

Modulhandbuch

Cybercrime/ Cybersecurity (M.Sc.)

Inhaltsverzeichnis

<i>MNR</i>	<i>MC</i>	<i>Modulbezeichnung</i>	<i>Seite</i>
7701	03-CCYB1	<u>Cybercrime I</u>	4
7702	03-CGDMF	<u>Grundlagen der Mobilfunkforensik</u>	5
7703	03-CDP	<u>Datenbankprogrammierung</u>	7
7704	03-CINVI	<u>Intelligente Videoanalyse</u>	8
7705	03-CIOT	<u>Internet of Things</u>	10
7706	03-STMOD	<u>Stochastic Models</u>	11
7707	03-CFOMC	<u>Foundations of Modern Cryptography</u>	13
7708	03-CCYB2	<u>Cybercrime II</u>	15
7709	03-CSVG	<u>Der Sachverständige vor Gericht</u>	16
7710	03-CSPR	<u>Softwarepraktikum</u>	17
7711	03-CDKPR	<u>Datenkompression</u>	18
7712	03-GFRE	<u>Geoforensik und Reverse Engineering</u>	20
7713	03-AITF-20	<u>Artificial Intelligence - Theory and Foundations</u>	21
7714	03-CCA	<u>Cryptanalysis</u>	22
7715	03-CSEO	<u>Social Engineering und OSINT</u>	24
7716	03-CKPFM	<u>Komplexpraktikum Forensische Methoden</u>	25
7717	03-CESS	<u>Entwurf sicherer Systeme</u>	26
7718	03-CDNCF-21	<u>Datennetze/ Cloud Forensik</u>	27
7719	03-CCF	<u>Car Forensics</u>	28
7720	03-CPPDF	<u>Predictive Policing/Dunkelfeld</u>	29
7721	03-CDWUG	<u>Digitale Werte und Güter</u>	31
7722	03-MPCY	<u>Masterprojekt</u>	32

Hinweis zur Bestellung der Prüfer:

Die in dem Modulhandbuch genannten Verantwortlichen werden für die jeweilige Modulprüfung zum Prüfer bestellt.

Formen für Prüfungsvorleistungen und Prüfungsleistungen:

PVL-Formen: Te = Testat, s = schriftlich, m = mündlich, LT = Labortestat, PA = Projektarbeit, Prüfungsformen: M = Modulprüfung, Pl = Prüfungsleistung, s = schriftlich, m = mündlich, a = alternativ, sn = sonstige, A = alternativ, B = Beleg, K = Kolloquium, LB = Laborbericht, MA = Masterarbeit

Sonstige Abkürzungen:

V = Vorlesung (SWS), S = Seminar/Übung (SWS), P = Praktikum (SWS), T = Tutorium (SWS), PVL = Prüfungsvorleistung, PL = Prüfungsleistung, CP = Credit Points, SWS = Semesterwochenstunden, MNR = Modulnummer, MC = Modulcode

7701 Cybercrime I

Modulname:	Cybercrime I	Unterrichtssprache:	deutsch					
Modulnummer:	7701	Abschluss:	M.Sc.					
Modulcode:	03-CCYB1	Häufigkeit:	jahresweise					
Pflicht/Wahl:	Pflicht	Dauer:	1					
Studiengang:	Cybercrime/ Cybersecurity	Regelsemester:	1					
Ausbildungsziele:	Straftaten im Phänomenbereich Cybercrime stellen eine wachsende Herausforderung für die Strafverfolgungsbehörden in Deutschland dar. Die bloße Anzahl solcher Straftaten nimmt jährlich zu (vgl. Bundeslagebild Cybercrime) und gleichzeitig steigt der technische Aufwand bei der Begehung solcher Straftaten ständig. Cybercrime umfasst die Straftaten, die sich gegen das Internet, Datennetze, informationstechnische Systeme oder deren Daten richten sowie Straftaten die mittels dieser Informationstechnik begangen werden. Im Modul Cybercrime I soll auf die sogenannte IuK-Kriminalität im engeren Sinne (Computerkriminalität) eingegangen werden. Die entsprechenden Gesetzesnormen werden vorgestellt und Begehensweisen für die einzelnen Delikte erläutert. Es wird ein besonderer Augenmerk auf die Kriminalistik gelegt. Zu den einzelnen Begehensweisen werden Kriminalstrategie und Kriminaltaktik dargelegt. Nach Abschluss des Moduls kennen die Studierenden alle relevanten Gesetzesnormen und Begehensweisen. Sie können selbstständig effiziente Ermittlungsansätze für solche Fälle entwerfen und eigenständig aufklären. Gegen Ende des Moduls wird auf die Bedeutung der Computerkriminalität im internationalen Kontext eingegangen und internationale Normen und Verfahren dargelegt.							
Lehrinhalte:	IuK Kriminalität im engeren Sinne: • Computerbetrug (§ 263a StGB) • Fälschung beweisheblicher Daten, Täuschung im Rechtsverkehr bei Datenverarbeitung (§§ 269, 270 StGB) • Datenveränderung (§ 303a) • Computersabotage (§ 303b StGB) • Ausspähen von Daten (§ 202a StGB) • Abfangen von Daten (§ 202b StGB) • Softwarepiraterie: Herstellen, Überlassen, Verbreiten oder Verschaffen von sog. "Hacker-Werkzeugen", die illegalen Zwecken dienen (§ 202c StGB) Cybercrime im Internationalen Kontext • Die EU-Cybercrime Richtlinie • Computer Fraud and Abuse Act und Nachfolgende Regelungen in Vereinigten Staaten • Zwischenstaatliche Vereinbarungen, G8, UN, ITU							
Lernmethoden:	Die seminaristisch durchgeführte Vorlesung vermittelt grundlegende (theoretische) Kenntnisse mittels Folien, Beamer-Präsentationen und Tafel. Im betreuten Praktikum bearbeiten die Studenten ausgewählte Fälle aus dem Phänomenbereich Cybercrime. Für das Selbststudium werden konkrete Anregungen gegeben.							
Literatur:	• Dieter Kochheim: Cybercrime und Strafrecht in der Informations- und Kommunikationstechnik. C.H.Beck, 2015 • Michael Büchel, Peter Hirsch: Internetkriminalität: Phänomene-Ermittlungshilfen-Prävention (Grundlagen der Kriminalistik, Band 48). Kriminalistik, 2014. • BKA, Cybercrime: Bundeslagebild (jährlich neu) • Chuck Easttom, Jeff Taylor: Computer Crime, Investigation, and the Law. Cengage Learning PTR, 2010. • United Nations: Comprehensive Study on Cybercrime. 2013 • ITU: Understanding cybercrime: Phenomena, challenges and legal response. 2012							
Arbeitslast:	60 Stunden Lehrveranstaltungen 90 Stunden Vor- und Nachbereitung der Lehrveranstaltungen, Prüfungsvorbereitung							
Anbieter:	03 Fakultät Angewandte Computer- und Biowissenschaften							
Dozententeam (Rollen):	Prof. Dr. rer. nat. Dirk Labudde (Inhaltverantwortlicher)							
Lerneinheitsformen und Prüfungen:	Modulstruktur	V	S	P	T	PVL	PL	CP
	Cybercrime I	2	0	2	0		Mm/30	5

7702 Grundlagen der Mobilfunkforensik

<i>Modulname:</i>	Grundlagen der Mobilfunkforensik	<i>Unterrichtssprache:</i>	deutsch
<i>Modulnummer:</i>	7702	<i>Abschluss:</i>	M.Sc.
<i>Modulcode:</i>	03-CGDMF	<i>Häufigkeit:</i>	jahresweise
<i>Pflicht/Wahl:</i>	Pflicht	<i>Dauer:</i>	1
<i>Studiengang:</i>	Cybercrime/ Cybersecurity	<i>Regelsemester:</i>	1
<i>Ausbildungsziele:</i>	Weltweit existieren über 6 Mrd. Mobilfunknutzer, dies macht mehr als 90% der Weltbevölkerung aus. Bereits im Jahr 2013 waren in 85% aller Kriminalfälle mobile Endgeräte involviert. Trotz der stetig wachsenden Bedeutung mobiler Endgeräte wie Mobiltelefonen, Smart-Phones, PDAs und Musikgeräten gilt die forensische Untersuchung solcher Geräte als teuer und kompliziert. Im Modul "Grundlagen der Mobilfunkforensik" sollen verbreitete Mobilfunkstandards, Betriebssysteme und Grundlagen der Architektur von mobilen Endgeräten strukturiert dargestellt werden. In einem zweiten Teil sollen forensische Tools für mobile Endgeräte vorgestellt und Szenarien erörtert werden. Nach Abschluss des Moduls sollen die Studierenden Kompetenzen im Bereich Mobilfunkforensik der Art erworben haben, dass sie selbstständig in der Lage sind derart gelagerte Spureenträger zu untersuchen.		
<i>Lehrinhalte:</i>	Mobilfunksysteme: Mobilfunksysteme und Mobilfunkstandards der 2. bis 4. Generation (GSM, GPRS, UMTS, LTE), Frequenzbereiche und Frequenzregulierung, Grundlagen zellularer Mobilfunksysteme, Systemeigenschaften (Sendeleistungen, Datenraten, Übertragungsbandbreiten, usw.), Netzwerkarchitekturen und Systemkomponenten, Adressen und Kennziffern zum Auffinden eines Teilnehmers, Luftschnittstelle (Medienzugriffs- und Übertragungsverfahren, Kanalstrukturen), Mobilitätsmanagement, IT-Sicherheit. Mobilfunkforensik: • Grundlagen und Begriffe der Mobilfunkforensik • Smartcards: insbesondere SIM • Mobile Betriebssysteme: insbesondere Android, iOS, WindowsPhone • Architektur von Mobilfunkendgeräten: insbesondere Speichertechnologien • Forensische Tools: insbesondere UFED, XRY • Der IMSICatcher		
<i>Lernmethoden:</i>	Im Rahmen des Masterstudiums werden Vorlesungen mittels Beamer-Präsentationen und Tafel gehalten, in denen wichtige theoretische und praxisrelevante Grundlagen vermittelt werden. In diesem Zusammenhang werden ausgewählte Probleme vertiefend diskutiert und Strategien zur Problemlösung vorgestellt. Anhand von konkreten Fallbeispielen werden Herangehensweisen an definierte Mobilfunkendgeräte sowie mögliche Lösungsstrategien erörtert. Im Praktikum werden ausgewählte Aufgabenstellungen am Spureenträger praktisch verwirklicht. Für das Selbststudium werden konkrete Anregungen und Aufgaben gestellt.		
<i>Literatur:</i>	• Satish Bommisetty, Rohit Tamma, Heather Mahalik: Practical Mobile Forensics. Packt Publishing 2014. • Wolfgang Rankl, Wolfgang Effing: Handbuch der Chipkarten: Aufbau - Funktionsweise - Einsatz von Smart Cards. 5. Auflage, Hanser, 2008. • Bernhard Walke: Mobilfunknetze und ihre Protokolle 1, Stuttgart 2001, ISBN 3-519-26430-7. • Jonathan Zdziarski : iOS Forensic Investigative Methods, 2012. • M. Sauter, Grundkurs Mobile Kommunikationssysteme, Springer, 6. Aufl., 2015, ISBN-13: 978-3658083427. • C. F. Lüders, Mobilfunksysteme, Vogel, 2001, ISBN-10: 3802318471. • J. Hoy, Forensic Radio Survey Techniques for Cell Site Analysis, John Wiley & Sons, 2015, ISBN 9781118925737.		
<i>Arbeitslast:</i>	60 Stunden Lehrveranstaltungen 90 Stunden Vor- und Nachbereitung der Lehrveranstaltungen, Prüfungsvorbereitung		
<i>Anbieter:</i>	<u>03 Fakultät Angewandte Computer- und Biowissenschaften</u>		
<i>Dozententeam (Rollen):</i>	<u>Prof. Dr.-Ing. Volker Delpert</u> (Dozent, Inhaltverantwortlicher) <u>Prof. Dr. rer. pol. Ronny Bodach</u> (Dozent, Inhaltverantwortlicher)		

