RUHR-UNIVERSITÄT BOCHUM

FAKULTÄT FÜR INFORMATIK

RUB

Modulhandbuch

für den Bachelorstudiengang

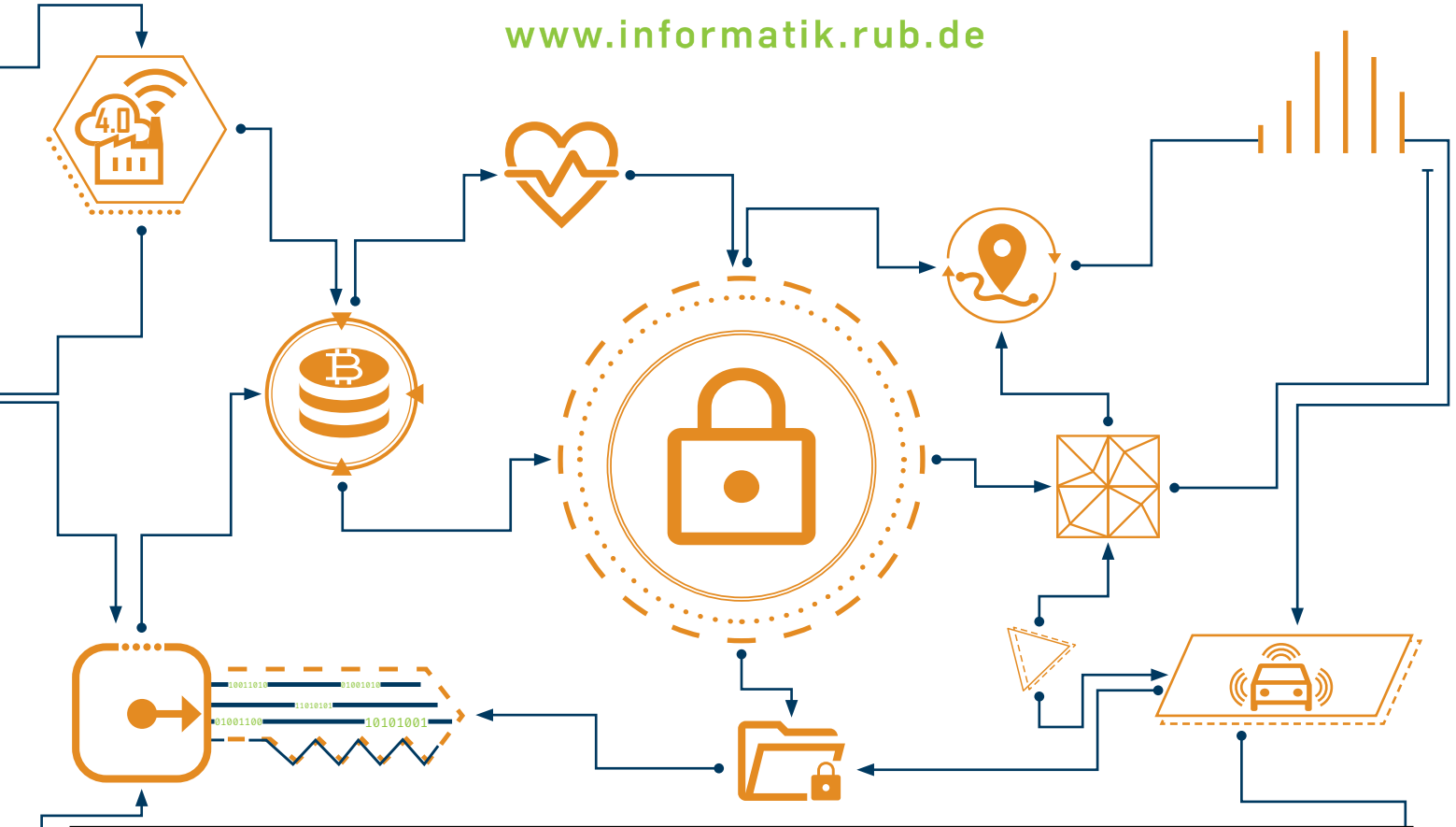
IT-SICHERHEIT

STAND WINTERSEMESTER 2022/23

https://informatik.rub.de/studium/studiengaenge/its/

RUB | Faculty of Computer Science

www.informatik.rub.de



ITS Bachelor PO2022

PFLICHTMODULE

Mathematik 1 - Grundlagen

MODULNUMMER: 212027

KÜRZEL: MATHE1

MODULBEAUFTRAGTER: Prof. Dr. Gregor Leander

DOZENT: Gregor Leander

FAKULTÄT: Fakultät für Informatik

SPRACHE: Deutsch

SWS: 7 SWS

CREDITS: 9 CP

WORKLOAD: 270h

ANGEBOTEN IM: jedes Wintersemester

BESTANDTEILE UND VERANSTALTUNGSART:

LERNZIELE: Nach dem erfolgreichen Abschluss des Moduls - kennen Studierende grundlegende Begriffe und Schreibweisen der Mathematik - können Studierende die erlernten Techniken selbstständig anwenden und mathematische Sachverhalte darstellen - kennen Studierende die Grundlagen abstrakter mathematischer Strukturen und verschiedene Beispiele für Gruppen, Ringe und Körper - verstehen die Studierenden den abstrakten Vektorraumbegriff über beliebigen Körpern, können mit linearer Unabhängigkeit, Dimensionen und mit linearen Abbildungen umgehen - sind Studierende in der Lage, lineare Gleichungssysteme explizit zu lösen sowie Eigenwerte und Eigenvektoren zu berechnen

INHALT: Dieses Modul gibt eine allgemeine Einführung in mathematische Grundlagen und behandelt wichtige Gebiete der Linearen Algebra. Folgende Themengebiete werden behandelt: Grundlagen der Mathematik - grundlegende mathematische Begriffe - Schreibweisen - Aussagenlogik - Mengenlehre - Relationen Algebraische Grundlagen - ganze Zahlen - Restklassen - Gruppen-, Ringe- und Körper-Axiome Lineare Algebra - Vektorräume - Basen - Dimension - Skalarprodukte - lineare Abbildungen - lineare Gleichungssysteme - Basiswechsel - Determinanten - Eigenwerttheorie

VORAUSSETZUNGEN FÜR CREDITS: Bestandene Modulabschlussprüfung

VORAUSSETZUNGEN: keine

LITERATUR: B. Kreußler und G. Pfister: „Mathematik für Informatiker“, Springer Verlag

Mathematik 2 - Algorithmische Mathematik

MODULNUMMER: 150136

KÜRZEL: MATHE2

MODULBEAUFTRAGTER: Prof. Dr. Christian Stump

DOZENT: Prof. Dr. Christian Stump

FAKULTÄT: Fakultät für Mathematik

SPRACHE: Deutsch

SWS: 7 SWS

CREDITS: 9 CP

WORKLOAD: 270 h

ANGEBOTEN IM: jedes Sommersemester

BESTANDTEILE UND VERANSTALTUNGSART: Mathematik 2 – Vorlesung (4 SWS) Mathematik 2 – Übung (3 SWS)

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

INHALT: Diese Lehrveranstaltung behandelt die folgenden Themen: Euklidscher Algorithmus, Gruppen-, Ring-, Körperaxiome, Symmetriegruppen, Polynomarithmetik, formale Potenzreihen, modulare Arithmetik, Lemma von Bezout, Kleiner Satz von Fermat, diskreter Logarithmus, RSA-Verschlüsselungsverfahren, Primzahltests, Chinesischer Restesatz, p-adische Brüche, Newton-Verfahren, Asymptotische Notation durch Landausymbole, Binomialkoeffizienten, Rekursionsgleichungen, Erzeugendefunktionen, Prinzip der Inklusion-Exklusion, Vier-Farben-Problem, Djikstra-Algorithmus, Satz von Cayley, Hamiltonkreise, Google PageRank Algorithmus, Satz von Perron-Frobenoius Konkrete Algorithmen werden in Computeralgebra-Systemen implementiert.

VORAUSSETZUNGEN FÜR CREDITS: Bestandene Modulabschlussprüfung und erfolgreiche Teilnahme an den praktischen Übungen am Rechner

VORAUSSETZUNGEN: keine

VORKENNTNISSE: Mathematische Schulausbildung (gymnasiale Oberstufe) und Inhalte des Moduls Mathematik 1

LITERATUR: B. Kreußler und G. Pfister: „Mathematik für Informatiker“, Springer Verlag

SONSTIGE INFORMATIONEN: In den Übungen werden die Inhalte der Vorlesung vertieft und in Kleingruppen in Computeralgebra-Systemen implementiert. Aktuelle Informationen wie Vorlesungstermine,

Räume oder aktuelle Dozent*innen und Übungsleiter*innen sind im Vorlesungsverzeichnis der Ruhr-Universität https://vvz.rub.de/ und im eCampus https://www.rub.de/ecampus/ecampus-webclient/ zu finden.

Informatik 1 - Programmieren

MODULNUMMER: 212004

KÜRZEL: INFO1

MODULBEAUFTRAGTER: Prof. Dr. Tobias Glasmachers

DOZENT: Tobias Glasmachers

FAKULTÄT: Fakultät für Informatik

SPRACHE: Deutsch

SWS: 6 SWS

CREDITS: 8 CP

WORKLOAD: 240 h

ANGEBOTEN IM: jedes Wintersemester

BESTANDTEILE UND VERANSTALTUNGSART:

LERNZIELE: Nach dem erfolgreichen Abschluss des Moduls - kennen die Studierenden die wichtigsten Konzepte imperativer und objektorientierter Programmierung - können die Studierenden eigene Programme entwerfen und implementieren - können die Studierenden mit Grundbegriffen der Informatik wie etwa Korrektheit, Laufzeit, Boolesche Algebra, Invarianten und abstrakten Datentypen arbeiten - sind Studierende in der Lage, die einfachen Datenstrukturen (Array und Dictionary) gezielt einzusetzen und kennen Standardalgorithmen darauf, insbesondere zum Sortieren von Arrays

INHALT: Zentrales Thema der Veranstaltung ist das Erlernen der Programmierung und der wichtigsten Programmierkonzepte sowie die ersten Grundbegriffe der Informatik: - Imperative Programmierung (Variablen, Kontrollstrukturen, Funktionen und Rekursion, Fehlerbehandlung, Ereignisbehandlung) - Einfache Datenstrukturen (Array und Dictionary, AVL-Baum, Hash-Tabelle) - Objektorientierung (Klassen, Sichtbarkeit, Schnittstellen, Vererbung) - Einführung in eine Reihe von Informatik-Konzepten (Invarianten, Laufzeitanalyse, Sortieralgorithmen, Repräsentation von Daten im Rechner, Boolesche Algebra) Die Veranstaltung nutzt die Programmiersprache TScript („teaching script“) für einen möglichst einfachen und motivierenden Einstieg in die Programmierung. Gegen Ende der Vorlesung erfolgt ein Umstieg auf die Programmiersprache Python.

VORAUSSETZUNGEN FÜR CREDITS: Bestandene Modulabschlussprüfung

VORAUSSETZUNGEN: keine

VORKENNTNISSE: Mathematische Schulausbildung (gymnasiale Oberstufe) und Besuch des Vorkurses Mathematik sowie generelles Interesse an technischen Themen und Sachverhalten

LITERATUR: Die Vorlesung orientiert sich nicht direkt an einem Lehrbuch. Viele Standardwerke mit Titeln wie „Einführung in die Informatik“ verfolgen grob ähnliche Lernziele. Sämtliches Lehrmaterial steht online zur Verfügung.

