

**Bachelor of Science (B.Sc.)**

**„Wirtschaftsinformatik“**

der Universität Mannheim

- Modulkatalog -

**Appendix**

Akademisches Jahr

HWS 2019 / FSS 2020

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

<b>Modulnr.</b>	<b>Name des Moduls</b>	<b>Semester</b>	<b>Sprache</b>	<b>ECTS</b>	<b>Seite</b>
CS 408	Selected Topics in IT-Security	FSS	Englisch	6	3
MAN 455	Digital Social Innovation Lab "Young Academy"	FSS	Englisch	6	5
	Präsentationskompetenz und Rhetorik	FSS	Deutsch	2	6
CS 404	Kryptographie I	HWS	Englisch	6	10

CS 408	<b>Selected Topics in IT-Security</b> <i>Selected Topics in IT-Security</i>
Form der Veranstaltung	Lecture with exercises
Typ der Veranstaltung	Vertiefung Informatik
Modulniveau	Bachelor
ECTS	6
Arbeitsaufwand	Präsenzstudium: 56 h pro Semester (4 SWS)
	Eigenstudium: 8 h pro Woche <ul style="list-style-type: none"> <li>• davon Vor- und Nachbereitung der Veranstaltung und freies Selbststudium: 6 h pro Woche</li> <li>• davon Vorbereitung für die Prüfung, z.B. Prüfungs-/Seminarabschlussarbeits- und Präsentationsvorbereitung: 2 h pro Woche</li> </ul>
Vorausgesetzte Kenntnisse	No formal prerequisites. However, knowledge with respect to the content of the following lectures are suggested: Praktische Informatik I und II, Lineare Algebra, Kenntnisse in Programmierung
Lehrinhalte	<p><b>Background and Learning Objectives</b></p> <p>The large-scale deployment of Internet-based services and the open nature of the Internet come alongside with the increase of security threats against existing services. As the size of the global network grows, the incentives of attackers to abuse the operation of online applications also increase and their advantage in mounting successful attacks becomes considerable.</p> <p>These cyber-attacks often target the resources, availability, and operation of online services. In the recent years, a considerable number of online services such as Amazon, CNN, eBay, and Yahoo were hit by online attacks; the losses in revenues of Amazon and Yahoo were almost 1.1 million US dollars. With an increasing number of services relying on online resources, security becomes an essential component of every system.</p> <p><b>Content Description</b></p> <p>This lecture covers the security of computer, software systems, and tamper resistant hardware. The course starts with a basic introduction on encryption functions, spanning both symmetric and</p>

	<p>asymmetric encryption techniques, discusses the security of the current encryption standard AES and explains the concept of Zero-Knowledge proofs. The course then continues with a careful examination of wired and wireless network security issues, and web security threats and mechanisms. This part also extends to analysis of buffer overflows. Finally, the course also covers a set of selected security topics such as trusted computing and electronic voting.</p> <p>Topics:</p> <ul style="list-style-type: none"> <li>• Encryption Schemes (Private Key vs. Public Key, Block cipher security) and Cryptographic Protocols</li> <li>• Cryptanalysis, e.g., side channel attacks</li> <li>• Network Security</li> <li>• Wireless Security</li> <li>• Web Security (SQL, X-Scripting)</li> <li>• Buffer Overflows</li> <li>• Malware &amp; Botnets</li> <li>• Trusted computing</li> <li>• Electronic Voting</li> <li>• OS Security</li> </ul>
Lern- und Kompetenzziele	<p>This course aims to increase the security awareness of students and offers them a basic understanding with respect to a variety of interesting topics. After this course, students will be able to (1) learn about symmetric and asymmetric encryption schemes, (2) classify and describe vulnerabilities and protection mechanisms of popular network protocols, web protocols, and software systems (2) analyze / reason about basic protection mechanisms for modern OSs, software and hardware systems.</p>
Medienformen	Slides, Writing (Board, electronic), Handouts
Begleitende Literatur	Will be announced in the lecture.
Lehr- und Lernmethoden	lecture, regular exercises
Art der Prüfungsleistung	written exam
Prüfungsvorleistungen	Es müssen 40% der Punkte aus der ersten Hälfte der Übungsblätter und 40% der Punkte aus der zweiten Hälfte der Übungsblätter erreicht werden
Prüfungsdauer	90 min

Sprache	Englisch
Angebotsturnus	unregelmäßig
Lehrende/r	Prof. Dr. Frederik Armknecht, Ghassan Karame
Modulverantwortlicher	Prof. Dr. Frederik Armknecht
Dauer des Moduls	1 Semester
Weiterführende Module	-
Verwendbarkeit	B.Sc. Wirtschaftsinformatik, B.Sc. Medien- und Kommunikationswissenschaft, M.Sc. Wirtschaftspädagogik, Lehramt Informatik, Beifach Angewandte Informatik
Einordnung in Fachsemester	5./6. Fachsemester