Lerneinheitenformen und Prüfungen:	Modulstruktur	V	S	P	T	PVL	PL	CP
	<u>Grundlagen der Mobilfunkforensik</u>	2	1	1	0		Ms/90	5

7703 Datenbankprogrammierung

Modulname:	Datenbankprogrammierung	Unterrichtssprache:	deutsch					
Modulnummer:	7703	Abschluss:	M.Sc.					
Modulcode:	03-CDP	Häufigkeit:	jahresweise					
Pflicht/Wahl:	Pflicht	Dauer:	1					
Studiengang:	Cybercrime/ Cybersecurity	Regelsemester:	1					
Ausbildungsziele:	Datenbanken haben sich als allgegenwärtiges Werkzeug im öffentlichen, wissenschaftlichen und wirtschaftlichen Leben etabliert. Diese Vorlesung soll vorhandene Kenntnisse aus einer grundlegenden Datenbankvorlesung im Bachelor vertiefen bzw. erweitern, indem insbesondere auf die Programmierung von Anwendungen im Bereich Datenbanken- und Informationssysteme eingegangen wird. Das ganze Modul soll den Bereich der Datenbankprogrammierung aus dem Fokus der Cybersecurity beleuchten. Dabei sollen Sicherheitsaspekte bei der Anwendungsentwicklung stets im Mittelpunkt stehen und der Begriff der Datenbanksicherheit mit Leben gefüllt werden. Nach Abschluss den Moduls sind die Studierenden in der Lage sichere Anwendungen im Bereich Datenbanken- und Informationssysteme zu entwickeln und die Sicherheit von Datenbankanwendungen zu analysieren und richtig einzuschätzen. Die Teilnehmer können nach der Vorlesung verschiedene APIs zur Anbindung von Anwenderprogrammen an Datenbanken verwenden: Schwerpunkt bildet die Programmierung mit Java und JDBC. Sie können Programme innerhalb eines Datenbanksystems erstellen, wie Stored Procedures, Trigger. Weitere Fähigkeiten stellen die Überwindung des Impedance Mismatch: Abbildung von relationalen Datentupeln auf Objekte in Java und Data Access Object Pattern dar.							
Lehrinhalte:	• Bestandteile von DB-Anwendungen • Fragestellungen bei Datenbankprogrammierung verschiedenerer Datenbank Architekturen • Die Codd'schen Regeln • Der "Impedance Mismatch" • Datenbankprogrammierung innerhalb der Datenbank - Stored Procedures & Trigger • Java Database Connectivity (JDBC) • Transaktionssteuerung • Datenbanksicherheit • Konsistenzkontrolle • Datenbanksicherheit unter Verwendung von statistischen Verfahren							
Lernmethoden:	In der Vorlesung werden die Prinzipien der Datenbankprogrammierung und der Datenbanksicherheit definiert und vorgestellt. Die Vorlesung erfolgt mittels Beamer-Präsentationen und Tafelanschrieb. Die Aufgaben für das Praktikum werden vorgestellt und Lösungsstrategien skizziert. In den betreuten Praktika werden die in der Vorlesung vorgestellten Probleme der Datenbankprogrammierung und der Datenbanksicherheit von den Teilnehmern sowohl selbständig, als auch in Gruppenarbeit am Rechner implementiert. Ein Framework unterstützt diese Arbeit.							
Literatur:	• Alfred Basta, Melissa Zgola: Database Security. Cengage Learning, 2011. • David Litchfield, Chris Anley: The Database Hacker's Handbook: Defending Database Servers. John Wiley & Sons, 2005. • George Reese: Database Programming with JDBC & Java. O'Reilly, 2000.							
Arbeitslast:	60 Stunden Lehrveranstaltungen 90 Stunden Vor- und Nachbereitung der Lehrveranstaltungen, Prüfungsvorbereitung							
Anbieter:	<u>03 Fakultät Angewandte Computer- und Biowissenschaften</u>							
Dozententeam (Rollen):								
Lerneinheitsformen und Prüfungen:	Modulstruktur	V	S	P	T	PVL	PL	CP
	<u>Datenbankprogrammierung</u>	2	0	2	0		Ms/90	5

7704 Intelligente Videoanalyse

<i>Modulname:</i>	Intelligente Videoanalyse	<i>Unterrichtssprache:</i>	deutsch
<i>Modulnummer:</i>	7704	<i>Abschluss:</i>	M.Sc.
<i>Modulcode:</i>	03-CINVI	<i>Häufigkeit:</i>	jahresweise
<i>Pflicht/Wahl:</i>	Pflicht	<i>Dauer:</i>	1
<i>Studiengang:</i>	Cybercrime/ Cybersecurity	<i>Regelsemester:</i>	1
<i>Ausbildungsziele:</i>	Das Modul "Intelligente Videoanalyse" vermittelt Studierenden zunächst Grundlagen der Bilderkennung von der Aufnahme bis zur höheren Bilddeutung. Detaillierte Kenntnisse über die notwendige Beschaffenheit der zugrundeliegenden Systemarchitekturen befähigt die Studierenden infolge dazu, aufgezeigte Lösungen zu adaptieren und Videomaterialien selbständig und (halb-)automatisiert zu bearbeiten. Dies umfasst zuerst die strukturelle Analyse, bei der semantisch zusammenhängende Videosegmente identifiziert werden, wodurch sich die zu verarbeitende Datenmenge in nachfolgenden Schritten signifikant reduzieren lässt. Darauf aufbauend sollen relevante und häufig genutzte Inhalte aus diesen extrahiert und im Rahmen der IT-Forensik im Kontext der vorliegenden Szene interpretierbar gestaltet werden. Die Verarbeitung großer Mengen an audiovisuellen Aufnahmen und die gezielte Entwicklung und Optimierung von Verfahren mit hoher Genauigkeit und geringer Falsch-Alarm-Rate setzt eine flexible und nachhaltige Softwareinfrastruktur voraus. Es wird ein detailliertes Bild von der Herangehensweise, den Konzepten, Techniken und Grenzen der automatisierten Videoanalyse sowie zugehöriger Optimierungsmöglichkeiten vermittelt. Dies schließt klassische und moderne maschinelle Detektionsverfahren ein, die insbesondere den hohen qualitativen Anforderungen im Big Data-Bereich Rechnung tragen.		
<i>Lehrinhalte:</i>	Grundlagen: • Modelle zum Bildverstehen • Entstehung, Vorverarbeitung und Analyse von Bildern • Höhere Bilddeutung Systemarchitekturen: • Struktur generischer Mustererkennungssysteme • Paradigmen und Eigenschaften holistischer Bilderkennungssysteme • Systemanforderungen, Evaluation und Optimierung • Merkmale und Klassifikation • Flexible und nachhaltige Frameworks für die Videoanalyse Strukturelle Videoanalyse: • Schnittgrenzenerkennung • Datenreduktion durch adaptive Keyframeextraktion Inhaltsbasierte Videoanalyse: • Detektion von Gesichtern, Personen, Orten und generischen Objekten • Fortgeschrittene Klassifikation mit Boosting und Deep Learning • Transferlernen aus unterschiedlichen Domänen für Big Data • 3D-Rekonstruktion und Szeneninterpretation		
<i>Lernmethoden:</i>	Die Vorlesung vermittelt grundlegende Kenntnisse mittels Folien, Beamer-Präsentationen und Tafel und vertieft diese in den zugehörigen Übungen und Praktika weiter, um das methodische Verständnis zu erhöhen.		
<i>Literatur:</i>	• Burger, Wilhelm ; Burger, Mark J. (2005). Digitale Bildverarbeitung: Eine Einführung mit Java und ImageJ, Springer, 2. Auflage. • Gibbon, David C.; Liu, Zhu (2008). Introduction to Video Search Engines, Springer. • Hammoud, Riad I. (2006). Interactive Video: Algorithms and Technologies, Springer. • Ritter, Marc (2014). Optimierung von Algorithmen zur Videoanalyse : Ein Analyseframework für die Anforderungen lokaler Fernsehsender. In: Wissenschaftliche Schriftenreihe Dissertationen der Medieninformatik, Nr. 3, Universitätsverlag der Technischen Universität Chemnitz, 336 S. • Sonka, M.; Hlavac, V.; Boyle, R. (2014). Image Processing, Analysis, and Machine Vision, Cengage Learning, 2014 • Steinmüller, Johannes (2008): Bildanalyse : Von der Bildverarbeitung zur räumlichen Interpretation von Bildern, Springer.		
<i>Arbeitslast:</i>	60 Stunden Lehrveranstaltungen 90 Stunden Vor- und Nachbereitung der Lehrveranstaltungen, Prüfungsvorbereitung		
<i>Anbieter:</i>	03 Fakultät Angewandte Computer- und Biowissenschaften		

<i>Dozententeam (Rollen):</i>	<u>Prof. Dr. rer. nat. Marc Ritter</u> (Dozent, Inhaltverantwortlicher)							
<i>Lerneinheitsformen und Prüfungen:</i>	<i>Modulstruktur</i>	<i>V</i>	<i>S</i>	<i>P</i>	<i>T</i>	<i>PVL</i>	<i>PL</i>	<i>CP</i>
	<u>Intelligente Videoanalyse</u>	2	0	2	0	LT	Ms/60	5

