RUHR-UNIVERSITÄT BOCHUM

RUB

Masterstudiengang IT-Sicherheit / Netze und Systeme PO 13

Modulhandbuch

Fakultät für Elektrotechnik und Informationstechnik

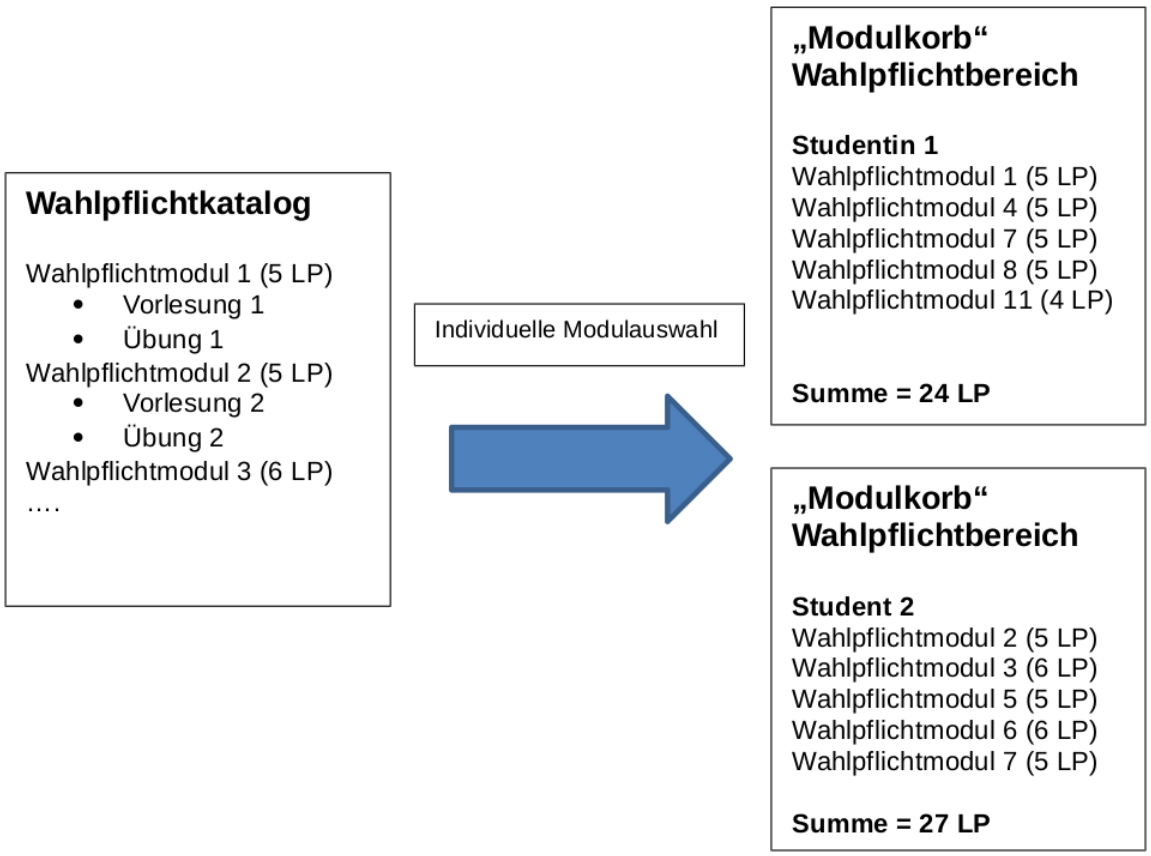
Erläuterung zum Wahlpflichtbereich des Studiengangs

Bei dem Wahlpflichtbereich (Theorie und Anwendungen der IT-Sicherheit) handelt es sich jeweils um einen „Modulkorb“, der sich aus verschiedenen Modulen zusammensetzt. Die wählbaren Module sind im Wahlpflichtkatalog zusammengestellt. Die Studierenden können mit ihrer konkreten Auswahl eigene Schwerpunkte setzen.

Die Leistungspunkte (LP) jedes einzelnen Moduls werden den Studierenden nach der bestandenen Modulprüfung gutgeschrieben. Jedes einzelne Modul kann dabei innerhalb eines Semesters abschlossen werden.

Der Wahlpflichtbereich, also der Modulkorb, ist abgeschlossen, wenn die Studierenden Module aus dem zugehörigen Wahlpflichtkatalog im angegebenen Umfang abgeschlossen haben.

Die nachfolgende Grafik verdeutlicht diese Zusammenhänge:



Inhaltsverzeichnis

Kapitel 1

Module

1.1 Betriebssystemsicherheit

Nummer: 149342
Verantwortlicher: Prof. Dr. Thorsten Holz
Arbeitsaufwand: 150 Stunden (entsprechend der Lehrveranstaltungen)
Leistungspunkte: 5

Veranstaltungen:

141342: Betriebssystemsicherheit 4 SWS (S.39)

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

Inhalt: Im Rahmen dieses Moduls werden grundlegende Angriffstechniken (z.B. *Buffer Overflows* oder *Race Conditions*) sowie Schutzmaßnahmen (z.B. nicht-ausführbarer Speicher oder *Address Space Layout Randomization*) behandelt. Ferner werden Themen wie Virtualisierung/Hypervisor sowie das sogenannte Einsperrungs-Problem (*Confinement Problem*) und die damit verbundene Analyse der verdeckten Kanäle in einem Computer-System behandelt. Ein weiterer Themenkomplex dieses Moduls ist moderne Schadsoftware. Dazu werden zunächst die Grundbegriffe in diesem Bereich erläutert und danach verschiedene Methoden zur Erkennung von Schadsoftware diskutiert. Wichtige Algorithmen in diesem Bereich werden vorgestellt und verschiedene Ansätze für Intrusion Detection Systeme werden behandelt.

Prüfungsform: Modulklausur

Stellenwert der Note für die Endnote: 5 / 106

1.2 Diskrete Mathematik

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

Veranstaltungen:

150308: Diskrete Mathematik 6 SWS (S.50)

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

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

Prüfungsform: Klausurarbeit (180 Minuten)

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

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

Stellenwert der Note für die Endnote: 8 / 106

1.3 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.55)

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 / 106

1.4 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.57)

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 / 106

1.5 Einführung in die theoretische Informatik

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

Veranstaltungen:

150310: Einführung in die theoretische Informatik 4 SWS (S.59)

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

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

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

Prüfungsform: siehe Lehrveranstaltungen

Stellenwert der Note für die Endnote: 6 / 106

1.6 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.82)

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 / 106

1.7 Master-Praktikum ITS

Nummer: 149918
Verantwortlicher: Studiendekan ITS
Arbeitsaufwand: 90 Stunden (entsprechend der Lehrveranstaltungen)
Leistungspunkte: 3
Semester: 3. Semester (MaITS/N), 1-3. Semester (MaITS/I)
Dauer: 1 Semester

Veranstaltungen:

142363: Master-Forschungspraktikum Human-Centred Security	3 SWS	(S.87)
142061: Master-Forschungspraktikum Usable Security und Privacy	3 SWS	(S.89)
142364: Master-Praktikum (Laborstudien) Human-Centred Security	3 SWS	(S.91)
142027: Master-Praktikum ARM Processors for Embedded Cryptography	3 SWS	(S.93)
143143: Master-Praktikum Embedded Linux	3 SWS	(S.95)
142020: Master-Praktikum Embedded Smartcard Microcontrollers	3 SWS	(S.96)
142181: Master-Praktikum Entwurf integrierter Digitalschaltungen mit VHDL	3 SWS	(S.98)
142022: Master-Praktikum Java-Card	3 SWS	(S.100)
142221: Master-Praktikum Machine Learning and Security	3 SWS	(S.102)
142246: Master-Praktikum Programmanalyse	3 SWS	(S.104)
150584: Master-Praktikum SAGE in der Kryptographie	2 SWS	(S.106)
142249: Master-Praktikum Schwachstellenanalyse	3 SWS	(S.107)
142248: Master-Praktikum Security Appliances	3 SWS	(S.109)
142023: Master-Praktikum Seitenkanalangriffe	3 SWS	(S.111)
150000: Master-Praktikum Smart Contracts	3 SWS	(S.113)
142250: Master-Praktikum TLS Implementierung	3 SWS	(S.114)
142026: Master-Praktikum Wireless Physical Layer Security	3 SWS	(S.116)
142243: Master-Praktikum zur Hackertechnik	3 SWS	(S.118)
142040: Master-Projekt DSP	3 SWS	(S.120)
142024: Master-Projekt Eingebettete Sicherheit	3 SWS	(S.122)
142241: Master-Projekt Netz- und Datensicherheit	3 SWS	(S.123)
142184: Master-Projekt Virtual Prototyping von Embedded Systems	3 SWS	(S.124)
211006: Praktikum zur Kryptanalyse	2 SWS	(S.169)
211006: Praktikum zur Kryptanalyse	2 SWS	(S.169)

Ziele: Die Studierenden sind befähigt, in einem kleinen Team Aufgaben aus dem Bereich der IT-Sicherheit zu lösen und die Ergebnisse in ingenieurwissenschaftlicher Weise zu dokumentieren. Sie können gezielt Methoden der strukturierten Analyse anwenden und deren Wirkung analysieren.

Inhalt: Das Modul besteht aus einem Praktikum oder einem Projekt.

In den Praktika werden fortgeschrittene Themen der IT-Sicherheit behandelt. Mögliche Themen sind hier die FPGA-Programmierung von Kryptoverfahren oder Trusted Computing.

In einem Projekt werden komplexe Themen eigenständig im Verlauf eines Semesters bearbeitet. Mögliche Themen sind Implementierung von Web-basierten Sicherheitsmechanismen, oder SmartCard Implementierungen.

Prüfungsform: Praktikum oder Projektarbeit

Voraussetzungen für die Vergabe von Kreditpunkten: siehe Lehrveranstaltungen

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

Stellenwert der Note für die Endnote: 0 / 106

1.8 Master-Seminar ITS

Nummer: 149917
Verantwortlicher: Studiendekan ITS
Arbeitsaufwand: 90 Stunden (entsprechend der Lehrveranstaltungen)
Leistungspunkte: 3
Semester: 3. Semester (MaITS/N), 1.-3. Semester (MaITS/I)
Dauer: 1 Semester

Veranstaltungen:

150521: Fortgeschrittene Themen des Model Checking	2 SWS	(S.66)
143242: Master-Seminar Aktuelle Themen der IT-Sicherheit	3 SWS	(S.126)
143250: Master-Seminar Applied Privacy and Anonymity	3 SWS	(S.128)
143245: Master-Seminar Digitale Signaturen	3 SWS	(S.129)
143021: Master-Seminar Embedded Security	3 SWS	(S.130)
143248: Master-Seminar Human Centered Security and Privacy	3 SWS	(S.131)
150538: Master-Seminar Kryptographie	3 SWS	(S.132)
150999: Master-Seminar Kryptologie	3 SWS	(S.133)
143240: Master-Seminar Netz- und Datensicherheit	3 SWS	(S.134)
150534: Master-Seminar on Secure Multiparty Computation	3 SWS	(S.137)
141211: Master-Seminar Physical Layer Security Journal Club	2 SWS	(S.139)
143251: Master-Seminar Privacy and Security in Mobile Operating Systems	3 SWS	(S.141)
150540: Master-Seminar Research oriented Cryptography	3 SWS	(S.142)
143244: Master-Seminar Security and Privacy of Wireless Networks and Mobile Devices	3 SWS	(S.143)
141034: Master-Seminar Security Engineering	3 SWS	(S.144)
148212: Master-Seminar Sichere Hardware	3 SWS	(S.145)
143022: Master-Seminar Smart Technologies for the Internet of Things	3 SWS	(S.146)
143163: Master-Seminar Sprach- und Mustererkennung	3 SWS	(S.148)
143291: Master-Seminar Usable Security and Privacy Research	3 SWS	(S.150)
150542: Seminar on Knowledge Graphs	2 SWS	(S.184)
150562: Seminar Satisfiability	2 SWS	(S.186)
150537: Seminar zur Kryptographie	2 SWS	(S.187)
150560: Seminar zur Real World Cryptoanalysis	2 SWS	(S.188)
150539: Seminar zur symmetrische Kryptographie	2 SWS	(S.189)
150520: Seminar über Grenzen in der theoretischen Informatik	2 SWS	(S.190)

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): Master IT-Sicherheit/Netze und Systeme, Master IT-Sicherheit/Informationstechnik

Stellenwert der Note für die Endnote: 0 / 106

1.9 Master-Startup ITS

Nummer: 149875
Verantwortlicher: Studiendekan ITS
Arbeitsaufwand: Keine Stunden (entsprechend der Lehrveranstaltungen)
Leistungspunkte: 1
Semester: 1., 2. oder 3. Semester

Veranstaltungen:

140002: Master-Startup ITS 2 SWS (S.151)

Ziele: Erleichterung des Einstiegs in das Studium; Vernetzung der Studierenden untereinander; Einsicht in Berufsbilder, Karrieremöglichkeiten etc.

Inhalt: Studienbegleitende Informationen, Exkursionen, Vorträge etc.

Prüfungsform: Es handelt sich um eine freiwillige Zusatzveranstaltung.

Stellenwert der Note für die Endnote: 0 / 106

1.10 Masterarbeit ITS

Nummer: 149890
Verantwortlicher: Studiendekan ITS
Arbeitsaufwand: 900 Stunden (entsprechend der Lehrveranstaltungen)
Leistungspunkte: 30
Semester: 4. Semester (MaITS/N), 4. Semester (MaITS/I)
Dauer: 6 Monate

Veranstaltungen:

144102: Masterarbeit ITS (S.152)

Ziele: Die Teilnehmer sind mit Arbeitsmethoden der wissenschaftlichen Forschung und der Projektorganisation vertraut. Ihre fortgeschrittenen Kenntnisse und Arbeitsergebnisse können sie verständlich präsentieren.

Inhalt: Weitgehend eigenständige Lösung einer wissenschaftlichen Aufgabe unter Anleitung. Teilnahme an 5 Kolloquiumsvorträgen über die Ergebnisse von Masterarbeiten in der Fakultät ET/IT. Präsentation der eigenen Ergebnisse der Masterarbeit im Kolloquium.

Prüfungsform: Abschlussarbeit

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

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

Stellenwert der Note für die Endnote: 30 / 106

1.11 Netzsicherheit 1

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

Veranstaltungen:

141242: Netzsicherheit 1 4 SWS (S.160)

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

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

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

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

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

Prüfungsform: Klausurarbeit (120 Minuten)

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

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

Stellenwert der Note für die Endnote: 5 / 106

1.12 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.162)

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 / 106

1.13 Nichttechnische Wahlfächer

Nummer: 149891
Verantwortlicher: Studiendekan ITS
Arbeitsaufwand: Mindestens 120 Stunden (entsprechend der Lehrveranstaltungen)
Leistungspunkte: ≥ 4
Semester: 1.-3. Semester (MaITS/I)
Dauer: 1 Semester

Veranstaltungen:

141105: Nichttechnische Veranstaltungen (S.164)

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

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

Prüfungsform: siehe Lehrveranstaltungen

Voraussetzungen für die Vergabe von Kreditpunkten: siehe Lehrveranstaltungen

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

Stellenwert der Note für die Endnote: 0 / 106

1.14 Rechnerarchitektur

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

Veranstaltungen:

141140: Rechnerarchitektur für ET/IT und ITS (PO 13) 4 SWS (S.179)

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

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

Prüfungsform: siehe Lehrveranstaltungen

Stellenwert der Note für die Endnote: 5 / 106

1.15 Theorie und Anwendungen der IT-Sicherheit

Nummer: 149919
Verantwortlicher: Studiendekan ITS
Arbeitsaufwand: Mindestens 720 Stunden (entsprechend der Lehrveranstaltungen)
Leistungspunkte: $\geq$24

Veranstaltungen:

141251: Aktuelle Themen im Bereich der Internet-Sicherheit	4 SWS	(S.30)
148207: Algebraische Codierung für die sichere Datenübertragung	3 SWS	(S.32)
1503341: Asymmetrische Kryptanalyse	3 SWS	(S.34)
141348: Aufbau eines Managementsystems für Informationssicherheit nach DIN ISO/IEC 27001	3 SWS	(S.35)
141244: Authentische Schlüsselvereinbarung: Formale Modelle und Anwendungen	4 SWS	(S.37)
150357: Boolesche Funktionen mit Anwendungen in der Kryptographie	4 SWS	(S.41)
150361: Cryptocurrencies	3 SWS	(S.42)
260081: Datenschutz	3 SWS	(S.43)
150332: Deep Learning	4 SWS	(S.45)
141347: Digitale Forensik	4 SWS	(S.46)
148229: Digitale Signaturen	4 SWS	(S.48)
150326: Einführung in die asymmetrische Kryptanalyse	4 SWS	(S.52)
141480: Einführung in die Datenanalyse mit Anwendungen in der IT-Sicherheit und Privatsphäre	3 SWS	(S.53)
141036: Einführung in die Usable Security and Privacy	4 SWS	(S.61)
142031: Einführung ins Hardware Reverse Engineering	4 SWS	(S.63)
150347: Elliptische Kurven und Kryptographie	4 SWS	(S.65)
141341: Human Aspects of Cryptography Adoption and Use	4 SWS	(S.68)
141024: Implementierung kryptographischer Verfahren	4 SWS	(S.70)
141247: Introduction to System Safety Engineering and Management	2 SWS	(S.72)
150262: Komplexitätstheorie	6 SWS	(S.74)
148219: Kryptanalytische Werkzeuge	4 SWS	(S.76)
141031: Kryptographie auf hardwarebasierten Plattformen	4 SWS	(S.78)
148203: Kryptographie auf programmierbarer Hardware	4 SWS	(S.80)
150343: Kryptographische Protokolle	4 SWS	(S.84)
150345: Logik in der Informatik	4 SWS	(S.85)
141027: Menschliches Verhalten in der IT Sicherheit	4 SWS	(S.153)
141252: Message-Level Security	4 SWS	(S.155)
141032: Methoden der Benutzer-Authentisierung	3 SWS	(S.157)
150324: Model Checking	4 SWS	(S.158)
141028: Physical Attacks and Countermeasures	4 SWS	(S.166)
150306: Post-Quantum Kryptographie	4 SWS	(S.168)
148215: Private and Anonymous Communication	4 SWS	(S.170)
150355: Probabilistische Algorithmen	4 SWS	(S.171)
141241: Programmanalyse	4 SWS	(S.172)
150277: Public Key Verschlüsselung	4 SWS	(S.174)

Ziele: Die Studierenden haben ein vertieftes Verständnis in ausgewählten Themen der IT-Sicherheit. Sie kennen entsprechende Methoden und sind befähigt, diese zielgerichtet einzusetzen bzw. anzuwenden.

Inhalt: Anwendungs- oder theoriespezifische Vertiefung der IT-Sicherheit. Vertiefungen können beispielsweise in der Netzsicherheit, der eingebetten Sicherheit, oder der Systemsicherheit liegen.

