a state-of-the-art solution, and evaluate its performance.

### Learning goals: soft skills

Self-competences (time management, goal-oriented work, ability to analyze problems and to find practical solutions), communication skills (Work together in small teams, oral and written presentation of solutions, critical examination of implementations)

### Contents

Robot middleware (ROS), simultaneous localization and mapping (SLAM), 3D representations of objects and environments, object detection and recognition, person detection and tracking, action recognition, action planning and control, mobile manipulation, human-robot interaction.

### Prerequisites

#### Recommended:

At least 1 of the following:

- MA-INF 4113 – Cognitive Robotics
- MA-INF 4114 – Robot Learning

### Course meetings

Teaching format	Group size	h/week	Workload[h]	CP	
Lab	8	4	60 T / 210 S	9	T = face-to-face teaching S = independent study

### Graded exams

Oral presentation, written report

### Ungraded coursework (required for admission to the exam)

Project work; attendance in course sessions in accordance with the exam regulations of 2023, § 12(6).

### Literature

- S. Thrun, W. Burgard and D. Fox: Probabilistic Robotics. MIT Press, 2005.
- B. Siciliano, O. Khatib (Eds.): Springer Handbook of Robotics, 2008.
- Selected research papers.

## MA-INF 4306 Lab Development and Application of Data Mining and Learning Systems

Workload	Credit points	Duration	Frequency
270 h	9 CP	1 semester	every semester
Module coordinator	Lecturer(s)		
Prof. Dr. Stefan Wrobel	Prof. Dr. Stefan Wrobel		
Programme	Mode	Semester	
M. Sc. Cyber Security	Optional	2. or 3.	

### Learning goals: technical skills

Students will acquire in-depth knowledge in the design, implementation, and experimental evaluation of machine learning and data mining systems. They learn how to work with existing state-of-the-art machine learning and data mining algorithms and apply them to real-world and synthetic datasets, usually extending them for the requirements of their particular learning/mining task.

### Learning goals: soft skills

Ability to analyze problems theoretically and to find creative and practical solutions; to examine one's solutions and results critically; to classify one's own results into the state-of-the-art of the respective area; to prepare readable documentation of software and research results; to present, defend and discuss design decisions and results in the team/group and to other students clearly and in accordance with academic standards; to collaborate constructively with others in small teams over a longer period of time; to aim at long-range goals under limited resources; to work under pressure.

### Contents

Design, adaptation, implementation, and systematic experimental evaluation of specialised data mining and learning algorithms, from classical to state-of-the-art, from all areas of machine learning and data mining. Search and optimization algorithms. Common open source libraries for machine learning and data mining.

### Prerequisites

#### Recommended:

Basic notions and algorithms from machine learning and data mining are required. It is recommended to take at least one of the following courses first:

- MA-INF 4111 – Principles of Machine Learning
- MA-INF 4112 – Algorithms for Data Science

### Course meetings

Teaching format	Group size	h/week	Workload[h]	CP
Lab	8	4	60 T / 210 S	9

T = face-to-face teaching  
S = independent study

### Graded exams

Oral presentation, written report

### Ungraded coursework (required for admission to the exam)

Project work; attendance in course sessions in accordance with the exam regulations of 2023, § 12(6).

### Forms of media

Computer Software, Documentation, Research Papers.

### Literature

The relevant literature will be announced towards the end of the previous semester.

---

**MA-INF 4308 Lab Vision Systems**


---

Workload	Credit points	Duration	Frequency
270 h	9 CP	1 semester	every semester
Module coordinator	Lecturer(s)		
Prof. Dr. Sven Behnke	Prof. Dr. Sven Behnke		
Programme	Mode	Semester	
M. Sc. Cyber Security	Optional	2. or 3.	

**Learning goals: technical skills**

Students will acquire knowledge of the design and implementation of parallel algorithms on GPUs. They will apply these techniques to accelerate standard machine learning algorithms for data-intensive computer vision tasks.

**Learning goals: soft skills**

Self-competences (time management, goal-oriented work, ability to analyze problems and to find practical solutions), communication skills (Work together in small teams, oral and written presentation of solutions, critical examination of implementations)

**Contents**

Basic matrix and vector computations with GPUs (CUDA). Classification algorithms, such as multi-layer perceptrons, support-vector machines, k-nearest neighbors, linear-discriminant analysis. Image preprocessing and data handling. Quantitative performance evaluation of learning algorithms for segmentation and categorization.

