RUHR-UNIVERSITÄT BOCHUM

RUB

Grundstudium Studiengang Sicherheit in der Informationstechnik

PO 04

Modulhandbuch

Fakultät für Elektrotechnik und Informationstechnik

Inhaltsverzeichnis

Kapitel 1

Module

1.1 Computernetze I

Nummer: 149143
Kürzel: CN1
Verantwortlicher: Prof. Dr.-Ing. York Tüchelmann
Arbeitsaufwand: 0 Stunden (entsprechend der Lehrveranstaltungen)
Leistungspunkte: 3

Ziele: Lernziel dieser Lehrveranstaltung ist es Strukturen, Komponenten und Aufbau sowie Kommunikationsprozesse einschließlich der wichtigen Algorithmen (z. B. Routing) und Protokolle (z. B. HTTP, TCP/IP) von Computernetzen kennenzulernen, zu verstehen und anwenden zu können.

Inhalt: Im Teil A dieser Lehrveranstaltung (s.u.) werden Grundwissen und Zusammenhänge hinsichtlich Struktur, Aufbau und Funktionsweise von Computernetzen vermittelt. Auf Basis des abstrakten ISO/OSI-Referenzmodells werden als wesentliche Netzwerkkomponenten die ISO/OSI-Layer spezifischen Koppelelemente (Hub, Switch, Router) detailliert behandelt und hinsichtlich ihrer Funktionalität vergleichend diskutiert. Strukturen und Architektur lokaler Netze (Ethernet, Token-Ring, ATM insbesondere als Backbone) bilden einen weiteren Schwerpunkt. Teil B behandelt vertiefend die Spezifikationen der einzelnen Layer am praktisch relevanten TCP/IP-Schichten-Modell. Betrachtet werden dabei sowohl Lokale Netze (Local Area Networks) als auch Weitverkehrsnetze (Wide Area Networks); insbesondere das Internet. Ein umfangreiches abschließendes Kapitel führt in Firewallsysteme und -architekturen ein. Im Detail ergibt sich damit die folgende inhaltliche Gliederung:

Teil A Strukturen, Komponenten, Aufbau

- Computernetze - Strukturen - Topologien - Begriffe
- Referenzmodelle und Protokollarchitekturen
- Koppelelemente in Computernetzen
- Lokale Netze - Strukturen und Aufbau

Teil B Spezifikationen für LAN und Internetworking

- Application Layer / Anwendungsschicht
- Transport Layer / Transportschicht
- Network Layer / Vermittlungsschicht
- Data Link Layer / Datenübertragungs- und Sicherungsschicht
- Sicherheitskomponente Firewallsysteme

Prüfungsform: siehe Lehrveranstaltungen

Veranstaltungen:

148069: Computernetze I 3 SWS (S.24)

1.2 Diskrete Mathematik

Nummer: 149880
Kürzel: DM-ITS
Verantwortlicher: Studiendekan ITS
Arbeitsaufwand: 0 Stunden (entsprechend der Lehrveranstaltungen)
Leistungspunkte: 10

Ziele: Die Studierenden beherrschen den professionellen Umgang mit abstrakten, diskreten Strukturen. Dazu gehört die Fähigkeit, konkrete Problemstellungen mit solchen Strukturen zu modellieren und scharfsinnige Schlussfolgerungen aus gegebenen Informationen zu ziehen (Anwendung kombinatorischer Schlussweisen). Dazu gehört weiterhin ein Verständnis für grundlegende algorithmische Techniken und die Analyse von Algorithmen. Die jeweils grundlegenden Konzepte (in Kombinatorik, Graphtheorie, elementarer Zahlentheorie und elementarer Wahrscheinlichkleitstheorie) wurden erworben. Die intellektuelle Fähigkeit, die logischen Zusammenhänge zwischen den Konzepten zu überblicken, und 'versteckte' Anwendungsmöglichkeiten zu erkennen, wurde geschult.

Inhalt: Diskrete Mathematik beschäftigt sich mit endlichen Strukturen. Der erste Teil des Moduls gliedert sich in 5 Abschnitte. Abschnitt 1 ist der Kombinatorik gewidmet. Insbesondere werden grundlegende Techniken vermittelt, um so genannte Zählprobleme zu lösen. In Abschnitt 2 beschäftigen wir uns mit der Graphentheorie. Graphen werden zur Modellierung von Anwendungsproblemen benutzt. Wir behandeln Techniken zur Graphexploration, und weitere ausgesuchte Graphprobleme. Abschnitt 3 vermittelt Grundkenntnisse in elementarer Zahlentheorie, und endet mit einem Ausblick auf kryptographische Anwendungen. Grundlegende Designtechniken für effiziente Algorithmen bilden das zentrale Thema von Abschnitt 4. Daneben geht es auch um das Aufstellen und Lösen von Rekursionsgleichungen. Abschnitt 5 liefert eine Einführung in die Wahrscheinlichkeitstheorie mit Schwergewicht auf diskreten Wahrscheinlichkeitsräumen.

Der zweite Teil des Moduls Diskrete Mathematik beschäftigt sich mit endlichen algebraischen Strukturen, insbesondere mit endlichen Gruppen, Ringen und Körpern, vor allem im Hinblick auf solche Eigenschaften, wie sie in der Kryptologie, Datenverarbeitung und Kodierung Anwendung finden.

Prüfungsform: siehe Lehrveranstaltungen

Veranstaltungen:

148173: Diskrete Mathematik II 4 SWS (S.29)
150308: Diskrete Mathematik 6 SWS (S.30)

1.3 Einführung in die Computertechnik

Nummer: 149020
Kürzel: EinfCT
Verantwortlicher: Dr.-Ing. Helmut Jacob
Arbeitsaufwand: 0 Stunden (entsprechend der Lehrveranstaltungen)
Leistungspunkte: 3

Ziele: Die Veranstaltung "Einführung in die Computertechnik" wird nicht mehr angeboten. Für Studierende im Diplomstudiengang ITS wird die zugehörige Prüfung weiterhin angeboten. AI-Studierende müssen ab Wintersemester 2008/2009 die Vorlesung "Computerarchitektur" bei Prof. Tüchelmann als Ersatzveranstaltung belegen.

Inhalt: Die Veranstaltung "Einführung in die Computertechnik" wird nicht mehr angeboten. Für Studierende im Diplomstudiengang ITS wird die zugehörige Prüfung weiterhin angeboten. AI-Studierende müssen ab Wintersemester 2008/2009 die Vorlesung "Computerarchitektur" bei Prof. Tüchelmann als Ersatzveranstaltung belegen.

Prüfungsform: siehe Lehrveranstaltungen

Veranstaltungen:

148047: Einführung in die Computertechnik 3 SWS (S.32)

1.4 Einführung in die Kryptographie und Datensicherheit

Nummer: 149022
Kürzel: KryptoDS
Verantwortlicher: Prof. Dr.-Ing. Christof Paar
Arbeitsaufwand: 0 Stunden (entsprechend der Lehrveranstaltungen)
Leistungspunkte: 6

Ziele: Ziel ist das Verständnis der wichtigsten kryptographischen Verfahren in der Praxis. Dies beinhaltet die Denkweisen, die in der modernen Kryptographie eingesetzt werden.

Inhalt: In der Vorlesung werden zunächst einige grundlegende Begriffe der Datensicherheit erläutert. Danach werden einige historisch wichtige Verschlüsselungsverfahren vorgestellt. Den Hauptteil der Vorlesung bildet die Besprechung von praktisch wichtigen Verschlüsselungsverfahren. Als bedeutende Vertreter der symmetrischen Verfahren werden der Data Encryption Standard (DES) und der Advanced Encryption Standard (AES) behandelt. Als Vertreter asymmetrischer (oder public-key) Verfahren werden RSA, diskrete Logarithmus Verfahren (Diffie-Hellman, ElGamal) und elliptische Kurven vorgestellt. Aufbauend auf die kryptographischen Primitive werden höhere Sicherheitsfunktionen entwickelt. Insbesonderen werden Digitale Signaturen, Message Authentication Codes, Hash Funktionen, Zertifikate, Protokolle zum Schlüsselaustausch, Klassifizierung von Sicherheitsdiensten und Identifikationsprotokolle vorgestellt.

Neben diesen kryptographischen Verfahren werden die notwendigen zahlentheoretischen Grundlagen (u.a. Ringe ganzer Zahlen, Euklidscher Algorithmus, Exponentiationsalgorithmen) behandelt.

Prüfungsform: siehe Lehrveranstaltungen

Veranstaltungen:

1.5 Elektronik

Nummer: 149380
Kürzel: Elek
Verantwortlicher: Prof. Dr.-Ing. Ulrich Kunze
Arbeitsaufwand: 0 Stunden (entsprechend der Lehrveranstaltungen)
Leistungspunkte: 10

Ziele: siehe zugeordnete Lehrveranstaltungen

Inhalt: siehe zugeordnete Lehrveranstaltungen

Prüfungsform: siehe Lehrveranstaltungen

Veranstaltungen:

148163: Elektronische Bauelemente	3 SWS	(S.38)
148013: Elektronische Materialien	3 SWS	(S.39)
148177: Elektronische Schaltungen	4 SWS	(S.41)

1.6 Energietechnischetechnische Aspekte der Informationstechnik

Nummer: 149400
Kürzel: EnAsInf
Verantwortlicher: Prof. Dr.-Ing. Constantinos Sourkounis
Arbeitsaufwand: 0 Stunden (entsprechend der Lehrveranstaltungen)
Leistungspunkte: 3

Ziele: Folgt.

Inhalt: Folgt.

Prüfungsform: siehe Lehrveranstaltungen

Veranstaltungen:

148066: Energietechnische Aspekte der Informationstechnik 3 SWS (S.43)

1.7 Grundlagen der Elektrotechnik

Nummer: 149280
Kürzel: GdET
Verantwortlicher: Prof. Dr.-Ing. Peter Awakowicz
Arbeitsaufwand: 0 Stunden (entsprechend der Lehrveranstaltungen)
Leistungspunkte: 7

Ziele: Die Studierenden besitzen ein grundlegendes Verständnis der Maxwellschen Theorie in Integralform, sowie einiger Anwendungen dieser Theorie. Sie sind in der Lage, einfache Aufgabenstellungen dazu rechnerisch zu bearbeiten.

