Master of Science (M.Sc.)

„Business Informatics“

University of Mannheim

– Module catalog –

Appendix

Academic Year

HWS 2020 / FSS 2021

Die folgenden Veranstaltungen wurden nach Veröffentlichung des Modulkatalogs dem Kursprogramm hinzugefügt.

Modulnr.	Name des Moduls	Semester	Sprache	ECTS	Seite
CS 652	Data Security	FSS	English	6	3
CS 654	Internet of Things Security	HWS	English	6	5
CS 655	Cryptography	FSS	English	6	7
CS 719	Seminar on Process Analytics	HWS	English	4	9
IE 692	Advanced Process Mining	FSS	English	6	11
IE 704	Seminar AI Systems Engineering	FSS/HWS	English	4	13
IS 607	Digital Innovation	HWS	English	6	MMM*
IE 676	Network Analysis	HWS	English	6	15

* For a detailed description please use the module catalog of the „Mannheim Master in Management“: http://www.bwl.uni-mannheim.de/en/studium/master_programs/mmm/module_catalog/

CS 652	**Data Security**
Form of module	Lecture with exercises
Type of module	Specialization course
Level	Master
ECTS	6
Workload	Hours per semester present: 56h (4 SWS)
	Self-study: 112h
Prerequisites	There are no formal prerequisites but knowledge in cryptography or IT-security is recommended, e.g., by attending the lectures “Kryptographie I” or “Selected Topics in IT-Security”
Aim of module	Nowadays, users are more and more revealing data to the outside – either willingly as in the context of cloud computing or possibly unconsciously as in the case of the Internet of Things. The aim of the module is to raise awareness by showing various security threats, e.g., traces left in the Internet, but also possible countermeasures, e.g., anonymization of data or the use of dedicated encryption schemes.
Learning outcomes and qualification goals	Expertise: Students will acquire the knowledge to identify security threats and to select and use appropriate countermeasures. (MK2)
	Methodological competence: Successful participants will be able to understand state-of-the-art methods of IT security and cryptography, as well as being able to select, apply and evaluate the most appropriate techniques for a variety of different security-sensitive scenarios. In particular they are able to realize possible risks in new scenarios and to transfer given solutions to these.
	Personal competence: The analytic, concentrated, and precise thinking of the students is trained. By the independent treatment of applications, e.g. in the course of the exercises, their abstraction capacity is further developed and the transfer of the learned material to related questions is trained.

Media	Annotated lecture slides, exercise sheets
Literature	Will be announced in the lecture
Methods	Reworking the lecture and studying the relevant literature in self-study, working together on concrete examples during the lecture, solving exercises in self-study and in practice in cooperation with fellow students
Form of assessment	Written exam
Admission requirements for assessment	-
Duration of assessment	90 minutes
Language	English
Offering	Spring semester
Lecturer	Prof. Dr. Frederik Armknecht
Person in charge	Prof. Dr. Frederik Armknecht
Duration of module	1 semester
Further modules	-
Range of application	M.Sc. Mannheim Master in Data Science, M.Sc. Wirtschaftsinformatik, Lehramt Informatik
Semester	1st/2nd/3rd semester

CS 653	**Internet of Things Security**
Form of module	Lecture and accompanying practical sessions
Type of module	Specialization course
Level	Master
ECTS	6
Workload	4 SWS
	Self-study: 112 h per semester 56 h: pre and post lecture studying and revision • 28 h: practical task completion 28 h: examination preparation
Prerequisites	Programming skills in C or C++
Aim of module	The course provides an introduction to the security of Internet of Things (IoT). It will cover the following topics: • Relevant attacks in the modern Industrial and Consumer IoT environments • Programming of IoT devices • Cryptography suitable for devices with constrained resources • Implementation techniques targeting different goals • IoT standards and protocols
Learning outcomes and qualification goals	Expertise: Students will acquire the knowledge about the most relevant security threats in IoT environments, as well as suitable security solutions
	Methodological competence: analysing and understanding of security weaknesses, implementation of protection mechanisms
	Personal competence: the student has the capability to program IoT devices targeting different optimization goals. The student understands the main attacks on IoT devices together with countermeasures.
Media	Lecture and tutorial slides, exercise sheets
Literature	-
Methods	The course consists of lectures and exercises. At the exercise sessions the students will learn how to implement cryptographic algorithms on Arduino Uno devices which will

