Modulhandbuch zum berufsbegleitenden Bachelorstudiengang Informatik/IT-Sicherheit

Prof. Dr.-Ing. Felix C. Freiling

Friedrich-Alexander Universität
Lehrstuhl für Informatik 1

Stand: 21. März 2024

Inhaltsverzeichnis

Vorwort

Dieses Dokument enthält die Beschreibungen aller Module des berufsbegleitenden Bachelorstudiengangs Informatik/IT-Sicherheit.

Die auf der Folgeseite abgebildete Curriculumübersicht dient der allgemeinen Orientierung und der Zuordnung der Module zu den einzelnen Studiensemestern. Die Auflistung der Module in diesem Modulhandbuch entspricht dem zeitlichen Ablauf des Studiengangs.

Die Module sind den folgenden Fachgebieten zugeordnet:

- Mathematisch-naturwissenschaftliche Grundlagen
- Informatik Grundlagen
- IT-Sicherheit Grundlagen
- Informatik Vertiefung
- IT-Sicherheit Vertiefung

Die Wahlpflichtmodule gehören alle zum Fachgebiet „IT-Sicherheit Vertiefung“. Insgesamt müssen aus einem Angebot von z.Z. 13 Wahlpflichtmodulen 6 Module absolviert werden.

Auf Seite 5 ist der Studienverlaufsplan dargestellt, dem insbesondere Art und Umfang der Prüfungs- und Studienleistungen für die einzelnen Module zu entnehmen ist.

Dieses Modulhandbuch korrespondiert mit der Studien- und Prüfungsordnung des Studiengangs in der Fassung vom 15.08.2019 und ist Gegenstand fortgesetzter Evaluierungen.

Curriculumsübersicht

9	Wahlpflichtmodul 6	Bachelorarbeit		
8	Wahlpflichtmodul 4	Wahlpflichtmodul 5	Sicherheitsmanagement	Projekt
7	Wahlpflichtmodul 2	Wahlpflichtmodul 3	Netzsicherheit 3	Projekt
6	Wahlpflichtmodul 1	Realisierung von Softwareprojekten	Netzsicherheit 2	Seminar
5	Kryptographie 2	Compilerbau	Netzsicherheit 1	Einführung in die digitale Forensik
4	Kryptographie 1	Systemnahe Programmierung	Systemsicherheit 2	Proseminar
3	Theoretische Informatik	Algorithmen und Datenstrukturen	Systemsicherheit 1	
2	Rechnerstrukturen	Programmierkonzepte	Mathematik 2a	Mathematik 2b
1	Einführung in die IT-Sicherheit	Einführung in das Programmieren	Mathematik 1	Konzeptionelle Modellierung

Modulbezeichnung	Lehrveranstaltung	SWS				ECTS	1.	2.	3.	4.	5.	6.	7.	8.	9.	Art und Umfang der Prüfungs- und Studienleistungen[1)]
		V	Ü	P	S		ECTS	ECTS	ECTS	ECTS	ECTS	ECTS	ECTS	ECTS	ECTS	
Einführung in die IT-Sicherheit	Einführung in die IT-Sicherheit	x	x			5	5									PL (K, 60min)
Grundlagen der Programmierung	Einführung in das Programmieren	x	x			10	5									PL (K,120min)
	Programmierkonzepte	x	x					5								
Mathematik 1	Mathematik 1	x	x			5	5									PL (K, 60min)
Konzeptionelle Modellierung	Konzeptionelle Modellierung	x	x			5	5									PL (K, 90min)
Mathematik 2	Mathematik 2a	x	x			5		5								PL (K,120min)
	Mathematik 2b	x	x			5		5								
Rechnerstrukturen	Rechnerstrukturen	x	x			5		5								PL (K, 60min)
Systemsicherheit 1	Systemsicherheit 1	x	x			10			10							PL (K,120min)
Algorithmen und Datenstrukturen	Algorithmen und Datenstrukturen	x	x			5			5							PL (K,60min)
Theoretische Informatik	Theoretische Informatik	x	x			5			5							PL (K, 60min)
Kryptographie 1	Kryptographie 1	x	x							5						PL (K, 120min)
Systemnahe Programmierung	Systemnahe Programmierung	x	x			5				5						PL (SeL)
Systemsicherheit 2	Systemsicherheit 2	x	x			5				5						PL (K, 60min)
Proseminar IT-Sicherheit	Proseminar IT-Sicherheit				x	5				5						PL (SeL) (schriftl. Ausarbeitung ca. 6-15 S. und mündl. Präsentation 30min mit anschließender Diskussion 15min).
Einführung in die digitale Forensik	Einführung in die digitale Forensik	x	x			5					5					PL (SeL)
Compilerbau	Compilerbau	x	x			5					5					PL (K, 60min)
Netzsicherheit 1	Netzsicherheit 1	x	x			5					5					PL (K, 120min)
Kryptographie 2	Kryptographie 2	x	x			5					5					PL (K, 120min)
Netzsicherheit 2	Netzsicherheit 2	x	x			5						5				PL (K, 120min)
Realisierung von Softwareprojekten	Realisierung von Softwareprojekten	x	x			5						5				PL (SeL)
Seminar IT-Sicherheit	Seminar IT-Sicherheit				x	5						5				PL (SeL) (schriftl. Ausarbeitung ca. 8-20 S. und mündl. Präsentation 30min mit anschließender Diskussion 15min)
Wahlpflichtbereich (vgl. § 26a)	vgl. § 26 Abs. 2	x	x	x		30						5	10	10	5	vgl. § 26a Abs. 3
Netzsicherheit 3	Netzsicherheit 3	x	x			5							5			PL (K, 120min)
Projekt IT-Sicherheit	Projekt IT-Sicherheit			x		10							5	5		PL (SeL) (schriftl. Ausarbeitung ca. 10 S. und mündl. Präsentation 30min mit anschließender Diskussion 15min)
Sicherheitsmanagement	Sicherheitsmanagement	x	x			5								5		PL (SeL)
Bachelorarbeit	Bachelorarbeit					15									12	PL: Bachelorarbeit und Referat sowie Diskussion
	Kolloquium														3	
Summe SWS: 36 Summe ECTS: 180							20	20	20	20	20	20	20	20	20	

[1)] Legende zu Abkürzungen in dieser Spalte:
PL = Prüfungsleistung (benotet) gemäß § 6 Abs. 3
SL = Studienleistung (unbenotet) gemäß § 6 Abs. 3
K = Klausur mit Zeitangabe
SeL = Seminarleistung gemäß § 6 Abs. 3
PrL = Praktikumsleistung gemäß § 6 Abs. 3

Einführung in die IT-Sicherheit (Introduction to IT Security)

Modulbezeichnung:	Einführung in die IT-Sicherheit (Introduction to IT Security)
Verwendbarkeit:	Bachelorstudiengang Informatik/IT-Sicherheit (Pflichtmodul)
Lehrveranstaltungen und Lehrformen:	Einführung in die IT-Sicherheit Selbstlernphasen, Übungen, Online-Phasen, Präsenzveranstaltung
Modulverantwortliche(r):	Prof. Dr. Daniel Hammer
Lehrende:	Prof. Dr. Daniel Hammer
Dauer:	1 Semester
Credits:	5 ECTS-Punkte
Studien- und Prüfungsleistungen:	Klausur: 60 min.
Berechnung der Modulnote:	100% der schriftlichen Prüfungsnote
Notwendige Voraussetzungen für die Teilnahme:	
Empfohlene Voraussetzungen für die Teilnahme:	
Unterrichts- und Prüfungssprache:	Deutsch
Zuordnung des Moduls zu den Fachgebieten des Curriculums:	IT-Sicherheit Grundlagen
Einordnung ins Fachsemester:	Ab Studiensemester 1
Arbeitsaufwand bzw. Gesamtworkload:	Präsenzstudium: 15 Zeitstunden Fernstudienanteil: 135 Zeitstunden • davon Selbststudium: 105 Zeitstunden • davon Aufgaben: 20 Zeitstunden • davon Online-Betreuung: 10 Zeitstunden Summe: 150 Zeitstunden

Lerninhalte:	Auf folgende Themengebiete wird eingegangen: • Grundlagen des Sicherheitsmanagements, des Risikomanagements und der -analyse • Notfallplanung • Bedrohungsfaktoren der IT-Sicherheit und deren Schutzmaßnahmen • Grundlagen der Zugriffskontrolle und -verwaltung • Mechanismen der Authentisierung, SSO-Technologien • Darstellung der Angriffe auf Zugriffskontrollsysteme • Einführung in die Kryptographie, symmetrische und asymmetrische Verschlüsselungsverfahren, Darstellung der Angriffe auf Kryptosysteme, kryptographische Hashfunktionen, digitale Signatur • Einführung in die Steganographie • Einführung in die Sicherheitsaspekte vernetzter Umgebungen, Grundlagen des DNS, E-Mail-Missbrauch • Spam, Phishing, Network Security

Lernziele und Kompetenzen:	*Fachkompetenz:* Die Studierenden haben Grundkenntnisse des Sicherheitsmanagements, des Risikomanagements und der -analyse. Die Studierenden haben sich Grundlagen der Zugriffskontrolle und -verwaltung angeeignet, können Mechanismen der Authentisierung unterscheiden und erklären sowie SSO-Technologien beschreiben. Sie sind in der Lage, die unterschiedlichen Angriffe auf Zugriffskontrollsysteme darzustellen. Sie haben Grundkenntnisse der Kryptographie und Steganographie, können symmetrische und asymmetrische Verschlüsselungsverfahren differenzieren, Angriffe auf Kryptosysteme darstellen sowie kryptographische Hashfunktionen und digitale Signatur erklären. Zudem sind die Studierenden mittels ihrer Grundkenntnisse über die Sicherheitsaspekte vernetzter Umgebungen und das DNS in der Lage, diese zu erläutern. Sie können einen E-Mail-Missbrauch und Spam erklären sowie Phishing aufzeigen und ihre Lösungsansätze darstellen. *Methodenkompetenz:* Die Studierenden können eine Notfallplanung erläutern, die Bedrohungsfaktoren der IT-Sicherheit beschreiben und klassifizieren sowie deren Schutzmaßnahmen skizzieren und anwenden. Der Lernende kann die Phasen eines Hackerangriffs strukturieren, Malware analysieren und einordnen und die entsprechenden Schutzmaßnahmen anwenden. *Sozialkompetenz:* Aufgrund der Teamarbeit, unter anderem an dem Präsenzwochenende, sind die Studierenden fähig, Lösungswege in der Gruppe zu entwickeln und Aufgaben kooperativ zu lösen. *Selbstkompetenz:* Die Studierenden haben sich eine Meinung über IT-Sicherheit gebildet. Sie sind fähig, Ihre Lernzeit zu strukturieren und Modulinhalte über unterschiedliche Lernphasen verteilt zu bearbeiten.
Häufigkeit des Angebots:	Wintersemester
Medienformen:	Studienbriefe in schriftlicher und elektronischer Form, Onlinematerial in Lernplattform, Übungen und Projekt über Lernplattform, Online-Konferenzen, Chat und Forum, Präsenzveranstaltung mit Rechner und Beamer.
Literaturhinweise:	• Sicherheit in Informationssystemen, (Vorlesungsskript), Daniel Hammer, 2012 • Angewandte Kryptographie, Bruce Schneier, 1996 • Netzsicherheit, Günter Schäfer, 2003 • Cyberwar: Das Internet als Kriegsschauplatz, Sandro Gaycken, 2011 Weitere Literatur wird in der Lehrveranstaltung bekannt gegeben.

Grundlagen der Programmierung (Fundamentals of Programming)

Modulbezeichnung:	Grundlagen der Programmierung (Fundamentals of Programming)
Verwendbarkeit:	Bachelorstudiengang Informatik/IT-Sicherheit (Pflichtmodul)
Lehrveranstaltungen und Lehrformen:	Einführung in das Programmieren Programmierkonzepte Selbstlernphasen, Übungen, Online-Phasen, Präsenzveranstaltung
Modulverantwortliche(r):	Prof. Dr. Felix Freiling
Lehrende:	Philipp Klein
Dauer:	2 Semester
Credits:	10 ECTS-Punkte
Studien- und Prüfungsleistungen:	Digitale Klausur: 120 Minuten
Berechnung der Modulnote:	100% der Klausurnote
Notwendige Voraussetzungen für die Teilnahme:	
Empfohlene Voraussetzungen für die Teilnahme:	
Unterrichts- und Prüfungssprache:	Deutsch
Zuordnung des Moduls zu den Fachgebieten des Curriculums:	Informatik Grundlagen
Einordnung ins Fachsemester:	Ab Studiensemester 1
Arbeitsaufwand bzw. Gesamtworkload:	Für dieses Modul: Präsenzzeit: 30 h Eigenstudium: 270 h • Durcharbeiten der Studienbriefe: 110 h • Wahrnehmen der Online Betreuung und Beratung: 25 h • Ausarbeiten von Aufgaben: 115 h • Individuelle Prüfungsvorbereitung der Studierenden: 20 h

Lerninhalte:	**Einführung in das Programmieren (Introduction to Programming)** Eine Einführung in die Programmiersprache Java. Mit Hilfe der Entwicklungsumgebung Visual Studio Code wird den Studierenden der Umgang mit Java und Objektorientierung vertraut gemacht. Themen sind unter anderem: • Ausdrücke und Algorithmische Kernsprache von Java • Sprachbeschreibung und Objekttypen • Eine Einführung in bereits existierende Methoden und Klassen in der Programmiersprache Java • Polymorphie und Generics • Testen und Test Driven Development mit JUnit Darüber hinaus erhalten die Studierenden einen praktischen Einblick in die folgenden programmierrelevanten Technologien/Techniken: • Versionsverwaltung mit Git **Programmierkonzepte (Principles of Programming)** Diese Lehrveranstaltung knüpft nahtlos an die Veranstaltung „Einführung in das Programmieren“ an. Die Studierenden lernen weitere Komponenten der Programmiersprache Java kennen, wie beispielsweise: • Exceptionhandling • I/O-Verarbeitung • Rekursion • Komplexität von Algorithmen

Lernziele und Kompetenzen:	*Fachkompetenz:* Die Studierenden können beliebige Programme in Java erstellen. Sprachkomponenten, die Sie noch nicht kennen, können Sie sich in kürzester Zeit aneignen. Zudem sind die Studierenden in der Lage, sich selbstständig neue Programmiersprachen beizubringen. Sie schreiben sichere Programme und wissen, wo potenzielle Schwachstellen in einem Programm zu finden sind. *Methodenkompetenz:* Die Studierenden beherrschen den Umgang mit beliebigen IDEs. Sie können fremde Programme untersuchen und den Kontrollfluss nachvollziehen. Sie sind in der Lage, Schwachstellen und Fehler in einem Programm zu finden und zu beseitigen. *Sozialkompetenz:* Durch das gemeinsame Lösen von Aufgaben erlangen die Studierenden die Fähigkeit, eigene Handlungsziele mit den Einstellungen und Werten einer Gruppe zu verknüpfen und ihre Teamfähigkeit zu stärken. In der Präsenzphase erlangen sie u. a. durch Pair-Programming die Kompetenz, eigene Ideen gegenüber einem anderen Programmierer zu kommunizieren, Kompromisse zu bilden und diese im Team umzusetzen. *Selbstkompetenz:* Die Studierenden erlangen die Fähigkeit zur Bildung einer Meinung über eigene Programme und Programme anderer. Darüber hinaus erlangen sie die Fähigkeit, in komplexen Situationen zu handeln und eine Lösung für komplexe Probleme zu finden.
Häufigkeit des Angebots:	Wintersemester
Medienformen:	Studienbriefe in schriftlicher und elektronischer Form, Onlinematerial in Lernplattform, Übungen und Projekt über Lernplattform, Online-Konferenzen, Chat und Forum, Präsenzveranstaltung mit Rechner und Beamer
Literaturhinweise:	• IT-Sicherheit, Claudia Eckert, 2012 • Java lernen mit BlueJ, David J. Barnes, Michael Kölling, 2013 • Weitere Literatur wird in der Lehrveranstaltung bekannt gegeben.

Mathematik 1 (Mathematics 1)

Modulbezeichnung:	Mathematik 1 (Mathematics 1)
Verwendbarkeit:	Bachelorstudiengang Informatik/IT-Sicherheit (Pflichtmodul)
Lehrveranstaltungen und Lehrformen:	Mathematik 1 Selbstlernphasen, Übungen, Online-Phasen, Präsenzveranstaltung
Modulverantwortliche(r):	Prof. Dr. Harald Baier
Lehrende:	Prof. Dr. Harald Baier
Dauer:	1 Semester
Credits:	5 ECTS-Punkte
Studien- und Prüfungsleistungen:	Klausur: 60 min.
Berechnung der Modulnote:	100% der schriftlichen Prüfungsnote
Notwendige Voraussetzungen für die Teilnahme:	keine
Empfohlene Voraussetzungen für die Teilnahme:	Mathematik Gymnasium Oberstufe
Unterrichts- und Prüfungssprache:	Deutsch
Zuordnung des Moduls zu den Fachgebieten des Curriculums:	Mathematisch-naturwissenschaftliche Grundlagen
Einordnung ins Fachsemester:	Ab Studiensemester 1
Arbeitsaufwand bzw. Gesamtworkload:	Präsenzstudium: 30 Zeitstunden Fernstudienanteil: 120 Zeitstunden • Selbststudium: 90 Zeitstunden • Aufgaben: 20 Zeitstunden • Online-Betreuung: 10 Zeitstunden **Summe: 150 Zeitstunden**
Lerninhalte:	In diesem Modul werden die folgenden Themengebiete behandelt: • Mengen • Elementare Aussagelogik • Beweisverfahren • Reelle und komplexe Zahlen • Zahlentheorie und modulare Arithmetik • Vektoren und Vektorräume (Vektorrechnung im $\mathbb{R}^3$, Begriff des Vektorraums, Beispiele für Vektorräume) • Matrizen, Determinanten

Lernziele und Kompetenzen:	*Fachkompetenz:* Die Studierenden können die Arithmetik reeller und komplexer Zahlen erläutern und diese anwenden. Des Weiteren kennen Sie die Grundbegriffe der Zahlentheorie sowie der modularen Arithmetik und können mit diesen umgehen, insbesondere effizient modular Potenzieren. Darüber hinaus kennen Sie das RSA-Kryptosystem und erlangen Wissen über die zugrundeliegende Sicherheit. Sie können den Begriff 'Vektorraum' erklären und können diesen auf konkrete Vektorräume anwenden. Darüber hinaus sind Sie in der Lage, mit Vektoren und Matrizen zu rechnen, insbesondere Matrizen zu invertieren. *Methodenkompetenz:* Die Studierenden erwerben die Fähigkeit, mit den Lehrinhalten des Moduls aktiv umgehen zu können und können Fragestellungen, Aufgaben und Probleme, die sich aus der Lehrveranstaltung ergeben, selbstständig bearbeiten und lösen. *Sozialkompetenz:* Die Studierenden können durch Gruppenarbeit an den Präsenzwochenenden Übungsaufgaben kooperativ lösen und in Teams arbeiten. Darüber hinaus besitzen sie die Fähigkeit, in komplexen Situationen zu handeln und Lösungen für Aufgabenstellungen zu entwickeln. *Selbstkompetenz:* Die Studierenden können aufgrund der Teamarbeit problemorientiert diskutieren. Sie haben die Fähigkeit, sich eine Meinung über die Themen von Mathematik 1 zu bilden und können das erlangte Wissen im Bereich der Informatik einsetzen.
Häufigkeit des Angebots:	Wintersemester
Medienformen:	Studienbriefe in schriftlicher und elektronischer Form, Onlinematerial in Lernplattform, Übungen und Projekt über Lernplattform, Online-Konferenzen, Chat und Forum, Präsenzveranstaltung mit Rechner und Beamer.