Inhalt: Inhalt des Moduls ist die Maxwellsche Theorie in Integralform. Diese beschreibt alle makroskopischen, elektromagnetischen Erscheinungen. Ihre Kenntnis wird in zahlreichen Lehrveranstaltungen im weiteren Studienverlauf vorausgesetzt. Das Modul beinhaltet die folgenden Themen:

- Das elektrostatische Feld: Elektrische Feldstärke; elektrische Flussdichte; elektrisches Potential; die Kapazität; Energie und Kräfte im elektostatischen Feld; Materie im elektrischen Feld
- Der elektrische Strom: Stromdichte und Stromstärke; ohmsches Gesetz; Strömungsfelder; Energieumsetzung im elektrischen Stromkreis
- Gleichstromschaltungen: Strom und Spannungen im einfachen Stromkreis; Zweipole; Zusammenschaltung von Zweipolen; die Kirchhoffschen Regeln
- Das magnetische Feld: Magnetische Flussdichte; magnetische Erregung; Lorentz-Kraft; Durchflutungsgesetz; die magnetischen Eigenschaften der Materie; magnetische Kreise; Anwendungen der magnetischen Kraftwirkung
- Die elektromagnetische Induktion: Bewegungsinduktion; Transformationsinduktion; Induktionsgesetz; Selbst- und Gegeninduktion; Berechnung von Induktivitäten; Energie im magnetischen Feld; Wirbelströme und Stromverdrängung
- Der Transformator: Der ideale Transformator; Ersatzschaltungen für den realen Transformator; Einsatzbereiche von Transformatoren

Prüfungsform: siehe Lehrveranstaltungen

Veranstaltungen:

148007: Grundlagen der Elektrotechnik I	4 SWS	(S.44)
148008: Grundlagen der Elektrotechnik II	3 SWS	(S.46)

1.8 Grundlagen der Informatik

Nummer: 149322
Kürzel: GdInform-AI04_DiplITS
Verantwortlicher: Prof. Dr.-Ing. Helmut Balzert
Arbeitsaufwand: 0 Stunden (entsprechend der Lehrveranstaltungen)
Leistungspunkte: 6

Ziele: Dieses Modul befähigt die Studierenden - verbunden mit den praktischen Übungen am Computersystem - professionell kleine Programme problemgerecht zu entwickeln, zu analysieren, zu überprüfen, adäquat in der UML zu beschreiben und in die Programmiersprache Java zu transformieren, zu übersetzen, auszuführen und zu testen.

Inhalt: In dem Modul "Grundlagen der Informatik" werden die wichtigsten Programmierparadigmen am Beispiel zweier Programmiersprachen vermittelt. Nachdem im ersten Semester die Konzepte der strukturierten Programmierung z.B. Variablen, Typen, Ausdrücke, Anweisungen, Kontrollstrukturen und Rekursion eingeführt und anhand von Übungen veranschaulicht wurden, werden im zweiten Semester die Konzepte der objektorientierten Programmierung am Beispiel von Java vermittelt. Besonderer Wert wird innerhalb dieses Moduls auf eine systematische Vorgehensweise gelegt. So werden unterschiedliche Diagrammtypen der UML (Unified Modeling Language) erläutert sowie grundlegende Entwurfsmuster vorgestellt.

Prüfungsform: siehe Lehrveranstaltungen

Veranstaltungen:

1.9 Grundlagen der Informationstechnik

Nummer: 149162
Kürzel: GdInfTe
Verantwortlicher: Prof. Dr.-Ing. Rainer Martin
Arbeitsaufwand: 0 Stunden (entsprechend der Lehrveranstaltungen)
Leistungspunkte: 7

Ziele: In vielen informationstechnischen Anwendungen (Mobilfunk, Fernsehen etc.) werden Informationen aus physikalischen Signalen gewonnen, verarbeitet und übertragen. Es kann sich dabei um akustische Signale (Sprache, Musik), Bild- und Videosignale, oder auch medizinische Signale (EKG, EEG) handeln. Sofern die Signale nichtelektrischer Natur sind, werden sie in aller Regel vor einer weiteren Verarbeitung in elektrische Signale umgewandelt. Analoge und digitale elektronische Geräte spielen daher bei der Verarbeitung und Übertragung informationstragender Signale eine überragende Rolle. Die Studierenden beherrschen die grundlegenden Prinzipien analoger und digitaler Systeme auf verschiedenen Abstraktionsstufen. Dabei wurde ein Kanon an Fertigkeiten entwickelt, der für das weitere Studium von großer Bedeutung ist. Neben den eher mathematisch-handwerklichen Fertigkeiten, wie zum Beispiel das Rechnen mit komplexen Zahlen und die Grundlagen der Wahrscheinlichkeitsrechnung, werden auch wichtige methodische Fertigkeiten beherrscht. Dabei steht die Analyse und selbständige Bearbeitung von Aufgabenstellung, und die Umsetzung der physikalisch/technischen Beschreibung in ein mathematisches Modell im Mittelpunkt. Die Studierenden verstehen nach einem erfolgreichen Abschluss des Moduls die Prinzipien der A/D-Umsetzung, wissen wie der Informationsgehalt eines Signals berechnet wird, und kennen die Eigenschaften linearer Systeme. Sie verstehen die mathematischen Verfahren zur Analyse linearer Netzwerke (Superpositionsprinzip, Methode der Ersatzquelle, graphentheoretische Verfahren), und können sie anwenden. Sie wissen, wie diese Verfahren für harmonische Wechselgrößen im eingeschwungenen Zustand, und für allgemeine periodische Signale einzusetzen sind. Sie erweitern ihre elektrotechnischen Kenntnisse und mathematische Fertigkeiten, um das Zeit- und Frequenzverhalten einfacher linearer Netzwerke, z.B. linearer Zweitornetzwerke, zu analysieren.

Inhalt: Im ersten Teil der Vorlesung 'Grundlagen der Informationstechnik I' werden die Grundbegriffe informationstechnischer Systeme vorgestellt, und anhand aktueller Anwendungen diskutiert. Die Beschreibung und die Eigenschaften analoger, diskreter und digitaler Signale stehen dabei im Mittelpunkt. Informationstheoretische Überlegungen führen schließlich zur Bestimmung des mittleren Informationsgehalts dieser Signale, und zu optimalen Codierverfahren.

Der zweite Teil dieser Vorlesung behandelt die Grundlagen linearer elektrischer Netzwerke. Dabei sind insbesondere sinusförmige (harmonische) Ströme und Spannungen als Anregungssignale von Interesse. Die komplexe Wechselstromrechnung wird als mathematisch elegantes Werkzeug zur Berechnung dieser Netzwerke im eingeschwungenen Zustand eingeführt.

In der Vorlesung 'Grundlagen der Informationstechnik II' stehen Berechnungsverfahren für Netzwerke, die aus ohmschen Widerständen, idealen Kondensatoren, Spulen und Quellen zusammengesetzt sind, im Mittelpunkt. Dabei werden überwiegend harmonische Anregungsgrößen betrachtet, und das Verhalten dieser Netzwerke als Funktion der Frequenz analysiert. Tiefpass-, Hochpass- und Bandpassfilter werden eingeführt, und deren Verhalten wird berechnet. Darüber hinaus werden Schalt- und Ausgleichsvorgänge in elektrischen Netzwerken behandelt. Zum Abschluss der Vorlesung wird ein Ausblick auf die zeitdiskrete Verarbeitung informationstragender Signale mittels digitaler Prozessoren gegeben.

Prüfungsform: siehe Lehrveranstaltungen

Veranstaltungen:

1.10 Grundlagenpraktikum ITS

Nummer: 149240
Kürzel: PrakITS
Verantwortlicher: Prof. Dr. Jörg Schwenk
Arbeitsaufwand: 0 Stunden (entsprechend der Lehrveranstaltungen)
Leistungspunkte: 3

Ziele: Die Studierenden kennen praktische Aspekte der IT-Sicherheit sowie der (Un-)Sicherheit konkreter Verfahren und Produkte.

Inhalt: In 10 Versuchen und 2 Ersatzversuchen wird eine praktische Einführung in die IT-Security gegeben. Jeder Versuch muss anhand eines Handouts vorbereitet werden, und eine kurze Versuchsauswertung muss abgegeben werden. Die Themen umfassen zur Zeit (Anpassungen aufgrund aktueller Entwicklungen sind möglich):

- GnuPG (PGP) zum Verschlüsseln und Signieren verwenden
- Protokollanalyse mit Ethereal
- Benutzung der Tools Nessus und nmap zur Sicherheitsuntersuchung
- Group Key Agreement
- Cryptography with Bouncy Castle
- Firewalls
- Voice over IP (VoIP)
- OpenSSL und Zertifikate
- Kerberos Server aufsetzen
- Buffer Overflow Attacken
- Web Services Security
- Spoofing Angriffe
- Angriffe in geswitchten Netzwerken (ettercap)
- Sicheres CGI-Scripting mit Perl
- XML Verschlüsselung und Signatur
- E-Mail Sicherheit / SMIME

Prüfungsform: siehe Lehrveranstaltungen

Veranstaltungen:

142240: Bachelor-Grundlagenpraktikum ITS 3 SWS (S.22)

1.11 Mathematik A

Nummer: 149619
Kürzel: MatheA-Dipl
Verantwortlicher: Dr. Günter Felbecker
Arbeitsaufwand: 0 Stunden (entsprechend der Lehrveranstaltungen)
Leistungspunkte: 14

Ziele: Nach dem Besuch der Vorlesung sind die Teilnehmer gerüstet, grundlegende mathematische Ingenieraufgaben der Algebra und Analysis zu lösen. Sie kennen Laplace- und Fouriertrasformation die zur Lösung von Ingenieuraufgaben weit verbreitet sind.

Inhalt: Reelle und komplexe Zahlen Vektoren, Matrizen, Determinanten, Eigenwerte, Eigenvektoren Folgen, Reihen Elementare Funktionen, Potenzreihen Grenzwerte, Stetigkeit Differenzialrechnung Integralrechnung Einfache gewöhnliche Differenzialgleichungen Differenzialrechnung für Funktionen von mehreren Variablen Orthonormalsysteme, Fourierreihen Integralrechnung für Funktionen von mehreren Variablen Kurvenintegrale, Flächenintegrale Integralsätze Laplace- und Fouriertransformation

Prüfungsform: siehe Lehrveranstaltungen

Veranstaltungen:

148000: Mathematik I 8 SWS (S.56)
148004: Mathematik II 6 SWS (S.57)

1.12 Netzsicherheit

Nummer: 149241
Kürzel: NS
Verantwortlicher: Prof. Dr. Jörg Schwenk
Arbeitsaufwand: 0 Stunden (entsprechend der Lehrveranstaltungen)
Leistungspunkte: 6

Ziele: Verständnis aller technischen Aspekte der Netzsicherheit. Es soll klar werden, dass Kryptographie allein nicht ausreicht. Organisatorische Aspekte der Sicherheit werden nur kurz behandelt. Eigenständige Überlegungen zur Verbesserung der Sicherheit sollen die Studierenden auf ihre Rolle im Berufsleben vorbereiten.

Inhalt: Kryptographie wird eingesetzt, um die Vertraulichkeit und Integrität von Daten zu schützen, die über Datennetze übertragen werden. Hierbei werden sowohl symmetrische Verfahren (Pay-TV, Mobilfunk, WLAN) als auch asymmetrische bzw. hybride Verfahren (E-Mail, WWW, VPN) eingesetzt. In der Vorlesung werden konkrete kryptographische Systeme zur Absicherung von Netzen betrachtet, und von allen Seiten auf ihre Sicherheit hin beleuchtet. Neben den Systemen selbst werden dabei auch publizierte Angriffe auf diese Systeme besprochen; die Studenten werden aufgefordert, selbst wissenschaftliche Überlegungen zur Verbesserung der Sicherheit anzustellen.

