

Modulhandbuch
Studiengang Bachelor of Arts (K) Informatik NF
Prüfungsordnung: 079-2-2009

Sommersemester 2018
Stand: 09. April 2018

Universität Stuttgart
Keplerstr. 7
70174 Stuttgart

Kontaktpersonen:

Studiendekan/in:	Univ.-Prof. Stefan Wagner Institut für Softwaretechnologie Tel.: 0711/685-88455 E-Mail: stefan.wagner@informatik.uni-stuttgart.de
Studiengangsmanager/in:	Katrin Schneider Institut für Maschinelle Sprachverarbeitung Tel.: 685 88520 E-Mail: katrin.schneider@informatik.uni-stuttgart.de
Prüfungsausschussvorsitzende/r:	Univ.-Prof. Stefan Funke Institut für Formale Methoden der Informatik E-Mail: Stefan.Funke@informatik.uni-stuttgart.de
Fachstudienberater/in:	Stefan Zimmer Institut für Parallele und Verteilte Systeme E-Mail: stefan.zimmer@ipvs.uni-stuttgart.de
Stundenplanverantwortliche/r:	Apl. Prof. Ulrich Hertrampf Institut für Formale Methoden der Informatik Tel.: 7816-344 E-Mail: ulrich.hertrampf@f05.uni-stuttgart.de

Inhaltsverzeichnis

Präambel	4
Qualifikationsziele	5
100 Module im Nebenfach	6
10260 Programmierkurs	7
10280 Programmierung und Software-Entwicklung	9
12060 Datenstrukturen und Algorithmen	11
14360 Einführung in die Technische Informatik	13
23530 Automaten und Formale Sprachen	15
320 Katalog ISG	16
10030 Architektur von Anwendungssystemen	17
10080 Datenbanken und Informationssysteme	19
10110 Grundlagen der Künstlichen Intelligenz	21
10170 Imaging Science	23
10210 Mensch-Computer-Interaktion	25
10220 Modellierung	27
36530 Rechnerorganisation 1	29
39250 Distributed Systems I	31
42410 Grundlagen des Wissenschaftlichen Rechnens	33
42420 High Performance Computing	34
42460 Numerische Simulation	36
42480 Ausgewählte Kapitel des Wissenschaftlichen Rechnens	37
71740 System and Web Security	38
71760 Security and Privacy	39
78640 Grundlagen der Informationssicherheit	41
78900 Introduction to Modern Cryptography	43
330 Katalog ISW	45
10030 Architektur von Anwendungssystemen	46
10040 Bildsynthese	48
10060 Computergraphik	50
10080 Datenbanken und Informationssysteme	51
10110 Grundlagen der Künstlichen Intelligenz	53
10120 Modellbildung und Simulation	55
10170 Imaging Science	56
10180 Information Retrieval and Text Mining	58
10210 Mensch-Computer-Interaktion	59
10220 Modellierung	61
36530 Rechnerorganisation 1	63
39040 Rechnernetze	65
39250 Distributed Systems I	67
42410 Grundlagen des Wissenschaftlichen Rechnens	69
42420 High Performance Computing	70
42460 Numerische Simulation	72
42480 Ausgewählte Kapitel des Wissenschaftlichen Rechnens	73
71740 System and Web Security	74
71760 Security and Privacy	75
72240 Model-Driven Software Development	77
78640 Grundlagen der Informationssicherheit	78
78900 Introduction to Modern Cryptography	80

Präambel

Informatik ist die Wissenschaft von der Informationsverarbeitung und den informationsverarbeitenden Systemen. Sie umfasst deren Theorie und Methodik, den Einsatz dieser Systeme, aber auch die Auswirkungen. Die Informatik ist damit ein Grundpfeiler der modernen Informationsgesellschaft. Informatiksysteme durchdringen unser tägliches Leben. Was noch vor wenigen Jahren unvorstellbar war, ist heute selbstverständlicher Standard. Die weltweite freie Bereitstellung von Wissen und die Möglichkeit, sich ohne Kosten per E-Mail auszutauschen sowie riesige Datenmengen, etwa in Form von Musik und Filmen zu speichern, bedeutet eine gesellschaftliche Neuerung, an deren Gestaltung man durch ein Informatikstudium aktiv mitwirken kann.

Durch Verfahren der Modellbildung und Abstraktion formuliert die Informatik allgemeine Gesetze, die der Informationsverarbeitung zugrunde liegen, und sucht Standardlösungen für praxisrelevante Aufgaben. Von wachsender Bedeutung wird dabei die Beherrschung immer komplexer werdender verteilter und vernetzter Systeme. Informatikerinnen und Informatiker operieren mit abstrakten Zeichen und Objekten, untersuchen Daten-, Sprach- und Systemstrukturen und entwickeln formale Programmiersprachen zur Formulierung von Algorithmen, Prozessen, Systemen und speziellen Anwendungen. Die Hard- und Software-Systeme stehen dabei als Forschungsobjekte und gleichzeitig als Werkzeuge im Mittelpunkt der Arbeit. Durch Visualisierung und Simulation werden neue Anwendungen erschlossen. Informatik ist einerseits eine Strukturwissenschaft, andererseits dominieren aber heute die ingenieurwissenschaftlichen Methoden und Verfahren. Die Informatik an der Universität Stuttgart ist geprägt durch hohen Praxisbezug und Anwendungen, ohne dabei die notwendigen Grundlagen zu vernachlässigen.

Auf den Bachelor-Studiengang Informatik bauen die Master-Studiengänge auf, die vom Fachbereich Informatik im Anschluss an das Bachelor-Studium angeboten werden. Dazu gehören neben den deutschsprachigen Masterstudiengängen _Informatik_ und _Softwaretechnik_ auch die englischsprachigen Masterstudiengänge _Computer_ _Science_ und _Computational Linguistics_. Es wird empfohlen, den Master als Abschluss eines universitären Studiums anzustreben

Die Studien- und Prüfungsordnung für den Bachelorstudiengang _Informatik_ beschreibt den Aufbau des Studiums und die Organisation der Prüfungen. Sie stellt das Regelwerk und die Rechtsgrundlage für eine einheitliche Handhabung des Studienablaufs und der Bewertung der Studien- und Prüfungsleistungen dar. Sie wendet sich dabei sowohl an die Studierenden als auch an die Prüfenden sowie an die entsprechenden Organe der Universität Stuttgart.

Aus Gründen der sprachlichen Vereinfachung wird grundsätzlich nur die grammatikalisch männliche Form für Personen verwendet. Sinngemäß ist stets auch die entsprechende weibliche Form gemeint.

Qualifikationsziele

Das Curriculum des Studienganges sieht im 1. und 2. Semester eine Vertiefung der mathematischen und technischen Grundlagen der Informatik in Pflichtmodulen vor. Im 3. bis 6. Semester liegt der Schwerpunkt der Ausbildung auf diversen Grundlagen- und Spezialisierungsfächern verschiedener Bereiche der Informatik. Zusätzliche Inhalte sind Seminare, fachliche Module als Wahlpflichtbereich sowie fachübergreifende Schlüsselqualifikationen. Im 6. Semester liegt ein weiterer Schwerpunkt auf der Bachelorarbeit. Mit der Bachelorarbeit ist die Befähigung zu zeigen, innerhalb einer vorgegebenen Frist eine komplexe Aufgabenstellung aus dem Bereich der Informatik selbständig nach wissenschaftlichen Methoden zu bearbeiten und die Ergebnisse sachgerecht darzustellen.

Die Absolventinnen und Absolventen des Bachelorkombistudienganges Informatik

- verfügen über ein vertieftes mathematisches und ingenieurwissenschaftliches Wissen, welches sie befähigt, Probleme und Aufgabenstellungen der Informatik zu verstehen und kritisch einzuschätzen.
- sind in der Lage, jenes erlangte Wissen auf Erkenntnisse der Ingenieurwissenschaften anzuwenden.
- verfügen über Fachwissen auf den Gebieten der theoretischen, praktischen, technischen und angewandten Informatik und können Aufgabenstellungen der Informatik wissenschaftlich erkennen, beschreiben und bewerten, analysieren und lösen.
- haben umfassendes Verständnis über Softwareentwicklungsmethoden und Rechnersysteme, ihre Anwendungsmöglichkeiten und verfügen über die Fertigkeit, Konzepte und Lösungen für neue Softwaresysteme zu entwickeln.
- verfügen über eine verantwortliche und selbständige wissenschaftliche Arbeitsweise.

Die Beschäftigungsbereiche der Absolventinnen und Absolventen liegen u. a. in der Datenverarbeitungs- und Entwicklungsindustrie und in industriellen, kommerziellen, verwaltungstechnischen und wissenschaftlichen Anwendungen von Datenverarbeitungssystemen.

100 Module im Nebenfach

Zugeordnete Module:	10260	Programmierkurs
	10280	Programmierung und Software-Entwicklung
	12060	Datenstrukturen und Algorithmen
	14360	Einführung in die Technische Informatik
	23530	Automaten und Formale Sprachen
	320	Katalog ISG
	330	Katalog ISW

Modul: 10260 Programmierkurs

2. Modulkürzel:	051520010	5. Moduldauer:	Einsemestrig
3. Leistungspunkte:	3 LP	6. Turnus:	Wintersemester
4. SWS:	2	7. Sprache:	Weitere Sprachen
8. Modulverantwortlicher:	Univ.-Prof. Dr. Jonas Kuhn		
9. Dozenten:	Jason Utt		
10. Zuordnung zum Curriculum in diesem Studiengang:	B.A. (K) Informatik NF, PO 079-2-2009, 2. Semester → Module im Nebenfach		
11. Empfohlene Voraussetzungen:			
12. Lernziele:	<p>Selbstständiges Erstellen von Programmen und Lösung von Programmieraufgaben in der Programmiersprache Python, mit einem Schwerpunkt auf Konzepten, die für die maschinelle Sprachverarbeitung und Computerlinguistik wichtig sind.</p> <p>--</p> <p>Independently writing programs and solving programming tasks in the programming language Python, with emphasis on concepts relevant for Natural Language Processing and Computational Linguistics.</p>		
13. Inhalt:	<p>Das Modul Programmierkurs richtet sich primär an Studierende der Maschinellen Sprachverarbeitung (3. Semester), Computerlinguistik und Digital Humanities. Vermittelt werden die wichtigsten Konzepte der Programmiersprache Python und praktische Erfahrung bei der Erstellung von Python-Programmen bei der Verarbeitung von sprachlichen Daten und Ressourcen. Die Modulveranstaltung und die Materialien sind in der Regel überwiegend englischsprachig, es werden jedoch deutschsprachige Hilfestellungen angeboten.</p> <p>--</p> <p>The module primarily targets students in Natural Language Processing (3rd semester), Computational Linguistics and Digital Humanities. It covers the key concepts of the programming language Python and provides practical experience in writing Python programs in the context of processing linguistic data and resources.</p> <p>Typically, the lectures of the module course as well as the materials are in English, however, students not fluent in English in the programming context will receive support in German.</p>		
14. Literatur:	Folien. Slides.		
15. Lehrveranstaltungen und -formen:	• 102601 Übung Programmierkurs		
16. Abschätzung Arbeitsaufwand:	Präsenzzeit: 21 Stunden Nachbearbeitungszeit: 69 Stunden		
17. Prüfungsnummer/n und -name:	10261 Programmierkurs (USL), Sonstige, Gewichtung: 1 Übungsschein - Scheinkriterien werden zu Beginn der Veranstaltung angekündigt. Criteria for credits are announced at the beginning of the course.		
18. Grundlage für ... :			

19. Medienform:

20. Angeboten von:

Grundlagen der Computerlinguistik

Modul: 10280 Programmierung und Software-Entwicklung

2. Modulkürzel:	051520005	5. Moduldauer:	Einsemestrig
3. Leistungspunkte:	9 LP	6. Turnus:	Wintersemester
4. SWS:	6	7. Sprache:	Deutsch
8. Modulverantwortlicher:		Frank Leymann	
9. Dozenten:		Frank Leymann	
10. Zuordnung zum Curriculum in diesem Studiengang:		B.A. (K) Informatik NF, PO 079-2-2009, 1. Semester → Module im Nebenfach	
11. Empfohlene Voraussetzungen:		Keine. Teilnahme an einem Vorkurs Java ist hilfreich aber nicht notwendig.	
12. Lernziele:		Die Teilnehmer haben einen Überblick über das Gebiet der Informatik. Sie haben die wichtigsten Konzepte einer höheren Programmiersprache und ihrer Verwendung verstanden und sind in der Lage, kleine Programme (bis zu einigen hundert Zeilen) zu analysieren und selbst zu konzipieren und zu implementieren. Sie kennen die Möglichkeiten, Daten- und Ablaufstrukturen zu entwerfen, zu beschreiben und zu codieren. Sie haben die Abstraktionskonzepte moderner Programmiersprachen verstanden. Sie kennen die Techniken und Notationen zur Definition kontextfreier Programmiersprachen und können damit arbeiten.	
13. Inhalt:		<ul style="list-style-type: none"> • Die Programmiersprache Java und die virtuelle Maschine • Objekte, Klassen, Schnittstellen, Blöcke, Programmstrukturen, Kontrakte • Klassenmodellierung mit der UML • Objekterzeugung und -ausführung • Boolesche Logik • Verzweigungen, Schleifen, Routinen, Abstraktionen, Modularisierung, Variablen, Zuweisungen • Rechner, Hardware • Syntaxdarstellungen • Übersicht über Programmiersprachen und -werkzeuge • Grundlegende Datenstrukturen und Algorithmen • Vererbung, Polymorphe • Semantik • Programmierung graphischer Oberflächen • Übergang zum Software Engineering 	
14. Literatur:		<ul style="list-style-type: none"> • Appelrath, Hans-Jürgen und Ludewig, Jochen, Skriptum Informatik - eine konventionelle Einführung, Verlag der Fachvereine Zürich und B.G. Teubner Stuttgart, 4. Auflage 1999 • Meyer, Bertrand, Touch of Class, Springer-Verlag, 2009 • Savitch, Walter, Java. An Introduction to Problem Solving and Programming, Pearson, 6. Auflage, 2012 	
15. Lehrveranstaltungen und -formen:		<ul style="list-style-type: none"> • 102801 Vorlesung Programmierung und Softwareentwicklung • 102802 Übung Programmierung und Softwareentwicklung 	
16. Abschätzung Arbeitsaufwand:		Präsenzstunden: 63 h Eigenstudiumstunden: 207 h Gesamtstunden: 270 h	

17. Prüfungsnummer/n und -name:	<ul style="list-style-type: none">• 10281 Programmierung und Software-Entwicklung (PL), Schriftlich, 90 Min., Gewichtung: 1• V Vorleistung (USL-V), Schriftlich oder Mündlich [10281] Programmierung und Software-Entwicklung (PL), schriftliche Prüfung, 90 Min., Gewicht: 1.0, [Prüfungsvorleistung] Vorleistung (USL-V), schriftlich, eventuell mündlich, Vorleistung: Übungsschein. Voraussetzungen werden zu Beginn vom Dozenten festgesetzt. Dazu gehören eine bestimmte Anzahl von Vorträgen in den Übungen und ein bestimmter Teil der Übungspunkte.
18. Grundlage für ... :	Datenstrukturen und Algorithmen
19. Medienform:	<ul style="list-style-type: none">• Folien über Beamer• Tafelanschrieb
20. Angeboten von:	Architektur von Anwendungssystemen

Modul: 12060 Datenstrukturen und Algorithmen

2. Modulkürzel:	051510005	5. Moduldauer:	Einsemestrig
3. Leistungspunkte:	9 LP	6. Turnus:	Sommersemester
4. SWS:	6	7. Sprache:	Deutsch
8. Modulverantwortlicher:	Univ.-Prof. Dr.-Ing. Andrés Bruhn		
9. Dozenten:	Andrés Bruhn		
10. Zuordnung zum Curriculum in diesem Studiengang:	B.A. (K) Informatik NF, PO 079-2-2009, 2. Semester → Module im Nebenfach		
11. Empfohlene Voraussetzungen:	Modul 10280 Programmierung und Software-Entwicklung		
12. Lernziele:	<p>Die Studierenden kennen nach engagierter Mitarbeit in dieser Veranstaltung diverse zentrale Algorithmen auf geeigneten Datenstrukturen, die für eine effiziente Nutzung von Computern unverzichtbar sind. Sie können am Ende zu gängigen Problemen geeignete programmiersprachliche Lösungen angeben und diese in einer konkreten Programmiersprache formulieren.</p> <p>Die Lernziele lassen sich wie folgt zusammenfassen:</p> <ul style="list-style-type: none"> • Kenntnis der Eigenschaften elementarer und häufig benötigter Algorithmen • Verständnis für die Auswirkungen theoretischer und tatsächlicher Komplexität • Erweiterung der Kompetenz im Entwurf und Verstehen von Algorithmen und der zugehörigen Datenstrukturen • Erste Begegnung mit nebenläufigen Algorithmen 		
13. Inhalt:	<p>Es werden die folgenden Themen behandelt:</p> <ul style="list-style-type: none"> • Vorgehensweise bei der Entwicklung und Implementierung von Algorithmen • Komplexität und Effizienz von Algorithmen, O-Notation • Listen (Stack, Queue, doppelt verkettete Listen) • Sortierverfahren (Selection-, Insertion-, Bubble-, Merge-, Quick-Sort) • Bäume (Binär-, AVL-, 2-3-4-, Rot-Schwarz-, B-Bäume, Suchbäume, Traversierung, Heap) • Räumliche Datenstrukturen (uniforme Gitter, Oktal-, BSP-, kD-, CSG-Bäume, Bounding-Volumes) • Graphen (Datenstrukturen, DFS, BFS, topologische Traversierung, Dijkstra-, A*, Bellman-Ford-Algorithmen, minimale Spannbäume, maximaler Fluss) • Räumliche Graphen (Triangulierung, Voronoi, Delaunay, Graph-Layout) • Textalgorithmen (String-Matching, Knuth-Morris-Pratt, Boyer-Moore, reguläre Ausdrücke, Levenshtein-Distanz) • Hashing (Hashfunktionen, Kollisionen) • Verteilte Algorithmen (Petri-Netze, Programmieren nebenläufiger Abläufe, einige parallele und parallelisierte Algorithmen) • Algorithmenentwurf und -muster (inkrementell, greedy, divide-and-conquer, dynamische Programmierung, Backtracking, randomisierte Algorithmen) 		

- Maschinelles Lernen (überwachtes Lernen, Entscheidungsbäume, SVM, neuronale Netze, unüberwachtes Lernen, k-Means)

14. Literatur:

- G. Saake, K. Sattler. *Algorithmen und Datenstrukturen: Eine Einführung mit Java* . 5. Auflage, dpunkt-Verlag, 2013
- T. Ottmann, P. Widmayer. *Algorithmen und Datenstrukturen* . 5. Auflage, Springer-Verlag, 2012

15. Lehrveranstaltungen und -formen:

- 120601 Vorlesung Datenstrukturen und Algorithmen
- 120602 Übung Datenstrukturen und Algorithmen

16. Abschätzung Arbeitsaufwand:

17. Prüfungsnummer/n und -name:

- 12061 Datenstrukturen und Algorithmen (PL), Schriftlich, 120 Min., Gewichtung: 1
 - V Vorleistung (USL-V), Schriftlich oder Mündlich
- Prüfungsvorleistung: Übungsschein. Die genauen Details der Übungsleistungen und Ihrer Anrechnung werden zu Beginn der Lehrveranstaltung bekannt gegeben.