7705 Internet of Things

Modulname:	Internet of Things	Unterrichtssprache:	deutsch					
Modulnummer:	7705	Abschluss:	M.Sc.					
Modulcode:	03-CIOT	Häufigkeit:	jahresweise					
Pflicht/Wahl:	Wahlpflicht	Dauer:	1					
Studiengang:	Cybercrime/ Cybersecurity	Regelsemester:	1					
Ausbildungsziele:	Vermittlung von Kenntnissen über die Vernetzung und die Bestandteile des Internets der Dinge - Internet of Things. Ausgehend von einzelnen Komponenten wie RFID- Systeme, Sensoren, Aktoren, Embedded Systeme wird die vernetzte Kommunikation über das Internet demonstriert. Die Studierenden erwerben Wissen bezüglich des Aufbaus, der Funktionsweise und der Implementierung von IoT Anwendungen in Hard- und Software.							
Lehrinhalte:	• Einführung in das Internets der Dinge (IoT) • Protokolle und Technologien • Sensoren, Aktoren und deren Funktionsprinzip und Anschluss • RFID-Systeme in Hard- und Software • Mikrocontroller und TCP/IP Stack als Kommunikationsendpunkte • Datenkommunikation über das Internet mit embedded Systemen und angeschlossenen Sensoren und Aktoren • Wireless Sensor Network Technologie-Funksensoren IEEE 802.15.4							
Lernmethoden:	• Vorlesungen, Beamer-Präsentationen, Tafel; • Übungen und Praktika im Computerpool, Präsentation							
Literatur:	• Tanenbaum, A.: Computernetzwerke, International Edition 2011 • Meyer, Martin: Kommunikationstechnik:, Vieweg +Teubner Verlag GmbH, 2011 ISBN 978-3-8348-1338-1 • Tietze, U.; Schenk, Ch.: Halbleiter-Schaltungstechnik. - Springer Verlag: Berlin Heidelberg New York u.a. - ISBN 3-540-56184-6 • www.Keil.com - uVison4/5 und 32 Bit ARM-Controller LPC1768 Dokumentation, 2014							
Arbeitslast:	75 Stunden Lehrveranstaltungen 75 Stunden Vor- und Nachbereitung der Lehrveranstaltungen, Prüfungsvorbereitung							
Anbieter:	03 Fakultät Angewandte Computer- und Biowissenschaften							
Dozententeam (Rollen):	Prof. Dr. Dr.-Ing. Hartmut Luge (Dozent, Inhaltverantwortlicher)							
Lerneinheitsformen und Prüfungen:	Modulstruktur	V	S	P	T	PVL	PL	CP
	Internet of Things	2	2	1	0		Ms/90	5

7706 Stochastic Models

<i>Modulname:</i>	Stochastic Models	<i>Unterrichtssprache:</i>	deutsch					
<i>Modulnummer:</i>	7706	<i>Abschluss:</i>	M.Sc.					
<i>Modulcode:</i>	03-STMOD	<i>Häufigkeit:</i>	jahresweise					
<i>Pflicht/Wahl:</i>	Wahlpflicht	<i>Dauer:</i>	1					
<i>Studiengang:</i>	Cybercrime/ Cybersecurity	<i>Regelsemester:</i>	1					
<i>Ausbildungsziele:</i>	Das Hauptziel ist die Vermittlung fundierter Kenntnisse in Bereich der Modellbildung und stochastischen Simulation sowie deren Anwendung in statistischen Methoden. Die Studierenden lernen den Umgang mit verschiedenen Klassen von stochastischen Prozessen kennen. Praxisnahe Anwendungsbeispiele werden im Praktikumsteil am Computer implementiert. Auf diese Weise soll bei den Studierenden ein tiefgehendes Verständnis für die Modellierung stochastischer Prozesse herausgebildet werden. Studierende erlernen die Fähigkeit Probleme konzeptionell zu erfassen, zu strukturieren, zu modellieren und - insbesondere mittels stochastischer Simulation - eigenständig zu lösen. The main objective is the acquirement of solid knowledge of probabilistic modeling and stochastic simulation, as well as their application to statistical methods. Students learn to handle various classes of stochastic processes. Practical applications will be discussed in detail and implemented and solved using computerized methods. Based on that, students will gain a deep understanding of modeling stochastic processes. Additionally, students will acquire the abilities to comprehend practical problems conceptually, to structure and model them, and to independently solve them, particularly using stochastic simulations.							
<i>Lehrinhalte:</i>	Im Modul Stochastische Modelle werden diskrete und kontinuierliche stochastische Prozesse vorgestellt, insbesondere Markovketten, Martingal-Prozesse, Geburts-Todesprozesse sowie Verzweigungs- und Koaleszenzprozesse eingegangen. Es wird insbesondere auf die Simulation von stochastischen Prozessen (z.B. MCMC) eingegangen sowie deren Anwendung in statistischen Verfahren (Bayes'sche Verfahren, Approximativ Bayes'sche Verfahren). In this module discrete and continuous stochastic processes are introduced, in particular, Markov chains, Martingal-processes, birth-death processes, branching and coalescence processes. Particular focus lies on simulation techniques of stochastic processes (e.g. MCMC) as well as on their applications in statistical procedures (Bayesian and approximate Bayesian methods).							
<i>Lernmethoden:</i>	Klassische Vorlesung (Präsentationen, Animationen und Illustrationen enthaltend), Übungen, studentische Vorträge in Seminaren, Bearbeitung von Aufgabenstellungen mittels Computeralgebrasystemen/ Matrizen-sprachen (z.B. Mathematica, Maple, MatLab) , statistischer Software (z.B. SAS, SPSS, R) und Programmiersprachen (Python, C++). Classic lecture (presentations, animations and illustrations containing), exercises, student presentations in seminars, processing of tasks using computer algebra systems/ matrix-languages (e.g. , Mathematica, maple, Matlab), statistical software (e.g. , SAS, SPSS, R) and programming languages (Python, C++).							
<i>Literatur:</i>	H. Bauer: Wahrscheinlichkeitstheorie. de Gruyter, 4. Auflage (1991). P. Billingsley: Probability and measure. Wiley (1986). R. Durrett: Probability theory and examples . Cambridge University Press, 4. Auflage (30. August 2010). G. Pflug: Stochastische Modelle in der Informatik. B.G. Teubner Stuttgart, 1986. I. M. Sobol: Die Monte-Carlo-Methode, Taschenbücher Nr. 41. Harri Deutsch, Frankfurt a. M., 1985.							
<i>Arbeitslast:</i>	60 Stunden Lehrveranstaltungen 90 Stunden Vor- und Nachbereitung der Lehrveranstaltungen, Prüfungsvorbereitung							
<i>Anbieter:</i>	<u>03 Fakultät Angewandte Computer- und Biowissenschaften</u>							
<i>Dozententeam (Rollen):</i>	<u>Prof. Dr. rer. nat. habil. Kristan Schneider</u> (Inhaltverantwortlicher)							
<i>Lerneinheitsformen und Prüfungen:</i>	<i>Modulstruktur</i>	<i>V</i>	<i>S</i>	<i>P</i>	<i>T</i>	<i>PVL</i>	<i>PL</i>	<i>CP</i>
	<u>Stochastic Models</u>	2	1	1	0		Ms/120	5

7707 Foundations of Modern Cryptography

<i>Modulname:</i>	Foundations of Modern Cryptography	<i>Unterrichtssprache:</i>	deutsch, englisch
<i>Modulnummer:</i>	7707	<i>Abschluss:</i>	M.Sc.
<i>Modulcode:</i>	03-CFOMC	<i>Häufigkeit:</i>	jahresweise
<i>Pflicht/Wahl:</i>	Wahlpflicht	<i>Dauer:</i>	1
<i>Studiengang:</i>	Cybercrime/ Cybersecurity	<i>Regelsemester:</i>	1
<i>Ausbildungsziele:</i>	This master's-level course aims to provide students with a comprehensive foundation in modern cryptography. By the end of the course, students will: • gain a solid understanding of the mathematical foundations of modern cryptography, including number theory, algebra, and complexity theory, • develop proficiency in designing and analyzing cryptographic protocols, understanding their security models, and applying formal proofs, • learn how modern cryptographic schemes, such as encryption, authentication, and digital signatures, are constructed and proven secure, • become familiar with the fundamental cryptographic primitives and how they underpin real-world security systems, • prepare for further research and development in cryptographic theory, algorithms, and applications.		
<i>Lehrinhalte:</i>	Mathematical Foundations of Cryptography: Number theory (modular arithmetic, prime factorization, quadratic residues). Algebraic structures (groups, rings, fields, elliptic curves). Complexity theory and the role of NP-completeness in cryptographic design. Symmetric-Key Cryptography: Block ciphers (DES, AES, Feistel networks) and their security analysis. Stream ciphers and hash functions. Modes of operation and authenticated encryption. Public-Key Cryptography: RSA, Rabin, ElGamal, Diffie-Hellman, ECC cryptosystems and digital signature schemes.		
<i>Lernmethoden:</i>	Lectures: Interactive lectures explaining the theoretical underpinnings of modern cryptographic techniques. Seminars: Regular assignments to reinforce the theoretical concepts learned in class and to apply them in practical scenarios. Labs: Programming exercises that include cryptographic algorithm implementations in SageMath.		
<i>Literatur:</i>	Boneh, D., & Shoup, V. (2020). A Graduate Course in Applied Cryptography. https://crypto.stanford.edu/~dabo/cryptobook. McAndrew, A. (2011). Introduction to Cryptography with Open-Source Software. CRC Press.		
<i>Fachkompetenz:</i>	Expertise in the mathematical and theoretical foundations of modern cryptography. Ability to design, implement, and analyze cryptographic primitives and protocols. Proficiency in applying formal methods to prove the security of cryptographic systems. Understanding of the role of cryptography in real-world applications such as secure communication, data protection, and authentication.		
<i>Methodenkompetenz:</i>	Ability to apply advanced mathematical techniques to cryptographic problem-solving. Proficiency in the use of cryptographic libraries and algorithmic design in the context of modern cryptography. Skills in critically evaluating existing cryptographic systems, both in terms of their theoretical security and practical implementation.		
<i>Selbstkompetenz:</i>	Capacity to learn and apply advanced cryptographic concepts and research independently. Ability to think critically and solve complex cryptographic problems in a systematic and structured manner. Self-motivation to stay updated with the latest trends, challenges, and breakthroughs in the field of cryptography.		
<i>Sozialkompetenz:</i>	Active participation in seminars and group discussions, contributing ideas and engaging with the work of others. Ability to navigate the ethical considerations of cryptography, such as responsible disclosure and cryptographic security in public policy.		

<i>Arbeitslast:</i>	60 Stunden Lehrveranstaltungen 90 Stunden Vor- und Nachbereitung der Lehrveranstaltungen, Prüfungsvorbereitung							
<i>Anbieter:</i>	<u>03 Fakultät Angewandte Computer- und Biowissenschaften</u>							
<i>Dozententeam (Rollen):</i>	<u>Prof. Dr. rer. nat. Klaus Dohmen</u> (Dozent, Inhaltverantwortlicher, Prüfer, Aufsicht) <u>Prof. Dr. rer. nat. habil. Thomas Villmann</u> () <u>Dr. Mandy Lange-Geisler</u> (Planer, Prüfer, Aufsicht) <u>Prof. Dr. rer. nat. Franka Baaske</u> (Planer)							
<i>Lerneinheitsformen und Prüfungen:</i>	<i>Modulstruktur</i>	<i>V</i>	<i>S</i>	<i>P</i>	<i>T</i>	<i>PVL</i>	<i>PL</i>	<i>CP</i>
	<u>Foundations of Modern</u> <u>Cryptography</u>	2	1	1	0	LT	Ma	5

