

Modulhandbuch

des

Bachelorstudiengangs Cyber Security

der

Rheinischen Friedrich-Wilhelms-Universität Bonn

Fassung vom 29. März 2025

Inhaltsverzeichnis

1	Pflichtbereich	2
2	Fachgebundener Wahlpflichtbereich Informatik	20
3	Fachgebundener Wahlpflichtbereich Cyber Security	54
4	Nicht-fachgebundener Wahlpflichtbereich	64
4.1	Mathematik	64
4.2	Psychologie	64
4.3	Wirtschaftswissenschaften	65
4.4	Geographie	66
4.5	Photogrammetrie	66
4.6	Physik/Astronomie	66
4.7	Chemie	67
4.8	Philosophie	67
4.9	Molekulare Biomedizin	67
4.10	Meteorologie und Geophysik	68
4.11	Entrepreneurship und Unternehmensführung	68
4.12	Ethik	68

1 Pflichtbereich

BA-INF 011	V4Ü2	9 LP	Logik und diskrete Strukturen	3
BA-INF 015		4 LP	Techniken des wissenschaftlichen Arbeitens	4
BA-INF 016	V4Ü2	9 LP	Algorithmen und Programmierung	5
BA-INF 020	V4Ü2	9 LP	Grundlagen der Mathematik	6
BA-INF 023	V2Ü2	6 LP	Systemnahe Informatik	7
BA-INF 025	Lab4	6 LP	Praktikum Objektorientierte Softwareentwicklung	8
BA-INF 032	V4Ü2	9 LP	Algorithmen und Berechnungskomplexität I	9
BA-INF 034	V2Ü2	6 LP	Systemnahe Programmierung	10
BA-INF 035	V3Ü1	6 LP	Datenzentrierte Informatik	11
BA-INF 053	Sem2P3	9 LP	Projektgruppe Cyber Security	12
BA-INF 054	P2	9 LP	Berufspraktikum Cyber Security	13
BA-INF 061		12 LP	Bachelorarbeit	14
BA-INF 062		2 LP	Begleitseminar zur Bachelorarbeit	15
BA-INF 101	V2Ü2	6 LP	Kommunikation in Verteilten Systemen	16
BA-INF 128	V2Ü2	6 LP	Angewandte Mathematik: Stochastik	17
BA-INF 143	V4Ü2	9 LP	IT-Sicherheit	18
BA-INF 145	V4Ü2	9 LP	Usable Security and Privacy	19

BA-INF 011 Logik und diskrete Strukturen

Workload	Umfang	Dauer	Turnus
270 h	9 LP	1 Semester	jährlich
Modulverantwortliche*r	Lehrende		
Prof. Dr. Heiko Röglin	Prof. Dr. Anne Driemel, Prof. Dr. Thomas Kesselheim, Prof. Dr. Heiko Röglin, PD Dr. Elmar Langetepe		
Studiengang	Modus	Studiensemester	
B. Sc. Cyber Security	Pflicht	1.	

Lernziele: fachliche Kompetenzen

Erwerb von Grundkenntnissen über Gegenstände und Methoden in Mathematischer Logik und Diskreter Mathematik, die im Studium der Informatik benötigt werden; Erwerb und Einübung der Fähigkeit, diese Kenntnisse selbständig zur Lösung von Problemen einzusetzen, mit dem Ziel sicherer Beherrschung.

Lernziele: Schlüsselkompetenzen

Sozialkompetenz (Kommunikationsfähigkeit, Präsentation eigener Lösungsansätze und zielorientierte Diskussion im Gruppenrahmen, Teamfähigkeit), Methodenkompetenz (Analysefähigkeit, Abstraktes Denken, Führen von Beweisen), Individualkompetenz (Leistungs- und Lernbereitschaft, Kreativität, Ausdauer).

Inhalte

Mengen, Relationen, Abbildungen; Kardinalität von Mengen; Monoide, Gruppen, Ringe, Körper; Restklassenring modulo n ; Aufbau des Zahlensystems; Deduktionsbeweis, indirekter Beweis, Beweis durch vollständige Induktion, Schubfachschluß, Diagonalschluß; abzählende Kombinatorik; Aussagenkalkül, Korrektheit und Vollständigkeit, Syntax und Semantik, Signaturen und Strukturen; Prädikatenkalkül 1. Stufe, Substitution, Normalformen; endliche Automaten, reguläre Sprachen.

Teilnahmevoraussetzungen

keine

Veranstaltungen

Lehrform	Gruppengröße	SWS	Workload[h]	LP	
Vorlesung		4	60 P / 105 S	5,5	P = Präsenzstudium S = Selbststudium
Übungen		2	30 P / 75 S	3,5	

Benotete Prüfungsleistungen

Schriftliche Prüfung

Unbenotete Studienleistungen (für Zulassung zur Modulprüfung erforderlich)

Bearbeitung regelmäßig erscheinender Übungsblätter. Die Bearbeitung kann in Gruppen von bis zu drei Studierenden erfolgen. Insgesamt müssen 50% der Punkte erreicht werden. Jede*r Studierende muss einmal die Lösung einer Aufgabe vorstellen.

Literatur

- Steeger: Diskrete Strukturen
- Schöning: Logik für Informatiker
- Graham/Knuth/Patashnik: Concrete Mathematics

BA-INF 015 Techniken des wissenschaftlichen Arbeitens

Workload	Umfang	Dauer	Turnus
120 h	4 LP	1 Semester	jährlich

Modulverantwortliche*r	Lehrende
Dr. Nils Goerke	Dr. Nils Goerke

Studiengang	Modus	Studiensemester
B. Sc. Cyber Security	Pflicht	2. oder 4.

Lernziele: fachliche Kompetenzen

Grundkenntnisse über Form und Stil wissenschaftlicher Quellen, Publikations- und Präsentationsformen wissenschaftlicher Resultate. Erlernen von grundlegenden Techniken der Literaturrecherche, des Erarbeitens und Referierens wissenschaftlicher Quellen; Präsentationstechniken (Vortrag, Ausarbeitung); Grundlagen des wissenschaftlichen Schreibens.

Lernziele: Schlüsselkompetenzen

Studierende erwerben die Fähigkeiten, die Problemstellungen von Aufgaben zu erkennen und lösungsorientiert zu formulieren sowie die Lösungen schriftlich zu dokumentieren, mündlich zu präsentieren und kontrovers zu diskutieren.

Inhalte

Basiswissen zu wiss. Arbeiten, wiss. Kommunikationsformen., wiss. Recherche, wiss. Schreiben und wiss. Präsentation. Wechselnde Inhalte aus allen Bereichen der Informatik, die für die eigentlichen didaktischen Ziele des Moduls (s.o) besonders geeignet sind und geringe fachliche Vorkenntnisse erfordern.

Teilnahmevoraussetzungen

keine

Veranstaltungen

Lehrform	Gruppengröße	SWS	Workload[h]	LP	
Vorlesung		1	15 P / 15 S	1	P = Präsenzstudium
Übungen		2	30 P / 60 S	3	S = Selbststudium

Benotete Prüfungsleistungen

Keine

Unbenotete Studienleistungen (für Zulassung zur Modulprüfung erforderlich)

(i) Die erfolgreiche Bearbeitung und Abgabe einer im Übungsbetrieb angebotenen Schreibübung. (ii) Eine Schreibleistung in Form einer wissenschaftlichen Ausarbeitung zu einem vorgegeben Thema. Die Schreibleistung ist fristgerecht zu einem festgelegten Abgabetermin einzureichen. Sie muss eine genuine Leistung darstellen und vorgegeben Mindestanforderungen erfüllen. (iii) Die erfolgreiche Bearbeitung, Abgabe und Präsentation einer im Übungsbetrieb angebotenen Präsentationsübung. (iv) Eine Präsentationsleistung im Sinne eines mediengestützten Vortrags über ein vorgegebenes wissenschaftliches Thema. Die Präsentationsleistung ist in Form eines Foliensatzes fristgerecht zu einem festgelegten Abgabetermin einzureichen und zu einem festgelegten Präsentationstermin vorzutragen. Sie muss eine genuine Leistung darstellen und vorgegeben Mindestanforderungen erfüllen.

Literatur

- S. Hohmann: Wissenschaftliches Arbeiten für Naturwissenschaftler und Informatiker, Teubner, 2007.
- N. Franck, J. Stary: Die Technik des wissenschaftlichen Arbeitens, 13. Aufl., Schöningh, 2006. ISBN 10: 3835102001

BA-INF 016 Algorithmen und Programmierung

Workload	Umfang	Dauer	Turnus
270 h	9 LP	1 Semester	jährlich
Modulverantwortliche*r	Lehrende		
Dr. Felix Jonathan Boes	Dr. Felix Jonathan Boes, Prof. Dr. Michael Meier		
Studiengang	Modus	Studiensemester	
B. Sc. Cyber Security	Pflicht	1.	

Lernziele: fachliche Kompetenzen

Fähigkeit, Aufgabenstellungen algorithmisch zu formalisieren und einen algorithmischen Lösungsansatz in einer objektorientierten Programmiersprache angemessen und im Detail realisieren zu können.

Lernziele: Schlüsselkompetenzen

kommunikative Kompetenzen (angemessene mündl. und schriftl. Präsentation von Lösungen), soziale Kompetenzen (Teamfähigkeit beim Problemlösen in Kleingruppen, Diskussion und Bewertung unterschiedlicher Lösungsansätze), Selbstkompetenzen (Analysefähigkeit und Kreativität beim Design von Schaltungen, konstruktiver Umgang mit Kritik)

Inhalte

Begriff des Algorithmus; Beschreibungen von Algorithmen; Konstruktion und Verifikation rekursiver und iterativer Algorithmen; programmiersprachliche Grundkonzepte; Konzepte objektorientierter Softwareentwicklung; fundamentale Datenstrukturen; Bäume; Such- und Sortieralgorithmen; Hashing

Teilnahmevoraussetzungen

keine

Veranstaltungen

Lehrform	Gruppengröße	SWS	Workload[h]	LP	
Vorlesung		4	60 P / 105 S	5,5	P = Präsenzstudium
Übungen		2	30 P / 75 S	3,5	S = Selbststudium

Benotete Prüfungsleistungen

Schriftliche Prüfung

Unbenotete Studienleistungen (für Zulassung zur Modulprüfung erforderlich)

Bearbeitung regelmäßig erscheinender Übungsblätter in Gruppen von bis zu drei Studierenden. Jedes Gruppenmitglied muss die eingereichten Lösungen von mindestens 70% der Übungsblätter erfolgreich präsentieren.

Literatur

- Stroustrup, Bjarne: The C++ programming language. Pearson Education, 2013.
- Thomas H. Corman, Charles E. Leiserson, Ronald L. Rivest, Clifford Stein: Introduction to Algorithms. MIT Press 2013.

BA-INF 020 Grundlagen der Mathematik

Workload	Umfang	Dauer	Turnus
270 h	9 LP	1 Semester	jährlich

Modulverantwortliche*r	Lehrende
	Dr. Thoralf Räsch, Dr. Michael Welter

Studiengang	Modus	Studiensemester
B. Sc. Cyber Security	Pflicht	2.

Lernziele: fachliche Kompetenzen

Die fachlichen Kompetenzen von BA-INF 021 oder BA-INF 022.

Lernziele: Schlüsselkompetenzen

Mathematische Formulierung von Problemen, abstraktes Denken, Konzentrationsfähigkeit, selbständige Lösung mathematischer Aufgaben, Präsentation der Lösungsansätze

Inhalte

Das Modul besteht aus den Inhalten von BA-INF 021 oder BA-INF 022.

Teilnahmevoraussetzungen

keine

Veranstaltungen

Lehrform	Gruppengröße	SWS	Workload[h]	LP	
Vorlesung		4	60 P / 105 S	5,5	P = Präsenzstudium
Übungen		2	30 P / 75 S	3,5	S = Selbststudium

Benotete Prüfungsleistungen

Schriftliche Prüfung

Unbenotete Studienleistungen (für Zulassung zur Modulprüfung erforderlich)

Siehe die Modulbeschreibung von BA-INF 021 bzw. BA-INF 022.

BA-INF 023 Systemnahe Informatik

Workload	Umfang	Dauer	Turnus
180 h	6 LP	1 Semester	jährlich
Modulverantwortliche*r	Lehrende		
Prof. Dr. Peter Martini	Prof. Dr. Peter Martini, Dr. Matthias Frank		
Studiengang	Modus	Studiensemester	
B. Sc. Cyber Security	Pflicht	2.	

Lernziele: fachliche Kompetenzen

Die Studierenden lernen die wichtigsten grundlegenden Konzepte aus den Bereichen effiziente Betriebsmittelverwaltung und Interprozess-Kommunikation kennen. Hinzu kommen Kenntnisse des Zusammenspiels zwischen Hard- und Software. Sie gewinnen die Fähigkeit zur Entwicklung effizienter modularer Systeme. Sie erwerben damit die theoretische bzw. konzeptuelle Grundlage für eigenständiges Arbeiten im Bereich der systemnahen Programmierung. Außerdem erarbeiten sie grundlegendes Verständnis des Spannungsfeldes zwischen praktischer Implementierbarkeit bzw. Effizienz aus praktischer Sicht einerseits und abstrakter, modellorientierter Sicht andererseits.

Lernziele: Schlüsselkompetenzen

produktives Arbeiten in Kleingruppen, kritische Reflexion konkurrierender Lösungsansätze, Diskutieren und Präsentieren in Gruppen.

Inhalte

Aufgabe und Struktur von Betriebssystemen, vom Programm zum lauffähigen Code: Lader, Binder, Übersetzung höherer Programmiersprachen (Überblick), Prozesse und Prozessverwaltung, Speicher und Speicherverwaltung, Verteilte Systeme, Dateisystem und Dateiverwaltung, Sicherheitsaspekte

Teilnahmevoraussetzungen

keine

Veranstaltungen

Lehrform	Gruppengröße	SWS	Workload[h]	LP	
Vorlesung		2	30 P / 45 S	2,5	P = Präsenzstudium S = Selbststudium
Übungen		2	30 P / 75 S	3,5	

Benotete Prüfungsleistungen

Schriftliche Prüfung

Unbenotete Studienleistungen (für Zulassung zur Modulprüfung erforderlich)

Teilnahme an zwei Leistungstests. Für jeden Test müssen 30% der Punkte erreicht werden. Insgesamt müssen 50% der Punkte erreicht werden.

Literatur

- Coulouris et al, "Distributed Systems - Concepts and Design", Addison-Wesley, 4th Edition, 2005
- Silberschatz, Galvin, Gagne, "Operating Systems Concepts", 7th Edition, Wiley, 2005
- Tanenbaum, "Modern Operating Systems", 2nd Edition, Prentice-Hall, 2001

BA-INF 025 Praktikum Objektorientierte Softwareentwicklung

Workload	Umfang	Dauer	Turnus
180 h	6 LP	1 Semester	jährlich

Modulverantwortliche*r	Lehrende
Dr. Felix Jonathan Boes	Dr. Felix Jonathan Boes

Studiengang	Modus	Studiensemester
B. Sc. Cyber Security	Pflicht	2.

Lernziele: fachliche Kompetenzen

Fähigkeit, größere Aufgabenstellungen gemäß den Prinzipien der objektorientierten Softwareentwicklung zu analysieren und im Team in einer objektorientierten Programmiersprache angemessen und effizient realisieren zu können.

Lernziele: Schlüsselkompetenzen

soziale Kompetenzen (Teamfähigkeit bei Aufgabenbearbeitung in Kleingruppen); Selbstkompetenzen (Zeitmanagement und Selbstorganisation, konstruktiver Umgang mit Kritik, Erarbeiten von Lösungen bei knappen Ressourcen), kommunikative Kompetenzen (angemessene mündliche und schriftliche Präsentation)

Inhalte

UML; Versionskontrolle; Paradigmen der objektorientierten Softwareentwicklung. Es werden i.a. 3 Softwareprojekte mit jeweils ca. 4 Wochen Bearbeitungszeit in Gruppen durchgeführt werden.

Teilnahmevoraussetzungen

Empfohlen:

Algorithmen und Programmierung.

Veranstaltungen

Lehrform	Gruppengröße	SWS	Workload[h]	LP	P = Präsenzstudium S = Selbststudium
Lab	3	4	60 P / 120 S	6	

Benotete Prüfungsleistungen

Keine

Unbenotete Studienleistungen (für Zulassung zur Modulprüfung erforderlich)

(i) Entwicklung von drei Softwareprojekten in Gruppen von drei Studierenden. (ii) Teilnahme an Präsentationen der zu entwickelnden Softwareprojekte alle zwei Wochen (insgesamt sechs Termine). (iii) Erfolgreiche Abschlusspräsentation der drei Softwareprojekte. Jede der drei Abschlusspräsentationen muss erfolgreich bestanden werden. Kriterien zur Vergabe von Leistungspunkten: Softwarepräsentation, Softwaredokumentation

BA-INF 032 Algorithmen und Berechnungskomplexität I

Workload	Umfang	Dauer	Turnus
270 h	9 LP	1 Semester	jährlich

Modulverantwortliche*r	Lehrende
Prof. Dr. Heiko Röglin	Prof. Dr. Anne Driemel, Prof. Dr. Thomas Kesselheim, Prof. Dr. Heiko Röglin, PD Dr. Elmar Langetepe

Studiengang	Modus	Studiensemester
B. Sc. Cyber Security	Pflicht	3.

Lernziele: fachliche Kompetenzen

Es wird die Fähigkeit vermittelt, grundlegende Algorithmen und Datenstrukturen zu entwerfen und zu analysieren. Ebenso werden Kenntnisse in formalen Sprachen und Automatentheorie vermittelt.

Lernziele: Schlüsselkompetenzen

Präsentation eigener Lösungsansätze und zielorientierte Diskussion im Rahmen der Übungen

Inhalte

Grundlagen und formale Beschreibungsmethoden, Begriff des Algorithmus und der Berechenbarkeit, Maschinenmodelle, Automatentheorie und lexikalische Analyse, Divide-and-Conquer, Sortieren, elementare Datenstrukturen, Tiefensuche (DFS) und Breitensuche (BFS), dynamische Programmierung, Greedy-Algorithmen, Verwaltung dynamischer Mengen, Hashing, elementare Graphenalgorithmen, Lineare Programmierung

Teilnahmevoraussetzungen

keine

Veranstaltungen

Lehrform	Gruppengröße	SWS	Workload[h]	LP	
Vorlesung		4	60 P / 105 S	5,5	P = Präsenzstudium S = Selbststudium
Übungen		2	30 P / 75 S	3,5	

Benotete Prüfungsleistungen

Schriftliche Prüfung

Unbenotete Studienleistungen (für Zulassung zur Modulprüfung erforderlich)

Bearbeitung regelmäßig erscheinender Übungsblätter. Die Bearbeitung kann in Gruppen von bis zu drei Studierenden erfolgen. Insgesamt müssen 40% der Punkte erreicht werden.

Literatur

Vorlesungsbegleitende Skripte und ausgewählte Kapitel aus den Monographien:

- N. Blum: Algorithmen und Datenstrukturen, Oldenbourg, 2004
- N. Blum: Einführung in Formale Sprachen, Berechenbarkeit, Informations- und Lerntheorie, Oldenbourg, 2007
- T. H. Cormen, CH. E. Leiserson, R. L. Rivest: Introduction to the Theory of Computation, PWS, 1997
- M. Karpinski, Einführung in die Informatik, Lecture Notes, Universität Bonn, 2005
- J. Kleinberg, E. Tardos: Algorithm Design, Addison-Wesley, 2005

BA-INF 034 Systemnahe Programmierung

Workload	Umfang	Dauer	Turnus
180 h	6 LP	1 Semester	jährlich
Modulverantwortliche*r	Lehrende		
Prof. Dr. Peter Martini	Dr. Matthias Frank, Dr. Matthias Wübbeling		
Studiengang	Modus	Studiensemester	
B. Sc. Cyber Security	Pflicht	3.	

Lernziele: fachliche Kompetenzen

Die Studierenden sollen in der Lage sein, Techniken der system- und maschinennahen Programmierung (d.h. verteilte, parallele, ereignisorientierte sowie prozessnahe Programmierung) angemessen und im Detail realisieren zu können.

Lernziele: Schlüsselkompetenzen

Ein Schwerpunkt in den unterstützenden Übungen liegt in der praktischen Umsetzung in Kleingruppen (Teamfähigkeit) sowie der Diskussion und dem Vertreten eigener Lösungen

Inhalte

Netzwerk-/Socket-Programmierung (in C/C++), Input-Output-Multiplexing, Serverstrukturen, verteilte Programmierung (Remote Method Invocation), Shared-Memory-/Thread-Programmiermodelle, Specification and Description Language (ereignisorientierte Programmierung), Fortgeschrittene Konzepte von Nebenläufigkeit, u.a. Channels, Coroutinen, Share-Memory-by-Communicating, Dynamic Memory Allocation und Memory Pooling; Maschinenprogrammierung in Assembler

Teilnahmevoraussetzungen

Empfohlen:

BA-INF 023 – Systemnahe Informatik

Veranstaltungen

Lehrform	Gruppengröße	SWS	Workload[h]	LP	
Vorlesung		2	30 P / 45 S	2,5	P = Präsenzstudium
Übungen		2	30 P / 75 S	3,5	S = Selbststudium

Benotete Prüfungsleistungen

Schriftliche Prüfung

Unbenotete Studienleistungen (für Zulassung zur Modulprüfung erforderlich)

Es erscheinen wöchentliche Übungszettel mit praktischen Programmieraufgaben. Die Aufgaben werden in Gruppen von den Studierenden bearbeitet (2 oder 3, max. 4 Gruppenteilnehmer*innen, abhängig von der Gesamt-Teilnehmerzahl). Die Lösungen werden über ein Versionierungssystem eingereicht und von den Tutor*innen bewertet. Ferner muss die Lösung in der Gruppe bei den wöchentlichen Übungsterminen dem/der Tutor*in vorgestellt werden. Zur Klausurzulassung sind mindestens 50% der möglichen Punktzahl über alle Aufgaben zu erreichen. Es werden mehrere Bonus-Aufgaben gestellt, deren Punkte über die zugrunde gelegte Gesamtzahl (100%-Grenze) hinausgehen.