Informatik 2 - Algorithmen und Datenstrukturen

MODULNUMMER: 211002

KÜRZEL: INFO2

MODULBEAUFTRAGTER: Prof. Dr. Buchin Maike

DOZENT: Professorin Dr. Maike Buchin

FAKULTÄT: Fakultät für Informatik

SPRACHE: Deutsch

SWS: 6 SWS

CREDITS: 8 CP

WORKLOAD: 240 h

ANGEBOTEN IM: jedes Sommersemester

BESTANDTEILE UND VERANSTALTUNGSART:

LERNZIELE: Nach dem erfolgreichen Abschluss des Moduls - können Studierende Algorithmen formal beschreiben und deren Korrektheit beweisen - können Studierende die Laufzeit und den Speicherbedarf von Algorithmen und Daten-strukturen analysieren und bewerten - kennen Studierende grundlegende Datenstrukturen - kennen Studierende grundlegende Schemata zum Entwurf von Algorithmen - sind Studierende in der Lage, Algorithmen und Datenstrukturen für spezifische Probleme zu entwickeln - haben die Studierenden die Grundlagen der Programmiersprache Java kennengelernt

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

VORAUSSETZUNGEN FÜR CREDITS: Bestandene Modulabschlussprüfung

VORAUSSETZUNGEN: keine

VORKENNTNISSE: Inhalte der Module Informatik 1 und Mathematik 1, insbesondere Programmieren und lineare Algebra

LITERATUR: 1. Dietzfelbinger, K. Mehlhorn, P. Sanders: „Algorithmen und Datenstrukturen – Die Grundwerkzeuge“, Springer Verlag 2. T. H. Cormen, C. E. Leiserson, R. Rivest, C. Stein: „Algorithmen – Eine Einführung“, Oldenbourg Verlag

SONSTIGE INFORMATIONEN: Aktuelle Informationen wie Vorlesungstermine, Räume oder aktuelle Dozent*innen und Übungsleiter*innen sind im Vorlesungsverzeichnis der Ruhr-Universität https://vvz.rub.de/

und im eCampus https://www.rub.de/ecampus/ecampus-webclient/ zu finden.

Informatik 3 - Theoretische Informatik

MODULNUMMER: 212002

KÜRZEL: INFO3

MODULBEAUFTRAGTER: Prof. Dr. Thomas Zeume

DOZENT: Prof. Dr. Maike Buchin

FAKULTÄT: Fakultät für Informatik

SPRACHE: Deutsch

SWS: 6 SWS

CREDITS: 8 CP

WORKLOAD: 240 h

ANGEBOTEN IM: jedes Wintersemester

BESTANDTEILE UND VERANSTALTUNGSART:

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

INHALT: Die Lehrveranstaltung gibt einen systematischen Überblick über die folgenden Themengebiete: - Endliche Automaten und reguläre Ausdrücke - Kellerautomaten und kontextfreie Grammatiken - Turingmaschinen und Entscheidbarkeit - Nichtdeterminismus und NP-Vollständigkeitstheorie

VORAUSSETZUNGEN FÜR CREDITS: Bestandene Modulabschlussprüfung

VORAUSSETZUNGEN: keine

VORKENNTNISSE: Inhalte der Module Informatik 2 – Algorithmen und Datenstrukturen und Mathematik 2 -Algorithmische Mathematik

LITERATUR: 1. Schöning, Uwe "Theoretische Informatik - kurzgefasst" 2. Hopcroft, John E., Motwani, Rajeev, Ullman, Jeffrey D. "Einführung in die Automatentheorie, Formale Sprachen und Komplexität" 3. Sipser, Michael "Introduction to the Theory of Computation"

SONSTIGE INFORMATIONEN: Aktuelle Informationen wie Vorlesungstermine, Räume oder aktuelle Dozent*innen und Übungsleiter*innen sind im Vorlesungsverzeichnis der Ruhr-Universität https://vvz.rub.de/ und im eCampus https://www.rub.de/ecampus/ecampus-webclient/ zu finden.

Einführung in die Kryptographie 1

MODULNUMMER: 212010

KÜRZEL: Krypto1

MODULBEAUFTRAGTER: Prof. Dr.-Ing. Christof Paar

DOZENT: Prof.Dr.-Ing Christof Paar

FAKULTÄT: Fakultät für Informatik

SPRACHE: Deutsch

SWS: 4 SWS

CREDITS: 5 CP

WORKLOAD: 150 Stunden

ANGEBOTEN IM: jedes Wintersemester

BESTANDTEILE UND VERANSTALTUNGSART:

LERNZIELE: Nach dem erfolgreichen 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 sie sind mit den Grundlagen des abstrakten Denkens in der IT Sicherheitstechnik vertraut. - erreichen die Studierenden durch Beschreibungen ausgewählter praxisrelevanter Algorithmen, wie beispielsweise des AES- oder RSA-Algorithmus, ein algorithmisches und technisches Verständnis zur praktischen Anwendung - erhalten sie einen Überblick über die in Unternehmen eingesetzten Lösungen - sind sie in der Lage, argumentativ eine bestimmte Lösung zu verteidigen

INHALT: Das Modul bietet einen allgemeinen Einstieg in die Funktionsweise moderner Kryptografie und Datensicherheit. Es werden grundlegende Begriffe und mathematische/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: 1. 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. 2. 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 FÜR CREDITS: Bestandene Modulabschlussprüfung

VORAUSSETZUNGEN: keine

VORKENNTNISSE: Inhalte der Pflichtmodule Mathematik 1 – Grundlagen und Mathematik 2 – Algorithmische Mathematik sowie Fähigkeit zum logischen und abstrakten Denken

LITERATUR: 1. C. Paar, J. Pelzl: „Kryptografie verständlich: Ein Lehrbuch für Studierende und Anwender”, Springer Verlag, 2016 2. C. Paar, J Pelzl: “Understanding Cryptography: A Textbook for Students and Practitioners”, Springer Verlag, 2009

Einführung in die Kryptographie 2

MODULNUMMER: 211009

KÜRZEL: Krypto2

MODULBEAUFTRAGTER: Prof. Dr.-Ing. Christof Paar

DOZENT: Prof. Dr.-Ing. Christof Paar

FAKULTÄT: Fakultät für Informatik

SPRACHE: Deutsch

SWS: 4 SWS

CREDITS: 5 CP

WORKLOAD: 150 Stunden

ANGEBOTEN IM: jedes Sommersemester

BESTANDTEILE UND VERANSTALTUNGSART:

LERNZIELE: Nach erfolgreichem Abschluss des Moduls - verfügen die Studierenden über Kenntnisse der grundlegenden Anwendungen asymmetrischer und hybrider Verfahren - können die Studierenden entscheiden, unter welchen Bedingungen man in der Praxis bestimmte Verfahren einsetzt und wie die Sicherheitsparameter zu wählen sind - sind die Studierenden mit den Grundlagen des abstrakten Denkens in der IT-Sicher-heitstechnik vertraut - erreichen die Studierenden durch Beschreibungen ausgewählter praxisrelevanter Algorithmen, wie beispielsweise des Diffie-Hellman-Schlüsselaustausches oder der ECC-basierten Verfahren, ein algorithmisches und technisches Verständnis zur praktischen Anwendung - erhalten die Studierenden dabei einen Überblick über die in Unternehmen eingesetzten Lösungen

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 wird in zwei Teilen gegliedert: 1. 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 Hash-Funktionen, die eine große Rolle für digitalen Signaturen und Message Authentication Codes (MACs oder kryptografische Checksummen) spielen. 2. 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 FÜR CREDITS: Bestandene Modulabschlussprüfung

VORAUSSETZUNGEN: keine

VORKENNTNISSE: Inhalte des Moduls Einführung in die Kryptographie 1

LITERATUR: 1. C. Paar, J. Pelzl: „Kryptografie verständlich: Ein Lehrbuch für Studierende und Anwender“, Springer Verlag, 2016 2. C. Paar, J. Pelzl: „Understanding Cryptography: A Textbook for Students and

Practitioners“, Springer Verlag, 2009

Technische Informatik 1 - Rechnerarchitektur

MODULNUMMER: 141142

KÜRZEL: TI1

MODULBEAUFTRAGTER: Dr. rer. nat. Philipp Niemann

DOZENT: Studiendekan der Fakultät für Informatik

FAKULTÄT: Fakultät für Elektrotechnik und Informationstechnik

SPRACHE: Deutsch

SWS: 4 SWS

CREDITS: 5 CP

WORKLOAD: 150 h

ANGEBOTEN IM: jedes Wintersemester

BESTANDTEILE UND VERANSTALTUNGSART:

LERNZIELE: Nach dem erfolgreichen Abschluss des Moduls kennen die Studierenden Zusammenhänge und haben Detailkenntnisse von den Komponenten und der Funktionsweise moderner Computersysteme. Dies schließt neben dem Prozessor auch das Speichersystem und die Schnittstellen zu weiteren Systemkomponenten ein sind die Studierenden auf der Basis dieser Kenntnisse in der Lage, Computersysteme und deren Komponenten bezüglich verschiedener Metriken, wie z.B. Energieverbrauch, Rechenleistung, Speicherperformance etc. auf deren Eignung für eine bestimmte Aufgabe zu bewerten haben die Studierenden 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, sodass neben dem im Detail vorgestellten Beispielprozessor mit MIPS Architektur auch moderne Hochleistungsprozessoren mit x86-64 ISA, Prozessoren für eingebettete Systeme auf Basis der ARM-Architektur, extrem energiesparende Prozessoren auf Basis des MSP430, wie sie beispielsweise in IoT-Geraten zum Einsatz kommen, und anwendungsspezifische Spezialprozessoren auf Basis der Tensilica Xtensa Plattform vorgestellt werden.

VORAUSSETZUNGEN FÜR CREDITS: Bestandene Modulabschlussprüfung

VORAUSSETZUNGEN: keine

VORKENNTNISSE: werden die Fähigkeit für strukturiertes, algorithmisches Denken sowie das Erfassen von komplexen Abhängigkeiten und Interaktionsmustern vorausgesetzt.

LITERATUR: 1. A. S. Tanenbaum: „Computerarchitektur“, Pearson, 2005 2. A. S. Tanenbaum: „Computerarchitektur. Strukturen – Konzepte – Grundlagen“, Pearson, 2006 3. J. LR. Hennessy, D. Patterson: „Rechnerorganisation und Rechnerentwurf: Die Hardware/Software-Schnittstelle“, Oldenbourg Verlag, 2011 4. A. S. Tanenbaum: „Strukctured Computer Organization“, Prentice Hall, 2005

SONSTIGE INFORMATIONEN: Die Übungen werden zwecks Vorbereitung den Studierenden spätesten eine Woche vor dem Übungstermin im Netz zum Download bereitgestellt. Die Durchführung der Übungen (Erarbeitung der Ergebnisse im Dialog mit den Studierenden) erfolgt nicht in einem festen Zeitraster, sondern gemäß dem Vorlesungsfortschritt. Aktuelle Informationen wie Vorlesungstermine, Räume oder aktuelle Dozent*innen und Übungsleiter*innen sind im Vorlesungsverzeichnis der Ruhr-Universität https://vvz.rub.de/ und im eCampus https://www.rub.de/ecampus/ecampus-webclient/ zu finden.

