Ermittlung pauschal anrechnungsfähiger Lernergebnisse auf hochschulische Studiengänge

vorläufiges

Modulhandbuch

Bachelorstudiengang

IT-Sicherheit

Open C³S

Gefördert vom:
Bundesministerium für Bildung und Forschung
ESF Europäischer Sozialfonds für Deutschland
EUROPÄISCHE UNION
AUFSTIEG DURCH BILDUNG >> OFFENE HOCHSCHULEN

Modulbeschreibung

Studiengang:	Bachelor IT-Sicherheit
Modulbezeichnung:	Einführung in die IT-Sicherheit
Lehrveranstaltungen:	Einführung in die IT-Sicherheit
Dozent(in):	Prof. Dr. Daniel Hammer
Modulverantwortliche(r):	Prof. Dr. Daniel Hammer
Modulentwickler(in):	
Inhalt:	Im Modul Einführung in die IT-Sicherheit wird auf folgende Themengebiete eingegangen: • Grundlagen des Sicherheitsmanagements, des Risikomanagements und der -analyse • Notfallplanung • Bedrohungsfaktoren der IT-Sicherheit und deren Schutzmaßnahmen • Grundlagen der Zugriffskontrolle und -verwaltung • Mechanismen der Authentisierung, SSO-Technologien • Darstellung der Angriffe auf Zugriffskontrollsysteme • Einführung in die Kryptographie, symmetrische und asymmetrische Verschlüsselungsverfahren, Darstellung der Angriffe auf Kryptosysteme, kryptographische Hashfunktionen, digitale Signatur • Einführung in die Steganographie • Einführung in die Sicherheitsaspekte vernetzter Umgebungen, Grundlagen des DNS, E-Mail-Missbrauch • Spam, Phishing, Network Security

Lernziele/Kompetenzen:	*Fachkompetenz:* Die Studierenden erwerben Grundkenntnisse des Sicherheitsmanagements, des Risikomanagements und der -analyse. Die Studierenden eignen sich Grundlagen der Zugriffskontrolle und -verwaltung an, können Mechanismen der Authentisierung unterscheiden und erklären und SSO-Technologien beschreiben. Sie sind in der Lage die unterschiedlichen Angriffe auf Zugriffskontrollsysteme darzustellen. Sie erwerben Grundkenntnisse der Kryptographie und Steganographie, können symmetrische und asymmetrische Verschlüsselungsverfahren differenzieren, Angriffe auf Kryptosysteme darstellen, kryptographische Hashfunktionen und digitale Signatur erklären. Die Studierenden erlangen das Grundwissen über die Sicherheitsaspekte vernetzter Umgebungen. Dabei erwerben sie die Grundlagen des DNS und sind in der Lage sie zu erläutern. Sie können einen E-Mail-Missbrauch erklären und Spam, sowie Phishing aufzeigen und ihre Lösungsansätze darstellen. *Methodenkompetenz:* Die Studierenden können eine Notfallplanung erläutern, die Bedrohungsfaktoren der IT-Sicherheit beschreiben und klassifizieren und deren Schutzmaßnahmen anwenden bzw. eigenständig skizzieren. Der Lernende kann die Phasen eines Hackerangriffs aufzeigen und erwirbt Kenntnisse über Malware und die entsprechenden Schutzmaßnahmen. *Sozialkompetenz:* Aufgrund der Teamarbeit, unter anderem in dem Präsenzwochenende, erweitern die Studierenden die Fähigkeit der Teamfähigkeit und Sozialkompetenz. Die Studierenden erlangen die Fähigkeit zur Bildung einer Meinung über IT-Sicherheit. Darüber hinaus erlangen die Studierenden die Fähigkeit, in komplexen Situationen zu handeln und eine Lösung für schwierige Probleme zu finden.
Notwendige Voraussetzungen:	
Empfohlene Voraussetzungen:	
Einpassung in den Studienplan:	Ab Studiensemester 1
Verwendbarkeit des Moduls:	Dieses Modul ist verwendbar für • Studierende der Informatik • Studierende der Wirtschaftsinformatik • Studierende der Mathematik und Informatik auf Bachelorniveau. Dieses Modul kann nicht als Wahlpflichtmodul gewählt werden, sondern ist ein Pflichtmodul.
Studien- und Prüfungsleistungen:	Schriftliche Prüfung: 60 min.
Berechnung der Modulnote:	Schriftliche Prüfung
Turnus des Angebots:	in jedem Semester
Wiederholung der Prüfungen:	
Anerkannte Module:	
Anerkannte Lernergebnisse:	

Generelle Zielsetzung des Moduls:	Modul zur Einführung in das Basiswissen der IT-Sicherheit
Arbeitsaufwand bzw. Gesamtworkload:	Präsenzstudium: 15 Zeitstunden Fernstudienanteil: 135 Zeitstunden • Selbststudium: 105 Zeitstunden • Aufgaben: 20 Zeitstunden • Online-Betreuung: 10 Zeitstunden Summe: 150 Zeitstunden
Lerninhalt und Niveau:	Das Niveau der Lerninhalte liegt gemessen am DQR-Niveau bei 6 (Bachelor)
Leistungspunkte:	5 ECTS
Moduldauer:	1 Semester
Unterrichtssprache:	Deutsch
Medienformen:	Studienbriefe in schriftlicher und elektronischer Form, Onlinematerial in Lernplattform, Übungen und Projekt über Lernplattform, Online-Konferenzen, Chat und Forum, Präsenzveranstaltung mit Rechner und Beamer.
Literatur:	• Sicherheit in Informationssystemen, (Vorlesungsskript), Daniel Hammer, 2012 • Angewandte Kryptographie, Bruce Schneier, 1996 • Netzsicherheit, Günter Schäfer, 2003 • Cyberwar, Sandro Gaycken, 2011 Weitere Literatur wird in der Lehrveranstaltung bekannt gegeben.

Modulbeschreibung

Studiengang:	Bachelor IT-Sicherheit
Modulbezeichnung:	Grundlagen der Programmierung
Lehrveranstaltungen:	Einführung in das Programmieren, Programmierkonzepte
Dozent(in):	Prof. Dr. Felix Freiling
Modulverantwortliche(r):	Prof. Dr. Felix Freiling
Modulentwickler(in):	
Inhalt:	Eine Einführung in die Programmiersprache Java. Mit Hilfe der Entwicklungsumgebung BlueJ wird den Studierenden der Umgang mit Java vertraut gemacht: • Ausdrücke und algorithmische Kernsprache von Java • Sprachbeschreibung und Objekttypen • Eine Einführung in bereits existierende Methoden und Klassen in der Programmiersprache Java
Lernziele/Kompetenzen:	*Fachkompetenz:* Die Studierenden erwerben fundierte Kenntnisse über die Programmiersprache Java sowie deren Syntax und Semantik. Sie können mit der Entwicklungsumgebung BlueJ umgehen und Java Programme entwickeln sowie diese inspizieren. Die Studierenden können Klassen und Methoden selbständig erzeugen und auswerten. *Methodenkompetenz:* Die Studierenden beherrschen die Arbeitstechnik, mit der Entwicklungsumgebung BlueJ umzugehen. Weiter beherrschen sie die Problemlösefähigkeit ein Java Programm auf Fehler zu untersuchen. *Sozialkompetenz:* Durch das gemeinsame Lösen von Aufgaben erlangen die Studierenden die Fähigkeit eigene Handlungsziele mit den Einstellungen und Werten einer Gruppe zu verknüpfen und ihre Teamfähigkeit zu stärken. Die Studierenden erlangen die Fähigkeit zur Bildung einer Meinung über eigene Programme und Programme anderer. Darüber hinaus erlangen sie die Fähigkeit in komplexen Situationen zu handeln und eine Lösung für komplexe Probleme zu finden.
Notwendige Voraussetzungen:	Für die Lehrveranstaltung „Programmierkonzepte“ ist die Teilnahme an der Lehrveranstaltung „Einführung in das Programmieren“ eine notwendige Voraussetzung.
Empfohlene Voraussetzungen:	
Einpassung in den Studienplan:	Einführung in das Programmieren (ab Studiensemester 1), Programmierkonzepte (ab Studiensemester 2)

Verwendbarkeit des Moduls:	Dieses Modul ist verwendbar für • Studierende der Informatik • Studierende der Wirtschaftsinformatik • Studierende der Mathematik und Informatik auf Bachelorniveau. Dieses Modul kann nicht als Wahlpflichtmodul gewählt werden, sondern ist ein Pflichtmodul.
Studien- und Prüfungsleistungen:	Schriftliche Prüfung: 120 min.
Berechnung der Modulnote:	Schriftliche Prüfung
Turnus des Angebots:	Wintersemester (Einführung in das Programmieren), Sommersemester(Programmierkonzepte)
Wiederholung der Prüfungen:	
Anerkannte Module:	
Anerkannte Lernergebnisse:	
Generelle Zielsetzung des Moduls:	Zur Förderung und Verstärkung der Fachkompetenz
Arbeitsaufwand bzw. Gesamtworkload:	Summe: 300 h Präsenzzeit: 60 h • Vorlesungsteil: 20 h • Übungsteil: 10 h • Praktischer Teil: 20 h • Prüfungsvorbereitungsveranstaltung: 8 h • Prüfung: 2 h Eigenstudium: 240 h • Durcharbeiten der Studienbriefe: 100 h • Durcharbeiten des Online-Lernmaterials: 20 h • Wahrnehmen der Online Betreuung und Beratung: 20 h • Ausarbeiten von Aufgaben: 60 h • Individuelle Prüfungsvorbereitung der Studierenden: 40 h
Lerninhalt und Niveau:	Niveau der Lerninhalte liegt gemessen am DQR-Niveau bei 6 (Bachelor)
Leistungspunkte:	10 ECTS
Moduldauer:	2 Semester
Unterrichtssprache:	Deutsch
Medienformen:	Studienbriefe in schriftlicher und elektronischer Form, Onlinematerial in Lernplattform, Übungen und Projekte über Lernplattform, Online-Konferenzen, Chat und Forum, Präsenzveranstaltungen mit Computer und Beamer

Literatur:	Begleitende und vertiefende Literatur wird empfohlen: 1. Touch of class, Betrand Mayer, 2009 2. IT-Sicherheit, Claudia Eckert, 2012 3. Handbuch Java Band 1, Universität Hannover, 2010 4. Einführung in Java mit BlueJ, Florian Siebler, 2011 5. Java lernen mit BlueJ, David J. Barnes, Michael Kölling, 2006 Weitere Literatur wird in der Lehrveranstaltung bekanntgegeben.