7708 Cybercrime II

<i>Modulname:</i>	Cybercrime II	<i>Unterrichtssprache:</i>	deutsch
<i>Modulnummer:</i>	7708	<i>Abschluss:</i>	M.Sc.
<i>Modulcode:</i>	03-CCYB2	<i>Häufigkeit:</i>	jahresweise
<i>Pflicht/Wahl:</i>	Pflicht	<i>Dauer:</i>	1
<i>Studiengang:</i>	Cybercrime/ Cybersecurity	<i>Regelsemester:</i>	2
<i>Ausbildungsziele:</i>	Im Modul Cybercrime II soll auf die sogenannte luK-Kriminalität im weiteren Sinne (Tatmittel Internet) eingegangen werden. Die entsprechenden Gesetzesnormen werden vorgestellt und Begehensweisen für die einzelnen Delikte erläutert. Es wird ein besonderer Augenmerk auf die Kriminalistik gelegt. Zu den einzelnen Begehensweisen werden Kriminalstrategie und Kriminaltaktik dargelegt. Nach Abschluss des Moduls kennen die Studierenden relevante Gesetzesnormen und Begehensweisen. Sie können selbstständig effiziente Ermittlungsansätze für solche Fälle entwerfen und eigenständig aufklären.		
<i>Lehrinhalte:</i>	luK Kriminalität im weiteren Sinne: • Verbreitung pornographischer Schriften (Kinderpornographie) über das Internet • Verbreitung von Gewaltdarstellungen im Internet • Onlinemarktplätze (Drogenhandel, Waffenhandel, Menschenhandel) • Urheberrechtsdelikte Cybercrime im Staatsschutz • Internetdelikte PMK Rechts • Internetdelikte PMK Links • Internetdelikte PMK Islamismus Einsatz von luK in der Organisierten Kriminalität • Geldwäsche im Internet • Bedeutung von luK für grenzüberschreitende Kriminalität • Fälschungen luK im Strafverfahren • luK als falsche Beweise		
<i>Lernmethoden:</i>	Die seminaristisch durchgeführte Vorlesung vermittelt grundlegende (theoretische) Kenntnisse mittels Folien, Beamer-Präsentationen und Tafel. Im betreuten Praktikum bearbeiten die Studenten ausgewählte Fälle aus dem Phänomenbereich Cybercrime. Für das Selbststudium werden konkrete Anregungen gegeben.		
<i>Literatur:</i>	• Gerrit Manssen, Jörg Fritzsche, Robert Uerpmann-Witzack: Strafrechtliche Verantwortlichkeit der Informationsvermittler im Netz. LIT, 2006 • Philip Jenkins: Beyond Tolerance: Child Pornography. NYU Press, 2001. • Jörg Kinzig: Die rechtliche Bewältigung von Erscheinungsformen der Organisierten Kriminalität, Berlin, 2004. • Sean S. Costigan, Jake Perry: Cyberspaces and Global Affairs. Routledge, 2012. • Bösche, Andreas: Rechtsextremismus im Internet. Schattenseiten des www. Hall 2001 • Rüdiger Quedenfeld, Udo Mühlroth, Martin Plischke, Marc Studer: Handbuch Bekämpfung der Geldwäsche und Wirtschaftskriminalität. ESV, 2013.		
<i>Arbeitslast:</i>	60 Stunden Lehrveranstaltungen 90 Stunden Vor- und Nachbereitung der Lehrveranstaltungen, Prüfungsvorbereitung		
<i>Anbieter:</i>	<u>03 Fakultät Angewandte Computer- und Biowissenschaften</u>		
<i>Dozententeam (Rollen):</i>	Prof. Dr. rer. nat. Dirk Labudde (Dozent, Inhaltverantwortlicher)		
<i>Lerneinheitsformen und Prüfungen:</i>	<i>Modulstruktur</i> <u>Cybercrime II</u>	<i>V S P T PVL PL CP</i> 2 0 2 0 Mm/30 5	

7709 Der Sachverständige vor Gericht

Modulname:	Der Sachverständige vor Gericht	Unterrichtssprache:	deutsch					
Modulnummer:	7709	Abschluss:	M.Sc.					
Modulcode:	03-CSVG	Häufigkeit:	jahresweise					
Pflicht/Wahl:	Pflicht	Dauer:	1					
Studiengang:	Cybercrime/ Cybersecurity	Regelsemester:	2					
Ausbildungsziele:	IT-Forensiker wie Ermittler müssen die Ergebnisse Ihrer Arbeit in Gutachten darlegen. An solche Gutachten werden definierte formale Ansprüche gestellt. Auch müssen diese Gutachten vor Gericht vertreten werden, auch hier gibt es einen formalen Rahmen der einzuhalten ist. Neben den formalen Kriterien gibt es eine Menge ungeschriebene Gesetze einzuhalten und der Sachverständige soll auch rhetorisch überzeugen. Das Modul "Der Sachverständige vor Gericht" soll die Anforderungen an ein Gutachten beziehungsweise an einen Sachverständigenvortrag vermitteln. Daneben sollen sprachliche und rhetorische Besonderheiten im Strafprozess dargelegt werden.							
Lehrinhalte:	• Das Sachverständigengutachten • Der Sachverständigenvortrag • Der Sachverständige in der StPO • Juristische Rhetorik • Sprache und Duktus des Sachverständigenvortrags							
Lernmethoden:	In der Vorlesung werden wichtige theoretische und praxisrelevante Grundlagen vermittelt. Im Seminar werden ausgewählte Probleme vertiefend diskutiert und Strategien zur Problemlösung vorgestellt. Anhand eines konkreten Falls soll eigenständig ein Gutachten geschrieben und ein Sachverständigenvortrag vorbereitet werden. Für das Selbststudium werden konkrete Anregungen und Aufgaben gestellt. Das Erstellte Gutachten soll in einem Sachverständigenvortrag dargestellt werden. In einem Rollenspiel wird eine Gerichtsverhandlung nachgestellt.							
Literatur:	• Walter Byerlein: Praxishandbuch Sachverständigenrecht. CH.. Beck, 2000. • Harald Krammer, Jürgen Schille, Alexeander Schmidt, Alfred Tanczos: Sachverständige und ihre Gutachten. Manz 2015 • Fritjof Haft: Juristische Rhetorik. Alber Studienbuch, 2009.							
Arbeitslast:	60 Stunden Lehrveranstaltungen 90 Stunden Vor- und Nachbereitung der Lehrveranstaltungen, Prüfungsvorbereitung							
Anbieter:	03 Fakultät Angewandte Computer- und Biowissenschaften							
Dozententeam (Rollen):	Prof. Dr. rer. nat. Dirk Labudde (Dozent)							
Lerneinheitsformen und Prüfungen:	Modulstruktur	V	S	P	T	PVL	PL	CP
	Der Sachverständige vor Gericht	1	3	0	0		Mm/30	5

7710 Softwarepraktikum

Modulname:	Softwarepraktikum	Unterrichtssprache:	deutsch																																
Modulnummer:	7710	Abschluss:	M.Sc.																																
Modulcode:	03-CSPR	Häufigkeit:	jahresweise																																
Pflicht/Wahl:	Pflicht	Dauer:	1																																
Studiengang:	Cybercrime/ Cybersecurity	Regelsemester:	2																																
Ausbildungsziele:	Die Studierenden sind in der Lage, als Mitglied eines Softwareentwicklungsteams an einem realistischen Softwareprojekt von der Aufgabenstellung bis zur Inbetriebnahme des Softwaresystems zu arbeiten. Dabei werden alle Fach- und Methodenkompetenzen, die im bisherigen Masterstudium, vor allem in der Qualifizierungslinie Softwarearchitektur erworben worden sind, vom Studierenden erprobt, geübt und gefestigt. Die Studierenden können gemeinsam an einer Aufgabenstellung aus dem Bereich Cybersecurity arbeiten und übernehmen Rollenverantwortung innerhalb des Teams. Sie beherrschen ihre Kommunikationsfähigkeiten in der jeweilig festgelegten Rolle als Verantwortlicher, Fach- oder Methodenspezialist. Sie beherrschen die grundlegenden Anforderungen des Projektmanagements. Sie sind in der Lage, auf schwierige Projektsituationen so zu reagieren, dass das Gesamtziel der Erstellung eines Softwareprototypen nicht gefährdet wird. Die Studierenden sind in der Lage, professionelle und fachlich korrekte begleitende Dokumentationen zu den einzelnen Projektphasen unter Zuhilfenahme spezieller Tools zu erstellen. Sie können vollendete Projektabschnitte (Meilensteine) in einer Kurzpräsentation vor dem Entwicklungsteam, dem Dozenten-/Coachingteam und fachlich interessierten Außenstehenden so vorstellen, dass die Einbettung in den Gesamtkontext immer zu erkennen ist. Die Studierenden sind für den berufliche Einsatz trainiert, softwaretechnische Prinzipien, Methoden und Werkzeuge auf praxisrelevante Fallbeispiele im Feld der Cybersecurity anzuwenden und bis zu einem Demonstrationsprototypen als Teil eines Teams zu entwickeln. Dabei können sie die ersten eigene praktischen Erfahrungen vorweisen. Sie haben Erfahrungen sowohl in klassischer als auch in agiler Vorgehensweise, da das eingesetzte und speziell dafür entwickelte Vorgehensmodell Elemente aus beiden Welten enthält.																																		
Lehrinhalte:	• Bearbeitung einer praxisrelevanten Aufgabenstellung im Projektteam. • Bearbeitung gemäß einem Vorgehensmodell der Softwaretechnik mit agilen und klassischen Elementen, Anwendung der Lehrinhalte aus der Qualifizierungslinie Softwarearchitektur, Einsatz von zweckmäßigen UML-Werkzeugen • Projektstatusberichte und Zwischenpräsentationen gemäß Projektmeilensteine • Abschlusspräsentation der Gruppenarbeit und des Prototypen durch die Teammitglieder																																		
Lernmethoden:	• Bildung von Projektgruppen • Visualisierungstechniken, Moderation, Präsentation, Beamer-Einsatz bei Teambesprechungen, • Praktisches Arbeiten am Rechner (Einsatz von CASE-Werkzeugen)																																		
Literatur:	• Balzert, Helmut: Lehrbuch der Softwaretechnik: Entwurf, Implementierung, Installation und Betrieb, Spektrum Akademischer Verlag 2011 • Sommerville, Ian: Software Engineering - 9. Aufl., Pearson Studium 2012 • Oestereich, Bernd: Analyse und Design mit der UML 2.5: Objektorientierte Softwareentwicklung, Oldenbourg Wissenschaftsverlag 2013 • Balzert, Heide: Lehrbuch der Objektmodellierung: Analyse und Entwurf mit der U.M.L. 2, . Spektrum Akademischer Verlag 2011																																		
Arbeitslast:	60 Stunden Lehrveranstaltungen 90 Stunden Vor- und Nachbereitung der Lehrveranstaltungen, Prüfungsvorbereitung																																		
Anbieter:	<u>03 Fakultät Angewandte Computer- und Biowissenschaften</u>																																		
Dozententeam (Rollen):	<u>Prof. Dr. rer. nat. Dirk Labudde</u> (Dozent) <u>Prof. Dr. rer. pol. Dirk Pawlaszczyk</u> (Dozent) <u>M.Sc. Stefan Schildbach</u> (Dozent)																																		
Lerneinheitsformen und Prüfungen:	<table><tr><td>Modulstruktur</td><td>V</td><td>S</td><td>P</td><td>T</td><td>PVL</td><td>PL</td><td>CP</td></tr><tr><td><u>Softwarepraktikum</u></td><td>0</td><td>0</td><td>4</td><td>0</td><td></td><td></td><td>5</td></tr><tr><td><u>Teilprüfung 1</u></td><td></td><td></td><td></td><td></td><td></td><td>PI4sn/B</td><td></td></tr><tr><td><u>Teilprüfung 2</u></td><td></td><td></td><td></td><td></td><td></td><td>PI4m/20</td><td></td></tr></table>			Modulstruktur	V	S	P	T	PVL	PL	CP	<u>Softwarepraktikum</u>	0	0	4	0			5	<u>Teilprüfung 1</u>						PI4sn/B		<u>Teilprüfung 2</u>						PI4m/20	
Modulstruktur	V	S	P	T	PVL	PL	CP																												
<u>Softwarepraktikum</u>	0	0	4	0			5																												
<u>Teilprüfung 1</u>						PI4sn/B																													
<u>Teilprüfung 2</u>						PI4m/20																													

