RUHR-UNIVERSITÄT BOCHUM

RUB

Bachelorstudiengang IT-Sicherheit / Informationstechnik PO 13

Modulhandbuch

Fakultät für Elektrotechnik und Informationstechnik

Inhaltsverzeichnis

Kapitel 1

Module

1.1 Allgemeine Elektrotechnik 1

Nummer: 149125
Verantwortlicher: Prof. Dr.-Ing. Ilona Rolfes
Arbeitsaufwand: 150 Stunden (entsprechend der Lehrveranstaltungen)
Leistungspunkte: 5

Veranstaltungen:

141130: Allgemeine Elektrotechnik 1 - Elektrische Netzwerke 4 SWS (S.46)

Ziele: Die Studierenden beherrschen die Grundlagen und Gesetze zur Berechnung von Strömen und Spannungen in elektrischen Gleich- und Wechselstromkreisen. Sie haben die Fähigkeit, elektrische Netzwerke zu analysieren, mathematisch korrekt zu beschreiben und umzuwandeln. Sie haben die Grundlagen der komplexen Wechselstromrechnung verstanden und können diese auf praktische Beispiele anwenden.

Inhalt: Das Modul bietet einen allgemeinen Einstieg in die Grundlagen der elektrischen Netzwerke. Es werden grundlegende Begriffe und Verfahren erläutert.

Die Vorlesung lässt sich in fünf Teile gliedern:

- Lineare Gleichstromschaltungen: Zählpfeile; Strom- und Spannungsquellen; Die Kirchhoffschen Gleichungen; einfache Widerstandsnetzwerke (Spannungsteiler, Stromteiler); reale Strom- und Spannungsquellen; Wechselwirkungen zwischen Quelle und Verbraucher (Zusammenschaltung von Spannungsquellen, Leistungsanpassung, Wirkungsgrad); Superpositionsprinzip; Analyse umfangreicher Netzwerke.
- Übergang zu zeitabhängigen Strom und Spannungsformen: Übersicht sowie Einführung verschiedener Kenngrößen (Mittelwert, Gleichrichtwert, Effektivwert, Maximalwert, Spitzenwert, Spitze-Spitze-Wert, Schwingungsbreite).
- Wechselstrom und Wechselspannung: Das Zeigerdiagramm; Komplexe Wechselstromrechnung; Beschreibung konzentrierter RLC Bauelemente und idealer Quellen; Einführung der Ortskurven; Berechnung einfacher Wechselstromkreise über die komplexe Ebene; Energie und Leistung bei Wechselspannung; Leistungsanpassung.
- Analyse von Netzwerken: Maschenstromverfahren; Knotenpotenzialverfahren.
- Einführung zu Zweitoren: Torbedingung; Zweitorgleichungen in Matrixform (Impedanz-, Admittanz-, Hybrid-, Kettenform); Zweitoreigenschaften (Reziprozität, Symmetrie); Matrizen elementarer Zweitore.

Prüfungsform: siehe Lehrveranstaltungen

Stellenwert der Note für die Endnote: 5 / 143

1.2 Bachelorarbeit und Kolloquium

Nummer: 149885
Verantwortlicher: Studiendekan ITS
Arbeitsaufwand: 450 Stunden (entsprechend der Lehrveranstaltungen)
Leistungspunkte: 15
Semester: 6. Semester (BaITS/I)
Dauer: 3 Monate

Veranstaltungen:

144002: Bachelorarbeit ITS (S.76)
144004: Kolloquium ITS (S.112)

Ziele: Die Studierenden beherrschen die Grundkenntnisse der wissenschaftlichen Arbeit, der Projektorganisation und der Präsentation wissenschaftlicher Ergebnisse.

Inhalt: Lösung einer wissenschaftlichen Aufgabe unter Anleitung. Teilnahme an 5 Kolloquiumsvorträgen über die Ergebnisse von Bachelorarbeiten in der Fakultät ET & IT. Präsentation der eigenen Ergebnisse der Bachelorarbeit im Kolloquium.

Prüfungsform: Abschlussarbeit und Kolloquiumsvortrag

Voraussetzungen für die Vergabe von Kreditpunkten: Erfolgreiches Bestehen der Abschlussarbeit und des Kolloquiumsvortrags.

Verwendung des Moduls (in anderen Studiengängen): Bachelor IT-Sicherheit/Informationstechnik

Stellenwert der Note für die Endnote: 15 / 143

1.3 Betriebssysteme

Nummer: 149242
Verantwortlicher: Prof. Dr. Thorsten Holz
Arbeitsaufwand: 150 Stunden (entsprechend der Lehrveranstaltungen)
Leistungspunkte: 5
Semester: 4. Semester (BaITS/I)
Dauer: 1 Semester

Veranstaltungen:

141246: Betriebssysteme 4 SWS (S.77)

Ziele: Die Studierenden erlangen ein solides Grundverständnis von modernen Betriebssystemen, ihrer Funktion und ihrer Implementierung. Die Studierenden sind nach Abschluss des Moduls in der Lage, verschiedene Aspekte eines Betriebssystems wie Prozess- und Speichermanagement zu verstehen und zu nutzen, sie können dabei verschiedene Designentscheidungen eigenständig analysieren und bewerten. Sie sind in der Lage, bestimmte Aspekte eines Betriebssystems selbst zu designen und diese argumentativ zu verteidigen.

Inhalt: Es werden die wichtigsten Grundlagen zu Betriebssystemen vorgestellt. Dazu gehören zum Beispiel:

- Betriebssystemkonzepte
- Prozesse und Threads, Interprozesskommunikation
- Scheduling-Mechanismen
- Speicherverwaltung, Speicherabstraktionen, Paging
- Dateisysteme
- Eingabe- und Ausgabeverwaltung
- Algorithmen zur Vermeidung von Deadlocks

Ergänzend zur Vorlesung werden Übungsaufgaben gestellt und in der Übungsstunde besprochen. Um den Bezug zu modernen Betriebssystemen (aktuellen Versionen von Linux, Windows, und macOS) herzustellen, werden die Themen an praktischen Beispielen illustriert. Dies ermöglicht es den Studierenden, die in der Vorlesung besprochenen Themen praktisch nachzuvollziehen.

Prüfungsform: Klausurarbeit (120 Minuten)

Voraussetzungen für die Vergabe von Kreditpunkten: Erfolgreiches Bestehen der Modulklausur.

Verwendung des Moduls (in anderen Studiengängen): Bachelor IT-Sicherheit/Informationstechnik, Bachelor Angewandte Informatik, Bachelor Informatik

Stellenwert der Note für die Endnote: 5 / 143

1.4 Computernetze

Nummer: 149145
Verantwortlicher: Prof. Dr. Jörg Schwenk
Arbeitsaufwand: 150 Stunden (entsprechend der Lehrveranstaltungen)
Leistungspunkte: 5
Semester: 2. Semester (BaITS/I)
Dauer: 1 Semester

Veranstaltungen:

141250: Computernetze 4 SWS (S.80)

Ziele:

Nach dem erfolgreichen Abschluss des Moduls

- kennen Studierende die wichtigsten Standards, die das heutige Internet verwendet.
- kennen Studierende grundlegende Angriffskonzepte auf Computernetzwerke
- verstehen Studierende den Zusammenhang zwischen den einzelnen Schichten eines Computernetzwerks und der darin enthaltenen Protokolle
- können Studierende die wichtigsten Netzwerktools für Analysezwecke anwenden

Inhalt: Das Modul gibt eine Einführung in grundlegenden Protokolle und Anwendungen von Computernetzen. Der Schwerpunkt der Vorlesung liegt auf Standardprotokollen und -Algorithmen, wie sie in modernen Computernetzwerken (zum Beispiel im Internet) eingesetzt werden.

Anhand eines Schichtenmodells werden die wichtigsten Grundlagen nach dem Top-Down Ansatz vorgestellt und analysiert. Dazu gehören zum Beispiel auf der obersten Schicht DNS und HTTPS im Application Layer; TCP und UDP im Transport Layer; IPv4/IPv6 und Routing Algorithmen im Network Layer; sowie MAC und ARP im untersten Link Layer. Neben der reinen Funktionsweise dieser Standards werden Sicherheitsaspekte auf allen Schichten betrachtet.

Ergänzend zur Vorlesung werden Übungsaufgaben über die eLearning Plattform Moodle gestellt und in der Übungsstunde besprochen. Weiterhin wird in jeder Übung ein "Tool der Woche" vorgestellt. Dabei handelt es sich jeweils um eine spezielle Software, die man als "Netzwerker" unbedingt kennen sollte (z.B. traceroute, nmap, ...). Alle besprochenen Tools sind frei verfügbar und werden den Studenten als eine Lernplattform (virtuelle Maschine) zur Verfügung gestellt.

Als Primärliteratur wird "Computernetzwerke: Der Top-Down Ansatz" von Kurose und Ross (Pearson Verlag) verwendet.

Prüfungsform: Klausurarbeit (120 Minuten)

Voraussetzungen für die Vergabe von Kreditpunkten: Erfolgreiches Bestehen der Modulklausur.

Verwendung des Moduls (in anderen Studiengängen): Bachelor IT-Sicherheit/Informationstechnik, Bachelor Angewandte Informatik, Bachelor Informatik

Stellenwert der Note für die Endnote: 5 / 143

1.5 Diskrete Mathematik

Nummer: 149873
Verantwortlicher: Priv.-Doz. Dr. Björn Schuster
Arbeitsaufwand: 240 Stunden (entsprechend der Lehrveranstaltungen)
Leistungspunkte: 8
Semester: 1. Semester (MaITS/N)
Dauer: 1 Semester

Veranstaltungen:

150308: Diskrete Mathematik 6 SWS (S.86)

Ziele: Ein allgemeines Lernziel ist der professionelle 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 werden die jeweils grundlegenden Konzepte (in Kombinatorik, Graphtheorie, elementarer Zahlentheorie und elementarer Wahrscheinlichkleitstheorie) erworben. Es wird die intellektuelle Fähigkeit geschult, die logischen Zusammenhänge zwischen den Konzepten zu überblicken,und 'versteckte' Anwendungsmöglichkeiten zu erkennen.

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.

Prüfungsform: Klausurarbeit (180 Minuten)

Voraussetzungen für die Vergabe von Kreditpunkten: Erfolgreiches Bestehen der Modulklausur.

Verwendung des Moduls (in anderen Studiengängen): Master IT-Sicherheit/Netze und Systeme

Stellenwert der Note für die Endnote: 8 / 143

1.6 Einführung in die Kryptographie 1

Nummer: 149026
Verantwortlicher: Prof. Dr.-Ing. Christof Paar
Arbeitsaufwand: 150 Stunden (entsprechend der Lehrveranstaltungen)
Leistungspunkte: 5
Semester: 1. Semester (BaITS/I), 1. Semester (MaITS/N)
Dauer: 1 Semester

Veranstaltungen:

141022: Einführung in die Kryptographie 1 4 SWS (S.89)

Ziele: Nach erfolgreichem Abschluss des Moduls verfügen die Studierenden über Kenntnisse der grundlegenden Anwendungen symmetrischer Verfahren und über Grundkenntnisse der asymmetrischen Kryptographie. Sie können entscheiden, unter welchen Bedingungen man in der Praxis bestimmte Verfahren einsetzt und wie die Sicherheitsparameter zu wählen sind. Mit den Grundlagen des abstrakten Denkens in der IT Sicherheitstechnik sind sie vertraut.

Zum anderen erreichen die Studierenden durch Beschreibungen ausgewählter praxisrelevanter Algorithmen, wie z. B. des AES- oder RSA-Algorithmus, ein algorithmisches und technisches Verständnis zur praktischen Anwendung. Die Studierenden erhalten dabei einen Überblick über die in Unternehmen eingesetzten Lösungen. Sie sind in der Lage, argumentativ eine bestimmte Lösung zu verteidigen. Die Vorlesungen werden zusätzlich auch als Videos in Deutsch und Englisch angeboten. Die Studierenden können daher durch das zweisprachige eLearning-Angebot Sprachkompetenzen in der Wissenschaftssprache Englisch erwerben.

Inhalt: Das Modul bietet einen allgemeinen Einstieg in die Funktionsweise moderner Kryptografie und Datensicherheit. Es werden grundlegende Begriffe und mathematisch/technische Verfahren der Kryptografie und der Datensicherheit erläutert. Praktisch relevante symmetrische und asymmetrische Verfahren und Algorithmen werden vorgestellt und an praxisrelevanten Beispielen erläutert.

Die Vorlesung lässt sich in zwei Teile gliedern: Die Funktionsweise der symmetrischen Kryptographie einschließlich der Beschreibung historisch bedeutender symmetrischer Verschlüsselungsverfahren (Caesar Chiffre, Affine Chiffre) und aktueller symmetrischer Verfahren (Data Encryption Standard, Advanced Encryption Standard, Stromchiffren, One Time Pad) werden im ersten Teil behandelt.

Der zweite Teil besteht aus einer Einleitung zu asymmetrischen Verfahren und einem ihrer wichtigsten Stellvertretern (RSA). Hierzu wird eine Einführung der Grundlagen der Zahlentheorie durchgeführt, um ein grundlegendes Verständnis der Verfahren sicherzustellen (u.a. Ringe ganzer Zahlen, Gruppen, Körper, diskrete Logarithmen, euklidischer Algorithmus). Nichtsdestotrotz liegt der Schwerpunkt auf der algorithmischen Einführung des asymmetrischen Verfahrens.

Prüfungsform: Klausurarbeit (120 Minuten)

Voraussetzungen für die Vergabe von Kreditpunkten: Erfolgreiches Bestehen der Modulklausur.

Verwendung des Moduls (in anderen Studiengängen): Bachelor IT-Sicherheit/Informationstechnik, Bachelor Angewandte Informatik, Bachelor Informatik, Master IT-Sicherheit/Netze und Systeme

Stellenwert der Note für die Endnote: 5 / 143

1.7 Einführung in die Kryptographie 2

Nummer: 149027
Verantwortlicher: Prof. Dr.-Ing. Christof Paar
Arbeitsaufwand: 150 Stunden (entsprechend der Lehrveranstaltungen)
Leistungspunkte: 5
Semester: 2. Semester (BaITS/I), 2. Semester (MaITS/N)
Dauer: 1 Semester

Veranstaltungen:

141023: Einführung in die Kryptographie 2 4 SWS (S.91)

Ziele: Nach erfolgreichem Abschluss des Moduls verfügen die Studierenden über Kenntnisse der grundlegenden Anwendungen asymmetrischer und hybrider Verfahren. Sie können entscheiden, unter welchen Bedingungen man in der Praxis bestimmte Verfahren einsetzt und wie die Sicherheitsparameter zu wählen sind. Mit den Grundlagen des abstrakten Denkens in der IT Sicherheitstechnik sind sie vertraut. Zum anderen erreichen die Studierenden durch Beschreibungen ausgewählter praxisrelevanter Algorithmen, wie z.B. des Diffie-Hellmann-Schlüsselaustausch oder ECC-basierten Verfahren, ein algorithmisches und technisches Verständnis zur praktischen Anwendung. Die Studierenden erhalten dabei einen Überblick über die in Unternehmen eingesetzten Lösungen. Sie sind in der Lage, argumentativ eine bestimmte Lösung zu verteidigen. Die Vorlesungen werden zusätzlich auch als Videos in Deutsch und Englisch angeboten. Die Studierenden können daher durch das zweisprachige eLearning-Angebot Sprachkompetenzen in der Wissenschaftssprache Englisch erwerben.

Inhalt: Das Modul bietet einen allgemeinen Einstieg in die Funktionsweise moderner Kryptografie und Datensicherheit. Es werden grundlegende Begriffe und mathematisch/technische Verfahren der Kryptografie und der Datensicherheit erläutert. Praktisch relevante asymmetrische Verfahren und Algorithmen werden vorgestellt und an praxisrelevanten Beispielen erläutert. Die Vorlesung lässt sich in zwei Teile gliedern: Der erste Teil beginnt mit einer Einleitung zu asymmetrischen Verfahren und deren wichtigsten Stellvertretern (Diffie-Hellman, elliptische Kurven). Der Schwerpunkt liegt auf der algorithmischen Einführung der asymmetrischen Verfahren, die sowohl Verschlüsselungsalgorithmen als auch digitale Signaturen beinhalten. Abgeschlossen wird dieser Teil durch Hashfunktionen, die eine große Rolle für digitalen Signaturen und Message Authentication Codes (MACs oder kryptografische Checksummen) spielen. Im zweiten Teil der Vorlesung werden Grundlagen von Sicherheitslösungen aufbauend auf den Konzepten der symmetrischen und asymmetrischen Kryptographie besprochen. Dabei wird vor allem auf die in Unternehmen notwendigen und eingesetzten Lösungen (PKI, digitale Zertifikate etc.) eingegangen.

Prüfungsform: Klausurarbeit (120 Minuten)

Voraussetzungen für die Vergabe von Kreditpunkten: Erfolgreiches Bestehen der Modulklausur.

Verwendung des Moduls (in anderen Studiengängen): Bachelor IT-Sicherheit/Informationstechnik, Bachelor Angewandte Informatik, Bachelor Informatik, Master IT-Sicherheit/Netze und Systeme

Stellenwert der Note für die Endnote: 5 / 143

1.8 Einführung in die theoretische Informatik

Nummer: 149667
Verantwortlicher: Prof. Dr. Alexander May
Arbeitsaufwand: 180 Stunden (entsprechend der Lehrveranstaltungen)
Leistungspunkte: 6

Veranstaltungen:

150310: Einführung in die theoretische Informatik 4 SWS (S.93)

Ziele: Der professionelle Umgang mit abstrakten, diskreten Strukturen wird beherrscht. Dazu gehört die Fähigkeit, konkrete Problemstellungen mit solchen Strukturen zu modellieren, und scharfsinnige Schlussfolgerungen aus gegebenen Informationen zu ziehen. 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 Wahrscheinlichkeitstheorie) wurden erworben. Die intellektuelle Fähigkeit, die logischen Zusammenhänge zwischen den Konzepten zu überblicken, und "versteckte" Anwendungsmöglichkeiten zu erkennen, wurde geschult.

Inhalt: Es wird eine Einführung in die Kodierungstheorie und in die Theorie der Berechenbarkeit gegeben.

- Themenübersicht:
  - Turingmaschine
  - Komplexitätsklassen P und NP
  - Polynomielle Reduktion
  - Quadratische Reste
  - Eindeutig entschlüsselbare Codes
  - Kompakte und optimale Codes
  - Lineare und duale Codes

Prüfungsform: siehe Lehrveranstaltungen

Stellenwert der Note für die Endnote: 6 / 143

1.9 Grundlagenpraktikum ITS

Nummer: 149240
Verantwortlicher: Prof. Dr. Jörg Schwenk
Arbeitsaufwand: 90 Stunden (entsprechend der Lehrveranstaltungen)
Leistungspunkte: 3

Veranstaltungen:

142240: Grundlagenpraktikum ITS 3 SWS (S.100)

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

Stellenwert der Note für die Endnote: 0 / 143

1.10 Industriepraktikum

Nummer: 149888
Verantwortlicher: Studiendekan ITS
Arbeitsaufwand: 450 Stunden (entsprechend der Lehrveranstaltungen)
Leistungspunkte: 15
Semester: 6. Semester (BaITS/I)
Dauer: 3 Monate

Veranstaltungen:

144011: Industriepraktikum ITS (S.104)

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: Praktikum über 450 Arbeitsstunden + schriftlicher Praktikumsbericht

Voraussetzungen für die Vergabe von Kreditpunkten: Nachweis über die 450 Arbeitsstunden und Abgabe eines schriftlichen Praktikumsberichts.

Verwendung des Moduls (in anderen Studiengängen): Bachelor IT-Sicherheit/Informationstechnik

Stellenwert der Note für die Endnote: 0 / 143

1.11 Informatik 1

Nummer: 149329
Verantwortlicher: Prof. Dr.-Ing. Helmut Balzert
Arbeitsaufwand: 150 Stunden (entsprechend der Lehrveranstaltungen)
Leistungspunkte: 5

Veranstaltungen:

141328: Informatik 1 - Programmierung für ET/IT (PO 13) und ITS (PO 13) 4 SWS (S.105)

Ziele: Die Studierenden haben einen systematischen Überblick über Prinzipien, Methoden, Konzepte und Notationen des "Programmierens im Kleinen", und seine Einordnung in die verschiedenen Kontexte. Dieses Wissen - verbunden mit den praktischen Übungen am Computersystem - befähigt die Studierenden, 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 bzw. darin 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

Prüfungsform: siehe Lehrveranstaltungen

Stellenwert der Note für die Endnote: 5 / 143

1.12 Informatik 2

Nummer: 149330
Verantwortlicher: Prof. Dr.-Ing. Helmut Balzert
Arbeitsaufwand: 150 Stunden (entsprechend der Lehrveranstaltungen)
Leistungspunkte: 5

Veranstaltungen:

141321: Informatik 2 - Algorithmen und Datenstrukturen 4 SWS (S.107)

Ziele: Die Studierenden haben einen systematischen Überblick über Prinzipien, Methoden, Konzepte und Notationen des "Programmierens im Kleinen", und seine Einordnung in die verschiedenen Kontexte. Dieses Wissen - verbunden mit den praktischen Übungen am Computersystem - befähigt die Studierenden, 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 bzw. darin 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

Prüfungsform: siehe Lehrveranstaltungen

Stellenwert der Note für die Endnote: 5 / 143

1.13 Informatik 3

Nummer: 149303
Verantwortlicher: Prof. Dr.-Ing. Jürgen Oehm
Arbeitsaufwand: 150 Stunden (entsprechend der Lehrveranstaltungen)
Leistungspunkte: 5

Veranstaltungen:

141300: Informatik 3 - Digitaltechnik 4 SWS (S.109)

Ziele: Die Studierenden haben elementare 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 haben sie zentrale Kenntnisse 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. Mit diesem Wissen sind die Studierenden in der Lage, 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.

Prüfungsform: siehe Lehrveranstaltungen

Stellenwert der Note für die Endnote: 5 / 143

1.14 Kernfächer

Nummer: 149910
Verantwortlicher: Studiendekan ITS
Arbeitsaufwand: 450 Stunden (entsprechend der Lehrveranstaltungen)
Leistungspunkte: 15

Veranstaltungen:

150357: Boolesche Funktionen mit Anwendungen in der Kryptographie	4 SWS	(S.79)
260081: Datenschutz	3 SWS	(S.82)
141347: Digitale Forensik	4 SWS	(S.84)
150326: Einführung in die asymmetrische Kryptanalyse	4 SWS	(S.88)
141036: Einführung in die Usable Security and Privacy	4 SWS	(S.95)
142031: Einführung ins Hardware Reverse Engineering	4 SWS	(S.97)
150347: Elliptische Kurven und Kryptographie	4 SWS	(S.99)
141024: Implementierung kryptographischer Verfahren	4 SWS	(S.102)
141031: Kryptographie auf hardwarebasierten Plattformen	4 SWS	(S.113)
150324: Model Checking	4 SWS	(S.123)
141245: Web-Sicherheit	4 SWS	(S.145)
141249: Web-und Browsersicherheit	4 SWS	(S.146)

Ziele: Die Studierenden haben vertiefte Kenntnisse in einer Auswahl von Kerngebieten der IT-Sicherheit.