Literaturhinweise:	Als begleitende Literatur wird empfohlen: • eigenes Skript (Studienbriefe) Als vertiefende Literatur wird empfohlen: • Teschl, G.; Teschl, S.: Mathematik für Informatiker Band 1: Diskrete Mathematik und Lineare Algebra, Springer-Verlag, ISBN 978-3-642-37972-7, Springer; Auflage: 4 • Teschl, G.; Teschl, S.: Mathematik für Informatiker Band 2: Analysis und Statistik, Springer-Verlag, ISBN 978-3-642-54274-9, Springer; Auflage: 3 • Arens, T.; Hettlich, F.; Karpfinger, C.; Kockelkorn, U.; Lichtenegger, K.; Stachel, H.: Mathematik, Springer-Verlag, ISBN: 978-3-827-42347-4, Springer; Auflage: 2 • Arens, T.; Hettlich, F.; Karpfinger, C.; Kockelkorn, U.; Lichtenegger, K.; Stachel, H.: Arbeitsbuch Mathematik - Aufgaben, Hinweise, Lösungen und Lösungswege, Springer-Verlag, ISBN: 978-3-827-42410-5, Springer; • Arens, T.; Busam, F.; Hettlich, F.; Karpfinger, C.; Stachel, H.; Lichtenegger, K.: Grundwissen Mathematikstudium - Analysis und Lineare Algebra mit Querverbindungen, Springer-Verlag, ISBN: 978-3-827-42309-2, Springer; • Houston, K.: Wie man mathematisch denkt - Eine Einführung in die mathematische Arbeitstechnik für Studienanfänger, Springer Spektrum, ISBN: 978-3-8274-2997-1; Springer

Konzeptionelle Modellierung (Conceptual Modelling)

Modulbezeichnung:	Konzeptionelle Modellierung (Conceptual Modelling)
Verwendbarkeit:	Bachelorstudiengang Informatik/IT-Sicherheit (Pflichtmodul)
Lehrveranstaltungen und Lehrformen:	Konzeptionelle Modellierung Selbstlernphasen, Übungen, Online-Phasen, Präsenzveranstaltung
Modulverantwortliche(r):	Prof. Dr. Richard Lenz
Lehrende:	Prof. Dr. Richard Lenz/Prof. Dr. Felix Freiling/Philipp Klein
Dauer:	1 Semester
Credits:	5 ECTS-Punkte
Studien- und Prüfungsleistungen:	Klausur: 90 min.
Berechnung der Modulnote:	100% der schriftlichen Prüfungsnote
Notwendige Voraussetzungen für die Teilnahme:	
Empfohlene Voraussetzungen für die Teilnahme:	
Unterrichts- und Prüfungssprache:	Deutsch
Zuordnung des Moduls zu den Fachgebieten des Curriculums:	Informatik Grundlagen
Einordnung ins Fachsemester:	Ab Studiensemester 1
Arbeitsaufwand bzw. Gesamtworkload:	Präsenzzeit: 15 h Eigenstudium: 135 h • Durcharbeiten der Studienbriefe: 50 h • Durcharbeiten des Online-Lernmaterials: 15 h • Wahrnehmen der Online-Betreuung und Beratung: 15 h • Ausarbeiten von Aufgaben: 30 h • Individuelle Prüfungsvorbereitung der Studierenden: 25 h
Lerninhalte:	Im Modul konzeptionelle Modellierung wird auf folgende Themengebiete eingegangen: • Grundlagen der Modellierung • Entity-Relationship Modell (ER-Modell) • Metamodellierung und XML

Lernziele und Kompetenzen:	*Fachkompetenz:* Die Studierenden erwerben fundierte Kenntnisse über die Grundlagen der Modellierung sowie über das Entity-Relationship-Modell (ER-Modell). Darüber hinaus erwerben Sie fundiertes Wissen über die Datenbanksprache SQL sowie die Auszeichnungssprache XML. *Methodenkompetenz:* Die Studierenden haben die Fähigkeit zu beurteilen, wann eine Datenbank sinnvoll ist und können zwischen verschiedenen Typen von Datenbanksystemen unterscheiden. *Sozialkompetenz:* Die Konflikt- und Kommunikationsfähigkeit der Studierenden wird in den gemeinsamen Online-Tutorien und Diskussionsforen geschult. *Selbstkompetenz:* Die Studierenden erlangen die Fähigkeit zur Bildung einer Meinung über die selbstentwickelten Datenmodellierungen und die Datenmodellierungen anderer. Darüber hinaus erlangen sie die Fähigkeit, in herausfordernden Situationen zu handeln und eine Lösung für komplexe Probleme zu finden.
Häufigkeit des Angebots:	Wintersemester
Medienformen:	Studienbriefe in schriftlicher und elektronischer Form, Onlinematerial in Lernplattform, Übungen und Projekte über Lernplattform, Online-Konferenzen, Chat und Forum, Präsenzveranstaltungen mit Computer und Beamer.
Literaturhinweise:	Als optionale weiterführende Literatur wird empfohlen: • Datenbanksysteme: Eine Einführung, Alfons Kemper und Andre Eickler • An Introduction to Database Systems, C. J. Date • Information Modeling and Relational Database, T. Halpin und T-Morgan • Mehrrechner- Datenbanksysteme, E. Rahm • Datenbankmodelle, Datenbanksprachen und Datenbankmanagementsysteme, G. Vossen • Datenbanken – Konzepte und Sprachen, G. Saake, K. Sattler und A. Heuer • Relationale Datenbanken, Hermann Sauer

Mathematik 2 (Mathematics 2)

Modulbezeichnung:	Mathematik 2 (Mathematics 2)
Verwendbarkeit:	Bachelorstudiengang Informatik/IT-Sicherheit (Pflichtmodul)
Lehrveranstaltungen und Lehrformen:	Mathematik 2a und Mathematik 2b Selbstlernphasen, Übungen, Online-Phasen, Präsenzveranstaltung
Modulverantwortliche(r):	Prof. Dr. Harald Baier
Lehrende:	Prof. Dr. Harald Baier
Dauer:	1 Semester
Credits:	10 ECTS-Punkte
Studien- und Prüfungsleistungen:	Klausur: 120 min., aufgeteilt in zwei Klausurblöcke mit jeweils 60 min. (Mathematik 2a und Mathematik 2b)
Berechnung der Modulnote:	100% der schriftlichen Prüfungsnote
Notwendige Voraussetzungen für die Teilnahme:	
Empfohlene Voraussetzungen für die Teilnahme:	Erfolgreicher Abschluss des Moduls • Mathematik 1
Unterrichts- und Prüfungssprache:	Deutsch
Zuordnung des Moduls zu den Fachgebieten des Curriculums:	Mathematisch-naturwissenschaftliche Grundlagen
Einordnung ins Fachsemester:	Ab Studiensemester 2
Arbeitsaufwand bzw. Gesamtworkload:	Präsenzstudium: 60 Zeitstunden Fernstudienanteil: 240 Zeitstunden • Selbststudium: 180 Zeitstunden • Aufgaben: 40 Zeitstunden • Online-Betreuung: 20 Zeitstunden **Summe: 300 Zeitstunden**

Lerninhalte:	In diesem Modul werden die folgenden Themengebiete behandelt: **Mathematik 2a:** • Folgen und Funktionen (Konvergenz von Folgen und Reihen, Stetigkeit von Funktionen) • Differentialrechnung einer und mehrerer Veränderlichen • Partielle Ableitungen **Mathematik 2b:** • Integralrechnung einer und mehreren Veränderlichen • Numerik (Rechnerarithmetik, Algorithmen, Lineare Gleichungssysteme, Interpolation, Approximation, Numerische Integration, Numerische Differentiation) • Kombinatorik und endliche Wahrscheinlichkeitstheorie (Elementare Zählprobleme, Binominialkoeffizient und Teilmengen, Permutation, Partitionen, Grundbegriffe der endlichen Wahrscheinlichkeitstheorie, bedingte Wahrscheinlichkeiten, Zufallsgrößen) • Wahrscheinlichkeitsrechnung (ausgewählte diskrete Verteilungen, Normalverteilung, Testverteilung)

Lernziele und Kompetenzen:	*Fachkompetenz:* **Mathematik 2a:** Die Studierenden können entscheiden, ob Folgen bzw. Reihen konvergent sind oder nicht und ggf. Grenzwerte berechnen. Des Weiteren können Sie die elementaren Funktionen der Analysis erläutern und haben Kenntnisse über ihre grundlegenden Eigenschaften. Sie verstehen die Differentialrechnung und können diese anwenden. **Mathematik 2b:** Die Studierenden verstehen die Integralrechnung und können diese anwenden. Sie wissen, wie Computersysteme Zahlen darstellen und können die Laufzeit eines Algorithmus berechnen. Sie kennen die Begriffe Interpolation, Approximation, numerische Integration und Differentiation. Weiter kennen Sie die elementaren Zählprobleme und können mit Hilfe des Binominialkoeffizienten die Anzahl von Möglichkeiten berechnen. Am Ende kennen Sie die Grundbegriffe der endlichen Wahrscheinlichkeitstheorie und können mit den Begriffen bedingte Wahrscheinlichkeiten und Zufallsgrößen umgehen. Darüber hinaus kennen Sie ausgewählte diskrete Verteilungen, Normalverteilung, Testverteilung und können damit umgehen. *Methodenkompetenz:* Die Studierenden können mit dem erlangten Wissen aus dem Modul sicher umgehen und können Aufgaben und Problemstellungen nachvollziehen und lösen. *Sozialkompetenz:* Die Studierenden erlernen die fachgebundene Diskussion, die sich aus der gemeinsamen Teamarbeit zum Lösen von Aufgaben ergeben. *Selbstkompetenz:* Die Studierenden erlangen die Fähigkeit sich eine Meinung über die Themen von Mathematik 2 zu bilden und besitzen darüber hinaus die Kompetenz Sie in den entsprechenden Gebieten der Informatik einsetzen zu können.
Häufigkeit des Angebots:	Sommersemester
Medienformen:	Studienbriefe in schriftlicher und elektronischer Form, Onlinematerial in Lernplattform, Übungen und Projekt über Lernplattform, Online-Konferenzen, Chat und Forum, Präsenzveranstaltung mit Rechner und Beamer.

Literaturhinweise:	Als begleitende Literatur wird empfohlen: • eigenes Skript (Studienbriefe) Als vertiefende Literatur wird empfohlen: • Teschl, G.; Teschl, S.: Mathematik für Informatiker Band 1: Diskrete Mathematik und Lineare Algebra, Springer-Verlag, ISBN 978-3-642-37972-7, Springer; Auflage: 4 • Teschl, G.; Teschl, S.: Mathematik für Informatiker Band 2: Analysis und Statistik, Springer-Verlag, ISBN 978-3-642-54274-9, Springer; Auflage: 3 • Knorrenschild, M.: Numerische Mathematik - Eine beispielorientierte Einführung, Fachbuchverlag Leipzig, ISBN: 978-3-446-43233-8, Auflage: 5 • Arens, T.; Hettlich, F.; Karpfinger, C.; Kockelkorn, U.; Lichtenegger, K.; Stachel, H.: Mathematik, Springer-Verlag, ISBN: 978-3-8274-2347-4, Springer; Auflage: 2 • Arens, T.; Hettlich, F.; Karpfinger, C.; Kockelkorn, U.; Lichtenegger, K.; Stachel, H.: Arbeitsbuch Mathematik - Aufgaben, Hinweise, Lösungen und Lösungswege, Springer-Verlag, ISBN: 978-3-827-42410-5, Springer; • Arens, T.; Busam, F.; Hettlich, F.; Karpfinger, C.; Stachel, H.; Lichtenegger, K.: Grundwissen Mathematikstudium - Analysis und Lineare Algebra mit Querverbindungen, Springer-Verlag, ISBN: 978-3-827-42309-2, Springer;

Rechnerstrukturen (Digital Logic Design)

Modulbezeichnung:	Rechnerstrukturen (Digital Logic Design)
Verwendbarkeit:	Bachelorstudiengang Informatik/IT-Sicherheit (Pflichtmodul)
Lehrveranstaltungen und Lehrformen:	Rechnerstrukturen Selbstlernphasen, Übungen, Online-Phasen, Präsenzveranstaltung
Modulverantwortliche(r):	Prof. Dr. Jürgen Teich
Lehrende:	Prof. Dr. Jürgen Teich, Dr. Stefan Wildermann
Dauer:	1 Semester
Credits:	5 ECTS-Punkte
Studien- und Prüfungsleistungen:	Klausur: 60 Min.
Berechnung der Modulnote:	100% der schriftlichen Prüfungsnote
Notwendige Voraussetzungen für die Teilnahme:	
Empfohlene Voraussetzungen für die Teilnahme:	
Unterrichts- und Prüfungssprache:	Deutsch
Zuordnung des Moduls zu den Fachgebieten des Curriculums:	Informatik Grundlagen
Einordnung ins Fachsemester:	Ab Studiensemester 2
Arbeitsaufwand bzw. Gesamtworkload:	Präsenzstudium: 15 Zeitstunden Fernstudienanteil: 135 Zeitstunden • Selbststudium: 105 Zeitstunden • Aufgaben: 20 Zeitstunden • Online-Betreuung: 10 Zeitstunden Summe: 150 Zeitstunden
Lerninhalte:	Im Modul Rechnerstrukturen wird auf folgende Themengebiete eingegangen: Aufbau und Prinzip von Rechnern, Daten und ihre Codierung, Boolesche Algebra und Schaltalgebra, Schaltnetze (Symbole, Darstellung), Optimierung von Schaltnetzen (Minimierung Boolescher Funktionen), Realisierungsformen von Schaltnetzen (ROM, PLA, FPGA), Automaten und Schaltwerke (Moore/Mealy, Zustandscodierung und -minimierung), Flipflops, Register, Zähler, Speicher, Taktung und Synchronisation, Realisierungsformen von Schaltwerken, Realisierung der Grundrechenarten Addition, Subtraktion und Multiplikation, Gleitkommazahlen (Darstellung, Fehler, Rundung, Standards, Einheiten), Steuerwerksentwurf.

Lernziele und Kompetenzen:	*Fachkompetenz:* Die Studierenden erwerben theoretische und praxisorientierte Grundkenntnisse der Informationstheorie, über die computergerechte Darstellung von Daten, Rechnerarithmetik, Digitaltechnik und des Schaltungsentwurfs. Außerdem eignen Sie sich Grundlagen der Schaltalgebra an und können Schaltnetze bzw. -werke beschreiben und klassifizieren. *Methodenkompetenz:* Die Studierenden erlangen das Grundwissen über den Aufbau von Rechnerstrukturen und können z. B. die Funktionsweise von Speichern und arithmetischen Einheiten erläutern. Außerdem erarbeiten und diskutieren die Studierenden verschiedene Lösungswege für die Datencodierung sowie den Entwurf und die Optimierung von digitalen Hardwareschaltungen. *Sozialkompetenz:* Aufgrund der Teamarbeit, unter anderem an dem Präsenzwochenende, sind die Studierenden fähig, Lösungswege in der Gruppe zu entwickeln und Aufgaben kooperativ zu lösen. *Selbstkompetenz:* Die Studierenden können den Aufbau und die Funktionsweise von Rechnern verstehen und nachvollziehen und haben die grundlegenden Prinzipien moderner Computer verinnerlicht. Desweiteren verfügen sie nach Absolvieren des Moduls über Kenntnisse der verschiedenen Abstraktionsebenen von Computern und deren Zusammenwirken. Die Studierenden verstehen die Komplexität des Hardwareentwurfs und, dass Hardware heutzutage mit Software am Rechner entwickelt und simuliert wird. Ihnen wird bewusst, dass IT sehr schnelllebig ist und dass Detailwissen eine kurze Halbwertzeit hat. Sie sind in der Lage sich je nach Bedarf selbst weiterzubilden.
Häufigkeit des Angebots:	Sommersemester
Medienformen:	Onlinematerial in Lernplattform, Übungen und Projekt über Lernplattform, Online-Konferenzen, Chat und Forum, Präsenzveranstaltung mit Rechner und Beamer.
Literaturhinweise:	• Grundlagen der Digitaltechnik, Hans Martin Lipp, Jürgen Becker. Oldenburg Verlag, 2011. • Logic Synthesis, Srinivas Devadas, Abhijit Ghosh, Kurt Keutzer. McGraw-Hill, 1994. • Logic Synthesis and Verification Algorithms, Gary D. Hachtel, Fabio Somenzi. Kluwer Academic, 1996. • Synthesis And Optimization of Digital Circuits, Giovanni De Micheli. McGraw-Hill, 1994. • Datenstrukturen und effiziente Algorithmen für die Logiksynthese kombinatorischer Schaltungen, P. Molitor, C. Scholl. Teubner Verlag, 1999. Weitere Literatur wird in der Lehrveranstaltung bekannt gegeben.

Systemsicherheit 1 (System Security 1)

Modulbezeichnung:	Systemsicherheit 1 (System Security 1)
Verwendbarkeit:	Bachelorstudiengang Informatik/IT-Sicherheit (Pflichtmodul)
Lehrveranstaltungen und Lehrformen:	Systemsicherheit 1 Selbstlernphasen, Übungen, Online-Phasen, Präsenzveranstaltung
Modulverantwortliche(r):	Prof. Dr.-Ing. Felix Freiling
Lehrende:	Prof. Dr.-Ing. Felix Freiling, Prof. Dr.-Ing. Hans-Georg Eßer
Dauer:	1 Semester
Credits:	10 ECTS
Studien- und Prüfungsleistungen:	Klausur: 120 min.
Berechnung der Modulnote:	100% der schriftlichen Prüfungsnote
Notwendige Voraussetzungen für die Teilnahme:	
Empfohlene Voraussetzungen für die Teilnahme:	Kenntnisse in einer höheren Programmiersprache sind dringend empfohlen. Kenntnisse in Rechnerarchitektur (Vorlesung Rechnerstrukturen) sind nützlich aber nicht notwendig.
Unterrichts- und Prüfungssprache:	Deutsch mit Literatur auf Englisch
Zuordnung des Moduls zu den Fachgebieten des Curriculums:	Informatik Grundlagen
Einordnung ins Fachsemester:	Ab Studiensemester 3
Arbeitsaufwand bzw. Gesamtworkload:	Präsenzstudium: 30 Zeitstunden Fernstudienanteil: 270 Zeitstunden • Selbststudium: 210 Zeitstunden • Aufgaben: 40 Zeitstunden • Online-Betreuung: 20 Zeitstunden Summe: 300 Zeitstunden

Lerninhalte:	Betriebssysteme erlauben komfortablen Zugang zu den Ressourcen eines Rechners und erfüllen eine Brückenfunktion zwischen Anwendung und Hardware. Betriebssysteme koordinieren auch die parallele Aufgabenausführung auf einem Rechner und erlauben so die Leistungsfähigkeit paralleler Hardwarearchitekturen direkt in die Anwendung zu bringen. Diese Lehrveranstaltung stellt die grundsätzlichen Konzepte von Betriebssystemen anhand des Lehrbetriebssystems ULIX vor (http://ulixos.org). Der Schwerpunkt liegt dabei einerseits auf der Implementierung von Betriebssystemen, andererseits auf der Benutzung von Betriebssystemkonzepten zur nebenläufigen Programmierung. Inhaltsübersicht: • Betriebssysteme aus Anwenderssicht • Virtueller Speicher • Virtuelle Prozessoren (Threads) • Synchronisationsprimitive (Spin Locks, Semaphore, Monitore) • Nebenläufige Programmierung
Lernziele und Kompetenzen:	*Fachkompetenz:* Die Studierenden erwerben fundierte Kenntnisse über die Funktionsweise von Betriebssystemen, deren Implementierung sowie die Benutzung von Betriebssystemmechanismen zur nebenläufigen Programmierung. Sie können die erlernten Konzepte in echten Betriebssystemen erkennen und können einfache Varianten der Konzepte im Lehrbetriebssystem ULIX hinzufügen. *Methodenkompetenz:* Die Studierenden können nebenläufige Programme analysieren und auf Fehler überprüfen. Sie können korrekte nebenläufige Programme selbst erstellen. Die Studierenden können Implementierungsalternativen von Betriebssystemkonzepten objektiv vergleichen und eine begründete Auswahl für eine konkrete Anwendungssituation treffen. *Sozialkompetenz:* Durch die gemeinsame Arbeit an Übungen im Rahmen des Präsenzwochenendes und der Online-Veranstaltungen verbessern die Studierenden ihre Teamfähigkeit und Sozialkompetenz. *Selbstkompetenz:* Die Studierenden lernen, komplexe Fragestellungen selbstständig zu durchdenken und ihren Lernerfolg selbst zu planen und einzuschätzen.
Häufigkeit des Angebots:	Wintersemester
Medienformen:	Studienbriefe in schriftlicher und elektronischer Form, Onlinematerial in Lernplattform, Übungen und Projekt über Lernplattform, Online-Konferenzen, Chat und Forum, Präsenzveranstaltung mit Computer und Projektor.

Literaturhinweise:	• Hans-Georg Eßer, Felix Freiling: The Design and Implementation of the ULIX Operating System, FAU Erlangen-Nürnberg, 2015 (*als Lehrbrief verfügbar*). Weiterführende Literatur (kein Erwerb nötig) • Jürgen Nehmer, Peter Sturm: Systemsoftware – Grundlagen moderner Betriebssysteme. dpunkt.verlag, 2. Auflage, 2001. • Andrew S. Tanenbaum: Modern Operating Systems. Prentice Hall, 3. Auflage, 2008. • William Stallings: Operating Systems: Internals and Design Principles. Prentice Hall, 9. Auflage, 2017. • Marshall Kirk McKusick, George V. Neville-Neil: The Design and Implementation of the FreeBSD Operating System. Addison-Wesley, 2. Auflage, 2014. • Maurice J. Bach: The Design of the Unix Operating System. Prentice-Hall, 1986. • John Lions: Lions' Commentary on UNIX 6th Edition with Source Code. Peer to Peer Communications, 1996. • Andrew S. Tanenbaum, Albert S. Woodhull: Operating Systems Design and Implementation (The MINIX book). 3. Auflage, Pearson, 2006.