7711 Datenkompression

<i>Modulname:</i>	Datenkompression	<i>Unterrichtssprache:</i>	deutsch
<i>Modulnummer:</i>	7711	<i>Abschluss:</i>	M.Sc.
<i>Modulcode:</i>	03-CDKPR	<i>Häufigkeit:</i>	jahresweise
<i>Pflicht/Wahl:</i>	Pflicht	<i>Dauer:</i>	1
<i>Studiengang:</i>	Cybercrime/ Cybersecurity	<i>Regelsemester:</i>	2
<i>Ausbildungsziele:</i>	Das Modul vermittelt den Studierenden theoretisches und praxisorientiertes Wissen über die Algorithmen und die Verfahren der verlustfreien und verlustbehafteten Datenkompression. Der Schwerpunkt wird auf die Datenkompression von Bildern und Bildsequenzen gelegt. Nach dem Abschluss des Moduls können die Teilnehmer die Möglichkeiten und die Grenzen der Datenkompression richtig einschätzen. Sie verstehen die Herangehensweise, die Konzepte und die Techniken der Datenkompression und sind in der Lage, ausgewählte Algorithmen zur Datenkompression in Softwarekomponenten zu implementieren und sie anzuwenden.		
<i>Lehrinhalte:</i>	Grundlagen der Datenkompression: Grundbegriffe (Redundanz, Irrelevanz), informationstheoretische Grundlagen (Entscheidungsgehalt, Entropie, Quellen- und Coderedundanz), visuelle Wahrnehmungseigenschaften des Menschen, Farbsysteme und Farbraumtransformation, Bewertungskriterien (Kompressionsverhältnis, Signalqualität); Signal- und systemtheoretische Grundlagen: Analog/Digital-Wandlung, Korrelationsfunktion, Diskrete Faltung, Transformation (Karhunen-Loève-Transformation, Diskrete-Kosinus-Transformation, Diskrete Walsh-Hadamard-Transformation, Diskrete-Wavelet-Transformation); Verfahren zur redundanzmindernden Codierung: Präcodierung (Laufängen- und Phrasencodierung), Shannon-Fano-Codierung, Huffman-Codierung, arithmetische Codierung; Methoden zur Datenreduktion: Unterabtastung, skalare Quantisierung, Vektorquantisierung, Codebuchentwurf in der Vektorquantisierung (Gradientenverfahren, Fuzzy-Sets, Methoden der statistischen Mechanik, Evolutionsstrategien); Standards der Bild- und Videocodierung (JPEG, JPEG 2000, MPEG, H.262, H.264, H.265) sowie Bildübertragungssysteme (DVB-C, DVB-S/S2, DVB-T/T2, IP-TV).		
<i>Lernmethoden:</i>	Die Lehrinhalte werden in den Seminaren mit Hilfe von PowerPoint-Präsentationen (Notebook und Beamer) sowie Tafel und Kreide vermittelt. Unterstützt wird das Verständnis durch anschauliche Demonstrationen mithilfe von Softwaretools. Im Praktikum entwickeln die Studierenden Softwarekomponenten, mit denen sie bekannte sowie neue Algorithmen und Verfahren zur Datenkompression anwenden, ihre Wirkungsweise veranschaulichen und ihre Leistungsfähigkeit miteinander vergleichen können.		
<i>Literatur:</i>	• T. Strutz: Bilddatenkompression, Grundlagen, Codierung, Wavelets, JPEG, MPEG, H.264, 4. Aufl., Vieweg + Teubner, ISBN 978-3834804723, 2009. • J.-R. Ohm, Multimedia Signal Coding and Transmission, Springer, ISBN 978-3-662-46691-9, 2015. • W. Fischer, Digitale Fernseh- und Hörfunktechnik in Theorie und Praxis, 4. Aufl., Springer, ISBN 978-3642538957, 2016. • R. Mäusl, Fernsehtechnik, Vom Studiosignal zum DVB-Sendesignal, 4. Aufl., Hüthig, ISBN 978-3-7785-3996-5, 2006. • JPEG, Information technology - Digital compression and coding of continuous-tone still images - Requirements and Guidelines, T.81, 1992. • JPEG 2000, Information technology - JPEG 2000 image coding system: Core coding system, ISO/IEC 15444-1 ... 15444-11, 2004. • MPEG-2/H.262, Information technology, Generic coding of moving pictures and associated audio, Recommendation H.262, ISO/IEC 13818-2, 1994. • MPEG-4AVC/H.264, Advanced video coding for generic audio-visual services, ITU-T Recommendation H.264, 2003. • HEVC/H.265, High efficiency video coding, ITU-T Recommendation H.265, 2015. • Electronics Letters, Journal, Institution of Engineering and Technology (IET), ISSN 0013-5194. • IEE Proceedings - Vision, Image and Signal Processing, Journal, Institution of Engineering and Technology (IET), ISSN 1350-245X. • IEEE Transactions on Communications, Journal, Institute of Electrical and Electronics Engineers (IEEE), IEEE Communications Society, ISSN 0090-6778.		
<i>Arbeitslast:</i>	60 Stunden Lehrveranstaltungen 90 Stunden Vor- und Nachbereitung der Lehrveranstaltungen, Prüfungsvorbereitung		
<i>Anbieter:</i>	<u>03 Fakultät Angewandte Computer- und Biowissenschaften</u>		
<i>Dozententeam (Rollen):</i>	<u>Prof. Dr.-Ing. Volker Delpört</u> (Dozent, Inhaltverantwortlicher)		

Lerneinheitenformen und Prüfungen:	Modulstruktur	V	S	P	T	PVL	PL	CP
	<u>Datenkompression</u>	0	2	2	0			5
	<u>Teilprüfung 1</u>						PI4sn/B	
	<u>Teilprüfung 2</u>						PI4s/90	

7712 Geoforensik und Reverse Engineering

<i>Modulname:</i>	Geoforensik und Reverse Engineering	<i>Unterrichtssprache:</i>	deutsch
<i>Modulnummer:</i>	7712	<i>Abschluss:</i>	M.Sc.
<i>Modulcode:</i>	03-GFRE	<i>Häufigkeit:</i>	Sommersemester
<i>Pflicht/Wahl:</i>	Wahlpflicht	<i>Dauer:</i>	1
<i>Studiengang:</i>	Cybercrime/ Cybersecurity	<i>Regelsemester:</i>	2
<i>Ausbildungsziele:</i>	Die Studierenden können Geo-Daten auf Datenträgern identifizieren und sichern. Jeder Teilnehmer ist vertraut mit gängigen Speicherformaten für Geopositionsdaten. Sie sind in der Lage Positions- und Routenverläufe zu visualisieren und in einen zeitlichen Ablauf zu bringen. Die Teilnehmer verfügen über Kenntnisse in Bezug auf die Störung von Fälschung von GPS-Signalen. Jeder Teilnehmer verfügt über fachliche Kenntnisse in Bezug auf die Analyse von Binärcode-Dateien und ist geschult im Umgang mit entsprechenden Disassembling-Werkzeugen.		
<i>Lehrinhalte:</i>	Geoinformationssysteme, Polarkoordinaten, GeoDaten, Speicherung, Verarbeitung und Visualisierung von Positionsdaten, Geotracking, Auswertung von Drohnen-Images, GNSS Grundlagen, Jamming & Spoofing von GPS-Signalen, Auswertung von PE-Dateien, Disassembling-Techniken, Anti-Debugging-Techniken, Malware-Forensics		
<i>Lernmethoden:</i>	Die Lehrinhalte werden in den Seminaren mit Hilfe von PowerPoint-Präsentationen (Notebook und Beamer) sowie Tafel und Kreide vermittelt. Das Modul wird hybrid angeboten. Lehrmaterialien werden über die fakultätseigene Lehrplattform bereit gestellt. Unterstützt wird das Verständnis durch anschauliche Demonstrationen mithilfe von Softwaretools. Im Praktikum müssen die Studierende konkrete fallbezogene Aufgabenstellungen aus dem Bereich Geo-Forensik eigenständig bearbeiten und lösen. Dafür werden Image-Dateien zur Verfügung gestellt.		
<i>Literatur:</i>	Buch: Practical Reverse Engineering: x86, x64, ARM, Windows Kernel, Reversing Tools, and Obfuscation. Wiley 2014. Buch: Geoinformatik in Theorie und Praxis - Grundlagen von Geoinformationssystemen, Fernerkundung und digitaler Bildverarbeitung, Norbert de Lange (Hrsg.), Springer 2018. Buch: Forensik in der digitalen - Welt Moderne Methoden der forensischen Fallarbeit in der digitalen und digitalisierten realen Welt herausgegeben von: Dirk Labudde, Michael Spranger Verlag: Springer Berlin Heidelberg 2017. Buch: Mobile Forensics - The File Format Handbook. Common File Formats and File Systems Used in Mobile Devices. Christian Hummert, Dirk Pawlaszczyk (Eds.). Springer 2022. https://doi.org/10.1007/978-3-030-98467-0		
<i>Arbeitslast:</i>	60 Stunden Lehrveranstaltungen 90 Stunden Vor- und Nachbereitung der Lehrveranstaltungen, Prüfungsvorbereitung		
<i>Anbieter:</i>	<u>03 Fakultät Angewandte Computer- und Biowissenschaften</u>		
<i>Dozententeam (Rollen):</i>			
<i>Lerneinheitenformen und Prüfungen:</i>	<i>Modulstruktur</i> <u>Geoforensik und Reverse Engineering</u>	<i>V</i> <i>S</i> <i>P</i> <i>T</i> <i>PVL</i> <i>PL</i> <i>CP</i> 2 2 0 0 Mm/30 5	