Inhalt: Es sind Lehrveranstaltungen aus dem Katalog der Kernfächer auszuwählen.

Prüfungsform: siehe Lehrveranstaltungen

Stellenwert der Note für die Endnote: 15 / 143

1.15 Kryptographie

Nummer: 149666
Verantwortlicher: Prof. Dr. Alexander May
Arbeitsaufwand: 240 Stunden (entsprechend der Lehrveranstaltungen)
Leistungspunkte: 8
Semester: 3. Semester (MaITS/N), 5. Semester (BaITS/I)
Dauer: 1 Semester

Veranstaltungen:

150312: Kryptographie 6 SWS (S.115)

Ziele: Die Studierdenden haben 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. Die Teilnehmer sind zur Analyse und dem Design aktueller und zukünftiger kryptographischer Methoden befähigt. Zudem weisen sie ein Bewusstsein für Methodik und Mächtigkeit verschiedenster Angriffsszenarien auf.

Inhalt: Es wird eine Einführung in moderne Methoden der symmetrischen und asymmetrischen Kryptographie geboten. Dazu wird ein Angreifermodell definiert und die Sicherheit der vorgestellten Verschlüsselungs-, Hash- und Signaturverfahren unter wohldefinierten KomplexitŠtsannahmen in diesem Angreifermodell nachgewiesen.

- Themenübersicht:
  - Sichere Verschlüsselung gegenüber KPA-, CPA- und CCA-Angreifern
  - Pseudozufallsfunktionen und -permutationen
  - Message Authentication Codes
  - Kollisionsresistente Hashfunktionen
  - Blockchiffren
  - Konstruktion von Zufallszahlengeneratoren
  - Diffie-Hellman Schlüsselaustausch
  - Trapdoor Einwegpermutationen
  - Public Key Verschlüsselung: RSA, ElGamal, Goldwasser-Micali, Rabin, Paillier
  - Einwegsignaturen
  - Signaturen aus kollisionsresistenten Hashfunktionen
  - Random-Oracle Modell

Prüfungsform: Klausurarbeit (120 Minuten)

Voraussetzungen für die Vergabe von Kreditpunkten: Erfolgreiches Bestehen der Modulklausur.

Verwendung des Moduls (in anderen Studiengängen): Bachelor IT-Sicherheit/Informationstechnik, Bachelor Informatik, Master IT-Sicherheit/Netze und Systeme

Stellenwert der Note für die Endnote: 8 / 143

1.16 Mathematik 1

Nummer: 149662
Verantwortlicher: Dr. rer. nat. Mario Lipinski
Arbeitsaufwand: 300 Stunden (entsprechend der Lehrveranstaltungen)
Leistungspunkte: 10
Semester: 1. Semester (BaET)
Dauer: 1 Semester

Veranstaltungen:

150110: Mathematik 1 für ET/IT (PO 13+20) und ITS (PO 13) 8 SWS (S.117)

Ziele: Die Studierenden beherrschen folgende mathematische Methoden zur Lösung ingenieurwissenschaftlicher Probleme und können diese anwenden:

- Eigenschaften reeller und komplexer Zahlen
- Elementare Eigenschaften der linearen Algebra
- Differential- und Integralrechnung für Funktionen von einer Veränderlichen
- Einfache gewöhnliche Differentialgleichungen

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.

Prüfungsform: Klausurarbeit (120 Minuten)

Voraussetzungen für die Vergabe von Kreditpunkten: Erfolgreiches Bestehen der Modulklausur.

Verwendung des Moduls (in anderen Studiengängen): Bachelor Elektrotechnik und Informationstechnik

Stellenwert der Note für die Endnote: 10 / 143

1.17 Mathematik 2

Nummer: 149663
Verantwortlicher: Dr. rer. nat. Mario Lipinski
Arbeitsaufwand: 300 Stunden (entsprechend der Lehrveranstaltungen)
Leistungspunkte: 10
Semester: 2. Semester (BaET)
Dauer: 1 Semester

Veranstaltungen:

150112: Mathematik 2 für ET/IT (PO 13+20) und ITS (PO 13) 8 SWS (S.120)

Ziele: Die Studierenden beherrschen folgende mathematische Methoden zur Lösung ingenieurwissenschaftlicher Probleme und können diese anwenden:

- Differenzialrechnung für Funktionen von mehreren Variablen
- Orthonormalsysteme, insbesondere Fourierreihen
- Integralrechnung für Funktionen von mehreren Variablen
- Eigenschaften der Laplace- und Fouriertransformation

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.

Prüfungsform: Klausurarbeit (120 Minuten)

Voraussetzungen für die Vergabe von Kreditpunkten: Erfolgreiches Bestehen der Modulklausur.

Verwendung des Moduls (in anderen Studiengängen): Bachelor Elektrotechnik und Informationstechnik

Stellenwert der Note für die Endnote: 10 / 143

1.18 Netzsicherheit 1

Nummer: 149243
Verantwortlicher: Prof. Dr. Jörg Schwenk
Arbeitsaufwand: 150 Stunden (entsprechend der Lehrveranstaltungen)
Leistungspunkte: 5
Semester: 1. Semester (MaITS/N)
Dauer: 1 Semester

Veranstaltungen:

141242: Netzsicherheit 1 4 SWS (S.125)

Ziele: Studierende verfügen nach erfolgreichem Abschluss des Moduls über ein umfassendes Verständnis der technischen Aspekte von Netzsicherheit. Sie haben erkannt, dass Kryptographie alleine nicht ausreicht, um sicherheitstechnische Probleme zu lösen. Sie haben ein umfassendes Systemverständnis für komplexe IT-Systeme erworben. Durch eigenständige Überlegungen zur Verbesserung der Netzsicherheit bereiten sich die Studierenden auf ihre Rolle im Berufsleben vor. Sie können neue Probleme analysieren und neue Lösungsmöglichkeiten entwickeln. Sie können im Gespräch den Nutzen der von ihnen erarbeiteten Lösungen argumentativ begründen. Sie haben verstanden, dass nicht-technische Faktoren wie Fragen der Haftung und der entstehenden Kosten Entscheidungen zur IT-Sicherheit maßgeblich mit beeinflussen.

Inhalt: Wenn Kryptographie in einer technischen Umgebung wie einem Computer-, Daten- oder Telefonnetz eingesetzt wird, hängt die Sicherheit außer von rein kryptographischen Faktoren auch von der technischen Einbettung der Verschlüsselungs- und Signaturalgorithmen ab. Prominente Beispiele (für fehlerhafte Einbettungen) sind EFAIL (efail.de), Angriffe auf die WLAN-Verschlüsselungssysteme WEP und WPA (KRACK) und diverse Angriffe auf TLS (Bleichenbacher, POODLE, DROWN, ROBOT). Das Modul „Netzsicherheit 1“ beschäftigt sich mit konkreten Netzen zur Datenübertragung und beleuchtet diese von allen Seiten auf ihre Sicherheit hin. Es umfasst folgende Teile:

- Einführung: Internet
- Einführung: Vertraulichkeit
- Einführung: Integrität
- Einführung: Kryptographische Protokolle
- PPP-Sicherheit (insb. PPTP), EAP-Protokolle
- WLAN-Sicherheit (WEP, WPA, Wardriving, KRACK)
- GSM- und UMTS-Mobilfunk (Authentisierung und Verschlüsselung)
- IPSec (ESP und AH, IKEv1 und v2, Angriffe auf IPSec)
- Dateiverschlüsselung mit OpenPGP (Datenformat, Efail, Klima-Rosa)

- E Mail-Verschlüsselung mit S/MIME (SMTP, Datenformat, Efail, POP3, IMAP)

Neben den Systemen selbst werden dabei auch publizierte Angriffe auf diese Systeme besprochen; die Studierenden stellen selbst wissenschaftliche Überlegungen zur Verbesserung der Sicherheit an.

Prüfungsform: Klausurarbeit (120 Minuten)

Voraussetzungen für die Vergabe von Kreditpunkten: Erfolgreiches Bestehen der Modulklausur.

Verwendung des Moduls (in anderen Studiengängen): Master IT-Sicherheit / Netze und Systeme

Stellenwert der Note für die Endnote: 5 / 143

1.19 Netzsicherheit 2

Nummer: 149244
Verantwortlicher: Prof. Dr. Jörg Schwenk
Arbeitsaufwand: 150 Stunden (entsprechend der Lehrveranstaltungen)
Leistungspunkte: 5
Semester: 4. Semester (BaITS/I), 2. Semester (MaITS/N)
Dauer: 1 Semester

Veranstaltungen:

141243: Netzsicherheit 2 4 SWS (S.127)

Ziele: Studierende verfügen nach erfolgreichem Abschluss des Moduls über ein umfassendes Verständnis der technischen Aspekte von Netzsicherheit. Sie haben erkannt, dass Kryptographie alleine nicht ausreicht, um sicherheitstechnische Probleme zu lösen. Sie haben ein umfassendes Systemverständnis für komplexe IT-Systeme erworben. Durch eigenständige Überlegungen zur Verbesserung der Netzsicherheit bereiten sich die Studierenden auf ihre Rolle im Berufsleben vor. Sie können neue Probleme analysieren und neue Lösungsmöglichkeiten entwickeln. Sie können im Gespräch den Nutzen der von ihnen erarbeiteten Lösungen argumentativ begründen. Sie haben verstanden, dass nicht-technische Faktoren wie Fragen der Haftung und der entstehenden Kosten Entscheidungen zur IT-Sicherheit maßgeblich mit beeinflussen.

Inhalt: Wenn Kryptographie in einer technischen Umgebung wie einem Computer-, Daten- oder Telefonnetz eingesetzt wird, hängt die Sicherheit außer von rein kryptographischen Faktoren auch von der technischen Einbettung der Verschlüsselungs- und Signaturalgorithmen ab. Prominente Beispiele (für fehlerhafte Einbettungen) sind EFAIL (efail.de), Angriffe auf die WLAN-Verschlüsselungssysteme WEP und WPA (KRACK) und diverse Angriffe auf TLS (Bleichenbacher, POODLE, DROWN, ROBOT). Das Modul „Netzsicherheit“ beschäftigt sich mit konkreten Netzen zur Datenübertragung und beleuchtet diese von allen Seiten auf ihre Sicherheit hin. Es umfasst folgende Teile:

- Sicherheit von HTTP (HTTP Authentication, Secure HTTP, Architektur von SSL/TLS)
- Transport Layer Security (TLS1.2, Versionen SSL 2.0 bis TLS 1.3)
- Angriffe auf SSL und TLS (BEAST, CRIME, POODLE, Lucky13, Bleichenbacher, DROWN, Heartbleed, Invalid Curve)
- Secure Shell - SSH
- das Domain Name System und DNSSEC (faktorisierbare Schlüssel)
- Sicherheit von Webanwendungen (HTML, URI, XSS, CSRF, SQLi, SSO)
- XML- und JSON-Sicherheit

Neben den Systemen selbst werden dabei auch publizierte Angriffe auf diese Systeme besprochen; die Studierenden stellen selbst wissenschaftliche Überlegungen zur Verbesserung der Sicherheit an.

Prüfungsform: Klausurarbeit (120 Minuten)

Voraussetzungen für die Vergabe von Kreditpunkten: Erfolgreiches Bestehen der Modulabschlussklausur.

Verwendung des Moduls (in anderen Studiengängen): Bachelor IT-Sicherheit/Informationstechnik, Master IT-Sicherheit/Netze und Systeme

Stellenwert der Note für die Endnote: 5 / 143

1.20 Nichttechnische Wahlfächer

Nummer: 149891
Verantwortlicher: Studiendekan ITS
Arbeitsaufwand: Mindestens 270 Stunden (entsprechend der Lehrveranstaltungen)
Leistungspunkte: ≥ 9
Semester: 1.-3. Semester (MaITS/I)
Dauer: 1 Semester

Veranstaltungen:

141105: Nichttechnische Veranstaltungen (S.129)

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: Die nichttechnischen Wahlfächer erweitern die Soft Skills. Z.B. wird die englische Fachsprache verbessert, in die Grundlagen der Rechtswissenschaften eingeführt oder Grundkenntnisse der Betriebswirtschaft vermittelt. Bei der Auswahl haben die Studierenden die Möglichkeit eine Auswahl entsprechend der eigenen Interessen zu treffen.

Prüfungsform: siehe Lehrveranstaltungen

Voraussetzungen für die Vergabe von Kreditpunkten: siehe Lehrveranstaltungen

Verwendung des Moduls (in anderen Studiengängen): Master IT-Sicherheit/Informationstechnik

Stellenwert der Note für die Endnote: 0 / 143

1.21 Praxistage

Nummer: 149871
Verantwortlicher: Dekan
Arbeitsaufwand: 30 Stunden (entsprechend der Lehrveranstaltungen)
Leistungspunkte: 1

Veranstaltungen:

141090: Praxistage für ET/IT und ITS (PO 13) 1 SWS (S.131)

Ziele: Während der „Praxistage“ haben alle Studienanfänger in ihrem ersten Studiensemester gelernt, gemeinsam an einer Aufgabe zu arbeiten: Die Programmierung humanoider Roboter. In der Veranstaltung haben die Teilnehmer die Vielfalt des technisch Möglichen entdeckt und können erste eigene Ideen verwirklichen. Neben den Programmierkenntnissen wurden auch ihr konzeptionelle Arbeitsvermögen, die eigene Kreativität und Teamfähigkeit geschult.

Inhalt: An der Veranstaltung „Praxistage“ nehmen alle Erstsemester der Bachelor-Studiengänge Elektrotechnik und Informationstechnik und IT-Sicherheit / Informationstechnik teil. Im Rahmen der dreitägigen Lehrveranstaltung treten die Studierenden in 2er-Gruppen gegeneinander an.

Jede Gruppe arbeitet mit einem Roboter „Robonova I“, dessen 16 Servomotoren vielseitige Bewegungen ermöglichen. Die Aufgabe der Teilnehmer ist es, gemeinschaftlich Ideen zu entwickeln und diese anschließend über eine geeignete Programmierung umzusetzen. Das Wettbewerbsverfahren besteht aus einem Pflichtteil und einer Kür. Zunächst soll es darum gehen, eine vorgegebene Aufgabe zu erfüllen, in einem zweiten Schritt folgt eine freie Kombination von Bewegungsfolgen. Hier sind der Phantasie der Gruppe keine Grenzen gesetzt.

Prüfungsform: siehe Lehrveranstaltungen

Stellenwert der Note für die Endnote: 0 / 143

1.22 Programmieren in C

Nummer: 149872
Verantwortlicher: Dekan
Arbeitsaufwand: 90 Stunden (entsprechend der Lehrveranstaltungen)
Leistungspunkte: 3

Veranstaltungen:

149872: Programmieren in C 3 SWS (S.132)

Ziele: Die Studierenden beherrschen die grundlegenden Sprachkonstrukte von C mit Betonung der prozeduralen Betrachtungsweise und haben ein Verständnis 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

Prüfungsform: siehe Lehrveranstaltungen

Stellenwert der Note für die Endnote: 0 / 143

1.23 Rechnerarchitektur

Nummer: 149155
Verantwortlicher: Prof. Dr.-Ing. Michael Hübner
Arbeitsaufwand: 150 Stunden (entsprechend der Lehrveranstaltungen)
Leistungspunkte: 5

Veranstaltungen:

141140: Rechnerarchitektur für ET/IT und ITS (PO 13) 4 SWS (S.134)

Ziele: Die Studierenden kennen Zusammenhänge und haben Detailkenntnisse zum Aufbau, zu Komponenten und zur Funktionsweise moderner Computersysteme in Hard- und Software. Damit verfügen sie über die Basis, sowohl in der Computertechnik selbst, als auch in deren Anwendungsbereichen wie z.B. den eingebetteten Systemen, Computerkomponenten und -systeme auslegen und entwickeln zu können. Die Teilnehmer dieser Veranstaltung beherrschen die grundsätzliche Arbeitsweise von Prozessoren und deren Mikroarchitektur (z.B. Pipelinestufen, Befehlsabarbeitung, auflösen von Pipelinekonflikten etc.).

Inhalt: Ausgehend von grundlegenden Computerstrukturen (Von-Neumann-Archi- tektur, 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, Core, Ultra Sparc III) runden die generellen Wissensinhalte ab. Einen besonderen inhaltlichen Schwerpunkt bildet die tiefgehende Erklärung sowie Programmierung der Mikroarchitekturebene als Ergänzung zu anderen Lehrveranstaltungen im Bereich der Informatik / Computertechnik (Programmiersprachen, Eingebettete Prozessoren).

Prüfungsform: siehe Lehrveranstaltungen

Stellenwert der Note für die Endnote: 5 / 143

1.24 Systemsicherheit

Nummer: 149341
Verantwortlicher: Prof. Dr. Thorsten Holz
Arbeitsaufwand: 150 Stunden (entsprechend der Lehrveranstaltungen)
Leistungspunkte: 5
Semester: 4. Semester (BaITS/I)
Dauer: 1 Semester

Veranstaltungen:

141340: Systemsicherheit 4 SWS (S.138)

Ziele: Die Studierenden beherrschen wichtige theoretische und praktische Aspekte von Sicherheitsprotokollen. Sie sind in die Lage, die Sicherheit gegebener Protokolle zu analysieren, Schwachstellen im Design aufzudecken sowie selbständig neue Protokolle zu entwickeln. Darüber hinaus haben sie grundlegende Kenntnisse aus dem Bereich der Systemsicherheit wie beispielsweise Anonymität, Privatsphäre, Zugriffskontrolle und physische Sicherheit.

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.

Prüfungsform: Klausurarbeit (120 Minuten)

Voraussetzungen für die Vergabe von Kreditpunkten: Erfolgreiches Bestehen der Modulklausur.

Verwendung des Moduls (in anderen Studiengängen): Bachelor IT-Sicherheit/Informationstechnik, Bachelor Informatik, Master IT-Sicherheit/Netze und Systeme

Stellenwert der Note für die Endnote: 5 / 143

1.25 Systemtheorie 1

Nummer: 149056
Verantwortlicher: Prof. Dr.-Ing. Rainer Martin
Arbeitsaufwand: 150 Stunden (entsprechend der Lehrveranstaltungen)
Leistungspunkte: 5
Semester: 2. Semester (BaET), 2. Semester (BaITS/I)
Dauer: 1 Semester

Veranstaltungen:

141170: Systemtheorie 1 - Signale und Systeme 4 SWS (S.141)

Ziele: Die Studierenden beherrschen die wesentlichen Grundlagen der Systemtheorie. Sie kennen die mathematische Beschreibung von Signalen und Systemen im Zeitbereich und deren wesentliche Merkmale. Sie kennen die Grundlagen der Wahrscheinlichkeitsrechnung und können mit diskreten und kontinuierlichen Zufallsvariablen rechnen. Sie verstehen die Grundbegriffe der Informationstheorie und können diese anwenden.

Inhalt:

1. **Signale und Systeme**

   Signale, Kenngrößen und Eigenschaften von Signalen, Elementare Operationen, Signalsynthese und Signalanalyse, periodischer Signale, Analog-Digital und Digital-Analog Umsetzung, lineare und nichtlineare Systeme

2. **Einführung in die Wahrscheinlichkeitsrechnung**

   Einführung und Definitionen, Mehrstufige Zufallsexperimente, Diskrete Zufallsvariablen, Kontinuierliche Zufallsvariablen

3. **Grundbegriffe der Informationstheorie**

   Grundlegende Fragestellungen der Informationstheorie, Entropiebegriffe, Anwendungen

Prüfungsform: Klausurarbeit (120 Minuten)

Voraussetzungen für die Vergabe von Kreditpunkten: Erfolgreiches Bestehen der Modulklausur.

Verwendung des Moduls (in anderen Studiengängen): Bachelor Elektrotechnik und Informationstechnik, Bachelor IT-Sicherheit/Informationstechnik

Stellenwert der Note für die Endnote: 5 / 143

1.26 Systemtheorie 2

Nummer: 149100
Verantwortlicher: Prof. Dr.-Ing. Aydin Sezgin
Arbeitsaufwand: 180 Stunden (entsprechend der Lehrveranstaltungen)
Leistungspunkte: 6
Semester: 3. Semester (BaET)
Dauer: 1 Semester

Veranstaltungen:

141218: Systemtheorie 2 - Signaltransformation 5 SWS (S.142)

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 Lerninhalte. 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 dem Modul 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

Prüfungsform: Klausurarbeit (120 Minuten)

Voraussetzungen für die Vergabe von Kreditpunkten: Erfolgreiches Bestehen der Modulklausur.

Stellenwert der Note für die Endnote: 6 / 143

1.27 Tutorium

Nummer: 149874
Verantwortlicher: Friederike Kogelheide
Arbeitsaufwand: Keine Stunden (entsprechend der Lehrveranstaltungen)
Leistungspunkte:

Veranstaltungen:

140000: Tutorium 2 SWS (S.144)

Ziele: Den Studierenden wird der Einstieg in das Studium erleichtert. Sie sind über inhaltliche und administrative Zusammenhänge informiert, haben Lerngruppen gebildet und haben verschiedene Kompetenzen der Lehrveranstaltungen der ersten Studiensemester vertieft.

Inhalt: Das Tutorium erleichtert allen Bachelor-Studienanfängern der Fakultät für Elektrotechnik und Informationstechnik in den ersten beiden Semestern den Einstieg ins Studium. Beim Tutorium handelt es sich um eine freiwillige Zusatzveranstaltung. In den wöchentlichen Treffen unterstützen so genannte „Tutoren“, meist Studierende aus höheren Semestern, die Erstsemester in der Anfangsphase ihres Studiums. Zunächst werden die Studenten mit der Uni insbesondere mit der Fakultät und den Einrichtungen bekannt gemacht. Die weiteren Themen erstrecken sich von der studentischen Selbstverwaltung über lerntechnische Fragen bis hin zu Freizeitangeboten in der Bochumer Umgebung. Im späteren Verlauf des Tutoriums rücken dann immer stärker fachliche Fragen in den Vordergrund.

Prüfungsform: Es handelt sich um eine freiwillige Zusatzveranstaltung.

