RUHR-UNIVERSITÄT BOCHUM

RUB

Hauptstudium Studiengang Sicherheit in der Informationstechnik

PO 04

Modulhandbuch

Fakultät für Elektrotechnik und Informationstechnik

Inhaltsverzeichnis

Kapitel 1

Module

1.1 Automatisierungstechnik

Nummer: 149000
Kürzel: Auto
Verantwortlicher: Prof. Dr.-Ing. Jan Lunze
Arbeitsaufwand: 0 Stunden (entsprechend der Lehrveranstaltungen)
Leistungspunkte: 4

Ziele: Es werden die fachspezifischen Grundlagen der Automatisierungstechnik vermittelt. Die Übungen tragen dazu bei, erste Erfahrungen im Umgang und der Anwendung der systemtheoretisch begründeten Methoden auf unterschiedliche Anwendungsbeispiele zu sammeln. Dabei werden die Methoden zur Beschreibung und Analyse dynamischer Systeme und zum Steuerungsentwurf erlernt, wobei sowohl wertkontinuierliche als auch ereignisdiskrete Systeme behandelt werden.

Inhalt: Das Modul besteht aus einer Lehrveranstaltung, die die grundlegenden automatisierungstechnischen Aufgaben und Methoden in drei Teilen behandelt:

1. Einführung (Ziele und Aufgaben der Automatisierungstechnik, grundlegende Eigenschaften dynamischer Systeme)
2. Automatisierung kontinuierlicher Systeme (Beschreibung und Verhalten kontinuierlicher Systeme, Steuerbarkeit und Beobachtbarkeit, Stabilität, Einstellregeln für PID-Regler, Zustandsbeobachtung und Diagnose kontinuierlicher Systeme)
3. Automatisierung und Verhalten diskreter Systeme (Beschreibung diskreter Systeme, Entwurf diskreter Steuerungen, Zustandsbeobachtung und Diagnose diskreter Systeme)

Prüfungsform: siehe Lehrveranstaltungen

Veranstaltungen:

148191: Automatisierungstechnik 4 SWS (S.37)

1.2 Computerarchitektur und Betriebssysteme

Nummer: 149141
Kürzel: CompArch
Verantwortlicher: Prof. Dr.-Ing. Michael Hübner
Arbeitsaufwand: 0 Stunden (entsprechend der Lehrveranstaltungen)
Leistungspunkte: 4

Ziele: Ziel dieser Lehrveranstaltung ist es, Zusammenhänge und Detailkenntnisse zum Aufbau, zu Komponenten und zur Funktionsweise moderner Computersysteme in Hard- und Software zu vermitteln. Damit soll für die Studierenden die Basis geschaffen werden, sowohl in der Computertechnik selbst, als auch in deren Anwendungsbereichen wie z.B. der Automatisierungstechnik Computerkomponenten und -systeme auslegen und entwickeln zu können.

Inhalt:
Ausgehend von grundlegenden Computerstrukturen (Von-Neumann-Architektur, SISD, SIMD, MIMD) werden grundlegende Fähigkeiten zum anforderungsgerechten Entwurf und zur anwendungsbezogenen Realisierung von Computersystemen vermittelt. Konkrete Beispiele heutiger Computer für unterschiedliche Anwendungsfelder (8051, Pentium 4, Ultra Sparc III) runden die generellen Wissensinhalte ab. Einen besonderen inhaltlichen Schwerpunkt bildet die Programmierung der Mikroarchitekturebene als Ergänzung zu anderen Lehrveranstaltungen im Bereich der Informatik / Computertechnik (Programmiersprachen, Eingebettete Prozessoren). Ein abschließendes Kapitel beinhaltet wesentliche Betriebssystemfunktionen.

Prüfungsform: siehe Lehrveranstaltungen

Veranstaltungen:

148194: Computerarchitektur und Betriebssysteme 4 SWS (S.45)

1.3 Computernetze II

Nummer: 149144
Kürzel: CN2
Verantwortlicher: Prof. Dr.-Ing. York Tüchelmann
Arbeitsaufwand: 0 Stunden (entsprechend der Lehrveranstaltungen)
Leistungspunkte: 3

Ziele: Die Lehrveranstaltung vermittelt detaillierte Kenntnisse hinsichtlich Planung, Design und Auslegung von Computernetzen. Behandelt werden dabei sowohl Lokale Netze (Local Area Networks) als auch Weitverkehrsnetze (Wide Area Networks). Die Studierenden sollen so in die Lage versetzt werden, aufgrund von Nutzeranforderungen Entwurfsziele zu formulieren, Konzepte zu erarbeiten, technische Anforderungen und Parameter bezüglich Verkehrslasten, Applikationen und Protokollen zu spezifizieren, um auf dieser Basis ein Computernetz planen und auslegen zu können.

Inhalt: Planung und Auslegung von Computernetzen * Einführung

- **Planung von IT-Netzen – Einflussgrößen, Planungs- und Auslegungsparameter**
  - Information, IT-Netze und Unternehmenserfolg
  - Unternehmensweite informationslogistische Einflussparameter
  - Nicht-technische und technische Auslegungsparameter
  - Quantifizierung von Systemeigenschaften
  - Dokumentation der Planung
  - Systemansatz und Vorgehensweise
- **Netzwerkanalyse**
  - Anforderungsanalyse
  - Informationsflussanalyse
- **Netzwerkarchitektur**
  - Netzwerkarchitekturmodelle und Netzwerkarchitekturen
  - Routing – Architektur
  - Netzwerkmanagement – Architektur
  - Performance – Architektur
- Technologie- und Komponentenauswahl

Ergänzend zu Vorlesung und Übung wird ein veranstaltungsbegleitendes Projekt angeboten.

Prüfungsform: siehe Lehrveranstaltungen

Veranstaltungen:

148070: Computernetze II 3 SWS (S.47)

1.4 Datenstrukturen

Nummer: 149614
Kürzel: DaStr
Verantwortlicher: Prof. Dr. Eberhard Bertsch
Arbeitsaufwand: 0 Stunden (entsprechend der Lehrveranstaltungen)
Leistungspunkte: 6

Ziele: Es geht sowohl um Ideen zur Entwicklung "schneller" Software, als auch um eine weiterführende Diskussion der prinzipiellen Effizienz in Begriffen von Platz und Zeit. Die Studierenden sollen nach Absolvierung des Moduls in der Lage sein, verschiedene Implementierungen einfacher Programmieraufgaben mit umfangreichen Datenmengen zu vergleichen und deren Vor- und Nachteile hinsichtlich Platz- und Zeit-Bedarf abzuwägen.

Inhalt: Die Bedeutung des Stoffes besteht darin, dass angehende Informatiker erst durch vergleichende Betrachtung verschiedener Möglichkeiten zur Darstellung von Daten in die Lage versetzt werden, statt irgendeiner beliebigen Programmiertechnik, die für ein gegebenes Problem jeweils optimal geeignete auszuwählen. Die durchweg maßgeblichen Merkmale bei der Erörterung solcher Techniken sind Übersichtlichkeit und Sparsamkeit bezüglich Speicherplatz und Rechenzeit.

Prüfungsform: siehe Lehrveranstaltungen

Veranstaltungen:

150322: Datenstrukturen 6 SWS (S.52)

1.5 Diplomarbeit

Nummer: 149886
Kürzel: DA-ITS
Verantwortlicher: Studiendekan ITS
Arbeitsaufwand: 900 Stunden (entsprechend der Lehrveranstaltungen)
Leistungspunkte: 25

Ziele: Die Diplomprüfung bildet den berufsqualifizierenden Abschluss des Studiums im Diplomstudiengang Sicherheit in der Informationstechnik an der Ruhr-Universität Bochum. Durch die Diplomprüfung soll festgestellt werden, ob die Kandidatin bzw. der Kandidat die für den Übergang in die Berufspraxis notwendigen gründlichen Fachkenntnisse erworben hat, die fachlichen Zusammenhänge überblickt und die Fähigkeit besitzt, wissenschaftliche Methoden und Erkenntnisse anzuwenden.

Die Diplomprüfung führt zum wissenschaftlich berufsqualifizierenden Abschluss des Studiums. Durch die Diplomprüfung soll festgestellt werden, ob der Kandidat bzw. die Kandidatin fundierte Kenntnisse und die Fähigkeit zur selbstständigen Anwendung anspruchsvoller wissenschaftlicher Methoden erlernt hat. Die Studierenden sollen zur kritischen Einordnung der wissenschaftlichen Erkenntnisse sowie zu verantwortlichem, interdisziplinärem Denken und Handeln befähigt werden und sollen komplexe Probleme der Sicherheit in der Informationstechnik analysieren und Lösungen erarbeiten können. Die Diplomprüfung setzt sich aus der kumulativen Bewertung aller im Hauptstudium absolvierten Prüfungen in den zugeordneten Lehrveranstaltungen und der Diplomarbeit zusammen.

Inhalt: Die Diplomarbeit ist eine schriftliche Prüfungsarbeit und schließt das Studium ab. Sie soll zeigen, dass der Kandidat bzw. die Kandidatin in der Lage ist, innerhalb einer vorgegebenen Frist ein anspruchsvolles Problem der Sicherheit in der Informationstechnik selbstständig mit wissenschaftlichen Methoden zu bearbeiten.

Prüfungsform: siehe Lehrveranstaltungen

Veranstaltungen:

148181: Diplomarbeit ITS 25 SWS (S.55)

1.6 Industriepraktikum

Nummer: 149888
Kürzel: IndPrak-ITS
Verantwortlicher: Studiendekan ITS
Arbeitsaufwand: 0 Stunden (entsprechend der Lehrveranstaltungen)
Leistungspunkte:

Ziele: Nach der Praktikantentätigkeit haben die Studierenden u.a. Einblicke in die betrieblichen Arbeitsweisen und Sozialstrukturen gewonnen. Sie haben Konstruktions-, Entwurfs- und Entwicklungsmethoden, mit Verfahrens- und Betriebsaufgaben, sowie mit industriellen Produktionseinrichtungen kennengelernt. Kommunikative und soziale Schlüsselqualifikationen sind aus dem Umgang mit Vorgesetzten und Teammitgliedern bekannt.

Inhalt: Die berufsbezogene Tätigkeit in einem Industrieunternehmen, wobei unter Anleitung fachbezogene Probleme gehört werden, soll frühzeitig auf die Berufstätigkeit vorbereiten.

Prüfungsform: siehe Lehrveranstaltungen

Veranstaltungen:

144011: Industriepraktikum ITS (S.65)

1.7 Kommunikationstechnik

Nummer: 149042
Kürzel: KomTe
Verantwortlicher: Prof. Dr.-Ing. Heinz Göckler
Arbeitsaufwand: 150 Stunden (entsprechend der Lehrveranstaltungen)
Leistungspunkte: 6

Ziele: Die Teilnehmer gewinnen vertiefte fachspezifische Grundkenntnisse der digitalen Signalverarbeitung und dem Anwendungsschwerpunkt der Übertragung digitaler Signale.

Die Studierenden kennen die grundlegenden Methoden zur Beschreibung und Analyse von digitalen Systemen, sowie den Aufbau von realisierenden Strukturen und Algorithmen, die grundlegenden Methoden und Verfahren zur Übertragung digitaler Datensignale über frequenzbandbegrenzte Kanäle, und die Konzepte zur Behandlung kommunikationstechnischer Aufgabenstellungen.

Inhalt: Das Modul umfasst die folgenden zwei Lehrveranstaltungen, deren detaillierter Inhalt der jeweiligen Einzelbeschreibung zu entnehmen ist:

1. Digitale Signalverarbeitung: Systemtheorie digitaler Systeme mit den Schwerpunkten Grundlagen, Beschreibungsmethoden, Strukturen, Anwendungen.

2. Übertragung digitaler Signale: Lineare und nichtlineare Modulation, Struktur von Modulatoren. Nyquist-Bedingungen, Augendiagramme, signalangepasstes Filter, Korrelationsempfang. Kohärente und inkohärente Demodulation, Nachrichtendetektion. Kanal mit additivem weißen Gauß'schen Rauschen, Entscheidungsregeln, Maximum-A-Posteriori- und Maximum-Likelihood-Verfahren, Symbolfehler- und Bitfehler-Wahrscheinlichkeit, Kanalkapazität, Shannon-Grenze, Leistungs-Band- breite-Diagramm.

Prüfungsform: siehe Lehrveranstaltungen

Veranstaltungen:

148020: Digitale Signalverarbeitung 4 SWS (S.53)
148186: Übertragung digitaler Signale 3 SWS (S.152)

1.8 Kryptographie

Nummer: 149889
Kürzel: Krypto
Verantwortlicher: Studiendekan ITS
Arbeitsaufwand: 0 Stunden (entsprechend der Lehrveranstaltungen)
Leistungspunkte: 8

Ziele: Lernziel dieser Veranstaltung ist ein Verständnis der wesentlichen mathematischen Methoden und Verfahren, auf denen moderne kryptographische Verfahren beruhen. Die Tiefe der Behandlung der Verfahren geht deutlich über das in den vorhergehenden Veranstaltungen vermittelte Maß hinaus. Als Ziel sollen die Teilnehmer die Fähigkeit zur Analyse und dem Design aktueller, und zukünftiger kryptographischer Methoden erhalten. Zudem wird ein Bewusstsein für Methodik und Mächtigkeit verschiedenster Angriffsszenarien vermittelt.

Inhalt: Die Veranstaltung 'Kryptographie' behandelt die grundlegenden mathematischen Prinzipien moderner kryptographischer Verfahren. Die notwendigen mathematischen Grundkenntnisse der Algebra, Zahlentheorie, Komplexitätstheorie, Kombinatorik und Wahrscheinlichkeitsrechnung werden im Laufe der Vorlesung vertieft und ergänzt. In Abschnitt 1 der Veranstaltung werden wesentliche Bereiche der symmetrischen Kryptographie behandelt. Dieser Abschnitt beinhaltet insbesondere Block- und Strom- Algorithmen, sowie Hashfunktionen. Bei der Darstellung wird stets auf den mathematischen Hintergrund bzw. die präzise mathematische Formulierung eingegangen.

Der Abschnitt 2 des Moduls befasst sich mit den wichtigsten asymmetrischen Verfahren. Ein wesentlicher Abschnitt befasst sich mit dem RSA Algorithmus, und den sich anschließenden mathematischen Fragestellungen wie Primzahltests und Faktorisierung großer Zahlen. Weitere Gebiete sind Verfahren, die auf diskreten Logarithmen basisieren, sowie die Analyse gängiger Algorithmen für die digitale Signatur. Im abschließenden Abschnitt 3 werden verschiedene, auf den bisherigen Verfahren basierende kryptographische Protokolle (DH-Schlüsselaustausch, Zero Knowledge, Commitment Schemata) erörtert.

Prüfungsform: siehe Lehrveranstaltungen

Veranstaltungen:

148155: Kryptographie I 4 SWS (S.75)
148156: Kryptographie II 4 SWS (S.76)

1.9 Mikroelektronik

Nummer: 149180
Kürzel: MikElek
Verantwortlicher: Prof. Dr.-Ing. Nils Pohl
Arbeitsaufwand: 0 Stunden (entsprechend der Lehrveranstaltungen)
Leistungspunkte: 4

Ziele: Das Ziel dieser Vorlesung besteht darin, dem Hörer den aktuellen Stand der Technik in CMOS-Digitalschaltungen zu vermitteln, welches Konzept- und Systemingenieure, sowie VLSI-Designer brauchen, um erfolgreich zu arbeiten. Dabei werden sowohl die theoretischen Grundlagen der Bauelemente, als auch der Schritt vom Bauelement über die Schaltung zum System gelehrt.

Inhalt: Diese Vorlesung führt ein in die wesentlichen Grundlagen für die Materie der integrierten Schaltungen und Systeme. Nach einer einführenden Behandlung der Grundlagen und Anwendungen der Mikroelektronik schreitet die Vorlesung über die Behandlung einer Reihe von Einzelheiten integrierter Halbleiterbauelemente zu den integrierten digitalen CMOS-Grundschaltungen, voran. Zuletzt wendet sich die Vorlesung komplexeren Aufgabenstellungen beim Entwurf von integrierten Systemkomponenten und Systemen zu.

Prüfungsform: siehe Lehrveranstaltungen

Veranstaltungen:

148025: Integrierte Digitalschaltungen 4 SWS (S.68)

1.10 Projektarbeit

Nummer: 149881
Kürzel: PrakFach-DiplITS
Verantwortlicher: Studiendekan ITS
Arbeitsaufwand: 180 Stunden (entsprechend der Lehrveranstaltungen)
Leistungspunkte: 6

Ziele: folgt

Inhalt: folgt

Prüfungsform: siehe Lehrveranstaltungen

Veranstaltungen:

142020: Master-Praktikum Embedded Smartcard Microcontrollers	3 SWS	(S.80)
142181: Master-Praktikum Entwurf integrierter Digitalschaltungen mit VHDL	3 SWS	(S.82)
148151: Master-Praktikum FPGA	3 SWS	(S.84)
148067: Master-Praktikum Integrierte Informationssysteme	3 SWS	(S.86)
142246: Master-Praktikum Programmanalyse	3 SWS	(S.87)
142023: Master-Praktikum Seitenkanalangriffe	3 SWS	(S.89)
142243: Master-Praktikum zur Hackertechnik	3 SWS	(S.90)
148174: Master-Praktikum zur Programmierung sicherer Webservices	3 SWS	(S.92)
142241: Master-Projekt Netz- und Datensicherheit	3 SWS	(S.94)
142184: Master-Projekt Virtual Prototyping von Embedded Systems	3 SWS	(S.96)

1.11 Signale und Systeme

Nummer: 149046
Kürzel: SiSy
Verantwortlicher: Prof. Dr.-Ing. Heinz Göckler
Arbeitsaufwand: 0 Stunden (entsprechend der Lehrveranstaltungen)
Leistungspunkte: 4

Ziele: Das Lernziel der Vorlesung bzw. des Moduls Signale und Systeme besteht darin, die Grundlagen der Systemtheorie, eine weitgehend allgemeine mathematische Methode zur Beschreibung und Darstellung von Signalen, der Signalverarbeitung und -übertragung zu vermitteln.

Die Studierenden kennen die grundlegenden Methoden und Ansätze der Systemtheorie kontinuierlicher und diskreter Signale und Systeme, so dass sie damit praktisch umgehen können und ingenieurmäßige Aufgaben mittleren Schwierigkeitsgrads vornehmlich auf den Gebieten der Nachrichten- und Automatisierungstechnik lösen können.

Inhalt: Das Modul umfasst nur die eine Lehrveranstaltung 'Signale und Systeme', deren detaillierter Inhalt der Einzelbeschreibung dieser Lehrveranstaltung entnommen werden kann:

Mathematische Modelle für die Beschreibung von Signalen und die sie verarbeitenden Systeme werden in der Vorlesung Signale und Systeme vermittelt:

- Kontinuierliche und diskrete Signale,
- zeitdiskrete lineare und zeitinvariante (LTI) Systeme,
- die z-Transformation, Laplace- und diverse Varianten der Fourier-Transformation,
- zeitkontinuierliche LTI-Systeme,
- Abtastung zeitkontinuierlicher Signale,
- Frequenzbereichsanalyse von LTI-Systemen.

Prüfungsform: siehe Lehrveranstaltungen

Veranstaltungen:

148108: Signale und Systeme 4 SWS (S.129)

1.12 Softwaretechnik

Nummer: 149326
Kürzel: SWT
Verantwortlicher: Prof. Dr.-Ing. Helmut Balzert
Arbeitsaufwand: 0 Stunden (entsprechend der Lehrveranstaltungen)
Leistungspunkte: 6

Ziele: Der Studierende wird anschließend an dieses Modul fähig sein, auf der Grundlage von Basiskonzepten und Basismethoden systematisch ein Requirements Engineering durchzuführen und Anforderungen in fachliche Lösungen unter Einsatz der UML zu überführen. Außerdem ist er in der Lage, auf der Grundlage der Anforderungen und des Systemkontextes geeignete Architekturen zu konzipieren, zu bewerten, zu vergleichen und zu realisieren. Besonderen Wert wird auf den Einsatz von Entwurfsmustern gelegt. Es wird eine Struktur zur Beschreibung von Entwurfsmustern eingeführt. Aus verschiedenen Kategorien werden repräsentative Muster und mögliche Implementierungen dargestellt. Ein wichtiges Lernziel besteht darin, dass die Studierenden selbstständig bei Bedarf weitere Entwurfsmuster auswählen, sich aneignen, bewerten und Softwaresysteme damit entwerfen und implementieren können. Durch die Kenntnis von Entwurfsmustern sollen die Studierenden auch komplexe Bibliotheken nutzen können, in denen Konzepte von Entwurfsmustern verwendet werden.

Inhalt: Innerhalb der Veranstaltungen 'Softwaretechnik I und II' lernen die Studierenden Prinzipien, Methoden und Werkzeuge der Planungs-, Definitions-, Entwurfs-, Implementierungs-, Abnahme- und Einführungsphase von Software-Systemen kennen und anwenden. Es werden die einzelnen Phasen der Software-Entwicklung mit ihren Konzepten, Methoden und Werkzeugen behandelt.

Prüfungsform: siehe Lehrveranstaltungen

Veranstaltungen:

1.13 Studienarbeit

Nummer: 149896
Kürzel: SA-ITS
Verantwortlicher: Studiendekan ITS
Arbeitsaufwand: 450 Stunden (entsprechend der Lehrveranstaltungen)
Leistungspunkte: 12

Ziele: Erwerb von Grundkenntnissen der wissenschaftlichen Arbeit, der Projektorganisation und der Präsentation wissenschaftlicher Ergebnisse.

Inhalt: Lösung einer wissenschaftlichen Aufgabe unter Anleitung.

Prüfungsform: siehe Lehrveranstaltungen

Veranstaltungen:

148183: Studienarbeit ITS 12 SWS (S.137)

1.14 Systemsicherheit

Nummer: 149340
Kürzel: SySi
Verantwortlicher: Prof. Dr. Thorsten Holz
Arbeitsaufwand: 0 Stunden (entsprechend der Lehrveranstaltungen)
Leistungspunkte: 6

Ziele: Ziel der Veranstaltungen dieses Moduls ist die Vermittlung der wichtigsten Methoden und Werkzeuge moderner Netz- und IT-Sicherheit, welche zur Konzeption und Entwicklung sicherer IT-Systeme in der Praxis benötigt werden. Insbesondere soll die Fähigkeit zum Modellieren konkreter Fragestellungen und Anforderungsanalysen aus vorhandenen Systeminformationen bzw. Systemgegebenheiten vermittelt werden. Hierzu gehört neben der Einführung in die verschiedenen Sicherheitskonzepte auch die Vertiefung ausgewählter Bereiche der Kryptographie und Sicherheitstechnologie, wie beispielsweise das Design und die Sicherheitsanalyse kryptographischer Protokolle. Wichtige theoretische und praktische Aspekte der Sicherheit von Betriebssystemen werden vermittelt, insbesondere werden sowohl Angriffs- als auch Verteidigungstechniken detailliert erläutert und anhand der Übungen praktisch ausprobiert. Ziel ist ein umfassender Überblick zu Sicherheitsaspekten modern Betriebssysteme sowie den Unzulänglichkeiten existierender Verfahren.

Inhalt: Im Rahmen dieses Moduls werden grundlegende Sicherheitsdefinitionen, Sicherheitsziele, Vertrauensmodelle, Klassifizierung möglicher Angriffe, wesentliche Sicherheitsaspekte für kryptographische Primitiven, sowie für die Systemsicherheit wichtige Protokollprimitive behandelt. Ferner werden wichtige Protokolle für Authentikation und Schlüsselaustausch bzw. -transport, und deren Sicherheitsaspekte diskutiert und deren Einsatz in verschiedenen, gängigen Internet-Sicherheitsprotokollen betrachtet. Darüber hinaus werden grundlegende Angriffstechniken (z.B. *Buffer Overflows* oder *Race Conditions*) sowie Schutzmaßnahmen (z.B. nicht-ausführbarer Speicher oder *Address Space Layout Randomization*) zur Sicherheit von Betriebssystemen behandelt. Ein weiterer Themenkomplex dieses Moduls ist moderne Schadsoftware. Dazu werden zunächst die Grundbegriffe in diesem Bereich erläutert und danach verschiedene Methoden zur Erkennung von Schadsoftware diskutiert. Wichtige Algorithmen in diesem Bereich werden vorgestellt und verschiedene Ansätze für Intrusion Detection Systeme werden behandelt.