Literatur

- C. A. R. Hoare: Communicating Sequential Processes, Prentice Hall International, Electronic version 2004 edited by Jim Davies, <http://www.usingcsp.com/cspbook.pdf>
- W. Richard Stevens et al.: UNIX Network Programming – The Sockets Networking API, Prentice Hall International, 3rd Edition, 2003
- Andrew S. Tanenbaum, Maarten van Steen: Distributed Systems: Principles and Paradigms, Prentice Hall International 2006
- Markus Zahn: UNIX-Netzwerkprogrammierung mit Threads, Sockets und SSL, Springer 2006

Weitere Literaturhinweise werden rechtzeitig vor Vorlesungsbeginn bekannt gegeben.

BA-INF 035 Datenzentrierte Informatik

Workload	Umfang	Dauer	Turnus
180 h	6 LP	1 Semester	jährlich
Modulverantwortliche*r	Lehrende		
Prof. Dr. Elena Demidova	Prof. Dr. Elena Demidova		
Studiengang	Modus	Studiensemester	
B. Sc. Cyber Security	Pflicht	3.	

Lernziele: fachliche Kompetenzen

Fähigkeit zur Einordnung verschiedener Datenmanagement- und Analyseparadigmen für große Datenbestände; insbesondere Beherrschung der praktischen und theoretischen Grundlagen relationaler Datenbanken sowie praktische und theoretische Grundlagen des maschinellen Lernens.

Lernziele: Schlüsselkompetenzen

- Kommunikative Kompetenzen (mündl./schriftl. Präsentation, „Verteidigung„ von Lösungen)
- Selbstkompetenzen (Zeitmanagement und Selbstorganisation, Kreativität)
- soziale Kompetenz (Diskurs und Arbeitsteilung in Kleingruppen)

Inhalte

- Grundlagen von Datenbanksystemen (relationale Datenbanken, ER-Modellierung, DB-Entwurf, Relationenalgebra, Anfragesprachen und Transaktionen)
- Grundlagen von Datenanalyse (Datenexploration, Statistik, Datenaufbereitung, Feature-Extraktion und Selektion, Grundlegende Machine Learning Algorithmen sowie die Evaluation von Analyseergebnissen)

Teilnahmevoraussetzungen

keine

Veranstaltungen

Lehrform	Gruppengröße	SWS	Workload[h]	LP	
Vorlesung		3	45 P / 45 S	3	P = Präsenzstudium
Übungen		1	15 P / 75 S	3	S = Selbststudium

Benotete Prüfungsleistungen

Schriftliche Prüfung

Unbenotete Studienleistungen (für Zulassung zur Modulprüfung erforderlich)

Bearbeitung regelmäßig erscheinender Übungsblätter. Die Bearbeitung kann in Gruppen von, abhängig von der Gesamt-Teilnehmerzahl, bis zu drei, vier oder fünf Studierenden erfolgen. Insgesamt müssen 50% der Punkte erreicht werden. Für 80% der Aufgabenblätter müssen jeweils 40% der Punkte erreicht werden. Jede*r Studierende muss einmal die Lösung einer Aufgabe vorstellen.

Literatur

- A.Kemper, A. Eickler: Datenbanksysteme: Eine Einführung, 10. Auflage, Oldenbourg Verlag, 2015
- Ethem Alpaydin. Maschinelles Lernen, 2. Auflage, De Gruyter Studium, 2019
- Jiawei Han, Micheline Kamber, Jian Pei: Data Mining: Concepts and Techniques, 3. Auflage. Morgan Kaufmann Publishers, 2011

BA-INF 053 Projektgruppe Cyber Security

Workload	Umfang	Dauer	Turnus
270 h	9 LP	1 Semester	jährlich

Modulverantwortliche*r	Lehrende
Prof. Dr. Michael Meier	alle Dozenten der Informatik

Studiengang	Modus	Studiensemester
B. Sc. Cyber Security	Pflicht	4.

Lernziele: fachliche Kompetenzen

Fähigkeit, im Bereich Cyber Security in kleinen Teams größere Projektaufgaben (Entwicklung von Softwaremodulen oder Hardwarekomponenten) zu planen, nach einem selbstentwickelten Projektplan zu lösen und die Resultate angemessen im Plenum zu diskutieren und zu präsentieren; Einarbeitung im einführenden Seminaranteil durch selbstständige Literatuarbeit und Vortragen der Resultate vor dem Projektteam.

Lernziele: Schlüsselkompetenzen

Inhalte

Themen können aus allen Bereichen der Informatik mit klarem Bezug zu Cyber Security stammen.

Teilnahmevoraussetzungen

keine

Veranstaltungen

Lehrform	Gruppengröße	SWS	Workload[h]	LP	
Seminar	8	2	30 P / 60 S	3	P = Präsenzstudium S = Selbststudium
Praktikum	8	3	45 P / 135 S	6	

Benotete Prüfungsleistungen

Projektarbeit

Unbenotete Studienleistungen (für Zulassung zur Modulprüfung erforderlich)

keine

BA-INF 054 Berufspraktikum Cyber Security

Workload	Umfang	Dauer	Turnus
270 h	9 LP	1 Semester	jährlich
Modulverantwortliche*r	Lehrende		
Prof. Dr. Michael Meier	alle Dozenten der Informatik		
Studiengang	Modus	Studiensemester	
B. Sc. Cyber Security	Pflicht	5.	

Lernziele: fachliche Kompetenzen

Fähigkeit, Sachverhalte der IT-Sicherheit verständlich und zielgruppengerecht (evtl. auch für Nicht-Informatiker) darzustellen. Fähigkeit, Fachwissen der IT-Sicherheit auf praktische Fragestellungen in der Industrie anzuwenden. Fähigkeit, in einer Hierarchie mit Vorgesetzten zu arbeiten. Kompetenzen in der Kommunikation auf den verschiedenen hierarchischen Stufen innerhalb eines Unternehmens.

Lernziele: Schlüsselkompetenzen

Transferfähigkeiten, Team- und Kooperationskompetenz, Kommunikationskompetenz sowie Kreativität und Flexibilität in der Anwendung von Kenntnissen, Erfahrungen und Methoden.

Inhalte

Es wird ein Projekt in einem externen Unternehmen bearbeitet, bei dem die Anwendung von Methoden der IT-Sicherheit im Vordergrund steht. Die Inhalte sind projektabhängig.

Teilnahmevoraussetzungen

Erforderlich:

BA-INF 053 - Projektgruppe Cyber Security

Bemerkungen

Eigeninitiative bei der Vermittlung eines Praktikumsplatzes in Unternehmen ist erwünscht. Das Praktikum soll mindestens sechs Arbeitswochen dauern und vorwiegend in der vorlesungsfreien Zeit stattfinden. Eine Anmeldung ist erst möglich, wenn die erforderlichen Teilnahmevoraussetzungen vorliegen und ein Dozent festgestellt hat, dass ein den Anforderungen entsprechender Praktikumsplatz zur Verfügung steht.

Veranstaltungen

Lehrform	Gruppengröße	SWS	Workload[h]	LP	P = Präsenzstudium S = Selbststudium
Berufspraktikum	1	2	30 P / 240 S	9	

Benotete Prüfungsleistungen

Keine

Unbenotete Studienleistungen (für Zulassung zur Modulprüfung erforderlich)

Berufspraktikum im Umfang von mindestens 6 Wochen Vollzeit; Praktikumsbericht und Vortrag

BA-INF 061 Bachelorarbeit

Workload	Umfang	Dauer	Turnus
360 h	12 LP	1 Semester	jedes Semester

Modulverantwortliche*r	Lehrende
	Alle Dozenten der Cyber Security

Studiengang	Modus	Studiensemester
B. Sc. Cyber Security	Pflicht	6.

Lernziele: fachliche Kompetenzen
Fähigkeit zur selbstständigen Bearbeitung eines wissenschaftlichen Themas von der Recherche bis zur Dokumentation der Resultate

Lernziele: Schlüsselkompetenzen
Angemessene wissenschaftliche Präsentation in Wort und Schrift

Inhalte
Die Themen können aus allen Bereichen der Cyber Security stammen.

Teilnahmevoraussetzungen
Erforderlich: BA-INF 053 - Projektgruppe Cyber Security

Veranstaltungen					
Lehrform	Gruppengröße	SWS	Workload[h]	LP	
Selbstständige Anfertigung einer wiss. Arbeit unter individueller Betreuung		0	360 S	12	P = Präsenzstudium S = Selbststudium

Benotete Prüfungsleistungen
Schriftliche Prüfung

Unbenotete Studienleistungen (für Zulassung zur Modulprüfung erforderlich)
keine

Literatur
Quellen zur Einarbeitung in das Thema werden individuell bereit gestellt und/oder müssen durch selbstständiges Recherchieren ergänzt werden.

BA-INF 062 Begleitseminar zur Bachelorarbeit

Workload	Umfang	Dauer	Turnus
60 h	2 LP	1 Semester	jedes Semester
Modulverantwortliche*r	Lehrende		
	Alle Dozenten der Informatik		
Studiengang	Modus	Studiensemester	
B. Sc. Cyber Security	Pflicht	6.	
Lernziele: fachliche Kompetenzen			
Fähigkeit zur Präsentation selbst erarbeiteter Ergebnisse, Fähigkeit zur kritischen Diskussion über eigene und fremde Ergebnisse.			
Lernziele: Schlüsselkompetenzen			
Informationskompetenz, Kompetenz in wissenschaftlicher Recherche, Vermittlungskompetenz, Methodenkompetenz und fachliche Flexibilität.			
Inhalte			
Die Themen können aus allen Bereichen der Informatik stammen.			
Teilnahmevoraussetzungen			
keine			
Veranstaltungen			
Lehrform	Gruppengröße	SWS	Workload[h] LP
Seminar		2	30 P / 30 S 2
P = Präsenzstudium S = Selbststudium			
Benotete Prüfungsleistungen			
Vortrag mit Präsentation der Ergebnisse der Bachelorarbeit			
Unbenotete Studienleistungen (für Zulassung zur Modulprüfung erforderlich)			
keine			
Literatur			
Quellen zur Einarbeitung in das Thema werden individuell bereit gestellt und/oder müssen durch selbstständiges Recherchieren ergänzt werden.			

BA-INF 101 Kommunikation in Verteilten Systemen

Workload	Umfang	Dauer	Turnus
180 h	6 LP	1 Semester	jährlich
Modulverantwortliche*r	Lehrende		
Prof. Dr. Peter Martini	Prof. Dr. Peter Martini, Dr. Matthias Frank		
Studiengang	Modus	Studiensemester	
B. Sc. Cyber Security	Pflicht	3. oder 5.	

Lernziele: fachliche Kompetenzen

Die Studierenden erlernen die wichtigsten grundlegenden Konzepte aus dem Bereich der Kommunikation in verteilten Systemen. Hierzu gehören praxisorientierte Kenntnisse der verschiedenen Protokollebenen (technologieorientiert, transportorientiert sowie anwendungsorientiert) sowie logischer und physikalischer Strukturen von Kommunikationssystemen. Sie lernen das dynamische Verhalten vorherzusagen und bei der Planung zu berücksichtigen.

Lernziele: Schlüsselkompetenzen

Die Übungen unterstützen die Teamfähigkeit sowie die Fähigkeit zur Präsentation und Diskussion von Ergebnissen.

Inhalte

Signal Darstellung und Synchronisation, Adressierung und Routing in Kommunikationssystemen, Flusskontrolle und Überlastabwehr, Multimediale Kommunikation

Teilnahmevoraussetzungen

Empfohlen:

BA-INF 023 – Systemnahe Informatik

Veranstaltungen

Lehrform	Gruppengröße	SWS	Workload[h]	LP	
Vorlesung		2	30 P / 45 S	2,5	P = Präsenzstudium S = Selbststudium
Übungen		2	30 P / 75 S	3,5	

Benotete Prüfungsleistungen

Schriftliche Prüfung

Unbenotete Studienleistungen (für Zulassung zur Modulprüfung erforderlich)

Bearbeitung regelmäßig erscheinender Übungsblätter. Die Bearbeitung kann in Gruppen von bis zu drei Studierenden erfolgen. Insgesamt müssen 50% der Punkte erreicht werden. Für 70% der Aufgabenblätter müssen jeweils 20% der Punkte erreicht werden. Jede*r Studierende muss dreimal die Lösung einer Aufgabe vorstellen.

Literatur

- Douglas E. Comer: Internetworking with TCP/IP; Vol. I: Principles, Protocols, and Architecture, Prentice Hall, 4th Edition, 2002
- W. Stallings: Data & Computer Communications, 6th Edition, Prentice Hall International Editions, 2000
- Tanenbaum: Computer Networks, Pearson Education, 4th Edition, 2002
- Weitere Literaturhinweise werden rechtzeitig vor Vorlesungsbeginn bekannt gegeben.

BA-INF 128 Angewandte Mathematik: Stochastik

Workload	Umfang	Dauer	Turnus
180 h	6 LP	1 Semester	jährlich
Modulverantwortliche*r	Lehrende		
Prof. Dr. Reinhard Klein	Prof. Dr. Jürgen Gall, Prof. Dr. Reinhard Klein		
Studiengang	Modus	Studiensemester	
B. Sc. Cyber Security	Pflicht	4.	

Lernziele: fachliche Kompetenzen

- Erlernen fortgeschrittener mathematischer Modelle
- Einsatz der Modelle in konkreten Anwendungen
- Anwendung von Stochastik-Werkzeugen auf informatische Probleme

Lernziele: Schlüsselkompetenzen

- Sozialkompetenz (insb. Transfer- und Teamfähigkeit)
- Selbstkompetenz (insb. Leistungsbereitschaft, fachliche Flexibilität und Kreativität)

Inhalte

- Wahrscheinlichkeitsräume
- Zufallsvariablen
- Stochastische Standardmodelle
- Bedingte Wahrscheinlichkeit und Unabhängigkeit
- Erwartungswert und Varianz
- Wahrscheinlichkeitsdichten, Normalverteilungen
- Gesetze der großen Zahlen
- Markov-Ketten
- Statistische Modelle
- Maximum-Likelihood-Schätzer

Teilnahmevoraussetzungen

Empfohlen:

solide Kenntnisse in Linearer Algebra und/oder Analysis

Veranstaltungen

Lehrform	Gruppengröße	SWS	Workload[h]	LP	
Vorlesung		2	30 P / 45 S	2,5	P = Präsenzstudium S = Selbststudium
Übungen		2	30 P / 75 S	3,5	

Benotete Prüfungsleistungen

Schriftliche Prüfung

Unbenotete Studienleistungen (für Zulassung zur Modulprüfung erforderlich)

Bearbeitung regelmäßig erscheinender Übungsblätter. Die Bearbeitung kann in Gruppen von bis zu drei Studierenden erfolgen. Insgesamt müssen 50% der Punkte erreicht werden. Für 70% der Aufgabenblätter müssen jeweils 50% der Punkte erreicht werden. Jede*r Studierende muss einmal die Lösung einer Aufgabe vorstellen.

Literatur

- begleitendes Vorlesungsskript
- H.-O. Georgii: Stochastik, 3. Auflage, Walter de Gruyter 2007
- L. Dümbgen: Stochastik für Informatiker, Springer 2003
- R. Motvani, P. Raghavan: Randomized Algorithms, Cambridge University Press, 2002

BA-INF 143 IT-Sicherheit

Workload	Umfang	Dauer	Turnus
270 h	9 LP	1 Semester	jährlich
Modulverantwortliche*r	Lehrende		
Prof. Dr. Michael Meier	Prof. Dr. Michael Meier, Dr. Felix Boes		
Studiengang	Modus	Studiensemester	
B. Sc. Cyber Security	Pflicht	1.	

Lernziele: fachliche Kompetenzen

Die Veranstaltung führt in den Themenbereich der Sicherheit informationstechnischer Systeme ein. Die Studierenden lernen, welche Interessen nach Sicherheit gewahrt werden sollen und welche technischen und organisatorischen Anforderungen sich aus den Sicherheitsinteressen ergeben. Es wird vermittelt, welche inhaltlichen Sicherheitsanforderungen mit welchen technischen Sicherheitsmaßnahmen unterstützt werden können. Darüber hinaus erfahren die Studierenden, wie IT-Systeme unter dem Gesichtspunkt der Sicherheit entworfen, realisiert und betrieben werden können. Die Teilnehmer erlangen einen Überblick zu den genannten Aspekten und möglichen Lösungsansätzen.

Lernziele: Schlüsselkompetenzen

Grundlagen der IT-Sicherheit. Fähigkeit, IT-Sicherheitsmechanismen zur physischen Absicherung, Authentifikation und Zugriffskontrolle sowie die Anwendung grundlegender kryptographischer Verfahren zu verstehen, wesentliche Eigenschaften zu kennen und umzusetzen.

Inhalte

- Grundlagen zu IT-Systemen, insbesondere zu Netzen und Betriebssystemen
- Sicherheitsinteressen und Schutzziele
- Authentifikation
- Zugriffskontrolle
- Angewandte Kryptographie
- IT-Sicherheitsmanagement

Teilnahmevoraussetzungen

keine

Veranstaltungen

Lehrform	Gruppengröße	SWS	Workload[h]	LP	
Vorlesung		4	60 P / 105 S	5,5	P = Präsenzstudium
Übungen		2	30 P / 75 S	3,5	S = Selbststudium

Benotete Prüfungsleistungen

Klausurarbeit

Unbenotete Studienleistungen (für Zulassung zur Modulprüfung erforderlich)

Bearbeitung regelmäßig erscheinender Übungsblätter. Die Bearbeitung kann in Gruppen von bis zu drei Studierenden erfolgen. Insgesamt müssen 50% der Punkte erreicht werden. Jede*r Studierende muss zweimal die Lösung einer Aufgabe vorstellen.

Literatur

- M. Bishop, Computer Security: Art and Science, Addison-Wesley, Boston
- C. Eckert, IT-Sicherheit: Konzepte – Verfahren – Protokolle, Oldenbourg
- J. Biskup, Security in Computing Systems – Challenges, Approaches and Solutions, Springer, Berlin.

BA-INF 145 Usable Security and Privacy

Workload	Umfang	Dauer	Turnus
270 h	9 LP	1 Semester	jährlich
Modulverantwortliche*r	Lehrende		
Prof. Dr. Matthew Smith	Prof. Dr. Matthew Smith		
Studiengang	Modus	Studiensemester	
B. Sc. Cyber Security	Pflicht	4.	

Lernziele: fachliche Kompetenzen

Diese Veranstaltung führt in die Thematik Faktor Mensch in der IT-Sicherheit ein. Usable Security beschäftigt sich im Kern mit der Erforschung von auf den Menschen zugeschnittenen Sicherheitsmechanismen und der Evaluierung dieser bezüglich ihrer Anwendbarkeit durch Benutzergruppen. Während bestehende Sicherheitsmechanismen für die meisten Anwendungsfälle theoretisch ausreichende Sicherheit gewährleisten könnten, wird dieses theoretisch mögliche Sicherheitsniveau selten erreicht. Sicherheitstechnologien werden fehlerhaft bedient oder gänzlich umgangen, da sie oft zu komplex und zeitaufwändig sind. Die Vorlesung führt die Herausforderung im Bereich der benutzbaren IT-Sicherheit ein und zeigt das Systeme, die Sicherheitsmechanismen beinhalten, sozio-technologischen Systemen sind, die in ihrer Gänze untersucht werden müssen. Dazu werden Methoden zur empirische Untersuchungen von Benutzerverhaltens beigebracht.

Lernziele: Schlüsselkompetenzen

- Grundlegende Fachliteratur aus dem Bereich Usable Security kennen.
- Empirische Studien im Bereich Usable Security verstehen.
- Methoden zum Studiendesign und Durchführung anwenden können.