18. Grundlage für ... :

19. Medienform:

20. Angeboten von:

Intelligente Systeme

Modul: 14360 Einführung in die Technische Informatik

2. Modulkürzel:	051400105	5. Moduldauer:	Einsemestrig
3. Leistungspunkte:	6 LP	6. Turnus:	Wintersemester
4. SWS:	4	7. Sprache:	Deutsch
8. Modulverantwortlicher:	Univ.-Prof. Dr. Otto Eggenberger		
9. Dozenten:	Otto Eggenberger		
10. Zuordnung zum Curriculum in diesem Studiengang:	B.A. (K) Informatik NF, PO 079-2-2009, 3. Semester → Module im Nebenfach		
11. Empfohlene Voraussetzungen:	Keine		
12. Lernziele:	Der/die Studierende kennt die grundlegende Funktionsweise eines Computers, versteht die elektrotechnischen Grundlagen und Technologien und kann einfache digitale Schaltungen analysieren, entwerfen und optimieren.		
13. Inhalt:	<p>Grundlegende Funktionsweise eines Computers</p> <ul style="list-style-type: none"> • Informationsdarstellung • Zahlendarstellung und Codes • Digitale Grundbausteine • Logische Funktionen, Speicherelemente • Befehlsausführung, Programmablauf <p>Elektrotechnische Grundlagen</p> <ul style="list-style-type: none"> • Physikalische Grundbegriffe • Elektrische Spannung, elektrischer Strom • Elektrische Netzwerke • Halbleiterbauelemente • Digitale Grundsaltungen <p>Digitale Schaltungen</p> <ul style="list-style-type: none"> • Schaltnetzwerke • Boolesche Algebra und Schaltalgebra • Darstellung und Minimierung von Schaltfunktionen • Rückkopplung, Zustandsbegriff • Automaten und sequentielle Netzwerke • Digitale Standardschaltungen • Entwurfsmethodik 		
14. Literatur:	<ul style="list-style-type: none"> • Dirk W. Hoffman: Grundlagen der technischen Informatik, Hanser, 2007 • Bernd Becker, Rolf Drechsler, Paul Molitor: Technische Informatik, Pearson Studium, 2005 • Jörg Keller, Wolfgang J. Paul: Hardware Design, Teubner, 3. Aufl. 2005 		
15. Lehrveranstaltungen und -formen:	<ul style="list-style-type: none"> • 143602 Gruppenübungen Einführung in die Technische Informatik • 143601 Vorlesung Einführung in die Technische Informatik 		
16. Abschätzung Arbeitsaufwand:			
17. Prüfungsnummer/n und -name:	14361 Einführung in die Technische Informatik (PL), Schriftlich, 60 Min., Gewichtung: 1 [14361] Einführung in die Technische Informatik (PL), schriftliche Prüfung, 60 Min., Gewicht: 1.0		

18. Grundlage für ... : Rechnerorganisation 1

19. Medienform:

20. Angeboten von: Grundlagen der Informatik

Modul: 23530 Automaten und Formale Sprachen

2. Modulkürzel:	050420007	5. Moduldauer:	Einsemestrig
3. Leistungspunkte:	6 LP	6. Turnus:	Wintersemester
4. SWS:	4	7. Sprache:	Deutsch
8. Modulverantwortlicher:	apl. Prof. Dr. rer. nat. habil. Ulrich Hertrampf		
9. Dozenten:	Volker Diekert Ulrich Hertrampf		
10. Zuordnung zum Curriculum in diesem Studiengang:	B.A. (K) Informatik NF, PO 079-2-2009, 4. Semester → Module im Nebenfach		
11. Empfohlene Voraussetzungen:	Mathematik (Schulkenntnisse)		
12. Lernziele:	Die Studierenden beherrschen wichtige theoretische Grundlagen der Informatik, insbesondere die Theorie und Algorithmik endlicher Automaten. Hierzu gehört das Kennenlernen, Einordnen und Trennung der Chomskyschen Sprachklassen.		
13. Inhalt:	Deterministische- bzw. nichtdeterministische endliche Automaten, reguläre Ausdrücke, Minimierung endlicher Automaten, Iterationslemmata für reguläre und kontextfreie Sprachen, Normalformen, Kellerautomaten, Lösen des Wortproblems kontextfreier Sprachen mit dem CYK-Algorithmus, linear beschränkte Automaten, kontextsensitive Grammatiken, Typ 0-Grammatiken und Turingmaschinen.		
14. Literatur:	<ul style="list-style-type: none"> • Uwe Schöning, Theoretische Informatik - kurzgefasst, 1999 		
15. Lehrveranstaltungen und -formen:	<ul style="list-style-type: none"> • 235301 Vorlesung Automaten und Formale Sprachen • 235302 Gruppenübungen Automaten und Formale Sprachen 		
16. Abschätzung Arbeitsaufwand:			
17. Prüfungsnummer/n und -name:	<ul style="list-style-type: none"> • 23531 Automaten und Formale Sprachen (PL), Schriftlich, 60 Min., Gewichtung: 1 • V Vorleistung (USL-V), Schriftlich oder Mündlich [23531] Automaten und Formale Sprachen (PL), schriftliche Prüfung, 60 Min., Gewicht: 1.0 [Prüfungsvorleistung] Vorleistung (USL-V), schriftlich, eventuell mündlich 		
18. Grundlage für ... :	Algorithmik, Berechenbarkeit und Komplexität		
19. Medienform:			
20. Angeboten von:	Theoretische Informatik		

320 Katalog ISG

Zugeordnete Module:	10030	Architektur von Anwendungssystemen
	10080	Datenbanken und Informationssysteme
	10110	Grundlagen der Künstlichen Intelligenz
	10170	Imaging Science
	10210	Mensch-Computer-Interaktion
	10220	Modellierung
	36530	Rechnerorganisation 1
	39250	Distributed Systems I
	42410	Grundlagen des Wissenschaftlichen Rechnens
	42420	High Performance Computing
	42460	Numerische Simulation
	42480	Ausgewählte Kapitel des Wissenschaftlichen Rechnens
	71740	System and Web Security
	71760	Security and Privacy
	78640	Grundlagen der Informationssicherheit
	78900	Introduction to Modern Cryptography

Modul: 10030 Architektur von Anwendungssystemen

2. Modulkürzel:	052010002	5. Moduldauer:	Einsemestrig
3. Leistungspunkte:	6 LP	6. Turnus:	Sommersemester
4. SWS:	4	7. Sprache:	Deutsch
8. Modulverantwortlicher:	Univ.-Prof. Dr. Frank Leymann		
9. Dozenten:	Frank Leymann		
10. Zuordnung zum Curriculum in diesem Studiengang:	B.A. (K) Informatik NF, PO 079-2-2009, 4. Semester → Katalog ISW --> Module im Nebenfach B.A. (K) Informatik NF, PO 079-2-2009, 4. Semester → Katalog ISG --> Module im Nebenfach		
11. Empfohlene Voraussetzungen:	Vorlesungen des Grundstudiums.		
12. Lernziele:	Die Vorlesung erläutert den Begriff der Architektur von Anwendungssystemen und die Rolle des Architekten solcher Systeme. Die wesentlichen Bestandteile von Anwendungsarchitektur wie etwa Datenbanksysteme, Anwendungsserver, Messaging Systeme, Workflowsysteme und TP-Monitore werden diskutiert. Die wesentlichen Mustern zur Erstellung von Anwendungssystemen sind verstanden.		
13. Inhalt:	Architekturelle Stile wie etwa N-stufige Aufbauten oder Service-Orientierung werden vorgestellt. Architekturmuster werden detailliert. Fundamentale Konzepte wie Transaktionen und Queuing werden eingeführt. Darauf aufbauend wird Direct TP vs Queues TP diskutiert. Grundlegende Qualitätseigenschaften wie Verfügbarkeit und Skalierbarkeit werden erläutert und Mechanismen zu deren Erzielen eingeführt. Die Rolle von Komponenten und Programmierung im Großen wird herausgearbeitet und Modell-getriebene Architektur vorgestellt.		
14. Literatur:	<ul style="list-style-type: none"> - A. Silberschatz, H. F. Korth, S. Sudarshan, Database System Concepts, 2002. - B. Neubauer, T. Ritter, F. Stoinnski, CORBA Komponenten, 2004. - F. Buschmann, R. Meunier, H. Rohnert, P. Sommerlad, M. Stal, Pattern-orientierte Software Architektur - Ein Patternsystem, 1998. - F. Leymann, D. Roller, Production Workflow, 2000. - L. Hohmann, Beyond Software Architecture, 2003. - M. Fowler, Patterns of Enterprise Application Architecture, 2003. - P. Bernstein, E. Newcomer, Principles of Transaction Processing, 1997. - S. Conrad, W. Hasselbring, A. Koschel, R. Tritsch, Enterprise Application Integration, 2006. - S. Weerawarana, F. Curbera, F. Leymann, T. Storey, D. Ferguson, Web Services Platform Architecture, 2005. - W. Emmerich, Konstruktion von verteilten Objekten, 2003. 		
15. Lehrveranstaltungen und -formen:	<ul style="list-style-type: none"> • 100301 Vorlesung Grundlagen der Architektur von Anwendungssystemen • 100302 Übung Grundlagen der Architektur von Anwendungssystemen 		
16. Abschätzung Arbeitsaufwand:			

17. Prüfungsnummer/n und -name:	10031 Architektur von Anwendungssystemen (PL), Schriftlich, 90 Min., Gewichtung: 1 [10031] Architektur von Anwendungssystemen (PL), schriftliche Prüfung, 60 Min., Gewicht: 1.0
18. Grundlage für ... :	- Modul Loose Coupling and Message Based Applications - Modul Service Computing - Modul Business Process Management
19. Medienform:	Vorlesungen mit begleitenden Übungen
20. Angeboten von:	Architektur von Anwendungssystemen

Modul: 10080 Datenbanken und Informationssysteme

2. Modulkürzel:	051200025	5. Moduldauer:	Einsemestrig
3. Leistungspunkte:	6 LP	6. Turnus:	Wintersemester
4. SWS:	4	7. Sprache:	Deutsch
8. Modulverantwortlicher:	Univ.-Prof. Dr.-Ing. Bernhard Mitschang		
9. Dozenten:	Bernhard Mitschang Holger Schwarz		
10. Zuordnung zum Curriculum in diesem Studiengang:	B.A. (K) Informatik NF, PO 079-2-2009, 5. Semester → Katalog ISG --> Module im Nebenfach B.A. (K) Informatik NF, PO 079-2-2009, 5. Semester → Katalog ISW --> Module im Nebenfach		
11. Empfohlene Voraussetzungen:	Kenntnisse zu Grundlagen der Datenbanken und Informationssysteme beispielsweise aus der Vorlesung "Modellierung" werden vorausgesetzt.		
12. Lernziele:	Die Studierenden haben die erforderlichen Kenntnisse für Datenbankprogrammierer in angemessenem Umfang erworben.		
13. Inhalt:	<p>Die Vorlesung "Datenbanken und Informationssysteme" ist als Einstiegsveranstaltung in das Vertiefungsgebiet Datenbanksysteme konzipiert. Aufbauend auf dem Inhalt der Vorlesung "Modellierung" werden insbesondere Entwurfs- und Realisierungsaspekte von Datenbanksystemen betrachtet. Die Entwicklung, Installation und Administration von Datenbanksystemen bestimmen hier sowohl Stoffauswahl als auch Detaillierungsgrad. Als Grundlage für alle weiteren Betrachtungen wird ein Schichtenmodell zur Beschreibung eines allgemeinen Datenbanksystems vorgestellt. Darauf aufbauend werden die einzelnen Systemschichten im Detail diskutiert, die dort zu realisierenden Komponenten betrachtet sowie die jeweils vorherrschenden Algorithmen beschrieben und bewertet. Im Einzelnen werden folgende Aspekte vertieft:</p> <ul style="list-style-type: none"> • Anwendungsprogrammierschnittstelle • Externspeicherverwaltung • DBS-Pufferverwaltung • Speicherungsstrukturen und Zugriffspfadstrukturen • Anfrageverarbeitung und Anfrageoptimierung • Transaktionsverarbeitung, Synchronisation • Logging und Recovery. 		
14. Literatur:	<ul style="list-style-type: none"> • A. Kemper, A. Eickler, Datenbanksysteme - Eine Einführung, 2004. • Th. Härder, E. Rahm, Datenbanksysteme, 2008. • H. Garcia-Molina, J. D. Ullman, J. Widom, Database Systems. The Complete Book, 2003. • R. Elmasri, S. Navathe, Fundamentals of Database Systems, 2003. 		
15. Lehrveranstaltungen und -formen:	<ul style="list-style-type: none"> • 100802 Übung Datenbanken und Informationssysteme • 100801 Vorlesung Datenbanken und Informationssysteme 		
16. Abschätzung Arbeitsaufwand:			

17. Prüfungsnummer/n und -name:
- 10081 Datenbanken und Informationssysteme (PL), Schriftlich oder Mündlich, 60 Min., Gewichtung: 1
 - V Vorleistung (USL-V), Schriftlich oder Mündlich
 - Schriftliche oder mündliche Prüfungsleistung, 60 Min., Gewicht: 1.0,
 - Prüfungsvorleistung: Modalitäten werden in der ersten Vorlesung angegeben
-

18. Grundlage für ... :

19. Medienform:

20. Angeboten von: Datenbanken und Informationssysteme

Modul: 10110 Grundlagen der Künstlichen Intelligenz

2. Modulkürzel:	051900205	5. Moduldauer:	Einsemestrig
3. Leistungspunkte:	6 LP	6. Turnus:	Wintersemester
4. SWS:	4	7. Sprache:	Deutsch
8. Modulverantwortlicher:	Univ.-Prof. Dr. Marc Toussaint		
9. Dozenten:	Daniel Hennes Marc Toussaint Andrés Bruhn		
10. Zuordnung zum Curriculum in diesem Studiengang:	B.A. (K) Informatik NF, PO 079-2-2009, 5. Semester → Katalog ISW --> Module im Nebenfach B.A. (K) Informatik NF, PO 079-2-2009, 5. Semester → Katalog ISG --> Module im Nebenfach		
11. Empfohlene Voraussetzungen:	- Modul 10190 Mathematik für Informatiker und Softwaretechniker		
12. Lernziele:	Der Student / die Studentin beherrscht die Grundlagen der Künstlichen Intelligenz, kann Probleme der KI selbständig einordnen und mit den erlernten Methoden und Algorithmen bearbeiten.		
13. Inhalt:	<ul style="list-style-type: none"> • Intelligenz • Agentenbegriff • Problemlösen durch Suchen, Suchverfahren • Probleme mit Rand- und Nebenbedingungen • Spiele • Aussagen- und Prädikatenlogik • Logikbasierte Agenten, Wissensrepräsentation • Inferenz • Planen • Unsicherheit, probabilistisches Schließen • Probabilistisches Schließen über die Zeit • Entscheidungstheorie 		
14. Literatur:	<ul style="list-style-type: none"> • S. Russell, P. Norvig, Künstliche Intelligenz: Ein Moderner Ansatz, 3. Aufl., 2012 • S. Russell, P. Norvig, Artificial Intelligence: A Modern Approach, 3rd Edition, 2009 		
15. Lehrveranstaltungen und -formen:	<ul style="list-style-type: none"> • 101101 Vorlesung Grundlagen der Künstlichen Intelligenz • 101102 Übung Grundlagen der Künstlichen Intelligenz 		
16. Abschätzung Arbeitsaufwand:			
17. Prüfungsnummer/n und -name:	<ul style="list-style-type: none"> • 10111 Grundlagen der Künstlichen Intelligenz (PL), Schriftlich, 90 Min., Gewichtung: 1 • V Vorleistung (USL-V), Schriftlich oder Mündlich [10111] Grundlagen der Künstlichen Intelligenz (PL), schriftliche Prüfung, 90 Min., Gewicht: 1.0 Prüfungsvorleistung: Übungsschein, Kriterien werden in der ersten Vorlesung bekannt gegeben [Prüfungsvorleistung] Vorleistung (USL-V), schriftlich, eventuell mündlich 		
18. Grundlage für ... :			
19. Medienform:			

20. Angeboten von: Autonome Systeme

Modul: 10170 Imaging Science

2. Modulkürzel:	051900210	5. Moduldauer:	Einsemestrig
3. Leistungspunkte:	6 LP	6. Turnus:	Sommersemester
4. SWS:	4	7. Sprache:	Englisch
8. Modulverantwortlicher:	Univ.-Prof. Dr.-Ing. Andrés Bruhn		
9. Dozenten:	Andrés Bruhn		
10. Zuordnung zum Curriculum in diesem Studiengang:	B.A. (K) Informatik NF, PO 079-2-2009, 4. Semester → Katalog ISW --> Module im Nebenfach B.A. (K) Informatik NF, PO 079-2-2009, 4. Semester → Katalog ISG --> Module im Nebenfach		
11. Empfohlene Voraussetzungen:	- Modul 10190 Mathematik für Informatiker und Softwaretechniker		
12. Lernziele:	Der Student / die Studentin beherrscht die Grundlagen der Repräsentation und Verarbeitung digitaler Bilder, kann Probleme aus dem Fachgebiet einordnen und selbständig mit den erlernten Algorithmen und Verfahren lösen.		
13. Inhalt:	<ul style="list-style-type: none"> • Grundlagen aus der Optik:Lochkamera, Linsengleichung • Bildaufnahme:Kameras, Objektive, Beleuchtung, Aufnahmeprozess • Bildrepräsentation:Diskretisierung, Farbräume • Elementare Bildbearbeitung:Punktoperationen (z.B. Kontrastverstärkung, Binarisierung) • Lineare und nichtlineare Filter:Faltung, morphologische Operatoren • Fouriertransformation, Bilddarstellung und -bearbeitung im Fourierraum, Abtasttheorem • Orthogonale Transformationen:Cosinus, Wavelets • Kompression:Generische Verfahren (RLE, Entropie), spezielle Bildverfahren (z.B. jpeg) • Video:Formate, Kompression (z.B. MPEG) • Bildverbesserung und Restauration • Elementare Segmentierungsverfahren 		
14. Literatur:	<ul style="list-style-type: none"> • Bässmann, Henning, Kreys, Jutta, Bildverarbeitung Ad Oculos, 2004. • Forsyth, David and Ponce, Jean, Computer Vision. A Modern Approach, 2003. • Gonzalez, Rafael C., Woods, Richard E., Eddins, Steven L., Digital Image Processing, 2004. • Bigun, J.: Vision with Direction, 2006. • Klaus D. Tönnies, Grundlagen der Bildverarbeitung, 2005. • L. G. Shapiro, G. C. Stockman, Computer Vision, 2001. 		
15. Lehrveranstaltungen und -formen:	<ul style="list-style-type: none"> • 101701 Vorlesung Imaging Science • 101702 Übung Imaging Science 		
16. Abschätzung Arbeitsaufwand:			
17. Prüfungsnummer/n und -name:	<ul style="list-style-type: none"> • 10171 Imaging Science (PL), Schriftlich oder Mündlich, 120 Min., Gewichtung: 1 • V Vorleistung (USL-V), Schriftlich oder Mündlich [10171] Imaging Science (PL), schriftlich, eventuell mündlich, 120 Min., Gewicht: 1.0, 		