	be distributed to each participant. Each student will also receive an individual practical task that needs to be accomplished until the end of the term and the report has to be submitted.
Form of assessment	Practical tasks + oral examination
Admission requirements for assessment	Successful completion of the practical task
Duration of assessment	20 minutes
Language	English
Offering	Fall Semester
Lecturer	Dr. Matthias Hamann, Dr. Vasily Mikhalev, Christian Müller
Person in charge	Dr. Vasily Mikhalev
Duration of module	1 semester
Further modules	-
Range of application	M.Sc. Wirtschaftsinformatik, M.Sc. Mannheim Master in Data Science, Lehramt Informatik
Semester	1st/2nd/3rd semester

CS 654	**Cryptography**
Form of Module	Lecture with Exercise
Type of Module	Specialization Course
Level	Master
ECTS	6
Workload	Hours per semester present: 56 (4 SWS)
	Self-study: 98h (70h lectures/exercises, 28h exam preparation
Prerequitsites	Basis skills in linear algebra, probability theory, algorithms and data structures
Aim of Module	- Basic concepts of cryptography - Mathematical Background - Basics of Information Theory - Block Ciphers (DES, AES, etc.) - Stream Ciphers - Secure Key Exchange Protocols (Diffie-Hellman protocol, etc.) - Public Key encryption (RSA) - Cryptographic Hash Functions - Signature Systems and Message Authentication Codes
Learning Outcomes and qualification goals	Expertise: After the course the students are able to identify security risks in various modern scenarios of data traffic like online banking, wireless communication, online trade ...
	Methodological competence: The students are able to formulate and formalize security goals for various use cases and to choose and to apply appropriate methods to reach these goals. Examples here are to provide data security data encryption, to establish trusted electronical data encryption, to establish trusted electronical communication channels, or to apply methods for secure authentication
	Personal competence: The course trains abstract thinking and the ability to formally model application scenarios. By solving exercises independently, the transfer of the learned material to related questions is promoted.
Media	Exercise sheets and lecture slides available online, blackboard

Literature	- Christof Paar, Bart Preneel, Jan Pelzl: Understanding Cryptography: A Terxtbook for Students and Practitioners, Springer 2009 - Douglas R. Stinson: Cryptography - Theory and Practice, Taylor & Francis, 2005 - Alan G. Konheim: Cryptography: A Primer, John Wiley & Sons, 1981
Methods	Lecture, exercises every two weeks, book studies
Form of assessment	Written or oral examination (TBA)
Admission requirements for assessment	-
Duration of assessment	TBA
Language	English
Offering	FSS
Person in Charge	Prof. Dr. Matthias Krause
Duration of Module	1 Semester
Further Modules	Cryptography II
Range of Application	Msc Business Informatics, Msc Data Science, Lehramt Informatik
Semester	1./2./3. Semester

CS 719	**Seminar on Process Analysis**
Form of Module	Seminar
Type of Module	Seminar
Level	Master
ECTS	5
Workload	150 h per semester
Prerequisites	Any course about process modeling, analysis, or mining
Aim of module	In this seminar, students perform scientific research, either in the form of a literature review or by conducting a small experiment (or a mixture of both), and prepare a written scientific report and presentation about the results. Topics of interest relate to research areas such as process analysis, process mining, stream processing, and robotic process automation. The paper and the presentation are prepared under the guidance of a professor and/or a research staff member. Specific topics shall be suggested by the lecturers, though students are free to make proposals as well.
Learning Outcomes and Qualification Goals	Expertise: • Students will acquire a deep understanding of the research topic. They are expected to describe and summarize the topic in their own words, as well as to judge the contribution of the research papers to ongoing research.
Learning outcomes and qualification goals Media	Methodological competence: Students will develop methods and skills to find relevant literature for their topic, to prepare methodologically sound scientific experiments (if applicable), to write a well-structured scientific paper, and to present their results. Students will also be aware of the need to avoid plagiarism. The key qualification Scientific Research is highly recommended as a prerequisite for the seminar.
	Personal qualification: Students will acquire skills on how to find relevant literature for a research topic, organize a small research task, write a well-structured, concise paper about it and present the results of their work. They will be well prepared to write and present a Master's Thesis.