Inhalte

Folien sind in englischer Sprache:

Foundations

- Introduction
- Ethics
- Usability Measures
- Evaluation Methods Qualitative
- Evaluation Methods Quantitative
- Crash Course Statistics
- Biases

Application Areas:

- Passwords
- Warnings
- Server Configuration
- Email and Message Encryption
- Secure Programming

Teilnahmevoraussetzungen

Empfohlen:

- IT-Sicherheit

Veranstaltungen

Lehrform	Gruppengröße	SWS	Workload[h]	LP	
Vorlesung		4	60 P / 105 S	5,5	P = Präsenzstudium
Übungen		2	30 P / 75 S	3,5	S = Selbststudium

Benotete Prüfungsleistungen

Schriftliche Prüfung (eKlausur)

Unbenotete Studienleistungen (für Zulassung zur Modulprüfung erforderlich)

Erfolgreiche Übungsteilnahme

2 Fachgebundener Wahlpflichtbereich Informatik

BA-INF 013	V4Ü2	9 LP	Technische Informatik	21
BA-INF 021	V4Ü2	9 LP	Lineare Algebra	22
BA-INF 022	V4Ü2	9 LP	Analysis	23
BA-INF 036	V3Ü1	6 LP	Softwaretechnologie	24
BA-INF 041	V3Ü1	6 LP	Algorithmen und Berechnungskomplexität II	25
BA-INF 104	V4Ü2	9 LP	Randomisierte und approximative Algorithmen	26
BA-INF 105	V4Ü2	9 LP	Einführung in die Computergrafik und Visualisierung	27
BA-INF 106	V4Ü2	9 LP	Lineare und ganzzahlige Optimierung	28
BA-INF 107	V4Ü2	9 LP	Einführung in die Diskrete Mathematik	29
BA-INF 108	V2Ü2	6 LP	Geschichte des maschinellen Rechnens I	30
BA-INF 109	V2Ü2	6 LP	Relationale Datenbanken	31
BA-INF 110	V4Ü2	9 LP	Grundlagen der Künstlichen Intelligenz	32
BA-INF 114	V4Ü2	9 LP	Grundlagen der algorithmischen Geometrie	33
BA-INF 123	V2Ü2	6 LP	Computational Intelligence	34
BA-INF 126	V2Ü2	6 LP	Geschichte des maschinellen Rechnens II	35
BA-INF 127	V2Ü2	6 LP	Angewandte Mathematik: Numerik	36
BA-INF 131	V2Ü2	6 LP	Intelligente Sehsysteme	37
BA-INF 132	V2Ü2	6 LP	Grundlagen der Robotik	38
BA-INF 137	V2Ü2	6 LP	Einführung in die Sensordatenfusion	39
BA-INF 139		6 LP	Tutorenschulung/ Vermittlung von Informatikinhalt	40
BA-INF 144	V4Ü2	9 LP	Algorithmische Grundlagen des maschinellen Lernens	41
BA-INF 149	V2Ü2	6 LP	Graphenalgorithmen	42
BA-INF 150	V2Ü2	6 LP	Einführung in die Data Science	43
BA-INF 153	V2Ü2	6 LP	Einführung in Deep Learning für Visual Computing	44
BA-INF 154	V2Ü2	6 LP	Medizinische Bildanalyse	46
BA-INF 157	V2Ü2	6 LP	Introduction to Machine Learning	47
BA-INF 159	V2Ü2	6 LP	Agile Software Development	48
BA-INF 160	V2Ü2	6 LP	Grundlagen der Künstlichen Intelligenz 1	50
BA-INF 162	V2Ü2	6 LP	Webtechnologien	52

BA-INF 013 Technische Informatik

Workload	Umfang	Dauer	Turnus
270 h	9 LP	1 Semester	jährlich
Modulverantwortliche*r	Lehrende		
Prof. Dr. Matthias Hullin	Dr. Johannes Müllers		
Studiengang	Modus	Studiensemester	
B. Sc. Cyber Security	Wahlpflicht	3. oder 5.	

Lernziele: fachliche Kompetenzen

Die Studierenden lernen die Grundlagen der Technischen Informatik kennen. Sie sind anschließend in der Lage, eigene digitale Schaltungen zu entwickeln, verstehen die Prinzipien des Pipelinings und Cachings und kennen die Grundzüge moderner Computerarchitekturen

Lernziele: Schlüsselkompetenzen

kommunikative Kompetenzen (angemessene mündl. und schriftl. Präsentation von Lösungen), soziale Kompetenzen (Teamfähigkeit beim Problemlösen in Kleingruppen, Diskussion und Bewertung unterschiedlicher Lösungsansätze), Selbstkompetenzen (Analysefähigkeit und Kreativität beim Design von Schaltungen, konstruktiver Umgang mit Kritik)

Inhalte

Schaltalgebra, Gatter, Schaltnetze, Speicherglieder, Schaltwerke, Schaltungsentwurf, Zahldarstellungen, Rechenwerke, Datenpfad und Steuerung, Mikroprogrammierung, Pipelines, Caches

Teilnahmevoraussetzungen

keine

Veranstaltungen

Lehrform	Gruppengröße	SWS	Workload[h]	LP	
Vorlesung		4	60 P / 105 S	5,5	P = Präsenzstudium
Übungen		2	30 P / 75 S	3,5	S = Selbststudium

Benotete Prüfungsleistungen

Schriftliche Prüfung

Unbenotete Studienleistungen (für Zulassung zur Modulprüfung erforderlich)

Bearbeitung regelmäßig erscheinender Übungsblätter. Die Bearbeitung kann in Gruppen von bis zu drei Studierenden erfolgen. Insgesamt müssen 50% der Punkte erreicht werden. Jede*r Studierende muss zweimal die Lösung einer Aufgabe vorstellen. Einer der Übungszettel wird in Form eines Leistungstests durchgeführt, der auch als Probeklausur dient.

Literatur

- Dirk W. Hoffmann: Grundlagen der Technischen Informatik. Hanser Fachbuchverlag, ISBN-10: 3446406913, ISBN-13: 978-3446406919
- Wolfram Schiffmann, Robert Schmitz: Technische Informatik 1. Grundlagen der digitalen Elektronik. Springer, Berlin, ISBN-10: 354040418X, ISBN-13: 978-3450404187

BA-INF 021 Lineare Algebra

Workload	Umfang	Dauer	Turnus
270 h	9 LP	1 Semester	jährlich

Modulverantwortliche*r	Lehrende
	Dr. Thoralf Räsch, Dr. Michael Welter

Studiengang	Modus	Studiensemester
B. Sc. Cyber Security	Wahlpflicht	2.

Lernziele: fachliche Kompetenzen

- Verständnis für lineare Zusammenhänge
- Ausprägung von mathematischer Intuition und geometrischer Vorstellungskraft
- Kenntnis von algebraischen Strukturen am Beispiel
- Einblick in die Anwendungen der linearen Algebra durch Vorstellung ausgewählter Problemstellungen
- Erkennen des Bezugs zu numerischen Verfahren

Lernziele: Schlüsselkompetenzen

Analytische Formulierung von Problemen, abstraktes Denken, Konzentrationsfähigkeit, selbständige Lösung mathematischer Aufgaben, Präsentation der Lösungsansätze

Inhalte

Vektorräume: Grundbegriffe (Körper allgemein, Vektorräume, Lineare Abhängigkeit, Basis, Dimension; Lineare Unterräume, Erzeugendensysteme; (direkte) Summe von Vektorräumen), Lineare Abbildungen (Definition, elementare Eigenschaften; Kern und Bild, Quotientenvektorräume, Lineare Abbildungen und Matrizen, Rang, Isomorphismen, Koordinatentransformationen, Rang und Äquivalenz von Matrizen), Lösen linearer Gleichungen (Affine Unterräume, Lösungsgesamtheit, Gauß-Elimination), Determinanten (Permutationen, Existenz und Eindeutigkeit der Determinante, schnelle Determinantenberechnung, Determinante eines Endomorphismus, Orientierung), Normalformen von Matrizen (Ähnlichkeit von Matrizen, Eigenwerte und Eigenvektoren, (charakteristische) Polynome, Diagonalisierbarkeit, Tridiagonalisierbarkeit, Jordansche Normalform), Euklidische und unitäre Vektorräume (Skalarprodukte, Gram-Schmidt-Orthonormalisierung, orthogonale und unitäre Gruppen, Hauptachsentransformation)

Teilnahmevoraussetzungen

keine

Veranstaltungen

Lehrform	Gruppengröße	SWS	Workload[h]	LP	
Vorlesung		4	60 P / 105 S	5,5	P = Präsenzstudium S = Selbststudium
Übungen		2	30 P / 75 S	3,5	

Benotete Prüfungsleistungen

Schriftliche Prüfung

Unbenotete Studienleistungen (für Zulassung zur Modulprüfung erforderlich)

Bearbeitung regelmäßig erscheinender Übungsblätter. Die Bearbeitung kann in Gruppen von bis zu zwei Studierenden erfolgen. Insgesamt müssen 50% der Punkte erreicht werden.

Literatur

- K. Jänich, Lineare Algebra, Springer 2001
- G. Fischer, Lineare Algebra, Vieweg, 2000

BA-INF 022 Analysis

Workload	Umfang	Dauer	Turnus
270 h	9 LP	1 Semester	jährlich

Modulverantwortliche*r	Lehrende
	Dr. Michael Welter, Dr. Thoralf Räsch

Studiengang	Modus	Studiensemester
B. Sc. Cyber Security	Wahlpflicht	2.

Lernziele: fachliche Kompetenzen

Umgang mit reellen und komplexen Zahlen sowie Folgen und Reihen. Kenntnis der Differential- und Integralrechnung von Funktionen einer Variablen. Kenntnis der Differentialrechnung von Funktionen mehrerer reeller Variablen. Kenntnis und Umgang mit elementaren Funktionen. Fähigkeit, mathematische Argumentationen durchzuführen

Lernziele: Schlüsselkompetenzen

Analytische Formulierung von Problemen, abstraktes Denken, Konzentrationsfähigkeit, selbständige Lösung mathematischer Aufgaben, Präsentation der Lösungsansätze

Inhalte

Zahlen (Reelle und Komplexe Zahlen; Wurzeln, Potenzen), Folgen, Reihen, Konvergenz (Definition, Konvergenz, Monotonie, Häufungswert, Cauchy-Kriterium, Exponentialfunktion, Potenzreihen), Komplexe Exponential-, Sinus-, Cosinusfunktion (Polarkoordinaten, Multiplikation, n-te Wurzeln, Analysis in $\mathbb{C}$, Konvergenz im $\mathbb{R}^n$, Grenzwerte von Funktionen, Stetigkeit (Folgen, Reihen, Potenzreihen und Stetigkeit in $\mathbb{C}$; Konvergenz von Folgen, Unendliche Reihen, Komplexe Funktionen, Potenzreihen), Funktionen (Grenzwerte, Stetige Funktionen: Zwischenwertsatz, Nullstellensatz, Monotonie, Umkehrfunktion, Gleichmäßige Stetigkeit; Funktionenfolgen), Differentialrechnung (Differenzierungsregeln; Umkehrfunktionen, Extremrechnung, Mittelwertsatz; Höhere Ableitungen, Satz von Taylor), Riemann-Integral (Integrabilitätskriterium, Hauptsätze, Partielle Integration; Integration durch Substitution, Mittelwertsatz der Integralrechnung, Integration rationaler Funktionen), Fourier-Reihen, Differentialrechnung im $\mathbb{R}^n$ (Partielle Differenzierbarkeit, Differenzierbarkeit und Stetigkeit, Richtungsableitung, Satz von Taylor)

Teilnahmevoraussetzungen

keine

Veranstaltungen

Lehrform	Gruppengröße	SWS	Workload[h]	LP	
Vorlesung		4	60 P / 105 S	5,5	P = Präsenzstudium S = Selbststudium
Übungen		2	30 P / 75 S	3,5	

Benotete Prüfungsleistungen

Schriftliche Prüfung

Unbenotete Studienleistungen (für Zulassung zur Modulprüfung erforderlich)

Individuelle Bearbeitung regelmäßig erscheinender Übungsblätter. Jedes Übungsblatt enthält mindestens drei schriftlich zu bearbeitende Aufgaben. Pro Aufgabe können 10 Punkte erzielt werden. Für jedes Übungsblatt müssen 5 Punkte erzielt werden. Sollte wegen Krankheit eine Abgabe verpasst werden, so muss diese in der Folgewoche bzw. nach Genesung nachgeliefert werden. Ebenso ist eine korrigierte Abgabe nachzureichen, wenn mit einer Abgabe weniger als 5 Punkte erreicht werden.

Literatur

O. Foster: Analysis 1-2, Vieweg 1984

BA-INF 036 Softwaretechnologie

Workload	Umfang	Dauer	Turnus
180 h	6 LP	1 Semester	jährlich
Modulverantwortliche*r	Lehrende		
Dr. Günter Kniesel	Dr. Günter Kniesel		
Studiengang	Modus	Studiensemester	
B. Sc. Cyber Security	Wahlpflicht	5.	

Lernziele: fachliche Kompetenzen

Die Studierenden sollen in der Lage sein, ein komplettes Softwareprojekt (von der Anforderungserhebung bis zur Implementierung und deren Qualitätssicherung) im Team durchzuführen und dabei moderne Hilfsmittel der Softwarequalitätssicherung, Versions- und Projektverwaltung einzusetzen.

Lernziele: Schlüsselkompetenzen

- Soziale Kompetenzen (Teamfähigkeit bei Aufgabenbearbeitung in Kleingruppen)
- Selbstkompetenzen (Zeitmanagement und Selbstorganisation, konstruktiver Umgang mit Kritik, Erarbeiten von Lösungen bei knappen Ressourcen)
- kommunikative Kompetenzen (angemessene mündliche und schriftliche Präsentation)

Inhalte

- Notationen der UML und ihre Abbildung in objektorientierten Code
- Entwurfstechniken (Abbot, CRC, design by contract, Entwurfsmuster)
- Anforderungserhebung und -analyse, System- und Objektentwurf, Testen
- Softwarearchitekturen
- Komponentenmodelle
- Software-Prozessmodelle
- Software-Konfigurations-Management
- Projekt-Management

Teilnahmevoraussetzungen

Erforderlich:

BA-INF 025 – Praktikum Objektorientierte Softwareentwicklung

Empfohlen:

BA-INF 016 - Algorithmen und Programmierung

Veranstaltungen

Lehrform	Gruppengröße	SWS	Workload[h]	LP	
Vorlesung		3	45 P / 75 S	4	P = Präsenzstudium
Übungen		1	15 P / 45 S	2	S = Selbststudium

Benotete Prüfungsleistungen

Schriftliche Prüfung

Unbenotete Studienleistungen (für Zulassung zur Modulprüfung erforderlich)

Jeweils 50% der Punkte für theoretische und praktische Übungsaufgaben. Die Punkte sind durch *eigene* Beiträge (schriftliche Abgaben und/oder mündliche Erläuterungen) zu erwerben. Es müssen mindestens drei ausreichend gute Lösungen von praktischen Aufgaben selbst präsentiert werden. Ausreichend gut bedeutet dabei, dass die präsentierte Lösung mindestens 50% der Punkte erreicht.

Medieneinsatz

Projektion, Videos

Literatur

- Ian Sommerville: Software Engineering. Pearson, 2018
- Bernd Bruegge, Allen H. Dutoit: Object-Oriented Software Engineering: Using UML, Patterns, and Java. 2nd Edition Prentice Hall, September 2003

BA-INF 041 Algorithmen und Berechnungskomplexität II

Workload	Umfang	Dauer	Turnus
180 h	6 LP	1 Semester	jährlich
Modulverantwortliche*r	Lehrende		
Prof. Dr. Heiko Röglin	Prof. Dr. Anne Driemel, Prof. Dr. Thomas Kesselheim, Prof. Dr. Heiko Röglin, PD Dr. Elmar Langetepe		
Studiengang	Modus	Studiensemester	
B. Sc. Cyber Security	Wahlpflicht	4.	

Lernziele: fachliche Kompetenzen

Es wird die Fähigkeit vermittelt, selbstständig die Berechnungskomplexität von Problemen zu analysieren. Ebenso werden Techniken zum Entwurf und zur Analyse von randomisierten Algorithmen und von Approximationsalgorithmen vermittelt.

Lernziele: Schlüsselkompetenzen

Präsentation eigener Lösungsansätze und zielorientierte Diskussion im Rahmen der Übungen

Inhalte

Grenzen der Berechenbarkeit, Unentscheidbarkeit, Rekursionstheorie, NP-schwere Probleme, Theorie der NP-Vollständigkeit (Satz von Cook), polynomielle Reduktionen, randomisierte Algorithmen, Approximationsalgorithmen, Approximationshärte

Teilnahmevoraussetzungen

Empfohlen:

BA-INF 032 – Algorithmen und Berechnungskomplexität I

Veranstaltungen

Lehrform	Gruppengröße	SWS	Workload[h]	LP	
Vorlesung		3	45 P / 45 S	3	P = Präsenzstudium S = Selbststudium
Übungen		1	15 P / 75 S	3	

Benotete Prüfungsleistungen

Schriftliche Prüfung

Unbenotete Studienleistungen (für Zulassung zur Modulprüfung erforderlich)

Bearbeitung regelmäßig erscheinender Übungsblätter. Die Bearbeitung kann in Gruppen von bis zu drei Studierenden erfolgen. Insgesamt müssen 40% der Punkte erreicht werden.

Literatur

Vorlesungsbegleitende Skripte und ausgewählte Kapitel aus den Monographien:

- N. Blum: Algorithmen und Datenstrukturen, Oldenbourg, 2004
- N. Blum: Einführung in Formale Sprachen, Berechenbarkeit, Informations- und Lerntheorie, Oldenbourg, 2007
- T. H. Cormen, CH. E. Leiserson, R. L. Rivest: Introduction to the Theory of Computation, PWS, 1997
- M. Karpinski, Einführung in die Informatik, Lecture Notes, Universität Bonn, 2005
- J. Kleinberg, E. Tardos: Algorithm Design, Addison-Wesley, 2005
- C. H. Papadimitriou: Computational Complexity, Addison-Wesley, 1994
- M. Sipser: Introduction to the Theory of Computation, PWS, 1997

BA-INF 104 Randomisierte und approximative Algorithmen

Workload	Umfang	Dauer	Turnus
270 h	9 LP	1 Semester	alle 2 Jahre
Modulverantwortliche*r	Lehrende		
Prof. Dr. Heiko Röglin	Prof. Dr. Heiko Röglin, Prof. Dr. Thomas Kesselheim		
Studiengang	Modus	Studiensemester	
B. Sc. Cyber Security	Wahlpflicht	5.	

Lernziele: fachliche Kompetenzen

Die Studierenden sollen moderne Methoden des Entwurfes und Analyse effizienter Algorithmen lernen, insbesondere randomisierte und approximative Lösungsmethoden für die zuvor inhärent intractablen Berechnungsprobleme.

Lernziele: Schlüsselkompetenzen

Präsentation eigener Lösungsansätze und zielorientierte Diskussion im Rahmen der Übungen

Inhalte

Grundlegende Konzepte und Paradigmen der effizienten Berechnungen, randomisierte, MonteCarlo- und Las Vegas-Algorithmen, approximative Algorithmen, Entwurf und Analyse, probabilistische Methoden, Markov-Ketten, Anwendungen in der kombinatorischen Optimierung, Network Design und Internet-Algorithmen

Teilnahmevoraussetzungen

Empfohlen:

BA-INF 032 – Algorithmen und Berechnungskomplexität I

Veranstaltungen

Lehrform	Gruppengröße	SWS	Workload[h]	LP	
Vorlesung		4	60 P / 105 S	5,5	P = Präsenzstudium S = Selbststudium
Übungen		2	30 P / 75 S	3,5	

Benotete Prüfungsleistungen

Mündliche Prüfung

Unbenotete Studienleistungen (für Zulassung zur Modulprüfung erforderlich)

Bearbeitung regelmäßig erscheinender Übungsblätter. Die Bearbeitung kann in Gruppen von bis zu drei Studierenden erfolgen. Insgesamt müssen 25% der Punkte erreicht werden.

Literatur

- M. Karpinski, Randomisierte und approximative Algorithmen für harte Berechnungsprobleme, Lecture Notes (5. Auflage), Universität Bonn, 2007
- M. Karpinski, W. Rytter, Fast Parallel Algorithms for Graph Matching Problems, Oxford University Press, 1998
- R. Motwani, P. Raghavan, Randomized Algorithms, Cambridge University Press, 1995
- V.V. Vazirani, Approximation Algorithms, Springer, 2001

BA-INF 105 Einführung in die Computergrafik und Visualisierung

Workload	Umfang	Dauer	Turnus
270 h	9 LP	1 Semester	jährlich
Modulverantwortliche*r	Lehrende		
Prof. Dr. Matthias B. Hullin	Prof. Dr. Matthias B. Hullin		
Studiengang	Modus	Studiensemester	
B. Sc. Cyber Security	Wahlpflicht	4. oder 6.	