Prüfungsvorleistung (USL-V): Übungsschein, Kriterien werden in der ersten Vorlesung bekannt gegeben, schriftlich, eventuell mündlich

18. Grundlage für ... : Modul Computer Vision
Modul Correspondence Problems in Computer Vision

19. Medienform:

20. Angeboten von: Intelligente Systeme

Modul: 10210 Mensch-Computer-Interaktion

2. Modulkürzel:	051900001	5. Moduldauer:	Einsemestrig
3. Leistungspunkte:	6 LP	6. Turnus:	Sommersemester
4. SWS:	4	7. Sprache:	Deutsch
8. Modulverantwortlicher:	Jun.-Prof. Dr. Niels Henze		
9. Dozenten:	Niels Henze Tonja Machulla		
10. Zuordnung zum Curriculum in diesem Studiengang:	B.A. (K) Informatik NF, PO 079-2-2009, 4. Semester → Katalog ISW --> Module im Nebenfach B.A. (K) Informatik NF, PO 079-2-2009, 4. Semester → Katalog ISG --> Module im Nebenfach		
11. Empfohlene Voraussetzungen:	Modul 10280 Programmierung und Software-Entwicklung		
12. Lernziele:	Studierende entwickeln ein Verständnis für Modelle, Methoden und Konzepte der Mensch-Computer-Interaktion. Sie lernen verschiedene Ansätze für den Entwurf, die Entwicklung und Bewertung von Benutzungsschnittstellen kennen und verstehen deren Vor- und Nachteile.		
13. Inhalt:	<p>Die Vorlesung vermittelt Konzepte, Prinzipien, Modelle, Methoden und Techniken für die effektive Entwicklung von benutzerfreundlichen Mensch-Computer-Schnittstellen. Das Thema moderner Benutzungsschnittstellen wird dabei für klassische Computer aber auch für mobile Geräte, eingebettete Systeme, Automobile und intelligente Umgebungen betrachtet. Die folgenden Themen werden in der Vorlesung behandelt:</p> <ul style="list-style-type: none"> • Einführung in die Grundlagen der Mensch-Computer Interaktion, historische Entwicklung • Entwurfsprinzipien und Modelle für moderne Benutzungsschnittstellen und interaktive Systeme • Informationsverarbeitung des Menschen, Wahrnehmung, Motorik, Eigenschaften und Fähigkeiten des Benutzers • Interaktionskonzepte und -stile, Metaphern, Normen, Regeln und Style Guides • Ein- und Ausgabegeräte, Entwurfsraum für interaktive Systeme • Analyse-, Entwurfs- und Entwicklungsmethoden und -werkzeuge für Benutzungsschnittstellen • Prototypische Realisierung und Implementierung von interaktiven Systemen, Werkzeuge • Architekturen für interaktive Systeme, User Interface Toolkits und Komponenten • Akzeptanz, Evaluationsmethoden und Qualitätssicherung 		
14. Literatur:	<ul style="list-style-type: none"> • Bernhard Preim, Raimund Dachsel. Interaktive Systeme 1: Grundlagen, Graphical User Interfaces, Informationsvisualisierung. Springer, Berlin, 2. Auflage. 2010 • Alan Dix, Janet Finley, Gregory Abowd, Russell Beale, Human-Computer Interaction, 2004 • Ben Shneiderman, Catherine Plaisant, Designing the User Interfaces, 2005 		
15. Lehrveranstaltungen und -formen:	<ul style="list-style-type: none"> • 102101 Vorlesung Mensch-Computer-Interaktion • 102102 Übung Mensch-Computer-Interaktion 		

16. Abschätzung Arbeitsaufwand:

17. Prüfungsnummer/n und -name:

- 10211 Mensch-Computer-Interaktion (PL), Schriftlich, 90 Min.,
Gewichtung: 1
- V Vorleistung (USL-V), Schriftlich oder Mündlich
Prüfungsvorleistung: Übungsschein

18. Grundlage für ... :

19. Medienform:

20. Angeboten von: Soziokognitive Systeme

Modul: 10220 Modellierung

2. Modulkürzel:	052010001	5. Moduldauer:	Einsemestrig
3. Leistungspunkte:	6 LP	6. Turnus:	Sommersemester
4. SWS:	4	7. Sprache:	Deutsch
8. Modulverantwortlicher:	Univ.-Prof. Dr. Frank Leymann		
9. Dozenten:	Bernhard Mitschang Frank Leymann Uwe Breitenbücher		
10. Zuordnung zum Curriculum in diesem Studiengang:	B.A. (K) Informatik NF, PO 079-2-2009, 4. Semester → Katalog ISW --> Module im Nebenfach B.A. (K) Informatik NF, PO 079-2-2009, 4. Semester → Katalog ISG --> Module im Nebenfach		
11. Empfohlene Voraussetzungen:	<ul style="list-style-type: none"> • Modul 10280 Programmierung und Software-Entwicklung • Modul 12060 Datenstrukturen und Algorithmen • Modul 40090 Systemkonzepte und -programmierung 		
12. Lernziele:	Am Ende des Moduls sind die Studierenden in der Lage, wesentliche Artefakte eines IT Systems zu modellieren. Der Zusammenhang und das Zusammenspiel solcher Artefakte ist verstanden. Die Rolle von Metamodellen und deren Erstellung ist klar.		
13. Inhalt:	<ul style="list-style-type: none"> • Entity-Relationship Modell und komplexe Objekte • Relationenmodell und Relationenalgebra , Überblick SQL - Transformationen von ER nach Relationen, Normalisierung • XML, DTD, XML-Schema, Info-Set, Namensräume • Metamodelle und Repository - RDF, RDF-S und Ontologien • UML • Petri Netze, Workflownetze • BPMN 		
14. Literatur:	<ul style="list-style-type: none"> • A. Silberschatz, H. F. Korth, S. Sudarshan, Database System Concepts, 2002. • R. Eckstein, S. Eckstein, XML und Datenmodellierung , dpunkt.verlag 2004. • M. Hitz, G. Kappel, E. Kapsammer, W. Retschitzegger, UML @ Work • Objektorientierte Modellierung mit UML2, 2005. • P. Hitzler, M. Krötzsch, S. Rudolph, Y. Sure, Semantic Web, 2008. • T.J. Teorey, Database Modeling und Design, 2nd Edition, 1994. • H.J. Habermann, F. Leymann, Repository , Oldenbourg 1993. • W. Reisig, Petri-Netze , Vieweg und Teubner 2010. • B. Silver, BPMN Method und Style ,Cody-Cassidy Press 2009. 		
15. Lehrveranstaltungen und -formen:	<ul style="list-style-type: none"> • 102201 Vorlesung Modellierung • 102202 Übung Modellierung 		
16. Abschätzung Arbeitsaufwand:			
17. Prüfungsnummer/n und -name:	<ul style="list-style-type: none"> • 10221 Modellierung (PL), Schriftlich, 90 Min., Gewichtung: 1 • V Vorleistung (USL-V), Schriftlich oder Mündlich 		

[10221] Modellierung (PL), schriftliche Prüfung, 90 Min., Gewicht:
1.0, Prüfungsvorleistung: Übungsschein [Prüfungsvorleistung]
Vorleistung (USL-V), schriftlich, eventuell mündlich

18. Grundlage für ... : Architektur von Anwendungssystemen Datenbanken und
Informationssysteme

19. Medienform:

20. Angeboten von: Architektur von Anwendungssystemen

Modul: 36530 Rechnerorganisation 1

2. Modulkürzel:	051700006	5. Moduldauer:	Einsemestrig
3. Leistungspunkte:	6 LP	6. Turnus:	Sommersemester
4. SWS:	4	7. Sprache:	Deutsch
8. Modulverantwortlicher:	Univ.-Prof. Dr.-Ing. Sven Simon		
9. Dozenten:	Sven Simon		
10. Zuordnung zum Curriculum in diesem Studiengang:	B.A. (K) Informatik NF, PO 079-2-2009, 5. Semester → Katalog ISW --> Module im Nebenfach B.A. (K) Informatik NF, PO 079-2-2009, 5. Semester → Katalog ISG --> Module im Nebenfach		
11. Empfohlene Voraussetzungen:	Einführung in die Technische Informatik (14360) oder Technische Grundlagen der Informatik (78650)		
12. Lernziele:	<ul style="list-style-type: none"> • Kenntnisse über die Grundlagen der Organisation von Rechnern und deren maschinennahe Programmierung • Grundzüge über die Beschreibung und den Entwurf von Hardwaresystemen 		
13. Inhalt:	Aufbau, Entwurf und maschinennahe Programmierung von Mikroprozessoren werden erläutert. In den Übungen wird das Wissen durch schriftliche Aufgaben sowie Labor-Übungen vertieft. Im Einzelnen werden behandelt: <ul style="list-style-type: none"> • Grundstrukturen: Logik Multiplexer, Speicher, Addierer, Multiplizierer, ALU • Zahlensysteme; Typ Integer, Typ Float, Gleitkommazahlen • Informationsdarstellung in Hardware: Daten- und Befehlsformate, Befehlssätze • Instruction Set Architecture • Assemblerprogrammierung • Grundzüge einer Hardware-Beschreibungssprache • RISC und CISC Architekturen • Steuerwerksentwurf und Mikroprogrammierung • Pipelining und Hazards • Speicherorganisation: Cachestrukturen und virtueller Speicher, Seitenverwaltung • Multi-Core Prozessoren • GPU-Architekturen und Programmierung • FPGA-Architekturen 		
14. Literatur:	Literatur, siehe Veranstaltungshinweise		
15. Lehrveranstaltungen und -formen:	<ul style="list-style-type: none"> • 365301 Vorlesung Rechnerorganisation 1 • 365302 Praktische und theoretische Übungen Rechnerorganisation 1 		
16. Abschätzung Arbeitsaufwand:			
17. Prüfungsnummer/n und -name:	<ul style="list-style-type: none"> • 36531 Rechnerorganisation 1 (PL), Schriftlich, 90 Min., Gewichtung: 1 • V Vorleistung (USL-V), Schriftlich 		
18. Grundlage für ... :			
19. Medienform:			

20. Angeboten von: Parallele Systeme

Modul: 39250 Distributed Systems I

2. Modulkürzel:	051200015	5. Moduldauer:	Einsemestrig
3. Leistungspunkte:	6 LP	6. Turnus:	Wintersemester
4. SWS:	4	7. Sprache:	Englisch
8. Modulverantwortlicher:	Kurt Rothermel		
9. Dozenten:	Kurt Rothermel Frank Dürr		
10. Zuordnung zum Curriculum in diesem Studiengang:	B.A. (K) Informatik NF, PO 079-2-2009, 5. Semester → Katalog ISG --> Module im Nebenfach B.A. (K) Informatik NF, PO 079-2-2009, 5. Semester → Katalog ISW --> Module im Nebenfach		
11. Empfohlene Voraussetzungen:	<ul style="list-style-type: none"> - Programmierung und Software-Entwicklung - Datenstrukturen und Algorithmen - Systemkonzepte und -programmierung 		
12. Lernziele:	<p>The Students will gain an understanding of the basic characteristics, concepts and methods of distributed systems. Furthermore, the ability to analyze existing distributed applications and platforms with regard to its specific properties will be obtained. The implementation of distributed applications as well as system platforms based on the shown methods of that course is another objective. Due to the knowledge provided in that course, the students will be able to communicate with other experts of other professional disciplines, about topics in the field of distributed systems.</p>		
13. Inhalt:	<ol style="list-style-type: none"> 1) Introduction to distributed systems 2) System models 3) Communication: Messages, Remote Procedure Call (RPC), Remote Method Invocation RMI 4) Naming: Generating and Resolution 5) Time Management and clocks in distributed Systems: Applications, logical clocks, physical clocks, synchronization of clocks 6) Global state: concepts, snapshot algorithms, distributed Debugging 7) Transaction management: Serializability, barrier methods, 2-phase-commit-protocols 8) Data replication: primary copy, consensus-protocols and other algorithms 9) Safety/Security: Methods for confidentiality, integrity, authentication and authorization 10) Multicast-algorithms: processing model, broadcast-semantics and algorithms 		
14. Literatur:	Literatur, siehe Webseite zur Veranstaltung		
15. Lehrveranstaltungen und -formen:	<ul style="list-style-type: none"> • 392502 Übungen Verteilte Systeme • 392501 Vorlesung Verteilte Systeme 		
16. Abschätzung Arbeitsaufwand:			
17. Prüfungsnummer/n und -name:	<ul style="list-style-type: none"> • 39251 Distributed Systems I (PL), Schriftlich oder Mündlich, 60 Min., Gewichtung: 1 		

- V Vorleistung (USL-V), Schriftlich oder Mündlich
[39251] Distributed Systems I (PL), schriftlich oder mündlich, 120
Min., Gewicht: 1.0, [Prüfungsvorleistung] Vorleistung (USL-V),
schriftlich, eventuell mündlich
-

18. Grundlage für ... :

19. Medienform:

20. Angeboten von: Verteilte Systeme

Modul: 42410 Grundlagen des Wissenschaftlichen Rechnens

2. Modulkürzel:	051240020	5. Moduldauer:	Einsemestrig
3. Leistungspunkte:	6 LP	6. Turnus:	Wintersemester
4. SWS:	4	7. Sprache:	Deutsch
8. Modulverantwortlicher:	Univ.-Prof. Dr. Dirk Pflüger		
9. Dozenten:	Miriam Mehl Stefan Zimmer Dirk Pflüger		
10. Zuordnung zum Curriculum in diesem Studiengang:	B.A. (K) Informatik NF, PO 079-2-2009, 4. Semester → Katalog ISG --> Module im Nebenfach B.A. (K) Informatik NF, PO 079-2-2009, 6. Semester → Katalog ISW --> Module im Nebenfach		
11. Empfohlene Voraussetzungen:	- Modul 10190 Mathematik für Informatiker und Softwaretechniker und - Modul 10240 Numerische und Stochastische Grundlagen der Informatik bzw. - Modul 41590 Einführung in die Numerik und Stochastik für Softwaretechniker		
12. Lernziele:	Kenntnis grundlegender Konzepte, Algorithmen und Methoden des Wissenschaftlichen Rechnens. Fähigkeit, mit den erlernten Kenntnissen selbständig Methoden zu entwickeln, zu analysieren und umzusetzen, mit denen anwendungsorientierte Probleme effizient und genau gelöst werden können.		
13. Inhalt:	- Überblick über die Simulationspipeline und die Wechselwirkungen zwischen den einzelnen Schritten - Skalenabhängige Modellierung - Diskretisierung (Gitter, Finite Elemente, Zeitschrittverfahren) - Algorithmen (Gittergenerierung, Adaptivität, Lineare Löser, Linked-Cell, Fast Multipole) - Parallelisierung (Gitterpartitionierung, Lastbalancierung) - Kurzer Überblick über die Visualisierung		
14. Literatur:	Martin Hanke-Bourgeois: Grundlagen der numerischen Mathematik und des wissenschaftlichen Rechnens, Vieweg+Teubner Verlag 2009.		
15. Lehrveranstaltungen und -formen:	<ul style="list-style-type: none"> • 424102 Übung Grundlagen des Wissenschaftlichen Rechnens • 424101 Vorlesung Grundlagen des Wissenschaftlichen Rechnens 		
16. Abschätzung Arbeitsaufwand:	Präsenzstunden: 42 h Eigenstudiumstunden: 138 h Gesamtstunden: 180 h		
17. Prüfungsnummer/n und -name:	42411 Grundlagen des Wissenschaftlichen Rechnens (PL), Schriftlich oder Mündlich, 90 Min., Gewichtung: 1 [42411] Grundlagen des Wissenschaftlichen Rechnens (PL), schriftlich oder mündlich, 90 Min., Gewicht: 1.0		
18. Grundlage für ... :			
19. Medienform:			
20. Angeboten von:	Simulation Software Engineering		

Modul: 42420 High Performance Computing

2. Modulkürzel:	051240040	5. Moduldauer:	Einsemestrig
3. Leistungspunkte:	6 LP	6. Turnus:	Sommersemester
4. SWS:	4	7. Sprache:	Deutsch
8. Modulverantwortlicher:	Univ.-Prof. Dr. Dirk Pflüger		
9. Dozenten:	Martin Bernreuther Miriam Mehl Dirk Pflüger		
10. Zuordnung zum Curriculum in diesem Studiengang:	B.A. (K) Informatik NF, PO 079-2-2009, 6. Semester → Katalog ISW --> Module im Nebenfach B.A. (K) Informatik NF, PO 079-2-2009, 6. Semester → Katalog ISG --> Module im Nebenfach		
11. Empfohlene Voraussetzungen:	<ul style="list-style-type: none"> • Modul 10190 Mathematik für Informatiker und Softwaretechniker und • Modul 10240 Numerische und Stochastische Grundlagen der Informatik bzw. • Modul 41590 Einführung in die Numerik und Stochastik für Softwaretechniker 		
12. Lernziele:	<ul style="list-style-type: none"> • Fähigkeit, parallele Algorithmen auf unterschiedlichen parallelen Plattformen mit Hilfe geeigneter algorithmischer Modelle zu bewerten. • Kenntnis verschiedener Programmiermodelle für Parallelrechner mit verteiltem und gemeinsamem Speicher. • Fähigkeit, auch fortgeschrittene Implementierungsaufgaben aus dem Bereich des Höchstleistungsrechnens auf Basis ausgewählter Programmiermodelle zu bewältigen. 		
13. Inhalt:	<p>Die Vorlesung beschäftigt sich mit den Grundlagen paralleler Programmierung und paralleler Algorithmen speziell im Hinblick auf die Anwendungsbereiche Wissenschaftliches Rechnen und High Performance Computing. Verwandte Fragestellungen aus dem Bereich der Theorie (parallele Modelle und parallele Komplexität, etc.) sowie aus der Rechnertechnik (parallele Architekturen) werden begleitend diskutiert. Nach einer allgemeinen Einführung (Klassifizierung von Parallelrechnern, Ebenen von Parallelität, Performance und Architekturen, etc.), werden die Grundlagen paralleler Programme eingeführt (Notation/Syntax, Synchronisation und Kommunikation, Design paralleler Programme, etc.). Sowohl die Programmierung auf Systemen mit gemeinsamem Speicher als auch auf Systemen mit verteiltem Speicher werden besprochen. Dabei wird jeweils mindestens ein geeignetes Programmiermodell (z.B. OpenMP, MPI, CUDA) vertieft behandelt. Aus dem Bereich des High Performance Computing werden begleitend klassische Algorithmen und Implementierungstechniken als Beispiele behandelt, z.B. parallele Algorithmen aus der linearen Algebra (Matrixmultiplikation, etc. oder einfache Verfahren zur Lösung partieller Differentialgleichungen). Zusätzlich können Themen wie Lastverteilung und Lastbalancierung (Grundlagen, Algorithmen zur Partitionierung und Lastbalancierung, etc.) vorgestellt werden.</p>		

