RUHR-UNIVERSITÄT BOCHUM

RUB

Bachelorstudiengang IT-Sicherheit / Informationstechnik PO 20

Modulhandbuch

Fakultät für Elektrotechnik und Informationstechnik

Inhaltsverzeichnis

Kapitel 1

Module

1.1 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.64)
144004: Kolloquium ITS (S.95)

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 / 149

1.2 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.65)

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 / 149

1.3 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.68)

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 / 149

1.4 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.78)

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 / 149

1.5 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.80)

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 / 149

1.6 Elektrotechnik

Nummer: 149007
Verantwortlicher: Prof. Dr.-Ing. Ilona Rolfes
Arbeitsaufwand: 180 Stunden (entsprechend der Lehrveranstaltungen)
Leistungspunkte: 6
Semester: 1. Semester (BaITS/I)
Dauer: 1 Semester

Veranstaltungen:

141129: Elektrotechnik 1 - Elektrische Netzwerke 5 SWS (S.86)

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:

- 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: Klausurarbeit (120 Minuten)

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

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

Stellenwert der Note für die Endnote: 6 / 149

1.7 Freie Wahlfächer

Nummer: 149030
Verantwortlicher: Studiendekan ITS
Arbeitsaufwand: 270 Stunden (entsprechend der Lehrveranstaltungen)
Leistungspunkte: 9
Semester: 3. und 5. Semester (BaITS/I), 1.-3. Semester (MaITS/I), 1. Semester (MaITS/N)
Dauer: 1-3 Semester

Veranstaltungen:

141106: freie Veranstaltungswahl (S.89)

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

Inhalt: Bei der Auswahl geeigneter Lehrveranstaltungen kann das Vorlesungsverzeichnis der Ruhr-Universität verwendet werden. Dies schließt Veranstaltungen aller Fakultäten, des Optionalbereichs und des Zentrums für Fremdsprachenausbildung (Veranstaltungen aus Bachelor- oder Masterstudiengängen) mit ein, also auch die Angebote der nichttechnischen Veranstaltungen.

Zu beachten ist allerdings, dass bei Masterstudierenden in allen Fällen eine Anerkennung von Fächern aus dem zugehörigen Bachelorstudiengang nur sehr eingeschränkt möglich ist.

Weiterhin ist auch der Besuch von Lehrveranstaltungen anderer Universitäten möglich - z.B. im Rahmen der Kooperationsvereinbarung mit der Fakultät für Elektrotechnik und Informationstechnik der TU Dortmund.

Prüfungsform: siehe Lehrveranstaltungen

Voraussetzungen für die Vergabe von Kreditpunkten: siehe Lehrveranstaltungen

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

Stellenwert der Note für die Endnote: 0 / 149

1.8 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.94)

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 / 149

1.9 Informatik 1

Nummer: 149006
Verantwortlicher: Prof. Dr. Tobias Glasmachers
Arbeitsaufwand: 240 Stunden (entsprechend der Lehrveranstaltungen)
Leistungspunkte: 8
Semester: 1. Semester (BaITS/I)
Dauer: 1 Semester

Veranstaltungen:

141343: Programmierung für ITS (PO 20) 6 SWS (S.112)

Ziele: Nach dem erfolgreichen Abschluss des Moduls - kennen die Teilnehmer die wichtigsten Konzepte imperativer und objektorientierter Programmierung, - können die Teilnehmer eigene Programme entwerfen und implementieren, - können die Teilnehmer mit Grundbegriffen der Informatik wie etwa Korrektheit, Laufzeit, Boole'scher Algebra, Invarianten und abstrakten Datentypen arbeiten, - können die Teilnehmer die einfache Datenstrukturen (Arrays, Dictionaries) gezielt einsetzen und kennen Standardalgorithmen darauf, insbesondere zum Sortieren von Arrays.

Inhalt: Zentrales Thema der Veranstaltung ist das Erlernen der Programmierung und der wichtigsten Programmierkonzepte sowie die ersten Grundbegriffe der Informatik: - Imperative Programmierung (Variablen, Kontrollstrukturen, Funktionen und Rekursion, Fehlerbehandlung, Ereignisbehandlung) - einfache Datenstrukturen (Array und Dictionary) - Objektorientierung (Klassen, Sichtbarkeit, Schnittstellen, Vererbung) - Einführung in eine Reihe von Informatik-Konzepten (Invarianten, Laufzeitanalyse, Sortieralgorithmen, Repräsentation von Daten im Rechner, Boole'sche Algebra) Die Veranstaltung nutzt die Programmiersprache TScript ("teaching-script") für einen möglichst einfachen und motivierenden Einstieg in die Programmierung. Als Beispiele werden weiterhin die Programmiersprachen Python und Java genutzt.

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: 8 / 149

1.10 Informatik 2

Nummer: 149009
Verantwortlicher: Prof. Dr. Maike Buchin
Arbeitsaufwand: 240 Stunden (entsprechend der Lehrveranstaltungen)
Leistungspunkte: 8
Semester: 2. Semester (BaITS/I)
Dauer: 1 Semester

Veranstaltungen:

150322: Datenstrukturen und Algorithmen für ITS (PO 20) 6 SWS (S.72)

Ziele:

Nach dem erfolgreichen Abschluss des Moduls

- können Studierende Algorithmen formal beschreiben und deren Korrektheit beweisen
- können Studierende die Laufzeit und den Speicherbedarf von Algorithmen und Datenstrukturen analysieren und bewerten
- kennen Studierende grundlegende Datenstrukturen
- kennen Studierende grundlegende Schemata zum Entwurf von Algorithmen
- können Studierende Algorithmen und Datenstrukturen für spezifische Probleme entwickeln

Inhalt: Die Vorlesung gibt einen systematischen Überblick über den Entwurf und die Analyse von Algorithmen und Datenstrukturen. Dazu werden zunächst grundlegenden Methoden der Analyse (insbesondere Korrektheit, Laufzeit und Speicherbedarf) von Algorithmen vorgestellt. Anschließend werden einige Algorithmen zum Sortieren und Suchen analysiert. Ebenfalls werden verschiedene grundlegende Datenstrukturen (Listen, Felder, Suchbäume und Heaps) vorgestellt. Schließlich werden Graphen betrachtet: Ihre Darstellung und diverse Algorithmen auf Graphen (Durchläufe, kürzeste Wege, minimale Spannbäume). In den Übungen lernen die Studierende sowohl die theoretische Analyse von Algorithmen und Datenstrukturen als auch deren praktische Umsetzung in einer modernen Programmiersprache (z.B. Python).

Prüfungsform: Klausurarbeit (180 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: 8 / 149

1.11 Informatik 3

Nummer: 149028
Verantwortlicher: Prof. Dr. Eike Kiltz
Arbeitsaufwand: 240 Stunden (entsprechend der Lehrveranstaltungen)
Leistungspunkte: 8
Semester: 3. Semester (BaITS/I)
Dauer: 1 Semester

Veranstaltungen:

150302: Theoretische Informatik 6 SWS (S.129)

Ziele:

Nach dem erfolgreichen Abschluss des Moduls

- beherrschen die Studierenden den professionellen Umgang mit Berechnungsmodellen und ihren Beziehungen zu Sprachklassen. Dazu gehört die intellektuelle und methodische Fähigkeit, den Nachweis der Zugehörigkeit bzw. Nichtzugehörigkeit zu einer solchen Klasse zu führen.
- Durch Einüben von Beweistechniken wie wechselseitige Simulation oder berechenbare Reduktionen ist die Einsicht gereift, dass an der Oberfläche verschieden aussehende Konzepte im Kern identisch sein können. Zudem erlaubt dies den Studierenden, neue Anwendungsprobleme selbständig zu klassifizieren.
- erlernen die Studierenden ein einfach handhabbares Rechnermodell, die Turingmaschine, das ihnen fortan als Abstraktion für alle möglichen Rechner dient.
- erlangen die Studierenden fundamentale Einsichten, welche Probleme mit Hilfe von Rechnern effizient entschieden, mit Hilfe effizient entschieden, entschieden, zum Teil entschieden oder prinzipiell nicht entschieden werden können. Dadurch erlangen Sie ein tieferes Verständnis von Komplexität von Berechnungsproblemen.