Modulbeschreibung

Studiengang:	Bachelor It-Sicherheit
Modulbezeichnung:	Mathematik 1
Lehrveranstaltungen:	Mathematik 1
Dozent(in):	Prof. Dr. Harald Baier
Modulverantwortliche(r):	Prof. Dr. Harald Baier
Modulentwickler(in):	
Inhalt:	In diesem Modul werden die folgenden Themengebiete behandelt: • Grundlagen (Mengen, Elementare Aussagelogik, Beweisverfahren, reelle und komplexe Zahlen) • Vektoren und Vektorräume (Vektorrechnung im ^{3}, Begriff des Vektorraums, Beispiele für Vektorräume) • Matrizen, Determinanten, Lineare Gleichungssysteme • Folgen und Funktionen (Konvergenz von Folgen und Reihen, Stetigkeit von Funktionen)
Lernziele/Kompetenzen:	*Fachkompetenz:* Die Studierenden verstehen die Arithmetik reeller und komplexer Zahlen und können diese anwenden. Sie können entscheiden, ob Folgen bzw. Reihen konvergent sind oder nicht und ggfls. Grenzwerte berechnen. Des Weiter kennen sie die elementaren Funktionen der Analysis und haben Kenntnis über ihre grundlegenden Eigenschaften. Sie kennen weiter die Definition des Begriffs 'Vektorraum' und können diese auf konkrete Vektorräume anwenden. Darüber hinaus beherrschen Sie den Umgang mit Vektoren und Matrizen. Sie können mit dem Begriff 'Stetigkeit' einer reellen Funktion umgehen und können beurteilen, wann diese Eigenschaft eine gegebene Funktion hat. *Methodenkompetenz:* Die Studierenden erwerben die Fähigkeit mit den Lehrinhalten des Moduls aktiv umgehen zu können und können Fragestellungen, Aufgaben und Probleme, die sich aus der Lehrveranstaltung ergeben, selbständig bearbeiten und lösen. *Sozialkompetenz:* Die Studierenden erlernen die Teamarbeit, durch gemeinsames Lösen von Übungsaufgaben an den Präsenzwochenenden. Sie erlangen weiter die Fähigkeit, in komplexen Situationen zu handeln und eine Lösung für schwierige Probleme zu finden. Die Studierenden können aufgrund der Teamarbeit problemorientiert diskutieren. Die Studierenden erlangen die Fähigkeit sich eine Meinung über die Themen von Mathematik I zu bilden und können das erlangte Wissen im Bereich der Informatik einsetzten.
Notwendige Voraussetzungen:	keine
Empfohlene Voraussetzungen:	Mathematik Gymnasium Oberstufe
Einpassung in den Studienplan:	Ab Studiensemester 1

Verwendbarkeit des Moduls:	Dieses Modul ist verwendbar für • Studierende der Informatik • Studierende der Wirtschaftsinformatik • Studierende der Mathematik und Informatik auf Bachelorniveau.
Studien- und Prüfungsleistungen:	Schriftliche Prüfung: 60 min.
Berechnung der Modulnote:	Schriftliche Prüfung
Turnus des Angebots:	Wintersemester
Wiederholung der Prüfungen:	
Anerkannte Module:	
Anerkannte Lernergebnisse:	
Generelle Zielsetzung des Moduls:	Modul zur Förderung und Verstärkung der Fachkompetenz
Arbeitsaufwand bzw. Gesamtworkload:	Summe: 150h Präsenzanteil: 30h • Vorlesungsteil: 12h • Virtuelle Lehre: 10h • Übungsteil: 2h • Prüfungsvorbereitungsveranstaltung: 5h • Prüfung: 1h Fernstudienanteil: 120h • Durcharbeiten der Studienbriefe: 70h • Wahrnehmen der Online Betreuung und Beratung: 10h • Ausarbeiten von Aufgaben: 20h • Individuelle Prüfungsvorbereitung der Studierenden: 20h
Lerninhalt und Niveau:	Das Niveau der Lerninhalte liegt gemessen am DQR-Niveau bei 6 (Bachelor)
Leistungspunkte:	5 ECTS
Moduldauer:	1 Semester
Unterrichtssprache:	Deutsch
Medienformen:	Studienbriefe in schriftlicher und elektronischer Form, Onlinematerial in Lernplattform, Übungen und Projekt über Lernplattform, Online-Konferenzen, Chat und Forum, Präsenzveranstaltung mit Rechner und Beamer.

Literatur:	Als begleitende und vertiefende Literatur wird empfohlen: • Eigenes Skript • Blickensdörfer u. a.: Mathematik für Physiker und Ingenieure – Analysis 1 • Brill, Manfred: Mathematik für Informatiker, Hanser-Verlag, ISBN 3-446-22802-0 • Teschl, G; Teschl, S.: Mathematik für Informatiker, Springer-Verlag, ISBN 3-540-25782-9, Springer; Auflage: 2 (4. Mai 2004) Weitere Literatur wird in der Lehrveranstaltung bekannt gegeben.

Modulbeschreibung

Studiengang:	Bachelor IT-Sicherheit
Modulbezeichnung:	Konzeptionelle Modellierung
Lehrveranstaltungen:	Konzeptionelle Modellierung
Dozent(in):	Prof. Dr. Felix Freiling
Modulverantwortliche(r):	Prof. Dr. Felix Freiling
Modulentwickler(in):	
Inhalt:	Im Modul konzeptionelle Modellierung wird auf folgende Themengebiete eingegangen: • Grundlagen der Modellierung • Entity-Relationship Modell (ER-Modell) • UML und relationale Datenmodellierung • Metamodellierung und XML • Datenmodellierung und Domänenmodellierung
Lernziele/Kompetenzen:	*Fachkompetenz:* Die Studierenden erwerben fundierte Kenntnisse über die Grundlagen der Modellierung sowie über das Entity-Relationship Modell (ER-Modell). Darüber hinaus lernen sie, die vereinheitlichte Modellierungssprache UML und relationale Datenbanken kennen. *Methodenkompetenz:* Die Studierenden beherrschen die Fähigkeit zu beurteilen, wann eine Datenbank sinnvoll ist und können zwischen verschiedenen Typen von Datenbanksystemen unterscheiden. *Sozialkompetenz:* Die Konflikt- und Kommunikationsfähigkeit der Studierenden wird in den gemeinsamen Online-Tutorien und Diskussionsforen geschult. Die Studierenden erlangen die Fähigkeit zur Bildung einer Meinung über die selbstentwickelten Datenmodellierungen und die Datenmodellierungen anderer. Darüber hinaus erlangen sie die Fähigkeit, in herausfordernden Situationen zu handeln und eine Lösung für komplexe Probleme zu finden.
Notwendige Voraussetzungen:	Keine
Empfohlene Voraussetzungen:	Keine
Einpassung in den Studienplan:	Ab Studiensemester 1

Verwendbarkeit des Moduls:	Dieses Modul ist verwendbar für • Studierende der Informatik • Studierende der Wirtschaftsinformatik • Studierende der Mathematik und Informatik auf Bachelorniveau. Dieses Modul kann nicht als Wahlpflichtmodul gewählt werden, sondern ist ein Pflichtmodul.
Studien- und Prüfungsleistungen:	Schriftliche Prüfung: 60 min.
Berechnung der Modulnote:	Schriftliche Prüfung
Turnus des Angebots:	Wintersemester
Wiederholung der Prüfungen:	
Anerkannte Module:	
Anerkannte Lernergebnisse:	
Generelle Zielsetzung des Moduls:	Zur Förderung und Verstärkung der Fachkompetenz
Arbeitsaufwand bzw. Gesamtworkload:	Summe: 150 h Präsenzzeit: 30 h • Vorlesungsteil: 10 h • Übungsteil: 5 h • Praktischer Teil: 10 h • Prüfungsvorbereitungsveranstaltung: 4 h • Prüfung: 1 h Eigenstudium: 120 h • Durcharbeiten der Studienbriefe: 50 h • Durcharbeiten des Online-Lernmaterials: 10 h • Wahrnehmen der Online Betreuung und Beratung: 10 h • Ausarbeiten von Aufgaben: 30 h • Individuelle Prüfungsvorbereitung der Studierenden: 20 h
Lerninhalt und Niveau:	Niveau der Lerninhalte liegt gemessen am DQR-Niveau bei 6 (Bachelor)
Leistungspunkte:	5 ECTS
Moduldauer:	1 Semester
Unterrichtssprache:	Deutsch
Medienformen:	Studienbriefe in schriftlicher und elektronischer Form, Onlinematerial in Lernplattform, Übungen und Projekte über Lernplattform, Online-Konferenzen, Chat und Forum, Präsenzveranstaltungen mit Computer und Beamer.

Literatur:	Als begleitende und vertiefende Literatur wird empfohlen: • Konzeptionelle Modellierung, Richard Lenz, 2012 Weitere Literatur wird in der Lehrveranstaltung bekanntgegeben.

Modulbeschreibung

Studiengang:	Bachelor It-Sicherheit
Modulbezeichnung:	Mathematik 2
Lehrveranstaltungen:	Mathematik 2a und 2b
Dozent(in):	Prof. Dr. Harald Baier
Modulverantwortliche(r):	Prof. Dr. Harald Baier
Modulentwickler(in):	
Inhalt:	In diesem Modul werden die folgenden Themengebiete behandelt: Mathematik 2a: • Numerik (Rechnerarithmetik, Algorithmen, Lineare Gleichungssysteme, Interpolation, Approximation, Numerische Integration, Numerische Differentiation) • Zahlentheorie und modulare Arithmetik (Binäre Zahlendarstellung, Algebraische Grundbegriffe, Teilbarkeit und Primzahlen, Primfaktorzerlegung, größter gemeinsamer Teiler, modulares Potenzieren, RSA-Kryptosystem) • Kombinatorik und endliche Wahrscheinlichkeitstheorie (Elementare Zählprobleme, Binominalkoeffizient und Teilmengen, Permutation, Partitionen, Grundbegriffe der endlichen Wahrscheinlichkeitstheorie, bedingte Wahrscheinlichkeiten, Zufallsgrößen) Mathematik 2b: • Graphentheorie (Grundbegriffe, gerichtete und ungerichtete Graphen, Komplement, Clique und Anticlique, Kontenüberdeckung, gewichtete Graphen, Netzwerk, Subgraphen, Isomorphismus, Eulerische Graphen und Hamiltonkreise, Bäume und Wälder, Planare Graphen, Matchings, Färben und Speicherung von Graphen) • Integralrechnung • Differentialrechnung • Einführung in die Komplexitätstheorie • Wahrscheinlichkeitsrechnung (ausgewählte diskrete Verteilungen, Normalverteilung, Testverteilung)

Lernziele/Kompetenzen:	*Fachkompetenz:* Mathematik 2a: Die Studierenden wissen, wie Computersysteme Zahlen darstellen und können die Laufzeit eines Algorithmus berechnen. Sie kennen die Begriffe Interpolation, Approximation, numerische Integration und Differentiation. Des Weiter kennen Sie die Grundbegriffe der Zahlentheorie, sowie der modularen Arithmetik und können mit diesen umgehen. Sie können Primzahlen zerlegen und modular Potenzieren. Darüber hinaus kennen Sie das RSA-Kryptosystem und erlangen Wissen über die zugrundeliegende Sicherheit. Weiter kennen Sie die elementaren Zählprobleme und können mit Hilfe des Binominalkoeffizienten die Anzahl von Möglichkeiten berechnen. Am Ende kennen Sie die Grundbegriffe der endlichen Wahrscheinlichkeitstheorie und können mit den Begriffen bedingte Wahrscheinlichkeiten und Zufallsgrößen umgehen. Mathematik 2b: Die Studierenden kennen die grundlegenden Begriffe der Graphentheorie und können mit Graphen sicher umgehen. Sie verstehen die Integral- und Differentialrechnung und können diese anwenden. Des Weiter kennen Sie die wichtigsten Themengebiete der Komplexitätstheorie und können mit diesen umgehen. Sie wissen was Turingmaschinen sind und können Probleme anhand von Komplexitätsklassen klassifizieren. Darüber hinaus kennen Sie ausgewählte diskrete Verteilungen, Normalverteilung, Testverteilung und können damit umgehen *Methodenkompetenz:* Die Studierenden können mit dem erlangten Wissen aus dem Modul sicher umgehen und können Aufgaben und Problemstellungen nachvollziehen und lösen. *Sozialkompetenz:* Die Studierenden erlernen die fachgebundene Diskussion, die sich aus der gemeinsamen Teamarbeit zum Lösen von Aufgaben ergeben. Die Studierenden erlangen die Fähigkeit sich eine Meinung über die Themen von Mathematik 2 zu bilden und besitzen darüber hinaus die Kompetenz Sie in den entsprechenden Gebieten der Informatik einsetzen zu können.
Notwendige Voraussetzungen:	Erfolgreicher Abschluss des Moduls • Mathematik 1
Empfohlene Voraussetzungen:	
Einpassung in den Studienplan:	Ab Studiensemester 2

Verwendbarkeit des Moduls:	Dieses Modul ist verwendbar für • Studierende der Informatik • Studierende der Wirtschaftsinformatik • Studierende der Mathematik und Informatik auf Bachelorniveau. Dieses Modul kann nicht als Wahlpflichtmodul gewählt werden, sondern ist ein Pflichtmodul.
Studien- und Prüfungsleistungen:	Schriftliche Prüfung: 120 min. (Mathematik 2a und 2b)
Berechnung der Modulnote:	Schriftliche Prüfung
Turnus des Angebots:	Sommersemester
Wiederholung der Prüfungen:	
Anerkannte Module:	
Anerkannte Lernergebnisse:	
Generelle Zielsetzung des Moduls:	Modul zur Förderung und Verstärkung der Fachkompetenz
Arbeitsaufwand bzw. Gesamtworkload:	Summe: 300h Präsenzanteil: 60h • Vorlesungsteil: 24h • Virtuelle Lehre: 20h • Übungsteil: 5h • Prüfungsvorbereitungsveranstaltung: 9h • Prüfung: 2h Fernstudienanteil: 240h • Durcharbeiten der Studienbriefe: 140h • Wahrnehmen der Online Betreuung und Beratung: 20h • Ausarbeiten von Aufgaben: 40h • Individuelle Prüfungsvorbereitung der Studierenden: 40h
Lerninhalt und Niveau:	Das Niveau der Lerninhalte liegt gemessen am DQR-Niveau bei 6 (Bachelor)
Leistungspunkte:	10 ECTS
Moduldauer:	1 Semester
Unterrichtssprache:	Deutsch
Medienformen:	Studienbriefe in schriftlicher und elektronischer Form, Onlinematerial in Lernplattform, Übungen und Projekt über Lernplattform, Online-Konferenzen, Chat und Forum, Präsenzveranstaltung mit Rechner und Beamer.