14. Literatur:	<ul style="list-style-type: none">• T. Rauber, G. Rünger: „Parallele Programmierung , 2. Aufl., Springer 2007, (in English: T. Rauber, G. Rünger: „Parallel Programming: for Multicore and Cluster Systems , Springer 2010).• K.A. Berman, J.L. Paul: Sequential and Parallel Algorithms , PWS Publishing Company, 1997.• B. Chapman, G. Jost, R. van der Pas: Using OpenMP - Portable Shared Memory Parallel Programming , MIT Press, 2008.• W. Gropp, E. Lusk, und R. Thakur: Using MPI-2: Advanced Features of the Message-Passing Interface, das Buch ist auch in deutscher Übersetzung erhältlich.• D. Kirk, W.-M. Hwu Programming Massively Parallel Processors.
15. Lehrveranstaltungen und -formen:	<ul style="list-style-type: none">• 424201 Vorlesung High Performance Computing• 424202 Übung High Performance Computing
16. Abschätzung Arbeitsaufwand:	
17. Prüfungsnummer/n und -name:	42421 High Performance Computing (PL), Schriftlich oder Mündlich, 90 Min., Gewichtung: 1 [42421] High Performance Computing (PL), schriftlich oder mündlich, 90 Min., Gewicht: 1.0
18. Grundlage für ... :	
19. Medienform:	
20. Angeboten von:	Simulation Software Engineering

Modul: 42460 Numerische Simulation

2. Modulkürzel:	051240060	5. Moduldauer:	Einsemestrig
3. Leistungspunkte:	6 LP	6. Turnus:	Wintersemester
4. SWS:	4	7. Sprache:	Deutsch
8. Modulverantwortlicher:	Univ.-Prof. Dr. Dirk Pflüger		
9. Dozenten:	Miriam Mehl Stefan Zimmer Dirk Pflüger		
10. Zuordnung zum Curriculum in diesem Studiengang:	B.A. (K) Informatik NF, PO 079-2-2009, 5. Semester → Katalog ISG --> Module im Nebenfach B.A. (K) Informatik NF, PO 079-2-2009, 5. Semester → Katalog ISW --> Module im Nebenfach		
11. Empfohlene Voraussetzungen:	<ul style="list-style-type: none"> • Modul 10190 Mathematik für Informatiker und Softwaretechniker und • Modul 10240 Numerische und Stochastische Grundlagen der Informatik bzw. • Modul 41590 Einführung in die Numerik und Stochastik für Softwaretechniker • Modul 42410 Grundlagen des wissenschaftlichen Rechnens 		
12. Lernziele:	Fähigkeit zur Implementierung numerischer Methoden und Entwicklung und Umsetzung geeigneter Datenstrukturen.		
13. Inhalt:	Strukturmechanik, Strömungsmechanik, Finite Elemente, Finite Differenzen sowie praktische Aspekte der effizienten und parallelen Umsetzung auf Rechnern.		
14. Literatur:	<ul style="list-style-type: none"> • Griebel, Dornseifer, Neunhoeffler: Numerical simulation in fluid dynamics : a practical introduction, SIAM, 1998 / Numerische Simulation in der Strömungsmechanik, Vieweg 1995 • Griebel, Knappek, Zumbusch, Caglar: Numerische Simulation in der Moleküldynamik : Numerik, Algorithmen, Parallelisierung, Anwendungen, Springer 2004 • Braess: Finite Elemente : Theorie, schnelle Löser und Anwendungen in der Elastizitätstheorie, Springer, 2007 		
15. Lehrveranstaltungen und -formen:	<ul style="list-style-type: none"> • 424601 Vorlesung Numerische Simulation • 424602 Übung Numerische Simulation 		
16. Abschätzung Arbeitsaufwand:			
17. Prüfungsnummer/n und -name:	42461 Numerische Simulation (LBP), Schriftlich oder Mündlich, 90 Min., Gewichtung: 1		
18. Grundlage für ... :			
19. Medienform:			
20. Angeboten von:	Simulation Software Engineering		

Modul: 42480 Ausgewählte Kapitel des Wissenschaftlichen Rechnens

2. Modulkürzel:	051240030	5. Moduldauer:	Einsemestrig
3. Leistungspunkte:	6 LP	6. Turnus:	Wintersemester
4. SWS:	4	7. Sprache:	Deutsch
8. Modulverantwortlicher:	Univ.-Prof. Dr. Dirk Pflüger		
9. Dozenten:	Miriam Mehl Dirk Pflüger Stefan Zimmer		
10. Zuordnung zum Curriculum in diesem Studiengang:	B.A. (K) Informatik NF, PO 079-2-2009, 6. Semester → Katalog ISG --> Module im Nebenfach B.A. (K) Informatik NF, PO 079-2-2009, 6. Semester → Katalog ISW --> Module im Nebenfach		
11. Empfohlene Voraussetzungen:	<ul style="list-style-type: none"> • Modul 10190 Mathematik für Informatiker und Softwaretechniker und • Modul 10240 Numerische und Stochastische Grundlagen der Informatik bzw. • Modul 41590 Einführung in die Numerik und Stochastik für Softwaretechniker • Modul 42410 Grundlagen des wissenschaftlichen Rechnens 		
12. Lernziele:	Die Teilnehmer kennen ausgewählte aktuelle Forschungsthemen des wissenschaftlichen Rechnens und können mit der zugehörigen Primärliteratur arbeiten.		
13. Inhalt:	Aktuelle weiterführende Forschungsthemen des wissenschaftlichen Rechnens, wie z.B. adaptive Finite Elemente, hierarchische Basen und dünne Gitter, robuste Multilevellöser, Wavelets und schnelle Wavelettransformation, p-Version oder Spektralverfahren.		
14. Literatur:	Primärliteratur zu den behandelten Themen: <ul style="list-style-type: none"> • Bungartz/Griebel: Sparse Grids, Acta Numerica, Volume 13, p. 147-269. • Quarteroni/Valli: Numerical approximation of partial differential equations. • Quarteroni: Numerical models for differential problems. 		
15. Lehrveranstaltungen und -formen:	<ul style="list-style-type: none"> • 424801 Vorlesung Ausgewählte Kapitel des Wissenschaftlichen Rechnens • 424802 Übung Ausgewählte Kapitel des Wissenschaftlichen Rechnens 		
16. Abschätzung Arbeitsaufwand:			
17. Prüfungsnummer/n und -name:	42481 Ausgewählte Kapitel des Wissenschaftlichen Rechnens (PL), Schriftlich oder Mündlich, 90 Min., Gewichtung: 1 [42481] Ausgewählte Kapitel des Wissenschaftlichen Rechnens (PL), schriftlich oder mündlich, 90 Min., Gewicht: 1.0		
18. Grundlage für ... :			
19. Medienform:			
20. Angeboten von:	Simulation Software Engineering		

Modul: 71740 System and Web Security

2. Modulkürzel:	052900002	5. Moduldauer:	Einsemestrig
3. Leistungspunkte:	6 LP	6. Turnus:	Sommersemester
4. SWS:	4	7. Sprache:	Englisch
8. Modulverantwortlicher:	Univ.-Prof. Dr. rer. nat. Ralf Küsters		
9. Dozenten:	Ralf Küsters		
10. Zuordnung zum Curriculum in diesem Studiengang:	B.A. (K) Informatik NF, PO 079-2-2009, → Katalog ISG --> Module im Nebenfach B.A. (K) Informatik NF, PO 079-2-2009, → Katalog ISW --> Module im Nebenfach		
11. Empfohlene Voraussetzungen:	Solide Kenntnisse in mindestens einer Programmiersprache.		
12. Lernziele:	<ul style="list-style-type: none"> • Students are sensitized for common security vulnerabilities and attack vectors in computer systems and the web, • Students are familiar with concrete attacks on computer systems and the web, and understand the underlying principles, • Students are familiar with common defense mechanisms. 		
13. Inhalt:	<p>IT-systems are constantly under attack, by various kinds of attackers with diverse interests: criminal organizations with monetary interests, intelligence agencies, industrial espionage by states and companies.</p> <p>The course covers the most common attack vectors on computer systems, including mobile devices, and the web, including, for example, stack and heap overflows, format string vulnerabilities, integer overflows, return-oriented-programming, Cross-Site-Scripting (CSS/XSS), SQL Injections, and Cross-Site-Request-Forgery (XSRF), etc.</p> <p>The course also discusses common defense mechanisms, including, for example, access control mechanisms, address space layout randomization (ASLR), static code analysis, security monitoring, input/output sanitization, prepared statements, etc.</p>		
14. Literatur:	Will be announced in class		
15. Lehrveranstaltungen und -formen:	<ul style="list-style-type: none"> • 717401 Vorlesung System and Web Security • 717402 Übung System and Web Security 		
16. Abschätzung Arbeitsaufwand:	Vorlesung und Übung System- und Websicherheit		
17. Prüfungsnummer/n und -name:	<ul style="list-style-type: none"> • 71741 System and Web Security (PL), Schriftlich, Gewichtung: 1 • V Vorleistung (USL-V), Unbenotete Studienleistung als Vorleistung (USL-V); ausreichende Punktzahl in den Übungen Prüfungsleistung (PL): Klausur (90 Minuten) zur Vorlesung und Übung System- und Websicherheit		
18. Grundlage für ... :			
19. Medienform:	Projektor, Tafel		
20. Angeboten von:	Informationssicherheit		

Modul: 71760 Security and Privacy

2. Modulkürzel:	052900004	5. Moduldauer:	Einsemestrig
3. Leistungspunkte:	6 LP	6. Turnus:	Sommersemester
4. SWS:	4	7. Sprache:	Englisch
8. Modulverantwortlicher:	Univ.-Prof. Dr. rer. nat. Ralf Küsters		
9. Dozenten:	Ralf Küsters		
10. Zuordnung zum Curriculum in diesem Studiengang:	B.A. (K) Informatik NF, PO 079-2-2009, → Katalog ISG --> Module im Nebenfach B.A. (K) Informatik NF, PO 079-2-2009, → Katalog ISW --> Module im Nebenfach		
11. Empfohlene Voraussetzungen:	Kenntnisse aus den Vorlesungen <i>Grundlagen der Informationssicherheit</i> (Bachelor) sowie <i>Introduction to Modern Cryptography</i> (Master) sind vorteilhaft, werden allerdings nicht zwingend vorausgesetzt. Die Veranstaltung verlangt solide Kenntnisse in den Grundlagen der Informatik und der Mathematik wie sie in den ersten vier Semestern eines Bachelorstudiengangs in Informatik (oder Mathematik) vermittelt werden.		
12. Lernziele:	Students will acquire an in-depth understanding of central topics in information security and privacy.		
13. Inhalt:	This course covers some of the most important, typically advanced topics in information security and privacy. The selection of topics can vary from term to term, depending on the development of the field and the focus of the information security group. Possible topics include: <ul style="list-style-type: none"> • Zero-Knowledge Protocols: a fundamental concept in many advanced secure and privacy preserving systems • Verification of cryptographic protocols: What does it mean for protocols, such as TLS, to be secure? How can we prove security? Can we prove security using automated tools? • Blockchains, Smart Contracts, and applications, such as cryptocurrencies, e.g., Bitcoin and Ethereum. • Secure Multi-Party Computation: how can multiple parties compute a common function without revealing their input? E.g., how can two millionaires figure out who earns more without revealing their income to each other? • Differential Privacy and Privacy-Preserving Data Mining: how to make use of information in (statistical) databases without revealing information about individuals? • E-Voting: Can we have a system where voters can make sure that their votes were actually counted even when the voting servers are completely malicious? • Web-based security protocols, such as web-based single-sign on protocols • Advanced attacks and defenses in as well as models of web security 		
14. Literatur:	Will be announced in class.		
15. Lehrveranstaltungen und -formen:	<ul style="list-style-type: none"> • 717601 Vorlesung Security and Privacy • 717602 Übung Security and Privacy 		

16. Abschätzung Arbeitsaufwand:	Vorlesung und Übung zu Security and Privacy
17. Prüfungsnummer/n und -name:	<ul style="list-style-type: none">• 71761 Security and Privacy (PL), Schriftlich oder Mündlich, Gewichtung: 1• V Vorleistung (USL-V), Unbenotete Studienleistung als Vorleistung (USL-V); ausreichende Punktzahl in den Übungen Prüfungsleistung (PL): Klausur (90 Minuten) oder mündliche Prüfung (30 Minuten) zur Vorlesung und Übung Security and Privacy
18. Grundlage für ... :	
19. Medienform:	Projektor, Tafel
20. Angeboten von:	Informationssicherheit

Modul: 78640 Grundlagen der Informationssicherheit

2. Modulkürzel:	052900001	5. Moduldauer:	Einsemestrig
3. Leistungspunkte:	6 LP	6. Turnus:	Wintersemester
4. SWS:	4	7. Sprache:	Deutsch
8. Modulverantwortlicher:	Univ.-Prof. Dr. rer. nat. Ralf Küsters		
9. Dozenten:	Ralf Küsters		
10. Zuordnung zum Curriculum in diesem Studiengang:	B.A. (K) Informatik NF, PO 079-2-2009, → Katalog ISW --> Module im Nebenfach B.A. (K) Informatik NF, PO 079-2-2009, → Katalog ISG --> Module im Nebenfach		
11. Empfohlene Voraussetzungen:	Empfohlen werden Kenntnisse in den Grundlagen der Informatik und Mathematik wie sie in den ersten beiden Semestern eines Bachelorstudiengangs Informatik/Mathematik vermittelt werden.		
12. Lernziele:	Die Veranstaltung soll Studierende einerseits einen Überblick über die Informationssicherheit vermitteln und sie für dieses Thema sensibilisieren. Zum anderen lernen Studierende grundlegende Konzepte der Informationssicherheit kennen.		
13. Inhalt:	<p>Die moderne digitale Gesellschaft ist ohne Informationssicherheit nicht denkbar. Daten und sogar Geld sind digital, Kommunikation ist digital, kritische Infrastrukturen (Banken, Industrieanlagen, Verkehrsmittel, etc.) hängen stark von IT-Systemen ab. Es gibt kaum Lebensbereiche, die nicht von der Digitalisierung durchdrungen sind. Die digitale Welt ist deshalb ein attraktives Ziel für Angreifer aller Art (Kriminelle, Geheimdienste, Industriespione, Staaten, etc.) und mittlerweile ständigen Angriffen ausgesetzt. Diese Veranstaltung bietet eine erste Einführung in die Informationssicherheit. Unter anderem werden folgende Themen behandelt, wobei jeweils in der Praxis eingesetzte Verfahren betrachtet werden, deren Sicherheit untersucht wird und bekannte Angriffe vorgestellt werden.</p> <ul style="list-style-type: none"> • Grundlagen der Kryptographie • (Un-)Sicherheit von Netzwerkprotokollen, wie TCP, DNS, BGP, einschließlich <ul style="list-style-type: none"> • Denial-of-Service-Angriffe • Firewalls • Kryptographische Protokolle (TLS, SSH, WPA2, etc.) <ul style="list-style-type: none"> • Zertifikate und Public-Key-Infrastrukturen • Authentifizierung und Schlüsselaustausch • Zugriffskontrolle, z.B. in Linux, SELinux und Android • Grundlagen der Websicherheit • Ausblick Systemsicherheit 		
14. Literatur:	Wird in der Veranstaltung bekanntgegeben.		
15. Lehrveranstaltungen und -formen:	• 786401 Vorlesung/Übung zu Grundlagen der Informationssicherheit		
16. Abschätzung Arbeitsaufwand:			
17. Prüfungsnummer/n und -name:	<ul style="list-style-type: none"> • V Vorleistung (USL-V), • 78641 Grundlagen der Informationssicherheit (PL), Schriftlich oder Mündlich, Gewichtung: 1 		

Unbenotete Studienleistung als Vorleistung (USL-V); ausreichende Punktzahl in den Übungen sowie ggf. in einer Zwischenklausur;
Prüfungsleistung (PL): Klausur (90 Minuten) oder mündliche Prüfung (30 Minuten) zur Vorlesung und Übung Grundlagen der Informationssicherheit

18. Grundlage für ... :

19. Medienform: Projector, blackboard

20. Angeboten von: Informationssicherheit

Modul: 78900 Introduction to Modern Cryptography

2. Modulkürzel:	052900003	5. Moduldauer:	Einsemestrig
3. Leistungspunkte:	6 LP	6. Turnus:	Wintersemester
4. SWS:	4	7. Sprache:	Englisch
8. Modulverantwortlicher:	Univ.-Prof. Dr. rer. nat. Ralf Küsters		
9. Dozenten:	Ralf Küsters		
10. Zuordnung zum Curriculum in diesem Studiengang:	B.A. (K) Informatik NF, PO 079-2-2009, → Katalog ISG --> Module im Nebenfach B.A. (K) Informatik NF, PO 079-2-2009, → Katalog ISW --> Module im Nebenfach		
11. Empfohlene Voraussetzungen:	Die Veranstaltung verlangt solide Kenntnisse in den Grundlagen der Mathematik wie sie in den ersten drei oder vier Semestern eines Bachelorstudiengangs in Informatik/Mathematik vermittelt werden. Kenntnisse der Inhalte der Vorlesung <i>Grundlagen der Informationssicherheit</i> sind nützlich, aber keine zwingende Voraussetzung.		
12. Lernziele:	Students will acquire an in-depth understanding of cryptography. They will be able to judge and assess the security of cryptographic constructions used in practice (encryption schemes, digital signatures, messages authentication codes, etc.) and will be able to read scientific papers on cryptography.		
13. Inhalt:	<p>p { margin-bottom: 0.1in; direction: ltr; color: rgb(0, 0, 10); line-height: 120%; text-align: left; }p.western { font-family: "Calibri", serif; font-size: 11pt; }p.cjk { font-family: "Times New Roman"; font-size: 11pt; }p.cjl { font-family: "Times New Roman"; font-size: 11pt; }p.cjl { font-family: "Times New Roman"; font-size: 11pt; }a:link { color: rgb(0, 0, 255); }a.cjl:link { font-family: "Times New Roman"; }</p> <p>Cryptography is everywhere! We heavily rely on cryptography in our everyday life when we do, for example, online shopping and online banking, pay with credit or debit card, open doors with electronic keys, or when we use social networks, instant messengers, online games, WiFi, mobile networks, or electronic currencies. Here, cryptography is essential in order to guarantee various central security properties such as secrecy and integrity of messages as well as authenticity of the communication partners. This course provides an introduction to modern cryptography. In the traditional approach to cryptography, cryptographers proposed, for example, encryption algorithms, and then others, cryptanalysts, tried to break them. In modern cryptography, cryptographers try to prove that their cryptographic constructions are secure under certain assumptions, even when attacked by powerful adversaries. Hence, cryptography turned from pure art to science.</p> <p>The course covers several fundamental cryptographic primitives, including (symmetric and asymmetric) encryption, hash functions, digital signatures, and message authentication codes. These primitives are important building blocks for other cryptographic constructions and for cryptographic protocols (TLS, SSH, WPA2, etc.), used by billions of people every day. The course presents common cryptographic constructions as used in practice, such</p>		

as AES with various encryption modes (e.g., CBC, CTR), RSA, ElGamal, HMAC, PKCS#1, DSA. It also discusses public-key infrastructures and cryptographic protocols.