Prüfungsform: siehe Lehrveranstaltungen

Veranstaltungen:

148161: Netzsicherheit I 3 SWS (S.58)
148187: Netzsicherheit II 3 SWS (S.59)

1.13 Programmiersprachen

Nummer: 149894
Kürzel: ProgSp
Verantwortlicher: Studiendekan ITS
Arbeitsaufwand: 0 Stunden (entsprechend der Lehrveranstaltungen)
Leistungspunkte: 3

Ziele: Ziel der Lehrveranstaltung "Programmiersprachen" ist es, die Studierenden in die Grundlagen der Sprache C mit Betonung der prozeduralen Betrachtungsweise einzuführen. Sie sollen danach in der Lage sein, C-Sourcecode zu analysieren, und einfache C-Routinen selbst zu schreiben. Da die C-Syntax auch in vielen anderen Bereichen zum Einsatz kommt (Spezifikationen, Skriptsprachen, Linux/ Unix) ist dies auch eine wichtige Grundlage für das weitere Studium.

Inhalt: Als zweite Programmiersprache soll hier (nach Java in den „Grundlagen der Informatik") die Sprache C (nicht C++) eingeführt werden. C eignet sich insbesondere dazu, „hardwarenah" zu programmieren. • Von der Maschinensprache zu C • Die Struktur von C-Programmen Variable und Datentypen in C • Bildschirm Ein-/Ausgabe • Kontrollstrukturen • Funktionen • Programmierstill, Programmierrichtlinien Felder und Zeichenketten • Ausdrücke • Arbeiten mit Dateien • Strukturen, Aufzählungstypen • Zeiger • Speicherklassen • Vertiefung einiger Themen • Buffer Overflow- und Formatstring-Angriffe • C in der Praxis

Prüfungsform: siehe Lehrveranstaltungen

Veranstaltungen:

148002: Programmieren in C 3 SWS (S.60)

1.14 Technische Informatik

Nummer: 149302
Kürzel: TechInf
Verantwortlicher: Prof. Dr.-Ing. Jürgen Oehm
Arbeitsaufwand: 0 Stunden (entsprechend der Lehrveranstaltungen)
Leistungspunkte: 6

Ziele: Ziel der Lehrveranstaltung 'Digitaltechnik' ist die Vermittlung elementarer Grundlagenkenntnisse aus den Bereichen Boolesche Algebra, Kostenoptimierung digitaler Schaltungen, Aufbau und die Wirkungsweisen von digitalen Grundschaltungen, Aufbau und Funktion von Basisfunktionalitäten, aus denen sich z.B. ein Mirkoprozessorsystem zusammensetzt (wie z.B. Zähler, Schieberegister, ALU, Bustreiber, Speicher). Mit diesem Wissen sollten die Studenten in der Lage sein, zukünftige Entwicklungen in den Integrationstechnologien, und damit in der Digitaltechnik, bezüglich ihrer Möglichkeiten und Grenzen einzuschätzen.

Durch eigene Experimente erwerben die Teilnehmer der Lehrveranstaltung 'Eingebettete Prozessoren' vertiefte Programmierkenntnisse zur Assemblerprogrammierung eines konkreten Mikrocontrollers, und zur Anwendungsprogrammierung in der Sprache C für diesen Mikrocontroller.

Inhalt: Das Modul umfaßt mit seinen Lerninhalten zentrale Themengebiete der Digitaltechnik und darauf aufbauend die der Mikroprozessortechnik.

Die Digitaltechnik setzt in ihrem Kern auf die zentralen schaltungstechnischen Grundfunktionen NAND, NOR und NOT auf. Über diese Grundfunktionen werden digitale Ja/Nein-Informationen miteinander verknüpft. Aus den Grundfunktionen setzen sich höherwertige digitale Funktionsgruppen wie z.B. Flipflops, Zähler, Schieberegister, Multiplexer, Rechenwerke und Speicher zusammen. Diese sind wiederum Teilfunktionen von so komplexen Systemen wie Mikroprozessor und Mikrocontroller. Die heutige Entwicklung geht dahin, immer mehr digitale Funktionen auf einem Chip zu integrieren - vorzugsweise in der VLSI-gerechten CMOS-Technik. Weiterhin werden in der Lehrveranstaltung 'Digitaltechnik' zentrale Kenntnisse vermittelt über den inneren schaltungstechnischen Aufbau aktueller Logikfamilien, die besonderen Eigenschaften einer CMOS-Logik, die Skalierungseigenschaften von CMOS-Technologien und ihre Auswirkungen auf die elektrischen Eigenschaften logischer Schaltungen und Systeme.

Die Digitaltechnik ist in Verbindung mit der auf ihr aufbauenden Computertechnologie aus der aktuellen technischen Entwicklung nicht mehr wegzudenken. Die moderne Computertechnologie ist ein kompliziertes Zusammenspiel aus Hardware und Software. In ihren Schnittstellenbereichen eingebettet befinden sich jeweils Mikrocontroller mit geeigneter Programmierung. Mikroprozessoren bzw. Mikrocontroller als eingebettete Einheiten eignen sich wegen ihrer freien Programmierbarkeit und ihrer signaltechnischen Anpassungsfähigkeit an unterschiedlichste Anwendungsfälle ideal dazu, als miniaturisierte Steuerzentralen in Geräten eingesetzt zu werden. Mikroprozessoren bzw. Mikrocontroller als eingebettete Einheiten sind in den innovativen

Produkten unserer Zeit typisch, wesentlicher Bestandteil einer technischen Lösung.

Aufbauend auf dem in der Lehrveranstaltung 'Digitaltechnik' erworbenen Wissen vermittelt die Lehrveranstaltung 'Eingebettete Prozessoren' Grundlagenkenntnisse zum Gesamtspektrum der Anwendungen von prozessorgestützten Schaltungen, wobei die wichtigsten Merkmale des Leistungsstands an Fallbeispielen erläutert werden. Die Lehrveranstaltung vermittelt weiterhin Grundlagenkenntnisse zu typischen Hardware-Komponenten gemäß dem Stand der Technik, und mit Hilfe konkreter beispielhafter Datenblätter, Grundlagenkenntnisse zu Grundsätzen der Assemblerprogrammierung für aktuelle repräsentative Mikrocontroller. Das Zielsystem für die Programmierprobleme ist ein mikrocontrollergestütztes Minimodul, das für ein breites Spektrum von Anwendungen geeignet ist, und zusammen mit der Entwicklungs-Software für eine eigenständige Programmentwicklung zur Verfügung gestellt wird. Während das Assemblerprogrammieren an einigen einfachen Beispielen geübt wird, ist das Ziel des C-Programmier-Problems etwas komplexer: die Nutzung des Minimoduls zur bedienbaren Erfassung und Auswertung von Temperaturen.

Prüfungsform: siehe Lehrveranstaltungen

Veranstaltungen:

148169: Digitaltechnik	3 SWS	(S.26)
148175: Eingebettete Prozessoren	3 SWS	(S.36)

Kapitel 2

Veranstaltungen

2.1 142240: Bachelor-Grundlagenpraktikum ITS

Nummer:	142240
Lehrform:	Praktikum
Medienform:	Internet rechnerbasierte Präsentation
Verantwortlicher:	Prof. Dr. Jörg Schwenk
Dozenten:	Prof. Dr. Jörg Schwenk M. Sc. Marcus Niemietz student. Hilfskräfte
Sprache:	Deutsch
SWS:	3
angeboten im:	Wintersemester und Sommersemester

Termine im Wintersemester:

Beginn: Montag den 26.10.2015
Praktikum Montags: ab 14:00 bis 17:00 Uhr im ID 2/168

Termine im Sommersemester:

Beginn: Montag den 11.04.2016
Praktikum Montags: ab 14:00 bis 17:00 Uhr im ID 2/168

Ziele: Die Studierenden kennen praktische Aspekte der IT-Sicherheit sowie der (Un-)Sicherheit konkreter Verfahren und Produkte.

Inhalt: In 10 Versuchen und 2 Ersatzversuchen wird eine praktische Einführung in die IT-Security gegeben. Jeder Versuch muss anhand eines Handouts vorbereitet werden, und eine kurze Versuchsauswertung muss abgegeben werden. Die Themen umfassen zur Zeit (Anpassungen aufgrund aktueller Entwicklungen sind möglich):

- Netzwerk-Analyse mit nmap & Wireshark
- Kryptographie in Java
- Buffer Overflow Attacken
- Angriffe in geswitchten Netzwerken
- Konfiguration von Firewalls
- Verwenden von GnuPG (PGP) zum Verschlüsseln und Signieren
- E-Mail Sicherheit
- Web Angriffe
- Spoofing Angriffe
- Sicherheit in der Gruppenkommunikation

- Sicheres CGI-Scripting
- MD5 Kollisionen in Postscript
- Angriffe auf RSA
- Angriffe auf WEP

Voraussetzungen: keine

Empfohlene Vorkenntnisse: Grundkenntnisse aus den Bereichen Kryptographie, Programmiersprache, und Computernetze

Prüfung: Praktikum, studienbegleitend

2.2 148069: Computernetze I

Nummer:	148069
Lehrform:	Vorlesung mit integrierten Übungen
Medienform:	Blackboard Folien rechnerbasierte Präsentation
Verantwortlicher:	Prof. Dr.-Ing. York Tüchelmann
Dozenten:	Prof. Dr.-Ing. York Tüchelmann wiss. Mitarbeiter
Sprache:	Deutsch
SWS:	3
angeboten im:	

Ziele: Lernziel dieser Lehrveranstaltung ist es Strukturen, Komponenten und Aufbau, sowie Kommunikationsprozesse einschließlich der wichtigen Algorithmen (z. B. Routing) und Protokolle (z. B. HTTP, TCP/IP) von Computernetzen kennenzulernen, zu verstehen und anwenden zu können.