Es sind Module aus dem Wahlpflichtkatalog des Studienschwerpunktes auszuwählen. Jedes Modul besteht aus je einer Lehrveranstaltung (Vorlesung + Übung) mit eigener Modulabschlussprüfung.

Zur Vermeidung von Mehrfachbeschreibungen jeweils identischer Module und Lehrveranstaltungen, wird direkt auf die Lehrveranstaltungsbeschreibung verwiesen, die auch die jeweils zugehörigen LP enthält.

Insgesamt sind im Wahlpflichtbereich Module im Gesamtumfang von mindestens 24 Leistungspunkten zu wählen.

Prüfungsform: siehe Lehrveranstaltungen

Stellenwert der Note für die Endnote: 24 / 106

1.16 Wahlfächer

Nummer: 149898
Verantwortlicher: Studiendekan ITS
Arbeitsaufwand: Mindestens 120 Stunden (entsprechend der Lehrveranstaltungen)
Leistungspunkte: ≥ 4

Veranstaltungen:

141106: freie Veranstaltungswahl (S.67)

Ziele: Die Studierenden haben vertiefte Kenntnisse in technischen oder nichttechnischem Gebieten entsprechend ihrer Wahl. Dies beinhaltet sowohl die fachliche Vertiefung als auch den Erwerb von 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 Master-, Bachelor- oder Diplomstudiengängen) mit ein, also auch die Angebote der nichttechnischen Veranstaltungen . Im Rahmen einer Kooperationsvereinbarung mit der Fakultät für Elektrotechnik und Informationstechnik der TU Dortmund ist auch die Wahl dort angebotener Veranstaltungen möglich.

Prüfungsform: siehe Lehrveranstaltungen

Stellenwert der Note für die Endnote: 0 / 106

Kapitel 2

Veranstaltungen

2.1 141251: Aktuelle Themen im Bereich der Internet-Sicherheit

Nummer:	141251
Lehrform:	Vorlesungen und Übungen
Medienform:	Moodle
Verantwortlicher:	Prof. Dr. Jörg Schwenk
Dozent:	Prof. Dr. Jörg Schwenk
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 aktuellen Forschungsthemen im Bereich der Internet-Sicherheit. Sie haben die neuesten Angriffe und Sicherheitsmechanismen kennengelernt. Zusätzlich wissen Sie, wie man mit Sicherheitsschwachstellen korrekt umgeht und wie man diese an den Hersteller meldet. Durch die wissenschaftsnahe Themen haben die Studierenden Einblicke in die Forschung im Bereich der Internetsicherheit gekriegt, wodurch sie sich auch auf ihre potentielle Forschungsrolle vorbereitet haben.

Inhalt: In der Vorlesung werden ausgewählte Themen der IT-Sicherheit behandelt, die vom Lehrstuhl für Netz- und Datensicherheit in den letzten Jahren publiziert wurden. Es werden unter anderem folgende Themen behandelt:

- Portable Document Flaws
- Overview over Cryptographic Modelling with the Example of Messaging
- 0-RTT and Tor
- Padding Oracles
- Racoon
- Breaking Microsoft RMS 2020
- IPsec-Bleichenbacher
- DEMONS: DNS-Poisoning by Exhaustive Misappropriation of Network Sockets
- DOM
- XS Leaks
- UI Redressing

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

0em

Anmeldung: Diese Veranstaltung wird online durchgeführt. Bitte melden Sie sich bei einer Teilnahme im nachfolgenden Moodle-Kurs an:

- Aktuelle Themen im Bereich der Internet-Sicherheit (141251-WiSe20/21)

Voraussetzungen: Keine

Empfohlene Vorkenntnisse: Die Veranstaltung baut (unter anderem) auf diesen Kursen auf:

- Netzsicherheit 1 und 2
- Einführung in die Kryptographie

Arbeitsaufwand: 150 Stunden

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

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

2.2 148207: Algebraische Codierung für die sichere Datenübertragung

Nummer: 148207
Lehrform: Vorlesungen und Übungen
Medienform: Tafelanschrieb
Verantwortlicher: Prof. Dr. Jörg Schwenk
Dozent: Dr.-Ing. Klaus Huber
Sprache: Deutsch
SWS: 3
Leistungspunkte: 4
Angeboten im:

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

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

Gliederung

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

- Izyklische Codes für die Mannheim Metrik

6. Das Kryptosystem von McEliece
7. Die MacWilliamstransformation

Voraussetzungen: keine

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

Arbeitsaufwand: 120 Stunden

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

Prüfungsform: schriftlich, 120 Minuten

2.3 1503341: Asymmetrische Kryptanalyse

Nummer: 1503341
Lehrform: Vorlesungen und Übungen
Verantwortlicher: Prof. Dr. Alexander May
Dozent: Prof. Dr. Alexander May
Sprache: Deutsch
SWS: 3
Leistungspunkte: 4
Angeboten im:

Ziele: Die Studierenden beherrschen die wichtigsten Algorithmen in der Kryptanalyse

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

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

Voraussetzungen: keine

Empfohlene Vorkenntnisse:

- Inhalte der Vorlesungen:
  - Einführung in die Kryptographie 1 und 2
  - Einführung in die asymmetrische Kryptanalyse

Arbeitsaufwand: 120 Stunden

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

Prüfungsform: mündlich, 30 Minuten

2.4 141348: Aufbau eines Managementsystems für Informationssicherheit nach DIN ISO/IEC 27001

Nummer:	141348
Lehrform:	Vorlesungen und Übungen
Medienform:	rechnerbasierte Präsentation
Verantwortlicher:	Prof. Dr. Thorsten Holz
Dozent:	Dr.-Ing. Sebastian Uellenbeck
Sprache:	Deutsch
SWS:	3
Leistungspunkte:	4
Gruppengröße:	max. 20
Angeboten im:	Wintersemester und Sommersemester

Ziele: Die Studierenden haben ein fundiertes Verständnis über den Aufbau eines ISMS nach ISO 27001 und kennen die notwendigen Schritte, um ein Unternehmen zur Zertifizierungsreife zu begleiten. Studierenden können eigenständig neue Probleme analysieren und neue Lösungsmöglichkeiten entwickeln. Sie können mit diesem Verständnis mit ihren Kollegen über ISO/IEC 27001 diskutieren und auftretende Probleme im Gespräch korrekt klassifizieren.

Inhalt: Die Lehrveranstaltung vermittelt fokussiert Inhalte aus der ISO/IEC 27001 Auditorensicht. Dazu ist folgende Gliederung geplant:

- Zielsetzung
- Prinzipien und Terminologien
- Auditprinzipien gemäß ISO 19011:2011 Richtlinien
- ISO 19011
- ISO 27001:2013 Dokumentation
- Auditvorbereitung: Pre-Audit Meeting und Auditpläne
- Vorbereitung von Checklisten
- Audittechniken
- Auditorenpräsentationen
- Auditergebnisse und Abschlusstreffen
- Abweichungen, Bericht der Beobachtungen und Folgemaßnahmen
- Folgemaßnahmen

Weitergehend werden technische Lösungsmittel besprochen, die auf dem Weg zur ISO 27001 Zertifizierung hilfreich sein können. Hierzu zählen unter anderem Security Information and Event Management Systeme (SIEM) und Identity Management Systeme (IdM).

Voraussetzungen: keine

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

Arbeitsaufwand: 120 Stunden

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

Prüfungsform: schriftlich, 90 Minuten

Voraussetzungen für die Vergabe von Kreditpunkten: Bestandene Modulprüfung

2.5 141244: Authentische Schlüsselvereinbarung: Formale Modelle und Anwendungen

Nummer:	141244
Lehrform:	Vorlesungen und Übungen
Medienform:	rechnerbasierte Präsentation Tafelanschrieb
Verantwortlicher:	Prof. Dr. Jörg Schwenk
Dozenten:	Prof. Dr. Jörg Schwenk Dipl.-Math. Marcus Brinkmann
Sprache:	Deutsch
SWS:	4
Leistungspunkte:	5
Angeboten im:	Sommersemester

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

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

- Kryptographische Grundlagen (Kurze Widerholung der Wahrscheinlichkeitstehorie, Informationstheorie, etc.)
- Beweisbare Sicherheit
- Analyse von Schlüsselaustauschprotokollen, mit besonderem Fokus auf praktische Beispielprotokolle (wie TLS oder SSH)

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

Voraussetzungen: keine

Empfohlene Vorkenntnisse:

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

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

2.6 141342: Betriebssystemsicherheit

Nummer:	141342
Lehrform:	Vorlesungen und Übungen
Medienform:	e-learning Moodle rechnerbasierte Präsentation
Verantwortlicher:	Prof. Dr. Thorsten Holz
Dozent:	Prof. Dr. Thorsten Holz
Sprache:	Deutsch
SWS:	4
Leistungspunkte:	5
Gruppengröße:	60
Angeboten im:	Wintersemester

Ziele: Die Studierenden beherrschen theoretische und praktische Aspekte der Sicherheit von Softwaresystemen und sind zu einer kritischen Betrachtung der Systemsicherheit in der Lage. Insbesondere erwerben die Studierenden die Fähigkeit zum Modellieren konkreter Fragestellungen und Anforderungsanalysen aus vorhandenen Systeminformationen bzw. Systemgegebenheiten. Sie können eigenständig neue Probleme analysieren und neue Lösungsmöglichkeiten entwickeln. Die Studierenden sind in der Lage, neue Sicherheitsmodelle selbst zu erstellen und diese argumentativ zu verteidigen.

Inhalt: Im Rahmen dieser Veranstaltung werden verschiedene Sicherheitsaspekte von Betriebssystemen vorgestellt und erläutert. Dazu werden sowohl wichtige Angriffsmethoden (z.B. *Buffer Overflows*, *Race Conditions*, *Microarchitectural Attacks* etc.) als auch Abwehrstrategien (z.B. nicht-ausführbarer Speicher, *Address Space Layout Randomization* oder *Memory Tagging*) diskutiert. Andere Themen der Vorlesung sind *Fuzzing*, Obfuskierung sowie die sogenannte Einsperrungs-Problem (*Confinement Problem*) und die damit verbundene Analyse der verdeckten Kanäle in einem Computer-System.

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

Voraussetzungen: keine

Empfohlene Vorkenntnisse: Erfahrung in systemnaher Programmierung sowie 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, Bonuspunkte für erfolgreiche Bearbeitung der Übungsblätter

2.7 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

2.8 150361: Cryptocurrencies

Nummer:	150361
Lehrform:	Vorlesungen und Übungen
Medienform:	rechnerbasierte Präsentation Tafelanschrieb
Verantwortlicher:	Jun. Prof. Dr. Sebastian Faust
Dozent:	Jun. Prof. Dr. Sebastian Faust
Sprache:	Deutsch
SWS:	3
Leistungspunkte:	4.5
Angeboten im:	

Ziele: Verständnis von kryptographischen Protokollen und Techniken im Einsatzgebiet von digitalen Währungen

Inhalt: Die Studierenden erlenen kryptographische Verfahren und Protokolle, die in der digitalen Wirtschaft eingesetzt werden. Neben Brands eCash verfahren, werden wird eine Einführung in kryptographische Währungen wie z.B. Bitcoin gegeben.

Themen sind: - kryptographische Protokolle - eCash - Kryptographische Währungen basierend auf Proof of Works (z.B. Bitcoin & Litecoin) - Alternative Mining Puzzles - Alternative kryptographische Währungen basierend auf Proof of Stake - Broadcast Verschlüsselung und sicheres Verteilen von digitalen Inhalten

Voraussetzungen: keine

Empfohlene Vorkenntnisse: Grundkenntnisse aus der Vorlesung Kryptographie

Arbeitsaufwand: 135 Stunden

Der Arbeitsaufwand berechnet sich wie folgt: 14 Wochen zu je 3 SWS ergeben 42 Stunden Anwesenheit. Zum Lösen der Übungsaufgaben sind zwei Stunden je Woche vorgesehen. Es verbleiben 65 Stunden zur Vor- und Nachbereitung und zur Prüfungsvorbereitung.

Prüfungsform: schriftlich, 120 Minuten

2.9 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

2.10 150332: Deep Learning

Nummer:	150332
Lehrform:	Vorlesungen und Übungen
Medienform:	Folien
	Tafelanschrieb
Verantwortlicher:	Prof. Dr. Asja Fischer
Dozent:	Prof. Dr. Asja Fischer
Sprache:	Deutsch
SWS:	4
Leistungspunkte:	5
Angeboten im:	Wintersemester und Sommersemester

Ziele: Die Vorlesung hat das Ziel, einen Einblick in dieses Gebiet zu vermitteln. Zu Beginn werden die grundlegenden Begriffe und Konzepte des maschinellen Lernens eingeführt. Im weiteren Verlauf wird auf verschiedene neuronale Netze, Gradienten-basierte Optimierungsverfahren und generative Modelle eingegangen.

Inhalt: Deep Learning ist ein Untergebiet des maschinellen Lernens, welches in den letzten Jahren zu Durchbrüchen in zahlreichen Anwendungsgebieten (wie z.B. in der Objekt- und Spracherkennung und der maschinellen Übersetzung) geführt hat.

Deep Learning Methoden finden unter anderem Anwendung im Bereich IT Security

Empfohlene Vorkenntnisse: Grundkenntnisse der Linearen Algebra und Wahrscheinlichkeitstheorie sind von Vorteil.

Arbeitsaufwand: 150 Stunden

Der Arbeitsaufwand berechnet sich wie folgt: 15 Wochen zu je 2 SWS ergeben 30 Stunden Anwesenheit. Es verbleiben 120 Stunden zur Vor- und Nachbereitung und zur Prüfungsvorbereitung.

Prüfungsform: schriftlich, 120 Minuten

2.11 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

2.12 148229: Digitale Signaturen

Nummer: 148229
Lehrform: Vorlesungen und Übungen
Medienform: Tafelanschrieb
Verantwortlicher: Prof. Dr. Jörg Schwenk
Dozenten: Prof. Dr.-Ing. Tibor Jager
Dr.-Ing. Sebastian Lauer
Sprache: Deutsch
SWS: 4
Leistungspunkte: 5
Angeboten im:

Ziele: Im Rahmen dieser Vorlesung wird ein solides Grundverständnis für die Konstruktion von sicheren digitalen Signaturverfahren vermittelt. Grundlegende und moderne Techniken werden in der Vorlesung erklärt und anhand von Übungsaufgaben vertieft. Dies stellt eine ideale Vorbereitung auf eine forschungsnahe Abschlussarbeit in der (theoretischen) Kryptographie dar.

Inhalt:

- Grundlagen zu digitalen Signaturen
- Einmalsignaturverfahren
- Chamäleon-Hashfunktionen
- RSA-basierte Signaturverfahren
- Pairing-basierte Signaturverfahren
- Ausgewählte praktische Signaturverfahren und Angriffe

Voraussetzungen: keine

Empfohlene Vorkenntnisse: Vorausgesetzt werden grundlegende Kryptographie-Kenntnisse, wie sie in der Vorlesung "Einführung in die Kryptographie und Datensicherheit" vermittelt werden. Dies schliesst zum Beispiel ein Grundverständnis des RSA-Verfahrens und des diskreten Logarithmusproblems ein.

Grundkenntnisse der theoretischen Informatik (z.B. Reduktionsbeweise) oder fortgeschrittene Kenntnisse der Kryptographie und diskreten Mathematik sind empfehlenswert.

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, 90 Minuten

2.13 150308: Diskrete Mathematik

Nummer:	150308
Lehrform:	Vorlesungen und Übungen
Medienform:	Folien
	Tafelanschrieb
Verantwortlicher:	Priv.-Doz. Dr. Björn Schuster
Dozent:	Priv.-Doz. Dr. Björn Schuster
Sprache:	Deutsch
SWS:	6
Leistungspunkte:	8
Angeboten im:	Wintersemester

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

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

Voraussetzungen: keine

Empfohlene Vorkenntnisse: Elementare Grundkenntnisse in Analysis und linearer Algebra

Arbeitsaufwand: 240 Stunden

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

Prüfungsform: schriftlich, 180 Minuten

2.14 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

2.15 141480: Einführung in die Datenanalyse mit Anwendungen in der IT-Sicherheit und Privatsphäre

Nummer:	141480
Lehrform:	Vorlesungen und Übungen
Medienform:	Moodle rechnerbasierte Präsentation Tafelanschrieb
Verantwortlicher:	Prof. Dr. rer. nat. Sascha Fahl
Dozent:	Prof. Dr. rer. nat. Sascha Fahl
Sprache:	Deutsch
SWS:	3
Leistungspunkte:	4
Angeboten im:	

Ziele: Die Studierenden erlernen die grundlegenden Fähigkeiten Datensätze wie sie etwa im Rahmen von Benutzerstudien oder Logfiles mit Bezug zu IT-Sicherheit anfallen mit Hilfe von empirischen und visuellen Methoden zu analysieren. Darüber hinaus erlangen sie praktische Fertigkeiten im Umgang mit der statistischen Auswertung mit der Programmiersprache Python und diversen Datenanalysebibliotheken.

Inhalt: Die Vorlesung behandelt insbesondere folgende Themen:

Einführung

- Überblick
- Motivation
- Statistische Grundlagen

Methodische Grundlagen

- Einführung in die Datenerhebung (z.b. Experiment- und Surveydesign)
- Einführung explorative Datenauswertung
- Deskriptive Statistik
- Hypothesentests
- Korrelation/Regressionsanalyse

Zentrale Themen

- Statistische Verfahren zur Datenauswertung
- Python zur statistischen Auswertung
- Visuelle Datenauswertung
- Case Studies

Voraussetzungen: Keine

Empfohlene Vorkenntnisse: Keine besonderen Vorkenntnisse erforderlich, Grundkenntnisse der IT-Sicherheit und Erfahrungen in Python sind aber hilfreich.

Arbeitsaufwand: 120 Stunden

Der Arbeitsaufwand setzt sich wie folgt zusammen: 15 Wochen zu je 3 SWS Anwesenheit (entspricht in Summe 45 Stunden). Für die Nachbereitung der Vorlesung und Vor- und Nachbereitung der Übung sind etwa 3 Stunden pro Woche, in Summe 45 Stunden, erforderlich. Etwa 30 Stunden sind für die Klausurvorbereitung vorgesehen.

2.16 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

2.17 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

2.18 150310: Einführung in die theoretische Informatik

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

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

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

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

Voraussetzungen: keine

Empfohlene Vorkenntnisse: Grundkenntisse über Diskrete Mathematik und Algorithmen

Arbeitsaufwand: 180 Stunden

Der Arbeitsaufwand ergibt sich wie folgt: 14 Wochen zu je 5 SWS entsprechen in Summe 70 Stunden Anwesenheit. Für die Nachbereitung der Vorlesung und die Vor- und Nachbereitung der Übungen sind etwa 4 Stunden pro Woche, in Summe 56 Stunden, erforderlich. Etwa 54 Stunden sind für die Klausurvorbereitung vorgesehen.