Literatur:	Als begleitende und vertiefende Literatur wird empfohlen: 1. Eigenes Skript 2. Diskrete Strukturen Bd.1, Verlag: Springer, Berlin 2007, 2. Aufl., Springer-Lehrbuch 3. Numerik: Eine Einführung für Mathematiker und Informatiker (Ma-thematische Grundlagen der Informatik), Vieweg Verlagsgesellschaft; Auflage: 1994 (1. Januar 1994) 4. Algebraische Grundlagen der Informatik: Strukturen - Zahlen - Verschlüsselung - Codierung (German Edition): Zahlen - Strukturen - Codierung – Verschlüsselung, Vieweg+Teubner Verlag; Auflage: 3., überarb. u. erw. Aufl. 2007 (20. September 2012) 5. Diskrete Strukturen 1. Kombinatorik, Graphentheorie, Algebra, Springer; Auflage: 2., Aufl. (13. September 2007) 6. Einführung in die Wahrscheinlichkeitstheorie und Statistik, Springer; Auflage: 2 (4. Mai 2004) 7. Blickensdörfer u. a.: Mathematik für Physiker und Ingenieure – Analysis 1 8. Blickensdörfer u. a.: Mathematik für Physiker und Ingenieure – Analysis 2 9. Brill, Manfred: Mathematik für Informatiker, Hanser-Verlag, ISBN 3-446-22802-0 10. Teschl, G; Teschl, S.: Mathematik für Informatiker Bd. 2, Springer-Verlag 11. Wegener, I: Komplexitätstheorie: Grenzen der Effizienz von Algorithmen (Springer-Lehrbuch) (German Edition); Auflage: 2003 Weitere Literatur wird in der Lehrveranstaltung bekannt gegeben.

Modulbeschreibung

Studiengang:	Bachelor IT-Sicherheit
Modulbezeichnung:	Rechnerstrukturen
Lehrveranstaltungen:	Rechnerstrukturen
Dozent(in):	Prof. Dr. Daniel Hammer
Modulverantwortliche(r):	Prof. Dr. Daniel Hammer
Modulentwickler(in):	
Inhalt:	Im Modul Rechnerstrukturen wird auf folgende Themengebiete eingegangen: • Darstellung von Daten in einer computergerechten Weise • Schaltalgebra • Wichtige Rechnerstrukturen, einschließlich Prozessoren, Peripheriegeräten, Speicherorganisation und Verbindungsstrukturen • Maschinenorientierte Programmiersprachen
Lernziele/Kompetenzen:	*Fachkompetenz:* Die Studierenden erwerben Grundkenntnisse über die computergerechte Darstellung von Daten. Ferner eignen sie sich Grundlagen der Schaltalgebra an und können Schaltnetze bzw -werke beschreiben und klassifizieren. *Methodenkompetenz:* Die Studierenden erlangen das Grundwissen über Rechnerarchitektur und können den Aufbau und die Komponenten verschiedener Rechnerarchitekturen darstellen und z.B. das Prinzip des Universalrechners erläutern und Prozessoren, Peripheriegeräte und Speicherorganisation erklären. *Sozialkompetenz:* Aufgrund der Teamarbeit, unter anderem in dem Präsenzwochenende, erweitern die Studierenden die Fähigkeit der Teamfähigkeit und Sozialkompetenz. Die Studierenden können den Aufbau und die Funktionsweise von Rechnern verstehen und nachvollziehen. Desweiteren verfügen sie nach Absolvieren des Moduls über Kenntnisse der verschiedenen Abstraktionsebenen von Computern und deren Zusammenwirken. Ihnen wird bewußt, dass IT sehr schnell-lebig ist und dass Detailwissen eine kurze Halbwertzeit hat. Sie sind in der Lage sich je nach Bedarf selbst weiterzubilden. Nach Bearbeitung diese Moduls verstehen die Studierenden den Computer als System und haben die grundlegenden Prinzipien verinnerlicht.
Notwendige Voraussetzungen:	
Empfohlene Voraussetzungen:	Einführung in die IT-Sicherheit
Einpassung in den Studienplan:	Ab Studiensemester 2

Verwendbarkeit des Moduls:	Dieses Modul ist verwendbar für • Studierende der Informatik • Studierende der Wirtschaftsinformatik • Studierende der Mathematik und Informatik auf Bachelorniveau. Dieses Modul kann nicht als Wahlpflichtmodul gewählt werden, sondern ist ein Pflichtmodul.
Studien- und Prüfungsleistungen:	Schriftliche Prüfung: 60 min.
Berechnung der Modulnote:	Schriftliche Prüfung
Turnus des Angebots:	in jedem Semester
Wiederholung der Prüfungen:	
Anerkannte Module:	
Anerkannte Lernergebnisse:	
Generelle Zielsetzung des Moduls:	Modul zur Förderung und Verstärkung der Fachkompetenz
Arbeitsaufwand bzw. Gesamtworkload:	Präsenzstudium: 15 Zeitstunden Fernstudienanteil: 135 Zeitstunden • Selbststudium: 105 Zeitstunden • Aufgaben: 20 Zeitstunden • Online-Betreuung: 10 Zeitstunden Summe: 150 Zeitstunden
Lerninhalt und Niveau:	Das Niveau der Lerninhalte liegt gemessen am DQR-Niveau bei 6 (Bachelor)
Leistungspunkte:	5 ECTS
Moduldauer:	1 Semester
Unterrichtssprache:	Deutsch
Medienformen:	Studienbriefe in schriftlicher und elektronischer Form, Onlinematerial in Lernplattform, Übungen und Projekt über Lernplattform, Online-Konferenzen, Chat und Forum, Präsenzveranstaltung mit Rechner und Beamer.
Literatur:	• Rechnerarchitektur & Betriebssysteme, (Vorlesungsskript), Daniel Hammer, 2012 • Rechneraufbau und Rechnerstrukturen, W. Oberschelp, G.Vossen, 2003 • Computerarchitektur,Andrew S. Tanenbaum, 2005 • Einführung in die Rechnerarchitektur, Christian. Märtin, Leipzig, 2003 Weitere Literatur wird in der Lehrveranstaltung bekannt gegeben.

Modulbeschreibung

Studiengang:	Bachelor IT-Sicherheit
Modulbezeichnung:	Systemsicherheit 1
Lehrveranstaltungen:	Systemsicherheit 1a und 1b
Dozent(in):	Prof. Dr. Daniel Hammer
Modulverantwortliche(r):	Prof. Dr. Daniel Hammer
Modulentwickler(in):	
Inhalt:	In diesem Modul werden die folgenden Themengebiete behandelt: Systemsicherheit 1a: • Eine Einführung in die Grundlagen von Betriebssystemen, ihre Aufgaben und Ausprägungen • Prozesse, Threads, Prozessmodell und Prozesssteuerung • Synchronisation, Context Switch • Deadlocks Systemsicherheit 1b: • Grundwissen über Dateisysteme • Grundlagen der Speicherverwaltung und virtuelle Speicher • Basiswissen über Scheduling • Ein- und Ausgabe

Lernziele/Kompetenzen:	*Fachkompetenz:* Systemsicherheit 1a: Die Studierenden erwerben Grundkenntnisse über Betriebssysteme, ferner eignen sie sich Grundlagen der Prozessorganisation an, können Prozesse und Threads erklären, das Prozessmodell und die Prozesssteuerung beschreiben und Synchronisation und Context Switch erläutern. Außerdem erwerben sie Grundkenntnisse über Deadlocks. Systemsicherheit 1b: Die Studierenden erlangen anhand von UNIX-Beispielen das Basiswissen über Dateisysteme und sie erwerben Kenntnisse über den Aufbau eines Dateisystems. Ferner eignen sie sich Grundlagen der Speicherverwaltung an. Außerdem erhalten sie das Basiswissen über Scheduling und die Ein- und Ausgabe. *Methodenkompetenz:* Die Studierenden kennen unterschiedliche Arten von Betriebssystemen und können sie differenzieren und wissen außerdem wie ein ausführbares Programm entsteht. Sie sind in der Lage zwischen Prozessen und Threads zu unterscheiden und das Prozessmodell, die Prozesssteuerung und Context Switch zu erläutern. Die Lernenden können anhand der erlernten Lösungsansätze einen wechselseitigen Ausschluss lösen. Sie sind nach Durcharbeiten dieses Moduls in der Lage eigenständig Deadlocks zu modellieren und sie können Deadlock-Behandlungsstrategien anwenden. *Sozialkompetenz:* Aufgrund der Teamarbeit, unter anderem in den Präsenzwochenenden, erweitern die Studierenden die Fähigkeit der Teamfähigkeit und Sozialkompetenz. Die Lernenden erlangen die Fähigkeit zur Bildung einer Meinung über IT-Sicherheit. Darüber hinaus erlangen sie die Fähigkeit, in komplexen Situationen zu handeln und eine Lösung für schwierige Probleme zu finden.
Notwendige Voraussetzungen:	
Empfohlene Voraussetzungen:	
Einpassung in den Studienplan:	Ab Studiensemester 3
Verwendbarkeit des Moduls:	Dieses Modul ist verwendbar für • Studierende der Informatik • Studierende der Wirtschaftsinformatik • Studierende der Mathematik und Informatik auf Bachelorniveau. Dieses Modul kann nicht als Wahlpflichtmodul gewählt werden, sondern ist ein Pflichtmodul.
Studien- und Prüfungsleistungen:	Schriftliche Prüfung: 120 min.
Berechnung der Modulnote:	Schriftliche Prüfung
Turnus des Angebots:	in jedem Semester

Wiederholung der Prüfungen:	
Anerkannte Module:	
Anerkannte Lernergebnisse:	
Generelle Zielsetzung des Moduls:	Modul zur Förderung und Verstärkung der Fachkompetenz
Arbeitsaufwand bzw. Gesamtworkload:	Präsenzstudium: 30 Zeitstunden Fernstudienanteil: 270 Zeitstunden • Selbststudium: 210 Zeitstunden • Aufgaben: 40 Zeitstunden • Online-Betreuung: 20 Zeitstunden Summe: 300 Zeitstunden
Lerninhalt und Niveau:	Das Niveau der Lerninhalte liegt gemessen am DQR-Niveau bei 6 (Bachelor)
Leistungspunkte:	10 ECTS
Moduldauer:	1 Semester
Unterrichtssprache:	Deutsch
Medienformen:	Studienbriefe in schriftlicher und elektronischer Form, Onlinematerial in Lernplattform, Übungen und Projekt über Lernplattform, Online-Konferenzen, Chat und Forum, Präsenzveranstaltung mit Rechner und Beamer.
Literatur:	• Rechnerarchitektur & Betriebssysteme, (Vorlesungsskript), Daniel Hammer, 2012 • Betriebssysteme, Eduard Glatz, 2005 • Moderne Betriebssysteme, Andrew S. Tanenbaum, 2003 • Betriebssysteme - Prinzipien und Umsetzung, William Stallings, 2005 • Netzsicherheit, Günter Schäfer, 2003 • Computer Security, Dieter Gollmann, 2010 • Security Engineering - A guide to Building - Dependable Distributed Systems, Ross Anderson, 2010 • Deadline Scheduling for Real-Time Systems, John A. Stankovic, 1998 • Fundamentals of Operating Systems, R.D.Eager, A.M.Lister, 1993 Weitere Literatur wird in der Lehrveranstaltung bekannt gegeben.