Prüfungsform: siehe Lehrveranstaltungen

Veranstaltungen:

141342: Betriebssystemsicherheit	4 SWS	(S.41)
148178: Systemsicherheit I	3 SWS	(S.140)
148017: Systemsicherheit II	3 SWS	(S.142)

1.15 Vertiefungsmodul 1

Nummer: 149882
Kürzel: Vertfach1
Verantwortlicher: Studiendekan ITS
Arbeitsaufwand: Mindestens 240 Stunden (entsprechend der Lehrveranstaltungen)
Leistungspunkte: ≥ 8

Ziele: folgt

Inhalt: folgt

Prüfungsform: siehe Lehrveranstaltungen

Veranstaltungen:

148117: Advanced Digital System Design	3 SWS	(S.28)
148207: Algebraische Codierung für die sichere Datenübertragung	3 SWS	(S.30)
148120: Aspekte der modernen Kryptografie I	3 SWS	(S.32)
148121: Aspekte der modernen Kryptografie II	3 SWS	(S.34)
141244: Authentische Schlüsselvereinbarung: Formale Modelle und Anwendungen	3 SWS	(S.35)
148016: Betriebssystemsicherheit	3 SWS	(S.39)
148116: Beweisbar sichere Verschlüsselung	3 SWS	(S.43)
150304: Datenbanksysteme	6 SWS	(S.49)
148167: Datenschutz	3 SWS	(S.50)
150320: Effiziente Algorithmen	6 SWS	(S.56)
141168: Embedded Multimedia	4 SWS	(S.57)
148048: Endliche Körper und ihre Anwendungen	4 SWS	(S.59)
148049: FoL Krypto - Forschungsorientierte Lehre Kryptographie	3 SWS	(S.61)
148196: Implementierung kryptographischer Verfahren I	3 SWS	(S.63)
148150: Implementierung kryptographischer Verfahren II	3 SWS	(S.64)
148085: Informationstheoretische Sicherheit	3 SWS	(S.66)
148082: Konvexe Optimierung in der Signalverarbeitung und Kommunikation	3 SWS	(S.69)
148154: Kryptanalyse I	3 SWS	(S.71)
148153: Kryptanalyse II	3 SWS	(S.72)
148203: Kryptographie auf programmierbarer Hardware	4 SWS	(S.73)
310002: Künstliche Neuronale Netze	2 SWS	(S.77)
148018: Malware und Embedded Malware	3 SWS	(S.79)
143242: Master-Seminar Aktuelle Themen der IT-Sicherheit	3 SWS	(S.101)
148094: Master-Seminar Betriebssystemsicherheit und Trusted Computing	3 SWS	(S.103)
148072: Master-Seminar Computernetze und IT-Sicherheit	3 SWS	(S.104)
143021: Master-Seminar Embedded Security	3 SWS	(S.105)
148080: Master-Seminar Integrierte Schaltungen und Systeme für Mobilfunkanwendungen	3 SWS	(S.107)
148079: Master-Seminar Integrierte Schaltungen und Systeme für schnelle Datenübertragung im Internet	3 SWS	(S.108)

1.16 Vertiefungsmodul 2

Nummer: 149883
Kürzel: Vertfach2
Verantwortlicher: Studiendekan ITS
Arbeitsaufwand: Mindestens 240 Stunden (entsprechend der Lehrveranstaltungen)
Leistungspunkte: ≥ 8

Ziele: folgt

Inhalt: folgt

Prüfungsform: siehe Lehrveranstaltungen

Veranstaltungen:

148117: Advanced Digital System Design	3 SWS	(S.28)
148207: Algebraische Codierung für die sichere Datenübertragung	3 SWS	(S.30)
148120: Aspekte der modernen Kryptografie I	3 SWS	(S.32)
148121: Aspekte der modernen Kryptografie II	3 SWS	(S.34)
141244: Authentische Schlüsselvereinbarung: Formale Modelle und Anwendungen	3 SWS	(S.35)
148016: Betriebssystemsicherheit	3 SWS	(S.39)
148116: Beweisbar sichere Verschlüsselung	3 SWS	(S.43)
150304: Datenbanksysteme	6 SWS	(S.49)
148167: Datenschutz	3 SWS	(S.50)
150320: Effiziente Algorithmen	6 SWS	(S.56)
141168: Embedded Multimedia	4 SWS	(S.57)
148048: Endliche Körper und ihre Anwendungen	4 SWS	(S.59)
148049: FoL Krypto - Forschungsorientierte Lehre Kryptographie	3 SWS	(S.61)
148196: Implementierung kryptographischer Verfahren I	3 SWS	(S.63)
148150: Implementierung kryptographischer Verfahren II	3 SWS	(S.64)
148085: Informationstheoretische Sicherheit	3 SWS	(S.66)
148082: Konvexe Optimierung in der Signalverarbeitung und Kommunikation	3 SWS	(S.69)
148154: Kryptanalyse I	3 SWS	(S.71)
148153: Kryptanalyse II	3 SWS	(S.72)
148203: Kryptographie auf programmierbarer Hardware	4 SWS	(S.73)
310002: Künstliche Neuronale Netze	2 SWS	(S.77)
148018: Malware und Embedded Malware	3 SWS	(S.79)
143242: Master-Seminar Aktuelle Themen der IT-Sicherheit	3 SWS	(S.101)
148094: Master-Seminar Betriebssystemsicherheit und Trusted Computing	3 SWS	(S.103)
148072: Master-Seminar Computernetze und IT-Sicherheit	3 SWS	(S.104)
143021: Master-Seminar Embedded Security	3 SWS	(S.105)
148080: Master-Seminar Integrierte Schaltungen und Systeme für Mobilfunkanwendungen	3 SWS	(S.107)
148079: Master-Seminar Integrierte Schaltungen und Systeme für schnelle Datenübertragung im Internet	3 SWS	(S.108)

1.17 Vertiefungsmodul 3

Nummer: 149884
Kürzel: Vertfach3
Verantwortlicher: Studiendekan ITS
Arbeitsaufwand: Mindestens 240 Stunden (entsprechend der Lehrveranstaltungen)
Leistungspunkte: ≥ 8

Ziele: folgt

Inhalt: folgt

Prüfungsform: siehe Lehrveranstaltungen

Veranstaltungen:

148117: Advanced Digital System Design	3 SWS	(S.28)
148207: Algebraische Codierung für die sichere Datenübertragung	3 SWS	(S.30)
148120: Aspekte der modernen Kryptografie I	3 SWS	(S.32)
148121: Aspekte der modernen Kryptografie II	3 SWS	(S.34)
141244: Authentische Schlüsselvereinbarung: Formale Modelle und Anwendungen	3 SWS	(S.35)
148016: Betriebssystemsicherheit	3 SWS	(S.39)
148116: Beweisbar sichere Verschlüsselung	3 SWS	(S.43)
150304: Datenbanksysteme	6 SWS	(S.49)
148167: Datenschutz	3 SWS	(S.50)
150320: Effiziente Algorithmen	6 SWS	(S.56)
141168: Embedded Multimedia	4 SWS	(S.57)
148048: Endliche Körper und ihre Anwendungen	4 SWS	(S.59)
148049: FoL Krypto - Forschungsorientierte Lehre Kryptographie	3 SWS	(S.61)
148196: Implementierung kryptographischer Verfahren I	3 SWS	(S.63)
148150: Implementierung kryptographischer Verfahren II	3 SWS	(S.64)
148085: Informationstheoretische Sicherheit	3 SWS	(S.66)
148082: Konvexe Optimierung in der Signalverarbeitung und Kommunikation	3 SWS	(S.69)
148154: Kryptanalyse I	3 SWS	(S.71)
148153: Kryptanalyse II	3 SWS	(S.72)
148203: Kryptographie auf programmierbarer Hardware	4 SWS	(S.73)
310002: Künstliche Neuronale Netze	2 SWS	(S.77)
148018: Malware und Embedded Malware	3 SWS	(S.79)
143242: Master-Seminar Aktuelle Themen der IT-Sicherheit	3 SWS	(S.101)
148094: Master-Seminar Betriebssystemsicherheit und Trusted Computing	3 SWS	(S.103)
148072: Master-Seminar Computernetze und IT-Sicherheit	3 SWS	(S.104)
143021: Master-Seminar Embedded Security	3 SWS	(S.105)
148080: Master-Seminar Integrierte Schaltungen und Systeme für Mobilfunkanwendungen	3 SWS	(S.107)
148079: Master-Seminar Integrierte Schaltungen und Systeme für schnelle Datenübertragung im Internet	3 SWS	(S.108)

1.18 Wahlfächer

Nummer: 149837
Kürzel: Wafa-Erg
Verantwortlicher: Studiendekan ETIT
Arbeitsaufwand: 450 Stunden (entsprechend der Lehrveranstaltungen)
Leistungspunkte: 15

Ziele: xxx

Inhalt: xxx

Prüfungsform: siehe Lehrveranstaltungen

Veranstaltungen:

141106: freie Veranstaltungswahl (S.62)

Kapitel 2

Veranstaltungen

2.1 148117: Advanced Digital System Design

number: 148117
teaching methods: lecture with tutorials
media: Folien
Handouts
responsible person: Prof. Dr.-Ing. Christof Paar
lecturer: Dr. Tolga Yalcin
language: english
HWS: 3
angeboten im:

goals:

- Digital Design Revisited: Combinational and sequential circuits, hardware description languages, programmable logic and ASICs, design methodologies and tools.
- Hardware Architectures Revisited: Integer arithmetic circuits, floating point arithmetic circuits, finite field arithmetic circuits, parallel vs serial architectures, array architectures, distributed and parallel computing.
- Advanced Digital Design: Low-power design techniques, high-speed design techniques, clocking issues (metastability, synchronization, etc), signal interfacing, on-chip/on-board communication, design verification and testing.
- Digital Signal Processing Circuits: Digital filters: FIR and IIR filter design, fast Fourier transform: parallel/serial FFT circuit design,
- Communication Circuits: Forward error correction (FEC): BCH codec design, digital modulation/demodulation: QAM modem design.
- Cryptographic Circuits: Block ciphers: case study - PRESENT, hash functions: case study - KECCAK, asymmetric cryptography: Case study - ECC.
- The course content will be adjusted depending on the class profile, i.e. in case of too many computer science students, basic microcontroller design can be added, etc.

content: The lecture is recommended for all ITS and ETIT students who want to have a deeper understanding of practical issues in design of modern digital systems, covering a broad range of applications from telecommunication to cryptographic circuits. The students will have the chance to implement a practical design project in an HDL language of their choice (VHDL/Verilog-HDL) for a chosen target platform (FPGA or ASIC).

requirements: none

recommended knowledge: Preliminary knowledge of basic logic design (logic gates, flip-flops, state machines, etc) is a must. Computer architecture is a plus. The students are also expected to have a basic knowledge of MATLAB environment as well as fundamental digital design tools (simulation, synthesis, etc).

2.2 148207: Algebraische Codierung für die sichere Datenübertragung

Nummer: 148207
Lehrform: Vorlesungen und Übungen
Medienform: Tafelanschrieb
Verantwortlicher: Prof. Dr. Jörg Schwenk
Dozent: Dr.-Ing. Klaus Huber
Sprache: Deutsch
SWS: 3
angeboten im:

Ziele: Die Studierenden beherrschen detailliert die gängigsten Blockcodes wie BCH-, RS- und Goppacodes. Am Schluss der Vorlesung sind die Studierenden mit den Grundprinzipien der algebraischen Codierungstheorie vertraut und in der Lage Codierer und Decodierer für Standardcodes zu entwickeln.

Inhalt: Die (algebraische) Kanalcodierung stellt Methoden und Verfahren bereit, um Nachrichten gegenüber zufälligen Störungen auf einem Übertragungskanal zu sichern. Sie ist damit neben der Kryptologie ein wichtiges Gebiet der IT-Sicherheit. Die angewandten Prinzipien und Hilfsmittel sind sowohl in Codierung als auch Kryptologie oft dieselben oder ähnlich. So werden beispielsweise in beiden Disziplinen endliche Körper umfassend genutzt, in der algebraischen Codierung sind die benutzten Körper allerdings meist verhältnismäßig klein. Als weiteres Beispiel wäre der Euklidsche Algorithmus zu nennen, der in Kryptologie und Codierung eine zentrale Rolle spielt.

Gliederung

1. Übersicht und Einführung
2. Grundlagen
    - Lineare, Nichtlineare Codes,
    - Fehlererkennung und Korrektur,
    - Generator- und Prüfmatrizen,
    - Codeschranken,
    - Hammingcodes
3. Die wichtigsten Codeklassen
    - BCH-, RS-, Goppacodes
4. Decodierverfahren für die Hammingmetrik
    - Verfahren zur Decodierung von BCH-, RS-, und Goppacodes mittels des erweiterten Euklidschen Algorithmus.

5. Codes für andere Metriken
    - Berlekamps negazyklische Codes für die Lee-Metrik
    - Izyklische Codes für die Mannheim Metrik
6. Das Kryptosystem von McEliece
7. Die MacWilliamstransformation

Voraussetzungen: keine

Empfohlene Vorkenntnisse: Spezielle Vorkenntnisse sind nicht erforderlich. Die nötigen mathematischen Hilfsmittel (z.B. endliche Körper oder zahlentheoretische Grundlagen) werden je nach Bedarf während der Vorlesung erarbeitet und mit Übungsaufgaben vertieft.

2.3 148120: Aspekte der modernen Kryptografie I

Nummer:	148120
Lehrform:	Vorlesungen und Übungen
Medienform:	rechnerbasierte Präsentation Tafelanschrieb
Verantwortlicher:	Prof. Dr. Frederik Armknecht
Dozent:	Prof. Dr. Frederik Armknecht
Sprache:	Deutsch
SWS:	3
Leistungspunkte:	4
angeboten im:	

Ziele: Da das Internet und andere Formen der elektronischen Kommunikation immer mehr Verbreitung finden, wird elektronische Sicherheit zunehmend wichtiger. Das Ziel der modernen Kryptographie ist es, existierende elektronische Systeme auf ihre Sicherheit zu untersuchen, und neue zu entwerfen, die ein gewünschtes Maß an Sicherheit bieten. Beide Ziele erfordern präzise Antworten auf die beiden folgenden fundamentalen Fragen: Was meinen wir mit sicher? Wie kann man gewiss sein, dass ein System oder Algorithmus sicher ist? Am Ende der Vorlesung sollte der Student/die Studentin ein fundiertes Verständnis der Basiswerkzeuge der modernen Kryptographie haben, und geübt sein im Beweisen von Sicherheit.

Inhalt: Im ersten Teil der Vorlesung werden die notwendigen Grundlagen für eine formale Behandlung von Sicherheit gelegt. Neben dem Bereitstellen einiger mathematischer und informationstechnischer Grundlagen werden unterschiedliche Ansätze zur Definition von “sicher” diskutiert.

Im zweiten Teil werden grundlegende kryptographische Primitive erklärt, und die zugehörigen Vorstellung von Sicherheit definiert. Besonderer Wert wird hierbei auf präzise formale Definitionen gelegt, welche für ein akkurates Verständnis von, und für wissenschaftliches Arbeiten in der Kryptographie notwendig sind. Außerdem werden verschiedene Sicherheitsbeweise durchgeführt um zu illustrieren, wie Sicherheit in der modernen Kryptographie argumentiert wird, und um das Arbeiten mit unterschiedlichen Beweistechniken zu üben.

Voraussetzungen: Keine

Empfohlene Vorkenntnisse: Keine

Arbeitsaufwand: 120 Stunden

Der Arbeitsaufwand ergibt sich wie folgt: 14 Wochen zu je 3 SWS entsprechen in Summe 42 Stunden Anwesenheit. Für die Nachbereitung der

Vorlesung und die Vor- und Nachbereitung der Übungen sind etwa 4 Stunden pro Woche, in Summe 56 Stunden, erforderlich. Etwa 22 Stunden sind für die Klausurvorbereitung vorgesehen.

2.4 148121: Aspekte der modernen Kryptografie II

Nummer:	148121
Lehrform:	Vorlesungen und Übungen
Medienform:	rechnerbasierte Präsentation Tafelanschrieb
Verantwortlicher:	Prof. Dr. Frederik Armknecht
Dozent:	Prof. Dr. Frederik Armknecht
Sprache:	Deutsch
SWS:	3
Leistungspunkte:	4
angeboten im:	

Ziele: Das Ziel der modernen Kryptographie ist es, existierende elektronische Systeme auf ihre Sicherheit zu untersuchen und neue zu entwerfen, die ein gewünschtes Maß an Sicherheit bieten. Während die Vorlesung 'Aspekte der modernen Kryptographie I' die Sicherheit kryptographischer Primitive wie Verschlüsselung formal behandelte, beschäftigt sich diese Vorlesung nun überwiegend mit der beweisbaren Sicherheit von Protokollen wie beispielsweise Schlüsselaustausch. Ziel ist es, die verschiedenen Ansätze für beweisbare Sicherheit von Protokollen zu erlernen, und an ausgewählten Beispielen zu festigen.

Inhalt: Zu Beginn werden die grundlegenden Konzepte der beweisbaren Sicherheit wiederholt, damit man der Vorlesung auch folgen kann, wenn man nicht 'Aspekte der modernen Kryptographie I' besucht hat. Danach werden einige Beispiele von beweisbar sicheren kryptographischen Primitiven besprochen, die aus Zeitmangel nicht in 'Aspekte der modernen Kryptographie I' behandelt werden können. Der Schwerpunkt der Vorlesung ist eine Auswahl der wichtigsten Methoden für das formale Beweisen der Sicherheit von Protokollen, wie beispielsweise simulationsbasierte Beweise. Diese sollen an gängigen Protokollen wie Zero-Knowledge-Beweisen, Commitment-Schemes, oder Schlüsselvereinbarungsprotokollen illustriert werden.

Empfohlene Vorkenntnisse: „Aspekte der modernen Kryptographie I“ ist von Vorteil, aber nicht notwendig; Grundlagen der Kryptographie und der beweisbaren Sicherheit (letzeres wird aber nochmals kurz wiederholt)

Arbeitsaufwand: 120 Stunden

Der Arbeitsaufwand ergibt sich wie folgt: 14 Wochen zu je 3 SWS entsprechen in Summe 42 Stunden Anwesenheit. Für die Nachbereitung der Vorlesung und die Vor- und Nachbereitung der Übungen sind etwa 4 Stunden pro Woche, in Summe 56 Stunden, erforderlich. Etwa 22 Stunden sind für die Klausurvorbereitung vorgesehen.

2.5 141244: Authentische Schlüsselvereinbarung: Formale Modelle und Anwendungen

Nummer:	141244
Lehrform:	Vorlesungen und Übungen
Medienform:	rechnerbasierte Präsentation Tafelanschrieb
Verantwortlicher:	Prof. Dr. Jörg Schwenk
Dozenten:	Prof. Dr. Jörg Schwenk M. Sc. Sebastian Lauer
Sprache:	Deutsch
SWS:	3
angeboten im:	Sommersemester

Termine im Sommersemester:

Beginn: Dienstag den 12.04.2016
Vorlesung Dienstags: ab 12:15 bis 13:45 Uhr im ID 04/413
Übung Dienstags: ab 14:00 bis 14:45 Uhr im ID 04/413

Ziele: Die Studierenden verstehen die Besonderheit kryptographischer Protokolle, bei denen nicht mehr ein Algorithmus im Vordergrund steht, sondern die Interaktion verschiedener Einheiten. Sie kennen die wichtigsten Konzepte bzgl. der beweisbaren Sicherheit von Protokollen. Die wichtigsten Bausteine kryptographischer Protokolle werden behandelt, so dass die Studierenden in der Lage sind, direkt in die wissenschaftliche Literatur zu diesem Thema einzusteigen.

Inhalt: Diese Vorlesung bietet eine Einführung in das Gebiet der kryptographischen Protokolle, die den Einsatz bekannter und neuer Verfahren der Kryptographie in der Kommunikation zwischen mehreren Instanzen beschreibt. Hierbei wird sowohl Wert auf die Beschreibungen als auch auf die Sicherheit gelegt. Die Vorlesung umfasst folgende Themen:

- Kryptographische Grundlagen (Kurze Widerholung der Wahrscheinlichkeitstehorie, Informationstheorie, etc.)
- Beweisbare Sicherheit
- Analyse von Schlüsselaustauschprotokollen, insbesondere TLS und SSH

Die Zusammenstellung ist nicht fest und kann nach Absprache mit den Hörern auch geändert werden.

Voraussetzungen: keine

Empfohlene Vorkenntnisse:

- Grundkenntnisse Kryptographie
- Empfehlung: Durcharbeiten der ersten 40 Folien vom Skript Kryptographie I von Prof. Alexander May

Prüfung: schriftlich, 120 Minuten

2.6 148191: Automatisierungstechnik

Nummer:	148191
Lehrform:	Vorlesungen und Übungen
Medienform:	Blackboard
	Folien
	Tafelanschrieb
Verantwortlicher:	Prof. Dr.-Ing. Jan Lunze
Dozenten:	Prof. Dr.-Ing. Jan Lunze
	M. Sc. Sven Bodenburg
Sprache:	Deutsch
SWS:	4
angeboten im:	

Ziele: Es werden die fachspezifischen Grundlagen der Automatisierungstechnik vermittelt. Die Übungen tragen dazu bei, erste Erfahrungen im Umgang und der Anwendung der systemtheoretisch begründeten Methoden auf unterschiedliche Anwendungsbeispiele zu sammeln. Dabei werden die Methoden zur Beschreibung und Analyse dynamischer Systeme und zum Steuerungsentwurf erlernt, wobei sowohl wertkontinuierliche als auch ereignisdiskrete Systeme behandelt werden.

Inhalt: Die Vorlesung behandelt die grundlegenden automatisierungstechnischen Aufgaben und Methoden in drei Teilen:

- Einführung
  - Ziele und Aufgaben der Automatisierungstechnik
  - Grundlegende Eigenschaften dynamischer Systeme
- Automatisierung kontinuierlicher Systeme
  - Beschreibung und Verhalten kontinuierlicher Systeme
  - Steuerbarkeit und Beobachtbarkeit
  - Stabilität
  - Einstellregeln für PID-Regler
  - Zustandsbeobachtung und Diagnose kontinuierlicher Systeme
- Automatisierung und Verhalten diskreter Systeme
  - Beschreibung diskreter Systeme
  - Entwurf diskreter Steuerungen
  - Zustandsbeobachtung und Diagnose diskreter Systeme

Voraussetzungen: keine

Empfohlene Vorkenntnisse:

- Module Mathematik A, B, C
- Modul Signale und Systeme
- Modul Systemanalyse

Literatur:

[1] Lunze, Jan "Automatisierungstechnik", Oldenbourg Wissenschaftsverlag, 2012

2.7 148016: Betriebssystemsicherheit

Nummer:	148016
Lehrform:	Vorlesungen und Übungen
Medienform:	Folien
	Handouts
Verantwortlicher:	Prof. Dr.-Ing. Ahmad-Reza Sadeghi
Dozenten:	Prof. Dr.-Ing. Ahmad-Reza Sadeghi
	Dipl.-Ing. Biljana Cubaleska
Sprache:	Deutsch
SWS:	3
angeboten im:	

Ziele: Ziel dieser Veranstaltung ist es, die Rolle der Betriebssystemsicherheit für die Sicherheit aller darauf laufenden Anwendungen zu zeigen, Probleme aufzudecken und Techniken zu deren Behebung zu behandeln. Neue Technologien zur Behebung einiger Sicherheitsprobleme sollen auch vorgestellt werden. Durch die im Labor für Betriebssystemsicherheit durchzuführenden Übungen soll der praktische Umgang mit vielen Aspekten der Betriebssystemsicherheit vermittelt werden.

Inhalt: Die Sicherheit heutiger IT-Systeme ist ein Faktor, der viele Anwendungen ermöglicht und ausschlaggebend für deren Funktionsfähigkeit und Akzeptanz ist. Obwohl auf der Anwendungsebene eine Menge an ausgereiften Sicherheitsmechanismen (sowohl kryptographisch, als auch nicht kryptographisch) schon vorhanden sind, scheitert die Sicherheit vieler Anwendungen trotzdem, und zwar häufig wegen Lücken in der Sicherheit des darunter liegenden Betriebssystems. Das Thema dieser Vorlesung ist der für die Sicherheit aller IT-Systeme ausschlaggebende Teil der Betriebssystemsicherheit.

Bevor aber der Begriff „sicheres Betriebssystem“ definiert, und auf die für die Sicherheit der Betriebssysteme grundlegenden Konzepte eingegangen wird, werden die Grundlagen der Betriebssysteme eingeführt. Besonders die Bereiche, die für die Sicherheit eines Betriebssystems ausschlaggebend sind, werden ausführlich behandelt: Techniken zur Speicher- und Prozessverwaltung, Dateiensysteme, Verwaltung von Ein- und Ausgänge, Zugangskontrolle, sowie Verhinderung von Deadlocks. Es wird auf die Probleme hingewiesen, und sowohl auf die gängigen als auch auf neuen Techniken zu deren Behebung eingegangen.

Ein Kernteil dieser Veranstaltung ist die Vorstellung der gängigen sowohl von innen als auch von außen stammenden Angriffe auf Betriebssysteme, und Vorstellung der Mechanismen zur deren Verhinderung. Beispiele, die ausführlich behandelt werden, sind Techniken gegen Buffer Overflows, Abwehr gegen Schadcode (Viren, Würmer, Trojaner) und Verhinderung verdeckter Kanäle. Behandelt wird auch das Thema Virtualisierung und deren Anwendungen. Auch die reaktiven Sicherheitsmechanismen, wie Speicherung wichtiger Betriebsdaten (Logging), Überprüfung (Auditing), und Wiederherstellung (Recovery) werden diskutiert. Behandelt wird auch die Zertifizierung der Systeme und zwar am Beispiel des Orange Book und der Common Criteria. Dabei

wird auch der Begriff „vertrauenswürdiges System“ definiert.

Zum Schluss wird die Sicherheit der gängigen Betriebssysteme, wie zum Beispiel Windows, Unix/Linux, und MAC analysiert. Auch Hypervisor-basierte Betriebssysteme, wie VAX-VMM, oder Perseus werden vorgestellt.

Die Vorlesung wird mit praktischen Übungen begleitet, die im neu eingerichteten Labor für Betriebssystemsicherheit realisiert werden.

Empfohlene Vorkenntnisse: Grundlagen der Kryptographie, Informatik sowie Betriebssysteme

Literatur:

[1] Gasser, Morrie "BUILDING A SECURE COMPUTER SYSTEM", Van Nostrand Reinhold, 1988
[2] Gagne, Greg, Galvin, Peter Baer, Silberschatz, Avi "Operating System Concepts", Wiley & Sons, 2008
[3] Jaeger, Trent "Operating System Security", None, 2008

2.8 141342: Betriebssystemsicherheit

Nummer:	141342
Lehrform:	Vorlesungen und Übungen
Medienform:	e-learning rechnerbasierte Präsentation
Verantwortlicher:	Prof. Dr. Thorsten Holz
Dozenten:	Prof. Dr. Thorsten Holz Dipl.-Biol. Robert Gawlik
Sprache:	Deutsch
SWS:	4
angeboten im:	Wintersemester

Termine im Wintersemester:

Beginn: Montag den 19.10.2015
Vorlesung Montags: ab 14:15 bis 15:45 Uhr im ID 04/471
Vorlesung Montags: ab 14:15 bis 15:45 Uhr im ID 04/459
Übung Montags: ab 16:15 bis 17:45 Uhr im ID 04/471
Übung Montags: ab 16:15 bis 17:45 Uhr im ID 04/459

Ziele: Die Studierenden beherrschen theoretische und praktische Aspekte der Sicherheit von Betriebssystemen und sind zu einer kritischen Betrachtung der Systemsicherheit in der Lage.

Inhalt: Im ersten Teil der Veranstaltung werden verschiedene Sicherheitsaspekte von Betriebssystemen vorgestellt und erläutert. Dazu werden sowohl wichtige Angriffsmethoden (z.B. *Buffer Overflows* oder *Race Conditions*) als auch Abwehrstrategien (z.B. nicht-ausführbarer Speicher oder *Address Space Layout Randomization*) diskutiert. Andere Themen, die im Mittelpunkt dieses Teils der Vorlesung stehen, sind Virtualisierung/Hypervisor sowie das sogenannte Einsperrungs-Problem (*Confinement Problem*) und die damit verbundene Analyse der verdeckten Kanäle in einem Computer-System.

Im zweiten Teil der Veranstaltung liegt der Schwerpunkt auf Schadsoftware. Dazu werden zunächst die Grundbegriffe in diesem Bereich erläutert und danach verschiedene Methoden zur Erkennung von Schadsoftware diskutiert. Wichtige Algorithmen in diesem Bereich werden vorgestellt und verschiedene Ansätze für Intrusion Detection Systeme werden behandelt.