**Prerequisites**
**Recommended:**

At least 1 of the following:

MA-INF 2201 - Computer Vision

MA-INF 4111 – Intelligent Learning and Analysis Systems: Machine Learning

MA-INF 4204 – Technical Neural Nets

**Course meetings**

Teaching format	Group size	h/week	Workload[h]	CP	
Lab	8	4	60 T / 210 S	9	T = face-to-face teaching S = independent study

**Graded exams**

Oral presentation, written report

**Ungraded coursework (required for admission to the exam)**

Project work; attendance in course sessions in accordance with the exam regulations of 2023, § 12(6).

**Literature**

- R. Szeliski: Computer Vision: Algorithms and Applications, Springer 2010.
  - C. M. Bishop: Pattern Recognition and Machine Learning, Springer 2006.
  - NVidia CUDA Programming Guide, Version 4.0, 2011.
-

## MA-INF 4322 Lab Machine Learning on Encrypted Data

Workload	Credit points	Duration	Frequency
270 h	9 CP	1 semester	every year
Module coordinator	Lecturer(s)		
Dr. Michael Nüsken	Dr. Michael Nüsken		
Programme	Mode	Semester	
M. Sc. Cyber Security	Optional	2. or 3.	

### Learning goals: technical skills

The students will carry out a practical task (project) in the context of Cryptography, including test and documentation of the implemented software/system.

### Learning goals: soft skills

Ability to properly present and defend design decisions, to prepare readable documentation of software; skills in constructively collaborating with others in small teams over a longer period of time; ability to classify one's own results into the state-of-the-art of the resp. area

### Contents

With the rise of more and more mechanisms and installations of data science methodology to automatically analyze large amounts of possibly privacy infringing data we have to carefully understand how to protect our data. Also more and more fake data shows up and we have to find ways to distinguish faked from trustable data. At the same time we want to allow insightful research and life-easing analyzes to be possible. This seeming contradiction has lead to various efforts for unifying both: protecting data and allowing analyzes, at least to some extent and possibly under some restrictions.

The target of the lab is to understand how computations on encrypted data may work in one particular application that we are choosing together. Ideally, we can come up with a novel solution for performing an unconsidered algorithm. We study the tasks and tools, select algorithms, find a protocol, prototype an implementation, perform a security analysis, present an evaluation.

### Prerequisites

#### Recommended:

Good knowledge in cryptography is vital, e.g. by one or more modules out of:

- MA-INF 1103 - Cryptography,
- MA-INF 1223 - Privacy Enhancing Technologies, and
- MA-INF 1209 - Seminar Advanced Topics in Cryptography.

### Course meetings

Teaching format	Group size	h/week	Workload[h]	CP	
Lab	8	4	60 T / 210 S	9	T = face-to-face teaching S = independent study

### Graded exams

Oral presentation, written report

### Ungraded coursework (required for admission to the exam)

Project work; attendance in course sessions in accordance with the exam regulations of 2023, § 12(6).

## MA-INF 4324 Seminar Advanced Topics in Data Science

Workload	Credit points	Duration	Frequency
120 h	4 CP	1 semester	at least every 2 years
Module coordinator	Lecturer(s)		
Prof. Dr. Elena Demidova	Prof. Dr. Elena Demidova		
Programme	Mode	Semester	
M. Sc. Cyber Security	Optional	2. or 3.	

### Learning goals: technical skills

Enhanced and in-depth knowledge in specialized topics in the data science, including understanding of the data science process, statistical and machine learning-based data analytics methods, specialized data representation techniques, evaluation methods, and domain-specific applications.

### Learning goals: soft skills

Acquire the competence to independently search for and study state-of-the-art scientific literature in depth, read critically, identify the most relevant content, and assess research results in the context of the corresponding research area; to discuss research results with a knowledgeable scientific audience; to present prior work by others in writing and in presentations with visual media in a way that adheres to academic standards, that is well-structured and didactically effective, and that motivates the audience to participate; to formulate and accept criticism; to manage one's time with relatively open assignments and long-ranging deadlines.

### Contents

Statistical and machine learning-based methods of data analytics, including typical steps of the data science process: data generation, integration, cleaning, exploration, modelling and evaluation. Specialized data representation and analytics methods for selected data types and applications in specific domains.

### Prerequisites

#### Recommended:

MA-INF 4328 - Spatio-Temporal Data Analytics

### Course meetings

Teaching format	Group size	h/week	Workload[h]	CP
Seminar	10	2	30 T / 90 S	4

T = face-to-face teaching  
S = independent study

### Graded exams

Oral presentation, written report

### Ungraded coursework (required for admission to the exam)

Attendance in course sessions in accordance with the exam regulations of 2023, § 12(6).