Inhalt: In dieser Lehrveranstaltung werden Grundlagen und Zusammenhänge hinsichtlich Struktur, Aufbau und Funktionsweise von Computernetzen mit folgenden Inhalten vermittelt:

•Computernetze und Internet - Einführung und Überblick - Strukturelle Merkmale des Internet - Verzögerung, Verlust und Durchsatz in paketvermittelten Netzen - Protokollschichten und Dienstmodelle

•Application Layer / Anwendungsschicht - HTTP - Hypertext Transfer Protocol - FTP - File Transfer Protocol - SMTP - Simple Mail Transfer Protocol - SIP - Session Initiation Protocol - DNS - Domain Name Service - P2P- Prinzip und Anwendungen

•Transport Layer / Transportschicht - Generelle Design - Prinzipien der Transportschicht - Verbindungslose Kommunikation UDP - User Datagram Protocol - Verbindungsorientierte Kommunikation TCP - Transmission Control Protocol

•Network Layer / Vermittlungsschicht - Generelle Design – Prinzipien der Vermittlungsschicht - Router, Routing – Algorithmen - Network Layer im Internet (IPv4, IPv6) - Steuerprotokolle im Internet

•Data Link Layer / Datenübertragungs- und Sicherungsschicht - Data Link Layer - Einführung und Grundlagen - Fehlerbehandlung - Protokolle für Mehrfachzugriffe - Adressierung auf der Sicherungsschicht - Ethernet - Switches auf der Sicherungsschicht - Asynchronous Transfer Mode (ATM) - Multi Protocol Label Switching (MPLS)

•Wireless Networks - Wireless Links und ihre Charakteristiken - 802.11 Wireless LANs

•Sicherheitskomponenten für Computernetze - Sicherheitserwartungen, Bedrohungen und Risiken und Sicherheitsstrategien - Firewall – Systeme: Paketfilter und Proxy - Systeme - Architekturen für Firewall-Systeme

Empfohlene Vorkenntnisse: Basiswissen der Informationstechnik / Kommunikationstechnik

Literatur:

[1] Kurose, James F., Ross, Keith W. "Computer Networking: A Top-Down Approach Featuring the Internet", Addison Wesley Longman Publishing Co, 2005
[2] Tanenbaum, Andrew S. "Computer Networks", Prentice Hall, 2003
[3] Kurose, James, Ross, Keith "Computernetze . Ein Top-Down-Ansatz mit Schwerpunkt Internet", Pearson Studium, 2002
[4] Tanenbaum, Andrew S. "Computernetzwerke", Pearson Studium, 2003

2.3 148169: Digitaltechnik

Nummer:	148169
Lehrform:	Vorlesungen und Übungen
Medienform:	Folien rechnerbasierte Präsentation Tafelanschrieb
Verantwortlicher:	Prof. Dr.-Ing. Jürgen Oehm
Dozenten:	Prof. Dr.-Ing. Jürgen Oehm Dipl.-Ing. André Feiler Dipl.-Ing. Dominic Funke Dipl.-Ing. Ivan Stoychev
Sprache:	Deutsch
SWS:	3
angeboten im:	

Ziele: Ziel der Lehrveranstaltung 'Digitaltechnik' ist die Vermittlung elementarer Grundlagenkenntnisse aus den Bereichen Boolesche Algebra, Kostenoptimierung digitaler Schaltungen, Aufbau und die Wirkungsweisen von digitalen Grundschaltungen, Aufbau und Funktion von Basisfunktionalitäten aus denen sich z.B. ein Mikroprozessorsystem zusammensetzt (wie z.B. Zähler, Schieberegister, ALU, Bustreiber, Speicher). Weiterhin werden in der Lehrveranstaltung 'Digitaltechnik' zentrale Kenntnisse über den inneren schaltungstechnischen Aufbau aktueller Logikfamilien vermittelt, die besonderen Eigenschaften einer CMOS-Logik, die Skalierungseigenschaften von CMOS-Technologien und ihre Auswirkungen auf die elektrischen Eigenschaften logischer Schaltungen und Systeme. Mit diesem Wissen sollten die Studenten in der Lage sein, zukünftige Entwicklungen in den Integrationstechnologien, und damit in der Digitaltechnik bezüglich ihrer Möglichkeiten und Grenzen einzuschätzen.

Inhalt:

- Historischer Rückblick, Motivation Digitaltechnik
- Boolesche Algebra
- Zahlendarstellungen, Rechenwerke, ALU
- Flankendetektoren, Flip-Flops (FFs)
- Teiler, Zähler, Schieberegister, Halbleiterspeicher
- Tools zur Logikanalyse
- Dioden-Logik, Dioden Transistor Logik, Transistor Transistor Logik, CMOS-Logik
- CMOS Technologie, Moore's Law
- CMOS Standard-Zellen Konzept

Die Vorlesung beginnt mit den theoretischen Grundlagen der Schaltalgebra. Danach werden verschiedene Verfahren zur Vereinfachung von logischen Netzwerken vorgestellt. Die vereinfachten logischen Netzwerke gilt es dann auf der Basis der schaltungstechnischen logischen Grundfunktionen NAND, NOR und NOT in kostenoptimale logische Netzwerke zu überführen. Dabei wird der Begriff der Kosten sowohl unter dem Gesichtspunkt des Hardwareaufwands, als auch unter dem Gesichtspunkt der Summe der Gatterlaufzeiten in den Signalpfaden eingeführt. Der zweite Teil der Vorlesung beschäftigt sich mit den zentralen Eigenschaften der wichtigsten Logikfamilien. Voran gestellt werden zunächst die klassischen Logikfamilien (Dioden-Logik, Dioden-Transistor-Logik, Transistor-Transistor-Logik) in Verbindung mit ihren typischen Merkmalen. Vor dem Hintergrund des aktuellen Technologiefortschritts werden daran anschließend die zentralen Merkmale einer CMOS-Technologie, das Moore'sche Gesetz, die Auswirkungen von Technologieskalierungen auf die Schaltzeiten der CMOS-Gatter, die CMOS-Logik und das CMOS-Standard-zellenkonzept vorgestellt. Der dritte Teil der Vorlesung beschäftigt sich mit den höherwertigen digitalen Funktionsgruppen. Dazu gehören z.B. Flipflops, Zähler, Schieberegister, Multiplexer/Demultiplexer, Rechenwerke/ALU und Speicher. Die Konzepte synchroner/asynchroner Taktsteuerungen und paralleler/sequentieller Datenverarbeitung werden in Verbindung mit den möglichen unterschiedlichen Architekturen der höherwertigen Funktionsgruppen diskutiert.

Empfohlene Vorkenntnisse:

- Grundlagen der Elektronik

Erforderlich sind zudem elementare Kenntnisse in:

- Grundlagen der Elektrotechnik
- Mathematik

Literatur:

[1] Katz, Randy H. "Contemporary Logic Design", Prentice Hall, 1993
[2] Beikirch, Helmut, Seifart, Manfred "Digitale Schaltungen", Verlag Technik, 1998
[3] Borucki, Lorenz, Stockfisch, Georg "Digitaltechnik", Teubner Verlag, 1989
[4] Pernards, Peter "Digitaltechnik I. Grundlagen, Entwurf, Schaltungen", Hüthig, 2001
[5] Fricke, Klaus "Digitaltechnik. Lehr- und Übungsbuch für Elektrotechniker und Informatiker", Vieweg, 2005
[6] Becker, Jürgen, Lipp, Hans Martin "Grundlagen der Digitaltechnik", Oldenbourg, 2005
[7] Gamm, Eberhard, Schenk, Christoph, Tietze, Ulrich "Halbleiter - Schaltungstechnik", Springer, 2002
[8] "Handbuch der Elektronik. Digitaltechnik", Medien Institut Bremen, 1999
[9] Eshragian, Karman, Eshragian, Kamran, Weste, Neil H. E. "Principles of CMOS VLSI Design: A Systems Perspective", Addison Wesley Longman Publishing Co, 1993
[10] Henke, Karsten, Wuttke, Heinz-Dieter "Schaltsysteme. Eine automatenorientierte Einführung", Pearson Studium, 2002
[11] Siemers, Christian, Sikora, Axel "Taschenbuch Digitaltechnik", Hanser Fachbuchverlag, 2002
[12] Schiffmann, Wolfram, Schmitz, Robert "Technische Informatik 1. Grundlagen der digitalen Elektronik", Springer, 2003

2.4 148173: Diskrete Mathematik II

Nummer: 148173
Lehrform: Vorlesungen und Übungen
Medienform: Tafelanschrieb
Verantwortlicher: Prof. Dr. Alexander May
Dozent: Prof. Dr. Alexander May
Sprache: Deutsch
SWS: 4
angeboten im:

Ziele: Die Studierenden beherrschen den professionellen Umgang mit abstrakten, diskreten Strukturen. Dazu gehört die Fähigkeit, konkrete Problemstellungen mit solchen Strukturen zu modellieren und scharfsinnige Schlussfolgerungen aus gegebenen Informationen zu ziehen (Anwendung kombinatorischer Schlussweisen). Dazu gehört weiterhin ein Verständnis für grundlegende algorithmische Techniken, und die Analyse von Algorithmen. In den einzelnen Abschnitten der Vorlesung wurden die jeweils grundlegenden Konzepte (in Kombinatorik, Graphtheorie, elementarer Zahlentheorie und elementarer Wahrscheinlichkleitstheorie) erworben. Die intellektuelle Fähigkeit, die logischen Zusammenhänge zwischen den Konzepten zu überblicken, und 'versteckte' Anwendungsmöglichkeiten zu erkennen, wurde geschult.

Inhalt: Diskrete Mathematik beschäftigt sich mit endlichen algebraischen Strukturen, insbesondere mit endlichen Gruppen, Ringen und Körpern, vor allem in Hinblick auf solche Eigenschaften, wie sie in der Kryptologie, Datenverarbeitung und Kodierung Anwendung finden. Dabei werden betrachtet: Relationen und Halbgruppen, Minimale Erzeugendensysteme, Worthalbgruppen und Codes, Gruppen, Ringe und Körper, Quadratisches Reziprozitätsgesetz, Bruchrechnung, Polynomalgebren, Ideale, Endliche Körper und Ellipitsche Kurven

Voraussetzungen: keine

Empfohlene Vorkenntnisse: Grundvorlesungen Mathematik (Analysis, Lineare Algebra) und eine Programmiervorlesung

2.5 150308: Diskrete Mathematik

Nummer:	150308
Lehrform:	Vorlesungen und Übungen
Medienform:	Folien
	Tafelanschrieb
Verantwortlicher:	Priv.-Doz. Dr. Björn Schuster
Dozent:	Priv.-Doz. Dr. Björn Schuster
Sprache:	Deutsch
SWS:	6
angeboten im:	Wintersemester

Termine im Wintersemester:

Beginn: Dienstag den 20.10.2015
Vorlesung Dienstags: ab 16:00 bis 18:00 Uhr im HIB
Vorlesung Mittwochs: ab 12:00 bis 14:00 Uhr im HZO 50
Übung (alternativ) Dienstags: ab 08:00 bis 10:00 Uhr im NB 02/99
Übung (alternativ) Dienstags: ab 10:00 bis 12:00 Uhr im NA 02/99
Übung (alternativ) Dienstags: ab 14:00 bis 16:00 Uhr im NA 6/99
Übung (alternativ) Mittwochs: ab 08:00 bis 10:00 Uhr im NA 5/99
Übung (alternativ) Mittwochs: ab 10:00 bis 12:00 Uhr im NA 6/99
Übung (alternativ) Mittwochs: ab 10:00 bis 12:00 Uhr im NB 02/99

Ziele: Die Studierenden beherrschen den professionellen Umgang mit abstrakten, diskreten Strukturen. Dazu gehört die Fähigkeit, konkrete Problemstellungen mit solchen Strukturen zu modellieren und scharfsinnige Schlussfolgerungen aus gegebenen Informationen zu ziehen (Anwendung kombinatorischer Schlussweisen). Dazu gehört weiterhin ein Verständnis für grundlegende algorithmische Techniken, und die Analyse von Algorithmen. In den einzelnen Abschnitten der Vorlesung wurden die jeweils grundlegenden Konzepte (in Kombinatorik, Graphtheorie, elementarer Zahlentheorie und elementarer Wahrscheinlichkleitstheorie) erworben. Die intellektuelle Fähigkeit, die logischen Zusammenhänge zwischen den Konzepten zu überblicken, und 'versteckte' Anwendungsmöglichkeiten zu erkennen, wurde geschult.