Algorithmen und Datenstrukturen (Algorithms and Data Structures)

Modulbezeichnung:	Algorithmen und Datenstrukturen (Algorithms and Data Structures)
Verwendbarkeit:	Bachelorstudiengang Informatik/IT-Sicherheit (Pflichtmodul)
Lehrveranstaltungen und Lehrformen:	Algorithmen und Datenstrukturen Selbstlernphasen, Übungen, Online-Phasen, Präsenzveranstaltung
Modulverantwortliche(r):	Prof. Dr. Felix Freiling
Lehrende:	Dr. Werner Massonne
Dauer:	1 Semester
Credits:	5 ECTS-Punkte
Studien- und Prüfungsleistungen:	Klausur: 60 Min.
Berechnung der Modulnote:	100% der schriftlichen Prüfungsnote
Notwendige Voraussetzungen für die Teilnahme:	
Empfohlene Voraussetzungen für die Teilnahme:	• Programmierkonzepte • Mathematik 1 • Mathematik 2 (Wahrscheinlichkeitsrechnung aus Lehrveranstaltung Mathematik 2b)
Unterrichts- und Prüfungssprache:	Deutsch
Zuordnung des Moduls zu den Fachgebieten des Curriculums:	Informatik Grundlagen
Einordnung ins Fachsemester:	Ab Studiensemester 3
Arbeitsaufwand bzw. Gesamtworkload:	Präsenzstudium: 15 Zeitstunden Fernstudienanteil: 135 Zeitstunden • Selbststudium: 90 Zeitstunden • Aufgaben: 30 Zeitstunden • Online-Betreuung: 15 Zeitstunden **Summe: 150 Zeitstunden**

Lerninhalte:	In diesem Modul werden die folgenden Themengebiete behandelt: • Programmierkurs zur Erlernung der Programmierung in C • Analysemodell, Lauzeitmodelle und allgemeine Analysetechniken für Algorithmen • Strukturierte Datentypen wie Arrays, Listen, Bäume und Graphen • Verschiedene Sortieralgorithmen mit ihren Laufzeitanalysen • Algorithmen auf Mengen: Suchen, TRIES, Hashing, Union-Find und Priority Queues • Balancierte Suchbäume, insbesondere AVL-Bäume und B-Bäume • Repräsentation von Graphen und fundamentale Algorithmen auf Graphen • Vertiefung der Graphenalgorithmen: Zusammenhangskomponenten und Bestimmung kürzester Pfade • Implementierung der vorgestellten Algorithmen in C
Lernziele und Kompetenzen:	*Fachkompetenz:* Die Studierenden erwerben fundierte Kenntnisse in der Programmiersprache C. Sie lernen grundlegende Datenstrukturen und Algorithmen der Informatik kennen und erlernen, diese bezüglich Effizienz einzuschätzen und in einer konkreten Programmiersprache umzusetzen. *Methodenkompetenz:* Die Studierenden erwerben die Fähigkeit, konkrete Programmieraufgaben in einer höheren Programmiersprache zu formulieren. Lernende können hierbei die Gesamtaufgabe strukturieren und in Teilaufgaben zerlegen. Die Studierenden erlernen die Fähigkeit, geeignete Datenstrukturen und Algorithmen zur Abbildung von Programmieraufgaben zu finden, die eine effiziente Umsetzung gestatten. *Sozialkompetenz:* Aufgrund der Teamarbeit, unter anderem in den Präsenzwochenenden, erweitern die Studierenden ihre Teamfähigkeit und Sozialkompetenz. *Selbstkompetenz:* Die Studierenden erlangen die Fähigkeit zur Bildung einer Meinung über die eigenen Programme und die Programme anderer. Darüber hinaus erlangen sie die Fähigkeit, in komplexen Situationen zu handeln und eine Lösung für komplexe Probleme zu finden.
Häufigkeit des Angebots:	Wintersemester
Medienformen:	Studienbriefe in schriftlicher und elektronischer Form, Onlinematerial in Lernplattform, Übungen und Projekt über Lernplattform, Online-Konferenzen, Chat und Forum, Präsenzveranstaltung mit Rechner und Beamer

Literaturhinweise:	Begleitende Literatur: • eigenes Skript (Studienbriefe) Als weiterführende Literatur wird empfohlen: • Algorithmen und Datenstrukturen: Die Grundwerkzeuge; Dietzfelbinger, Mehlhorn and Sanders, 2014 • Algorithmen - Eine Einführun; Corman, Leiserson, Rivest und Stein, 2013

Theoretische Informatik (Theoretical Computer Science)

Modulbezeichnung:	Theoretische Informatik (Theoretical Computer Science)
Verwendbarkeit:	Bachelorstudiengang Informatik/IT-Sicherheit (Pflichtmodul)
Lehrveranstaltungen und Lehrformen:	Theoretische Informatik Selbstlernphasen, Übungen, Online-Phasen, Präsenzveranstaltung
Modulverantwortliche(r):	Prof. Dr. Steffen Lange
Lehrende:	Prof. Dr. Steffen Lange
Dauer:	1 Semester
Credits:	5 ECTS-Punkte
Studien- und Prüfungsleistungen:	Klausur: 60 min.
Berechnung der Modulnote:	100% der schriftlichen Prüfungsnote
Notwendige Voraussetzungen für die Teilnahme:	
Empfohlene Voraussetzungen für die Teilnahme:	Erfolgreicher Abschluss des Moduls • Mathematik 2
Unterrichts- und Prüfungssprache:	Deutsch
Zuordnung des Moduls zu den Fachgebieten des Curriculums:	Informatik Grundlagen
Einordnung ins Fachsemester:	Ab Studiensemester 3
Arbeitsaufwand bzw. Gesamtworkload:	Präsenzstudium: 15 Zeitstunden Fernstudienanteil: 135 Zeitstunden • Selbststudium: 90 Zeitstunden • Aufgaben: 30 Zeitstunden • Online-Betreuung: 15 Zeitstunden **Summe: 150 Zeitstunden**

Lerninhalte:	In diesem Modul werden die folgenden Themengebiete behandelt: • Grundbegriffe: Wörter, Alphabete, formale Sprachen, Entscheidungsprobleme, (effiziente) Lösungsalgorithmen für Entscheidungsprobleme • Formale Sprachen/Automatentheorie: Chomsky-Grammatiken, Chomsky-Hierarchie, Wortproblem, entscheidbare und effektiv aufzählbare Sprachen, rechtslineare Sprachen, endliche Automaten, nichtdeterministische Automaten, Nerode-Relation und Nerode-Index, Minimierungsalgorithmus für deterministische Automaten, kontextfreie Sprachen, Chomsky-Normalform, CYK-Algorithmus, Pumping-Lemma für kontextfreie Sprachen, Kellerautomaten, deterministische Kellerautomaten • Berechnungstheorie: unlösbare algorithmische Probleme

Lernziele und Kompetenzen:	*Fachkompetenz:* Die Studierenden erlangen ein Verständnis für grundlegende Konzepte, Begriffe und Zusammenhänge aus den Teilgebieten Formale Sprachen uud Automatentheorie sowie Berechnungstheorie und haben ein Verständnis für grundlegende Beweismethoden entwickelt. Sie haben die Fähigkeit herausbildet, einfache Beweise selbständig zu führen. Außerden haben Sie Kenntnis von der Leistungsfähigkeit unterschiedlicher Beschreibungsmittel und haben die Fähigkeit entwickelt, die Beschreibungsmittel selbständig zu gebrauchen. Darüber hinaus haben Sie das Wissen zum Zusammenhang zwischen der Leistungsfähigkeit und der algorithmischen Beherrschbarkeit unterschiedlicher Beschreibungsmittel erlangt. Die Studierenden haben desweiteren ein Verständnis für nichtdeterministische Maschinenmodelle und deren Bedeutung entwickelt. Sie können mit den deterministischen und nichtdeterministischen Maschinenmodellen umgehen. Sie haben ferner ein erstes Verständnis für die algorithmische Lösbarkeit/Unlösbarkeit von Problemen entwickelt. *Methodenkompetenz:* Die Studierenden können Fragen zu den oben genannten Fachkompetenzen schriftlich beantworten. Sie können zu gegebenen formalen Sprachen Grammatiken und Automaten entwickeln, welche die gegebene formale Sprache erzeugt und akzeptiert. Darüber hinaus können Sie die Korrektheit der entwickelten Grammatiken und Automaten zeigen. Sie können einen gegebenen deterministischen Automaten minimieren und gegebene kontextfreie Grammatiken in die Chomsky-Normalform umwandeln. Weiter können Sie zeigen, ob eine gegebene Sprache rechtslinear bzw. kontextfrei ist oder nicht, und Sie können erläutern, zu welcher Klasse der Chomsky-Hierarchie eine gegebene Sprache gehört. Sie beherrschen die grundlegenden Beweismethoden und haben die Fähigkeit, einfache Beweise selbständig zu führen. Sie kennen Beispiele für unlösbare algorithmische Probleme und wissen, wie sich nachweisen lässt, dass ein algorithmisches Problem unlösbar ist. *Sozialkompetenz:* Die Studierenden sind in der Lage als Team zusammenzuarbeiten und so Lösungen für die gestellten Aufgaben zu finden. Darüber hinaus können Sie zu den Themen eine fachgebundene Diskussion führen. *Selbstkompetenz:* Die Studierenden sind in der Lage die Lösungen zu den Aufgaben und Problemen mündlich und schriftlich zu formulieren und zu präsentieren. Dadurch können Sie sich auch gegen Einwände in einer Diskussion verteidigen. Sie sind in der Lage selbständig geeignete Literatur zu finden und einzusetzen.
Häufigkeit des Angebots:	Wintersemester
Medienformen:	Studienbriefe in schriftlicher und elektronischer Form, Onlinematerial in der Lernplattform, Übungen über die Lernplattform, Online-Konferenzen, Chat und Forum, Präsenzveranstaltung mit Rechner und Beamer sowie Tafel.

Literaturhinweise:	Als begleitende Literatur wird ein Vorlesungsskript zur Verfügung gestellte. Als vertiefende Literatur wird empfohlen: 1. Hromkovič, J.: Theoretische Informatik, Teubner Verlag, Stuttgart, 2011. 2. Schöning, U.: Theoretische Informatik – kurz gefaßt, Spektrum Akademischer Verlag, Heidelberg, 2008. 3. Wegener, I.: Theoretische Informatik – eine algorithmenorientierte Einführung, Teubner Verlag, Stuttgart, 2005.

Kryptographie 1 (Cryptography 1)

Modulbezeichnung:	Kryptographie 1 (Cryptography 1)
Verwendbarkeit:	Bachelorstudiengang Informatik/IT-Sicherheit (Pflichtmodul)
Lehrveranstaltungen und Lehrformen:	Kryptographie 1 Selbstlernphasen, Übungen, Online-Phasen, Präsenzveranstaltung
Modulverantwortliche(r):	Prof. Dr. Christof Paar
Lehrende:	Prof. Dr. Christof Paar
Dauer:	1 Semester
Credits:	5 ECTS-Punkte
Studien- und Prüfungsleistungen:	Klausur: 120 min.
Berechnung der Modulnote:	100 % der schriftlichen Prüfungsnote
Notwendige Voraussetzungen für die Teilnahme:	
Empfohlene Voraussetzungen für die Teilnahme:	
Unterrichts- und Prüfungssprache:	Deutsch und Englisch
Zuordnung des Moduls zu den Fachgebieten des Curriculums:	IT-Sicherheit Grundlagen
Einordnung ins Fachsemester:	Ab Studiensemester 4
Arbeitsaufwand bzw. Gesamtworkload:	Präsenzstudium: 15 Zeitstunden Fernstudienanteil: 135 Zeitstunden • Selbststudium: 85 Zeitstunden • Aufgaben: 40 Zeitstunden • Online-Betreuung: 10 Zeitstunden **Summe: 150 Zeitstunden**
Lerninhalte:	In diesem Modul werden zunächst einige grundlegende Begriffe der Kryptographie erläutert. Danach werden mehrere historisch wichtige Verschlüsselungsverfahren vorgestellt. Weiterhin wird das Konzept einer perfekt sicheren Chiffre eingeführt und es werden die grundlegenden Bausteine für Stromchiffren ausführlich besprochen. Als bedeutende Vertreter der symmetrischen Verschlüsselungsverfahren werden der Data Encryption Standard (DES) und der Advanced Encryption Standard (AES) behandelt. Zum Abschluss wird weiteres grundlegendes Wissen über Blockchiffren vermittelt.

Lernziele und Kompetenzen:	*Fachkompetenz:* Die Studierenden kennen die Bedeutung von symmetrischen kryptographischen Verfahren und verstehen die Strukturen der prominentesten symmetrischen Primitiven. Darüber hinaus verinnerlichen die Studenten die Sicherheitskonzepte und diverse Angriffsziele von symmetrischen Verfahren. *Methodenkompetenz:* Die Studierenden beherrschen die Denkweisen, die in der modernen Kryptographie eingesetzt werden und können diese anhand von symmetrischen Verfahren nachvollziehen. *Sozialkompetenz:* Die Studenten tauschen sich über Probleme beim Verstehen von symmetrischen kryptographischen Verfahren aus und diskutieren Lösungswege von Problemen. *Selbstkompetenz:* Die Studenten erlangen die Fähigkeit aktuelle symmetrische kryptographische Verfahren zu verstehen und eine fundierte Meinung über die Sicherheit dieser Verfahren zu vertreten. Darüber hinaus besitzen die Studierenden alle Voraussetzungen neue symmetrische Verfahren aus der aktuellen Fachliteratur zu verstehen und ihre Bedeutung einzuschätzen.
Häufigkeit des Angebots:	Sommersemester
Medienformen:	Onlinematerial in Lernplattform, Übungen über Lernplattform, Online-Konferenzen, Chat und Forum
Literaturhinweise:	• Kryptographie verständlich, Christof Paar, Jan Pelzl, 2016 • Understanding Cryptography, Christof Paar, Jan Pelzl, 2010 • Handbook of Applied Cryptography, Alfred J. Menezes, Paul C van Oorschot, Scott A Vanstone, 1996

Systemnahe Programmierung (Machine-Oriented Programming)

Modulbezeichnung:	Systemnahe Programmierung (Machine-Oriented Programming)
Verwendbarkeit:	Bachelorstudiengang Informatik/IT-Sicherheit (Pflichtmodul)
Lehrveranstaltungen und Lehrformen:	Systemnahe Programmierung Selbstlernphasen, Übungen, Online-Phasen, Präsenzveranstaltung
Modulverantwortliche(r):	Prof. Dr. Felix Freiling
Lehrende:	Dr. Werner Massonne
Dauer:	1 Semester
Credits:	5 ECTS-Punkte
Studien- und Prüfungsleistungen:	Hausarbeit
Berechnung der Modulnote:	100% der schriftlichen Prüfungsnote
Notwendige Voraussetzungen für die Teilnahme:	
Empfohlene Voraussetzungen für die Teilnahme:	• Rechnerstrukturen • Algorithmen und Datenstrukturen
Unterrichts- und Prüfungssprache:	Deutsch
Zuordnung des Moduls zu den Fachgebieten des Curriculums:	Informatik Grundlagen
Einordnung ins Fachsemester:	Ab Studiensemester 4
Arbeitsaufwand bzw. Gesamtworkload:	Präsenzstudium: 15 Zeitstunden Fernstudienanteil: 135 Zeitstunden • Selbststudium: 90 Zeitstunden • Aufgaben: 30 Zeitstunden • Online-Betreuung: 15 Zeitstunden **Summe: 150 Zeitstunden**

Lerninhalte:	In diesem Modul werden die folgenden Themengebiete behandelt: • Allgemeine Rechner- und Betriebssystemstrukturen • Innere Strukturen des Betriebssystems Microsoft Windows • Assemblerprogrammierung der Intel-Architektur-32 (IA-32) • Codeerzeugung, Codeoptimierung und Programmanalyse für IA-32 • Systemnahe Sicherheitsaspekte, insbesondere Mechanismen von Buffer Overflow und sonstigen Sicherheitslücken sowie Gegenmaßnahmen zur Verhinderung ihrer Ausbeutung • Obfuscation und sonstige Malware-Techniken. Malware-Analyse durch das Analyseprogramm IDA anhand realer Beispiele
Lernziele und Kompetenzen:	*Fachkompetenz:* Die Studierenden haben fundierte Kenntnisse in der Programmierung von IA-32 auf Maschinenebene. Sie können Maschinencode aus der Hochsprache C erzeugen und haben einen Überblick über Verfahren zur Codeoptimierung und Codeverschleierung (Obfuscation). Die Studierenden haben einen Einblick in die Funktionsweise von Malware auf Systemebene und können einfache Malware selbstständig analysieren. *Methodenkompetenz:* Die Studierenden haben die Fähigkeit, systemnahe Programme zu erstellen und zu verstehen. Die Studierenden können Probleme auf dieser Ebene der Programmierung erkennen und Schwachstellen identifizieren und analysieren. *Sozialkompetenz:* Aufgrund der Teamarbeit, unter anderem an den Präsenzwochenenden, erweitern die Studierenden ihre Teamfähigkeit und Sozialkompetenz. *Selbstkompetenz:* Durch das eigenverantwortliche Entwickeln von Programmen erweitern die Studierenden ihr selbstständiges Handeln. Durch die Präsentation ihrer Ergebnisse wird die Selbstsicherheit der Studierenden gestärkt.
Häufigkeit des Angebots:	Sommersemester
Medienformen:	Studienbriefe in schriftlicher und elektronischer Form, Onlinematerial in Lernplattform, Übungen und Projekt über Lernplattform, Online-Konferenzen, Chat und Forum, Präsenzveranstaltung mit Rechner und Beamer

Literaturhinweise:	Begleitende Literatur: • eigenes Skript (Studienbriefe) Als weiterführende Literatur wird empfohlen: • Intel 80386, Programmers Reference Manual, 1987 • Practical Malware Analysis: The Hands-On Guide to Dissecting Malicious Software, Sikorski and Honig, 2012

Systemsicherheit 2 (System Security 2)

Modulbezeichnung:	Systemsicherheit 2 (System Security 2)
Verwendbarkeit:	Bachelorstudiengang Informatik/IT-Sicherheit (Pflichtmodul)
Lehrveranstaltungen und Lehrformen:	Systemsicherheit 2 Selbstlernphasen, Übungen, Online-Phasen, Präsenzveranstaltung
Modulverantwortliche(r):	Prof. Dr. Daniel Hammer
Lehrende:	Prof. Dr. Daniel Hammer
Dauer:	1 Semester
Credits:	5 ECTS-Punkte
Studien- und Prüfungsleistungen:	Klausur: 60 min.
Berechnung der Modulnote:	100% der schriftlichen Prüfungsnote
Notwendige Voraussetzungen für die Teilnahme:	
Empfohlene Voraussetzungen für die Teilnahme:	Systemsicherheit 1
Unterrichts- und Prüfungssprache:	Deutsch
Zuordnung des Moduls zu den Fachgebieten des Curriculums:	IT-Sicherheit Vertiefung
Einordnung ins Fachsemester:	Ab Studiensemester 4
Arbeitsaufwand bzw. Gesamtworkload:	Präsenzstudium: 15 Zeitstunden Fernstudienanteil: 135 Zeitstunden • Selbststudium: 105 Zeitstunden • Aufgaben: 20 Zeitstunden • Online-Betreuung: 10 Zeitstunden Summe: 150 Zeitstunden
Lerninhalte:	Im Modul Systemsicherheit 2 wird auf folgende Themengebiete eingegangen: • Sicherheitsmechanismen- und modelle • Vorstellung und Erläuterung der Sicherheitsaspekte von Betriebssystemen. • Malware • Angriffsszenarien • Abwehrmechanismen

Lernziele und Kompetenzen:	*Fachkompetenz:* Die Studierenden erlangen anhand von Beispielen das Basiswissen über Malware, wie Schadsoftware funktioniert und welche Gefahr von ihr ausgeht. Ferner erwerben sie Kenntnisse über die Sicherheitsmechanismen und -modelle von Betriebssystemen und können zwischen unterschiedlichen Angriffsszenarien differenzieren. Außerdem eignen sie sich das Wissen über die entsprechenden Abwehrmechanismen an. *Methodenkompetenz:* Die Studierenden können zwischen den unterschiedlichen Malware-Arten differenzieren und können die entsprechenden Schutzmaßnahmen einsetzen. Sie kennen die Sicherheitsmechanismen- und modelle von Betriebssystemen und ihre unterschiedlichen Sicherheitsaspekte. Außerdem wissen die Studierenden wie Programmierfehler ausgenutzt werden können, was Insider-Angriffe sind und wie und welche Abwehrmechanismen sie einsetzen können. *Sozialkompetenz:* Aufgrund der Teamarbeit, unter anderem in dem Präsenzwochenende, erweitern die Studierenden die Fähigkeit der Teamfähigkeit und Sozialkompetenz. *Selbstkompetenz:* Die Lernenden erlangen die Fähigkeit zur Bildung einer Meinung über IT-Sicherheit. Darüber hinaus erlangen sie die Fähigkeit, in komplexen Situationen zu handeln und eine Lösung für schwierige Probleme zu finden.
Häufigkeit des Angebots:	Sommersemester
Medienformen:	Studienbriefe in schriftlicher und elektronischer Form, Onlinematerial in Lernplattform, Übungen und Projekt über Lernplattform, Online-Konferenzen, Chat und Forum, Präsenzveranstaltung mit Rechner und Beamer.
Literaturhinweise:	• IT-Sicherheit: Konzepte - Verfahren - Protokolle, Claudia Eckert, 2014 • Moderne Betriebssysteme, Andrew S. Tanenbaum, 2009 • Betriebssysteme - Prinzipien und Umsetzung, William Stallings, 2005 • Malware, Eugene Kaspersky, 2008 • Computer Security, Dieter Gollmann, 2010 Weitere Literatur wird in der Lehrveranstaltung bekannt gegeben.

Proseminar IT-Sicherheit (Proseminar IT-Security)

Modulbezeichnung:	Proseminar IT-Sicherheit (Proseminar IT-Security)
Verwendbarkeit:	Bachelorstudiengang Informatik/IT-Sicherheit (Pflichtmodul)
Lehrveranstaltungen und Lehrformen:	Proseminar IT-Sicherheit Orientierungsphase mit Themenwahl, Ausarbeitung des Themas mit individueller Betreuung, Abschlussvortrag
Modulverantwortliche(r):	Prof. Dr.-Ing. Felix Freiling
Lehrende:	Die Betreuung kann durch alle am Studiengang beteiligten Professorinnen und Professoren sowie Dozentinnen und Dozenten erfolgen.
Dauer:	1 Semester
Credits:	5 ECTS-Punkte
Studien- und Prüfungsleistungen:	Schriftliche Ausarbeitung im Umfang von 6-15 Seiten und mündliche Präsentation im Umfang von 30 Minuten mit anschließender Diskussion im Umfang von 15 Minuten
Berechnung der Modulnote:	50% schriftliche Ausarbeitung + 50% Präsentation
Notwendige Voraussetzungen für die Teilnahme:	
Empfohlene Voraussetzungen für die Teilnahme:	• Erfolgreicher Abschluss der Grundlagen-und Orientierungsprüfung
Unterrichts- und Prüfungssprache:	Deutsch. Mit Zustimmung der Betreuerin bzw. des Betreuers darf die schriftliche Ausarbeitung in Englisch abgefasst werden.
Zuordnung des Moduls zu den Fachgebieten des Curriculums:	Informatik Grundlagen
Einordnung ins Fachsemester:	Studiensemester 4
Arbeitsaufwand bzw. Gesamtworkload:	Summe: 150 h Präsenzzeit: 1 h • Seminarvortrag: Präsentation und Diskussion Eigenstudium: 149 h • Themenbearbeitung • Besprechungen mit dem Betreuer • Vorbereitung der Präsentation
Lerninhalte:	Der Themenbereich des Proseminars wird vor Semesterbeginn bekanntgeben. Jeder Studierende erhält ein individuelles, begrenztes Thema (z.B. Buchkapitel oder Konferenzveröffentlichung). Dieses wird nach den Kriterien wissenschaftlichen Arbeitens schriftlich ausgearbeitet und mündlich vor den Mitstudenten und Betreuern präsentiert.