Stellenwert der Note für die Endnote: 0 / 143

1.28 Vertiefungspraktikum ITS

Nummer: 149915
Verantwortlicher: Studiendekan ITS
Arbeitsaufwand: 90 Stunden (entsprechend der Lehrveranstaltungen)
Leistungspunkte: 3

Veranstaltungen:

142362: Bachelor-Forschungspraktikum Human-Centred Security	3 SWS	(S.48)
142028: Bachelor-Praktikum ARM Processors for Embedded Cryptography	3 SWS	(S.50)
142245: Bachelor-Praktikum TLS Implementierung	3 SWS	(S.52)
142242: Bachelor-Projekt Netz- und Datensicherheit	3 SWS	(S.56)
150583: Bachelor-Vertiefungspraktikum SAGE in der Kryptographie	2 SWS	(S.69)
142025: Bachelor-Vertiefungspraktikum Wireless Physical Layer Security	3 SWS	(S.72)
142244: Bachelor-Vertiefungspraktikum zur Hackertechnik	3 SWS	(S.74)

Ziele: Die Studierenden sind befähigt, verschiedene Methoden der IT-Sicherheit praktisch umzusetzen und hinsichtlich ihrer Funktionalität zu prüfen.

Inhalt: Ein Praktikum oder Projekt wird aus einer verbindlichen Liste ausgewählt.

Prüfungsform: siehe Lehrveranstaltungen

Stellenwert der Note für die Endnote: 0 / 143

1.29 Vertiefungsseminar ITS

Nummer: 149916
Verantwortlicher: Studiendekan ITS
Arbeitsaufwand: 90 Stunden (entsprechend der Lehrveranstaltungen)
Leistungspunkte: 3
Semester: 5. Semester (BaITS/I)
Dauer: 1 Semester

Veranstaltungen:

143243: Bachelor-Seminar Aktuelle Themen der IT-Sicherheit	3 SWS	(S.57)
143020: Bachelor-Seminar Embedded Security	3 SWS	(S.59)
143249: Bachelor-Seminar Human Centered Security and Privacy	3 SWS	(S.60)
150508: Bachelor-Seminar Kryptographie	3 SWS	(S.61)
150507: Bachelor-Seminar Kryptologie	3 SWS	(S.62)
143241: Bachelor-Seminar Netz- und Datensicherheit	3 SWS	(S.63)
141035: Bachelor-Seminar Security Engineering	3 SWS	(S.65)
148213: Bachelor-Seminar Sichere Hardware	3 SWS	(S.66)
150509: Bachelor-Seminar Symmetrische Kryptographie	3 SWS	(S.67)
143290: Bachelor-Seminar Usable Security and Privacy Research	3 SWS	(S.68)
150537: Seminar zur Kryptographie	2 SWS	(S.136)
150560: Seminar zur Real World Cryptoanalysis	2 SWS	(S.137)

Ziele: Die Studierenden sind befähigt, selbständig Literatur zu einem gegebenen Thema zu sichten, die wesentlichen Inhalte zu erfassen und diese wiederzugeben. Sie haben die Schlüsselqualifikationen zur Präsentation ihrer Ergebnisse: sowohl die schriftliche Ausarbeitung eines Themas, als auch Präsentationstechniken und rhetorische Techniken.

Inhalt: Einzelthemen aus dem gewählten Seminarthema werden in Vorträgen dargestellt. Die Studierenden halten jeweils einen Vortrag, hören die Vorträge der anderen Studierenden und diskutieren die Inhalte miteinander. Dabei geht es nicht um die reine Wissensvermittlung, sondern das Erlernen des wissenschaftlichen Diskurses. Daraus resultiert eine Anwesenheitspflicht an der zu Beginn des Seminars festgelegten Anzahl von Einzelterminen.

Prüfungsform: Seminarbeitrag

Voraussetzungen für die Vergabe von Kreditpunkten: siehe Lehrveranstaltungen

Verwendung des Moduls (in anderen Studiengängen): Bachelor IT-Sicherheit/Informationstechnik

Stellenwert der Note für die Endnote: 0 / 143

Kapitel 2

Veranstaltungen

2.1 141130: Allgemeine Elektrotechnik 1 - Elektrische Netzwerke

Nummer:	141130
Lehrform:	Vorlesungen und Übungen
Medienform:	rechnerbasierte Präsentation
Verantwortlicher:	Prof. Dr.-Ing. Ilona Rolfes
Dozenten:	Prof. Dr.-Ing. Ilona Rolfes Dr.-Ing. Jan Barowski M. Sc. Dennis Pohle M. Sc. Jonas Schorlemer Dipl.-Ing. Martin Schreurs M. Sc. Jonas Wagner
Sprache:	Deutsch
SWS:	4
Leistungspunkte:	5
Gruppengröße:	ca. 350 - 400
Angeboten im:	Wintersemester

Ziele: Nach erfolgreichem Abschluss des Moduls verfügen die Studierenden über Kenntnisse der grundlegenden Gesetze und Verfahren zur Berechnung von Strömen und Spannungen in elektrischen Gleich- und Wechselstromkreisen. Sie haben die Fähigkeit, elektrische Netzwerke zu analysieren, mathematisch korrekt zu beschreiben und umzuwandeln. Sie haben die Grundlagen der komplexen Wechselstromrechnung verstanden und können diese auf praktische Beispiele anwenden.

Inhalt: Das Modul bietet einen allgemeinen Einstieg in die Grundlagen der elektrischen Netzwerke. Es werden grundlegende Begriffe und Verfahren erläutert.

Die Vorlesung lässt sich in fünf Teile gliedern:

- Lineare Gleichstromschaltungen: Zählpfeile; Strom- und Spannungsquellen; Die Kirchhoffschen Gleichungen; einfache Widerstandsnetzwerke (Spannungsteiler, Stromteiler); reale Strom- und Spannungsquellen; Wechselwirkungen zwischen Quelle und Verbraucher (Zusammenschaltung von Spannungsquellen, Leistungsanpassung, Wirkungsgrad); Superpositionsprinzip; Analyse umfangreicher Netzwerke.
- Übergang zu zeitabhängigen Strom und Spannungsformen: Übersicht sowie Einführung verschiedener Kenngrößen (Mittelwert, Gleichrichtwert, Effektivwert, Maximalwert, Spitzenwert, Spitze-Spitze-Wert, Schwingungsbreite).
- Wechselstrom und Wechselspannung: Das Zeigerdiagramm; Komplexe Wechselstromrechnung; Beschreibung konzentrierter RLC Bauelemente und idealer Quellen; Einführung der Ortskurven; Berechnung einfacher Wechselstromkreise über die komplexe Ebene; Energie und Leistung bei Wechselspannung; Leistungsanpassung.
- Analyse von Netzwerken: Maschenstromverfahren; Knotenpotenzialverfahren.
- Einführung zu Zweitoren: Torbedingung; Zweitorgleichungen in Matrixform (Impedanz-, Admittanz-, Hybrid-, Kettenform); Zweitoreigenschaften (Reziprozität, Symmetrie); Matrizen elementarer Zweitore.

Voraussetzungen: keine

Empfohlene Vorkenntnisse: Mathematische Vorkenntnisse über die Grundlagen der Differential- und Integralrechnung sowie der Linearen Algebra

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 Klausurvorbereitung vorgesehen.

Prüfungsform: schriftlich, 120 Minuten

Beschreibung der Prüfungsleistung: Termin findet wie geplant statt

Literatur:

[1] Pregla, Reinhold "Grundlagen der Elektrotechnik", Hüthig, 2009
[2] Martius, Siegfried, Schaller, Gerd, Schmidt, Lorenz-Peter "Grundlagen der Elektrotechnik 3", Pearson Studium, 2006

2.2 142362: Bachelor-Forschungspraktikum Human-Centred Security

Nummer:	142362
Lehrform:	Praktikum
Medienform:	Videoübertragung e-learning Folien Moodle rechnerbasierte Präsentation
Verantwortlicher:	Prof. Dr. Martina Angela Sasse
Dozenten:	Prof. Dr. Martina Angela Sasse M. A. Annalina Buckmann M. A. Jennifer Friedauer
Sprache:	Deutsch
SWS:	3
Leistungspunkte:	3
Angeboten im:	Wintersemester und Sommersemester

Ziele: Die Veranstaltung vermittelt praktische Kenntnisse über Forschungsdesign, -Methoden und Auswertungsverfahren der Bereiche Usability und Human-Centred Security und Privacy. Die Studierenden erhalten eine praktische Einführung in die Methoden qualitativer und quantitativer Methoden sowie die Evaluation. So werden sie in die Lage versetzt, eigenständig Studien im Bereich der Usability und Human-Centred Security und Privacy durchzuführen, auszuwerten und kritisch zu hinterfragen.

Inhalt: Aufbauend auf den Inhalten der Vorlesung Usable Security and Privacy widmet sich der Kurs vor allem den praktischen Aspekten der Forschung, des Studiendesigns und der Auswertung in den Forschungsbereichen Usability und Human-Centred Security und Privacy. Neben den Grundlagen der Durchführung von Nutzerstudien werden grundlegende qualitative und quantitative Methodenkenntnisse der Usability- und User Experience-Forschung, des Collaborative Design, Labor- und Feldstudien sowie statistische Datenerhebung und -auswertung behandelt und praktisch angewandt. Eigene Studienprojekte werden unter Anleitung entworfen, ausgeführt und diskutiert. Die Studierenden lernen, Sicherheits- und Nutzbarkeitsrelevante Fragestellungen zu entwickeln, methodisch anzugehen und praktisch zu beantworten. Dabei sammeln sie praktische Erfahrung der verschiedenen Forschungsmethoden und werden so auf die Durchführung eigener Studien vorbereitet.

*** Aufgrund der aktuellen Situation wird das Forschungspraktikum auch im WiSe 2020/21 auf ein kontaktarmes Format umgestellt. Der Link zum Online-Meeting wird nach Anmeldung per EMail zugesandt. ***

Voraussetzungen: Keine

Empfohlene Vorkenntnisse:

- Usable Security and Privacy
- Human-Centred Security

- Allgemeine Kenntnisse der IT-Sicherheit

Arbeitsaufwand: 90 Stunden

Der Arbeitsaufwand berechnet sich wie folgt: 15 Wochen zu je 3 Stunden Anwesenheit, entsprechen 45 Stunden. Zum Schreiben des geforderten Quelltextes werden weitere ca. 45 Stunden benötigt.

Prüfungsform: Praktikum, studienbegleitend

2.3 142028: Bachelor-Praktikum ARM Processors for Embedded Cryptography

Nummer:	142028
Lehrform:	Praktikum
Medienform:	Moodle
Verantwortlicher:	Prof. Dr.-Ing. Tim Güneysu
Dozenten:	Prof. Dr.-Ing. Tim Güneysu Dr.-Ing. Max Hoffmann
Sprache:	Deutsch
SWS:	3
Leistungspunkte:	3
Gruppengröße:	Maximal 50 Studenten. —- Max. 50 students.
Angeboten im:	Wintersemester

Ziele: Absolventen des Praktikums kennen den Aufbau und die interne Funktion von Mikrocontrollern. Sie wissen wie ein Prozessor Maschinensprache verarbeitet und sind selbst in der Lage mittels Assembly maschinennah zu programmieren. Zudem sind sie in der Lage, hocheffiziente Implementierungen für die ARM Architektur zu erstellen, welche eine deutliche Geschwindigkeitsverbesserung im Vergleich zu C Implementierungen vorweisen. Da das Praktikum im besonderen ARM-Prozessoren behandelt und ARM eindeutiger Marktführer der Embedded-Branche ist, sind die Inhalte dieses Praktikums äußerst relevant. Das Praktikum setzt sich selbst das Ziel möglichst praxisnah zu arbeiten und die Aufgaben interessant zu gestalten, sodass die Teilnehmer einen Nutzen für spätere Arbeiten daraus ziehen können.

Inhalt: In diesem Praktikum wird der Umgang mit ARM Mikrocontrollern erarbeitet. Dazu erhält jeder Teilnehmer ein Board mit einem ARM Cortex-M4 basierten Mikrocontroller. Die Teilnehmer erlernen zunächst die Grundlagen über CISC und RISC Mikrocontroller. Sie erlernen, wie Code von Hardware ausgeführt wird und wie sie selbst maschinennahen Code schreiben können. Bereits nach den ersten beiden Praktikumsterminen sind die Teilnehmer in der Lage, kleine Programme in Assembly für die ARM Architektur zu entwickeln. Während der folgenden Termine werden die Kenntnisse bezüglich der ARM Architektur und des Boards vertieft. Die Teilnehmer lernen, wie Mikrocontroller untereinander und mit Peripheriegeräten kommunizieren. Die theoretischen Inhalte werden von praktischen Hausaufgaben begleitet. Die Teilnehmer implementieren nach und nach Programme in C und Assembly, um verschiedene Funktionalitäten des Boards zu verwenden. Nachdem die Teilnehmer mit ARM Assembly vertraut geworden sind, werden unterschiedliche kryptographische Anwendungen implementiert. Dabei liegt der Fokus besonders auf Effizienz und es muss stets eine C Implementierung geschlagen werden. Die besten Teilnehmer erhalten ein Zertifikat sowie einen Preis.

Voraussetzungen: keine

Empfohlene Vorkenntnisse: Grundkenntnisse in Kryptographie (Einführung in die Kryptopgraphie I und II) und C

Arbeitsaufwand: 90 Stunden

Der Arbeitsaufwand berechnet sich wie folgt: 6 Termine zu je 3 Stunden entsprechen 18 Stunden Anwesenheit. Für die Vorbereitung werden 18 Stunden (3 Stunden je Termin für 6 Termine), für die Bearbeitung der Übungszettel 9 Stunden (3 Stunden je Übungszettel für drei Übungszettel), und für die Implementierungsaufgaben 45 Stunden veranschlagt.

Prüfungsform: Praktikum, studienbegleitend

Voraussetzungen für die Vergabe von Kreditpunkten: Bestehen des finalen Projektes. —- Finishing the final project.

2.4 142245: Bachelor-Praktikum TLS Implementierung

Nummer:	142245
Lehrform:	Praktikum
Medienform:	Moodle rechnerbasierte Präsentation
Verantwortlicher:	Prof. Dr. Jörg Schwenk
Dozenten:	Prof. Dr. Jörg Schwenk M. Sc. Matthias Gierlings M. Sc. Marcel Maehren M. Sc. Robert Merget
Sprache:	Deutsch
SWS:	3
Leistungspunkte:	3
Angeboten im:	Wintersemester

Ziele: Die Studierenden lernen ein modernes kryptographisches Protokoll detailliert kennen. Die Studierenden arbeiten mit Konzepten der modernen Softwareentwicklung. Ein Ausblick auf aktuelle Forschung in diesem Bereich wird gegeben.

Inhalt: Das TLS-Protokoll ist das wichtigste kryptographische Protokoll im Internet und wird beim Schutz von jeder wichtigen Webseite oder Webservices eingesetzt. In den letzten Jahren wurden viele Angriffe auf dieses Protokoll bekannt, wie z.B. POODLE, DROWN, Lucky 13 oder ROBOT. Deswegen wurde in den letzten Jahren in Zusammenarbeit von Industrie und Wissenschaft eine neue TLS Version entwickelt: TLS 1.3. Die neue Version sollte gegen alle bekannten Angriffe schützen und gleichzeitig die Performance von TLS erhöhen. TLS 1.3 verwendet nur die neuesten kryptographischen Mechanismen, so dass das Protokoll-Design für jeden Krypto-Entwickler und Designer von großem Interesse ist.

Im Rahmen des Praktikums implementieren die Studenten einen TLS 1.3 Server. Dabei wird diese Aufgabe in mehrere Teilaufgaben zerlegt und das Thema schrittweise an die Studenten herangeführt. Es werden weiterhin folgende Themen besprochen:

- Einführung in TLS, JUnit Tests und Git
- TLS 1.3
- Kryptographie mit Java
- Clean Code
- TLS-Attacker
- TLS Fuzzing

Empfohlene Vorkenntnisse:

- Erfolgreicher Abschluss der Lehrveranstaltung Netzsicherheit 2
- Programmierkenntnisse 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.

Prüfungsform: Praktikum, studienbegleitend

2.5 142021: Bachelor-Projekt Embedded Smartcard Microcontrollers

Nummer: 142021
Lehrform: Projekt
Medienform: Folien
rechnerbasierte Präsentation
Verantwortlicher: Prof. Dr.-Ing. Christof Paar
Dozenten: Prof. Dr.-Ing. Christof Paar
Dr.-Ing. Max Hoffmann
Sprache: Deutsch
SWS: 3
Leistungspunkte: 3
Angeboten im:

Ziele: Dieses Praktikum verfolgt im Wesentlichen die folgenden drei Lernziele: Erstens kennen die Teilnehmer des Praktikums eine 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.

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. Jeder Student erhält Zugriff auf eine Smartcard mit einem Atmel AVR Mikrocontroller, sowie einem Kartenschreib- bzw. -lesegerät. Dieser implementiert eine vorgegebene Blockchiffre (die jährlich wechselt) in Assembler, und muss diese auf der Smartcard unter realistischen Bedingungen lauffähig bekommen. Beispiele für Algorithmen sind AES, 3DES und lightweight Chiffren. Um die Motivation der Praktikumsteilnehmer zu erhöhen, werden die effizientesten Implementierungen mit einer Urkunde und einem Buchpreis belohnt.

Voraussetzungen: keine

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

Arbeitsaufwand: 90 Stunden

Für die Einarbeitung mit Betreuer werden 15 h angesetzt. Für die Bearbeitung des Projekts 50 h. Für die anschließende Ausarbeitung werden 25h angesetzt.

Prüfungsform: Projektarbeit, studienbegleitend

2.6 142242: Bachelor-Projekt Netz- und Datensicherheit

Nummer:	142242
Lehrform:	Projekt
Verantwortlicher:	Prof. Dr. Jörg Schwenk
Dozenten:	Prof. Dr. Jörg Schwenk
	M. Sc. Robert Merget
Sprache:	Deutsch
SWS:	3
Leistungspunkte:	3
Angeboten im:	Wintersemester und Sommersemester

Ziele: Die Studierenden analysieren die Sicherheit ausgewählter Protokolle und Implementierungen (z.B. TLS, IPsec, JSON Web Crypto), oder implementieren selber Tools für spezifische Sicherheitsanalysen (z.B. Plugins für Burp Suite).

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, oder zusammengefasst als Block (insgesamt ca. 90h) 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.

Es wird eine Projektaufgabe unter Anleitung bearbeitet. Themen sind hierbei Fragestellungen der Netz- und Datensicherheit. Beispiele sind die Software-Implementierung XML-basierter Protokolle oder TLS.

Voraussetzungen: keine

Empfohlene Vorkenntnisse: Grundlagen der Kryptographie, Datensicherheit und Netzsicherheit, Programmierkenntnisse (nachweisbar z.B. durch eine erfolgreiche Teilnahme am Praktikum Security Appliances)

Arbeitsaufwand: 90 Stunden

Für die Einarbeitung mit Betreuer werden 15 h angesetzt. Für die Bearbeitung des Projekts 50 h. Für die anschließende Ausarbeitung werden 25h angesetzt.

Prüfungsform: Projektarbeit, studienbegleitend

2.7 143243: Bachelor-Seminar Aktuelle Themen der IT-Sicherheit

Nummer:	143243
Lehrform:	Seminar
Medienform:	rechnerbasierte Präsentation
Verantwortlicher:	Prof. Dr. Thorsten Holz
Dozent:	Prof. Dr. Thorsten Holz
Sprache:	Deutsch
SWS:	3
Leistungspunkte:	3
Gruppengröße:	10-15 Studierende
Angeboten im:	Wintersemester und Sommersemester

Ziele: Die Studierenden lernen Methoden des forschungsnahen Lernens kennen und sind in der Lage, eigenständig ein eng umgrenztes Themengebiet anhand von einem wissenschaftlichen Paper zu erarbeiten. Die Studierenden lernen eigenständig Fachliteratur zu einem bestimmten Themengebiet zu verstehen und bekommen einen Einblick in aktuelle Forschungsthemen. Durch die Ausarbeitung haben die Studierenden das Schreiben eigener Texte und die Zusammenfassung komplexer Themengebiete geübt. Die Studierenden lernen durch das Konferenzseminar den Peer-Review-Prozess und wissenschaftliches Arbeiten kennen. Darüber hinaus liefert der Vortrag die Möglichkeit, die Präsentation von wissenschaftlichen Ergebnissen zu erlernen und den Stoff zu vertiefen.

Inhalt: In jedem Semester bietet der Lehrstuhl ein Bachelor-Seminar zum Thema "Aktuelle Themen der IT-Sicherheit" an, der Fokus liegt auf den Bereichen Softwaresicherheit, Neetzwerksicherheit, Privacy, Reverse Engineering und ähnlichen Themen aus dem Bereich der systemnahen IT-Sicherheit. Dazu sollen die Studierenden selbständig ein eng umfasstes Themengebiet bearbeiten und eine Ausarbeitung sowie einen Vortrag zu diesem Thema verfassen. Die Ausarbeitung hat einen Umfang von etwa 15 Seiten und der Vortrag soll etwa 20 Minuten dauern. Daran schließt sich eine Diskussion von 5 Minuten an.

Das Seminar wird als Konferenzseminar durchgeführt, der Ablauf ist ähnlich zu einer wissenschaftlichen Konferenz. Neben dem Erstellen einer wissenschaftlichen Ausarbeitung lernen die Studierenden das Peer-Review-Verfahren kennen: Ein wichtiger Aspekt des Seminars ist die Erstellung von konstruktiven Feedbacks zur Ausarbeitung anderer Studierender, zum Beispiel durch Hinweise zur Verbesserung der Darstellung. Ein solches Feedback soll dann auch in der eigenen Ausarbeitung berücksichtigt und eingearbeitet werden.

Voraussetzungen: keine

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

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.

Prüfungsform: Seminarbeitrag, studienbegleitend

Voraussetzungen für die Vergabe von Kreditpunkten: Die Ausarbeitung hat einen Umfang von etwa 15 Seiten und der Vortrag soll etwa 20 Minuten dauern. Daran schließt sich eine Diskussion von 5 Minuten an. Die Studierende geben im Rahmen des Konferenzseminars Feedback zu den Ausarbeitungen anderer Studierender.

2.8 143020: Bachelor-Seminar Embedded Security

Nummer:	143020
Lehrform:	Seminar
Medienform:	rechnerbasierte Präsentation
Verantwortlicher:	Priv.-Doz. Dr. Amir Moradi
Dozenten:	Priv.-Doz. Dr. Amir Moradi
	M. Sc. Anita Aghaie
	M. Sc. Aein Rezaei Shahmirzadi
Sprache:	Deutsch
SWS:	3
Leistungspunkte:	3
Angeboten im:	

Ziele: Die Teilnehmer können technische und wissenschafltiche Literatur finden, verstehen und auswerten. Sie erlernen das Verfassen technischer Berichte und Präsentationstechniken.