Prüfungsform: schriftlich, 120 Minuten

2.19 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

2.20 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

2.21 150347: Elliptische Kurven und Kryptographie

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

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

Inhalt:

Themenübersicht:

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

Voraussetzungen: keine

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

Arbeitsaufwand: 150 Stunden

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

2.22 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

2.23 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.

2.24 141341: Human Aspects of Cryptography Adoption and Use

Nummer:	141341
Lehrform:	Vorlesungen und Übungen
Medienform:	e-learning Internet Moodle rechnerbasierte Präsentation
Verantwortlicher:	Prof. Dr. Martina Angela Sasse
Dozenten:	Prof. Dr. Martina Angela Sasse M. Sc. Yasemin Acar M. Sc. Konstantin Fischer Prof. Dr. Martina Angela Sasse
Sprache:	Englisch
SWS:	4
Leistungspunkte:	5
Angeboten im:	Wintersemester

Ziele:

The aim of the lecture is to examine the reasons why

a) cryptographic solutions – which experts agree offer good protection against most oft the common attacks today – are not adopted by most individuals and organisations, and

b) end-users, developers and system administrators who do use cryptographic solutions in some form frequently make mistakes that undermine the security protection.

Inhalt: In 1999, Whitten & Tygar's seminal USENIX paper "Why Johnny Can't Encrypt" established that people cannot use PGP encryption correctly, even with a graphical user interface and instruction.

Over the past 20 years, there has been a string of Johnny papers on studies trying to encourage adoption or correct usage. The aim of this CASA lecture is to systematically examine the results of these studies and identify effective ways of promoting adoption and enable correct use of cryptography.

- Usability, utility and technology adoption
- Security threat models and people's mental models
- Complexity or simplicity – who needs to know what?
- Designing frictionless user journeys
- Methods for testing and tweaking

Voraussetzungen: None

Empfohlene Vorkenntnisse: Lecture "Introduction to Usable Security and Privacy"

Arbeitsaufwand: 150 Stunden

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

Prüfungsform: mündlich, 30 Minuten

2.25 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.

2.26 141247: Introduction to System Safety Engineering and Management

Nummer:	141247
Lehrform:	Vorlesung mit integrierten Übungen
Medienform:	rechnerbasierte Präsentation
Verantwortlicher:	Prof. Dr.-Ing. Tim Güneysu
Dozenten:	Prof. Dr.-Ing. Tim Güneysu B. Sc. Jakob Feldtkeller
Sprache:	Englisch
SWS:	2
Leistungspunkte:	3
Gruppengröße:	ca. 20-30 Teilnehmer
Angeboten im:	Sommersemester

Ziele: On completion of this block course, participants will:

- understand risk, and the factors influencing perception and acceptability of risk;
- be able to give definitions of safety-related terminology and discuss how the use of terminology varies between countries and industrial sectors;
- have an understanding of typical safety-critical systems lifecycles and the roles of the major groups of techniques within the lifecycle.

Inhalt: HINWEIS: Diese Veranstaltung wird ausschließlich in englischer Sprache angeboten.

Course Description: This block course provides an introduction to the basic concepts and principles of system safety, including risk, hazard, accidents, and failure, and techniques for safety analysis and assessment. It also provides a brief overview of related material, such as legal issues, management of safety critical projects, and human factors.

Topics include:

- Introduction to accidents, hazards and risk;
- Formal definitions of safety engineering terminology;
- Legal and moral context;
- System lifecycles view of safety activities;
- The concept of Safety Risk and making decisions about risk;
- Introduction to Safety Cases;
- Overview of safety analysis techniques;
- Safety-critical software;
- Introduction to Safety Cases;
- Introduction to Safety Management

In the end, participants have to complete an assessment approximately over the next six weeks which results in the final grade for this course.

Students can choose to only do a short assessment, which results in ungraded 2 CP for this course (only as a free elective course), instead of 3 graded CP (as a mandatory elective course).

Voraussetzungen: none

Arbeitsaufwand: 90 Stunden

The workload is accumulated as follows: 4 days with 8 HWS each correspond to a total of 32 hours of physical presence. For the preparation of exercises and further reading accumulated 30 hours are required. About 28 hours are required in preparation for the examination.

Prüfungsform: Projektarbeit, studienbegleitend

2.27 150262: Komplexitätstheorie

Nummer: 150262
Lehrform: Vorlesungen und Übungen
Medienform: Moodle
Verantwortlicher: Prof. Dr. Thomas Zeume
Dozent: Prof. Dr. Thomas Zeume
Sprache: Deutsch
SWS: 6
Leistungspunkte: 9
Angeboten im: Sommersemester

Ziele: Die Vorlesung hat das Ziel, einen breiten Überblick über die grundlegenden Konzepte und Resultate der Komplexitätstheorie zu geben:

- Klassische Resultate für Platz- und Zeitkomplexitätsklassen: z.B. die Korrespondenz zwischen Spielen und Speicherplatz-Beschränkungen, der Nachweis, dass sich mit mehr Platz oder Zeit auch mehr Probleme lösen lassen, weitere grundlegende Beziehungen zwischen Zeit- und Platzbasierten Klassen, und die Komplexitätswelt zwischen NP und PSPACE
- Grundzüge der Komplexitätstheorie paralleler, zufallsbasierter und approximativer Algorithmen
- Einführung in ausgewählte neuere Themen: Komplexitätstheorie des interaktiven Rechnens, des probabilistischen Beweisens und Fine-grained Complexity.

Diese Veranstaltung richtet sich an Studierende der Mathematik und Informatik.

Inhalt: Die Komplexitätstheorie untersucht und klassifiziert Berechnungsprobleme bezüglich ihrer algorithmischen Schwierigkeit. Ziel ist es, den inhärenten Ressourcenverbrauch bezüglich verschiedener Ressourcen wie Rechenzeit oder Speicherplatz zu bestimmen, und Probleme mit ähnlichem Ressourcenverbrauch in Komplexitätsklassen zusammenzufassen. Die bekanntesten Komplexitätsklassen sind sicherlich P und NP, die die in polynomieller Zeit lösbaren bzw. verifizierbaren Probleme umfassen. Die Frage, ob P und NP verschieden sind, wird als eine der bedeutendsten offenen Fragen der theoretischen Informatik, ja sogar der Mathematik, angesehen. P und NP sind jedoch nur zwei Beispiele von Komplexitätsklassen. Andere Klassen ergeben sich unter anderem bei der Untersuchung der des benötigten Speicherplatzes, der effizienten Parallelisierbarkeit von Problemen, der Lösbarkeit durch zufallsgesteuerte Algorithmen, und der approximativen Lösbarkeit von Problemen.

Voraussetzungen: Keine

Empfohlene Vorkenntnisse: Grundlagen der Theoretischen Informatik

Arbeitsaufwand: 270 Stunden

Der Arbeitsaufwand ergibt sich wie folgt: 15 Wochen zu je 6 SWS entsprechen in Summe 90 Stunden Anwesenheit. Für die Nachbereitung der Vorlesung und die Vor- und Nachbereitung

der Übungen sind etwa 6 Stunden pro Woche, in Summe 90 Stunden, erforderlich. Etwa 90 Stunden sind für die Klausurvorbereitung vorgesehen.

Prüfungsform: mündlich, 30 Minuten

Literatur:

[1] Papadimitroiu, C. "Computational Complexity ", Addison-Wesley, 1993
[2] "Computational Complexity: A Modern Approach", Cambridge University Press, 2009
[3] Wegener, Ingo "Komplexitätstheorie: Grenzen der Effizienz von Algorithmen", Springer Verlag, 2003
[4] Kozen, Dexter "Theory of Computation", Springer, 2006

2.28 148219: Kryptanalytische Werkzeuge

Nummer:	148219
Lehrform:	Vorlesungen und Übungen
Verantwortlicher:	Prof. Dr.-Ing. Tim Güneysu
Dozenten:	Prof. Dr.-Ing. Tim Güneysu
	Dr.-Ing. Tobias Schneider
	Dr.-Ing. Alexander Wild
Sprache:	Deutsch
SWS:	4
Leistungspunkte:	5
Angeboten im:	

Ziele: Die Teilnehmer kennen wesentliche praktische Komponenten und Werkzeuge der Kryptanalyse. Sie haben einen umfangreichen Überblick über Algorithmen und Techniken, die heutzutage zur Analyse bestehender Systeme einge-setzt werden. Des Weiteren können sie nicht nur Kenntnisse über die neuesten Analyseverfahren, sondern auch die Grenzen bezüglich Rechen,- Speicher- und finanzieller Aufwand anwenden. Mit dem vermittelten Wissen, ist es den Teilnehmern zum Ende des Kurses möglich, unterschiedliche Methoden zur Analyse von bestehenden Systemen erfolgreich anzuwenden sowie die Limitierungen von Sicherheitsanalysen einschätzen zu können.

Inhalt: Diese Veranstaltung stellt Methoden und Werkzeuge zur Analyse von Sicherheitsmechanismen und kryptographischen Systemen vor. Der praktische Bezug der Methoden steht hierbei im Vordergrund, sodass die Ansätze insbesondere bezüglich verschiedener Rechnerplattformen verglichen werden. Hauptbestandteile der Veranstaltung sind dabei Möglichkeiten der effizienten Passwort- und Schlüsselsuche bzw. -extraktion für kryptographische Systeme. Hierbei werden Lösungen und Werkzeuge für Rechenplattformen wie PC-Clustern, Grafikkarten sowie Spezialhardware vorgestellt.

Im Rahmen der Vorlesung werden neben wöchentlichen vorlesungsbegleitenden Übungen drei integrierte praktische Workshops angeboten, um die vermittelten Lerninhalte mittels selbstentwickelten kryptanalytischen Werkzeugen weiter zu vertiefen.

Die Themen dieser Workshops sind:

1) Werkzeuge zur Geheimnisidentifikation: Entwicklung effizienter Passwortsuchstrategien

2) Werkzeuge zur symmetrische Kryptanalyse: Durchführung eines Time-Memory Trade-Off Angriffs auf Blockchiffren

3) Werkzeuge zur asymmetrische Kryptanalyse: Angriff auf ein Elliptisches Kurven Kryptosystem mittels des verteilten Pollard-Rho Algorithmus

Voraussetzungen: keine

Empfohlene Vorkenntnisse: Grundkenntnisse der Kryptographie, über Rechnerarchitekturen und der Computerprogrammierung

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 2 Stunden pro Woche, in Summe 28 Stunden, erforderlich. Für drei begleitende Projekte sind je etwa 15 Stunden vorgesehen. Etwa 21 Stunden verblieben für die Klausurvorbereitung.

Prüfungsform: schriftlich, 120 Minuten

2.29 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.

2.30 148203: Kryptographie auf programmierbarer Hardware

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

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

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

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

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

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

Voraussetzungen: keine

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

1) Grundlagen der Kryptographie und Datensicherheit
2) Computerarchitektur
3) Basiswissen Digitaltechnik

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

1) Schaltungsentwurf mit VHDL

2) Parallele Algorithmen und deren Programmierung

3) Implementierung kryptographischer Systeme

Arbeitsaufwand: 150 Stunden

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

Prüfungsform: schriftlich, 120 Minuten

2.31 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

2.32 150343: Kryptographische Protokolle

Nummer: 150343
Lehrform: Vorlesungen und Übungen
Verantwortlicher: Prof. Dr. Eike Kiltz
Dozent: Prof. Dr. Eike Kiltz
Sprache: Deutsch
SWS: 4
Leistungspunkte: 5
Angeboten im: Sommersemester

Ziele: Die Studierenden verstehen die erweiterten mathematischen Methoden und Verfahren, auf denen moderne kryptographische Protokolle beruhen. Die Teilnehmer sind zur Analyse und dem Design aktueller und zukünftiger kryptographischer Methoden befähigt.

Inhalt: Die Vorlesung beschäftigt sich mit erweiterten kryptographischen Protokollen und deren Anwendungen. Hierbei wird insbesondere Wert auf eine formale Sicherheitsanalyse im Sinne von beweisbarer Sicherheit gelegt.

- Themenübersicht:
  - Identity-based Encryption
  - Digital Signatures
  - Secret sharing
  - Threshold Cryptography
  - Secure Multiparty Computation

Voraussetzungen: keine

Empfohlene Vorkenntnisse: Inhalte des Moduls Kryptographie

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

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

2.34 310508: Machine Learning: Supervised Methods

Nummer: 310508
Lehrform: Vorlesungen und Übungen
Verantwortlicher: Prof. Dr. Tobias Glasmachers
Dozent: Prof. Dr. Tobias Glasmachers
Sprache: Englisch
SWS: 4
Leistungspunkte: 6
Angeboten im: Sommersemester

Ziele: This lecture will cover a contemporary spectrum of supervised learning methods. All lecture material will be in English.

The course will use the inverted classroom concept. Students work through the relevant lecture material at home. The material is then consolidated in a 4 hours/week practical session.

Inhalt: The field of machine learning constitutes a modern approach to artificial intelligence. It is situated in between computer science, neuroscience, statistics, and robotics, with applications ranging all over science and engineering, medicine, economics, etc. Machine learning algorithms automate the process of learning, thus allowing prediction and decision making machines to improve with experience.

Voraussetzungen: The course requires basic mathematical tools from linear algebra, calculus, and probability theory. More advanced mathematical material will be introduced as needed. The practical sessions involve programming exercises in Python. Participants need basic programming experience. They are expected to bring their own devices (laptops).

Empfohlene Vorkenntnisse: None

Arbeitsaufwand: 180 Stunden

Der Arbeitsaufwand berechnet sich wie folgt: Die Kontaktzeit in der Vorlesung und der Übung beträgt 56 Stunden (14 * 28 Stunden + 14 * 28 Stunden). Die Vorbereitung der Übung, wozu auch implizit die Nachbereitung der Vorlesung besteht, wird mit 62 Stunden veranschlagt. Die Prüfungsvorbereitung wird mit 62 Stunden veranschlagt.

Prüfungsform: schriftlich, 90 Minuten

2.35 142363: Master-Forschungspraktikum Human-Centred Security

Nummer:	142363
Lehrform:	Praktikum
Medienform:	Tafelanschrieb
Verantwortlicher:	Prof. Dr. Martina Angela Sasse
Dozenten:	Prof. Dr. Martina Angela Sasse M. A. Annalina Buckmann
Sprache:	Deutsch
SWS:	3
Leistungspunkte:	3
Angeboten im:	Wintersemester und Sommersemester

Ziele: Die Veranstaltung vermittelt praktische Kenntnisse über Forschungsdesign, -Methoden und Auswertungsverfahren im Bereich 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

2.36 142061: Master-Forschungspraktikum Usable Security und Privacy

Nummer:	142061
Lehrform:	Praktikum
Medienform:	rechnerbasierte Präsentation
Verantwortlicher:	Prof. Dr. Markus Dürmuth
Dozenten:	Prof. Dr. Markus Dürmuth Dr.-Ing. Maximilian Golla Prof. Dr. Martina Angela Sasse
Sprache:	Deutsch
SWS:	3
Leistungspunkte:	3
Angeboten im:	Wintersemester und Sommersemester

Ziele: Diese Veranstaltung vermittelt praktische Kenntnisse in den Forschungsgebieten Usabel Security und Privacy. Die Studierenden werden in die Lage versetzt, eigenständig Studien hinsichtlich der Usability von sicherheits- und privacyrelevanten Systemen durchzuführen, auszuwerten und kritisch zu hinterfragen.

Inhalt: Neben der notwendigen theoretischen Methodik, die in großen Teilen von der Vorlesung Usable Security and Privacy abgedeckt wird, werden in diesem Kurs vor allem die praktischen Aspekte der Usable Security und Privacy Forschung besprochen. Zunächst werden die Grundlagen über die Durchführung von Nutzerstudien aus der Vorlesung wiederholt und mit Hilfe von aktuellen Beispielen aus dem Bereich Usable Security und Privavcy Forschung vertieft. In Gruppen werden anschließend, unter Anleitung, eigene Nutzerstudien geplant, getestet, durchgeführt, ausgewertet, verschriftlicht und bewertet. Zum Abschluss des Praktikums werden die Ergebnisse in einer Präsentation vorgestellt und in einer kurzen wissenschaftlichen Arbeit verschriftlicht und diskutiert. Alle Studierenden durchlaufen in Ihrer Gruppe dabei die folgenden Schritte:

- Entwurf von Forschungsfragen, Interview-Protokollen, Fragebögen etc.
- Entwicklung von Prototypen
- Pilotversuch und anschließende Überarbeitung
- Kurzvortrag zum aktuellen Fortschritt
- Durchführung der Studie mit mindestens 10 Personen (oder mehr, falls online)
- Abschlussvortrag
- Schreiben einer englischsprachigen 4-seitigen wissenschaftlichen Arbeit
- Erstellen eines kritischen Reviews (500 Wörter)

Voraussetzungen: Keine

Empfohlene Vorkenntnisse:

- Usable Security and Privacy
- Allgemeine Kenntnisse der IT-Sicherheit

Arbeitsaufwand: 90 Stunden

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

Prüfungsform: Praktikum, studienbegleitend

2.37 142364: Master-Praktikum (Laborstudien) Human-Centred Security

Nummer:	142364
Lehrform:	Praktikum
Medienform:	Videoübertragung Folien Moodle
Verantwortlicher:	Prof. Dr. Martina Angela Sasse
Dozenten:	Prof. Dr. Martina Angela Sasse M. Sc. Yasemin Acar M. Sc. Jana Böttner
Sprache:	Deutsch
SWS:	3
Leistungspunkte:	3
Angeboten im:	Wintersemester und Sommersemester

Ziele: Die Veranstaltung vermittelt theoretische und praktische Kenntnisse über Forschungsmethoden im Bereich usable Security mit einem besonderen Schwerpunkt auf Laborstudien. Es werden theoretische Kenntnisse vermittelt, auf deren Grundlage die Studierenden selbstständig eine Laborstudie planen und umsetzen und auf diese Weise praktische Kenntnisse erwerben sollen.

Inhalt: Wir entwickeln gemeinsam Laborstudien mit dem Ziel, Fragestellungen zum Thema Human-Centred Security zu untersuchen. Laborstudien können z. B. eingesetzt werden, um herauszufinden, ob Nutzer die Herausforderung, ein System sicher und korrekt zu bedienen bewältigen können. Eine technisch sichere Lösung hilft nur dann, wenn die Nutzer nicht selbst unbewusst oder bewusst durch ihr Verhalten das System kompromittieren. Wir lernen die Grundlagen, wie z. B. menschliches Verhalten in der IT-Sicherheit untersucht werden kann. Was ist notwendig, um Fragestellungen in der HCS beantworten zu können: Von der Hypothesenbildung über die Planung des Forschungsdesigns bis hin zur Auswertung werden wir uns Schritt für Schritt in Richtung einer laborfertigen Studie vortasten. Die theoretischen Inhalte werden direkt in die Praxis übersetzt, indem unter Anleitung in Kleingruppen eine eigene Laborstudie geplant und durchgeführt wird. Dadurch werden unterschiedliche Methoden kennengelernt, die im Rahmen von Laborstudien zum Einsatz kommen können.