Lernziele und Kompetenzen:	*Fachkompetenz:* Die Studierenden erkennen die Wichtigkeit des exakten wissenschaftlichen Arbeitens. Sie können eine begrenzte Fragestellung auf dem Gebiet der Informatik selbstständig recherchieren und ihre Ergebnisse präsentieren und verteidigen. *Methodenkompetenz:* Die Studierenden erkennen die Wichtigkeit des methodischen Arbeitens im wissenschaftlichen Umfeld und können diese Methodik bei einem begrenzten, vorgegebenen Thema anwenden. *Sozialkompetenz:* Durch die enge Zusammenarbeit mit dem Betreuer und die Präsentation der Ergebnisse in einem Kolloquium erweitern Studierenden ihre Teamfähigkeit und Sozialkompetenz. *Selbstkompetenz:* Die Studierenden können fachbezogene Inhalte klar und zielgruppengerecht schriftlich und mündlich präsentieren und argumentativ vertreten.
Häufigkeit des Angebots:	Sommersemester
Medienformen:	
Literaturhinweise:	

Einführung in die digitale Forensik (Introduction to digital forensics)

Modulbezeichnung:	Einführung in die digitale Forensik (Introduction to digital forensics)
Verwendbarkeit:	Bachelorstudiengang Informatik/IT-Sicherheit (Pflichtmodul)
Lehrveranstaltungen und Lehrformen:	Einführung in die digitale Forensik Selbstlernphasen, Übungen, Online-Phasen, Präsenzveranstaltung
Modulverantwortliche(r):	Prof. Dr. Harald Baier
Lehrende:	Prof. Dr. Harald Baier
Dauer:	1 Semester
Credits:	5 ECTS-Punkte
Studien- und Prüfungsleistungen:	Hausarbeit
Berechnung der Modulnote:	100% der schriftlichen Prüfungsnote
Notwendige Voraussetzungen für die Teilnahme:	
Empfohlene Voraussetzungen für die Teilnahme:	• Kenntnisse über digitale Zahlendarstellungen und Kodierungen (z.B. ASCII) • Grundkenntnisse im Umgang mit Betriebssystemen (insbesondere Linux) • Sicherheit im Umgang mit der Linux-Kommandozeile • Grundlegende Programmierkenntnisse Erfolgreicher Abschluss der Module • Einführung IT Sicherheit • Systemsicherheit 1
Unterrichts- und Prüfungssprache:	Deutsch
Zuordnung des Moduls zu den Fachgebieten des Curriculums:	IT-Sicherheit Vertiefung
Einordnung ins Fachsemester:	Ab Studiensemester 5
Arbeitsaufwand bzw. Gesamtworkload:	Präsenzstudium: 15 Zeitstunden Fernstudienanteil: 135 Zeitstunden • Selbststudium: 90 Zeitstunden • Aufgaben: 30 Zeitstunden • Online-Betreuung: 15 Zeitstunden **Summe: 150 Zeitstunden**

Lerninhalte:	In diesem Modul werden die folgenden Themengebiete behandelt: • Klassische forensische Wissenschaften und digitale Forensik • Grundlagen der digitalen Forensik • Digitale Spuren (Entstehung, Manipulier- und Kopierbarkeit, Personenbezogenheit) • Datenträgeranalyse (DOS / GPT Partitionsschema, HPA, DCO) • Einführung in die Dateisystemanalyse (Generelles Konzept, FAT, NTFS) • Analyse mit forensischen Tools (Sleuthkit, Autopsy, DFF, Filecarver) • Vorgehensmodelle und Gutachtenerstellung • Hashfunktionen in der digitalen Forensik • Praktische Bearbeitung von Aufgaben
Lernziele und Kompetenzen:	*Fachkompetenz:* Die Studierenden kennen die Grundlagen der digitalen Forensik und können diese anwenden. Sie haben Kenntnis über die Entstehung, der Manipulier- und Kopierbarkeit sowie der Personenbezogenheit von digitalen Spuren. Sie kennen weiter das grundlegende Konzept sowie die Eigenschaften der gängigen Dateisysteme FAT und NTFS und können mit diesem Wissen eine Dateisystemanalyse durchführen. Darüber hinaus kennen Sie die grundlegenden Schritte eines IT-Forensikers und können mit allgemeinen und speziellen forensischen Werkzeugen sicher umgehen. Des Weiteren sind die Studierenden mit der grundlegenden Funktionsweise kryptographischer Hashfunktionen, sowie deren Rolle in der digitalen Forensik vertraut. *Methodenkompetenz:* Die Studierenden beherrschen den Umgang mit den forensischen Tools und können wichtige Ergebnisse daraus eigenständig entnehmen. Sie sind mit den Grundprinzipien der IT-Forensik vertraut und können diese bei einer forensischen Untersuchung anwenden. Sie können weiter mit dem erlangten Wissen aus dem Modul sicher umgehen und können Aufgaben und Problemstellungen nachvollziehen und lösen. *Sozialkompetenz:* Die Studierenden erlernen aufgrund gemeinsamer forensischen Untersuchungen im Team zu arbeiten und können auftretende Probleme, Fragen und Aufgaben durch fachgebunden Diskussion lösen. *Selbstkompetenz:* Die Studierenden erlangen die Fähigkeit eine forensische Untersuchung durchzuführen und sind in der Lage die Ergebnisse zu bewerten. Des Weiteren besitzen Sie die Kompetenz sich an neue Gegebenheiten anzupassen und können so auf veränderte Hardware und Software reagieren.
Häufigkeit des Angebots:	Wintersemester

Medienformen:	Studienbriefe in schriftlicher und elektronischer Form, Onlinematerial in Lernplattform, Übungen und Projekt über Lernplattform, Online-Konferenzen, Chat und Forum, Präsenzveranstaltung mit Rechner und Beamer.
Literaturhinweise:	Als begleitende und vertiefende Literatur wird empfohlen: • Eigenes Skript • Brian Carrier: File System Forensic Analysis, 5th Printing. Addison-Wesley Longman, Amsterdam (17. März 2005), ISBN 978-0321268174. • Eoghan Casey (Hrsg.): Handbook of computer crime investigation. Forensic tools and technology. 6th Printing. Elsevier Academic Press, Amsterdam u. a. 2007, ISBN 978-0-12-163103-1. • Alexander Geschonneck: Computer-Forensik. Computerstraftaten erkennen, ermitteln, aufklären. 5. aktualisierte und erweiterte Auflage. dpunkt Verlag, Heidelberg 2011, ISBN 978-3-89864-774-8. Weitere Literatur wird in der Lehrveranstaltung bekannt gegeben.

Compilerbau (Compiler Construction)

Modulbezeichnung:	Compilerbau (Compiler Construction)
Verwendbarkeit:	Bachelorstudiengang Informatik/IT-Sicherheit (Pflichtmodul)
Lehrveranstaltungen und Lehrformen:	Compilerbau Selbstlernphasen, Übungen, Online-Phasen, Präsenzveranstaltung
Modulverantwortliche(r):	Prof. Dr. Felix Freiling
Lehrende:	Dr. Werner Massonne
Dauer:	1 Semester
Credits:	5 ECTS-Punkte
Studien- und Prüfungsleistungen:	Klausur: 60 Min.
Berechnung der Modulnote:	100% der schriftlichen Prüfungsnote
Notwendige Voraussetzungen für die Teilnahme:	
Empfohlene Voraussetzungen für die Teilnahme:	• Systemnahe Programmierung • Algorithmen und Datenstrukturen • Theoretische Informatik
Unterrichts- und Prüfungssprache:	Deutsch
Zuordnung des Moduls zu den Fachgebieten des Curriculums:	Informatik Vertiefung
Einordnung ins Fachsemester:	Ab Studiensemester 5
Arbeitsaufwand bzw. Gesamtworkload:	Präsenzstudium: 15 Zeitstunden Fernstudienanteil: 135 Zeitstunden • Selbststudium: 90 Zeitstunden • Aufgaben: 30 Zeitstunden • Online-Betreuung: 15 Zeitstunden **Summe: 150 Zeitstunden**

Lerninhalte:	Im Modul Compilerbau wird auf folgende Themengebiete eingegangen: • Anwendungsgebiete und Aufbau von Compilern • Lexikalische Analyse auf Basis von regulären Sprachen • Syntaktische Analyse auf Basis von kontextfreien Grammatiken • Semantische Analyse durch attributierte Grammatiken und syntaxgesteuerte Definitionen, Erzeugung von Zwischencode • Optimierung und Codeerzeugung • Entwicklungswerkzeuge: Scannergenerator Flex und Parsergenerator Bison
Lernziele und Kompetenzen:	*Fachkompetenz:* Die Studierenden erwerben fundierte Kenntnisse über die Funktionsweise und Arbeitsschritte von Compilern. Sie können die theoretischen Konzepte erklären, die benötigt werden, um ausgehend von einer formalen Sprachdefinition einen Compiler zu konstruieren. Mit Hilfe der Tools Flex und Bison können die Studierenden selbst Compiler für realistische Einsatzszenarien erzeugen. *Methodenkompetenz:* Die Studierenden beherrschen die Methodik, für eine gegebene Quellsprache und eine gewünschte Zielsprache einen phasenbasierten Compiler zu bauen. Dabei kommen gewöhnlich Tools zur Anwendung, die eine starke Unterstützung bei der Umsetzung der theoretischen Modelle bieten. *Sozialkompetenz:* Aufgrund der Teamarbeit, unter anderem in den Präsenzwochenenden, erweitern die Studierenden ihre Teamfähigkeit und Sozialkompetenz. *Selbstkompetenz:* Die Studierenden erlangen die Fähigkeit zur Bildung einer Meinung über die eigene Arbeitsweise und die Arbeitsweise anderer. Darüber hinaus erlangen sie die Fähigkeit, in komplexen Situationen zu handeln und eine Lösung für komplexe Probleme zu finden.
Häufigkeit des Angebots:	Wintersemester
Medienformen:	Studienbriefe in schriftlicher und elektronischer Form, Onlinematerial in Lernplattform, Übungen und Projekte über Lernplattform, Online-Konferenzen, Chat und Forum, Präsenzveranstaltungen mit Computer und Beamer.

Literaturhinweise:	Begleitende Literatur: • eigenes Skript (Studienbriefe) Als weiterführende Literatur wird empfohlen: • Übersetzerbau Band 2: Syntaktische und semantische Analyse, Reinhard Wilhelm, Helmut Seidl, Sebastian Hack, Springer Verlag, 2012 • Flex und Bison, John Levine, O'Reilly Media, 2009 • Compilerbau Teil 1+2, Alfred V. Aho, Ravi Sethi, Jeffrey D. Ullman, Oldenbourg Wissenschaftsverlag, 1999 • Übersetzerbau, Ralf Hartmut Güting and Martin Erwig, Springer Verlag, 1998

Netzsicherheit 1 (Network Security 1)

Modulbezeichnung:	Netzsicherheit 1 (Network Security 1)
Verwendbarkeit:	Bachelorstudiengang Informatik/IT-Sicherheit (Pflichtmodul)
Lehrveranstaltungen und Lehrformen:	Netzsicherheit 1 Selbstlernphasen, Übungen, Online-Phasen, Präsenzveranstaltung
Modulverantwortliche(r):	Prof. Dr. Jörg Schwenk
Lehrende:	Prof. Dr. Jörg Schwenk, Martin Grothe
Dauer:	1 Semester
Credits:	5 ECTS-Punkte
Studien- und Prüfungsleistungen:	Klausur: 120 min.
Berechnung der Modulnote:	100 % der schriftlichen Prüfungsnote
Notwendige Voraussetzungen für die Teilnahme:	
Empfohlene Voraussetzungen für die Teilnahme:	Erfolgreicher Abschluss der vorherigen Module insbesondere: • Grundlagen der Programmierung • Kryptographie 1
Unterrichts- und Prüfungssprache:	Deutsch und Englisch
Zuordnung des Moduls zu den Fachgebieten des Curriculums:	IT-Sicherheit Grundlagen
Einordnung ins Fachsemester:	Ab Studiensemester 5
Arbeitsaufwand bzw. Gesamtworkload:	Präsenzzeit: 15 Zeitstunden Fernstudienanteil: 135 Zeitstunden • Durcharbeiten der Studienbriefe: 80 Zeitstunden • Durcharbeiten des Online-Lernmaterials: 15 Zeitstunden • Wahrnehmen der Online Betreuung und Beratung: 10 Zeitstunden • Ausarbeiten von Aufgaben: 25 h • Individuelle Prüfungsvorbereitung der Studierenden: 5 Zeitstunden **Summe: 150 Zeitstunden**

Lerninhalte:	Kryptographie wird eingesetzt, um die Vertraulichkeit und Integrität von Daten zu schützen, die über Datennetze übertragen werden. Hierbei werden sowohl symmetrische Verfahren (Mobilfunk, WLAN), als auch asymmetrische bzw. hybride Verfahren (E-Mail, VPN) eingesetzt. In diesem Modul werden konkrete kryptographische Systeme zur Absicherung von Netzen betrachtet, und von allen Seiten auf ihre Sicherheit hin beleuchtet. Dieses Modul umfasst folgende Themen: • Grundlagen Kryptographie und das Internet • PPP Sicherheit (insb. PPTP), EAP Protokolle • WLAN Sicherheit (WEP, WPA, Wardriving, KRACK) • GSM und UMTS (Authentisierung und Verschlüsselung) • IPsec (ESP und AH, IKEv1/v2, Angriffe auf IPsec) • Dateiverschlüsselung mit OpenPGP (Datenformat, Efail, climate-pink) • E Mail Verschlüsselung mittels S/MIME (SMTP, Datenformat, Efail, POP3, IMAP) Neben den Systemen selbst werden dabei auch publizierte Angriffe auf diese Systeme besprochen; die Studenten werden aufgefordert, selbst wissenschaftliche Überlegungen zur Verbesserung der Sicherheit anzustellen.
Lernziele und Kompetenzen:	*Fachkompetenz:* Die Studierenden erkennen die wichtigen Strukturen von Sicherheitsmechanismen in lokalen Datennetzen, verstehen Übertragungs- und Authentifizierungsprotokolle in Datennetzen und können die darin verwendeten kryptographischen Verfahren ermitteln. Die Studenten können das Zusammenspiel der kryptographischen Verfahren in einem Protokoll auf erste Sicherheitslücken hin überprüfen und eine erste Einschätzung der Sicherheit des Protokolls liefern. *Methodenkompetenz:* Die Studierenden beherrschen den Umgang mit Fachliteratur und können ihr wichtige Informationen eigenständig entnehmen. Weiterhin sind die Studierenden mit verschiedenen Angriffstechniken vertraut, welche auf neue Protokolle und Verfahren übertragen werden können. *Sozialkompetenz:* Die Studenten tauschen sich über Probleme beim Erarbeiten und Anwenden von neuen Inhalten aus und können problemorientiert diskutieren. *Selbstkompetenz:* Die Studenten erlangen die Fähigkeit, sich eine Meinung über die Sicherheit von Protokollen zu bilden. Darüber hinaus besitzen sie die Kompetenz, neue Angriffe aus der aktuellen Fachliteratur zu verstehen und ihre Bedeutungen zu evaluieren. Die Studenten entwickeln ein „gesundes Misstrauen“ gegenüber vorgegebenen Sicherheitskonzepten.

Häufigkeit des Angebots:	Wintersemester
Medienformen:	Studienbriefe in elektronischer Form, Onlinematerial in Lernplattform, Übungen über Lernplattform, Online-Konferenzen, Chat und Forum
Literaturhinweise:	• Sicherheit und Kryptographie im Internet, Jörg Schwenk, 2020 Weitere Literatur wird in der Lehrveranstaltung bekannt gegeben.

Kryptographie 2 (Cryptography 2)

Modulbezeichnung:	Kryptographie 2 (Cryptography 2)
Verwendbarkeit:	Bachelorstudiengang Informatik/IT-Sicherheit (Pflichtmodul)
Lehrveranstaltungen und Lehrformen:	Kryptographie 2 Selbstlernphasen, Übungen, Online-Phasen, Präsenzveranstaltung
Modulverantwortliche(r):	Prof. Dr. Christof Paar
Lehrende:	Prof. Dr. Christof Paar
Dauer:	1 Semester
Credits:	5 ECTS-Punkte
Studien- und Prüfungsleistungen:	Klausur: 120 min.
Berechnung der Modulnote:	100 % der schriftlichen Prüfungsnote
Notwendige Voraussetzungen für die Teilnahme:	
Empfohlene Voraussetzungen für die Teilnahme:	
Unterrichts- und Prüfungssprache:	Deutsch und Englisch
Zuordnung des Moduls zu den Fachgebieten des Curriculums:	IT-Sicherheit Grundlagen
Einordnung ins Fachsemester:	Ab Studiensemester 5
Arbeitsaufwand bzw. Gesamtworkload:	Präsenzstudium: 15 Zeitstunden Fernstudienanteil: 135 Zeitstunden • Selbststudium: 85 Zeitstunden • Aufgaben: 40 Zeitstunden • Online-Betreuung: 10 Zeitstunden **Summe: 150 Zeitstunden**
Lerninhalte:	In diesem Modul werden asymmetrische kryptographische Verfahren behandelt. Die Schwerpunkte dieses Moduls liegen auf der Besprechung von praktisch wichtigen Verfahren und deren Einsatz für asymmetrische Basisdienste. Es werden Verfahren, die auf dem diskreten Logarithmusproblem beruhen (Diffie-Hellman, ElGamal, elliptische Kurven), als auch das RSA-Verfahren behandelt. Außerdem werden digitale Signaturen eingeführt. Es werden die Grundlagen der symmetrischen und asymmetrischen Schlüsselverteilung behandelt.

Lernziele und Kompetenzen:	*Fachkompetenz:* Die Studierenden kennen die Bedeutung von asymmetrischen kryptographischen Verfahren und verstehen die Strukturen der prominentesten asymmetrischen Primitiven. Darüber hinaus verstehen die Studenten die Sicherheitskonzepte und diverse Angriffsziele in der asymmetrischen Kryptographie. Die Studenten können ihr Wissen über die Kryptographie anwenden und Sicherheitslösungen finden. *Methodenkompetenz:* Die Studierenden beherrschen die Denkweisen, die in der modernen Kryptographie eingesetzt werden und können diese anhand von asymmetrischen Verfahren nachvollziehen. *Sozialkompetenz:* Die Studenten tauschen sich über Probleme beim Verstehen von asymmetrischen kryptographischen Verfahren aus und diskutieren Lösungswege von Problemen. *Selbstkompetenz:* Die Studenten erlangen die Fähigkeit aktuelle asymmetrische kryptographische Verfahren zu verstehen und eine fundierte Meinung über die Sicherheit dieser Verfahren zu vertreten. Darüber hinaus besitzen die Studierenden alle Voraussetzungen neue asymmetrische Verfahren aus der aktuellen Fachliteratur zu verstehen und ihre Bedeutung einzuschätzen. Das umfangreiche Wissen der Studenten befähigt sie Sicherheitslösungen zu finden und einzusetzen.
Häufigkeit des Angebots:	Wintersemester
Medienformen:	Onlinematerial in Lernplattform, Übungen über Lernplattform, Online-Konferenzen, Chat und Forum
Literaturhinweise:	• Kryptographie verständlich, Christof Paar, Jan Pelzl, 2016 • Understanding Cryptography, Christof Paar, Jan Pelzl, 2010 • Handbook of Applied Cryptography, Alfred J. Menezes, Paul C van Oorschot, Scott A Vanstone, 1996

Netzsicherheit 2 (Network Security 2)

Modulbezeichnung:	Netzsicherheit 2 (Network Security 2)
Verwendbarkeit:	Bachelorstudiengang Informatik/IT-Sicherheit (Pflichtmodul)
Lehrveranstaltungen und Lehrformen:	Netzsicherheit 2 Selbstlernphasen, Übungen, Online-Phasen, Präsenzveranstaltung
Modulverantwortliche(r):	Prof. Dr. Jörg Schwenk
Lehrende:	Prof. Dr. Jörg Schwenk, Robert Merget
Dauer:	1 Semester
Credits:	5 ECTS-Punkte
Studien- und Prüfungsleistungen:	Klausur: 120 min.
Berechnung der Modulnote:	100 % der schriftlichen Prüfungsnote
Notwendige Voraussetzungen für die Teilnahme:	
Empfohlene Voraussetzungen für die Teilnahme:	Erfolgreicher Abschluss der vorherigen Module insbesondere: • Modul Grundlagen der Programmierung • Modul Netzsicherheit 1 • Modul Kryptographie 1 • Modul Kryptographie 2
Unterrichts- und Prüfungssprache:	Deutsch und Englisch
Zuordnung des Moduls zu den Fachgebieten des Curriculums:	IT-Sicherheit Grundlagen
Einordnung ins Fachsemester:	Ab Studiensemester 6
Arbeitsaufwand bzw. Gesamtworkload:	Präsenzzeit: 15 Zeitstunden Fernstudienanteil: 135 Zeitstunden • Durcharbeiten der Studienbriefe: 80 Zeitstunden • Durcharbeiten des Online-Lernmaterials: 15 Zeitstunden • Wahrnehmen der Online Betreuung und Beratung: 10 Zeitstunden • Ausarbeiten von Aufgaben: 25 h • Individuelle Prüfungsvorbereitung der Studierenden: 5 Zeitstunden **Summe: 150 Zeitstunden**

Lerninhalte:	Wenn Kryptographie in einer technischen Umgebung wie einem Computer-, Daten- oder Telefonnetz eingesetzt wird, hängt die Sicherheit nicht nur von rein kryptographischen Faktoren ab, sondern auch von der technischen Umsetzung der Verschlüsselungs- und Signaturalgorithmen. Prominente Beispiele (für fehlerhafte Umsetzungen) sind EFAIL (efail.de), Angriffe auf die WLAN-Verschlüsselungssysteme WEP und WPA (KRACK) und verschiedene Angriffe auf TLS (Bleichenbacher, POODLE, DROWN, ROBOT). Das Modul "Netzwerksicherheit"befasst sich mit konkreten Netzen zur Datenübertragung und untersucht diese von allen Seiten auf ihre Sicherheit. Es umfasst die folgenden Inhalte • Sicherheit von HTTP (HTTP-Authentifizierung, Secure HTTP, Architektur von SSL/TLS) • Sicherheit der Transportschicht (TLS1.2, Versionen SSL 2.0 bis TLS 1. 3) • Angriffe auf SSL und TLS (BEAST, CRIME, POODLE, Lucky13, Bleichenbacher, DROWN, Heartbleed, Invalid Curve) • Secure Shell SSH • Domain Name System und DNSSEC Neben den Systemen selbst werden dabei auch publizierte Angriffe auf diese Systeme besprochen; die Studenten werden aufgefordert, selbst wissenschaftliche Überlegungen zur Verbesserung der Sicherheit anzustellen.
Lernziele und Kompetenzen:	*Fachkompetenz:* Die Teilnehmer erwerben die Grundlagen zum Einrichten sicherer Kommunikationskanäle. Darüber hinaus lernen sie verschiedene Wege, wie die einzelnen Anwendungen in der Vergangenheit angegriffen wurden. *Methodenkompetenz:* Die Studierenden beherrschen den Umgang mit Fachliteratur und können ihr wichtige Informationen eigenständig entnehmen. Weiterhin sind die Studierenden mit verschiedenen Angriffstechniken vertraut, welche auf neue Protokolle und Verfahren übertragen werden können. *Sozialkompetenz:* Die Studenten tauschen sich über Probleme beim Erarbeiten und Anwenden von neuen Inhalten aus und können problemorientiert diskutieren. *Selbstkompetenz:* Die Studenten erlangen die Fähigkeit, sich eine Meinung über die Sicherheit von Protokollen zu bilden. Darüber hinaus besitzen sie die Kompetenz, neue Angriffe aus der aktuellen Fachliteratur zu verstehen und ihre Bedeutungen zu evaluieren. Die Studenten entwickeln ein "gesundes Misstrauen"gegenüber vorgegebenen Sicherheitskonzepten.
Häufigkeit des Angebots:	Sommersemester
Medienformen:	Studienbriefe in elektronischer Form, Onlinematerial in Lernplattform, Online-Konferenzen, Chat und Forum

Literaturhinweise:	• Sicherheit und Kryptographie im Internet, Jörg Schwenk, 2020 Weitere Literatur wird in der Lehrveranstaltung bekannt gegeben.