Technische Informatik 2 - Digitaltechnik

MODULNUMMER: 141304

KÜRZEL: TI2

MODULBEAUFTRAGTER: Prof. Dr.-Ing. Jürgen Oehm

DOZENT: Prof. Dr.-Ing. Jürgen Oehm

FAKULTÄT: Fakultät für Elektrotechnik und Informationstechnik

SPRACHE: Deutsch

SWS: 4 SWS

CREDITS: 5 CP

WORKLOAD: 150 h

ANGEBOTEN IM: jedes Sommersemester

BESTANDTEILE UND VERANSTALTUNGSART:

LERNZIELE: Nach dem erfolgreichen Abschluss des Moduls haben die Studierenden umfassende Kenntnisse in den folgenden Bereichen erworben: Boolesche Algebra, Struktur und Funktionalität digitaler Grund-schaltungen, Kostenoptimierung digitaler Funktionsgruppen, Techniken zur taktsynchronen Verarbeitung von Daten, Kodierung und Verarbeitung von Daten, Struktur und Funktionalität solcher Grundfunktionalitäten, die insbesondere zentrale Bestandteile in Mikroprozessorarchitekturen und deren Umgebung sind verstehen die Studierenden die schaltungstechnischen Möglichkeiten und Grenzen moderner CMOS-Logikstrukturen, die als Richtlinien für den Wissenstransfair dienen können die Studierenden die aktuellen Entwicklungstrends in einer sich rasant entwickelnden digitalen Anwendungswelt besser verstehen und analysieren sind die Studierenden in der Lage, zukünftige Entwicklungen in den Integrationstechnologien und damit in der Digitaltechnik selbst bezüglich ihrer Möglichkeiten und Grenzen einzuschätzen

INHALT: Die Lehrveranstaltung gibt einen systematischen Überblick über die folgenden Themengebiete: Historischer Rückblick und Motivation Boolesche Algebra, minimale Schaltungen auf Basis von NAND und NOR Gatterlaufzeiten, Timing-Analyse, kritischer Pfad Zahlensysteme, Zahlenkodierungen, Fehlererkennung und Korrektur, Fest- und Fließkommadarstellungen Rechenschaltungen, arithmetisch logische Einheit (ALU), Flankendetektoren, bi-, mono- und astabile Schaltungen, transparente und nicht-transparente Flip-Flops (FF) Frequenzteiler, Zahler (asynchron, synchron), Automaten, Schieberegister Speicher: S-RAM, D-RAM, ROM, … (Aufbau und Organisationsformen) taktsynchrone Techniken zur Datenverarbeitung ALU in Umgebungen zur Mikroprogrammierung Konzepte zur serielle Datenübertragung Grundlagenidee von A/D- und D/A-Wandlern Konzept: skalierbare Standard-Logik-Zellen, CMOS-Logik Übersicht: Logikanalyse, Tools zur Logikanalyse, HDL Entwurfssprachen Mooresches Gesetz

VORAUSSETZUNGEN FÜR CREDITS: Bestandene Modulabschlussprüfung und erfolgreiche Teilnahme an den Übungen

VORAUSSETZUNGEN: keine

VORKENNTNISSE: Inhalte des Moduls Mathematik 1 – Grundlagen. Vorausgesetzt wird ein generelles Interesse an technischen Systemen, die Fähigkeit zu strukturieren, algorithmischem Denken sowie die

Fähigkeit zum Erfassen von komplexen Abhängigkeiten und Interaktionsmustern.

LITERATUR: 1. P. Peter: „Digitaltechnik I. Grundlagen, Entwurf, Schaltungen“, Hüthig Verlag 2. F. Klaus: „Digitaltechnik Lehr- und Übungsbuch für Elektrotechniker und Informatiker“, Vieweg Verlag 3. J. Becker und HM. Lipp: „Grundlagen der Digitaltechnik“, Oldenbourg Verlag

SONSTIGE INFORMATIONEN: Es wird eine vorlesungsbegleitende Zusatzübung (Tutorium) angeboten. Zur Lehrveranstaltung gibt es ein Vorlesungsskript, welches in einer virtuellen Ma-schine enthalten ist. Das Konzept eines interaktiven Vorlesungsskripts in der Umge-bung einer virtuellen Maschine wird im folgendem Video kurz vorgestellt: https://ruhr-uni-bochum.sciebo.de/s/bJD5aASWeOl1cvP Aktuelle Informationen wie Vorlesungstermine, Räume oder aktuelle Dozent*innen und Übungsleiter*innen sind im Vorlesungsverzeichnis der Ruhr-Universität https://vvz.rub.de/ und im eCampus https://www.rub.de/ecampus/ecampus-webclient/ zu finden.

Software Engineering

MODULNUMMER: 212000

KÜRZEL: SwEng

MODULBEAUFTRAGTER: Prof. Dr. Thorsten Berger

DOZENT: Prof. Dr. Thorsten Berger

FAKULTÄT: Fakultät für Informatik

SPRACHE: Englisch

SWS: 4 SWS

CREDITS: 5 CP

WORKLOAD: 150 h

ANGEBOTEN IM: jedes Wintersemester

BESTANDTEILE UND VERANSTALTUNGSART:

LERNZIELE: Nach dem erfolgreichen Abschluss des Moduls - verfügen die Studierenden über vertiefte Kenntnisse über ausgewählte Aspekte des Softwareentwicklungsprozesses - verfügen die Studierenden über Grundkenntnisse zum Thema Softwarequalität - kennen und verstehen die Studierenden die grundsätzlichen Ziele und Verantwort-lichkeiten im Software-Lebenszyklus - kennen und verstehen die Studierenden die verschiedenen Aktivitäten innerhalb des Software-Lebenszyklus und deren Abhängigkeiten - sind die Studierenden in der Lage, die vermittelten Software-Entwurfsmethoden und Entwicklungsprozesse fallspezifisch anzuwenden

INHALT: Die Studierenden lernen unterschiedliche Formen von (klassischen und agilen) Vorgehens-modellen in der Softwareentwicklung kennen. Sie lernen Methoden der Anforderungserhebung, des Entwurfs und des Testens kennen und setzen diese in reale Fallbeispiele selbstständig um.

VORAUSSETZUNGEN FÜR CREDITS: Bestandene Modulabschlussprüfung

VORAUSSETZUNGEN: Keine

VORKENNTNISSE: Inhalte der Module Informatik 1 – Programmierung und Informatik 2 – Algorithmen und Datenstrukturen

LITERATUR: s. Webseite der Veranstaltung

SONSTIGE INFORMATIONEN: Aktuelle Informationen wie Vorlesungstermine, Räume oder aktuelle Dozent*innen und Übungsleiter*innen sind im Vorlesungsverzeichnis der Ruhr-Universität https://vvz.rub.de/ und im eCampus https://www.rub.de/ecampus/ecampus-webclient/ zu finden.

Betriebssysteme

MODULNUMMER: 211005

KÜRZEL: BS

MODULBEAUFTRAGTER: Prof. Dr.-Ing. Timo Hönig

DOZENT: Prof. Dr.-Ing Timo Hönig

FAKULTÄT: Fakultät für Informatik

SPRACHE: Deutsch

SWS: 4 SWS

CREDITS: 5 CP

WORKLOAD: 150 h

ANGEBOTEN IM: jedes Sommersemester

BESTANDTEILE UND VERANSTALTUNGSART:

LERNZIELE: Nach dem erfolgreichen Absolvieren des Moduls - erlangen die Studierenden ein solides Grundverständnis von modernen Betriebssystemen, ihrer Funktion und ihrer Implementierung - sind die Studierenden in der Lage, verschiedene Aspekte eines Betriebssystems wie Prozess- und Speichermanagement zu verstehen und zu nutzen, sie können dabei verschiedene Designentscheidungen eigenständig analysieren und bewerten - sind die Studierenden in der Lage, bestimmte Aspekte eines Betriebssystems selbst zu designen und diese argumentativ zu verteidigen

INHALT: In diesem Modul werden die wichtigsten Grundlagen zu Betriebssystemen vorgestellt. Dazu gehören zum Beispiel: - Betriebssystemkonzepte - Prozesse und Threads, Interprozesskommunikation - Scheduling-Mechanismen - Speicherverwaltung, Speicherabstraktionen, Paging - Dateisysteme - Eingabe- und Ausgabeverwaltung - Algorithmen zur Vermeidung von Deadlocks - Grundlagen der Sicherheit von Betriebssystemen In den letzten Wochen der Veranstaltung, abhängig vom verfügbaren Zeitfenster, werden spezielle Themen wie beispielsweise Multimedia-Betriebssysteme, Multiprozessorsysteme und Entwurf von Betriebssystemen, behandelt. Um den Bezug zu modernen Betriebssystemen (aktuellen Versionen von Linux, Windows und macOS) herzustellen, werden die Themen an praktischen Beispielen illustriert. Dies ermöglicht es den Studierenden, die in der Vorlesung besprochenen Themen praktisch nachzuvollziehen.

VORAUSSETZUNGEN FÜR CREDITS: Bestandene Modulabschlussprüfung und erfolgreiche Teilnahme an den Übungen

VORAUSSETZUNGEN: Keine

VORKENNTNISSE: Grundkenntnisse der Informatik (Inhalte der Module Informatik 1 – Programmierung und Technische Informatik 1 – Rechnerarchitektur)

LITERATUR: 1. W. Stallings: „Internals and Design Principles“, Pearson Verlag 2. A. S. Tanenbaum: „Moderne Betriebssysteme“, Pearson Verlag 3. A. S. Tanenbaum: „Modern Operating Systems“, Pearson Verlag

Systemsicherheit

MODULNUMMER: 211011

KÜRZEL: SysSec

MODULBEAUFTRAGTER: Prof. Dr. Ghassan Karame

DOZENT: Prof. Dr.-Ing. Jörg Schwenk

FAKULTÄT: Fakultät für Informatik

SPRACHE: Deutsch

SWS: 4 SWS

CREDITS: 5 CP

WORKLOAD: 150 h

ANGEBOTEN IM: jedes Sommersemester

BESTANDTEILE UND VERANSTALTUNGSART: Systemsicherheit – Vorlesung (2 SWS)Systemsicherheit – Übung (2 SWS)

LERNZIELE: At the end of this course, students will be able to (1) classify and describe vulnerabilities and protection mechanisms of popular systems and protocols, and (2) analyze / reason about basic protection mechanisms for modern OSs, software, and hardware systems. Students will also develop the ability to reason about the security of a given protocol and independently develop appropriate security defenses and security models.

INHALT: While clearly beneficial, the large-scale deployment of online services has resulted in the increase of security threats against existing services. As the size of the global network grows, the incentives of attackers to abuse the operation of online applications also increase and their advantage in mounting successful attacks becomes considerable. These cyber-attacks often target the resources, availability, and operation of online services. With an increasing number of services relying on online resources, integrating proper security measures therefore becomes integral to ensure the correct functioning of every online service. In this course, we discuss important theoretical and analytical aspects in system security. The focus of the course is to understand basic attack strategies on modern systems and platforms, with a focus on side-channel attacks, software-based attacks, malware analysis, as well as software-based defenses (e.g., address space randomization and non-executable memory) and hardware-based defenses (e.g., using TPMs and TEEs). Other topics of the course include analyzing the security of modern cryptocurrencies and ML platforms, and similar aspects in system security. An integral part of this course are exercises and homeworks, which aim to deepen the understanding of the material with practical examples.

VORAUSSETZUNGEN FÜR CREDITS: Bestandene Modulabschlussprüfung

VORAUSSETZUNGEN: Keine

VORKENNTNISSE: background in Cryptographic primitives (encryption methods, signatures, MACs, hash functions), principles of communication networks, is recommended.

LITERATUR: 1. D. Gollmann: „Computer Security“, Wiley and Sons 2. A.J. Menezes, P.C. van Oorschot and A. S. Vanstone: “Handbook of Applied Cryptography”, CRC Press 3. C. Boyd and A. Manthuria:

“Protocols for Authentication and Key Establishment”, Springer Verlag 4. R. Anderson: “Security Engineering – A Guide for Building Dependeble Distributed Systems”, Wiley and Sons

SONSTIGE INFORMATIONEN: Aktuelle Informationen wie Vorlesungstermine, Räume oder aktuelle Dozent*innen und Übungsleiter*innen sind im Vorlesungsverzeichnis der Ruhr-Universität https://vvz.rub.de/ und im eCampus https://www.rub.de/ecampus/ecampus-webclient/ zu finden.