Inhalt: Die Vorlesung gibt einen systematischen Überblick über die folgenden Themengebiete:

- Endliche Automaten und reguläre Ausdrücke
- Kellerautomaten und kontextfreie Grammatiken
- Turing-Maschinen und Entscheidbarkeit
- Nichtdeterminismus und NP-Vollständigkeitstheorie

Prüfungsform: Klausurarbeit (180 Minuten)

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

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

Stellenwert der Note für die Endnote: 8 / 149

1.12 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.98)

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 / 149

1.13 Mathematik 1

Nummer: 149005
Verantwortlicher: Prof. Dr. Gregor Leander
Arbeitsaufwand: 270 Stunden (entsprechend der Lehrveranstaltungen)
Leistungspunkte: 9
Semester: 1. Semester (BaITS/I)
Dauer: 1 Semester

Veranstaltungen:

150128: Mathematik 1 für Informatik und ITS (PO 20) 7 SWS (S.101)

Ziele:

Nach dem erfolgreichen Abschluss des Moduls

- kennen Studierende grundlegende Begriffe und Schreibweisen der Mathematik
- können Studierende die Techniken selbstständig anwenden und mathematische Sachverhalte darstellen,
- kennen Studierende die Grundlagen abstrakter mathematischer Strukturen und verschiedene Beispiel für Gruppen, Ringe und Körper
- Verstehen die Studierenden den abstrakten Vektorraumbegriff über beliebigen Körpern, können mit linearer Unabhängigkeit, Dimensionen und mit linearen Abbildungen umgehen.
- Die Studierenden können lineare Gleichungssysteme explizit lösen sowie Eigenwerte und Eigenvektoren berechnen.

Inhalt: Dieses Modul gibt eine allgemeine Einführung in mathematische Grundlagen und behandelt wichtige Gebiete der Linearen Algebra. Folgende Themen werden behandelt:

Grundlagen der Mathematik:

- Grundlegende mathematische Begriffe
- Schreibweisen
- Aussagenlogik
- Mengenlehre
- Relationen

Algebraische Grundlagen:

- ganze Zahlen
- Restklassen
- Gruppen-, Ringe- und Körper-Axiome

Lineare Algebra:

- Vektorräume
- Basen
- Dimension
- Skalarprodukte
- lineare Abbildungen
- lineare Gleichungssysteme
- Basiswechsel
- Determinanten
- Eigenwerttheorie

Prüfungsform: Klausurarbeit (180 Minuten)

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

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

Stellenwert der Note für die Endnote: 9 / 149

1.14 Mathematik 2

Nummer: 149008
Verantwortlicher: Studiendekan ITS
Arbeitsaufwand: 270 Stunden (entsprechend der Lehrveranstaltungen)
Leistungspunkte: 9
Semester: 2. Semester (BaITS/I)
Dauer: 1 Semester

Veranstaltungen:

150136: Mathematik 2 für Informatik und ITS (PO 20) 8 SWS (S.103)

Ziele: Nach dem erfolgreichen Abschluss des Moduls - kennen Studierende grundlegende Begriffe, Beweismethoden und Algorithmen aus der elementaren Zahlentheorie, - können Studierende die Beweistechniken selbstständig anwenden und mathematische Sachverhalte darstellen, - kennen Studierende erstes Sätze und Methoden aus der Kombinatorik und insbesondere aus der Graphentheorie und verstehen deren strukturelle Eigenschaften, - kennen Studierende erste fundamentale Algorithmen aus der Zahlentheorie und der Kombinatorik, können diese formalisieren, selbstständig implementieren sowie deren Laufzeiten analysieren

Inhalt: Euklidscher Algorithmus, Gruppen-, Ring-, Körperaxiome, Symmetriegruppen, Polynomarithmetik, formale Potenzreihen, modulare Arithmetik, Lemma von Bezout, Kleiner Satz von Fermat, diskreter Logarithmus, RSA-Verschlüsselungsverfahren, Primzahltests, Chinesischer Restesatz, p-adische Brüche, Newton-Verfahren, Asymptotische Notation durch Landausymbole, Binomialkoeffizienten, Rekursionsgleichungen, Erzeugendefunktionen, Prinzip der Inklusion-Exklusion, Vier-Farben-Problem, Djikstra-Algorithmus, Satz von Cayley, Hamiltonkreise, Google PageRank Algorithmus, Satz von Perron-Frobenoius, Implementierung konkreter Algorithmen in Computer-Algebra-Systemen

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

Stellenwert der Note für die Endnote: 9 / 149

1.15 Netzsicherheit 1

Nummer: 149003
Verantwortlicher: Prof. Dr. Jörg Schwenk
Arbeitsaufwand: 240 Stunden (entsprechend der Lehrveranstaltungen)
Leistungspunkte: 8
Semester: 3. Semester (BaITS/I)
Dauer: 1 Semester

Veranstaltungen:

142240: Grundlagenpraktikum ITS	3 SWS	(S.90)
141242: Netzsicherheit 1	4 SWS	(S.107)

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) + Praktikum

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

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

Stellenwert der Note für die Endnote: 8 / 149

1.16 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.109)

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 / 149

1.17 Signale und Systeme

Nummer: 149010
Verantwortlicher: Prof. Dr.-Ing. Rainer Martin
Arbeitsaufwand: 150 Stunden (entsprechend der Lehrveranstaltungen)
Leistungspunkte: 5
Semester: 2. Semester (BaITS/I)
Dauer: 1 Semester

Veranstaltungen:

141170: Systemtheorie 1 - Signale und Systeme 4 SWS (S.127)

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)

Stellenwert der Note für die Endnote: 5 / 149

1.18 Software Engineering

Nummer: 149029
Verantwortlicher: Studiendekan ITS
Arbeitsaufwand: 150 Stunden (entsprechend der Lehrveranstaltungen)
Leistungspunkte: 5
Semester: 3 Semester (BaITS/I)
Dauer: 1 Semester

Veranstaltungen:

141346: Software Engineering 4 SWS (S.124)

Ziele: Die Studierenden kennen die grundsätzlichen Prozesse und Phasen der Software-Entwicklung. Sie können ein Pflichtenheft mit Anforderungen und GUI-Prototypen erstellen. Sie können mit den wesentlichen Diagrammformaten der UML umgehen. Sie wissen, wie man ein Modell in eine objektorientierte Programmiersprache umsetzt.

Inhalt:

- methodische Entwicklung objektorientierter Softwaresysteme
- Einführung der Unified Modeling Language (UML)
- wesentliche Diagrammformate der UML (Use Cases, Klassendiagramme, Sequenzdiagramme und Zustandsdiagramme)
- typische Arbeitsschritte der Anforderungsermittlung in der Softwareentwicklung, der Erstellung der Softwarespezifikation und des Softwareentwurfs

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 / 149

1.19 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.125)

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 / 149

1.20 Technische Informatik 1

Nummer: 149002
Verantwortlicher: Studiendekan ETIT
Arbeitsaufwand: 150 Stunden (entsprechend der Lehrveranstaltungen)
Leistungspunkte: 5
Semester: 3. Semester (BaITS)
Dauer: 1 Semester

Veranstaltungen:

141026: Rechnerarchitektur für ET/IT und ITS (PO 20) 4 SWS (S.114)

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. Energieverbrauch, 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.