7713 Artificial Intelligence - Theory and Foundations

Modulname:	Artificial Intelligence - Theory and Foundations	Unterrichtssprache:	deutsch, englisch					
Modulnummer:	7713	Abschluss:	M.Sc.					
Modulcode:	03-AITF-20	Häufigkeit:	jahresweise					
Pflicht/Wahl:	Wahlpflicht	Dauer:	1					
Studiengang:	Cybercrime/ Cybersecurity	Regelsemester:	2					
Ausbildungsziele:	In der Lehrveranstaltung erwerben die Studierenden Wissen über grundlegende mathematisch-algorithmische Prinzipien im maschinellen Lernen. Schwerpunkt bilden neuronale Netze und Modelle des Hebb"schen Lernens zur Mustererkennung und Klassifikation. Im Computerpraktikum erlernen die Studierenden, einfache Algorithmen in ihrem (mathematischen) Verhalten zu untersuchen. The course provides the basic principles and algorithms in CI. Particularly, neural networks for clustering and classification as well as Hebb learning are in the main focus. Completing the course, students are able to program basic models and to study their behavior.							
Lehrinhalte:	Biologische Neuronen, Perzeptron,Hopfield Netzwerke, Mehrschicht-Netzwerke, Hebb"sches Lernen, Vektorquantisierung.							
Lernmethoden:	Kreide und Tafel, Präsentationen Chalk and blackboard, slides							
Literatur:	C. Bishop: Pattern Recognition and Machine Learning. Springer, 2007. S. Haykin: Neural Networks. Pearson Education, 2004. R. Kruse: Computational Intelligence. Teubner, 2011. H. Ritter, T. Martinetz & K. Schulten: Neural Computation and Self-Organizing Maps. Addison-Wesley, 1992. M. Mayamoto: Fuzzy Clustering. Springer 2010. M. Biehl: The Shallow and the Deep: A biased introduction to neural networks and old school machine learning, Groningen University Press, 2023 A. Krogh et al.: Introduction To The Theory Of Neural Computation, Santa Fe Institutes Sereies,1991 Bishop/Bishop: deep Learning: Foundation and Concepts, Springer, 2024							
Arbeitslast:	60 Stunden Lehrveranstaltungen 90 Stunden Vor- und Nachbereitung der Lehrveranstaltungen, Prüfungsvorbereitung							
Anbieter:	03 Fakultät Angewandte Computer- und Biowissenschaften							
Dozententeam (Rollen):	Prof. Dr. rer. nat. habil. Thomas Villmann (Dozent, Inhaltverantwortlicher)							
Lerneinheitsformen und Prüfungen:	Modulstruktur	V	S	P	T	PVL	PL	CP
	Artificial Intelligence - Theory and Foundations	2	1	1	0		Mm/30	5

7714 Cryptanalysis

<i>Modulname:</i>	Cryptanalysis	<i>Unterrichtssprache:</i>	deutsch, englisch
<i>Modulnummer:</i>	7714	<i>Abschluss:</i>	M.Sc.
<i>Modulcode:</i>	03-CCA	<i>Häufigkeit:</i>	jahresweise
<i>Pflicht/Wahl:</i>	Wahlpflicht	<i>Dauer:</i>	1
<i>Studiengang:</i>	Cybercrime/ Cybersecurity	<i>Regelsemester:</i>	2
<i>Ausbildungsziele:</i>	This advanced master's-level course is designed to provide students with a deep understanding of cryptanalysis, the art and science of breaking cryptographic systems. By the end of the course, students will: • acquire the knowledge and skills required to analyze and break both classical and modern cryptographic systems, • develop proficiency in various cryptanalytic techniques such as brute-force attacks, differential and linear cryptanalysis and algebraic attacks, • understand the principles and methods of cryptographic security, including how weaknesses in cryptographic protocols and algorithms can be exploited, • gain insight into the real-world applications of cryptanalysis in the context of securing communication systems, cryptographic protocols, and emerging technologies, • be prepared to carry out research in cryptanalysis, contributing to the development of more secure cryptographic systems.		
<i>Lehrinhalte:</i>	Introduction to Cryptanalysis: Overview of classical and modern cryptographic systems and the need for cryptanalysis. Classical Cryptography and Attacks: Frequency analysis, brute-force attacks, and classical cipher attacks (Caesar cipher, Vigenère cipher, Enigma). Modern Symmetric-Key Cryptanalysis: Differential and linear cryptanalysis of block ciphers (e.g., DES, AES). Statistical and algebraic attacks on block ciphers and stream ciphers. Cryptanalysis of hash functions and MACs (e.g., SHA, HMAC). Public-Key Cryptography Attacks: Integer factorization and attacks on RSA. Elliptic Curve Cryptography (ECC) and attacks on ECC-based schemes. Attacks on digital signature schemes and key exchange protocols (e.g., Diffie-Hellman, ElGamal).		
<i>Lernmethoden:</i>	Lectures: Theoretical lectures covering the cryptanalytic techniques and cryptographic concepts relevant to the course. Seminars: Regular assignments and presentations by students. Labs: Programming assignments and problem-solving sessions.		
<i>Literatur:</i>	G.V. Bard: Algebraic Cryptanalysis. Springer, 2009. M.J. Hinek: Cryptanalysis of RSA and Its Variants. CRC Press, 2010. M. Stamp & R.M. Low: Applied Cryptanalysis. Breaking Ciphers in the Real World. Wiley, 2007. Original research papers.		
<i>Fachkompetenz:</i>	In-depth understanding of cryptographic weaknesses and vulnerabilities. Ability to apply advanced cryptanalytic techniques to analyze and break modern cryptographic algorithms. Competence in identifying and exploiting cryptographic flaws, both in theory and in practice. Knowledge of the ethical implications of cryptanalysis and its role in securing communications and systems.		
<i>Methodenkompetenz:</i>	Mastery of advanced cryptanalytic methods such as differential cryptanalysis, linear cryptanalysis, and algebraic attacks. Ability to design cryptanalytic attacks and analyze the effectiveness of cryptographic systems. Familiarity with frameworks and libraries for performing cryptanalysis. Development of skills to critically evaluate the security of cryptographic protocols, considering both theoretical and practical aspects.		
<i>Selbstkompetenz:</i>	Strong critical thinking and problem-solving abilities, with the capacity to adapt methods based on new findings and emerging challenges in the cryptographic landscape.		

<i>Sozialkompetenz:</i>	Effective communication of cryptographic vulnerabilities and attack methodologies, both in written and verbal formats. Contribution to collective learning through active participation in seminars, case study presentations, and research discussions.							
<i>Arbeitslast:</i>	60 Stunden Lehrveranstaltungen 90 Stunden Vor- und Nachbereitung der Lehrveranstaltungen, Prüfungsvorbereitung							
<i>Anbieter:</i>	<u>03 Fakultät Angewandte Computer- und Biowissenschaften</u>							
<i>Dozententeam (Rollen):</i>	<u>Prof. Dr. rer. nat. Klaus Dohmen</u> (Dozent, Inhaltverantwortlicher, Prüfer, Aufsicht) <u>Prof. Dr. rer. nat. habil. Thomas Villmann</u> (<u>Dr. Mandy Lange-Geisler</u> (Planer, Prüfer) <u>Prof. Dr. rer. nat. Franka Baaske</u> (Planer)							
<i>Teilnahmevoraussetzungen:</i>	Modul Foundations of Modern Cryptography							
<i>Lerneinheitsformen und Prüfungen:</i>	<i>Modulstruktur</i>	<i>V</i>	<i>S</i>	<i>P</i>	<i>T</i>	<i>PVL</i>	<i>PL</i>	<i>CP</i>
	<u>Cryptanalysis</u>	2	1	1	0		Ma	5

7715 Social Engineering und OSINT

<i>Modulname:</i>	Social Engineering und OSINT	<i>Unterrichtssprache:</i>	deutsch					
<i>Modulnummer:</i>	7715	<i>Abschluss:</i>	M.Sc.					
<i>Modulcode:</i>	03-CSEO	<i>Häufigkeit:</i>	jahresweise					
<i>Pflicht/Wahl:</i>	Pflicht	<i>Dauer:</i>	1					
<i>Studiengang:</i>	Cybercrime/ Cybersecurity	<i>Regelsemester:</i>	3					
<i>Ausbildungsziele:</i>	Die Studierenden verfügen über Wissen zu den Grundlagen von Social Engineering. Sie sind mit gängigen Techniken vertraut und kennen die psychologischen Grundlagen der einzelnen Angriffsmuster. Sie kennen Abwehrstrategien gegen Social Engineering und sind in der Lage Sicherheitsrichtlinien und Schulungen zu entwickeln. Jeder Teilnehmer kennt die Möglichkeiten von OSINT (Open Source Intelligence) zur Datengewinnung. Er kann selbstständig Werkzeuge einsetzen um Daten automatisiert zu sammeln, zusammenzuführen und auszuwerten. Dabei wird er mit den Besonderheiten von Big Data konfrontiert. Alle Kursteilnehmer sind vertraut mit der Daten Gewinnung aus Sozialen Netzwerken, Webseiten, Medien und anderen offenen Quellen. Sie lernen Personen zu identifizieren und zu lokalisieren.							
<i>Lehrinhalte:</i>	Grundlagen des Social Engineering • Reziprozität • Konsistenz • Commitement Andrere Techniken • Phishing • Dumpster Diving Abwehrstrategien gegen Social Engineering Grundlagen von OSINT • Arten von offenen Quellen • Automatisiertes Sammeln von Informationen • Zusammenführen von Informationen • Auswertung offener Quellen • Big Data							
<i>Lernmethoden:</i>	Die seminaristisch durchgeführte Vorlesung vermittelt grundlegende (theoretische) Kenntnisse mittels Folien, Beamer-Präsentationen und Tafel. Im betreuten Praktikum bearbeiten die Studenten an ausgewählte Problemen aus dem Bereich Social Engineering und OSINT. Diese werden vertiefend diskutiert und typisch Strategien und Angriffsmuster an Beispielszenarien aufgezeigt. Für das Selbststudium werden konkrete Anregungen gegeben.							
<i>Literatur:</i>	• Kevin D. Mitnick, William L. Simon: Die Kunst der Täuschung. Risikofaktor Mensch. mitp, Heidelberg 2006 • Cialdini, R. B.: Die Psychologie des Überzeugens. Verlag Hans Huber, 2007. • Stefan Schumacher: Psychologische Grundlagen des Social Engineering. In: Die Datenschleuder. 94, 2010 • Arthuer S. Hulnick: 'The Dilemma of Open Source Intelligence: Is OSINT Really Intelligence?', pages 229-241, The Oxford Handbook of National Security Intelligence, 2010 -Andreas Weyert : Hacking mit Kali. Francis, 2014.							
<i>Arbeitslast:</i>	60 Stunden Lehrveranstaltungen 90 Stunden Vor- und Nachbereitung der Lehrveranstaltungen, Prüfungsvorbereitung							
<i>Anbieter:</i>	03 Fakultät Angewandte Computer- und Biowissenschaften							
<i>Dozententeam (Rollen):</i>	Prof. Dr. rer. nat. Dirk Labudde (Dozent, Inhaltverantwortlicher)							
<i>Lerneinheitsformen und Prüfungen:</i>	<i>Modulstruktur</i>	<i>V</i>	<i>S</i>	<i>P</i>	<i>T</i>	<i>PVL</i>	<i>PL</i>	<i>CP</i>
	Social Engineering und OSINT	1	0	3	0		Mm/30	5