Für die Anmeldung bitte eine E-Mail an jana.boettner@ruhr-uni-bochum.de senden.
Veranstaltungstermine:

- 29.10.2021 von 10:00 bis 11.00 Uhr im ID 04/413
- 26.11.2021 von 10:00 bis 17:00 Uhr
- 10.12.2021 von 10:00 bis 17:00 Uhr
- 21.01.2022 von 10:00 bis 17:00 Uhr

Voraussetzungen: Keine

Empfohlene Vorkenntnisse: Keine

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.

2.38 142027: Master-Praktikum ARM Processors for Embedded Cryptography

Nummer:	142027
Lehrform:	Praktikum
Medienform:	Moodle
Verantwortlicher:	Prof. Dr.-Ing. Tim Güneysu
Dozenten:	Prof. Dr.-Ing. Tim Güneysu Dr.-Ing. Max Hoffmann
Sprache:	Deutsch
SWS:	3
Leistungspunkte:	3
Gruppengröße:	max. 50
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: 90 Stunden

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

Prüfungsform: Praktikum, studienbegleitend

Voraussetzungen für die Vergabe von Kreditpunkten: Bestehen des finalen Projektes.

2.39 143143: Master-Praktikum Embedded Linux

Nummer: 143143
Lehrform: Praktikum
Verantwortlicher: Prof. Dr.-Ing. Michael Hübner
Dozent: Prof. Dr.-Ing. Michael Hübner
Sprache: Deutsch
SWS: 3
Leistungspunkte: 3
Angeboten im:

Ziele: Die Studierenden haben die Grundlagen von Embedded Linux kennen gelernt und können auch dieses Betriebssystem praktisch auf einen FPGA integrieren. Besonders der Umgang mit späteren Erweiterungen der Hardware und die Anbindung an den Prozessor bietet eine hervorragende Möglichkeit Kenntnisse dieser modernen Entwurfsmethodik zu erwerben.

Inhalt: Das Master-Praktikum Embedded Linux zeigt die Funktion und praktische Realisierung von embedded Linux auf einem FPGA Board. Hierbei werden alle Schritte durchlaufen, bis ein Kernel auf einem FPGA integriert ist und über ein Terminal angesprochen werden kann. Im Folgenden werden Hardwareerweiterungen für das Prozessorsystem entwickelt und Treiber für diese Erweiterungen programmiert.

Voraussetzungen: keine

Empfohlene Vorkenntnisse: Programmieren in C

Arbeitsaufwand: 90 Stunden

Der Arbeitsaufwand berechnet sich wie folgt: 8 Wochen zu je 3 SWS entsprechen 24 Stunden Anwesenheit. Für die Vorbereitung und Ausarbeitung werden jeweils 8 Stunden, insgesamt 64 Stunden veranschlagt. Es verbleiben 2 Stunden für die sonstige Organisation der Praktikumsdurchführung.

Prüfungsform: Praktikum, studienbegleitend

2.40 142020: Master-Praktikum Embedded Smartcard Microcontrollers

Nummer: 142020
Lehrform: Praktikum
Medienform: Folien
rechnerbasierte Präsentation
Verantwortlicher: Prof. Dr.-Ing. Christof Paar
Dozenten: Prof. Dr.-Ing. Christof Paar
Dr.-Ing. Max Hoffmann
Sprache: Deutsch
SWS: 3
Leistungspunkte: 3
Angeboten im:

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

Inhalt: In diesem Praktikum werden zwei Themengebiete erarbeitet. Zunächst erlernen die Teilnehmer des Praktikums Grundlagen über CISC und RISC Mikrocontroller. Bereits nach dem ersten Praktikumstermin sind die Studenten in der Lage kleine Programme in Assembler für die Atmel RISC AVR Architektur zu entwickeln. Während der folgenden Termine werden die Kenntnisse bezüglich der AVR Architektur vertieft. Darüber hinaus müssen die Praktikumsteilnehmer immer komplexere Programme als Hausaufgaben schreiben. Im zweiten Teil des Praktikums erlernen die Studenten den Umgang mit Smartcards und den zugehörigen Industriestandards. Der Standard ISO 7816 und die zugehörigen T=0/T=1 Übertragungsprotokolle werden vorgestellt. Jeder Student erhält Zugriff auf eine Smartcard mit einem Atmel AVR Mikrocontroller, sowie einem Kartenschreib- bzw. -lesegerät. Dieser implementiert zwei vorgegebene Blockchiffren (die jährlich wechseln) in Assembler, und muss diese auf der Smartcard unter realistischen Bedingungen lauffähig bekommen. Beispiele für Algorithmen sind AES, 3DES und lightweight Chiffren. Um die Motivation der Praktikumsteilnehmer zu erhöhen, werden die effizientesten Implementierungen mit einer Urkunde und einem Buchpreis belohnt.

Voraussetzungen: keine

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

Arbeitsaufwand: 90 Stunden

Der Arbeitsaufwand berechnet sich wie folgt: 6 Termine zu je 3 Stunden entsprechen 18 Stunden Anwesenheit. Für die Vorbereitung werden 18 Stunden (3 Stunden je Termin für 6

Termine), für die Bearbeitung der Übungszettel 9 Stunden (3 Stunden je Übungszettel für drei Übungszettel), für die Implementierung der Chiffre in Gruppenarbeit 40 Stunden und für die Vorbereitung auf das Prüfungsgespräch 5 Stunden veranschlagt.

Prüfungsform: Praktikum, studienbegleitend

2.41 142181: Master-Praktikum Entwurf integrierter Digitalschaltungen mit VHDL

Nummer: 142181
Lehrform: Praktikum
Verantwortlicher: Prof. Dr.-Ing. Michael Hübner
Dozent: M. Sc. Keyvan Shahin
Sprache: Deutsch
SWS: 3
Leistungspunkte: 3
Angeboten im:

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

Inhalt: Der Entwurf von VLSI-Schaltungen ist aufgrund der großen Anzahl von Bauelementen nur zu beherrschen, wenn man Hardware-Beschreibungssprachen wie VHDL für den Entwurf einsetzt. Eine ganze Reihe von Eigenschaften macht VHDL für den Mikroelektronik-Entwurf so interessant. Dazu zählen: VHDL ist nicht technologiespezifisch, es ist das geeignete Medium zum Austausch zwischen Entwerfern untereinander und mit dem Chiphersteller, VHDL unterstützt Hierarchie und Top-down- und Bottom-up-Entwurfsmethoden, es unterstützt ferner Verhaltens-, Struktur- und Datenfluss-Beschreibung, es ist ein IEEE-Standard, Testmuster können mit derselben Sprache generiert werden u.a.m.

Das Praktikum findet basierend auf aktuellen FPGA-Architekturen und mit aktueller Synthesesoftware statt. Nach einem einführenden Tutorial in die Entwicklungsumgebung “Vivado” von Xilinx, werden Schaltwerke und Schaltnetze für unterschiedlichste Aufgaben erstellt, simuliert und auf echter Hardware getestet.

Voraussetzungen: keine

Empfohlene Vorkenntnisse: Wünschenswert sind Kenntnisse des Faches “Integrierte Digitalschaltungen”

Arbeitsaufwand: 90 Stunden

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

Prüfungsform: Praktikum, studienbegleitend

Literatur:

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

2.42 142022: Master-Praktikum Java-Card

Nummer: 142022
Lehrform: Praktikum
Verantwortlicher: Prof. Dr.-Ing. Christof Paar
Dozenten: Prof. Dr.-Ing. Christof Paar
Dr.-Ing. Pawel Swierczynski
Sprache: Deutsch
SWS: 3
Leistungspunkte: 3
Angeboten im:

Ziele: Nach dem erfolgreichen Abschluss des Praktikums versteht der Studierende folgende Zusammenhänge:

- Authentifizierung (Challenge/Response Protokoll) gegenüber dem Kartenmanager der Java Card zur Verwaltung des Systems
- Erstellen von kryptographischen Java Card Applets
- Aufruf der Funktionen des Hardware Co-Prozessors
- Übertragung und Installation von Java Card Applets
- Ansteuern von Java Card Applets
- Verarbeiten eingehender APDUs sowie Erstellen ausgehender APDUs, usw.
- Umgang mit dem Übertragungsprotokoll in C++

Inhalt: In diesem Praktikum erlernen die Teilnehmer den sicheren Umgang mit Java Cards. Diese Smart Cards können spezielle Java Applets auf einem Mikrocontroller ausführen. Die Programmiersprache Java kommt in Millionen von eingebetteten Geräten zum Einsatz, z.B. in SIM Karten, die den GSM Standard implementieren. Dabei stellen Java Cards die kleinste aller bekannten Java Plattformen dar. Diese führen einen reduzierten Satz von Java Code aus und bieten eine Schnittstelle zu sicheren kryptographischen Co-Prozessoren (DES, 3-DES, AES, usw.), welche den Ver- und Entschlüsselungsprozess erheblich beschleunigen. Der erste Teil des Praktikums erläutert Grundlagen über die Funktionsweise und den Aufbau von Java Cards. Anschließend wird den Teilnehmern vermittelt, wie die Authentifizierung (SCP01/SCP02) gegenüber einer Java Card funktioniert. In einem dritten Schritt erlernen die Teilnehmer das Erstellen von Java Card Applets, deren Konvertierung und Upload auf die Java Card selbst. Anschließend wird den Teilnehmern vermittelt wie die eigenes erstellten Java Applikationen gemäß dem GlobalPlatform Standard selektiert und ausgefuehrt werden können. Ein Großteil der Programmierarbeiten erfolgt dabei in C++. In einem Abschlussprojekt werden einige sicherheitsrelevante Anwendungen - inklusive einer Blockchiffre - für die Java Card implementiert.

Voraussetzungen: keine

Empfohlene Vorkenntnisse: keine

Arbeitsaufwand: 90 Stunden

Der Arbeitsaufwand berechnet sich wie folgt: 6 Termine zu je 3 Stunden entsprechen 18 Stunden Anwesenheit. Für die Vorbereitung werden 18 Stunden (3 Stunden je Termin für 6 Termine), für die Bearbeitung der Übungszettel 9 Stunden (3 Stunden je Übungszettel für drei Übungszettel), für die Implementierung der Chiffre in Gruppenarbeit 40 Stunden und für die Vorbereitung auf das Prüfungsgespräch 5 Stunden veranschlagt.

Prüfungsform: Praktikum, studienbegleitend

2.43 142221: Master-Praktikum Machine Learning and Security

Nummer:	142221
Lehrform:	Praktikum
Medienform:	e-learning Moodle rechnerbasierte Präsentation
Verantwortlicher:	Prof. Dr. Thorsten Holz
Dozenten:	Prof. Dr. Thorsten Holz M. Sc. Thorsten Eisenhofer M. Sc. Joel Frank
Sprache:	Deutsch
SWS:	3
Leistungspunkte:	3
Gruppengröße:	max. 20
Angeboten im:	Wintersemester und Sommersemester

Ziele: The students obtain a profound understanding of modern machine learning techniques and their applications in the area of computer security. More specifically, the participants are proficient in corresponding ML algorithms and can analyze complex problems on their own. The students can design and implement ML algorithms on their own and learn how to perform research in the intersection of machine learning and computer security.

Inhalt: The practical course provides an introduction to various machine learning (ML) techniques and their application in computer security. In six exercises, we plan to cover the following topics:

- Linear and logistic regression
- Clustering algorithms (e.g., k-nearest neighbors) and classification algorithms
- Unsupervised Learning
- Support vector machines (SVM)
- Deep Learning
- Adversarial Machine Learning

We will cover different applications of these techniques in areas such as:

- Spam classification
- Malware clustering
- Deep fake detection

The course will cover tools such as NumPy and PyTorch. We expect that students perform their own research and investigation to solve the exercises.

Voraussetzungen: Keine

Empfohlene Vorkenntnisse: Basic knowledge of Python is strongly recommended. The course Deep Learning offered by Prof. Fischer covers some recommended basics.

Arbeitsaufwand: 90 Stunden

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

Prüfungsform: Praktikum, studienbegleitend

Voraussetzungen für die Vergabe von Kreditpunkten: Successful completion of six exercise sheets.

2.44 142246: Master-Praktikum Programmanalyse

Nummer:	142246
Lehrform:	Praktikum
Medienform:	Moodle rechnerbasierte Präsentation
Verantwortlicher:	Prof. Dr. Thorsten Holz
Dozent:	Prof. Dr. Thorsten Holz
Sprache:	Deutsch
SWS:	3
Leistungspunkte:	3
Gruppengröße:	max. 20
Angeboten im:	

Ziele: Die Studierenden haben ein tiefergehendes Verständnis der Funktionsweise aktueller Schadsoftware und kennen Techniken zur Analyse und zur Abwehr. Im Besonderen beherrschen die Teilnehmer entsprechende Techniken des Reverse-Engineerings und können selbstständig komplexe Schadsoftware analysieren. Die Studierenden können eigenständig Tools entwerfen und implementieren. Darüber hinaus lernen die Studierenden, eigenständig Recherche im Bereich Schadsoftware durchzuführen.

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

Unter anderem werden die folgenden Themen behandelt:

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

Voraussetzungen: keine

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

Arbeitsaufwand: 90 Stunden

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

Prüfungsform: Praktikum, studienbegleitend

Voraussetzungen für die Vergabe von Kreditpunkten: Erfolgreiche Bearbeitung von sechs von sieben Aufgabenblättern.

2.45 150584: Master-Praktikum SAGE in der Kryptographie

Nummer: 150584
Lehrform: Praktikum
Verantwortlicher: Prof. Dr. Gregor Leander
Dozent: Prof. Dr. Gregor Leander
Sprache: Deutsch
SWS: 2
Leistungspunkte: 3
Angeboten im:

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

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

Voraussetzungen: keine

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

Arbeitsaufwand: 90 Stunden

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

Prüfungsform: Praktikum, studienbegleitend

2.46 142249: Master-Praktikum Schwachstellenanalyse

Nummer:	142249
Lehrform:	Praktikum
Medienform:	e-learning Moodle rechnerbasierte Präsentation
Verantwortlicher:	Prof. Dr. Thorsten Holz
Dozenten:	Prof. Dr. Thorsten Holz Dr. Ali Abbasi M. Sc. Tobias Scharnowski
Sprache:	Deutsch
SWS:	3
Leistungspunkte:	3
Gruppengröße:	max. 20
Angeboten im:	Sommersemester

Ziele: Die Studierenden haben ein tiefergehendes Verständnis der Funktionsweise aktueller Angriffsmethoden und Schutzmechanismen. Sie kennen verschiedene Techniken aus diesen beiden Bereichen und können diese umsetzen. Im Besonderen beherrschen die Teilnehmer entsprechende Techniken des Reverse-Engineerings und können selbstständig komplexe Schwachstellen analysieren. Die Studierenden können eigenständig Tools entwerfen und implementieren. Darüber hinaus lernen die Studierenden, eigenständig Recherche im Bereich Softwaresicherheit durchzuführen.

Inhalt: Das Praktikum ist eine Vertiefung der Inhalte, die in der Vorlesung "Betriebssystemsicherheit" vorgestellt wurden. Die Teilnehmer sollen in Gruppen von zwei Studierenden insgesamt sieben unterschiedliche Beispiele von Softwareschwachstellen mit steigendem Schwierigkeitsgrad analysieren und implementieren. Die zu analysierenden Schwachstellentypen werden jeweils an einem eigenen Präsenztermin besprochen und entsprechende Analyse- und Exploitingmethoden vorgestellt. In vielen Fällen wird darüber hinaus Eigenrecherche und Autodidaktik zur Lösung der Aufgaben notwendig sein. Unter anderem werden die folgenden Themen behandelt:

- Verschiedene Klassen von Angriffen
- Softwareschwachstellen für ARM und Intel
- Umgehung von Schutzmechanismen wie DEP und ASLR
- Reverse Engineering von proprietären Binärdateien

Voraussetzungen: keine

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

Arbeitsaufwand: 90 Stunden

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

Prüfungsform: Praktikum, studienbegleitend

Voraussetzungen für die Vergabe von Kreditpunkten: Erfolgreiche Bearbeitung von sechs von sieben Aufgabenblättern.

2.47 142248: Master-Praktikum Security Appliances

Nummer:	142248
Lehrform:	Praktikum
Medienform:	e-learning Handouts rechnerbasierte Präsentation
Verantwortlicher:	Prof. Dr. Jörg Schwenk
Dozenten:	Prof. Dr. Jörg Schwenk Dr.-Ing. Dennis Felsch Dr.-Ing. Christian Mainka Dr.-Ing. Paul Rösler
Sprache:	Deutsch
SWS:	3
Leistungspunkte:	3
Angeboten im:	

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

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

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

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

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

Das Praktikum wird mit Unterstützung der Utimaco GmbH durchgeführt.

Voraussetzungen: keine

Empfohlene Vorkenntnisse: Programmierkenntnisse in C und Java

Studenten die bereits die Bachelorversion dieses Praktikums bestanden haben, dürfen leider nicht teilnehmen.

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

2.48 142023: Master-Praktikum Seitenkanalangriffe

Nummer:	142023
Lehrform:	Praktikum
Verantwortlicher:	Prof. Dr. Amir Moradi
Dozenten:	Prof. Dr. Amir Moradi M. Sc. David Knichel M. Sc. Nicolai Müller
Sprache:	Deutsch
SWS:	3
Leistungspunkte:	3
Gruppengröße:	max. 8
Angeboten im:	Wintersemester

Ziele:

- Verstehen und durchführen von Seitenkanalmessungen einer Mikrocontroller-Plattform unter Nutzung von Oszilloskopen
- Praktische Analyse und Beurteilung der Seitenkanalsicherheit von Kryptographischen Implementierungen
- Aufbereitung und Präsentation von Ergebnissen einer Seitenkanalanlyse
- Verstehen und Implementieren von Seitenkanalgegenmaßnahmen auf einer Microcontroller-Plattform und erkennen von platformbedingten Problemen hierbei

Inhalt:

1. Einführung & Statistik
2. Pattern Matching & SPA
3. Messungen & CPA auf Software
4. Leakage Detection & CPA auf Hardware
5. CPA mit Alignment
6. Boolean Masking der AES S-Box
7. Abschlussprojekt

Das Master-Praktikum Seitenkanalangriffe vermittelt die nötigen praktischen Fähigkeiten kryptographische Implementierungen auf ihre Seitenkanalsicherheit hin zu untersuchen und entsprechende Gegenmaßnahmen zu implementieren. Das Praktikum wurde vollständig überarbeitet und wird ab dem Wintersemester 18/19 auf einer aktuellen ARM M0-Platform durchgeführt. Die Studenten müssen selbständig Messungen durchführen und Gegenmaßnahmen auf dem Mikrocontroller implementieren.

Voraussetzungen: keine

Empfohlene Vorkenntnisse: Die Vorlesungen “Implementierung kryptografischer Verfahren” und “Physical Attacks and Countermeasures” vermittelt nützliches Vorwissen, dieses wird jedoch nicht vorausgesetzt.