Lernziele: fachliche Kompetenzen

Kenntnis der wichtigsten Daten und Datenstrukturen zur Repräsentation dreidimensionaler Szenen (Geometrie, Lichtquellen, optische Materialeigenschaften, Texturen), Kenntnis von Operationen und Methoden zur Erzeugung realistischer Bilder aus 3D-Szenenbeschreibungen (Rendering-Pipeline), Kenntnis der grundlegenden Konzepte der wissenschaftlichen Visualisierung (Visualization-Pipeline), Verständnis der Graphik-API „OpenGL“, und die Fähigkeit, einfache Rendering- und Visualisierungstechniken zu implementieren

Lernziele: Schlüsselkompetenzen

Analytische Formulierung von Problemen, Kreativität, selbständige Lösung praktischer Probleme der Computer Graphik und Visualisierung, Präsentation der von Lösungsansätzen und Implementierungen, Medienfertigkeiten, Informationsgewinnung, Team- und Moderationsfähigkeiten, Selbstmanagement

Inhalte

Rasterisierungsalgorithmen, Linien- und Polygon-Clipping, Affine Transformationen, Projektive Abbildungen und Perspektive, 3D-Clipping und Sichtbarkeitsberechnungen, Rendering-Pipeline, Farbe, Beleuchtungsmodelle und Bilderzeugung, Benutzen und Programmieren von Graphikhardware, Raytracing, Compositing, Texture Mapping, Datenstrukturen für Graphik und Visualisierung, Kurven-, Flächen- und Volumenrepräsentationen, Volumenvisualisierung, Visualisierungspipeline, Filterung, grundlegende Mappingtechniken, Visualisierung von 3D-Skalar- und Vektorfeldern

Teilnahmevoraussetzungen

Empfohlen:

- BA-INF 127 – Angewandte Mathematik: Numerik oder
- BA-INF 128 – Angewandte Mathematik: Stochastik

Veranstaltungen

Lehrform	Gruppengröße	SWS	Workload[h]	LP	
Vorlesung		4	60 P / 105 S	5,5	P = Präsenzstudium
Übungen		2	30 P / 75 S	3,5	S = Selbststudium

Benotete Prüfungsleistungen

(i) Abschlussbericht und -präsentation Programmierprojekt (40%); (ii) Schriftliche Prüfung (60%)

Unbenotete Studienleistungen (für Zulassung zur Modulprüfung erforderlich)

(i) Bearbeitung regelmäßig erscheinender Übungsblätter. Die Bearbeitung kann in Gruppen von bis zu drei Studierenden erfolgen. Insgesamt müssen 50% der Punkte erreicht werden. Für 70% der Aufgabenblätter müssen jeweils 50% der Punkte erreicht werden. Die Aufgaben sind aufgeteilt in theoretische und praktische Aufgaben, und die zu erzielenden Punkte gelten separat für beide Teile. Jede*r Studierende muss zweimal die Lösung einer Aufgabe vorstellen. (ii) Bearbeitung eines Programmierprojekts und Anfertigung eines animierten Kurzfilms oder interaktiven 3D-Anwendung auf Grundlage eines selbst entwickelten Bildsynthese-Frameworks. Die Bearbeitung kann in Gruppen von bis zu drei Studierenden erfolgen.

Literatur

- Fabio Ganovelli et al.: Introduction to Computer Graphics: A Practical Learning Approach, Chapman and Hall/CRC 2014
- P. Shirley et al.: Fundamentals of Computer Graphics, 2nd edition, A K Peters, 2005
- D. Hearn, P. Baker: Computer Graphics with Open GL, Prentice Hall; 4 edition (November 19, 2010)
- J. Encarnação, W. Straßer, R. Klein: Graphische Datenverarbeitung I, Oldenbourg, 1995

BA-INF 106 Lineare und ganzzahlige Optimierung

Workload	Umfang	Dauer	Turnus
270 h	9 LP	1 Semester	jährlich
Modulverantwortliche*r	Lehrende		
Prof. Dr. Jens Vygen	Alle Dozenten der Diskreten Mathematik		
Studiengang	Modus	Studiensemester	
B. Sc. Cyber Security	Wahlpflicht	4. oder 6.	

Lernziele: fachliche Kompetenzen

Verständnis der grundlegenden Zusammenhänge der Polyedertheorie und der Theorie der linearen und ganzzahligen Optimierung, Kenntnis der wichtigsten Algorithmen, Fähigkeit zur geeigneten Modellierung praktischer Probleme als mathematische Optimierungsprobleme und deren Lösung

Lernziele: Schlüsselkompetenzen

Mathematische Modellierung praktischer Probleme, Entwicklung von Lösungsstrategien, abstraktes Denken, schriftliche Bearbeitung von Übungsaufgaben und Präsentation der Lösungen in Übungsgruppen

Inhalte

Modellierung von Optimierungsproblemen als (ganzzahlige) lineare Programme, Polyeder, Fourier-Motzkin-Elimination, Farkas' Lemma, Dualitätssätze, Simplexverfahren, Netzwerk-Simplex, Ellipsoidmethode, Bedingungen für Ganzzahligkeit von Polyedern, TDI-Systeme, vollständige Unimodularität, Schnittebenenverfahren

Teilnahmevoraussetzungen

Erforderlich:

- BA-INF 011 – Logik und diskrete Strukturen und
- BA-INF 021 – Lineare Algebra

Veranstaltungen

Lehrform	Gruppengröße	SWS	Workload[h]	LP	
Vorlesung		4	60 P / 105 S	5,5	P = Präsenzstudium
Übungen		2	30 P / 75 S	3,5	S = Selbststudium

Benotete Prüfungsleistungen

Schriftliche Prüfung

Unbenotete Studienleistungen (für Zulassung zur Modulprüfung erforderlich)

Bearbeitung regelmäßig erscheinender Übungsblätter. Die Bearbeitung kann in Gruppen von bis zu zwei Studierenden erfolgen. Insgesamt müssen 50% der Punkte erreicht werden. Jede*r Studierende muss zweimal die Lösung einer Aufgabe vorstellen.

Literatur

- Schrijver: Theory of Linear and Integer Programming. Wiley 1986
- V. Chvatal : Linear Programming. Freeman 1983
- B. Korte, J. Vygen : Kombinatorische Optimierung: Theorie und Algorithmen (Kapitel 3 bis 5). Springer, 2. Auflage 2012
- R.K. Ahuja, T.L. Magnanti, J.B. Orlin: Network Flows (Kapitel 11). Prentice Hall 1993
- B. Gärtner, J. Matousek: Understanding and Using Linear Programming, Springer, Berlin, 2006.

BA-INF 107 Einführung in die Diskrete Mathematik

Workload	Umfang	Dauer	Turnus
270 h	9 LP	1 Semester	jährlich
Modulverantwortliche*r	Lehrende		
Prof. Dr. Jens Vygen	Alle Dozenten der Diskreten Mathematik		
Studiengang	Modus	Studiensemester	
B. Sc. Cyber Security	Wahlpflicht	3. oder 5.	

Lernziele: fachliche Kompetenzen

Kenntnis der wichtigsten Algorithmen für grundlegende kombinatorische Optimierungsprobleme, Fähigkeit zur Bewertung verschiedener algorithmischer Lösungen und zur geeigneten Modellierung praktischer Probleme als kombinatorische Optimierungsprobleme

Lernziele: Schlüsselkompetenzen

Mathematische Modellierung praktischer Probleme, wie sie etwa in Chipdesign, Verkehrsplanung, Logistik, Telekommunikation, Internet alltäglich auftreten. Entwicklung von Lösungsstrategien, abstraktes Denken, schriftliche Bearbeitung von Übungsaufgaben und Präsentation der Lösungen in Übungsgruppen

Inhalte

Branchings, Goldberg-Tarjan-Algorithmus, minimale Schnitte, Zusammenhang, kostenminimale Flüsse, Anwendungen von Flüssen in Netzwerken, bipartites Matching, Multicommodity flows und disjunkte Wege

Teilnahmevoraussetzungen

Erforderlich:

BA-INF 011 – Logik und diskrete Strukturen

Veranstaltungen

Lehrform	Gruppengröße	SWS	Workload[h]	LP	
Vorlesung		4	60 P / 105 S	5,5	P = Präsenzstudium
Übungen		2	30 P / 75 S	3,5	S = Selbststudium

Benotete Prüfungsleistungen

Schriftliche Prüfung

Unbenotete Studienleistungen (für Zulassung zur Modulprüfung erforderlich)

Bearbeitung regelmäßig erscheinender Übungsblätter. Die Bearbeitung kann in Gruppen von bis zu zwei Studierenden erfolgen. Insgesamt müssen 50% der Punkte erreicht werden. Jede*r Studierende muss zweimal die Lösung einer Aufgabe vorstellen.

Literatur

- R.K. Ahuja, T.L. Magnanti, J.B. Orlin: Network Flows. Prentice Hall 1993 (Kapitel 4 bis 10, 12, 13)
- B. Korte, J. Vygen: Kombinatorische Optimierung: Theorie und Algorithmen. Springer, 2. Auflage 2012 (Kapitel 6 bis 9 und 19)
- R. Diestel : Graphentheorie. Springer, Vierte Auflage 2010
- T.H. Cormen, C.E. Leiserson, R.L. Rivest, C. Stein : Introduction to Algorithms. MIT Press, Third Edition 2009
- D. Jungnickel : Graphs, Networks and Algorithms. Springer, Fourth Edition 2013
- W. Cook, W. Cunningham, W. Pulleyblank, A. Schrijver : Combinatorial Optimization. Wiley 1997
- A. Schrijver : Combinatorial Optimization: Polyhedra and Efficiency. Springer 2003

BA-INF 108 Geschichte des maschinellen Rechnens I

Workload	Umfang	Dauer	Turnus
180 h	6 LP	1 Semester	jährlich

Modulverantwortliche*r	Lehrende
Prof. Dr. Ina Prinz	Prof. Dr. Ina Prinz

Studiengang	Modus	Studiensemester
B. Sc. Cyber Security	Wahlpflicht	4.

Lernziele: fachliche Kompetenzen

Die Studierenden bekommen einen Überblick über die wesentlichen Erfindungen in der Geschichte des maschinellen Rechnens und aus den Anfängen der Informatik vermittelt. Dabei sollen nicht nur theoretische Grundlagen zur Erfindung von Rechenmaschinen und Computern im Vordergrund stehen, sondern auch das selbständige Untersuchen der historischen Objekte. Die Studierenden erwerben grundlegende Kenntnisse der Geschichte der Informatik und werden dazu befähigt, aktuelle Entwicklungen der Informatik historisch einzuordnen.

Lernziele: Schlüsselkompetenzen

Kritische Reflektionen über die Informatikgeschichte, kommunikative Kompetenzen im Übungsbetrieb, soziale Kompetenzen bei Kleingruppenarbeit in den Übungen, Kreativität bei der Untersuchung historischer Rechengeräte und bei der Programmierung historischer Computer, Zeitmanagement.

Inhalte

Anfänge von Zahlen, Zahlensystemen und des Rechnens; erste Rechenhilfsmittel: Soroban, Suanpan. Schtschoty, Napierstäbe; mechanische Darstellung von Zahlen: Sprossenrad, Staffelwalze, Stellsegment; Entwicklung von Rechenmaschinen: Addiermaschinen, Vierspeziesmaschinen, Spezialmaschinen; Übertragungsmechanismen: Zehnerübertrag; Innovationen um die Jahrhundertwende bis zum Untergang der mechanischen Rechenmaschine

Teilnahmevoraussetzungen

keine

Veranstaltungen

Lehrform	Gruppengröße	SWS	Workload[h]	LP	
Vorlesung		2	30 P / 45 S	2,5	P = Präsenzstudium
Übungen		2	30 P / 75 S	3,5	S = Selbststudium

Benotete Prüfungsleistungen

Mündliche Prüfung

Unbenotete Studienleistungen (für Zulassung zur Modulprüfung erforderlich)

(i) Bearbeitung regelmäßig erscheinender Übungsblätter. Die Bearbeitung kann in Gruppen von bis zu drei Studierenden erfolgen. Für 60% der Aufgabenblätter müssen jeweils 50% der Punkte erreicht werden. (ii) Erfolgreiche Bearbeitung eines Programmierprojekts. Die Bearbeitung kann in Gruppen von bis zu drei Studierenden erfolgen. Das Projektergebnis muss präsentiert werden.

Medieneinsatz

Exponate des Arithmeums

Literatur

- Aspray, W.: Computing before Computers. Ames, 1990.
- Bauer, Friedrich L.: Origins and Foundations of Computing. Berlin 2010.
- Korte, Bernhard: Zur Geschichte des maschinellen Rechnens. Bonn, 1981.
- Prinz, Ina: Historische Rechenmaschinen. Bonn, 2010.

BA-INF 109 Relationale Datenbanken

Workload	Umfang	Dauer	Turnus
180 h	6 LP	1 Semester	jährlich
Modulverantwortliche*r	Lehrende		
Dr. Thomas Bode	Dr. Thomas Bode		
Studiengang	Modus	Studiensemester	
B. Sc. Cyber Security	Wahlpflicht	4. oder 6.	

Lernziele: fachliche Kompetenzen

Die Studierenden lernen grundlegende Fähigkeiten für den Betrieb und die Anwendung relationaler Datenbankmanagementsysteme. Dies umfasst auch neuere Anwendungsbereiche wie z.B. das Data Warehousing.

Lernziele: Schlüsselkompetenzen

kommunikative Kompetenzen (mündl. Präsentation/"Verteidigung" von eigenen Lösungen), Selbstkompetenzen (Zeitmanagement und Selbstorganisation, Kreativität, konstruktiver Umgang mit Kritik), soziale Kompetenz (Diskurs und produktive Arbeitsteilung in Kleingruppen)

Inhalte

Fortgeschrittenere Konzepte in SQL (z.B. SQL-Invoked Routines, objektrelationale Erweiterungen), Anwendungsschnittstellen für SQL, Java und RDBMS, Sekundärspeicherabbildung von Tabellen, Indexstrukturen, Clustering und Partitionierung, Anfragebearbeitung (Algorithmen und Kostenmodelle), logische und physische Optimierung, Transaktionskonzepte, Sicherheit

Teilnahmevoraussetzungen

Empfohlen:

- BA-INF 035 Datenzentrierte Informatik und
- BA-INF 025 Praktikum Objektorientierte Softwareentwicklung

Veranstaltungen

Lehrform	Gruppengröße	SWS	Workload[h]	LP	
Vorlesung		2	30 P / 45 S	2,5	P = Präsenzstudium
Übungen		2	30 P / 75 S	3,5	S = Selbststudium

Benotete Prüfungsleistungen

Mündliche Prüfung

Unbenotete Studienleistungen (für Zulassung zur Modulprüfung erforderlich)

Erfolgreiche Bearbeitung eines Programmierprojekts. Die Bearbeitung kann in Gruppen von bis zu zwei Studierenden erfolgen.

Literatur

- Jim Melton, Alan R. Simon: SQL:1999 – Understanding Relational Language Components, San Francisco, Morgan Kaufmann, 2002
- Jim Melton: Advanced SQL:1999 – Understanding Object-Relational and other Advanced Features, San Francisco, Morgan Kaufmann, 2003
- Can Türker, Gunter Saake: Objektrelationale Datenbanken – ein Lehrbuch. Heidelberg, dpunkt-Verlag, 2006
- weitere Literatur wird in der Vorlesung bekanntgegeben

BA-INF 110 Grundlagen der Künstlichen Intelligenz

Workload	Umfang	Dauer	Turnus
270 h	9 LP	1 Semester	jährlich
Modulverantwortliche*r	Lehrende		
Prof. Dr. Stefan Wrobel	Dr. Tamas Horvath, Dr. Florian Seiffarth		
Studiengang	Modus	Studiensemester	
B. Sc. Cyber Security	Wahlpflicht		

Lernziele: fachliche Kompetenzen

Die Studierenden lernen der wichtigsten grundlegenden Paradigmen und Methoden der Künstlichen Intelligenz (KI) kennen. Sie erwerben die Fähigkeit, eine gegebene Aufgabenstellung mit geeigneten Wissensrepräsentations- und Inferenzmethoden der KI darstellen und lösen zu können.

Lernziele: Schlüsselkompetenzen

Studierende erwerben die Fähigkeiten, Problemstellungen zu erkennen und lösungsorientiert zu formulieren sowie die Lösungen und erstellten Programme schriftlich zu dokumentieren, mündlich zu präsentieren und kontrovers zu diskutieren.

Inhalte

Agentenkonzept, Problemlösung durch Suchverfahren, heuristische Suche, logische und probabilistische Wissenrepräsentation und Inferenz, Planungssysteme, Nutzentheorie und Nutzenfunktionen, Entscheidungstheorie und Entscheidungsprozesse, Lernverfahren, Grundlagen zu Bildverstehen und Robotik

Teilnahmevoraussetzungen

Empfohlen:

- BA-INF 011 – Logik und diskrete Strukturen,
- BA-INF 016 – Algorithmen und Programmierung,
- BA-INF 032 – Algorithmen und Berechnungskomplexität I

Bemerkungen

Dieses Modul wird nicht mehr angeboten. Es wird durch BA-INF 160 Grundlagen der Künstlichen Intelligenz I und BA-INF 161 Grundlagen der Künstlichen Intelligenz II ersetzt. Im Sommersemester 2025 werden für diejenigen, die nicht BA-INF 160 absolvieren, noch Prüfungstermine für BA-INF 110 angeboten.

Veranstaltungen

Lehrform	Gruppengröße	SWS	Workload[h]	LP	
Vorlesung		4	60 P / 105 S	5,5	P = Präsenzstudium
Übungen		2	30 P / 75 S	3,5	S = Selbststudium

Benotete Prüfungsleistungen

Schriftliche Prüfung

Unbenotete Studienleistungen (für Zulassung zur Modulprüfung erforderlich)

Bearbeitung regelmäßig erscheinender Übungsblätter. Die Bearbeitung kann in Gruppen von bis zu drei Studierenden erfolgen. Insgesamt müssen 50% der Punkte erreicht werden. Jede*r Studierende muss zweimal die Lösung einer Aufgabe vorstellen. Die erste Vorstellung muss für Aufgaben von einem der ersten fünf Übungsblätter erfolgen, in den ersten sechs Wochen der Vorlesungszeit. Die zweite Vorstellung muss für eines der folgenden fünf Übungsblätter erfolgen, innerhalb von zwölf Wochen nach Anfang der Vorlesungszeit.

Medieneinsatz

Folien, Tafel, Videos und Demoprogramme

Literatur

- Stuart Russel, Peter Norvig: Künstliche Intelligenz: Ein moderner Ansatz. 3. Auflage, Pearson Studium 2012.
- Stuart Russel, Peter Norvig: Künstliche Intelligenz: Ein moderner Ansatz. 2. Auflage, Pearson Studium 2004.
- Nils J. Nilsson: Artificial Intelligence: A New Synthesis. Morgan Kaufman, 1998.

BA-INF 114 Grundlagen der algorithmischen Geometrie

Workload	Umfang	Dauer	Turnus
270 h	9 LP	1 Semester	jährlich
Modulverantwortliche*r	Lehrende		
Prof. Dr. Anne Driemel	Prof. Dr. Anne Driemel, Prof. Dr. Rolf Klein, PD Dr. Elmar Langetepe, Dr. Herman Haverkort		
Studiengang	Modus	Studiensemester	
B. Sc. Cyber Security	Wahlpflicht	4. oder 6.	

Lernziele: fachliche Kompetenzen

Erwerb von Grundkenntnissen über Gegenstände und Methoden der Algorithmischen Geometrie; Erwerb und Einübung der Fähigkeit, diese Kenntnisse selbständig zur Lösung von Problemen einzusetzen, mit dem Ziel sicherer Beherrschung.

Lernziele: Schlüsselkompetenzen

Sozialkompetenz (Kommunikationsfähigkeit, Präsentation eigener Lösungsansätze und zielorientierte Diskussion im Gruppenrahmen, Teamfähigkeit), Methodenkompetenz (Analysefähigkeit, Abstraktes Denken, Führen von Beweisen), Individualkompetenz (Leistungs- und Lernbereitschaft, Kreativität, Ausdauer).

Inhalte

Grundlegende kombinatorische Eigenschaften geometrischer Strukturen; Entwurf und Analyse effizienter geometrischer Algorithmen und Datenstrukturen; Anwendung algorithmischer Paradigmen auf geometrische Probleme; Sweep-Verfahren; Schnittpunkte von Strecken; Geometrische Datenstrukturen; Konvexe Hülle; Polygone; Sichtbarkeit; Voronoi-Diagramm; Delaunay-Triangulation; Online Strategien; inkrementelle Konstruktion; Divide and Conquer; Randomisierung. Die Grundkenntnisse umfassen Definitionen und Theoreme zu den aufgeführten Gegenständen.

Teilnahmevoraussetzungen

Empfohlen:

BA-INF 011 – Logik und diskrete Strukturen

Veranstaltungen

Lehrform	Gruppengröße	SWS	Workload[h]	LP	
Vorlesung		4	60 P / 105 S	5,5	P = Präsenzstudium
Übungen		2	30 P / 75 S	3,5	S = Selbststudium

Benotete Prüfungsleistungen

Mündliche Prüfung

Unbenotete Studienleistungen (für Zulassung zur Modulprüfung erforderlich)

Bearbeitung regelmäßig erscheinender Übungsblätter. Die Bearbeitung kann in Gruppen von bis zu drei Studierenden erfolgen. Insgesamt müssen 50% der Punkte erreicht werden.

Literatur

- Klein: Algorithmische Geometrie
- de Berg/van Kreveld/Overmars/Cheong: Computational Geometry

BA-INF 123 Computational Intelligence

Workload	Umfang	Dauer	Turnus
180 h	6 LP	1 Semester	jährlich

Modulverantwortliche*r	Lehrende
Prof. Dr. Sven Behnke	Prof. Dr. Sven Behnke, Dr. Nils Goerke

Studiengang	Modus	Studiensemester
B. Sc. Cyber Security	Wahlpflicht	4. oder 6.