Modulbeschreibung

Studiengang:	Bachelor IT-Sicherheit
Modulbezeichnung:	Algorithmen und Datenstrukturen (in C)
Lehrveranstaltungen:	Algorithmen und Datenstrukturen (in C)
Dozent(in):	Prof. Dr. Felix Freiling
Modulverantwortliche(r):	Prof. Dr. Felix Freiling
Modulentwickler(in):	
Inhalt:	In diesem Modul werden die folgenden Themengebiete behandelt: • Programmierkurs zur Erlernung der Programmierung in C • Analysemodell, Lauzeitmodelle und allgemeine Analysetechniken für Algorithmen • Strukturierte Datentypen wie Arrays, Listen, Bäume und Graphen • Verschiedene Sortieralgorithmen mit ihren Laufzeitanalysen • Algorithmen auf Mengen: Suchen, TRIES, Hashing, Union-Find und Priority Queues • Balancierte Suchbäume, insbesondere AVL-Bäume und B-Bäume • Repräsentation von Graphen und fundamentale Algorithmen auf Graphen • Vertiefung der Graphenalgorithmen: Zusammenhangskomponenten und Bestimmung kürzester Pfade • Implementierung der vorgestellten Algorithmen in C
Lernziele/Kompetenzen:	*Fachkompetenz:* Die Studierenden erwerben fundierte Kenntnisse in der Programmiersprache C. Sie lernen grundlegende Datenstrukturen und Algorithmen der Informatik kennen und erlernen, diese bezüglich Effizienz einzuschätzen und in einer konkreten Programmiersprache umzusetzen. *Methodenkompetenz:* Die Studierenden erwerben die Fähigkeit, konkrete Programmieraufgaben in einer höheren Programmiersprache zu formulieren. Lernende können hierbei die Gesamtaufgabe strukturieren und in Teilaufgaben zerlegen. Die Studierenden erlernen die Fähigkeit, geeignete Datenstrukturen und Algorithmen zur Abbildung von Programmieraufgaben zu finden, die eine effiziente Umsetzung gestatten. *Sozialkompetenz:* Aufgrund der Teamarbeit, unter anderem in den Präsenzwochenenden, erweitern die Studierenden ihre Teamfähigkeit und Sozialkompetenz. Die Studierenden erlangen die Fähigkeit zur Bildung einer Meinung über die eigenen Programme und die Programme anderer. Darüber hinaus erlangen sie die Fähigkeit, in komplexen Situationen zu handeln und eine Lösung für komplexe Probleme zu finden.

Notwendige Voraussetzungen:	Erfolgreicher Abschluss der vorherigen Module, insbesondere • Programmierkonzepte • Mathematik 1
Empfohlene Voraussetzungen:	Erfolgreicher Abschluss der Module • Mathematik 2 (Wahrscheinlichkeitsrechnung aus Lehrveranstaltung Mathematik 2a)
Einpassung in den Studienplan:	Ab Studiensemester 3
Verwendbarkeit des Moduls:	Dieses Modul ist verwendbar für • Studierende der Informatik • Studierende der Wirtschaftsinformatik • Studierende der Mathematik und Informatik auf Bachelorniveau. Dieses Modul kann nicht als Wahlpflichtmodul gewählt werden, sondern ist ein Pflichtmodul.
Studien- und Prüfungsleistungen:	Schriftliche Prüfung: 60 min.
Berechnung der Modulnote:	Schriftliche Prüfung
Turnus des Angebots:	Wintersemester
Wiederholung der Prüfungen:	
Anerkannte Module:	
Anerkannte Lernergebnisse:	
Generelle Zielsetzung des Moduls:	Modul zur Förderung und Verstärkung der Fachkompetenz
Arbeitsaufwand bzw. Gesamtworkload:	Präsenzstudium: 15 Zeitstunden Fernstudienanteil: 135 Zeitstunden • Selbststudium: 90 Zeitstunden • Aufgaben: 40 Zeitstunden • Online-Betreuung: 5 Zeitstunden **Summe: 150 Zeitstunden**
Lerninhalt und Niveau:	**Das Niveau der Lerninhalte liegt gemessen am DQR-Niveau bei 6 (Bachelor)**
Leistungspunkte:	5 ECTS
Moduldauer:	1 Semester
Unterrichtssprache:	Deutsch
Medienformen:	Studienbriefe in schriftlicher und elektronischer Form, Onlinematerial in Lernplattform, Übungen und Projekt über Lernplattform, Online-Konferenzen, Chat und Forum, Präsenzveranstaltung mit Rechner und Beamer

Literatur:	Als begleitende und vertiefende Literatur wird empfohlen: • Programmieren in C, Kernighan und Ritchie, 1990 • Algorithmen – kurz gefasst, Uwe Schöning, 1997 • Algorithms and Data Structures: The Basic Toolbox, Mehlhorn and Sanders, 2010 • Algorithmen - Eine Einführung, Corman, Leiserson, Rivest und Stein, 2010 • Datenstrukturen und Effiziente Algorithmen, Band 1: Sortieren und Suchen, Kurt Mehlhorn, 1986 Weitere Literatur wird in der Lehrveranstaltung bekannt gegeben.

Modulbeschreibung

Studiengang:	Bachelor IT-Sicherheit
Modulbezeichnung:	Kryptographie 1
Lehrveranstaltungen:	Kryptographie 1
Dozent(in):	Prof. Dr. Christof Paar
Modulverantwortliche(r):	Prof. Dr. Christof Paar
Modulentwickler(in):	
Inhalt:	In diesem Modul werden zunächst einige grundlegende Begriffe der Datensicherheit erläutert. Danach werden einige historisch wichtige Verschlüsselungsverfahren vorgestellt. Die Schwerpunkte dieses Moduls liegen auf der Besprechung von praktisch wichtigen Verschlüsselungsverfahren, Hashfunktionen und Message Authentication Codes (MAC). Als bedeutende Vertreter der symmetrischen Verfahren werden der Data Encryption Standard (DES) und der Advanced Encryption Standard (AES) behandelt.
Lernziele/Kompetenzen:	*Fachkompetenz:* Die Studierenden kennen die Bedeutung von symmetrischen kryptographischen Verfahren und verstehen die Strukturen der prominentesten symmetrischen Primitiven. Darüber hinaus verinnerlichen die Studenten die Sicherheitskonzepte und diverse Angriffsziele von symmetrischen Verfahren. Die Grundprinzipien asymmetrischer Kryptographie werden verstanden. *Methodenkompetenz:* Die Studierenden beherrschen die Denkweisen, die in der modernen Kryptographie eingesetzt werden und können diese anhand von symmetrischen Verfahren nachvollziehen. *Sozialkompetenz:* Die Studenten tauschen sich über Probleme beim Verstehen von symmetrischen kryptographischen Verfahren aus und diskutieren Lösungswege von Problemen. Die Studenten erlangen die Fähigkeit aktuelle symmetrische kryptographische Verfahren zu verstehen und eine fundierte Meinung über die Sicherheit dieser Verfahren zu vertreten. Darüber hinaus besitzen die Studierenden alle Voraussetzungen neue symmetrische Verfahren aus der aktuellen Fachliteratur zu verstehen und ihre Bedeutungen einzuschätzen.
Notwendige Voraussetzungen:	
Empfohlene Voraussetzungen:	
Einpassung in den Studienplan:	Ab Studiensemester 3

Verwendbarkeit des Moduls:	Dieses Modul ist verwendbar für • Studierende der IT-Sicherheit • Studierende der Informatik • Studierende der Wirtschaftsinformatik • Studierende der Mathematik und Informatik auf Bachelorniveau. Dieses Modul kann nicht als Wahlpflichtmodul gewählt werden, sondern ist ein Pflichtmodul.
Studien- und Prüfungsleistungen:	Schriftliche Prüfung: 120 min.
Berechnung der Modulnote:	Schriftliche Prüfung
Turnus des Angebots:	Jedes Semester
Wiederholung der Prüfungen:	
Anerkannte Module:	
Anerkannte Lernergebnisse:	
Generelle Zielsetzung des Moduls:	Modul zur Förderung und Verstärkung der Fachkompetenz
Arbeitsaufwand bzw. Gesamtworkload:	Summe: 150 h Präsenzzeit: 2 h • Prüfung: 2h Eigenstudium: 148 h • Durcharbeiten der Studienbriefe: 85 h • Durcharbeiten des Online-Lernmaterials: 15 h • Wahrnehmen der Online Betreuung und Beratung: 10 h • Ausarbeiten von Aufgaben: 30 h • Individuelle Prüfungsvorbereitung der Studierenden: 8 h
Lerninhalt und Niveau:	Das Niveau der Lerninhalte liegt gemessen am DQR-Niveau bei 6 (Bachelor)
Leistungspunkte:	5 ECTS
Moduldauer:	1 Semester
Unterrichtssprache:	Deutsch, Englisch
Medienformen:	Studienbriefe in schriflicher und elektronischer Form, Online-material in Lernplattform, Übungen über Lernplattform, Online-Konferenzen, Chat und Forum
Literatur:	• Understanding Cryptography, Christof Paar, Jan Pelzl, 2010 • Handbook of Applied Cryptography, Alfred J. Menezes, Paul C van Oorschot, Scott A Vanstone, 1996 Weitere Literatur wird in der Lehrveranstaltung bekannt gegeben.