### Literature

Relevant literature will be announced at the beginning of the seminar

---

**MA-INF 4325 Lab Data Science in Practice**


---

Workload	Credit points	Duration	Frequency
270 h	9 CP	1 semester	every year
Module coordinator	Lecturer(s)		
Prof. Dr. Elena Demidova	Dr. Rajjat Dadwal		
Programme	Mode	Semester	
M. Sc. Cyber Security	Optional	2. or 3.	

**Learning goals: technical skills**

This module concentrates on practical experience in data analytics. Participants acquire basic knowledge and practical experience in the design and implementation of data science workflows for specific data types and applications.

**Learning goals: soft skills**

- Communication skills: the ability to work in teams.
- Self-competences: the ability to analyse problems and find practical solutions. Time management, creativity, presentation of results.

**Contents**

Practical application of statistical and machine learning-based methods to solve data analytics problems on real-world datasets and evaluate proposed solutions.

**Prerequisites**
**Recommended:**

MA-INF 4328 - Spatio-Temporal Data Analytics

**Course meetings**

Teaching format	Group size	h/week	Workload[h]	CP
Lab	8	4	60 T / 210 S	9

T = face-to-face teaching  
S = independent study

**Graded exams**

Oral presentation, written report

**Ungraded coursework (required for admission to the exam)**

Project work; attendance in course sessions in accordance with the exam regulations of 2023, § 12(6).

---

## MA-INF 4326 Explainable AI and Applications

Workload	Credit points	Duration	Frequency
180 h	6 CP	1 semester	every year
Module coordinator	Lecturer(s)		
Dr. Rafet Sifa	Prof. Dr. Rafet Sifa, Dr. Lorenz Sparrenberg		
Programme	Mode	Semester	
M. Sc. Cyber Security	Optional	2. or 3.	

### Learning goals: technical skills

- Know the dual-model functioning of the human mind, and two main AI paradigms
- Develop white-box neural AI systems
- Understand the problems and limitations of Blackbox Deep-Learning systems, and Know the state-of-the-art Methods for Interpreting Deep-Learning systems (XAI)

### Learning goals: soft skills

- Know System 1 and 2 of the mind, pros and cons of symbolic AI and connectionist AI
- Develop neural-geometric systems that have both good features of symbolic AI and connectionist AI
- Know the limitation of famous Deep-Learning systems, such as GPT3, self-driving. Know standard methods to explore the explainability of Deep-Learning systems

### Contents

1. Introduction: fates of large Deep-Learning systems, e.g. Watson, GPT, self-driving cars
2. Dual-system theories (System 1 and 2), nine laws of cognition, criteria of semantic models
3. The target and the state-of-art methods of XAI
4. Neural-symbolic AI
5. Cognitive maps, Collages, Mental Spatial Representation, Events
6. Qualitative Spatial Representation and Reasoning
7. Rotating Sphere Embedding: A New Wheel for Neural-Symbolic Unification
8. Neural Syllogistic Reasoning
9. Recognizing Variable Environments
10. Humor Understanding
11. Rotating Spheres as building-block semantic components for Language, Vision, and Action

### Prerequisites

none

### Course meetings

Teaching format	Group size	h/week	Workload[h]	CP	
Lecture		2	30 T / 45 S	2.5	T = face-to-face teaching
Exercises		2	30 T / 75 S	3.5	S = independent study

### Graded exams

Written exam (120 minutes)

### Ungraded coursework (required for admission to the exam)

The completion of regularly provided exercise sheets. The work can be done in groups of up to four students. A total of 50% of the points must be achieved.

**Literature**

- Kahneman, D. (2011). Thinking fast and slow. Farrar, Straus and Giroux.
  - Gaedenfors, P. (2017). The Geometry of Meaning. MIT Press.
  - Attardo, Hempelmann, Maio (2003). Script Oppositions and Logical Mechanisms: Modeling Incongruities and their Resolutions, HUMOR 15(1)3–46
  - Tversky, B. (2019). Mind in Motion. Basic Books, New York.
  - Dong, et al. (2020). Learning Syllogism with Euler Neural-Networks. arXiv:2007.07320
  - Dong, T. (2021). A Geometric Approach to the Unification of Symbolic Structure and Neural Networks. Springer.
  - Knauff and Spohn (2021). Handbook of Rationality. MIT Press, Cambridge, MA, USA.
  - Samek et.al. (2019), Explainable AI: Interpreting, Explaining and Visualizing Deep Learning. Springer.
  - Greg Dean (2019). Step by Step to Stand-Up Comedy (Revised Edition). ISBN: 978-0-9897351-7-9
-