Im praktischen Teil der Veranstaltung wird die Sicherheit von mehreren realen Systemen analysiert. Ein integraler Teil der Veranstaltung sind die Übungen, die den Stoff mit praktischen Beispielen veranschaulichen und vertiefen.

http://10kstudents.eu/s/img/10K_students_logo.png

Voraussetzungen: keine

Empfohlene Vorkenntnisse: Erfahrung in systemnaher Programmierung sowie der Programmiersprache C sind hilfreich für das Verständnis der vermittelten Themen.

Prüfung: schriftlich, 120 Minuten

2.9 148116: Beweisbar sichere Verschlüsselung

Nummer:	148116
Lehrform:	Vorlesung mit integrierten Übungen
Medienform:	Folien
	Tafelanschrieb
Verantwortlicher:	Prof. Dr.-Ing. Christof Paar
Dozent:	Dr. Bodo Möller
Sprache:	Deutsch
SWS:	3
angeboten im:	

Ziele: Ziel der Lehrveranstaltung ist das Kennenlernen und Anwenden von formalen Methoden zum Beurteilen der Sicherheit kryptographischer Verfahren, speziell auch das Kennenlernen von verschiedenen Sicherheitsbegriffen und grundlegenden Konstruktionen für die Verschlüsselung.

Inhalt: Wann können kryptographische Verfahren als sicher gelten? Auf Ad-hoc-Konstruktionen kann man sich oft nicht verlassen: Es gibt viele Beispiele von subtilen Schwachstellen, die leicht zu übersehen sind. Auf der sicheren Seite ist man, wenn man beweisen kann, dass eine Konstruktion Sicherheit bietet.

Eine Voraussetzung dafür ist die Formalisierung der Sicherheitsziele, also eine präzise Beschreibung, was von den Verfahren erwartet wird. Hierfür kann man ein formalisiertes Angriffsspiel beschreiben, in dem ein Angreifer mit einem Verfahren interagiert. Sind die Erfolgsaussichten jedes denkbaren Angreifers verschwindend gering, so ist das Sicherheitsziel erreicht.

Eine Aussicht auf einen vollständigen Sicherheitsbeweis für ein kryptographisches Verfahren hat man allerdings nur in den wenigsten Fällen (sonst wären fundamentale Fragen der Komplexitätstheorie geklärt). Man muss sich also mit bescheideneren Zielen begnügen. Wir unterscheiden zwischen kryptographischen Primitiven einerseits, und darauf aufbauenden kryptographischen Konstruktionen andererseits. Setzen wir (einfache) Sicherheitseigenschaften der Primitive voraus, so können wir (kompliziertere) Eigenschaften von Konstruktionen beweisen. Ein solcher Beweis durch Reduktion sagt nichts für irgendwelche bestimmten Primitive, kann aber jedenfalls die Stimmigkeit einer Konstruktion an sich bestätigen.

Die Vorlesung behandelt Konzepte und Techniken der beweisbaren Sicherheit in der Kryptographie, und konzentriert sich dabei exemplarisch auf die Verschlüsselung. Es gibt zahlreiche Szenarien und Sicherheitsbegriffe für Verschlüsslung, und eine Vielfalt an kryptographischen Primitiven und kryptographischen Konstruktionen:

- symmetrische Verschlüsselung, Public-Key-Verschlüsselung
- Chosen-plaintext attack (CPA), chosen-ciphertext attack (CCA); left-or-right (LoR), real-or-random (RoR), indis-

tinguishability of encryption (IND), semantische Sicherheit; non-malleability (NM), integrity of ciphertexts (INT-CTXT)

- pseudorandom generator, pseudorandom function, pseudorandom permutation, super-pseudorandom permutation; Public-Key-Verfahren
- Modes of operation, hybride Verschlüsselung

Von konkreten kryptographischen Primitiven (wie etwa AES) wird abstrahiert, trotzdem können kryptographische Konstruktionen aus der Praxis betrachtet werden, z.B. aus dem SSL/TLS-Protokoll.

Voraussetzungen: keine

Empfohlene Vorkenntnisse: Grundkenntnisse Kryptographie

2.10 148194: Computerarchitektur und Betriebssysteme

Nummer:	148194
Lehrform:	Vorlesungen und Übungen
Medienform:	Folien rechnerbasierte Präsentation Tafelanschrieb
Verantwortlicher:	Prof. Dr.-Ing. Michael Hübner
Dozenten:	Prof. Dr.-Ing. Michael Hübner M. Sc. Muhammed Soubhi Al Kadi M. Sc. Fynn Schwiegelshohn
Sprache:	Deutsch
SWS:	4
angeboten im:	

Ziele: Die Studierenden kennen Zusammenhänge und haben Detailkenntnisse zum Aufbau, zu Komponenten und zur Funktionsweise moderner Computersysteme in Hard- und Software. Damit haben sie die Basis, um sowohl in der Computertechnik selbst, als auch in deren Anwendungsbereichen - wie z.B. der Automatisierungstechnik - Computerkomponenten und -systeme auszulegen, und zu entwickeln.

Um die Studierenden zum Einen hinsichtlich Teamarbeit, Kommunikationsfähigkeit und Dokumentationsfähigkeit weiter zu qualifizieren und zum Zweiten anwendungsbezogene, praxisrelevante Problemstellungen und deren Lösungsmöglichkeiten zu vermitteln, wird veranstaltungsbegleitend ein Projekt angeboten, das im Team von 3 - 4 Studierenden zu bearbeiten ist. Abhängig von der inhaltlichen und formal-stilistischen Ausarbeitung kann ein Bonus von bis zu 10% erworben werden, der bei der Abschlussklausur angerechnet wird.

Inhalt: Im ersten Teil der Veranstaltung werden, ausgehend von grundlegenden Computerstrukturen (Von-Neumann-Architektur, SISD, SIMD, MIMD), grundlegende Fähigkeiten zum anforderungsgerechten Entwurf, und zur anwendungsbezogenen Realisierung von Computersystemen vermittelt. Konkrete Beispiele heutiger Computer für unterschiedliche Anwendungsfelder (8051, Pentium 4, Core-Architektur, Ultra Sparc III) runden die generellen Wissensinhalte ab. Einen besonderen inhaltlichen Schwerpunkt bildet die Programmierung der Mikroarchitekturebene als Ergänzung zu anderen Lehrveranstaltungen im Bereich der Informatik / Computertechnik (Programmiersprachen, Eingebettete Prozessoren). Im zweiten Teil der Veranstaltung werden die Basisfunktionen moderner Betriebssysteme behandelt. Schwerpunkte sind hier die Organisation von Prozessen mit Prozessscheduling und Interprozesskommunikation sowie die Behandlung von Deadlocks.

Im Detail ist die Lehrveranstaltung wie folgt gegliedert:

- Einführung

  - Grundstrukturen und Definitionen
  - Prinzipien moderner Computerarchitektur
- Struktur und Aufbau von Computersystemen
  - Klassische “Von-Neumann-Struktur”
  - Parallelitätsprinzipien
  - Klassifikation und Merkmale von Computerarchitekturen
- Logisch digitale Ebene
  - CPU-Chips und Busse
  - Schnittstellen
- Mikroarchitekturebene
  - Fallbeispiel einer Mikroarchitektur
  - Design der Mikroarchitekturebene
  - Methoden der Leistungsoptimierung
  - Beispiele der Mikroarchitekturebene
- Betriebssystemebene
  - Prozesse und Threads (Scheduling, Interprozesskommunikation)
  - Deadlock-Behandlung
  - Organisation virtueller Speicher
  - Virtuelle E/A-Instruktionen

Voraussetzungen: keine

Empfohlene Vorkenntnisse: Inhalt aus den Vorlesungen:

- Digitaltechnik
- Programmiersprachen
- Eingebettete Prozessoren

Literatur:

[1] Tanenbaum, Andrew S. ”Computerarchitektur. Strukturen - Konzepte - Grundlagen”, Pearson, 2006
[2] Tanenbaum, Andrew S. ”Modern Operating Systems”, Pearson, 2009
[3] Tanenbaum, Andrew S. ”Moderne Betriebssysteme”, Pearson, 2009
[4] Bode, Arndt, Hennessy, John L., Patterson, David A. ”Rechnerorganisation und -entwurf”, Spektrum Akademischer Verlag, 2005
[5] Tanenbaum, Andrew S. ”Structured Computer Organization”, Prentice Hall, 2005

2.11 148070: Computernetze II

Nummer:	148070
Lehrform:	Vorlesungen und Übungen
Medienform:	Folien rechnerbasierte Präsentation
Verantwortlicher:	Prof. Dr.-Ing. York Tüchelmann
Dozenten:	Prof. Dr.-Ing. York Tüchelmann wiss. Mitarbeiter
Sprache:	Deutsch
SWS:	3
angeboten im:	

Ziele: Die Studierenden sollen in die Lage versetzt werden, Computernetze unter Berücksichtigung von Geschäftsprozessen und Workflows im Unternehmen, daraus resultierenden Nutzer- und Anwendungs-anforderungen sowie weiteren nicht-tech-nischen und technischen Randbedingungen und Parametern im Unternehmen Computer-netze planen und auslegen zu können. Dazu sind Entwurfsziele und Wege zu deren Umsetzung zu formulieren, Konzepte zu erarbeiten, technische Anforderungen und Parameter bezüglich den Performance-Kenngrößen Zuverlässigkeit, Datenrate und Verzögerungen zu spezifizieren, um auf dieser Basis ein Computernetz nach Optimierungskriterien planen und auslegen zu können.

Inhalt: Die Lehrveranstaltung vermittelt eine Systematik und methodische Vorgehens-weisen zur Planung und Auslegung von Computernetzen - insbesondere für Netze großer Unternehmen, Verwaltungen und anderer Institutionen mit folgenden Inhalten:

•Einflussgrößen, Planungs- und Auslegungs-parameter - Unternehmensspezifische Einflussfaktoren -Nicht-technische und technische Auslegungsparameter -Performance Parameter

•Grundlagen der Planung und Auslegung -Prozess der Planung und Auslegung -Varianten der Strukturierung -Dokumentation des Planungs- und Auslegungsprozesses -Güte der Planung und Auslegung

•Erfassung und Analyse von Rahmenbedin-gungen und Anforderungen -Ist-Analyse -Anforderungsanalyse -Datenflussanalyse

•Entwicklung von Basisarchitekturen -Switching -Routing Architektur - Security Architektur -Performance Architektur

•Entwicklung von Erweiterungs-architekturen -Computernetz-Management Architektur -Content Delivery Architektur

•Hardwareauswahl und –positionierung

•Prüfung und Umsetzung des Entwurfs

Empfohlene Vorkenntnisse: Basiswissen der Informationstechnik / Kommunikationstechnik

Literatur:

[1] Kurose, James F., Ross, Keith W. "Computer Networking: A Top-Down Approach", Addison Wesley Longman, 2009
[2] Kurose, James, Ross, Keith "Computernetze. Ein Top-Down-Ansatz mit Schwerpunkt Internet", Pearson, 2008
[3] McCabe, James D. "Network Analysis, Architecture and Design", Morgan Kaufmann, 2007

2.12 150304: Datenbanksysteme

Nummer: 150304
Lehrform: Vorlesungen und Übungen
Medienform: Tafelanschrieb
Verantwortlicher: Dr. Edgar Korthauer
Dozent: Dr. Edgar Korthauer
Sprache: Deutsch
SWS: 6
angeboten im: Wintersemester

Ziele: Die Studierenden sind in der Lage einschlägige Systemdokumentation und wissenschaftliche Literatur über Datenbanksysteme zu verstehen.

Inhalt:

- Implementierungstechniken für Datenstrukturen, die in Datenbanken Verwendung finden
- Konzeptionelle Grundlagen des Entity-Relationship-Modells
- Relationenalgebra
- Relationenkalkül
- Elemente der Sprache SQL und verwandter Systeme
- Normalformenlehre
- Optimierung von Anfragen durch Transformation
- Aspekte der parallelen Ausführung und Fehlerbehebung für Transaktionen

Voraussetzungen: keine

Empfohlene Vorkenntnisse: Grundlagen der Informatik und Datenstrukturen

Prüfung: schriftliche Prüfung, 90 Minuten

Literatur:

[1] Eickler, Andrè, Kemper, Alfons "Datenbanksysteme - Eine Einführung", Oldenbourg Verlag, 2009
[2] R., Elmasri, S., Navathe "Grundlagen von Datenbanksystemen", Pearson, 2009

2.13 148167: Datenschutz

Nummer:	148167
Lehrform:	Vorlesungen und Übungen
Medienform:	Folien rechnerbasierte Präsentation Tafelanschrieb
Verantwortlicher:	Prof. Dr.-Ing. Thomas Andreas Herrmann
Dozenten:	Prof. Dr.-Ing. Thomas Andreas Herrmann Dr. Kai-Uwe Loser
Sprache:	Deutsch
SWS:	3
angeboten im:	

Ziele: Datenschutz befasst sich mit der Frage, wie man Bürger, Arbeitnehmer, Kunden, Patienten etc. vor dem Mißbrauch von elektronisch gespeicherten Daten zu ihrer Person schützen kann. Es besteht die Anforderung an Informatiker, Computersysteme so zu gestalten, dass sie die Umsetzung datenschutzrechtlicher Prinzipien unterstützen. Die Vorlesung befasst sich daher mit den Grundzügen des Datenschutzrechtes und den praktischen Auswirkungen für Informatiker. Dabei wird vor allem Wert darauf gelegt, die zentralen Prinzipien verstehbar zu machen. Neben dem allgemeinen Datenschutzgesetz werden auch Spezialregelungen behandelt, die z.B. für die Regulierung der Telekommunikation, oder für den Einsatz elektronischer Datenverarbeitung in der Arbeitswelt zum Einsatz kommen. Darüber hinaus wird verdeutlicht, welche Konsequenzen für die Entwicklung von Software-Systemen zu ziehen sind. Lernziel der Vorlesung ist es, dass die Studierenden künftig in der Lage sind, zu erkennen, an welchen Stellen ihres beruflichen Wirkens der Datenschutz relevant ist, und wie sie vorgehen müssen, um sich geeignete Informationen oder Sachverstand zu besorgen. Das zu vermittelnde Wissen soll so grundlegend sein, daß man sich auch auf neue Entwicklungen (wie etwa Novellierungen und Ergänzungen des Bundesdatenschutzgesetzes) einstellen kann.

Inhalt:

- Was ist informationelle Selbstbestimmung?
- Aufbau des Bundesdatenschutzgesetzes
- Welche Datenregister gibt es?
- Welche Rechte haben die von der Datenspeicherung Betroffenen?
- Was passiert mit personenbezogenen Daten in vernetzten Systemen?
- Welche organisatorischen und technischen Maßnahmen helfen, personenbezogene Daten zu sichern?
- Spezielle Bereiche der Datenverarbeitung: Telekommunikation, Wirtschaft, Medizin

Empfohlene Vorkenntnisse: keine

Prüfung: Projektarbeit, studienbegleitend

Literatur:

[1] Gola, Peter, Jaspers, Andreas "Das BDSG im Überblick", Datakontext Fachverlag G, 2006
[2] Ehmann, Eugen, Gerling, Rainer W., Tinnefeld, Marie-Theres "Einführung in das Datenschutzrecht. Datenschutz und Informationsfreiheit in europäischer Sicht", Oldenbourg, 2004

2.14 150322: Datenstrukturen

Nummer:	150322
Lehrform:	Vorlesungen und Übungen
Medienform:	Folien
	Tafelanschrieb
Verantwortlicher:	Jun. Prof. Dr. Maike Buchin
Dozent:	Jun. Prof. Dr. Maike Buchin
Sprache:	Deutsch
SWS:	6
angeboten im:	Sommersemester

Ziele: Die Vorlesung soll die Fähigkeit schulen, bekannte Datenstrukturen professionell einzusetzen, neue Datenstrukturen bei Bedarf selbst zu entwerfen, die Korrektheit eines Algorithmus sauber zu begruenden und seine Laufzeit zu analysieren.

Inhalt: Nach einer Besprechung grundlegender Datentypen (wie Listen, Stacks, Queues und B“aume) werden zunaechst Datenstrukturen diskutiert, die zur Repräsentation von Mengen geeignet sind und dabei bestimmte Mengenoperationen unterstützen (wie zum Beispiel Dictionaries, Priority Queues und UNION-FIND-Datenstruktur). Weiterhin gehen wir auf Repräsentationen von Graphen ein, behandeln diverse Graphalgorithmen (wie zum Beispiel Tiefen- und Breitensuche, kürzeste Wege, transitive Hülle, starke Komponenten und minimaler Spannbaum) sowie diverse Sortierverfahren (Mergesort, Heapsort, Quicksort, Bucketsort, Radixsort).

Voraussetzungen: keine

Empfohlene Vorkenntnisse:

- Elementare Sprachmerkmale der Programmiersprache Java ™,
- Mathematik-Kenntnisse im Umfang von „Höhere Mathematik I und II“

Prüfung: schriftliche Prüfung, 90 Minuten

Literatur:

[1] Drake, Peter "Data Structures and Algorithms in Java", Prentice Hall, 2005
[2] Dieker, Stefan, Güting, Ralf H. "Datenstrukturen und Algorithmen", Teubner Verlag, 2004

2.15 148020: Digitale Signalverarbeitung

Nummer:	148020
Lehrform:	Vorlesungen und Übungen
Medienform:	Folien Handouts rechnerbasierte Präsentation Tafelanschrieb
Verantwortlicher:	Prof. Dr.-Ing. Dorothea Kolossa
Dozent:	Prof. Dr.-Ing. Dorothea Kolossa
Sprache:	Deutsch
SWS:	4
angeboten im:	

Ziele: Vermittlung von systematischen Methoden zur vollständigen Beschreibung und Analyse bzw. Simulation digitaler Systeme, sowohl im Zeit-, als auch im Frequenzbereich. Systemtheorie linearer und zeitinvarianter zeitdiskreter Systeme zur Verarbeitung bzw. Transformation von Signalfolgen gemäß mathematisch formulierbarer Vorschriften.

Die Studierenden kennen die grundlegenden Methoden zur Beschreibung und Analyse von digitalen Systemen, sowie den Aufbau von realisierenden Strukturen und Algorithmen. Sie sind in der Lage, grundlegende Aufgaben im Zusammenhang mit der Analyse und Simulation digitaler Systeme zu formulieren, zu interpretieren, zu verstehen und zu lösen.

Inhalt:

- Zeitdiskrete und digitale Signale (reell, komplex)
- Eigenschaften diskreter Signale und Systeme im Zeit- und Frequenzbereich
- Abtasttheoreme für reelle und komplexe Tiefpasssignale
- z-Transformation: Existenz, Eigenschaften, Stabilität digitaler Systeme
- Zeitdiskrete und Diskrete Fourier-Transformation: Eigenschaften, Beziehungen zu anderen Transformationen
- Deterministische Spektralanalyse: DFT-Analyse periodischer Signale, Gebrauch von Fensterfunktionen
- Übertragungsfunktion: Pol-/Nullstellen-Darstellung, Frequenzgang
- Realisierbarkeitsbedingungen für digitale Systeme
- Entwurf rekursiver Filter
- Entwurf linearphasiger FIR-Filter
- Strukturen digitaler Filter: Kanonische rekursive (IIR) und nichtrekursive (FIR) Strukturen

- Merkmale und Einsatz digitaler Signalprozessoren

Voraussetzungen: keine

Empfohlene Vorkenntnisse: DSVITS-Variante:

- Mathematik A + B
- Grundlagen der Elektrotechnik und Elektronik
- Grundlagen der Informationstechnik
- Grundlagen der Informatik.

DSVETuIT-Variante:

- Mathematik A + B
- Grundlagen der Elektrotechnik I und II
- Grundlagen der Informationstechnik I und II.

Veranstaltung: Signale und Systeme

2.16 148181: Diplomarbeit ITS

Nummer: 148181
Lehrform: Diplomarbeit
Verantwortlicher: Studiendekan ITS
Dozent: Hochschullehrer der Fakultät ET/IT
Sprache: Deutsch
SWS: 25
Leistungspunkte: 30
angeboten im:

Ziele: Die Diplomprüfung bildet den berufsqualifizierenden Abschluss des Studiums im Diplomstudiengang Sicherheit in der Informationstechnik an der Ruhr-Universität Bochum. Durch die Diplomprüfung soll festgestellt werden, ob die Kandidatin bzw. der Kandidat die für den Übergang in die Berufspraxis notwendigen gründlichen Fachkenntnisse erworben hat, die fachlichen Zusammenhänge überblickt und die Fähigkeit besitzt, wissenschaftliche Methoden und Erkenntnisse anzuwenden.

Die Diplomprüfung führt zum wissenschaftlich berufsqualifizierenden Abschluss des Studiums. Durch die Diplomprüfung soll festgestellt werden, ob der Kandidat bzw. die Kandidatin fundierte Kenntnisse und die Fähigkeit zur selbstständigen Anwendung anspruchsvoller wissenschaftlicher Methoden erlernt hat. Die Studierenden sollen zur kritischen Einordnung der wissenschaftlichen Erkenntnisse sowie zu verantwortlichem, interdisziplinärem Denken und Handeln befähigt werden und sollen komplexe Probleme der Sicherheit in der Informationstechnik analysieren und Lösungen erarbeiten können. Die Diplomprüfung setzt sich aus der kumulativen Bewertung aller im Hauptstudium absolvierten Prüfungen in den zugeordneten Lehrveranstaltungen und der Diplomarbeit zusammen.

Inhalt: Die Diplomarbeit ist eine schriftliche Prüfungsarbeit und schließt das Studium ab. Sie soll zeigen, dass der Kandidat bzw. die Kandidatin in der Lage ist, innerhalb einer vorgegebenen Frist ein anspruchsvolles Problem der Sicherheit in der Informationstechnik selbstständig mit wissenschaftlichen Methoden zu bearbeiten.

Empfohlene Vorkenntnisse: Vorkenntnisse entsprechend dem gewählten Thema erforderlich

Arbeitsaufwand: 900 Stunden

6 Monate Vollzeittätigkeit

Prüfung: Abschlussarbeit, studienbegleitend

2.17 150320: Effiziente Algorithmen

Nummer:	150320
Lehrform:	Vorlesungen und Übungen
Medienform:	Folien
	Internet
	Tafelanschrieb
Verantwortlicher:	Priv.-Doz. Dr. Daniela Kacso
Dozent:	Priv.-Doz. Dr. Daniela Kacso
Sprache:	Deutsch
SWS:	6
Leistungspunkte:	9
angeboten im:	Sommersemester

Ziele: Die Studierenden kennen grundlegende Datenstrukturen und effiziente Algorithmen und sind mit Analysetechniken vertraut (Korrektheitsbeweis und Laufzeitanalyse).

Inhalt: Die Lehrveranstaltung kann sowohl in das Gebiet der praktischen als auch in das Gebiet der theoretischen Informatik eingeordnet werden. Die zentralen Themen sind die folgenden:

- Berechnung kürzester Pfade in einem Graphen bei ganzzahligen Kantenkosten
- Berechnung eines maximalen Flusses in einem Transportnetzwerk
- Berechnung einer optimalen Lösung bei einem Zuordnungsproblem (auch Matching-Problem genannt)

Darüberhinaus beschäftigen wir uns mit Anwendungen dieser grundlegenden Probleme.

Voraussetzungen: keine

Empfohlene Vorkenntnisse: Inhalte der Veranstaltung “Datenstrukturen”

Arbeitsaufwand: 270 Stunden

Der Arbeitsaufwand berechnet sich wie folgt: 14 Wochen zu je 6 SWS ergeben 84 Stunden Anwesenheit. Zur Vor-und Nachbereitung sind 126 Stunden sowie für die Prüfungsvorbereitung 60 Stunden vorgesehen.

Prüfung: schriftliche Prüfung, 120 Minuten

2.18 141168: Embedded Multimedia

Nummer:	141168
Lehrform:	Vorlesung mit integrierten Übungen
Medienform:	Blackboard rechnerbasierte Präsentation
Verantwortlicher:	Prof. Dr.-Ing. Rainer Martin
Dozent:	Dr. Wolfgang Theimer
Sprache:	Deutsch
SWS:	4
angeboten im:	Sommersemester

Termine im Sommersemester:

Beginn: Mittwoch den 13.04.2016
Vorlesung m. int. Übung Mittwochs: ab 16:15 bis 17:45 Uhr im ID 03/401
Übung: nach Absprache

Ziele: Die Studierenden haben grundlegende Fertigkeiten für das Systemdesign, die Implementierung, sowie die Integrations- und Testphase von Multimedialösungen im Bereich Embedded Systems. Sie sind befähigt, Hardware- und Softwarearchitekturen von eingebetteten Multimediasystemen zu bewerten. Sie haben anhand einer Plattform mit dem Unix-Echtzeitbetriebssystem QNX Programmiererfahrungen gesammelt und in einem Projektteam eine Aufgabe aus dem Bereich der Multimediakommunikation gelöst.

Inhalt: Die Lehrveranstaltung vermittelt die Grundlagen zur Durchführung von Entwicklungsarbeiten im Bereich der eingebetteten Systeme, und hat den Fokus Multimediatechnologien. Zu Beginn der Vorlesung wird eine kurze Einführung in die Entwicklungsprozesse wie System Engineering, Softwareentwicklung und Testvorgehen gegeben, um die Projektteams methodisch vorzubereiten. Anschließend werden grundlegende Hardware- und Softwarearchitekturen von Embedded Systems präsentiert, um sie zu befähigen, Lösungskonzepte einordnen zu können. Der Fokus der Lehrveranstaltung liegt danach in der detaillierten Analyse einer Smartphone-Plattform am Beispiel von BlackBerry 10. Die Nutzung der Prozessorplattform und der Multimediaperipherie-komponenten wird anhand der Eclipse-basierten Momentix-Entwicklungsumgebung unter C/C++ vertieft. Im Rahmen der praktischen Umsetzung in einem Projektteam erwerben die Studierenden die Fähigkeiten, gemeinsam ein Entwicklungsproblem zu strukturieren, ein Lösungskonzept zu entwickeln, und unter Zuhilfenahme von existierenden Softwaremodulen zu einer Gesamtlösung zu integrieren. Die Herangehensweise des Projektteams, und die Lösung sind vom Projektteam zu dokumentieren und abschließend allen Teilnehmern zu präsentieren.