Introduction to Cryptography 2

MODULNUMMER: 211009

KÜRZEL: Krypto2

MODULBEAUFTRAGTER: Prof. Dr.-Ing. Christof Paar

DOZENT: Prof. Dr.-Ing. Christof Paar, M. Sc. Julian Speith, M. Sc. Paul Staat, M. Sc. Johannes Tobisch

FAKULTÄT: Fakultät für Informatik

SPRACHE: Deutsch

SWS: 4 SWS

CREDITS: 5 CP

WORKLOAD: 150 h

ANGEBOTEN IM: each summer semester

BESTANDTEILE UND VERANSTALTUNGSART: Introduction to Cryptography 2– Lecture (2 SWS)Introduction to Cryptography 2 – Exercise (2 SWS)

LERNZIELE: After successfully completing the module - the students have knowledge of the basic applications of asymmetric and hybrid methods - The students can decide under which conditions certain procedures are to be used in practice and how the safety parameters are to be selected - the students are familiar with the basics of abstract thinking in IT security technology - Through descriptions of selected practical algorithms, such as the Diffie-Hellman key exchange or the ECC-based procedure, the students achieve an algorithmic and technical understanding for practical application - The students get an overview of the solutions used in companies

INHALT: The module offers a general introduction to the functionality of modern cryptography and data security. Basic terms and mathematical / technical procedures of cryptography and data security are explained. Practically relevant asymmetrical procedures and algorithms are presented and explained using practical examples. The lecture is divided into two parts: 1. The first part begins with an introduction to asymmetric methods and their most important representatives (Diffie-Hellman, elliptic curves). The focus is on the algorithmic introduction of asymmetrical procedures, which contain both encryption algorithms and digital signatures. This part is completed by hash functions, which play a major role for digital signatures and message authentication codes (MACs or cryptographic checksums). 2. In the second part of the lecture, the basics of security solutions based on the concepts of symmetrical and asymmetrical cryptography are discussed. Above all, the solutions required and used in companies (PKI, digital certificates, etc.) are discussed.

VORAUSSETZUNGEN FÜR CREDITS: Bestandene Modulabschlussprüfung

VORAUSSETZUNGEN: None

VORKENNTNISSE: Contents of the module Introduction to Cryptography 1

LITERATUR: 1. C. Paar, J. Pelzl: „Kryptografie verständlich: Ein Lehrbuch für Studierende und Anwender“, Springer Verlag, 2016 2. C. Paar, J. Pelzl: „Understanding Cryptography: A Textbook for Students and Practitioners“, Springer Verlag, 2009

AKTUELLE INFORMATIONEN: In the summer semester 2022 the course will be offered exclusively digitally, the first lecture will take place on 6 April 22. All required information and materials will be provided via the Moodle (https://moodle.ruhr-uni-bochum.de/course/view.php?id=40775) course. Enrollment in the Moodle course is possible without a password and should be done exclusively with a RUB mail address (exception: UA Ruhr). Lecture: Wednesday 9:45 - 11:45 (digital) Tutorial (alternative): Wednesday 12:15 - 13:15 (digital) Tutotial: Wednesday 14:15 - 15:45

SONSTIGE INFORMATIONEN: Current information such as lecture dates, rooms or current lecturers and instructors can be found in the course directory of the Ruhr-Universität https://vvz.rub.de/ and in the eCampus https://www.rub.de/ecampus/ecampus-webclient /

Elektrotechnik 1 - Elektrische Netzwerke

MODULNUMMER: 141129

KÜRZEL: ET1

MODULBEAUFTRAGTER: PROF. DR.-ING. Ilona Rolfes

DOZENT: Prof. Dr.-Ing. Ilona Rolfes

FAKULTÄT: Fakultät für Elektrotechnik und Informationstechnik

SPRACHE: Deutsch

SWS: 5 SWS

CREDITS: 6 CP

WORKLOAD:

ANGEBOTEN IM: jedes Wintersemester

BESTANDTEILE UND VERANSTALTUNGSART:

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

INHALT: Die Veranstaltung bietet einen allgemeinen Einstieg in die Grundlagen der elektrischen Netzwerke. Es werden grundlegende Begriffe und Verfahren erläutert. Die Vorlesung lässt sich in fünf Teile gliedern: Lineare Gleichstromschaltungen: Zählpfeile; Strom- und Spannungsquellen; Die Kirchhoff´schen Gleichungen; einfache Widerstandsnetzwerke (Spannungsteiler, Stromteiler); reale Strom- und Spannungsquellen; Wechselwirkungen zwischen Quelle und Verbraucher (Zusammenschaltung von Spannungsquellen, Leistungsanpassung, Wirkungsgrad); Superpositionsprinzip; Analyse umfangreicher Netzwerke. Übergang zu zeitabhängigen Strom und Spannungsformen: Übersicht sowie Einführung verschiedener Kenngrößen (Mittelwert, Gleichrichtwert, Effektivwert, Maximalwert, Spitzenwert, Spitze-Spitze-Wert, Schwingungsbreite). Wechselstrom und Wechselspannung: Das Zeigerdiagramm; Komplexe Wechselstromrechnung; Beschreibung konzentrierter RLC Bauelemente und idealer Quellen; Einführung der Ortskurven; Berechnung einfacher Wechselstromkreise über die komplexe Ebene; Energie und Leistung bei Wechselspannung; Leistungsanpassung. Analyse von Netzwerken: Maschenstromverfahren; Knotenpotenzialverfahren. Einführung zu Zweitoren: Torbedingung; Zweitorgleichungen in Matrixform (Impedanz-, Admittanz-, Hybrid-, Kettenform); Zweitoreigenschaften (Reziprozität, Symmetrie); Matrizen elementarer Zweitore.

VORAUSSETZUNGEN FÜR CREDITS: Bestandene Modulabschlussprüfung

VORAUSSETZUNGEN: Keine

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

AKTUELLE INFORMATIONEN: Diese Veranstaltung ersetzt die LV "Allgemeine Elektrotechnik 1 - Elektrische Netzwerke" (Nr. 141130) der PO 13.

SONSTIGE INFORMATIONEN: Die Vorlesung und die Übung finden als Live-Veranstaltung online zu den oben angegebenen Zeiten statt. Zusätzlich erfolgt eine Vertiefung und Übung der Inhalte im Rahmen von Präsenzübungen in Kleingruppen an der Universität. Das Password für den moodle-Kurs im Wintersemster lautet: ET-EN-WS21

Systemtheorie 1 - Signale und Systeme

MODULNUMMER: 141170

KÜRZEL: SYS1

MODULBEAUFTRAGTER: Prof. Dr.-Ing. Rainer Martin

DOZENT: Prof. Dr.-Ing. Rainer Martin

FAKULTÄT: Fakultät für Elektrotechnik und Informationstechnik

SPRACHE: Deutsch

SWS: 4 SWS

CREDITS: 5 CP

WORKLOAD:

ANGEBOTEN IM: jedes Sommersemester

BESTANDTEILE UND VERANSTALTUNGSART: Termine: Siehe eCampus

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

INHALT: 1. Signale und Systeme Signale, Kenngrößen und Eigenschaften von Signalen, Elementare Operationen, Signalsynthese und Signalanalyse, periodischer Signale, Analog-Digital und Digital-Analog Umsetzung, lineare und nichtlineare Systeme 2. Einführung in die Wahrscheinlichkeitsrechnung Einführung und Definitionen, Mehrstufige Zufallsexperimente, Diskrete Zufallsvariablen, Kontinuierliche Zufallsvariablen 3. Grundbegriffe der Informationstheorie Grundlegende Fragestellungen der Informationstheorie, Entropiebegriffe, Anwendungen

VORAUSSETZUNGEN FÜR CREDITS: Bestandene Modulabschlussprüfung

VORAUSSETZUNGEN: Keine

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

AKTUELLE INFORMATIONEN: Diese Veranstaltung ersetzt ab dem Sommersemester 2021 die LV "Systemtheorie 1 - Grundgebiete" (Nr. 141171).

SONSTIGE INFORMATIONEN: Die Veranstaltung wird im Sommersemester 2021 im Online-Format mit schriftlichen Unterrichtsmaterialien, Lehrvideos, Übungsblättern, Online-Forum und Live-Chat durchgeführt. Ankündigungen und Details entnehmen Sie bitte dem entsprechenden Moodle-Kurs (Kurspasswort: $Dirac$):

Netzsicherheit 1

MODULNUMMER: 212012

KÜRZEL: N1

MODULBEAUFTRAGTER: Prof. Dr. Jörg Schwenk

DOZENT:

FAKULTÄT: Fakultät für Informatik

SPRACHE: Deutsch

SWS: 4 SWS

CREDITS: 5 CP

WORKLOAD:

ANGEBOTEN IM: jedes Wintersemester

BESTANDTEILE UND VERANSTALTUNGSART:

LERNZIELE: Studierende verfügen nach erfolgreichem Abschluss des Moduls über ein umfassendes Verständnis der technischen Aspekte von Netzsicherheit. Sie haben erkannt, dass Krypto-graphie 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 Lösungs¬möglich-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 Signatur¬algorithmen ab. Prominente Beispiele (für fehlerhafte Einbettungen) sind EFAIL (efail.?de), Angriffe auf die WLAN-Verschlüsselungssysteme WEP und WPA (KRACK) und diverse Angriffe auf TLS (Bleichenbacher, POODLE, DROWN, ROBOT). Das Modul „Netzsicherheit 1“ beschäftigt sich mit konkreten Netzen zur Datenübertragung und beleuchtet diese von allen Seiten auf ihre Sicherheit hin. Es umfasst folgende Teile: - Einführung: Internet - Einführung: Vertraulichkeit - Einführung: Integrität - Einführung: Kryptographische Protokolle - PPP-Sicherheit (insb. PPTP), EAP-Protokolle - WLAN-Sicherheit (WEP, WPA, Wardriving, KRACK) - GSM- und UMTS-Mobilfunk (Authentisierung und Verschlüsselung) - IPSec (ESP und AH, IKEv1 und v2, Angriffe auf IPSec) - Dateiverschlüsselung mit OpenPGP (Datenformat, Efail, Klima-Rosa) - E Mail-Verschlüsselung mit S/MIME (SMTP, Datenformat, Efail, POP3, IMAP) Neben den Systemen selbst werden dabei auch publizierte Angriffe auf diese Systeme besprochen; die Studierenden stellen selbst wissenschaftliche Überlegungen zur Verbesserung der Sicherheit an.

VORAUSSETZUNGEN FÜR CREDITS: Bestandene Modulabschlussprüfung

VORAUSSETZUNGEN: Keine

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

LITERATUR: Schwenk, Jörg "Sicherheit und Kryptographie im Internet", Vieweg, 2014

Grundlagenpraktikum ITS

MODULNUMMER: 211400

KÜRZEL: GrdPrITS

MODULBEAUFTRAGTER: M. Sc. Noß Dominik

DOZENT: Prof. Dr. Jörg Schwenk

FAKULTÄT: Fakultät für Informatik

SPRACHE: Deutsch

SWS: 3 SWS

CREDITS: 3 CP

WORKLOAD:

ANGEBOTEN IM: jedes Semester

BESTANDTEILE UND VERANSTALTUNGSART:

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

INHALT: In 10 Versuchen und 2 Ersatzversuchen wird eine praktische Einführung in die IT-Security gegeben. Wie hört man Netzwerkverkehr ab? Wie greift man eine Website an? Wie exploitet man Buffer Overflows? Jeder Versuch wird in einer detaillierten Anleitung beschrieben, welche im Vorfeld vorbereitet werden muss. Zu jedem Thema muss eine Versuchsauswertung abgegeben werden. Die Themen umfassen zur Zeit (Anpassungen aufgrund aktueller Entwicklungen sind möglich): -Kryptographische Angriffe auf RSA -Angriffe in geswitchten Netzwerken -Buffer Overflow Attacken -Forensische Analyse eines Ransomware-Angriffs -Konfiguration von Firewalls -Programmatische Analyse von Netzwerkdaten mit LibPcap -Einführung in Linux -MD5 Kollisionen in Postscript -Netzwerk-Analyse mit nmap & Wireshark -Security Incident and Event Management (SIEM) mit Splunk -Web Angriffe

VORAUSSETZUNGEN FÜR CREDITS: Erfolgreich abgeschlossenes Projekt und positiv bewertete abgegebene Dokumentation

VORAUSSETZUNGEN: Das Praktikum ist bestanden, sobald 10 einwandfreie Versuchsauswertungen abgegeben wurden.