Inhalt: Die Diskrete Mathematik beschäftigt sich mit endlichen Strukturen. Die Vorlesung gliedert sich in 5 Abschnitte. Abschnitt 1 ist der Kombinatorik gewidmet. Insbesondere werden grundlegende Techniken vermittelt, um sogenannte Zählprobleme zu lösen. In Abschnitt 2 beschäftigen wir uns mit der Graphentheorie. Graphen werden zur Modellierung von Anwendungsproblemen benutzt. Wir behandeln Techniken zur Graphenexploration und weitere ausgesuchte Graphenprobleme. Abschnitt 3 vermittelt Grundkenntnisse in elementarer Zahlentheorie und endet mit einem Ausblick auf kryptographische Anwendungen. Grundlegende Designtechniken für effiziente Algorithmen bilden das zentrale Thema von Abschnitt 4. Daneben geht es auch um das Aufstellen und Lösen von Rekursionsgleichungen. Abschnitt 5

liefert eine Einführung in die Wahrscheinlichkeitstheorie mit Schwergewicht auf diskreten Wahrscheinlichkeitsräumen.

Voraussetzungen: keine

Empfohlene Vorkenntnisse: Elementare Grundkenntnisse in Analysis und linearer Algebra

Prüfung: schriftlich, 180 Minuten

2.6 148047: Einführung in die Computertechnik

Nummer:	148047
Lehrform:	Vorlesung mit integrierten Übungen
Medienform:	Folien
	Tafelanschrieb
Verantwortlicher:	Dr.-Ing. Helmut Jacob
Dozent:	Dr.-Ing. Helmut Jacob
Sprache:	Deutsch
SWS:	3
angeboten im:	

Ziele: Ziel der Veranstaltung ist es, einen grundlegenden Einblick in wichtige gerätetechnische und konzeptuelle Aspekte der heute üblichen Computersysteme zu geben. (Personal-Computer, Workstation, Server, Industriecomputer, Computernetze). Für die Aufteilung der Computerfunktionen gibt es Standard-Schnittstellen, deren Sinn und Aufbau verständlich gemacht wird (FSB; JEDEC, PCI, AGP, IDE/SCSI, USB). Die zentrale Funktionseinheit ist der Prozessor (oder Prozessor-Cluster), deren prinzipieller Aufbau untersucht wird (Pipeline-Struktur, Cache-Konzept, physikalische und virtuelle Adressierung, Maschinenbefehle, Programmverarbeitung, Interrupt-Konzept). Ein anderer Schwerpunkt liegt im Einblick in aktuelle Speichertechnologien (SDRAM, DDR-DRAM, Modul-Standards). Ohne die Funktion der Peripheriegeräte wäre der Betrieb der zentralen Einheiten ohne Wirkung zur Außenwelt. Deshalb gibt es auch eine Einführung in die Funktion von Standard-Peripheriegeräten.

Inhalt:

- Entwicklung der Halbleitertechnologie
- Computerklassen und das Messen der Computerleistung
- Physikalische und grundlegende logische Merkmale von Computernetzen
- Elementare Aufbaumerkmale der Personal-Computer/Workstation/Server
- Steuerung des Datenverkehrs auf einem Motherboard (Chipsatz)
- Der Datenverkehr zwischen der Peripherie und dem Hauptspeicher (PCI, AGP)
- Konzept für die Meldung externer programmsteuernder Ereignisse (Interrupt Controller)
- Cache-Konzepte

- Aufbau und Schnittstelle von Prozessoren (Beispiele: Pentium4, Athlon)
- Maschinenbefehle, virtuelle und physikalische Adressierung
- Strukturmerkmale von DRAM-Speicher-ICs, synchrone DRAMs
- Aufbau von Speichermodulen und ihre Arbeitsweise im System
- Standardschnittstellen für die bitserielle/parallele Ein- und Ausgabe, Microcontroller
- Graphische Bildschirme und Bildschirm-Controller
- Festplatten und Festplatten-Controller

Empfohlene Vorkenntnisse: keine

2.7 148003: Einführung in die Kryptographie und Datensicherheit I

Nummer:	148003
Lehrform:	Vorlesungen und Übungen
Medienform:	Blackboard
	Tafelanschrieb
Verantwortlicher:	Prof. Dr.-Ing. Christof Paar
Dozenten:	Prof. Dr.-Ing. Christof Paar
	M. Sc. Christian Zenger
Sprache:	Deutsch
SWS:	3
angeboten im:	

Ziele: Verständnis der wichtigsten symmetrischen Verschlüsselungsverfahren in der Praxis und Grundlagen der asymmetrischen Kryptographie. Darüberhinaus die Denkweisen der modernen Kryptographie.

Inhalt: Es werden zunächst grundlegende Begriffe der Kryptographie und Datensicherheit eingeführt. Nach der Vorstellung einiger historischer Verschlüsselungsverfahren werden Stromchiffren behandelt. Den Hauptteil der Vorlesung bilden Blockchiffren und deren Anwendung. Als bedeutender Vertreter der symmetrischen Verfahren werden der Data Encryption Standard (DES) und der Advanced Encryption Standard (AES) behandelt. Gegen Ende der Vorlesung wird das Prinzip der asymmetrische Kryptographie sowie das in der Praxis wichtiste asymmetrischer Verfahren, der RSA-Algorithmus, vorgestellt.

Neben den kryptographischen Algorithmen werden die notwendigen mathematischen Grundlagen (u.a. Ringe ganzer Zahlen, Euklidscher Algorithmus, endliche Körper) eingeführt.

Voraussetzungen: keine

Empfohlene Vorkenntnisse: Fähigkeit zum abstrakten und logischen Denken.

Literatur:

[1] Paar, Christof, Pelzl, Jan "Understanding Cryptography: A Textbook for Students and Practitioners", Springer, 2009

2.8 148006: Einführung in die Kryptographie und Datensicherheit II

Nummer:	148006
Lehrform:	Vorlesungen und Übungen
Medienform:	Blackboard
	Tafelanschrieb
Verantwortlicher:	Prof. Dr.-Ing. Christof Paar
Dozenten:	Prof. Dr.-Ing. Christof Paar
	M. Sc. Christian Zenger
Sprache:	Deutsch
SWS:	3
angeboten im:	

Ziele: Verständnis der für die Praxis wichtigsten asymmetrischen Verschlüsselungsverfahren sowie Einsatz von Krypto-Primitiven für die Realisierung von Sicherheitsdiensten.

Inhalt: Einen wichtigen Teil der Vorlesung bilden asymmetrische kryptographische Verfahren basierend auf dem diskreten Logarithmusproblem. Es werden hier der Schlüsselaustausch nach Diffie-Hellman, die Elgamal-Verschlüsselung und Verfahren mit elliptischen Kurven behandelt. Nachfolgend werden Schemata und Protokolle basierend auf symmetrischen und asymmetrischen Primitiven entwickelt. Behandelt werden: Digitale Signaturen, Message Authentication Codes (MACs), Hash-Funktionen, Zertifikate, Protokolle zum Schlüsselaustausch sowie Sicherheitsdienste.

Voraussetzungen: Keine

Empfohlene Vorkenntnisse: Stoff aus der Vorlesung Einführung in die Kryptographie I

Literatur:

[1] Paar, Christof, Pelzl, Jan "Understanding Cryptography: A Textbook for Students and Practitioners", Springer, 2009

2.9 148175: Eingebettete Prozessoren

Nummer: 148175
Lehrform: Vorlesungen und Übungen
Medienform: Tafelanschrieb
Verantwortlicher: Prof. Dr.-Ing. Tim Güneysu
Dozent: Prof. Dr.-Ing. Tim Güneysu
Sprache: Deutsch
SWS: 3
angeboten im:

Ziele:

1) Das Spektrum der Anwendungen von prozessorgestützten Schaltungen zu klassifizieren.

2) Die Entwicklung von Programmen für eingebettete Systemen mit Hilfe einer industriellen integrierten Entwicklungsumgebung (z.B. AVR Studio)

3) Assemblerprogrammierung für aktuelle Microcontroller erlernen und mit Hilfe eines Projektes auf dem Zielsystem zu üben.

4) Die Anwendungsprogrammierung in der Sprache C am gleichen Projekt zu üben und Unterschiede zur Assemblerprogrammierung herauszustellen

5) Den Blick über die geübten, konkreten, praktischen Programmierprobleme hinaus zu heben, und formale Konzepte plausibel zu machen: die Prinzipien formaler Systemmodellierung, Regeln für die Entwicklung und Validierung von Systemen mit eingebetteten Prozessoren, Verfahren des HW-SW-Codesigns.

Das Ziel ist also, die wesentlichen Kenntnisse und Fähigkeiten für den Entwurf, und die Anwendung von Schaltungen mit eingebetteten Prozessoren zu vermitteln.

Inhalt: Über die Nützlichkeit von technischen Geräten entscheidet ein Anwender durch den Vergleich ihrer Funktionen mit Blick auf einen bestimmten Zweck. Also muss ein Entwickler bzw. Hersteller versuchen, möglichst viele potentielle Anwender durch Verbesserung der Funktionen von seinem Produkt zu überzeugen. Der aktuelle Stand der Technik bietet Entwicklern integrierte Schaltungen an, die sie dabei sehr wirkungsvoll einsetzen können: die Mikroprozessoren bzw. Mikrocontroller. Diese Einheiten eignen sich wegen ihrer freien Programmierbarkeit, und ihrer signaltechnischen Anpassungsfähigkeit an unterschiedlichste Anwendungsfälle ideal dazu, als miniaturisierte Steuerzentralen in Geräten eingesetzt zu werden.

In dieser Vorlesung werden anhand eines praktischen Systems (einem ASURO-Roboter des Deutschen Zentrums für Luft- und Raumfahrt) die Möglichkeiten eines Mikrocontrollers systematisch erarbeitet und vorgestellt.

Dabei soll die theoretische Arbeit mit Hilfe von praktischen Übungen direkt am ASURO-Roboter von den Teilnehmern umgesetzt werden.

Voraussetzungen: keine

Empfohlene Vorkenntnisse:

- Grundkenntnisse Digitaltechnik
- Schaltungsentwurf
- Grundlegende Kenntnisse der Informationstechnik
- C-Programmierkenntnisse

Prüfung: schriftlich, 120 Minuten

2.10 148163: Elektronische Bauelemente

Nummer:	148163
Lehrform:	Vorlesungen und Übungen
Medienform:	rechnerbasierte Präsentation
	Tafelanschrieb
Verantwortlicher:	Prof. Dr.-Ing. Ulrich Kunze
Dozenten:	Prof. Dr.-Ing. Ulrich Kunze
	Dr.-Ing. Claudia Bock
	Dipl.-Ing. Ihor Petrov
Sprache:	Deutsch
SWS:	3
angeboten im:	

Ziele: Die Teilnehmer gewinnen einen den Einblick über den aktuellen Stand der Technik von passiven und aktiven elektronischen Bauelementen und ein Verständnis für die Grundlagen der Elektronik. Es wird ein fundiertes Verständnis der physikalischen Funktionsweise der Bauelemente, ihre Beschreibung durch Modelle und Ersatzschaltbilder in sinnvollen Näherungen sowie für die Anwendung in Grundschaltungen gewonnen.