In the spirit of modern cryptography, we ask the following questions: What does it mean for an encryption algorithm, digital signature, etc. to be secure? Under which assumptions can we prove security? For several cryptographic constructions used in practice, including those mentioned above, we prove security or present attacks. This provides a deep understanding of the security/insecurity of the cryptography that surrounds us.

14. Literatur:	<ul style="list-style-type: none"> • Ralf Küsters and Thomas Wilke. Moderne Kryptographie - Eine Einführung. Vieweg + Teubner, 2011. • Jonathan Katz and Yehuda Lindell. Introduction to Modern Cryptography - Second Edition. CRC Press 2015.
15. Lehrveranstaltungen und -formen:	<ul style="list-style-type: none"> • 789001 Vorlesung und Übung zu Introduction to Modern Cryptography
16. Abschätzung Arbeitsaufwand:	Vorlesung und Übung zu Introduction to Modern Cryptography
17. Prüfungsnummer/n und -name:	<ul style="list-style-type: none"> • V Vorleistung (USL-V), • 78901 Introduction to Modern Cryptography (PL), Schriftlich oder Mündlich, Gewichtung: 1 <p>Unbenotete Studienleistung als Vorleistung (USL-V); ausreichende Punktzahl in den Übungen Prüfungsleistung (PL): Klausur (90 Minuten) oder mündliche Prüfung (30 Minuten) zur Vorlesung und Übung Introduction to Modern Cryptography</p>
18. Grundlage für ... :	
19. Medienform:	Projector, blackboard
20. Angeboten von:	Informationssicherheit

330 Katalog ISW

Zugeordnete Module:	10030	Architektur von Anwendungssystemen
	10040	Bildsynthese
	10060	Computergraphik
	10080	Datenbanken und Informationssysteme
	10110	Grundlagen der Künstlichen Intelligenz
	10120	Modellbildung und Simulation
	10170	Imaging Science
	10180	Information Retrieval and Text Mining
	10210	Mensch-Computer-Interaktion
	10220	Modellierung
	36530	Rechnerorganisation 1
	39040	Rechnernetze
	39250	Distributed Systems I
	42410	Grundlagen des Wissenschaftlichen Rechnens
	42420	High Performance Computing
	42460	Numerische Simulation
	42480	Ausgewählte Kapitel des Wissenschaftlichen Rechnens
	71740	System and Web Security
	71760	Security and Privacy
	72240	Model-Driven Software Development
	78640	Grundlagen der Informationssicherheit
	78900	Introduction to Modern Cryptography

Modul: 10030 Architektur von Anwendungssystemen

2. Modulkürzel:	052010002	5. Moduldauer:	Einsemestrig
3. Leistungspunkte:	6 LP	6. Turnus:	Sommersemester
4. SWS:	4	7. Sprache:	Deutsch
8. Modulverantwortlicher:	Univ.-Prof. Dr. Frank Leymann		
9. Dozenten:	Frank Leymann		
10. Zuordnung zum Curriculum in diesem Studiengang:	B.A. (K) Informatik NF, PO 079-2-2009, 4. Semester → Katalog ISW --> Module im Nebenfach B.A. (K) Informatik NF, PO 079-2-2009, 4. Semester → Katalog ISG --> Module im Nebenfach		
11. Empfohlene Voraussetzungen:	Vorlesungen des Grundstudiums.		
12. Lernziele:	Die Vorlesung erläutert den Begriff der Architektur von Anwendungssystemen und die Rolle des Architekten solcher Systeme. Die wesentlichen Bestandteile von Anwendungsarchitektur wie etwa Datenbanksysteme, Anwendungsserver, Messaging Systeme, Workflowsysteme und TP-Monitore werden diskutiert. Die wesentlichen Mustern zur Erstellung von Anwendungssystemen sind verstanden.		
13. Inhalt:	Architekturelle Stile wie etwa N-stufige Aufbauten oder Service-Orientierung werden vorgestellt. Architekturmuster werden detailliert. Fundamentale Konzepte wie Transaktionen und Queuing werden eingeführt. Darauf aufbauend wird Direct TP vs Queues TP diskutiert. Grundlegende Qualitätseigenschaften wie Verfügbarkeit und Skalierbarkeit werden erläutert und Mechanismen zu deren Erzielen eingeführt. Die Rolle von Komponenten und Programmierung im Großen wird herausgearbeitet und Modell-getriebene Architektur vorgestellt.		
14. Literatur:	<ul style="list-style-type: none"> - A. Silberschatz, H. F. Korth, S. Sudarshan, Database System Concepts, 2002. - B. Neubauer, T. Ritter, F. Stoinnski, CORBA Komponenten, 2004. - F. Buschmann, R. Meunier, H. Rohnert, P. Sommerlad, M. Stal, Pattern-orientierte Software Architektur - Ein Patternsystem, 1998. - F. Leymann, D. Roller, Production Workflow, 2000. - L. Hohmann, Beyond Software Architecture, 2003. - M. Fowler, Patterns of Enterprise Application Architecture, 2003. - P. Bernstein, E. Newcomer, Principles of Transaction Processing, 1997. - S. Conrad, W. Hasselbring, A. Koschel, R. Tritsch, Enterprise Application Integration, 2006. - S. Weerawarana, F. Curbera, F. Leymann, T. Storey, D. Ferguson, Web Services Platform Architecture, 2005. - W. Emmerich, Konstruktion von verteilten Objekten, 2003. 		
15. Lehrveranstaltungen und -formen:	<ul style="list-style-type: none"> • 100301 Vorlesung Grundlagen der Architektur von Anwendungssystemen • 100302 Übung Grundlagen der Architektur von Anwendungssystemen 		

16. Abschätzung Arbeitsaufwand:

17. Prüfungsnummer/n und -name:	10031 Architektur von Anwendungssystemen (PL), Schriftlich, 90 Min., Gewichtung: 1 [10031] Architektur von Anwendungssystemen (PL), schriftliche Prüfung, 60 Min., Gewicht: 1.0
18. Grundlage für ... :	- Modul Loose Coupling and Message Based Applications - Modul Service Computing - Modul Business Process Management
19. Medienform:	Vorlesungen mit begleitenden Übungen
20. Angeboten von:	Architektur von Anwendungssystemen

Modul: 10040 Bildsynthese

2. Modulkürzel:	051900012	5. Moduldauer:	Einsemestrig
3. Leistungspunkte:	6 LP	6. Turnus:	Sommersemester
4. SWS:	4	7. Sprache:	Deutsch
8. Modulverantwortlicher:	Univ.-Prof. Dr. Thomas Ertl		
9. Dozenten:	Thomas Ertl Daniel Weiskopf		
10. Zuordnung zum Curriculum in diesem Studiengang:	B.A. (K) Informatik NF, PO 079-2-2009, 4. Semester → Katalog ISW --> Module im Nebenfach		
11. Empfohlene Voraussetzungen:	- Modul 10060 Computergraphik		
12. Lernziele:	Die Studierenden besitzen Wissen über verschiedene Ansätze und Algorithmen der dreidimensionalen Computergraphik, physikalisch-basierte Verfahren wie Raytracing und Radiosity, die den Lichttransport und die Wechselwirkung mit Materie modellieren, und numerische Methoden wie Monte-Carlo-Integration und Finite-Elemente-Verfahren die es erlauben, die Rendering-Gleichung zu lösen. Darüber hinaus kennen sie interaktive Verfahren, die unter Ausnutzung programmierbarer Grafik-Hardware realistische Beleuchtungseffekte in Echtzeit approximieren können, sowie bildbasierte Ansätze, die ohne geometrische Daten realistische Darstellungen erzeugen. Bild-basierte Verfahren verzichten auf eine geometrische Repräsentation der Szene und erzeugen neue Ansichten aus anderen aufgenommenen Bildern.		
13. Inhalt:	In dieser Vorlesung werden die folgenden Themen behandelt: <ul style="list-style-type: none"> • Grafik Hardware und APIs, OpenGL • Texturen, prozedurale Modelle • Schattenberechnungen • Szenengraphen, Culling, Level-of-Detail Verfahren • Physikalisch-basierte Beleuchtungsberechnung, Fotorealistische Bildsynthese • Lokale Beleuchtungsmodelle • Raytracing, Monte-Carlo Methoden • Radiosity • Bild-basiertes Rendering 		
14. Literatur:	<ul style="list-style-type: none"> • Andrew S. Glassner: Principles of Digital Image Synthesis, 1995 • D. Eberly: 3D Game Engine Design: A Practical Approach to Real-Time Computer Graphics, 2000 • J. Foley, A. van Dam, S. Feiner, J. Hughes: Computer Graphics: Principle and Practice, 1990 • Literatur, siehe Webseite zur Veranstaltung • P. Dutre, P. Bekaert, K. Bala: Advanced Global Illumination, 2003 • Tomas Akenine-Möller, Eric Haines: Real-Time Rendering, 2002 • Matt Pharr, Greg Humphreys: Physically Based Rendering: From Theory To Implementation, Morgan Kaufmann Auflage: 2nd revised edition. (26. August 2010) • Peter Shirley et al: Fundamentals of Computer Graphics, Third Edition, A.K. Peters, July 2009 		
15. Lehrveranstaltungen und -formen:	<ul style="list-style-type: none"> • 100401 Vorlesung Bildsynthese 		

- 100402 Übung Bildsynthese
-

16. Abschätzung Arbeitsaufwand:

17. Prüfungsnummer/n und -name:

- 10041 Bildsynthese (PL), Mündlich, 30 Min., Gewichtung: 1
 - V Vorleistung (USL-V), Schriftlich oder Mündlich
- [10041] Bildsynthese (PL), mündliche Prüfung, 30 Min., Gewicht: 1.0 [Prüfungsvorleistung] Vorleistung (USL-V), schriftlich, eventuell mündlich, Übungsschein.
-

18. Grundlage für ... :

19. Medienform:

20. Angeboten von:

Praktische Informatik (Dialogsysteme)

Modul: 10060 Computergraphik

2. Modulkürzel:	051900002	5. Moduldauer:	Einsemestrig
3. Leistungspunkte:	6 LP	6. Turnus:	Wintersemester
4. SWS:	4	7. Sprache:	Deutsch
8. Modulverantwortlicher:	Univ.-Prof. Dr. Thomas Ertl		
9. Dozenten:	Thomas Ertl Daniel Weiskopf Michael Krone Guido Reina		
10. Zuordnung zum Curriculum in diesem Studiengang:	B.A. (K) Informatik NF, PO 079-2-2009, 5. Semester → Katalog ISW --> Module im Nebenfach		
11. Empfohlene Voraussetzungen:	<ul style="list-style-type: none"> • Modul 10210 Mensch-Computer-Interaktion • Modul 41590 Einführung in die Numerik und Stochastik 		
12. Lernziele:	Die Studierenden haben Wissen über die Grundlagen der Computergraphik sowie praktische Fähigkeiten in der Graphikprogrammierung erworben.		
13. Inhalt:	<p>Folgende Themen werden in der Vorlesung behandelt:</p> <ul style="list-style-type: none"> • Überblick über den Prozess der Bildsynthese • Graphische Geräte, visuelle Wahrnehmung, Farbsysteme • Grundlegende Rastergraphik und Bildverarbeitung • Raytracing und Beleuchtungsmodelle • 2D und 3D Geometrietransformationen, 3D Projektion • Graphikprogrammierung in OpenGL 3 • Texturen • Polygonale und hierarchische Modelle • Rasterisierung und Verdeckungsrechnung • Grundlagen der geometrischen Modellierung (Kurven, Flächen) • Räumliche Datenstrukturen <p>Die Veranstaltung besteht aus Vorlesung mit Übungen. Die Übungen umfassen praktische Programmierübungen, theoretische Themen und Programmierprojekte.</p>		
14. Literatur:	<ul style="list-style-type: none"> • J. Encarnacao, W. Strasser, R. Klein: Graphische Datenverarbeitung (Band1 und 2), 1997 • J. Foley, A. van Dam, S. Feiner, J. Hughes: Computer Graphics: Principle and Practice, 1990 		
15. Lehrveranstaltungen und -formen:	<ul style="list-style-type: none"> • 100601 Vorlesung Computergraphik • 100602 Übung Computergraphik 		
16. Abschätzung Arbeitsaufwand:			
17. Prüfungsnummer/n und -name:	<ul style="list-style-type: none"> • 10061 Computergraphik (PL), Schriftlich, 60 Min., Gewichtung: 1 • V Vorleistung (USL-V), Schriftlich oder Mündlich <p>Prüfungsvorleistung: Übungsschein.</p>		
18. Grundlage für ... :			
19. Medienform:			
20. Angeboten von:	Praktische Informatik (Dialogsysteme)		

Modul: 10080 Datenbanken und Informationssysteme

2. Modulkürzel:	051200025	5. Moduldauer:	Einsemestrig
3. Leistungspunkte:	6 LP	6. Turnus:	Wintersemester
4. SWS:	4	7. Sprache:	Deutsch
8. Modulverantwortlicher:	Univ.-Prof. Dr.-Ing. Bernhard Mitschang		
9. Dozenten:	Bernhard Mitschang Holger Schwarz		
10. Zuordnung zum Curriculum in diesem Studiengang:	B.A. (K) Informatik NF, PO 079-2-2009, 5. Semester → Katalog ISG --> Module im Nebenfach B.A. (K) Informatik NF, PO 079-2-2009, 5. Semester → Katalog ISW --> Module im Nebenfach		
11. Empfohlene Voraussetzungen:	Kenntnisse zu Grundlagen der Datenbanken und Informationssysteme beispielsweise aus der Vorlesung "Modellierung" werden vorausgesetzt.		
12. Lernziele:	Die Studierenden haben die erforderlichen Kenntnisse für Datenbankprogrammierer in angemessenem Umfang erworben.		
13. Inhalt:	<p>Die Vorlesung "Datenbanken und Informationssysteme" ist als Einstiegsveranstaltung in das Vertiefungsgebiet Datenbanksysteme konzipiert. Aufbauend auf dem Inhalt der Vorlesung "Modellierung" werden insbesondere Entwurfs- und Realisierungsaspekte von Datenbanksystemen betrachtet. Die Entwicklung, Installation und Administration von Datenbanksystemen bestimmen hier sowohl Stoffauswahl als auch Detaillierungsgrad. Als Grundlage für alle weiteren Betrachtungen wird ein Schichtenmodell zur Beschreibung eines allgemeinen Datenbanksystems vorgestellt. Darauf aufbauend werden die einzelnen Systemschichten im Detail diskutiert, die dort zu realisierenden Komponenten betrachtet sowie die jeweils vorherrschenden Algorithmen beschrieben und bewertet. Im Einzelnen werden folgende Aspekte vertieft:</p> <ul style="list-style-type: none"> • Anwendungsprogrammierschnittstelle • Externspeicherverwaltung • DBS-Pufferverwaltung • Speicherungsstrukturen und Zugriffspfadstrukturen • Anfrageverarbeitung und Anfrageoptimierung • Transaktionsverarbeitung, Synchronisation • Logging und Recovery. 		
14. Literatur:	<ul style="list-style-type: none"> • A. Kemper, A. Eickler, Datenbanksysteme - Eine Einführung, 2004. • Th. Härder, E. Rahm, Datenbanksysteme, 2008. • H. Garcia-Molina, J. D. Ullman, J. Widom, Database Systems. The Complete Book, 2003. • R. Elmasri, S. Navathe, Fundamentals of Database Systems, 2003. 		
15. Lehrveranstaltungen und -formen:	<ul style="list-style-type: none"> • 100802 Übung Datenbanken und Informationssysteme • 100801 Vorlesung Datenbanken und Informationssysteme 		
16. Abschätzung Arbeitsaufwand:			

17. Prüfungsnummer/n und -name:
- 10081 Datenbanken und Informationssysteme (PL), Schriftlich oder Mündlich, 60 Min., Gewichtung: 1
 - V Vorleistung (USL-V), Schriftlich oder Mündlich
 - Schriftliche oder mündliche Prüfungsleistung, 60 Min., Gewicht: 1.0,
 - Prüfungsvorleistung: Modalitäten werden in der ersten Vorlesung angegeben
-