VORKENNTNISSE: Grundkenntnisse aus den Bereichen Kryptographie, Programmiersprache, und Computernetze

Netzsicherheit 2

MODULNUMMER: 211013

KÜRZEL: N2

MODULBEAUFTRAGTER: Prof. Dr. Jörg Schwenk

DOZENT: Prof. Dr. Jörg Schwenk, M. Sc. Robert Merget

FAKULTÄT: Fakultät für Informatik

SPRACHE: Deutsch

SWS: 4 SWS

CREDITS: 5 CP

WORKLOAD:

ANGEBOTEN IM: jedes Sommersemester

BESTANDTEILE UND VERANSTALTUNGSART: WICHTIGER HINWEIS: Diese Website wird derzeit nur unregelmäßig aktualisiert. Stattdessen finden Sie aktuelle Informationen zu allen Lehrveranstaltungen des Lehrstuhls für Netz- und Datensicherheit finden Sie unter https://informatik.rub.de/nds/teaching/courses/

LERNZIELE: 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 Signatur¬algorithmen 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.

VORAUSSETZUNGEN FÜR CREDITS: Bestandene Modulabschlussprüfung

VORAUSSETZUNGEN: Keine

VORKENNTNISSE: Grundkenntnisse in TCP/IP, Grundkenntnisse der Sicherheitsprobleme von Computer-

netzen auf dem Niveau populärer Fachzeitschriften (z.B. c't).

Kryptographie

MODULNUMMER: 212017

KÜRZEL: KRYPTO

MODULBEAUFTRAGTER: Prof. Dr. Alexander May

DOZENT: Prof. Dr. Eike Kiltz

FAKULTÄT: Fakultät für Informatik

SPRACHE: Deutsch

SWS: 6 SWS

CREDITS: 8 CP

WORKLOAD:

ANGEBOTEN IM: jedes Wintersemester

BESTANDTEILE UND VERANSTALTUNGSART:

LERNZIELE: 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 FÜR CREDITS: Bestandene Modulabschlussprüfung

VORAUSSETZUNGEN: Keine

VORKENNTNISSE: Inhalte der Vorlesungen Einführung in die Kryptographie 1 und 2

LITERATUR: Katz, Lindell, "Introduction to Modern Cryptography", Chapman & Hall/CRC, 2008

Einführung in die Usable Security and Privacy

MODULNUMMER: 211036

KÜRZEL: eUSP

MODULBEAUFTRAGTER: Prof. Dr. Martina Angela Sasse

DOZENT: Prof. Dr. Angela Sasse

FAKULTÄT: Fakultät für Informatik

SPRACHE: Deutsch

SWS: 3 SWS

CREDITS: 4 CP

WORKLOAD:

ANGEBOTEN IM: jedes Sommersemester

BESTANDTEILE UND VERANSTALTUNGSART:

LERNZIELE: 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 FÜR CREDITS: Bestandene Modulabschlussprüfung

VORAUSSETZUNGEN: Keine

VORKENNTNISSE: Allgemeine Kenntnisse der IT-Sicherheit

SONSTIGE INFORMATIONEN: Den Moodle-Kurs für diese Veranstaltung finden sie unter folgendem Link: https://?moodle.?ruhr-uni-bochum.?de/?m/?course/?view.?php??id=39240

Kryptographie

MODULNUMMER: 150312

KÜRZEL: Krypto

MODULBEAUFTRAGTER: Prof. Dr. Alexander May

DOZENT: Prof. Dr. Alexander May

FAKULTÄT: Fakultät für Informatik

SPRACHE: Deutsch

SWS: 6 SWS

CREDITS: 8 CP

WORKLOAD: 240 h

ANGEBOTEN IM: jedes Wintersemester

BESTANDTEILE UND VERANSTALTUNGSART: a) Vorlesung Kryptographie (150312) b) Übung (150313)

LERNZIELE: 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. ? 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 FÜR CREDITS: Bestandene Modulabschlussprüfung

VORAUSSETZUNGEN: Keine

VORKENNTNISSE: Keine

LITERATUR: Katz, Lindell, "Introduction to Modern Cryptography", Chapman und Hall/CRC, 2008

SONSTIGE INFORMATIONEN: Diese Veranstaltung ist im Vorlesungsverzeichnis der Mathematik als "Kryptographie I + II" aufgeführt.

Tutorium

MODULNUMMER: 140000

KÜRZEL: TUTO

MODULBEAUFTRAGTER: M. SC. Jan Richter-Brockmann

DOZENT: Friederike Kogelheide Tutoren

FAKULTÄT: Fakultät für Elektrotechnik und Informationstechnik

SPRACHE: Deutsch

SWS: 2

CREDITS:

WORKLOAD:

ANGEBOTEN IM: jedes Wintersemester

BESTANDTEILE UND VERANSTALTUNGSART:

LERNZIELE: Den Studierenden wird der Einstieg in das Studium erleichtert. Sie sind über inhalt- ¨ liche und administrative Zusammenh¨ange informiert, haben Lerngruppen gebildet und haben verschiedene Kompetenzen der Lehrveranstaltungen der ersten Studiensemester vertieft.

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

VORAUSSETZUNGEN FÜR CREDITS: Keine

VORAUSSETZUNGEN: Keine

VORKENNTNISSE: Bereitschaft zur aktiven Mitarbeit und zur Gestaltung des eigenen Studienverlaufs

VERTIEFUNGSMODULE

Model Checking

MODULNUMMER: 211000

KÜRZEL: ModCh

MODULBEAUFTRAGTER: Prof. Dr. Thomas Zeume

DOZENT: Prof. Dr. Thomas Zeume

FAKULTÄT: Fakultät für Informatik

SPRACHE: Deutsch

SWS: 4

CREDITS: 5

WORKLOAD:

ANGEBOTEN IM: jedes Sommersemester

BESTANDTEILE UND VERANSTALTUNGSART:

LERNZIELE: 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 FÜR CREDITS: Bestandene Modulabschlussprüfung

VORAUSSETZUNGEN: keine

VORKENNTNISSE: - Grundlagenvorlesungen Mathematik - Hilfreich: Logik in der Informatik, Datenstrukturen und elementare Programmierkenntnisse

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

Digitale Forensik

MODULNUMMER: 211017

KÜRZEL: DiFo

MODULBEAUFTRAGTER: Dr. rer. nat. Christofer Fein

DOZENT: Studiendekan IT-Sicherheit

FAKULTÄT: Fakultät für Informatik

SPRACHE: Deutsch

SWS: 4 SWS

CREDITS: 5 CP

WORKLOAD:

ANGEBOTEN IM: jedes Wintersemester

BESTANDTEILE UND VERANSTALTUNGSART:

LERNZIELE: 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 FÜR CREDITS: Bestandene Modulabschlussprüfung

VORAUSSETZUNGEN: Keine

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

Einführung in die asymmetrische Kryptanalyse (nicht im SoSe 22)

MODULNUMMER: 211018

KÜRZEL: AsKryp

MODULBEAUFTRAGTER: Prof. Dr. Alexander May

DOZENT: Prof. Dr. Alexander May

FAKULTÄT: Fakultät für Informatik

SPRACHE: Deutsch

SWS: 4 SWS

CREDITS: 5 CP

WORKLOAD:

ANGEBOTEN IM: jedes Sommersemester

BESTANDTEILE UND VERANSTALTUNGSART:

LERNZIELE: 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 FÜR CREDITS: Bestandene Modulabschlussprüfung

VORAUSSETZUNGEN: Keine

VORKENNTNISSE: Inhalte der Vorlesungen Einführung in die Kryptographie 1 und 2

LITERATUR: https://www.cits.ruhr-uni-bochum.de/lehre/sose2021/sose2021-kryptanalyse.html

SONSTIGE INFORMATIONEN: Zur Vorlesung existiert ein Skript.

Logik in der Informatik

MODULNUMMER: 212013

KÜRZEL: LogCS

MODULBEAUFTRAGTER: Prof. Dr. Thomas Zeume

DOZENT: Prof. Dr. Thomas Zeume

FAKULTÄT: Fakultät für Informatik

SPRACHE: Deutsch

SWS: 4 SWS

CREDITS: 5 CP

WORKLOAD: 150h

ANGEBOTEN IM: jedes Wintersemester

BESTANDTEILE UND VERANSTALTUNGSART: Bis WS 22/23 wurde die Veranstaltung im SS angeboten.

LERNZIELE: 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 FÜR CREDITS: Bestandene Modulabschlussprüfung

VORAUSSETZUNGEN: Mathematik Grundlagenvorlesungen

VORKENNTNISSE: Mathematik Grundlagenvorlesungen

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

Boolesche Funktionen mit Anwendungen in der Kryptographie

MODULNUMMER: 211020

KÜRZEL: BooFu

MODULBEAUFTRAGTER: Prof. Dr. Gregor Leander

DOZENT: Prof. Dr. Gregor Leander

FAKULTÄT: Fakultät für Informatik

SPRACHE: Deutsch

SWS: 4 SWS

CREDITS: 5 CP

WORKLOAD:

ANGEBOTEN IM: jedes Sommersemester

BESTANDTEILE UND VERANSTALTUNGSART:

LERNZIELE: 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 FÜR CREDITS: Bestandene Modulabschlussprüfung

VORAUSSETZUNGEN: Keine

VORKENNTNISSE: Grundlegende Kenntnisse über endliche Körper

LITERATUR: Wir orientieren uns in der Vorlesung an den beiden Kapiteln von Claude Carlet über Boolesche Funktionen. Diese kann man online finden unter: http://?www.?math.?univ-paris13.?fr/?~carlet/chap-fcts-Bool-corr.?pdf und http://?www.?math.?univ-paris13.?fr/?~carlet/chap-vectorial-fcts-corr.?pdf

Implementierung Kryptographischer Verfahren

MODULNUMMER: 212020

KÜRZEL: ImKrVe

MODULBEAUFTRAGTER: DR.-ING. Pascal Sasdrich

DOZENT: Prof. Dr. Tim Güneysu

FAKULTÄT: Fakultät für Informatik

SPRACHE: Deutsch

SWS: 4 SWS

CREDITS: 5 CP

WORKLOAD:

ANGEBOTEN IM: jedes Wintersemester

BESTANDTEILE UND VERANSTALTUNGSART:

LERNZIELE: Studierende erlernen die grundlegenden Algorithmen für die effiziente Implementierung re-chen¬intensiver Kryptoverfahren. Insbesondere den Umgang von Algorithmen mit sehr langen Operanden haben sie nach Abschluss des Moduls verstanden, ebenso wie das Zusammen¬spiel von Implementierungs-methoden 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 be-handelt, 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 Metho-den 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-Algorith-mus wird die Montgomery-Multiplikation behandelt. Im dritten Teil werden sichere Implementierungen be-sprochen. 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 Grundla-gen 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 Nach-schreibetermin 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 (SoSe22: Deadline 15.04.22).

VORAUSSETZUNGEN FÜR CREDITS: Bestandene Modulabschlussprüfung

VORAUSSETZUNGEN: Keine

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

Kryptographie auf hardwarebasierten Plattformen

MODULNUMMER: 212019

KÜRZEL: KaH

MODULBEAUFTRAGTER: M. SC. Jan Richter-Brockmann

DOZENT: Prof. Dr.-Ing. Tim Güneysu, B. Sc. Johannes Mono, M. Sc. Jan Richter-Brockmann

FAKULTÄT: Fakultät für Informatik

SPRACHE: Deutsch

SWS: 4 SWS

CREDITS: 5 CP

WORKLOAD: 150 Stunden

ANGEBOTEN IM: jedes Wintersemester

BESTANDTEILE UND VERANSTALTUNGSART:

LERNZIELE: 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 FÜR CREDITS: Bestandene Modulabschlussprüfung

VORAUSSETZUNGEN: Keine

VORKENNTNISSE: Die Vorlesung baut auf Grundlagenstoff der folgenden Vorlesungen auf: 1. Grundlagen der Kryptographie und Datensicherheit 2. Basiswissen Digitaltechnik

LITERATUR: Rodriguez-Henriquez F., Saqib, N.A., DiazPerez A., Koc, C.K.: Cryptographic Algorithms on Reconfigurable Hardware, Springer Verlag, ISBN: 0-387-33883-7 Weitere Literatur ist im Skript zur Vorlesung (Vorversion) angegeben, welches über das Blackboard verfügbar ist.