## MA-INF 4328 Spatio-Temporal Data Analytics

Workload	Credit points	Duration	Frequency
180 h	6 CP	1 semester	every year
Module coordinator	Lecturer(s)		
Prof. Dr. Elena Demidova	Dr. Rajjat Dadwal, Prof. Dr. Elena Demidova		
Programme	Mode	Semester	
M. Sc. Cyber Security	Optional	1. or 2.	

### Learning goals: technical skills

This module introduces the students to the advanced methods, data structures, and data analytics algorithms for spatio-temporal data. At the end of the module, the students will be capable of choosing appropriate data representations, data structures and algorithms for specific applications and correctly applying relevant statistical and machine learning-based data analytics procedures.

### Learning goals: soft skills

Communication skills: oral and written presentation and discussion of solutions. Self-competences: the ability to analyze and solve problems.

### Contents

The module topics include data structures, data representation and analysis methods, and algorithms that enable analyzing spatio-temporal data and building predictive models effectively and effectively. Furthermore, we will study the corresponding evaluation techniques and novel applications.

### Prerequisites

#### Recommended:

Basic knowledge of data science and machine learning; programming skills. Recommended reading:

- Sarah Boslaugh. Statistics in a Nutshell. A Desktop Quick Reference, O'Reilly Media, Inc., 2nd Edition, (2012).
- Ethem Alpaydin. Machine Learning. The MIT Press (2021).

### Course meetings

Teaching format	Group size	h/week	Workload[h]	CP	
Lecture		2	30 T / 45 S	2.5	T = face-to-face teaching
Exercises		2	30 T / 75 S	3.5	S = independent study

### Graded exams

Written exam (90 minutes)

### Ungraded coursework (required for admission to the exam)

The completion of regularly provided exercise sheets. The work can be done in groups of up to three, four or five students, depending on the total number of students taking the course. A total of 50% of the points must be achieved. For 80% of the exercise sheets, 40% of the points must be achieved for each sheet. Each student must present a solution to an exercise in the exercise sessions once.

## MA-INF 4331 Lab Perception and Learning for Robotics

Workload	Credit points	Duration	Frequency
270 h	9 CP	1 semester	at least every year
Module coordinator	Lecturer(s)		
JProf. Dr. Hermann Blum	JProf. Dr. Hermann Blum		
Programme	Mode	Semester	
M. Sc. Cyber Security	Optional	2. or 3.	

### Learning goals: technical skills

Participants learn how to practically approach a robot perception problem. They learn how to critically read a research paper, how to conduct experiments in the context of robot perception, and how to report and present scientific findings.

### Learning goals: soft skills

Ability to analyze problems theoretically and to find creative and practical solutions; to examine one's solutions and results critically; to classify one's own results into the state-of-the-art of the respective area; to prepare readable documentation of software and research results; to present, defend and discuss design decisions and results in the team/group and to other students clearly and in accordance with academic standards; to collaborate constructively with others in small teams over a longer period of time; to aim at long-range goals under limited resources; to work under pressure.

### Contents

In small groups, students apply their knowledge of robot perception, deep learning, and computer vision to a novel problem. They analyze the problem, read into relevant literature, propose and implement a solution, and empirically test it. They then refine their approach based on an analysis of the experimental outcomes. The course projects are related to one of multiple of the following topics: Robot localization, planning, navigation, manipulation; Practical aspects of Deep Learning; Sensor models, calibration, capture, processing. Software deployment.

### Prerequisites

#### Recommended:

Students are expected to have general programming skills and prior experience with python. Students will need to operate linux terminal systems such as the university's GPU cluster.

It is recommended to first take two of the following modules:

- MA-INF 2201 Computer Vision
- MA-INF 2213 Advanced Computer Vision
- MA-INF 4113 Cognitive Robotics

### Course meetings

Teaching format	Group size	h/week	Workload[h]	CP	
Lab	8	4	60 T / 210 S	9	T = face-to-face teaching S = independent study

### Graded exams

Oral presentation, written report

### Ungraded coursework (required for admission to the exam)

Project work; attendance in course sessions in accordance with the exam regulations of 2023, § 12(6).