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 / 149

1.21 Technische Informatik 2

Nummer: 149032
Verantwortlicher: Prof. Dr.-Ing. Jürgen Oehm
Arbeitsaufwand: 150 Stunden (entsprechend der Lehrveranstaltungen)
Leistungspunkte: 5
Semester: 2. Semester (BaET), 4. Semester (BaITS/I)
Dauer: 1 Semester

Veranstaltungen:

141304: Digitaltechnik 4 SWS (S.75)

Ziele: Die Studierenden erwerben umfassende Kenntnisse in den Bereichen Boolesche Algebra, Struktur und Funktionalität digitaler Grundschaltungen, Kostenoptimierung digitaler Funktionsgruppen, Techniken zur taktsynchronen Verarbeitung von Daten, Kodierung und Verarbeitung von Daten, Struktur und Funktionalität solcher Grundfunktionalitäten, die insbesondere zentrale Bestandteile in Mikroprozessorarchitekturen und deren Umgebung sind. Richtlinien für den Wissenstransfer sind die schaltungstechnischen Möglichkeiten und Grenzen moderner CMOS-Logikstrukturen, um den Studierenden gleichzeitig auch aktuelle Entwicklungstrends in einer sich rasant entwickelnden digitalen Anwendungswelt besser verständlich zu machen.

Inhalt:

- Historischer Rückblick und Motivation
- Boolesche Algebra, minimale Schaltungen auf Basis von NAND und NOR
- Gatterlaufzeiten, Timing-Analyse, kritischer Pfad
- Zahlensysteme, Zahlenkodierungen, Fehlererkennung und Korrektur, Fest- und Fließkommadarstellungen
- Rechenschaltungen, arithmetisch logische Einheit (ALU),
- Flankendetektoren, bi-, mono- und astabile Schaltungen, transparente und nicht-transparente Flip-Flops (FF)
- Frequenzteiler, Zähler (asynchron, synchron), Automaten, Schieberegister
- Speicher: S-RAM, D-RAM, ROM, ... (Aufbau und Organistationsformen)
- taktsynchrone Techniken zur Datenverarbeitung
- ALU in Umgebungen zur Mikroprogrammierung, Mikroprogrammierung
- Konzepte zur serielle Datenübertragung
- Grundlagenidee von A/D- und D/A-Wandlern
- Konzept: skalierbare Standard-Logik-Zellen, CMOS-Logik
- Übersicht: Logikanalyse, Tools zur Logikanalyse, HDL Entwurfssprachen
- Moore, More than Moore

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, Bachelor Angewandte Informatik, Bachelor Informatik

Stellenwert der Note für die Endnote: 5 / 149

1.22 Tutorium

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

Veranstaltungen:

140000: Tutorium 2 SWS (S.131)

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 / 149

1.23 Usable Security

Nummer: 149031
Verantwortlicher: Prof. Dr. Markus Dürmuth
Arbeitsaufwand: 150 Stunden (entsprechend der Lehrveranstaltungen)
Leistungspunkte: 5
Semester: 4. Semester (BaITS/I)
Dauer: 1 Semester

Veranstaltungen:

141036: Einführung in die Usable Security and Privacy 4 SWS (S.82)

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:

- What is Usable Security?
- Human Behavior in IT Security
- Overview: Central application Scenarios
- Definitions/ Tasks/ Goals of Usable Security
- Human Error
- Cyber security awareness and education
- Cyber security culture
- What is hard for humans? - on limitations of the human
- User authentication
- Secure email and messaging
- Certicate warnings
- Privacy
- Social engineering and Phishing
- Captchas

Prüfungsform: Klausurarbeit (120 Minuten)

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

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

Stellenwert der Note für die Endnote: 5 / 149

1.24 Vertiefungspraktikum ITS

Nummer: 149004
Verantwortlicher: Studiendekan ITS
Arbeitsaufwand: 120 Stunden (entsprechend der Lehrveranstaltungen)
Leistungspunkte: 4
Semester: 5. Semester (BaITS/I)
Dauer: 1 Semester

Veranstaltungen:

142362: Bachelor-Forschungspraktikum Human-Centred Security	3 SWS	(S.44)
142028: Bachelor-Praktikum ARM Processors for Embedded Cryptography	3 SWS	(S.46)
142245: Bachelor-Praktikum TLS Implementierung	3 SWS	(S.48)
142242: Bachelor-Projekt Netz- und Datensicherheit	3 SWS	(S.50)
142025: Bachelor-Vertiefungspraktikum Wireless Physical Layer Security	3 SWS	(S.60)
142244: Bachelor-Vertiefungspraktikum zur Hackertechnik	3 SWS	(S.62)
211006: Praktikum zur Kryptanalyse	2 SWS	(S.111)

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: Praktikum oder Projektarbeit

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 / 149

1.25 Vertiefungsseminar ITS

Nummer: 149023
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.51)
143249: Bachelor-Seminar Human Centered Security and Privacy	3 SWS	(S.53)
143241: Bachelor-Seminar Netz- und Datensicherheit	3 SWS	(S.54)
141035: Bachelor-Seminar Security Engineering	3 SWS	(S.57)
143290: Bachelor-Seminar Usable Security and Privacy Research	3 SWS	(S.58)
150521: Fortgeschrittene Themen des Model Checking	2 SWS	(S.88)
150562: Seminar Satisfiability	2 SWS	(S.119)
150537: Seminar zur Kryptographie	2 SWS	(S.120)
150560: Seminar zur Real World Cryptoanalysis	2 SWS	(S.121)
150539: Seminar zur symmetrische Kryptographie	2 SWS	(S.122)
150520: Seminar über Grenzen in der theoretischen Informatik	2 SWS	(S.123)

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 / 149

1.26 Wahlpflichtfächer

Nummer: 149046
Verantwortlicher: Studiendekan ITS
Arbeitsaufwand: 450 Stunden (entsprechend der Lehrveranstaltungen)
Leistungspunkte: 15
Semester: 4./5. Semester (BaITS/I)
Dauer: 1 Semester

Veranstaltungen:

150357: Boolesche Funktionen mit Anwendungen in der Kryptographie	4 SWS	(S.67)
260081: Datenschutz	3 SWS	(S.70)
141347: Digitale Forensik	4 SWS	(S.73)
150326: Einführung in die asymmetrische Kryptanalyse	4 SWS	(S.77)
142031: Einführung ins Hardware Reverse Engineering	4 SWS	(S.84)
141024: Implementierung kryptographischer Verfahren	4 SWS	(S.92)
141031: Kryptographie auf hardwarebasierten Plattformen	4 SWS	(S.96)
150345: Logik in der Informatik	4 SWS	(S.100)
150324: Model Checking	4 SWS	(S.105)
141254: Red- and Blue Teaming	4 SWS	(S.116)
141249: Web-und Browsersicherheit	4 SWS	(S.132)

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

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

Prüfungsform: siehe Lehrveranstaltungen

Voraussetzungen für die Vergabe von Kreditpunkten: siehe Lehrveranstaltungen

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

Stellenwert der Note für die Endnote: 15 / 149

Kapitel 2

Veranstaltungen

2.1 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
Sprache:	Deutsch
SWS:	3
Leistungspunkte:	4
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

2.2 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:	4
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.

Voraussetzungen: keine

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

Arbeitsaufwand: 120 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 75 Stunden veranschlagt.

Prüfungsform: Praktikum, studienbegleitend

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

2.3 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:	4
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: 120 Stunden

Der Arbeitsaufwand berechnet sich wie folgt: 12 Wochen zu je 3 Stunden entsprechen 36 Stunden Anwesenheit. Für die Vorbereitung und Ausarbeitung der Protokolle werden jeweils 7 Stunden, insgesamt 84 Stunden veranschlagt.

Prüfungsform: Praktikum, studienbegleitend

2.4 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:	4
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: 120 Stunden

Für die Einarbeitung mit Betreuer werden 20 Stunden angesetzt. Für die Bearbeitung des Projekts 70 Stunden. Für die anschließende Ausarbeitung werden 30 Stunden angesetzt.

Prüfungsform: Projektarbeit, studienbegleitend

2.5 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:

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.

2.6 143249: Bachelor-Seminar Human Centered Security and Privacy

Nummer:	143249
Lehrform:	Seminar
Medienform:	Videoübertragung e-learning Internet 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

2.7 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
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.