Web- und Browsersicherheit

MODULNUMMER: 212061

KÜRZEL: WebBroSec

MODULBEAUFTRAGTER: Dr.-Ing. Mario Heiderich

DOZENT:

FAKULTÄT: Fakultät für Informatik

SPRACHE: Deutsch

SWS: 4 SWS

CREDITS: 5 CP

WORKLOAD:

ANGEBOTEN IM: jedes Wintersemester

BESTANDTEILE UND VERANSTALTUNGSART:

LERNZIELE: 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

VORAUSSETZUNGEN FÜR CREDITS: Bestandene Modulabschlussprüfung

Einführung ins Hardware Reverse Engineering

MODULNUMMER: 212025

KÜRZEL: HaReEng

MODULBEAUFTRAGTER: M.Sc. Steffen Becker

DOZENT:

FAKULTÄT: Fakultät für Informatik

SPRACHE: Englisch

SWS: 4 SWS

CREDITS: 5 CP

WORKLOAD:

ANGEBOTEN IM: jedes Wintersemester

BESTANDTEILE UND VERANSTALTUNGSART:

LERNZIELE: 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. Des Weiteren 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

VORAUSSETZUNGEN FÜR CREDITS: Bestandene Modulabschlussprüfung und erfolgreiche Teilnahme an den praktischen Übungen am Rechner

VORAUSSETZUNGEN: Keine

VORKENNTNISSE: Inhalte der Vorlesungen Technische Informatik 1 - Rechnerarchitektur und Technische

Informatik 2 - Digitaltechnik.

SONSTIGE INFORMATIONEN: Die Modulprüfung ist in eine schriftliche Klausur (max. 60%) und mehrere vorlesungsbegleitende Projekte (max. 40%) aufgeteilt. Zusätzlich können bis zu 5% Bonus erworben und insgesamt maximal 100% erreicht werden. Zur Bearbeitung der Projekte wird ein PC mit ca. 15GB verfügbarem Festplattenspeicher benötigt. Setzen Sie sich bitte mit den Dozenten in Verbindung, falls Sie keinen PC zur Verfügung haben.

Implementation of Cryptographic Schemes

MODULNUMMER: 141024

KÜRZEL: ImKrVe

MODULBEAUFTRAGTER: Prof. Dr.-Ing. Christof Paar

DOZENT: Dr.-Ing. Falk Schellenberg

FAKULTÄT: Fakultät für Informatik

SPRACHE: Deutsch

SWS: 4 SWS

CREDITS: 5 CP

WORKLOAD:

ANGEBOTEN IM: each winter semester

BESTANDTEILE UND VERANSTALTUNGSART:

LERNZIELE: The students have an understanding of methods for fast and secure implementation of symmetric and asymmetric cryptography.

INHALT: The first two topics are algorithms for efficient implementation of asymmetric cryptography. These include algorithms for fast exponentiation as well as data structures and algorithms for multiple precision arithmetic. The third topic of the lecture covers implementation attacks with focus on fault injection and differential power analysis (DPA). As a part of the lecture there will be projects in which the learned algorithms have to be implemented. The final grade is made up of a written exam (70%) and programming projects (30%) (also for the additional exam in the summer term). Students willing to work on the projects in the summer term are required to contact falk.?schellenberg@?rub.?de per mail within the first two weeks of the lecture period (summer term 2022: deadline 15.04.22).

VORAUSSETZUNGEN FÜR CREDITS: Bestandene Modulabschlussprüfung

VORAUSSETZUNGEN: None

VORKENNTNISSE: - Basic knowledge in cryptography - Basic knowledge in the programming languages C or C++

Datenschutz

MODULNUMMER: 260081

KÜRZEL: D

MODULBEAUFTRAGTER: Dr. Kai-Uwe Loser

DOZENT: Dr. Kai-Uwe Loser

FAKULTÄT: Institut für Arbeitswissenschaften

SPRACHE: Deutsch

SWS: 3 SWS

CREDITS: 5 CP

WORKLOAD: 150h

ANGEBOTEN IM: jedes Wintersemester

BESTANDTEILE UND VERANSTALTUNGSART:

LERNZIELE: Datenschutz befasst sich mit der Frage, wie man Bürger, Arbeitnehmer, Kunden, Patienten etc. vor negativen Auswirkungen durch die Verarbeitung von 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 Prinzipien des Datenschutzrechtes und den praktischen Auswirkungen für Informatiker. Dabei wird vor allem Wert darauf gelegt, diese zentralen Prinzipien verstehbar zu machen. Neben dem Datenschutzgrundverordnung werden auch Spezialregelungen behandelt, die z.B. für die Regulierung der Telekommunikation, oder für den Einsatz elektronischer Datenverarbeitung in der Arbeitswelt zum Einsatz kommen. Die DSGVO ist inzwischen auch über den europäischen Raum hinaus ein akzeptierter Standard. Unterschiedliche Rechtsphilosophische Betrachtungen werden thematisiert, um zu vermitteln, wo international Sichtweisen und Fragestellunegn divergieren. Insgesamt wird das Thema konstruktiv betrachtet: das Thema Privacy by Design, wird auf allen Ebenen betrachtet. 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. Nach dem erfolgreichen Abschluss des Moduls ? kennen Studierende die Grundzüge des Datenschutzrechtes, ? verstehen Studierende die gesellschaftlichen Hintergründe, ? können Datenverarbeitungsprozesse hinsichtlich der Relevanz des Datenschutzrechts analysieren und ? können Lösungsmuster anwenden um Systeme datenschutzfreundlich und datenschutzrechtskonform zu gestalten.

INHALT: ? Was ist Datenschutz, informationelle Selbstbestimmung und Privacy? ? Welche Folgen haben Verarbeitungen personenbezogener Daten? Woher entstehen diese Folgen? ? Was sind die Prinzipien des Datenschutzes ? Welche Rechte haben die von der Verarbeitung betroffenen Personen? ? Was passiert mit personenbezogenen Daten in vernetzten Systemen? ? Welche organisatorischen und technischen Maßnahmen helfen, personenbezogene Daten zu sichern? ? Was ist Privacy by Design und wie kann das umgesetzt werden? ? Spezielle Bereiche der Datenverarbeitung: Telekommunikation, Wirtschaft, Medizin

VORAUSSETZUNGEN FÜR CREDITS: Bestandene Modulabschlussprüfung

VORAUSSETZUNGEN: Keine

VORKENNTNISSE: Keine

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

Web-Sicherheit

MODULNUMMER: 141245

KÜRZEL: WS

MODULBEAUFTRAGTER: Prof. Dr. Jörg Schwenk

DOZENT: Prof. Dr. Jörg Schwenk Dr.-Ing. Dennis Felsch M. Sc. Dominik Noß

FAKULTÄT: Fakultät für Informatik

SPRACHE: Deutsch

SWS: 4

CREDITS: 5

WORKLOAD: 150 Stunden

ANGEBOTEN IM: unregelmäßig

BESTANDTEILE UND VERANSTALTUNGSART:

LERNZIELE: 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 Si gnature * 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 FÜR CREDITS: Keine

VORAUSSETZUNGEN: Keine

VORKENNTNISSE: Grundkenntnisse Kryptographie und HTML

Elliptische Kurven und Kryptographie (nicht im WiSe 22/23)

MODULNUMMER: 150347

KÜRZEL: EKK

MODULBEAUFTRAGTER: Prof. Dr. Eike Kiltz

DOZENT: Prof. Dr. Alexander May

FAKULTÄT: Fakultät für Informatik

SPRACHE: Deutsch

SWS: 4

CREDITS: 5

WORKLOAD: 150 Stunden

ANGEBOTEN IM: unregelmäßig

BESTANDTEILE UND VERANSTALTUNGSART:

LERNZIELE: 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 Schlusselaustausch, ElGamal Ver- Schlüsselung, DSA Signaturen ¨ • Berechnung des diskreten Logarithmus • Bilineare Abbildungen über elliptischen Kurve

VORAUSSETZUNGEN FÜR CREDITS: Keine

VORAUSSETZUNGEN: Keine

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

PRAKTISCHE VERTIEFUNG

Bachelor-Seminar Netz- und Datensicherheit

MODULNUMMER: 212121

KÜRZEL: NDS

MODULBEAUFTRAGTER: Prof. Dr. Jörg Schwenk

DOZENT: Prof. Dr. Jörg Schwenk, M. Sc. Matthias Gierlings

FAKULTÄT: Fakultät für Informatik

SPRACHE: Deutsch

SWS: 3 SWS

CREDITS: 3 CP

WORKLOAD:

ANGEBOTEN IM: jedes Semester

BESTANDTEILE UND VERANSTALTUNGSART:

LERNZIELE: 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/?

VORAUSSETZUNGEN FÜR CREDITS: Bestandene schriftliche und mündliche Prüfung

VORAUSSETZUNGEN: Keine

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

LITERATUR: Musterlösungen: - 08.?02.?2016 - Exposé (Beispiel 1) (https://www.nds.ruhr-uni-bochum.de/media/ei/lehrmaterialien/23/f40dce41131f2e2ff888f29afedfb76e4ad2be0a/Expose.pdf) - 10.?02.?2016 - Exposé (Beispiel 2) (https://www.nds.ruhr-uni-bochum.de/media/ei/lehrmaterialien/23/d02022011580dfa24808afebcbb69f22c8c2760f/Expose%20Mobile%20Money%20-%20Mobile%20Problems.pdf) - 10.?02.?2016 - Präsentation (Beispiel) (https://www.nds.ruhr-uni-bochum.de/media/ei/lehrmaterialien/290/66a4c2fcccf594e1fcdedf4278fd3fa69309beef/Pr%C3%A4sentation%20-%20Brendel%2C%20Sascha.pdf)

AKTUELLE INFORMATIONEN: siehe: https://informatik.rub.de/nds/teaching/courses/seminar/

Bachelor-Praktikum zur Hackertechnik

MODULNUMMER: 212413

KÜRZEL: BPH

MODULBEAUFTRAGTER: Prof. Dr. Jörg Schwenk

DOZENT: Prof. Dr. Jörg Schwenk, M. Sc. Lukas Knittel

FAKULTÄT: Fakultät für Informatik

SPRACHE: Deutsch

SWS: 3 SWS

CREDITS: siehe Prüfungsordnung

WORKLOAD:

ANGEBOTEN IM: jedes Semester

BESTANDTEILE UND VERANSTALTUNGSART:

LERNZIELE: 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 FÜR CREDITS: Bestandenes Praktikum

VORAUSSETZUNGEN: Keine

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

AKTUELLE INFORMATIONEN: siehe: https://informatik.rub.de/nds/teaching/hackerpraktikum/

Bachelor-Praktikum TLS Implementierung

MODULNUMMER: 212414

KÜRZEL: BPTLS

MODULBEAUFTRAGTER: Prof. Dr. Jörg Schwenk

DOZENT: Prof. Dr. Jörg Schwenk,, M. Sc. Marcel Maehren, M. Sc. Nurullah Erinola

FAKULTÄT: Fakultät für Informatik

SPRACHE: Deutsch

SWS: 3 SWS

CREDITS: siehe Prüfungsordnung

WORKLOAD:

ANGEBOTEN IM: jedes Wintersemester

BESTANDTEILE UND VERANSTALTUNGSART:

LERNZIELE: 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

VORAUSSETZUNGEN FÜR CREDITS: Bestandenes Praktikum

VORAUSSETZUNGEN: Keine

VORKENNTNISSE: - Erfolgreicher Abschluss der Lehrveranstaltung Netzsicherheit 2 - Programmierkenntnisse in Java

LITERATUR: Referenzen: - Robert Cecil Martin: Clean Code: Refactoring, Patterns, Testen und Techniken für sauberen Code - RFC 8446: The Transport Layer Security (TLS) Protocol Version 1.3 (https://?tools.?ietf.?org/?html/?rfc8446)

AKTUELLE INFORMATIONEN: Siehe: https://informatik.rub.de/nds/teaching/courses/praktikum-tls/

SONSTIGE INFORMATIONEN: Die Veranstaltung wird Vollständig Online/über Zoom durchgeführt. Details werden über Moodle bekannt gegeben.