18. Grundlage für ... :

19. Medienform:

20. Angeboten von: Datenbanken und Informationssysteme

Modul: 10110 Grundlagen der Künstlichen Intelligenz

2. Modulkürzel:	051900205	5. Moduldauer:	Einsemestrig
3. Leistungspunkte:	6 LP	6. Turnus:	Wintersemester
4. SWS:	4	7. Sprache:	Deutsch
8. Modulverantwortlicher:	Univ.-Prof. Dr. Marc Toussaint		
9. Dozenten:	Daniel Hennes Marc Toussaint Andrés Bruhn		
10. Zuordnung zum Curriculum in diesem Studiengang:	B.A. (K) Informatik NF, PO 079-2-2009, 5. Semester → Katalog ISW --> Module im Nebenfach B.A. (K) Informatik NF, PO 079-2-2009, 5. Semester → Katalog ISG --> Module im Nebenfach		
11. Empfohlene Voraussetzungen:	- Modul 10190 Mathematik für Informatiker und Softwaretechniker		
12. Lernziele:	Der Student / die Studentin beherrscht die Grundlagen der Künstlichen Intelligenz, kann Probleme der KI selbständig einordnen und mit den erlernten Methoden und Algorithmen bearbeiten.		
13. Inhalt:	<ul style="list-style-type: none"> • Intelligenz • Agentenbegriff • Problemlösen durch Suchen, Suchverfahren • Probleme mit Rand- und Nebenbedingungen • Spiele • Aussagen- und Prädikatenlogik • Logikbasierte Agenten, Wissensrepräsentation • Inferenz • Planen • Unsicherheit, probabilistisches Schließen • Probabilistisches Schließen über die Zeit • Entscheidungstheorie 		
14. Literatur:	<ul style="list-style-type: none"> • S. Russell, P. Norvig, Künstliche Intelligenz: Ein Moderner Ansatz, 3. Aufl., 2012 • S. Russell, P. Norvig, Artificial Intelligence: A Modern Approach, 3rd Edition, 2009 		
15. Lehrveranstaltungen und -formen:	<ul style="list-style-type: none"> • 101101 Vorlesung Grundlagen der Künstlichen Intelligenz • 101102 Übung Grundlagen der Künstlichen Intelligenz 		
16. Abschätzung Arbeitsaufwand:			
17. Prüfungsnummer/n und -name:	<ul style="list-style-type: none"> • 10111 Grundlagen der Künstlichen Intelligenz (PL), Schriftlich, 90 Min., Gewichtung: 1 • V Vorleistung (USL-V), Schriftlich oder Mündlich [10111] Grundlagen der Künstlichen Intelligenz (PL), schriftliche Prüfung, 90 Min., Gewicht: 1.0 Prüfungsvorleistung: Übungsschein, Kriterien werden in der ersten Vorlesung bekannt gegeben [Prüfungsvorleistung] Vorleistung (USL-V), schriftlich, eventuell mündlich 		
18. Grundlage für ... :			
19. Medienform:			

20. Angeboten von: Autonome Systeme

Modul: 10120 Modellbildung und Simulation

2. Modulkürzel:	051240010	5. Moduldauer:	Einsemestrig
3. Leistungspunkte:	6 LP	6. Turnus:	Sommersemester
4. SWS:	4	7. Sprache:	Deutsch
8. Modulverantwortlicher:	Univ.-Prof. Dr. Dirk Pflüger		
9. Dozenten:	Miriam Mehl Stefan Zimmer Dirk Pflüger		
10. Zuordnung zum Curriculum in diesem Studiengang:	B.A. (K) Informatik NF, PO 079-2-2009, 5. Semester → Katalog ISW --> Module im Nebenfach		
11. Empfohlene Voraussetzungen:	<ul style="list-style-type: none"> • Modul 10190 Mathematik für Informatiker und Softwaretechniker • Modul 10240 Numerische und Stochastische Grundlagen der Informatik 		
12. Lernziele:	Beherrschung des grundsätzlichen Vorgehens in der Modellbildung. Kenntnis einer Auswahl diskreter und kontinuierlicher Modelle und entsprechender Simulationsmethoden. Fähigkeit, mit den erlernten Kenntnissen selbständig numerische Methoden problemorientiert um- und einzusetzen.		
13. Inhalt:	<p>Diese Vorlesung bietet eine Einführung in die Grundlagen der Modellbildung und Simulation mit dem Ziel der Vorbereitung auf weiterführende Vorlesungen in diesem Bereich. Da Simulationsmethoden oft für viele verschiedene Problemklassen einsetzbar sind, ist die Vorlesung methodisch strukturiert. Den Hauptteil der Vorlesung bilden hierbei diskrete Modelle sowie deren Behandlung, aber auch kontinuierliche Modelle werden ergänzend gestreift. Ob diskrete Ereignissimulation, spieltheoretische Ansätze, Zelluläre Automaten, Räuber-Beute Modelle oder Fuzzy-Mengen: die verschiedenen Modellierungsansätze sind so vielfältig wie die Problemstellungen, auf die sie angewendet werden. Verkehrssimulation, Populationswachstum, Wahlen oder Regelung sind nur einige der Anwendungsbereiche aus den Natur- und Ingenieurwissenschaften.</p>		
14. Literatur:	<ul style="list-style-type: none"> • Modellbildung und Simulation - Eine anwendungsorientierte Einführung, Bungartz, H.-J., Zimmer, S., Buchholz, M., Pflüger, D., Springer Verlag, eXamen.press, 2013, ISBN 978-3-642-38656-6 		
15. Lehrveranstaltungen und -formen:	<ul style="list-style-type: none"> • 101201 Vorlesung Modellbildung und Simulation • 101202 Übung Modellbildung und Simulation 		
16. Abschätzung Arbeitsaufwand:			
17. Prüfungsnummer/n und -name:	10121 Modellbildung und Simulation (PL), Schriftlich oder Mündlich, 90 Min., Gewichtung: 1		
18. Grundlage für ... :			
19. Medienform:			
20. Angeboten von:	Simulation Software Engineering		

Modul: 10170 Imaging Science

2. Modulkürzel:	051900210	5. Moduldauer:	Einsemestrig
3. Leistungspunkte:	6 LP	6. Turnus:	Sommersemester
4. SWS:	4	7. Sprache:	Englisch
8. Modulverantwortlicher:	Univ.-Prof. Dr.-Ing. Andrés Bruhn		
9. Dozenten:	Andrés Bruhn		
10. Zuordnung zum Curriculum in diesem Studiengang:	B.A. (K) Informatik NF, PO 079-2-2009, 4. Semester → Katalog ISW --> Module im Nebenfach B.A. (K) Informatik NF, PO 079-2-2009, 4. Semester → Katalog ISG --> Module im Nebenfach		
11. Empfohlene Voraussetzungen:	- Modul 10190 Mathematik für Informatiker und Softwaretechniker		
12. Lernziele:	Der Student / die Studentin beherrscht die Grundlagen der Repräsentation und Verarbeitung digitaler Bilder, kann Probleme aus dem Fachgebiet einordnen und selbständig mit den erlernten Algorithmen und Verfahren lösen.		
13. Inhalt:	<ul style="list-style-type: none"> • Grundlagen aus der Optik:Lochkamera, Linsengleichung • Bildaufnahme:Kameras, Objektive, Beleuchtung, Aufnahmeprozess • Bildrepräsentation:Diskretisierung, Farbräume • Elementare Bildbearbeitung:Punktoperationen (z.B. Kontrastverstärkung, Binarisierung) • Lineare und nichtlineare Filter:Faltung, morphologische Operatoren • Fouriertransformation, Bilddarstellung und -bearbeitung im Fourierraum, Abtasttheorem • Orthogonale Transformationen:Cosinus, Wavelets • Kompression:Generische Verfahren (RLE, Entropie), spezielle Bildverfahren (z.B. jpeg) • Video:Formate, Kompression (z.B. MPEG) • Bildverbesserung und Restauration • Elementare Segmentierungsverfahren 		
14. Literatur:	<ul style="list-style-type: none"> • Bässmann, Henning, Kreys, Jutta, Bildverarbeitung Ad Oculos, 2004. • Forsyth, David and Ponce, Jean, Computer Vision. A Modern Approach, 2003. • Gonzalez, Rafael C., Woods, Richard E., Eddins, Steven L., Digital Image Processing, 2004. • Bigun, J.: Vision with Direction, 2006. • Klaus D. Tönnies, Grundlagen der Bildverarbeitung, 2005. • L. G. Shapiro, G. C. Stockman, Computer Vision, 2001. 		
15. Lehrveranstaltungen und -formen:	<ul style="list-style-type: none"> • 101701 Vorlesung Imaging Science • 101702 Übung Imaging Science 		
16. Abschätzung Arbeitsaufwand:			
17. Prüfungsnummer/n und -name:	<ul style="list-style-type: none"> • 10171 Imaging Science (PL), Schriftlich oder Mündlich, 120 Min., Gewichtung: 1 • V Vorleistung (USL-V), Schriftlich oder Mündlich [10171] Imaging Science (PL), schriftlich, eventuell mündlich, 120 Min., Gewicht: 1.0, 		

Prüfungsvorleistung (USL-V): Übungsschein, Kriterien werden in der ersten Vorlesung bekannt gegeben, schriftlich, eventuell mündlich

18. Grundlage für ... : Modul Computer Vision
Modul Correspondence Problems in Computer Vision

19. Medienform:

20. Angeboten von: Intelligente Systeme

Modul: 10180 Information Retrieval and Text Mining

2. Modulkürzel:	052401010	5. Moduldauer:	Einsemestrig
3. Leistungspunkte:	6 LP	6. Turnus:	Wintersemester
4. SWS:	4	7. Sprache:	Deutsch
8. Modulverantwortlicher:	Dr. Roman Klinger		
9. Dozenten:	Sebastian Pado Roman Klinger		
10. Zuordnung zum Curriculum in diesem Studiengang:	B.A. (K) Informatik NF, PO 079-2-2009, 5. Semester → Katalog ISW --> Module im Nebenfach		
11. Empfohlene Voraussetzungen:	Erfahrung mit Programmierung und Unix, erster Kontakt mit Verfahren des Maschinellen Lernens		
12. Lernziele:	Die Studierenden haben ein grundlegendes Verständnis der Konzepte und Algorithmen des Information Retrieval und Text Mining entwickelt.		
13. Inhalt:	<ul style="list-style-type: none"> • Textpräprozessierung • invertierte Indexe • IR-Modelle (z.B. Vektorraum-basiertes IR) • Linkanalyse • Clustering • Frage-Antwort-Systeme • korpusbasierter Erwerb von lexikalischem und Weltwissen 		
14. Literatur:	- Chris Manning, Prabhakar Raghavan, Hinrich Schütze, Introduction to Information Retrieval, 2008 Cambridge University Press.		
15. Lehrveranstaltungen und -formen:	<ul style="list-style-type: none"> • 101801 Vorlesung Information Retrieval and Text Mining • 101802 Übung Information Retrieval and Text Mining 		
16. Abschätzung Arbeitsaufwand:	Präsenzstunden: 42 h Eigenstudiumstunden: 138 h Gesamtstunden: 180 h		
17. Prüfungsnummer/n und -name:	<ul style="list-style-type: none"> • 10181 Information Retrieval and Text Mining (PL), Schriftlich, Gewichtung: 1 • 10182 Information Retrieval und Text Mining - Hausübungen (USL), Sonstige, Gewichtung: 1 [10181] Information Retrieval und Text Mining (PL), schriftliche Prüfung, 60 Min., Gewicht: 1.0 [10182] Information Retrieval und Text Mining - Hausübungen (USL), Sonstiges		
18. Grundlage für ... :			
19. Medienform:			
20. Angeboten von:	Theoretische Computerlinguistik		

Modul: 10210 Mensch-Computer-Interaktion

2. Modulkürzel:	051900001	5. Moduldauer:	Einsemestrig
3. Leistungspunkte:	6 LP	6. Turnus:	Sommersemester
4. SWS:	4	7. Sprache:	Deutsch
8. Modulverantwortlicher:	Jun.-Prof. Dr. Niels Henze		
9. Dozenten:	Niels Henze Tonja Machulla		
10. Zuordnung zum Curriculum in diesem Studiengang:	B.A. (K) Informatik NF, PO 079-2-2009, 4. Semester → Katalog ISW --> Module im Nebenfach B.A. (K) Informatik NF, PO 079-2-2009, 4. Semester → Katalog ISG --> Module im Nebenfach		
11. Empfohlene Voraussetzungen:	Modul 10280 Programmierung und Software-Entwicklung		
12. Lernziele:	Studierende entwickeln ein Verständnis für Modelle, Methoden und Konzepte der Mensch-Computer-Interaktion. Sie lernen verschiedene Ansätze für den Entwurf, die Entwicklung und Bewertung von Benutzungsschnittstellen kennen und verstehen deren Vor- und Nachteile.		
13. Inhalt:	<p>Die Vorlesung vermittelt Konzepte, Prinzipien, Modelle, Methoden und Techniken für die effektive Entwicklung von benutzerfreundlichen Mensch-Computer-Schnittstellen. Das Thema moderner Benutzungsschnittstellen wird dabei für klassische Computer aber auch für mobile Geräte, eingebettete Systeme, Automobile und intelligente Umgebungen betrachtet. Die folgenden Themen werden in der Vorlesung behandelt:</p> <ul style="list-style-type: none"> • Einführung in die Grundlagen der Mensch-Computer Interaktion, historische Entwicklung • Entwurfsprinzipien und Modelle für moderne Benutzungsschnittstellen und interaktive Systeme • Informationsverarbeitung des Menschen, Wahrnehmung, Motorik, Eigenschaften und Fähigkeiten des Benutzers • Interaktionskonzepte und -stile, Metaphern, Normen, Regeln und Style Guides • Ein- und Ausgabegeräte, Entwurfsraum für interaktive Systeme • Analyse-, Entwurfs- und Entwicklungsmethoden und -werkzeuge für Benutzungsschnittstellen • Prototypische Realisierung und Implementierung von interaktiven Systemen, Werkzeuge • Architekturen für interaktive Systeme, User Interface Toolkits und Komponenten • Akzeptanz, Evaluationsmethoden und Qualitätssicherung 		
14. Literatur:	<ul style="list-style-type: none"> • Bernhard Preim, Raimund Dachsel. Interaktive Systeme 1: Grundlagen, Graphical User Interfaces, Informationsvisualisierung. Springer, Berlin, 2. Auflage. 2010 • Alan Dix, Janet Finley, Gregory Abowd, Russell Beale, Human-Computer Interaction, 2004 • Ben Shneiderman, Catherine Plaisant, Designing the User Interfaces, 2005 		
15. Lehrveranstaltungen und -formen:	<ul style="list-style-type: none"> • 102101 Vorlesung Mensch-Computer-Interaktion • 102102 Übung Mensch-Computer-Interaktion 		

16. Abschätzung Arbeitsaufwand:

17. Prüfungsnummer/n und -name:

- 10211 Mensch-Computer-Interaktion (PL), Schriftlich, 90 Min.,
Gewichtung: 1
 - V Vorleistung (USL-V), Schriftlich oder Mündlich
Prüfungsvorleistung: Übungsschein
-

18. Grundlage für ... :

19. Medienform:

20. Angeboten von:

Soziokognitive Systeme

Modul: 10220 Modellierung

2. Modulkürzel:	052010001	5. Moduldauer:	Einsemestrig
3. Leistungspunkte:	6 LP	6. Turnus:	Sommersemester
4. SWS:	4	7. Sprache:	Deutsch
8. Modulverantwortlicher:	Univ.-Prof. Dr. Frank Leymann		
9. Dozenten:	Bernhard Mitschang Frank Leymann Uwe Breitenbücher		
10. Zuordnung zum Curriculum in diesem Studiengang:	B.A. (K) Informatik NF, PO 079-2-2009, 4. Semester → Katalog ISW --> Module im Nebenfach B.A. (K) Informatik NF, PO 079-2-2009, 4. Semester → Katalog ISG --> Module im Nebenfach		
11. Empfohlene Voraussetzungen:	<ul style="list-style-type: none"> • Modul 10280 Programmierung und Software-Entwicklung • Modul 12060 Datenstrukturen und Algorithmen • Modul 40090 Systemkonzepte und -programmierung 		
12. Lernziele:	Am Ende des Moduls sind die Studierenden in der Lage, wesentliche Artefakte eines IT Systems zu modellieren. Der Zusammenhang und das Zusammenspiel solcher Artefakte ist verstanden. Die Rolle von Metamodellen und deren Erstellung ist klar.		
13. Inhalt:	<ul style="list-style-type: none"> • Entity-Relationship Modell und komplexe Objekte • Relationenmodell und Relationenalgebra , Überblick SQL - Transformationen von ER nach Relationen, Normalisierung • XML, DTD, XML-Schema, Info-Set, Namensräume • Metamodelle und Repository - RDF, RDF-S und Ontologien • UML • Petri Netze, Workflownetze • BPMN 		
14. Literatur:	<ul style="list-style-type: none"> • A. Silberschatz, H. F. Korth, S. Sudarshan, Database System Concepts, 2002. • R. Eckstein, S. Eckstein, XML und Datenmodellierung , dpunkt.verlag 2004. • M. Hitz, G. Kappel, E. Kapsammer, W. Retschitzegger, UML @ Work • Objektorientierte Modellierung mit UML2, 2005. • P. Hitzler, M. Krötzsch, S. Rudolph, Y. Sure, Semantic Web, 2008. • T.J. Teorey, Database Modeling und Design, 2nd Edition, 1994. • H.J. Habermann, F. Leymann, Repository , Oldenbourg 1993. • W. Reisig, Petri-Netze , Vieweg und Teubner 2010. • B. Silver, BPMN Method und Style ,Cody-Cassidy Press 2009. 		
15. Lehrveranstaltungen und -formen:	<ul style="list-style-type: none"> • 102201 Vorlesung Modellierung • 102202 Übung Modellierung 		
16. Abschätzung Arbeitsaufwand:			
17. Prüfungsnummer/n und -name:	<ul style="list-style-type: none"> • 10221 Modellierung (PL), Schriftlich, 90 Min., Gewichtung: 1 • V Vorleistung (USL-V), Schriftlich oder Mündlich 		

[10221] Modellierung (PL), schriftliche Prüfung, 90 Min., Gewicht:
1.0, Prüfungsvorleistung: Übungsschein [Prüfungsvorleistung]
Vorleistung (USL-V), schriftlich, eventuell mündlich