Anmeldung Die Anmeldung und Vergabe der Seminarthemen erfolgt über das Seminarvergabesystem: https://seminar.hgi.rub.de/

Einführungsveranstaltung 2021-10-14, 14:00: Webinar, Anwesenheitpflicht

Prüfungsleistung Die Prüfungsleistung des Seminars besteht aus einem schriftlichen und einem mündlichen Teil. Das Seminar ist bestanden, wenn sowohl der schriftliche als auch der mündliche Prüfungsteil bestanden sind.

Schriftlicher Prüfungsteil Als Teil der schriftlichen Prüfung reicht jeder Seminarteilnehmer die folgenden eigenständig angefertigten schriftlichen Ausarbeitungen fristgerecht ein:

- Exposee (späteste Abgabe: 2021-10-20)
- Peer-Review Version der Seminararbeit (späteste Abgabe: 2021-11-16)
- Peer-Review (späteste Abgabe: 2021-11-30)
- Überarbeitete Version der Seminararbeit (späteste Abgabe: 2021-12-15)
- Finale Version der Seminararbeit (späteste Abgabe: 2022-02-04)

Der schriftliche Prüfungsteil ist bestanden, wenn alle Einreichungsfristen eingehalten wurden und die finale Version der Seminararbeit mit “ausreichend oder besser” bewertet ist.

Mündlicher Prüfungsteil Im Rahmen einer Blockveranstaltung am Semesterende trägt jeder Seminarteilnehmer sein Seminarthema im Rahmen einer 15- bis 20- minütigen Präsentation vor und beantwortet im Rahmen eines Prüfungsgesprächs Fragen zum Seminarthema. Der mündliche Prüfungsteil ist bestanden, wenn Vortrag und Prüfungsgespräch mit mindestens “ausreichend” bewertet wird.

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

2.8 141035: Bachelor-Seminar Security Engineering

Nummer:	141035
Lehrform:	Seminar
Medienform:	Folien
	Handouts
Verantwortlicher:	Prof. Dr. Amir Moradi
Dozenten:	Prof. 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

2.9 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

2.10 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
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.

Prüfungsform: Praktikum, studienbegleitend

2.11 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:	4
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: 120 Stunden

Der Arbeitsaufwand berechnet sich wie folgt: 6 Termine zu je 3 Stunden entsprechen 18 Stunden Anwesenheit. Für die Vorbereitung werden 24 Stunden (4 Stunden je Termin für 6 Termine), für die Bearbeitung der Übungszettel 12 Stunden (4 Stunden je Übungszettel für drei Übungszettel), und für die Implementierungsaufgaben 66 Stunden veranschlagt.

Prüfungsform: Praktikum, studienbegleitend

2.12 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
Sprache:	Deutsch
SWS:	3
Leistungspunkte:	4
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: 120 Stunden

Teilnahme an mindestens 7 Vorträgen zu je 1 Stunde mit jeweils anschließender Diskussion ergibt in etwa 12 Stunden. Die Bearbeitung von insgesamt 9 Versuchen mit je 5 Stunden Durchführung und je 7 Stunden Vor- und Nachbereitung ergibt 90 Stunden.

Prüfungsform: Praktikum, studienbegleitend

2.13 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

2.14 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

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

2.15 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: schriftlich, 120 Minuten

2.16 141250: Computernetze

Nummer:	141250
Lehrform:	Vorlesungen und Übungen
Medienform:	Moodle rechnerbasierte Präsentation
Verantwortlicher:	Prof. Dr. Jörg Schwenk
Dozenten:	Dr.-Ing. Christian Mainka M. Sc. Matthias Gierlings M. Sc. Louis Jannett 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.

2.17 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

2.18 150322: Datenstrukturen und Algorithmen für ITS (PO 20)

Nummer:	150322
Lehrform:	Vorlesungen und Übungen
Medienform:	Folien
	Tafelanschrieb
Verantwortlicher:	Prof. Dr. Maike Buchin
Dozent:	Prof. Dr. Maike Buchin
Sprache:	Deutsch
SWS:	6
Leistungspunkte:	8
Gruppengröße:	400
Angeboten im:	Sommersemester

Ziele: Nach dem erfolgreichen Abschluss des Moduls - können Studierende Algorithmen formal beschreiben und deren Korrektheit beweisen - können Studierende die Laufzeit und den Speicherbedarf von Algorithmen und Datenstrukturen analysieren und bewerten - kennen Studierende grundlegende Datenstrukturen - kennen Studierende grundlegende Schemata zum Entwurf von Algorithmen - können Studierende Algorithmen und Datenstrukturen für spezifische Probleme entwickeln

Inhalt: Die Vorlesung gibt einen systematischen Überblick über den Entwurf und die Analyse von Algorithmen und Datenstrukturen. Dazu werden zunächst grundlegenden Methoden der Analyse (insbesondere Korrektheit, Laufzeit und Speicherbedarf) von Algorithmen vorgestellt. Anschließend werden einige Algorithmen zum Sortieren und Suchen analysiert. Ebenfalls werden verschiedene grundlegende Datenstrukturen (Listen, Felder, Suchbäume und Heaps) vorgestellt. Schließlich werden Graphen betrachtet: Ihre Darstellung und diverse Algorithmen auf Graphen (Durchläufe, kürzeste Wege, minimale Spannbäume). In den Übungen lernen die Studierende sowohl die theoretische Analyse von Algorithmen und Datenstrukturen als auch deren praktische Umsetzung in einer modernen Programmiersprache (z.B. Python).

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.

Voraussetzungen für die Vergabe von Kreditpunkten: Bestandene Modulabschlussprüfung

2.19 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

Voraussetzungen für die Vergabe von Kreditpunkten: Bestandene Modulklausur

2.20 141304: Digitaltechnik

Nummer:	141304
Lehrform:	Vorlesungen und Übungen
Medienform:	Folien rechnerbasierte Präsentation
Verantwortlicher:	Prof. Dr.-Ing. Jürgen Oehm
Dozent:	Prof. Dr.-Ing. Jürgen Oehm
Sprache:	Deutsch
SWS:	4
Leistungspunkte:	5
Angeboten im:	Sommersemester

Ziele: Die Studierenden erwerben umfassende Kenntnisse in den Bereichen Boolesche Algebra, Struktur und Funktionalität digitaler Grundschaltungen, Kostenoptimierung digitaler Funktionsgruppen, Techniken zur taktsynchronen Verarbeitung von Daten, Kodierung und Verarbeitung von Daten, Struktur und Funktionalität solcher Grundfunktionalitäten, die insbesondere zentrale Bestandteile in Mikroprozessorarchitekturen und deren Umgebung sind. Richtlinien für den Wissenstransfer sind die schaltungstechnischen Möglichkeiten und Grenzen moderner CMOS-Logikstrukturen, um den Studierenden gleichzeitig auch aktuelle Entwicklungstrends in einer sich rasant entwickelnden digitalen Anwendungswelt besser verständlich zu machen.

Inhalt:

- Historischer Rückblick und Motivation
- Boolesche Algebra, minimale Schaltungen auf Basis von NAND und NOR
- Gatterlaufzeiten, Timing-Analyse, kritischer Pfad
- Zahlensysteme, Zahlenkodierungen, Fehlererkennung und Korrektur, Fest- und Fließkommadarstellungen
- Rechenschaltungen, arithmetisch logische Einheit (ALU),
- Flankendetektoren, bi-, mono- und astabile Schaltungen, transparente und nichttransparente Flip-Flops (FF)
- Frequenzteiler, Zähler (asynchron, synchron), Automaten, Schieberegister
- Speicher: S-RAM, D-RAM, ROM, ... (Aufbau und Organistationsformen)
- taktsynchrone Techniken zur Datenverarbeitung
- ALU in Umgebungen zur Mikroprogrammierung, Mikroprogrammierung
- Konzepte zur serielle Datenübertragung
- Grundlagenidee von A/D- und D/A-Wandlern
- Konzept: skalierbare Standard-Logik-Zellen, CMOS-Logik

- Übersicht: Logikanalyse, Tools zur Logikanalyse, HDL Entwurfssprachen
- Moore, More than Moore