	Scientific papers and books; presentation with PowerPoint or LaTeX
Literature	Depends on the selected topic of the seminar
Teaching and Learning Methods	Conduct scientific work independently under the guidance of a professor or research staff member
Form of assessment	Seminar report (70%), oral presentation (30%)
Admission requirements for assessment	-
Duration of assessment	N/A
Language	English
Offering	Fall semester
Lecturers	Prof. Dr. Han van der Aa and research staff members
Person in charge	Prof. Dr. Han van der Aa
Duration of module	1 semester
Further modules	-
Range of Application	M. Sc. Wirtschaftsinformatik, M.Sc. Mannheim Master in Data Science
Semester	3rd semester
CS 719	Seminar on Process Analysis

IE 692	**Advanced Process Mining**
Form of Module	Lecture
Type of Module	Specialization course
Level	Master
ECTS	6
Workload	150 h per semester
Prerequisites	Basic programming knowledge, preferably in python, is strongly recommended. Experience with Petri nets, other process model notations, or basic process mining is helpful but not necessary. IS 514 is NOT a prerequisite.
Aim of module	Process mining is an emerging branch of data science that aims at deriving qualitative and quantitative insights on the execution of organizational processes, based on the analysis of recorded event sequences. The course features lectures and exercises that focus on the formal foundations, algorithms, and techniques of process mining. Specifically, this course covers aspects such as: • Process discovery, which aims to derive a process model from recorded events • Conformance checking, which aims to identify deviations between event data and process models • Process enhancement, which aims to augment process models with information on the temporal, organizational, and data perspectives of a process • Predictive monitoring, which aims to make predictions about ongoing process instances • Techniques to preprocess, abstract, cluster event data for improved analyses For the above subjects, the course will cover fundamental algorithms as well as advanced, state-of-the-art techniques. During the exercises that follow each lecture, you will practice through pen-and-paper exercises, as well as implementation and evaluation using open source process mining tools and libraries. • The lectures and exercises are complemented by a practical assignment in which students will work in groups on a project that involves implementation and/or evaluation of a process mining technique.

Learning Outcomes and Qualification Goals	After completing this course, you will be able to: • Understand the importance and potential of process mining • Know and apply both fundamental and advanced techniques for core process mining tasks • Be able to analyze real-world data using open-source process mining tools
Media Literature Teaching and Learning Methods	• Pen-and-paper plus programming exercises (mainly Python). • Project involving open-source process mining tools and libraries, possibly with implementation (in Python or Java) Pen-and-paper exam
	• Wil van der Aalst: Process Mining: Data Science in Action, 2nd edition (Recommended) • Josep Carmona et al. Conformance checking, 1st edition (Recommended) • Additional academic papers suggested per lecture
	• Lectures • Homework exercises to practice with joint discussion in exercise sessions Group project (2-3 students)
Form of assessment	80% written exam 20% group assignment
Admission requirements for assessment	-
Duration of assessment	The exam will take 60 minutes, the assignment will be spread over various weeks with a single deadline towards the end of the semester.
Language	English
Offering	Spring semester
Lecturers	Prof. Dr. Han van der Aa
Person in charge	Prof. Dr. Han van der Aa
Duration of module	1 semester
Further modules	-
Range of Application	M. Sc. Wirtschaftsinformatik, M.Sc. Mannheim Master in Data Science
Semester	2nd semester