Voraussetzungen: keine

Empfohlene Vorkenntnisse:

- Kenntnis der Programmiersprache C/C++
- Grundlagen der Signalverarbeitung

Prüfung: mündlich, 30 Minuten

2.19 148048: Endliche Körper und ihre Anwendungen

Nummer: 148048
Lehrform: Vorlesungen und Übungen
Medienform: Tafelanschrieb
Verantwortlicher: Prof. Dr. Roberto M. Avanzi
Dozent: Prof. Dr. Roberto M. Avanzi
Sprache: Deutsch
SWS: 4
Leistungspunkte: 6
angeboten im:

Ziele: Die Vorlesung bietet die Möglichkeit, die Kenntnisse über endliche Körper zu vertiefen, und eine Einführung in deren praktischen Aspekten und Anwendungen zu bekommen, z.B. in Vorbereitung auf einer Abschlussarbeit über kryptographische Anwendungen von elliptischen, oder hyperelliptischen Kurven.

Inhalt: Endliche Körper sind überall - in der Mathematik und in den anderen Naturwissenschaften, auch in den Computerwissenschaften. Bereits die einfachsten endlichen Körper, die uns schon im ersten Semester begegnen, nämlich Z/pZ, wobei p eine Primzahl ist, besitzen eine sehr reiche mathematische Struktur, und haben wichtigen Anwendungen in der Kryptologie, und in der Codierungstheorie: zum Beispiel für die sichere Verschlüsselung von Nachrichten, oder für die zuverlässige Speicherung von Daten auf CDs. Die über solche Körper definierten Kurven sind auch von großen Bedeutung in der Kryptologie und Codierungstheorie - Ihre Untersuchung ist aber auch eines der “heißesten” Forschungsgebiete der modernen algebraischen Geometrie.

Wie auch eine Konferenz-Serie, und eine mathematische Zeitschrift trägt die Vorlesung den Titel ’Endliche Körper und ihre Anwendungen’. Selbstverständlich ist es unmöglich alles in einem Semester zu bearbeiten. Die Lehrveranstaltung wird eine Auswahl folgender Themen anbieten:

- Grundlagen der Theorie und praktische Aspekte der endlichen Körper
- Anwendungen in der Kryptographie und Codierungstheorie
- Aspekte der Implementierung
- Faktorisierungsalgorithmen und die Konstruktion irreduzibler Polynome gegebenen Grades

Die praktischen und rechnerischen Aspekte des Stoffes werden dabei betont.

Voraussetzungen: keine

Empfohlene Vorkenntnisse: Grundkentnisse von linearer Algebra und evtl. von Computerprogrammierung

Arbeitsaufwand: 180 Stunden

Der Arbeitsaufwand ergibt sich wie folgt: 14 Wochen zu je 4 SWS entsprechen in Summe 56 Stunden Anwesenheit. Für die Nachbereitung der Vorlesung und die Vor- und Nachbereitung der Übungen sind etwa 5 Stunden pro Woche, in Summe 70 Stunden, erforderlich. Etwa 24 Stunden sind für die Klausurvorbereitung vorgesehen.

2.20 148049: FoL Krypto - Forschungsorientierte Lehre Kryptographie

Nummer: 148049
Lehrform: Vorlesungen und Übungen
Verantwortlicher: Dr. Christopher Wolf
Dozent: Dr. Christopher Wolf
Sprache: Deutsch
SWS: 3
Leistungspunkte: 4
angeboten im:

Ziele: gemeinsames schreiben eines Artikels für eine Kryptographie-Konferenz

Inhalt: Kryptographie durchzieht unseren Alltag: Beim Handy-Gespräch, bei der Abhebung am Geldautomaten, bei der Bestellung im Internet. Jedes Mal schützt Kryptographie uns Kryptographie. Diese Vorlesung aus dem Bereich "Forschungsorientierte Lehre" greift ein aktuelles Thema aus der Kryptographie-Forschung auf und bereitet es so für Studierende auf, dass sie sich am aktuellen Forschungsprozess in der Kryptographie beteiligen können. Das genaue Thema wird in Absprache mit den Studierenden festgelegt.

Voraussetzungen: Voraussetzung sind ein abgeschlossener Bachelor in Mathematik, IT-Sicherheit oder verwandten Fächer.

Arbeitsaufwand: 120 Stunden

Der Arbeitsaufwand ergibt sich wie folgt: 14 Wochen zu je 3 SWS entsprechen in Summe 42 Stunden Anwesenheit. Für die Nachbereitung der Vorlesung und die Vor- und Nachbereitung der Übungen sind etwa 4 Stunden pro Woche, in Summe 56 Stunden, erforderlich. Etwa 22 Stunden sind für die Klausurvorbereitung vorgesehen.

2.21 141106: freie Veranstaltungswahl

Nummer: 141106
Lehrform: Beliebig
Verantwortlicher: Dekan
Dozent: Dozenten der RUB
Sprache: Deutsch
angeboten im: Wintersemester und Sommersemester

Ziele: Innerhalb des Moduls setzen die Studierenden entsprechend ihrer Interessen verschiedene Schwerpunkte. Dafür steht Ihnen das breite Angebot der ganzen Universität zur Verfügung. Sie beherrschen entsprechend ihrer Auswahl verschiedene Schlüsselqualifikationen.

Inhalt: Bei der Auswahl geeigneter Lehrveranstaltungen kann das Vorlesungsverzeichnis der Ruhr-Universität verwendet werden. Dies schließt Veranstaltungen aller Fakultäten, des Optionalbereichs und des Zentrums für Fremdsprachenausbildung (Veranstaltungen aus Bachelor- oder Masterstudiengängen) mit ein, also auch die Angebote der nichttechnischen Veranstaltungen . Im Rahmen einer Kooperationsvereinbarung mit der Fakultät für Elektrotechnik und Informationstechnik der TU Dortmund ist auch die Wahl dort angebotener Veranstaltungen möglich.

In der Fakultät wird speziell in diesem Bereich die Veranstaltung

> Methodik des wissenschaftlichen Publizierens

angeboten. Aus dem Bereich IT-Sicherheit gibt es das Angebot

> Aufbau eines Managementsystems für Informationssicherheit nach DIN ISO/IEC 27001

Voraussetzungen: entsprechend den Angaben zu der gewählten Veranstaltungen

Empfohlene Vorkenntnisse: entsprechend den Angaben zu der gewählten Veranstaltungen

Prüfung: mündlich, 30 Minuten

Beschreibung der Prüfungsleistung: Die Prüfung kann entsprechend der gewählten Veranstaltungen variieren.

2.22 148196: Implementierung kryptographischer Verfahren I

Nummer:	148196
Lehrform:	Vorlesungen und Übungen
Medienform:	Blackboard
	Tafelanschrieb
Verantwortlicher:	Prof. Dr.-Ing. Christof Paar
Dozent:	Dr.-Ing. David Oswald
Sprache:	Deutsch
SWS:	3
angeboten im:	

Ziele: Die Studierenden haben ein Verständnis für Methoden für die schnelle und sichere Realisierung asymmetrischer Krypto-Verfahren.

Inhalt: Zwei große Themenblöcke bilden schnelle Algorithmen für die effiziente Implementierung asymmetrischer Krypto-Verfahren. Zum einen werden verschiedene Exponentiationsalgorithmen behandelt, zum anderen Datenstrukturen und Software-Algorithmen für die schnelle Arithmetik mit großen Zahlen. Im dritten Themenblock werden Implementierungsangriffe behandelt, insbesondere Fehlerinjektionsattacken und differentielle Stromprofilanalysen (DPA). Teil der Vorlesung sind Programmierprojekte, in den die eingeführten Algorithmen umgesetzt werden.

Voraussetzungen: keine

Empfohlene Vorkenntnisse:

- Grundkenntnisse Kryptographie
- Grundkenntnisse der Programmiersprache C bzw. C++

Literatur:

[1] Hankerson, Darrel, Menezes, Alfred J., Vanstone, Scott "Guide to Elliptic Curve Cryptography", Springer, 2004
[2] Menezes, Alfred J., van Oorschot, Paul C., Vanstone, Scott A. "Handbook of Applied Cryptography", CRC Press, 1996

2.23 148150: Implementierung kryptographischer Verfahren II

Nummer: 148150
Lehrform: Vorlesung
Medienform: Blackboard
Tafelanschrieb
Verantwortlicher: Prof. Dr.-Ing. Christof Paar
Dozent: Prof. Dr.-Ing. Christof Paar
Sprache: Deutsch
SWS: 3
angeboten im:

Ziele: Verständnis für Methoden für die schnelle Realisierung symmetrischer und asymmetrischer Krypto-Verfahren.

Inhalt: Es werden fortgeschrittene Implementierungstechniken der modernen Kryptographie behandelt. Inhalte sind Techniken für die effiziennte und sichere Software-Realisierung von Blockchiffren, schnelle Algorithmen für Modulararithmetik sowie Hardware- und Software-Algorithmen für das Rechnen in endlichen Körpern. Teil der Vorlesung sind Programmierprojekte, in denen die eingeführten Algorithmen umgesetzt werden.

Voraussetzungen: keine

Empfohlene Vorkenntnisse: Grundkenntnisse der Programmiersprache C bzw. C++, Vorlesung Einführung in die Kryptographie I

Literatur:

[1] Menezes, Alfred J., van Oorschot, Paul C., Vanstone, Scott A. "Handbook of Applied Cryptography", CRC Press, 1996

2.24 144011: Industriepraktikum ITS

Nummer: 144011
Lehrform: Industriepraktikum
Verantwortlicher: Studiendekan ITS
Dozent: Mitarbeiter von Firmen
Sprache: Deutsch
angeboten im: Wintersemester und Sommersemester

Termine im Wintersemester:

Beginn: nach Absprache

Termine im Sommersemester:

Beginn: nach Absprache

Ziele: Nach der Praktikantentätigkeit haben die Studierenden u.a. Einblicke in die betrieblichen Arbeitsweisen und Sozialstrukturen gewonnen. Sie haben Konstruktions-, Entwurfs- und Entwicklungsmethoden, mit Verfahrens- und Betriebsaufgaben, sowie mit industriellen Produktionseinrichtungen kennengelernt. Kommunikative und soziale Schlüsselqualifikationen sind aus dem Umgang mit Vorgesetzten und Teammitgliedern bekannt.

Inhalt: Die berufsbezogene Tätigkeit in einem Industrieunternehmen, wobei unter Anleitung fachbezogene Probleme gehört werden, soll frühzeitig auf die Berufstätigkeit vorbereiten.

Voraussetzungen: siehe Prüfungsordnung

Empfohlene Vorkenntnisse: entsprechend des Tätigkeitsbereichs der gewählten Firma

Prüfung: Praktikum, studienbegleitend

2.25 148085: Information-Theoretic Secrecy

number: 148085
teaching methods: lecture with tutorials
media: rechnerbasierte Präsentation
Tafelanschrieb
responsible person: Prof. Dr.-Ing. Aydin Sezgin
lecturers: Prof. Dr.-Ing. Aydin Sezgin
M. Sc. Anas Chaaban
language: english
HWS: 3
angeboten im:

goals: The students understand the concepts of information theoretic measures to achieve secrecy. Equipped with tools and methods acquired during the lectures, new setups can be investigated.

content: The broadcast nature of wireless systems makes it more vulnerable to eavesdroppers to extract data from the received signals. The conventional way to achieve confidentiality is by using cryptographic encryption based on keys. The idea behind is that the eavesdropper is assumed to have limited time or computational resources. While this approach has both it advantages and disadvantages, the information theoretic approach can be regarded as a powerful alternative or as an additional level of protection to achieve security in wireless networks. A distinct feature of the information theoretic approach is that the eavesdropper is assumed to have unlimited time and resources available. Furthermore, this approach guarantees both reliability and security, which the other approach can not. In this lecture, we will cover the following aspects and setups

- Review: Entropy, Mutual Informaiton, Differential Entropy, Strongly Typical Sequences
- Confidentiality and Encryption
- Information Theoretic Security
- Basic Wyner Wiretap Channel
- Specific Multiuser Wiretap Channels
- common Randomness and Secret-Key Agreement
- Network Coding, Source Coding
- Cross-Layer Design

recommended knowledge:

- Communcations Engineering (since WS 2011/2012)
- Stochastic Signals
- Signals and Systems

Exam: mündlich, 30 Minuten

2.26 148025: Integrierte Digitalschaltungen

Nummer:	148025
Lehrform:	Vorlesungen und Übungen
Medienform:	rechnerbasierte Präsentation
	Tafelanschrieb
Verantwortlicher:	Prof. Dr.-Ing. Nils Pohl
Dozenten:	Prof. Dr.-Ing. Nils Pohl
	Dr.-Ing. Pierre Mayr
Sprache:	Deutsch
SWS:	4
angeboten im:	

Ziele: Das Ziel dieser Vorlesung besteht darin, den Studierenden den aktuellen Stand der Technik in CMOS-Digitalschaltungen zu vermitteln, welches Konzept- und Systemingenieure, sowie VLSI-Designer brauchen, um erfolgreich zu arbeiten. Dabei werden sowohl die theoretischen Grundlagen der Bauelemente, als auch der Schritt vom Bauelement über die Schaltung zum System gelehrt.

Inhalt: Diese Vorlesung führt ein in die wesentlichen Grundlagen für die Materie der integrierten Schaltungen und Systeme. Nach einer einführenden Behandlung der Grundlagen und Anwendungen der Mikroelektronik schreitet die Vorlesung über die Behandlung einer Reihe von Einzelheiten integrierter Halbleiterbauelemente zu den integrierten digitalen CMOS-Grundschaltungen voran. Zuletzt wendet sich die Vorlesung komplexeren Aufgabenstellungen beim Entwurf von integrierten Systemkomponenten und Systemen zu.

Empfohlene Vorkenntnisse:

- Elektronische Bauelemente
- Digitaltechnik
- Elektronische Schaltungen

2.27 148082: Convex Optimization in Signal Processing and Communications

number: 148082
teaching methods: lecture with tutorials
media: rechnerbasierte Präsentation
Tafelanschrieb
responsible person: Prof. Dr.-Ing. Aydin Sezgin
lecturers: Prof. Dr.-Ing. Aydin Sezgin
M. Sc. Anas Chaaban
language: english
HWS: 3
angeboten im:

goals: The students have a very good knowledge of basic concepts, the theory of convex optimization and algorithms and are able to extend and improve results in various directions resulting in conference and journal publications.

content: In this lecture, we will discuss the following topics:

- Introduction and Motivation
- Convex Sets
- Basic Concepts: Convex functions
- Properties of Convex Functions. Examples. Convex optimization problems.
- Linear Programming. Least-square problems. Quadratic programming. Optimal control problem.
- Geometric programming. Semi-definite programming
- Theory: Lagrangian. Dual optimization problem. Duality gap. Slater's condition. Duals of LP.
- Economics and Pricing Interpretation. Sensitivity analysis. Saddle points. Game Theory.
- Duality theory for minimax optimization
- Duals of QP. Controllability-observability duality. Dual of lp optimization. SDP relaxation.
- Complementary slackness condition. Karush-Kuhn-Tucker (KKT) Conditions. Waterlling example. Optics example.
- Interpretation of the KKT condition. Regularity condition for local optimality. Generalized inequalities.
- Algorithms: Descent methods. Newton's method. Equality Constrained Minimization. Infeasible-start Newton's Method.
- Interior-Point Method. Generalized Inequality.
- Applications in Signal Processing and Communication.

requirements: none

recommended knowledge:

- Mathematics I-IV
- Communications Engineering
- Signals and Systems
- Communications Engineering

literature:

[1] Boyd, S., Vandenberghe, L. "Convex Optimization", Cambridge University Press, 2004
[2] Bertsekas, Dimitri P. "Nonlinear Programming", Athena Scientific, 1999

2.28 148154: Kryptanalyse I

Nummer: 148154
Lehrform: Vorlesungen und Übungen
Medienform: Tafelanschrieb
Verantwortlicher: Prof. Dr. Alexander May
Dozent: Prof. Dr. Alexander May
Sprache: Deutsch
SWS: 3
angeboten im:

Termine im Sommersemester:

Beginn: Montag den 07.04.2014

Ziele: Erlernen der wichtigsten Algorithmen in der Kryptanalyse

Inhalt: Die Vorlesung Kryptanalyse I gibt einen Einblick in grundlegende Methoden der Kryptanalyse.

- Brute Force und Geburtstagsangriffe
- Time-Memory Tradeoffs
- Seitenkanalangriffe
- Gittertheorie und der LLL-Algorithmus
- Gitterbasierte Angriffe auf RSA
- Hidden Number Problem und Angriffe auf DSA
- Faktorisieren mit Faktorbasen
- Diskreter Logarithmus, Index-Calculus

Empfohlene Vorkenntnisse: Grundkenntnisse über Kryptographie

2.29 148153: Kryptanalyse II

Nummer: 148153
Lehrform: Vorlesungen und Übungen
Medienform: Tafelanschrieb
Verantwortlicher: Prof. Dr. Alexander May
Dozent: Prof. Dr. Alexander May
Sprache: Deutsch
SWS: 3
Leistungspunkte: 4
angeboten im:

Ziele: Erlernen der wichtigsten Algorithmen in der Kryptanalyse

Inhalt: Die Vorlesung Kryptanalyse II gibt einen Einblick in fortgeschrittene Methoden der Kryptanalyse.

- Pollards p-1 Methode
- Faktorisieren mit Elliptischen Kurven
- Pohlig-Hellman Algorithmus
- Cold-Boot Angriffe und Fehlerkorrektur von Schlüsseln
- Generalisiertes Geburtstagsproblem
- Lösen von polynomiellen Gleichungssystemen mit Gröbnerbasen
- Hilbert Basissatz und Buchberger Algorithmus
- Fourier und Hadamard Walsh Transformation

Empfohlene Vorkenntnisse: Inhalte der Vorlesung Kryptanalyse I

Arbeitsaufwand: 120 Stunden

Der Arbeitsaufwand ergibt sich wie folgt: 7 Wochen zu je 6 SWS entsprechen in Summe 42 Stunden Anwesenheit. Für die Nachbereitung der Vorlesung und die Vor- und Nachbereitung der Übungen sind etwa 6 Stunden pro Woche, in Summe 42 Stunden, erforderlich. Etwa 36 Stunden sind für die Klausurvorbereitung vorgesehen.

2.30 148203: Kryptographie auf programmierbarer Hardware

Nummer:	148203
Lehrform:	Vorlesungen und Übungen
Medienform:	rechnerbasierte Präsentation Tafelanschrieb
Verantwortlicher:	Prof. Dr.-Ing. Tim Güneysu
Dozent:	Prof. Dr.-Ing. Tim Güneysu
Sprache:	Deutsch
SWS:	4
Leistungspunkte:	5
angeboten im:	

Ziele: Die Studierenden kennen die Konzepte der praxisnahen Hardwareentwicklung mit abstrakten Hardwarebeschreibungssprachen (VHDL) und die Simulation von Hardwareschaltungen auf FPGAs. Sie beherrschen Standardtechniken der hardwarenahen Prozessorentwicklung und sind zur Implementierung von symmetrischen und asymmetrischen Kryptosystemen auf modernen FPGA-Systemen in der Lage.

Inhalt: Kryptographische Systeme stellen aufgrund ihrer Komplexität insbesondere an kleine Prozessoren und eingebettete Systeme hohe Anforderungen. In Kombination mit dem Anspruch von hohem Datendurchsatz bei geringsten Hardwarekosten ergeben sich hier für den Entwickler grundlegende Probleme, die in dieser Vorlesung beleuchtet werden sollen.

Die Vorlesung behandelt die interessantesten Aspekte, wie man aktuelle kryptographische Verfahren auf praxisnahen Hardwaresystemen implementiert. Dabei werden Kryptosysteme wie die Blockchiffre AES, die Hashfunktionen SHA-1 sowie asymmetrische Systeme RSA und ECC behandelt. Weiterhin werden auch spezielle Hardwareanforderungen wie beispielsweise der Erzeugung echten Zufalls (TRNG) sowie der Einsatz von Physically Unclonable Functions (PUF) besprochen.

Die effiziente Implementierung dieser Kryptosysteme, insbesondere in Bezug auf die Optimierung für Hochgeschwindigkeit, wird auf modernen FPGAs besprochen und in praktischen Übungen mit Hilfe der Hardwarebeschreibungssprache VHDL umgesetzt.

Vorlesungsbegleitend wird ein Blackboard-Kurs angeboten, der zusätzliche Inhalte sowie die praktischen Übungen bereithält.

Voraussetzungen: keine

Empfohlene Vorkenntnisse: Die Vorlesung baut auf Grundlagenstoff der folgenden Vorlesungen auf:

1) Grundlagen der Kryptographie und Datensicherheit

2) Computerarchitektur

3) Basiswissen Digitaltechnik

Empfehlenswert sind weiterhin Kenntnisse in folgenden Themenbereichen, die in der Vorlesung nur auszugsweise behandelt werden:

1) Schaltungsentwurf mit VHDL

2) Parallele Algorithmen und deren Programmierung

3) Implementierung kryptographischer Systeme

Arbeitsaufwand: 150 Stunden

Der Arbeitsaufwand berechnet sich wie folgt: 14 Wochen zu je 4 SWS entsprechen in Summe 56 Stunden Anwesenheit. Für die Übungsaufgaben mit integrierten kleinen Programmieraufgaben und der Nachbereitung der Vorlesung sind etwa 70 Stunden (ca. 5 Stunden / Woche) vorgesehen. Da bei regelmäßiger Bearbeitung der Übungen der gesamte Lehrstoff vertieft wird, sind für die Prüfungsvorbereitung lediglich 24 Stunden angesetzt.

2.31 148155: Kryptographie I

Nummer:	148155
Lehrform:	Vorlesungen und Übungen
Medienform:	Blackboard
	Tafelanschrieb
Verantwortlicher:	Prof. Dr. Alexander May
Dozent:	Prof. Dr. Alexander May
Sprache:	Deutsch
SWS:	4
angeboten im:	

Ziele: Lernziel dieser Veranstaltung ist ein Verständnis der wesentlichen mathematischen Methoden und Verfahren, auf denen moderne kryptographische Verfahren beruhen. Die Tiefe der Behandlung der Verfahren geht deutlich über das in den vorhergehenden Veranstaltungen vermittelte Maß hinaus. Als Ziel sollen die Teilnehmer die Fähigkeit zur Analyse und dem Design aktueller und zukünftiger kryptographischer Methoden erhalten. Zudem wird ein Bewusstsein für Methodik und Mächtigkeit verschiedenster Angriffsszenarien vermittelt.

Inhalt: Die Veranstaltung 'Kryptographie' behandelt die grundlegenden mathematischen Prinzipien moderner kryptographischer Verfahren. Die notwendigen mathematischen Grundkenntnisse der Algebra, Zahlentheorie, Komplexitätstheorie, Kombinatorik und Wahrscheinlichkeitsrechnung werden im Laufe der Vorlesung vertieft und ergänzt. In Abschnitt 1 der Veranstaltung werden wesentliche Bereiche der symmetrischen Kryptographie behandelt. Dieser Abschnitt beinhaltet insbesondere Block- und Strom- Algorithmen, sowie Hashfunktionen. Bei der Darstellung wird stets auf den mathematischen Hintergrund bzw. die präzise mathematische Formulierung eingegangen.

Empfohlene Vorkenntnisse:

- Modul Diskrete Mathematik
- Modul Einführung in die Kryptographie und Datensicherheit

Literatur:

[1] Koblitz, Neal "A Course in Number Theory and Cryptography", Springer, 1994
[2] Forster, Otto "Algorithmische Zahlentheorie", Vieweg, 1996
[3] Menezes, Alfred J., van Oorschot, Paul C., Vanstone, Scott A. "Handbook of Applied Cryptography", CRC Press, 1996
[4] Daemen, Joan, Rijmen, Vincent "The Design of Rijndael. AES.", Springer, 2001

2.32 148156: Kryptographie II

Nummer:	148156
Lehrform:	Vorlesungen und Übungen
Medienform:	Blackboard
	Tafelanschrieb
Verantwortlicher:	Prof. Dr. Alexander May
Dozent:	Prof. Dr. Alexander May
Sprache:	Deutsch
SWS:	4
angeboten im:	

Ziele: Lernziel dieser Veranstaltung ist ein Verständnis der wesentlichen mathematischen Methoden und Verfahren, auf denen moderne kryptographische Verfahren beruhen. Die Tiefe der Behandlung der Verfahren geht deutlich über das in den vorhergehenden Veranstaltungen vermittelte Maß hinaus. Als Ziel sollen die Teilnehmer die Fähigkeit zur Analyse und dem Design aktueller und zukünftiger kryptographischer Methoden erhalten. Zudem wird ein Bewusstsein für Methodik und Mächtigkeit verschiedenster Angriffsszenarien vermittelt.

Inhalt: Der Abschnitt 2 des Moduls befasst sich mit den wichtigsten asymmetrischen Verfahren. Ein wesentlicher Teil befasst sich mit dem RSA Algorithmus und den sich anschließenden mathematischen Fragestellungen, wie Primzahltests und Faktorisierung großer Zahlen. Weitere Gebiete sind Verfahren die auf den diskreten Logarithmen basisieren, sowie die Analyse gängiger Algorithmen für die digitale Signatur. Im abschließenden Abschnitt 3 werden verschiedene, auf den bisherigen Verfahren basierende kryptographische Protokolle (DH-Schlüsselaustausch, Zero Knowledge, Commitment Schemata) erörtert.

Empfohlene Vorkenntnisse:

- Modul Diskrete Mathematik
- Modul Einführung in die Kryptographie und Datensicherheit

Literatur:

[1] Shoup, Victor "A Computational Introduction to Number Theory and Algebra", Cambridge University Press, 2005
[2] Koblitz, Neal "A Course in Number Theory and Cryptography", Springer, 1994
[3] Forster, Otto "Algorithmische Zahlentheorie", Vieweg, 1996
[4] Buchmann, Johannes "Einführung in die Kryptographie", Springer, 2003

2.33 310002: Künstliche Neuronale Netze

Nummer:	310002
Lehrform:	Vorlesungen und Übungen
Medienform:	Folien rechnerbasierte Präsentation Tafelanschrieb
Verantwortlicher:	Priv.-Doz. Dr. Rolf P. Würtz
Dozenten:	Priv.-Doz. Dr. Rolf P. Würtz Wissenschaftliche Mitarbeiter
Sprache:	Deutsch
SWS:	2
angeboten im:	Wintersemester

Ziele: Die Studierenden beherrschen eine Reihe von Standardverfahren sowie neuerer Entwicklungen aus dem Bereich der künstlichen neuronalen Netze, die Funktionsweise und Anwendungsmöglichkeiten der behandelten Modelle sowie ihr Zusammenhang mit konventionellen mathematischen Methoden. Sie kennen Möglichkeiten und Grenzen der einzelnen Verfahren, sowohl für unüberwachtes als auch für überwachtes Lernen. Die Studierenden haben ein Verständnis der Technik künstlicher neuronaler Netzwerke zur Mustererkennung und Funktionsapproximation, sowie Stärken und Schwächen für praktische Anwendungen.