Inhalt: Die Teilnehmer erarbeiten sich eigentständig ein ausgewähltes Thema aus der eingebetteten Sicherheit und dem größeren Gebiet der allgemeinen IT-Sicherheit. In der Regel werden hierfür wissenschaftliche Veröffentlichungen untersucht. Die Studenten fertigen eine Ausarbeitung und präsentieren ihre Ergebnisse.

Das Spektrum möglicher Themen reicht von der Sicherheitsanalyse eingebetteter Systeme über kryptographische Algorithmen bis hin zur Sicherheit in neuartigen Anwendungsszenarien wie beispielsweise der Elektromobilität.

Voraussetzungen: keine

Empfohlene Vorkenntnisse: Grundlegende Kenntnisse der Kryptographie

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.

Prüfungsform: Seminarbeitrag, studienbegleitend

2.9 143249: Bachelor-Seminar Human Centered Security and Privacy

Nummer:	143249
Lehrform:	Seminar
Medienform:	Videoübertragung e-learning Folien Moodle rechnerbasierte Präsentation
Verantwortlicher:	Prof. Dr. Martina Angela Sasse
Dozenten:	Prof. Dr. Martina Angela Sasse M. Sc. Konstantin Fischer
Sprache:	Deutsch
SWS:	3
Leistungspunkte:	3
Angeboten im:	Wintersemester und Sommersemester

Ziele: Die Studierenden haben einen Einblick in aktuelle Forschungsthemen und können eigenständig Fachliteratur zu einem bestimmten Themengebiet verstehen. Sie sind in der Lage eigene Texte und die Zusammenfassung komplexer Themengebiete zu verfassen. Darüber hinaus können sie einen Vortrag zur Präsentation von wissenschaftlichen Ergebnissen halten.

Inhalt: Es wird eine Auswahl an aktuellen Forschungsarbeiten im Bereich der nutzerorientierten Sicherheit und Privatheit bereitgestellt. Thematische Schwerpunkte sind u.a. die Nutzbarkeit von sicheren Authentifizierungsverfahren, Phishing und Selbstwirksamkeit in der IT-Sicherheit. Dazu erarbeiten die Studierenden anhand von Forschungsarbeiten selbständig ein Themengebiet und produzieren ein “Literature Review” als Seminararbeit. Zum Abschluss des Seminars hält jeder Student einen Vortrag über seine Arbeit.

Voraussetzungen: Keine

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.

Prüfungsform: Seminarbeitrag, studienbegleitend

2.10 150508: Bachelor-Seminar Kryptographie

Nummer: 150508
Lehrform: Seminar
Medienform: rechnerbasierte Präsentation
Verantwortlicher: Prof. Dr. Eike Kiltz
Dozent: Prof. Dr. Eike Kiltz
Sprache: Deutsch
SWS: 3
Leistungspunkte: 3
Angeboten im:

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.

Prüfungsform: Seminarbeitrag, studienbegleitend

2.11 150507: Bachelor-Seminar Kryptologie

Nummer: 150507
Lehrform: Seminar
Medienform: rechnerbasierte Präsentation
Verantwortlicher: Prof. Dr. Alexander May
Dozent: Prof. Dr. Alexander May
Sprache: Deutsch
SWS: 3
Leistungspunkte: 3
Angeboten im:

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.

Prüfungsform: Seminarbeitrag, studienbegleitend

2.12 143241: Bachelor-Seminar Netz- und Datensicherheit

Nummer:	143241
Lehrform:	Seminar
Medienform:	rechnerbasierte Präsentation
Verantwortlicher:	Prof. Dr. Jörg Schwenk
Dozenten:	Prof. Dr. Jörg Schwenk M. Sc. Matthias Gierlings Dr.-Ing. Martin Grothe
Sprache:	Deutsch
SWS:	3
Leistungspunkte:	3
Angeboten im:	Wintersemester und Sommersemester

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

Inhalt: Ausgewählte Themen der IT-Sicherheit mit Bezug zur Netz- und Datensicherheit werden von den Studierenden eigenständig erarbeitet.

Vorläufige Termine/Meilensteine

- 27.10.20, 14:15: Einführungsveranstaltung (Webinar, Anwesenheitpflicht)
- 11.11.20: Abgabe Exposé
- 07.12.20: Abgabe Vorabversion
- 17.12.20: Abgabe gegenseitiges Feedback
- 11.01.21: Abgabe überarbeitete Version
- 25.01.21: Betreuerfeedback
- 01.02.21: Abgabe endgültige Version
- TBD: Abschlusspräsentation (Webinar, Anwesenheitpflicht)

Hinweis: Es werden keine Teilnahme-/Leistungsscheine ausgestellt. Die Ergebnisse werden direkt an das Prüfungsamt gemeldet.

Bei Fragen zu eurem Thema bitte den Betreuer direkt kontaktieren.

Ausarbeitungen: Vorlage: http://nds.rub.de/teaching/theses/seminar/

Anmerkungen:

Alle registrierten Seminarteilnehmer erhalten rechtzeitig Einladungen mit Links/Einwahldaten zu Onlineterminen per E-Mail (Onlineveranstaltungen finden typischerweise via Zoom statt).

Ziel des Seminars ist die Vorstellung einer wissenschaftlichen Veröffentlichung. Hierzu werden bereits veröffentlichte Artikel zur Auswahl angeboten.

Die Seminarteilnehmer sollen die Veröffentlichung im Rahmen des Seminars verständlich erarbeiten und evtl. benötigte Grundlagen kurz und präzise einführen.

Die Zuteilung von Seminar-Themen geschieht über die zentrale Seminarverteilung https://seminar.hgi.rub.de/. Nach der Zuteilung des vorausgewählten Seminarthemas ist ein zweiseitiges Exposé über das Thema (Idee des Papiers und Struktur, zu erklärende Fragestellungen und Fokus der Seminararbeit) beim jeweiligen Betreuer einzureichen.

Die Ausarbeitung sollte folgenden Umfang haben:

- 12 Seiten für Bachelorstudierende
- 15 Seiten für Masterstudierende
- 25 Seiten für Themen, die von zwei Personen bearbeitet werden

Ausnahmen oder Abweichungen sind mit dem jeweiligen Betreuer abzustimmen. Vor dem endgültigen Abgabetermin wird es zwei Feedbackrunden geben (einmal von den anderen Seminarteilnehmern, einmal vom Betreuer). Die jeweiligen Anmerkungen sind in der finalen Version zu berücksichtigen bzw. zu korrigieren.

Ein Seminarvortrag umfasst üblicherweise 15-20 Minuten, einschließlich einer anschließenden Fragerunde. Das Foliendesign sowie die Vortragssprache (deutsch, englisch) sind freigestellt. Bitte reichen Sie Ihre Ausarbeitung und Präsentation im PDF Format ein. Powerpoint-Formate sind nicht erlaubt. Fragen und Korrekturen durch die Betreuer sind während des Vortrags möglich.

Anwesenheitspflicht:

- Zur Einführungsveranstaltung besteht Anwesenheitspflicht.
- Am Ende des Semesters werden die Vorträge innerhalb eine Blocktermins abgehalten (KEINE WÖCHENTLICHEN TERMINE!). An diesem Termin besteht Anwesenheitspflicht.

Voraussetzungen: keine

Empfohlene Vorkenntnisse: Grundlegende Kenntnisse der Kryptographie und / oder Netzwerksicherheit, sowie Latex Kenntnisse.

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 benotet werden.

Prüfungsform: Seminarbeitrag, studienbegleitend

2.13 141035: Bachelor-Seminar Security Engineering

Nummer:	141035
Lehrform:	Seminar
Medienform:	Folien
	Handouts
Verantwortlicher:	Priv.-Doz. Dr. Amir Moradi
Dozenten:	Priv.-Doz. Dr. Amir Moradi
	M. Sc. Aein Rezaei Shahmirzadi
Sprache:	Englisch
SWS:	3
Leistungspunkte:	3
Angeboten im:	Wintersemester und Sommersemester

Ziele: Die Teilnehmer können technische und wissenschafltiche Literatur finden, verstehen und auswerten. Sie erlernen das Verfassen technischer Berichte und Präsentationstechniken.

Inhalt: Die Teilnehmer erarbeiten sich eigentständig ein ausgewähltes Thema aus dem Bereich des Security Engineering und dem größeren Gebiet der allgemeinen IT-Sicherheit. In der Regel werden hierfür wissenschaftliche Veröffentlichungen untersucht. Die Studenten fertigen eine Ausarbeitung und präsentieren ihre Ergebnisse.

Das Spektrum möglicher Themen reicht von der Design- und Entwurfsmethodiken zur Entwicklung sicherer Systeme, CAD for Security, Security for Design sowie insbesondere die Untersuchung von grundsätzlichen Schwachstellen in Anwendungen der IT-Sicherheit.

Empfohlene Vorkenntnisse: Einführung in die Kryptographie Grundlagen der Netz- und Systemsicherheit

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.

Prüfungsform: Seminarbeitrag, studienbegleitend

2.14 148213: Bachelor-Seminar Sichere Hardware

Nummer: 148213
Lehrform: Seminar
Medienform: rechnerbasierte Präsentation
Verantwortlicher: Prof. Dr.-Ing. Tim Güneysu
Dozent: Prof. Dr.-Ing. Tim Güneysu
Sprache: Deutsch
SWS: 3
Leistungspunkte: 3
Angeboten im:

Ziele: Die Teilnehmer können technische und wissenschafltiche Literatur finden, beschaffen verstehen und auswerten. Sie können diese wissenschaftlich präsentieren.

Inhalt: Ausgewählte Themen der IT-Sicherheit werden von den Studierenden eigenständig erarbeitet. Das Spektrum möglicher Themen reicht von der Sicherheitsanalyse eingebetteter Systeme über kryptographische Algorithmen für leistungsbeschränkte Geräte bis hin zu verschiedenen Aspekten der hardwarenahen Sicherheit. Soweit möglich werden Themen in Anlehnung an eine gerade laufende Wahlpflichtveranstaltung gewählt, um didaktische Synergieeffekte zu nutzen.

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.“

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.

Prüfungsform: Seminarbeitrag, studienbegleitend

2.15 150509: Bachelor-Seminar Symmetrische Kryptographie

Nummer: 150509
Lehrform: Seminar
Medienform: rechnerbasierte Präsentation
Verantwortlicher: Prof. Dr. Gregor Leander
Dozent: Prof. Dr. Gregor Leander
Sprache: Deutsch
SWS: 3
Leistungspunkte: 3
Angeboten im:

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

Inhalt: Die Teilnehmer erarbeiten sich eigentständig ein ausgewähltes Thema aus der symmetrischen Kryptographie. In der Regel werden hierfür wissenschaftliche Veröffentlichungen von einer wichtigen Kryptographie-Konferenzen untersucht. Die Studenten fertigen eine Ausarbeitung und präsentieren ihre Ergebnisse.

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.

Prüfungsform: Seminarbeitrag, studienbegleitend

2.16 143290: Bachelor-Seminar Usable Security and Privacy Research

Nummer:	143290
Lehrform:	Seminar
Medienform:	Folien
Verantwortlicher:	Prof. Dr. Markus Dürmuth
Dozenten:	Prof. Dr. Markus Dürmuth M. Sc. Philipp Markert
Sprache:	Deutsch
SWS:	3
Leistungspunkte:	3
Angeboten im:	Wintersemester und Sommersemester

Ziele: Die Studierenden lernen den aktuellen Forschungsstand des Feldes "Usable Security and Privacy" kennen. Sie bekommen Erfahrung im kritischen Umgang mit wissenschaftlicher Literatur und erlangen einen Überblick über Themen und Forschungsmethoden. Zusätzlich dazu erlangen die Studierenden einen Einblick in die Publikationspraxis im Forschungsgebiet. Dazu wird der Begutachtungsprozess einer hochwertigen wissenschaftlichen Konferenz simuliert. Studierende schreiben Gutachten für Publikationen, setzen sich damit in einer Dikussionsrunde kritische auseinander und werden abschließend Vorträge zu ausgewählten Publikationen halten.

Inhalt: Das Seminar behandelt insbesondere folgende Themen:

Einführung Überblick Motivation Themen und Forschungsmethoden

Wissenschaftliche Praxis Reviews für Paper Rebuttals und Meta-Reviews PC Meeting Konferenztag

Zentrale Themen Zentrale Fragestellungen und angewandte Methoden der benutzbaren IT-Sicherheit. Wissenschaftliche Publikationspraxis: Von der Einreichung, über die Auswahl von Beiträgen bis zur Vorstellung auf einer Konferenz

Voraussetzungen: Keine

Empfohlene Vorkenntnisse: Keine

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.

Prüfungsform: Seminarbeitrag, studienbegleitend

2.17 150583: Bachelor-Vertiefungspraktikum SAGE in der Kryptographie

Nummer: 150583
Lehrform: Praktikum
Verantwortlicher: Prof. Dr. Gregor Leander
Dozent: Prof. Dr. Gregor Leander
Sprache: Deutsch
SWS: 2
Leistungspunkte: 3
Angeboten im:

Ziele: Die Studierenden lernen das open source Computeralgebrasystem "SAGE" kennen. Anhand von mehreren kleineren Projekten werden kryptographisch relevante Aufgaben gelöst.

Inhalt: Die Software "SAGE" bietet ein mächtiges Werkzeug um relativ einfach und schnell viele Probleme in der Kryptographie praktisch umzusetzen. Wir beschäftigen uns beispielhaft unter Anderem mit Algorithmen zum Faktoiriziden, dem Berechnen von diskreten Logarithmen und dem Lösen von Gleichungssystemen.

Voraussetzungen: Grundkenntnisse über Kryptographie, wie sie zum Beispiel in der "Einführung in die Kryptographie I und II" behandelt werden, sind hilfreich, aber nicht nötig

Empfohlene Vorkenntnisse: Grundkenntnisse über Kryptographie, wie sie zum Beispiel in der "Einführung in die Kryptographie I und II" behandelt werden, sind hilfreich, aber nicht nötig.

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.

Prüfungsform: Praktikum, studienbegleitend

2.18 142247: Bachelor-Vertiefungspraktikum Security Appliances

Nummer:	142247
Lehrform:	Praktikum
Medienform:	e-learning Handouts rechnerbasierte Präsentation
Verantwortlicher:	Prof. Dr. Jörg Schwenk
Dozenten:	Prof. Dr. Jörg Schwenk Dr.-Ing. Dennis Felsch Dr.-Ing. Christian Mainka M. Sc. Paul Rösler
Sprache:	Deutsch
SWS:	3
Leistungspunkte:	3
Angeboten im:	

Ziele: Die Studierenden haben einen umfassenden Einblick in die Welt der bargeldlosen Zahlung und Zahlungsabwicklung. Sie haben ein Verständnis für die verwendeten Datenformate, Prozesse und die notwendige Infrastruktur entwickelt und den Umgang, die Programmierung und den Betrieb von Hardware-Sicherheitsmodulen (HSM)erlernt. Sie bescherrschen die Einbindung und Verwendung einer HSM in Java unter Verwendung der Java Cryptographic Extension (JCE) sowie die Programmierung einer Firewall-Anwendung für Service-orientierte Architekturen (SOA).

Inhalt: Egal ob die neue App für das Handy, der schnelle Einkauf im Netz oder das Abendessen im Restaurant - täglich nutzen wir die Bequemlichkeit bargeldloser Zahlungssysteme ohne auch nur einen Gedanken an die notwendige Infrastruktur, die Prozesse und vor allem die Sicherheit hinter der Fassade zu verlieren.

Dieses Praktikum bietet eine Einführung in die Infrastruktur hinter bargeldlosem Zahlungsverkehr am Beispiel von Kreditkarten-basierter Zahlung. Inhalte sind die notwendigen Prozesse, Datenformate und deren Sicherheit.

Während des Praktikums werden notwendige Prozesse zur Abwicklung einer Zahlung nachimplementiert und in einer simulierten Point-of-Sales-Umgebung getestet. Hierbei steht besonders die notwendige Hardware zur sicheren Zahlungsabwicklung im Vordergrund. Die erarbeiteten Softwarekomponenten werden mit echten und simulierten Hardware-Sicherheitsmodulen (HSMs) interagieren.

Die Teilnehmer erwartet eine Schulung im Umgang mit HSMs direkt durch den Hersteller Utimaco. Des Weiteren wird auch ein tiefer Einblick in die Arbeitsweise von XML-Firewall-Hardware am Beispiel einer IBM DataPower-Appliance vermittelt.

Das Praktikum wird mit Unterstützung der Utimaco GmbH durchgeführt.

Voraussetzungen: keine

Empfohlene Vorkenntnisse: Programmierkenntnisse in C und 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.

Prüfungsform: Praktikum, studienbegleitend

2.19 142025: Bachelor-Vertiefungspraktikum Wireless Physical Layer Security

Nummer:	142025
Lehrform:	Praktikum
Medienform:	Folien rechnerbasierte Präsentation
Verantwortlicher:	Prof. Dr.-Ing. Christof Paar
Dozent:	Dr.-Ing. Christian Zenger
Sprache:	Deutsch
SWS:	3
Leistungspunkte:	3
Angeboten im:	Wintersemester und Sommersemester

Ziele: Dieses Praktikum verfolgt im Wesentlichen die folgenden drei Lernziele: Erstens kennen die Teilnehmer des Praktikums eine Software Defined Radio (SDR) Architektur und deren Programmierung mit ‚GNU Radio'. Zweitens wird der Umgang mit SDRs, sowie Wissen über die entsprechenden Funkstandards und potenzielle Angriffe beherrscht. Drittens sind die Implementierungs- und Evaluierungsaspekte von modernen Funkkanal-basierten Sicherheitsarchitekturen bekannt. Python wird als Programmiersprachen verwendet. 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 Software Defined Radios (SDRs). Bereits nach dem ersten Praktikumstermin sind die Studenten in der Lage passive Lauschangriffe mit GNU Radio für die RTL-SDR Architektur zu entwickeln. Während der folgenden Termine werden die Kenntnisse bezüglich der SDR Architektur und Funkstandards vertieft. Darüber hinaus müssen die Praktikumsteilnehmer immer komplexere Programme als Hausaufgaben schreiben. Im zweiten Teil des Praktikums erlernen die Studenten den Umgang mit Funkkanal-basierten Sicherheitsarchitekturen. Der Kanal-basierte Schlüsselgenerierung und Kanal-basiertes Fingerprinting werden vorgestellt. Die Studenten werden anschließend in Gruppen à drei Personen aufgeteilt. Jede Gruppe erhält ein Messsetup basierend aus drei Raspberry Pis, Funkmodulen und einer Messsoftware, sowie eine Virtuelle Maschine mit vorkonfiguriertem Evaluationsframework. Jede Gruppe implementiert eine vorgegebene Kanal-basierte Sicherheitsarchitektur (jährliche eine andere) in Python, und muss diese im Evaluationsframework unter realistischen Bedingungen lauffähig bekommen. Um die Motivation der Praktikumsteilnehmer zu erhöhen, werden die effizientesten Implementierungen mit Buchpreisen belohnt.

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

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

Arbeitsaufwand: 90 Stunden

Der Arbeitsaufwand berechnet sich wie folgt: 6 Termine zu je 3 Stunden entsprechen 18 Stunden Anwesenheit. Für die Vorbereitung werden 18 Stunden (3 Stunden je Termin für 6 Termine), für die Bearbeitung der Übungszettel 9 Stunden (3 Stunden je Übungszettel für drei Übungszettel), und für die Implementierungsaufgaben 45 Stunden veranschlagt.

Prüfungsform: Praktikum, studienbegleitend

2.20 142244: Bachelor-Vertiefungspraktikum zur Hackertechnik

Nummer:	142244
Lehrform:	Praktikum
Medienform:	Videoübertragung e-learning Folien Internet Moodle
Verantwortlicher:	Prof. Dr. Jörg Schwenk
Dozenten:	Prof. Dr. Jörg Schwenk M. Sc. Lukas Knittel Dr.-Ing. Marcus Niemietz
Sprache:	Deutsch
SWS:	3
Leistungspunkte:	3
Angeboten im:	Wintersemester und Sommersemester

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

Teilnahme an mindestens 7 Vorträgen zu je 1 Stunde mit jeweils anschließender Diskussion ergibt in etwa 9 Stunden. Die Bearbeitung von insgesamt 9 Versuchen mit je 5 Stunden Durchführung und je 4 Stunden Vor- und Nachbereitung ergibt 81 Stunden.

Prüfungsform: Praktikum, studienbegleitend

2.21 144002: Bachelorarbeit ITS

Nummer: 144002
Lehrform: Bachelorarbeit
Verantwortlicher: Studiendekan ITS
Dozent: Hochschullehrer der Fakultät ET/IT
Sprache: Deutsch
Leistungspunkte: 12
Gruppengröße: /
Angeboten im: Wintersemester und Sommersemester

Ziele: Die Studierenden beherrschen die Grundkenntnisse der wissenschaftlichen Arbeit, der Projektorganisation und der Präsentation wissenschaftlicher Ergebnisse.

Inhalt: Lösung einer wissenschaftlichen Aufgabe unter Anleitung. Teilnahme an 5 Kolloquiumsvorträgen über die Ergebnisse von Bachelorarbeiten in der Fakultät ET & IT. Präsentation der eigenen Ergebnisse der Bachelorarbeit im Kolloquium.

Abschlussarbeiten können grundsätzlich bei allen Hochschullehrern der Fakultät und bei den am Studiengang beteiligten Hochschullehrern der Fakultät für Mathematik angefertigt werden.

Eine Übersicht der Hochschullehrer der **Fakultät für Elektrotechnik und Informationstechnik** befindet sich unter: https://www.ei.rub.de/fakultaet/professuren/

In der Fakultät für Mathematik sind dies:

- **Lehrstuhl für Kryptologie und IT-Sicherheit - Prof. May**
  http://www.cits.rub.de
- **Lehrstuhl für Kryptographie - Prof. Kiltz** http://www.foc.rub.de/
- **Arbeitsgruppe für Symmetrische Kryptographie - Prof. Leander**
  http://www.cits.rub.de/personen/index.html

Voraussetzungen: siehe Prüfungsordnung

Empfohlene Vorkenntnisse: Vorkenntnisse entsprechend dem gewählten Thema erforderlich

Arbeitsaufwand: 360 Stunden

3 Monate Vollzeittätigkeit

Prüfungsform: Abschlussarbeit, studienbegleitend

2.22 141246: Betriebssysteme

Nummer:	141246
Lehrform:	Vorlesungen und Übungen
Medienform:	e-learning Moodle rechnerbasierte Präsentation
Verantwortlicher:	Jun. Prof. Dr.-Ing. Timo Hönig
Dozent:	Jun. Prof. Dr.-Ing. Timo Hönig
Sprache:	Deutsch
SWS:	4
Leistungspunkte:	5
Gruppengröße:	170
Angeboten im:	Sommersemester

Ziele: Die Studierenden erlangen ein solides Grundverständnis von modernen Betriebssystemen, ihrer Funktion und ihrer Implementierung. Die Studierenden sind nach Abschluss des Moduls in der Lage, verschiedene Aspekte eines Betriebssystems wie Prozess- und Speichermanagement zu verstehen und zu nutzen, sie können dabei verschiedene Designentscheidungen eigenständig analysieren und bewerten. Sie sind in der Lage, bestimmte Aspekte eines Betriebssystems selbst zu designen und diese argumentativ zu verteidigen.