Bachelor-Praktikum ARM Processors for Embedded Cryptography

MODULNUMMER: 212407

KÜRZEL: ARM

MODULBEAUFTRAGTER: Dr.-Ing. Max Hoffmann

DOZENT: Prof. Dr.-Ing. Tim Güneysu, Dr.-Ing. Max Hoffmann

FAKULTÄT: Fakultät für Informatik

SPRACHE: Deutsch

SWS: 3 SWS

CREDITS: siehe Prüfungsordnung

WORKLOAD:

ANGEBOTEN IM: jedes Wintersemester

BESTANDTEILE UND VERANSTALTUNGSART:

LERNZIELE: 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 FÜR CREDITS: Bestandenes Praktikum

VORAUSSETZUNGEN: Keine

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

Bachelor-Seminar Usable Security and Privacy Research

MODULNUMMER: 141033

KÜRZEL: BSUsSec

MODULBEAUFTRAGTER: Prof. Dr. Markus Dürmuth

DOZENT: Prof. Dr. Markus Dürmuth, M. Sc. Philipp Markert

FAKULTÄT: Fakultät für Informatik

SPRACHE: Deutsch

SWS: 3 SWS

CREDITS: 4 CP

WORKLOAD:

ANGEBOTEN IM: jedes Semester

BESTANDTEILE UND VERANSTALTUNGSART:

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

INHALT: Das Seminar behandelt insbesondere folgende Themen: Einführung: Überblick Motivation Themen und Forschungsmethoden Wissenschaftliche Praxis: Reviews für Paper Rebuttals und Meta-Reviews PC Meeting Konferenztag Zentrale Themen. Zentrale Fragestellungen und angewandte Methoden der benutzbaren IT-Sicherheit. Wissenschaftliche Publikationspraxis: Von der Einreichung, über die Auswahl von Beiträgen bis zur Vorstellung auf einer Konferenz

VORAUSSETZUNGEN FÜR CREDITS: Bestandener Seminarbeitrag

VORAUSSETZUNGEN: Keine

VORKENNTNISSE: Keine

SONSTIGE INFORMATIONEN: Die Seminarthemen der Arbeitsgruppe werden über die Webseite der zentralen Seminarvergabe (https://?seminar.?hgi.?rub.?de) vergeben. Dort befinden sich ebenfalls weitere Informationen zur Bedienung und zum Auswahlverfahren. Der Anmeldezeitraum wird über die RUB-Mailingliste its-announce bekannt gegeben. Die Nutzung der zentralen Seminarvergabe ist Voraussetzung für die Vergabe eines Themas sowie für die erfolgreiche Teilnahme am Seminar. Die Vorbesprechung wird online in der ersten oder zweiten Vorlesungswoche stattfinden. Weitere Details erhalten die Studierenden rechtzeitig per Mail.

Bachelor-Forschungspraktikum Human-Centred Security

MODULNUMMER: 212408

KÜRZEL: BPHCS

MODULBEAUFTRAGTER: Prof. Dr. Martina Angela Sasse

DOZENT: Prof. Dr. Martina Angela Sasse, Markus Schöps

FAKULTÄT: Fakultät für Informatik

SPRACHE: Deutsch

SWS: 3 SWS

CREDITS: siehe Prüfungsordnung

WORKLOAD:

ANGEBOTEN IM: jedes Semester

BESTANDTEILE UND VERANSTALTUNGSART:

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

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

VORAUSSETZUNGEN FÜR CREDITS: Bestandenes Praktikum

VORAUSSETZUNGEN: Keine

VORKENNTNISSE: - Usable Security and Privacy - Human-Centred Security - Allgemeine Kenntnisse der IT-Sicherheit

SONSTIGE INFORMATIONEN: Die Zahl der Teilnehmenden ist limitiert. Eine Voranmeldung und Platzreservierung per E-Mail an markus.schoeps@ruhr-uni-bochum.de ist daher zwischen dem 22.09.22 und dem 18.10.22 (23.59 Uhr) dringend erforderlich. Anmeldung bitte mit folgenden Angaben: - Name - Email-Adresse - Studiengang + Matrikelnummer - Vorkenntnisse im Bereich Usable/Human-Centred Security and Privacy Alle weiteren Details werden am Vorbesprechungstermin geklärt.

Bachelor-Seminar Security Engineering

MODULNUMMER: 212112

KÜRZEL: BSSE

MODULBEAUFTRAGTER: Prof. Dr.-Ing. Tim Güneysu

DOZENT: Prof. Dr.-Ing. Tim Güneysu, M. Sc. Anna Guinet

FAKULTÄT: Fakultät für Informatik

SPRACHE: Deutsch

SWS: 3 SWS

CREDITS: 3 CP

WORKLOAD:

ANGEBOTEN IM: jedes Semester

BESTANDTEILE UND VERANSTALTUNGSART:

LERNZIELE: 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.

VORAUSSETZUNGEN FÜR CREDITS: Bestandener Seminarbeitrag

VORKENNTNISSE: - 'Einführung in die Kryptographie' - 'Grundlagen der Netz- und Systemsicherheit'

SONSTIGE INFORMATIONEN: Alle Seminarthemen des Lehrstuhls werden über die Website der zentralen Seminarvergabe vergeben. Dort befinden sich ebenfalls weitere Informationen zur Bedienung und zum Auswahlverfahren (https://informatik.rub.de/seceng/lehre/seminare/seminar_ws_2022).

Bachelor-Projekt Netz- und Datensicherheit

MODULNUMMER: 212412

KÜRZEL: BPNDS

MODULBEAUFTRAGTER: Prof. Dr. Jörg Schwenk

DOZENT: Prof. Dr. Jörg Schwenk, Matthias Gierlings

FAKULTÄT: Fakultät für Informatik

SPRACHE: Deutsch

SWS: 3 SWS

CREDITS: siehe Prüfungsordnung

WORKLOAD:

ANGEBOTEN IM: jedes Semester

BESTANDTEILE UND VERANSTALTUNGSART:

LERNZIELE: 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 FÜR CREDITS: Bestandene Projektarbeit

VORAUSSETZUNGEN: Keine

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

SONSTIGE INFORMATIONEN: Die Themenvergabe für dieses Projekt erfolgt jederzeit nach individueller Absprache mit den Mitarbeitern des Lehrstuhls bzw. mit Herrn Gierlings (matthias.gierlings@ruhr-uni-bochum.de)

Praktikum zur Kryptanalyse

MODULNUMMER: 211006

KÜRZEL: PZK

MODULBEAUFTRAGTER: Prof. Dr. Alexander May

DOZENT: Prof. Dr. Alexander May

FAKULTÄT: Fakultät für Informatik

SPRACHE: Deutsch

SWS: 2

CREDITS: 3

WORKLOAD: 90 Stunden

ANGEBOTEN IM: jedes Wintersemester

BESTANDTEILE UND VERANSTALTUNGSART:

LERNZIELE: Nach dem erfolgreichen Abschluss des Praktikums • kennen die Studierenden die bekanntesten und 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 FÜR CREDITS: Keine

VORAUSSETZUNGEN: Keine

VORKENNTNISSE: Gute bis sehr gute Kenntnisse in den Programmiersprachen C oder C++

Seminar zur Real World Cryptoanalysis

MODULNUMMER: 150560

KÜRZEL: SRWC

MODULBEAUFTRAGTER: Prof. Dr. Alexander May

DOZENT: Prof. Dr. Alexander May

FAKULTÄT: Fakultät für Informatik

SPRACHE: Deutsch

SWS: 2

CREDITS: 4

WORKLOAD: 120 Stunden

ANGEBOTEN IM: jedes Semester

BESTANDTEILE UND VERANSTALTUNGSART:

LERNZIELE: 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

VORAUSSETZUNGEN FÜR CREDITS: Keine

VORAUSSETZUNGEN: Keine

VORKENNTNISSE: Ein allgemeines Verst¨andnis von IT-Sicherheit ist hilfreich. Weiterhin sind, je nach Thema, Inhalte nutzlich, wie sie etwa in den Vorlesungen Kryptographie ¨ I + II und Kryptoanalyse vermittelt werden. In der Regel lassen sich aber Themen abh¨angig von bereits besuchten Veranstaltungen finden.

Seminar Satisfiability

MODULNUMMER: 150562

KÜRZEL: SS

MODULBEAUFTRAGTER: Prof. Dr. Thomas Zeume

DOZENT: Prof. Dr. Thomas Zeume

FAKULTÄT: Fakultät für Informatik

SPRACHE: Deutsch

SWS: 2

CREDITS: 3

WORKLOAD: 90 Stunden

ANGEBOTEN IM: jedes Wintersemester

BESTANDTEILE UND VERANSTALTUNGSART:

LERNZIELE: siehe Inhalt

INHALT: Das Erfüllbarkeitsproblem für logische Formeln — lasst 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 schwierigen Probleme: Jedes Problem aus NP lässt sich auf SAT zurückfuhren, 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.

VORAUSSETZUNGEN FÜR CREDITS: Keine

VORAUSSETZUNGEN: Keine

VORKENNTNISSE: Keine

AKTUELLE INFORMATIONEN: Das Seminar entfällt im WS 22/23

Seminar zur Kryptographie

MODULNUMMER: 150537

KÜRZEL: SK

MODULBEAUFTRAGTER: Prof. Dr. Gregor Leander

DOZENT: Prof. Dr. Gregor Leander

FAKULTÄT: Fakultät für Informatik

SPRACHE: Deutsch

SWS: 2

CREDITS: 3

WORKLOAD: 90 Stunden

ANGEBOTEN IM: jedes Sommersemester

BESTANDTEILE UND VERANSTALTUNGSART:

LERNZIELE: Die Studierenden können sich selbständig Originalarbeiten aus dem Bereich Kryptographie aneignen, und wissenschaftliche Ergebnisse präsentieren.

INHALT: Aktuelle Forschungsarbeiten der wichtigsten Kryptographie-Konferenzen

VORAUSSETZUNGEN FÜR CREDITS: Keine

VORAUSSETZUNGEN: Keine

VORKENNTNISSE: Inhalte des Moduls “Kryptographie”

Seminar über Grenzen in der theoretischen Informatik

MODULNUMMER: 150520

KÜRZEL: SUGTI

MODULBEAUFTRAGTER: Prof. Dr. Thomas Zeume

DOZENT: Prof. Dr. Thomas Zeume

FAKULTÄT: Fakultät für Informatik

SPRACHE: Deutsch

SWS: 2

CREDITS: 3

WORKLOAD: 90 Stunden

ANGEBOTEN IM: jedes Sommersemester

BESTANDTEILE UND VERANSTALTUNGSART:

LERNZIELE: 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?