Realisierung von Softwareprojekten (Implementation of Software Engineering Projects)

Modulbezeichnung:	Realisierung von Softwareprojekten (Implementation of Software Engineering Projects)
Verwendbarkeit:	Bachelorstudiengang Informatik/IT-Sicherheit (Pflichtmodul)
Lehrveranstaltungen und Lehrformen:	Realisierung von Softwareprojekten Selbstlernphasen, Übungen, Online-Phasen, Präsenzveranstaltung
Modulverantwortliche(r):	Prof. Dr. Felix Freiling
Lehrende:	Philipp Klein
Dauer:	1 Semester
Credits:	5 ECTS-Punkte
Studien- und Prüfungsleistungen:	Hausarbeit (Umfang ca. 100 Zeitstunden)
Berechnung der Modulnote:	100% der Hausarbeitsnote
Notwendige Voraussetzungen für die Teilnahme:	
Empfohlene Voraussetzungen für die Teilnahme:	• Grundlagen der Programmierung • Konzeptionelle Modellierung
Unterrichts- und Prüfungssprache:	Deutsch
Zuordnung des Moduls zu den Fachgebieten des Curriculums:	Informatik Vertiefung
Einordnung ins Fachsemester:	Ab Studiensemester 6
Arbeitsaufwand bzw. Gesamtworkload:	Präsenzstudium: 15 Zeitstunden Fernstudienanteil: 135 Zeitstunden • Selbststudium: 25 Zeitstunden • Hausarbeit: 100 Zeitstunden • Online-Betreuung: 10 Zeitstunden **Summe: 150 Zeitstunden**

Lerninhalte:	Das Modul *Realisierung von Softwareprojekten* beinhaltet eine überwiegend praktische Herangehensweise bezüglich der Entwicklung von Software in einem Unternehmen. Im Fokus stehen konkrete Technologien und Anwendungen, die meist stellvertretend für eine ganze Gruppe betrachtet werden. So wird beispielsweise die Versionskontrollsoftware *Git* im Detail betrachtet, das Gelernte lässt sich aber auf andere Versionskontrollsoftware übertragen. Die Inhalte dieses Moduls sind: • Versionskontrolle mit Git • Webentwicklung mit Django • Softwaretesting • Continuous Integration mit GitlabCI • Deployment • Theorie der Softwareentwicklung
Lernziele und Kompetenzen:	*Fachkompetenz:* Die Studierenden erwerben fundierte Kenntnisse über den Prozess der Softwareentwicklung und die dabei vielfach eingesetzte Software. *Methodenkompetenz:* Die Studierenden beherrschen die grundlegenden Fertigkeiten und Applikationen, um bei einem Softwareprojekt in einem Unternehmen zeitnah produktiv mitarbeiten zu können. *Sozialkompetenz:* Aufgrund des Theoriewissens und der praktischen Anwendung von Vorgehensmodellen wie *Scrum* können sich die Studierenden in andere Rollen hineinversetzen und entsprechende Entscheidungen treffen. *Selbstkompetenz:* Durch ausprobieren von verschiedenster Software, die tatsächlich in Unternehmen bei der Softwareentwicklung eingesetzt wird, verändert sich auch die Umsetzung von eigenen Projekten. Die Studierenden haben erkannt, dass ein wenig Mehraufwand zu einer effizienteren Softwareentwicklung führt.
Häufigkeit des Angebots:	Sommersemester
Medienformen:	Studienbriefe in schriftlicher und elektronischer Form, Onlinematerial in Lernplattform, Übungen und Projekt über Lernplattform, Online-Konferenzen, Chat und Forum, Präsenzveranstaltung mit Rechner und Beamer

Literaturhinweise:	Als optionale weiterführende Literatur wird empfohlen: • Harry Percival: Test-Driven Development with Python, O'Reilly 2017 • S. Chacon, Ben Straub: Pro Git, Apress 2014, https://git-scm.com/book/en/v2 • Norman Don: The Design of Everyday Things, Vahlen 2016 Weitere Literatur wird in der Lehrveranstaltung bekanntgegeben

Seminar IT-Sicherheit (Seminar IT-Security)

Modulbezeichnung:	Seminar IT-Sicherheit (Seminar IT-Security)
Verwendbarkeit:	Bachelorstudiengang Informatik/IT-Sicherheit (Pflichtmodul)
Lehrveranstaltungen und Lehrformen:	Seminar IT-Sicherheit Orientierungsphase mit Themenwahl, Ausarbeitung des Themas mit individueller Betreuung, Abschlussvortrag
Modulverantwortliche(r):	Prof. Dr.-Ing. Felix Freiling
Lehrende:	Die Betreuung kann durch alle am Studiengang beteiligten Professorinnen und Professoren sowie Dozentinnen und Dozenten erfolgen.
Dauer:	1 Semester
Credits:	5 ECTS-Punkte
Studien- und Prüfungsleistungen:	Schriftliche Ausarbeitung im Umfang von 8-20 Seiten und mündliche Präsentation im Umfang von 30 Minuten mit anschließender Diskussion im Umfang von 15 Minuten
Berechnung der Modulnote:	50% schriftliche Ausarbeitung + 50% Präsentation
Notwendige Voraussetzungen für die Teilnahme:	
Empfohlene Voraussetzungen für die Teilnahme:	• Proseminar • Erfolgreicher Abschluss der Grundlagen-und Orientierungsprüfung
Unterrichts- und Prüfungssprache:	Deutsch. Mit Zustimmung der Betreuerin bzw. des Betreuers darf die schriftliche Ausarbeitung in Englisch abgefasst werden.
Zuordnung des Moduls zu den Fachgebieten des Curriculums:	Informatik Vertiefung
Einordnung ins Fachsemester:	Studiensemester 6
Arbeitsaufwand bzw. Gesamtworkload:	Summe: 150 h Präsenzzeit: 1 h • Seminarvortrag: Präsentation und Diskussion Eigenstudium: 149 h • Themenbearbeitung • Besprechungen mit dem Betreuer • Vorbereitung der Präsentation

Lerninhalte:	Der Themenbereich des Seminars wird vor dem Semester bekanntgeben. Jeder Studierende erhält ein individuelles Thema, in der Regel in Form eines initialen Papers. Von diesem ausgehend werden tiefere Literaturrecherchen zur Ergründung des Gesamtthemas durchgeführt. Die Ergebnisse werden nach den Kriterien wissenschaftlichen Arbeitens schriftlich ausgearbeitet und mündlich vor den Mitstudenten und Betreuern präsentiert.
Lernziele und Kompetenzen:	*Fachkompetenz:* Die Studierenden erweitern ihre im Proseminar erworbenen Kompetenzen. Sie können eine komplexere Fragestellung auf dem Gebiet der Informatik selbstständig recherchieren und ihre Ergebnisse präsentieren und verteidigen. *Methodenkompetenz:* Die Studierenden haben einen vertieften Einblick in die Methodiken wissenschaftlichen Arbeitens können diese Methodiken bei einem größeren, vorgegebenen Thema anwenden. *Sozialkompetenz:* Durch die Enge Zusammenarbeit mit dem Betreuer und die Präsentation der Ergebnisse in einem Kolloquium erweitern Studierenden ihre Teamfähigkeit und Sozialkompetenz. *Selbstkompetenz:* Die Studierenden können komplexe fachbezogene Inhalte klar und zielgruppengerecht schriftlich und mündlich präsentieren und argumentativ vertreten.
Häufigkeit des Angebots:	Sommersemester
Medienformen:	
Literaturhinweise:	

Weiterführende Themen der Computerforensik (Advanced topics in digital forensics)

Modulbezeichnung:	Weiterführende Themen der Computerforensik (Advanced topics in digital forensics)
Verwendbarkeit:	Bachelorstudiengang Informatik/IT-Sicherheit (Wahlpflichtmodul)
Lehrveranstaltungen und Lehrformen:	Weiterführende Themen der Computerforensik Selbstlernphasen, Übungen, Online-Phasen, Präsenzveranstaltung
Modulverantwortliche(r):	Prof. Dr. Harald Baier
Lehrende:	Prof. Dr. Harald Baier
Dauer:	1 Semester
Credits:	5 ECTS-Punkte
Studien- und Prüfungsleistungen:	Seminarleistung (schriftliche Ausarbeitung(ca. 10 Seiten) und Präsentation (20 Minuten))
Berechnung der Modulnote:	50% der schriftlichen + 50% der mündlichen Prüfungsnote
Notwendige Voraussetzungen für die Teilnahme:	
Empfohlene Voraussetzungen für die Teilnahme:	• Kenntnisse über digitale Zahlendarstellungen und Kodierungen (z.B. ASCII) • Grundkenntnisse im Umgang mit Betriebssystemen (insbesondere Linux) • Sicherheit im Umgang mit der Linux-Kommandozeile • Grundlegende Programmierkenntnisse Erfolgreicher Abschluss des Moduls • Einführung in die digitale Forensik
Unterrichts- und Prüfungssprache:	Deutsch
Zuordnung des Moduls zu den Fachgebieten des Curriculums:	IT-Sicherheit Vertiefung
Einordnung ins Fachsemester:	Ab Studiensemester 6
Arbeitsaufwand bzw. Gesamtworkload:	Präsenzstudium: 15 Zeitstunden Fernstudienanteil: 135 Zeitstunden • Selbststudium: 90 Zeitstunden • Aufgaben: 30 Zeitstunden • Online-Betreuung: 15 Zeitstunden **Summe: 150 Zeitstunden**

Lerninhalte:	In diesem Modul werden die folgenden Themengebiete behandelt: • Gutachtenerstellung • Aufbau und forensische Untersuchung der Windows-Registry • Windows Artefakte • Möglichkeiten und Techniken der Anti-Forensik • Sicherung und forensische Analyse des Hauptspeichers • Forensische Analyse von SQLite Datenbanken
Lernziele und Kompetenzen:	*Fachkompetenz:* Die Studierenden erlernen die Analyse und Auswertung der grundlegenden forensischen Artefakte innerhalb des Windows Betriebssystems und haben Kenntnisse in der Untersuchung anwendungsspezifischer Daten. Des Weiteren sind die Studierenden mit den weiterführenden Techniken der Hauptspeicherforensik vertraut. Sie kennen weiter gängige anti-forensische Maßnahmen und sind sich deren Auswirkungen auf den Untersuchungsprozess bewusst. Darüber hinaus werden den Studierenden Konzepte für die Erstellung gerichtsverwertbarer Gutachten vermittelt. Zudem erlernen die Studierenden den Aufbau und die forensische Analyse von gängigen SQLite Datenbanken. *Methodenkompetenz:* Die Studierenden beherrschen den Umgang mit den forensischen Tools und können wichtige Ergebnisse daraus eigenständig entnehmen. Sie sind mit weiterführenden Themen und Konzepten der IT-Forensik vertraut und können diese bei einer forensischen Untersuchung anwenden. Sie können weiter mit dem erlangten Wissen aus dem Modul sicher umgehen und können Aufgaben und Problemstellungen nachvollziehen und lösen. *Sozialkompetenz:* Die Studierenden erlernen aufgrund gemeinsamer forensischer Untersuchungen im Team zu arbeiten und können auftretende Probleme, Fragen und Aufgaben durch fachgebunde Diskussionen lösen. *Selbstkompetenz:* Die Studierenden erlangen die Fähigkeit eine forensische Untersuchung durchzuführen und sind in der Lage die Ergebnisse zu bewerten. Des Weiteren besitzen sie die Kompetenz sich an neue Gegebenheiten anzupassen und können so auf veränderte Hardware und Software reagieren.
Häufigkeit des Angebots:	ca. alle 2 Jahre
Medienformen:	Studienbriefe in schriftlicher und elektronischer Form, Onlinematerial in Lernplattform, Übungen und Projekt über Lernplattform, Online-Konferenzen, Chat und Forum, Präsenzveranstaltung mit Rechner und Beamer.

Literaturhinweise:	Als begleitende und vertiefende Literatur wird empfohlen: • Eigenes Skript • Michael Hale Ligh, et al.: The Art of Memory Forensics: Detecting Malware and Threats in Windows, Linux, and Mac Memory. John Wiley & Sons, 2014, ISBN 978-1118825099 • Harlan Carvey: Windows Registry Forensics: Advanced Digital Forensic Analysis of the Windows Registry. Elsevier, 2011, ISBN 978-0128032916 • Paul Sanderson, et al.: SQLite Forensics. Independently published, 2018, ISBN 978-1980293071 • Eoghan Casey (Hrsg.): Handbook of computer crime investigation. Forensic tools and technology. 6th Printing. Elsevier Academic Press, Amsterdam u. a. 2007, ISBN 978-0-12-163103-1. • Alexander Geschonneck: Computer-Forensik. Computerstraftaten erkennen, ermitteln, aufklären. 5. aktualisierte und erweiterte Auflage. dpunkt Verlag, Heidelberg 2011, ISBN 978-3-89864-774-8. Weitere Literatur wird in der Lehrveranstaltung bekannt gegeben.

Kryptographische Protokolle (Cryptographic Protocols)

Modulbezeichnung:	Kryptographische Protokolle (Cryptographic Protocols)
Verwendbarkeit:	Bachelorstudiengang Informatik/IT-Sicherheit (Wahlpflichtmodul)
Lehrveranstaltungen und Lehrformen:	Kryptographische Protokolle Selbstlernphasen, Übungen, Online-Phasen, Präsenzveranstaltung
Modulverantwortliche(r):	Prof. Dr. Jörg Schwenk
Lehrende:	Prof. Dr. Jörg Schwenk
Dauer:	1 Semester
Credits:	5 ECTS-Punkte
Studien- und Prüfungsleistungen:	Klausur: 120 min.
Berechnung der Modulnote:	100 % der schriftlichen Prüfungsnote
Notwendige Voraussetzungen für die Teilnahme:	
Empfohlene Voraussetzungen für die Teilnahme:	• Modul Kryptographie 1 • Modul Kryptographie 2
Unterrichts- und Prüfungssprache:	Deutsch und Englisch
Zuordnung des Moduls zu den Fachgebieten des Curriculums:	IT-Sicherheit Vertiefung
Einordnung ins Fachsemester:	Ab Studiensemester 6
Arbeitsaufwand bzw. Gesamtworkload:	Präsenzzeit: 15 Zeitstunden Fernstudienanteil: 135 Zeitstunden • Durcharbeiten der Studienbriefe: 80 Zeitstunden • Durcharbeiten des Online-Lernmaterials: 15 Zeitstunden • Wahrnehmen der Online Betreuung und Beratung: 10 Zeitstunden • Ausarbeiten von Aufgaben: 25 h • Individuelle Prüfungsvorbereitung der Studierenden: 5 Zeitstunden **Summe: 150 Zeitstunden**

Lerninhalte:	Dieses Modul bietet eine Einführung in das Gebiet der kryptographischen Protokolle, die den Einsatz bekannter und neuer Verfahren der Kryptographie in der Kommunikation zwischen mehreren Instanzen beschreiben. Hierbei wird sowohl Wert auf die Beschreibungen als auch auf die Sicherheit gelegt. Das Modul umfasst als Einführung allgemeine kryptographische Grundlagen, die Konzepte der beweisbaren Sicherheit und eine Einführung zu kryptographischen Protokollen. Den Schwerpunkt des Moduls werden Schlüsselaustausch Protokolle bilden. Den Abschluss des Moduls bildet eine detaillierte Beschreibung und formale Sicherheitsanalyse von TLS, dem wohl am weitesten verbreitete Authentifizierungs- und Schlüsseltausch Protokolls im Internet.
Lernziele und Kompetenzen:	*Fachkompetenz:* Die Studierenden verstehen die Besonderheit kryptographischer Protokolle, bei denen nicht mehr ein Algorithmus im Vordergrund steht, sondern die Interaktion verschiedener Einheiten. Die Studenten erkennen die praktische Relevanz der Kryptographie und begreifen die Schwierigkeit, kryptographische Protokolle - wie sie im Internet eingesetzt werden - formal auf ihre Sicherheit hin zu analysieren. Die Studenten kennen wichtige Sicherheitsziele und Sicherheitsmodelle, welche sie auf echte Protokolle anwenden können. *Methodenkompetenz:* Die Studierenden beherrschen den Umgang mit kryptographischer Fachliteratur und können ihr wichtige Ergebnisse eigenständig entnehmen. Weiterhin sind die Studierenden mit verschiedenen Beweistechniken und Sicherheitsmodellen vertraut, welche für formale Sicherheitsanalysen neuer Protokolle angewendet werden können. *Sozialkompetenz:* Die Studenten tauschen sich über Probleme beim Verstehen und Anwenden von neuen Modellen und Techniken aus und können wissenschaftlich zielorientiert diskutieren. *Selbstkompetenz:* Die Studenten erlangen die Fähigkeit, kryptographische Protokolle zu analysieren und eine wissenschaftlich begründete Einschätzung ihrer Sicherheit zu bilden. Darüber hinaus besitzen sie die Kompetenz, neue Protokolle aus der aktuellen Fachliteratur zu verstehen und ihre Sicherheit eigenständig zu evaluieren.
Häufigkeit des Angebots:	ca. alle 2 Jahre
Medienformen:	Studienbriefe in schriflicher und elektronischer Form, Onlinematerial in Lernplattform, Übungen über Lernplattform, Online-Konferenzen, Chat und Forum
Literaturhinweise:	• Jonathan Katz, Yehuda Lindell : Introduction to Modern Cryptography • Alan Turing: On computable numbers, with an application to the Entscheidungsproblem (1937) • Hopcroft, Motwani, Ullman: Introduction to Automata Theory, Languages and Computation Weitere Literatur wird in der Lehrveranstaltung bekannt gegeben.

Sicherheit mobiler Systeme (Mobile Security)

Modulbezeichnung:	Sicherheit mobiler Systeme (Mobile Security)
Verwendbarkeit:	Bachelorstudiengang Informatik/IT-Sicherheit (Wahlpflichtmodul)
Lehrveranstaltungen und Lehrformen:	Sicherheit mobiler Systeme Selbstlernphasen, Übungen, Online-Phasen, Präsenzveranstaltung
Modulverantwortliche(r):	Prof. Dr. Thorsten Holz
Lehrende:	Prof. Dr. Thorsten Holz
Dauer:	1 Semester
Credits:	5 ECTS-Punkte
Studien- und Prüfungsleistungen:	Klausur: 60 min.
Berechnung der Modulnote:	100 % der schriftlichen Prüfungsnote
Notwendige Voraussetzungen für die Teilnahme:	
Empfohlene Voraussetzungen für die Teilnahme:	• Programmierung • Kryptographie • Netzsicherheit 1-3
Unterrichts- und Prüfungssprache:	Deutsch und Englisch
Zuordnung des Moduls zu den Fachgebieten des Curriculums:	IT-Sicherheit Vertiefung
Einordnung ins Fachsemester:	Ab Studiensemester 6
Arbeitsaufwand bzw. Gesamtworkload:	Präsenzzeit: 15 Zeitstunden Fernstudienanteil: 135 Zeitstunden • Durcharbeiten der Studienbriefe: 80 Zeitstunden • Durcharbeiten des Online-Lernmaterials: 15 Zeitstunden • Wahrnehmen der Online Betreuung und Beratung: 10 Zeitstunden • Ausarbeiten von Aufgaben: 25 h • Individuelle Prüfungsvorbereitung der Studierenden: 5 Zeitstunden **Summe: 150 Zeitstunden**

Lerninhalte:	In diesem Modul erwerben die Teilnehmer Kenntnisse über Sicherheitsaspekte von verschiedenen mobilen Systemen, insbesondere zur Sicherheit von Smartphones. Im ersten Teil des Moduls liegt der Schwerpunkt auf der Beschreibung der wichtigsten Sicherheitsfunktionen von mobilen Systemen. Im zweiten Teil des Moduls wird die Sicherheit von Smartphones genauer beleuchtet und verschiedene Sicherheitsaspekte werden genauer betrachtet, der Fokus liegt dabei auf Apps für Smartphones. In der Vorlesung werden verschiedene Sicherheitsaspekte von mobilen Systemen vorgestellt. Anhand von konkreten Beispielen wird erläutert, wie verschiedene Arten von mobilen Systemen aufgebaut sind und welche Sicherheitsrisiken diese besitzen. Dies umfasst unter anderem die folgenden Themen: • Design von GSM und UMTS (Sicherheitsaspekte, Lokalisierungsverfahren, Verbindungsmanagement) • Sicherheit von Satellitentelefonen (GMR) • Sicherheitsaspekte von DECT • Design mobiler Betriebssysteme (Android und iOS) • Analyse von (mobilen) Apps
Lernziele und Kompetenzen:	*Fachkompetenz:* Die Studierenden erlernen die wichtigen Strukturen von Sicherheitsaspekten in mobilen Datennetzen, verstehen die darin verwendeten kryptographischen Verfahren sowie das Zusammenspiel verschiedener Protokolle. Die Studierenden können das Zusammenspiel der kryptographischen Verfahren in einem Protokoll auf erste Sicherheitslücken hin überprüfen und eine erste Einschätzung der Sicherheit des Protokolls liefern. Dazu werden auch konkrete Angriffe auf existierende Systeme vorgestellt, um ein tiefergehendes Verständnis zu erlangen. *Methodenkompetenz:* Die Studierenden beherrschen den Umgang mit (englischer) Fachliteratur und können ihr wichtige Informationen eigenständig entnehmen. Weiterhin sind die Studierenden mit verschiedenen Angriffs- und Analysetechniken vertraut, welche auf neue Systeme, Protokolle und Verfahren übertragen werden können. *Sozialkompetenz:* Die Studierenden tauschen sich über Probleme beim Erarbeiten und Anwenden von neuen Inhalten aus und können problemorientiert diskutieren. Die konstruktive Diskussion wird im Rahmen von Übungen erlernt. *Selbstkompetenz:* Die Studierenden erlangen die Fähigkeit, sich selbständig eine Meinung über die Sicherheit von verschiedenen mobilen Systemen zu bilden. Darüber hinaus besitzen sie die Kompetenz, neue Angriffe aus der aktuellen Fachliteratur zu verstehen und ihre Bedeutungen zu evaluieren. Die Studierenden entwickeln ein „gesundes Misstrauen“ gegenüber vorgegebenen Sicherheitskonzepten.
Häufigkeit des Angebots:	ca. alle 2 Jahre

Medienformen:	Studienbriefe in schriflicher und elektronischer Form, Online-material in Lernplattform, Übungen über Lernplattform, Online-Konferenzen, Chat und Forum
Literaturhinweise:	• Hannes Federrath: Sicherheit mobiler Kommunikation: Schutz in GSM-Netzen, Mobilitätsmanagement und mehr-seitige Sicherheit, Vieweg, 1999 • Noureddine Boudriga: Security of Mobile Communications, Auerbach Publications, 2009 • Miller et al.: iOS Hacker's Handbook, Wiley, 2012 Weitere Literatur wird in der Lehrveranstaltung bekannt gegeben.