7716 Komplexpraktikum Forensische Methoden

Modulname:	Komplexpraktikum Forensische Methoden	Unterrichtssprache:	deutsch					
Modulnummer:	7716	Abschluss:	M.Sc.					
Modulcode:	03-CKPFM	Häufigkeit:	jahresweise					
Pflicht/Wahl:	Pflicht	Dauer:	1					
Studiengang:	Cybercrime/ Cybersecurity	Regelsemester:	3					
Ausbildungsziele:	Die Bedrohungslage für Unternehmen und Behörden steigt immer weiter an: laut Bitkom waren von 2015 bis 2016 53% der Unternehmen in Deutschland direkt von Wirtschaftsspionage, Sabotage oder Datendiebstahl betroffen - Tendenz steigend. Durch die zunehmende Vernetzung von Geräten und Diensten Vergrößert sich die virtuelle Angriffsfläche in Organisationen. Damit wachsen auch die unmittelbaren Auswirkungen eines Cyber-Angriffs und die damit verbundenen Schäden innerhalb einer Organisation. Um bei Angriffen oder Notfällen eine strukturierte und zielführende Vorgehensweise zu wahren, ist ein wirkungsvolles Krisenmanagement erforderlich. Dies stellt eine komplexe Aufgabe dar, da viele verschiedene Akteure berücksichtigt werden müssen. Hinzu kommt ein geringes Risiko- und Gefahrenbewusstsein innerhalb von Organisationen. -Das eigene Bewusstsein für die Gefahren von Cyberangriffen bezogen auf den Einzelnen und ganze Unternehmen schärfen • Souverän in Krisensituationen reagieren zu können • Die Verbesserung der Kommunikation sowie die gemeinsame Lösungsfindung im Krisenfall • die eigenen Abläufe und interne sowie externe Prozesse in Krisensituationen besser nachvollziehen können							
Lehrinhalte:	• Kommunikationstheorie • Entscheidungsmodell und Problemlösungsprozess • Krisensimulation • Review der Simulation							
Lernmethoden:	Simulation von realitätsnahen Krisensituationen Handlungsorientierte Empfehlungen zur Lösung von Krisensituationen Business Impact Analyse und Entwicklung eines Risikomodells							
Literatur:								
Arbeitslast:	60 Stunden Lehrveranstaltungen 90 Stunden Vor- und Nachbereitung der Lehrveranstaltungen, Prüfungsvorbereitung							
Anbieter:	03 Fakultät Angewandte Computer- und Biowissenschaften							
Dozententeam (Rollen):								
Lerneinheitsformen und Prüfungen:	Modulstruktur	V	S	P	T	PVL	PL	CP
	Komplexpraktikum Forensische Methoden	0	2	2	0			5
	Teilprüfung 1						PI4sn/LB	
	Teilprüfung 2						PI4sn/LB	

7717 Entwurf sicherer Systeme

Modulname:	Entwurf sicherer Systeme	Unterrichtssprache:	deutsch					
Modulnummer:	7717	Abschluss:	M.Sc.					
Modulcode:	03-CESS	Häufigkeit:	jahresweise					
Pflicht/Wahl:	Pflicht	Dauer:	1					
Studiengang:	Cybercrime/ Cybersecurity	Regelsemester:	3					
Ausbildungsziele:	Ziel des Moduls ist es, den Studierenden Wissen über den Entwurf sicherer Systeme zu vermitteln. Nach dem Absolvieren dieses Kurses verfügen die Teilnehmer insbesondere über vertiefte Kenntnisse sowie Fertigkeiten bei der Planung um Umsetzung sicherer IT-Systeme. Sie sind vertraut mit wesentlichen Design-Prinzipien und Verfahren in diesem Bereich und können das Erlernte auch praktisch anwenden. Jeder Teilnehmer kann ein bestehendes System in Bezug auf Schwachstellen analysieren und Schutzmaßnahmen formulieren.							
Lehrinhalte:	• Objektorientierte Modellierung und Entwurf, Designpattern • Security by Design • Defense in Depth,Multilevel Security • Bedrohungsanalysen • Multilateral Security • Attack Surface Reduction • Least Privilege • Design for Evil • Security through Diversity Design und Bewertung von Security Policies, Sicherheitsmechanismen Schwachstellen-Analyse und Angriffssimulation							
Lernmethoden:	Im Rahmen der seminaristisch durchgeführten Lehrveranstaltung werden wichtige theoretische und praxisrelevante Grundlagen vermittelt. In diesem Zusammenhang werden ausgewählte Probleme vertiefend diskutiert und Strategien zur Problemlösung vorgestellt. Anhand von konkreten Fallbeispielen werden Sicherheitsprobleme sowie mögliche Lösungsstrategien erörtert. Für das Selbststudium werden konkrete Anregungen und Aufgaben gestellt. Die Lehrinhalte werden mittels Folien, Beamer-Präsentationen, Tafel dargestellt.							
Literatur:	• Eckert, C.: IT-Sicherheit: Konzepte, Verfahren, Protokolle. 7. Auflage, Oldenbourg-Verlag, 2012. • Skriha, Walter, Schmitz, Roland: Sichere Systeme: Konzepte, Architekturen und Frameworks. Springer Verlag, 2009.							
Arbeitslast:	60 Stunden Lehrveranstaltungen 90 Stunden Vor- und Nachbereitung der Lehrveranstaltungen, Prüfungsvorbereitung							
Anbieter:	03 Fakultät Angewandte Computer- und Biowissenschaften							
Dozententeam (Rollen):	Prof. Dr. rer. pol. Dirk Pawlaszczyk (Inhaltverantwortlicher)							
Lerneinheitsformen und Prüfungen:	Modulstruktur	V	S	P	T	PVL	PL	CP
	Entwurf sicherer Systeme	2	0	2	0		Mm/30	5

7718 Datennetze/ Cloud Forensik

Modulname:	Datennetze/ Cloud Forensik	Unterrichtssprache:	deutsch					
Modulnummer:	7718	Abschluss:	M.Sc.					
Modulcode:	03-CDNCF-21	Häufigkeit:	jahresweise					
Pflicht/Wahl:	Pflicht	Dauer:	1					
Studiengang:	Cybercrime/ Cybersecurity	Regelsemester:	3					
Ausbildungsziele:	Die Studierenden verfügen über Wissen zu den technischen Grundlagen von Cloudanwendungen. Sie sind vertraut mit den gängigen Verfahren zur Datensicherheit lokal und innerhalb der Cloud. Jeder Teilnehmer kennt die Besonderheiten und Herausforderungen bei der forensischen Analyse von Clouddaten. Alle Kursteilnehmer sind vertraut mit der Handhabung forensischer Werkzeuge, die für die Sicherstellung und Untersuchung von digitalen Spuren innerhalb der Cloud verwendet werden können und wenden diese praktisch an.							
Lehrinhalte:	Cloud Computing Stack, Cloud Security and Privacy, Internet-fähige Endgeräte, Smartphones und Cloud Computing, Besonderheiten des forensischen Untersuchungsprozesses in Cloudumgebungen, technische und rechtliche Aspekte, konkrete Vorgehensmodelle und Handlungsanweisungen für die Untersuchung von Cloud-Storage-Lösungen, Verschlüsselung von Cloud-Daten, forensische Analyse aktueller Cloud-Anwendungen (Dropbox, Micosoft Aszure, Cloudflare, Amazon Cloud Front, Amazone S3, Google Drive etc.)							
Lernmethoden:	Die seminaristisch durchgeführte Vorlesung vermittelt grundlegende (theoretische) Kenntnisse mittels Folien, Beamer-Präsentationen und Tafel. Im betreuten Praktikum bearbeiten die Studenten ausgewählte Aufgaben aus dem Bereich Datennetze / Cloud Forensik. Für das Selbststudium werden konkrete Anregungen gegeben.							
Literatur:	• Raymond Choo, Darren Quick, Ben Martini : Cloud Storage Forensics. 1. Edition. Elsevier LTD, Oxford (2014) • Keyun Ruan: Cybercrime and Cloud Forensics Applications for Investigation Processes (2013) • Wilie E. May: NIST Cloud Computing 2 Forensic Science Challenges. Draft NISTIR 8006 (2014) • Josiah A. Dykstra: Digital Forensics for Infrastructure-as-a-Service Cloud Computing. Dissertation. (2013) http://www.cisa.umbc.edu/papers/dissertations/dykstra-dissertation-2013.pdf • Cloud Computing Security, Roland L. Krutz and Russel Dean Vines, 2010, Wiley.							
Arbeitslast:	60 Stunden Lehrveranstaltungen 90 Stunden Vor- und Nachbereitung der Lehrveranstaltungen, Prüfungsvorbereitung							
Anbieter:	<u>03 Fakultät Angewandte Computer- und Biowissenschaften</u>							
Dozententeam (Rollen):								
Lerneinheitsformen und Prüfungen:	Modulstruktur	V	S	P	T	PVL	PL	CP
	<u>Datennetze/ Cloud Forensik</u>	2	0	2	0		Mm/30	5

7719 Car Forensics

Modulname:	Car Forensics	Unterrichtssprache:	deutsch					
Modulnummer:	7719	Abschluss:	M.Sc.					
Modulcode:	03-CCF	Häufigkeit:	jahresweise					
Pflicht/Wahl:	Wahlpflicht	Dauer:	1					
Studiengang:	Cybercrime/ Cybersecurity	Regelsemester:	3					
Ausbildungsziele:	Die Digitalisierung von Kraftfahrzeugen schreitet stetig voran. Neben elektronischen Steuergeräten, die in modernen Fahrzeugen verbaut sind, entstehen in Themenfeldern wie Car2Car-, Car2Infrastructure und Car2Person-Kommunikation neue Felder, die eine Spezialisierung der elektronischen Forensik in den Bereich Car Forensics unabdingbar machen. Trotz der stetig wachsenden Bedeutung von Kfz für die Kriminalistik, gilt die forensische Untersuchung von Fahrzeugen als teuer und kompliziert. Im Modul "Car Forensics" sollen verbreitete Standards, Bussysteme und Grundlagen der Architektur von Steuergeräten in Kfz strukturiert dargestellt werden. In einem zweiten Teil sollen forensische Tools für Fahrzeuge vorgestellt und Szenarien erörtert werden. Nach Abschluss des Moduls sollen die Studierenden Kompetenzen im Bereich Car Forensics der Art erworben haben, dass sie selbstständig in der Lage sind derart gelagerte Spureinträger zu untersuchen.							
Lehrinhalte:	• Bussysteme: CAN, LIN, K-Line • Grundlagen und Begriffe der Car Forensics • Steuergeräte: insbesondere Funktion von Wegfahrsperrern • Kfz-Untersuchungen • Architektur von Kfz, insbesondere Fahrzeugelektronik • Forensische Tools • Car2Car-, Car2Infrastructure und Car2Person-Kommunikation							
Lernmethoden:	Das Seminar vermittelt grundlegende (theoretische) Kenntnisse mittels Folien, Beamer-Präsentationen und Tafel in kleinen Gruppen. An Beispielen sollen die Studierenden mit der Materie vertraut gemacht werden. Im betreuten Praktikum sollen die Studenten eigenständig Datensicherungen an Kraftfahrzeugen durchführen und die gewonnenen Daten selbstständig auswerten. Im Seminar werden ausgewählte Themen vertieft und Aufgaben gemeinsam erarbeitet. Für das Selbststudium werden konkrete Anregungen gegeben.							
Literatur:	In dem jungen Forschungsfeld haben sich noch keine Standardwerke etabliert. Die Studierenden erhalten Skripte und aktuelle Forschungsergebnisse im Seminar. • Thomas Käfer: Car-Forensics. Books on Demand, 2015.							
Arbeitslast:	60 Stunden Lehrveranstaltungen 90 Stunden Vor- und Nachbereitung der Lehrveranstaltungen, Prüfungsvorbereitung							
Anbieter:	03 Fakultät Angewandte Computer- und Biowissenschaften							
Dozententeam (Rollen):	Dipl.-Ing. (FH) Heiko Polster (Dozent, Inhaltverantwortlicher)							
Lerneinheitsformen und Prüfungen:	Modulstruktur	V	S	P	T	PVL	PL	CP
	Car Forensics	0	2	2	0	PA	Mm/30	5