<b>MAN 455</b>	<b>Digital Social Innovation Lab "Young Academy"</b> <b>Digital Social Innovation Lab "Young Academy"</b>
Form der Veranstaltung	Learning format with workshop sessions combined with online teaching elements, i.e., a Massive Open Online Course (MOOC)
Typ der Veranstaltung	Vertiefung Informatik
Modulniveau	Bachelor
ECTS	6
Arbeitsaufwand	Präsenzstudium: 28 h pro Semester (2 SWS)
	Eigenstudium: ca. 140 h pro Semester
Vorausgesetzte Kenntnisse	No formal prerequisites. General interest in the topics of digitalization, sustainability, and social entrepreneurship.
Einschreibung	Yes; Further Information on the registration: Website of the CSR chair / Portal2
Lehrinhalte	The Digital Social Innovation Lab is a blended learning format comprised of an online teaching element, i.e., a Massive Open Online Course (MOOC) on the topic of "Purpose and New Work" and offline workshops in which students work in teams and apply Design Thinking Methods to develop an idea for a social start-up. The online course will be offered via the platform OpenSAP and students will participate in the MOOC parallel to the offline workshops. The MOOC will contain short knowledge quizzes. In the classroom sessions, students will start with ideation and idea-reframing and then develop their own social business model. Additionally, they will learn about social impact measurement and get input on storytelling and a pitch training. At the end of the seminar, the student teams will have to present their project ideas at the final pitch event in front of an expert jury.

Lern- und Kompetenzziele	Besides applying methods of Design Thinking, participants will get to know the basics of purpose-driven business modelling as well as social impact measurement. They will gain a deeper understanding of how social entrepreneurship/intrapreneurship can contribute to sustainable development as defined in the United Nations Sustainable Development Goals. LG 1, LG 3, LG 4
Begleitende Literatur	Will be announced in the lecture.
Art der Prüfungsleistung	(Poster-) Presentation at the final pitch event (20%) and written summary of the social business model canvas, 12 pages per group (80%)
Prüfungsvorleistungen	Completion of the MOOC
Prüfungsdauer	-
Sprache	Englisch
Angebotsturnus	Frühjahrssemester
Lehrende/r	Prof. Dr. Laura Marie Edinger-Schons/ Markus Mosig M.Sc.
Modulverantwortlicher	Prof. Dr. Laura Marie Edinger-Schons
Dauer des Moduls	1 Semester
Weiterführende Module	-
Verwendbarkeit	B.Sc. Wirtschaftsinformatik
Einordnung in Fachsemester	5./6. Fachsemester

<b>Präsentationskompetenz und Rhetorik</b> <i>Presentation skills and rhetoric</i>	
Form der Veranstaltung	Blockseminar
Typ der Veranstaltung	Schlüsselqualifikation
Modulniveau	Bachelor
ECTS	2 (für Studierende, die ihr Studium ab dem HWS 2015/16 aufgenommen haben) bzw. 3 (für Studierende, die ihr Studium im HWS 2013/14 oder HWS 2014/15 aufgenommen haben)
Arbeitsaufwand	Präsenzstudium: 28 h pro Semester (2 SWS)
	Selbststudium: 22 h pro Semester
Vorausgesetzte Kenntnisse	-
Lehrinhalte	Nach Zielstellung interessieren, überzeugen, informieren und ggf. zu einer Entscheidung oder Handlung im weiteren Sinne führen. Durch Sprache überzeugen und verständlich informieren. Souverän und kompetent auftreten, im Idealfall bezüglich Fachkompetenz, Präsentationskompetenz, Rhetorik, Argumentation und Überzeugungskraft
Lern- und Kompetenzziele	Fachkompetenz: -
	Methodenkompetenz: -
	Personale Kompetenz: Die Studierenden sind in der Lage ein Thema klar, verständlich und anschaulich zu präsentieren und zu kommunizieren.  (BF6)
Begleitende Literatur	Literaturliste wird zu Beginn des Seminars zur Verfügung gestellt.
Lehr- und Lernmethoden	Seminar
Art der Prüfungsleistung	Form, Umfang und Gewichtung der zu erbringenden Prüfungsleistungen werden zu Beginn des Semesters bekannt gegeben.
Prüfungsvorleistungen	-



Prüfungsdauer	
Angebotsturnus	<b>Frühjahrssemester</b>
Lehrende/r	Dozenten der Service & Marketing GmbH
Modulverantwortlich	Service & Marketing GmbH
Dauer des Moduls	1 Semester
Weiterführende Module	-
Verwendbarkeit	B.Sc. Wirtschaftsinformatik
Einordnung Fachsemester	in 6. Fachsemester