Arbeitsaufwand: 90 Stunden

Der Arbeitsaufwand berechnet sich wie folgt: 6 Termine zu je 3 Stunden entsprechen 18 Stunden Anwesenheit. Für die Vorbereitung werden 18 Stunden (3 Stunden je Termin für 6 Termine), für die Bearbeitung der Übungszettel 9 Stunden (3 Stunden je Übungszettel für drei Übungszettel), für die Implementierung der Chiffre in Gruppenarbeit 40 Stunden und für die Vorbereitung auf das Prüfungsgespräch 5 Stunden veranschlagt.

Prüfungsform: Praktikum, studienbegleitend

Voraussetzungen für die Vergabe von Kreditpunkten: Es werden 5 Versuche durchgeführt die vor Ort durchgeführt und zu Hause ausgewertet werden. Es ist eine kurze Zusammenfassung der Ergebnisse und ggf. Programmcode einzureichen. Für das Abschlussprojekt muss eine Gegenmaßnahme implementiert und getestet werden. Zum Bestehen müssen alle Versuche und das Abschlussprojekt erfolgreich abgeschlossen werden.

2.49 150000: Master-Praktikum Smart Contracts

Nummer: 150000
Lehrform: Praktikum
Medienform: Moodle
rechnerbasierte Präsentation
Verantwortlicher: Jun. Prof. Dr. Sebastian Faust
Dozent: Jun. Prof. Dr. Sebastian Faust
Sprache: Deutsch
SWS: 3
Leistungspunkte: 3
Angeboten im:

Ziele: Die Studierenden erarbeiten den praktischen Umgang mit kryptographischen Währungen. Die Teilnehmer des Praktikums lernen die Funktionsweise der kryptographischen Währungen Bitcoin und Ethereum kennen und lernen wie man sicher mit diesen Währungen bezahlt. Dazu gehört neben dem Senden und Empfangen von Transaktionen vor allem die Programmierung von Smart Contracts.

Inhalt: Im Rahmen dieses Praktikums sollen die kryptographischen Währungen Bitcoin und Ethereum vorgestellt werden. Dabei werden zunächst die Grundlagen von Blockchain Technologie vermittelt um die zugrundeliegenden kryptographischen Bausteine zu verstehen. Darauf aufbauend sollen die Studierenden sich mit der Funktionsweise der dezentralen Netzwerke und des Minings vertraut machen. Anschließend wird die Programmierung von Smart Contracts und deren Integration in bestehende Software ausführlich betrachtet. Auch die Sicherheit von Smart Contract Programmierung soll dabei genauer untersucht werden. Die Programmierung dieser Contracts in Ethereum wird mit der Programmiersprache Solidity erfolgen.

Voraussetzungen: keine

Empfohlene Vorkenntnisse: Grundkenntnisse im Bereich Blockchain Technologien wie z.B. aus der Vorlesung Financial Cryptography/Cryptocurrencies sind wünschenswert, aber nicht erforderlich. Erfahrungen in Programmierung mit JavaScript sind hilfreich.

Arbeitsaufwand: 90 Stunden

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

Prüfungsform: Praktikum, studienbegleitend

2.50 142250: Master-Praktikum TLS Implementierung

Nummer:	142250
Lehrform:	Praktikum
Medienform:	Moodle rechnerbasierte Präsentation
Verantwortlicher:	Prof. Dr. Jörg Schwenk
Dozenten:	Prof. Dr. Jörg Schwenk M. Sc. Matthias Gierlings M. Sc. Marcel Maehren M. Sc. Robert Merget
Sprache:	Deutsch
SWS:	3
Leistungspunkte:	3
Angeboten im:	Wintersemester

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

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

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

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

Empfohlene Vorkenntnisse:

- Erfolgreicher Abschluss der Lehrveranstaltung Netzsicherheit 2
- Programmierkenntnisse in Java

Arbeitsaufwand: 90 Stunden

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

Prüfungsform: Praktikum, studienbegleitend

2.51 142026: Master-Praktikum Wireless Physical Layer Security

Nummer:	142026
Lehrform:	Praktikum
Medienform:	Folien rechnerbasierte Präsentation
Verantwortlicher:	Prof. Dr.-Ing. Christof Paar
Dozent:	Dr.-Ing. Christian Zenger
Sprache:	Deutsch
SWS:	3
Leistungspunkte:	3
Angeboten im:	Wintersemester und Sommersemester

Ziele: Dieses Praktikum verfolgt im Wesentlichen die folgenden drei Lernziele: Erstens kennen die Teilnehmer des Praktikums eine Software Defined Radio (SDR) Architektur und deren Programmierung mit ‚GNU Radio'. Zweitens wird der Umgang mit SDRs, sowie Wissen über die entsprechenden Funkstandards und potenzielle Angriffe beherrscht. Drittens sind die Implementierungs- und Evaluierungsaspekte von modernen Funkkanal-basierten Sicherheitsarchitekturen bekannt. Python wird als Programmiersprachen verwendet. Über die technischen Ziele hinaus wird die Arbeitsfähigkeit in Gruppen erlernt, sowie Projektplanung und Zeitmanagement vermittelt.

Inhalt: In diesem Praktikum werden zwei Themengebiete erarbeitet. Zunächst erlernen die Teilnehmer des Praktikums Grundlagen über Software Defined Radios (SDRs). Bereits nach dem ersten Praktikumstermin sind die Studenten in der Lage passive Lauschangriffe mit GNU Radio für die RTL-SDR Architektur zu entwickeln. Während der folgenden Termine werden die Kenntnisse bezüglich der SDR Architektur und Funkstandards vertieft. Darüber hinaus müssen die Praktikumsteilnehmer immer komplexere Programme als Hausaufgaben schreiben. Im zweiten Teil des Praktikums erlernen die Studenten den Umgang mit Funkkanal-basierten Sicherheitsarchitekturen. Der Kanal-basierte Schlüsselgenerierung und Kanal-basiertes Fingerprinting werden vorgestellt. Die Studenten werden anschließend in Gruppen à drei Personen aufgeteilt. Jede Gruppe erhält ein Messsetup basierend aus drei Raspberry Pis, Funkmodulen und einer Messsoftware, sowie eine Virtuelle Maschine mit vorkonfiguriertem Evaluationsframework. Jede Gruppe implementiert eine vorgegebene Kanal-basierte Sicherheitsarchitektur (jährliche eine andere) in Python, und muss diese im Evaluationsframework unter realistischen Bedingungen lauffähig bekommen. Um die Motivation der Praktikumsteilnehmer zu erhöhen, werden die effizientesten Implementierungen mit Buchpreisen belohnt.

Voraussetzungen: keine

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

Arbeitsaufwand: 90 Stunden

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

Prüfungsform: Praktikum, studienbegleitend

2.52 142243: Master-Praktikum zur Hackertechnik

Nummer:	142243
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:	3
Angeboten im:	Wintersemester und Sommersemester

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

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

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

- Cross Site Scripting (XSS)
- Cross Site Request Forgery (CSRF)
- Session Hijacking
- Session Fixation
- SQL Injection (SQLi)
- Local/Remote File Inclusion (LFI/RFI)
- Path Traversal
- Remote Code Execution (RCE)
- Logical Flaws
- Information Leakage

- Insufficient Authorization

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

Voraussetzungen: keine

Empfohlene Vorkenntnisse:

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

Arbeitsaufwand: 90 Stunden

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

2.53 142040: Master-Projekt DSP

Nummer:	142040
Lehrform:	Projekt
Medienform:	Videoübertragung Folien Moodle
Verantwortlicher:	Prof. Dr.-Ing. Dorothea Kolossa
Dozenten:	Prof. Dr.-Ing. Dorothea Kolossa M. Sc. Wentao Yu
Sprache:	Deutsch
SWS:	3
Leistungspunkte:	3
Gruppengröße:	8
Angeboten im:	Sommersemester

Ziele: Neben den Strategien und Methoden zur Bewältigung der technischen Herausforderungen beherrschen die Studierenden gleichzeitig die Organisation von größeren Projekten in Teams, Methoden der Projektplanung, strukturierte Softwareentwicklung incl. Spezifikation und Validierung.

Inhalt: Dieses Projekt wird aufgrund der aktuell implementierten Corona-Notfallregelungen an der RUB im Sommersemester 2021 als reine Online-Veranstaltung angeboten. Deshalb werden sämtliche Besprechungs- und Vortragstermine mit Hilfe von Videokonferenzen durchgeführt. Die genauen Details hierzu werden beim Vorbesprechungstermin am Freitag, den 16. April 2021 von 10:00 Uhr bis 11:00 Uhr mit den Teilnehmern besprochen.

Eine Anmeldung zu der Veranstaltung im Vorfeld ist zwingend erforderlich!

Senden Sie hierzu bitte bis spätestens zum 14. April 2021, 23:59 Uhr von ihrer RUB-Emailadresse eine Mail mit dem Betreff “Anmeldung Kurs 142040 SoSe2021” an wentao.yu[at]rub.de (mit benedikt.boenninghoff[at]rub.de im CC). Alle weiteren Informationen, insbesondere die Zugangsdaten zum Zugangsdaten zum Moodle-Kurs und zum Videokonferenzsystem werden den zugelassenen Teilnehmer*innen am 15. April 2021 per E-Mail übermittelt.

In dieser Veranstaltung implementieren Master-Studierende in Teams von 2 bis zu 10 Mitgliedern über den Verlauf eines Semesters hinweg ein größeres Data-Science-Projekt in Python. Ziel ist die Entwicklung und Erprobung eines maschinellen Lernverfahrens für die multimodale Autorprofilerstellung.

Interessierte Studierende sollten sich selbstständig in einer Gruppe von 2-10 Mitgliedern organisieren (als Unterstützung finden Sie im Moodle der Veranstaltung auch ein Diskussionsforum).

Im Lauf des Semesters wird dann eine wöchentliche Online-Besprechung (mit Teilnahmepflicht) stattfinden, um die Fortschritte der jeweiligen Woche zu besprechen und die jeweils nächsten Schritte zu planen. Das Labor wird abgeschlossen durch eine Einreichung der Lösung (via GitHub), einen schriftlichen Bericht (Latex), in dem der eingereichte Code und die Ergebisse dokumentiert sind, und durch einen Online-Abschlussvortrag.

Voraussetzungen: keine

Empfohlene Vorkenntnisse:

- Grundkenntnisse digitale Signalverarbeitung und maschinelles Lernen
- sichere Beherrschung mindestens einer Programmiersprache
- idealerweise Erfahrungen mit der Programmierung in Python

Arbeitsaufwand: 90 Stunden

Der Arbeitsaufwand berechnet sich wie folgt: 14 Wochen zu je 3 SWS ergeben 42 Stunden Anwesenheit. Es verbleiben 48 Stunden zur Vor- und Nachbereitung.

Prüfungsform: Projektarbeit, studienbegleitend

Voraussetzungen für die Vergabe von Kreditpunkten: Aktive und zielgerichtete Beteiligung an allen digitalen Laborterminen, Abgabe des Quellcodes, Bericht, Abschlussvortrag

2.54 142024: Master-Projekt Eingebettete Sicherheit

Nummer: 142024
Lehrform: Projekt
Verantwortlicher: Prof. Dr.-Ing. Christof Paar
Dozent: Prof. Dr.-Ing. Christof Paar
Sprache: Deutsch
SWS: 3
Leistungspunkte: 3
Angeboten im: Wintersemester und Sommersemester

Ziele: Die Studierenden beherrschen verschiedene Techniken, die für die Forschung im Bereich der modernen eingebetten Sicherheit relevant sind.

Inhalt: Es wird eine Projektaufgabe unter Anleitung bearbeitet. Themen sind hierbei Fragestellungen bezüglich Implementierungstechniken, physikalischer Angriffe oder Sicherheits-Design.

Voraussetzungen: keine

Empfohlene Vorkenntnisse: Grundkenntnisse der angewandten Kryptographie, sowie Grundkenntniss der Software- oder Hardware-Implementierung

Arbeitsaufwand: 90 Stunden

Der Arbeitsaufwand berecnet sich wie folgt: 14 Wochen zu je 3 SWS ergeben 42 Stunden Anwesenheit. Es verbleiben 48 Stunden zur Vor- und Nachbereitung.

Prüfungsform: Projektarbeit, studienbegleitend

2.55 142241: Master-Projekt Netz- und Datensicherheit

Nummer:	142241
Lehrform:	Projekt
Verantwortlicher:	Prof. Dr. Jörg Schwenk
Dozenten:	Prof. Dr. Jörg Schwenk M. Sc. Robert Merget
Sprache:	Deutsch
SWS:	3
Leistungspunkte:	3
Angeboten im:	Wintersemester und Sommersemester

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

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

Zur Klarstellung: Es ist nicht vorgesehen, dass sie verschiedene Themenblöcke nacheinander abarbeiten (wie es bei den Grundlagenpraktika der Fall ist), sondern sie werden nur ein Thema im Praktikum vertiefen. Die Bearbeitung kann je nach Vereinbarung mit dem Betreuer semesterbegleitend, oder zusammengefasst als Block (insgesamt ca. 90h) erfolgen; je nach Verfügbarkeit des Betreuers ist auch eine Bearbeitung in den Semesterferien grundsätzlich möglich.

Die Themenliste stellt nur Themenstichworte dar; die detaillierte Besprechung, und endgültige Definition des Themas erfolgt zusammen mit dem jeweiligen Fachbetreuer.

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

Voraussetzungen: keine

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

Arbeitsaufwand: 90 Stunden

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

Prüfungsform: Projektarbeit, studienbegleitend

2.56 142184: Master-Projekt Virtual Prototyping von Embedded Systems

Nummer:	142184
Lehrform:	Projekt
Verantwortlicher:	Prof. Dr.-Ing. Michael Hübner
Dozenten:	Prof. Dr.-Ing. Michael Hübner M. Sc. Florian Fricke M. Sc. Tomás Grimm Prof. Dr.-Ing. Michael Hübner
Sprache:	Englisch
SWS:	3
Leistungspunkte:	3
Angeboten im:	

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

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

1. Introduction to Virtual Prototyping basic concepts, systems, tools, languages, etc.
2. SystemC basic course

This course is based on the IEEE SystemC TLM2.0 library, and aims to provide the basic understanding about the SystemC language and the Transaction-Level Modeling (TLM) standard.:

- Introduction to Transaction-Level Modeling
- Working with Loosely-Timed models
- Working with Approximately-Timed models
- Debugging methods

3. Tensilica Processor design framework

The objective is to provide hands-on knowledge about the Cadence Xtensa Xplorer framework to design custom processor architectures based on the Xtensa LX series processors:

- Tensilica Processor Architecture
- Programming Cores with Tensilica Instruction Extensions
- Developing Software for Xtensa Processors

- Xtensa Debug and Trace
- Support for Emulation

4. Virtual System Platform

This course uses the Cadence Virtual System Platform to integrate hardware and software platforms using fast processor models. The simulation platforms are based on SystemC/TLM2.0 models and allows for fast hardware emulation and early software development.

- Tool overview
- Selected examples
- Custom models design and analysis
- Fast processor models integration
- System-on-Chip ESL design

Voraussetzungen: none

Empfohlene Vorkenntnisse: Basic programming knowledge in C/C++

Arbeitsaufwand: 90 Stunden

Der Arbeitsaufwand berechnet sich wie folgt: Das Praktikum findet als Blockveranstaltung statt mit 4 1/2 Tagen Dauer, entsprechend 36 Stunden Anwesenheit. Für die Vorbereitung werden 18 Stunden (9 Stunden je Abschnitt), für die Ausarbeitung des Praktikumsberichts 36 Stunden (18 Stunden je Abschnitt) veranschlagt.

Prüfungsform: Projektarbeit, studienbegleitend

2.57 143242: Master-Seminar Aktuelle Themen der IT-Sicherheit

Nummer: 143242
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 wissenschaftlichen Papern 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 Seminar zum Thema "Aktuelle Themen der IT-Sicherheit" an, der Fokus liegt auf den Bereichen Softwaresicherheit, Netzwerksicherheit, Privacy, Reverse Engineering und ähnlichen Themen aus dem Bereich der systemnahen IT-Sicherheit. Dazu sollen die Studierenden selbständig ein komplexes Themengebiet bearbeiten und eine Ausarbeitung sowie einen Vortrag zu diesem Thema verfassen. Die Ausarbeitung hat einen Umfang von etwa 20 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.

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 20 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.

2.58 143250: Master-Seminar Applied Privacy and Anonymity

Nummer:	143250
Lehrform:	Seminar
Medienform:	Folien
	Moodle
Verantwortlicher:	Prof. Dr. Thorsten Holz
Dozenten:	Dr. Martin Degeling
	Dr.-Ing. Katharina Kohls
Sprache:	Englisch
SWS:	3
Leistungspunkte:	3
Gruppengröße:	5-10 Studierende
Angeboten im:	

Ziele: Die Studierenden lernen Methoden des forschungsnahen Lernens kennen und sind in der Lage eigenständig ein vorab definiertes Themengebiet anhand wissenschaftlicher Texte zu erarbeiten. Dies beinhaltet einerseits die Vorbereitung eines Vortrags zur Vorstellung der erarbeiteten Inhalte sowie das anleiten einer Diskussion in der Gruppe zu den Forschungsarbeiten. Andererseits werden durch die schriftliche Ausarbeitung das wissenschaftliche Schreiben und die Zusammenfassung komplexer Themengebiete geübt.

Inhalt: Das Seminar umfasst aktuelle wissenschaftliche Arbeiten zu Anonymität und Privatheit im Internet mit realistischen Anwendungsfällen. Beispiele dafür sind offene Angriffsvektoren auf das Anonymitätssystem Tor und die jeweiligen Sicherheitsrisiken für Nutzer:innen, oder Methoden zur Handhabung von Privatsphäreeinstellungen in Onlineanwendungen. Durch die Kombination wissenschaftlicher und realer Problemstellungen ist es möglich, existierende Herausforderungen besser zu verstehen und langfristige Lösungen für zukünftige Systeme zu erarbeiten.