18. Grundlage für ... : Architektur von Anwendungssystemen Datenbanken und
Informationssysteme

19. Medienform:

20. Angeboten von: Architektur von Anwendungssystemen

Modul: 36530 Rechnerorganisation 1

2. Modulkürzel:	051700006	5. Moduldauer:	Einsemestrig
3. Leistungspunkte:	6 LP	6. Turnus:	Sommersemester
4. SWS:	4	7. Sprache:	Deutsch
8. Modulverantwortlicher:	Univ.-Prof. Dr.-Ing. Sven Simon		
9. Dozenten:	Sven Simon		
10. Zuordnung zum Curriculum in diesem Studiengang:	B.A. (K) Informatik NF, PO 079-2-2009, 5. Semester → Katalog ISW --> Module im Nebenfach B.A. (K) Informatik NF, PO 079-2-2009, 5. Semester → Katalog ISG --> Module im Nebenfach		
11. Empfohlene Voraussetzungen:	Einführung in die Technische Informatik (14360) oder Technische Grundlagen der Informatik (78650)		
12. Lernziele:	<ul style="list-style-type: none"> • Kenntnisse über die Grundlagen der Organisation von Rechnern und deren maschinennahe Programmierung • Grundzüge über die Beschreibung und den Entwurf von Hardwaresystemen 		
13. Inhalt:	Aufbau, Entwurf und maschinennahe Programmierung von Mikroprozessoren werden erläutert. In den Übungen wird das Wissen durch schriftliche Aufgaben sowie Labor-Übungen vertieft. Im Einzelnen werden behandelt: <ul style="list-style-type: none"> • Grundstrukturen: Logik Multiplexer, Speicher, Addierer, Multiplizierer, ALU • Zahlensysteme; Typ Integer, Typ Float, Gleitkommazahlen • Informationsdarstellung in Hardware: Daten- und Befehlsformate, Befehlssätze • Instruction Set Architecture • Assemblerprogrammierung • Grundzüge einer Hardware-Beschreibungssprache • RISC und CISC Architekturen • Steuerwerksentwurf und Mikroprogrammierung • Pipelining und Hazards • Speicherorganisation: Cachestrukturen und virtueller Speicher, Seitenverwaltung • Multi-Core Prozessoren • GPU-Architekturen und Programmierung • FPGA-Architekturen 		
14. Literatur:	Literatur, siehe Veranstaltungshinweise		
15. Lehrveranstaltungen und -formen:	<ul style="list-style-type: none"> • 365301 Vorlesung Rechnerorganisation 1 • 365302 Praktische und theoretische Übungen Rechnerorganisation 1 		
16. Abschätzung Arbeitsaufwand:			
17. Prüfungsnummer/n und -name:	<ul style="list-style-type: none"> • 36531 Rechnerorganisation 1 (PL), Schriftlich, 90 Min., Gewichtung: 1 • V Vorleistung (USL-V), Schriftlich 		
18. Grundlage für ... :			
19. Medienform:			

20. Angeboten von:

Parallele Systeme

Modul: 39040 Rechnernetze

2. Modulkürzel:	051200010	5. Moduldauer:	Einsemestrig
3. Leistungspunkte:	6 LP	6. Turnus:	Sommersemester
4. SWS:	4	7. Sprache:	Deutsch
8. Modulverantwortlicher:	Univ.-Prof. Dr. Kurt Rothermel		
9. Dozenten:	Kurt Rothermel Frank Dürr		
10. Zuordnung zum Curriculum in diesem Studiengang:	B.A. (K) Informatik NF, PO 079-2-2009, 4. Semester → Katalog ISW --> Module im Nebenfach		
11. Empfohlene Voraussetzungen:	<ul style="list-style-type: none"> - Programmierung und Software-Entwicklung - Datenstrukturen und Algorithmen - Grundkenntnisse in Java 		
12. Lernziele:	<ul style="list-style-type: none"> - Versteht grundsätzliche Eigenschaften, Konzepte und Methoden von Rechnernetzen, insbesondere dem Internet. - Versteht Schichten und deren Zusammenwirken in einem Protokollstapel - Kann Rechnernetze aufbauen, verwalten und analysieren. - Kann Protokolle entwickeln und in Schichtenarchitektur einbetten. - Kann höhere Kommunikationsdienste zur Entwicklung von netzgestützten Systemen anwenden. - Kann sich mit Experten anderer Domänen über Methoden der Rechnernetze verständigen. 		
13. Inhalt:	<ul style="list-style-type: none"> • Einführung in die Rechnernetze, ISO Referenzmodell, • Bitübertragungsschicht: Übertragungsmedien, analoge und digitale Informationskodierung und -übertragung, Vermittlungsarten, • Sicherungsschicht: Betriebsarten, Fehlererkennung und -behandlung, Flusskontrolle, • Lokale Netze: CSMA/CD, Token Ring, Token Bus, FDDI, Kopplung, • Vermittlungsschicht: Verbindungsorientierter und verbindungsloser Dienst, Leitwegbestimmung, Überlastkontrolle, • Internetworking, • Internet-Protokoll, • Transportschicht: ausgewählte Realisierungsprobleme und Internet-Protokolle, • Echtzeitkommunikation: IntServ, DiffServ, Sicherheit: Verfahren, IPsec, SSL, TLS. 		
14. Literatur:	<ul style="list-style-type: none"> • A.S. Tanenbaum, Computer Networks, 4th Edition, 2003 - D.E. Comer, Computernetzwerke und Internets, 2000 • D.E. Comer, Internetworking with TCP/IP Volume I: Principles, Protocols, and Architecture, 1995 • J. F. Kurose, K. W. Ross, Computer Networks: a top-down approach featuring the Internet, 2001 • L.L. Peterson, B.S. Davie, Computer Networks: A Systems Approach, 1999 		
15. Lehrveranstaltungen und -formen:	<ul style="list-style-type: none"> • 390401 VL Rechnernetze 		

- 390402 ÜB Rechnernetze
-

16. Abschätzung Arbeitsaufwand:

17. Prüfungsnummer/n und -name:

- 39041 Rechnernetze (PL), Schriftlich oder Mündlich, 90 Min.,
Gewichtung: 1
 - V Vorleistung (USL-V), Schriftlich oder Mündlich
Prüfungsdauer: 90 min schriftlich oder 30 min mündlich
-

18. Grundlage für ... :

19. Medienform:

20. Angeboten von:

Verteilte Systeme

Modul: 39250 Distributed Systems I

2. Modulkürzel:	051200015	5. Moduldauer:	Einsemestrig
3. Leistungspunkte:	6 LP	6. Turnus:	Wintersemester
4. SWS:	4	7. Sprache:	Englisch
8. Modulverantwortlicher:	Kurt Rothermel		
9. Dozenten:	Kurt Rothermel Frank Dürr		
10. Zuordnung zum Curriculum in diesem Studiengang:	B.A. (K) Informatik NF, PO 079-2-2009, 5. Semester → Katalog ISG --> Module im Nebenfach B.A. (K) Informatik NF, PO 079-2-2009, 5. Semester → Katalog ISW --> Module im Nebenfach		
11. Empfohlene Voraussetzungen:	<ul style="list-style-type: none"> - Programmierung und Software-Entwicklung - Datenstrukturen und Algorithmen - Systemkonzepte und -programmierung 		
12. Lernziele:	<p>The Students will gain an understanding of the basic characteristics, concepts and methods of distributed systems. Furthermore, the ability to analyze existing distributed applications and platforms with regard to its specific properties will be obtained. The implementation of distributed applications as well as system platforms based on the shown methods of that course is another objective. Due to the knowledge provided in that course, the students will be able to communicate with other experts of other professional disciplines, about topics in the field of distributed systems.</p>		
13. Inhalt:	<ol style="list-style-type: none"> 1) Introduction to distributed systems 2) System models 3) Communication: Messages, Remote Procedure Call (RPC), Remote Method Invocation RMI 4) Naming: Generating and Resolution 5) Time Management and clocks in distributed Systems: Applications, logical clocks, physical clocks, synchronization of clocks 6) Global state: concepts, snapshot algorithms, distributed Debugging 7) Transaction management: Serializability, barrier methods, 2-phase-commit-protocols 8) Data replication: primary copy, consensus-protocols and other algorithms 9) Safety/Security: Methods for confidentiality, integrity, authentication and authorization 10) Multicast-algorithms: processing model, broadcast-semantics and algorithms 		
14. Literatur:	Literatur, siehe Webseite zur Veranstaltung		
15. Lehrveranstaltungen und -formen:	<ul style="list-style-type: none"> • 392502 Übungen Verteilte Systeme • 392501 Vorlesung Verteilte Systeme 		
16. Abschätzung Arbeitsaufwand:			
17. Prüfungsnummer/n und -name:	<ul style="list-style-type: none"> • 39251 Distributed Systems I (PL), Schriftlich oder Mündlich, 60 Min., Gewichtung: 1 		

- V Vorleistung (USL-V), Schriftlich oder Mündlich
[39251] Distributed Systems I (PL), schriftlich oder mündlich, 120
Min., Gewicht: 1.0, [Prüfungsvorleistung] Vorleistung (USL-V),
schriftlich, eventuell mündlich
-

18. Grundlage für ... :

19. Medienform:

20. Angeboten von: Verteilte Systeme

Modul: 42410 Grundlagen des Wissenschaftlichen Rechnens

2. Modulkürzel:	051240020	5. Moduldauer:	Einsemestrig
3. Leistungspunkte:	6 LP	6. Turnus:	Wintersemester
4. SWS:	4	7. Sprache:	Deutsch
8. Modulverantwortlicher:	Univ.-Prof. Dr. Dirk Pflüger		
9. Dozenten:	Miriam Mehl Stefan Zimmer Dirk Pflüger		
10. Zuordnung zum Curriculum in diesem Studiengang:	B.A. (K) Informatik NF, PO 079-2-2009, 4. Semester → Katalog ISG --> Module im Nebenfach B.A. (K) Informatik NF, PO 079-2-2009, 6. Semester → Katalog ISW --> Module im Nebenfach		
11. Empfohlene Voraussetzungen:	- Modul 10190 Mathematik für Informatiker und Softwaretechniker und - Modul 10240 Numerische und Stochastische Grundlagen der Informatik bzw. - Modul 41590 Einführung in die Numerik und Stochastik für Softwaretechniker		
12. Lernziele:	Kenntnis grundlegender Konzepte, Algorithmen und Methoden des Wissenschaftlichen Rechnens. Fähigkeit, mit den erlernten Kenntnissen selbständig Methoden zu entwickeln, zu analysieren und umzusetzen, mit denen anwendungsorientierte Probleme effizient und genau gelöst werden können.		
13. Inhalt:	- Überblick über die Simulationspipeline und die Wechselwirkungen zwischen den einzelnen Schritten - Skalenabhängige Modellierung - Diskretisierung (Gitter, Finite Elemente, Zeitschrittverfahren) - Algorithmen (Gittergenerierung, Adaptivität, Lineare Löser, Linked-Cell, Fast Multipole) - Parallelisierung (Gitterpartitionierung, Lastbalancierung) - Kurzer Überblick über die Visualisierung		
14. Literatur:	Martin Hanke-Bourgeois: Grundlagen der numerischen Mathematik und des wissenschaftlichen Rechnens, Vieweg+Teubner Verlag 2009.		
15. Lehrveranstaltungen und -formen:	<ul style="list-style-type: none"> • 424102 Übung Grundlagen des Wissenschaftlichen Rechnens • 424101 Vorlesung Grundlagen des Wissenschaftlichen Rechnens 		
16. Abschätzung Arbeitsaufwand:	Präsenzstunden: 42 h Eigenstudiumstunden: 138 h Gesamtstunden: 180 h		
17. Prüfungsnummer/n und -name:	42411 Grundlagen des Wissenschaftlichen Rechnens (PL), Schriftlich oder Mündlich, 90 Min., Gewichtung: 1 [42411] Grundlagen des Wissenschaftlichen Rechnens (PL), schriftlich oder mündlich, 90 Min., Gewicht: 1.0		
18. Grundlage für ... :			
19. Medienform:			
20. Angeboten von:	Simulation Software Engineering		

Modul: 42420 High Performance Computing

2. Modulkürzel:	051240040	5. Moduldauer:	Einsemestrig
3. Leistungspunkte:	6 LP	6. Turnus:	Sommersemester
4. SWS:	4	7. Sprache:	Deutsch
8. Modulverantwortlicher:	Univ.-Prof. Dr. Dirk Pflüger		
9. Dozenten:	Martin Bernreuther Miriam Mehl Dirk Pflüger		
10. Zuordnung zum Curriculum in diesem Studiengang:	B.A. (K) Informatik NF, PO 079-2-2009, 6. Semester → Katalog ISW --> Module im Nebenfach B.A. (K) Informatik NF, PO 079-2-2009, 6. Semester → Katalog ISG --> Module im Nebenfach		
11. Empfohlene Voraussetzungen:	<ul style="list-style-type: none"> • Modul 10190 Mathematik für Informatiker und Softwaretechniker und • Modul 10240 Numerische und Stochastische Grundlagen der Informatik bzw. • Modul 41590 Einführung in die Numerik und Stochastik für Softwaretechniker 		
12. Lernziele:	<ul style="list-style-type: none"> • Fähigkeit, parallele Algorithmen auf unterschiedlichen parallelen Plattformen mit Hilfe geeigneter algorithmischer Modelle zu bewerten. • Kenntnis verschiedener Programmiermodelle für Parallelrechner mit verteiltem und gemeinsamem Speicher. • Fähigkeit, auch fortgeschrittene Implementierungsaufgaben aus dem Bereich des Höchstleistungsrechnens auf Basis ausgewählter Programmiermodelle zu bewältigen. 		
13. Inhalt:	<p>Die Vorlesung beschäftigt sich mit den Grundlagen paralleler Programmierung und paralleler Algorithmen speziell im Hinblick auf die Anwendungsbereiche Wissenschaftliches Rechnen und High Performance Computing. Verwandte Fragestellungen aus dem Bereich der Theorie (parallele Modelle und parallele Komplexität, etc.) sowie aus der Rechnertechnik (parallele Architekturen) werden begleitend diskutiert. Nach einer allgemeinen Einführung (Klassifizierung von Parallelrechnern, Ebenen von Parallelität, Performance und Architekturen, etc.), werden die Grundlagen paralleler Programme eingeführt (Notation/Syntax, Synchronisation und Kommunikation, Design paralleler Programme, etc.). Sowohl die Programmierung auf Systemen mit gemeinsamem Speicher als auch auf Systemen mit verteiltem Speicher werden besprochen. Dabei wird jeweils mindestens ein geeignetes Programmiermodell (z.B. OpenMP, MPI, CUDA) vertieft behandelt. Aus dem Bereich des High Performance Computing werden begleitend klassische Algorithmen und Implementierungstechniken als Beispiele behandelt, z.B. parallele Algorithmen aus der linearen Algebra (Matrixmultiplikation, etc. oder einfache Verfahren zur Lösung partieller Differentialgleichungen). Zusätzlich können Themen wie Lastverteilung und Lastbalancierung (Grundlagen, Algorithmen zur Partitionierung und Lastbalancierung, etc.) vorgestellt werden.</p>		

14. Literatur:	<ul style="list-style-type: none">• T. Rauber, G. Rünger: „Parallele Programmierung , 2. Aufl., Springer 2007, (in English: T. Rauber, G. Rünger: „Parallel Programming: for Multicore and Cluster Systems , Springer 2010).• K.A. Berman, J.L. Paul: Sequential and Parallel Algorithms , PWS Publishing Company, 1997.• B. Chapman, G. Jost, R. van der Pas: Using OpenMP - Portable Shared Memory Parallel Programming , MIT Press, 2008.• W. Gropp, E. Lusk, und R. Thakur: Using MPI-2: Advanced Features of the Message-Passing Interface, das Buch ist auch in deutscher Übersetzung erhältlich.• D. Kirk, W.-M. Hwu Programming Massively Parallel Processors.
15. Lehrveranstaltungen und -formen:	<ul style="list-style-type: none">• 424201 Vorlesung High Performance Computing• 424202 Übung High Performance Computing
16. Abschätzung Arbeitsaufwand:	
17. Prüfungsnummer/n und -name:	42421 High Performance Computing (PL), Schriftlich oder Mündlich, 90 Min., Gewichtung: 1 [42421] High Performance Computing (PL), schriftlich oder mündlich, 90 Min., Gewicht: 1.0
18. Grundlage für ... :	
19. Medienform:	
20. Angeboten von:	Simulation Software Engineering

Modul: 42460 Numerische Simulation

2. Modulkürzel:	051240060	5. Moduldauer:	Einsemestrig
3. Leistungspunkte:	6 LP	6. Turnus:	Wintersemester
4. SWS:	4	7. Sprache:	Deutsch
8. Modulverantwortlicher:	Univ.-Prof. Dr. Dirk Pflüger		
9. Dozenten:	Miriam Mehl Stefan Zimmer Dirk Pflüger		
10. Zuordnung zum Curriculum in diesem Studiengang:	B.A. (K) Informatik NF, PO 079-2-2009, 5. Semester → Katalog ISG --> Module im Nebenfach B.A. (K) Informatik NF, PO 079-2-2009, 5. Semester → Katalog ISW --> Module im Nebenfach		
11. Empfohlene Voraussetzungen:	<ul style="list-style-type: none"> • Modul 10190 Mathematik für Informatiker und Softwaretechniker und • Modul 10240 Numerische und Stochastische Grundlagen der Informatik bzw. • Modul 41590 Einführung in die Numerik und Stochastik für Softwaretechniker • Modul 42410 Grundlagen des wissenschaftlichen Rechnens 		
12. Lernziele:	Fähigkeit zur Implementierung numerischer Methoden und Entwicklung und Umsetzung geeigneter Datenstrukturen.		
13. Inhalt:	Strukturmechanik, Strömungsmechanik, Finite Elemente, Finite Differenzen sowie praktische Aspekte der effizienten und parallelen Umsetzung auf Rechnern.		
14. Literatur:	<ul style="list-style-type: none"> • Griebel, Dornseifer, Neunhoeffler: Numerical simulation in fluid dynamics : a practical introduction, SIAM, 1998 / Numerische Simulation in der Strömungsmechanik, Vieweg 1995 • Griebel, Knappek, Zumbusch, Caglar: Numerische Simulation in der Moleküldynamik : Numerik, Algorithmen, Parallelisierung, Anwendungen, Springer 2004 • Braess: Finite Elemente : Theorie, schnelle Löser und Anwendungen in der Elastizitätstheorie, Springer, 2007 		
15. Lehrveranstaltungen und -formen:	<ul style="list-style-type: none"> • 424601 Vorlesung Numerische Simulation • 424602 Übung Numerische Simulation 		
16. Abschätzung Arbeitsaufwand:			
17. Prüfungsnummer/n und -name:	42461 Numerische Simulation (LBP), Schriftlich oder Mündlich, 90 Min., Gewichtung: 1		
18. Grundlage für ... :			
19. Medienform:			
20. Angeboten von:	Simulation Software Engineering		