Inhalt: Darstellung der für den Aufbau von elektronischen Schaltungen und Geräten wesentlichen Grundbausteine, ihrer Wirkungsweise, ihres Aufbaus und ihrer Grenzen. Behandlung “realer Bauelemente” der Elektronik, die im Gegensatz zu “idealen Bauelementen” in ihrer Wirkungsweise nicht nur durch einen gewünschten physikalischen Effekt, sondern durch zusätzliche (unerwünschte) physikalische Effekte beschrieben werden. Der größte Teil der Vorlesung wird dazu verwendet, ein grundlegendes Verständnis der Wirkungsweise von Halbleiterbauelementen zu vermitteln, welche die Basis für die heutige Elektronik/Mikroelektronik darstellen.

Empfohlene Vorkenntnisse: Mathematik: Differential- und Integralrechnung; Kenntnis der Vorlesungen “Grundlagen der Elektrotechnik” und “Elektronische Materialien”

Literatur:

[1] Reisch, Michael ”Halbleiter-Bauelemente, 2. Aufl.”, Springer Verlag, 2007
[2] Sze, Simon M. ”Semiconductor Devices, Physics and Technology, 2nd ed.”, Wiley & Sons, 2002
[3] Ivers-Tiffée, Ellen, von Münch, Waldemar ”Werkstoffe der Elektrotechnik, 10. Aufl.”, Teubner Verlag, 2007
[4] Seither, Hans, Zinke, Otto ”Widerstände, Kondensatoren, Spulen und ihre Werkstoffe, 2. Aufl.”, Springer Verlag, 1982

2.11 148013: Elektronische Materialien

Nummer:	148013
Lehrform:	Vorlesungen und Übungen
Medienform:	rechnerbasierte Präsentation
	Tafelanschrieb
Verantwortlicher:	Prof. Dr.-Ing. Ulrich Kunze
Dozenten:	Prof. Dr.-Ing. Ulrich Kunze
	M. Sc. Epaminondas Karaissaridis
	Dipl.-Ing. Ihor Petrov
	M. Sc. Joeren von Pock
Sprache:	Deutsch
SWS:	3
angeboten im:	

Ziele: Die Studierenden haben ein grundlegendes Verständnis über die strukturellen Eigenschaften kristalliner Materialien, die elektrischen Eigenschaften von Metallen und deren struktureller Basis sowie über die elektronischen Eigenschaften reiner und dotierter Halbleiter erlangt. Am Beispiel der pn-Diode haben sie die Einsicht in das Zusammenwirken von Feld- und Diffusionsströmen gewonnen und sind so für das Verständnis der Funktion bipolarer Bauelemente vorbereitet.

Inhalt: Die Funktion elektronischer Bauelemente gründet sich auf die Eigenschaften der Materialien, aus denen sie hergestellt werden. Was aber macht ein Material zum Leiter oder Isolator? Warum dient der Halbleiter als Grundstoff für aktive elektronische Bauelemente der Mikroelektronik? Durch die Lehrveranstaltung 'Elektronische Materialien' soll ein grundlegendes Verständnis für die elektronischen Eigenschaften von Metallen und Halbleitern erlangt werden. Dabei wird vom Zusammenhalt der festen Stoffe, der chemischen Bindung, sowie von der vielfach vorliegenden kristallinen Ordnung ausgegangen. Am Beispiel der Metalle wird ein Modell für das Zustandekommen des elektrischen Widerstands für Gleich- und Wechselströme entwickelt. Nach der Erörterung der Mischbarkeit von Metallen für Legierungen werden einige wichtige Anwendungen vorgestellt. Bei den Halbleitern wird zunächst die Energielücke eingeführt und ein Überblick der wichtigsten Materialien gegeben. Die zentralen Kapitel über reine und dotierte Halbleiter befassen sich mit den elektronischen Eigenschaften und der Möglichkeit, diese je nach Anwendung in weiten Grenzen einstellen zu können. Den Abschluss der Grundlagenbetrachtung bildet eine vertiefte Diskussion der physikalischen Mechanismen für den Stromtransport in Halbleitern. Auf dieser Basis wird schließlich ein einfaches Halbleiter-Bauelement, die pn-Diode, eingeführt und ihre Funktionsweise und Kenndaten erörtert.

Empfohlene Vorkenntnisse: Mathematik: Differential- und Integralrechnung, Grundlagen Chemie, Physik (Grundkurse gymnasiale Oberstufe), Grundlagen Elektrotechnik (1. Sem.)

Prüfung: schriftlich, 120 Minuten

Literatur:

[1] von Münch, Waldemar "Einführung in die Halbleitertechnologie", Teubner Verlag, 1998
[2] Ivers-Tiffee, Ellen, von Münch, Waldemar "Werkstoffe der Elektrotechnik", Teubner Verlag, 2007

2.12 148177: Elektronische Schaltungen

Nummer:	148177
Lehrform:	Vorlesungen und Übungen
Medienform:	Folien
	Tafelanschrieb
Verantwortlicher:	Prof. Dr.-Ing. Thomas Musch
Dozenten:	Prof. Dr.-Ing. Thomas Musch
	M. Sc. Patrik Gebhardt
Sprache:	Deutsch
SWS:	4
angeboten im:	

Ziele: Die Vorlesung verfolgt das Ziel, die Studierenden mit den grundlegenden Aspekten der strukturierten Analyse elektronischer Schaltungen bekannt zu machen. Diese sind für das Verständnis komplexerer Schaltungen notwendig, und bilden die Basis für die Lösung elektronischer Aufgabenstellung und die Synthese von elektronischen Schaltungen.

Inhalt: Die Vorlesung 'Elektronische Schaltungen' vermittelt die Grundlagen der Schaltungstechnik mit elektronischen Bauelementen. Ausgehend von den Eigenschaften diskreter passiver und aktiver Elemente wird für steigende Schaltungskomplexität das Übertragungsverhalten analytisch ermittelt, eine vereinfachte Beschreibung abgeleitet und deren Gültigkeit mit Hilfe von CAD-Verfahren bestimmt. Großsignal- und Kleinsignaleigenschaften mit den Ersatzschaltungen werden behandelt, sowie auf die Einflüsse von Mit- und Gegenkopplung eingegangen. Die Struktur grundlegender Schaltungen wie Operationsverstärker, Endstufen, Oszillatoren und Komparatoren wird erarbeitet, und die Eigenschaften kommerzieller Bauelemente diskutiert. Weiterhin erfolgt eine Einführung das thermische Verhalten von Schaltungen und in elementare digitale Schaltungen.

- Einführung
- Halbleiterbauelemente, Temperatureinfluss, Großsignal- und Kleinsignalverhalten
- Transistorgrundschaltungen
- Arbeitspunkteinstellung und Temperaturstabilität
- Erweiterte Grundschaltungen, Differenzverstärker, Stromspiegel, Ausgangsstufen
- Rückgekoppelte Schaltungen, Mit- und Gegenkopplung
- Operationsverstärker, Oszillatoren, Komparatoren
- Stromversorgungs-Schaltungen, lineare und geschaltete Leistungsendstufen

- Wärmeabfuhr und thermische Ersatzschaltung
- Elementare Digitalschaltungen
- CAD-Verfahren zur Schaltungssimulation

Empfohlene Vorkenntnisse: Inhalte der Vorlesung “Elektronische Bauelemente”

Literatur:

[1] Kim, Ernest M., Schubert, Thomas F. ”Active and Non-Linear Electronics”, Wiley & Sons, 1996
[2] Seifart, Manfred ”Analoge Schaltungen”, Hüthig, 1989
[3] Gray, Paul R., Meyer, Robert G. ”Analysis and Design of Analog Integrated Circuits”, Wiley/VCH, Weinheim, 1993
[4] Kamins, Theodore I., Muller, Richard S. ”Device Electronics for Integrated Circuits”, Wiley & Sons, 1986
[5] Gamm, Eberhard, Schenk, Christoph, Tietze, Ulrich ”Halbleiter - Schaltungstechnik”, Springer, 2002
[6] Antognetti, Paolo, Massobrio, Giuseppe ”Semiconductor Device Modelling with SPICE”, McGraw-Hill Professional, 1993
[7] Hoefer, E., Nielinger, H. ”SPICE - Analyseprogramm für elektronische Schaltungen”, Springer, 1985

2.13 148066: Energietechnische Aspekte der Informationstechnik

Nummer:	148066
Lehrform:	Vorlesung mit integrierten Übungen
Medienform:	rechnerbasierte Präsentation
Verantwortlicher:	Prof. Dr.-Ing. Constantinos Sourkounis
Dozent:	Prof. Dr.-Ing. Constantinos Sourkounis
Sprache:	Deutsch
SWS:	3
angeboten im:	

Ziele: Die Vorlesung soll dazu dienen, den Studierenden ein Grundwissen und einen Wortschatz zu vermitteln, mit dem sie mit Energieversorgungsexperten zusammenarbeiten können.

Inhalt: Inhalt ist neben den Grundlagen die elektrische Energieversorgung, die Rechnerenergieversorgung, die Anwendung energietechnischer Systeme sowie die Informationsübertragung und -verarbeitung in der Energietechnik.

Voraussetzungen: keine

Empfohlene Vorkenntnisse: keine

2.14 148007: Grundlagen der Elektrotechnik I

Nummer:	148007
Lehrform:	Vorlesungen und Übungen
Medienform:	Blackboard
	Folien
	Tafelanschrieb
Verantwortlicher:	Prof. Dr.-Ing. Peter Awakowicz
Dozenten:	Prof. Dr.-Ing. Peter Awakowicz
	Dipl.-Ing. Andre Bergner
	Dipl.-Ing. Benjamin Denis
	Dr.-Ing. Ralf Hereth
	Dipl.-Math. Björn Offerhaus
	Dr.-Ing. Gerhard Roll
	Dipl.-Ing. Cornelia Ruhrmann
	Dipl.-Ing. Tim Styrnoll
Sprache:	Deutsch
SWS:	4
angeboten im:	

Ziele: Die Studierenden haben eiune grundlegende Vorstellung von elektrischen Quellenfeldern und dem elektrischen Strömungsfeld. Sie sind in der Lage, dazu einfache Aufgabenstellungen rechnerisch zu bearbeiten. Dies ist die Basis für die Vorlesung "Grundlagen der Elektrotechnik II", deren Ziel das grundlegende Verständnis der vollständigen Maxwellsche Theorie in Integralform, sowie einiger einfacher Anwendungen dieser Theorie ist.

Inhalt: Inhalt der Vorlesung ist die Maxwellsche Theorie in Integralform, wobei der Schwerpunkt in dieser Vorlesung auf dem elektrischen Feld und dem elektrischen Strömungsfeld liegt. Die Vorlesung besitzt die folgende Gliederung:

- Das elektrostatische Feld: Elektrische Feldstärke; elektrische Flussdichte; elektrisches Potential; die Kapazität; Energie und Kräfte im elektostatischen Feld; Materie im elektrischen Feld
- Der elektrische Strom: Stromdichte und Stromstärke; ohmsches Gesetz; Strömungsfelder; Energieumsetzung im elektrischen Stromkreis
- Gleichstromschaltungen: Strom und Spannungen im einfachen Stromkreis; Zweipole; Zusammenschaltung von Zweipolen; die Kirchhoffschen Regeln
- Das magnetische Feld: Magnetische Flussdichte; magnetische Erregung; Lorentz-Kraft; Durchflutungsgesetz

Voraussetzungen: keine

Empfohlene Vorkenntnisse: Notwendig sind Kenntnisse über die Grundlagen der Differential-, Integral- und Vektorrechnung, wie sie im Mathematikunterricht im Grundkurs der gymnasiale Oberstufe unterrichtet werden.