Spam (Spam)

Modulbezeichnung:	Spam (Spam)
Verwendbarkeit:	Bachelorstudiengang Informatik/IT-Sicherheit (Wahlpflichtmodul)
Lehrveranstaltungen und Lehrformen:	Spam Selbstlernphasen, Übungen, Online-Phasen, Präsenzveranstaltung
Modulverantwortliche(r):	Dr. Christopher Wolf
Lehrende:	Prof. Dr. Jörg Schwenk
Dauer:	1 Semester
Credits:	5 ECTS-Punkte
Studien- und Prüfungsleistungen:	Klausur: 60 min.
Berechnung der Modulnote:	100 % der schriftlichen Prüfungsnote
Notwendige Voraussetzungen für die Teilnahme:	
Empfohlene Voraussetzungen für die Teilnahme:	
Unterrichts- und Prüfungssprache:	Deutsch und Englisch
Zuordnung des Moduls zu den Fachgebieten des Curriculums:	IT-Sicherheit Vertiefung
Einordnung ins Fachsemester:	Ab Studiensemester 6
Arbeitsaufwand bzw. Gesamtworkload:	Präsenzzeit: 15 Zeitstunden Fernstudienanteil: 135 Zeitstunden • Durcharbeiten der Studienbriefe: 80 Zeitstunden • Durcharbeiten des Online-Lernmaterials: 15 Zeitstunden • Wahrnehmen der Online Betreuung und Beratung: 10 Zeitstunden • Ausarbeiten von Aufgaben: 25 h • Individuelle Prüfungsvorbereitung der Studierenden: 5 Zeitstunden **Summe: 150 Zeitstunden**

Lerninhalte:	E-Mails sind immer noch das wichtigste Kommunikationsmedium in der Arbeitswelt. Vor diesem Hintergrund stellt das Auftreten von Spam nicht nur ein Ärgernis dar, sondern verursacht auch einen enormen wirtschaftlichen Schaden. Um zu verstehen, wie Spam entsteht, wird ein tieferer Einblick in das SMTP-Protokoll und den Protokollfluss zwischen Sender und Empfänger dargestellt und die Verlässlichkeit der verschiedenen im E-Mail-Quellcode enthaltenen Daten und deren Manipulationsmöglichkeiten in Form einer Analyse der Header-Felder erläutert. Es werden verschiedene Formen der Anti-Spam-Maßnahmen präsentiert. Darunter fallen einfache Methoden wie Black- und Whitelists sowie Machine-Learning-Ansätze wie bspw. Bayessche Filter. Als weitere Anti-Spam-Techniken werden SPF, DKIM und DMARC sowie die Abhängigkeiten dieser Verfahren untereinander dargestellt. Eine Darstellung der EFAIL-Angriffe auf Vertraulichkeit und Integrität der Nachrichten wird in Verbindung gesetzt zu möglichen Gegenmaßnahmen, die auf Erfahrungen mit DKIM aufbauen.
Lernziele und Kompetenzen:	*Fachkompetenz:* Die Studierenden erwerben grundlegendes Wissen im Bereich der Email-Kommunikation. Sie sind in der Lage Spam- und Anti-Spam Techniken zu erläutern und kennen rechtliche Aspekte von Spam. *Methodenkompetenz:* Die Studierenden beherrschen den Umgang mit Fachliteratur und können ihr wichtige Informationen eigenständig entnehmen. Sie verstehen die Wirksamkeit von Spam-Filtern und können diese konfigurieren. *Sozialkompetenz:* Die Studenten tauschen sich über Probleme beim Erarbeiten und Anwenden von neuen Inhalten aus und können problemorientiert diskutieren. *Selbstkompetenz:* Die Studenten erlangen die Fähigkeit Techniken im Spam-Umfeld aktueller Fachliteratur zu entnehmen und ihre Bedeutungen zu evaluieren.
Häufigkeit des Angebots:	ca. alle 2 Jahre
Medienformen:	Studienbriefe in schriflicher und elektronischer Form, Onlinematerial in Lernplattform, Übungen über Lernplattform, Online-Konferenzen, Chat und Forum
Literaturhinweise:	Literatur wird in der Lehrveranstaltung bekannt gegeben.

Netzwerkforensik (Network Forensics)

Modulbezeichnung:	Netzwerkforensik (Network Forensics)
Verwendbarkeit:	Bachelorstudiengang Informatik/IT-Sicherheit (Wahlpflichtmodul)
Lehrveranstaltungen und Lehrformen:	Netzwerkforensik Selbstlernphasen, Übungen, Online-Phasen, Präsenzveranstaltung
Modulverantwortliche(r):	Prof. Dr. Jessica Steinberger
Lehrende:	Prof. Dr. Jessica Steinberger
Dauer:	1 Semester
Credits:	5 ECTS-Punkte
Studien- und Prüfungsleistungen:	Klausur: 60 Min.
Berechnung der Modulnote:	100% der schriftlichen Prüfungsnote
Notwendige Voraussetzungen für die Teilnahme:	
Empfohlene Voraussetzungen für die Teilnahme:	• Netzsicherheit 1 • Netzsicherheit 2
Unterrichts- und Prüfungssprache:	Deutsch
Zuordnung des Moduls zu den Fachgebieten des Curriculums:	IT-Sicherheit Vertiefung
Einordnung ins Fachsemester:	Ab Studiensemester 6
Arbeitsaufwand bzw. Gesamtworkload:	Präsenzstudium: 15 Zeitstunden Fernstudienanteil: 135 Zeitstunden • Selbststudium: 90 Zeitstunden • Aufgaben: 30 Zeitstunden • Online-Betreuung: 15 Zeitstunden **Summe: 150 Zeitstunden**

Lerninhalte:	In diesem Modul werden die folgenden Themengebiete behandelt: • Vorgehensmodell des "Network Security Monitoring" • Hashfunktionen in der Forensik • Grundlagen der Netzwerkprotokolle und deren Angriffsvektoren • Arten von Netzwerkangriffen und deren Auswirkungen im Netzwerkdatenverkehr • Einblicke in die Datengewinnung aus verschiedenen Netzwerkkomponenten • IT-forensische Analyse von Netzwerkdatenverkehr • Umgang mit Werkzeugen der Netzwerkforensik • Visualisierung von Netzwerkdaten • Gutachtenerstellung

Lernziele und Kompetenzen:	*Fachkompetenz:* Die Studierenden kennen die Grundlagen der Netzwerkprotokolle und die verschiedenen Datenquellen, welche der IT-forensischen Analyse als Grundlage dienen können. Hierauf aufbauend lernen die Studierenden die mögliche Auswirkungen von Netzwerkangriffen unter Nutzung einzelner Netzwerkprotokolle kennen und bewerten. Die Studierenden sind in der Lage die Datengewinnung aus verschiedenen Netzwerkkomponenten vorzunehmen und können sicher mit den Werkzeugen der Netzwerkforensik umgehen. Die Studierenden lernen verschiedene Methoden kennen, um netzbasierte Daten zu visualisieren. Weiterhin sind die Studierenden in der Lage eine forensische Analyse von Netzwerkdaten durchzuführen und können das Ergebnis gerichtsverwertbar dokumentieren. *Methodenkompetenz:* Die Studierenden kennen die Grundlagen und benötigten Werkzeuge für die Durchführung einer netzwerkforensischen Analyse. Sie wissen welche Datenquellen bei einer forensischen Analyse verwendet werden und wie die Netzwerkdaten gesammelt werden können. Mit diesem Wissen sind sie in der Lage aktiv umzugehen und können im Bedarfsfall ein Gutachten, welches dem Prinzip eines forensischen Vorgehensmodell folgt, selbstständig ausarbeiten. Zusätzliche Informationen können sie selbstständig aus der Literatur erarbeiten. Sie können mit dem durch das Modul erlangten Wissen sicher umgehen und können Aufgaben und Problemstellungen nachvollziehen und lösen. *Sozialkompetenz:* Die Studierenden tauschen sich durch Gruppenarbeit an dem Präsenzwochenende aus und können auftretende Probleme, Fragen und Aufgaben durch fachgebunden Diskussion lösen. *Selbstkompetenz:* Die Studierenden erlangen die Fähigkeit netzwerkforensische Analysen anhand des Prinzips eines forensischen Vorgehensmodells durchzuführen und sind in der Lage die Ergebnisse gerichtsverwertbar zu verschriftlichen und zu präsentieren. Des Weiteren besitzen sie die Kompetenz sich an neue Gegebenheiten anzupassen und können so auf Neuerungen in dem Themengebiet reagieren.
Häufigkeit des Angebots:	ca. alle 2 Jahre
Medienformen:	Studienbriefe in schriftlicher und elektronischer Form, Onlinematerial in Lernplattform, Übungen und Projekt über Lernplattform, Online-Konferenzen, Chat und Forum, Präsenzveranstaltung mit Rechner und Beamer.

Literaturhinweise:	Als begleitende Literatur wird empfohlen: • Eigenes Skript Als vertiefende Literatur wird empfohlen: • Field, Andy ; Miles, Jeremy ; Field, Zoë: Discovering Statistics Using R. London: SAGE, 2012, ISBN 978-1-446-25846-0. • Messier, Ric: Network Forensics. New York: John Wiley & Sons, 2017. ISBN 978-1-119-32828-5. • Tan, Pang-Ning ; Steinbach, Michael ; Karpatne, Anuj ; Kumar, Vipin: Introduction to Data Mining. München: Pearson, 2019. ISBN 978-0-133-12890-1. • Eckert, Claudia: IT-Sicherheit : Konzepte - Verfahren - Protokolle. Berlin: Walter de Gruyter GmbH & Co KG, 2018. ISBN 978-3-110-56390-0. • Theodoridis, Sergios ; Koutroumbas, Konstantinos: Pattern Recognition. Amsterdam: Elsevier, 2006. ISBN 978-0-080-51361-4. • van Steen, Maarten; Tanenbaum, Andrew S.: Distributed Systems. Ort: CreateSpace Independent Publishing Platform, 2017. -ISBN 978-1-543-05738-6. • Collins, Michael: Network Security Through Data Analysis : From Data to Action. Sebastopol: Ö'Reilly Media, Inc.", 2017. -ISBN 978-1-491-96281-7. • Forshaw, James: Attacking Network Protocols : A Hacker's Guide to Capture, Analysis, and Exploitation. München: No Starch Press, 2018. ISBN 978-1-593-27844-1.

Maschinelles Lernen und Sicherheit (Machine Learning and Security)

Modulbezeichnung:	Maschinelles Lernen und Sicherheit (Machine Learning and Security)
Verwendbarkeit:	Bachelorstudiengang Informatik/IT-Sicherheit (Wahlpflichtmodul)
Lehrveranstaltungen und Lehrformen:	Maschinelles Lernen und Sicherheit Selbstlernphasen, Übungen, Online-Phasen, Präsenzveranstaltung
Modulverantwortliche(r):	PD Dr. Christian Riess
Lehrende:	PD Dr. Christian Riess
Dauer:	1 Semester
Credits:	5 ECTS-Punkte
Studien- und Prüfungsleistungen:	Klausur: 60 Min.
Berechnung der Modulnote:	100% der schriftlichen Prüfungsnote
Notwendige Voraussetzungen für die Teilnahme:	
Empfohlene Voraussetzungen für die Teilnahme:	• Englischkenntnisse • Programmierkenntnisse in Python
Unterrichts- und Prüfungssprache:	Deutsch und Englisch
Zuordnung des Moduls zu den Fachgebieten des Curriculums:	IT-Sicherheit Vertiefung
Einordnung ins Fachsemester:	Ab Studiensemester 6
Arbeitsaufwand bzw. Gesamtworkload:	Präsenzstudium: 15 Zeitstunden Fernstudienanteil: 135 Zeitstunden • Selbststudium: 90 Zeitstunden • Aufgaben: 30 Zeitstunden • Online-Betreuung: 15 Zeitstunden **Summe: 150 Zeitstunden**

Lerninhalte:	Das Modul behandelt grundlegende Algorithmen des maschinelles Lernens. In den Übungen und in der Präsenzveranstaltung werden diese Methoden auf Anwendungen in der IT-Sicherheit angewendet. Die Einführung in das maschinelle Lernen folgt kapitelweise dem Lehrbuch von Zhi-Hua Zhou, "Machine Learning", wir behandeln hier Kapitel 1–11. Bitte beachten Sie, dass das Lehrbuch nicht auf deutsch, sondern nur auf englisch und chinesisch verfügbar ist. Die in dem Modul behandelten Kapitel beinhalten die Themen • Grundlegende Terminologie • Modellauswahl und Evaluation • Lineare Modelle • Entscheidungsbäume • Neuronale Netze • Support Vector-Maschinen • Bayessche Klassifikation • Klassifikator-Ensembles • Clustering • Dimensionsreduktion • Merkmalsreduktion In den Übungen und in der Präsenzveranstaltung werden von den Teilnehmern anwendungsspezifische Herausforderungen in der IT-Sicherheit untersucht. Für ausgewählte Fragestellungen werden auf Standard-Datensätzen prototypisch maschinelle Lernverfahren implementiert und evaluiert.
Lernziele und Kompetenzen:	*Fachkompetenz:* Die Studierenden kennen grundlegende Algorithmen des maschinellen Lernens. Sie können diese Methoden für Anwendungen in der Sicherheit einsetzen. Die Studierenden kennen verschiedene Metriken und Verfahren zur empirischen Evaluation maschineller Lernverfahren. *Methodenkompetenz:* Die Studierenden können Verfahren des maschinellen Lernens für Anwendungen in der Sicherheit programmieren und die Leistungsfähigkeit der Verfahren evaluieren. Die Absolventen verfügen über Fähigkeiten, praktische Anwendungen des maschinellen Lernens zu realisieren. *Sozialkompetenz:* Aufgrund der Teamarbeit, unter anderem an den Präsenzwochenenden, erweitern die Studierenden ihre Teamfähigkeit und Sozialkompetenz. *Selbstkompetenz:* Durch das eigenverantwortliche Entwickeln von Programmen erweitern die Studierenden ihr selbstständiges Handeln. Durch die Präsentation ihrer Ergebnisse wird die Selbstsicherheit der Studierenden gestärkt.
Häufigkeit des Angebots:	ca. alle 2 Jahre

Medienformen:	Lehrbuch, kurzes Einführungsvideo pro Kapitel, Übungen über Lernplattform, Online-Konferenzen, Chat und Forum, Präsenzveranstaltung mit Rechner und Beamer
Literaturhinweise:	• Lehrbuch zum Studium: Zhi-Hua Zhou, "Machine Learning", übersetzt von Shaowu Liu, Springer 2021. Online verfügbar über OPAC. • Weitere Literatur wird bedarfsweise in der Lehrveranstaltung bekanntgegeben

Incident Management

Modulbezeichnung:	Incident Management
Verwendbarkeit:	Bachelorstudiengang Informatik/IT-Sicherheit (Wahlpflichtmodul)
Lehrveranstaltungen und Lehrformen:	Incident Management Selbstlernphasen, Übungen, Online-Phasen, Präsenzveranstaltung
Modulverantwortliche(r):	Prof. Dr. Daniel Hammer
Lehrende:	Prof. Dr. Daniel Hammer
Dauer:	1 Semester
Credits:	5 ECTS-Punkte
Studien- und Prüfungsleistungen:	Klausur: 60 min.
Berechnung der Modulnote:	100% der schriftlichen Prüfungsnote
Notwendige Voraussetzungen für die Teilnahme:	
Empfohlene Voraussetzungen für die Teilnahme:	
Unterrichts- und Prüfungssprache:	Deutsch
Zuordnung des Moduls zu den Fachgebieten des Curriculums:	Informatik Vertiefung
Einordnung ins Fachsemester:	Ab Studiensemester 6
Arbeitsaufwand bzw. Gesamtworkload:	Präsenzstudium: 15 Zeitstunden Fernstudienanteil: 135 Zeitstunden • Selbststudium: 105 Zeitstunden • Aufgaben: 20 Zeitstunden • Online-Betreuung: 10 Zeitstunden Summe: 150 Zeitstunden
Lerninhalte:	Im Modul Incident Management wird auf folgende Themengebiete eingegangen: • Grundwissen des Incident Management • IT-Service Management (ITSM) • IT-Security Management • Risikomanagement

Lernziele und Kompetenzen:	*Fachkompetenz:* Die Studierenden erlangen mit diesem Modul das Basiswissen über das Incident Management und das Risikomanagement. Sie können die Schritte des Incident Management Prozesses nachvollziehen und sind imstande grundlegende Begriffe des Incident Management zu erklären und einzuordnen und können zwischen den spezifischen Rollen im Incident Management differenzieren. Ferner sind die Studierenden in der Lage einen Risikomanagementprozess mit seinen einzelnen Phasen zu erklären und kennen die bekannten Methoden und Werkzeuge des Risikomanagements. *Methodenkompetenz:* Die Studierenden sind in der Lage den Incident Management Prozess selber anzuwenden und eine Risikoberechnung aus der Wahrscheinlichkeit und der Schadenshöhe durchzuführen. Ferner können die Studierenden die einzelnen Schritte des Risikomanagementprozesses nachvollziehen und anwenden. *Sozialkompetenz:* Aufgrund der Teamarbeit, unter anderem in dem Präsenzwochenende, erweitern die Studierenden die Fähigkeit der Teamfähigkeit und Sozialkompetenz. *Selbstkompetenz:* Die Lernenden erlangen die Fähigkeit zur Bildung einer Meinung über IT-Sicherheit. Darüber hinaus erlangen sie die Fähigkeit, in komplexen Situationen zu handeln und eine Lösung für schwierige Probleme zu finden.
Häufigkeit des Angebots:	alle 2 Jahre
Medienformen:	Studienbriefe in schriftlicher und elektronischer Form, Onlinematerial in Lernplattform, Übungen und Projekt über Lernplattform, Online-Konferenzen, Chat und Forum, Präsenzveranstaltung mit Rechner und Beamer.
Literaturhinweise:	• IT-Sicherheit: Konzepte - Verfahren - Protokolle, Claudia Eckert, 2006 • Moderne Betriebssysteme, Andrew S. Tanenbaum, 2003 • Betriebssysteme - Prinzipien und Umsetzung, William Stallings, 2005 • Malware, Eugene Kaspersky, 2008 • Computer Security, Dieter Gollmann, 2010 Weitere Literatur wird in der Lehrveranstaltung bekannt gegeben.

Ethisches Hacking (Ethical Hacking)

Modulbezeichnung:	Ethisches Hacking (Ethical Hacking)
Verwendbarkeit:	Bachelorstudiengang Informatik/IT-Sicherheit (Wahlpflichtmodul)
Lehrveranstaltungen und Lehrformen:	Ethisches Hacking Selbstlernphasen, Übungen, Online-Phasen, Präsenzveranstaltung
Modulverantwortliche(r):	Prof. Dr. rer. nat. Daniel Hammer
Lehrende:	Prof. Dr. rer. nat. Daniel Hammer
Dauer:	1 Semester
Credits:	5 ECTS-Punkte
Studien- und Prüfungsleistungen:	Klausur: 60 min.
Berechnung der Modulnote:	100% der schriftlichen Prüfungsnote
Notwendige Voraussetzungen für die Teilnahme:	
Empfohlene Voraussetzungen für die Teilnahme:	Rechnerstrukturen, Systemsicherheit 1+2, Netzsicherheit 1
Unterrichts- und Prüfungssprache:	Deutsch
Zuordnung des Moduls zu den Fachgebieten des Curriculums:	IT-Sicherheit Vertiefung
Einordnung ins Fachsemester:	Ab Studiensemester 6
Arbeitsaufwand bzw. Gesamtworkload:	Präsenzstudium: 15 Zeitstunden Fernstudienanteil: 135 Zeitstunden • Selbststudium: 105 Zeitstunden • Aufgaben: 20 Zeitstunden • Online-Betreuung: 10 Zeitstunden Summe: 150 Zeitstunden

Lerninhalte:	Im Modul Ethical Hacking wird auf folgende Themengebiete eingegangen: • Definition und Anwendung der Begriffe Angriff, Hacking, Hacker, Ethisches Hacking und Cyberkriminalität • Taktische Prinzipien und das Dilemma des Verteidigers • Tätermotivation und Zielauswahl • Die Anatomie des möglichen Opfers • Reconnaissance und automatisierte Informationsbeschaffung • DNS-Enumeration, DNS-Cache Snooping • Fingerprinting und Schwachstellenermittlung • Google als Hacking Tool • Social Engineering • Schwachstellenermittlung an einem Zielsystem • Ausführung eines Angriffs und Kompromittierung des Systems • Spurenbeseitigung • Technische und nicht-technische Methoden des ethischen Hackings • Techniken, Tools und Anwendungsbeispiele

Lernziele und Kompetenzen:	*Fachkompetenz:* Die Studierenden kennen die fundamentalen Begriffe und Prinzipien, welche die Gefahrensituation eines Computersystems beschreiben. Sie sind in der Lage Interessengruppen für die Angriffe auf IT-Infrastrukturen zu identifizieren und deren zentrale Handlungsprinzipien sowie Strategien darzustellen. Darüber hinaus können sie die grundlegenden Positionen und ethische Handlungslinien der Verteidiger charakterisieren, welche deren Basis der digitalen Selbstverteidigung bilden. Die Studierenden sind in der Lage, die Phasen eines Hacking-Angriffs zu skizzieren und deren strukturelle Chronologie zu beschreiben. Sie können die Vorgehensweise der Hacker in jeder einzelnen Phase in ihrer Methode und den verwendeten Technologien, Protokollen und Tools beschreiben. Darüber hinaus sind die Studierenden befähigt, verschiedene Angriffsformen zu charakterisieren und zu unterscheiden, sowie passende Verteidigungsstrategien zu benennen und geeignete Mittel und Wege aufzuzeigen. Sie verstehen die Wege der Informationsbeschaffung aus öffentlichen Quellen oder des Social Engineerings und den dabei verfolgten Angreiferprinzipien der Tarnung und Täuschung. *Methodenkompetenz:* Die Studierenden sind in der Lage den Gefährdungsgrad einer IT-Infrastruktur einzuschätzen und daraus ableitend die Voraussetzung für einen erfolgreichen Hacking-Angriff zu benennen und zu charakterisieren. Aus der bei Hacking-Angriffen verfolgten Chronologie und Methodik sind die Studierenden außerdem in der Lage Mittel und Strategien zur Früherkennung der jeweiligen Bedrohungsszenarien geeignete Schutzmaßnahmen zu skizzieren und anzuwenden. Dafür sind sie in der Lage, die dazu nötigen Tools auszuwählen und in einem Anwendungsszenario zielführend einzusetzen. Aus der Kenntnis der Durchführung eines erfolgreichen Angriffs auf ein computergesteuertes Informationssystem sind die Studierenden in der Lage einen solchen Angriff zu planen und im Zuge eines Sicherheitstests selbst auszuführen und dabei gleichzeitig ethische und rechtliche Leitlinien zu befolgen. *Sozialkompetenz:* Aufgrund der Teamarbeit, unter anderem an dem Präsenzwochenende, sind die Studierenden fähig, Lösungswege in der Gruppe zu entwickeln und Aufgaben kooperativ zu lösen. *Selbstkompetenz:* Die Studierenden haben sich eine Meinung über IT-Sicherheit gebildet. Sie sind fähig, Ihre Lernzeit zu strukturieren und Modulinhalte über unterschiedliche Lernphasen verteilt zu bearbeiten.
Häufigkeit des Angebots:	ca. alle 2 Jahre
Medienformen:	Studienbriefe in schriftlicher und elektronischer Form, Onlinematerial in Lernplattform, Übungen und Projekt über Lernplattform, Online-Konferenzen, Chat und Forum, Präsenzveranstaltung mit Rechner und Beamer.