Empfohlene Vorkenntnisse: Elementare Kenntnisse der Elektrotechnik 1 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, 120 Minuten

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] Eshragian, Karman, Eshragian, Kamran, Weste, Neil H. E. "Principles of CMOS VLSI Design: A Systems Perspective", Addison Wesley Longman Publishing Co, 1993
[8] Siemers, Christian, Sikora, Axel "Taschenbuch Digitaltechnik", Hanser Fachbuchverlag, 2002

2.21 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: schriftlich, 120 Minuten

2.22 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. Paul Staat M. Sc. Johannes Tobisch
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

2.23 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. Julian Speith M. Sc. Paul Staat M. Sc. Johannes Tobisch
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

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

2.24 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. Jennifer Friedauer M. Sc. Franziska Herbert M. Sc. Jonas Hielscher M. Sc. Marvin Kowalewski Prof. Dr. Martina Angela Sasse
Sprache:	Deutsch
SWS:	4
Leistungspunkte:	5
Angeboten im:	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 (Das Passwort zum Moodle-Kurs im SS 2021 lautet: UsableSoSe2021). Den Moodle-Kurs finden Sie unter dem Link oben rechts oder über die Kurs-Suche in Moodle.

Beginn der Vorlesung: Donnerstag den 15.04.2021 Beginn der Übung: Donnerstag den 22.04.2021

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 15.04.2021 - Die Dozenten stellen sich vor - Formalia zur Vorlesung

Teil 1: 22.04. bis 10.06.2021

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: 17.06. bis 15.07.2021

Applications (Prof. Dr. Markus Dürmuth)

- User authentication
- Secure email and messaging

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

22.07.2021 - Fragestunde zur Klausur
XX.XX.2021 - Klausurtermin

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

2.25 142031: Einführung ins Hardware Reverse Engineering

Nummer:	142031
Lehrform:	Vorlesung mit integrierten Übungen
Medienform:	Folien 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:	Englisch
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 "Technische Informatik 1 - Rechnerarchitektur" und "Technische Informatik 2 - Digitaltechnik".

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: schriftlich, 120 Minuten

2.26 141129: Elektrotechnik 1 - Elektrische Netzwerke

Nummer:	141129
Lehrform:	Vorlesungen und Übungen
Medienform:	rechnerbasierte Präsentation
Verantwortlicher:	Prof. Dr.-Ing. Ilona Rolfes
Dozent:	Prof. Dr.-Ing. Ilona Rolfes
Sprache:	Deutsch
SWS:	5
Leistungspunkte:	6
Gruppengröße:	ca. 350 - 400
Angeboten im:	Wintersemester

Ziele: Nach erfolgreichem Abschluss der Veranstaltung 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: Die Veranstaltung 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: 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 5 Stunden pro Woche, in Summe 70 Stunden, erforderlich. Etwa 40 Stunden sind für die Klausurvorbereitung vorgesehen.

Prüfungsform: schriftlich, 120 Minuten

2.27 150521: Fortgeschrittene Themen des Model Checking

Nummer: 150521
Lehrform: Seminar
Medienform: Moodle
Verantwortlicher: Prof. Dr. Thomas Zeume
Dozent: Prof. Dr. Thomas Zeume
Sprache: Deutsch
SWS: 2
Leistungspunkte: 3
Angeboten im: Sommersemester

Ziele: In der Veranstaltung Model Checking haben wir die theoretischen Grundlagen des Model Checkings kennen gelernt. Insbesondere haben wir die Spezifikationssprachen LTL und CTL eingeführt, ihre Ausdrucksstärke untersucht, und die wichtigsten algorithmischen Ansätze für das Model Checking erarbeitet.

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.

In diesem Seminar wollen wir uns mit weiterführenden, aktuellen Themen im Bereich Model Checking beschäftigen.

Voraussetzungen: Keine

Empfohlene Vorkenntnisse: Veranstaltung “Model Checking”

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

2.28 141106: freie Veranstaltungswahl

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

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

Inhalt: Bei der Auswahl geeigneter Lehrveranstaltungen kann das Vorlesungsverzeichnis der Ruhr-Universität verwendet werden. Dies schließt Veranstaltungen aller Fakultäten, des Optionalbereichs und des Zentrums für Fremdsprachenausbildung (Veranstaltungen aus Bachelor- oder Masterstudiengängen) mit ein, also auch die Angebote der nichttechnischen Veranstaltungen.

Zu beachten ist allerdings, dass bei Masterstudierenden in allen Fällen eine Anerkennung von Fächern aus dem zugehörigen Bachelorstudiengang nur sehr eingeschränkt möglich ist.

Weiterhin ist auch der Besuch von Lehrveranstaltungen anderer Univeristäten möglich - z.B. im Rahmen der Kooperationsvereinbarung mit der Fakultät für Elektrotechnik und Informationstechnik der TU Dortmund.

In der Fakultät wird speziell in diesem Bereich die Veranstaltung Methodik des wissenschaftlichen Publizierens angeboten. Im Rahmen der Kooperation mit der TU Dortmund wird folgende Veranstaltung angeboten: Musikdatenanalyse.

- nichttechnische Veranstaltungen: http://www.ei.rub.de/studium/lehrveranstaltungen/392/
- Methodik des wissenschaftlichen Publizierens: https://www.ei.rub.de/studium/lehrveranstaltungen/747
- Musikdatenanalyse: http://www.ei.rub.de/studium/lehrveranstaltungen/785/,

Voraussetzungen: entsprechend den Angaben zu der gewählten Veranstaltungen

Empfohlene Vorkenntnisse: entsprechend den Angaben zu der gewählten Veranstaltungen

Prüfungsform: None, studienbegleitend

Beschreibung der Prüfungsleistung: Die Prüfungsform und das Anmeldeverfahren kann entsprechend der gewählten Veranstaltungen variieren.

2.29 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: Für Studierende, die in der PO 2020 eingeschrieben sind, ist die Anmeldung zum Grundlagenpraktikum ETIT erst nach erfolgtem Beratungsgespräch möglich. Die Teilnahme an dem Beratungsgespräch sollte bis spätestens Ende Mai erfolgen.

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

2.30 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 Implementierung 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 verbreiteten 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 (SoSe21: Deadline 23.04.21).

MOODLE PASSWORT ikvWS2122$

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, 120 Minuten

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.

2.31 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

2.32 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

2.33 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

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.

2.34 150312: Kryptographie

Nummer:	150312
Lehrform:	Vorlesungen und Übungen
Medienform:	Blackboard
	Tafelanschrieb
Verantwortlicher:	Prof. Dr. Eike Kiltz
Dozent:	Prof. Dr. Eike Kiltz
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

2.35 150345: Logik in der Informatik

Nummer: 150345
Lehrform: Vorlesungen und Übungen
Medienform: Moodle
Verantwortlicher: Prof. Dr. Thomas Zeume
Dozent: Prof. Dr. Thomas Zeume
Sprache: Deutsch
SWS: 4
Leistungspunkte: 5
Angeboten im: Sommersemester

Ziele: In dieser Veranstaltung werden die formalen Grundlagen von modernen Logiken behandelt, mit einem Fokus auf ihrer Anwendung in der Informatik. Neben der klassischen Aussagenlogik und Prädikatenlogik betrachten wir auch Modallogik. Für jede dieser Logiken formalisieren wir Syntax und Semantik, lernen wie sich informatische Szenarien in ihnen modellieren lassen, und betrachten Algorithmen und Kalküle für Unerfüllbarkeit und Folgerungsbeziehung.

Inhalt: Logische Methoden spielen in vielen modernen Anwendungen der Informatik eine wichtige Rolle. Aus Datenbanken werden relevante Informationen mit Hilfe auf Logik basierender Anfragesprachen extrahiert; die formale Verifikation von Software und Hardware basiert auf logischen Spezifikationssprachen und Algorithmen für diese; und Methoden für das automatisierte Schlussfolgern in der künstlichen Intelligenz haben ihre Grundlage in der formalen Logik.