Voraussetzungen: Keine

Empfohlene Vorkenntnisse: Keine

Arbeitsaufwand: 90 Stunden

Der Arbeitsaufwand berechnet sich wie folgt: Die Seminarvorträge finden kontinulierlich während des Semesters statt. Es besteht Anwesenheitspflicht. Für die Vorbereitung und Diskussion der Vorträge sind durchschnittlich (je nach Teilnehmerzahl) 20 Stunden anzusetzen. Die Erarbeitung des Seminarthemas findet eigenverantwortlich mit Unterstützung der betreuenden Mitarbeiter:innen 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

2.59 143245: Master-Seminar Digitale Signaturen

Nummer: 143245
Lehrform: Seminar
Medienform: rechnerbasierte Präsentation
Verantwortlicher: Prof. Dr. Jörg Schwenk
Dozent: Dr.-Ing. Sebastian Lauer
Sprache: Deutsch
SWS: 3
Leistungspunkte: 3
Angeboten im:

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

Inhalt: Im Rahmen dieses Seminars wird ein solides Grundverständnis für die Konstruktion von sicheren digitalen Signaturverfahren vermittelt. Folgende Themen werden behandelt und vertieft:

- Einmalsignaturverfahren
- Chamäleon-Hashfunktionen
- RSA-basierte Signaturverfahren
- Pairing-basierte Signaturverfahren
- Blind-Signatures
- Verifiable Random Functions
- Group-Signatures
- Identity-based Signatures

Voraussetzungen: keine

Empfohlene Vorkenntnisse:

- Grundlegende Kenntnisse der Kryptographie
- Vorlesung “Kryptographie” von Prof. Dr. Alexander May

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

2.60 143021: Master-Seminar Embedded Security

Nummer: 143021
Lehrform: Seminar
Medienform: rechnerbasierte Präsentation
Verantwortlicher: Prof. Dr.-Ing. Christof Paar
Dozent: Prof. Dr.-Ing. Christof Paar
Sprache: 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. Die Teilnehmer bescherrschen den akademischen Umgang mit technischer und wissenschaftlicher Literatur und kennen Stand der Forschung.

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

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

Voraussetzungen: keine

Arbeitsaufwand: 90 Stunden

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

Prüfungsform: Seminarbeitrag, studienbegleitend

2.61 143248: Master-Seminar Human Centered Security and Privacy

Nummer:	143248
Lehrform:	Seminar
Medienform:	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

2.62 150538: Master-Seminar Kryptographie

Nummer: 150538
Lehrform: Seminar
Medienform: rechnerbasierte Präsentation
Verantwortlicher: Prof. Dr. Eike Kiltz
Dozent: Prof. Dr. Eike Kiltz
Sprache: Deutsch
SWS: 3
Leistungspunkte: 3
Angeboten im:

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

Inhalt: Aktuelle Forschungsarbeiten der wichtigsten Kryptographie-Konferenzen.

Voraussetzungen: keine

Empfohlene Vorkenntnisse: Inhalte des Moduls “Kryptographie”

Arbeitsaufwand: 90 Stunden

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

Prüfungsform: Seminarbeitrag, studienbegleitend

2.63 150999: Master-Seminar Kryptologie

Nummer: 150999
Lehrform: Seminar
Medienform: rechnerbasierte Präsentation
Verantwortlicher: Prof. Dr. Gregor Leander
Dozent: Prof. Dr. Gregor Leander
Sprache: Deutsch
SWS: 3
Leistungspunkte: 3
Angeboten im:

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

Inhalt: Aktuelle Forschungsarbeiten der wichtigsten Kryptographie-Konferenzen.

Voraussetzungen: keine

Empfohlene Vorkenntnisse: Inhalte des Moduls “Kryptographie”

Arbeitsaufwand: 90 Stunden

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

Prüfungsform: Seminarbeitrag, studienbegleitend

2.64 143240: Master-Seminar Netz- und Datensicherheit

Nummer:	143240
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, Anwesenheitspflicht

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.

Prüfungsform: Seminarbeitrag, studienbegleitend

2.65 150534: Master-Seminar on Secure Multiparty Computation

Nummer: 150534
Lehrform: Seminar
Verantwortlicher: Jun. Prof. Dr. Sebastian Faust
Dozent: Jun. Prof. Dr. Sebastian Faust
Sprache: Deutsch
SWS: 3
Leistungspunkte: 3
Angeboten im:

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

Inhalt: ichere Multiparty Computation (MPC) Protokolle sind ein faszinierender Baustein der modernen Kryptographie. Ein MPC Protokoll erlaubt es Parteien sicher und verteilt beliebige Funktionen zu berechnen selbst wenn die Teilnehmer des Protokolls beliebig von den Vorschriften des Protokolls abweichen können. In dem Seminar werden wir grundsätzliche Konzepte und Protokolle aus dem Gebiet der MPC durchnehmen. Das Seminar orientiert sich dazu unter anderem an folgendem Buch:

Secure Multiparty Computation and Secret Sharing, Ronald Cramer, Ivan Bjerre Damgård, Jesper Buus Nielsen

Voraussichtliche Themen sind:

- Verifiable secret sharing
- Definition von MPC Protokollen (passiv/aktiv)
- OT Protokolle
- Informationstheoretisch sichere MPC Protokolle
- Effizientere MPC Protokolle gegen PPT Angreifer
- Sichere 2-Parteien Protokolle mit Yao Garbled Circuits

Voraussetzungen: keine

Empfohlene Vorkenntnisse: Kenntnisse aus der Vorlesung Kryptographie notwendig. Kenntnisse aus Spezialvorlesungen aus der Kryptographie sind von Vorteil.

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

2.66 141211: Master-Seminar Physical Layer Security Journal Club

Nummer:	141211
Lehrform:	Seminar
Medienform:	rechnerbasierte Präsentation Tafelanschrieb
Verantwortlicher:	Prof. Dr.-Ing. Aydin Sezgin
Dozent:	Prof. Dr.-Ing. Aydin Sezgin
Sprache:	Englisch
SWS:	2
Leistungspunkte:	3
Gruppengröße:	2
Angeboten im:	Sommersemester

Ziele: The students understand the concepts of physical-layer measures to achieve secrecy. They know how to extract the core concept and contribution from a scientific manuscript. They are able to present and introduce in an oral talk the tools and methods utilized in the respective manuscript.

Inhalt: The students are exposed to scientific manuscript within the area of physcical-layer security, which includes but is not limited to

- private information retrieval
- secure distributed computation
- wiretapping
- key generation
- authentification
- oblivious transfer
- instance hiding

They study and review the corresponding scientific paper, extract the

- essense of the problem
- importance of the problem studied
- the methodology on how the problem is tackled
- the solution
- and the insights.

Finally, they preu00adpau00adre a short sciu00adenu00adtiu00adfic talk and give a presentation to fellow stuu00addents.

Voraussetzungen: Keine

Empfohlene Vorkenntnisse:

- System Theory
- Communications Engineering
- Stochastic Signals

Arbeitsaufwand: 90 Stunden

Der Arbeitsaufwand ergibt sich wie folgt: 14 Wochen zu je 2 SWS entsprechen in Summe 28 Stunden Anwesenheit. Für die Nachbereitung der Vorlesung und die Vor- und Nachbereitung der Übungen sind etwa 3 Stunden pro Woche, in Summe 42 Stunden, erforderlich. Etwa 20 Stunden sind für die Prüfungsvorbereitung vorgesehen.

Prüfungsform: Seminarbeitrag, studienbegleitend

Voraussetzungen für die Vergabe von Kreditpunkten: Erfolgreicher Abschlussbericht

2.67 143251: Master-Seminar Privacy and Security in Mobile Operating Systems

Nummer:	143251
Lehrform:	Seminar
Medienform:	Moodle
Verantwortlicher:	Prof. Dr. Thorsten Holz
Dozenten:	Dr. Martin Degeling
	Dr. Veelasha Moonsamy
Sprache:	Englisch
SWS:	3
Leistungspunkte:	3
Angeboten im:	Wintersemester und Sommersemester

Ziele: Using methods of research-oriented learning, students will gain the ability to work on a pre-defined scientific topic based on state-of-the-art research publications. This includes a presentation of the contents as well as a discussion of critical aspects of one paper and students will be asked to provide summaries for each session. The seminar concludes with each student providing an outline for an open research question and study methodology that will be reviewed by other course participants.

Inhalt: The seminar combines current scientific work in the area of security and privacy of mobile devices with realistic problem statements. Examples of this are attacks and counter-measures as well as an overview of how the mobile device ecosystem (e.g. Android and iOS) work. The seminar will cover technical aspects as well as the perspective of human-computer-interaction with respect to mobile security and privacy.

Voraussetzungen: None

Arbeitsaufwand: 90 Stunden

Der Arbeitsaufwand berechnet sich wie folgt: 14 Wochen zu je 3 Stunden entsprechen 42 Stunden Anwesenheit. Für die Vorbereitung und Ausarbeitung des Seminars werden 48 Stunden veranschlagt.

2.68 150540: Master-Seminar Research oriented Cryptography

Nummer: 150540
Lehrform: Seminar
Medienform: rechnerbasierte Präsentation
Verantwortlicher: Jun. Prof. Dr. Sebastian Faust
Dozent: Jun. Prof. Dr. Sebastian Faust
Sprache: Deutsch
SWS: 3
Leistungspunkte: 3
Angeboten im:

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

Inhalt: Wissenschaftliches Arbeiten in der Kryptographie

In einer kleinen Gruppe (max. 5 Teilnehmer) wird gemeinsam unter Anleitung des Dozenten eine aktuelle wissenschaftliche Arbeit/en aus dem Gebiet der Kryptographie zunächst betrachtet. Aufbauend auf den Erkenntnissen der Betrachtung werden Verbesserungen erarbeitet, die in Form einer neuen Arbeit aufgeschrieben werden. Das genaue Thema wird in der Vorbesprechung festgelegt.

Voraussetzungen: keine

Empfohlene Vorkenntnisse: mindestens „Kryptographie I+II“, vorteilhaft aber nicht notwendig: Besuch von Spezialvorlesungen der Kryptographie (Kryptographische Protokolle, Randomness in Cryptography, Digitale Signaturen, etc.). Inhaltlich sollen grundlegende wissenschaftliche Arbeitsweisen (Stichworte: Definitionen, Beweise, etc.) bekannt sein.

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

2.69 143244: Master-Seminar Security and Privacy of Wireless Networks and Mobile Devices

Nummer:	143244
Lehrform:	Seminar
Medienform:	Folien language skills training rechnerbasierte Präsentation Tafelanschrieb
Verantwortlicher:	Prof. Dr. Markus Dürmuth
Dozent:	Prof. Dr. Markus Dürmuth
Sprache:	Deutsch
SWS:	3
Leistungspunkte:	3
Angeboten im:	

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 Sicherheit in existierenden und entstehenden Funknetzwerken ebenso wie zur Sicherheit mobiler Geräte bereitgestellt. Thematische Schwerpunkte sind u.a. Sicherheitsaspekte in Ad-hoc Netzen, Location Privacy und Tracking, Authentifizierung auf mobilen Geräten etc. Dazu sollen die Studierenden anhand von Forschungsarbeiten selbständig ein Themengebiet erarbeiten und eine Ausarbeitung sowie einen Vortrag zu diesem Thema verfassen. Die Ausarbeitung hat einen Umfang von etwa 18 Seiten. Der Vortrag soll etwa 20 Minuten dauern, anschließend erfolgt eine Diskussion.

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: Praktikum, studienbegleitend

2.70 141034: Master-Seminar Security Engineering

Nummer:	141034
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

2.71 148212: Master-Seminar Sichere Hardware

Nummer: 148212
Lehrform: Seminar
Medienform: rechnerbasierte Präsentation
Verantwortlicher: Prof. Dr.-Ing. Tim Güneysu
Dozent: Prof. Dr.-Ing. Tim Güneysu
Sprache: Deutsch
SWS: 3
Leistungspunkte: 3
Angeboten im:

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

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

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

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

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

Voraussetzungen: keine

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

Arbeitsaufwand: 90 Stunden

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

Prüfungsform: Seminarbeitrag, studienbegleitend

2.72 143022: Master-Seminar Smart Technologies for the Internet of Things

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

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

Inhalt: Im Sommersemester 2018 werden in diesem Seminar lehrstuhlübergreifend Aspekte des modernen "Internet der Dinge" beleuchtet. Unter anderem befassen sich die Themen mit den Bereichen: Protokolle und Systemanforderungen bezüglich Geschwindigkeit, Stromverbrauch und Sicherheit. Die Themen werden am Vorbesprechungstermin an die Teilnehmer vergeben.

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

Voraussetzungen: keine

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

Arbeitsaufwand: 90 Stunden

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

Prüfungsform: Seminarbeitrag, studienbegleitend

2.73 143163: Master-Seminar Sprach- und Mustererkennung

Nummer:	143163
Lehrform:	Seminar
Medienform:	Videoübertragung e-learning Moodle
Verantwortlicher:	Prof. Dr.-Ing. Dorothea Kolossa
Dozenten:	Prof. Dr.-Ing. Dorothea Kolossa M. Sc. Jan Freiwald
Sprache:	Deutsch
SWS:	3
Leistungspunkte:	3
Gruppengröße:	max. 8
Angeboten im:	Sommersemester

Ziele: Die Studierenden lernen in diesem Seminar, eigenständig englischsprachige Fachliteratur zu einem bestimmten Themengebiet zu verstehen und bekommen einen Einblick in aktuelle Forschungsthemen. Sie können über fachliche Themen im Bereich der kognitiven Signalverarbeitung ziel- und anlassbezogen angemessen diskutieren. Ferner werden Grundsätze und Regeln der Präsentation von wissenschaftlichen Vorträgen im Allgemeinen besprochen und eingeübt. Die Studierenden sind in der Lage, einen wissenschaftlichen Vortrag so zu entwerfen und zu halten, dass er als gut gegliedert, verständlich und interessant empfunden wird.

Inhalt: In dieser Veranstaltung werden aktuelle Forschungsthemen aus der Sprach- und Mustererkennung tiefergehend betrachtet und in studentischen Vorträgen vorgestellt. Die Studierenden erarbeiten im Lauf eines Semesters einen 15-minütigen Vortrag zu einem jeweils aktuellen Zeitschriften- oder Konferenzartikel und stellen diesen im Seminar vor. Mögliche Themen sind beispielsweise die robuste und audiovisuelle Spracherkennung, Angriffe auf Deep-Learning-basierte Systeme und die erklärbare künstliche Intelligenz.

Voraussetzungen: keine

Empfohlene Vorkenntnisse: Kenntnisse in den Bereichen Digitale Signalverarbeitung, Maschinelles Lernen, Wahrscheinlichkeitsrechnung

Arbeitsaufwand: 90 Stunden

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

Prüfungsform: Seminarbeitrag, studienbegleitend

Voraussetzungen für die Vergabe von Kreditpunkten: Teilnahme an allen Seminarterminen, eigener Probe- und Hauptvortrag

2.74 143291: Master-Seminar Usable Security and Privacy Research

Nummer:	143291
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: 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

Inhalt: 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.

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

2.75 140002: Master-Startup ITS

Nummer:	140002
Lehrform:	Beliebig
Verantwortlicher:	Prof. Dr.-Ing. Tim Güneysu
Dozenten:	Prof. Dr.-Ing. Tim Güneysu
	M. Sc. Marvin Staib
	M. Sc. Jan Philipp Thoma
Sprache:	Deutsch
SWS:	2
Leistungspunkte:	1
Angeboten im:	Wintersemester und Sommersemester

Ziele: Erleichterung des Einstiegs in das Studium; Vernetzung der Studierenden untereinander; Einsicht in Berufsbilder, Karrieremöglichkeiten etc.

Inhalt: Studienbegleitende Informationen, Exkursionen, Vorträge etc.

Hinweise für WiSe 21/22: Das Master-Startup wird im kommenden Semester vorraussichtlich in Präsenz stattfinden und der Raum rechtzeitig bekannt gegeben.

Moodle Kurs: https://moodle.ruhr-uni-bochum.de/course/view.php?id=41302

Vorläufiges Programm:

13.10.2021 - Intro LS Security Engineering / Organisation
20.10.2021 - Edgeless Systems
27.10.2021 - T-Systems I
03.11.2021 - MPI
10.11.2021 - Kasper & Oswald GmbH
17.11.2021 - Rohde & Schwarz Cybersecurity
24.11.2021 - Volkswagen Infotainment
01.12.2021 - Studienberatung
08.12.2021 - T-Systems II
15.12.2021 - TÜV-IT
22.12.2021 - PHYSEC
12.01.2022 - VDV-ETS
19.01.2022 - VMRay GmbH
26.01.2022 - G-Data
02.02.2022 - TBA

Arbeitsaufwand: 30 Stunden

Der Arbeitsaufwand ergibt sich aus der Präsenzzeit bei den einzelnen Veranstaltungsterminen.

Prüfungsform: None, studienbegleitend

2.76 144102: Masterarbeit ITS

Nummer: 144102
Lehrform: Masterarbeit
Verantwortlicher: Studiendekan ITS
Dozent: Hochschullehrer der Fakultät ET/IT
Sprache: Deutsch
Leistungspunkte: 30
Angeboten im: Wintersemester und Sommersemester

Ziele: Die Teilnehmer sind mit Arbeitsmethoden der wissenschafltichen Forschung und der Projektorganisation vertraut. Ihre fortgeschrittenen Kenntisse und Arbeitsergebnisse können sie verständlich präsentieren.

Inhalt: Weitgehend eigenständige Lösung einer wissenschaftlichen Aufgabe unter Anleitung. Präsentation der eigenen Ergebnisse der Masterarbeit.

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: 900 Stunden

6 Monate Vollzeittätigkeit

Prüfungsform: Abschlussarbeit, studienbegleitend

2.77 141027: Menschliches Verhalten in der IT Sicherheit

Nummer:	141027
Lehrform:	Vorlesungen und Übungen
Medienform:	Videoübertragung e-learning Folien Internet Moodle
Verantwortlicher:	Prof. Dr. Martina Angela Sasse
Dozenten:	Prof. Dr. Martina Angela Sasse M. Sc. Maximilian Peiffer
Sprache:	Deutsch
SWS:	4
Leistungspunkte:	5
Angeboten im:	Sommersemester

Ziele: *WICHTIG: Bitte melden Sie sich selbstständig im Moodle-Kurs (der Link befindet sich oben rechts) an. Das Passwort lautet SS2021-cfq.*

Dieser Kurs richtet sich an Studierende im Master.

Ziel der Veranstaltung "Menschliches Verhalten in der IT Sicherheit" ist, dass die Studierenden verstehen lernen, welche Faktoren Einfluss auf das Sicherheitsverhalten bei Angestellten in Unternehmen und Konsumenten im Alltag nehmen, und welche Möglichkeiten bestehen, dieses zu beeinflussen und verändern.

Außerdem soll vermittelt werden, warum bestehende Ansätze des Information Security Management Systems (auch nach ISO 27000) in der Praxis oft nicht funktionieren, und wie wir sie erweitern bzw. anpassen sollten.

Inhalt: In der Veranstaltung "Menschliches Verhalten in der IT Sicherheit" sollen unter anderem folgende Themen behandelt werden:

- Risikowahrnehmung und -verständnis
- Traditionelle Ansätze des Information Security Management Systems (Grundkonzepte der ISO 27000 Standard Familie)
- Wirtschaftliche Lösungen für Sicherheit in Unternehmen: Integration von Risikomanagement in Produktions- und Leistungsziele und Geschäftsabläufe in Unternehmen
- Kosten-Nutzen-Analyse von Sicherheitsmaßnahmen (analytische Methoden)
- Evaluation der Kosten und Nutzen von Sicherheitsmaßnahmen (empirische Methoden)
- Unternehmenswerte und –normen und ihr Einfluss auf Sicherheitsverhalten, Einfluss von Verhalten durch andere (bspw. Kollegen und Unternehmensführung)
- Effektive Kommunikation von Risiken und Sicherheitsmaßnahmen innerhalb des Unternehmens

- Effektive Kommunikation von Risiken und Sicherheitsmaßnahmen für Kunden, Konsumenten und Bürger
- Was ist Change Management? Konzepte, Methoden und Anwendung auf Planung, Evaluation und Anpassung von IT Sicherheitsverhalten

Die finale Note ist die Klausurnote. Zusätzlich können Bonuspunkte (10%) erworben werden. Weitere Informationen zur Bewertung werden in der ersten Veranstaltung bekanntgegeben.