Literaturhinweise:	• Michael T. Simpson, Kent Backman und James E. Corley. Ethical Hacking and Network Defense, Course Technology, 2013 • Sandro Gaycken. Cyberwar: Das Internet als Kriegsschauplatz. Open Source Press; 1. Auflage, 2010 • Johnny Long. Google Hacking for Penetration Testers, Syngress, 2008 Weitere Literatur wird in der Lehrveranstaltung bekannt gegeben.

Anonymität im Netz (Anonymity on the Internet)

Modulbezeichnung:	Anonymität im Netz (Anonymity on the Internet)
Verwendbarkeit:	Bachelorstudiengang Informatik/IT-Sicherheit (Wahlpflichtmodul)
Lehrveranstaltungen und Lehrformen:	Anonymität im Netz Selbstlernphasen, Übungen, Online-Phasen, Präsenzveranstaltung
Modulverantwortliche(r):	Prof. Dr. Daniel Hammer
Lehrende:	Prof. Dr. Daniel Hammer
Dauer:	1 Semester
Credits:	5 ECTS-Punkte
Studien- und Prüfungsleistungen:	Klausur: 60 min.
Berechnung der Modulnote:	100% der schriftlichen Prüfungsnote
Notwendige Voraussetzungen für die Teilnahme:	
Empfohlene Voraussetzungen für die Teilnahme:	Netzsicherheit 1, Kryptographie 1
Unterrichts- und Prüfungssprache:	Deutsch
Zuordnung des Moduls zu den Fachgebieten des Curriculums:	IT-Sicherheit Vertiefung
Einordnung ins Fachsemester:	Ab Studiensemester 6
Arbeitsaufwand bzw. Gesamtworkload:	Präsenzstudium: 15 Zeitstunden Fernstudienanteil: 135 Zeitstunden • Selbststudium: 105 Zeitstunden • Aufgaben: 20 Zeitstunden • Online-Betreuung: 10 Zeitstunden Summe: 150 Zeitstunden

Lerninhalte:	Im Modul Anonymität im Netz wird auf folgende Themengebiete eingegangen: • Kommunikation in Netzwerken bei Anwesenheit innerer und äußerer Angreifer • Definition und Anwendung der Begriffe Anonymität, Unverkettbarkeit, Unbeobachtbarkeit • Konzepte von Unterscheidbarkeit, Verkettbarkeit und Pseudonymität • Privacy mit unterschiedlichem Schutzniveau von Kommunikationsdaten • Rechtliche Rahmenbedingungen von Anonymität und Datenschutz im Internet • Anonymisierungstechnologien, Overlay-Netzwerke • Anonymisierer, Digitales Mixen, Java Anon Proxy (JAP)/JonDo • TOR-Netzwerke und Hidden Services • Bedrohungsmodelle, Mechanismen zum Schutz privater Netzwerk-Kommunikation • Selbstschutz in sozialen Netzwerken, Deep Web und Kriminalität • Remailer-Systeme und OTR-Technologien • Techniken zur Identifizierung von Nutzern im Web • Auswirkungen der anonymisierten Internetnutzung

Lernziele und Kompetenzen:	*Fachkompetenz:* Die Studierenden kennen die grundlegenden Begriffe und Konzepte der Anonymität und des Schutzes der Privatsphäre in Computer-Netzwerken. Sie können darüber hinaus Anonymität von schwächeren Formen der Sicherung vertraulicher bzw. identitätsbezogener Informationen unterscheiden. Die Studierenden sind in der Lage, unterschiedliche Angriffe auf anonyme Netzwerk-Kommunikation und den Austausch vertraulicher Daten zu beschreiben und Abwehrmechanismen zu erläutern. Sie haben Grundkenntnisse über Anonymisierungstechnologien wie Anonymisierer, Digitale Mixer, Remailer-Systeme und TOR-Netzwerke und können deren Funktionsweise erläutern sowie OTR-Technologien beschreiben. Zudem können die Studierenden mittels ihrer Kenntnisse über die Sicherheitsaspekte vernetzter Umgebungen, Mechanismen des digitalen Mixens und die Funktionsweise von Overlay-Netzwerken zu den jeweiligen Bedrohungsszenarien passende Schutzmaßnahmen und Tools zielführend einsetzen. *Methodenkompetenz:* Die Studierenden können Voraussetzungen und Umstände erläutern, die zum Erreichen von Anonymität in einem Netzwerk kommunizierender Teilnehmer erforderlich sind. Sie sind außerdem in der Lage ausgehend von unterschiedlichen Zielen einer Kommunikation über Computer-Netzwerke und verschiedenen Ebenen des Schutzbedarfs der übertragenen Informationen, nötige Protokolle und die passende Technologie auszuwählen, die zum Erreichen dieser Zwecke notwendig ist. Sie sind in der Lage Bedrohungsszenarien zu erkennen und zu analysieren, sowie notwendige Schutzmaßnahmen zu skizzieren und anzuwenden. Die Studierenden sind imstande das Für und Wider von Anonymität bei unterschiedlichen Standpunkten und Rechtsauffassungen von Freiheit und Verbrechensbekämpfung zu diskutieren und Lösungsansätze zu erörtern. *Sozialkompetenz:* Aufgrund der Teamarbeit, unter anderem an dem Präsenzwochenende, sind die Studierenden fähig, Lösungswege in der Gruppe zu entwickeln und Aufgaben kooperativ zu lösen. *Selbstkompetenz:* Die Studierenden haben sich eine Meinung über IT-Sicherheit gebildet. Sie sind fähig, Ihre Lernzeit zu strukturieren und Modulinhalte über unterschiedliche Lernphasen verteilt zu bearbeiten.
Häufigkeit des Angebots:	ca. alle 2 Jahre
Medienformen:	Studienbriefe in schriftlicher und elektronischer Form, Onlinematerial in Lernplattform, Übungen und Projekt über Lernplattform, Online-Konferenzen, Chat und Forum, Präsenzveranstaltung mit Rechner und Beamer.

Literaturhinweise:	• Helmut Bäumler, Albert von Mutius (Hrsg.): Anonymität im Internet: Grundlagen, Methoden und Tools zur Realisierung eines Grundrechts, Vieweg 2003 • Phillip Brunst: Anonymität im Internet - rechtliche und tatsächliche Rahmenbedingungen, Duncker & Humblot, Berlin 2009 • Eric Siegel. Predictive Analytics: The Power to Predict Who Will Click, Buy, Lie, or Die, John Wiley & Sons, 2013 Weitere Literatur wird in der Lehrveranstaltung bekannt gegeben.

Open Source Intelligence & Spionageprävention (Open Source Intelligence & Espionage Prevention)

Modulbezeichnung:	Open Source Intelligence & Spionageprävention (Open Source Intelligence & Espionage Prevention)
Verwendbarkeit:	Bachelorstudiengang Informatik/IT-Sicherheit (Wahlpflichtmodul)
Lehrveranstaltungen und Lehrformen:	Open Source Intelligence & Spionageprävention Selbstlernphasen, Übungen, Online-Phasen, Präsenzveranstaltung
Modulverantwortliche(r):	Prof. Dr. Daniel Hammer
Lehrende:	Prof. Dr. Daniel Hammer
Dauer:	1 Semester
Credits:	5 ECTS
Studien- und Prüfungsleistungen:	Klausur: 60 min.
Berechnung der Modulnote:	100% der schriftlichen Prüfungsnote
Notwendige Voraussetzungen für die Teilnahme:	
Empfohlene Voraussetzungen für die Teilnahme:	Systemsicherheit 1+2
Unterrichts- und Prüfungssprache:	Deutsch
Zuordnung des Moduls zu den Fachgebieten des Curriculums:	IT-Sicherheit Vertiefung
Einordnung ins Fachsemester:	Ab Studiensemester 6
Arbeitsaufwand bzw. Gesamtworkload:	Präsenzstudium: 15 Zeitstunden Fernstudienanteil: 135 Zeitstunden • Selbststudium: 105 Zeitstunden • Aufgaben: 20 Zeitstunden • Online-Betreuung: 10 Zeitstunden Summe: 150 Zeitstunden

Lerninhalte:	Im Modul Open Source Intelligence & Spionageprävention wird auf folgende Themengebiete eingegangen: • Nachrichtensysteme und Beschaffung von Informationen • Vorstellung und Erläuterung der Grundprämissen und Mittel der Open Source Intelligence • Methoden und Techniken des Aufbereitens und Analysierens von Online-Informationen • Sicherheitsmechanismen und -modelle • Tools und Techniken • Angriffsszenarien • Diverse Referenzen wie Fachliteratur und wissenschaftliche Paper werden am Ende des Moduls gegeben
Lernziele und Kompetenzen:	*Fachkompetenz:* Die Studierenden erlangen das Basiswissen über Methoden und Techniken des Suchens, Aufbereitens und Analysierens öffentlich zugänglichen Informationen zu nachrichtendienstlichen und Spionage- bzw. Cyberangriffszwecken. Ferner erwerben sie Kenntnisse über relevante Sicherheitsmechanismen und -modelle und können zwischen unterschiedlichen Angriffsszenarien differenzieren. Außerdem eignen sie sich das Wissen über die entsprechenden Abwehrmechanismen an. *Methodenkompetenz:* Die Studierenden können zwischen den unterschiedlichen Arten von Open Source Intelligence und Spionage differenzieren und können entsprechende Schutzmaßnahmen entwickeln. Sie kennen Tools und Techniken kennen, wie Open Source und (nicht nur Wirtschafts-)Spionageinformationen gewonnen, aufbereitet und analysiert werden. Außerdem wissen die Studierenden wie Programmier- und Konfigurationsfehler ausgenutzt werden können, um den Abfluss kritischer Informationen zu ermöglichen und wie und welche Abwehrmechanismen sie dagegen einsetzen können. *Sozialkompetenz:* Aufgrund der Teamarbeit, unter anderem in dem Präsenzwochenende, erweitern die Studierenden die Fähigkeit der Teamfähigkeit und Sozialkompetenz. *Selbstkompetenz:* Die Lernenden erlangen die Fähigkeit zur Bildung einer Meinung über IT-Sicherheit. Darüber hinaus erlangen sie die Fähigkeit, in komplexen Situationen zu handeln und eine Lösung für schwierige Probleme zu finden.
Häufigkeit des Angebots:	ca. alle 2 Jahre
Medienformen:	Studienbriefe in schriftlicher und elektronischer Form, Onlinematerial in Lernplattform, Übungen und Projekt über Lernplattform, Online-Konferenzen, Chat und Forum, Präsenzveranstaltung mit Rechner und Beamer.

Literaturhinweise:	• Open Source Intelligence Techniques, Michael Bazzell, 2018 Weitere Literatur wird in der Lehrveranstaltung bekannt gegeben.

Mobilfunkforensik (Smartphone Forensics)

Modulbezeichnung:	Mobilfunkforensik (Smartphone Forensics)
Verwendbarkeit:	Bachelorstudiengang Informatik/IT-Sicherheit (Wahlpflichtmodul)
Lehrveranstaltungen und Lehrformen:	Mobilfunkforensik Selbstlernphasen, Übungen, Online-Phasen, Präsenzveranstaltung
Modulverantwortliche(r):	Dr. Michael Spreitzenbarth
Lehrende:	Dr. Michael Spreitzenbarth
Dauer:	1 Semester
Credits:	5 ECTS-Punkte
Studien- und Prüfungsleistungen:	Hausarbeit ca. 20 Seiten
Berechnung der Modulnote:	100% der Hausarbeitsnote
Notwendige Voraussetzungen für die Teilnahme:	
Empfohlene Voraussetzungen für die Teilnahme:	• Programmierkenntnisse in Python und Java • Linux-Kenntnisse • Kenntnisse forensische Grundsätze (z.B. Modul „Einführung in die digitale Forensik“)
Unterrichts- und Prüfungssprache:	Deutsch
Zuordnung des Moduls zu den Fachgebieten des Curriculums:	IT-Sicherheit Vertiefung
Einordnung ins Fachsemester:	Ab Studiensemester 6
Arbeitsaufwand bzw. Gesamtworkload:	Präsenzstudium: 15 Zeitstunden Fernstudienanteil: 135 Zeitstunden • Selbststudium: 90 Zeitstunden • Aufgaben: 30 Zeitstunden • Online-Betreuung: 15 Zeitstunden **Summe: 150 Zeitstunden**

Lerninhalte:	In diesem Modul werden die folgenden Themengebiete behandelt: 1. Aufbau des Android-Systems und Android SDK 2. Einführung in Mobilfunkforenisk für Android • Wie kommt man an die wichtigen Daten? • Rooting, Recovery und andere Zugriffsstrategien • Wo befinden sich die interessanten Daten und welches Aussehen/Format haben sie? • Einführung in SQLite • Bsp.: Manuelle Analyse einer Applikationsdatenbank 3. Aufbau von Android-Applikationen (Manifest, Dalvik-Bytecode, Zertifikate, native Bibliotheken usw.) 4. Schreiben von Android-Applikationen • Aufbau von Applikationen, Android-Manifest • Einführung in Rechte und Intents • Code-Beispiele und einfache Beispiel-Applikationen 5. Obfuskierung • Einführung in Obfuskierung • String-Obfuskierung (XOR, Crypt, ...) • Junkbytes zum Verwirren der Disassembler • Kollision mehrerer Apps zum Verschleiern der Schadfunktion • Schreiben einer einfachen obfuskierten Applikation • Analyse einer obfuskierten Applikation 6. Analyse von Android-Applikationen • Einführung in das Dekompilieren und Reversen von Android-Applikationen • Automatisierte Analysetechniken: Überblick, statische vs. dynamische Analyse • Einführung in die Tools Androguard, Codeinspect, JADx und JD-GUI • Bsp.: Manuelle Analyse einfacher Android-Malware • Bsp.: Teilautomatisierte Analyse komplexerer Android-Malware 7. Einführung in iOS, Aufbau des iOS-Systems 8. Einführung in Mobilfunkforenisk für iOS • Wie kommt man an die wichtigen Daten? • Jailbreaking und andere Zugriffsstrategien • Wo befinden sich die interessanten Daten und welches Aussehen/Format haben sie? • Einführung in Plist-Files • Bsp.: Manuelle Analyse einer Applikationsdatenbank

Lernziele und Kompetenzen:	*Fachkompetenz:* Die Studierenden kennen den Aufbau und die Funktionsweise von Android und dessen Applikationen sowie von iOS. Sie können die grundlegenden Methoden zur Vorbereitung einer forensischen Analyse von Android- und iOS-Mobiltelefonen anwenden. Darüber hinaus sind sie in der Lage, unterschiedliche Verfahren und Werkzeuge zur Analyse zu benennen und anzuwenden. *Methodenkompetenz:* Die Studierenden können einfache Applikationen für Android programmieren und haben Kenntnisse in der Analyse von Applikationen. Sie kennen die Schritte einer sicherheitskritischen Betrachtung von Android-Applikationen. Die Absolventen verfügen über Fähigkeiten, eine forensische Analyse von Mobiltelefonen auf der Basis von Android und iOS durchzuführen. *Sozialkompetenz:* Aufgrund der Teamarbeit, unter anderem an den Präsenzwochenenden, erweitern die Studierenden ihre Teamfähigkeit und Sozialkompetenz. *Selbstkompetenz:* Durch das eigenverantwortliche Entwickeln von Programmen erweitern die Studierenden ihr selbstständiges Handeln. Durch die Präsentation ihrer Ergebnisse wird die Selbstsicherheit der Studierenden gestärkt.
Häufigkeit des Angebots:	ca. alle 2 Jahre
Medienformen:	Studienbriefe in schriftlicher und elektronischer Form, Onlinematerial in Lernplattform, Übungen und Projekt über Lernplattform, Online-Konferenzen, Chat und Forum, Präsenzveranstaltung mit Rechner und Beamer
Literaturhinweise:	Literatur wird in der Lehrveranstaltung bekannt gegeben.

Blockchain und Kryptowährungen (Blockchain and Cryptocurrencies)

Modulbezeichnung:	Blockchain und Kryptowährungen (Blockchain and Cryptocurrencies)
Verwendbarkeit:	Bachelorstudiengang Informatik/IT-Sicherheit (Wahlpflichtmodul)
Lehrveranstaltungen und Lehrformen:	Blockchain und Kryptowährungen Selbstlernphasen, Übungen, Online-Phasen, Präsenzveranstaltung
Modulverantwortliche(r):	Prof. Dr. Dominique Schröder
Lehrende:	Prof. Dr. Dominique Schröder
Dauer:	1 Semester
Credits:	5 ECTS-Punkte
Studien- und Prüfungsleistungen:	Hausarbeit ca. 10 Seiten
Berechnung der Modulnote:	100% der Hausarbeitsnote
Notwendige Voraussetzungen für die Teilnahme:	
Empfohlene Voraussetzungen für die Teilnahme:	• Englischkenntnisse • Programmierkenntnisse in z.B. Python, Java oder Rust
Unterrichts- und Prüfungssprache:	Deutsch und Englisch
Zuordnung des Moduls zu den Fachgebieten des Curriculums:	IT-Sicherheit Vertiefung
Einordnung ins Fachsemester:	Ab Studiensemester 6
Arbeitsaufwand bzw. Gesamtworkload:	Präsenzstudium: 15 Zeitstunden Fernstudienanteil: 135 Zeitstunden • Selbststudium: 90 Zeitstunden • Aufgaben: 30 Zeitstunden • Online-Betreuung: 15 Zeitstunden **Summe: 150 Zeitstunden**

Lerninhalte:	In diesem Modul werden die folgenden Themengebiete behandelt: • Einführung in die Blockchain Technologie • Einführung in die Kryptographie – Was bedeutet Sicherheit? – Was ist eine Verschlüsselung, digitale Signatur und eine Hashfunktion? – Welche Standards gibt es? • Einführung in die Blockchain Technologie – Was ist die Blockchain? – Was ist ein Fork? – Was ist eine Konsensverfahren? – Welche verschiedenen Arten von Blockchain gibt es und wie unter-scheiden sich diese (Public/Private/Consortium) • Praktische Blockchain Realisierungen – Anwendungen der Blockchain Technologie – Blockchain Implementierungen • Einführung in Kryptowährungen – Geschichte der digitalen Währungen – Grundlegende Komponenten – Was ist eine Wallet? • Einführung in Bitcoin – Wie funktioniert Bitcoin? – Wie funktioniert das Konsenzverfahren in Bitcoin? – Wie funktioniert das Mining – Bsp.: Verwendung von Kryptowährungen • Anonymität und Bitcoin – Sind Zahlungen in Bitcoin wirklich anonym? – Techniken zur Verbesserung der Anonymität in Bitcoin • Alternative Kryptowährungen – Überblick über unterschiedliche Kryptowährungen – Anonyme Kryptowährungen, z.B. Monero und ZCash • Projekt (Hausarbeit): Im Rahmen des Projekts werden Themen aus dem Bereich der Kryptowährungen bearbeitet. Dabei soll eine Brücke zwischen der Theorie und der Praxis geschlagen werden, bei dem jedes Projekt zunächst die theoretischen Grundlagen erarbeitet und erläutert, sowie deren praktische Realisierbarkeit durch eine Implementierung bestätigt.

Lernziele und Kompetenzen:	*Fachkompetenz:* Die Studierenden kennen grundlegende kryptographische Verfahren, sowie den Aufbau und die Funktionsweise der Blockchain und von Bitcoin. Sie können die grundlegenden Methoden zum Schutz von sensiblen Daten anwenden. Des Weiteren können sie die Blockchain Technologie zur Realisierung von praktischen Problemen anwenden. Die Studierenden kennen die Funktionsweise von Bitcoin, sie kennen die Vor- und Nachteile digitaler Währungen. *Methodenkompetenz:* Die Studierenden können einfache Applikationen für Kryptowährungen programmieren. Die Absolventen verfügen über Fähigkeiten, praktische Anwendungen im Bereich der Kryptowährungen zu realisieren. *Sozialkompetenz:* Aufgrund der Teamarbeit, unter anderem an den Präsenzwochenenden, erweitern die Studierenden ihre Teamfähigkeit und Sozialkompetenz. *Selbstkompetenz:* Durch das eigenverantwortliche Entwickeln von Programmen erweitern die Studierenden ihr selbstständiges Handeln. Durch die Präsentation ihrer Ergebnisse wird die Selbstsicherheit der Studierenden gestärkt.
Häufigkeit des Angebots:	ca. alle 2 Jahre
Medienformen:	Onlinematerial in Lernplattform, Übungen und Projekt über Lernplattform, Online-Konferenzen, Chat und Forum, Präsenzveranstaltung mit Rechner und Beamer
Literaturhinweise:	Literatur wird in der Lehrveranstaltung bekannt gegeben.