Inhalt:

- Problem Mustererkennung
- Problem Regression
- Kleinste Quadrate
- Lineare Diskriminanten
- Einschichtennetzwerke
- Limitierung von Einschichtennetzwerken
- Perzeptron Konvergenztheorem
- Mehrschichtennetzwerke
- Backpropagation
- Approximationstheorie für Zweischichtennetzwerke
- Perzeptron Konvergenztheorem
- RBF-Netzwerke
- Neuronale Karten

Voraussetzungen: keine

Empfohlene Vorkenntnisse:

- Lineare Algebra
- Differentialrechnung
- Wahrscheinlichkeitsrechnung

Prüfung: Projektarbeit, studienbegleitend

Literatur:

[1] C. M., Bishop "Pattern Recognition and Machine Learning", Springer Verlag, 2006

2.34 148018: Malware und Embedded Malware

Nummer: 148018
Lehrform: Vorlesungen und Übungen
Verantwortlicher: Prof. Dr. Thorsten Holz
Dozent: Prof. Dr. Thorsten Holz
Sprache: Deutsch
SWS: 3
angeboten im:

Ziele: Ziel dieser Veranstaltung ist ein tiefergehendes Verständnis von Schadsoftware und aktuellen Bedrohungen. Basierend auf diesen Vorkenntnissen werden dann einige Schutzmechanismen vorgestellt und deren Vor- und Nachteile diskutiert.

Inhalt: Im Rahmen der Vorlesung werden verschiedene Arten von moderner Schadsoftware behandelt. Dazu werden verschiedene Angriffsvektoren besprochen, einige Beispiele von Schadsoftware detailliert vorgestellt sowie ein Überblick über aktuelle Forschungsprojekte in diesem Bereich gegeben.

Diese Vorlesung wird nicht mehr angeboten.

Empfohlene Vorkenntnisse: Vorlesung "Programmanalyse" ist hilfreich, aber nicht notwendige Voraussetzung. Vorkenntnisse aus den Vorlesungen Netzsicherheit I/II und Systemsicherheit I/II sind hilfreich zum Verständnis der Themen. Erfahrung in systemnaher Programmierung und C sind ebenfalls hilfreich.

2.35 142020: Master-Praktikum Embedded Smartcard Microcontrollers

Nummer:	142020
Lehrform:	Praktikum
Medienform:	Folien
	rechnerbasierte Präsentation
Verantwortlicher:	Prof. Dr.-Ing. Christof Paar
Dozenten:	Prof. Dr.-Ing. Christof Paar
	M. Sc. Pawel Swierczynski
Sprache:	Deutsch
SWS:	3
angeboten im:	Wintersemester

Termine im Wintersemester:

Vorbesprechung: Mittwoch den 21.10.2015 ab 16:00 im ID 2/632
Praktikum Mittwochs: ab 16:15 bis 17:45 Uhr im ID 04/401

Ziele: Dieses Fortgeschrittenenpraktikum verfolgt im Wesentlichen die folgenden drei Lernziele: Erstens kennen die Teilnehmer des Praktikums eine zeitgemäße 8-Bit Mikrocontrollerarchitektur und deren Programmierung in Assembler. Zweitens wird der Umgang mit Smartcards, sowie Wissen über die entsprechenden Industriestandards beherrscht. Drittens sind die Implementierungsaspekte praktisch relevanter Blockchiffren (AES, 3DES, lightweight Chiffren etc.) bekannt. Dabei ist relevant, dass sowohl C, als auch Assembler die dominanten Programmiersprachen für Smartcards und viele andere eingebettete kryptographische Lösungen sind.

Über die technischen Ziele hinaus wird die Arbeitsfähigkeit in Gruppen erlernt, sowie Projektplanung und Zeitmanagement vermittelt.

Inhalt: In diesem Praktikum werden zwei Themengebiete erarbeitet. Zunächst erlernen die Teilnehmer des Praktikums Grundlagen über CISC und RISC Mikrocontroller. Bereits nach dem ersten Praktikumstermin sind die Studenten in der Lage kleine Programme in Assembler für die Atmel RISC AVR Architektur zu entwickeln. Während der folgenden Termine werden die Kenntnisse bezüglich der AVR Architektur vertieft. Darüber hinaus müssen die Praktikumsteilnehmer immer komplexere Programme als Hausaufgaben schreiben. Im zweiten Teil des Praktikums erlernen die Studenten den Umgang mit Smartcards und den zugehörigen Industriestandards. Der Standard ISO 7816 und die zugehörigen T=0/T=1 Übertragungsprotokolle werden vorgestellt. Die Studenten werden anschließend in Gruppen à drei Personen aufgeteilt. Jede Gruppe erhält eine Smartcard mit einem Atmel AVR Mikrocontroller, sowie einem Kartenschreib- bzw. -lesegerät. Jede Gruppe implementiert eine vorgegebene Blockchiffre (jährliche eine andere) in Assembler, und muss diese auf der Smartcard unter realistischen Bedingungen lauffähig bekommen. In den vergangenen drei Jahren wurde der AES,

IDEA und RC6 erfolgreich implementiert. Um die Motivation der Praktikumsteilnehmer zu erhöhen, werden die effizientesten Implementierungen mit Buchpreisen belohnt.

Voraussetzungen: keine

Empfohlene Vorkenntnisse: Grundkenntnisse Kryptographie, z.B. aus dem Modul Einführung in die Kryptographie und Datensicherheit.

Prüfung: Praktikum, studienbegleitend

2.36 142181: Master-Praktikum Entwurf integrierter Digitalschaltungen mit VHDL

Nummer:	142181
Lehrform:	Praktikum
Verantwortlicher:	Prof. Dr.-Ing. Michael Hübner
Dozenten:	Prof. Dr.-Ing. Michael Hübner M. Sc. Muhammed Soubhi Al Kadi
Sprache:	Deutsch
SWS:	3
Leistungspunkte:	3
angeboten im:	Wintersemester

Termine im Wintersemester:

Vorbesprechung: Donnerstag den 22.10.2015 ab 16:15 im ID 1/103
Praktikum Donnerstags: ab 14:00 bis 17:00 Uhr im ID 03/139

Ziele: Die Studierenden sind zum Entwurf integrierter Digitalschaltungen unter Verwendung der Hardware-Beschreibungssprache VHDL befähigt. Sie können mit modernen Entwurfswerkzeugen der Mikroelektronik umgehen.

Inhalt: Der Entwurf von VLSI-Schaltungen ist aufgrund der großen Zahl von Bauelementen nur zu beherrschen, wenn man Hardware-Beschreibungssprachen wie VHDL für den Entwurf einsetzt. Eine ganze Reihe von Eigenschaften macht VHDL für den Mikroelektronik-Entwurf so interessant. Dazu zählen: VHDL ist nicht technologiespezifisch, es ist das geeignete Medium zum Austausch zwischen Entwerfern untereinander und mit dem Chiphersteller, VHDL unterstützt Hierarchie und Top-down- und Bottom-up-Entwurfsmethoden, es unterstützt ferner Verhaltens-, Struktur- und Datenfluss-Beschreibung, es ist ein IEEE-Standard, Testmuster können mit derselben Sprache generiert werden u.a.m. Das Praktikum besteht aus einem Einführungs- und Übungsteil und einem Entwurfsprojekt, z.B. Komponenten aus einem Mikroprocessor oder dem Digitalteil eines UMTS-Transceivers. Dieses Projekt wird unter den Praktikumsgruppen aufgeteilt und die Einzelentwürfe am Ende des Semesters wieder zusammengeführt und getestet. Das Praktikum hat etwa folgenden Ablauf:

- Einführung in UNIX und VHDL
- einführendes Entwurfsbeispiel
- Übung 1 bis 3
- Projekt: Vorstellung der Spezifikation
- Projekt: Entwurf und Simulation

- Projekt: Synthese
- Projekt: Simulation der Gatterlaufzeiten
- Projekt: Verlustleistungsanalyse
- Projekt: Layout (Platzierung und Verdrahtung)

Voraussetzungen: keine

Empfohlene Vorkenntnisse: Wünschenswert sind Kenntnisse des Faches "Integrierte Digitalschaltungen"

Arbeitsaufwand: 90 Stunden

Der Arbeitsaufwand berechnet sich wie folgt: 12 Termine zu je 3 SWS entsprechen 36 Stunden Anwesenheit. Für die Vorbereitung werden 24 Stunden (2 Stunden je Praktikumstermin), für die Ausarbeitung der Dokumentation 24 Stunden (2 Stunden je Termin) und für die Zwischen- und Abschlussbesprechung inkl. Vorbereitung der Präsentationen 6 Stunden (jeweils 3 Stunden) veranschlagt.

Prüfung: Praktikum, studienbegleitend

Literatur:

[1] Reichardt, Jürgen, Schwarz, Bernd "VHDL-Synthese: Entwurf digitaler Schaltungen und Systeme", Oldenbourg, 2009

2.37 148151: Master-Praktikum FPGA

Nummer:	148151
Lehrform:	Praktikum
Medienform:	Blackboard
Verantwortlicher:	Prof. Dr.-Ing. Christof Paar
Dozenten:	Prof. Dr.-Ing. Christof Paar
	Dipl.-Inform. Ralf Zimmermann
Sprache:	Deutsch
SWS:	3
angeboten im:	

Ziele:

- Xilinx Toolchain zur Programmierung von FPGAs nutzen können
- Effiziente Test-Benches entwickeln können
- Fehler in fremdem VHDL Codes an Hand von Simulation finden und beheben können
- Algorithmen auf die Hardware von FPGAs optimieren können

Inhalt: Ziel dieses Praktikums ist die effiziente Implementierung von kryptografischen Verfahren auf Field Programmable Gate Arrays (FPGA). Bei dem Praktikum handelt es sich um ein Semesterprojekt, welches zum großen Teil zu Hause bearbeitet werden kann. Es wird zu Beginn des Praktikums einige Übungen bzw. Seminare in Form von Blockveranstaltungen geben, in welchen technische Einzelheiten des Projektes erläutert, Hilfestellungen gegeben sowie Übungsaufgaben verteilt werden.

Das Semesterprojekt besteht im Wesentlichen aus den folgenden Aufgabengebieten (vorläufiger Plan):

1. Verstehen der FPGA Architektur sowie VHDL Grundstrukturen
2. Erstellen eines einfachen VHDL Designs mit der Entwicklungsumgebung Xilinx ISE
3. Entwicklung weiterer einfacher Anwendungen auf dem FPGA Entwicklungs-Board
4. Testbench-Entwicklung zur (automatischen, begleitenden) Überprüfung des Designs
5. Programmierung und Optimierung eines kryptographischen Algorithmus in VHDL
6. Echtzeitbetrieb der entwickelten Module auf einem FPGA mit Hilfe eines Kommunikationsframeworks

Voraussetzungen: keine

Empfohlene Vorkenntnisse:

- Grundlegende VHDL-Kenntnisse
- Kenntnisse der Kryptografie

2.38 148067: Master-Praktikum Integrierte Informationssysteme

Nummer: 148067
Lehrform: Praktikum
Verantwortlicher: Prof. Dr.-Ing. York Tüchelmann
Dozent: Prof. Dr.-Ing. York Tüchelmann
Sprache: Deutsch
SWS: 3
angeboten im:

Termine im Wintersemester:

Praktikum: nach Absprache

Termine im Sommersemester:

Praktikum: nach Absprache

Ziele: Ziel des Praktikums 'Integrierte Ziel des Praktikums 'Integrierte Informationssysteme' ist es, grundlegende Kenntnisse aus den Bereichen Computernetze und IT-Sicherheit auf besondere Problemstellungen praktisch anzuwenden und in 14-tägigen Kurzprojekten zu vertiefen.

Inhalt: Inhaltlich ist das Praktikum in die Bereiche Auslegung von Computernetzen und ausgewählte Problemstellungen der IT-Sicherheit integriert. Der Inhalt des Praktikums wird jeweils mit dem Betreuer gemeinsam festgelegt. Zu jeder Praktikumsausarbeitung gehört ein detailliert erstelltes Protokoll sowie eine Präsentation der Ergebnisse.

Empfohlene Vorkenntnisse: Linux Grundkenntnisse, Basiswissen zu Simulationen, Kenntnisse zu Programmen wie Maple, Matlab oder Omnet++

2.39 142246: Master-Praktikum Programmanalyse

Nummer:	142246
Lehrform:	Praktikum
Verantwortlicher:	Prof. Dr. Thorsten Holz
Dozenten:	Prof. Dr. Thorsten Holz
	Dr.-Ing. Felix Schuster
Sprache:	Deutsch
SWS:	3
Leistungspunkte:	3
angeboten im:	Wintersemester

Termine im Wintersemester:

Vorbesprechung: Mittwoch den 19.10.2016 ab 12:00 bis 13:00 Uhr

Ziele: Die Studierenden haben ein tiefergehendes Verständnis der Funktionsweise aktueller Schadsoftware und kennen Techniken zur Analyse und zur Abwehr. Im Besonderen beherrschen die Teilnehmer entsprechende Techniken des Reverse-Engineerings unter Windows.

Inhalt: Das Praktikum ist eine Vertiefung der Inhalte, die in den Vorlesungen "Programmanalyse" und "Betriebssystemsicherheit" vorgestellt wurden. Die Teilnehmer sollen in Gruppen insgesamt sieben unterschiedliche Beispiele von realer Schadsoftware mit steigendem Schwierigkeitsgrad analysieren. Die zu analysierenden Schadsoftwarebeispiele werden jeweils zu einem eigenen Präsenztermin besprochen und entsprechende Analysemethoden vorgestellt. In vielen Fällen wird darüber hinaus Eigenrecherche und Autodidaktik zur Lösung der Aufgaben notwendig sein. Unter anderem werden die folgenden Themen behandelt:

- Entpacken/Entschleiern von Schadsoftware
- Statische und dynamische Analyse von Schadsoftware
- Entwicklung von Analyse-Tools
- Entwicklung von Kontrollstrukturen (C&C) für existierende Schadsoftware

Voraussetzungen: keine

Empfohlene Vorkenntnisse: Grundkenntnisse im Bereich des Reverse-Engineerings sind wünschenswert, z.B. durch erfolgreichen Abschluss der Vorlesung "Programmanalyse" und Erfahrung mit x86-Assembler. Erfahrung in systemnaher Programmierung unter Windows (Assembler, C) ist hilfreich.

Arbeitsaufwand: 90 Stunden

Der Arbeitsaufwand berechnet sich wie folgt: Die Anwesenheit beträgt 3 SWS * 14 Wochen, also 42 Stunden. Zum Schreiben des geforderten Quelltextes werden weitere ca. 48 Stunden benötigt.

Prüfung: Praktikum, studienbegleitend

2.40 142023: Master-Praktikum Seitenkanalangriffe

Nummer:	142023
Lehrform:	Praktikum
Verantwortlicher:	Priv.-Doz. Dr. Amir Moradi
Dozenten:	Priv.-Doz. Dr. Amir Moradi M. Sc. Falk Schellenberg
Sprache:	Deutsch
SWS:	3
angeboten im:	Wintersemester

Termine im Wintersemester:

Vorbesprechung: Mittwoch den 28.10.2015 ab 17:00 im ID 2/632

Ziele: Die Teilnehmer haben einen Einblick in praktische Seitenkanalangriffe und Gegenmaßnahmen.

Inhalt:

1. Introduction to Statistics + Introduction to Power Measurements (2 Sessions)
2. SPA + DPA (3 Sessions)
3. Countermeasures (masking, hiding) (1 Session)
4. First Main Project: Build your own SC-Resistant AES (2 Weeks)
5. Attacks on Countermeasures (1 Session)
6. Second Main Project: Attack the AES protected by other Teams (2 Weeks)
7. Final Session (1 Session)

Voraussetzungen: keine

Empfohlene Vorkenntnisse: Die Vorlesung "Implementierung kryptografischer Verfahren I" vermittelt nützliches Vorwissen, dieses wird jedoch nicht vorrausgesetzt.

Prüfung: Praktikum, studienbegleitend

2.41 142243: Master-Praktikum zur Hackertechnik

Nummer:	142243
Lehrform:	Praktikum
Medienform:	Folien
Verantwortlicher:	Prof. Dr. Jörg Schwenk
Dozenten:	Prof. Dr. Jörg Schwenk
	M. Sc. Marcus Niemietz
Sprache:	Deutsch
SWS:	3
Leistungspunkte:	3
angeboten im:	Wintersemester und Sommersemester

Termine im Wintersemester:

Beginn: Mittwoch den 21.10.2015 ab 16:15 im ID 03/445
Praktikum Mittwochs: ab 16:15 bis 17:45 Uhr im ID 2/168

Termine im Sommersemester:

Beginn: Mittwoch den 13.04.2016 ab 16:15 im ID 03/445
Praktikum Mittwochs: ab 16:15 bis 17:45 Uhr im ID 2/168

Ziele: Die teilnehmenden Studierenden haben ein weit gefächertes Wissen über die häufigsten Schwachstellen in Webapplikationen. Außerdem wissen sie, wie sie derartige Schwachstellen manuell finden können, ohne die Hilfe von automatisierten Webapplikations-Scannern in Anspruch zu nehmen. Darüber hinaus kennen die Studierenden entsprechende Schutzmaßnahmen sowie deren Wirksamkeit.

Inhalt: Webapplikationen sind im Zeitalter des Web-2.0 immer mehr zum Ziel von Angreifern geworden. So werden per SQL-Injektion fremde Datenbanken kompromittiert, per XSS-Schwachstelle Browsersessions gestohlen und per Cross-Site-Request-Forgery bekommt man von heute auf morgen unzählige neue Freunde in einem sozialen Netzwerk. Dazu wird nur ein einfacher Webbrowser benötigt.

Im Laufe dieses Praktikums sollen die Studierenden eine fiktive Online-Banking-Applikation angreifen und dabei die im Laufe der Veranstaltung erlernten Methoden und Techniken einsetzen. Dieses beinhaltet folgende Themengebiete:

- Cross Site Scripting (XSS)
- Cross Site Request Forgery (CSRF)
- Session Hijacking

- Session Fixation
- SQL Injection (SQLi)
- Local/Remote File Inclusion (LFI/RFI)
- Path Traversal
- Remote Code Execution (RCE)
- Logical Flaws
- Information Leakage
- Insufficient Authorization

Das Wissen der Studierenden wird zudem durch externe Experten aus der Industrie und IT-Sicherheits-Szene, die in Vorträgen über verschiedene Thematiken der Webapplikations-Sicherheit referieren werden, angereichert.

Voraussetzungen: keine

Empfohlene Vorkenntnisse:

- Ausgeprägtes Interesse an IT-Sicherheit, speziell am Thema "Websicherheit"
- Grundlegende Kenntnisse über TCP/IP und HTTP(S)
- Grundlegende Kenntnisse über HTML / JavaScript
- Grundkenntnisse in PHP oder einer ähnlichen Scriptsprache
- Inhalte der Vorlesungen Netzsicherheit 1 und 2

Arbeitsaufwand: 90 Stunden

Der Arbeitsaufwand berechnet sich wie folgt: 12 Wochen zu je 3h entsprechen 36 Stunden Anwesenheit. Für die Vorbereitung und Ausarbeitung der Protokolle werden jeweils 4,5 Stunden, insgesamt 54 Stunden veranschlagt.

Prüfung: Praktikum, studienbegleitend

2.42 148174: Master-Praktikum zur Programmierung sicherer Webservices

Nummer:	148174
Lehrform:	Praktikum
Verantwortlicher:	Prof. Dr. Jörg Schwenk
Dozenten:	Prof. Dr. Jörg Schwenk M. Sc. Christian Mainka Dr.-Ing. Christopher Meyer
Sprache:	Deutsch
SWS:	3
Leistungspunkte:	3
angeboten im:	

Ziele: Die Studierenden beherrschen die Bearbeitung von XML Dokumenten, die Erstellung von sicheren Web Services, Angriffe auf XML Signaturen und XML Encryption. Weiterhin sind sie sicher im Umgang mit diversen sicherheitsrelevanten Javaklassen.

Inhalt: Bearbeitung von XML Dokumenten

- Java Design Patterns
- Java XML Processing: DOM, SAX, StAX
- Projekt: Angriff auf XML Encryption
- Single Sign-On mit SAML

IBM Datapower XS40

- Umgang mit einem der verbreitesten XML-Security Gateways, Sicherung von Web Services anhand von diesem Gateway

Java Security

- JCA und JCE
- Java Security Manager
- Java Secure Coding Guidelines

Voraussetzungen: keine

Empfohlene Vorkenntnisse:

- Teilnahme an der Veranstaltung XML- und Webservices Security
- Kenntnisse über Web Services und WS-Security
- gute Programmiererfahrung in Java

Arbeitsaufwand: 90 Stunden

Der Arbeitsaufwand berechnet sich wie folgt: 12 Wochen zu je 3h entsprechen 36 Stunden Anwesenheit. Für die Vorbereitung und Ausarbeitung der Protokolle werden jeweils 4,5 Stunden, insgesamt 54 Stunden veranschlagt.

Prüfung: Praktikum, studienbegleitend

2.43 142241: Master-Projekt Netz- und Datensicherheit

Nummer:	142241
Lehrform:	Projekt
Verantwortlicher:	Prof. Dr. Jörg Schwenk
Dozenten:	Prof. Dr. Jörg Schwenk
	Dr.-Ing. Juraj Somorovsky
Sprache:	Deutsch
SWS:	3
Leistungspunkte:	3
angeboten im:	Wintersemester und Sommersemester

Termine im Wintersemester:

Vorbesprechung: nach Absprache

Termine im Sommersemester:

Vorbesprechung: nach Absprache

Ziele: Die Studierenden beherrschen den Umgang mit modernen Entwurfswerkzeugen für sichere Protokolle (z.B. auf Basis von Apache WS-security).

Inhalt: Das Praktikum ist ein nicht angeleitetes Fortgeschrittenenpraktikum. Es umfasst nur ein Thema, das die Studierenden selbständig bearbeiten. Je nach Thema wird Ihnen der entsprechende Betreuer zugeordnet.

Zur Klarstellung: Es ist nicht vorgesehen, dass sie verschiedene Themenblöcke nacheinander abarbeiten (wie es bei den Grundlagenpraktika der Fall ist), sondern sie werden nur ein Thema im Praktikum vertiefen. Die Bearbeitung kann je nach Vereinbarung mit dem Betreuer semesterbegleitend (z.B. 3h die Woche), oder zusammengefasst als Block (insgesamt ca. 40h) erfolgen; je nach Verfügbarkeit des Betreuers ist auch eine Bearbeitung in den Semesterferien grundsätzlich möglich.

Die Themenliste stellt nur Themenstichworte dar; die detaillierte Besprechung, und endgültige Definition des Themas erfolgt zusammen mit dem jeweiligen Fachbetreuer. Die Themen von Prof. Schwenk werden nach Vergabe von einem wissenschaftlichen Mitarbeiter betreut.

Bei Interesse an der Durchführung eines Praktikums wenden Sie Sich bitte an die Lehrstuhlmitarbeiter.

Voraussetzungen: keine

Empfohlene Vorkenntnisse:

- Grundkenntnisse Kryptographie und Computernetze

- Themenabhängig sind Programmierkenntnisse erforderlich

Arbeitsaufwand: 90 Stunden

Der Arbeitsaufwand berechnet sich wie folgt: Die Anwesenheit beträgt 3 SWS * 14 Wochen, also 42 Stunden. Zum Schreiben des geforderten Quelltextes werden weitere ca. 48 Stunden benötigt.

Prüfung: Projektarbeit, studienbegleitend

2.44 142184: Master Project Virtual Prototyping of Embedded Systems

number: 142184
teaching methods: project
responsible person: Prof. Dr.-Ing. Michael Hübner
lecturers: Prof. Dr.-Ing. Michael Hübner
Benedikt Janßen
M. Sc. Jones Yudi Mori Alves da Silva
M. Sc. Osvaldo Navarro
language: english
HWS: 3
angeboten im: winter term

dates in winter term:

Vorbesprechung: Mittwoch the 21.10.2015 from 16:15 in ID 1/103
Praktikum Montags: from 09:00 to 12:00 o'clock in ID 03/121

goals: The students master the design of "Embedded Systems" with the help of "Virtual Prototyping". Besides using tools for modeling, simulation and analysis of a virtual "Embedded System", the students will also be able to use SystemC, a hardware description language based on C++, and to model selected peripheral components. Furthermore they can implement applications in connection with the designed processor platform and a real-time operating system.

content: Within the project's scope, the methods of "Virtual Prototyping" are taught and reinforced with practical examples. The course's agenda is described below:

1.a – Introduction to Virtual Prototyping Basic concepts, systems, tools, languages, etc.

1.b – SystemC basics Cadence iSL SystemC course.

2.a – Fast processor models: OVP Introduction What are the Open Virtual Platforms, which are the advantages in using a virtual processor model and where to get it?

Fast models, cross-compilation and simulation The first part is to understand how to use the too by running different applications in some processor models.

- How to initialize the tool and organize a new project.
- What is cross-compilation? How to do this in OVP API?
- Executing and profiling a simulation.
- Analyse the same software in different processor models.

The second part shows the differences between processor descriptions using OVP API.

- Opening and analysing a processor model.
- How to modify the model?
- How to create a new cross-compiler for a custom model?
- Executing and profiling a simulation.

Multi-processor simulation In this part the aim is to understand a simple multicore system with shared memory.

- Analysing the example. How the communication among the processors is performed? How the software is partitioned/mapped to the processors?
- Simulation and analysis of the architecture.
- How to modify the software?
- How to add more processors?

2.b – Cadence Virtual System Platform Introduction
Basic examples on how to import models, connect them and simulate.

- Tool overview.
- Selected examples.
- Customizing and analysing the simulation.

Integrating SystemC and RTL models The objective is to create and simulate mixed systems (different design levels: SystemC+RTL integration).

- Abstraction
  design levels: What are Loosely-timed models, Approximately-timed models and Cycle-accurate models?
- How to combine this models using the VSP tool? Simple examples.
- What can be analysed in a mixed simulation?

Using fast OVP models The aim of this part is to import OVP models into VSP tool.

- How to create a SystemC wrapper for an OVP processor model?
- Importing and using OVP models in VSP.
- Comparison among OVP and RTL processor models in VSP.