Prüfung: schriftlich, 60 Minuten

Literatur:

[1] Pregla, Reinhold "Grundlagen der Elektrotechnik", Hüthig, 2009
[2] Albach, Manfred "Grundlagen der Elektrotechnik 1. Erfahrungssätze, Bauelemente, Gleichstromschaltungen", Pearson Studium, 2004

2.15 148008: Grundlagen der Elektrotechnik II

Nummer:	148008
Lehrform:	Vorlesungen und Übungen
Medienform:	Blackboard
	Folien
	Tafelanschrieb
Verantwortlicher:	Prof. Dr.-Ing. Peter Awakowicz
Dozenten:	Prof. Dr.-Ing. Peter Awakowicz
	Dipl.-Ing. Andre Bergner
	Dipl.-Math. Björn Offerhaus
	Dr.-Ing. Gerhard Roll
	Dipl.-Ing. Cornelia Ruhrmann
	Dipl.-Ing. Tim Styrnoll
Sprache:	Deutsch
SWS:	3
angeboten im:	

Ziele: Die Studierenden haben ein grundlegendes Verständnis der Maxwellsche Theorie in Integralform, sowie einiger einfacher Anwendungen dieser Theorie. Sie sind in der Lage, einfache Aufgabenstellungen dazu rechnerische zu bearbeiten. Die Maxwellsche Theorie beschreibt alle makroskopischen, elektromagnetischen Erscheinungen. Ihre Kenntnis wird in zahlreichen Lehrveranstaltungen im weiteren Studienverlauf vorausgesetzt.

Inhalt: Inhalt der Vorlesung ist die Maxwellsche Theorie in Integralform, wobei der Schwerpunkt in dieser Vorlesung auf dem magnetischen Feld und Induktionsvorgängen liegt. Die Vorlesung besitzt die folgende Gliederung:

- Das magnetische Feld (Fortsetzung aus der Vorlesung 'Grundlagen der Elektrotechnik I'): Die magnetischen Eigenschaften der Materie; magnetische Kreise; Anwendungen der magnetischen Kraftwirkung
- Die elektromagnetische Induktion: Bewegungsinduktion; Transformationsinduktion; Induktionsgesetz; Selbst- und Gegeninduktion; Berechnung von Induktivitäten; Energie im magnetischen Feld; Wirbelströme und Stromverdrängung
- Der Transformator: Der ideale Transformator; Ersatzschaltungen für den realen Transformnator; Einsatzbereiche von Transformatoren

Voraussetzungen: keine

Empfohlene Vorkenntnisse: Die Vorlesung baut auf dem Stoff der Vorlesung "Grundlagen der Elektrotechnik I" auf.

Prüfung: schriftlich, 60 Minuten

Literatur:

[1] Pregla, Reinhold "Grundlagen der Elektrotechnik", Hüthig, 2009
[2] Albach, Manfred "Grundlagen der Elektrotechnik 1. Erfahrungssätze, Bauelemente, Gleichstromschaltungen", Pearson Studium, 2004

2.16 148001: Grundlagen der Informatik I

Nummer:	148001
Lehrform:	Vorlesung und Praxisübungen
Medienform:	e-learning rechnerbasierte Präsentation
Verantwortlicher:	Prof. Dr.-Ing. Helmut Balzert
Dozenten:	Prof. Dr.-Ing. Helmut Balzert M. Sc. Michael Goll
Sprache:	Deutsch
SWS:	3
angeboten im:	

Ziele: Globales Ziel dieser Veranstaltung ist es, einen systematischen Überblick über Prinzipien, Methoden, Konzepte und Notationen des "Programmierens im Kleinen", und seine Einordnung in die verschiedenen Kontexte zu geben. Dieses Wissen - verbunden mit den praktischen Übungen am Computersystem - soll den Studierenden befähigen, professionell effiziente Programme problemgerecht zu entwickeln, zu analysieren, zu überprüfen, adäquat in der UML (Unified Modeling Language) zu beschreiben und in die Programmiersprache Java zu transformieren, zu übersetzen und auszuführen.

Inhalt:

- Basiskonzepte
  - Variablen, Konstanten, einfache Typen
  - Zuweisung, Ausdrücke
  - Anweisungen, Konsolen-E/A
  - Einfaches Testen
- Kontrollstrukturen
  - Sequenz
  - Auswahl
  - Wiederholung
  - Schachtelung
  - Ausnahmebehandlung
- Mehrfachverwendung
  - Prozeduren
  - Funktionen
  - Rekursion
- Basiskonzepte der Objektorientierung
  - Objekte

- Klassen
- Konstruktoren
- Generalisierung
- Vererbung

Voraussetzungen: Keine.

Empfohlene Vorkenntnisse: Fähigkeit zum abstrakten und logischen Denken; Fähigkeit, dynamische Abläufe zu verstehen und zu konzipieren.

Literatur:

[1] Balzert, Helmut "Java: Einstieg in die Programmierung, 3. Auflage", W3l, 2010
[2] Balzert, Helmut "Java:Objektorientiert programmieren, 2. Auflage", W3l, 2010

2.17 148005: Grundlagen der Informatik II

Nummer:	148005
Lehrform:	Vorlesung und Praxisübungen
Medienform:	rechnerbasierte Präsentation
Verantwortlicher:	Prof. Dr.-Ing. Helmut Balzert
Dozenten:	Prof. Dr.-Ing. Helmut Balzert M. Sc. Michael Goll
Sprache:	Deutsch
SWS:	3
angeboten im:	

Ziele: Globales Ziel dieser Veranstaltung ist es, einen systematischen Überblick über Prinzipien, Methoden, Konzepte und Notationen des "Programmierens im Kleinen", und seine Einordnung in die verschiedenen Kontexte zu geben. Dieses Wissen - verbunden mit den praktischen Übungen am Computersystem - soll den Studierenden befähigen, professionell effiziente Programme problemgerecht zu entwickeln, zu analysieren, zu überprüfen, adäquat in der UML (Unified Modeling Language) zu beschreiben und in die Programmiersprache Java zu transformieren, zu übersetzen und auszuführen.

Inhalt:

- Basiskonzepte der Objektorientierung
  - Polymorphismus
  - Schnittstellen
  - Assoziationen
  - Assoziationen und Referenzen
  - Mehrere Klassen
  - Containerklassen
  - GUI-Klassen
  - Speicherklassen
- GUI-Programmierung
  - GUI (AWT)
  - Ereignisverarbeitung
- Grafikprogrammierung
  - GUI (Swing)
  - Dialog- und E/A-Gestaltung
  - DB-Anbindung
  - Tabellen und SQL
  - JDBC
  - Drei-Schichten-Modell

- Applet-Programmierung
  - HTML und CSS
  - Applet vs. Anwendung
- Algorithmen und Datenstrukturen
  - Listen
  - Bäume

Voraussetzungen: Keine.

Empfohlene Vorkenntnisse: Grundlagen der Informatik 1

Literatur:

[1] Balzert, Helmut, Priemer, Jürgen "Java: Anwendungen programmieren, 2. Auflage", W3l, 2010
[2] Balzert, Helmut "Java:Objektorientiert programmieren, 2. Auflage", W3l, 2010

2.18 148009: Grundlagen der Informationstechnik I

Nummer:	148009
Lehrform:	Vorlesungen und Übungen
Medienform:	rechnerbasierte Präsentation
Verantwortlicher:	Prof. Dr.-Ing. Rainer Martin
Dozenten:	Prof. Dr.-Ing. Rainer Martin wiss. Mitarbeiter
Sprache:	Deutsch
SWS:	4
angeboten im:	

Ziele: Ziel dieser Vorlesung ist die Vermittlung der Struktur und Funktionsweise informationstechnischer Systeme, sowie typischer Berechnungsverfahren. Unter anderem wird die Fähigkeit zur Berechnung der zur Übertragung eines digitalen Signals erforderlichen Datenrate, des mittleren Informationsgehaltes eines Signals, der Übertragungskapazität eines Kanals, optimaler Quellencodes, und einfacher fehlerkorrigierender Codes erworben. Die Befähigung zum selbstständigen Rechnen von Übungsaufgaben ist dabei ein wesentliches Qualifikationsziel der Lehrveranstaltung.

Inhalt: In vielen informationstechnischen Anwendungen (Telefonie, Mobilfunk, Fernsehen etc.) werden Informationen aus physikalischen Signalen gewonnen, verarbeitet und übertragen. Es kann sich dabei um akustische Signale (Sprache, Musik), Bild- und Videosignale, oder auch medizinische Signale (EKG, EEG) handeln. Sofern die Signale nicht-elektrischer Natur sind, werden sie in aller Regel vor einer weiteren Verarbeitung mit Hilfe von Sensoren in elektrische Signale umgewandelt. Analoge und digitale elektronische Geräte spielen daher bei der Verarbeitung und Übertragung informationstragender Signale eine überragende Rolle.

In der Vorlesung Grundlagen der Informationstechnik I werden die Grundbegriffe informationstechnischer Systeme vorgestellt und anhand aktueller Anwendungen diskutiert. Die Beschreibung und die Eigenschaften analoger, diskreter und digitaler Signale stehen dabei im Mittelpunkt. Informationstheoretische Überlegungen führen schließlich zur Bestimmung des mittleren Informationsgehalts dieser Signale und zu optimalen Codierverfahren.

Empfohlene Vorkenntnisse:

- Solide Kenntnisse der Schulmathematik
- Bereitschaft zur aktiven Mitarbeit in der Vorlesung und in den Übungsgruppen

Literatur:

[1] Pierce, John R. "An Introduction to Information Theory", Dover Publications Inc., 1980
[2] M. Bossert, , T. Frey, "Signal- und Systemtheorie, 2. Auflage", Vieweg Verlag, 2008

2.19 148010: Grundlagen der Informationstechnik II

Nummer:	148010
Lehrform:	Vorlesungen und Übungen
Medienform:	rechnerbasierte Präsentation
Verantwortlicher:	Prof. Dr.-Ing. Rainer Martin
Dozenten:	Prof. Dr.-Ing. Herbert Hudde
	wiss. Mitarbeiter
Sprache:	Deutsch
SWS:	3
angeboten im:	

Ziele: Ziel dieser Vorlesung ist die Vermittlung der elektronischen Grundlagen informationstechnischer Systeme, sowie typischer Berechnungsverfahren. Unter anderem wird die Fähigkeit zur Analyse und Berechnung linearer Wechselstromnetzwerke und zur Berechnung von Frequenzgängen linearer RLC-Zweitornetzwerke erworben. Die Befähigung zum selbstständigen Rechnen von Übungsaufgaben ist dabei ein wesentliches Qualifikationsziel der Lehrveranstaltung.