Voraussetzungen: Keine

Empfohlene Vorkenntnisse: Für ITS-Studierende wird der vorherige Besuch der Vorlesung "Einführung in die Usable Security and Privacy" von Prof. Dr. M. Angela Sasse und Prof. Dr. Markus Dürmuth empfohlen.

Nicht ITS-Studierende sollten über Grundlagenkenntnisse der IT Sicherheit verfügen. Hierzu bietet sich je nach Fachbereich die Vorlesung "IT Sicherheit für Geisteswissenschaftler" von Prof. Dr. Markus Dürmuth an.

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

2.78 141252: Message-Level Security

Nummer:	141252
Lehrform:	Vorlesungen und Übungen
Medienform:	Moodle rechnerbasierte Präsentation
Verantwortlicher:	Prof. Dr. Jörg Schwenk
Dozenten:	Dr.-Ing. Christian Mainka M. Sc. Louis Jannett Dr.-Ing. Vladislav Mladenov M. Sc. Simon Rohlmann
Sprache:	Deutsch
SWS:	4
Leistungspunkte:	5
Gruppengröße:	ca. 50
Angeboten im:	Wintersemester

Ziele: Studierende verfügen nach erfolgreichem Abschluss der Vorlesung über ein umfassendes Verständnis der Sicherheit der folgenden Technologien: Datenformate im Web, Authentifizierungs- und Autorisierungsprotokollen und Dokumentenformaten. Durch die praxisnahe Arbeit im Rahmen der Übungen bauen die Studenten ihre Recherche-Fähigkeiten aus und erlernen weiterhin den sicheren Umgang mit verschiedenen Penetrationswerkzeugen. Am Ende der Vorlesung sind die Studenten in der Lage systematisch umfassende Sicherheitsanalysen sowie praktische Angriffe auf die behandelten Technologien selbständig durchzuführen. Weiterhin sind die Studenten in der Lage das erlernte Wissen auf andere Technologien zu übertragen und komplexere Angriffsmöglichkeiten selbst durch kreatives Denken zu finden und auszunutzen.

Inhalt: Die Vorlesung behandelt das Thema *Message-Level Security*. Anders als bei SSL/TLS, welches einen sicheren Transportkanal aufbaut, geht es bei Message-Level Security darum, Nachrichten - wie beispielsweise HTTP Requests – auf Nachrichtenebene zu schützen. Hierbei kommt es auf die korrekte Verwendung von kryptographischen Verfahren als auch eine sichere Bereitstellung von API-Schnittstellen an.

Im Rahmen der Vorlesung werden verschiedene Verfahren von Message-Level Security beleuchtet.

Die Vorlesung behandelt dabei verschiedene Verfahren von Message-Level Security:

- **JSON** ist eine universelle Datenbeschreibungssprache, die unter anderem von jedem modernen Browser unterstützt wird. Mithilfe von JSON-Signature und JSON-Encryption JSON Nachrichten direkt geschützt werden. Doch reicht das aus oder können diese Sicherheitsmechanismen umgangen werden?

- **OAuth** ist eine sehr weit verbreitete Technologie zum Delegieren von Berechtigungen und wird heutzutage von allen großen Webseiten wie Facebook, Google, Twitter, Github, uvm. eingesetzt. Die Vorlesung erklärt tief-gehende Details und gängige Fehler/Angriffe, die bei der Verwendung von OAuth entstehen können.

- **OpenID Connect** ist eine Erweiterung für OAuth, um Benutzer auf Webseiten mithilfe eines Drittanbieters zu authentifizieren (Single Sign-On, z.B. Google Login). OpenID

Connect hat sich in den letzten Jahren zum defacto Standard für Web-Logins über Drittanbieter etabliert. In der Vorlesung wird detailliert erklärt, was die Unterschiede zu OAuth sind und welche Angriffe auf OpenID Connect möglich sind.

- **SAML** steht für *Security Assertion Markup Language* und ist ein Single Sign-On Standard, der weitere Verbreitung in Business-Szenerien findet. Allerdings existieren zahlreiche Angriffe von Identitätsdiebstahl bis hin zu *Remote Code Execution*.
- **PDF** ist das vermutlich am weitesten verbreitetste universelle Dokumentenaustauschformat. In der Vorlesung werden die Sicherheitseigenschaften von PDFs beleuchtet. Insbesondere werden hierbei digitale Signaturen untersucht, welche z.B. bei Verträgen zum Einsatz kommen. Wird es uns gelingen, signierte Dokumente zu fälschen?

Den Studenten wird ein tief-gehendes Verständnis der Systeme vermittelt. Zu allen untersuchten Systemen werden Angriffe vorgestellt, die sowohl aus der akademischen Welt als auch aus der Pentesting-Community stammen. Die Übungen bieten die Möglichkeit, das erlernte Wissen praktisch auszuprobieren. Hierzu erhalten die Studenten eine virtuelle Maschine.

Empfohlene Vorkenntnisse:

- Grundkenntnisse HTTP, HTML und Kryptographie
- Grundkenntnisse der englischen Sprache, da dies die Sprache von Foliensatz, Übungsaufgaben und Virtuelle Maschine sind

Arbeitsaufwand: 150 Stunden

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

Prüfungsform: schriftlich, 120 Minuten

Beschreibung der Prüfungsleistung:

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

2.79 141032: Methoden der Benutzer-Authentisierung

Nummer:	141032
Lehrform:	Vorlesungen und Übungen
Medienform:	Moodle
Verantwortlicher:	Prof. Dr. Markus Dürmuth
Dozenten:	Prof. Dr. Markus Dürmuth
	M. Sc. Leona Lassak
	M. Sc. Philipp Markert
Sprache:	Deutsch
SWS:	3
Leistungspunkte:	4
Angeboten im:	Wintersemester

Ziele: Die Studierenden haben einen umfassenden Überblick über die verschiedenen Möglichkeiten zur Benutzerauthentifizierung.

Inhalt: Diese Vorlesung behandelt verschiedene Formen der Benutzerauthentisierung. Ausgehend von Passwörtern, die wir wohl alle täglich benutzen, wollen wir untersuchen wie genau Passwörter eingesetzt werden, warum sie nicht besonders sicher sind, und wie wir ihre Sicherheit erhöhen können. Weiter betrachten wir zahlreiche Alternativen, wie Einmal-Passwörter, grafische Passwörter (z. B. Android-Entsperrmuster oder Windows 10), Sicherheitstokens (z. B. YubiKey oder RSA SecurID), oder biometrische Verfahren (z. B. Gesichtserkennung oder basierend auf Gehirnaktivitat), und lernen deren Funktionsweise sowie Vor- und Nachteile kennen.

Voraussetzungen: keine

Empfohlene Vorkenntnisse: Solide Programmierkenntnisse

Arbeitsaufwand: 120 Stunden

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

Prüfungsform: schriftlich, 120 Minuten

2.80 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

2.81 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

2.82 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.

2.83 141105: Nichttechnische Veranstaltungen

Nummer: 141105
Lehrform: Beliebig
Verantwortlicher: Dekan
Dozent: Dozenten der RUB
Sprache: Deutsch
Angeboten im: Wintersemester und Sommersemester

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

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

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

Aus anderen Bereichen gibt es folgende Kurse:

Der Ingenieur als Manager

Methods and Instruments of Technology Management

Projektmanagemant für Ingenieure

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

Coaching für Existenzgründer

Unsicherheitserfahrung und Bewältigungsstrategien im unternehmerischen Kontext – Simulationsbasierte Lernansätze

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

0em

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

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

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

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

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

Voraussetzungen: entsprechend den Angaben zu der gewählten Veranstaltungen

Empfohlene Vorkenntnisse: entsprechend den Angaben zu der gewählten Veranstaltungen

Prüfungsform: None, studienbegleitend

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

2.84 141028: Physical Attacks and Countermeasures

Nummer:	141028
Lehrform:	Vorlesungen und Übungen
Medienform:	Moodle rechnerbasierte Präsentation
Verantwortlicher:	Prof. Dr. Amir Moradi
Dozenten:	Prof. Dr. Amir Moradi M. Sc. David Knichel M. Sc. Nicolai Müller
Sprache:	Englisch
SWS:	4
Leistungspunkte:	5
Gruppengröße:	10-15
Angeboten im:	Sommersemester

Ziele: Die Studierenden

- verstehen wie und warum physikalische Angriffe funktionieren.
- sind in der Lage Messdaten anhand der erlernten Methoden auszuwerten und die Sicherheit einer Implementierung zu bewerten.
- erkennen die Gefahr von physikalischen Angriffen für Implementierungen von kryptographischen Algorithmen.
- kennen mögliche Gegenmaßnahmen und wissen wie diese anzuwenden sind, um ein System gegen physikalische Angriffe zu schützen.

Inhalt: Moderne kryptographische Algorithmen bieten ausreichend Schutz gegen die bekannten mathematischen und kryptanalytischen Angriffe. In der Praxis werden diese Algorithmen für sicherheits-kritische Anwendungen auf verschiedenen Plattformen implementiert. Dies geschieht sowohl als Programmcode (Software) als auch mit logischen Elementen/Schaltungen (Hardware). Der physikalische Zugang zu kryptographischen Implementierungen (z.B., eine Smartcard oder ein Smartphone, welche zum Bezahlen benutzt werden), in welchen der geheime Schlüssel eingebettet ist, hat zur Entstehung einer neuen Klasse von Angriffen, genannt physikalische Angriffe, geführt. Diese Angriffe zielen darauf ab den geheimen Schlüssel, welcher vom kryptographischen Algorithmus benutzt wird, zu extrahieren. Ein erfolgreicher physikalischer Angriff deutet nicht auf Schwächen im Algorithmus sondern auf Schwachstellen in der Implementierung hin. Daher müssen bereits in der Entwicklungsphase von kryptographischen Implementierungen physikalische Angriffe als potentielles Risiko berücksichtigt und bestmöglich verhindert werden. Das Ziel dieser Lehrveranstaltung ist es einen Überblick über bekannte physikalische Angriffe und deren Gegenmaßnahmen zu geben. Im ersten Teil der Vorlesung werden die verschiedenen Angriffstypen eingeführt, während im zweiten Teil der Fokus auf Gegenmaßnahmen liegt.

Voraussetzungen: none

Empfohlene Vorkenntnisse: Verständnis der englischen Sprache, Grundkenntnisse der Digitaltechnik, Grundkenntnisse der Datensicherheit und Kryptographie, solide Programmierkenntnisse in mindestens einer Programmiersprache (z.B. C++), Grundkenntnisse der Computerarchitektur, Grundkenntnisse der Signalverarbeitung

Arbeitsaufwand: 150 Stunden

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

Prüfungsform: schriftlich, 120 Minuten

Voraussetzungen für die Vergabe von Kreditpunkten: Projektbasiertes Arbeiten ist ein großer Teil der Lehrveranstaltung. Zusätzlich zu einer schriftlichen Prüfung gibt es wöchentliche Projektarbeiten (Hausaufgaben) und ein abschließendes Seminar. Alle Teile müssen individuell bearbeitet werden, sind bewertet und gehen in die Endnote ein. Für das erfolgreiche Bestehen des Kurses muss die Klausur mit mindestens 50
Wöchentliche Projektarbeiten (Hausaufgaben): 30
Klausur: 60
Abschließendes Seminar: 20
Dies ergibt eine Summe von 110

2.85 150306: Post-Quantum Kryptographie

Nummer: 150306
Lehrform: Vorlesungen und Übungen
Medienform: rechnerbasierte Präsentation
Tafelanschrieb
Verantwortlicher: Prof. Dr. Eike Kiltz
Dozent: Prof. Dr. Eike Kiltz
Sprache: Deutsch
SWS: 4
Leistungspunkte: 5
Angeboten im: Wintersemester

Ziele: Die Vorlesung richtet sich an Mathematik-, ITS- und AI-Studierende im Master-Studienabschnitt.

Inhalt: Sie beschäftigt sich mit kryptographischen Verfahren, welche im Gegensatz zu RSA und Diskreter Logarithmus basierter Verfahren Sicherheit gegen Quantencomputer bieten.

- Quantencomputer und Quantenalgorithmen
- Gitter-basierte Kryptographie
- Code-basierte Kryptographie
- Hash-basierte Kryptographie
- Multivariate Kryptographie

Voraussetzungen: Vorausgesetzt wird die Kenntnis der Anfängerveranstaltung Kryptographie.

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

2.86 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

2.87 148215: Private and Anonymous Communication

Nummer: 148215
Lehrform: Vorlesungen und Übungen
Medienform: rechnerbasierte Präsentation
Verantwortlicher: Prof. Dr. Christina Pöpper
Dozent: Prof. Dr. Christina Pöpper
Sprache: Englisch
SWS: 4
Leistungspunkte: 5
Angeboten im:

Ziele: The students are able to describe, classify, and assess techniques for private and anonymous communication. They are able to reason about the motivation for using these techniques and can describe different scenarios and applications. They are able to describe, classify, and (to a certain extent) counter attacks on privacy and anonymity. The students understand the architectures of different tools, approaches, and techniques that have been proposed and developed in this context. They are able to reason about the achieved levels of protection and also gain practical experience with different tools.

Inhalt: The focus of this course are privacy-enhancing technologies and anonymity techniques. Central elements are privacy metrics and techniques, vulnerabilities and attack mechanisms as well as detection, protection, and prevention techniques. The course will cover techniques for anonymous communication and browsing (e.g., Tor), anonymity in electronic payment systems (e.g., E-Cash, Bitcoin), steganographic and censorship circumvention techniques, communication hiding, and location privacy. The course may also cover special topics such as electronic voting or privacy in social networks.

Voraussetzungen: none

Empfohlene Vorkenntnisse: Knowledge of the contents of Netzsicherheit and Computernetze as well as expertise in programming will be beneficial.

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

2.88 150355: Probabilistische Algorithmen

Nummer: 150355
Lehrform: Vorlesungen und Übungen
Verantwortlicher: Prof. Dr. Alexander May
Dozent: Prof. Dr. Alexander May
Sprache: Deutsch
SWS: 4
Leistungspunkte: 5
Angeboten im:

Ziele: In der Vorlesung Probabilistische Algorithmen werden probabilistische Methoden zur Analyse von Algorithmen verwendet.

Inhalt:

- Diskrete Zufallsvariablen und Momente
- Chernoff Schranken
- Bälle, Urnen und zufällige Graphen
- Probabilistische Methode
- Markovketten und Random Walks
- Entropie
- Monte Carlo Methode
- Universelle Hashfunktionen

Voraussetzungen: keine

Empfohlene Vorkenntnisse: Diskrete 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: mündlich, 30 Minuten

2.89 141241: Programmanalyse

Nummer:	141241
Lehrform:	Vorlesungen und Übungen
Medienform:	e-learning Moodle rechnerbasierte Präsentation
Verantwortlicher:	Prof. Dr. Thorsten Holz
Dozenten:	Prof. Dr. Thorsten Holz Dr.-Ing. Tim Blazytko M. Sc. Emre Güler M. Sc. Sergej Schumilo
Sprache:	Deutsch
SWS:	4
Leistungspunkte:	5
Gruppengröße:	40
Angeboten im:	Sommersemester

Ziele: Die Studierenden kennen verschiedene Konzepte, Techniken und Tools aus dem Bereich der Programmanalyse. Dies beinhaltet den Überblick über verschiedene Konzepte aus dem Bereich Reverse Engineering sowie Binäranalyse. Die Studierenden haben grundlegendes Verständnis von sowohl statischen als auch dynamischen Methoden zur Analyse eines gegebenen Programms. Sie sind in der Lage, verschiedene Aspekte der Programmanalyse zu beschreiben und auf neue Problemstellungen anzuwenden.

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

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

Daneben wird im ersten Teil der Vorlesung eine Einführung in x86/x64 Assembler gegeben sowie die grundlegenden Techniken aus dem Themenbereich Reverse Engineering vorgestellt. Begleitet wird die Vorlesung von Übungen, in denen die vorgestellten Konzepte und Techniken praktisch eingeübt werden.

Voraussetzungen: keine

Empfohlene Vorkenntnisse: Erfahrung in systemnaher Programmierung, Assembler sowie Programmieren in C sind hilfreich für das Verständnis der vermittelten Themen. Vorkenntnisse aus den Vorlesungen Systemsicherheit/Betriebssystemsicherheit sind hilfreich aber nicht notwendig zum Verständnis der 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 sowie erfolgreiche Bearbeitung der Übungsblätter

2.90 150277: Public Key Verschlüsselung

Nummer:	150277
Lehrform:	Vorlesungen und Übungen
Medienform:	rechnerbasierte Präsentation Tafelanschrieb
Verantwortlicher:	Jun. Prof. Dr. Nils Fleischhacker
Dozent:	Jun. Prof. Dr. Nils Fleischhacker
Sprache:	Deutsch
SWS:	4
Leistungspunkte:	5
Angeboten im:	Wintersemester

Ziele: Die Studierenden haben einen Einblick in in theoretische und praktische Aspekte der Public Key Verschlüsselung erhalten.

Inhalt: Die Vorlesung gibt einen Einblick in theoretische und praktische Aspekte der Public Key Verschlüsselung. Dies umfasst Grundlagen und formalen Definitionen von Sicherheit (CPA, CCA1, CCA2), die beweisbare Sicherheit verschiedener theoretischer und praktischer Konstruktionen, sowie die Verbindungen von Public Key Verschlüsselung zu anderen Aspekten der Kryptographie.

Voraussetzungen: Als Voraussetzung für die Vorlesung sind Vorkenntnisse in Kryptographie und beweisbarer Sicherheit, insbesondere von Reduktionsbeweisen, hilfreich aber nicht zwingend erforderlich.

Arbeitsaufwand: 150 Stunden

Der Arbeitsaufwand berechnet sich wie folgt: 15 Wochen zu je 4 SWS ergeben 60 Stunden Anwesenheit. Zum Lösen der Übungsaufgaben sind zwei Stunden je Woche vorgesehen. Es verbleiben 60 Stunden zur Vor- und Nachbereitung und zur Prüfungsvorbereitung.

Prüfungsform: mündlich, 30 Minuten

2.91 150318: Quantenalgorithmen

Nummer: 150318
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 Grundlagen für Quantenalgorithmen.