3.a – Processor design: ArchC Introduction

- What is an Architecture Description Language (ADL)?
- ArchC framework overview.

[system-message] [system-message]system-message
WARNING/2 in <string>, line 83
Bullet list ends without a blank line; unexpected unindent. backrefs:
Analysis of a processor description, cross-compilation and simulation

- How to describe a processor model in ArchC?
- Cross-compilation and simulation.

[system-message] [system-message]system-message
WARNING/2 in <string>, line 88
Bullet list ends without a blank line; unexpected unindent. backrefs:
Exploring the design space of a processor model

- Modifying a custom processor model.
- How to generate a custom toolchain?
- Some examples.

MPSoCBench

- Multi-processor analysis framework based on ArchC and SystemC-TLM.
- Overview of the framework. How to configure and perform simulations?
- Understanding the different NoC types.
- Software partition and mapping on several processors.

3.b – Cache Modeling: Alpha-Sim + CACTI Cache Size Tradeoff
In this exercise you will simulate caches with different sizes to observe tradeoffs between this parameter, performance and energy consumption. The tasks for this exercise are as follows:

- Choose and simulate 10 L1 data cache configurations with different size in CACTI, plus the default configuration. Take notes about energy consumption and access time.
- Run sim-alpha with each cache configuration. Make sure that for each configuration you select the hit latency that corresponds better with the access time observed with CACTI in the previous step. Assume the hit latency is the ratio of cache access time to clock cycle, rounded up.
- Plot results:

[system-message] [system-message]system-message
WARNING/2 in <string>, line 118
Bullet list ends without a blank line; unexpected unindent. backrefs:
1 graph showing miss rate vs cache size 1 graph showing energy consumption vs cache size 1 graph showing execution time vs cache size

- Draw conclusions about results

[system-message] [system-message]system-message
WARNING/2 in <string>, line 123
Bullet list ends without a blank line; unexpected unindent. backrefs:
Associativity Tradeoff
The tasks for this exercise are as follows:

- Choose and simulate 5 L1 data cache configurations with different associativity in CACTI, plus the default configuration. Take notes about energy consumption and access time.
- Run sim-alpha with each cache configuration. Make sure that for each configuration you select the hit latency that corresponds better with the access time observed with CACTI in the previous step.
- Plot results:

1 graph showing miss rate vs associativity 1 graph showing energy consumption vs associativity 1 graph showing execution time vs associativity Draw conclusions about results
Block Size Tradeoff The tasks for this exercise are as follows:

- Choose and simulate 5 L1 data cache configurations with different block size in CACTI, plus the default configuration. Take notes about energy consumption and access time.
- Run sim-alpha with each cache configuration. Make sure that for each configuration you select the hit latency that corresponds better with the access time observed with CACTI in the previous step.
- Plot results:

[system-message] [system-message]system-message
WARNING/2 in <string>, line 146
Bullet list ends without a blank line; unexpected unindent. backrefs:
1 graph showing miss rate vs block size 1 graph showing energy consumption vs block size 1 graph showing execution time vs block size • Draw conclusions about results Overall Configuration Tasks

- 1Considering the results obtained choose three candidate configurations that you think will improve the performance and energy consumption of the default configuration.
- Explain reasoning behind each selection
- Simulate chosen candidates with CACTI and sim-alpha
- Draw conclusions. Which candidate is the best?
- If a victim buffer is enabled, how is the performance affected and why?

requirements: none

recommended knowledge: Basic programming knowledge in C/C++

Exam: Projektarbeit, continual assessment

2.45 143242: Master-Seminar Aktuelle Themen der IT-Sicherheit

Nummer:	143242
Lehrform:	Seminar
Medienform:	Folien
	Handouts
Verantwortlicher:	Prof. Dr. Thorsten Holz
Dozent:	Prof. Dr. Thorsten Holz
Sprache:	Deutsch
SWS:	3
angeboten im:	Wintersemester und Sommersemester

Termine im Wintersemester:

Vorbesprechung: Mittwoch den 21.10.2015 ab 10:15 bis 11:45 Uhr im ID 03/419

Termine im Sommersemester:

Vorbesprechung: Mittwoch den 13.04.2016 ab 10:15 bis 11:45 Uhr im ID 03/411

Ziele: Die Studierenden haben Methoden des forschungsnahen Lernens kennen gelernt und sind in der Lage eigenständig ein eng umgrenztes Themengebiet anhand von wissenschaftlichen Papern zu erarbeiten. Durch die Ausarbeitung haben die Studierenden das Schreiben eigener Texte und die Zusammenfassung komplexer Themengebiete geübt. Darüber hinaus können die Studierenden einen Vortrag zur Präsentation von wissenschaftlichen Ergebnissen mit Bezug zu der aktuellen Forschung halten.

Inhalt: In jedem Semester bietet der Lehrstuhl ein Seminar zum Thema "Aktuelle Themen der IT-Sicherheit" an, der Fokus liegt auf den Bereichen Malware-Analyse, Systemsicherheit, Sicherheit im Internet und ähnlichen Themen aus dem Bereich der systemnahen IT-Sicherheit. Dazu sollen die Studierenden selbständig ein komplexes Themengebiet bearbeiten und eine Ausarbeitung sowie einen Vortrag zu diesem Thema verfassen. Die Ausarbeitung hat einen Umfang von etwa 20-25 Seiten und der Vortrag soll etwa 20 Minuten dauern. Daran schließt sich eine Diskussion von 5 Minuten an.

Voraussetzungen: keine

Empfohlene Vorkenntnisse: Vorkenntnisse über Systemsicherheit und Netzsicherheit z.B. aus den Vorlesungen Systemsicherheit 1/2 und Netzsicherheit 1/2

Prüfung: Seminarbeitrag, studienbegleitend

2.46 148094: Master-Seminar Betriebssystemsicherheit und Trusted Computing

Nummer:	148094
Lehrform:	Seminar
Verantwortlicher:	Prof. Dr.-Ing. Ahmad-Reza Sadeghi
Dozenten:	Prof. Dr.-Ing. Ahmad-Reza Sadeghi
	Dr.-Ing. Marcel Winandy
Sprache:	Deutsch
SWS:	3
Leistungspunkte:	3
angeboten im:	

Ziele: Das thematische Ziel dieses Seminars ist die Sicherheits- und Datenschutzaspekte von IT-Systemen, die jeden Bürger betreffen, zu analysieren. Der Fokus dieser Veranstaltung liegt dabei auf der selbständigen Einarbeitung der Seminarteilnehmer in ein wissenschaftliches Thema, durch Literaturrecherche und dem Umgang mit der Primär-Literatur (Veröffentlichungen in Konferenzbänder und Zeitschriften). Aufbauend auf der Recherche soll eine Ausarbeitung und eine Präsentation zu dem jeweiligen Thema erstellt werden.

Inhalt: Verschiedene Themen werden unter den Teilnehmern zur Bearbeitung verteilt, sowie auf Literaturempfehlungen hingewiesen. Die Themen werden mit Bezug zu den aktuellen Projekten der Arbeitsgruppe nach Bedarf ausgewählt. Themenschwerpunkte sind derzeit Systemsicherheit, IT-Sicherheit im Gesundheitswesen und Usable Security. Jeder Studierende bearbeitet sein Thema selbständig im Laufe des Semesters. Die Unterstützung des Betreuers kann zu jeder Zeit in Anspruch genommen werden. Die Themen werden abschließend von den Studierenden in einem 20 bis 30-minütigen Vortrag präsentiert sowie in einer maximal 15 Seiten langen Ausarbeitung schriftlich zusammengefasst.

Empfohlene Vorkenntnisse: Je nach Themenbereich sind Vorkenntnisse im Bereich der Kryptografie und Systemsicherheit von Vorteil.

Arbeitsaufwand: 90 Stunden

Der Arbeitaufwand berechnet sich wie folgt: Das Seminar findet im wöchentlichen Turnus mit je drei Vorträagen zu je ca. 30 Minuten plus 15 Minuten Diskussion statt. Es besteht Anwesenheitspflicht. Dafür sind durchschnittlich (je nach Teilnehmerzahl) 8 Termine (24 Stunden) anzusetzen. Die Erarbeitung des Seminarthemas erfolgt eigenverantwortlich mit Unterstützung der betreuenden Mitarbeiter. Eine schriftliche Ausarbeitung von ca. 6 Seiten ist zu erstellen. Die Themen sind so gewählt, dasshierfür eine Arbeitszeit von 66 Stunden anzusetzen ist.

2.47 148072: Master-Seminar Computernetze und IT-Sicherheit

Nummer: 148072
Lehrform: Seminar
Verantwortlicher: Prof. Dr.-Ing. York Tüchelmann
Dozent: Prof. Dr.-Ing. York Tüchelmann
Sprache: Deutsch
SWS: 3
Leistungspunkte: 3
angeboten im:

Ziele: Lernziel ist die selbständige Auseinandersetzung mit einem Thema aus dem Bereich der Computernetze. Der Schwerpunkt liegt auf der Informationsakquisition und -darstellung, sowohl in schriftlicher Form als Ausarbeitung, oder auch im Rahmen einer rechnergestützten Präsentation. Zusätzlich soll die Fähigkeit der kritischen Auseinandersetzung mit einem Thema im Rahmen einer Fachdiskussion gefördert werden.

Inhalt: Die im Rahmen eines Semesters angebotenen Seminarthemen werden zu Beginn des Semesters bekannt gegeben und decken forschungsorientierte Themen auf dem Gebiet der Computernetze ab. Es wird darauf geachtet, dass die Themen einen engen Bezug zu aktuellen Problemstellungen, dem Stand der Technik und neuen Forschungserkentnissen der Informationstechnik haben. Einen Themenschwerpunkt bildet die Planung, Auslegung und Qualitätsbewertung von Netzwerken. Mögliche Themen umfassen sowohl die zum Betrieb eines Netzwerkes benötigte Hardware, als auch netzwerkfähige Software. Des weiteren werden Themen aus dem Gebiet der Netzwerksimulation angeboten. Ein zweiter Schwerpunkt ist die Absicherung von Computernetzen mit Hilfe passiver und aktiver Systeme wie Firewalls, Virenscanner oder Intrusion Detection Systeme (IDS).

Voraussetzungen: Vertieftes Wissen der Informationstechnik / Kommunikationstechnik

Empfohlene Vorkenntnisse: Inhalte aus den Vorlesungen “Computernetze I und II”.

Arbeitsaufwand: 90 Stunden

Die Arbeitsbelastung berechnet sich wie folgt: 14 Wochen zu je 3 SWS entsprechen in Summe 42 Stunden Anwesenheit. 48 Stunden werden für die Vorbereitung des eigenen Seminarvortrages angesetzt.

2.48 143021: Master-Seminar Embedded Security

Nummer:	143021
Lehrform:	Seminar
Medienform:	rechnerbasierte Präsentation
Verantwortlicher:	Prof. Dr.-Ing. Christof Paar
Dozent:	Prof. Dr.-Ing. Christof Paar
Sprache:	Deutsch
SWS:	3
Leistungspunkte:	3
angeboten im:	Wintersemester und Sommersemester

Termine im Wintersemester:

Vorbesprechung: Mittwoch den 21.10.2015 ab 14:00 im ID 2/632

Termine im Sommersemester:

Vorbesprechung: Mittwoch den 13.04.2016 ab 14:15 im ID 2/632

Ziele: Die Teilnehmer bescherrschen den akademischen Umgang mit technischer und wissenschaftlicher Literatur. Sie kennen Stand der Forschung.

Inhalt: Fortgeschrittene Themen der IT-Sicherheit werden von den Studierenden eigenständig erarbeitet. Das Spektrum möglicher Themen reicht von der Sicherheitsanalyse eingebetteter Systeme, über kryptografische Algorithmen für leistungsbeschränkte Geräte bis hin zu verschiedenen Aspekten der mobilen Sicherheit. Im Gegensatz zu dem Seminar im Bachelorstudiengang werden hier in der Regel Themen mit Bezug zu der aktuellen Forschung aufgegriffen.

Voraussetzungen: keine

Empfohlene Vorkenntnisse: Wie auch im letzten Semester werden die Seminarthemen des Lehrstuhls über die Webseite der zentralen Seminarvergabe vergeben. Dort befinden sich ebenfalls weitere Informationen zur Bedienung und zum Auswahlverfahren.

Der Anmeldezeitraum liegt in der Regel am Ende des vorangehenden Semesters. Der genaue Zeitraum wird über die RUB-Mailingliste its-announce bekannt gegeben.

Wichtig: Die Nutzung der zentralen Seminarvergabe ist Voraussetzung für die Vergabe eines Themas sowie für die erfolgreiche Teilnahme am Seminar.

Arbeitsaufwand: 90 Stunden

Der Arbeitsaufwand berechnet sich wie folgt: Die Seminarvorträge finden als Blockveranstaltung statt. Es besteht Anwesenheitspflicht. Dafür sind durchschnittlich (je nach Teilnehmerzahl) 20 Stunden anzusetzen. Die Erarbeitung des Seminarthemas findet eigenverantwortlich mit Unterstützung der betreuenden Mitarbeiter statt. Eine schriftliche Ausarbeitung von ca. 20 Seiten ist zu erstellen. Die Themen sind so gewählt, dass hierfür eine Arbeitszeit von 70 Stunden anzusetzen ist. Eine Klausurvorbereitung entfällt, da der Vortrag und die Ausarbeitung beurteilt werden.

Prüfung: Seminarbeitrag, studienbegleitend

2.49 148080: Master-Seminar Integrierte Schaltungen und Systeme für Mobilfunkanwendungen

Nummer: 148080
Lehrform: Seminar
Verantwortlicher: Prof. Dr.-Ing. Josef Hausner
Dozent: Prof. Dr.-Ing. Josef Hausner
Sprache: Deutsch
SWS: 3
angeboten im:

Ziele: Ein Ziel des Seminars liegt darin, dass die Studierenden den Umgang mit anspruchsvoller technischer und wissenschaftlicher Literatur erlernen. Gleichzeitig soll das Seminar bei den Teilnehmern das Fachwissen in dem speziellen Sachgebiet dieses Seminars vertiefen. Ein weiteres Ziel des Seminars besteht darin, dass die Studierenden lernen, den zu dem jeweiligen Thema erarbeiteten Stoff übersichtlich im Rahmen einer Präsentation zusammenzustellen und ansprechend vorzutragen.

Inhalt: In diesem Seminar werden ausgewählte Beispiele von Architekturen für Mobilfunksysteme, Mobilfunkstandards sowie integrierte Schaltungen aus dem Analogteil von Mobilfunkgeräten behandelt. Zu den Schaltungsbeispielen gehören Verstärker, Mischer, Oszillatoren und Analog-Digital-Umsetzer. Es werden aber auch aktuelle Techniken wie OFDM (Orthogonal Frequency Division Multiplexing) und CDMA (Code Division Multiple Access) und ausgewählte Anwendungen wie z.B. RFID und Positionsbestimmung für Mobilfunkgeräte vorgestellt. Die Seminarthemen werden von den Studierenden - mit Unterstützung des jeweils betreuenden wissenschaftlichen Mitarbeiters - eigenständig bearbeitet.

Voraussetzungen: keine

Empfohlene Vorkenntnisse:

- Kenntnisse der Kernvorlesungen des Studienganges
- Kenntnisse der Schaltungstechnik

2.50 148079: Master-Seminar Integrierte Schaltungen und Systeme für schnelle Datenübertragung im Internet

Nummer: 148079
Lehrform: Seminar
Verantwortlicher: Prof. Dr.-Ing. Josef Hausner
Dozent: Prof. Dr.-Ing. Josef Hausner
Sprache: Deutsch
SWS: 3
angeboten im:

Ziele: Ein Ziel des Seminars liegt darin, dass die Studierenden den Umgang mit anspruchsvoller technischer und wissenschaftlicher Literatur erlernen. Gleichzeitig soll das Seminar bei den Teilnehmern das Fachwissen in dem speziellen Sachgebiet dieses Seminars vertiefen. Ein weiteres Ziel des Seminars besteht darin, dass die Studierenden lernen, den zu dem jeweiligen Thema erarbeiteten Stoff übersichtlich im Rahmen einer Powerpoint-Präsentation zusammenszustellen und ansprechend vorzutragen.

Inhalt: In diesem Seminar werden ausgewählte Themen zu integrierten Schaltungen und Systemen für die schnelle Datenübermittlung im Internet behandelt, wobei der Schwerpunkt auf der Datenübertragung über optische Fasern für die Fernverbindung bzw. über verdrillte Leitungspaare und DSL-Techniken für die so genannte "letzte Meile" liegt. Die Seminarthemen werden von den Studierenden - mit Unterstützung des jeweils betreuenden wissenschaftlichen Mitarbeiters - eigenständig bearbeitet.

Voraussetzungen: keine

Empfohlene Vorkenntnisse:

- Kenntnisse der Kernvorlesungen des Studienganges
- Kenntnisse der Schaltungstechnik

2.51 148096: Master-Seminar Kryptanalyse und beweisbare Sicherheit

Nummer: 148096
Lehrform: Seminar
Verantwortlicher: Prof. Dr. Frederik Armknecht
Dozent: Prof. Dr. Frederik Armknecht
Sprache: Deutsch
SWS: 3
Leistungspunkte: 3
angeboten im:

Ziele: Dieses Seminar hat zwei Ziele. Zunächst sollen die Teilnehmer Einblicke in die unterschiedlichsten Aspekte der modernen Kryptographie erhalten, um sich unter anderem ein Bild davon machen zu können, wie vielfältig die Themenstellungen sind.

Weiterhin sollen die Studenten das Halten verständlicher Vorträge erüben. Im späteren Berufsleben kommt man desöfteren in die Situation, möglicherweise komplizierte Sachverhälte unterschiedlichsten Publika zu präsentieren. Deshalb liegt der Hauptaugenmerk darauf, dass die Inhalte der Arbeiten so präsentiert werden, dass die Mitstudierenden die wichtigsten Ideen mitnehmen können. Konsquenterweise wird kein Wert auf eine Ausarbeitung gelegt, sondern auf eine überzeugende Präsentation.

Inhalt: Während die Kryptographie in ihren Anfängen hauptsächlich den Austausch geheimer Daten im Fokus hatte, ist inzwischen das Aufgabengebiet extrem verbreitert worden. Akutelle Themenstellungen umfassend vielfältige Aspekte wie beweisbare Sicherheit, digitale Signaturen, Hashfunktionen, Zero-Knowledge Proofs, usw.

Aufgrund der enormen Vielfalt gibt es Aspekte der modernen Kryptographie, die in den Vorlesungen nicht angesprochen werden können. Deshalb sollen in diesem Seminar einzelne Arbeiten präsentiert werden, die aus unterschiedlichen Gründen wichtige oder interessante Beiträge zur modernen Kryptographie geleistet haben, die aber in den Vorlesungen kaum oder gar nicht zur Sprache kommen können. Diese Arbeiten berühren die unterschiedlichsten Themengebiete wie Kryptanalyse, beweisbare Sicherheit (bspw. interessante Beweistechniken), theoretische Fundamente, etc.

Hauptkriterium für die Auswahl der Arbeiten ist, dass diese nach unseren Einschätzungen aus den verschiedensten Gründen interessant sind. Die einzelnen Arbeiten können unter dem Punkt “Materialien” heruntergeladen werden.

Vorschläge für weitere Arbeiten sind ausdrücklich willkommen.

Voraussetzungen: keine

Empfohlene Vorkenntnisse: Je nach Themegebiet sind die notwendigen Vorkenntnisse unterschiedlich. Abhängig von der endgültigen Auswahl

der Themen und Teilnehmer soll dafür gesorgt werden, dass die wichtigsten Grundlagen während des Vortrages bereitgestellt werden. Allerdings sind Grundkenntnisse in Kryptographie unabdingbar.

Arbeitsaufwand: 90 Stunden

Der Arbeitsaufwand berechnet sich wie folgt: 14 Wochen zu je 3 SWS entsprechen in Summe 42 Stunden Anwesenheit. 48 Stunden werden für die Vorbereitung des eigenen Seminarvortrages angesetzt.

2.52 150537: Master-Seminar Kryptologie

Nummer:	150537
Lehrform:	Seminar
Medienform:	rechnerbasierte Präsentation
Verantwortlicher:	Prof. Dr. Alexander May
Dozent:	Prof. Dr. Alexander May
Sprache:	Deutsch
SWS:	3
Leistungspunkte:	3
angeboten im:	Sommersemester

Ziele: Die Studierenden können sich selbständig Originalarbeiten aus dem Bereich Kryptograhie aneigenen, und wissenschaftliche Ergebnisse präsentieren.

Inhalt: Aktuelle Forschungsarbeiten der wichtigsten Kryptographie-Konferenzen.

Voraussetzungen: keine

Empfohlene Vorkenntnisse: Inhalte des Moduls “Kryptographie”

Arbeitsaufwand: 90 Stunden

Der Arbeitsaufwand berechnet sich wie folgt: Die Seminarvorträge finden wöchentlich statt. Es besteht Anwesenheitspflicht. Dafür sind durchschnittlich (je nach Teilnehmerzahl) 20 Stunden anzusetzen. Die Erarbeitung des Seminarthemas findet eigenverantwortlich mit Unterstützung der betreuenden Mitarbeiter statt. Eine schriftliche Ausarbeitung von ca. 20 Seiten ist zu erstellen. Die Themen sind so gewählt, dass hierfür eine Arbeitszeit von 70 Stunden anzusetzen ist.

Prüfung: Seminarbeitrag, studienbegleitend

2.53 143240: Master-Seminar Netz- und Datensicherheit

Nummer:	143240
Lehrform:	Seminar
Medienform:	rechnerbasierte Präsentation
Verantwortlicher:	Prof. Dr. Jörg Schwenk
Dozenten:	Prof. Dr. Jörg Schwenk
	Dr.-Ing. Juraj Somorovsky
Sprache:	Deutsch
SWS:	3
Leistungspunkte:	3
angeboten im:	Wintersemester und Sommersemester

Termine im Wintersemester:

Vorbesprechung: Dienstag den 20.10.2015 ab 14:15 im ID 04/413
Seminar Dienstags: ab 14:15 bis 16:45 Uhr im ID 04/413

Termine im Sommersemester:

Vorbesprechung: Dienstag den 12.04.2016 ab 15:00 im ID 04/413
Seminar Dienstags: ab 15:00 bis 16:45 Uhr im ID 04/413

Ziele: Die Teilnehmer können mit technischer und wissenschaftlicher Literatur für Forschung und Entwicklung umgehen und die Ergebnisse wissenschaftlich präsentieren.

Inhalt: Ausgewählte Themen der IT-Sicherheit mit Bezug zur Netz- und Datensicherheit werden von den Studierenden eigenständig erarbeitet. Soweit möglich werden Themen in Anlehnung an eine gerade laufende Wahlpflichtveranstaltung gewählt, um didaktische Synergieeffekte zu nutzen.

Voraussetzungen: keine

Empfohlene Vorkenntnisse: Grundlegende Kenntnisse der Kryptographie und / oder Netzwerktechnik

Arbeitsaufwand: 90 Stunden

Der Arbeitsaufwand berechnet sich wie folgt: Die Seminarvorträge finden als Blockveranstaltung statt. Es besteht Anwesenheitspflicht. Dafür sind durchschnittlich (je nach Teilnehmerzahl) 20 Stunden anzusetzen. Die Erarbeitung des Seminarthemas findet eigenverantwortlich mit Unterstützung der betreuenden Mitarbeiter statt. Eine schriftliche Ausarbeitung von ca. 20 Seiten ist zu erstellen. Die Themen sind so gewählt, dass hierfür eine Arbeitszeit von 70 Stunden anzusetzen ist.

Prüfung: Seminarbeitrag, studienbegleitend

2.54 148050: Master-Seminar Post-Quantum Kryptographie

Nummer: 148050
Lehrform: Seminar
Verantwortlicher: Dr. Christopher Wolf
Dozent: Dr. Christopher Wolf
Sprache: Deutsch
SWS: 2
angeboten im:

Ziele: Die Teilnehmer können technische und wissenschafltiche Literatur finden, beschaffen verstehen, auswerten und einem Fachpublikum angemessen vortragen.

Inhalt: Da Quantenrechner mit einer genügend großen Anzahl von Quantenbits (q-Bits) sowohl effizient faktorisieren wie auch Logarithmen in endlichen Gruppen berechnen können, macht dies kryptographische Verfahren wie RSA und ECC unsicher. In diesem Seminar behandeln wir alternative kryptographische Primitive, die selbst in einer Post-Quantum-Welt verwendet werden können, um sichere Kommunikation zu ermöglichen. Im Seminar werden hierzu grundlegende Themen behandelt:

- Vergleich der Sicherheit verschiedener Verfahrensklassen
- D-Log und Faktorisieren mit dem Shor-Algorithmus
- Verfahren basierend auf
  a) Gittern
  b) Hash-Funktionen
  c) Multivariaten quadratischen Polynomen
  d) Codierungstheorie

Voraussetzungen: keine

Empfohlene Vorkenntnisse: Kryptographie I oder Kryptographie II

2.55 143022: Master-Seminar Smart Technologies for the Internet of Things

Nummer:	143022
Lehrform:	Seminar
Medienform:	rechnerbasierte Präsentation
Verantwortlicher:	Prof. Dr.-Ing. Michael Hübner
Dozenten:	Prof. Dr.-Ing. Michael Hübner
	Prof. Dr.-Ing. Diana Göhringer
	Prof. Dr. Thorsten Holz
	Prof. Dr.-Ing. Dorothea Kolossa
	Prof. Dr.-Ing. Rainer Martin
	Prof. Dr.-Ing. Aydin Sezgin
Sprache:	Deutsch
SWS:	3
Leistungspunkte:	3
angeboten im:	Sommersemester

Termine im Sommersemester:

Vorbesprechung: Dienstag den 19.04.2016 ab 16:15 im ID 03/455

Ziele: Im Seminar werden nicht nur fachliche Kenntnisse vermittelt, sondern auch die Grundsätze und Regeln der Präsentation von Vorträgen im Allgemeinen besprochen und eingeübt. Jeder Teilnehmer ist in der Lage, einen Vortrag so zu entwerfen und zu halten, dass er als wohlgegliedert, verständlich und interessant empfunden wird. Ferner können sie über fachliche Themen angemessen diskutieren.

Inhalt: Im Sommersemester 2016 werden in diesem Seminar lehrstuhlübergreifend Aspekte des modernen "Internet der Dinge" beleuchtet. Unter anderem befassen sich die Themen mit den Bereichen: Protokolle und Systemanforderungen bezüglich Geschwindigkeit, Stromverbrauch und Sicherheit. Die Themen werden am Vorbesprechungstermin an die Teilnehmer vergeben.