Modulbeschreibung

Studiengang:	Bachelor IT-Sicherheit
Modulbezeichnung:	Theoretische Informatik
Lehrveranstaltungen:	Theoretische Informatik
Dozent(in):	Prof. Dr. Harald Baier
Modulverantwortliche(r):	Prof. Dr. Harald Baier
Modulentwickler(in):	
Inhalt:	In diesem Modul werden die folgenden Themengebiete behandelt: • Grundbegriffe: Wörter, Alphabete, Relationen, Operationen über Relationen • Formale Sprachen/Automatentheorie: Chomsky Grammatiken, Chomsky Hierarchie, Wortproblem, Reguläre Sprachen, deterministische und nichtdeterministische Automaten, Minimierungsalgorithmus für deterministische Automaten, Kontextfreie Sprachen, CYK-Algorithmus • Berechnungstheorie: Berechenbarkeitsmodelle (RAM und Turingmaschinen), Churchsche These, Unentscheidbarkeit und Turingreduzierbarkeit • Komplexitätstheorie: nichtdeterministische Turing-Maschinen, Komplexitätsmaße, Komplexitätsklassen, linear beschränkte Automaten und kontext-sensitive Sprachen, das P=NP? Problem, polynomielle Reduzierbarkeit, NP-Vollständigkeit

Lernziele/Kompetenzen:	*Fachkompetenz:* Die Studierenden erlangen ein Verständnis für grundlegende Konzepte, Begriffe und Zusammenhänge aus den Teilgebieten Automatentheorie, formale Sprachen, Berechnungstheorie und P/NP-Theorie und haben ein Verständnis für grundlegende Beweismethoden entwickelt. Sie haben die Fähigkeit herausgebildet, einfache Beweise selbständig zu führen. Des Weiter haben Sie Kenntnis von der Leistungsfähigkeit unterschiedlicher Beschreibungsmittel und haben die Fähigkeit entwickelt, die Beschreibungsmittel selbständig zu gebrauchen. Darüber hinaus haben Sie das Wissen um den Zusammenhang zwischen der Leistungsfähigkeit und der algorithmischen Beherrschbarkeit unterschiedlicher Beschreibungsmittel erlangt. Die Studierenden haben weiter ein Verständnis für nichtdeterministische Maschinenmodelle und deren Bedeutung entwickelt. Sie können mit den deterministischen und nichtdeterministischen Maschinenmodellen umgehen und haben ein Verständnis für die algorithmische Lösbarkeit/-Nichtlösbarkeit von Problemen sowie die inhärente Komplexität von Problemen entwickelt. *Methodenkompetenz:* Die Studierenden können Fragen zu den oben genannten Fachkompetenzen schriftlich beantworten. Sie können zu gegebenen formalen Sprachen Grammatiken und Automaten entwickeln, welche die gegebene formale Sprache erzeugt und akzeptiert. Darüber hinaus können Sie die Korrektheit ihrer Entwicklung zeigen. Sie können einen gegebenen deterministischen Automaten minimieren und gegebene kontextfreie Grammatiken in die Chomsky-Normalform umwandeln. Weiter können Sie zeigen, ob eine einfache Sprache regulär ist oder nicht und für die Sprache erläutern, zu welcher Klasse von Sprachen sie gehört. Sie beherrschen die grundlegenden Beweismethoden und haben die Fähigkeit, einfache Beweise selbständig zu führen. Sie können einfache Programme bei den unterschiedlichen Berechenbarkeitsmodelle formulieren, ihre Korrektheit beweisen und zeigen ob eine vorgegebene Menge entscheidbar/unentscheidbar ist. Sie können weiter zeigen, ob eine gegebene Menge NP-vollständig ist. *Sozialkompetenz:* Die Studierenden sind in der Lage als Team zusammenzuarbeiten und so Lösungen für die gestellten Aufgaben zu finden. Darüber hinaus können Sie zu den Themen eine fachgebundene Diskussion führen. Die Studierenden sind in der Lage die Lösungen zu den Aufgaben und Problemen mündlich und schriftlich zu formulieren und zu präsentieren. Dadurch könne Sie sich auch gegen Einwände in einer Diskussion verteidigen. Sie sind in der Lage selbständig geeignete Literatur zu finden und einzusetzen.
Notwendige Voraussetzungen:	Erfolgreicher Abschluss des Moduls • Mathematik 2
Empfohlene Voraussetzungen:	
Einpassung in den Studienplan:	Ab Studiensemester 4

Verwendbarkeit des Moduls:	Dieses Modul ist verwendbar für • Studierende der Informatik • Studierende der Wirtschaftsinformatik • Studierende der Mathematik und Informatik auf Bachelorniveau. Dieses Modul kann nicht als Wahlpflichtmodul gewählt werden, sondern ist ein Pflichtmodul.
Studien- und Prüfungsleistungen:	Schriftliche Prüfung: 60 min.
Berechnung der Modulnote:	Schriftliche Prüfung
Turnus des Angebots:	Sommersemester
Wiederholung der Prüfungen:	
Anerkannte Module:	
Anerkannte Lernergebnisse:	
Generelle Zielsetzung des Moduls:	Modul zur Förderung und Verstärkung der Fachkompetenz
Arbeitsaufwand bzw. Gesamtworkload:	Summe: 150h Präsenzanteil: 30h • Vorlesungsteil: 12h • Virtuelle Lehre: 10h • Übungsteil: 2h • Prüfungsvorbereitungsveranstaltung: 5h • Prüfung: 1h Fernstudienanteil: 120h • Durcharbeiten der Studienbriefe: 70h • Wahrnehmen der Online Betreuung und Beratung: 10h • Ausarbeiten von Aufgaben: 20h • Individuelle Prüfungsvorbereitung der Studierenden: 20h
Lerninhalt und Niveau:	Das Niveau der Lerninhalte liegt gemessen am DQR-Niveau bei 6 (Bachelor)
Leistungspunkte:	5 ECTS
Moduldauer:	1 Semester
Unterrichtssprache:	Deutsch
Medienformen:	Studienbriefe in schriftlicher und elektronischer Form, Onlinematerial in Lernplattform, Übungen und Projekt über Lernplattform, Online-Konferenzen, Chat und Forum, Präsenzveranstaltung mit Rechner und Beamer.

Literatur:	Als begleitende und vertiefende Literatur wird empfohlen: 1. Eigenes Skript 2. Hromkovic, J.: Theoretische Informatik, Teubner Verlag, Stuttgart, 2002. 3. Schöning, U.: Theoretische Informatik – kurz gefaßt, Spektrum Akademischer Verlag, Heidelberg, 1997. 4. I. Wegener, I.: Theoretische Informatik – eine algorithmenorientierte Einführung, Teubner Verlag, Stuttgart, 1999. 5. Wegener, I: Komplexitätstheorie: Grenzen der Effizienz von Algorithmen (Springer-Lehrbuch) (German Edition); Auflage: 2003 Weitere Literatur wird in der Lehrveranstaltung bekannt gegeben.

Modulbeschreibung

Studiengang:	Bachelor IT-Sicherheit
Modulbezeichnung:	Systemnahe Programmierung
Lehrveranstaltungen:	Systemnahe Programmierung
Dozent(in):	Prof. Dr. Felix Freiling
Modulverantwortliche(r):	Prof. Dr. Felix Freiling
Modulentwickler(in):	
Inhalt:	In diesem Modul werden die folgenden Themengebiete behandelt: • Allgemeine Rechner- und Betriebssystemstrukturen • Innere Strukturen des Betriebssystems Microsoft Windows • Assemblerprogrammierung der Intel IA-32-Architektur • Codeerzeugung, Codeoptimierung und Programmanalyse für die IA-32-Architektur • Systemnahe Sicherheitsaspekte, insbesondere Mechanismen von Buffer Overflow und sonstigen Sicherheitslücken sowie Gegenmaßnahmen zur Verhinderung ihrer Ausbeutung • Obfuscation und sonstige Malware-Techniken. Malware-Analyse durch das Analyseprogramm IDA anhand realer Beispiele
Lernziele/Kompetenzen:	*Fachkompetenz:* Die Studierenden erwerben fundierte Kenntnisse in der Programmierung der Intel IA-32 Architektur auf Maschinenebene. Sie erlernen die Maschinencodeerzeugung aus der Hochsprache C und gewinnen einen Überblick über Verfahren zur Codeoptimierung und Codeverschleierung (Obfuscation). Die Studierenden gewinnen einen Einblick in die Funktionsweise von Malware auf Systemebene und können einfache Malware selbstständig analysieren. *Methodenkompetenz:* Die Studierenden erwerben die Fähigkeit, systemnahe Programme zu erstellen und zu verstehen. Die Übertragung des erworbenen Wissens auf andere Architekturen ist durch das Erkennen grundlegender Zusammenhänge gegeben. Die Studierenden können Probleme auf dieser Ebene der Programmierung erkennen und Schwachstellen identifizieren und analysieren. *Sozialkompetenz:* Aufgrund der Teamarbeit, unter anderem in den Präsenzwochenenden, erweitern die Studierenden ihre Teamfähigkeit und Sozialkompetenz. Durch das eigenverantwortliche Entwickeln von Programmen erweitern die Studierenden ihr selbstständiges Handeln. Durch die Präsentation ihrer Ergebnisse wird die Selbstsicherheit der Studierenden gestärkt.

Notwendige Voraussetzungen:	Erfolgreicher Abschluss der vorherigen Module, insbesondere: • Algorithmen und Datenstrukturen (in C) • Rechnerstrukturen
Empfohlene Voraussetzungen:	Erfolgreicher Abschluss der Module • Systemsicherheit 1a und 1b
Einpassung in den Studienplan:	Ab Studiensemester 4
Verwendbarkeit des Moduls:	Dieses Modul ist verwendbar für • Studierende der Informatik • Studierende der Wirtschaftsinformatik • Studierende der Mathematik und Informatik auf Bachelorniveau. Dieses Modul kann nicht als Wahlpflichtmodul gewählt werden, sondern ist ein Pflichtmodul.
Studien- und Prüfungsleistungen:	Schriftliche Prüfung: 60 min.
Berechnung der Modulnote:	Schriftliche Prüfung
Turnus des Angebots:	Sommersemester
Wiederholung der Prüfungen:	
Anerkannte Module:	
Anerkannte Lernergebnisse:	
Generelle Zielsetzung des Moduls:	Modul zur Förderung und Verstärkung der Fachkompetenz
Arbeitsaufwand bzw. Gesamtworkload:	Präsenzstudium: 15 Zeitstunden Fernstudienanteil: 135 Zeitstunden • Selbststudium: 90 Zeitstunden • Aufgaben: 40 Zeitstunden • Online-Betreuung: 5 Zeitstunden **Summe: 150 Zeitstunden**
Lerninhalt und Niveau:	**Das Niveau der Lerninhalte liegt gemessen am DQR-Niveau bei 6 (Bachelor)**
Leistungspunkte:	5 ECTS
Moduldauer:	1 Semester
Unterrichtssprache:	Deutsch
Medienformen:	Studienbriefe in schriftlicher und elektronischer Form, Onlinematerial in Lernplattform, Übungen und Projekt über Lernplattform, Online-Konferenzen, Chat und Forum, Präsenzveranstaltung mit Rechner und Beamer

Literatur:	Als begleitende und vertiefende Literatur wird empfohlen: • Intel 80386, Programmers Reference Manual, 1987 • Practical Malware Analysis: The Hands-On Guide to Dissecting Malicious Software, Sikorski and Honig, 2012 • Reversing: Secrets of Reverse Engineering, Eilam, 2005 Weitere Literatur wird in der Lehrveranstaltung bekannt gegeben.