Lernziele: fachliche Kompetenzen

fachliche Kompetenzen:

Verständnis der wesentlichen Paradigmen und Grundkonzepte der Computational Intelligence (CI). Kennenlernen typischer Datenstrukturen und Algorithmen. Praktische Erfahrungen bei der Entwicklung und Anwendung von CI-Methoden.

Lernziele: Schlüsselkompetenzen

integrativ vermittelte Schlüsselkompetenzen:

Analysefähigkeit, Kreativität, Team-, Präsentations- und Diskussionsfähigkeit, konstruktiver Umgang mit Kritik, Selbstmanagement, Leistungsbereitschaft, Zielstrebigkeit.

Inhalte

Künstliche Neuronale Netze, Evolutionäre Algorithmen, Fuzzy-Systeme

Teilnahmevoraussetzungen

keine

Veranstaltungen

Lehrform	Gruppengröße	SWS	Workload[h]	LP	
Vorlesung		2	30 P / 45 S	2,5	P = Präsenzstudium
Übungen		2	30 P / 75 S	3,5	S = Selbststudium

Benotete Prüfungsleistungen

Schriftliche Prüfung

Unbenotete Studienleistungen (für Zulassung zur Modulprüfung erforderlich)

Bearbeitung regelmäßig erscheinender Übungsblätter. Die Bearbeitung kann in Gruppen von bis zu zwei Studierenden erfolgen. Insgesamt müssen 50% der Punkte erreicht werden.

Literatur

- O. Kramer: Computational Intelligence, Springer, 2008
- D. Floreano, C. Mattiussi: Bio-Inspired Artificial Intelligence, MIT-Press, 2008
- A. Konar: Computational Intelligence, Springer, 2005

BA-INF 126 Geschichte des maschinellen Rechnens II

Workload	Umfang	Dauer	Turnus
180 h	6 LP	1 Semester	jährlich
Modulverantwortliche*r	Lehrende		
Prof. Dr. Ina Prinz	Prof. Dr. Ina Prinz		
Studiengang	Modus	Studiensemester	
B. Sc. Cyber Security	Wahlpflicht	5.	

Lernziele: fachliche Kompetenzen

Die Studierenden bekommen einen Überblick über die wesentlichen Erfindungen in der Geschichte des maschinellen Rechnens und aus den Anfängen der Informatik vermittelt. Dabei sollen nicht nur theoretische Grundlagen zur Erfindung von Rechenmaschinen und Computern im Vordergrund stehen, sondern auch das selbständige Untersuchen der historischen Objekte. Die Studierenden erwerben grundlegende Kenntnisse der Geschichte der Informatik und werden dazu befähigt, aktuelle Entwicklungen der Informatik historisch einzuordnen.

Lernziele: Schlüsselkompetenzen

Kritische Reflektionen über die Informatikgeschichte, kommunikative Kompetenzen im Übungsbetrieb, soziale Kompetenzen bei Kleingruppenarbeit in den Übungen, Kreativität bei der Untersuchung historischer Rechengeräte und bei der Programmierung historischer Computer, Zeitmanagement.

Inhalte

Teil II baut auf Modul 108: Geschichte des maschinellen Rechnens – Teil I auf: Die Entwicklung des Computers, Lochkarten als Datenspeicher, Entwicklung elektronischer Rechner, Programmierung und Benutzung von frühen Computern, Pioniere der Computerentwicklung

Teilnahmevoraussetzungen

Empfohlen:

BA-INF 108 – Geschichte des maschinellen Rechnens I

Veranstaltungen

Lehrform	Gruppengröße	SWS	Workload[h]	LP	
Vorlesung		2	30 P / 45 S	2,5	P = Präsenzstudium
Übungen		2	30 P / 75 S	3,5	S = Selbststudium

Benotete Prüfungsleistungen

Mündliche Prüfung

Unbenotete Studienleistungen (für Zulassung zur Modulprüfung erforderlich)

(i) Bearbeitung regelmäßig erscheinender Übungsblätter. Die Bearbeitung kann in Gruppen von bis zu drei Studierenden erfolgen. Für 60% der Aufgabenblätter müssen jeweils 50% der Punkte erreicht werden. (ii) Erfolgreiche, individuelle Bearbeitung eines Programmierprojekts. Das Projektergebnis muss präsentiert werden. (iii) Ausarbeitung und Halten eines Referats.

Medieneinsatz

Exponate des Arithmeums

Literatur

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

BA-INF 127 Angewandte Mathematik: Numerik

Workload	Umfang	Dauer	Turnus
180 h	6 LP	1 Semester	jährlich
Modulverantwortliche*r	Lehrende		
Prof. Dr. Reinhard Klein	Prof. Dr. Reinhard Klein		
Studiengang	Modus	Studiensemester	
B. Sc. Cyber Security	Wahlpflicht	3.	

Lernziele: fachliche Kompetenzen

- Erlernen fortgeschrittener mathematischer Modelle
- Einsatz der Modelle in konkreten Anwendungen
- Anwendung von numerischen Werkzeugen auf informatische Probleme

Lernziele: Schlüsselkompetenzen

- Sozialkompetenz (insb. Transfer- und Teamfähigkeit)
- Selbstkompetenz (insb. Leistungsbereitschaft, fachliche Flexibilität und Kreativität)

Inhalte

- Singulärwertzerlegung (Singular Value Decomposition)
- QR-Faktorisierung
- Eigenwertprobleme
- Kondition und Stabilität
- Floating Point Arithmetik
- Lineare Gleichungssysteme
- Differenzierbare Funktionen
- Differenzierbare Abbildungen
- Nichtlineare Gleichungen

Teilnahmevoraussetzungen

Erforderlich:

solide Kenntnisse in Linearer Algebra und Analysis

Veranstaltungen

Lehrform	Gruppengröße	SWS	Workload[h]	LP	
Vorlesung		2	30 P / 45 S	2,5	P = Präsenzstudium
Übungen		2	30 P / 75 S	3,5	S = Selbststudium

Benotete Prüfungsleistungen

Schriftliche Prüfung

Unbenotete Studienleistungen (für Zulassung zur Modulprüfung erforderlich)

Bearbeitung regelmäßig erscheinender Übungsblätter. Die Bearbeitung kann in Gruppen von bis zu drei Studierenden erfolgen. Insgesamt müssen 50% der Punkte erreicht werden. Für 70% der Aufgabenblätter müssen jeweils 50% der Punkte erreicht werden. Die Aufgaben sind aufgeteilt in theoretische und praktische Aufgaben, und die zu erzielenden Punkte gelten separat für beide Teile. Jede*r Studierende muss einmal die Lösung einer Aufgabe vorstellen.

Literatur

- begleitendes Vorlesungsskript
- Königsberger, Analysis II, Springer Berlin Heidelberg; Auflage: 5., korr. Aufl. (8. März 2004)
- Lloyd N. Trefethen und David Bau II, Numerical Linear Algebra, Society for Industrial and Applied Mathematics (1. Juni 1997)
- Martin Hanke-Bourgeois, Grundlagen der numerischen Mathematik, Vieweg+Teubner Verlag; Auflage: 3., akt. Aufl. 2009 (11. Dezember 2008)

BA-INF 131 Intelligente Sehsysteme

Workload	Umfang	Dauer	Turnus
180 h	6 LP	1 Semester	jährlich
Modulverantwortliche*r	Lehrende		
Prof. Dr. Wolfgang Koch	Prof. Dr. Wolfgang Koch, Claudia Bender, Dr. Felix Govaers		
Studiengang	Modus	Studiensemester	
B. Sc. Cyber Security	Wahlpflicht	3. oder 5.	

Lernziele: fachliche Kompetenzen

Studierende lernen grundlegende Paradigmen und Methoden von Intelligenen Sehsystemen kennen. Sie erwerben die Fähigkeit,

eine gegebene Aufgabenstellung mit geeigneten Modellierungsund Interpretationsmethoden darstellen und lösen zu können.

Lernziele: Schlüsselkompetenzen

Studierende erwerben die Fähigkeiten, die Problemstellungen von Aufgaben zu erkennen und lösungsorientiert zu formulieren sowie die Lösungen und erstellten Programme schriftlich zu dokumentieren, mündlich zu präsentieren und kontrovers zu diskutieren.

Inhalte

Methoden zur Wissenrepräsentation und Inferenz, Geometrische Modellierung, Merkmalerkennung, Interpretationsstrategien, Anwendungen.

Teilnahmevoraussetzungen

keine

Veranstaltungen

Lehrform	Gruppengröße	SWS	Workload[h]	LP	
Vorlesung		2	30 P / 45 S	2,5	P = Präsenzstudium S = Selbststudium
Übungen		2	30 P / 75 S	3,5	

Benotete Prüfungsleistungen

Schriftliche Prüfung

Unbenotete Studienleistungen (für Zulassung zur Modulprüfung erforderlich)

Bearbeitung regelmäßig erscheinender Übungsblätter. Die Bearbeitung kann in Gruppen von bis zu drei Studierenden erfolgen. Insgesamt müssen 50% der Punkte erreicht werden. Jede*r Studierende muss zweimal die Lösung einer Aufgabe vorstellen. Die erste Vorstellung muss für eines der ersten fünf Übungsblätter erfolgen, also bis zum Ende der sechsten Vorlesungswoche des Moduls. Die zweite Vorstellung muss für eines der nächsten fünf Übungsblätter erfolgen, also bis zum Ende der elften Vorlesungswoche des Moduls.

Literatur

- Simon J. D. Prince: Computer Vision: Models, Learning, and Inference. Cambridge University Press, 2012.
- Rafael C. Gonzalez, Richard E. Woods: Digital Image Processing. 3rd Ed. Prentice Hall International, 2007.
- Klaus Tönnies: Grundlagen der Bildverarbeitung, Pearson Studium, 2005.

BA-INF 132 Grundlagen der Robotik

Workload	Umfang	Dauer	Turnus
180 h	6 LP	1 Semester	jährlich
Modulverantwortliche*r	Lehrende		
Prof. Dr. Sven Behnke	Prof. Dr. Sven Behnke, Dr. Nils Goerke		
Studiengang	Modus	Studiensemester	
B. Sc. Cyber Security	Wahlpflicht	3. oder 5.	

Lernziele: fachliche Kompetenzen

Verständnis des wesentlichen Paradigmen und Grundkonzepte der Robotik. Kennenlernen typischer Datenstrukturen und Algorithmen. Praktische Erfahrungen bei der Entwicklung und Anwendung von Robotik-Methoden.

Lernziele: Schlüsselkompetenzen

integrativ vermittelte Schlüsselkompetenzen:

Kommunikative Kompetenzen (angemessene mündl. und schriftl. Präsentation von Lösungen), soziale Kompetenzen (Teamfähigkeit beim Problemlösen in Kleingruppen, Diskussion und Bewertung unterschiedlicher Lösungsansätze), Selbstkompetenzen (Analysefähigkeit und Kreativität beim Problemlösen, konstruktiver Umgang mit Kritik, Leistungsbereitschaft, Zielstrebigkeit)

Inhalte

Robotersensorik und -aktorik, Regelungstechnik, Koordinatensysteme und Transformationen, Roboterarmkinematik, Kinematik mobiler Roboter, Pfadintegration, Selbstlokalisierung und Pfadplanung.

Teilnahmevoraussetzungen

keine

Veranstaltungen

Lehrform	Gruppengröße	SWS	Workload[h]	LP	
Vorlesung		2	30 P / 45 S	2,5	P = Präsenzstudium
Übungen		2	30 P / 75 S	3,5	S = Selbststudium

Benotete Prüfungsleistungen

Schriftliche Prüfung

Unbenotete Studienleistungen (für Zulassung zur Modulprüfung erforderlich)

Bearbeitung regelmäßig erscheinender Übungsblätter. Die Bearbeitung kann in Gruppen von bis zu zwei Studierenden erfolgen. Insgesamt müssen 50% der Punkte erreicht werden.

Literatur

- P. Corke: Robotics, Vision and Control, Springer, 2011
- B. Siciliano and O. Khatib (Herausgeber): Handbook of Robotics, Springer, 2008
- R. Siegwart and I.R. Nourbakhsh: Introduction to Autonomous Mobile Robots, MIT-Press, 2004
- B. Siciliano, L. Sciavicco, L. Villani: Robotics: Modelling, Planning and Control, Springer, 2008
- H. Choset, S. Hutchinson, G. Kantor: Principles of Robot Motion: Theory, Algorithms and Implementations, MIT-Press, 2005

BA-INF 137 Einführung in die Sensordatenfusion

Workload	Umfang	Dauer	Turnus
180 h	6 LP	1 Semester	jährlich
Modulverantwortliche*r	Lehrende		
PD Dr. Wolfgang Koch	PD Dr. Wolfgang Koch		
Studiengang	Modus	Studiensemester	
B. Sc. Cyber Security	Wahlpflicht	4. oder 6.	

Lernziele: fachliche Kompetenzen

Sensordatenfusion verknüpft unvollständige und fehlerhafte, aber einander ergänzende Messdaten, so dass ein zugrundeliegendes Phänomen der Realität besser verstanden wird. Die Vorlesung vermittelt dazu benötigten Grundlagen, die anhand vieler Anwendungsbeispiele veranschaulicht werden. Die Studierenden lernen dadurch wichtiges Handwerkszeug der Schätz- und Filterungstheorie, der Simulation und Performance-Evaluation kennen, die auch in anderen Gebieten der Informatik nützlich sind. Die benötigten Grundbegriffe der Stochastik werden in der Vorlesung eingeführt. Freude an mathematischer Einsicht und Geschick bei der Implementierung von Algorithmen sind Voraussetzung. Geeignete Studierende können im 5. Semester im Fraunhofer FKIE an Projekten mitwirken und/oder ihre Bachelor-Arbeit schreiben. Im Master-Studiengang kann das Thema weiter vertieft werden.

Lernziele: Schlüsselkompetenzen

Umgang mit Wahrscheinlichkeitsdichten, Ableitung von Algorithmen, Anwenden der Linearen Algebra auf Probleme der Wahrscheinlichkeitsrechnung.

Inhalte

diskrete und stetige Zufallsvariablen, Wahrscheinlichkeitsdichtefunktionen, Modellierung von unsicherem Wissen, Bayes-Formalismus, Gauß-Dichten und Gauß-Summen, Chi-Quadrat-Test, Kalman Filter

Teilnahmevoraussetzungen

Empfohlen:

alle Module aus folgender Liste:

BA-INF 021 – Lineare Algebra

BA-INF 022 – Analysis

Veranstaltungen

Lehrform	Gruppengröße	SWS	Workload[h]	LP	
Vorlesung		2	30 P / 45 S	2,5	P = Präsenzstudium
Übungen		2	30 P / 75 S	3,5	S = Selbststudium

Benotete Prüfungsleistungen

Mündliche Prüfung

Unbenotete Studienleistungen (für Zulassung zur Modulprüfung erforderlich)

Es sind 50% der maximal erreichbaren Punkte in den praktischen Programmierübungen notwendig. Es gibt eine praktische Übungsaufgabe, die eine Arbeitslast von ca. 10h ist. Die Abgabe der programmierten Lösung geschieht einzeln oder in Gruppenarbeit von bis zu drei Studierenden. Es werden insgesamt 10 Punkte vergeben, von denen 50% erreicht wurden, wenn das Kalman Filter mit Retrodiktion in lauffähiger und konsistenter Weise eigenständig programmiert wurde.

Literatur

W. Koch: "Tracking and Sensor Data Fusion: Methodological Framework and Selected Applications", Springer, 2014.

BA-INF 139 Tutorenschulung/ Vermittlung von Informatikinhalt

Workload	Umfang	Dauer	Turnus
180 h	6 LP	1 Semester	jährlich
Modulverantwortliche*r	Lehrende		
Dr. Dieter Engbring	Dr. Dieter Engbring		
Studiengang	Modus	Studiensemester	
B. Sc. Cyber Security	Wahlpflicht	5. oder 6.	

Lernziele: fachliche Kompetenzen

Wiederholung und Vertiefung der in den Übungsgruppen zu vermittelnden Inhalte

Lernziele: Schlüsselkompetenzen

Sozialkompetenzen: Kommunikationsfähigkeit, Präsentation (eigener) Lösungsansätze

Methodenkompetenzen: (didaktische) Analyse und Aufbereitung von Gegenständen der Informatik, Vermittlung informatischer Inhalte, Korrektur fehlerhafter Lösungen, Identifikation von Lernschwierigkeiten

Individualkompetenzen: Reflexionsfähigkeit, Kritikfähigkeit

Inhalte

- Merkmale guten Unterrichts
- Lernpsychologische Grundlagen des Lernens
- Fundamentale Ideen der Informatik/great Principles/
- Computational Thinking
- Leistungsmessung und -bewertung (Aufgabenkorrektur)
- Gruppenarbeit anleiten und begleiten
- "Übungsaufgaben als Lerngelegenheiten"
- Übungsaufgaben richtig besprechen/Umgang mit (typischen) Fehlern
- Interventionsmechanismen
- Entwicklung von Beobachtungsbögen
- Beobachtung anderer Tutorien/kollegiale Beratung

Teilnahmevoraussetzungen

keine

Veranstaltungen

Lehrform	Gruppengröße	SWS	Workload[h]	LP
Vorbereitungs- workshop	12	2	30 P / 30 S	2
Vorbereitung der Übungsgruppen		0	90 S	3
Hospitationen / Reflexionen		1	15 P / 15 S	1

P = Präsenzstudium
S = Selbststudium

Benotete Prüfungsleistungen

Keine

Unbenotete Studienleistungen (für Zulassung zur Modulprüfung erforderlich)

Aktive Seminarteilnahme; Hospitation von Tutorien anderer; schriftliche Aufbereitung und Ausarbeitung von Beobachtungen aus den anderen Tutorien; Reflexion der Lehre; Bilanz- und Perspektivgespräch. Zum Bestehen des Moduls sind den Anforderungen genügende Studienleistungen erforderlich.

BA-INF 144 Algorithmische Grundlagen des maschinellen Lernens

Workload	Umfang	Dauer	Turnus
270 h	9 LP	1 Semester	mind. alle 2 Jahre
Modulverantwortliche*r	Lehrende		
Prof. Dr. Thomas Kesselheim	Prof. Dr. Anne Driemel, Prof. Dr. Thomas Kesselheim, PD Dr. Elmar Langetepe, Prof. Dr. Heiko Röglin		
Studiengang	Modus	Studiensemester	
B. Sc. Cyber Security	Wahlpflicht	4. oder 6.	

Lernziele: fachliche Kompetenzen

- Kenntnis theoretischer Modelle im maschinellen Lernen
- Entwurf effizienter Lernalgorithmen und Analyse ihrer Eigenschaften
- Grenzen der Lernbarkeit

Lernziele: Schlüsselkompetenzen

Präsentation eigener Lösungsansätze und zielorientierte Diskussion im Rahmen der Übung

Inhalte

- Grundlegende Lernalgorithmen
- Klassifizierung und Regression
- Overfitting und Regularisierung
- PAC-Learning und VC-Dimension
- Clustering

Teilnahmevoraussetzungen

keine

Veranstaltungen

Lehrform	Gruppengröße	SWS	Workload[h]	LP	
Vorlesung		4	60 P / 105 S	5,5	P = Präsenzstudium
Übungen		2	30 P / 75 S	3,5	S = Selbststudium

Benotete Prüfungsleistungen

Mündliche Prüfung

Unbenotete Studienleistungen (für Zulassung zur Modulprüfung erforderlich)

Bearbeitung regelmäßig erscheinender Übungsblätter. Die Bearbeitung kann in Gruppen von bis zu drei Studierenden erfolgen. Insgesamt müssen 25% der Punkte erreicht werden. Jede*r Studierende muss einmal die Lösung einer Aufgabe vorstellen.

Literatur

Shai Shalev-Schwartz, Shai Ben-David. Understanding Machine Learning – From Theory to Algorithms. Cambridge University Press. ISBN 978-1-107-05713-5

BA-INF 149 Graphenalgorithmen

Workload	Umfang	Dauer	Turnus
180 h	6 LP	1 Semester	mind. alle 2 Jahre
Modulverantwortliche*r	Lehrende		
Prof. Dr. Petra Mutzel	Prof. Dr. Petra Mutzel		
Studiengang	Modus	Studiensemester	
B. Sc. Cyber Security	Wahlpflicht	4. oder 6.	

Lernziele: fachliche Kompetenzen

Entwurf und Analyse von Graphenalgorithmien; Modellierung und Lösung von vielfältigen Praxisproblemen, die mittels Graphenalgorithmien gelöst werden können; durch das Kennenlernen vieler verschiedener Graphenprobleme sowie die möglichen Herangehensweisen zur Lösung wird die Problemlösungskompetenz in der Praxis gestärkt.

Lernziele: Schlüsselkompetenzen

Sozialkompetenz (Kommunikationsfähigkeit, Präsentation eigener Lösungsansätze und zielorientierte Diskussion im Gruppenrahmen, Teamfähigkeit), Methodenkompetenz (Analysefähigkeit, Abstraktes Denken, Führen von Beweisen), Individualkompetenz (Leistungs- und Lernbereitschaft, Kreativität, Ausdauer).