Jeder Studierende hält einen Vortrag über ein spezielles Thema aus dem gestellten Problemkreis und erstellt einen ca. 20-seitigen Bericht. Zu allen Vorträgen gehört eine eingehende Diskussion, an der sich alle Teilnehmer beteiligen.

Vorläufige Termine für die Vorträge (Anwesenheitspflicht):
N.N.

Voraussetzungen: keine

Empfohlene Vorkenntnisse: Grundlegende Kenntnisse in Elektrotechnik und IT-Sicherheit.

Arbeitsaufwand: 90 Stunden

Der Arbeitsaufwand berechnet sich wie folgt: Die Seminarvorträge finden als Blockveranstaltung statt. Es besteht Anwesenheitspflicht. Dafür sind durchschnittlich (je nach Teilnehmerzahl) 20 Stunden anzusetzen. Die Erarbeitung des Seminarthemas findet eigenverantwortlich mit Unterstützung der betreuenden Mitarbeiter statt. Eine schriftliche Ausarbeitung von ca. 20 Seiten ist zu erstellen. Die Themen sind so gewählt, dass hierfür eine Arbeitszeit von 70 Stunden anzusetzen ist. Eine Klausurvorbereitung entfällt, da der Vortrag und die Ausarbeitung beurteilt werden.

Prüfung: Seminarbeitrag, studienbegleitend

2.56 148211: Master-Seminar Softwaretechnik

Nummer: 148211
Lehrform: Seminar
Verantwortlicher: Prof. Dr.-Ing. Helmut Balzert
Dozent: Prof. Dr.-Ing. Helmut Balzert
Sprache: Deutsch
SWS: 3
angeboten im:

Ziele: Erlernen des akademischen Umgangs mit technischer und wissenschaftlicher Literatur. Erstellen von Seminarausarbeitungen, Präsentation von wissenschaftlichen Ergebnissen.

Inhalt: Themaschwerpunkt im SS15: "Vorbereitung auf das Berufsleben"

Unterthemen: 1. Gibt es das noch? Die richtige Kleidung zum richtigen Anlass? 2. Denglisch - cool oder un-cool? 3. Respekt - was ist das? 4. Stil - Was bedeutet das für Sie im Beruf? 5. Ohne Stil - cool, Mit Stil - Kultur? 6. Ethik im Beruf - meine Top 5 7. Kann mein Chef mein Freund sein? 8. "Alle per DU" im Betrieb - Toll oder nicht so Toll? 9. Mein Arbeitsplatz – Open Space (Großraumbüro) oder Think Tank (Einzelzimmer)? 10. Kann Lohn immer gerecht sein? 11. Sollte das Gehalt aller Mitarbeiter öffentlich sein? 12. Work-Life-Balance vs. Work-Life-Tides – was ist der richtige Weg? 13. Brauchen auch Informatiker einen hippokratischen Eid?

Wir bitten Interessenten, sich bis zum 15.03.2015 per E-Mail an softwaretechnik@rub.de mit folgenden Daten anzumelden: Name, Matrikelnummer, Studiengang, Semester. Für die individuelle Themenvergabe bitte Ergebnisse folgender Vorlesungen angeben (soweit abgeschlossen): Informatik 1, Informatik 2, Softwaretechnik 1, Softwaretechnik 2, Web Engineering, Nebenläufige Programmierung.

Der kostenlose E-Learning-Kurs "Wissenschaftliches Arbeiten" muss im Semester durchgearbeitet werden.

Voraussetzungen: keine

Empfohlene Vorkenntnisse: Informatik 1 und 2, Web-Engineering und/oder Softwaretechnik. Vorrang haben Meisterschüler im Masterstudium. Teilnehmerbegrenzung: max. 12 Teilnehmer

Prüfung: Seminarbeitrag, studienbegleitend

Literatur:

[1] Balzert, Helmut, Schröder, Marion, Schäfer, Christian "Wissenschaftliches Arbeiten, 2. Auflage", W3l, 2011

2.57 310509: Nebenläufige Programmierung

Nummer:	310509
Lehrform:	Vorlesungen und Übungen
Medienform:	e-learning rechnerbasierte Präsentation
Verantwortlicher:	Dr.-Ing. Doga Arinir
Dozent:	Dr.-Ing. Doga Arinir
Sprache:	Deutsch
SWS:	3
angeboten im:	Sommersemester

Ziele: Die Studierenden haben grundlegende Fähigkeiten und Techniken, um nebenläufige Programme sicher entwickeln zu können. Es kennen softwaretechnische Entwurfsmuster, welche bekannte Probleme bei nebenläufigen Programmen wie zum Beispiel die Verklemmung vermeiden lassen. Die Teilnehmer können

- die Performanz von Programmen durch den Einsatz der nebenläufigen Programmierung verbessern,
- bestehende Programme analysieren und mögliche Fehler erkennen und
- die Sprachmerkmale und Schnittstellen von JAVA für die nebenläufige Programmierung sicher anwenden.

Inhalt: Moderne Hardware-Architekturen lassen sich nur durch den Einsatz nebenläufiger Programme richtig ausnutzen. Die nebenläufige Programmierung garantiert bei richtiger Anwendung eine optimale Auslastung der Hardware. Jedoch sind mit einem sorglosen Einsatz dieser Technik auch viele Risiken verbunden. Die Veranstaltung stellt Vorteile und Probleme nebenläufiger Programme dar und zeigt, wie sich die Performanz von Programmen verbessern lässt:

- Nebenläufigkeit: Schnelleinstieg
  - Anwendungen vs. Prozesse
  - Programme und ihre Ausführung
  - Vorteile & Probleme von nebenläufigen Programmen
    - Verbesserung der Performanz
    - Synchronisation
    - Realisierung kritischer Abschnitte
    - Monitore
    - Lebendigkeit
    - Verklemmungen
- Threads in Java
- UML-Modellierung von Nebenläufigkeit

- Neues zur Nebenläufigkeit in Java 5 und Java 6
- Realisierung von Nebenläufigkeit
- Fortgeschrittene Java-Konzepte für Nebenläufigkeit

Voraussetzungen: keine

Empfohlene Vorkenntnisse: Inhalte der Vorlesungen:

- Informatik 1
- Informatik 2
- Web-Engineering
- Softwaretechnik 1

Literatur:

[1] Arinir, Doga, Ziesche, Peter "Java: Nebenläufige und verteilte Programmierung, 2. Auflage", W3l, 2010

2.58 148084: Network Information Theory

number:	148084
teaching methods:	lecture with tutorials
media:	Blackboard
	e-learning
	Folien
	Internet
	rechnerbasierte Präsentation
	Tafelanschrieb
responsible person:	Prof. Dr.-Ing. Aydin Sezgin
lecturers:	Prof. Dr.-Ing. Aydin Sezgin
	M. Sc. Anas Chaaban
language:	english
HWS:	3
angeboten im:	

goals: Time and Location: Lecture hours are Mondays from 4-6pm in ID 2/232.

The students have a very good knowledge of tools and concepts from network information theory and are able to extend and improve results in various directions resulting in conference and journal publications.

The goal of the course is to provide a survey of the state-of-the-art on topics like interference management, distributed storage repair, network coding etc. The course might be of relevance to graduate students interested in communication and signal processing. The focus in this course is on theoretical aspects of multi-user networks. The presentation style of the lectures is rather informal, favoring broad intuition over mathematical rigor. The technical (and finer) details have to be investigated by the students within the project part of the course.

content: What is really the best way to operate communication networks? What are the fundamenal limits to communicate over such networks? Those are the questions adressed in this course on network information theory, which provides strategic guidance and guidlines for the design of communication networks.

(Network) information theory provides fundamental bounds on the performance of communication systems. Thus, those bounds serve perfectly as fundamental benchmarks, which allows a comparison between different communication system designs. This also gives design guidlines for the system engineer, who has to invent transeiver strategies to achieve those bounds. The mathematical theory of communication goes back to C.E.Shannon. In 1948, Shannon published his landmark paper, which fundamentally changed the way how a system was designed. Interestingly, it took about 50 years with the invention of the so called turbo codes until it was shown that those bounds are indeed achieveable and thus very relevant for the practice. Before the rise of turbo codes, information theory was regarded more or less

as esoteric. Even more interesting is the fact, that the first capacity achieving codes (low density parity check codes, LDPC) were invented already in the 1960s by Gallager. Unfortunately, back then there was now way (computers were not so powerful yet) to numerically evaluate the LDPC codes. In retrospect, it took less than 20 years to devise strategies to achieve those fundamtenal bounds. Given the signal processing advances, the capabilities of computers, and some ingenuity by engineers, encourages to postulate that the time gap between characterizing the bounds and achieving it is going to take significanlty less time. Thus it is more importan than ever to characterize those bounds for communication systems, which provides intuition on how to design a system and also set the design goals.

The courses briefly reviews the information theoretic results obtained from point to point communication. The results are then extended in great details to multi-user networks as those are of high importance in todays information era, especially given the rise of high data rate requirements by mobile devices. The goal of this course is thus to understand and derive the fundamental limits of multi-user communication systems which give guidelines for system engineers to design future networks.

Course Information

- Information Theory Basics: Entropy, Mutual Information, AEP
- Single-User Source and Channel Coding
- Single-User Gaussian Channels: AWGN, Parallel, Fading
- MIMO Channels
- Multiple-Access Channel
- Slepian-Wolf & MAC with Correlated Sources
- Broadcast Channel
- MAC-Broadcast Duality & MIMO Broadcast Channel
- Interference Channel
- Relay Channel
- Rate Distortion Theory
- Sensor Networks
- Ad-Hoc Network Capacity
- Network Coding
- Feedback
- Multiple description
- Side information
- Channel with state

requirements: none

recommended knowledge:

- Signals and Systems
- Communcations Engineering
- Mathematics I-IV
- Stochastic Signals I+II

literature:

[1] Cover, T., Thomas, J. "Elements of Information Theory", Wiley & Sons, 2006
[2] El-Gamal, A., Kim, Y.-H. "Network Information Theory", Cambridge University Press, 2011

2.59 141028: Physical Attacks and Countermeasures

number: 141028
teaching methods: lecture with tutorials
responsible person: Priv.-Doz. Dr. Amir Moradi
lecturer: Priv.-Doz. Dr. Amir Moradi
language: english
HWS: 4
Leistungspunkte: 5
angeboten im: summer term

dates in summer term:

Beginn: Montag the 11.04.2016
Vorlesung Montags: from 14:15 to 15:45 o'clock in ID 03/471
Übung Montags: from 16:00 to 16:45 o'clock in ID 03/471
Praxisübung Montags: from 17:00 to 17:45 o'clock in ID 2/632

goals: The students

- have Awareness of danger of cryptanalysis attacks targeting implementation of cryptographic algorithms
- understand the kinds of physical attacks, their prerequisites, and their required conditions to work
- know the countermeasure schemes to make a design protected against each physical attack

content: The modern cryptographic algorithms provide a reasonable level of security against the known mathematical and analytical cryptanalysis attacks. At the end the cryptographic algorithms are realized to be used in a security-enabled application. This realization is done by implementing the desired cryptographic algorithm using some program codes (in software) or using logic elements (in hardware). Physical access of the users to the cryptographic devices (e.g., a smartcard used for payment, a contactless card used for authentication, and smartphones) where a secret key is embedded brought a new form of attacks called physical attacks. This kind of attacks aims at extracting the secret key used by the cryptographic algorithm from the target implementation. Breaking a system by means of a physical attack does not infer to the weakness of the algorithm, but of the implementation. Therefore, considering such kinds of attack when designing a cryptographic device is a must. The goal of this lecture is to give an overview about the known physical attacks and most considerably the schemes developed to counter such a kind of attacks. In the first part of the lecture different kinds of physical attacks are introduced, while we focus later on countermeasures and the methods to make implementations resistant against the known physical attacks.

requirements: none

recommended knowledge: basic knowledge of data security and cryptography, a programming language (C++), computer architecture

Arbeitsaufwand: 150 Stunden

Der Arbeitsaufwand ergibt sich wie folgt: 14 Wochen zu je 4 SWS entsprechen in Summe 56 Stunden Anwesenheit. Für die Nachbereitung der Vorlesung und die Vor- und Nachbereitung der Übungen sind etwa 4 Stunden pro Woche, in Summe 56 Stunden, erforderlich. Etwa 38 Stunden sind für die Prüfungsvorbereitung vorgesehen.

Exam: mündlich, 30 Minuten

2.60 141241: Programmanalyse

Nummer:	141241
Lehrform:	Vorlesungen und Übungen
Medienform:	e-learning rechnerbasierte Präsentation
Verantwortlicher:	Prof. Dr. Thorsten Holz
Dozenten:	Dr.-Ing. Carsten Willems Dipl.-Inform. Behrad Garmany Dipl.-Biol. Robert Gawlik
Sprache:	Deutsch
SWS:	4
angeboten im:	Sommersemester

Termine im Sommersemester:

Beginn: Dienstag den 12.04.2016
Vorlesung Dienstags: ab 14:15 bis 15:45 Uhr im ID 04/471
Vorlesung Dienstags: ab 14:15 bis 15:45 Uhr im ID 04/459
Übung Donnerstags: ab 12:15 bis 13:45 Uhr im ID 04/471
Übung Donnerstags: ab 12:15 bis 13:45 Uhr im ID 04/459

Ziele: Die Studierenden kennen verschiedene Konzepte, Techniken und Tools aus dem Bereich der Programmanalyse. Dies beinhaltet den Überblick über verschiedene Konzepte aus dem Bereich Reverse Engineering sowie Malware-Analyse. Die Studierenden haben grundlegendes Verständnis von sowohl statischen als auch dynamischen Methoden zur Analyse eines gegebenen Programms.

Inhalt: In der Vorlesung werden unter anderem die folgenden Themen und Techniken aus dem Bereich der Programmanalyse behandelt:

- Statische und dynamische Analyse von Programmen
- Analyse von Kontroll- und Datenfluss
- Symbolische Ausführung
- Taint Tracking
- Virtual Machine Introspektion
- Binary Instrumentation
- Program Slicing
- Überblick zu existierenden Analysetools

Daneben wird im ersten Teil der Vorlesung eine detaillierte Einführung in x86 Assembler gegeben sowie die grundlegenden Techniken aus dem Themenbereich Reverse Engineering vorgestellt. Begleitet wird die Vorlesung von Übungen, in denen die vorgestellten Konzepte und Techniken praktisch ausprobiert werden sollen.

Voraussetzungen: keine

Empfohlene Vorkenntnisse: Erfahrung in systemnaher Programmierung, Assembler sowie Programmieren in C sind hilfreich für das Verständnis der vermittelten Themen. Vorkenntnisse aus den Vorlesungen Eingebettete Prozessoren (insbesondere Assembler-Programmierung) sowie Systemsicherheit/Betriebssystemsicherheit sind hilfreich aber nicht notwendig zum Verständnis der Themen.

Prüfung: schriftlich, 120 Minuten

2.61 150318: Quantenalgorithmen

Nummer: 150318
Lehrform: Vorlesungen und Übungen
Verantwortlicher: Prof. Dr. Alexander May
Dozent: Prof. Dr. Alexander May
Sprache: Deutsch
SWS: 3
angeboten im: Sommersemester

Ziele: Die Studierenden beherrschen die Grundlagen für Quantenalgorithmen.

Inhalt: Die Vorlesung gibt einen Einblick in die Konstruktion von Algorithmen für Quantenrechner.

- Themenübersicht:
  - Quantenbits und Quantengatter
  - Separabilität und Verschränkung
  - Teleportation
  - Quantenschlüsselaustausch
  - Quantenkomplexität
  - Simons Problem
  - Shors Faktorisierungsalgorithmus
  - Grovers Suchalgorithmus

Voraussetzungen: keine

Empfohlene Vorkenntnisse: Lineare Algebra, Algorithmen

Prüfung: mündlich, 30 Minuten

2.62 148115: Schutz kritischer Infrastrukturen und Informationssicherheit

Nummer: 148115
Lehrform: Vorlesungen und Übungen
Medienform: rechnerbasierte Präsentation
Verantwortlicher: Prof. Dr.-Ing. Christof Paar
Dozent: Dipl.-Ing. Dirk Schadt
Sprache: Deutsch
SWS: 3
angeboten im:

Ziele: Primäre Lernziele der Veranstaltung sind die Vermittlung grundlegender Kenntnisse über kritische Infrastrukturen, insbesondere jedoch deren Abhängigkeiten untereinander, und die Einflüsse der Informations- und Kommunikationstechnik als Infrastruktur an und für sich, und als wesentliche Komponente anderer Infrastrukturen.

Inhalt: Kritische Infrastrukturen (KRITIS) sind die vitalen Elemente unserer gesellschaftlichen Ordnung und bedürfen besonderer Aufmerksamkeit. Die Vorlesung betrachtet Historie und Definition von KRITIS, unterschiedliche Sichtweisen wie Sektoren und Prozesse, und gegenseitigen Abhängigkeiten. Dazu vermittelt sie Beurteilungsansätze zu Bedrohungen, Risiken, Kritikalität, gegenseitigen Abhängigkeiten u.ä., sowie Verfahren zu Modellierung, Simulation und Informationsaustausch wie z.B. Frühwarnung, Notfallplanung, angemessene Informationsverteilung, und Wiederherstellung zur Verbesserung der Robustheit und zum Erhalt der Funktionalität. Darüber hinaus werden auch interdisziplinäre Randgebiete beleuchtet und Verbindungen der KRITIS-Problematik zu anderen Fachgebieten aufgezeigt. Vorschläge zur thematischen Zusammenarbeit, Ausbildungsbedarf und Literaturquellen runden die Vorlesung ab.

Voraussetzungen: Keine

Empfohlene Vorkenntnisse: Keine

2.63 148108: Signale und Systeme

Nummer:	148108
Lehrform:	Vorlesungen und Übungen
Medienform:	Folien rechnerbasierte Präsentation Tafelanschrieb
Verantwortlicher:	Prof. Dr.-Ing. Ilona Rolfes
Dozenten:	Prof. Dr.-Ing. Ilona Rolfes wiss. Mitarbeiter
Sprache:	Deutsch
SWS:	4
angeboten im:	

Ziele: Die Systemtheorie, d.h. eine weitgehend allgemeine mathematische Beschreibung der Signaldarstellung, der Signalverarbeitung und -übertragung in Systemen und die entsprechende Beschreibung der Systeme selbst, bilden die wesentlichen Lernziele. Die Studierenden kennen die grundlegenden Methoden zur Beschreibung und Analyse von analogen und digitalen Systemen, sowie den Aufbau von grundlegenden Schaltungen zur analogen und digitalen Signalverarbeitung. Sie sind in der Lage, alle Aufgaben im Zusammenhang mit der Analyse und der Interpretation von linearen und zeitinvarianten analogen und zeitdiskreten (digitalen) Systemen zu verstehen und zu lösen.

Inhalt: Bevor ein Ingenieur ein System entwickeln kann, das beispielsweise dem Austausch von Informationen über größere Entfernungen dienen soll, muss geklärt werden, mit welcher Art von Signalen ein solcher Austausch überhaupt möglich ist. Mathematische Modelle für die Signale und für die die Signale verarbeitenden Systeme werden in der Vorlesung vermittelt. Konkret werden behandelt:

- **Einführung**
  - Grundbegriffe zu Signalen und Systemen: Linearität und Zeitinvarianz: LTI-Systeme, Kausalität und Stabilität.
- **Kontinuierliche und diskrete Signale**
  - Reelle/komplexe, symmetrische, periodische, begrenzte und beschränkte Signale
  - Diskontinuierliche und schwingungsförmige Elementarsignale und deren Eigenschaften
  - Klassifikation von Signalen.
- **Diskrete LTI-Systeme**
  - Bestimmung des Übertragungsverhaltens mittels z-Transformation
  - Übertragungsverhalten im Zeitbereich: Diskrete Faltung

  - Übertragungsfunktion, Impulsantwort, Grundstrukturen
  - Eigenschaften: Stabilität, Eigenfunktionen, IIR- und FIR-Systeme
  - Anfangswertprobleme.

- **Die z-Transformation, zeitdiskrete und disrete Fourier-Transformation**
  - Definition und Existenz
  - Eigenschaften und Rechenregeln
  - Die Rücktransformation.

- **Kontinuierliche LTI-Systeme**
  - Verallgemeinerte Funktionen: Distributionen, Dirac-Impuls
  - Bestimmung des Übertragungsverhaltens mittels Laplace-Transformation
  - Übertragungsverhalten im Zeitbereich: Kontinuierliche Faltung
  - Übertragungsfunktion, Impulsantwort, Grundstrukturen
  - Eigenschaften: Stabilität, Eigenfunktionen
  - Zustandsraumdarstellung.

- **Die Laplace und Fourier-Transformation, Fourier-Reihe**
  - Definition und Existenz
  - Eigenschaften und Rechenregeln
  - Die Rücktransformation
  - Zusammenhang der Transformationen

- **Spektrale Beschreibung von LTI-Systemen**
  - Übertragungsfunktion und Frequenzgang
  - Filter und Allpässe

- **Diskretisierte kontinuierliche Signale**
  - Signalabtastung und Signalrekonstruktion

Voraussetzungen: keine

Empfohlene Vorkenntnisse:

- Mathematik A + B
- Grundlagen der Informationstechnik
- Grundlagen der Elektrotechnik und Elektronik (ITS) bzw. Grundlagen der Elektrotechnik (ETuIT)

Literatur:

[1] Bossert, Martin, Frey, Thomas "Signal- und Systemtheorie", Vieweg Verlag, 2004

2.64 148201: Softwaretechnik I

Nummer: 148201
Lehrform: Vorlesungen und Übungen
Medienform: rechnerbasierte Präsentation
Verantwortlicher: Prof. Dr.-Ing. Helmut Balzert
Dozent: Prof. Dr.-Ing. Helmut Balzert
Sprache: Deutsch
SWS: 3
angeboten im:

Ziele: Software-Entwicklung findet in Phasen statt. Ausgehend von den Anforderungen des Auftraggebers werden die Studierenden dazu befähigt über die Phasen Planung, Definition, Entwurf und Implementierung ein Software-Systems zu entwickeln, das nach der Abnahme gewartet, gepflegt und weiterentwickelt wird.

Inhalt: Wissenschaftsdisziplin:

- Einführung in die Software-Technik

Basistechniken:

- Prinzipien
- Methoden
- Werkzeuge

Basiskonzepte:

- Statik
  - Funktionalität
  - Funktionsstrukturen
  - Daten
  - Datenstrukturen
- Dynamik
  - Kontrollstrukturen
  - Geschäftsprozesse & Use Cases
  - Zustandsautomaten
  - Petrinetze
  - Szenarien
- Logik
  - Formale Logik

  - Constraints und OCL
  - Entscheidungstabellen
  - Regeln

Requirements Engineering:

- Anforderungen ermitteln und spezifizieren
- Schätzen des Aufwands
- Lastenheft und Pflichtenheft

Voraussetzungen: keine

Empfohlene Vorkenntnisse: Kenntnisse der Prinzipien, Methoden und Konzepte einer objektorientierten Programmiersprache, wie sie beispielsweise in den Lehrveranstaltungen “Grundlagen der Informatik I und II” vermittelt werden.

Prüfung: schriftlich, 120 Minuten

Literatur:

[1] Balzert, Helmut ”Lehrbuch der Softwaretechnik - Basiskonzepte und Requirements Engineering”, Spektrum Akademischer Verlag, 2009

2.65 141325: Softwaretechnik II

Nummer:	141325
Lehrform:	Vorlesungen und Übungen
Medienform:	rechnerbasierte Präsentation
Verantwortlicher:	Prof. Dr.-Ing. Helmut Balzert
Dozenten:	Dr.-Ing. Olaf Zwintzscher
	M. Sc. Michael Goll
Sprache:	Deutsch
SWS:	3
angeboten im:	

Ziele: Software-Entwicklung findet in Phasen statt. Ausgehend von den Anforderungen des Auftraggebers sind die Studierenden dazu befähigt über die Phasen Planung, Definition, Entwurf und Implementierung ein Software-Systems zu entwickeln, das nach der Abnahme gewartet, gepflegt und weiterentwickelt wird.

Inhalt:

- Entwurfsphase
- Architekturprinzipien
- Architektur- und Entwurfsmuster
- Nichtfunktionale Anordnungen
- Einflussfaktoren auf die Architektur
- Globalisierung
- Transaktionen
- Verteilte Architekturen
- Arten der Netzkommunikationen
- Softwaretechnische Infrastrukturen
- Subsysteme (Applikationen, Persistenz, Benutzungsoberfläche)
- Implementierungsphase
- Verteilungs-, Installations-, Abnahme- und Einführungsphase
- Betriebsphase

Voraussetzungen: keine

Empfohlene Vorkenntnisse: Erfahrungen in der Java-Programmierung, in der UML und im Requirements Engineering

- Inhalt aus der Vorlesung 'Softwaretechnik I'
- Inhalt aus der Vorlesung 'Grundlagen der Informatik I'
- Inhalt aus der Vorlesung 'Grundlagen der Informatik II'

Prüfung: schriftlich, 120 Minuten

Literatur:

[1] Balzert, Helmut "Lehrbuch der Softwaretechnik. Entwurf,Implementierung, Installation und Betrieb, 3. Auflage", Spektrum Akademischer Verlag, 2012

2.66 148171: Sprachimplementierung

Nummer:	148171
Lehrform:	Vorlesungen und Übungen
Medienform:	Folien rechnerbasierte Präsentation Tafelanschrieb
Verantwortlicher:	Prof. Dr. Eberhard Bertsch
Dozent:	Prof. Dr. Eberhard Bertsch
Sprache:	Deutsch
SWS:	6
angeboten im:	

Ziele: Die Studierenden haben Kenntnisse und Verständnis von Übersetzungsverfahren, speziell auch für prozedurale Programmiersprachen (wie C++, Java).

Inhalt: Die effiziente Implementierung von Programmiersprachen wie PASCAL, C oder JAVA gehört zu den wichtigsten und zugleich anspruchsvollsten Aufgaben der Praktischen Informatik. Im Laufe mehrerer Jahrzehnte wurde eine Reihe von Methoden entwickelt, die heute zum Kernbestand dieses Gebiets gehören, und die sich sinngemäß auch auf die Realisierung einfacherer Benutzer-Schnittstellen anwenden lassen. Hierzu gehören unter anderem: Lexikalische Analyse (Scanner); Syntax-Analyse, insbesondere mit LL(1)- und LR(1)-Grammatiken; statische Semantik; Laufzeitbehandlung von imperativen Konstrukten; dynamische Datentypen; Optimierung zur Compile-Zeit. Je nach Interesse seitens der Studierenden können methodisch verwandte Algorithmen zur Analyse von Zeichenketten einbezogen werden, die in der molekularen Biologie eine zunehmende Rolle spielen (beim Mustervergleich in DNA-Sequenzen und Proteinen).