VORAUSSETZUNGEN FÜR CREDITS: Keine

VORAUSSETZUNGEN: Keine

VORKENNTNISSE: Keine

Fortgeschrittene Themen des Model Checking

MODULNUMMER: 150521

KÜRZEL: FTMC

MODULBEAUFTRAGTER: Prof. Dr.-Ing. Dorothea Kolossa

DOZENT: Prof. Dr. Thomas Zeume

FAKULTÄT: Institut für Kommunikationsakustik

SPRACHE: Deutsch

SWS: 2

CREDITS: 3

WORKLOAD: 90 Stunden

ANGEBOTEN IM: jedes Sommersemester

BESTANDTEILE UND VERANSTALTUNGSART:

LERNZIELE: In der Veranstaltung Model Checking haben wir die theoretischen Grundlagen des Model Checkings kennen gelernt. Insbesondere haben wir die Spezifikationssprachen LTL und CTL eingefuhrt, ihre Ausdrucksst ¨ ¨arke untersucht, und die wichtigsten algorithmischen Ans¨atze fur 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 FÜR CREDITS: Keine

VORAUSSETZUNGEN: Keine

VORKENNTNISSE: Veranstaltung “Model Checking”

Seminar zur symmetrischen Kryptographie

MODULNUMMER: 212118

KÜRZEL: SSK

MODULBEAUFTRAGTER: Prof. Dr. Gregor Leander

DOZENT: Prof. Dr. Gregor Leander

FAKULTÄT: Fakultät für Informatik

SPRACHE: Deutsch

SWS: 2

CREDITS: 3

WORKLOAD: 90 Stunden

ANGEBOTEN IM: jedes Sommersemester

BESTANDTEILE UND VERANSTALTUNGSART:

LERNZIELE: 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 FÜR CREDITS: Keine

VORAUSSETZUNGEN: Keine

VORKENNTNISSE: Inhalte des Moduls “Kryptographie” hilfreich

Bachelor-Seminar Aktuelle Themen der IT-Sicherheit

MODULNUMMER: 143243

KÜRZEL: BSATITS

MODULBEAUFTRAGTER: Prof. Dr. Thorsten Holz

DOZENT: Prof. Dr. Thorsten Holz

FAKULTÄT: Fakultät für Informatik

SPRACHE: Deutsch

SWS: 3

CREDITS: 3

WORKLOAD: 90 Stunden

ANGEBOTEN IM: unregelmäßig

BESTANDTEILE UND VERANSTALTUNGSART:

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

INHALT: In jedem Semester bietet der Lehrstuhl ein Bachelor-Seminar zum Thema “Aktuelle Themen der IT-Sicherheit” an, der Fokus liegt auf den Bereichen Softwaresicherheit, Netzwerksicherheit, Privacy, Reverse Engineering und ähnlichen Themen aus dem Bereich der systemnahen IT-Sicherheit. Dazu sollen die Studierenden selbständig ein eng umfasstes Themengebiet bearbeiten und eine Ausarbeitung sowie einen Vortrag zu diesem Thema verfassen. Die Ausarbeitung hat einen Umfang von etwa 15 Seiten und der Vortrag soll etwa 20 Minuten dauern. Daran schließt sich eine Diskussion von 5 Minuten an. Das Seminar wird als Konferenzseminar durchgeführt, der Ablauf ist ähnlich zu einer wissenschaftlichen Konferenz. Neben dem Erstellen einer wissenschaftlichen Ausarbeitung lernen die Studierenden das Peer-Review-Verfahren kennen: Ein wichtiger Aspekt des Seminars ist die Erstellung von konstruktiven Feedbacks zur Ausarbeitung anderer Studierender, zum Beispiel durch Hinweise zur Verbesserung der Darstellung. Ein solches Feedback soll dann auch in der eigenen Ausarbeitung berücksichtigt und eingearbeitet werden.

VORAUSSETZUNGEN FÜR CREDITS: Keine

VORAUSSETZUNGEN: Keine

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

Bachelor-Vertiefungspraktikum SAGE in der Kryptographie

MODULNUMMER: 150583

KÜRZEL: BVPSK

MODULBEAUFTRAGTER: Prof. Dr. Gregor Leander

DOZENT: Prof. Dr. Gregor Leander

FAKULTÄT: Fakultät für Informatik

SPRACHE: Deutsch

SWS: 2

CREDITS:

WORKLOAD:

ANGEBOTEN IM: unregelmäßig

BESTANDTEILE UND VERANSTALTUNGSART:

LERNZIELE: 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 FÜR CREDITS: Keine

VORAUSSETZUNGEN: Grundkenntnisse über Kryptographie, wie sie zum Beispiel in der ¨ “Einführung in die Kryptographie I und II” behandelt werden, sind hilfreich, aber nicht nötig

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

FREIES WAHLFACH

Freie Veranstaltungswahl

MODULNUMMER: keine

KÜRZEL: FVW

MODULBEAUFTRAGTER: Siehe den jew. Eintrag im Vorlesungsverzeichnis

DOZENT: Studiendekan*in IT-Sicherheit

FAKULTÄT: Fakultät für Informatik

SPRACHE: beliebig

SWS:

CREDITS: je nach Veranstaltungswahl

WORKLOAD:

ANGEBOTEN IM: jedes Semester

BESTANDTEILE UND VERANSTALTUNGSART:

LERNZIELE: Innerhalb des Moduls setzen die Studierenden entsprechend ihrer Interessen verschiedene Schwerpunkte. Dafür steht Ihnen das breite Angebot der ganzen Universität zur Verfugung. 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. Aktuelle Informationen wie Vorlesungstermine, Räume oder aktuelle Dozent*innen und Übungsleiter*innen sind im Vorlesungsverzeichnis der Ruhr-Universität https://vvz.rub.de/ zu finden. Weiterhin ist auch der Besuch von Lehrveranstaltungen anderer Universitäten der UA Ruhr möglich, beispielsweise im Rahmen der Kooperationsvereinbarung mit der Technischen Universität Dortmund und mit der Universität Duisburg-Essen - siehe auch https://www.uaruhr.de/studium.html.de. Das Modul kann auch im Rahmen eines Auslandsstudiums belegt werden.

VORAUSSETZUNGEN FÜR CREDITS: Keine

VORAUSSETZUNGEN: entsprechend den Angaben zu der gewählten Veranstaltungen

VORKENNTNISSE: entsprechend den Angaben zu der gewählten Veranstaltungen

SONSTIGE INFORMATIONEN: Die Anzahl der insgesamt benötigten Credits für dieses Modul finden Sie in der Tabelle am Ende ihrer Prüfungsordnung (PO13, 20 oder 22).

INDUSTRIEPRAKTIKUM

Industriepraktikum ITS

MODULNUMMER: 212420

KÜRZEL: IndPrakITS

MODULBEAUFTRAGTER: Prof. Dr. Jörg Schwenk

DOZENT: Studiendekan*in IT-Sicherheit

FAKULTÄT: Fakultät für Informatik

SPRACHE: Deutsch

SWS: 450 Arbeitsstunden

CREDITS: 15 CP

WORKLOAD:

ANGEBOTEN IM: jedes Semester

BESTANDTEILE UND VERANSTALTUNGSART:

LERNZIELE: Mit dem Industriepraktikum gewinnen die Studierenden Einblicke in die spätere Berufstätigkeit, in die betrieblichen Arbeitsweisen und Sozialstrukturen. Sie lernen u.a. Prüf-, Entwurfs- und Entwicklungsmethoden sowie Verfahrens- und Betriebsaufgaben im Bereich der IT-Sicherheit kennen. Kommunikative und soziale Schlüsselqualifikationen sind aus dem Umgang mit Vorgesetzten und Teammitgliedern bekannt.

INHALT: Das Industriepraktikum soll vorrangig in Industriebetrieben, Dienstleistungsunternehmen und technischen Behörden abgeleistet werden, in denen Tätigkeiten im Bereich IT-Sicherheit durchgeführt werden. Die Betriebs- oder Gruppengröße spielt keine Rolle. Es muss eine verantwortliche Betreuerin bzw. ein verantwortlicher Betreuer das Praktikum begleiten. Eine Praktikantentätigkeit im eigenen Betrieb sowie im Betrieb von Verwandten oder der/des Lebenspartnerin/-s ist nicht zuläs¬sig. Der Gesamtumfang des Praktikums muss mindestens 450 Stunden betragen. Es dauert in der Regel drei Monate und kann in Teilzeit oder Vollzeit absolviert werden. Dies ist abhängig von der vereinbarten wöchentlichen Arbeitszeit. Eventuelle Fehltage z. B. durch Krankheit oder Betriebsurlaub sind genauso nachzuholen wie Fehltage durch gesetzliche Feiertage, sofern die geforderte Gesamtstundenzahl ansonsten nicht erreicht wird. Das Praktikum ist in der Regel in einem Betrieb und ohne Unterbrechung im sechsten Fachsemester durchzuführen. Eine Aufteilung auf mehrere Zeiträume bzw. verschiedene Betriebe ist jedoch prinzipiell zulässig. Die Durchführung des Praktikums im vollen Umfang und das Erstellen einer Dokumentation über die im Praktikum durchgeführten Tätigkeiten sind Bestandteil der Bachelorprüfung. Es handelt sich um ein Pflichtpraktikum.

VORAUSSETZUNGEN FÜR CREDITS: Siehe den jeweiligen Eintrag im Vorlesungsverzeichnis

VORAUSSETZUNGEN: Siehe Prüfungsordnung

VORKENNTNISSE: Entsprechend des Tätigkeitsbereichs der gewählten Firma

SONSTIGE INFORMATIONEN: Anmeldung über das Prüfungsamt der Fakultät für Informatik

ABSCHLUSSARBEIT

Bachelorarbeit ITS

MODULNUMMER: 144002

KÜRZEL: BITS

MODULBEAUFTRAGTER: Jede/r am Studiengang beteiligte Hochschullehrer*in

DOZENT: Studiendekan ITS

FAKULTÄT: Fakultät für Informatik

SPRACHE: Deutsch

SWS:

CREDITS: 12

WORKLOAD: 360 Stunden 3 Monate

ANGEBOTEN IM: jedes Semester

BESTANDTEILE UND VERANSTALTUNGSART:

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

INHALT: Lösung einer wissenschaftlichen Aufgabe unter Anleitung. Teilnahme an 5 Kolloquiumsvorträgen über die Ergebnisse von Bachelorarbeiten in der Fakultät ET & IT. Präsentation der eigenen Ergebnisse der Bachelorarbeit im Kolloquium. Abschlussarbeiten k¨onnen grunds¨atzlich bei allen Hochschullehrern der Fakult¨at und bei den am Studiengang beteiligten Hochschullehrern der Fakult¨at fur Mathematik angefertigt werden. ¨ Eine Ubersicht der Hochschullehrer der ¨ Fakult¨at fur Elektrotechnik und Informati- ¨ onstechnik befindet sich unter: https://www.ei.rub.de/fakultaet/professuren/ In der Fakult¨at fur Mathematik sind dies: ¨ • Lehrstuhl fur Kryptologie und IT-Sicherheit - Prof. May ¨ http://www.cits.rub.de • Lehrstuhl fur Kryptographie - Prof. Kiltz ¨ http://www.foc.rub.de/ • Arbeitsgruppe fur Symmetrische Kryptographie - Prof. Leander ¨ http://www.cits.rub.de/personen/index.html

VORAUSSETZUNGEN FÜR CREDITS: Keine

VORAUSSETZUNGEN: siehe Prüfungsordnung

VORKENNTNISSE: Vorkenntnisse entsprechend dem gewählten Thema erforderlich

Kolloquium ITS

MODULNUMMER: 144004

KÜRZEL: KITS

MODULBEAUFTRAGTER: Jede/r am Studiengang beteiligte Hochschullehrer*in

DOZENT: Studiendekan ITS

FAKULTÄT: Fakultät für Informatik

SPRACHE: Deutsch

SWS:

CREDITS: 3

WORKLOAD: 90 Stunden

ANGEBOTEN IM: jedes Semester

BESTANDTEILE UND VERANSTALTUNGSART:

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

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

VORAUSSETZUNGEN FÜR CREDITS: Keine

VORAUSSETZUNGEN: Anfertigung einer Bachelorarbeit

VORKENNTNISSE: Präsentationstechnik