Inhalte

Viele Anwendungsprobleme aus der Praxis können als Graphenprobleme formuliert werden. Wir studieren sowohl polynomielle Algorithmen als auch NP-schwierige Graphprobleme (z.B. Netzwerkdesignprobleme, Färbungsprobleme). Dabei betrachten wir sowohl spezielle Algorithmen als auch allgemeinere Methoden, wie z.B. Fixed-Parameter-Algorithmen und Methoden für Graphen mit kleiner Baumweite. Insbesondere studieren wir auch moderne aktuelle Problemvarianten, wie z.B. "Big Data" Algorithmen (z.B. Parallele und Datenstrom-Algorithmen) oder Probleme auf temporalen Graphen bei denen die Kanten nur zu gewissen Zeitpunkten vorhanden sind oder sich mit der Zeit ändern.

Teilnahmevoraussetzungen

Erforderlich:

BA-INF 032 - Algorithmen und Berechnungskomplexität I

Veranstaltungen

Lehrform	Gruppengröße	SWS	Workload[h]	LP	
Vorlesung		2	30 P / 45 S	2,5	P = Präsenzstudium
Übungen		2	30 P / 75 S	3,5	S = Selbststudium

Benotete Prüfungsleistungen

Mündliche Prüfung

Unbenotete Studienleistungen (für Zulassung zur Modulprüfung erforderlich)

Bearbeitung regelmäßig erscheinender Übungsblätter. Die Bearbeitung kann in Gruppen mit bis zu drei Studierenden erfolgen. Für die Zulassung zur Prüfung müssen 50% der Übungspunkte erreicht werden und jede*r Studierende muss zweimal die Lösung einer Aufgabe korrekt vorstellen. Jede*r Teilnehmende kreuzt zu Beginn jeder Übungsstunde in einer Liste an, welche Teilaufgaben er/sie erfolgreich bearbeitet hat und für die er/sie sich die Punkte anrechnen lassen möchte. Der/die Übungsleiter*in wählt dann jeweils eine*n Teilnehmende*n zur Präsentation einer (Teil-)aufgabe aus. Für komplexere Aufgaben ist eine vorherige schriftliche Abgabe vorgesehen. Die Punktzahl ergibt sich bei den schriftlichen Abgaben durch die erreichten Punkte der angekreuzten Aufgaben und bei den mündlichen Abgaben durch die Maximalpunktzahl der angekreuzten Aufgaben.

BA-INF 150 Einführung in die Data Science

Workload	Umfang	Dauer	Turnus
180 h	6 LP	1 Semester	jährlich
Modulverantwortliche*r	Lehrende		
Prof. Dr. Elena Demidova	Prof. Dr. Elena Demidova		
Studiengang	Modus	Studiensemester	
B. Sc. Cyber Security	Wahlpflicht	5.	

Lernziele: fachliche Kompetenzen

Dieses Modul konzentriert sich auf den gesamten datenwissenschaftlichen Prozess. Dieser Prozess umfasst die Integration und Bereinigung von Daten, die explorative Datenanalyse, die Datenmodellierung unter Verwendung statistischer und maschineller Lernmethoden sowie die Modellbewertung. Das Modul widmet besondere Aufmerksamkeit der Anwendung relevanter statistischer Methoden auf die datenwissenschaftlichen Workflows. Weiterhin wird die Analyse ausgewählter Datentypen berücksichtigt (z. B. Zeitreihen, Textdaten). Praktische Beispiele werden mit den relevanten Programmiersprachen (bspw. R) demonstriert.

Am Ende des Moduls sind die Studierenden in der Lage, die geeigneten datenwissenschaftlichen Methoden für bestimmte Datentypen auszuwählen und relevante statistische Verfahren und Algorithmen des maschinellen Lernens im Rahmen der Datenanalyse korrekt anzuwenden. Darüber hinaus erwerben die Studierenden praktische Kenntnisse in der Datenanalyse in den entsprechenden Programmiersprachen.

Lernziele: Schlüsselkompetenzen

- Sozialkompetenzen: Kommunikationsfähigkeit, Präsentation eigener Lösungsansätze.
- Individualkompetenzen: Fähigkeit, Probleme zu analysieren und zu lösen.

Inhalte

Statistische Methoden und Programmiersprachen für Data Science, Data-Science-Workflow, explorative Datenanalyse, Analyse spezifischer Datentypen (z. B. Zeitreihen, Textdaten), Auswahl und Bewertung von Modellen des maschinellen Lernens für Data Science Anwendungen.

Teilnahmevoraussetzungen

Empfohlen:

- BA-INF 035 - Datenzentrierte Informatik
- Programmierkenntnisse

Veranstaltungen

Lehrform	Gruppengröße	SWS	Workload[h]	LP	
Vorlesung		2	30 P / 45 S	2,5	P = Präsenzstudium
Übungen		2	30 P / 75 S	3,5	S = Selbststudium

Benotete Prüfungsleistungen

Schriftliche Prüfung

Unbenotete Studienleistungen (für Zulassung zur Modulprüfung erforderlich)

Bearbeitung regelmäßig erscheinender Übungsblätter. Die Bearbeitung kann in Gruppen von, abhängig von der Gesamt-Teilnehmerzahl, bis zu drei, vier oder fünf Studierenden erfolgen. Insgesamt müssen 50% der Punkte erreicht werden. Für 80% der Aufgabenblätter müssen jeweils 40% der Punkte erreicht werden. Jede*r Studierende muss einmal die Lösung einer Aufgabe vorstellen.

Literatur

Ausgewählte Kapitel aus:

- Statistics in a Nutshell, 2nd Edition, A Desktop Quick Reference, Sarah Boslaugh, O'Reilly Media, 2012
- R for Data Science (by Garrett Grolemund and Hadley Wickham) O'Reilly Media, 2017

Weitere Literaturhinweise werden während der Vorlesung bekannt gegeben.

BA-INF 153 Einführung in Deep Learning für Visual Computing

Workload	Umfang	Dauer	Turnus
180 h	6 LP	1 Semester	jährlich
Modulverantwortliche*r	Lehrende		
Prof. Dr. Reinhard Klein	Prof. Dr. Reinhard Klein, Nils Wandel		
Studiengang	Modus	Studiensemester	
B. Sc. Cyber Security	Wahlpflicht	6.	

Lernziele: fachliche Kompetenzen

Die Studierenden sollen in die Mathematik und die Theorie tiefer neuronaler Netze (Deep Neural Networks) eingeführt werden und das Gelernte in verschiedenen Anwendungen in Computer Vision und anderen Themen in KI einsetzen.

Lernziele: Schlüsselkompetenzen

Produktives Arbeiten in kleinen Teams, Entwicklung und Realisierung von individuellen Ansätzen und Lösungen, kritische Reflexion von verschiedenen Methoden, Diskussion in Gruppen.

Inhalte

Methoden des Deep Learning werden mit großem Erfolg sowohl in der Forschung als auch in Anwendungen eingesetzt und sind aus einer ganzen Reihe von Bereichen und Disziplinen, wie z.B. Computer Graphik, Computer Vision, Sprachverarbeitung, Robotik, usw., nicht mehr wegzudenken. Zu Beginn des Kurses werden zunächst notwendige mathematische Grundlagen, wie beispielsweise Optimierung mit Gradienten Abstieg oder Parameterschätzung, besprochen. Darauf aufbauend wird die Theorie der Feed Forward Networks, Convolutional Neural Networks, Autoencoder, Recurrent Networks und Transformer Networks vorgestellt. In den begleitenden Übungen wird besprochen und geübt, wie man sein eigenes Netzwerk für verschiedene Anwendungen aus dem Bereich Visual Computing, wie z.B. Objekterkennung oder Bildsegmentierung, entwerfen, implementieren und trainieren kann.

Teilnahmevoraussetzungen

Erforderlich:

Grundlegende Kenntnisse in:

- Lineare Algebra
- Analysis
- Angewandte Mathematik: Numerik oder Stochastik (wir empfehlen beide Veranstaltungen zu diesen Themen zu hören)
- Programmieren (z.B. Python oder Matlab oder C++)

Veranstaltungen

Lehrform	Gruppengröße	SWS	Workload[h]	LP	
Vorlesung		2	30 P / 45 S	2,5	P = Präsenzstudium S = Selbststudium
Übungen		2	30 P / 75 S	3,5	

Benotete Prüfungsleistungen

Schriftliche Prüfung

Unbenotete Studienleistungen (für Zulassung zur Modulprüfung erforderlich)

Bearbeitung regelmäßig erscheinender Übungsblätter. Die Bearbeitung kann in Gruppen von bis zu vier Studierenden erfolgen. Insgesamt müssen 50% der Punkte erreicht werden. Die Aufgaben sind aufgeteilt in theoretische und praktische Aufgaben, und die zu erzielenden Punkte gelten separat für beide Teile. Jede*r Studierende muss einmal die Lösung einer Aufgabe vorstellen.

Literatur

Goodfellow, I., Bengio, Y. and Courville, A., 2016. Deep learning. MIT press.

Weitere Literatur speziell zu Grundlagen

- Bishop, Christopher M., and Nasser M. Nasrabadi. Pattern recognition and machine learning. Vol. 4, no. 4. New York: springer, 2006.
 - Deisenroth, Marc Peter, A. Aldo Faisal, and Cheng Soon Ong. Mathematics for machine learning. Cambridge University Press, 2020.
-

BA-INF 154 Medizinische Bildanalyse

Workload	Umfang	Dauer	Turnus
180 h	6 LP	1 Semester	mind. alle 2 Jahre
Modulverantwortliche*r	Lehrende		
Prof. Dr. Thomas Schultz	Prof. Dr. Thomas Schultz		
Studiengang	Modus	Studiensemester	
B. Sc. Cyber Security	Wahlpflicht	5.	

Lernziele: fachliche Kompetenzen

Verständnis der wichtigsten Bildgebungsmodalitäten in der Medizin. Verständnis grundlegender Algorithmen zur Filterung, Registrierung, Segmentierung, Visualisierung und Klassifikation medizinischer Bilder. Praktische Erfahrung mit der Implementierung und Anwendung dieser Algorithmen.

Lernziele: Schlüsselkompetenzen

Sozialkompetenzen (Kooperations- und Kommunikationsfähigkeit, mündliche und schriftliche Ausdrucksfähigkeit), Methodenkompetenzen (Problemlösungsfähigkeit, selbstständiges Arbeiten, analytische Fähigkeiten), Selbstkompetenzen (Leistungsbereitschaft, Kreativität, Selbstmanagement)

Inhalte

Grundlagen von Röntgenbildgebung, CT, MRT, PET, Ultraschall, OCT. Lineare und nichtlineare Bildfilter. Affine und deformierbare Bildregistrierung. Unterschiedliche Strategien zur Bildsegmentierung (Schwellenwerte, Wasserscheidentransformation, Energieminimierungsansätze, Formmodelle). Beschreibung von Bildinhalten durch Merkmalsvektoren und Klassifikation mit maschinellem Lernen. Grundlagen von Deep-Learning-Ansätzen.

Teilnahmevoraussetzungen

Empfohlen:

- BA-INF 021 – Lineare Algebra
- BA-INF 022 – Analysis
- BA-INF 127 – Angewandte Mathematik: Numerik oder BA-INF 127 - Angewandte Mathematik: Stochastik

Veranstaltungen

Lehrform	Gruppengröße	SWS	Workload[h]	LP	
Vorlesung		2	30 P / 45 S	2,5	P = Präsenzstudium
Übungen		2	30 P / 75 S	3,5	S = Selbststudium

Benotete Prüfungsleistungen

Schriftliche Prüfung

Unbenotete Studienleistungen (für Zulassung zur Modulprüfung erforderlich)

Bearbeitung regelmäßig erscheinender Übungsblätter. Die Bearbeitung kann in Gruppen von bis zu drei Studierenden erfolgen. Insgesamt müssen 50% der Punkte erreicht werden. Jede*r Studierende muss einmal die Lösung einer Aufgabe vorstellen.

Medieneinsatz

Folien, Tafel

Literatur

- B. Preim, C. Botha: Visual Computing for Medicine. Theory, Algorithms, and Applications. 2nd edition, Morgan Kaufmann, 2014
- I.H. Bankman (Ed.): Handbook of Medical Image Processing and Analysis. Academic Press, 2009

BA-INF 157 Introduction to Machine Learning

Workload	Umfang	Dauer	Turnus
180 h	6 LP	1 Semester	jährlich
Modulverantwortliche*r	Lehrende		
Prof. Dr. Stefan Wrobel	Prof. Dr. Stefan Wrobel, Dr. Tamas Horvath		
Studiengang	Modus	Studiensemester	
B. Sc. Cyber Security	Wahlpflicht		

Lernziele: fachliche Kompetenzen

In this module the students will learn, implement and practice the most important algorithms of machine learning. The module concentrates on the core task of predictive learning from examples and on agent learning, and teaches the main classes of algorithms for these tasks. At the end of the module, students will be capable of choosing appropriate methods and systems for particular predictive learning applications and use them to arrive at convincing results, and will know where to start whenever adaptation or further development of algorithms and systems is necessary.

Lernziele: Schlüsselkompetenzen

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

Inhalte

Types of learning tasks, most important non-parametric and parametric methods for supervised learning (e.g., concept learning as search in ordered hypothesis spaces, decision tree learning, probabilistic approaches, neural networks, linear methods, kernel methods, probabilistic approaches), reinforcement learning, and hypothesis evaluation.

Teilnahmevoraussetzungen

keine

Bemerkungen

Dieses Modul wird nicht mehr angeboten. Es wird durch BA-INF 160 Grundlagen der Künstlichen Intelligenz I ersetzt. Im Sommersemester 2025 werden für diejenigen, die nicht BA-INF 160 absolvieren, noch Prüfungstermine für BA-INF 157 angeboten.

Veranstaltungen

Lehrform	Gruppengröße	SWS	Workload[h]	LP	
Vorlesung		2	30 P / 45 S	2,5	P = Präsenzstudium
Übungen		2	30 P / 75 S	3,5	S = Selbststudium

Benotete Prüfungsleistungen

Schriftliche Prüfung

Unbenotete Studienleistungen (für Zulassung zur Modulprüfung erforderlich)

Bearbeitung regelmäßig erscheinender Übungsblätter. Die Bearbeitung kann in Gruppen von bis zu fünf Studierenden erfolgen. Insgesamt müssen 50% der Punkte erreicht werden. Jede*r Studierende muss einmal die Lösung einer Aufgabe vorstellen.

Literatur

- Christopher M. Bishop: Pattern Recognition and Machine Learning. Second Edition, Springer, 2007.
- Ian Goodfellow, Yoshua Bengio, and Aaron Courville: Deep Learning. MIT Press, 2016.
- Trevor Hastie, Robert Tibshirani, Jerome Friedman: The Elements of Statistical Learning. Data Mining, Inference, and Prediction. Second Edition, Springer Series in Statistics, 2009.
- Tom Mitchell: Machine Learning. McGraw-hill New York, 1997.

BA-INF 159 Agile Software Development

Workload	Umfang	Dauer	Turnus
180 h	6 LP	1 Semester	jährlich
Modulverantwortliche*r	Lehrende		
Prof. Dr. Stephan Jonas	Prof. Dr. Stephan Jonas, Dr. Lara Marie Reimer		
Studiengang	Modus	Studiensemester	
B. Sc. Cyber Security	Wahlpflicht	6.	

Lernziele: fachliche Kompetenzen

Die Studierenden sollen Softwareprojekte mit agilen Methoden umsetzen können. Besonderer Fokus liegt dabei auf der Zusammenarbeit im Team und der regelmäßigen Kommunikation mit Stakeholdern des Projekts. Die Studierenden sollen in der Lage sein, Methoden, die in engem Zusammenhang mit agilen Methoden stehen (wie UI Prototyping, Code Reviews, CI/CD) selbstständig durchzuführen und in den Softwareentwicklungsprozess zu integrieren.

Lernziele: Schlüsselkompetenzen

- Soziale Kompetenzen: Kommunikation und Zusammenarbeit im Team und mit Projekt-Stakeholdern, Teamfähigkeit
- Selbstkompetenzen: Arbeits- und Zeitplanung, Umgang mit Feedback und Veränderungen der Anforderungen

Inhalte

- Agile Methoden, insbesondere Scrum und Kanban
- Kommunikation und Kollaboration
- Schätzung und Terminplanung
- Modellierung von Software-Lebenszyklen
- Entwurf von Benutzeroberflächen und Prototyping
- Software-Konfigurationsmanagement
- Branch-, Merge- und Code-Review-Management
- Freigabe- und Build-Management
- Continuous Integration und Tests
- Continuous Delivery und Feedback-Management

Teilnahmevoraussetzungen

Empfohlen:

BA-INF 036 - Softwaretechnologie

Veranstaltungen

Lehrform	Gruppengröße	SWS	Workload[h]	LP	
Vorlesung		2	30 P / 60 S	3	P = Präsenzstudium S = Selbststudium
Übungen		1	15 P / 15 S	1	
Praktikum	3-5	1	15 P / 45 S	2	

Benotete Prüfungsleistungen

Mündliche Prüfung

Unbenotete Studienleistungen (für Zulassung zur Modulprüfung erforderlich)

Erfolgreiche Bearbeitung eines Programmierprojekts. Die Bearbeitung kann in Gruppen von drei bis fünf Studierenden erfolgen. Das Projektergebnis muss präsentiert werden.

Medieneinsatz

Projektion, Videos, interaktive Übungen

Die Vorlesungen und Übungen basieren auf Interaktion. Wir erwarten eine aktive Teilnahme!

Zur Teilnahme an den Übungen wird ein mobiles Endgerät (Laptop/Tablet) benötigt, bitte bringen Sie dies entsprechend mit.

Literatur

Bernd Bruegge, Allen H. Dutoit: Object-Oriented Software Engineering: Using UML, Patterns, and Java. 2nd Edition Prentice Hall, September 2003

BA-INF 160 Grundlagen der Künstlichen Intelligenz 1

Workload	Umfang	Dauer	Turnus
180 h	6 LP	1 Semester	jährlich
Modulverantwortliche*r	Lehrende		
Prof. Dr. Stefan Wrobel	Dr. Tamas Horvath, Dr. Florian Seiffarth		
Studiengang	Modus	Studiensemester	
B. Sc. Cyber Security	Wahlpflicht	2. oder 4.	

Lernziele: fachliche Kompetenzen

Dieses Modul ist dem maschinellen Lernen gewidmet, einem der wichtigsten Bereiche der künstlichen Intelligenz. Die Studierenden lernen, implementieren und üben die wichtigsten Algorithmen des maschinellen Lernens. Das Modul konzentriert sich auf die Kernaufgaben des prädiktiven Lernens aus Beispielen und des Agentenlernens und lehrt die wichtigsten Klassen von Algorithmen für diese Aufgaben. Am Ende des Moduls sind die Studierenden in der Lage, geeignete Methoden und Systeme für spezifische Anwendungen des prädiktiven Lernens auszuwählen, einzusetzen und, wenn nötig, anzupassen oder weiterzuentwickeln.

Lernziele: Schlüsselkompetenzen

Studierende erwerben die Fähigkeiten, Problemstellungen zu erkennen und lösungsorientiert zu formulieren sowie die Lösungen und erstellten Programme schriftlich zu dokumentieren, mündlich zu präsentieren und kontrovers zu diskutieren.

Inhalte

Verschiedene Arten von Lernproblemen, wichtige nicht-parametrische und parametrische Methoden für überwachtes Lernen (z.B., Konzeptlernen als Suche in geordneten Hypothesenräumen, lernen von Entscheidungsbäumen, probabilistische Ansätze, Kernel-Methoden, lineare und logistische Regression, gradient descent, neuronale Netze, deep learning), Lerntheorie.

Teilnahmevoraussetzungen

keine

Bemerkungen

Das Modul kann nicht mit BA-INF 110 oder BA-INF 157 kombiniert werden.

Veranstaltungen

Lehrform	Gruppengröße	SWS	Workload[h]	LP	
Vorlesung		2	30 P / 45 S	2,5	P = Präsenzstudium
Übungen		2	30 P / 75 S	3,5	S = Selbststudium

Benotete Prüfungsleistungen

Schriftliche Prüfung

Unbenotete Studienleistungen (für Zulassung zur Modulprüfung erforderlich)

Bearbeitung regelmäßig erscheinender Übungsblätter. Die Bearbeitung kann in Gruppen von bis zu vier Studierenden erfolgen. Insgesamt müssen 50% der Punkte erreicht werden. Jede*r Studierende muss zweimal die Lösung einer Aufgabe vorstellen. Die erste Vorstellung muss für Aufgaben von einem der ersten fünf Übungsblätter erfolgen, in den ersten sechs Wochen der Vorlesungszeit. Die zweite Vorstellung muss für eines der folgenden fünf Übungsblätter erfolgen, innerhalb von zwölf Wochen nach Anfang der Vorlesungszeit.

Literatur

- Christopher M. Bishop: Pattern Recognition and Machine Learning. Second Edition, Springer, 2007.
 - Ian Goodfellow, Yoshoua Bengio, and Aaron Courville: Deep Learning. MIT Press, 2016.
 - Trevor Hastie, Robert Tibshirani, Jerome Friedman: The Elements of Statistical Learning. Data Mining, Inference, and Prediction. Second Edition, Springer Series in Statistics, 2009.
 - Tom Mitchell: Machine Learning. McGraw-hill New York, 1997.
-

BA-INF 162 Webtechnologien

Workload	Umfang	Dauer	Turnus
180 h	6 LP	1 Semester	jährlich
Modulverantwortliche*r	Lehrende		
Prof. Dr. Stephan Jonas	Prof. Dr. Stephan Jonas, Marko Jovanović		
Studiengang	Modus	Studiensemester	
B. Sc. Cyber Security	Wahlpflicht	4. oder 6.	