Voraussetzungen: Mathematik Grundlagenvorlesungen

Empfohlene Vorkenntnisse: Keine

Arbeitsaufwand: 150 Stunden

Der Arbeitsaufwand ergibt sich aus 56 Anwesenheitspflicht. Für die Vor- und Nachbereitung der Übungen werden 28 Stunden veranschlagt. 66 Stunden sind für die Klausurvorbereitung vorgesehen.

Prüfungsform: mündlich, 30 Minuten

Literatur:

[1] Schöning, Uwe "Logik für Informatiker", Spektrum Akademischer Verlag, 2000
[2] Kreuzer, M., Kühling, S. "Logik für Informatiker", Pearson, 2006

2.36 150128: Mathematik 1 für Informatik und ITS (PO 20)

Nummer:	150128
Lehrform:	Vorlesungen und Übungen
Verantwortlicher:	Prof. Dr. Gregor Leander
Dozent:	Prof. Dr. Gregor Leander
Sprache:	Deutsch
SWS:	7
Leistungspunkte:	9
Gruppengröße:	ca. 600
Angeboten im:	Wintersemester

Ziele:

Nach dem erfolgreichen Abschluss des Moduls

- kennen Studierende grundlegende Begriffe und Schreibweisen der Mathematik
- können Studierende die Techniken selbstständig anwenden und mathematische Sachverhalte darstellen,
- kennen Studierende die Grundlagen abstrakter mathematischer Strukturen und verschiedene Beispiel für Gruppen, Ringe und Körper
- Verstehen die Studierenden den abstrakten Vektorraumbegriff über beliebigen Körpern, können mit linearer Unabhängigkeit, Dimensionen und mit linearen Abbildungen umgehen.
- Die Studierenden können lineare Gleichungssysteme explizit lösen sowie Eigenwerte und Eigenvektoren berechnen.

Inhalt: Dieses Modul gibt eine allgemeine Einführung in mathematische Grundlagen und behandelt wichtige Gebiete der Linearen Algebra. Folgende Themen werden behandelt:

Grundlagen der Mathematik:

- Grundlegende mathematische Begriffe
- Schreibweisen
- Aussagenlogik
- Mengenlehre
- Relationen

Algebraische Grundlagen:

- ganze Zahlen
- Restklassen
- Gruppen-, Ringe- und Körper-Axiome

Lineare Algebra:

- Vektorräume
- Basen
- Dimension
- Skalarprodukte
- lineare Abbildungen
- lineare Gleichungssysteme
- Basiswechsel
- Determinanten
- Eigenwerttheorie

Empfohlene Vorkenntnisse: Mathematische Schulausbildung (gymnasiale 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: 270 Stunden

Der Arbeitsaufwand berechnet sich wie folgt: 14 Wochen zu je 7 SWS ergeben 98 Stunden Präsenzzeit. Es verbleiben 172 Stunden zur Vor- und Nachbereitung und zur Prüfungsvorbereitung.

Prüfungsform: schriftlich, 120 Minuten

2.37 150136: Mathematik 2 für Informatik und ITS (PO 20)

Nummer:	150136
Lehrform:	Vorlesungen und Übungen
Medienform:	Folien
	Tafelanschrieb
Verantwortlicher:	Prof. Dr. Christian Stump
Dozent:	Prof. Dr. Christian Stump
Sprache:	Deutsch
SWS:	8
Leistungspunkte:	9
Gruppengröße:	ca. 600
Angeboten im:	Sommersemester

Ziele:

Nach dem erfolgreichen Abschluss des Moduls

- kennen Studierende grundlegende Begriffe, Beweismethoden und Algorithmen aus der elementaren Zahlentheorie,
- können Studierende die Beweistechniken selbstständig anwenden und mathematische Sachverhalte darstellen,
- kennen Studierende erstes Sätze und Methoden aus der Kombinatorik und insbesondere aus der Graphentheorie und verstehen deren strukturelle Eigenschaften,
- kennen Studierende erste fundamentale Algorithmen aus der Zahlentheorie und der Kombinatorik, können diese formalisieren, selbstständig implementieren sowie deren Laufzeiten analysieren

Inhalt:

- Gruppen-, Ring-, Körperaxiome
- Permutationsgruppen
- Polynomarithmetik
- formale Potenzreihen
- p-adische Darstellungen
- Sieb des Eratosthenes
- Euklidscher Algorithmus
- Lemma von Bezout
- modulare Arithmetik
- diskreter Logarithmus

- Chinesischer Restesatz
- RSA-Verschlüsselungsverfahren
- Kleiner Satz von Fermat
- Satz von Euler
- Binomialkoeffizienten
- Rekursionsgleichungen
- Erzeugendefunktionen
- Prinzip der Inklusion-Exklusion
- Vier-Farben-Problem
- Satz von Cayley
- Hamiltonkreise
- Google PageRank Algorithmus
- Satz von Perron-Frobenius

Empfohlene Vorkenntnisse: Mathematische Schulausbildung (gymnasiale Oberstufe) und Inhalte des Moduls „Mathematik 1“

Arbeitsaufwand: 270 Stunden

Der Arbeitsaufwand berechnet sich wie folgt: 14 Wochen zu je 7 SWS ergeben 98 Stunden Präsenzzeit. Es verbleiben 182 Stunden zur Vor- und Nachbereitung und zur Prüfungsvorbereitung.

Voraussetzungen für die Vergabe von Kreditpunkten: Bestandene Modulabschlussprüfung und erfolgreiche Teilnahme an den praktischen Übungen am Rechner

2.38 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

2.39 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 M. Sc. Nurullah Erinola
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.

Veranstaltungsseite im Moodle: https://moodle.ruhr-uni-bochum.de/course/view.php?id=42146

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

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

Literatur:

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

2.40 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

[system-message] [system-message]system-message
WARNING/2 in `<string>`, line 17

Bullet list ends without a blank line; unexpected unindent. backrefs:

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

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

2.41 211006: Praktikum zur Kryptanalyse

Nummer: 211006
Lehrform: Praktikum
Medienform: Moodle
Verantwortlicher: Prof. Dr. Alexander May
Dozent: Prof. Dr. Alexander May
Sprache: Deutsch
SWS: 2
Leistungspunkte: 3
Angeboten im: Wintersemester

Ziele: Nach dem erfolgreichen Abschluss des Praktikums

- kennen die Studierenden die bekanntesten un wichtigsten Information Set Decoding Algorithmen und somit die besten Angriffe auf die aktuellen NIST Kanditaten McEliece und BIKE.
- können die Studierenden effiziente HPC Software schreiben, die auf bis zu 512 Kernen verteilt (kleinere) Kryptographische Instanzen brechen.
- kennen die Studierenden die Funktionsweise eines verteilt implementierten Systems und können darauf programmieren.
- kennen die Stundierenden die Grundlagen der Codebasierten Kryptographie.

Inhalt: Der inhaltliche Fokus dieses Praktikums liegt auf Code-basierten Kryptosystemen (wie McEliece, Niederreiter, BIKE) und der effizienten Implementierung von Algorithmen für Information Set Decoding.

Voraussetzungen: Keine

Empfohlene Vorkenntnisse: Gute bis sehr gute Kenntnisse in den Programmiersprachen C oder C++.

Arbeitsaufwand: 90 Stunden

Der Arbeitsaufwand berechnet sich wie folgt: Dem Praktikum geht eine Wöchentliche Einführungsveranstaltung für 4 Wochen voraus, dabei werden die wichtigsten Begriffe der Codetheorie eingeführt. Danach werden im Zwei-Wochen-Zyklus Programmieraufgaben veröffentlichen, die in Teams von bis zu 4 Studierenden gelöst werden müssen. Insgesamt sind 90 Stunden Arbeitszeit für das Praktikum anzusetzen.