7720 Predictive Policing/Dunkelfeld

<i>Modulname:</i>	Predictive Policing/Dunkelfeld	<i>Unterrichtssprache:</i>	deutsch
<i>Modulnummer:</i>	7720	<i>Abschluss:</i>	M.Sc.
<i>Modulcode:</i>	03-CPPDF	<i>Häufigkeit:</i>	jahresweise
<i>Pflicht/Wahl:</i>	Wahlpflicht	<i>Dauer:</i>	1
<i>Studiengang:</i>	Cybercrime/ Cybersecurity	<i>Regelsemester:</i>	3
<i>Ausbildungsziele:</i>	In der Kriminalforschung bezeichnet das Dunkelfeld die Differenz zwischen den amtlich registrierten Straftaten, dem Hellfeld, und der vermutlich begangenen Kriminalität. Allein durch die Kriminalstatistiken kann vom Hellfeld nicht auf die tatsächliche Kriminalität geschlossen werden. Daher bedarf es der Dunkelfeldforschung, um das Dunkelfeld aufzuheben und einen systematischen Überblick über die Kriminalitätsentwicklung zu erreichen. Predictive Policing hingegen bezeichnet die Analyse von Falldaten zur Berechnung der Wahrscheinlichkeit zukünftiger Straftaten zur Steuerung des Einsatzes von Polizeikräften Nach Abschluss des Moduls können die Studierenden die amtlichen Kriminalstatistiken lesen und verstehen. Sie kennen die aktuellen Verfahren um Aussagen über das Dunkelfeld und damit über die tatsächliche Kriminalität zu treffen. Die Studierenden erhalten ein differenziertes Bild von der Möglichkeit des Predictive Policing und Aussagekraft von Aussagen über die Vorhersage von Straftaten. Sie können mit einfachen Methoden selbstständig Modelle entwickeln. Nach Abschluss des Moduls verfügen die Studierenden über einen abgerundeten Überblick über das Fachgebiet. Sie können selbstständig Modellansätze entwerfen und eigenständig berechnen.		
<i>Lehrinhalte:</i>	• Die Polizeiliche Kriminalstatistik • Hellfeld und Dunkelfeld • Kriminalitätsmessung • Kriminalitätsanalyse und kriminalstatistische Forschung • "Ethnic Profiling" • Re-Victimisierung • Ethische Implikationen von Predicted Policing • Rational-Choice-Theorie • Boost-Hypothese • Flag-Hypothese • Near-Repeat-Victimisation • Methoden zur Vorhersage • Modellierung von Kriminalität • Extrapolationsalgorithmen • Validierung von Kriminalitätsmodellen		
<i>Lernmethoden:</i>	Im Rahmen der seminaristischen Vorlesung werden wichtige theoretische Grundlagen vermittelt werden. In diesem Zusammenhang werden auch ausgewählte Probleme vertiefend diskutiert und Strategien zur Problemlösung vorgestellt. Anhand von konkreten Problemen werden die Studierenden mit Herangehensweisen konfrontiert und ausgewählte Themen werden eingehend erörtert. Für das Selbststudium werden konkrete Anregungen und Aufgaben gestellt. Im Praktikum sollen verschiedene Algorithmen aus dem Bereich Predictive Policing/Dunkelfeld in Software implementiert werden.		
<i>Literatur:</i>	• Uwe Dörmann, Wolfgang Heinz: Zahlen sprechen nicht für sich. Aufsätze zu Kriminalstatistik, Dunkelfeld und Sicherheitsgefühl aus drei Jahrzehnten. Luchterhand, 2004. • Thomas Feltes, Benjamin Schmidt: Policing Diversity: Über den Umgang mit gesellschaftlicher Vielfalt innerhalb und außerhalb der Polizei. Verlag für Polizeiwissenschaft, 2015. • John S. Dempsey, Linda S. Forst: An Introduction to Policing, Delmar Cengage Learning, 2015. • Runtker Rienks: Predictive Policing: Taking a Chance for a Safer Future. Korpsmedia, 2015. • Graham Farrell, Ken Pease: Once Bitten, Twice Bitten: Repeat Victimisation and its Implications for Crime Prevention. Crime Prevention Unit Series Paper No. 46, London, 1993.		
<i>Arbeitslast:</i>	60 Stunden Lehrveranstaltungen 90 Stunden Vor- und Nachbereitung der Lehrveranstaltungen, Prüfungsvorbereitung		
<i>Anbieter:</i>	<u>03 Fakultät Angewandte Computer- und Biowissenschaften</u>		
<i>Dozententeam (Rollen):</i>	<u>Prof. Dr. rer. nat. Dirk Labudde</u> (Dozent)		

Lerneinheitsformen und Prüfungen:	Modulstruktur	V	S	P	T	PVL	PL	CP
	<u>Predictive Policing/Dunkelfeld</u>	1	1	2	0	LT	Mm/30	5

7721 Digitale Werte und Güter

<i>Modulname:</i>	Digitale Werte und Güter	<i>Unterrichtssprache:</i>	deutsch
<i>Modulnummer:</i>	7721	<i>Abschluss:</i>	M.Sc.
<i>Modulcode:</i>	03-CDWUG	<i>Häufigkeit:</i>	jahresweise
<i>Pflicht/Wahl:</i>	Wahlpflicht	<i>Dauer:</i>	1
<i>Studiengang:</i>	Cybercrime/ Cybersecurity	<i>Regelsemester:</i>	3
<i>Ausbildungsziele:</i>	Digitale Werte und Güter sind hochaktuelle Themen und haben weitreichende gesellschaftliche Einflüsse. Dank digitaler Technologien können heutzutage Transaktionen grenzenlos und ohne Einfluss von Regierungen durchgeführt werden. Dies eröffnet nicht nur große gesellschaftliche Chancen wie länderübergreifende Kommunikation oder weltweiten Geldtransfer, sondern auch Gefahren und Risiken. Unternehmen und Forschungseinrichtungen setzen in zunehmendem Maße auf Technologien wie der Blockchain, um Dienste zu dezentralisieren. Auch Regierungen haben das Thema erkannt und bemühen sich, sinnvolle Regulierungs- und Überwachungsmethoden zu implementieren. Dank des erworbenen Fach- und Methodenwissens sind die Teilnehmer in der Lage • Dienste, die auf der Blockchaintechnologie beruhen, zu entwerfen, implementieren, administrieren und zu testen • Unternehmen, die auf die Blockchaintechnologie setzen, zu beraten. • Systeme, die auf der Blockchaintechnologie aufbauen, zu bewerten. Die Teilnehmer lernen und nutzen während des Studiums moderne Methoden und Werkzeuge und wenden diese für ihre eigenen Lösungen an.		
<i>Lehrinhalte:</i>	Grundlagen • Grundlagen Kryptografie und Kryptowährungen • Dezentralisierung durch die Blockchain, Konsensfindung • Erzeugen einer eigenen BTC-Adresse, Umgang mit Wallets, Erzeugen von Transaktionen, Verfolgen von Transaktionen im Netzwerk, Anonymität im Netzwerk, Alternative Mining Puzzles Erzeugen einer Altcoin • Aufsetzen eines eigenen Altcoin-Clients • Umsetzung einer Miningsoftware für die Altcoin • Durchführung von Angriffsszenarien innerhalb der Altcoin Gesellschaftliche Einordnung von Bitcoin • Regulierung • Geschichte • Community		
<i>Lernmethoden:</i>	Die seminaristisch durchgeführte Vorlesung vermittelt grundlegende (theoretische) Kenntnisse mittels Folien, Beamer-Präsentationen und Tafel. Im betreuten Praktikum bearbeiten die Studenten ausgewählte Fälle aus dem Feld: Digitale Werte und Güter. Für das Selbststudium werden konkrete Anregungen gegeben.		
<i>Literatur:</i>	• Andreas M. Antonopoulos: Mastering Bitcoin. O'Reilly Media, 2013. • Melanie Swan: Blockchain: Blueprint for a New Economy. O'Reilly and Associates, 2015. • Christof Paar, Jan Pelzl: Understanding Cryptography: A Textbook for Students and Practitioners. Springer, 2011.		
<i>Arbeitslast:</i>	60 Stunden Lehrveranstaltungen 90 Stunden Vor- und Nachbereitung der Lehrveranstaltungen, Prüfungsvorbereitung		
<i>Anbieter:</i>	03 Fakultät Angewandte Computer- und Biowissenschaften		
<i>Dozententeam (Rollen):</i>	Prof. Dr.-Ing. Andreas Ittner (Dozent, Inhaltverantwortlicher)		
<i>Lerneinheitsformen und Prüfungen:</i>	<i>Modulstruktur</i> <u>Digitale Werte und Güter</u>	<i>V</i> <i>S</i> <i>P</i> <i>T</i> <i>PVL</i> <i>PL</i> <i>CP</i> 2 0 2 0 Ms/90 5	

7722 Masterprojekt

Modulname:	Masterprojekt	Unterrichtssprache:	deutsch					
Modulnummer:	7722	Abschluss:	M.Sc.					
Modulcode:	03-MPCY	Häufigkeit:	jahresweise					
Pflicht/Wahl:	Pflicht	Dauer:	1					
Studiengang:	Cybercrime/ Cybersecurity	Regelsemester:	4					
Ausbildungsziele:	Die Masterarbeit kann in einem Unternehmen, einer Behörde, einer anderen Einrichtung oder an der Hochschule durchgeführt werden. Ziel ist der Nachweis der Fähigkeit, sich wissenschaftlich und selbständig mit einem abgeschlossenen Thema im Bereich Cyercrime/Cybersecurity auseinanderzusetzen. Bisher erworbenes Wissen und praktische Fähigkeiten werden angewendet und erweitert. Es soll damit die Berufsbefähigung nachgewiesen werden. Die Studierenden sind in der Lage: • Fachbezogene Inhalte und Konzepte darzustellen sowie Kenntnisse einschlägiger Forschungsgebiete anzuwenden. • Sie erkennen und formulieren Problemstellungen und können diese innerhalb eines vorgegebenen Zeitraums Lösen • Sie können sich neues Wissen selbständig aneignen und sind in der Lage, neue Erkenntnisse zur o. g. Problemstellung zu gewinnen							
Lehrinhalte:	Disziplinübergreifende und fachspezifische Mitarbeit an Industrie-, Forschungs- und Entwicklungsprojekten sowie Machbarkeitsstudien.							
Lernmethoden:	Selbständiges, wissenschaftliches Lernen allein oder im Team unter wissenschaftlicher Anleitung. Abschließendes Kolloquium (Präsentation und Diskussion)							
Literatur:								
Arbeitslast:	30 Stunden Lehrveranstaltungen 870 Stunden Vor- und Nachbereitung der Lehrveranstaltungen, Prüfungsvorbereitung							
Anbieter:	03 Fakultät Angewandte Computer- und Biowissenschaften							
Dozententeam (Rollen):								
Lerneinheitsformen und Prüfungen:	Modulstruktur	V	S	P	T	PVL	PL	CP
	Masterprojekt	0	0	0	1			30
	Masterarbeit						MA	
	Tutorium für Examenskandidaten	0	0	0	1			
	Kolloquium						PI4sn/K30	