### Literature

- S. Thrun, W. Burgard and D. Fox: Probabilistic Robotics. MIT Press, 2005
- I. Goodfellow, Y. Bengio and A. Courville: Deep Learning. MIT Press, 2016
- Per-project assigned literature

## MA-INF 4333 Geometric Deep Learning

Workload	Credit points	Duration	Frequency
180 h	6 CP	1 semester	every year
Module coordinator	Lecturer(s)		
Jun. Prof. Dr. Zorah Lähner	Prof. Dr. Zorah Lähner		
Programme	Mode	Semester	
M. Sc. Cyber Security	Optional	2. or 3.	

### Learning goals: technical skills

- Understanding advanced topics in the design of neural networks using geometric data
- Mathematical modelling of invariances and non-Euclidean domains in deep learning and guarantees that can be derived from these
- Gain an overview of practical applications in which this theory can be applied

### Learning goals: soft skills

- Problem solving skills: ability to identify and utilize analogies between new problems and previously seen ones
- Analytical and abstract thinking: develop a general intuition of computational problems, being able to adopt different perspectives of particular concepts

### Contents

This lecture will cover advanced topics in deep learning focusing on theory related to geometric data and the incorporation of invariances in network architectures. Topics include, among others, permutation invariance, differential geometry, the curse of dimensionality, neural fields and physics-informed neural networks. Students will learn how to process a variety of geometric data structures and implement deep learning algorithms on these related to applications in visual computing, physics and graph processing.

### Prerequisites

#### Recommended:

Students are recommended to have basic knowledge about deep learning and computer vision, for example gained in:

- MA-INF 4111 Principles of Machine Learning,
- MA-INF 2201 Computer Vision, or
- MA-INF 2222 Visual Data Analysis,

and proficiency in python.

### Course meetings

Teaching format	Group size	h/week	Workload[h]	CP	
Lecture		2	30 T / 45 S	2.5	T = face-to-face teaching
Exercises		2	30 T / 75 S	3.5	S = independent study

### Graded exams

Written exam (120 minutes)

### Ungraded coursework (required for admission to the exam)

none

# MA-INF 4334 Computational neuroscience: cognition and behaviour

Workload	Credit points	Duration	Frequency
180 h	6 CP	1 semester	every year
Module coordinator	Lecturer(s)		
Prof. Dr. Dr. Dominik Bach	Prof. Dr. Dr. Dominik Bach		
Programme	Mode	Semester	
M. Sc. Cyber Security	Optional	2-3.	

**Learning goals: technical skills**

- Conceptual knowledge and mathematical understanding of common behavioural and cognitive models from computational neuroscience
- Knowledge of common experimental methods used to develop and disambiguate such models
- Basic knowledge of fundamentals in neuroscience, cognitive/perceptual psychology and microeconomics
- In the exercises, students will learn to implement models and how to use them as benchmarks for bottom-up computational neuroscience models, and for automatic signature-testing of AI algorithms

**Learning goals: soft skills**

- Teamwork (exercises)
- Oral presentation in front of audience (exercises)

**Contents**

The two dominant paradigms in computational neuroscience are bottom-up (starting from the spontaneous behaviour of constituent elements of the nervous system) and top-down (starting from known functions of biological agents). This lecture introduces important topdown models of behaviour and cognition from three perspectives: computational (problem definition and optimal solutions), algorithmic (rational/engineering/descriptive solutions) and implementation (neural hardware). The lecture covers the following domains:

- decision-making with noisy information (value-based, time-integrated, multi-channel, sequential)
- information representation under resource constraints
- memory formation and storage in biological neural networks
- movement planning
- spatial navigation

**Prerequisites**

**Recommended:**

Recommended one out of:

- MA-INF 4113 Cognitive Robotics
- MA-INF 4114 Robot Learning
- MA-INF 4215 Humanoid Robotics
- MA-INF 4235 Reinforcement Learning

**Course meetings**

Teaching format	Group size	h/week	Workload[h]	CP	
Lecture		2	30 T / 45 S	2.5	T = face-to-face teaching
Exercises		2	30 T / 75 S	3.5	S = independent study

**Graded exams**

Written exam

**Ungraded coursework (required for admission to the exam)**

The completion of regularly provided exercise sheets. The work can be done in groups of up to four students. A total of 50% of the points must be achieved. Each group must present a solution to an exercise in the exercise sessions once.