Prüfungsform: Praktikum, studienbegleitend

2.42 141343: Programmierung für ITS (PO 20)

Nummer:	141343
Lehrform:	Vorlesung
Medienform:	e-learning
	Moodle
Verantwortlicher:	Prof. Dr. Tobias Glasmachers
Dozent:	Prof. Dr. Tobias Glasmachers
Sprache:	Deutsch
SWS:	6
Leistungspunkte:	8
Gruppengröße:	180
Angeboten im:	Wintersemester

Ziele: Nach dem erfolgreichen Abschluss des Moduls

- kennen die Teilnehmer die wichtigsten Konzepte imperativer und objektorientierter Programmierung,
- können die Teilnehmer eigene Programme entwerfen und implementieren,
- können die Teilnehmer mit Grundbegriffen der Informatik wie etwa Korrektheit, Laufzeit, Boole'scher Algebra, Invarianten und abstrakten Datentypen arbeiten,
- können die Teilnehmer die einfache Datenstrukturen (Arrays, Dictionaries) gezielt einsetzen und kennen Standardalgorithmen darauf, insbesondere zum Sortieren von Arrays.

Inhalt: Zentrales Thema der Veranstaltung ist das Erlernen der Programmierung und der wichtigsten Programmierkonzepte sowie die ersten Grundbegriffe der Informatik:

- Imperative Programmierung (Variablen, Kontrollstrukturen, Funktionen und Rekursion, Fehlerbehandlung, Ereignisbehandlung)
- einfache Datenstrukturen (Array und Dictionary)
- Objektorientierung (Klassen, Sichtbarkeit, Schnittstellen, Vererbung)
- Einführung in eine Reihe von Informatik-Konzepten (Invarianten, Laufzeitanalyse, Sortieralgorithmen, Repräsentation von Daten im Rechner, Boole'sche Algebra)

Die Veranstaltung nutzt die Programmiersprache TScript ("teaching-script") für einen möglichst einfachen und motivierenden Einstieg in die Programmierung. Als Beispiele werden weiterhin die Programmiersprachen Python und Java genutzt.

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 und die Klausurvorbereitung sind die restlichen 156 Stunden vorgesehen.

Prüfungsform: schriftlich, 120 Minuten

Voraussetzungen für die Vergabe von Kreditpunkten: bestandene Modulabschlussprüfung

2.43 141026: Rechnerarchitektur für ET/IT und ITS (PO 20)

Nummer:	141026
Lehrform:	Vorlesungen und Übungen
Medienform:	Videoübertragung Folien Moodle
Verantwortlicher:	Prof. Dr. Philipp Niemann
Dozent:	Prof. Dr. Philipp Niemann
Sprache:	Deutsch
SWS:	4
Leistungspunkte:	5
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 Prozessoen 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. Der inhaltliche Schwerpunkt der Vorlesung stellt die tiefgehende Analyse der Mikroarchitekturebene eines Prozessors dar, wobei auch moderne Verfahren zur Leistungssteigerung und deren Einsatzgebiete vorgestellt werden. 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.

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

Literatur:

[1] Hennessy, John L., Patterson, David A. "Computer Organization and Design MIPS Edition: The Hardware/Software Interface ", Morgan Kaufmann, 2013
[2] Drechsler, Rolf "Computer: Wie funktionieren Smartphone, Tablet & Co.? ", Springer Verlag, 2017
[3] Hoffmann, Dirk W. "Grundlagen der Technischen Informatik", Carl Hanser Verlag GmbH & Co.KG, 2009
[4] Austin, T., Tanenbaum, A.S. "Rechnerarchitektur (6. Auflage)", Pearson Studium, 2014
[5] Hennessy, John LeRoy , Patterson, David "Rechnerorganisation und Rechnerentwurf: Die Hardware/Software-Schnittstelle", Oldenbourg Wissenschaftsverlag, 2011
[6] Becker, Bernd "Technische Informatik: Eine einführende Darstellung", Oldenbourg Wissenschaftsverlag, 2008
[7] Becker, Bernd, Drechsler, Rolf, Molitor, Paul "Technische Informatik: Eine Einführung (Pearson Studium-IT)", Pearson Studium, 2005

2.44 141254: Red- and Blue Teaming

Nummer:	141254
Lehrform:	Vorlesungen und Übungen
Medienform:	e-learning
Verantwortlicher:	Prof. Dr. Jörg Schwenk
Dozent:	Dr.-Ing. Martin Grothe
Sprache:	Deutsch
SWS:	4
Leistungspunkte:	5
Angeboten im:	Wintersemester

Ziele: TBD

Inhalt: In dieser Lehrveranstaltung werden die Studierenden lernen, was die Aufgaben, Ziele und Pflichten eines Red Teams und eines Blue Teams sind. Dazu wird zu Beginn der Veranstaltung erklärt, wann welche Art von Sicherheitsüberprüfung in einem Unternehmen oder Organisation sinnvoll ist und welche Ziele damit überhaupt erreicht werden können. Dadurch sollen die Studierenden neben den technischen Kenntnissen und praktischen Fertigkeiten auch Projektorganisation, Budget Planung und das Verfassen von Berichten über Ihre Arbeit erlernen.

Das Niveau richtet sich vorrangig an Bachelor Studenten mit keiner oder geringer Erfahrung im offensiven bzw. defensiven Security Testing. Gleichzeitig sind erfahrene CTF Spieler herzlich willkommen und ich freue mich über einen regen Austausch in der Veranstaltung.

Die bisher geplanten Inhalte sind wie folgt aufgeschlüsselt:

- **Theorie:**
  - Einführung in das Thema Sicherheitsüberprüfungen (Kategorien, Nutzen/Ziele, Planung und Ablauf)
  - **Red Teaming**
    - Ursprünge und Geschichte des Red Teamings
    - Wichtige Standards, Best Practices und Organisationen
    - Arten, Aufgaben und Ziele eines Red Team Einsatzes
    - Planung, Ablauf und Nachbereitung eines Red Teaming Einsatzes
  - **Blue Teaming**
    - Einführung ins Blue Teaming
    - Wichtige Standards, Best Practices und Organisationen
    - Arten, Aufgaben und Ziele eines Blue Teams
    - Planung und Aufbau eins Blue Teams in der Organisation
  - **Technische Grundlagen**
    - Windows Betriebssystem, Services und Interna
    - Linux Betriebssystem und typische Serveranwendungen
    - wichtige Protokolle (Kerberos, SMB, usw.)
    - SIEM, Network Security Monitoring und IDS/IPS
  - **Angriffe**

    - Beispiele aus dem MITRE ATT&CK Framework
    - Für spezifische Windows Protokolle (Kerberos, SMB, etc.) und Services
    - Beispiele für Windows und Linux Privileg Escalation

- **Praxis:**
  - Die Bausteine aus der Theorie werden in Übungen und Hausaufgaben erklärt, vertieft und praktisch umgesetzt.
  - Dabei sollen die Aufgaben das Verständnis der Theorie erleichtern und das eigentliche praktische Umsetzen ermöglichen.
  - Umgang mit gängigen Penetration Testing Tools die in Kali Linux enthalten sind.

- **Organisation:**
  - Die Veranstaltung wird beim ersten Durchlauf im Wintersemester 2021/2022 als 2 Wochen Blockveranstaltung (14.03.2022 bis 25.03.2022) angeboten mit anschließender Klausur.
  - Jeder Veranstaltungstag beginnt um 9 Uhr und geht bis 18 Uhr
  - Es wird keine Teilnehmerbegrenzung geben.
  - Es wird Bonuspunkte geben, auch wenn noch keine Angaben über deren Vergabe getätigt werden kann.

- **Klausur:**
  - Es wird eine 2 stündige Klausur in rein schriftlicher Form am letzten Tag der Blockveranstaltung (25.03.2022 - Uhrzeit noch nicht klar) geben, die sowohl die Inhalte der Theorie und Praxis zum Gegenstand haben wird.