Modulbeschreibung

Studiengang:	Bachelor IT-Sicherheit
Modulbezeichnung:	Systemsicherheit 2
Lehrveranstaltungen:	Systemsicherheit 2
Dozent(in):	Prof. Dr. Daniel Hammer
Modulverantwortliche(r):	Prof. Dr. Daniel Hammer
Modulentwickler(in):	
Inhalt:	Im Modul Systemsicherheit 2 wird auf folgende Themengebiete eingegangen: • Malware • Sicherheitsmechanismen- und modelle • Vorstellung und Erläuterung der Sicherheitsaspekte von Betriebssystemen. • Angriffsszenarien • Abwehrmechanismen
Lernziele/Kompetenzen:	*Fachkompetenz:* Die Studierenden erlangen anhand von Beispielen das Basiswissen über Malware, wie diese Schadsoftware funktioniert und welche Gefahr von ihr ausgeht. Ferner erwerben sie Kenntnisse über die Sicherheitsmechanismen und -modelle von Betriebssystemen und können zwischen unterschiedlichen Angriffsszenarien differenzieren. Außerdem eignen sie sich das Wissen über die entsprechenden Abwehrmechanismen an. *Methodenkompetenz:* Die Studierenden können zwischen den unterschiedlichen Malware-Arten differenzieren und können die entsprechenden Schutzmaßnahmen einsetzen. Sie kennen die Sicherheitsmechanismen- und modelle von Betriebssystemen und ihre unterschiedlichen Sicherheitsaspekte. Außerdem wissen die Studierenden wie Programmierfehler ausgenutzt werden können, was Insider-Angriffe sind und wie und welche Abwehrmechanismen sie einsetzen können. *Sozialkompetenz:* Aufgrund der Teamarbeit, unter anderem in dem Präsenzwochenende, erweitern die Studierenden die Fähigkeit der Teamfähigkeit und Sozialkompetenz. Die Lernenden erlangen die Fähigkeit zur Bildung einer Meinung über IT-Sicherheit. Darüber hinaus erlangen sie die Fähigkeit, in komplexen Situationen zu handeln und eine Lösung für schwierige Probleme zu finden.
Notwendige Voraussetzungen:	
Empfohlene Voraussetzungen:	Systemsicherheit 1a/1b
Einpassung in den Studienplan:	Ab Studiensemester 4

Verwendbarkeit des Moduls:	Dieses Modul ist verwendbar für • Studierende der Informatik • Studierende der Wirtschaftsinformatik • Studierende der Mathematik und Informatik auf Bachelorniveau. Dieses Modul kann nicht als Wahlpflichtmodul gewählt werden, sondern ist ein Pflichtmodul.
Studien- und Prüfungsleistungen:	Schriftliche Prüfung: 60 min.
Berechnung der Modulnote:	Schriftliche Prüfung
Turnus des Angebots:	in jedem Semester
Wiederholung der Prüfungen:	
Anerkannte Module:	
Anerkannte Lernergebnisse:	
Generelle Zielsetzung des Moduls:	Modul zur Förderung und Verstärkung der Fachkompetenz
Arbeitsaufwand bzw. Gesamtworkload:	Präsenzstudium: 15 Zeitstunden Fernstudienanteil: 135 Zeitstunden • Selbststudium: 105 Zeitstunden • Aufgaben: 20 Zeitstunden • Online-Betreuung: 10 Zeitstunden Summe: 150 Zeitstunden
Lerninhalt und Niveau:	Das Niveau der Lerninhalte liegt gemessen am DQR-Niveau bei 6 (Bachelor)
Leistungspunkte:	5 ECTS
Moduldauer:	1 Semester
Unterrichtssprache:	Deutsch
Medienformen:	Studienbriefe in schriftlicher und elektronischer Form, Onlinematerial in Lernplattform, Übungen und Projekt über Lernplattform, Online-Konferenzen, Chat und Forum, Präsenzveranstaltung mit Rechner und Beamer.
Literatur:	• IT-Sicherheit: Konzepte - Verfahren - Protokolle, Claudia Eckert, 2006 • Moderne Betriebssysteme, Andrew S. Tanenbaum, 2003 • Betriebssysteme - Prinzipien und Umsetzung, William Stallings, 2005 • Malware, Eugene Kaspersky, 2008 • Computer Security, Dieter Gollmann, 2010 Weitere Literatur wird in der Lehrveranstaltung bekannt gegeben.

Modulbeschreibung

Studiengang:	Bachelor IT-Sicherheit
Modulbezeichnung:	Einführung in die digitale Forensik
Lehrveranstaltungen:	Einführung in die digitale Forensik
Dozent(in):	Prof. Dr. Harald Baier
Modulverantwortliche(r):	Prof. Dr. Harald Baier
Modulentwickler(in):	
Inhalt:	In diesem Modul werden die folgenden Themengebiete behandelt: • Klassische forensische Wissenschaften und digitale Forensik. • Grundlagen der digitalen Forensik. • Digitale Spuren (Entstehung, Manipulier- und Kopierbarkeit, Personenbezogenheit). • Einführung in die Dateisystemanalyse (Generelles Konzept. Dateisystem ext4). • Analyse mit forensischen Tools (Sleuthkit, DFF, X-Ways, Scalpel und strings). • Anwendungsforensik (SQLite Datenbanken, EXIF und Strings Analyse). • Mobilfunkforensik anhand von Fallbeispielen (Übersicht über Android OS, Flash Speicher, Struktur und Inhalt von wichtigen Verzeichnissen und Dateien). • Übersicht über Cloud Forensik, Post Mortem und Live Analyse, Analyse der Windows Registry. • Praktische Bearbeitung von Aufgaben

Lernziele/Kompetenzen:	*Fachkompetenz:* Die Studierenden kennen die Grundlagen der digitalen Forensik und können diese anwenden. Sie haben Kenntnis über die Entstehung, der Manipulier- und Kopierbarkeit sowie der Personenbezogenheit von digitalen Spuren. Sie kennen weiter das grundlegende Konzept sowie die Eigenschaften des ext4 Dateisystems und können mit diesem Wissen eine Dateisystemanalyse durchführen. Darüber hinaus kennen Sie die grundlegenden Schritte eines Computerforensikers und können mit allgemeinen und speziellen forensischen Tools sicher umgehen. (Allgemeine Tools: Sleuthkit, DFF, X-Ways, spezielle Tools: File Carving, Strings). Des Weiter können Sie forensische Analysen von Anwendungen (SQLite Datenbank-, EXIF-, String-Analyse) durchführen und haben ein grundlegendes Verständnis für die Analyse und Auswertung von Smartphones mit dem Android OS. Sie sind mit diesem Wissen über die Architektur, der Speicherstrategie und Sicherheitskonzept vom Android OS, dem Flash Speicher, der Struktur und dem Inhalt wichtiger Verzeichnisse in der Lage eine forensische Analyse eines Smartphones durchzuführen. *Methodenkompetenz:* Die Studierenden beherrschen den Umgang mit den forensischen Tools und können wichtige Ergebnisse daraus eigenständig entnehmen. Sie sind mit den Grundprinzipien der Computerforensik vertraut und können diese bei einer forensischen Untersuchung anwenden. Sie können weiter mit dem erlangten Wissen aus dem Modul sicher umgehen und können Aufgaben und Problemstellungen nachvollziehen und lösen. *Sozialkompetenz:* Die Studierenden erlernen aufgrund gemeinsamer forensischen Untersuchungen im Team zu arbeiten und können auftretende Probleme, Fragen und Aufgaben durch fachgebunden Diskussion lösen. Die Studierenden erlangen die Fähigkeit eine forensische Untersuchung durchzuführen und sind in der Lage die Ergebnisse zu bewerten. Des Weiter besitzen Sie die Kompetenz sich an neue Gegebenheiten anzupassen und können so auf veränderte Hardware und Software reagieren.
Notwendige Voraussetzungen:	Erfolgreicher Abschluss des Moduls • System Sicherheit 1a
Empfohlene Voraussetzungen:	Erfolgreicher Abschluss des Moduls • Einführung IT Sicherheit
Einpassung in den Studienplan:	Ab Studiensemester 5

Verwendbarkeit des Moduls:	Dieses Modul ist verwendbar für • Studierende der Informatik • Studierende der Wirtschaftsinformatik • Studierende der Mathematik und Informatik auf Bachelorniveau.
Studien- und Prüfungsleistungen:	Schriftliche Prüfung: 60 min.
Berechnung der Modulnote:	Schriftliche Prüfung
Turnus des Angebots:	Wintersemester
Wiederholung der Prüfungen:	
Anerkannte Module:	
Anerkannte Lernergebnisse:	
Generelle Zielsetzung des Moduls:	Modul zur Förderung und Verstärkung der Fachkompetenz
Arbeitsaufwand bzw. Gesamtworkload:	Summe: 150h Präsenzanteil: 30h • Vorlesungsteil: 12h • Virtuelle Lehre: 10h • Übungsteil: 2h • Prüfungsvorbereitungsveranstaltung: 5h • Prüfung: 1h Fernstudienanteil: 120h • Durcharbeiten der Studienbriefe: 70h • Wahrnehmen der Online Betreuung und Beratung: 10h • Ausarbeiten von Aufgaben: 20h • Individuelle Prüfungsvorbereitung der Studierenden: 20h
Lerninhalt und Niveau:	Das Niveau der Lerninhalte liegt gemessen am DQR-Niveau bei 6 (Bachelor)
Leistungspunkte:	5 ECTS
Moduldauer:	1 Semester
Unterrichtssprache:	Deutsch
Medienformen:	Studienbriefe in schriftlicher und elektronischer Form, Onlinematerial in Lernplattform, Übungen und Projekt über Lernplattform, Online-Konferenzen, Chat und Forum, Präsenzveranstaltung mit Rechner und Beamer.

Literatur:	Als begleitende und vertiefende Literatur wird empfohlen: 1. Eigenes Skript 2. Eoghan Casey (Hrsg.): Handbook of computer crime investigation. Forensic tools and technology. 6th Printing. Elsevier Academic Press, Amsterdam u. a. 2007, ISBN 978-0-12-163103-1. 3. Alexander Geschonneck: Computer-Forensik. Computerstraftaten erkennen, ermitteln, aufklären. 5. aktualisierte und erweiterte Auflage. dpunkt Verlag, Heidelberg 2011, ISBN 978-3-89864-774-8. Weitere Literatur wird in der Lehrveranstaltung bekannt gegeben.

Modulbeschreibung

Studiengang:	Bachelor IT-Sicherheit
Modulbezeichnung:	Compilerbau
Lehrveranstaltungen:	Compilerbau
Dozent(in):	Prof. Dr. Felix Freiling
Modulverantwortliche(r):	Prof. Dr. Felix Freiling
Modulentwickler(in):	Nadina Hintz
Inhalt:	Im Modul Compilerbau wird auf folgende Themengebiete eingegangen: • Analyse von kontextfreien Sprachen • Das Produzieren von Dateien mit JavaCC • Der Umgang mit dem token Manager • Das Schreiben eines einfaches yacc-Programms • Aufbau eines lex-Programms • Die Übersetzung eines lex-Programms in einen ablauffähigen Code
Lernziele/Kompetenzen:	*Fachkompetenz:* Die Studierenden erwerben fundierte Kenntnisse über den Compilerbau und den Java Compiler Compiler JavaCC. Sie lernen das Computerprogramm Yacc zur Herstellung von Compilern kennen sowie das Programm lex. *Methodenkompetenz:* Die Studierenden beherrschen die Fähigkeit, kontextfreie Sprachen zu analysieren und Dateien mit JavaCC zu produzieren. Weiter erwerben sie ein Verständnis über den Aufbau eines lex-Programmes und die Fähigkeit, ein lex-Programm in einen lauffähigen Code zu übersetzen. *Sozialkompetenz:* Aufgrund der Teamarbeit, unter anderem in den Präsenzwochenenden, erweitern die Studierenden ihre Teamfähigkeit und Sozialkompetenz. Die Studierenden erlangen die Fähigkeit zur Bildung einer Meinung über die eigene Arbeitsweise und die Arbeitsweise anderer. Darüber hinaus erlangen sie die Fähigkeit, in komplexen Situationen zu handeln und eine Lösung für komplexe Probleme zu finden.
Notwendige Voraussetzungen:	Erfolgreicher Abschluss der vorherigen Module insbesondere: • Systemnahe Programmierung • Algorithmen und Datenstrukturen
Empfohlene Voraussetzungen:	Keine
Einpassung in den Studienplan:	Ab Studiensemester 5

Verwendbarkeit des Moduls:	Dieses Modul ist verwendbar für • Studierende der Informatik • Studierende der Wirtschaftsinformatik • Studierende der Mathematik und Informatik auf Bachelorniveau. Dieses Modul kann nicht als Wahlpflichtmodul gewählt werden, sondern ist ein Pflichtmodul.
Studien- und Prüfungsleistungen:	Schriftliche Prüfung: 60 min.
Berechnung der Modulnote:	Schriftliche Prüfung
Turnus des Angebots:	Wintersemester
Wiederholung der Prüfungen:	
Anerkannte Module:	
Anerkannte Lernergebnisse:	
Generelle Zielsetzung des Moduls:	Zur Förderung und Verstärkung der Fachkompetenz
Arbeitsaufwand bzw. Gesamtworkload:	Summe: 150 h Präsenzzeit: 30 h • Vorlesungsteil: 10 h • Übungsteil: 5 h • Praktischer Teil: 10 h • Prüfungsvorbereitungsveranstaltung: 4 h • Prüfung: 1 h Eigenstudium: 120 h • Durcharbeiten der Studienbriefe: 50 h • Durcharbeiten des Online-Lernmaterials: 10 h • Wahrnehmen der Online Betreuung und Beratung: 10 h • Ausarbeiten von Aufgaben: 30 h • Individuelle Prüfungsvorbereitung der Studierenden: 20 h
Lerninhalt und Niveau:	Niveau der Lerninhalte liegt gemessen am DQR-Niveau bei 6 (Bachelor)
Leistungspunkte:	5 ECTS
Moduldauer:	1 Semester
Unterrichtssprache:	Deutsch
Medienformen:	Studienbriefe in schriftlicher und elektronischer Form, Onlinematerial in Lernplattform, Übungen und Projekte über Lernplattform, Online-Konferenzen, Chat und Forum, Präsenzveranstaltungen mit Computer und Beamer.