Voraussetzungen: keine

Empfohlene Vorkenntnisse: Grundlagen der Informatik

Literatur:

[1] Aho, Alfred V., Lam, Monica S., Sethi, Ravi "Compilers Principles, Techniques, & Tools", Addison Wesley Longman Publishing Co, 2005
[2] Maurer, Dieter, Wilhelm, Reinhard "Übersetzerbau. Theorie, Konstruktion, Generierung", Springer, 1996

2.67 148183: Studienarbeit ITS

Nummer: 148183
Lehrform: Studienarbeit
Verantwortlicher: Studiendekan ITS
Dozent: Hochschullehrer der Fakultät ET/IT
Sprache: Deutsch
SWS: 12
Leistungspunkte: 15
angeboten im:

Ziele: Erwerb von Grundkenntnissen der wissenschaftlichen Arbeit, der Projektorganisation und der Präsentation wissenschaftlicher Ergebnisse.

Inhalt: Lösung einer wissenschaftlichen Aufgabe unter Anleitung.

Voraussetzungen: siehe Prüfungsordnung

Empfohlene Vorkenntnisse: Vorkenntnisse entsprechend dem gewählten Thema erforderlich

Arbeitsaufwand: 450 Stunden

3 Monate Vollzeittätigkeit

Prüfung: Abschlussarbeit, studienbegleitend

2.68 141128: Systeme und Schaltungen der Mobilkommunikation

Nummer:	141128
Lehrform:	Vorlesungen und Übungen
Medienform:	Folien
	Handouts
	Tafelanschrieb
Verantwortlicher:	Priv.-Doz. Dr.-Ing. Michael Vogt
Dozent:	Priv.-Doz. Dr.-Ing. Michael Vogt
Sprache:	Deutsch
SWS:	3
angeboten im:	Sommersemester

Termine im Sommersemester:

Beginn: Freitag den 15.04.2016
Vorlesung Freitags: ab 10:15 bis 11:45 Uhr im ID 03/455
Übung Freitags: ab 12:00 bis 12:45 Uhr im ID 03/455

Ziele: Die Studierenden haben einen praxisnahen Einblick in moderne Konzepte, Systeme und Schaltungen der Mobilkommunikation.

Inhalt: Unter dem Sammelbegriff der Mobilkommunikation wird die Sprach- und Datenkommunikation mit mobilen, drahtlosen Endgeräten zusammengefasst. Anwendungen wie das mobile Telefonieren, drahtlose Rechnernetzwerke und nahezu unbeschränkte Kommunikationsmöglichkeiten sind Alltag geworden. Im Rahmen der Vorlesung werden die zugrundeliegenden Verfahren und Schaltungskonzepte sowie hochfrequenztechnische Komponenten und Aspekte der Mobilkommunikation behandelt.

Aus dem Inhalt:

- Einführung in die Mobilkommunikation, Überblick, Anwendungen
- Ausbreitungsbedigungen, Mobilfunkkanal, Funknetze, Vielfachzugriffsverfahren
- Digitale Modulationsverfahren, Frequenzspreizverfahren, OFDM
- Sende- und Empfangsschaltungen, Antennen, Mischer, Filter, Synthesizer
- Mobilkommunikationssysteme: GSM, UMTS, LTE, TETRA, WLAN, Bluetooth, DECT etc.

Voraussetzungen: keine

Empfohlene Vorkenntnisse: Vorlesung “Nachrichtentechnik”, Vorlesungen “Signale und Systeme I” und “Signale und Systeme II”

Prüfung: mündlich, 30 Minuten

2.69 148178: Systemsicherheit I

Nummer:	148178
Lehrform:	Vorlesungen und Übungen
Medienform:	e-learning
	rechnerbasierte Präsentation
Verantwortlicher:	Prof. Dr. Thorsten Holz
Dozent:	Prof. Dr. Thorsten Holz
Sprache:	Deutsch
SWS:	3
angeboten im:	

Ziele: Im Rahmen der Vorlesung werden wichtige theoretische und praktische Aspekte von Sicherheitsprotokollen vorgestellt und diskutiert. Die Studierenden sollen am Ende der Vorlesungsreihe in die Lage sein, die Sicherheit gegebener Protokolle zu analysieren, Schwachstellen im Design aufzudecken sowie selbständig neue Protokolle zu entwickeln. Darüber hinaus werden auch andere Aspekte aus dem Bereich der Systemsicherheit wie beispielsweise Anonymität, Zugriffskontrolle und physische Sicherheit betrachtet.

Inhalt: Schwerpunkte des Stoffes in dieser Veranstaltung sind die für die Systemsicherheit wichtigen Bereiche der Authentifikation, Schlüsseletablierung und das Management von Identitäten. Zunächst wird auf den Begriff *Systemsicherheit* und dessen Elemente (z.B. Schutzziele oder Angreifermodelle) eingegangen. Wichtige Begriffe wie beispielsweise *Dependability* oder *Faults* werden eingeführt und erläutert. Der Begriff *kryptographisches Protokoll* und dessen wünschenswerte Eigenschaften werden diskutiert, und die Wichtigkeit dieser Protokolle für die Sicherheit von Systemen hervorgehoben.

Die Vorlesung vertieft wichtige Protokolle für Authentifikation und Schlüsselaustausch, und erläutert beispielhaft ihren Einsatz in verschiedenen, etablierten Internet-Sicherheitsprotokollen. Die wichtigsten Ziele dieser Protokolle (wie z.B. “Freshness” der Nachrichten, starke Authentifikation, Etablierung “guter Schüssel”, Effizienz, oder Schlüsselbestätigung) und die Wege wie sie erreicht werden können, werden ausführlich behandelt. Angriffe auf Protokolle werden demonstriert, sowie Maßnahmen zur Behebung der identifizierten Schwachstellen gezeigt. Ziel ist es nachzuweisen, dass für sichere Protokolle sichere kryptographische Primitiven nicht genug sind, und dass beim Protokolldesign zusätzlich viele andere Faktoren in Betracht gezogen werden müssen. Die Prinzipien für den Entwurf robuster kryptografischer Protokolle werden begleitend zu allen Protokollen diskutiert. Darüber hinaus werden auch andere Aspekte aus dem Bereich der Systemsicherheit wie beispielsweise Anonymität und physische Sicherheit betrachtet. Ein Schwerpunkt liegt dabei auf dem Themengebiet *Zugriffskontrolle* und grundlegende Modelle wie *Bell-La Padula Modell*, *Biba Modell* oder *Chinese Wall* Werden vorgestellt.

Ein integraler Teil der Veranstaltung sind die Übungen, die den Stoff mit praktischen Beispielen verdeutlichen und vertiefen.

Empfohlene Vorkenntnisse: Kryptographische Primitive (Verschlüsselungsverfahren, Signaturen, MACs, Hash-Funktionen), Kommunikationsnetze, Inhalt des Moduls 'Einführung in die Kryptographie und Datensicherheit'

Literatur:

[1] Gollmann, Dieter "Computer Security", Wiley & Sons, 1999
[2] Menezes, Alfred J., van Oorschot, Paul C., Vanstone, Scott A. "Handbook of Applied Cryptography", CRC Press, 1996
[3] Boyd, Colin, Mathuria, Anish "Protocols for Authentication and Key Establishment", Springer Verlag, 2003
[4] Anderson, Ross "Security Engineering – A guide to Building Dependable Distributed Systeme", Wiley & Sons, 2001

2.70 148017: Systemsicherheit II

Nummer:	148017
Lehrform:	Vorlesungen und Übungen
Medienform:	e-learning rechnerbasierte Präsentation
Verantwortlicher:	Prof. Dr. Thorsten Holz
Dozent:	Prof. Dr. Thorsten Holz
Sprache:	Deutsch
SWS:	3
angeboten im:	

Ziele: Diese Veranstaltung hat das Ziel, wichtige theoretische und praktische Aspekte der Systemsicherheit darzustellen, sowie die Teilnehmer zu einer kritischen Betrachtung der Systemsicherheit zu motivieren.

Inhalt: Im ersten Teil der Veranstaltung werden verschiedene Sicherheitsaspekte von Betriebssystemen vorgestellt und erläutert. Dazu werden sowohl wichtige Angriffsmethoden (z.B. *Buffer Overflows* oder *Race Conditions*) als auch Abwehrstrategien (z.B. nicht-ausführbarer Speicher oder *Address Space Layout Randomization*) diskutiert. Andere Themen, die im Mittelpunkt dieses Teils der Vorlesung stehen, sind Virtualisierung/Hypervisor sowie das sogenannte Einsperrungs-Problem (*Confinement Problem*) und die damit verbundene Analyse der verdeckten Kanäle in einem Computer-System.

Im zweiten Teil der Veranstaltung liegt der Schwerpunkt auf Schadsoftware. Dazu werden zunächst die Grundbegriffe in diesem Bereich erläutert und danach verschiedene Methoden zur Erkennung von Schadsoftware diskutiert. Wichtige Algorithmen in diesem Bereich werden vorgestellt und verschiedene Ansätze für Intrusion Detection Systeme werden behandelt.

Im praktischen Teil der Veranstaltung wird die Sicherheit von mehreren realen Systemen analysiert. Ein integraler Teil der Veranstaltung sind die Übungen, die den Stoff mit praktischen Beispielen veranschaulichen und vertiefen.

Voraussetzungen: keine

Empfohlene Vorkenntnisse: Erfahrung in systemnaher Programmierung sowie C sind hilfreich für das Verständnis der vermittelten Themen.

Literatur:

[1] Anderson, Ross "Security Engineering – A guide to Building Dependable Distributed Systeme", Wiley & Sons, 2001

2.71 148218: Technische Zuverlässigkeit

Nummer:	148218
Lehrform:	Vorlesung mit integrierten Übungen
Medienform:	Folien rechnerbasierte Präsentation Tafelanschrieb
Verantwortlicher:	Prof. Dr.-Ing. Hans Dieter Fischer
Dozent:	Prof. Dr.-Ing. Hans Dieter Fischer
Sprache:	Deutsch
SWS:	3
angeboten im:	

Ziele: Die Studierenden haben erlernt, systematisch ein komplexes System in Teilbereiche aufzugliedern, für diese Teilbereiche Zuverlässigkeits-Kenngrößen zu ermitteln, um so die Zuverlässigkeit des Gesamtsystems konservativ zu berechnen. Der Einsatz von Software in informationstechnischen Einrichtungen mit Sicherheitsverantwortung unter Einschluss von abhängigen Ausfällen ist ihnen vertraut, damit die Verfügbarkeit dieser Einrichtungen die informationstechnische Sicherheit zukünftig nicht dominiert.

Inhalt: Zuverlässigkeit und Sicherheit sind entscheidende Kriterien für den wirtschaftlichen Erfolg der immer komplizierter werdenden technischen Systeme, zumal wenn sie Software im Sinne ausführbaren Codes enthalten. Gleichzeitig vollzieht sich in unserer Gesellschaft ein Bewusstseinswandel, der durch Akzeptanzprobleme technischer Einrichtungen - z.B. so genannter Elektrosmog bei Mobiltelefonen - geprägt ist. Hieraus resultieren eine Reihe immer strengerer gesetzlicher Auflagen. Neben der Funktionalität und der Wirtschaftlichkeit eines technischen Gerätes sind für Kunden immer häufiger nachgewiesene Eigenschaften wie hohe Verfügbarkeit, Fehlertoleranz und geringes Gefährdungspotential zusätzliche Kaufargumente. Daher ist für Hersteller und Betreiber von technischen Systemen die Verwirklichung ausreichender Sicherheit und Zuverlässigkeit zu akzeptablen Kosten übergeordnetes Ziel. Die Erfüllung von Zuverlässigkeitsanforderungen wird durch ein zielgerichtetes Zuverlässigkeits-Engineering nachweisbar erreicht. Die Veranstaltung ist in zwei Teilbereiche untergliedert. Der erste theoretische Teil befasst sich mit der Lebensdauer, insbesondere mit Exponentialverteilung, dem Boole'schen Zuverlässigkeitsmodell, mit Zuverlässigkeits-Schaltungen und ihrer Analyse, um Ausfall- und Systemfunktionen zu bestimmen, mit dem Markoff'schen Zuverlässigkeitsmodell, mit der Verfügbarkeitsanalyse abhängiger Ausfälle, und einer konservativen Verfügbarkeitsanalyse mit abhängigen Ausfällen in redundanten informationstechnischen Systemen mit Wiederholungsprüfungen. Der zweite eher praktische Teil befasst sich mit qualitätssichernden Maßnahmen für Software informationstechnischer Systeme mit Sicherheitsverantwortung, mit Maßnahmen zur Vermeidung gemeinsam verursachter Ausfälle und dem Prinzip der gestaffelten Verteidigung.

Voraussetzungen: keine

Empfohlene Vorkenntnisse: Signale und Systeme, Nachrichtentechnik

Prüfung: mündlich, 30 Minuten

2.72 148083: Topics in Advanced Wireless Communications

number:	148083
teaching methods:	lecture with tutorials
media:	rechnerbasierte Präsentation Tafelanschrieb
responsible person:	Prof. Dr.-Ing. Aydin Sezgin
lecturers:	Prof. Dr.-Ing. Aydin Sezgin M. Sc. Anas Chaaban
language:	english
HWS:	3
angeboten im:	

goals: The students have a very good knowledge of the hot topics in wireless communications and are able to extend and improve results in various directions resulting in conference and journal publications.

content: Wireless networks are an important part of everyday life and have numerous applications in different areas. The number of mobile devices now exceeds by far the number of landline phones. Especially in emerging markets such as China and India and also in the developing world, the success of wireless networks is remarkable due to the reduced efforts in the deployment in comparison to wired networks. Furthermore, during the last two decades we observe an ever increasing demand for higher rates and reliability. New wireless standards such as WiMAX and LTE are already being tested successfully in different parts of the world. Many standards are still subject of performance investigations, while being improved and extended in various ways. It is thus very important to know the fundamental limits of wireless networks and also how to achieve them in practise to meet the rising expectations of consumers. In this lecture, we will discuss several important aspects and properties of wireless networks such as

- Capacity
- Fading
- Antennas
- Tradeoffs
- Power allocation
- Interference
- Scheduling

All the above mentioned items are of high importance for current wireless networks and also useful in developing new techniques and algorithms for future wireless networks. The course is taught from a signal processing and communication theory perspective with occasional deviation to information theory. Fundamentals as well as several advanced topics are covered.

requirements: keine

recommended knowledge:

- Signals and Systems
- Communications Engineering
- Either basic knowledge of linear algebra, wireless communication, information theory and coding
- Or advanced knowledge of linear and bilinear/biaffine algebra

Exam: mündlich, 30 Minuten

2.73 150240: Theoretische Informatik

Nummer:	150240
Lehrform:	Vorlesungen und Übungen
Medienform:	Folien
	Tafelanschrieb
Verantwortlicher:	Jun. Prof. Dr. Maike Buchin
Dozent:	Jun. Prof. Dr. Maike Buchin
Sprache:	Deutsch
SWS:	6
angeboten im:	Wintersemester

Ziele: Die studierenden haben fundamentale Einsichten zum Verhältnis zwischen Automaten und Grammatiken und zum Verhältnis von Determinismus und Nicht-Determinismus. Durch Einüben von Beweistechniken wie wechselseitige Simulation oder (polynomiell) berechenbare Reduktionen ist die Einsicht gereift, dass an der Oberfläche verschieden aussehende Konzepte im Kern identisch sein können. Zudem wurde ein tieferes Verständnis von Komplexität erreicht. Auf den unteren Ebenen der Chomsky-Hierarchie finden sich effizient lösbare Anwendungsprobleme der Textmanipulation und Textanalyse. Auf den oberen Ebenen der Hierarchie haben die Studierenden Bekanntschaft mit dem Phänomen der inhärenten Härte (oder gar Unentscheidbarkeit) eines Problems gemacht.

Inhalt:

- Grammatiken (mit Schwerpunkt auf kontextfreien Grammatiken)
- Automaten
- endliche Automaten
- Kellerautomaten
- Turing-Maschinen
- Berechenbarkeitstheorie
- NP-Vollständigkeitstheorie

Voraussetzungen: keine

Empfohlene Vorkenntnisse: Nützlich (aber nicht zwingend erforderlich) sind elementare Grundkenntnisse in Informatik und Diskreter Mathematik sowie Vertrautheit mit mindestens einer Programmiersprache.

Prüfung: schriftliche Prüfung, 180 Minuten

Literatur:

[1] Hopcroft, John E., Motwani, Rajeev, Ullman, Jeffrey D. "Introduction to Automata Theory, Languages, and Computation", Addison Wesley Longman Publishing Co, 2001
[2] Sipser, Michael "Introduction to the Theory of Computation", Brooks Cole, 2005
[3] Schöning, Uwe "Theoretische Informatik - kurzgefasst", Spektrum Akademischer Verlag, 2001

2.74 148202: Web-Engineering

Nummer:	148202
Lehrform:	Vorlesungen und Übungen
Medienform:	e-learning rechnerbasierte Präsentation
Verantwortlicher:	Prof. Dr.-Ing. Helmut Balzert
Dozent:	Prof. Dr.-Ing. Helmut Balzert
Sprache:	Deutsch
SWS:	3
angeboten im:	

Ziele: Die Studierenden sind in der Lage, durchgehende Web-Anwendungen - beginnend mit HTML über JSPs, die Einbindung von Java Beans und den Anschluss an eine relationale Datenbank - zu erstellen.

Inhalt: Diese Veranstaltung gibt einen vertieften Einblick in die Programmierung von Web-Anwendungen. Ausgehend von einer Vertiefung von HTML und CSS, wird anschließend die Programmierung von JSPs und die Anbindung einer SQL-Datenbank vermittelt. Damit ist der Studierende dann in der Lage, durchgehende Web-Anwendungen - beginnend mit HTML über JSPs, die Einbindung von Java Beans und den Anschluss an eine relationale Datenbank - zu erstellen. Er lernt verschiedene Werkzeuge, Techniken, Konzepte und Programmiersprachen in Kombination einzusetzen. Zusätzlich lernt der Studierende, wie mit Hilfe der UML Web-Anwendungen modelliert werden können. Am Beispiel einer Fallstudie Web-Anzeigenmarkt lernt er statische Websites und dynamische Websites kennen. Parallel zu dieser Fallstudie soll er selbst eine Website für einen (virtuellen) Verein entwickeln. Inhaltsübersicht:

HTML, XHTML & CSS

- Von HTML zu XHTML
- CSS
- XHTML-Bilder
- XHTML-Image Maps
- XHTML-Medien
- Listen: XHTML & CSS
- CSS-Klassen
- CSS: kontextabhängige Stilregeln
- CSS: ID-Attribut
- CSS: Umrandungen
- CSS: Füllungen & Abstände
- CSS: Pseudo-Klassen & -Elemente

- XHTML: Tabellen
- XHTML: Frames
- XHTML: Formulare
- Websites: Entscheidungen

JSPs

- JSPs: Java auf dem Server
- Servlets: Basis von JSPs
- JSPs: Fehlersuche
- Zugriff auf relationale Datenbanken
- JSPs: Aufruf & Parameter
- Fallstudie Web-Anzeigenmarkt
- JSP: Implizite Objekte
- Sitzungsverfolgung
- JSP-Aktionen
- Entwurfsmuster
- JSPs: Ausblick

Voraussetzungen: keine

Empfohlene Vorkenntnisse: Es werden grundlegende Kenntnisse in der objektorientierten Programmierung, insbesondere in der Programmiersprache Java vorausgesetzt. Diese Inhalte werden in den Vorlesungen Grundlagen der Informatik I und II vermittelt.

Literatur:

[1] Balzert, Helmut, Krüger, Sandra "HTML, XHTML & CSS, 2. Auflage", W3l, 2011
[2] Wißmann, Dieter "JavaServer Pages, 3. Auflage", W3l, 2012
[3] Balzert, Helmut "JSP JavaServer Pages. Quick Reference Map", W3l, 2003

2.75 148197: XML- und Webservice-Sicherheit

Nummer:	148197
Lehrform:	Vorlesungen und Übungen
Medienform:	rechnerbasierte Präsentation
Verantwortlicher:	Prof. Dr. Jörg Schwenk
Dozenten:	Prof. Dr. Jörg Schwenk
	M. Sc. Dennis Felsch
	M. Sc. Christian Mainka
	Dipl.-Ing. Vladislav Mladenov
	Dr.-Ing. Juraj Somorovsky
Sprache:	Deutsch
SWS:	3
angeboten im:	

Ziele: Die Studierenden haben ein Verständnis für die neuartigen Sicherheitsanforderungen und Probleme, die durch den Einsatz von XML- und WS-Security entstehen.

Inhalt: Das WWW hat eine einzigartige Erfolgsgeschichte erlebt. Aus diesem Grund gehen immer mehr Firmen dazu über, Geschäftsprozesse mittels Webservices über WWW-Techniken zu vernetzen. Dazu wird heute SOAP eingesetzt, das Datenformat ist XML. In dieser Vorlesung soll es um die Sicherheit von Webservices gehen. Sie besteht aus drei Teilen: Im ersten Teil soll das heutige WWW vorgstellt werden, da viele Konzepte aus XML oder Webservices ohne grundlegende Kenntnisse der Standards http, HTML, Javascript, PHP, etc. nicht verständlich sind. Der zweite Teil bietet eine Einführung in XML und seine Co-Standards, insbesondere XML Signature und XML Encryption. Der dritte Teil stellt die WS-Security Protokoll Suite vor, so weit sie bis heute publiziert ist.

Voraussetzungen: keine

Empfohlene Vorkenntnisse:

- Grundkenntnisse Kryptographie und HTML
- Programmierkenntnisse in Java

2.76 148186: Übertragung digitaler Signale

Nummer: 148186
Lehrform: Vorlesungen und Übungen
Medienform: Tafelanschrieb
Verantwortlicher: Priv.-Doz. Dr.-Ing. Karlheinz Ochs
Dozent: Priv.-Doz. Dr.-Ing. Karlheinz Ochs
Sprache: Deutsch
SWS: 3
Leistungspunkte: 5
angeboten im:

Ziele: Die Studierenden verstehen die grundlegenden und bedeutenden Zusammenhänge bei der Übertragung digitaler Signale. Insbesondere kennen sie die zugrunde liegenden physikalischen Bezüge, wobei systematische Methoden zur Beschreibung, Analyse und Synthese für Systeme zur Übertragung digitaler Signale gelehrt werden.

Inhalt: Die Vorlesung befasst sich im Kontext der Mobilfunkstandards Global System for Mobile Communications (GSM) und Universal Mobile Telecommunications System (UMTS) mit grundlegenden Methoden zur Übertragung digitaler Signale. Das Kernstück bilden Modulationsverfahren, die in lineare und nichtlineare Verfahren unterteilt sind. Von den linearen Modulationsverfahren werden die Amplitudenumtastung, die Phasenumtastung, sowie die Quadraturamplitudenmodulation und von den nichtlinearen Modulationsverfahren werden die kontinuierliche Frequenzmodulation, die Minimumumtastung, die Gauß'sche Minimumumtastung, sowie die Phasenmodulation behandelt. Als Empfangstechniken werden kohärente und inkohärente Demodulationsverfahren angesprochen, wie zum Beispiel der Produkt-Demodulator, der Zwischenfrequenz-Demodulator, der Hüllkurvenempfänger, der Frequenz-Diskriminator und der Differenz-Demodulator, wozu auch auf die Träger- und die Symboltakt-Rückgewinnung eingegangen wird. Zudem wird die Impulsformung in Bezug auf Nachbarsymbolstörungen und benötigte Bandbreite eingehend erörtert. Zur Behandlung der Impulsformung gehört auch der durch Rauschen auf dem Kanal gestörte Empfang, der die signalangepasste Filterung und den Korrelationsempfang umfasst. Schließlich wird noch auf die Maximum-A-Posteriori- und Maximum-Likelihood-Entscheidungsregeln zur Nachrichtendetektion eingegangen und die resultierenden Symbolfehler- und Bitfehler-Wahrscheinlichkeiten werden anhand des Leistungs-Bandbreite-Diagrammes in Hinblick auf Kanalkapazität und Shannon-Grenze diskutiert.

Empfohlene Vorkenntnisse: Grundlagen zur Signal- und Systemtheorie sowie zu stochastischen Signalen.

Arbeitsaufwand: 150 Stunden

Der Arbeitsaufwand berechnet sich wie folgt: Präsenz in Vorlesungen und Übungen: 42 Stunden. Zur Vor- und Nachbereitung der Vorlesung und Übungen, sowei zur Prüfungsvorbereitung: 108 Stunden

2.77 150232: Zahlentheorie

Nummer: 150232
Lehrform: Vorlesungen und Übungen
Verantwortlicher: Prof. Dr. Jörg Winkelmann
Dozent: Prof. Dr. Jörg Winkelmann
Sprache: Deutsch
SWS: 6
angeboten im: Sommersemester

Ziele: Die Studierenden haben ein umfassendes Verständnis der zahlentheoretischen Grundlagen, die für die moderne Kryptologie essentiell sind.

Inhalt: Das Ziel dieser Vorlesung ist es, eine Einführung in die Zahlentheorie zu geben. Die notwendigen Hilfsmittel aus Algebra und Analysis, die nicht aus den oben zitierten Vorlesungen bekannt sind, werden in der Vorlesung bereitgestellt. Die elementare Zahlentheorie ist ein geeignetes Thema für künftige Lehrerinnen und Lehrer, da Schüler und Laien typischerweise Spass an den einfach zu formulierenden (aber nicht immer einfach zu lösenden) Fragestellungen der Zahlentheorie haben. Ausserdem ist die Zahlentheorie ein grundlegendes Werkzeug in der Kryptographie, und im Rahmen der arithmetischen Geometrie eng verwandt mit der algebraischen Geometrie. Behandelt werden insbesondere: Primfaktorzerlegung, Kongruenzen, Chinesischer Restsatz und Anwendungen, Zahlentheoretische Funktionen (z.B. die Riemannsche Zeta-Funktion), Quadratische Reste und Quadratsummen, Diophantische Gleichungen (z.B. die Pell'sche Gleichung), Kettenbrüche, Primzahlsatz.

Voraussetzungen: keine

Empfohlene Vorkenntnisse: Grundlegende Mathematikkenntnisse

Prüfung: schriftliche Prüfung, 180 Minuten