Inhalt: Es werden die wichtigsten Grundlagen zu Betriebssystemen vorgestellt. Dazu gehören zum Beispiel:

- Betriebssystemkonzepte
- Prozesse und Threads, Interprozesskommunikation
- Scheduling-Mechanismen
- Speicherverwaltung, Speicherabstraktionen, Paging
- Dateisysteme
- Eingabe- und Ausgabeverwaltung
- Algorithmen zur Vermeidung von Deadlocks

Ergänzend zur Vorlesung werden Übungsaufgaben gestellt und in der Übungsstunde besprochen. Um den Bezug zu modernen Betriebssystemen (aktuellen Versionen von Linux, Windows, und macOS) herzustellen, werden die Themen an praktischen Beispielen illustriert. Dies ermöglicht es den Studierenden, die in der Vorlesung besprochenen Themen praktisch nachzuvollziehen.

Voraussetzungen: keine

Empfohlene Vorkenntnisse: Grundkenntnisse der Informatik

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 Klausurvorbereitung vorgesehen.

Prüfungsform: schriftlich, 120 Minuten

Beschreibung der Prüfungsleistung: Termin wird vorläufig auf Ende März / Anfang April verschoben

Voraussetzungen für die Vergabe von Kreditpunkten: Bestandene Modulklausur, Bonuspunkte für erfolgreiche Bearbeitung der Übungsblätter

2.23 150357: Boolesche Funktionen mit Anwendungen in der Kryptographie

Nummer: 150357
Lehrform: Vorlesung
Verantwortlicher: Prof. Dr. Gregor Leander
Dozent: Prof. Dr. Gregor Leander
Sprache: Deutsch
SWS: 4
Leistungspunkte: 5
Angeboten im: Sommersemester

Ziele: Die Studierenden lernen die theoretischen Hintergründe von Booleschen Funktionen kennen.

Inhalt: In dieser Vorlesung beschäftigen wir uns mit der Theorie von Booleschen Funktionen. Der Fokus liegt hierbei auf den kryptographisch relevanten Kriterien für Boolesche Funktionen wie Nicht-Linearität und differentielle Uniformität.

Voraussetzungen: keine

Empfohlene Vorkenntnisse: Grundlegende Kenntnisse über endliche Körper

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 Klausurvorbereitung vorgesehen.

Prüfungsform: mündlich, 30 Minuten

2.24 141250: Computernetze

Nummer:	141250
Lehrform:	Vorlesungen und Übungen
Medienform:	Moodle rechnerbasierte Präsentation
Verantwortlicher:	Prof. Dr. Jörg Schwenk
Dozenten:	Dr.-Ing. Christian Mainka Dr.-Ing. Dennis Felsch M. Sc. Matthias Gierlings M. Sc. Simon Rohlmann
Sprache:	Deutsch
SWS:	4
Leistungspunkte:	5
Gruppengröße:	ca. 400
Angeboten im:	Sommersemester

Ziele: Nach dem erfolgreichen Abschluss des Moduls

- kennen Studierende die wichtigsten Standards, die das heutige Internet verwendet.
- kennen Studierende grundlegende Angriffskonzepte auf Computernetzwerke
- verstehen Studierende den Zusammenhang zwischen den einzelnen Schichten eines Computernetzwerks und der darin enthaltenen Protokolle
- können Studierende die wichtigsten Netzwerktools für Analysezwecke anwenden

Inhalt: Die Vorlesung gibt eine Einführung in grundlegenden Protokolle und Anwendungen von Computernetzen. Der Schwerpunkt der Vorlesung liegt auf Standardprotokollen und -Algorithmen, wie sie in modernen Computernetzwerken (zum Beispiel im Internet) eingesetzt werden.

Anhand eines Schichtenmodells werden die wichtigsten Grundlagen nach dem Top-Down Ansatz vorgestellt und analysiert. Dazu gehören zum Beispiel auf der obersten Schicht DNS und HTTPS im Application Layer; TCP und UDP im Transport Layer; IPv4/IPv6 und Routing Algorithmen im Network Layer; sowie MAC und ARP im untersten Link Layer. Neben der reinen Funktionsweise dieser Standards werden Sicherheitsaspekte auf allen Schichten betrachtet.

Ergänzend zur Vorlesung werden Übungsaufgaben über die eLearning Plattform Moodle gestellt und in der Übungsstunde besprochen. Weiterhin wird in jeder Übung ein “Tool der Woche” vorgestellt. Dabei handelt es sich jeweils um eine spezielle Software, die man als “Netzwerker” unbedingt kennen sollte (z.B. traceroute, nmap, ...). Alle besprochenen Tools sind frei verfügbar und werden den Studenten als eine Lernplattform (virtuelle Maschine) zur Verfügung gestellt.

Als Primärliteratur wird “Computernetzwerke: Der Top-Down Ansatz” von Kurose und Ross (Pearson Verlag) verwendet.

Voraussetzungen: keine

Empfohlene Vorkenntnisse: Grundkenntnisse der Informationstechnik

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 5 Stunden pro Woche, in Summe 70 Stunden, erforderlich. Etwa 24 Stunden sind für die Klausurvorbereitung vorgesehen.

Prüfungsform: schriftlich, 120 Minuten

Voraussetzungen für die Vergabe von Kreditpunkten: Erfolgreiches Bestehen der Modulabschlussklausur.

2.25 260081: Datenschutz

Nummer:	260081
Lehrform:	Vorlesungen und Übungen
Medienform:	Folien rechnerbasierte Präsentation Tafelanschrieb
Verantwortlicher:	Prof. Dr.-Ing. Thomas Andreas Herrmann
Dozent:	Dr. Kai-Uwe Loser
Sprache:	Deutsch
SWS:	3
Leistungspunkte:	5
Angeboten im:	Wintersemester

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

Arbeitsaufwand: 150 Stunden

Der Arbeitsaufwand berechnet sich wie folgt: Die Kontaktzeit in der Vorlesung und der Übung entspricht 45 Stunden (30 Stunden Vorlesung und 15 Stunden Übung). Für die Vorbereitung der Übung, wozu implizit auch die Nachbereitung der Vorlesung gehört, werden 45 Stunden veranschlagt. Weiterhin ist eine Projektarbeit anzufertigen, für die 60 Stunden angesetzt werden.

Prüfungsform: schriftlich, 90 Minuten

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

2.26 141347: Digitale Forensik

Nummer:	141347
Lehrform:	Vorlesungen und Übungen
Medienform:	e-learning Moodle rechnerbasierte Präsentation
Verantwortlicher:	Prof. Dr. Thorsten Holz
Dozent:	Dr. rer. nat. Christofer Fein
Sprache:	Deutsch
SWS:	4
Leistungspunkte:	5
Gruppengröße:	80
Angeboten im:	Wintersemester und Sommersemester

Ziele: Die Studierenden beherrschen verschiedene Konzepte, Techniken und Tools aus dem Themengebiet der digitalen Forensik. Sie kennen die relevanten Konzepte und haben ein Überblick zum Forensischen Prozess. Es ist grundlegendes Verständnis von verschiedenen Methoden zur Sammlung, Analyse und Aufbereitung digitaler Spuren in IT-Systemen vorhanden. Die Studierenden können eigenständig neue Probleme analysieren und neue Lösungsmöglichkeiten entwickeln. Sie können mit diesem Verständnis mit ihren Kollegen über Probleme der Computerforensik diskutieren und auftretende Probleme im Gespräch korrekt klassifizieren.

Inhalt: Digitale Forensik befasst sich mit der Sammlung, Analyse und Aufbereitung digitaler Spuren in IT-Systemen. Im Rahmen der Vorlesung werden diese drei Themenbereiche vorgestellt und jeweils erläutert, mit welchen Verfahren und Ansätzen man diese Aufgaben erreichen kann. Ein Schwerpunkt der Vorlesung liegt auf dem Bereich der Analyse von Dateisystemen. Dazu werden verschiedene Arten von Dateisystemen detailliert vorgestellt und diskutiert, wie relevante Daten erfasst, analysiert und aufbereitet werden können. Darüber hinaus werden weitere Themen aus dem Bereich der digitalen Forensik behandelt, z.B. die Analyse von Smartphones und SQLite-Datenbanken. Ein integraler Teil der Veranstaltung sind die Übungen, die den Stoff mit praktischen Beispielen verdeutlichen und vertiefen.

Voraussetzungen: keine

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

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 Klausurvorbereitung vorgesehen.

Prüfungsform: schriftlich, 120 Minuten

Beschreibung der Prüfungsleistung: Termin wird vorläufig auf Ende März / Anfang April verschoben

Voraussetzungen für die Vergabe von Kreditpunkten: Bestandene Modulklausur

2.27 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
Leistungspunkte: 8
Angeboten im: Wintersemester

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 behandelt grundlegende algebraische Strukturen mit Anwendungen auf symmetrische Zählprobleme und fehlerkorrigierende Codes.

Voraussetzungen: keine

Empfohlene Vorkenntnisse: Elementare Grundkenntnisse in Analysis und linearer Algebra

Arbeitsaufwand: 240 Stunden

Der Arbeitsaufwand ergibt sich wie folgt: 14 Wochen zu je 6 SWS entsprechen in Summe 84 Stunden Anwesenheit. Für die Nachbereitung der Vorlesung und die Vor- und Nachbereitung der Übungen sind etwa 8 Stunden pro Woche, in Summe 112 Stunden, erforderlich. Etwa 44 Stunden sind für die Klausurvorbereitung vorgesehen.

Prüfungsform: schriftlich, 180 Minuten

Beschreibung der Prüfungsleistung: Termin wird vorläufig auf Ende März / Anfang April verschoben

2.28 150326: Einführung in die asymmetrische Kryptanalyse

Nummer: 150326
Lehrform: Vorlesungen und Übungen
Verantwortlicher: Prof. Dr. Alexander May
Dozent: Prof. Dr. Alexander May
Sprache: Deutsch
SWS: 4
Leistungspunkte: 5
Angeboten im: Sommersemester

Ziele: Die Studierenden beherrschen die grundlegenden Algorithmen in der Kryptanalyse.

Inhalt: Die Vorlesung gibt einen Einblick in grundlegende Methoden der Kryptanalyse. Der Stoffplan umfasst die folgenden Themen:

- 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

Voraussetzungen: keine

Empfohlene Vorkenntnisse: Inhalte der Vorlesungen Einführung in die Kryptographie 1 und 2

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 Klausurvorbereitung vorgesehen.

Prüfungsform: mündlich, 30 Minuten

2.29 141022: Einführung in die Kryptographie 1

Nummer:	141022
Lehrform:	Vorlesungen und Übungen
Medienform:	Moodle Tafelanschrieb
Verantwortlicher:	Prof. Dr.-Ing. Christof Paar
Dozenten:	Prof. Dr.-Ing. Christof Paar M. Sc. Maik Ender M. Sc. Julian Speith M. Sc. Paul Staat
Sprache:	Deutsch
SWS:	4
Leistungspunkte:	5
Gruppengröße:	ca. 350-400
Angeboten im:	Wintersemester

Ziele: Nach erfolgreichem Abschluss der Lehrveranstaltung verfügen die Studierenden über Kenntnisse der grundlegenden Anwendungen symmetrischer Verfahren und über Grundkenntnisse der asymmetrischen Kryptographie. Sie können entscheiden, unter welchen Bedingungen man in der Praxis bestimmte Verfahren einsetzt und wie die Sicherheitsparameter zu wählen sind. Mit den Grundlagen des abstrakten Denkens in der IT Sicherheitstechnik sind sie vertraut.

Zum anderen erreichen die Studierenden durch Beschreibungen ausgewählter praxisrelevanter Algorithmen, wie z. B. des AES- oder RSA-Algorithmus, ein algorithmisches und technisches Verständnis zur praktischen Anwendung. Die Studierenden erhalten dabei einen Überblick über die in Unternehmen eingesetzten Lösungen. Sie sind in der Lage, argumentativ eine bestimmte Lösung zu verteidigen. Die Vorlesungen werden zusätzlich auch als Videos in Deutsch und Englisch angeboten. Die Studierenden können daher durch das zweisprachige eLearning-Angebot Sprachkompetenzen in der Wissenschaftssprache Englisch erwerben.

Inhalt: Die Lehrveranstaltung bietet einen allgemeinen Einstieg in die Funktionsweise moderner Kryptografie und Datensicherheit. Es werden grundlegende Begriffe und mathematisch/technische Verfahren der Kryptografie und der Datensicherheit erläutert. Praktisch relevante symmetrische und asymmetrische Verfahren und Algorithmen werden vorgestellt und an praxisrelevanten Beispielen erläutert.

Die Vorlesung lässt sich in zwei Teile gliedern: Die Funktionsweise der symmetrischen Kryptographie einschließlich der Beschreibung historisch bedeutender symmetrischer Verschlüsselungsverfahren (Caesar Chiffre, Affine Chiffre) und aktueller symmetrischer Verfahren (Data Encryption Standard, Advanced Encryption Standard, Stromchiffren, One Time Pad) werden im ersten Teil behandelt.

Der zweite Teil besteht aus einer Einleitung zu asymmetrischen Verfahren und einem ihrer wichtigsten Stellvertretern (RSA). Hierzu wird eine Einführung der Grundlagen der Zahlentheorie durchgeführt, um ein grundlegendes Verständnis der Verfahren sicherzustellen (u.a. Ringe ganzer Zahlen, Gruppen, Körper, diskrete Logarithmen, euklidischer Algorithmus). Nichtsdestotrotz liegt der Schwerpunkt auf der algorithmischen Einführung des asymmetrischen Verfahrens.

Voraussetzungen: keine

Empfohlene Vorkenntnisse: Fähigkeit zum abstrakten und logischen Denken.

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 Klausurvorbereitung vorgesehen.

Prüfungsform: schriftlich, 120 Minuten

Voraussetzungen für die Vergabe von Kreditpunkten: Bestandene Modulklausur

Literatur:

[1] Paar, Christof, Pelzl, Jan "Kryptografie verständlich: Ein Lehrbuch für Studierende und Anwender", Springer, 2016
[2] Paar, Christof, Pelzl, Jan "Understanding Cryptography: A Textbook for Students and Practitioners", Springer, 2009

2.30 141023: Einführung in die Kryptographie 2

Nummer:	141023
Lehrform:	Vorlesungen und Übungen
Medienform:	Videoübertragung Internet Moodle
Verantwortlicher:	Prof. Dr.-Ing. Christof Paar
Dozenten:	Prof. Dr.-Ing. Christof Paar M. Sc. Maik Ender M. Sc. Julian Speith M. Sc. Paul Staat
Sprache:	Deutsch
SWS:	4
Leistungspunkte:	5
Gruppengröße:	ca. 350-400
Angeboten im:	Sommersemester

Ziele: Nach erfolgreichem Abschluss der Lehrveranstaltung verfügen die Studierenden über Kenntnisse der grundlegenden Anwendungen asymmetrischer und hybrider Verfahren. Sie können entscheiden, unter welchen Bedingungen man in der Praxis bestimmte Verfahren einsetzt und wie die Sicherheitsparameter zu wählen sind. Mit den Grundlagen des abstrakten Denkens in der IT Sicherheitstechnik sind sie vertraut. Zum anderen erreichen die Studierenden durch Beschreibungen ausgewählter praxisrelevanter Algorithmen, wie z.B. des Diffie-Hellmann-Schlüsselaustausch oder ECC-basierten Verfahren, ein algorithmisches und technisches Verständnis zur praktischen Anwendung. Die Studierenden erhalten dabei einen Überblick über die in Unternehmen eingesetzten Lösungen. Sie sind in der Lage, argumentativ eine bestimmte Lösung zu verteidigen. Die Vorlesungen werden zusätzlich auch als Videos in Deutsch und Englisch angeboten. Die Studierenden können daher durch das zweisprachige eLearning-Angebot Sprachkompetenzen in der Wissenschaftssprache Englisch erwerben.

Inhalt: Die Lehrveranstaltung bietet einen allgemeinen Einstieg in die Funktionsweise moderner Kryptografie und Datensicherheit. Es werden grundlegende Begriffe und mathematisch/technische Verfahren der Kryptografie und der Datensicherheit erläutert. Praktisch relevante asymmetrische Verfahren und Algorithmen werden vorgestellt und an praxisrelevanten Beispielen erläutert. Die Vorlesung lässt sich in zwei Teile gliedern: Der erste Teil beginnt mit einer Einleitung zu asymmetrischen Verfahren und deren wichtigsten Stellvertretern (Diffie-Hellman, elliptische Kurven). Der Schwerpunkt liegt auf der algorithmischen Einführung der asymmetrischen Verfahren, die sowohl Verschlüsselungsalgorithmen als auch digitale Signaturen beinhalten. Abgeschlossen wird dieser Teil durch Hashfunktionen, die eine große Rolle für digitalen Signaturen und Message Authentication Codes (MACs oder kryptografische Checksummen) spielen. Im zweiten Teil der Vorlesung werden Grundlagen von Sicherheitslösungen aufbauend auf den Konzepten der symmetrischen und asymmetrischen Kryptographie besprochen. Dabei wird vor allem auf die in Unternehmen notwendigen und eingesetzten Lösungen (PKI, digitale Zertifikate etc.) eingegangen.

Voraussetzungen: keine

Empfohlene Vorkenntnisse: Inhalte der Vorlesung “Einführung in die Kryptographie 1”

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 Klausurvorbereitung vorgesehen.

Prüfungsform: schriftlich, 120 Minuten

Beschreibung der Prüfungsleistung: Termin wird vorläufig auf Ende März / Anfang April verschoben

Voraussetzungen für die Vergabe von Kreditpunkten: Bestandene Modulklausur

Literatur:

[1] Paar, Christof, Pelzl, Jan ”Kryptografie verständlich: Ein Lehrbuch für Studierende und Anwender”, Springer, 2016
[2] Paar, Christof, Pelzl, Jan ”Understanding Cryptography: A Textbook for Students and Practitioners”, Springer, 2009

2.31 150310: Einführung in die theoretische Informatik

Nummer: 150310
Lehrform: Vorlesungen und Übungen
Medienform: Tafelanschrieb
Verantwortlicher: Jun. Prof. Dr. Nils Fleischhacker
Dozent: Jun. Prof. Dr. Nils Fleischhacker
Sprache: Deutsch
SWS: 4
Leistungspunkte: 6
Angeboten im: Sommersemester

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. 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 Wahrscheinlichkeitstheorie) erlernt. Die intellektuelle Fähigkeit, die logischen Zusammenhänge zwischen den Konzepten zu überblicken, und "versteckte" Anwendungsmöglichkeiten zu erkennen, wurde geschult.

Inhalt: Die Vorlesung gibt eine Einführung in die Kodierungstheorie und in die Theorie der Berechenbarkeit.

- Themenübersicht:
  - Turingmaschine
  - Komplexitätsklassen P und NP
  - Polynomielle Reduktion
  - Quadratische Reste
  - Eindeutig entschlüsselbare Codes
  - Kompakte und optimale Codes
  - Lineare und duale Codes

Voraussetzungen: keine

Empfohlene Vorkenntnisse: Grundkenntisse über Diskrete Mathematik und Algorithmen

Arbeitsaufwand: 180 Stunden

Der Arbeitsaufwand ergibt sich wie folgt: 14 Wochen zu je 5 SWS entsprechen in Summe 70 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 54 Stunden sind für die Klausurvorbereitung vorgesehen.

Prüfungsform: schriftlich, 120 Minuten

Beschreibung der Prüfungsleistung: Termin wird vorläufig auf Ende März / Anfang April verschoben

2.32 141036: Einführung in die Usable Security and Privacy

Nummer:	141036
Lehrform:	Vorlesungen und Übungen
Medienform:	Moodle
Verantwortlicher:	Prof. Dr. Markus Dürmuth
Dozenten:	Prof. Dr. Markus Dürmuth M. A. Annalina Buckmann M. A. Jennifer Friedauer M. Sc. Franziska Herbert Prof. Dr. Martina Angela Sasse
Sprache:	Deutsch
SWS:	4
Leistungspunkte:	5
Angeboten im:	Wintersemester und Sommersemester

Ziele: Die Studierenden verstehen die grundsätzliche Problematik und Wichtigkeit der Benutzbarkeit von technischen Systemen durch Menschen, insbesondere im Umgang mit IT Sicherheitstechnik. Darüber hinaus erlangen sie ein grundlegendes Verständnis von Methoden und zentralen Erkenntnissen der Usable Security und Privacy Forschung, sowie grundlegende Handreichungen für die Praxis.

Inhalt: WICHTIG: Bitte melden Sie sich selbstständig im Moodle-Kurs (der Link befindet sich oben rechts) an. Die erste Vorlesung wird dort hochgeladen. Das Passwort lautet P4$$w0rdeUSP202021.

Beginn der Vorlesung: Donnerstag den 29.10.2020 Beginn der Übung: Donnerstag den 05.11.2020

Die Vorlesung ist in zwei Teile gegliedert, die von den beiden Dozierenden, Prof. Dr. M. Angela Sasse und Prof. Dr. Markus Dürmuth, gehalten werden. Beide Teile sind für die Klausur relevant. Sie behandelt insbesondere folgende Themen:

Einführung 29.10.2020 - Die Dozenten stellen sich vor - Formalia zur Vorlesung

Teil 1: 05.11. bis 03.12.2020

Human Factors (Prof. Dr. M. Angela Sasse)

- Human Factors - Definitions/ Tasks/ Goals of Usable Security
- Workload and Human Error
- Security awareness and education
- Types of Attacks and Attackers

Teil 2: 10.12. bis 21.01.2021

Applications (Prof. Dr. Markus Dürmuth)

- User authentication
- Secure email and messaging

- Certicate warnings
- Privacy
- Social engineering and Phishing
- Captchas

28.01.2021 - Klausurvorbereitungssitzung
04.02.2021 - Selbststudium/Klausurvorbereitung
11.02.2021 - Selbststudium/Klausurvorbereitung

Voraussetzungen: Keine

Empfohlene Vorkenntnisse: Grundkenntnisse der IT Sicherheit.

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 Klausurvorbereitung vorgesehen.