Literatur:	Als begleitende und vertiefende Literatur wird empfohlen: • Flex und Bison, John Levine, 2009 • Compiler construction using java, JavaCC and Yacc, Anthony J. Dos Reis, 2012 • Compilerbau Teil 1, Jeffrey d. Ullmann, 1999 Weitere Literatur wird in der Lehrveranstaltung bekanntgegeben.

Modulbeschreibung

Studiengang:	Bachelor IT-Sicherheit
Modulbezeichnung:	Netzsicherheit 1
Lehrveranstaltungen:	Netzsicherheit 1
Dozent(in):	Prof. Dr. Jörg Schwenk
Modulverantwortliche(r):	Prof. Dr. Jörg Schwenk
Modulentwickler(in):	
Inhalt:	Kryptographie wird eingesetzt, um die Vertraulichkeit und Integrität von Daten zu schützen, die über Datennetze übertragen werden. Hierbei werden sowohl symmetrische Verfahren (Mobilfunk, WLAN), als auch asymmetrische bzw. hybride Verfahren (E-Mail, WWW, VPN) eingesetzt. In diesem Modul werden konkrete kryptographische Systeme zur Absicherung von Netzen betrachtet, und von allen Seiten auf ihre Sicherheit hin beleuchtet. Dieses Modul umfasst folgende Themen: • Einführung in lokale Netze, • WLAN (IEEE 802.11), • VPN (IPSec, PPTP, IP Multicast), • Mobilfunk (GSM, UMTS), Neben den Systemen selbst werden dabei auch publizierte Angriffe auf diese Systeme besprochen; die Studenten werden aufgefordert, selbst wissenschaftliche Überlegungen zur Verbesserung der Sicherheit anzustellen.

Lernziele/Kompetenzen:	*Fachkompetenz:* Die Studierenden erkennen die wichtigen Strukturen von Sicherheitsmechanismen in lokalen Datennetzen, verstehen Übertragungs- und Authentifizierungsprotokolle in Datennetzen und können die darin verwendeten kryptographischen Verfahren ermitteln. Die Studenten können das Zusammenspiel der kryptographischen Verfahren in einem Protokoll auf erste Sicherheitslücken hin überprüfen und eine erste Einschätzung der Sicherheit des Protokolls liefern. *Methodenkompetenz:* Die Studierenden beherrschen den Umgang mit Fachliteratur und können ihr wichtige Informationen eigenständig entnehmen. Weiterhin sind die Studierenden mit verschiedenen Angriffstechniken vertraut, welche auf neue Protokolle und Verfahren übertragen werden können. *Sozialkompetenz:* Die Studenten tauschen sich über Probleme beim Erarbeiten und Anwenden von neuen Inhalten aus und können problemorientiert diskutieren. Die Studenten erlangen die Fähigkeit, sich eine Meinung über die Sicherheit von Protokollen zu bilden. Darüber hinaus besitzen sie die Kompetenz, neue Angriffe aus der aktuellen Fachliteratur zu verstehen und ihre Bedeutungen zu evaluieren. Die Studenten entwickeln ein „gesundes Misstrauen“ gegenüber vorgegebenen Sicherheitskonzepten.
Notwendige Voraussetzungen:	• Modul Grundlagen der Programmierung
Empfohlene Voraussetzungen:	• Modul Kryptographie 1
Einpassung in den Studienplan:	Ab Studiensemester 5
Verwendbarkeit des Moduls:	Dieses Modul ist verwendbar für • Studierende der IT-Sicherheit • Studierende der Informatik • Studierende der Wirtschaftsinformatik • Studierende der Mathematik und Informatik auf Bachelorniveau. Dieses Modul kann nicht als Wahlpflichtmodul gewählt werden, sondern ist ein Pflichtmodul.
Studien- und Prüfungsleistungen:	Schriftliche Prüfung: 120 min.
Berechnung der Modulnote:	Schriftliche Prüfung
Turnus des Angebots:	Jedes Semester

Wiederholung der Prüfungen:	
Anerkannte Module:	
Anerkannte Lernergebnisse:	
Generelle Zielsetzung des Moduls:	Modul zur Förderung und Verstärkung der Fachkompetenz
Arbeitsaufwand bzw. Gesamtworkload:	Summe: 150 h Präsenzzeit: 2 h • Prüfung: 2h Eigenstudium: 148 h • Durcharbeiten der Studienbriefe: 85 h • Durcharbeiten des Online-Lernmaterials: 15 h • Wahrnehmen der Online Betreuung und Beratung: 10 h • Ausarbeiten von Aufgaben: 30 h • Individuelle Prüfungsvorbereitung der Studierenden: 8 h
Lerninhalt und Niveau:	Das Niveau der Lerninhalte liegt gemessen am DQR-Niveau bei 6 (Bachelor)
Leistungspunkte:	5 ECTS
Moduldauer:	1 Semester
Unterrichtssprache:	Deutsch, aktuelle Fachliteratur in englischer Sprache
Medienformen:	Studienbriefe in schriflicher und elektronischer Form, Online-material in Lernplattform, Übungen über Lernplattform, Online-Konferenzen, Chat und Forum
Literatur:	• Sicherheit und Kryptographie im Internet, Jörg Schwenk, 2005 • Understanding Cryptography, Christof Paar, Jan Pelzl, 2010 • Computer Networks, Andrew S. Tanenbaum, 2002 Weitere Literatur wird in der Lehrveranstaltung bekannt gegeben.

Modulbeschreibung

Studiengang:	Bachelor IT-Sicherheit
Modulbezeichnung:	Kryptographie 2
Lehrveranstaltungen:	Kryptographie 2
Dozent(in):	Prof. Dr. Christof Paar
Modulverantwortliche(r):	Prof. Dr. Christof Paar
Modulentwickler(in):	
Inhalt:	In diesem Modul werden asymmetrische kryptographische Verfahren behandelt. Die Schwerpunkte dieses Moduls liegen auf der Besprechung von praktisch wichtigen Verfahren und deren Einsatz für asymmetrische Basisdienste. Es werden sowohl diskrete Logarithmusverfahren (Diffie-Hellman, Elgamal, elliptische Kurven), als auch das RSA-Verfahren behandelt. Außerdem werden digitale Signaturen eingeführt. Es werden die Grundlagen der symmetrischen und asymmetrischen Schlüsselverteilung behandelt.
Lernziele/Kompetenzen:	*Fachkompetenz:* Die Studierenden kennen die Bedeutung von asymmetrischen kryptographischen Verfahren und verstehen die Strukturen der prominentesten asymmetrischen Primitiven. Darüber hinaus verstehen die Studenten die Sicherheitskonzepte und diverse Angriffsziele in der asymmetrischen Kryptographie. Die Studenten können ihr Wissen über die Kryptographie anwenden und Sicherheitslösungen finden. *Methodenkompetenz:* Die Studierenden beherrschen die Denkweisen, die in der modernen Kryptographie eingesetzt werden und können diese anhand von asymmetrischen Verfahren nachvollziehen. *Sozialkompetenz:* Die Studenten tauschen sich über Probleme beim Verstehen von symmetrischen kryptographischen Verfahren aus und diskutieren Lösungswege von Problemen. Die Studenten erlangen die Fähigkeit aktuelle asymmetrische kryptographische Verfahren zu verstehen und eine fundierte Meinung über die Sicherheit dieser Verfahren zu vertreten. Darüber hinaus besitzen die Studierenden alle Voraussetzungen neue asymmetrische Verfahren aus der aktuellen Fachliteratur zu verstehen und ihre Bedeutungen einzuschätzen. Das umfangreiche Wissen der Studenten befähigt sie Sicherheitslösungen zu finden und einzusetzen.
Notwendige Voraussetzungen:	
Empfohlene Voraussetzungen:	
Einpassung in den Studienplan:	Ab Studiensemester 5

Verwendbarkeit des Moduls:	Dieses Modul ist verwendbar für • Studierende der IT-Sicherheit • Studierende der Informatik • Studierende der Wirtschaftsinformatik • Studierende der Mathematik und Informatik auf Bachelorniveau. Dieses Modul kann nicht als Wahlpflichtmodul gewählt werden, sondern ist ein Pflichtmodul.
Studien- und Prüfungsleistungen:	Schriftliche Prüfung: 120 min.
Berechnung der Modulnote:	Schriftliche Prüfung
Turnus des Angebots:	Jedes Semester
Wiederholung der Prüfungen:	
Anerkannte Module:	
Anerkannte Lernergebnisse:	
Generelle Zielsetzung des Moduls:	Modul zur Förderung und Verstärkung der Fachkompetenz
Arbeitsaufwand bzw. Gesamtworkload:	Summe: 150 h Präsenzzeit: 2 h • Prüfung: 2h Eigenstudium: 148 h • Durcharbeiten der Studienbriefe: 85 h • Durcharbeiten des Online-Lernmaterials: 15 h • Wahrnehmen der Online Betreuung und Beratung: 10 h • Ausarbeiten von Aufgaben: 30 h • Individuelle Prüfungsvorbereitung der Studierenden: 8 h
Lerninhalt und Niveau:	Das Niveau der Lerninhalte liegt gemessen am DQR-Niveau bei 6 (Bachelor)
Leistungspunkte:	5 ECTS
Moduldauer:	1 Semester
Unterrichtssprache:	Deutsch, Englisch
Medienformen:	Studienbriefe in schriflicher und elektronischer Form, Online-material in Lernplattform, Übungen über Lernplattform, Online-Konferenzen, Chat und Forum
Literatur:	• Understanding Cryptography, Christof Paar, Jan Pelzl, 2010 • Handbook of Applied Cryptography, Alfred J. Menezes, Paul C van Oorschot, Scott A Vanstone, 1996 Weitere Literatur wird in der Lehrveranstaltung bekannt gegeben.