## MA-INF 4335 Lab AI Alignment

Workload	Credit points	Duration	Frequency
270 h	9 CP	1 semester	every year
Module coordinator	Lecturer(s)		
Prof. Dr. Lucie Flek	Prof. Dr. Lucie Flek		
Programme	Mode	Semester	
M. Sc. Cyber Security	Optional	2. or 3.	

### Learning goals: technical skills

Through tutorials and a final project, you will gain hands-on experience in AI alignment techniques and have this chance to apply this knowledge to various interesting projects. Students will collaborate in small teams (a group of 3-4 students) and implement small research projects over the course of the term, advised by a researcher from the CAISA lab. Students will learn to reproduce important results from the field, study the scientific literature, generate and implement their own research ideas, and present their results as a presentation and as a paper.

### Learning goals: soft skills

### Contents

As AI systems such as Large Language Models become increasingly capable and start to be used in high-stakes scenarios, ensuring that they act safely is gaining importance. The research field of AI alignment studies methods to align the behavior and values of AI systems with the user and broader society in a robust, scalable, and interpretable way. The aim of this course is to explore cutting-edge research, insights, and trends in the field of AI alignment.

Schedule:

- Week 0: Organization meeting
- Week 1-5: Lectures and programming exercises
- Week 6: Presentation of project ideas
- Week 12: midterm presentation of results
- Final presentation
- Student paper

Concrete research topics are 1) value alignment, 2) emergent misalignment, 3) scalable oversight, and 4) mechanistic interpretability, among others.

### Prerequisites

#### Recommended:

One of the following courses is recommended:

- MA-INF 4115 - Introduction to Natural Language Processing,
- MA-INF 4235 - Reinforcement Learning,
- MA-INF 4204 - Technical Neural Nets.

### Course meetings

Teaching format	Group size	h/week	Workload[h]	CP	
Lab	8	4	60 T / 210 S	9	T = face-to-face teaching S = independent study

### Graded exams

Oral presentation, written report

### Ungraded coursework (required for admission to the exam)

Project work; attendance in course sessions in accordance with the exam regulations of 2023, § 12(6).

**Literature**

- Hendrycks, Dan: Introduction to AI Safety, Ethics, and Society.
  - Ouyang, Long et al.: Training language models to follow instructions with human feedback.
  - Bowman, Sam et al.: Measuring Progress on Scalable Oversight for Large Language Models.
  - Li, Nathaniel et al.: Measuring and Reducing Malicious Use With Unlearning.
  - Bricken, Trenton et al.: Towards monosemanticity: Decomposing language models with dictionary learning.
-

## MA-INF 4336 Seminar Selected Topics in Natural Language Processing

Workload	Credit points	Duration	Frequency
120 h	4 CP	1 semester	every year
Module coordinator	Lecturer(s)		
Prof. Dr. Lucie Flek	Prof. Dr. Lucie Flek		
Programme	Mode	Semester	
M. Sc. Cyber Security	Optional	2. or 3.	

### Learning goals: technical skills

In this course, students will learn to engage with technical research papers and other material that study the state-of-the-art approaches to Natural Language Processing. They will learn to synthesize, critically assess, and build upon the material by conducting required readings, weekly discussions. In particular:

- to read and examine the scientific literature critically,
- to identify and present examples of relevant real-world application fields of the scientific publication,
- to give a good scientific presentation to peers that is precise, informative, and engaging,
- to summarize and write a concise technical report including a critical discussion of the research paper (with additional literature research).

### Learning goals: soft skills

### Contents

In this weekly seminar, students will learn about selected research topics in natural language processing and its applications. In addition, it is an introduction to reading scientific papers, learning how to give a good presentation, and how to write a technical report.

To better explore how state-of-the-art research presentations can be constructed, as a part of the seminar students will also have a chance to attend and discuss presentations of researchers on more senior level presenting their papers (e.g. guest speakers).

### Prerequisites

#### Recommended:

One of the following courses is recommended (but not obligatory):

- MA-INF 4115 - Introduction to Natural Language Processing,
- MA-INF 4235 - Reinforcement Learning,
- MA-INF 4204 - Technical Neural Nets.

### Remarks

At most 20 participants

### Course meetings

Teaching format	Group size	h/week	Workload[h]	CP	
Seminar	20	2	30 T / 90 S	4	T = face-to-face teaching S = independent study

### Graded exams

Oral presentation, written report.

### Ungraded coursework (required for admission to the exam)

Attendance in course sessions in accordance with the exam regulations of 2023, § 12(6).

### Literature

- Jurafsky & Martin, Speech and Language Processing: <https://web.stanford.edu/~jurafsky/slp3/> .