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

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

Voraussetzungen: keine

Empfohlene Vorkenntnisse: Lineare Algebra, Algorithmen

Arbeitsaufwand: 150 Stunden

Der Arbeitsaufwand berechnet sich wie folgt: 15 Wochen zu je 3 SWS ergeben 45 Stunden Anwesenheit. Zum Lösen der Übungsaufgaben sind zwei Stunden je Woche vorgesehen. Es verbleiben 75 Stunden zur Vor- und Nachbereitung und zur Prüfungsvorbereitung.

Prüfungsform: schriftlich, 120 Minuten

2.92 141146: Quantenschaltungen

Nummer: 141146
Lehrform: Vorlesungen und Übungen
Medienform: Moodle
Verantwortlicher: Prof. Dr. Philipp Niemann
Dozent: Prof. Dr. Philipp Niemann
Sprache: Deutsch
SWS: 3
Leistungspunkte: 5
Angeboten im: Sommersemester

Ziele: Die Studierenden kennen Zusammenhänge und haben Detailkenntnisse bezüglich des Entwurfes von Schaltungen für Quantencomputer. Dies schließt neben Verfahren zur Synthese und Optimierung der Schaltungen auch die Simulation von Quantenschaltungen auf klassischen Computern ein. Darüber hinaus haben Teilnehmer dieser Veranstaltung ein Verständnis der spezifischen Herausforderungen sowohl auf logischer Ebene (z. B. hinsichtlich der Reversibilität der realisierten Funktionen und der exponentiellen Größe entsprechender Funktionsdarstellungen) sowie auf der physikalischen Ebene (etwa hinsichtlich der eingeschränkten Gatterbibliothek, topologischer Einschränkungen sowie Fehlertoleranz).

Inhalt: Nach einer kurzen Einführung in das Rechnen mit Quanten („Quantum Computing“) beschäftigt sich die Vorlesung mit der Frage, wie die dafür benötigten Schaltungen entworfen werden müssen, damit sie möglichst effizient auf echten Quantencomputern ausgeführt werden können. Da Quantenschaltungen außer dem Namen kaum etwas mit konventionellen Schaltkreisen gemeinsam haben, sind bei diesem Entwurf auch ganz andere Herausforderungen und Probleme zu lösen, die teilweise eher denen von Software-Compilern ähneln. Insbesondere ist auch kein tieferes Verständnis der quantenmechanischen Grundlagen nötig, um die Inhalte der Veranstaltung nachvollziehen zu können. Behandelt werden dabei u.a. folgende Themen:

- Synthese von reversiblen Boole'schen Funktionen
- Einbettung von nicht-reversiblen Boole'schen Funktionen
- Zerlegung von komplexen Quantengattern in elementare Quantengatter
- effiziente Funktionsdarstellung von Quantenschaltungen
- Simulation von Quantenschaltungen auf klassischen Rechnern
- Transformation von Quantenschaltungen für NISQ-Quantencomputer

Alle Themen und Verfahren werden anhand geeigneter Software-Werkzeuge (z.B. cirkit, QisKit) und soweit möglich auch auf öffentlich zugänglichen Quantenrechnern (z.B. IBM Q Experience) in der Praxis nachvollzogen.

Voraussetzungen: Keine

Arbeitsaufwand: 150 Stunden

Der Arbeitsaufwand ergibt sich wie folgt: 14 Wochen zu je 3 SWS entsprechen in Summe 42 Stunden Anwesenheit. Für die Nachbereitung der Vorlesung und die Vor- und Nachbereitung der Übungen sind etwa 4 Stunden pro Woche, in Summe 56 Stunden, erforderlich. Etwa 52 Stunden sind für die Klausurvorbereitung vorgesehen.

Prüfungsform: mündlich, 30 Minuten

Literatur:

[1] Niemann, Philipp, Wille, Robert "Compact Representations for the Design of Quantum Logic", Springer, 2017
[2] Chuang, Isaac L. , Nielsen, Michael A. "Quantum Computation and Quantum Information", Cambridge University Press, 2000
[3] Mermin, David N. "Quantum Computer Science - An Introduction", Cambridge University Press, 2007

2.93 158345: Randomness in Cryptography

Nummer:	158345
Lehrform:	Vorlesungen und Übungen
Medienform:	rechnerbasierte Präsentation Tafelanschrieb
Verantwortlicher:	Jun. Prof. Dr. Sebastian Faust
Dozent:	Jun. Prof. Dr. Sebastian Faust
Sprache:	Deutsch
SWS:	3
Leistungspunkte:	4.5
Angeboten im:	

Ziele: Gute Zufälligkeit ist eine fundamentale Voraussetzung für sichere kryptographische Algorithmen. Zufälligkeit wird benötigt um gute Schlüssel zu erzeugen und findet Einsatz bei vielen kryptographischen Algorithmen (wie z.B. beim Verschlüsseln). Leider ist es in der Praxis aufwendig gute Zufallswerte zu erzeugen. Die Vorlesung beschäftigt sich mit praktischen und theoretischen Techniken der Erzeugung von guten Zufallswerten und zeigt auf wie schlechte Zufallswerte in der Praxis zum Verlust von Sicherheit führen können.

Inhalt: Voraussichtliche Themen sind: - Praktische Angriffe auf Systeme mit schlechtem Zufall - Einführung in relevante Konzepte der Informationstheorie - Extraktoren und Kondensers zur Erzeugen von Zufälligkeit - Pseudozufälligkeit - Erzeugen von Zufälligkeit in der Praxis (dev/random und Fortuna in Windows und deren Sicherheitsanalyse) - Kryptographie mit ungenügender Zufälligkeit

Voraussetzungen: keine

Empfohlene Vorkenntnisse: Kryptographie I+II, Interesse an praktischen und theoretischen Fragestellungen in der Kryptographie.

Arbeitsaufwand: 135 Stunden

Der Arbeitsaufwand berechnet sich wie folgt: 14 Wochen zu je 3 SWS ergeben 42 Stunden Anwesenheit. Zum Lösen der Übungsaufgaben sind zwei Stunden je Woche vorgesehen. Es verbleiben 65 Stunden zur Vor- und Nachbereitung und zur Prüfungsvorbereitung.

Prüfungsform: mündlich, 30 Minuten

2.94 141140: Rechnerarchitektur für ET/IT und ITS (PO 13)

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

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

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

Empfohlene Vorkenntnisse: Keine

Arbeitsaufwand: 150 Stunden

Der Arbeitsaufwand ergibt sich wie folgt: 14 Wochen zu je 4 SWS entsprechen in Summe 56 Stunden Anwesenheit. Für die Nachbereitung der Vorlesung und die Vor- und Nachbereitung

der Übungen sind etwa 4 Stunden pro Woche, in Summe 56 Stunden, erforderlich. Etwa 38 Stunden sind für die Klausurvorbereitung vorgesehen.

Prüfungsform: schriftlich, 120 Minuten

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

2.95 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

2.96 150542: Seminar on Knowledge Graphs

Nummer: 150542
Lehrform: Seminar
Medienform: Moodle
Verantwortlicher: Jun. Prof. Dr.-Ing. Maribel Acosta Deibe
Dozent: Jun. Prof. Dr.-Ing. Maribel Acosta Deibe
Sprache: Englisch
SWS: 2
Leistungspunkte: 4
Angeboten im: Wintersemester

Ziele: The seminar includes four mandatory sessions:

1. **Kick-off session** (start of the semester): Lecture on the foundational technologies of the seminar and presentation on the list of topics.
2. **Preliminary presentation** (start of the semester): Seminar participants present initial ideas of the seminar thesis.
3. **Intermediate presentation** (mid-semester): Seminar participants report on the progress of their theses.
4. **Final presentation** (end of the semester): Seminar participants present their theses and final results.

In addition to the mandatory appointments, seminar participants may schedule individual meetings with the professor to discuss the progress of the work (highly recommended).

Inhalt: Knowledge Graphs (KG) allow for representing inter-connected facts or statements annotated with semantics. In KGs, concepts and entities are typically modeled as nodes while their connections are modeled as directed and labeled edges, creating a graph.

In recent years, KGs have become core components of modern data ecosystems. KGs, as building blocks of many Artificial Intelligence approaches, allow for harnessing and uncovering patterns from the data. Currently, KGs are used in the data-driven business processes of multinational companies like Google, Microsoft, IBM, eBay, and Facebook. Furthermore, thousands of KGs are openly available on the web following the Linked Data principles (https://lod-cloud.net/).

In this seminar, students will learn about state-of-the-art KG technologies and investigate relevant research problems in that field, including:

- Creating KGs from (semi-)structured on unstructured sources
- Representing facts in KGs: RDF, RDFS, OWL, Property Graphs
- Querying KGs: SPARQL, CypherQL
- KG Quality: metrics and tasks to enhance the quality of KGs
- Vector representations for KGs
- Publication of KGs on the web

Voraussetzungen: Basic knowledge about databases or semantic web is highly recommended but not mandatory.

Arbeitsaufwand: 120 Stunden

Der Arbeitsaufwand berechnet sich wie folgt: Die Seminarvorträge finden wöchentlich statt. Es besteht Anwesenheitspflicht. Dafür sind durchschnittlich (je nach Teilnehmerzahl) 30 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 90 Stunden anzusetzen ist.

2.97 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

2.98 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.

2.99 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

2.100 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

2.101 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.

2.102 150359: Sicherheit und Privatheit für Big Data

Nummer: 150359
Lehrform: Vorlesungen und Übungen
Medienform: rechnerbasierte Präsentation
Verantwortlicher: Dr.-Ing. Sven Schäge
Dozent: Dr.-Ing. Sven Schäge
Sprache: Deutsch
SWS: 3
Leistungspunkte: 4.5
Angeboten im:

Ziele: Die Studierenden sind befähigt, kryptographische Verfahren für BigData Anwendungen zu verifizieren, ihre Effizienz zu bewerten und in Anwendungen zielgerichtet einzusetzen.

Inhalt: Die Vorlesung behandelt Ansätze um Sicherheitsverfahren zu designen, zu analysieren oder zu vergleichen, die in Anwendungsszenarien mit großen Nutzerzahlen oder Datenmengen eingesetzt werden (können). Insbesondere sollen Verfahren betrachtet werden, mit Hilfe derer die zweckmäßige Anwendbarkeit klassischer Sicherheitssysteme in diesen Szenarien untersucht werden können.

Die Vorlesung ist inhaltlich in zwei Themenblöcke organisiert.

1) Der erste Themenblock behandelt realistische Modellierungen von Sicherheit in Mehrparteienmodellen und effiziente Sicherheitsreduktionen (tightness in multi-user cryptography). Hier geht es insbesondere um Anwendungen mit hohen Nutzerzahlen.
    - Effiziente Sicherheitsreduktionen (tightness) und ihre Auswirkung auf Systemparameter
    - Selbstreduzierbarkeit von kryptografischen Problemen und ihre Anwendung in Mehrparteienanwendungen
    - Nachweis untere Tightness
    - Schranken und optimal effiziente Sicherheitsreduktionen
2) Im zweiten Themenblock werden wichtige und praktische Verfahren vorgestellt, die effizient auf großen Datenmengen arbeiten. Wichtige Themen sind:
    - Searchable Encryption
    - Order-Preserving Encryption

Voraussetzungen: keine

Empfohlene Vorkenntnisse: Empfohlen wird der Besuch der Vorlesung Kryptographie.

Arbeitsaufwand: 135 Stunden

Der Arbeitsaufwand berechnet sich wie folgt: 14 Wochen zu je 3 SWS ergeben 42 Stunden Anwesenheit. Zum Lösen der Übungsaufgaben sind zwei Stunden je Woche vorgesehen. Es verbleiben 65 Stunden zur Vor- und Nachbereitung und zur Prüfungsvorbereitung.

Prüfungsform: mündlich, 30 Minuten

2.103 141030: Software-Implementierung kryptographischer Verfahren

Nummer: 141030
Lehrform: Vorlesungen und Übungen
Medienform: rechnerbasierte Präsentation
Verantwortlicher: Prof. Dr.-Ing. Tim Güneysu
Dozent: Dr.-Ing. Max Hoffmann
Sprache: Deutsch
SWS: 4
Leistungspunkte: 5
Angeboten im: Sommersemester

Ziele: Die Studierenden haben ein Verständnis für Methoden für die schnelle Software-Realisierung ausgewählter Krypto-Verfahren und diese selbst implementiert.

Inhalt: Es werden ausgewählte fortgeschrittene Implementierungstechniken der modernen Kryptographie behandelt.
Inhalte:

- Effiziente Implementierung von Blockchiffren
- Bitslicing
- Effiziente Arithmetik in GF(2^m)
- Effiziente Arithmetik auf elliptischen Kurven
- Spezielle Primzahlen zur schnellen modularen Reduktion
- Primzahltests
- Post-Quantum Kryptographie
- Secure Coding

Voraussetzungen: keine

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

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: Es müssen mindestens 50 Prozent aller möglichen Punkte in der Klausur und den Projekten erreicht werden.

2.104 150351: Symmetrische Kryptanalyse

Nummer: 150351
Lehrform: Vorlesungen und Übungen
Verantwortlicher: Prof. Dr. Gregor Leander
Dozent: Prof. Dr. Gregor Leander
Sprache: Deutsch
SWS: 4
Leistungspunkte: 5
Angeboten im: Wintersemester

Ziele: Die Studierenden haben ein vertieftes Verständnis für die Sicherheit symmetrischer Chiffren.

Inhalt: Wir behandeln die wichtigsten Themen in der symmetrischen Kryptanalyse. Nach einer ausführlichen Vorstellung von linearer und differentieller Kryptanalyse werden weitere Angriffe auf symmetrische Primitive, insbesondere Block-Chiffren behandelt. Hierzu zählen insbesondere Integral (auch Square) Attacken, Impossible Differentials, Boomerang-Angriffe und Slide-Attacken. Neben den Angriffen selbst werden auch immer die daraus resultierenden Design-Kriterien beschrieben, um neue Algorithmen sicher gegen die Angriffe zu machen.

Voraussetzungen: keine

Empfohlene Vorkenntnisse: 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: mündlich, 30 Minuten

Literatur:

[1] Knudsen, Lars, Robshaw, Matthew "The Block Cipher Companion", Springer, 2012

2.105 141033: Usable Security and Privacy

Nummer:	141033
Lehrform:	Vorlesung mit integrierten Übungen
Medienform:	Moodle rechnerbasierte Präsentation
Verantwortlicher:	Prof. Dr. Markus Dürmuth
Dozenten:	Prof. Dr. Markus Dürmuth M. Sc. Florian Farke
Sprache:	Englisch
SWS:	3
Leistungspunkte:	4
Angeboten im:	Sommersemester

Ziele: Die Studierenden verstehen, warum die Usability technischer Systeme entscheidenden Einfluss auf deren Sicherheit haben kann. Darüber hinaus sollen Sie in die Lage versetzt werden, einfache Studien zur Usability selbst durchzuführen.

Inhalt: Diese Veranstaltung vermitttelt Kenntnisse der Usable Security und Privacy. Die Themen umfassen insbesondere:

- Benutzbare Authentifizierung
- Nutzer und Phishing
- Vertrauen/ Trust, PKI, PGP
- Privatheit und Tor
- Privacy policies
- Design und Auswertung von Benutzerstudien

Voraussetzungen: Keine

Empfohlene Vorkenntnisse: Allgemeine Kenntnisse der IT-Sicherheit

Arbeitsaufwand: 120 Stunden

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

Prüfungsform: schriftlich, 120 Minuten

2.106 141245: Web-Sicherheit

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

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

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

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

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

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

Voraussetzungen: keine

Empfohlene Vorkenntnisse:

- Grundkenntnisse Kryptographie und HTML

Arbeitsaufwand: 150 Stunden

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

2.107 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

2.108 148216: Wireless Security

Nummer: 148216
Lehrform: Vorlesungen und Übungen
Medienform: rechnerbasierte Präsentation
Verantwortlicher: Prof. Dr. Christina Pöpper
Dozent: Prof. Dr. Christina Pöpper
Sprache: Englisch
SWS: 4
Leistungspunkte: 5
Angeboten im:

Ziele: Communication services and applications are increasingly leveraging the wireless medium. Given this development, the importance of information and network security in the wireless domain grows. Providing secure communication and network services in wireless environments creates challenges that often differ considerably from traditional wired systems.

The students are able to describe, classify, and assess security goals and attacks on wireless communication and in wireless networks. The students are able to describe the security architectures of different wireless systems and networks, in particular 802.11, GSM/UMTS, RFID, ad hoc and sensor networks. They will are able to reason about security protocols for wireless networks and can implement certain mechanisms to secure them.

Inhalt: The focus of this course are wireless environments such as wireless ad hoc, mesh, and sensor networks. Central elements of the course are the wireless communication channel, wireless network architectures and protocols. We will focus on the vulnerabilities, attack mechanisms as well as detection, protection and prevention techniques in wireless networks.

The course starts with wireless fundamentals and wireless channel basics. This includes jamming and modification attacks and respective countermeasures. It will then cover basic security protocols and protection mechanisms in cellular, WiFi and multi-hop networks. This will be followed by recent advances in the security of multi-hop networks. The considered techniques include security in off-the-shelf wireless technologies (such as WiFi, WiMAX, Mobile Telecommunication, RFID, Bluetooth) and in emerging wireless technologies (security in ad-hoc networks, key management, sensor networks).

Voraussetzungen: none

Empfohlene Vorkenntnisse: Knowledge of the course contents of Systemsicherheit, Netzsicherheit, and Computernetze can be beneficial.

Arbeitsaufwand: 150 Stunden

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

Prüfungsform: mündlich, 30 Minuten

2.109 150232: Zahlentheorie

Nummer:	150232
Lehrform:	Vorlesungen und Übungen
Medienform:	rechnerbasierte Präsentation Tafelanschrieb
Verantwortlicher:	Prof. Dipl.-Phys. Markus Reineke
Dozent:	Prof. Dipl.-Phys. Markus Reineke
Sprache:	Deutsch
SWS:	6
Leistungspunkte:	9
Angeboten im:	Sommersemester

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

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

Voraussetzungen: keine

Empfohlene Vorkenntnisse: Grundlegende Mathematikkenntnisse

Arbeitsaufwand: 270 Stunden

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

Prüfungsform: schriftlich, 180 Minuten

2.110 150353: Zero-Knowledge Proof Systems

Nummer: 150353
Lehrform: Vorlesungen und Übungen
Medienform: Moodle
Verantwortlicher: Jun. Prof. Dr. Nils Fleischhacker
Dozent: Jun. Prof. Dr. Nils Fleischhacker
Sprache: Englisch
SWS: 4
Angeboten im: Sommersemester

Ziele: x

Inhalt: Zero-Knowledge protocols are important building blocks for more complex cryptographic protocols. This class covers foundational aspects of zero-knowledge proofs, including: Lower bounds and round complexity, necessary assumptions, communication complexity, and zero-knowledge in a quantum world, as well as theoretical and practical constructions and their security proofs.

Empfohlene Vorkenntnisse:

- Einführung in die Kryptographie

Prüfungsform: mündlich, 30 Minuten