Lernziele: fachliche Kompetenzen

Das Modul vermittelt die fachlichen Kompetenzen, um moderne Webanwendungen zu entwerfen, zu entwickeln und zu optimieren. Die Studierenden erlernen die Grundlagen von Webtechnologien wie HTML, CSS und JavaScript sowie fortgeschrittene Techniken für Frameworks, Datenbankintegration und Deployment. Das Lernziel ist es, funktionale, ästhetische und performante Webseiten zu erstellen, die aktuelle Best Practices und Sicherheitsstandards berücksichtigen.

Lernziele: Schlüsselkompetenzen

- Technologische Kompetenz: Beherrschung grundlegender Webtechnologien wie HTML, CSS, JavaScript und PHP sowie fortgeschrittener Frameworks und Tools (z. B. React, Symfony, ?).
- Problemlösungsfähigkeit: Fähigkeit, technische Anforderungen zu analysieren, geeignete Lösungen zu entwickeln und diese in funktionale Webanwendungen umzusetzen.
- Gestalterische Kompetenz: Umsetzung von ansprechendem und nutzerzentriertem Design unter Berücksichtigung von Usability und Barrierefreiheit.

Inhalte

Einführung in Webtechnologien

- Grundlagen von Webentwicklung: Client-Server-Architektur
- Aufbau und Struktur von Webseiten (HTML)
- Styling und Design mit CSS
- Interaktive Elemente und dynamische Inhalte mit JavaScript

Frontend-Entwicklung

- Einführung in JavaScript-Frameworks und Bibliotheken
- Best Practices für Barrierefreiheit
- Performance-Optimierung im Frontend

Serverseitige Entwicklung mit PHP

- Grundlagen der serverseitigen Programmierung und MVC
- Einführung in PHP: Syntax, Variablen, Schleifen, Funktionen
- Verarbeitung von HTTP-Anfragen und -Antworten, Formulare
- Sessions und Cookies
- Frameworks
- Authentifizierung und Autorisierung (Security-Komponente)
- Arbeiten mit JSON und XML für API-Kommunikation
- Grundlegender Umgang mit ORM
- Fehler- und Ausnahmebehandlung
- Deployment

Teilnahmevoraussetzungen

Erforderlich:

- BA-INF 035 - Datenzentrierte Informatik
- BA-INF 036 – Softwaretechnologie

Veranstaltungen

Lehrform	Gruppengröße	SWS	Workload[h]	LP
Vorlesung		2	30 P / 60 S	3
Übungen		1	15 P / 15 S	1
Praktikum	5	1	15 P / 45 S	2

P = Präsenzstudium
S = Selbststudium

Benotete Prüfungsleistungen

Schriftliche Prüfung

Unbenotete Studienleistungen (für Zulassung zur Modulprüfung erforderlich)

Erfolgreiche Bearbeitung eines Programmierprojekts. Die Bearbeitung kann in Gruppen von drei bis fünf Studierenden erfolgen. Das Projektergebnis muss präsentiert werden.

Medieneinsatz

Projektion, Videos, interaktive Übungen.

Die Vorlesungen und Übungen basieren auf Interaktion. Wir erwarten eine aktive Teilnahme! Zur Teilnahme an den Übungen wird ein mobiles Endgerät (Laptop/Tablet) benötigt, bitte bringen Sie dies entsprechend mit.

3 Fachgebundener Wahlpflichtbereich Cyber Security

BA-INF 136	V2Ü2	6 LP	Reaktive Sicherheit	55
BA-INF 140	V2Ü2	6 LP	Grundlagen der Mensch-Computer-Interaktion	56
BA-INF 147	V2Ü2	6 LP	Netzwerksicherheit	57
BA-INF 152	V2Ü2	6 LP	Moderne Kryptographie und ihre Anwendung	58
BA-INF 155	V2Ü2	6 LP	Angewandte Binäranalyse	59
BA-INF 156	V2Ü2	6 LP	Digitale Forensik	60
BA-INF 158	V2Ü2	6 LP	Privatsphäre erhaltende Datenanalyse	62
BA-INF 163	V2Ü2	6 LP	Klassische Kryptografie	63

BA-INF 136 Reaktive Sicherheit

Workload	Umfang	Dauer	Turnus
180 h	6 LP	1 Semester	jährlich

Modulverantwortliche*r	Lehrende
Prof. Dr. Michael Meier	Prof. Dr. Michael Meier

Studiengang	Modus	Studiensemester
B. Sc. Cyber Security	Wahlpflicht	4. oder 6.

Lernziele: fachliche Kompetenzen

Die Veranstaltung stellt dar, wo das Präventionsparadigma zu kurz greift und motiviert ergänzende Maßnahmen für eine reaktive Sicherheit. Die Hörer werden für Verwundbarkeiten informationstechnischer Systeme sowie deren Entstehung bei der Entwicklung und beim Betrieb sensibilisiert. Darüber hinaus wird in die Erkennung und Analyse vorhandener Verwundbarkeiten sowie von Schadsoftware und Angriffen eingeführt. Einschlägige ausgewählte Techniken werden erläutert und ausgewählte Werkzeuge beschrieben. Wechselwirkungen mit dem Datenschutz werden aufgezeigt.

Lernziele: Schlüsselkompetenzen

Den Studierenden sollen Ursachen für Verwundbarkeiten bewusst werden. Sie sollen Techniken zum Umgang mit verwundbaren Systemen beherrschen. Dabei sollen Ansätze von Angreifern und Schadsoftware kennengelernt werden. Die Studierenden sollen methodische Kenntnisse zur Analyse von Schadsoftware und Angriffstechniken sowie zur Erkennung von Verwundbarkeiten und deren Ausnutzung erwerben und anwenden können. Außerdem sollen die Studierenden ausgewählte Techniken zur Balance von Überwachungs- und Datenschutzinteressen kennen lernen.

Inhalte

- Präventive IT-Sicherheit
- Netzverwundbarkeiten
- Programm- und Web-Verwundbarkeiten
- Malware
- Tarntechniken und Rootkits
- Honeypots
- Intrusion Detection

Teilnahmevoraussetzungen

Empfohlen:

- BA-INF 101 – Kommunikation in Verteilten Systemen,
- BA-INF 034 – Systemnahe Programmierung und
- BA-INF 143 – IT-Sicherheit

Veranstaltungen

Lehrform	Gruppengröße	SWS	Workload[h]	LP	
Vorlesung		2	30 P / 45 S	2,5	P = Präsenzstudium
Übungen		2	30 P / 75 S	3,5	S = Selbststudium

Benotete Prüfungsleistungen

Klausurarbeit

Unbenotete Studienleistungen (für Zulassung zur Modulprüfung erforderlich)

Bearbeitung regelmäßig erscheinender Übungsblätter. Die Bearbeitung kann in Gruppen von bis zu drei Studierenden erfolgen. Insgesamt müssen 50% der Punkte erreicht werden. Jede*r Studierende muss zweimal die Lösung einer Aufgabe vorstellen.

Literatur

- John Aycock. Computer Viruses and Malware. Springer, 2006.
- Michael Meier. Intrusion Detection effektiv! Modellierung und Analyse von Angriffsmustern. X.systems.press, Springer, 2007.
- Niels Provos und Thorsten Holz: Virtual Honeypots: From Botnet Tracking to Intrusion Detection. Addison Wesley, 2007.

BA-INF 140 Grundlagen der Mensch-Computer-Interaktion

Workload	Umfang	Dauer	Turnus
180 h	6 LP	1 Semester	jährlich
Modulverantwortliche*r	Lehrende		
Prof. Dr. Matthew Smith	Dr. Christian Tiefenau		
Studiengang	Modus	Studiensemester	
B. Sc. Cyber Security	Wahlpflicht	2.	

Lernziele: fachliche Kompetenzen

Ziel der Vorlesung ist die Vermittlung wichtiger Aspekte der Mensch-Computer Interaktion. Dabei werden sowohl Grundlagen menschlicher Informationsverarbeitung (bspw. physiologische Aspekte, Handlungsprozesse) als auch technische Ansätze zur Realisierung von Benutzungsschnittstellen (bspw. Ein- und Ausgabegeräte, Interaktionsstile) vorgestellt und diskutiert. Im weiteren Verlauf werden benutzerzentrierte Ansätze für den Entwurf und die Beurteilung interaktiver Computersysteme vorgestellt und wichtige Richtlinien für Usability besprochen. Neben Ansätzen der Konzeptentwicklungen werden nutzerzentrierte Methoden der Datenerhebung vorgestellt.

Lernziele: Schlüsselkompetenzen

Die Studierenden erhalten einen umfassenden Einblick in verschiedene Bereiche der Mensch-Computer Interaktion. Die Vorlesung soll dazu befähigen, die Wichtigkeit menschlicher Faktoren für die Funktion interaktiver Computersysteme richtig beurteilen zu können. Neben theoretischen Grundlagen sollen vor allem praktische Ansätze und Prozesse erlernt werden, welche die selbstständige Entwicklung und Evaluation von nutzerfreundlichen Computersystemen ermöglichen.

Inhalte

- Menschliche Informationsverarbeitung (Wahrnehmung, Kognition, Mentale Modelle & Fehler)
- Technische Rahmenbedingungen (UI Gestaltung, Interaktionsstile)
- Nutzerzentrierte Entwicklung & UX Design
- Anforderungsanalyse
- Prototypen
- Evaluation
- Besondere Aspekte der MCI (MobileHCI, VR, SecureHCI)

Teilnahmevoraussetzungen

keine

Veranstaltungen

Lehrform	Gruppengröße	SWS	Workload[h]	LP	
Vorlesung		2	30 P / 45 S	2,5	P = Präsenzstudium
Übungen		2	30 P / 75 S	3,5	S = Selbststudium

Benotete Prüfungsleistungen

Schriftliche Prüfung

Unbenotete Studienleistungen (für Zulassung zur Modulprüfung erforderlich)

Bearbeitung regelmäßig erscheinender Übungsblätter. Die Bearbeitung kann in Gruppen von bis zu drei Studierenden erfolgen. Insgesamt müssen 50% der Punkte erreicht werden. Für 70% der Aufgabenblätter müssen jeweils 50% der Punkte erreicht werden.

Medieneinsatz

Keynote, PDF

Literatur

Butz, Andreas and Antonio Krüger, "Mensch-Maschine-Interaktion", Walter de Gruyter GmbH und Co. KG, 2017

BA-INF 147 Netzwerksicherheit

Workload	Umfang	Dauer	Turnus
180 h	6 LP	1 Semester	jährlich
Modulverantwortliche*r	Lehrende		
Dr. Matthias Wübbeling	Dr. Matthias Wübbeling		
Studiengang	Modus	Studiensemester	
B. Sc. Cyber Security	Wahlpflicht	4. oder 6.	

Lernziele: fachliche Kompetenzen

Die Studierenden lernen grundlegende Informationen über Netzwerke, Netzwerkstacks und relevante Protokolle und damit einhergehende Sicherheits-Aspekte über alle Protokollebenen kennen und einzuschätzen. Die Studierenden sollen sichere Protokolle von unsicheren Protokollen unterscheiden können und Protokollerweiterungen mit nachträglich hinzugefügten Sicherheitsmechanismen kennenlernen, um unsichere Protokolle abzusichern.

Lernziele: Schlüsselkompetenzen

Die regelmäßigen Übungsaufgaben sollen in Gruppenarbeit bearbeitet werden. So erfahren die Studierenden Dynamiken bei der Teamarbeit und erhalten die Fähigkeiten zur Diskussion von Problemstellungen und der Präsentation von Ergebnissen.

Inhalte

ISO/OSI- und TCP/IP-Protokollstapel, Internetrouting (insb. BGP) und nachträgliche Sicherheitsmechanismen wie BGPsec oder RPKI, Klartext-Netzwerkprotokolle und Sicherheitserweiterungen für zentrale Dienste (DNS, DNSSec) und allgemeine Kommunikation (HTTP, SMTP, etc.), Sicherheitszentrierte Kommunikationsprotokolle (z.B. Axolotl), sichere Programmierung von Netzwerkprotokollen auf Anwendungsebene.

Teilnahmevoraussetzungen

Empfohlen:

- Kommunikation in Verteilten Systemen
- Systemnahe Informatik, Systemnahe Programmierung
- Erfahrung in C/C++-Programmierung

Veranstaltungen

Lehrform	Gruppengröße	SWS	Workload[h]	LP	
Vorlesung		2	30 P / 45 S	2,5	P = Präsenzstudium
Übungen		2	30 P / 75 S	3,5	S = Selbststudium

Benotete Prüfungsleistungen

Schriftliche Prüfung

Unbenotete Studienleistungen (für Zulassung zur Modulprüfung erforderlich)

Bearbeitung regelmäßig erscheinender Übungsblätter. Die Bearbeitung kann in Gruppen von bis zu drei Studierenden erfolgen. Insgesamt müssen 50% der Punkte erreicht werden. Die Aufgaben sind aufgeteilt in theoretische und praktische Aufgaben, und die zu erzielenden Punkte gelten separat für beide Teile.

Literatur

- A.S. Tanenbaum: Computernetzwerke, Pearson Education, 4. Überarbeitete Auflage, 2003
- L.L. Peterson, B. S. Davie: Computer Networks, Fifth Edition, 2012
- R. White, D. Slice, A. Retana: Optimal Routing Design, 2005
- S. Halabi: Internet Routing Architectures, 2001
- C. Eckert: IT-Sicherheit, 9. Auflage, 2014
- Weitere Literatur wird bei Bedarf rechtzeitig mitgeteilt

BA-INF 152 Moderne Kryptographie und ihre Anwendung

Workload	Umfang	Dauer	Turnus
180 h	6 LP	1 Semester	jährlich
Modulverantwortliche*r	Lehrende		
Prof. Dr. Michael Meier	Dr. Robin Fay, Prof. Dr. Michael Meier		
Studiengang	Modus	Studiensemester	
B. Sc. Cyber Security	Wahlpflicht	3. oder 5.	

Lernziele: fachliche Kompetenzen

Ziel der Veranstaltung ist, den Studierenden die Grundlagen der modernen Kryptographie und deren Anwendungen zu vermitteln. Den Studierenden soll eine intuitive Definition von Sicherheit in der Kryptographie vermittelt werden und aufgezeigt werden, welche Fehler bei der Anwendung entstehen können. Es soll das notwendige Handwerkszeug vermittelt werden, um Empfehlungen von Standardisierungsgremien und Behörden verstehen und bewerten zu können. Darüber hinaus sollen Studierende in die Lage versetzt werden, neue Angriffe auf Protokolle und Verfahren zu verstehen und deren Kritikalität bewerten zu können.

Lernziele: Schlüsselkompetenzen

Grundlagen der modernen Kryptographie. Klassen von kryptographischen Verfahren und konkrete Verfahren. Fähigkeit, Fehler bei der Verwendung von Protokollen und Angriffe auf Protokolle zu verstehen und deren Kritikalität zu bewerten.

Inhalte

- Grundlagen
- Sicherheitsbegriffe in der Kryptographie
- Zufallszahlen, Zufallszahlengeneratoren und Pseudozufall
- Symmetrische Verfahren
- Hash-Funktionen
- Asymmetrische Verfahren
- Post-Quantum-Kryptographie
- Anwendung von kryptographischen Verfahren

Teilnahmevoraussetzungen

Empfohlen:

- BA-INF 143 – IT-Sicherheit

Veranstaltungen

Lehrform	Gruppengröße	SWS	Workload[h]	LP	
Vorlesung		2	30 P / 45 S	2,5	P = Präsenzstudium
Übungen		2	30 P / 75 S	3,5	S = Selbststudium

Benotete Prüfungsleistungen

Schriftliche Prüfung

Unbenotete Studienleistungen (für Zulassung zur Modulprüfung erforderlich)

Teilnahme an einem Leistungstest. Für den Test müssen 50% der Punkte erreicht werden.

Literatur

- Serious Cryptography: A Practical Introduction to Modern Encryption; Jean-Philippe Aumasson; No Starch Press San Francisco, CA, USA; 2017
- Introduction to Modern Cryptography; Jonathon Katz and Yahuda Lindell; Chapman & Hall/Crc Cryptography and Network Security Series; Second Edition; 2015.

BA-INF 155 Angewandte Binäranalyse

Workload	Umfang	Dauer	Turnus
180 h	6 LP	1 Semester	jährlich
Modulverantwortliche*r	Lehrende		
Prof. Dr. Michael Meier	Dr. Eva-Maria Behner,, Dr. Lilli Bruckschen		
Studiengang	Modus	Studiensemester	
B. Sc. Cyber Security	Wahlpflicht	5.	

Lernziele: fachliche Kompetenzen

Die Studierenden lernen, eine unbekannte Binärdatei mit Hilfe verschiedener Techniken zu analysieren. Zudem sollen die Studierenden den Umgang mit aktuellen Werkzeugen in diesem Bereich lernen und deren Ergebnisse beurteilen können.

Lernziele: Schlüsselkompetenzen

Selbständiges Erfassen von konkreten Problemstellungen, Reflexion und Auswahl geeigneter Werkzeuge, soziale Kompetenzen (Teamfähigkeit beim Problemlösen in Kleingruppen sowie Diskussion über unterschiedliche Lösungsansätze).

Inhalte

In diesem Modul werden grundlegende und erste weiterführende Methoden der Binärcode-Analyse vermittelt:

- Grundlagen statische Analyse (z.B. Hashes, Strings, Dateiformate PE & ELF)
- Grundlagen dynamische Analyse (z.B. API Prozesse & Thread, Virtual Memory)
- Fortgeschrittene statische Analyse (z.B. Disassembler, IRs, AST, Decompiler)
- Fortgeschrittene dynamische Analyse (z.B. Debugging, Patching, Hooking)
- Datenflussanalyse (z.B. liveness Analyse, Dominance)
- Analyse von Android (z.B. Frida, JDK)

Teilnahmevoraussetzungen

Erforderlich:

keine

Empfohlen:

Grundlegende Kenntnisse in der Softwareentwicklung

Grundlegende C-Kenntnisse

Systemnahe Programmierung

Veranstaltungen

Lehrform	Gruppengröße	SWS	Workload[h]	LP	
Vorlesung		2	30 P / 45 S	2,5	P = Präsenzstudium
Übungen		2	30 P / 75 S	3,5	S = Selbststudium

Benotete Prüfungsleistungen

Mündliche Prüfung

Unbenotete Studienleistungen (für Zulassung zur Modulprüfung erforderlich)

Bearbeitung regelmäßig erscheinender Übungsblätter. Die Bearbeitung kann in Gruppen von bis zu zwei Studierenden erfolgen. Insgesamt müssen 50% der Punkte erreicht werden. Für 70% der Aufgabenblätter müssen jeweils 30% der Punkte erreicht werden.

Literatur

Die relevante Literatur wird zu Beginn der Vorlesung bekanntgegeben.

BA-INF 156 Digitale Forensik

Workload	Umfang	Dauer	Turnus
180 h	6 LP	1 Semester	jährlich
Modulverantwortliche*r	Lehrende		
Prof. Dr. Peter Martini	Prof. Dr. Elmar Padilla		
Studiengang	Modus	Studiensemester	
B. Sc. Cyber Security	Wahlpflicht	5.	

Lernziele: fachliche Kompetenzen

Die Studierenden sollen in die Lage versetzt werden, auf forensisch saubere Art und Weise digitale Spuren zu sichern und auszuwerten. Hierzu soll den Studierenden vermittelt werden, wo solche Spuren zu finden sind und wie sie extrahiert und sinnvoll korreliert werden können. Die Studierenden lernen in diesem Zuge nicht nur die zugrundeliegende Theorie, sondern auch die praktische Anwendung sowie den Umgang mit ausgewählten Werkzeugen der IT-Forensik.

Lernziele: Schlüsselkompetenzen

Selbstständiges Erfassen und Aufstellen von konkreten Problem- und Fragestellungen, Reflexion und Auswahl geeigneter Werkzeuge und Methoden, soziale Kompetenzen durch Teamfähigkeit beim Bearbeiten der Case Study in Kleingruppen sowie Diskussion über unterschiedliche Lösungsansätze, Ergebnispräsentation

Inhalte

In der Veranstaltung werden zunächst die wichtigsten Grundlagen für die forensisch saubere Arbeitsweise vorgestellt. Anschließend werden sowohl Methoden für die Extraktion als auch die Analyse von digitalen Spuren innerhalb der Datenträger-, Arbeitsspeicher- und Netzwerkforensik vermittelt. Dies beinhaltet unter anderem Log-Einträge, Betriebssystemdaten wie z. B. die Windows Registry oder anwendungsspezifische Daten wie Exif-Informationen. Für alle Inhalte wird neben den theoretischen Grundlagen stets auch die praktische Anwendbarkeit vermittelt.