Prüfungsform: schriftlich, 120 Minuten

Beschreibung der Prüfungsleistung: Termin wird vorläufig auf Ende März / Anfang April verschoben

2.33 142031: Einführung ins Hardware Reverse Engineering

Nummer:	142031
Lehrform:	Vorlesung mit integrierten Übungen
Medienform:	Videoübertragung e-learning Internet Moodle rechnerbasierte Präsentation
Verantwortlicher:	Prof. Dr.-Ing. Christof Paar
Dozenten:	Prof. Dr.-Ing. Christof Paar M. Sc. Nils Albartus M. Sc. Steffen Becker M. Sc. Julian Speith
Sprache:	Deutsch
SWS:	4
Leistungspunkte:	5
Angeboten im:	Wintersemester

Ziele: Die Studierenden sind mit den grundlegenden Aspekten des Entwurfs komplexer logischer Schaltkreise vertraut. Dazu gehören unter anderem das Verständnis von ASIC- und FPGA-Architekturen und der entsprechenden Workflows, sowie die Anwendung der dazugehörigen Tools unter der praktischen Verwendung von Hardwarebeschreibungssprachen (HDLs). Weiterhin haben die Studierenden ein tiefgehendes theoretisches Verständnis der verschiedenen Schritte des Hardware Reverse Engineering Prozesses und sind sich der Implikationen bewusst. Desweiteren erlangen die Studierenden im Rahmen mehrerer praktischer Projekte ein tiefgehendes Verständnis verschiedener Gate-level Netlist Reverse Engineering Methoden und werden ideal auf Abschlussarbeiten in diesem Bereich vorbereitet.

Inhalt: Das sogenannte Reverse Engineering von Geräten spielt sowohl für legitime Nutzer als auch für Hacker eine wichtige Rolle. Auf der einen Seite kann Reverse Engineering Unternehmen und Regierungen dabei unterstützen, Verletzungen am geistigen Eigentum oder gezielte Manipulationen aufzuspüren. Auf der anderen Seite setzen Hacker Reverse Engineering ein, um kostengünstig das geistige Eigentum anderer zu stehlen und zu kopieren, oder auch um durch den Einbau von Hintertüren Programme und Hardware-Schaltungen zu manipulieren.

Um die ersten Schritte im Hardware Reverse Engineering erfolgreich zu gehen, ist es zunächst einmal wichtig, dass die grundlegenden Konzepte des (Forward) Engineerings integrierter Schaltkreise erlernt werden. Der Inhalt dieser Vorlesung gliedert sich daher im Wesentlichen in die folgenden beiden Teile:

Der Inhalt dieser Vorlesung gliedert sich im Wesentlichen in zwei Teile:

Teil I: Grundprinzipien des VLSI Entwurfs (VLSI steht für Very-large-scale integration)

- Einführung in logische (kombinatorische) Schaltkreise
- Sequentielle Schaltkreise
- Hardware Description Languages (HDLs)

- Einführung in ASIC- und FPGA-Architekturen
- ASIC- und FPGA-Workflows

Teil II: Hardware Reverse Engineering

- PCB Analyse, Delayering, und Bildverarbeitung
- FPGA Bitstream Reverse Engineering
- Reverse Engineering von Gate-Level-Netzlisten

Empfohlene Vorkenntnisse: Inhalte der Vorlesungen Informatik 3 - Digitaltechnik und Rechnerarchitektur

Arbeitsaufwand: 150 Stunden

Der Arbeitsaufwand ergibt sich wie folgt: 12 Vorlesungen und Übungen entsprechen in Summe 36 Stunden Anwesenheit. Für die Nachbereitung der Vorlesung und die Vor- und Nachbereitung der Übung sind etwa 3 Stunden, in Summe 36 Stunden, erforderlich. Die Bearbeitungen der Hausübungen und Projekte nimmt ebenfalls etwa 36 Stunden in Anspruch. Etwa 42 Stunden sind für die Klausurvorbereitung vorgesehen.

Prüfungsform: mündlich, 30 Minuten

2.34 150347: Elliptische Kurven und Kryptographie

Nummer: 150347
Lehrform: Vorlesungen und Übungen
Medienform: rechnerbasierte Präsentation
Tafelanschrieb
Verantwortlicher: Prof. Dr. Alexander May
Dozent: Prof. Dr. Alexander May
Sprache: Deutsch
SWS: 4
Leistungspunkte: 5
Angeboten im:

Ziele: Die Studierenden beherrschen die arithmetischen und geometrischen Eigenschaften elliptischer Kurven und deren Anwendungen in der Kryptographie.

Inhalt:

Themenübersicht:

- Motivation
- Grundlagen aus der elementaren Gruppen und Zahlentheorie
- Elliptische Kurven über beliebigen Körpern
- Elliptische Kurven über endlichen Körpern
- Schnelle Arithmetik auf elliptischen Kurven
- Kryptographische Anwendungen: Diffie-Hellman Schlüsselaustausch, ElGamal Verschlüsselung, DSA Signaturen
- Berechnung des diskreten Logarithmus
- Bilineare Abbildungen über elliptischen Kurven

Voraussetzungen: keine

Empfohlene Vorkenntnisse: Inhalte der Veranstaltungen Einführung in die Kryptographie 1 und 2, Diskrete Mathematik und Einführung in die theoretische Informatik.

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 Klausurvorbereitung vorgesehen.

2.35 142240: Grundlagenpraktikum ITS

Nummer:	142240
Lehrform:	Praktikum
Medienform:	Internet rechnerbasierte Präsentation
Verantwortlicher:	Prof. Dr. Jörg Schwenk
Dozenten:	Prof. Dr. Jörg Schwenk M. Sc. Dominik Noß
Sprache:	Deutsch
SWS:	3
Leistungspunkte:	3
Angeboten im:	Wintersemester und Sommersemester

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):

- Kryptographische Angriffe auf RSA
- Angriffe in geswitchten Netzwerken
- Buffer Overflow Attacken
- Forensische Analyse eines Ransomware-Angriffs
- Konfiguration von Firewalls
- Programmatische Analyse von Netzwerkdaten mit LibPcap
- Einführung in Linux
- MD5 Kollisionen in Postscript
- Netzwerk-Analyse mit nmap & Wireshark
- Security Incident and Event Management (SIEM) mit Splunk
- Web Angriffe

Voraussetzungen: keine

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

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.

Prüfungsform: Praktikum, studienbegleitend

2.36 141024: Implementierung kryptographischer Verfahren

Nummer:	141024
Lehrform:	Vorlesungen und Übungen
Medienform:	Moodle Tafelanschrieb
Verantwortlicher:	Prof. Dr.-Ing. Christof Paar
Dozent:	Dr.-Ing. Falk Schellenberg
Sprache:	Deutsch
SWS:	4
Leistungspunkte:	5
Gruppengröße:	ca. 40 Teilnehmer
Angeboten im:	Wintersemester

Ziele: Studierende erlernen die grundlegenden Algorithmen für die effiziente Implementierung rechenintensiver Kryptoverfahren. Insbesondere den Umgang von Algorithmen mit sehr langen Operanden haben sie nach Abschluss des Moduls verstanden, ebenso wie das Zusammenspiel von Implementierungsmethoden und kryptographischer Sicherheit.

Inhalt: Diese Vorlesung gibt eine Einführung in Verfahren zur schnellen und sicheren Implemen-tierung kryptographischer Algorithmen. Im ersten Teil werden Methoden zum effizienten Potenzieren ausführlich behandelt, da diese für alle verbreiteten asymmetrischen Verfahren von großer Bedeutung sind. Für den weit ver-breiteten RSA Algorithmus werden zudem spezielle Beschleunigungsverfahren vorgestellt. Im zweiten Teil werden Algorithmen für effiziente Langzahlarithmetik entwickelt. Zunächst werden grundlegende Methoden zur Darstellung von Langzahlen in Rechnern und Verfahren zur Addition vorgestellt. Der Schwerpunkt dieses Teils liegt auf Algorithmen zur effizienten modularen Multiplikation. Neben dem Karatsuba-Algorithmus wird die Montgomery-Multiplikation behandelt. Im dritten Teil werden sichere Implementierungen besprochen. Es erfolgt eine Einführung in aktive und passive Seitenkanalattacken. Es werden aktive Attacken gegen Blockchiffren und RSA vorgestellt. Als wichtige Vertreter der passiven Attacken werden die Grundlagen von SPA (simple power analysis) und DPA (differential power analysis) eingeführt.

Die Endnote ergibt sich zu 70% aus einer Klausur und zu 30% aus studienbegleitenden Programmierprojekten (auch zum Nachschreibetermin im Sommersemester).

Studierende die in einem Sommersemester die Projekte anfertigen möchten müssen sich innerhalb der ersten beiden Vorlesungswochen per Mail an falk.schellenberg@rub.de melden (SoSe19: Deadline 24.04.20).

Voraussetzungen: keine

Empfohlene Vorkenntnisse:

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

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 Klausurvorbereitung vorgesehen.

Prüfungsform: schriftlich + studienbegleitend, 120 Minuten

Beschreibung der Prüfungsleistung: Termin wird vorläufig auf Ende März / Anfang April verschoben

Voraussetzungen für die Vergabe von Kreditpunkten: Die finale Bewertung für die Veranstaltung setzt sich zusammen aus: - schriftliche Klausur (Gewichtung 70- drei studienbegleitende Programmierprojekte während der Vorlesungszeit (Gewichtung 30Dieses gilt auch für den Nachschreibetermin im Sommersemester.

2.37 144011: Industriepraktikum ITS

Nummer: 144011
Lehrform: Industriepraktikum
Verantwortlicher: Studiendekan ITS
Dozent: Mitarbeiter von Firmen
Sprache: Deutsch
Leistungspunkte: 15
Angeboten im: Wintersemester und Sommersemester

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

Arbeitsaufwand: 450 Stunden

Der Gesamtumfang beträgt 450 Stunden, das entspricht, abhängig von der vereinbarten wöchentlichen Arbeitszeit, in der Regel 12 bis 14 vollen Wochen.

Prüfungsform: Praktikum, studienbegleitend

2.38 141328: Informatik 1 - Programmierung für ET/IT (PO 13) und ITS (PO 13)

Nummer: 141328
Lehrform: Vorlesung und Praxisübungen
Medienform: Folien
Verantwortlicher: Prof. Dr. Tobias Glasmachers
Dozent: Prof. Dr. Tobias Glasmachers
Sprache: Deutsch
SWS: 4
Leistungspunkte: 5
Angeboten im: Wintersemester

Ziele: Die Vorlesung verfolgt zwei übergeordnete Lernziele: Die Studierenden kennen grundlegende Begriffe und Konzepte der Informatik, und sie können programmieren. Die Teilnehmer kennen Variablen, Funktionen, die üblichen Kontrollstrukturen imperativer Programmiersprachen, Klassen und Objekte, sowie grundlegende und zusammengesetzte Datentypen. Sie können dieses Wissen anwenden, um in neuen Kontexten Probleme selbstständig durch die Erstellung eigener Programme zu lösen. Dazu entwerfen sie geeignete Datenstrukturen und einfache Algorithmen.

Inhalt: Die Veranstaltung nutzt die Programmiersprache TScript ("teaching-script") für einen möglichst einfachen und motivierenden Einstieg in die Programmierung.

Dabei werden die folgenden Themen behandelt:

- Anweisungen
- Variablen
- Kontrollstrukturen
- Funktionen, Lambda-Funktionen
- Rekursion
- Debuggen von Programmen
- Fehlerbehandlung
- Einfache GUI-Programmierung
- Objektorientierte Programmierung

Gleichzeitig werden die folgenden allgemeinen Konzepte vermittelt:

- Algorithmen und Programme, Korrektheit, Laufzeit
- formale Syntax von Programmiersprachen
- Problembeschreibung durch Daten, Programmzustand
- Problembeschreibung durch Algorithmen
- Grundzüge des objektorientierten Designs

Voraussetzungen: keine

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 Klausurvorbereitung vorgesehen.

Prüfungsform: schriftlich, 120 Minuten

Beschreibung der Prüfungsleistung: Prüfung findet online statt

2.39 141321: Informatik 2 - Algorithmen und Datenstrukturen

Nummer:	141321
Lehrform:	Vorlesung und Praxisübungen
Medienform:	Videoübertragung Internet Moodle
Verantwortlicher:	Prof. Dr.-Ing. Tim Güneysu
Dozenten:	Prof. Dr.-Ing. Tim Güneysu B. Sc. Markus Krausz
Sprache:	Deutsch
SWS:	4
Leistungspunkte:	5
Gruppengröße:	ca. 480 Teilnehmer
Angeboten im:	Sommersemester

Ziele: Die Studierenden erhalten einen systematischen Überblick über Prinzipien, Methoden, Konzepte und Notationen von verschiedenen Algorithmen und Datenstrukturen. Dieses Wissen - verbunden mit den praktischen Übungen am Computer - befähigt die Studierenden, (a) effiziente Programme problemgerecht zu entwickeln, (b) zu analysieren, (c) in die Programmiersprache C++ zu transformieren und (d) auf einer geeigneten Zielplattform auszuführen.

Inhalt: Die Vorlesung besteht aus vier größeren Blöcken, die wie folgt aufgeteilt sind: Im ersten Block werden Grundbegriffe eingeführt, der Fokus liegt auf dem Vergleich und der Bewertung von Algorithmen. Im zweiten Block werden klassische Sortalgorithmen (z: B. insertion sort, mergesort und quicksort) vorgestellt. Klassische Suchalgorithmen wie binäre Suche oder verschiedene Arten von Baumstrukturen werden im dritten Block vorgestellt. Im letzten Block wird ein Überblick über Graphalgorithmen und Operationen auf Strings gegeben. Begleitet wird die Vorlesung von Übungen, in denen die vorgestellten Konzepte und Techniken praktisch ausprobiert werden sollen.

Die Veranstaltung basiert auf dem Buch “Algorithms and Data Structures - The Basic Toolbox” von Mehlhorn und Sanders (siehe http://www.springer.com/de/book/9783540779773).

Voraussetzungen: keine

Empfohlene Vorkenntnisse: Inhalte der Vorlesung Informatik 1

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 Klausurvorbereitung vorgesehen.

Prüfungsform: schriftlich, 120 Minuten

Beschreibung der Prüfungsleistung: Termin findet wie geplant statt

Voraussetzungen für die Vergabe von Kreditpunkten: Bestandene Modulklausur (100Durch die erfolgreiche Teilnahme am Übungsbetrieb können bis 10

2.40 141300: Informatik 3 - Digitaltechnik

Nummer:	141300
Lehrform:	Vorlesungen und Übungen
Medienform:	Folien rechnerbasierte Präsentation Tafelanschrieb
Verantwortlicher:	Prof. Dr.-Ing. Jürgen Oehm
Dozenten:	Prof. Dr.-Ing. Jürgen Oehm M. Sc. Tobias Schwanke M. Sc. Dominik Veit
Sprache:	Deutsch
SWS:	4
Leistungspunkte:	5
Angeboten im:	Wintersemester

Ziele: Die Studenten erwerben umfassende Kenntnisse aus den Themenbereichen Boolesche Algebra, Aufbau und die Wirkungsweisen von digitalen Grundschaltungen, Kostenoptimierung digitaler Funktionsgruppen, Struktur und Funktionsweise von Grundfunktionalitäten, die insbesondere zentrale Komponenten von Mikroprozessorsystemen sind (wie z.B. Zählerstrukturen, Schieberegister, ALU, Bustreiber, Speicher). Ferner werden zentrale Kenntnisse über den inneren schaltungstechnischen Aufbau aktueller Logikfamilien vermittelt, insbesondere das Konzept und die Funktionsweise von CMOS-Logikschaltungen, die Skalierungseigenschaften von modernen CMOS-Technologien und die damit verbundenen Auswirkungen auf die Eigenschaften aktueller Geräte und Systeme. Mit diesem Wissen sind die Studierenden in der Lage, zukünftige Entwicklungen in den Integrationstechnologien, und damit in der Digitaltechnik selbst bezüglich ihrer Möglichkeiten und Grenzen einzuschätzen.

Die Gesamtbewertung setzt sich aus einer schriftlichen Prüfung (90%) und Hausaufgaben (10%) zusammen.

Inhalt:

- Historischer Rückblick,
- Motivation für Digitaltechnik,
- Boolesche Algebra,
- Zahlendarstellungen, Rechenschaltungen, arithmetisch logische Einheit (ALU),
- Flankendetektoren, bi-, mono- und astabile Schaltungen, Flip-Flops,
- Frequenzteiler, Zähler, Schieberegister, Speicher,
- Dioden-Logik, Dioden Transistor Logik, Transistor Transistor Logik, CMOS-Logik,
- CMOS-Technologie, CMOS-Standard-Zellen Konzept,
- Logikanalyse, Tools zur Logikanalyse,
- Mooresches Gesetz (Moore's law).

Die Vorlesung beginnt mit den theoretischen Grundlagen der booleschen Algebra. Danach werden verschiedene Verfahren zur Vereinfachung von logischen Netzwerken vorgestellt. Als

nächstes gilt es dann die minimierten logische Netzwerke in kosten- bzw. Hardware-minimale Logikschaltungen umzuwandeln. Dies erfordert, dass die zuvor minimierten logischen Schaltungen in solche logisch äquivalenten Schaltungen transformiert werden müssen, die nur noch aus NAND-, NOR- und NICHT-Funktionen bestehen. In diesem Zusammenhang wird herausgearbeitet, dass der Begriff 'Kosten' sowohl für den 'Hardware-Aufwand' stehen kann, als auch für die 'Summe der Gatterlaufzeiten innerhalb der kritischen Signalpfade'.

Der zweite Teil der Vorlesungsreihe beschäftigt sich mit den höherwertigen digitalen Funktionsgruppen. Dazu gehören z.B. Flipflops, Zählerstrukturen, 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.

Der dritte Teil der Vorlesungsreihe beschäftigt sich mit den zentralen Eigenschaften der wichtigsten Logikfamilien. Vorgestellt werden zunächst die historischen Logikfamilien (Dioden-Logik, Dioden-Transistor-Logik, Transistor-Transistor-Logik) in Verbindung mit ihren typischen Merkmalen. Danach wird das Hauptaugenmerk auf die CMOS-Logik gelegt, die Logikfamilie, die fast ausschließlich in allen modernen Geräten zur Anwendung kommt. Vor dem Hintergrund fortlaufender technologischer Fortschritte und den Eigenschaften von CMOS-Technologien, werden die mit den Technologie-Skalierungen einhergehenden Auswirkungen auf die Schaltzeiten von CMOS-Logik-Gattern dargestellt.

In Verbindung mit der abschließenden Vorstellung des sogenannten Mooresches Gesetzes endet die Vorlesungsreihe mit einem Ausblick auf mögliche technologische Entwicklungen in der Zukunft.

Voraussetzungen: keine

Empfohlene Vorkenntnisse:

- elementare Kenntnisse der Elektrotechnik und der Mathematik.

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 Klausurvorbereitung vorgesehen.

Prüfungsform: schriftlich + studienbegleitend, 120 Minuten

Beschreibung der Prüfungsleistung: Termin wird vorläufig auf Ende März / Anfang April verschoben

Literatur:

[1] Katz, Randy H. "Contemporary Logic Design", Prentice Hall, 1993
[2] Borucki, Lorenz, Stockfisch, Georg "Digitaltechnik", Teubner Verlag, 1989
[3] Pernards, Peter "Digitaltechnik I. Grundlagen, Entwurf, Schaltungen", Hüthig, 2001
[4] Fricke, Klaus "Digitaltechnik. Lehr- und Übungsbuch für Elektrotechniker und Informatiker", Vieweg, 2005
[5] Becker, Jürgen, Lipp, Hans Martin "Grundlagen der Digitaltechnik", Oldenbourg, 2005
[6] Gamm, Eberhard, Schenk, Christoph, Tietze, Ulrich "Halbleiter-Schaltungstechnik", Springer Verlag, 2016
[7] "Handbuch der Elektronik. Digitaltechnik", Medien Institut Bremen, 1999
[8] Eshragian, Karman, Eshragian, Kamran, Weste, Neil H. E. "Principles of CMOS VLSI Design: A Systems Perspective", Addison Wesley Longman Publishing Co, 1993
[9] Siemers, Christian, Sikora, Axel "Taschenbuch Digitaltechnik", Hanser Fachbuchverlag, 2002

2.41 144004: Kolloquium ITS

Nummer: 144004
Lehrform: Kolloquium
Verantwortlicher: Studiendekan ITS
Dozent: Hochschullehrer der Fakultät ET/IT
Sprache: Deutsch
Leistungspunkte: 3
Angeboten im: Wintersemester und Sommersemester

Ziele: Die Studierenden können die Ergebnisse ihrer Arbeit wissenschaftlich präsentieren.

Inhalt: Teilnahme an 5 Kolloquiumsvorträgen über die Ergebnisse von Bachelorarbeiten in der Fakultät ET & IT. Präsentation der eigenen Ergebnisse der Bachelorarbeit im Kolloquium.

Voraussetzungen: Anfertigung einer Bachelorarbeit

Empfohlene Vorkenntnisse: Präsentationstechnik

Arbeitsaufwand: 90 Stunden

Der Arbeitsaufwand berechnet sich wie folgt: Für den Besuch von Kolloquiumsvorträgen sind 10 Stunden anzusetzen. Die Erarbeitung des eigenen Themas findet eigenverantwortlich mit Unterstützung der betreuenden Mitarbeiter statt. Eine schriftliche Ausarbeitung von ca. 10 Seiten ist zu erstellen. Hierfür ist eine Arbeitszeit von 80 Stunden anzusetzen.

Prüfungsform: Seminarbeitrag, studienbegleitend

2.42 141031: Kryptographie auf hardwarebasierten Plattformen

Nummer:	141031
Lehrform:	Vorlesungen und Übungen
Medienform:	Moodle rechnerbasierte Präsentation Tafelanschrieb
Verantwortlicher:	Prof. Dr.-Ing. Tim Güneysu
Dozenten:	Prof. Dr.-Ing. Tim Güneysu B. Sc. Johannes Mono M. Sc. Jan Richter-Brockmann
Sprache:	Deutsch
SWS:	4
Leistungspunkte:	5
Gruppengröße:	ca 40-45 Teilnehmer
Angeboten im:	Wintersemester

Ziele: Die Studierenden erlernen die Konzepte der problemorientierten Hardwareentwicklung mit abstrakten Hardwarebeschreibungssprachen (VHDL) sowie die Simulation von Hardwareentwicklungen auf rekonfigurierbaren Plattformen. Sie beherrschen (a) Standard- und (b) Optimierungstechniken für kryptographische Systeme auf Hardwareebene und können (c) vollständige Implementierungen von symmetrischen und asymmetrischen Kryptosystemen auf modernen FPGA-Plattformen realisieren.

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 Moodle-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) Basiswissen Digitaltechnik

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.