- **Voraussetzungen:**
  - Damit ihr euch auf die neuen Inhalte konzentrieren könnt, sind folgende Vorlesungen aus unserer Sicht notwendig: Computernetze, Betriebssysteme, Systemsicherheit, Netzsicherheit 1
  - Ein leistungsstarker Laptop mit **mindestens** den folgenden Eigenschaften: 64 Bit CPU, 8 Threads, 16 GB Arbeitsspeicher und entweder Intel VT-x oder AMD-V

Voraussetzungen: Keine

Empfohlene Vorkenntnisse:

Empfehlungen für optionale Vorkenntnisse:

- Grundlegende Python Programmierung
- Bash bzw. Powershell Kenntnisse
- Absolvieren des Wargames “Bandit” von Overthewire.org

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: schriftlich, 120 Minuten

2.45 150562: Seminar Satisfiability

Nummer:	150562
Lehrform:	Seminar
Medienform:	rechnerbasierte Präsentation Tafelanschrieb
Verantwortlicher:	Prof. Dr. Thomas Zeume
Dozent:	Prof. Dr. Thomas Zeume
Sprache:	Deutsch
SWS:	2
Leistungspunkte:	3
Angeboten im:	Wintersemester

Ziele: siehe Inhalt

Inhalt: Das Erfüllbarkeitsproblem für logische Formeln — lässt sich eine gegebene logische Formel erfüllen? — ist eines der fundamentalen algorithmischen Probleme. Grund hierfür ist, dass sich viele andere wichtige algorithmische Probleme auf verschiedene Varianten des Erfüllbarkeitsproblems reduzieren lassen.

In diesem Seminar im Theoriebereich der Informatik wollen wir uns mit dem Erfüllbarkeitsproblem aus verschiedenen Perspektiven und für verschiedene Logiken beschäftigen.

Der Schwerpunkt wird auf dem Erfüllbarkeitsproblem für aussagenlogische Formeln und dem Erfüllbarkeitsproblem für (eingeschränkte) prädikatenlogische Formeln liegen:

Das Erfüllbarkeitsproblem für aussagenlogische Formeln (SAT) ist die Grundlage der Theorie der NPschwierigen Probleme: Jedes Problem aus NP lässt sich auf SAT zurückführen, ist also höchstens so schwierig wie SAT. Fortschritte beim Lösen von SAT übertragen sich deshalb auch in der Praxis oft auf andere Probleme aus NP. Das Erfüllbarkeitsproblem für (eingeschränkte) prädikatenlogische Formeln ist unter anderem die Grundlage für das Schlussfolgern in wissensbasierten Systemen und für die formale Verifikation von Hardware und Software. Für allgemeine prädikatenlogische Formeln ist das Erfüllbarkeitsproblem nicht algorithmisch lösbar (formal: unentscheidbar). In der Praxis werden daher oft eingeschränkte Klassen prädikatenlogischer Formeln benutzt, für die sich das Problem noch algorithmisch lösen lässt. Ziel des Seminars ist es, ein gutes Verständnis dafür zu entwickeln, mit welchen Varianten des Erfüllbarkeitsproblem sich algorithmisch gut umgehen lässt und für welche Art von Problemstellungen dies jeweils hilfreich ist.

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

2.46 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.

2.47 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 und Sommersemester

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

2.48 150539: Seminar zur symmetrische Kryptographie

Nummer: 150539
Lehrform: Seminar
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: Wir besprechen aktuelle Forschungsresultate in der symmetrischen Kryptographie.

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

2.49 150520: Seminar über Grenzen in der theoretischen Informatik

Nummer: 150520
Lehrform: Seminar
Medienform: Moodle
Verantwortlicher: Prof. Dr. Thomas Zeume
Dozent: Prof. Dr. Thomas Zeume
Sprache: Deutsch
SWS: 2
Leistungspunkte: 3
Angeboten im: Sommersemester

Ziele: In diesem Seminar wollen wir theoretische Grenzen aus verschiedensten Bereichen der theoretischen Informatik ausloten. Dabei soll der Fokus auf Grenzen aus der Logik, Komplexitäts- und Berechenbarkeitstheorie, sowie aus der Automatentheorie liegen.

Inhalt: Wo verläuft die Grenze zwischen Entscheidbarkeit und Unentscheidbarkeit? Welche Probleme lassen sich mit moderatem Ressourcenbedarf lösen? Wo liegen die Grenzen unserer Methoden für den Nachweis von unteren Schranken an den Ressourcenbedarf von Problemen? Was lässt sich überhaupt beweisen?

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.

2.50 141346: Software Engineering

Nummer: 141346
Lehrform: Vorlesungen und Übungen
Verantwortlicher: Prof. Dr. Thorsten Berger
Dozent: Prof. Dr. Thorsten Berger
Sprache: Deutsch
SWS: 4
Leistungspunkte: 5
Gruppengröße: ca. 300-400
Angeboten im: Wintersemester

Ziele: Die Studierenden kennen die grundsätzlichen Prozesse und Phasen der Software-Entwicklung. Sie können ein Pflichtenheft mit Anforderungen und GUI-Prototypen erstellen. Sie können mit den wesentlichen Diagrammformaten der UML umgehen. Sie wissen, wie man ein Modell in eine objektorientierte Programmiersprache umsetzt.

Inhalt:

- methodische Entwicklung objektorientierter Softwaresysteme
- Einführung der Unified Modeling Language (UML)
- wesentliche Diagrammformate der UML (Use Cases, Klassendiagramme, Sequenzdiagramme und Zustandsdiagramme)
- typische Arbeitsschritte der Anforderungsermittlung in der Softwareentwicklung, der Erstellung der Softwarespezifikation und des Softwareentwurfs

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.

2.51 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

2.52 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
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

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

2.53 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: Mathematische Vorkenntnisse über komplexe Zahlen, Funktionen und Reihen sowie die Grundlagen der Differential- und Integralrechnung

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

2.54 150302: Theoretische Informatik

Nummer: 150302
Lehrform: Vorlesungen und Übungen
Verantwortlicher: Prof. Dr. Maike Buchin
Dozent: Prof. Dr. Maike Buchin
Sprache: Deutsch
SWS: 6
Leistungspunkte: 8
Gruppengröße: 300
Angeboten im: Wintersemester

Ziele: Nach dem erfolgreichen Abschluss der Veranstaltung

- beherrschen die Studierenden den professionellen Umgang mit Berechnungsmodellen und ihren Beziehungen zu Sprachklassen. Dazu gehört die intellektuelle und methodische Fähigkeit, den Nachweis der Zugehörigkeit bzw. Nichtzugehörigkeit zu einer solchen Klasse zu führen.
- durch Einüben von Beweistechniken wie wechselseitige Simulation oder berechenbare Reduktionen ist die Einsicht gereift, dass an der Oberfläche verschieden aussehende Konzepte im Kern identisch sein können. Zudem erlaubt dies den Studierenden, neue Anwendungsprobleme selbständig zu klassifizieren.
- erlernen die Studierenden ein einfach handhabbares Rechnermodell, die Turingmaschine, das ihnen fortan als Abstraktion für alle möglichen Rechner dient.
- erlangen die Studierenden fundamentale Einsichten, welche Probleme mit Hilfe von Rechnern effizient entschieden, mit Hilfe effizient entschieden, entschieden, zum Teil entschieden oder prinzipiell nicht entschieden werden können. Dadurch erlangen Sie ein tieferes Verständnis von Komplexität von Berechnungsproblemen.

Inhalt: Die Vorlesung gibt einen systematischen Überblick über die folgenden Themengebiete:

- Endliche Automaten und reguläre Ausdrücke
- Kellerautomaten und kontextfreie Grammatiken
- Turing-Maschinen und Entscheidbarkeit
- Nichtdeterminismus und NP-Vollständigkeitstheorie

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, 150 Minuten

Voraussetzungen für die Vergabe von Kreditpunkten: Bestandene Modulabschlussprüfung

2.55 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

2.56 141249: Web-und Browsersicherheit

Nummer:	141249
Lehrform:	Vorlesungen und Übungen
Medienform:	Folien rechnerbasierte Präsentation
Verantwortlicher:	Prof. Dr. Jörg Schwenk
Dozenten:	Dr.-Ing. Mario Heiderich M. Sc. Simon Rohlmann
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