<b>CS 404</b>	<b>Kryptographie I Cryptographie I</b>
Form der Veranstaltung	Vorlesung mit begleitender Übung
Typ der Veranstaltung	Vertiefung Informatik
Modulniveau	Bachelor
ECTS	6
Arbeitsaufwand	Präsenzstudium: 56 h pro Semester (4 SWS)
	Eigenstudium: ca. 112 h pro Semester <ul style="list-style-type: none"> <li>• davon Vor- und Nachbereitung der Veranstaltung und freies Selbststudium: 84 h pro Semester</li> <li>• davon Vorbereitung für die Prüfung, z.B. Prüfungs-/Seminarabschlussarbeits- und Präsentationsvorbereitung: 28 h pro Semester</li> </ul>
Vorausgesetzte Kenntnisse	Es gibt keine formalen Voraussetzungen, aber folgende inhaltliche Vorkenntnisse werden empfohlen: Praktische Informatik I und II, Lineare Algebra, Algorithmen und Datenstrukturen, Analysis, Einführung in die Statistik
Lehrinhalte	In der Vorlesung erfolgt eine Einführung in die moderne Kryptographie, d.h. in die Theorie und der Praxis der Absicherung von digitalen Daten. Neben der Bereitstellung der für das Verständnis des Stoffs nötigen mathematischen, algorithmischen und informationstheoretischen Grundlagen werden vor allem die grundlegenden Konzepte und mehrere in der Praxis eingesetzte Verfahren vorgestellt. <p>Behandelt Themen sind beispielsweise:</p> <ul style="list-style-type: none"> <li>• Grundbegriffe der Kryptographie</li> <li>• Blockchiffren, z.B. Data Encryption Standard (DES) und Advanced Encryption Standard (AES), und Stromchiffren</li> <li>• Verfahren zum sicheren Schlüsselaustausch, bspw. das Diffie-Hellman Protokoll</li> </ul>

	<ul style="list-style-type: none"> <li>• Public-Key Verschlüsselungsverfahren, bspw. RSA</li> <li>• Hashfunktionen</li> <li>• Message Authentication Codes</li> </ul>
Lern- und Kompetenzziele	<p>Fachkompetenz:</p> <p>Nach Abschluss des Moduls sind die Studierenden befähigt, die größten Risiken im elektronischen Datenverkehr, wie sie bspw. beim Online-Banking oder Einkauf über Online-Händler wie Amazon auftreten können, zu erkennen und zu vermeiden.</p> <p>(BK1, BK2, BK7)</p>
	<p>Methodenkompetenz:</p> <p>Die Studierenden können in konkreten Anwendungsfällen notwendige Sicherheitsziele erkennen und passende Methoden auswählen und einsetzen. Beispiele sind Verfahren zur Geheimhaltung von Daten (Verschlüsselungen), den Aufbau einer vertrauenswürdigen Verbindung (Schlüsselaustausch) und der sicheren Authentifikation (Zertifikate und digitale Signaturen).</p> <p>(BK5, BF4, BF5)</p>
	<p>Personale Kompetenz:</p> <p>Das analytische, konzentrierte und präzise Denken der Studierenden wird geschult. Durch die eigenständige Behandlung von Anwendungen, z.B. im Rahmen der Übungsaufgaben, wird ihr Abstraktionsvermögen weiterentwickelt und der Transfer des erlernten Stoffes auf verwandte Fragestellungen gefördert.</p> <p>(BKO2)</p>
Medienformen	Anschrieb (Tafel, elektronisch), Folien, Handouts
Begleitende Literatur	<ul style="list-style-type: none"> <li>• Christof Paar, Bart Preneel, Jan Pelzl: Understanding Cryptography: A Textbook for Students and Practitioners, Springer, 2009.</li> <li>• Douglas R. Stinson: Cryptography - Theory and Practice, Taylor &amp; Francis, 2005.</li> <li>• Alan G. Konheim: Cryptography: A Primer, John Wiley &amp; Sons, 1981.</li> </ul>

Lehr- und Lernmethoden	Nacharbeit der Vorlesung und Studium der relevanten Literatur im Selbststudium, gemeinsames Durcharbeiten konkreter Beispiele während der Vorlesung, Lösen von Übungsaufgaben im Selbststudium und in der Übung in Kooperation mit den Kommilitonen.
Art der Prüfungsleistung	Schriftliche Prüfung
Prüfungsvorleistungen	-
Prüfungsdauer	90 Minuten
Sprache	Englisch
Angebotsturnus	Herbstsemester
Lehrende/r	Prof. Dr. Frederik Armknecht, Prof. Dr. Matthias Krause
Modulverantwortlicher	Prof. Dr. Frederik Armknecht, Prof. Dr. Matthias Krause
Dauer des Moduls	1 Semester
Weiterführende Module	-
Verwendbarkeit	B.Sc. Wirtschaftsinformatik, B.Sc. Wirtschaftsmathematik, M.Sc. Wirtschaftspädagogik, Lehramt Informatik, Beifach Angewandte Informatik
Einordnung in Fachsemester	5./6. Fachsemester