Prüfungsform: schriftlich, 120 Minuten

Beschreibung der Prüfungsleistung: Termin findet wie geplant statt

Voraussetzungen für die Vergabe von Kreditpunkten: Bestandene Modulklausur (100 Prozent der Modulabschlussnote). Durch die erfolgreiche Teilnahme am Übungsbetrieb können bis 10 Prozent Bonuspunkte erworben werden, die auf das Ergebnis der Modulklausur angerechnet werden können.

2.43 150312: Kryptographie

Nummer: 150312
Lehrform: Vorlesungen und Übungen
Medienform: Blackboard
Tafelanschrieb
Verantwortlicher: Prof. Dr. Alexander May
Dozent: Prof. Dr. Alexander May
Sprache: Deutsch
SWS: 6
Leistungspunkte: 8
Gruppengröße: ca. 200
Angeboten im: Wintersemester

Ziele: Die Studierenden haben 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. Die Teilnehmer sind zur Analyse und dem Design aktueller und zukünftiger kryptographischer Methoden befähigt. Zudem weisen sie ein Bewusstsein für Methodik und Mächtigkeit verschiedenster Angriffsszenarien auf.

Inhalt: Es wird eine Einführung in moderne Methoden der symmetrischen und asymmetrischen Kryptographie geboten. Dazu wird ein Angreifermodell definiert und die Sicherheit der vorgestellten Verschlüsselungs-, Hash- und Signaturverfahren unter wohldefinierten KomplexitŠtsannahmen in diesem Angreifermodell nachgewiesen.

- Themenübersicht:
  - Sichere Verschlüsselung gegenüber KPA-, CPA- und CCA-Angreifern
  - Pseudozufallsfunktionen und -permutationen
  - Message Authentication Codes
  - Kollisionsresistente Hashfunktionen
  - Blockchiffren
  - Konstruktion von Zufallszahlengeneratoren
  - Diffie-Hellman Schlüsselaustausch
  - Trapdoor Einwegpermutationen
  - Public Key Verschlüsselung: RSA, ElGamal, Goldwasser-Micali, Rabin, Paillier
  - Einwegsignaturen
  - Signaturen aus kollisionsresistenten Hashfunktionen
  - Random-Oracle Modell

Voraussetzungen: keine

Empfohlene Vorkenntnisse: Inhalte der Vorlesungen Einführung in die Kryptographie 1 und 2

Arbeitsaufwand: 240 Stunden

Der Arbeitsaufwand ergibt sich wie folgt: 14 Wochen zu je 6 SWS entsprechen in Summe 84 Stunden Anwesenheit. Für die Nachbereitung der Vorlesung und die Vor- und Nachbereitung der Übungen sind etwa 6 Stunden pro Woche, in Summe 84 Stunden, erforderlich. Etwa 72 Stunden sind für die Klausurvorbereitung vorgesehen.

Prüfungsform: schriftlich, 120 Minuten

Beschreibung der Prüfungsleistung: Termin wird vorläufig auf Ende März / Anfang April verschoben

2.44 150110: Mathematik 1 für ET/IT (PO 13+20) und ITS (PO 13)

Nummer:	150110
Lehrform:	Vorlesungen und Übungen
Medienform:	Tafelanschrieb
Verantwortlicher:	Dr. rer. nat. Mario Lipinski
Dozent:	Dr. rer. nat. Mario Lipinski
Sprache:	Deutsch
SWS:	8
Leistungspunkte:	10
Angeboten im:	Wintersemester

Ziele: Die Studierenden beherrschen folgende mathematische Methoden zur Lösung ingenieurwissenschaftlicher Probleme und können diese anwenden:

- Eigenschaften reeller und komplexer Zahlen
- Elementare Eigenschaften der linearen Algebra
- Differential- und Integralrechnung für Funktionen von einer Veränderlichen
- Einfache gewöhnliche Differentialgleichungen
- Orthonormalsysteme, insbesondere Fourierreihen

Inhalt:

1. Reelle und komplexe Zahlen
    - Konstruktion der Zahlbereiche N, Z. Q, R; Rechengesetze; Ordnungsrelation; Betrag (Dreiecksungleichung), max, min, sup, inf
    - einfache mathematische Symbole zur Beschreibung von Mengen und Aussagen ({,},=,:=,=¿,¡=¿,:¡=¿, Quantoren)
    - Summen- und Produktzeichen, Binomialkoeffizienten, Binomischer Satz, kleiner Gauß, Cauchy-Schwarz (vollständige Induktion)
    - Darstellung natürlicher/reeller Zahlen bzgl. verschiedener Basen insb. Binärzahlen (Existenz, Konstruktion, schriftlich rechnen)
    - komplexe Zahlen
        - Gaußsche Zahlenebene, Grundrechenarten, Betrag und komplexe Konjugation, Polarkoordinaten, Potenzen und komplexe Wurzeln
2. Elementare Funktionen I
    - Polynome und gebruchen rationale Funktionen
        - Nullstellen, Polynomdivision, Partialbruchzerlegung
    - trigonometrische Funktionen (Definition am Kreis, Additionstheoreme)
    - Wachstumsklassen

- Funktionen kombinieren/verknüpfen, Graphen verschieben, skalieren

3. Folgen, Stetigkeit, Reihen
   - Konvergenz/Grenzwert von Folgen, Rechenregeln, Beispiele
   - Definition Stetigkeit, Rechenregeln, (Gegen)Beispiele
     - Anwendungen: Existenz von Extermwerten, Zwischenwerten, Nullstellenbestimmung
   - Konvergenz/Summe/Grenzwert einer Reihe, Kriterien
4. Differentialrechnung
   - Definition Ableitung, Rechenregeln, Beispiele (Polynome, rationale und trigonometrische Funktionen)
   - höhere Ableitungen, Mittelwertsatz, lHospitalsche Regel, Taylorpolynome, Potenzreihen (Konvergenzradius, Beispiele)
   - Monotonie, Extremwertbestimmung, Existenz und Ableitung der Umkehrfunktion (Wurzelfunktionen, arc-Funktionen)
5. Integralrechnung
   - Definition Riemannsches Integral, Integrierbarkeit
   - Hauptsatz, Stammfunktion, Integrationsregeln, Mittelwertsatz
   - Definition und Eigenschaften des natürlichen Logarithmus, der eulerschen Zahl, allgemeiner Potenzen, Potenzgesetze
   - Integration von Funktionenfolgen und Reihen
   - uneigentliche Integrale -¿ Konvergenzkriterien für Reihen, Definition Laplace-/Fouriertransformation, Gamma-/Besselfunktion
6. Lineare Algebra
   - (reeller) Vektorraum
     - Definition, Skalarprodukt, Norm, lineare Unabhängigkeit, Dimension
   - Geraden, Ebenen, Abstände, Kreuzprodukt
   - Matrizen und lineare Abblidungen, Determinanten und Invertierbarkeit, Koordinatentransformationen, Spur
   - lineare Gleichungssysteme (Gaußscher Algorithmus), Inversenberechnung
   - Normalform von Matrizen, Eigenvektoren/-werte/-räume, Diagonalisierung
   - Ellipsen, Hyperbeln, Parabeln
7. Gewöhnliche Differentialgleichungen I
   - Elementare Lösungsmethoden für DGL erster Ordnung
   - Lineare DGL mit konstanten Koeffizienten (zweiter Ordnung)
8. Orthonormalsysteme

  - allgemeine Skalarprodukte, Approximation im quadratischen Mittel, Besselsche Ungleichung, Parsevalsche Gleichung
  - trigonometrisches Orthonormalsystem, reele Fourierreihe (allg. Frequenz), Konvergenzeigenschaften, Rechenregeln, Ableitung, Integration, komplexe Fourierreihe
  - komplexe Vektorräume, unitäre Matrizen, Ableitung und Integration von Funktionen R-¿C
- Immer: (Un)gleichungen lösen, Terme vereinfachen, abschätzen/runden z.B. mit Hilfe von Größenordnung, Konsistenzüberprüfung mit Hilfe von Einheiten

Voraussetzungen: keine

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.

Arbeitsaufwand: 300 Stunden

Der Arbeitsaufwand berechnet sich wie folgt: 14 Wochen zu je 8 SWS ergeben 112 Stunden Präsenzzeit. Es verbleiben 188 Stunden zur Vor- und Nachbereitung und zur Prüfungsvorbereitung.

Prüfungsform: schriftlich, 120 Minuten

Beschreibung der Prüfungsleistung: Termin wird vorläufig auf Ende März / Anfang April verschoben

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

2.45 150112: Mathematik 2 für ET/IT (PO 13+20) und ITS (PO 13)

Nummer: 150112
Lehrform: Vorlesungen und Übungen
Medienform: Tafelanschrieb
Verantwortlicher: Dr. rer. nat. Mario Lipinski
Dozent: Dr. rer. nat. Mario Lipinski
Sprache: Deutsch
SWS: 8
Leistungspunkte: 10
Angeboten im: Sommersemester

Ziele: Die Studierenden beherrschen folgende mathematische Methoden zur Lösung ingenieurwissenschaftlicher Probleme und können diese anwenden:

- Differenzialrechnung für Funktionen von mehreren Variablen
- Orthonormalsysteme, insbesondere Fourierreihen
- Integralrechnung für Funktionen von mehreren Variablen
- Eigenschaften der Laplace- und Fouriertransformation
- Funktionentheorie

Inhalt:

1. Differentialrechnung
    - Funktionen mehrerer Variablen
        - Graphen, Niveaumengen, Stetigkeit
    - Differentialrechnung
        - Richtungsableitung, partielle Ableitung und Gradient, totale Ableitung, Rechenregeln, Mittlelwertsatz, höhere Ableitungen
    - Anwendungen
        - Parameterintegrale, Taylorentwicklung, implizite Funktionen und Umkehrabbildungen, Extrema ohne Nebenbedingungen, Extrema mit Nebenbedingungen
2. Integralrechnung
    - Riemann Integral - Integrale über Intervalle, iterierte Integrale, messbare Mengen, Mittelwertsatz
    - Praktische Aspekte
        - Normalbereiche, Prinzip des Cavalieri, Rotationskörper, Substitution, Schwerpunkte, Trägheitsmoment
    - Uneigentliche Integrale

  - Uneigentliche Integrierbarkeit, Ausschöpfungsfolgen

3. Vektoranalysis
   - Kurven - Definition, Parametrisierung, Tangentenvektor, Länge, Kurvenintegral, Differentialoperatoren (rot, div), Potentialfelder, Satz von Poincaré, Vektorpotentiale
   - Flächen
     - Definition, Parametrisierung, Tangential- und Normalenvektoren, Flächeninhalt, Flächenintegral, Fluss eines Vektorfeldes
   - Integralsätze
     - Satz von Green, Satz von Stokes, Satz von Gauß
4. Funktionentheorie
   - Stetigkeit und Holomorphie
     - Funktionen einer komplexen Veränderlichen, Stetigkeit, Hauptwerte, Möbiustransformationen, komplexe Differenzierbarkeit, Holomorphie
   - konforme Abbildungen
     - Definition, Eigenschaften, Riemannscher Abbildungssatz
   - Kurvenintegrale
     - Komplexes Kurvenintegral, Rechenregeln, Cauchyscher Integralsatz, Cauchysche Integralformel, Stammfunktionen
   - Reihenentwicklungen
     - Darstellung durch Potenzreihen, isolierte Singularitäten, Darstellung durch Laurent-Reihen
   - Residuensatz
     - Residuum, Residuensatz, Anwendung auf reelle Integrale
5. Laplace- und Fouriertransformation
   - Laplacetransformation
     - Definition, Rechenregeln, inverse Laplacetransformation, Anwendung auf Integralgleichungen
   - Fouriertransformation
     - Definition, Rechenregeln, inverse Fouriertransformation

Voraussetzungen: keine

Empfohlene Vorkenntnisse: Inhalte der Vorlesung Mathematik 1

Arbeitsaufwand: 300 Stunden

Der Arbeitsaufwand berechnet sich wie folgt: 14 Wochen zu je 8 SWS ergeben 112 Stunden Präsenzzeit. Etwa weitere 8 Stunden pro Woche sind für die Vor- und Nachbereitung vorgesehen. Es verbleiben 76 Stunden zur Prüfungsvorbereitung.

Prüfungsform: schriftlich, 120 Minuten

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

2.46 150324: Model Checking

Nummer: 150324
Lehrform: Vorlesungen und Übungen
Medienform: Moodle
Verantwortlicher: Prof. Dr. Thomas Zeume
Dozent: Prof. Dr. Thomas Zeume
Sprache: Deutsch
SWS: 4
Leistungspunkte: 5
Angeboten im: Wintersemester

Ziele: In dieser Veranstaltung werden die theoretischen Grundlagen des Model Checkings vermittelt, mit einem Fokus auf logik-basierten Spezifikationssprachen. Die Spezifikationssprachen LTL und CTL werden eingeführt, ihre Ausdrucksstärke untersucht, und die wichtigsten algorithmischen Ansätze für das Model Checking vorgestellt. Diese Veranstaltung richtet sich an Studierende der Mathematik, Informatik und ITS.

Inhalt: Wie kann die Korrektheit von Software und Hardware formal überprüft werden? Im Model Checking werden Software- und Hardware-Module durch Transitionssysteme formalisiert; gewünschte Eigenschaften mit Hilfe logischer Formalismen formal beschrieben; und mit Hilfe von Algorithmen automatisiert überprüft, ob ein Transitionssystem eine formal spezifizierte Eigenschaft besitzt.

Voraussetzungen:

- Grundlagenvorlesungen Mathematik
- Einführung in die Theoretische Informatik (ggf. kann das nötige Wissen auch nachgeholt werden)
- Hilfreich: Logik in der Informatik, Datenstrukturen und elementare Programmierkenntnisse

Empfohlene Vorkenntnisse: Keine

Arbeitsaufwand: 150 Stunden

Der Arbeitsaufwand ergibt sich wie folgt: 15 Wochen zu je 4 SWS entsprechen in Summe 60 Stunden Anwesenheit. Für die Nachbereitung der Vorlesung und die Vor- und Nachbereitung der Übungen sind etwa 4 Stunden pro Woche, in Summe 60 Stunden, erforderlich. Etwa 30 Stunden sind für die Klausurvorbereitung vorgesehen.

Prüfungsform: mündlich, 30 Minuten

Literatur:

[1] Clarke, Edmund M., Grumberg, Orna, Kroening, Daniel, Peled, Doron, Veith, Helmut "Model Checking", MIT Press, 2018
[2] Baier, Christel, Katoen, Joost-Pieter "Principles of Model Checking", MIT Press, 2008

2.47 141242: Netzsicherheit 1

Nummer:	141242
Lehrform:	Vorlesungen und Übungen
Medienform:	Moodle rechnerbasierte Präsentation
Verantwortlicher:	Prof. Dr. Jörg Schwenk
Dozenten:	Prof. Dr. Jörg Schwenk Dipl.-Math. Marcus Brinkmann
Sprache:	Deutsch
SWS:	4
Leistungspunkte:	5
Gruppengröße:	ca. 100-150
Angeboten im:	Wintersemester

Ziele: Studierende verfügen nach erfolgreichem Abschluss des Moduls über ein umfassendes Verständnis der technischen Aspekte von Netzsicherheit. Sie haben erkannt, dass Kryptographie alleine nicht ausreicht, um sicherheitstechnische Probleme zu lösen. Sie haben ein umfassendes Systemverständnis für komplexe IT-Systeme erworben. Durch eigenständige Überlegungen zur Verbesserung der Netzsicherheit bereiten sich die Studierenden auf ihre Rolle im Berufsleben vor. Sie können neue Probleme analysieren und neue Lösungsmöglich-keiten entwickeln. Sie können im Gespräch den Nutzen der von ihnen erarbeiteten Lösungen argumentativ begründen. Sie haben verstanden, dass nicht-technische Faktoren wie Fragen der Haftung und der entstehenden Kosten Entscheidungen zur IT-Sicherheit maßgeblich mit beeinflussen.

Inhalt: Wenn Kryptographie in einer technischen Umgebung wie einem Computer-, Daten- oder Telefonnetz eingesetzt wird, hängt die Sicherheit außer von rein kryptographischen Faktoren auch von der technischen Einbettung der Verschlüsselungs- und Signaturalgorithmen ab. Prominente Beispiele (für fehlerhafte Einbettungen) sind EFAIL (efail.de), Angriffe auf die WLAN-Verschlüsselungssysteme WEP und WPA (KRACK) und diverse Angriffe auf TLS (Bleichenbacher, POODLE, DROWN, ROBOT). Das Modul „Netzsicherheit 1“ beschäftigt sich mit konkreten Netzen zur Datenübertragung und beleuchtet diese von allen Seiten auf ihre Sicherheit hin. Es umfasst folgende Teile:

- Einführung: Internet
- Einführung: Vertraulichkeit
- Einführung: Integrität
- Einführung: Kryptographische Protokolle
- PPP-Sicherheit (insb. PPTP), EAP-Protokolle
- WLAN-Sicherheit (WEP, WPA, Wardriving, KRACK)
- GSM- und UMTS-Mobilfunk (Authentisierung und Verschlüsselung)
- IPSec (ESP und AH, IKEv1 und v2, Angriffe auf IPSec)
- Dateiverschlüsselung mit OpenPGP (Datenformat, Efail, Klima-Rosa)

- E Mail-Verschlüsselung mit S/MIME (SMTP, Datenformat, Efail, POP3, IMAP)

Neben den Systemen selbst werden dabei auch publizierte Angriffe auf diese Systeme besprochen; die Studierenden stellen selbst wissenschaftliche Überlegungen zur Verbesserung der Sicherheit an.

Voraussetzungen: keine

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

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 Klausurvorbereitung vorgesehen.

Prüfungsform: schriftlich, 120 Minuten

Beschreibung der Prüfungsleistung: Termin findet wie geplant statt

Voraussetzungen für die Vergabe von Kreditpunkten: Erfolgreiches Bestehen der Modulabschlussklausur.

Literatur:

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

2.48 141243: Netzsicherheit 2

Nummer:	141243
Lehrform:	Vorlesungen und Übungen
Medienform:	rechnerbasierte Präsentation
Verantwortlicher:	Prof. Dr. Jörg Schwenk
Dozenten:	Prof. Dr. Jörg Schwenk
	M. Sc. Robert Merget
Sprache:	Deutsch
SWS:	4
Leistungspunkte:	5
Gruppengröße:	ca. 100-150
Angeboten im:	Sommersemester

Ziele: Studierende verfügen nach erfolgreichem Abschluss des Moduls über ein umfassendes Verständnis der technischen Aspekte von Netzsicherheit. Sie haben erkannt, dass Kryptographie alleine nicht ausreicht, um sicherheitstechnische Probleme zu lösen. Sie haben ein umfassendes Systemverständnis für komplexe IT-Systeme erworben. Durch eigenständige Überlegungen zur Verbesserung der Netzsicherheit bereiten sich die Studierenden auf ihre Rolle im Berufsleben vor. Sie können neue Probleme analysieren und neue Lösungsmöglichkeiten entwickeln. Sie können im Gespräch den Nutzen der von ihnen erarbeiteten Lösungen argumentativ begründen. Sie haben verstanden, dass nicht-technische Faktoren wie Fragen der Haftung und der entstehenden Kosten Entscheidungen zur IT-Sicherheit maßgeblich mit beeinflussen.

Inhalt: Wenn Kryptographie in einer technischen Umgebung wie einem Computer-, Daten- oder Telefonnetz eingesetzt wird, hängt die Sicherheit außer von rein kryptographischen Faktoren auch von der technischen Einbettung der Verschlüsselungs- und Signaturalgorithmen ab. Prominente Beispiele (für fehlerhafte Einbettungen) sind EFAIL (efail.de), Angriffe auf die WLAN-Verschlüsselungssysteme WEP und WPA (KRACK) und diverse Angriffe auf TLS (Bleichenbacher, POODLE, DROWN, ROBOT). Das Modul „Netzsicherheit“ beschäftigt sich mit konkreten Netzen zur Datenübertragung und beleuchtet diese von allen Seiten auf ihre Sicherheit hin. Es umfasst folgende Teile: * Sicherheit von HTTP (HTTP Authentication, Secure HTTP, Architektur von SSL/TLS) * Transport Layer Security (TLS1.2, Versionen SSL 2.0 bis TLS 1.3) * Angriffe auf SSL und TLS (BEAST, CRIME, POODLE, Lucky13, Bleichenbacher, DROWN, Heartbleed, Invalid Curve) * Secure Shell - SSH * das Domain Name System und DNSSEC (faktorisierbare Schlüssel) * Sicherheit von Webanwendungen (HTML, URI, XSS, CSRF, SQLi, SSO) * XML- und JSON-Sicherheit Neben den Systemen selbst werden dabei auch publizierte Angriffe auf diese Systeme besprochen; die Studierenden stellen selbst wissenschaftliche Überlegungen zur Ver-besserung der Sicherheit an.

Voraussetzungen: keine

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

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 Klausurvorbereitung vorgesehen.

Prüfungsform: schriftlich, 120 Minuten

Beschreibung der Prüfungsleistung: Termin wird vorläufig auf Ende März / Anfang April verschoben

Voraussetzungen für die Vergabe von Kreditpunkten: Erfolgreiches Bestehen der Modulabschlussklausur.

2.49 141105: Nichttechnische Veranstaltungen

Nummer: 141105
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: Neben den in der Studiengangsübersicht angegebenen Lehrveranstaltungen können die Studierenden aus dem Angebot der Ruhr-Universität weitere Veranstaltungen auswählen. Es muss sich dabei um nichttechnische Fächer handeln. Ausgenommen sind somit die Fächer der Ingenieurwissenschaften sowie der Physik und Mathematik. Möglich Inhalte sind dagegen Sprachen, BWL, Jura, Chemie etc.

Beispielsweise gibt es verschiedene spezielle **Englischkurse**: Es wird ein Kurs Technisches Englisch für Bachelorstudierende der Fakultät angeboten. Außerdem wird ein weiterführender Englischkurs Projects and management in technical contexts für Masterstudierende angeboten. Schließlich richtet sich der allgemeine Kurs Engineer your careers an Bachelor- und Masterstudierende.

Aus anderen Bereichen gibt es folgende Kurse:

Der Ingenieur als Manager

Methods and Instruments of Technology Management

Projektmanagemant für Ingenieure

Im Zusammenhang mit dem Thema "Existenzgründung" gibt es folgenden Kurs:

Coaching für Existenzgründer

Unsicherheitserfahrung und Bewältigungsstrategien im unternehmerischen Kontext – Simulationsbasierte Lernansätze

Bei der Auswahl kann außerdem das Vorlesungsverzeichnis der Ruhr-Universität verwendet werden, eine Beispiele sind:

0em

BWL: `https://www.wiwi.ruhr-uni-bochum.de/zfoeb`

Sprachen: `http://www.ruhr-uni-bochum.de/zfa/`

Recht: `https://zrsweb.zrs.rub.de/institut/qzr/`

Schreibzentrum: `https://www.zfw.rub.de/sz/` (z.B. Vorbereitung auf die Abschlussarbeit)

Bitte beachten Sie, dass die Vorlesungen "BWL für Ingenieure" und "BWL für Nichtökonomen" identischen Inhalt haben und deshalb nur eine von beiden Veranstaltungen anerkannt werden kann. Gleiches gilt für die Veranstaltungen "Kostenrechnung" und "Einführung in das Rechnungswesen/Controlling".