Inhalt: In vielen informationstechnischen Anwendungen (Telefonie, Mobilfunk, Fernsehen etc.) werden Informationen aus physikalischen Signalen gewonnen, verarbeitet und übertragen. Es kann sich dabei um akustische Signale (Sprache, Musik), Bild- und Videosignale, oder auch medizinische Signale (EKG, EEG) handeln. Sofern die Signale nicht-elektrischer Natur sind, werden sie in aller Regel vor einer weiteren Verarbeitung in elektrische Signale umgewandelt. Analoge und digitale elektronische Geräte spielen daher bei der Verarbeitung und Übertragung informationstragender Signale eine überragende Rolle. Der erste Teil dieser Vorlesung behandelt die Grundlagen linearer elektrischer Netzwerke. Dabei sind insbesondere sinusförmige (harmonische) Ströme und Spannungen als Anregungssignale von Interesse. Die “Komplexe Wechselstromrechnung” wird als mathematisch elegantes Werkzeug zur Berechnung dieser Netzwerke im eingeschwungenen Zustand eingeführt.Im zweiten Teil der Vorlesung Grundlagen der Informationstechnik II stehen Berechnungsverfahren für Netzwerke, die aus ohmschen Widerständen, idealen Kondensatoren, Spulen und Quellen zusammengesetzt sind, im Mittelpunkt. Es werden Tiefpass-, Hochpass- und Bandpassfilter eingeführt und deren Verhalten als Funktion der Frequenz berechnet.

Empfohlene Vorkenntnisse: Mathematik I

Prüfung: schriftlich, 90 Minuten

Literatur:

[1] Pregla, Reinhold "Grundlagen der Elektrotechnik", Hüthig, 2009

2.20 148000: Mathematik I

Nummer: 148000
Lehrform: Vorlesungen und Übungen
Medienform: Tafelanschrieb
Verantwortlicher: Dekan
Dozent: Dr. rer. nat. Mario Lipinski
Sprache: Deutsch
SWS: 8
angeboten im:

Ziele: Verstehen und Anwenden mathematischer Methoden zur Lösung ingenieurwissenschaftlicher Probleme.

Inhalt: Zunächst werden wichtige Eigenschaften reeller und komplexer Zahlen behandelt. Danach geht es um elementare Eigenschaften der linearen Algebra: Vektoren, Matrizen, Determinanten, Eigenwerte und Eigenvektoren. Der größte Teil der Vorlesung beschäftigt sich mit der Differential- und Integralrechnung für Funktionen von einer Veränderlichen: Konvergenz von Folgen und Reihen, elementare Funktionen, Potenzreihen, Grenzwerte, Stetigkeit, Differenzierbarkeit, Integralrechnung. Zum Schluss werden einfache gewöhnliche Differentialgleichungen, die in den Grundlagen der Elektrotechnik vorkommen, behandelt.

Empfohlene Vorkenntnisse: Gute Kenntnisse der Mathematik aus der Oberstufe. Empfohlen wird außerdem die Teilnahme am 4-wöchigen Vorkurs “Mathematik für Ingenieure und Naturwissenschaftler”, den die Fakultät für Mathematik vor Studienbeginn jeweils im September anbietet.

Literatur:

[1] Meyberg, K., Vachenauer, P. ”Höhere Mathematik 2”, Springer, 2007
[2] Burg, Klemens, Haf, Herbert, Wille, Friedrich ”Höhere Mathematik für Ingenieure 3. Gewöhnliche Differentialgleichungen, Distributionen, Integraltransformationen”, Teubner Verlag, 2002
[3] Meyberg, K., Vachenauer, P. ”Höhere Mathematik I”, Springer, 1995

2.21 148004: Mathematik II

Nummer: 148004
Lehrform: Vorlesungen und Übungen
Medienform: Tafelanschrieb
Verantwortlicher: Dr. rer. nat. Mario Lipinski
Dozent: Dr. rer. nat. Mario Lipinski
Sprache: Deutsch
SWS: 6
angeboten im:

Ziele: Verstehen und Anwenden mathematischer Methoden zur Lösung ingenieurwissenschaftlicher Probleme.

Inhalt: Das erste Kapitel behandelt die Differenzialrechnung für Funktionen von mehreren Variablen. Im zweiten Kapitel geht es um Orthonormalsysteme, insbesondere Fourierreihen. Das nächste Kapitel behandelt die Integralrechnung für Funktionen von mehreren Variablen, insbesondere Volumenintegrale, Kurvenintegrale, Flächenintegrale, und die für die Anwendung wichtigen Integralsätze. Im letzten Kapitel geht es um Eigenschaften der Laplace- und Fouriertransformation, die wichtige Hilfsmittel der Elektrotechnik sind.

Empfohlene Vorkenntnisse: Mathematik I

Literatur:

[1] Meyberg, K., Vachenauer, P. "Höhere Mathematik 2", Springer, 2007
[2] Burg, Klemens, Haf, Herbert, Wille, Friedrich "Höhere Mathematik für Ingenieure 3. Gewöhnliche Differentialgleichungen, Distributionen, Integraltransformationen", Teubner Verlag, 2002
[3] Meyberg, K., Vachenauer, P. "Höhere Mathematik I", Springer, 1995

2.22 148161: Netzsicherheit I

Nummer:	148161
Lehrform:	Vorlesungen und Übungen
Medienform:	rechnerbasierte Präsentation
Verantwortlicher:	Prof. Dr. Jörg Schwenk
Dozenten:	Prof. Dr. Jörg Schwenk
	Dr.-Ing. Christoph Bader
	Dr.-Ing. Florian Bergsma
	M. Sc. Matthias Horst
Sprache:	Deutsch
SWS:	3
angeboten im:	

Ziele: Verständnis aller technischen Aspekte der Netzsicherheit. Es soll klar werden, dass Kryptographie allein nicht ausreicht. Organisatorische Aspekte der Sicherheit werden nur kurz behandelt. Eigenständige Überlegungen zur Verbesserung der Sicherheit sollen die Studierenden auf ihre Rolle im Berufsleben vorbereiten.

Inhalt: Kryptographie wird eingesetzt, um die Vertraulichkeit und Integrität von Daten zu schützen, die über Datennetze übertragen werden. Hierbei werden sowohl symmetrische Verfahren (Pay-TV, Mobil-funk, WLAN), als auch asymmetrische bzw. hybride Verfahren (E-Mail, WWW, VPN) eingesetzt. In der Vorlesung werden konkrete kryptographische Systeme zur Absicherung von Netzen betrachtet, und von allen Seiten auf ihre Sicherheit hin beleuchtet. Dies umfasst folgende Themen:

- Broadcast Encryption (Pay-TV-Systeme, DVD-Verschlüsselung),
- Mobilfunk (GSM, UMTS),
- WLAN (IEEE 802.11),
- Firewalls, IDS, Malware,
- Web Services (XML Security, Microsoft Passport, WS-Security).

Neben den Systemen selbst werden dabei auch publizierte Angriffe auf diese Systeme besprochen; die Studenten werden aufgefordert, selbst wissenschaftliche Überlegungen zur Verbesserung der Sicherheit anzustellen.

Empfohlene Vorkenntnisse: Grundkenntnisse in TCP/IP, Grundkenntnisse der Sicherheitsprobleme von Computernetzen auf dem Niveau populärer Fachzeitschriften (z.B. c't).

Literatur:

[1] Schwenk, Jörg "Sicherheit und Kryptographie im Internet", Vieweg, 2014

2.23 148187: Netzsicherheit II

Nummer:	148187
Lehrform:	Vorlesungen und Übungen
Medienform:	rechnerbasierte Präsentation
Verantwortlicher:	Prof. Dr. Jörg Schwenk
Dozenten:	Prof. Dr. Jörg Schwenk
	M. Sc. Matthias Horst
	Dr.-Ing. Yong Li
Sprache:	Deutsch
SWS:	3
angeboten im:	

Ziele: Verständnis aller technischen Aspekte von Netzsicherheit. Es soll klar werden, dass Kryptographie allein nicht ausreicht. Organisatorische Aspekte der Sicherheit werden nur kurz behandelt. Eigenständige Überlegungen zur Verbesserung der Sicherheit sollen die Studierenden auf ihre Rolle im Berufsleben vorbereiten.

Inhalt: Kryptographie wird eingesetzt, um die Vertraulichkeit und Integrität von Daten zu schützen, die über Datennetze übertragen werden. Hierbei werden sowohl symmetrische Verfahren (Pay-TV, Mobil-funk, WLAN), als auch asymmetrische bzw. hybride Verfahren (E-Mail, WWW, VPN) eingesetzt. In der Vorlesung werden konkrete kryptographische Systeme zur Absicherung von Netzen betrachtet, und von allen Seiten auf ihre Sicherheit hin beleuchtet. Dies umfasst folgende Themen:

- OpenPGP,
- S/MIME,
- SSL,
- DNSSEC,
- VPN (IPSec, PPTP, IP Multicast),
- Web Services (XML Security, Microsoft Passport, WS-Security).

Neben den Systemen selbst werden dabei auch publizierte Angriffe auf diese Systeme besprochen; die Studenten werden aufgefordert, selbst wissenschaftliche Überlegungen zur Verbesserung der Sicherheit anzustellen.

Empfohlene Vorkenntnisse: Grundkenntnisse in TCP/IP, Grundkenntnisse der Sicherheitsprobleme von Computernetzen auf dem Niveau populärer Fachzeitschriften (z.B. c't).

Literatur:

[1] Schwenk, Jörg "Sicherheit und Kryptographie im Internet", Vieweg, 2014

2.24 148002: Programmieren in C

Nummer: 148002
Lehrform: Vorlesungen und Übungen
Medienform: Blackboard
rechnerbasierte Präsentation
Verantwortlicher: Dekan
Dozent: Dipl.-Math. Reinhard Mares
Sprache: Deutsch
SWS: 3
angeboten im:

Ziele: Die Vorlesung verfolgt im wesentlichen die folgenden zwei Lernziele:

- Vermittlung der grundlegenden Sprachkonstrukte von C mit Betonung der prozeduralen Betrachtungsweise.
- Vermittlung eines Verständnisses für die Sicherheitsproblematik von C.

Inhalt: Von der Maschinensprache zu C. Als zweite Programmiersprache (nach Java in den Grundlagen der Informatik) soll hier die Sprache ANSI-C (nicht C++) eingeführt werden. C eignet sich insbesondere dazu, hardwarenah zu programmieren. Darüber hinaus findet sich die Syntax von C in vielen anderen Sprachen (z.B. der PHP-Skriptsprache) in ähnlicher Form wieder. Behandelt werden:

- Die Struktur von C-Programmen
- Variablen und Datentypen in C
- Bildschirm Ein-/Ausgabe
- Kontrollstrukturen
- Funktionen
- Programmierstil, Programmierrichtlinien
- Felder und Zeichenketten
- Ausdrücke
- Arbeiten mit Dateien
- Strukturen, Aufzählungstypen
- Zeiger
- Speicherklassen
- Vertiefung einiger Themen

Empfohlene Vorkenntnisse: Grundzüge der Programmierung