Teilnahmevoraussetzungen

Erforderlich:

keine

Empfohlen:

BA-INF 023 Systemnahe Informatik

Veranstaltungen

Lehrform	Gruppengröße	SWS	Workload[h]	LP	
Vorlesung		2	30 P / 45 S	2,5	P = Präsenzstudium S = Selbststudium
Übungen		2	30 P / 75 S	3,5	

Benotete Prüfungsleistungen

Mündliche Prüfung

Unbenotete Studienleistungen (für Zulassung zur Modulprüfung erforderlich)

Erfolgreiche Bearbeitung einer Case Study. Die Bearbeitung kann in Gruppen von bis zu 4 Studierenden erfolgen. Die Ergebnisse sollen anschließend in einem Bericht zusammengefasst und vorgestellt werden.

Medieneinsatz

- Beamer
- Tafel
- Interaktive Übungsaufgaben auf eigener Plattform
- Freiwillige Übungen zum Selbststudium

Literatur

- Geschonneck: „Computer-Forensik“, ISBN-13 : 978-3864901331
- Kävrestad: „Fundamentals of Digital Forensics“, ISBN-13 : 978-3030389536
- Veröffentlichungen in dem Journal „Forensic Science International: Digital Investigation“ (vormals „Digital Investigation“)

Weitere Literatur wird in der Lehrveranstaltung bekannt gegeben.

BA-INF 158 Privatsphäre erhaltende Datenanalyse

Workload	Umfang	Dauer	Turnus
180 h	6 LP	1 Semester	jährlich
Modulverantwortliche*r	Lehrende		
Prof. Dr. Michael Meier	Markus Krämer, Prof. Dr. Michael Meier		
Studiengang	Modus	Studiensemester	
B. Sc. Cyber Security	Wahlpflicht	2., 4. oder 6.	

Lernziele: fachliche Kompetenzen

Die Veranstaltung vermittelt grundlegende und tiefergehende Kompetenzen im Bereich des angewandten Datenschutzes bei der Datenanalyse. Hierzu wird zunächst die rechtliche Situation betrachtet. Darüber hinaus werden Anonymisierungs- und Pseudonymisierungstechniken sowie Datensyntheseverfahren theoretisch und praktisch vermittelt. Des Weiteren werden Techniken zur Mehrparteienverarbeitung schützenswerter Daten erläutert. Ein besonderer Fokus liegt hierbei auf der Anwendung im Bereich maschinelles Lernen. Hierbei werden die Anwendbarkeit und Wechselwirkung mit dem Datenschutz untersucht.

Lernziele: Schlüsselkompetenzen

Die Studierenden sollen ein kritisches Verständnis für Aussagen bezüglich des Datenschutzes entwickeln. Darüber hinaus wird angestrebt, Kompetenzen nicht nur theoretisch, sondern vor allem auf der Anwendungsebene zu vermitteln. Im Bereich der Zusammenarbeit mehrerer Parteien sollen Kompetenzen bezüglich besserer und sichererer Datennutzung vermittelt werden. Dies gilt im Besonderen für den Bereich maschinelles Lernen, um den Fokus neben der Funktionalität auch auf das Thema Datenschutz zu lenken.

Inhalte

- Datenschutzrecht
- Anonymisierung
- Pseudonymisierung
- Secure Multiparty Computation
- Grundlagen der künstlichen Intelligenz
- Daten schützende KI-Verfahren
- Angriffe auf KI
- Datensynthese

Teilnahmevoraussetzungen

Erforderlich:

keine

Empfohlen:

- BA-INF 143 – IT-Sicherheit

Veranstaltungen

Lehrform	Gruppengröße	SWS	Workload[h]	LP	
Vorlesung		2	30 P / 45 S	2,5	P = Präsenzstudium
Übungen		2	30 P / 75 S	3,5	S = Selbststudium

Benotete Prüfungsleistungen

Schriftliche Prüfung

Unbenotete Studienleistungen (für Zulassung zur Modulprüfung erforderlich)

Teilnahme an zwei Leistungstests. Für jeden Test müssen 50% der Punkte erreicht werden.

BA-INF 163 Klassische Kryptografie

Workload	Umfang	Dauer	Turnus
180 h	6 LP	1 Semester	jährlich
Modulverantwortliche*r	Lehrende		
Prof. Dr. Michael Meier	Dr. Gerhard Schabhüser		
Studiengang	Modus	Studiensemester	
B. Sc. Cyber Security	Wahlpflicht	4. oder 6.	

Lernziele: fachliche Kompetenzen

Ziel der Veranstaltung ist es, den Studierenden die Grundlagen der klassischen Kryptografie und der Kryptoanalyse zu vermitteln. Den Studierenden soll ein Verständnis der Designkriterien symmetrischer Kryptoalgorithmen als auch Grundprinzipien und Techniken der Kryptoanalyse vermittelt werden. Dabei soll das notwendige mathematische Handwerkzeug vermittelt werden, um eben sowohl die Designkriterien als auch die Analysemethoden einordnen zu können und exemplarisch anwenden zu können.

Lernziele: Schlüsselkompetenzen

Grundlagen der klassischen Kryptografie, Boolesche Funktionen und deren (Kryptografie-relevante) Eigenschaften, Algorithmen zur Berechnung ebendieser Eigenschaften. Einordnung der Designkriterien für moderne Algorithmen.

Inhalte

Boolesche Funktionen

- Grundlagen
- Darstellungsformen
- Kryptografie-relevante Eigenschaften
- Fouriertransformation (Boolesche Funktionen) und deren Anwendung
- Algorithmen zur Berechnungsmethode der Eigenschaften

Linear rückgekoppelte Schieberegister

- Grundlagen
- Konnex zur Algebra
- Berlekamp-Massey-Algorithmus

Klassische Konstruktionen von Stromchiffren

- Schieberegisterbündel mit Combiner

Kryptoanalyse auf Basis linearer Korrelationen

Diverse statistische Korrelationen

Teilnahmevoraussetzungen

Empfohlen:

- BA-INF 021 Lineare Algebra

Veranstaltungen

Lehrform	Gruppengröße	SWS	Workload[h]	LP	
Vorlesung		2	30 P / 45 S	2,5	P = Präsenzstudium
Übungen		2	30 P / 75 S	3,5	S = Selbststudium

Benotete Prüfungsleistungen

Mündliche Prüfung

Unbenotete Studienleistungen (für Zulassung zur Modulprüfung erforderlich)

Teilnahme an einem Leistungstest. Für das Bestehen des Tests müssen 50% der Punkte erreicht werden.

Literatur

- Bruce Schneier. Applied Cryptography-
- Johannes Buchmann (2016). Einführung in die Kryptografie.

4 Nicht-fachgebundener Wahlpflichtbereich

4.1 Mathematik

Modulnr.	Art	LP	Modulname
V1G2	V4Ü2	9 LP	Analysis II
V1G4	V4Ü2	9 LP	Lineare Algebra II
V2A1	V4Ü2	9 LP	Einführung in die Algebra
V2A2	V4Ü2	9 LP	Einführung in die Mathematische Logik
V3A1	V4Ü2	9 LP	Algebra I
V3A2	V4Ü2	9 LP	Algebra II
V3A4	V4Ü2	9 LP	Mengenlehre
V2B1	V4Ü2	9 LP	Analysis III
V2B2	V4Ü2	9 LP	Einführung in die Partiellen Differentialgleichungen
V2B3	V4Ü2	9 LP	Einführung in die komplexe Analysis
V3B1	V4Ü2	9 LP	Partielle Differentialgleichungen und Funktionalanalysis
V3B3	V4Ü2	9 LP	Globale Analysis
V3C2	V4Ü2	9 LP	Kombinatorik, Graphen und Matroide
V2D1	V4Ü2	9 LP	Einführung in die Geometrie und Topologie
V3D1	V4Ü2	9 LP	Topologie I
V3D2	V4Ü2	9 LP	Topologie II
V3D3	V4Ü2	9 LP	Geometrie I
V3D4	V4Ü2	9 LP	Geometrie II
V2E1	V4Ü2	9 LP	Einführung in die Grundlagen der Numerik
V2E2	V4Ü2	9 LP	Einführung in die Numerische Mathematik
V3E1	V4Ü2	9 LP	Wissenschaftliches Rechnen I
V3E2	V4Ü2	9 LP	Wissenschaftliches Rechnen II
V2F1	V4Ü2	9 LP	Einführung in die Wahrscheinlichkeitstheorie
V2F2	V4Ü2	9 LP	Einführung in die Statistik
V3F1	V4Ü2	9 LP	Stochastische Prozesse
V3F2	V4Ü2	9 LP	Grundzüge der stochastischen Analysis

Die Module sind im [Modulhandbuch des Bachelorstudiengangs Mathematik¹](#) beschrieben.

4.2 Psychologie

Modulnr.	Art	LP	Modulname
502130100	V2Ü2	6 LP	Gegenstand, Geschichte und Methoden der Psychologie
502130200	V2Ü2	6 LP	Allgemeine Psychologie
552100100	V2Ü2	6 LP	Biologische und Klinische Psychologie
502130500	V2Ü2	6 LP	Differenzielle sowie Arbeits-, Betriebs- und Organisationspsychologie
502130400	V2Ü2	6 LP	Entwicklungs- und Pädagogische Psychologie
552100200	V2Ü2	6 LP	Pädagogische Psychologie
502130600	V2Ü2	6 LP	Sozial- und Rechtspsychologie

Die Module sind im [Modulhandbuch des Begleitfachs Psychologie²](#) beschrieben. Es müssen auch alle Vorlesungen vor Anfang über Basis belegt werden. Bitte informieren Sie sich rechtzeitig über Basis über die aktuellen Belegfristen!

¹<http://www.mathematics.uni-bonn.de/studium/de/studiengaenge/bachelorstudiengang-mathematik>

²<https://www.psychologie.uni-bonn.de/de/studium/studiengaenge/b-a-psychologie-begleitfach>

4.3 Wirtschaftswissenschaften

Modulnr.	Modulname
333191003	Grundzüge der BWL: Einführung in die Theorie der Unternehmung (BA VWL PF BWL TdU)
333191004	Grundzüge der BWL: Investition und Finanzierung (BA VWL PF BWL IuF)
333191009	Mikroökonomik A (BA VWL PF MIKRO A)
333191010	Mikroökonomik B (BA VWL PF MIKRO B)
333191011	Makroökonomik A (BA VWL PF MAKRO A)
333191012	Makroökonomik B (BA VWL PF MAKRO B)
333191013	Finanzmärkte und -institutionen (BA VWL PF FINANZM)
333191015	Ökonometrie (BA VWL PF ÖKON)
333190116	Grundzüge der Volkswirtschaftslehre (BA VWL PF VWL G)
333192102	Auktionen und Märkte (BA VWL WPF AUKMARKT)
333192104	Außenwirtschaft/International Economics (BA VWL WPF AUSSENW)
333192105	Geldtheorie und Geldpolitik (BA VWL WPF GELD)
333192107	Industrieökonomik (BA VWL WPF INDÖKON)
333192111	Arbeitsmärkte und Bevölkerungsökonomik (BA VWL WPF AMARKT BEVÖKON)
333192115	Development Economics (BA VWL WPF DEVELOP)
333192116	Experimentelle Wirtschaftsforschung (BA VWL WPF EXWIFO)
333192123	Applied Microeconometrics (BA VWL WPF AMICMETRICS)
333192124	Informationsökonomie/Information Economics (BA VWL WPF INFÖKON)
333192126	Collective Choice (BA VWL WPF CCHOICE)
333192127	Finanz- und Sozialpolitik (BA VWL WPF FISOPOL)
333192128	Bounded Rationality (BA WPF VWL BOUNDRAT)
333192201	Internationale Bankleistungen (BA VWL WPF IBL)
333192202	Bankmanagement (BA VWL WPF BANK)
333192203	Advanced Corporate Finance (BA VWL WPF ACORPFIN)
333192204	Personalökonomik (BA VWL WPF PERSONAL)
333192205	Kostenmanagement und Kostenrechnung (BA VWL WPF KOSTEN)
333192207	Internationale Rechnungslegung nach IFRS (BA VWL WPF IFRS)
333192211	Empirical Corporate Finance (BA VWL WPF EMPCORP)
333192213	Behavioral Finance (BA VWL WPF BEFINANCE)
333192302	Multivariate Statistik (BA VWL WPF MULTSTAT)
333192303	Computergestützte statistische Analyse (BA VWL WPF COMPSTAT)
Nr. fehlt noch	Political Economy
333192101	Spieltheorie/Game Theory (BA VWL WPF SPIEL)
Nr. fehlt noch	Stochastische Modelle (BA VWL WPF STOCHMO)
333192112	Umweltökonomik (BA VWL WPF UMWELT)
333192117	Vertragstheorie (BA VWL WPF VERTRAG)
333192119	Wirtschaftsgeschichte (BA VWL WPF WIGESCHI)
333192120	Verhaltensökonomik (BA VWL WPF VERHALTEN)
333192206	Unternehmensplanung (BA VWL WPF UPLANUNG)
333192209	Unternehmensbilanzen und Unternehmensbewertung (BA VWL WPF BILANZEN)
333192304	Zeitreihenanalyse (BA VWL WPF ZEIT)

Die Module sind in den [Modulhandbüchern des Bachelorstudiengangs Volkswirtschaftslehre](#)³ beschrieben.

Achtung: der Studiengang Volkswirtschaftslehre wird auf eine neue Prüfungsordnung umgestellt, wobei Module von 7,5 LP durch Module von 6 LP oder 9 LP ersetzt werden. Die hier abgedruckte Modulliste ist vielleicht nicht ganz aktuell. Bitte erkundigen Sie sich beim Fachbereich Wirtschaftswissenschaften, welche Module derzeit mit welchem Umfang angeboten werden.

Beim Modul “Grundzüge der Volkswirtschaftslehre” ist die Prüfung in zwei Teilprüfungen unterteilt, die sich auf zwei unterschiedliche Lehrveranstaltungen beziehen (Mikro und Makro). Für jede Lehrveranstaltung

³<https://www.econ.uni-bonn.de/de/studium/studienangebot/vwl/studienverlaufsplan-modulhandbuecher>

findet je ein Belegverfahren zu Beginn des Semesters und je eine Prüfungsanmeldung zu einem späteren Zeitpunkt statt (Termine sind auf den [Seiten des zuständigen Prüfungsamts](#)⁴ veröffentlicht. Studierende in den Studiengängen Informatik und Cyber Security bekommen für dieses Modul im Wintersemester 2024/2025 nach wie vor 7,5 Leistungspunkte.

4.4 Geographie

Modulnr.	Art	LP	Modulname
B0	V2	4 LP	Einführung in die Geographie (ohne Exkursion)
B1	V4	8 LP	Physische Geographie Basis
B3	V4	8 LP	Humangeographie Basis
B5	V4	6 LP	Regionale Geographie und räumliche Planung
B7	V4	10 LP	Geomatik

Die Module sind auf der Seite [Bachelor of Science Geographie](#)⁵ beschrieben. Es müssen auch alle Vorlesungen vor Anfang über Basis belegt werden. Bitte beachten Sie die Hinweise auf <https://www.geographie.uni-bonn.de/de/studium/organisation/termine#Lehranmeldung> und informieren Sie sich rechtzeitig über Basis über die aktuellen Belegfristen!

4.5 Photogrammetrie

Modulnr.	Art	LP	Modulname
B57		10 LP	<i>Photogrammetrie</i>
	V3Ü2		Photogrammetry I
	V2Ü1		Photogrammetry II
	T1		Photogrammetry

Die Module sind im [Modulhandbuch für den Studiengang Geodäsie und Geoinformation \(BSc\)](#)⁶ beschrieben.

4.6 Physik/Astronomie

Modulnr.	Art	LP	Modulname
physik011	V+Ü	5 LP	Physik für Naturwissenschaftler I
physik012	V+Ü	4 LP	Physik für Naturwissenschaftler II
astro121	V+Ü	4 LP	Einführung in die Astronomie
astro122	V+Ü	4 LP	Einführung in die extragalaktische Astronomie

Die Module sind im [Modulhandbuch „Lehrveranstaltungen für andere Fächer“](#)⁷ der Fachgruppe Physik/Astronomie beschrieben.

⁴<https://www.econ.uni-bonn.de/examinations/de/termine>

⁵<https://www.geographie.uni-bonn.de/de/studium/studiengaenge/bachelor/bsc>

⁶<http://www.gug.uni-bonn.de/de/bachelor-gug/im-studium>

⁷<http://tiny.iap.uni-bonn.de/mhb/mhb.php?stg=LVANDERE>

4.7 Chemie

Modulnr.	Art	LP	Modulname
BCh 20 1.1	V+Ü	6 LP	Allgemeine Chemie
BCh 20 1.2	V+Ü+P	9 LP	Anorganische und Analytische Chemie I (Qualitative Analyse I)
BCh 20 2.6/3.2	V+Ü	7 LP	Grundlagen der Organischen Chemie
BCh 20 1.3/2.3	V+Ü	10 LP	Physikalische Chemie I/II (zweisemestrig) (Molekulare Wechselwirkungen und chemische Thermodynamik)
BCh 20 3.4	V+Ü	5 LP	Theoretische Chemie I
BCh 20 4.4	V+Ü	5 LP	Theoretische Chemie II

Die Module sind auf der Seite [Chemie als Nebenfach](#)⁸ unter “Informatik (BSc)/Cyber Security (BSc)” beschrieben, bitte unbedingt beachten!

Es wird empfohlen, die Grundvorlesung BCh 20 1.1 zuerst zu absolvieren. Die Anmeldung zu diesen Modulen erfolgt durch direkte Prüfungsanmeldung in BASIS (kein Belegverfahren). Für eine Beratung wenden Sie sich bitte an das [Studiengangsmanagement der Chemie](#).

4.8 Philosophie

Modulnr.	Art	LP	Modulname
501100100	V, T, Ü	12 LP	Logik und Grundlagen
501100200	V, T, Ü	12 LP	Erkenntnistheorie
501100300	V, T, Ü	12 LP	Moralphilosophie
501100800	V, T, Ü	12 LP	Philosophiegeschichte I (Antike und Mittelalter)
501100900	V, Ü, S	12 LP	Philosophiegeschichte II (Neuzeit und Gegenwart)
501100600	V, Ü, S	12 LP	Wissenschaftsphilosophie
501100700	V, Ü, S	12 LP	Kulturphilosophie

Die Module sind im [Modulhandbuch des Begleitfachs Philosophie](#)⁹ beschrieben. Es müssen auch alle Vorlesungen vor Anfang über Basis belegt werden. Bitte informieren Sie sich rechtzeitig über Basis über die aktuellen Belegfristen!

4.9 Molekulare Biomedizin

Modulnr.	Art	LP	Modulname
MBMP-015	V2Ü2	5 LP	Genomik und Bioinformatik
MBMInf 1	V5S1	10 LP	Molekulare Zellbiologie und Genetik
MBMInf 2	V4Ü2	8 LP	Organische Chemie
MBMInf 4	V4Ü2	8 LP	Biophysik und Physikalische Chemie

Aufgrund seiner Brückenfunktion zwischen Informatik und Molekularer Biomedizin empfehlen wir allen Studierenden, die im nicht-fachgebundenen Wahlpflichtbereich einen entsprechenden Schwerpunkt setzen möchten, das Modul MBMP-015 zu absolvieren.

Die Module sind im Dokument [Module der Molekularen Biomedizin \(LIMES-Institut\) für den nichtfachgebundenen Wahlpflichtbereich im Bachelor Informatik](#)¹⁰ beschrieben.

⁸<https://www.chemie.uni-bonn.de/de/studium-lehre/studiengaenge/chemie-als-nebenfach>

⁹<https://www.philosophie.uni-bonn.de/studium/bachelor-philosophie>

¹⁰https://www.informatik.uni-bonn.de/de/studium/pruefungsamt/dokumente/molekulare-biomedizin_20241009.pdf

4.10 Meteorologie und Geophysik

Modulnr.	Art	LP	Modulname
mug110	V2Ü2	6LP	Einführung in die Meteorologie und Geophysik
mug210	V2Ü1S1	6LP	Physikalische Klimatologie
mug220	V2Ü2	6LP	Physik der festen Erde
mug310	V2Ü1P1	6LP	Fernerkundung
mug320	V2Ü2	6LP	Physik der Atmosphäre
mug410	V2Ü2S2	8LP	Synoptik und Wetterbesprechung

Die Module sind im [Modulhandbuch des Bachelorstudiengangs Meteorologie und Geophysik](#)¹¹ beschrieben. Eine Belegung über Basis ist nicht erforderlich. Die Prüfungsanmeldung erfolgt jedoch in Basis und es muss ein Beitritt zum jeweiligen eCampus-Kursen erfolgen.

4.11 Entrepreneurship und Unternehmungsführung

Modulnr.	Art	LP	Modulname
	V4	6LP	Entrepreneurship und Unternehmungsführung

Weitere Infos zur Veranstaltung finden sich hier: https://www.ies.uni-bonn.de/studium-und-lehre/veranstaltungen-1/entrepreneurship_und_unternehmensfuehrung.

4.12 Ethik

Modulnr.	Art	LP	Modulname
201043200	S1P1	6LP	Bonn Ethics Lab

Weitere Infos zur Veranstaltung finden sich hier: <https://ethicslab.uni-bonn.de/>.

¹¹<https://www.ifgeo.uni-bonn.de/de/studium/mug>