Voraussetzungen: entsprechend den Angaben zu der gewählten Veranstaltungen

Empfohlene Vorkenntnisse: entsprechend den Angaben zu der gewählten Veranstaltungen

Prüfungsform: None, studienbegleitend

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

2.50 141090: Praxistage für ET/IT und ITS (PO 13)

Nummer: 141090
Lehrform: Projekt
Verantwortlicher: Prof. Dr.-Ing. Nils Pohl
Dozent: Dr.-Ing. Pierre Mayr
Sprache: Deutsch
SWS: 1
Leistungspunkte: 1
Angeboten im: Wintersemester

Ziele: Während der „Praxistage“ erfahren die Studierenden, wie man gemeinsam an einer gegebenen Aufgabe arbeitet. In der Veranstaltung entdecken die Teilnehmer die Vielfalt des technisch Möglichen und verwirklichen ihre eigenen Ideen. Neben den Programmierkenntnissen werden konzeptionelles Arbeitsvermögen, Kreativität und Teamfähigkeit geschult.

Inhalt: Im Rahmen der dreitägigen Lehrveranstaltung treten die teilnehmenden Studierenden in Teams gegeneinander an.

Die Aufgabe ist es, gemeinschaftlich Ideen zu entwickeln und diese anschließend in eine geeignete Lösung zu überführen.

Gruppeneinteilung, Raumverteilung und Aufgabenstellung werden in der zentralen Einführungsveranstaltung vorgestellt. Wer gewinnen wird, entscheidet sich während der Abschlussveranstaltung.

Voraussetzungen: keine

Empfohlene Vorkenntnisse: Interesse an Technik

Arbeitsaufwand: 30 Stunden

Die Einführungsveranstaltung mit 2 Stunden Anwesenheit und drei Tage mit je 6 Stunden Anwesenheit ergibt 20 Stunden Anwesenheit. 10 Stunden sind für die Vorbereitung nach der Einführungsveranstaltung vorgesehen.

Prüfungsform: Projektarbeit, studienbegleitend

2.51 149872: Programmieren in C

Nummer:	149872
Lehrform:	Vorlesungen und Übungen
Medienform:	Moodle rechnerbasierte Präsentation
Verantwortlicher:	Prof. Dr. Markus Dürmuth
Dozenten:	Prof. Dr. Markus Dürmuth M. Sc. Theodor Schnitzler
Sprache:	Deutsch
SWS:	3
Leistungspunkte:	3
Angeboten im:	Wintersemester

Ziele: Die Studierenden beherrschen die grundlegenden Sprachkonstrukte von C mit Betonung der prozeduralen Betrachtungsweise und haben ein Verständnis für die Sicherheitsproblematik von C.

Inhalt: Alle Informationen zur Veranstaltung werden über den entsprechenden Moodle-Kurs kommuniziert. https://moodle.ruhr-uni-bochum.de/m/course/view.php?id=34476

Inhalte der Vorlesung

- Verfahren der strukturierten Programmierung
- Einführung in die Programmiersprache C (C90/C99/C11)
  - elementare Sprachkonstrukte(Standard-Datentypen, Ausdrücke, Kontrollstrukturen)
  - prozedurale Betrachtungsweise (Funktionen und Programmstrukturen)
  - klassische Datenstrukturen (Arrays, Verbunde) und Zeiger
  - dynamische Datenstrukturen
  - Sicherheitsproblematik

Voraussetzungen: keine

Empfohlene Vorkenntnisse: Vorhandene Grundkenntnisse in einer anderen Programmiersprache sind für das Verständnis der Vorlesung hilfreich, jedoch nicht Voraussetzung.

Arbeitsaufwand: 90 Stunden

Der Arbeitsaufwand berechnet sich wie folgt: 14 Wochen zu je 4 SWS entsprechen in Summe 56 Stunden Anwesenheit. Es verbleiben also 34 Stunden zur Vorbereitung der Rechnerübungen und zur Nachbereitung der Vorlesung. Die Klausurvorbereitung ist hier enthalten, da die Übungen auch zur Vorbereitung auf die Klausur dienen.

Prüfungsform: schriftlich, 90 Minuten

Beschreibung der Prüfungsleistung: Termin wird vorläufig auf Ende März / Anfang April verschoben

2.52 141140: Rechnerarchitektur für ET/IT und ITS (PO 13)

Nummer: 141140
Lehrform: Vorlesungen und Übungen
Verantwortlicher: Prof. Dr. Philipp Niemann
Dozent: Prof. Dr. Philipp Niemann
Sprache: Deutsch
SWS: 4
Leistungspunkte: 5
Gruppengröße: ca. 300-400
Angeboten im: Wintersemester

Ziele: Die Studierenden kennen Zusammenhänge und haben Detailkenntnisse bezüglich der Komponenten und der Funktionsweise moderner Computersysteme. Dies schließt neben dem Prozessor auch das Speichersystem und die Schnittstellen zu weiteren Systemkomponenten ein. Auf der Basis dieser Kenntnisse sind die Studierenden in der Lage Computersysteme und deren Komponenten bezüglich verschiedener Metriken, wie z.B. Rechenleistung, Speicherperformance etc. auf deren Eignung für eine bestimmte Aufgabe zu bewerten. Weiterhin haben die Teilnehmer dieser Veranstaltung die grundsätzliche Arbeitsweise und den prinzipiellen Aufbau von Prozessoren auf der Ebene der Mikroarchitektur verstanden und sind in der Lage, den Einfluss von Architekturmerkmalen, wie z.B. Pipelining oder Out-of-Order-Execution, auf die Befehlsausführung zu analysieren.

Inhalt: Die Veranstaltung Rechnerarchitektur befasst sich mit dem Aufbau und der Funktion moderner Prozessoren und Computersysteme. Ausgehend von grundlegenden Computerstrukturen wie der Von-Neumann- und der Harvard-Architektur werden der Aufbau, die Klassifizierung und die technische Realisierung von Rechnersystemen dargestellt. Hierbei wird die Programmierung auf Assemblerebene sowie die Verarbeitung von Programmen durch einen Prozessor erläutert. Darauf aufbauend folgen Methoden zu Leistungsbewertung von Prozessoren auf der Basis von standardisierten Benchmarks und verschiedene Metriken, um die Ergebnisse einordnen zu können. Der inhaltliche Schwerpunkt der Vorlesung stellt die tiefgehende Analyse der Mikroarchitekturebene eines Prozessors dar, wobei sowohl der Datenpfad als auch das Steuerwerk im Rahmen der Vorlesung schrittweise entwickelt und erläutert werden. Auf der Basis des in der Vorlesung vorgestellten Prozessors werden dann moderne Verfahren zur Leistungssteigerung und deren Einsatzgebiete vorgestellt. Neben dem eigentlichen Prozessor wird auch das Speichersystem moderner Computer und verschiedene Schnittstellen zu internen und externen Komponenten des Computersystems behandelt. Alle Themen werden mit aktuellen Beispielen aus verschiedenen Bereichen der Technik erläutert.

Empfohlene Vorkenntnisse: Keine

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 Klausurvorbereitung vorgesehen.

Prüfungsform: schriftlich, 120 Minuten

Voraussetzungen für die Vergabe von Kreditpunkten: Erfolgreiches Bestehen der Modulklausur.

2.53 150537: Seminar zur Kryptographie

Nummer: 150537
Lehrform: Seminar
Medienform: rechnerbasierte Präsentation
Verantwortlicher: Prof. Dr. Gregor Leander
Dozent: Prof. Dr. Gregor Leander
Sprache: Deutsch
SWS: 2
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.

Prüfungsform: Seminarbeitrag, studienbegleitend

Voraussetzungen für die Vergabe von Kreditpunkten: Es besteht Anwesenheitspflicht.

2.54 150560: Seminar zur Real World Cryptoanalysis

Nummer: 150560
Lehrform: Seminar
Medienform: Folien
Verantwortlicher: Prof. Dr. Alexander May
Dozent: Prof. Dr. Alexander May
Sprache: Deutsch
SWS: 2
Leistungspunkte: 4
Angeboten im: Wintersemester

Ziele: Ziel des Seminares ist es, sich selbstständig in eine wissenschaftliche Veröffentlichung einzuarbeiten, diese aufzubereiten und im Rahmen eines Vortrages den Teilnehmern zu präsentieren.

Inhalt: Das Seminar befasst sich mit praxisrelevanten Themen der Kryptographie und Kryptanalyse.

Empfohlene Vorkenntnisse: Ein allgemeines Verständnis von IT-Sicherheit ist hilfreich. Weiterhin sind, je nach Thema, Inhalte nützlich, wie sie etwa in den Vorlesungen Kryptographie I + II und Kryptoanalyse vermittelt werden. In der Regel lassen sich aber Themen abhängig von bereits besuchten Veranstaltungen finden.

Arbeitsaufwand: 120 Stunden

Der Arbeitsaufwand berechnet sich wie folgt: 14 Wochen zu je 3 SWS ergeben 42 Stunden Anwesenheit. Es verbleiben 78 Stunden zur Vor- und Nachbereitung.

Prüfungsform: Seminarbeitrag, studienbegleitend

2.55 141340: Systemsicherheit

Nummer:	141340
Lehrform:	Vorlesungen und Übungen
Medienform:	e-learning Moodle rechnerbasierte Präsentation
Verantwortlicher:	Prof. Dr. Thorsten Holz
Dozenten:	Prof. Dr. Thorsten Holz M. Sc. Thorsten Eisenhofer M. Sc. Moritz Schlögel
Sprache:	Deutsch
SWS:	4
Leistungspunkte:	5
Gruppengröße:	100
Angeboten im:	Sommersemester

Ziele: Die Studierenden beherrschen wichtige theoretische und praktische Aspekte von Sicherheitsmechanismen moderner Softwaresystemen. Sie sind in die Lage, die Sicherheit eines gegebenen Programms eigenständig zu analysieren, Schwachstellen im Design aufzudecken sowie selbständig Lösungsmöglichkeiten und Schutzmechanismen zu entwickeln. Darüber hinaus haben sie grundlegende Begriffe aus dem Bereich der Systemsicherheit kennengelernt. Sie sind in der Lage, neue Sicherheitsmodelle selbst zu erstellen und diese argumentativ zu verteidigen.

Inhalt: Im Rahmen der Vorlesung werden wichtige theoretische und praktische Aspekte aus dem Bereich der Systemsicherheit vorgestellt und diskutiert. Der Fokus liegt dabei auf verschiedenen Aspekten der Softwaresicherheit und verschiedene Angriffs- und Verteidigungstechniken werden vorgestellt. Die Studierenden sollen am Ende der Vorlesungsreihe in die Lage sein, die Sicherheit verschiedener Softwaresysteme zu analysieren, Schwachstellen im Design und der Implementierung aufzudecken sowie selbständig Sicherheitsmechanismen zu entwickeln. Darüber hinaus werden auch andere Aspekte aus dem Bereich der Systemsicherheit wie Privatheit und Anonymität betrachtet.

Voraussetzungen: keine

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 Klausurvorbereitung vorgesehen.

Prüfungsform: schriftlich, 120 Minuten

Voraussetzungen für die Vergabe von Kreditpunkten: Bestandene Modulklausur, Bonuspunkte für erfolgreiche Bearbeitung der Übungsblätter

2.56 141171: Systemtheorie 1 - Grundgebiete

Nummer:	141171
Lehrform:	Vorlesungen und Übungen
Medienform:	Folien
Verantwortlicher:	Prof. Dr.-Ing. Rainer Martin
Dozenten:	Prof. Dr.-Ing. Rainer Martin Dr.-Ing. Aleksej Chinaev Dipl.-Ing. Johannes Gauer M. Sc. Benjamin Lentz Dr.-Ing. Anil Nagathil
Sprache:	Deutsch
SWS:	4
Leistungspunkte:	5
Gruppengröße:	ca. 300 Teilnehmer
Angeboten im:	Sommersemester

Ziele: Die Studierenden beherrschen die wesentlichen Grundlagen der Systemtheorie. Sie kennen die mathematische Beschreibung von Signalen und Systemen im Zeitbereich und deren wesentliche Merkmale. Sie kennen die Grundlagen der Wahrscheinlichkeitsrechnung und können mit diskreten und kontinuierlichen Zufallsvariablen rechnen. Sie verstehen die Grundbegriffe der Informationstheorie und können diese anwenden.

Inhalt:

1. **Signale und Systeme**

   Signale, Kenngrößen und Eigenschaften von Signalen, Elementare Operationen, Signalsynthese und Signalanalyse, periodischer Signale, Analog-Digital und Digital-Analog Umsetzung, lineare und nichtlineare Systeme

2. **Einführung in die Wahrscheinlichkeitsrechnung**

   Einführung und Definitionen, Mehrstufige Zufallsexperimente, Diskrete Zufallsvariablen, Kontinuierliche Zufallsvariablen

3. **Grundbegriffe der Informationstheorie**

   Grundlegende Fragestellungen der Informationstheorie, Entropiebegriffe, Anwendungen

Voraussetzungen: keine

Empfohlene Vorkenntnisse: Inhalte der Vorlesung Mathematik 1

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 Klausurvorbereitung vorgesehen.

Prüfungsform: schriftlich, 120 Minuten

Beschreibung der Prüfungsleistung: Termin findet wie geplant statt

Voraussetzungen für die Vergabe von Kreditpunkten: Bestandene Modulklausur

Literatur:

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

2.57 141170: Systemtheorie 1 - Signale und Systeme

Nummer:	141170
Lehrform:	Vorlesungen und Übungen
Medienform:	Folien
	Moodle
Verantwortlicher:	Prof. Dr.-Ing. Rainer Martin
Dozent:	Prof. Dr.-Ing. Rainer Martin
Sprache:	Deutsch
SWS:	4
Leistungspunkte:	5
Gruppengröße:	ca. 300 Teilnehmer
Angeboten im:	Sommersemester

Ziele: Die Studierenden beherrschen die wesentlichen Grundlagen der Systemtheorie. Sie kennen die mathematische Beschreibung von Signalen und Systemen im Zeitbereich und deren wesentliche Merkmale. Sie kennen die Grundlagen der Wahrscheinlichkeitsrechnung und können mit diskreten und kontinuierlichen Zufallsvariablen rechnen. Sie verstehen die Grundbegriffe der Informationstheorie und können diese anwenden.

Inhalt:

1. **Signale und Systeme**

   Signale, Kenngrößen und Eigenschaften von Signalen, Elementare Operationen, Signalsynthese und Signalanalyse, periodischer Signale, Analog-Digital und Digital-Analog Umsetzung, lineare und nichtlineare Systeme

2. **Einführung in die Wahrscheinlichkeitsrechnung**

   Einführung und Definitionen, Mehrstufige Zufallsexperimente, Diskrete Zufallsvariablen, Kontinuierliche Zufallsvariablen

3. **Grundbegriffe der Informationstheorie**

   Grundlegende Fragestellungen der Informationstheorie, Entropiebegriffe, Anwendungen

Voraussetzungen: Keine

Empfohlene Vorkenntnisse: Inhalte der Vorlesung Mathematik 1

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 Klausurvorbereitung vorgesehen.

Voraussetzungen für die Vergabe von Kreditpunkten: Bestandene Modulklausur

2.58 141218: Systemtheorie 2 - Signaltransformation

Nummer:	141218
Lehrform:	Vorlesungen und Übungen
Verantwortlicher:	Prof. Dr.-Ing. Aydin Sezgin
Dozenten:	Prof. Dr.-Ing. Aydin Sezgin M. Sc. Simon Tewes
Sprache:	Deutsch
SWS:	5
Leistungspunkte:	6
Gruppengröße:	300
Angeboten im:	Wintersemester

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 Lerninhalte. 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: Inhalte der Veranstaltungen Mathematik 1 und 2

Arbeitsaufwand: 180 Stunden

Der Arbeitsaufwand ergibt sich wie folgt: 14 Wochen zu je 5 SWS entsprechen in Summe 70 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 54 Stunden sind für die Klausurvorbereitung vorgesehen.

Prüfungsform: schriftlich, 120 Minuten

Voraussetzungen für die Vergabe von Kreditpunkten: Erfolgreiche Modulklausur

Literatur:

[1] M. Bossert, , T. Frey, "Signal- und Systemtheorie, 2. Auflage", Vieweg Verlag, 2008

2.59 140000: Tutorium

Nummer: 140000
Lehrform: Beliebig
Verantwortlicher: Friederike Kogelheide
Dozent: Tutoren
Sprache: Deutsch
SWS: 2
Angeboten im: Wintersemester

Ziele: Den Studierenden wird der Einstieg in das Studium erleichtert. Sie sind über inhaltliche und administrative Zusammenhänge informiert, haben Lerngruppen gebildet und haben verschiedene Kompetenzen der Lehrveranstaltungen der ersten Studiensemester vertieft.

Inhalt: Das Tutorium erleichtert allen Bachelor-Studienanfängern der Fakultät für Elektrotechnik und Informationstechnik in den ersten beiden Semestern den Einstieg ins Studium. Beim Tutorium handelt es sich um eine freiwillige Zusatzveranstaltung. In den wöchentlichen Treffen unterstützen so genannte „Tutoren“, meist Studierende aus höheren Semestern, die Erstsemester in der Anfangsphase ihres Studiums. Zunächst werden die Studenten mit der Uni insbesondere mit der Fakultät und den Einrichtungen bekannt gemacht. Die weiteren Themen erstrecken sich von der studentischen Selbstverwaltung über lerntechnische Fragen bis hin zu Freizeitangeboten in der Bochumer Umgebung. Im späteren Verlauf des Tutoriums rücken dann immer stärker fachliche Fragen in den Vordergrund.

Voraussetzungen: keine

Empfohlene Vorkenntnisse: Bereitschaft zur aktiven Mitarbeit und zur Gestaltung des eigenen Studienverlaufs

2.60 141245: Web-Sicherheit

Nummer:	141245
Lehrform:	Vorlesungen und Übungen
Medienform:	rechnerbasierte Präsentation
Verantwortlicher:	Prof. Dr. Jörg Schwenk
Dozenten:	Prof. Dr. Jörg Schwenk Dr.-Ing. Dennis Felsch M. Sc. Dominik Noß
Sprache:	Deutsch
SWS:	4
Leistungspunkte:	5
Angeboten im:	

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

Inhalt: Die Vorlesung behandelt die Sicherheit von Web-Anwendungen (Teil 1), Web-Services (Teil 2) und Single-Sign-On-Verfahren (Teil 3).

Teil 1: Sicherheit von Webanwendungen * HTTP, HTML, JavaScript, CSS * Same Origin Policy * Cross-Site-Scripting (reflected, stored, DOM) * Gegenmaßnahmen (Filter, Content Security Policy, DOMPurify) * CSRF und Schutz gegen CSRF * UI-Redressing

Teil 2: Sicherheit von Webanwendungen * XML, XML Schema, XSLT, XPath * XML Signature * Signature Wrapping-Angriffe * XML Encryption, Angriffe

Teil 3: Sicherheit von Single-Sign-On * Einsatzszenarien von TLS * Sicherheit DNS * SAML * Microsoft Passport, XSS-Angriff * Generische Angriffe auf SSO * Generischer Schutz mittels TLS * OpenID, OAuth, OpenID Connect * Spezielle Angriffe auf SSO

Voraussetzungen: keine

Empfohlene Vorkenntnisse:

- Grundkenntnisse Kryptographie und HTML

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 Klausurvorbereitung vorgesehen.

2.61 141249: Web-und Browsersicherheit

Nummer:	141249
Lehrform:	Vorlesungen und Übungen
Medienform:	Folien rechnerbasierte Präsentation
Verantwortlicher:	Prof. Dr. Jörg Schwenk
Dozenten:	Dr.-Ing. Mario Heiderich Dr.-Ing. Dennis Felsch
Sprache:	Englisch
SWS:	4
Leistungspunkte:	5
Angeboten im:	Wintersemester

Ziele: Studierende verfügen nach erfolgreichem Abschluss des Moduls über ein umfassendes Verständnis der technischen Aspekte von Web- und Browsersicherheit. Sie haben ein umfassendes Systemverständnis für komplexe Webanwendungen erworben. Durch eigenständige Überlegungen und deren Umsetzung in praktischen Projekten zur Verbesserung der Netzsicherheit bereiten sich die Studierenden auf ihre Rolle im Berufsleben vor. Sie können neue Probleme analysieren und neue Lösungsmöglichkeiten entwickeln. Sie können im Gespräch den Nutzen der von ihnen erarbeiteten Lösungen argumentativ begründen.

Inhalt: Die Vorlesung wird als Blockveranstaltung angeboten. Die Veranstaltung ist auch für Studierende geeignet, die bereits XML- und Webservicesicherheit/Websicherheit gehört haben und ihr Wissen vertiefen möchten. Dies ist jedoch keine Voraussetzung.

What to bring

- A Laptop, OS doesn't matter
- Working Internet Connection

Kapitel 1: History & Basics

- The History of Web Security and Web Attacks
- The History of Browsers
- HTML, JavaScript, CSS

Kapitel 2: HTTP, Server, SQLi

- Attacks using HTTP and SSL/TLS
- SQL Injections
- Uploads
- SSRF, XXE & XEE

Kapitel 3: Cookies, Sessions, XSS

- Cookies & Sessions
- Same Origin Policy

- Authentication & Authiorization
- The Basics of Cross-Site Scripting

Kapitel 4: Advanced XSS

- Advanced XSS
- mXSS and DOM Mutations

Kapitel 5: Browsers & Beyond

- The DOM
- DOM Clobbering & DOM XSS
- jQuery, Expression Injections, AngularJS
- postMessage XSS
- SVG
- Flash Security

Kapitel 6: Sandboxing & Random Bits

- JavaScript Sandboxing
- The Human Factor
- Stories from the Real World

Arbeitsaufwand: 150 Stunden

Der Arbeitsaufwand ergibt sich wie folgt: 8 Tage zu je 7,5 SWS entsprechen in Summe 60 Stunden Anwesenheit. Für die Vor- und Nachbereitung der Übungen sind in Summe 45 Stunden erforderlich. Etwa 55 Stunden sind für die Klausurvorbereitung vorgesehen.

Prüfungsform: schriftlich, 120 Minuten