IE 704	**Seminar AI Systems Engineering**
Form of Module	Seminar
Type of Module	Seminar
Level	Master
ECTS	4
Workload	120 h per semester
Prerequisites	None
Aim of module	The student prepares a scientific paper and gives a presentation on a current research topic based on published research. State-of-the-art topics are proposed by the supervisors. The paper and the presentation are prepared under the guidance of a research staff member. Active participation in the seminar discussions is expected.
Learning Outcomes and Qualification Goals	<u>Expertise:</u> The student gains a deep understanding of the research topic. He/she is able to describe/summarize the topic in detail in his/her own words. He/she reflects on the topic and judges the contribution of the research papers.
	<u>Methodological competence:</u> The student is able to write a well-structured scientific paper and to present his/her results. He/she is also aware of the need to avoid plagiarism. The key qualification Scientific Research is highly recommended as a prerequisite for the seminar.
	<u>Personal qualification:</u> The student has learned how to write a well-structured, concise paper and give a presentation. This is part of the preparation to write and present a Master's Thesis.
Media	Scientific papers and books; final presentation with PowerPoint
Literature	Depends on the topic of the seminar.
Teaching and Learning Methods	Do scientific work independently under the guidance of a professor or a research staff member. Active discussions in a group of peers.
Form of Assessment	25% Reviews and Discussion 25% Presentation 25% Seminar paper submitted for review 25% "Camera-ready" seminar paper
Admission requirements for assessment	-

Duration of Assessment	N/A
Language	English
Offering	Various seminar topics every semester, see announcements on the chair website.
Lecturers	Dr. Christian Bartelt
Person in charge	Dr. Christian Bartelt
Duration of module	1 Semester
Further modules	-
Range of Application	M.Sc. Wirtschaftsinformatik, M.Sc. Mannheim Master in Data Science
Semester	3. Semester

IE 676	**Network Analysis**
Form of module	Lectures and Accompanying tutorials
Type of module	Elective
Level	Master
ECTS	*6*
Workload	*Hours per semester present: 28h + 46 h (2 + 2 SWS)*
	Self-study: 112 h per semester
Prerequisites	Recommended Knowledge: • Basic Linear Algebra • Basic Computer Programming • Basic Probabilities
Aim of module	Participants will learn about the structure, formation and processes that take place over networks such as social networks, the Web, financial networks, etc. They will learn basic concepts, measures and algorithms for analyzing such structures with a particular focus on the interpretation of the results and their implication in real-life situations.
Learning outcomes and qualification goals	Expertise: Students will acquire knowledge in a broad range of methods for analyzing networked data and their results' interpretation.
	Methodological competence: Successful participants will be able to: • Recognize the existence of networked structure in data; • Select and apply appropriate techniques to explore a networked structure and to analyze network effects like: identify key players, find communities, analyze processes such as diffusion of information, network formation and growth, epidemics, etc. • Interpret the results both theoretically and practically on real-life networks. (MK2, MF3, MF4, MKO1)
	Personal competence: -
Media	Lecture Slides, Exercise Sheets, Blackboard, Books, Software Tools
Literature	• Networks – An Introduction: M. E. J Newman, Oxford University Press, 2010

	• Networks, crowds and markets. Reasoning about a Highly Connected World – David Easley & Jon Kleinberg, Cambridge University Press 2010 • Social and Economic Networks: M.O. Jackson, Princeton University Press 2008
Methods	Lectures, exercises (pen on paper and programming), independent study
Form of assessment	Written examination
Admission requirements for assessment	Successful completion of the programming exercises;
Duration of assessment	90 minutes
Language	English
Offering	Fall semester
Lecturer	*Prof. Dr. Heiner Stuckenschmidt*
Person in charge	*Prof. Dr. Heiner Stuckenschmidt*
Duration of module	1 Semester
Further modules	-
Range of application	M.Sc. Wirtschaftsinformatik
Semester	2.-4.