Data Privacy

Modulbezeichnung:	Data Privacy
Verwendbarkeit:	Bachelorstudiengang Informatik/IT-Sicherheit (Wahlpflichtmodul)
Lehrveranstaltungen und Lehrformen:	Data Privacy Selbstlernphasen, Übungen, Online-Phasen, Präsenzveranstaltung
Modulverantwortliche(r):	Prof. Dr. Dominique Schröder
Lehrende:	Prof. Dr. Dominique Schröder
Dauer:	1 Semester
Credits:	5 ECTS-Punkte
Studien- und Prüfungsleistungen:	Hausarbeit
Berechnung der Modulnote:	100% der schriftlichen Prüfungsnote
Notwendige Voraussetzungen für die Teilnahme:	
Empfohlene Voraussetzungen für die Teilnahme:	• Englischkenntnisse • Programmierkenntnisse in z.B. Python, Java oder Russt
Unterrichts- und Prüfungssprache:	Deutsch und Englisch
Zuordnung des Moduls zu den Fachgebieten des Curriculums:	IT-Sicherheit Vertiefung
Einordnung ins Fachsemester:	Ab Studiensemester 6
Arbeitsaufwand bzw. Gesamtworkload:	Präsenzstudium: 15 Zeitstunden Fernstudienanteil: 135 Zeitstunden • Selbststudium: 90 Zeitstunden • Aufgaben: 30 Zeitstunden • Online-Betreuung: 15 Zeitstunden **Summe: 150 Zeitstunden**

Lerninhalte:	In diesem Modul werden die folgenden Themengebiete behandelt: • Einführung in Data Privacy • Einführung in Privacy – Motivation – Rekonstruktionsangriffe • Einführung in grundlegende Techniken zur Anonymisierung – Einführung in die grundlegenden Begriffe: k-Anonymität, l-diversity und t-closeness – Praktische Beispiele für die Anwendung – Möglichkeiten und Grenzen dieser Technik • Grundlagen der Wahrscheinlichkeitstheorie – Zufallsvariablen, Experimente, Erwartungswert – Laplace Verteilung, Exponentielle Verteilung • Einführung in Differential Privacy – Zentrales Modell der Differential Privacy – Formalisierung der ε-Differential Privacy – Komposition – Lokales Differential Privacy • Private-Information Retrieval – Was ist Private Information Retrieval? – Wie wird die Sicherheit definiert? – Effiziente Realisierungen • Oblivious RAM – Einführung in Oblivious RAM – Wie wird die Sicherheit definiert? – Effiziente Realisierungen – Erweiterung auf Oblivious Group ORAM • Ausgewählte Weiterführenden Themen – Homomorphe Verschlüsselung – Machine learning und Differential Privacy • Projekt (Hausarbeit): Im Rahmen des Projekts werden Themen aus dem Bereich der Data Privacy bearbeitet. Dabei soll eine Brücke zwischen der Theorie und der Praxis geschlagen werden, bei dem jedes Projekt zunächst die theoretischen Grundlagen erarbeitet und erläutert, sowie deren praktische Realisierbarkeit untersucht. Je nach Projekt, kann diese durch eine Implementierung bestätigt werden.

Lernziele und Kompetenzen:	*Fachkompetenz:* Die Studierenden kennen grundlegende Angriffe zur Rekonstruktion von (einfach) pseudonymisierten Datenbanken. Sie können die grundlegenden Methoden, wie zum Beispiel k-Anonymität zum einfachen Schutz von Daten anwenden. Die Studierenden kennen die Funktionsweise kryptographischen Verfahren, die einen anonymen Zugriff auf Daten gewährleisten. Die Studierenden kennen die Schutzgarantien von Differential Privacy und kennen die Vor- und Nachteile des zentralen und des lokalen Ansatzes. *Methodenkompetenz:* Die Studierenden können einfache Applikationen für zum Schutz der Daten programmieren. Die Absolventen verfügen über Fähigkeiten, praktische Anwendungen zum Schutz der Anonymität realisieren. *Sozialkompetenz:* Aufgrund der Teamarbeit, unter anderem an den Präsenzwochenenden, erweitern die Studierenden ihre Teamfähigkeit und Sozialkompetenz. *Selbstkompetenz:* Durch das eigenverantwortliche Entwickeln von Programmen erweitern die Studierenden ihr selbstständiges Handeln. Durch die Präsentation ihrer Ergebnisse wird die Selbstsicherheit der Studierenden gestärkt.
Häufigkeit des Angebots:	ca. alle 2 Jahre
Medienformen:	Onlinematerial in Lernplattform, Übungen und Projekt über Lernplattform, Online-Konferenzen, Chat und Forum, Präsenzveranstaltung mit Rechner und Beamer
Literaturhinweise:	Literatur wird in der Lehrveranstaltung bekannt gegeben.

Netzsicherheit 3 (Network Security 3)

Modulbezeichnung:	Netzsicherheit 3 (Network Security 3)
Verwendbarkeit:	Bachelorstudiengang Informatik/IT-Sicherheit (Pflichtmodul)
Lehrveranstaltungen und Lehrformen:	Netzsicherheit 3 Selbstlernphasen, Übungen, Online-Phasen, Präsenzveranstaltung
Modulverantwortliche(r):	Prof. Dr. Jörg Schwenk
Lehrende:	Prof. Dr. Jörg Schwenk
Dauer:	1 Semester
Credits:	5 ECTS-Punkte
Studien- und Prüfungsleistungen:	Klausur: 120 min.
Berechnung der Modulnote:	100 % der schriftlichen Prüfungsnote
Notwendige Voraussetzungen für die Teilnahme:	
Empfohlene Voraussetzungen für die Teilnahme:	• Ausgeprägtes Interesse an IT-Sicherheit, speziell am Thema Web-Sicherheit • Grundlegende Kenntnisse über TCP/IP • Grundkenntnisse im Programmieren • Netzsicherheit 1+2
Unterrichts- und Prüfungssprache:	Deutsch und Englisch
Zuordnung des Moduls zu den Fachgebieten des Curriculums:	IT-Sicherheit Grundlagen
Einordnung ins Fachsemester:	Ab Studiensemester 7
Arbeitsaufwand bzw. Gesamtworkload:	Präsenzzeit: 15 Zeitstunden Fernstudienanteil: 135 Zeitstunden • Durcharbeiten der Studienbriefe: 80 Zeitstunden • Durcharbeiten des Online-Lernmaterials: 15 Zeitstunden • Wahrnehmen der Online Betreuung und Beratung: 10 Zeitstunden • Ausarbeiten von Aufgaben: 25 h • Individuelle Prüfungsvorbereitung der Studierenden: 5 Zeitstunden **Summe: 150 Zeitstunden**

Lerninhalte:	Die Studierenden lernen Methoden und Techniken, wie Web-Applikationen angegriffen werden können. Dies umfasst die folgenden Themengebiete: • Grundlagen des WWW (URL, HTTP) • Grundlagen von Web-Clients (HTML, CSS, JS) • Sicherheitsmechanismen (SOP, CORS) • Angriffe auf Web-Clients (XSS, CSRF, DOM Clobbering) • Angriffe auf Web-Client - UI Redressing • Angriffe auf Datenbanken (SQLi) Für alle vorgestellten Angriffe werden zudem verbreitete Schutzmechanismen gezeigt und deren Wirksamkeit diskutiert.
Lernziele und Kompetenzen:	*Fachkompetenz:* Die Studierenden erwerben grundlegendes Wissen im Bereich der Sicherheit von Webanwendungen. Sie sind in der Lage die Sicherheit einer Webanwendung einzuschätzen und Angriffspunkte offenzulegen. *Methodenkompetenz:* Die Studierenden beherrschen den Umgang mit Fachliteratur und können ihr wichtige Informationen eigenständig entnehmen. Weiterhin sind die Studierenden mit verschiedenen Angriffstechniken vertraut, die auf neue Protokolle und Verfahren übertragen werden können. *Sozialkompetenz:* Die Studenten tauschen sich über Probleme beim Erarbeiten und Anwenden von neuen Inhalten aus und können problemorientiert diskutieren. *Selbstkompetenz:* Die Studenten erlangen die Fähigkeit, sich eine Meinung über die Sicherheit von Protokollen zu bilden. Darüber hinaus besitzen sie die Kompetenz, neue Angriffe aus der aktuellen Fachliteratur zu verstehen und ihre Bedeutungen zu evaluieren. Die Studenten entwickeln ein "gesundes Misstrauen" gegenüber vorgegebenen Sicherheitskonzepten.
Häufigkeit des Angebots:	Wintersemester
Medienformen:	Studienbriefe in elektronischer Form, Onlinematerial in Lernplattform, Übungen über Lernplattform, Online-Konferenzen, Chat und Forum
Literaturhinweise:	• Netzsicherheit 3, Jörg Schwenk, 2016 Weitere Literatur wird in der Lehrveranstaltung bekannt gegeben.

Projekt IT-Sicherheit (Project IT-Security)

Modulbezeichnung:	Projekt IT-Sicherheit (Project IT-Security)
Verwendbarkeit:	Bachelorstudiengang Informatik/IT-Sicherheit (Pflichtmodul)
Lehrveranstaltungen und Lehrformen:	Projekt IT-Sicherheit Orientierungsphase mit Themenwahl, Ausarbeitung des Themas mit individueller Betreuung, Abschlussvortrag
Modulverantwortliche(r):	Prof. Dr.-Ing. Felix Freiling
Lehrende:	Die Betreuung kann durch alle am Studiengang beteiligten Professorinnen und Professoren sowie Dozentinnen und Dozenten erfolgen.
Dauer:	2 Semester
Credits:	10 ECTS-Punkte
Studien- und Prüfungsleistungen:	Schriftliche Ausarbeitung im Umfang von ca. 10 Seiten und mündliche Präsentation im Umfang von 30 Minuten mit anschließender Diskussion im Umfang von 15 Minuten
Berechnung der Modulnote:	50% schriftliche Ausarbeitung + 50% Präsentation
Notwendige Voraussetzungen für die Teilnahme:	
Empfohlene Voraussetzungen für die Teilnahme:	• Proseminar • Erfolgreicher Abschluss der Grundlagen-und Orientierungsprüfung
Unterrichts- und Prüfungssprache:	Deutsch. Mit Zustimmung der Betreuerin bzw. des Betreuers darf die schriftliche Ausarbeitung in Englisch abgefasst werden.
Zuordnung des Moduls zu den Fachgebieten des Curriculums:	IT-Sicherheit Vertiefung
Einordnung ins Fachsemester:	Studiensemester 7 bis 8
Arbeitsaufwand bzw. Gesamtworkload:	Summe: 300 h Präsenzzeit: 1 h • Kolloquium Eigenstudium: 299 h • Themenbearbeitung • Besprechungen mit dem Betreuer • Vorbereitung der Präsentation
Lerninhalte:	Das Projekt kann in allen Teilbereichen der Informatik bearbeitet werden, hat aber in der Regel einen starken Bezug zu aktuellen Forschungsthemen der betreuenden Hochschule. Im Vordergrund stehen praktische Arbeiten im Umfeld eines laufenden Forschungsprojekts, wie z.B. Implementierungen.

Lernziele und Kompetenzen:	*Fachkompetenz:* Die Studierenden können umfangreiche praktische Arbeiten im Umfeld wissenschaftlicher Forschungsthemen selbstständig durchführen. *Methodenkompetenz:* Die Studierenden sind in der Lage, eigenständige Projekte zu bearbeiten, Informationen zu interpretieren und zu bewerten bzw. komplexe Sachverhalte der Informatik zu erkennen. *Sozialkompetenz:* Durch die Enge Zusammenarbeit mit dem Betreuer und die Präsentation der Ergebnisse in einem Kolloquium erweitern Studierenden ihre Teamfähigkeit und Sozialkompetenz. *Selbstkompetenz:* Die Studierenden können komplexe praktische Fragestellung bearbeiten und zielgruppengerecht schriftlich und mündlich präsentieren und argumentativ vertreten. Sie sind in der Lage, ihren eigenen Fortschritt zu überwachen und steuern.
Häufigkeit des Angebots:	Start im Wintersemester
Medienformen:	
Literaturhinweise:	

Sicherheitsmanagement (Security Management)

Modulbezeichnung:	Sicherheitsmanagement (Security Management)
Verwendbarkeit:	Bachelorstudiengang Informatik/IT-Sicherheit (Pflichtmodul)
Lehrveranstaltungen und Lehrformen:	Sicherheitsmanagement • Selbstlernphase • Übungen • Online-Phasen • Präsenzveranstaltung
Modulverantwortliche(r):	Dr. Christoph Wegener
Lehrende:	Wilhelm Dolle und Dr. Christoph Wegener
Dauer:	1 Semester
Credits:	5 ECTS-Punkte
Studien- und Prüfungsleistungen:	Seminar-/Hausarbeit im Umfang von 50h
Berechnung der Modulnote:	100% der Note der Seminar-/Hausarbeit
Notwendige Voraussetzungen für die Teilnahme:	
Empfohlene Voraussetzungen für die Teilnahme:	Grundlegende Kenntnisse in den allgemeinen Aspekten der Informationssicherheit
Unterrichts- und Prüfungssprache:	Deutsch, aktuelle Fachartikel auch in englischer Sprache
Zuordnung des Moduls zu den Fachgebieten des Curriculums:	IT-Sicherheit Vertiefung
Einordnung ins Fachsemester:	ab Studiensemester 8
Arbeitsaufwand bzw. Gesamtworkload:	Präsenzstudium: 15 Zeitstunden • Vorlesung/Präsentation: 12 Zeitstunden • Diskussion/Übungen: 3 Zeitstunden Fernstudienanteil: 135 Zeitstunden • Selbststudium: 70 Zeitstunden • Teilnahme an Online-Konferenzen: 15 Zeitstunden • Ausarbeiten der Seminar-/Hausarbeit: 50 Zeitstunden **Summe: 150 Zeitstunden**

Lerninhalte:	Das Kapitel *Einführung und Motivation* soll den Studierenden zunächst die notwendigen Grundlagen vermitteln und für die Grundideen und –ziele der Informationssicherheit motivieren. Dabei werden die Hauptziele der Informationssicherheit dargestellt, vor allem auch im Vergleich zu denen der IT-Sicherheit. Im Kapitel *Governance in der Informationssicherheit* lernen die Studierenden anschließend die wesentlichen Konzepte und Ideen der Governance im Bereich der Informationssicherheit kennen. Dabei werden sowohl die grundlegenden Elemente der Governance behandelt, zudem wird aufgezeigt, wie eine effektive Governance betrieben werden kann. Im Kapitel *Grundlagen des Risikomanagements* erlernen die Studierenden die Grundzüge des Risikomanagements. Nach einem einleitenden Teil, der unter anderem die grundlegenden Begrifflichkeiten vermitteln, wird aufgezeigt, wie der Prozess des Risikomanagements im Bereich der Informationssicherheit betrieben werden sollte. Nach diesen einführenden Überlegungen gliedert sich das Kapitel *Entwicklung und Management eines Programms zur Informationssicherheit* in zwei Abschnitte. • Zunächst wird der Prozess der *Entwicklung* eines Programms zur Informationssicherheit behandelt. Hier erlernen die Studierenden, aus welchen Komponenten ein Programm zur Informationssicherheit besteht und was beim Aufbau eines solchen beachtet werden muss. • Anschließend wird auf das Thema *Management* eines Programms zur Informationssicherheit eingegangen. Dabei erlernen die Studierenden, wie ein Programm zur Informationssicherheit aufrecht erhalten werden kann und welche Prozesse dafür aufzubauen sind. Insbesondere wird auch thematisiert, wie die zur Verfügung stehenden Ressourcen möglichst effizient eingesetzt werden können. Im Abschnitt *Grundlagen des Incident Management* erlernen die Studierenden, was im "Fall des Falles" zu tun ist. Dabei werden vor allem die Vorkommnisse behandelt, die im Rahmen des Risikomanagements nicht bzw. nicht ausreichend berücksichtigt werden konnten und die somit "unvorhergesehene" Ereignisse darstellen. Abschließend erlernen die Studierenden im Kapitel *Informationssicherheitsmanagement auf Basis von BSI IT-Grundschutz* den Aufbau eines Informationssicherheits-Managementsystems auf Basis von BSI IT-Grundschutz kennen. Dabei wird die Vorgehensweise anhand von konkreten Fallbeispielen exemplarisch erarbeitet.

Lernziele und Kompetenzen:	*Fachkompetenz:* Die Studierenden erwerben fundierte Kenntnisse über die grundlegenden Aspekte der Informationssicherheit und des Managements der Informationssicherheit, insbesondere in den Bereichen Governance in der Informationssicherheit, Risikomanagement, Incident Response Management und den Grundlagen des BSI IT-Grundschutzes. *Methodenkompetenz:* Die Studierenden beherrschen den Umgang mit Fachliteratur und können ihr wichtige Informationen eigenständig entnehmen. Weiterhin sind die Studierenden mit verschiedenen Problematiken im Rahmen des Managements von Informationssicherheit vertraut und können dieses Wissen an Praxisbeispielen umsetzen. *Sozialkompetenz:* Durch Erarbeitung von Fragestellungen in der Gruppe lernen die Studierenden die Sichtweisen verschiedener Bereiche der Informationssicherheit kennen und einen entsprechenden Ausgleich der Interessen zwischen den beteiligten Parteien im Unternehmen herbeizuführen. *Selbstkompetenz:* Die Studierenden erlangen die Fähigkeit, Informationssicherheit zu managen und sich in diesem Bereich selbständig weiter zu bilden bzw. zu entwickeln. Darüber hinaus erlangen sie die Kompetenz, dieses Wissen an die sich ständig ändernden Bedingungen im Unternehmen anzupassen.
Häufigkeit des Angebots:	jährlich im Sommersemester
Medienformen:	• Studienbriefe in schriftlicher und/oder elektronischer Form • ggf. Online-Materialen in der Lernplattform • ggf. unterstützende Übungen und/oder Projekte über die Lernplattform • Online-Konferenzen • Präsenzveranstaltung
Literaturhinweise:	• Informationssicherheit-Management: Leitfaden für Praktiker und Begleitbuch zur CISM-Zertifizierung • BSI-Standards zum IT-Grundschutz (insbesondere Standard BSI 100-2 bzw. BSI 200-2) und der aktuelle IT-Grundschutz-Katalog bzw. das aktuelle IT-Grundschutz-Kompendium • Grundlagen der ISO 27000-Serie • Praxisbuch zur ISO/IEC 27001 • diverse Leitfäden der ISACA Weitere Literatur wird in der Lehrveranstaltung bekannt gegeben.

Bachelorarbeit (Bachelor's thesis)

Modulbezeichnung:	Bachelorarbeit (Bachelor's thesis)
Verwendbarkeit:	Bachelorstudiengang Informatik/IT-Sicherheit (berufsbegleitender Bachelorstudiengang IT-Sicherheit)
Lehrveranstaltungen und Lehrformen:	Dieses Modul besteht aus der schriftlichen Bachelorarbeit (12 ECTS-Punkte) und dem Kolloquium (3 ECTS-Punkte).
Modulverantwortliche(r):	Prof. Dr.-Ing. Felix Freiling
Lehrende:	Die Betreuung kann von jeder Professorin und jedem Professor des Studiengangs sowie die an der Technischen Fakultät hauptberuflich am Department Informatik tätigen Hochschullehrerinnen bzw. Hochschullehrer erfolgen.
Dauer:	6 Monate
Credits:	15 ECTS-Punkte
Studien- und Prüfungsleistungen:	Schriftliche Ausarbeitung (Bachelorarbeit) im Umfang von 30-100 Seiten, mündliche Präsentation im Umfang von 30 Minuten und anschliessende Fachdiskussion im Umfang von 30 Minuten (Kolloquium)
Berechnung der Modulnote:	80% Bachelorarbeit und 20% Kolloquium
Notwendige Voraussetzungen für die Teilnahme:	• Studienleistungen im Umfang von mindestens 110 ECTS-Punkten • Erfolgreicher Abschluss der Grundlagen-und Orientierungsprüfung
Empfohlene Voraussetzungen für die Teilnahme:	
Unterrichts- und Prüfungssprache:	Deutsch. Mit Zustimmung der Betreuerin bzw. des Betreuers darf die Bachelorarbeit in Englisch abgefasst werden. Auf Antrag der bzw. des Studierenden kann die bzw. der Vorsitzende des Prüfungsausschusses mit Zustimmung der Betreuerin bzw. des Betreuers die Abfassung der Bachelorarbeit in einer anderen Sprache zulassen.
Zuordnung des Moduls zu den Fachgebieten des Curriculums:	IT-Sicherheit Vertiefung
Einordnung ins Fachsemester:	Studiensemester 9

Arbeitsaufwand bzw. Gesamtworkload:	Summe: 450 h Präsenzzeit: 1 h • Kolloquium Eigenstudium: 449 h • Themenbearbeitung • Besprechungen mit dem Betreuer • Vorbereitung der Präsentation
Lerninhalte:	Die Bachelorarbeit kann in allen Teilbereichen der Informatik geschrieben werden. Insbesondere relevant sind die folgenden Themen: • IT-Sicherheit im Allgemeinen • Netz- und Systemsicherheit • Digitale Forensik • Kryptographie • Softwareentwicklung • Theoretische Informatik • Compilerbau • Algorithmen und Datenstrukturen
Lernziele und Kompetenzen:	*Fachkompetenz:* Die Studierenden beherrschen die Grundlagen des wissenschaftlichen Arbeitens in ihrem Fachgebiet und können eine begrenzte Fragestellung auf dem Gebiet der Informatik selbstständig bearbeiten *Methodenkompetenz:* Die Studierenden sind in der Lage, Grundlegende Forschungsmethodik der Informatik anzuwenden, eigenständige Projekte zu bearbeiten, Informationen zu interpretieren und zu bewerten bzw. komplexe Sachverhalte der Naturwissenschaft zu erkennen. *Sozialkompetenz:* Durch die enge Zusammenarbeit mit dem Betreuer und die Präsentation der Ergebnisse in einem Kolloquium erweitern die Studierenden ihre Teamfähigkeit und Sozialkompetenz. *Selbstkompetenz:* Die Studierenden können komplexe fachbezogene Inhalte klar und zielgruppengerecht schriftlich und mündlich präsentieren und argumentativ vertreten. Sie sind in der Lage, ihren eigenen Fortschritt zu überwachen und zu steuern.
Häufigkeit des Angebots:	Jedes Semester
Medienformen:	

Literaturhinweise:	