Modul: 42480 Ausgewählte Kapitel des Wissenschaftlichen Rechnens

2. Modulkürzel:	051240030	5. Moduldauer:	Einsemestrig
3. Leistungspunkte:	6 LP	6. Turnus:	Wintersemester
4. SWS:	4	7. Sprache:	Deutsch
8. Modulverantwortlicher:	Univ.-Prof. Dr. Dirk Pflüger		
9. Dozenten:	Miriam Mehl Dirk Pflüger Stefan Zimmer		
10. Zuordnung zum Curriculum in diesem Studiengang:	B.A. (K) Informatik NF, PO 079-2-2009, 6. Semester → Katalog ISG --> Module im Nebenfach B.A. (K) Informatik NF, PO 079-2-2009, 6. Semester → Katalog ISW --> Module im Nebenfach		
11. Empfohlene Voraussetzungen:	<ul style="list-style-type: none"> • Modul 10190 Mathematik für Informatiker und Softwaretechniker und • Modul 10240 Numerische und Stochastische Grundlagen der Informatik bzw. • Modul 41590 Einführung in die Numerik und Stochastik für Softwaretechniker • Modul 42410 Grundlagen des wissenschaftlichen Rechnens 		
12. Lernziele:	Die Teilnehmer kennen ausgewählte aktuelle Forschungsthemen des wissenschaftlichen Rechnens und können mit der zugehörigen Primärliteratur arbeiten.		
13. Inhalt:	Aktuelle weiterführende Forschungsthemen des wissenschaftlichen Rechnens, wie z.B. adaptive Finite Elemente, hierarchische Basen und dünne Gitter, robuste Multilevellöser, Wavelets und schnelle Wavelettransformation, p-Version oder Spektralverfahren.		
14. Literatur:	Primärliteratur zu den behandelten Themen: <ul style="list-style-type: none"> • Bungartz/Griebel: Sparse Grids, Acta Numerica, Volume 13, p. 147-269. • Quarteroni/Valli: Numerical approximation of partial differential equations. • Quarteroni: Numerical models for differential problems. 		
15. Lehrveranstaltungen und -formen:	<ul style="list-style-type: none"> • 424801 Vorlesung Ausgewählte Kapitel des Wissenschaftlichen Rechnens • 424802 Übung Ausgewählte Kapitel des Wissenschaftlichen Rechnens 		
16. Abschätzung Arbeitsaufwand:			
17. Prüfungsnummer/n und -name:	42481 Ausgewählte Kapitel des Wissenschaftlichen Rechnens (PL), Schriftlich oder Mündlich, 90 Min., Gewichtung: 1 [42481] Ausgewählte Kapitel des Wissenschaftlichen Rechnens (PL), schriftlich oder mündlich, 90 Min., Gewicht: 1.0		
18. Grundlage für ... :			
19. Medienform:			
20. Angeboten von:	Simulation Software Engineering		

Modul: 71740 System and Web Security

2. Modulkürzel:	052900002	5. Moduldauer:	Einsemestrig
3. Leistungspunkte:	6 LP	6. Turnus:	Sommersemester
4. SWS:	4	7. Sprache:	Englisch
8. Modulverantwortlicher:	Univ.-Prof. Dr. rer. nat. Ralf Küsters		
9. Dozenten:	Ralf Küsters		
10. Zuordnung zum Curriculum in diesem Studiengang:	B.A. (K) Informatik NF, PO 079-2-2009, → Katalog ISG --> Module im Nebenfach B.A. (K) Informatik NF, PO 079-2-2009, → Katalog ISW --> Module im Nebenfach		
11. Empfohlene Voraussetzungen:	Solide Kenntnisse in mindestens einer Programmiersprache.		
12. Lernziele:	<ul style="list-style-type: none"> • Students are sensitized for common security vulnerabilities and attack vectors in computer systems and the web, • Students are familiar with concrete attacks on computer systems and the web, and understand the underlying principles, • Students are familiar with common defense mechanisms. 		
13. Inhalt:	<p>IT-systems are constantly under attack, by various kinds of attackers with diverse interests: criminal organizations with monetary interests, intelligence agencies, industrial espionage by states and companies.</p> <p>The course covers the most common attack vectors on computer systems, including mobile devices, and the web, including, for example, stack and heap overflows, format string vulnerabilities, integer overflows, return-oriented-programming, Cross-Site-Scripting (CSS/XSS), SQL Injections, and Cross-Site-Request-Forgery (XSRF), etc.</p> <p>The course also discusses common defense mechanisms, including, for example, access control mechanisms, address space layout randomization (ASLR), static code analysis, security monitoring, input/output sanitization, prepared statements, etc.</p>		
14. Literatur:	Will be announced in class		
15. Lehrveranstaltungen und -formen:	<ul style="list-style-type: none"> • 717401 Vorlesung System and Web Security • 717402 Übung System and Web Security 		
16. Abschätzung Arbeitsaufwand:	Vorlesung und Übung System- und Websicherheit		
17. Prüfungsnummer/n und -name:	<ul style="list-style-type: none"> • 71741 System and Web Security (PL), Schriftlich, Gewichtung: 1 • V Vorleistung (USL-V), Unbenotete Studienleistung als Vorleistung (USL-V); ausreichende Punktzahl in den Übungen Prüfungsleistung (PL): Klausur (90 Minuten) zur Vorlesung und Übung System- und Websicherheit 		
18. Grundlage für ... :			
19. Medienform:	Projektor, Tafel		
20. Angeboten von:	Informationssicherheit		

Modul: 71760 Security and Privacy

2. Modulkürzel:	052900004	5. Moduldauer:	Einsemestrig
3. Leistungspunkte:	6 LP	6. Turnus:	Sommersemester
4. SWS:	4	7. Sprache:	Englisch
8. Modulverantwortlicher:	Univ.-Prof. Dr. rer. nat. Ralf Küsters		
9. Dozenten:	Ralf Küsters		
10. Zuordnung zum Curriculum in diesem Studiengang:	B.A. (K) Informatik NF, PO 079-2-2009, → Katalog ISG --> Module im Nebenfach B.A. (K) Informatik NF, PO 079-2-2009, → Katalog ISW --> Module im Nebenfach		
11. Empfohlene Voraussetzungen:	Kenntnisse aus den Vorlesungen <i>Grundlagen der Informationssicherheit</i> (Bachelor) sowie <i>Introduction to Modern Cryptography</i> (Master) sind vorteilhaft, werden allerdings nicht zwingend vorausgesetzt. Die Veranstaltung verlangt solide Kenntnisse in den Grundlagen der Informatik und der Mathematik wie sie in den ersten vier Semestern eines Bachelorstudiengangs in Informatik (oder Mathematik) vermittelt werden.		
12. Lernziele:	Students will acquire an in-depth understanding of central topics in information security and privacy.		
13. Inhalt:	This course covers some of the most important, typically advanced topics in information security and privacy. The selection of topics can vary from term to term, depending on the development of the field and the focus of the information security group. Possible topics include: <ul style="list-style-type: none"> • Zero-Knowledge Protocols: a fundamental concept in many advanced secure and privacy preserving systems • Verification of cryptographic protocols: What does it mean for protocols, such as TLS, to be secure? How can we prove security? Can we prove security using automated tools? • Blockchains, Smart Contracts, and applications, such as cryptocurrencies, e.g., Bitcoin and Ethereum. • Secure Multi-Party Computation: how can multiple parties compute a common function without revealing their input? E.g., how can two millionaires figure out who earns more without revealing their income to each other? • Differential Privacy and Privacy-Preserving Data Mining: how to make use of information in (statistical) databases without revealing information about individuals? • E-Voting: Can we have a system where voters can make sure that their votes were actually counted even when the voting servers are completely malicious? • Web-based security protocols, such as web-based single-sign on protocols • Advanced attacks and defenses in as well as models of web security 		
14. Literatur:	Will be announced in class.		
15. Lehrveranstaltungen und -formen:	<ul style="list-style-type: none"> • 717601 Vorlesung Security and Privacy • 717602 Übung Security and Privacy 		

16. Abschätzung Arbeitsaufwand:	Vorlesung und Übung zu Security and Privacy
17. Prüfungsnummer/n und -name:	<ul style="list-style-type: none">• 71761 Security and Privacy (PL), Schriftlich oder Mündlich, Gewichtung: 1• V Vorleistung (USL-V), Unbenotete Studienleistung als Vorleistung (USL-V); ausreichende Punktzahl in den Übungen Prüfungsleistung (PL): Klausur (90 Minuten) oder mündliche Prüfung (30 Minuten) zur Vorlesung und Übung Security and Privacy
18. Grundlage für ... :	
19. Medienform:	Projektor, Tafel
20. Angeboten von:	Informationssicherheit

Modul: 72240 Model-Driven Software Development

2. Modulkürzel:	51520002	5. Moduldauer:	Einsemestrig
3. Leistungspunkte:	6 LP	6. Turnus:	Sommersemester
4. SWS:	4	7. Sprache:	Deutsch/Englisch
8. Modulverantwortlicher:	Univ.-Prof. Dr.-Ing. Steffen Becker		
9. Dozenten:	Steffen Becker		
10. Zuordnung zum Curriculum in diesem Studiengang:	B.A. (K) Informatik NF, PO 079-2-2009, → Katalog ISW --> Module im Nebenfach		
11. Empfohlene Voraussetzungen:	<ul style="list-style-type: none"> • Einführung in die Softwaretechnik • SE für St • PSE 		
12. Lernziele:	Grundlagen der modellgetriebenen Softwareentwicklung kennen und anwenden können, insbesondere Metamodelle und Transformationen erstellen zu können.		
13. Inhalt:	<p>Die Vorlesung gibt eine Einführung in Model-Driven Software Development und bettet sie ein in Softwaremodellierung und -entwicklung. Der Schwerpunkt liegt auf der OMG Sicht von modellgetriebener Softwareentwicklung. Dies beinhaltet OMG Standards wie MDA, QVT oder MOF. Nichtsdestotrotz führt die Vorlesung auch in die zu Grunde liegenden Konzepte dieser Standards ein und zeigt Querbezüge zu anderen Gebieten der Softwareentwicklung auf. Insbesondere werden die folgenden Fragen behandelt:</p> <ul style="list-style-type: none"> • Welche Techniken machen MDSD aus? • Wie kann man aus existierender Software Plattformen extrahieren? • Wie wird mittels MOF metamodelliert? • Wie werden Modelle transformiert? <p>Zu letzterem gibt die Vorlesung einen intensiven Einblick in Modell-zu-Modell und Modell-zu-Text Transformationsansätzen und -sprachen.</p>		
14. Literatur:	Model-Driven Software Development, T. Stahl und M. Völter		
15. Lehrveranstaltungen und -formen:	<ul style="list-style-type: none"> • 722401 Vorlesung Model-Driven Software Development • 722402 Übung Model-Driven Software Development 		
16. Abschätzung Arbeitsaufwand:	Vorlesung und praktische Übungen		
17. Prüfungsnummer/n und -name:	72241 Model-Driven Software Development (PL), Schriftlich oder Mündlich, 90 Min., Gewichtung: 1 Exam; duration: 90 min written exam or 30 min oral exam		
18. Grundlage für ... :	Quantitative Analyse von Software Designs (former SZS)		
19. Medienform:	Folien, Übungsblätter, Beispiele, Videoaufzeichnung		
20. Angeboten von:	Zuverlässige Software-Systeme		

Modul: 78640 Grundlagen der Informationssicherheit

2. Modulkürzel:	052900001	5. Moduldauer:	Einsemestrig
3. Leistungspunkte:	6 LP	6. Turnus:	Wintersemester
4. SWS:	4	7. Sprache:	Deutsch
8. Modulverantwortlicher:	Univ.-Prof. Dr. rer. nat. Ralf Küsters		
9. Dozenten:	Ralf Küsters		
10. Zuordnung zum Curriculum in diesem Studiengang:	B.A. (K) Informatik NF, PO 079-2-2009, → Katalog ISW --> Module im Nebenfach B.A. (K) Informatik NF, PO 079-2-2009, → Katalog ISG --> Module im Nebenfach		
11. Empfohlene Voraussetzungen:	Empfohlen werden Kenntnisse in den Grundlagen der Informatik und Mathematik wie sie in den ersten beiden Semestern eines Bachelorstudiengangs Informatik/Mathematik vermittelt werden.		
12. Lernziele:	Die Veranstaltung soll Studierende einerseits einen Überblick über die Informationssicherheit vermitteln und sie für dieses Thema sensibilisieren. Zum anderen lernen Studierende grundlegende Konzepte der Informationssicherheit kennen.		
13. Inhalt:	<p>Die moderne digitale Gesellschaft ist ohne Informationssicherheit nicht denkbar. Daten und sogar Geld sind digital, Kommunikation ist digital, kritische Infrastrukturen (Banken, Industrieanlagen, Verkehrsmittel, etc.) hängen stark von IT-Systemen ab. Es gibt kaum Lebensbereiche, die nicht von der Digitalisierung durchdrungen sind. Die digitale Welt ist deshalb ein attraktives Ziel für Angreifer aller Art (Kriminelle, Geheimdienste, Industriespione, Staaten, etc.) und mittlerweile ständigen Angriffen ausgesetzt. Diese Veranstaltung bietet eine erste Einführung in die Informationssicherheit. Unter anderem werden folgende Themen behandelt, wobei jeweils in der Praxis eingesetzte Verfahren betrachtet werden, deren Sicherheit untersucht wird und bekannte Angriffe vorgestellt werden.</p> <ul style="list-style-type: none"> • Grundlagen der Kryptographie • (Un-)Sicherheit von Netzwerkprotokollen, wie TCP, DNS, BGP, einschließlich <ul style="list-style-type: none"> • Denial-of-Service-Angriffe • Firewalls • Kryptographische Protokolle (TLS, SSH, WPA2, etc.) <ul style="list-style-type: none"> • Zertifikate und Public-Key-Infrastrukturen • Authentifizierung und Schlüsselaustausch • Zugriffskontrolle, z.B. in Linux, SELinux und Android • Grundlagen der Websicherheit • Ausblick Systemsicherheit 		
14. Literatur:	Wird in der Veranstaltung bekanntgegeben.		
15. Lehrveranstaltungen und -formen:	• 786401 Vorlesung/Übung zu Grundlagen der Informationssicherheit		
16. Abschätzung Arbeitsaufwand:			
17. Prüfungsnummer/n und -name:	<ul style="list-style-type: none"> • V Vorleistung (USL-V), • 78641 Grundlagen der Informationssicherheit (PL), Schriftlich oder Mündlich, Gewichtung: 1 		

Unbenotete Studienleistung als Vorleistung (USL-V); ausreichende Punktzahl in den Übungen sowie ggf. in einer Zwischenklausur;
Prüfungsleistung (PL): Klausur (90 Minuten) oder mündliche Prüfung (30 Minuten) zur Vorlesung und Übung Grundlagen der Informationssicherheit

18. Grundlage für ... :

19. Medienform: Projector, blackboard

20. Angeboten von: Informationssicherheit

Modul: 78900 Introduction to Modern Cryptography

2. Modulkürzel:	052900003	5. Moduldauer:	Einsemestrig
3. Leistungspunkte:	6 LP	6. Turnus:	Wintersemester
4. SWS:	4	7. Sprache:	Englisch
8. Modulverantwortlicher:	Univ.-Prof. Dr. rer. nat. Ralf Küsters		
9. Dozenten:	Ralf Küsters		
10. Zuordnung zum Curriculum in diesem Studiengang:	B.A. (K) Informatik NF, PO 079-2-2009, → Katalog ISG --> Module im Nebenfach B.A. (K) Informatik NF, PO 079-2-2009, → Katalog ISW --> Module im Nebenfach		
11. Empfohlene Voraussetzungen:	Die Veranstaltung verlangt solide Kenntnisse in den Grundlagen der Mathematik wie sie in den ersten drei oder vier Semestern eines Bachelorstudiengangs in Informatik/Mathematik vermittelt werden. Kenntnisse der Inhalte der Vorlesung <i>Grundlagen der Informationssicherheit</i> sind nützlich, aber keine zwingende Voraussetzung.		
12. Lernziele:	Students will acquire an in-depth understanding of cryptography. They will be able to judge and assess the security of cryptographic constructions used in practice (encryption schemes, digital signatures, messages authentication codes, etc.) and will be able to read scientific papers on cryptography.		
13. Inhalt:	<p>p { margin-bottom: 0.1in; direction: ltr; color: rgb(0, 0, 10); line-height: 120%; text-align: left; }p.western { font-family: "Calibri", serif; font-size: 11pt; }p.cjk { font-family: "Times New Roman"; font-size: 11pt; }p.cjl { font-family: "Times New Roman"; font-size: 11pt; }p.cjl { font-family: "Times New Roman"; font-size: 11pt; }a:link { color: rgb(0, 0, 255); }a.cjl:link { font-family: "Times New Roman"; }</p> <p>Cryptography is everywhere! We heavily rely on cryptography in our everyday life when we do, for example, online shopping and online banking, pay with credit or debit card, open doors with electronic keys, or when we use social networks, instant messengers, online games, WiFi, mobile networks, or electronic currencies. Here, cryptography is essential in order to guarantee various central security properties such as secrecy and integrity of messages as well as authenticity of the communication partners. This course provides an introduction to modern cryptography. In the traditional approach to cryptography, cryptographers proposed, for example, encryption algorithms, and then others, cryptanalysts, tried to break them. In modern cryptography, cryptographers try to prove that their cryptographic constructions are secure under certain assumptions, even when attacked by powerful adversaries. Hence, cryptography turned from pure art to science.</p> <p>The course covers several fundamental cryptographic primitives, including (symmetric and asymmetric) encryption, hash functions, digital signatures, and message authentication codes. These primitives are important building blocks for other cryptographic constructions and for cryptographic protocols (TLS, SSH, WPA2, etc.), used by billions of people every day. The course presents common cryptographic constructions as used in practice, such</p>		

as AES with various encryption modes (e.g., CBC, CTR), RSA, ElGamal, HMAC, PKCS#1, DSA. It also discusses public-key infrastructures and cryptographic protocols.

In the spirit of modern cryptography, we ask the following questions: What does it mean for an encryption algorithm, digital signature, etc. to be secure? Under which assumptions can we prove security? For several cryptographic constructions used in practice, including those mentioned above, we prove security or present attacks. This provides a deep understanding of the security/insecurity of the cryptography that surrounds us.

14. Literatur:	<ul style="list-style-type: none"> • Ralf Küsters and Thomas Wilke. Moderne Kryptographie - Eine Einführung. Vieweg + Teubner, 2011. • Jonathan Katz and Yehuda Lindell. Introduction to Modern Cryptography - Second Edition. CRC Press 2015.
15. Lehrveranstaltungen und -formen:	<ul style="list-style-type: none"> • 789001 Vorlesung und Übung zu Introduction to Modern Cryptography
16. Abschätzung Arbeitsaufwand:	Vorlesung und Übung zu Introduction to Modern Cryptography
17. Prüfungsnummer/n und -name:	<ul style="list-style-type: none"> • V Vorleistung (USL-V), • 78901 Introduction to Modern Cryptography (PL), Schriftlich oder Mündlich, Gewichtung: 1 <p>Unbenotete Studienleistung als Vorleistung (USL-V); ausreichende Punktzahl in den Übungen Prüfungsleistung (PL): Klausur (90 Minuten) oder mündliche Prüfung (30 Minuten) zur Vorlesung und Übung Introduction to Modern Cryptography</p>
18. Grundlage für ... :	
19. Medienform:	Projector, blackboard
20. Angeboten von:	Informationssicherheit