Modulbeschreibung

Studiengang:	Bachelor IT-Sicherheit
Modulbezeichnung:	Netzsicherheit 2
Lehrveranstaltungen:	Netzsicherheit 2
Dozent(in):	Prof. Dr. Jörg Schwenk
Modulverantwortliche(r):	Prof. Dr. Jörg Schwenk
Modulentwickler(in):	
Inhalt:	Kryptographie wird eingesetzt, um die Vertraulichkeit und Integrität von Daten zu schützen, die über Datennetze übertragen werden. Hierbei werden sowohl symmetrische Verfahren (Mobilfunk, WLAN), als auch asymmetrische bzw. hybride Verfahren (E-Mail, WWW, VPN) eingesetzt. In diesem Modul werden konkrete kryptographische Systeme zur Absicherung von Netzen der dritten und vierten Ebene des OSI Schichtenmodells betrachtet und von allen Seiten auf ihre Sicherheit hin beleuchtet. Dieses Modul umfasst folgende Themen: • SSL, • SSH, • OpenPGP, • S/MIME und • DNSSEC Neben den Systemen selbst werden dabei auch publizierte Angriffe auf diese Systeme besprochen; die Studenten werden aufgefordert, selbst wissenschaftliche Überlegungen zur Verbesserung der Sicherheit anzustellen. Als Grundlage werden kurz auch die Transportprotokolle TCP und UDP behandelt.
Lernziele/Kompetenzen:	*Fachkompetenz:* Die Teilnehmer erwerben die Grundlagen zum Einrichten sicherer Kommunikationskanäle. Darüber hinaus lernen sie verschiedene Wege, wie die einzelnen Anwendungen in der Vergangenheit angegriffen wurden. *Methodenkompetenz:* Die Studierenden beherrschen den Umgang mit Fachliteratur und können ihr wichtige Informationen eigenständig entnehmen. Weiterhin sind die Studierenden mit verschiedenen Angriffstechniken vertraut, welche auf neue Protokolle und Verfahren übertragen werden können. *Sozialkompetenz:* Die Studenten tauschen sich über Probleme beim Erarbeiten und Anwenden von neuen Inhalten aus und können problemorientiert diskutieren. Die Studenten erlangen die Fähigkeit, sich eine Meinung über die Sicherheit von Protokollen zu bilden. Darüber hinaus besitzen sie die Kompetenz, neue Angriffe aus der aktuellen Fachliteratur zu verstehen und ihre Bedeutungen zu evaluieren. Die Studenten entwickeln ein "gesundes Misstrauen"gegenüber vorgegebenen Sicherheitskonzepten.

Notwendige Voraussetzungen:	Erfolgreicher Abschluss der vorherigen Module insbesondere: • Modul Grundlagen der Programmierung • Modul Kryptographie 1 • Modul Kryptographie 2
Empfohlene Voraussetzungen:	
Einpassung in den Studienplan:	Ab Studiensemester 6
Verwendbarkeit des Moduls:	Dieses Modul ist verwendbar für • Studierende der IT-Sicherheit • Studierende der Informatik • Studierende der Wirtschaftsinformatik • Studierende der Mathematik und Informatik auf Bachelorniveau. Dieses Modul kann nicht als Wahlpflichtmodul gewählt werden, sondern ist ein Pflichtmodul.
Studien- und Prüfungsleistungen:	Schriftliche Prüfung: 120 min.
Berechnung der Modulnote:	Schriftliche Prüfung
Turnus des Angebots:	Jedes Semester
Wiederholung der Prüfungen:	
Anerkannte Module:	
Anerkannte Lernergebnisse:	
Generelle Zielsetzung des Moduls:	Modul zur Förderung und Verstärkung der Fachkompetenz
Arbeitsaufwand bzw. Gesamtworkload:	Summe: 150 h Präsenzzeit: 2 h • Prüfung: 2h Eigenstudium: 148 h • Durcharbeiten der Studienbriefe: 85 h • Durcharbeiten des Online-Lernmaterials: 15 h • Wahrnehmen der Online Betreuung und Beratung: 10 h • Ausarbeiten von Aufgaben: 30 h • Individuelle Prüfungsvorbereitung der Studierenden: 8 h
Lerninhalt und Niveau:	Das Niveau der Lerninhalte liegt gemessen am DQR-Niveau bei 6 (Bachelor)
Leistungspunkte:	5 ECTS
Moduldauer:	1 Semester
Unterrichtssprache:	Deutsch, aktuelle Fachliteratur in englischer Sprache

Medienformen:	Studienbriefe in schriflicher und elektronischer Form, Online-material in Lernplattform, Übungen über Lernplattform, Online-Konferenzen, Chat und Forum
Literatur:	• Sicherheit und Kryptographie im Internet, Jörg Schwenk, 2005 • Understanding Cryptography, Christof Paar, Jan Pelzl, 2010 • Computer Networks, Andrew S. Tanenbaum, 2002 Weitere Literatur wird in der Lehrveranstaltung bekannt gegeben.

Modulbeschreibung

Studiengang:	Bachelor IT-Sicherheit
Modulbezeichnung:	Realisierung von Softwareprojekten
Lehrveranstaltungen:	Realisierung von Softwareprojekten
Dozent(in):	Prof. Dr. Felix Freiling
Modulverantwortliche(r):	Prof. Dr. Felix Freiling
Modulentwickler(in):	
Inhalt:	Im Modul Realisierung von Softwareprojekten wird auf folgende Themengebiete eingegangen: • Model Driven Architecture UML • Sichere Softwareentwicklung / SDL Microsoft JavaScript • Grundlegende Kenntnisse in PHP
Lernziele/Kompetenzen:	*Fachkompetenz:* Die Studierenden erwerben fundierte Kenntnisse über Prozessmodellierung und lernen Zustandsdiagramme zu erstellen. Darüber hinaus erlangen sie Kenntnisse über Secure Coding Policies und Testing Policies. *Methodenkompetenz:* Die Studierenden beherrschen die Fähigkeiten ein Softwareprojekt zu entwerfen und umzusetzen sowie ein sicheres Programm zu schreiben. *Sozialkompetenz:* Aufgrund der Teamarbeit, unter anderem an den Präsenzwochenenden, erweitern die Studierenden ihre Teamfähigkeit und Sozialkompetenz. Durch die Eigenentwicklung von Softwareprojekten erweitern die Studierenden ihre Selbstständigkeit. Die Studierenden lernen somit Verantwortung für ihr Handeln zu übernehmen und steigern ihre Entscheidungsfähigkeit.
Notwendige Voraussetzungen:	Erfolgreicher Abschluss der vorherigen Module, insbesondere • Grundlagen der Programmierung • Programmierkonzepte • Konzeptionelle Modellierung
Empfohlene Voraussetzungen:	Keine
Einpassung in den Studienplan:	Ab Studiensemester 6

Verwendbarkeit des Moduls:	Dieses Modul ist verwendbar für • Studierende der Informatik • Studierende der Wirtschaftsinformatik • Studierende der Mathematik und Informatik auf Bachelorniveau. Dieses Modul kann nicht als Wahlpflichtmodul gewählt werden, sondern ist ein Pflichtmodul.
Studien- und Prüfungsleistungen:	Schriftliche Prüfung: 60 min.
Berechnung der Modulnote:	Schriftliche Prüfung
Turnus des Angebots:	Sommersemester
Wiederholung der Prüfungen:	
Anerkannte Module:	
Anerkannte Lernergebnisse:	
Generelle Zielsetzung des Moduls:	Zur Förderung und Verstärkung der Fachkompetenz
Arbeitsaufwand bzw. Gesamtworkload:	Summe: 150 h Präsenzzeit: 30 h • Vorlesungsteil: 10 h • Übungsteil: 5 h • Praktischer Teil: 10 h • Prüfungsvorbereitungsveranstaltung: 4 h • Prüfung: 1 h Eigenstudium: 120 h • Durcharbeiten der Studienbriefe: 50 h • Durcharbeiten des Online-Lernmaterials: 10 h • Wahrnehmen der Online Betreuung und Beratung: 10 h • Ausarbeiten von Aufgaben: 30 h • Individuelle Prüfungsvorbereitung der Studierenden: 20 h
Lerninhalt und Niveau:	Niveau der Lerninhalte liegt gemessen am DQR-Niveau bei 6 (Bachelor)
Leistungspunkte:	5 ECTS
Moduldauer:	1 Semester
Unterrichtssprache:	Deutsch
Medienformen:	Studienbriefe in schriftlicher und elektronischer Form, Onlinematerial in Lernplattform, Übungen und Projekte über Lernplattform, Online-Konferenzen, Chat und Forum, Präsenzveranstaltungen mit Computer und Beamer

Literatur:	Als Begleitende und vertiefende Literatur wird empfohlen: 1. Software-Engineering mit UML, Vieweg+Teubner Verlag, 2009 2. Das JavaScript-Handbuch, Ralph Steyer 2010 Literatur wird in der Lehrveranstaltung bekanntgegeben

Modulbeschreibung

Studiengang:	Bachelor IT-Sicherheit
Modulbezeichnung:	Kryptographische Protokolle
Lehrveranstaltungen:	Kryptographische Protokolle
Dozent(in):	Prof. Dr. Jörg Schwenk
Modulverantwortliche(r):	Prof. Dr. Jörg Schwenk
Modulentwickler(in):	
Inhalt:	Dieses Modul bietet eine Einführung in das Gebiet der kryptographischen Protokolle, die den Einsatz bekannter und neuer Verfahren der Kryptographie in der Kommunikation zwischen mehreren Instanzen beschreiben. Hierbei wird sowohl Wert auf die Beschreibungen als auch auf die Sicherheit gelegt. Das Modul umfasst als Einführung allgemeine kryptographische Grundlagen, die Konzepte der beweisbaren Sicherheit und eine Einführung zu kryptographischen Protokollen. Im Folgenden werden einfache Protokolle behandelt. Hierzu zählen Passwort/Nutzername Protokolle, Wechselcodes, das Challenge-and-Response Verfahren, das Diffie-Hellman Protokoll, ElGamal sowie Shamir's No-Key-Verfahren. Des Weiteren werden Zero Knowledge Protokolle und ihre Theorie besprochen. Den Schwerpunkt des Moduls werden Schlüsselaustausch Protokolle bilden. Hierfür werden die Sicherheitsmodelle von Belare - Rogaway sowie Canetti - Krawczyk eingeführt. Den Abschluss des Moduls bildet eine detaillierte Beschreibung und formale Sicherheitsanalyse von TLS, dem wohl am weitesten verbreitete Authentifizierungs- und Schlüsseltausch Protokolls im Internet.
Lernziele/Kompetenzen:	*Fachkompetenz:* Die Studierenden verstehen die Besonderheit kryptographischer Protokolle, bei denen nicht mehr ein Algorithmus im Vordergrund steht, sondern die Interaktion verschiedener Einheiten. Die Studenten erkennen die praktische Relevanz der Kryptographie und begreifen die Schwierigkeit, kryptographische Protokolle - wie sie im Internet eingesetzt werden - formal auf ihre Sicherheit hin zu analysieren. Die Studenten kennen wichtige Sicherheitsziele und Sicherheitsmodelle, welche sie auf echte Protokolle anwenden können. *Methodenkompetenz:* Die Studierenden beherrschen den Umgang mit kryptographischer Fachliteratur und können ihr wichtige Ergebnisse eigenständig entnehmen. Weiterhin sind die Studierenden mit verschiedenen Beweistechniken und Sicherheitsmodellen vertraut, welche für formale Sicherheitsanalysen neuer Protokolle angewendet werden können. *Sozialkompetenz:* Die Studenten tauschen sich über Probleme beim Verstehen und Anwenden von neuen Modellen und Techniken aus und können wissenschaftlich zielorientiert diskutieren. Die Studenten erlangen die Fähigkeit, kryptographische Protokolle zu analysieren und eine wissenschaftlich begründete Einschätzung ihrer Sicherheit zu bilden. Darüber hinaus besitzen sie die Kompetenz, neue Protokolle aus der aktuellen Fachliteratur zu verstehen und ihre Sicherheit eigenständig zu evaluieren.

Notwendige Voraussetzungen:	• Modul Kryptographie 1 • Modul Kryptographie 2
Empfohlene Voraussetzungen:	
Einpassung in den Studienplan:	Ab Studiensemester 9
Verwendbarkeit des Moduls:	Dieses Modul ist verwendbar für • Studierende der IT-Sicherheit • Studierende der Informatik • Studierende der Wirtschaftsinformatik • Studierende der Mathematik und Informatik auf Bachelorniveau. Dieses Modul kann als Wahlpflichtmodul gewählt werden, und ist kein Pflichtmodul.
Studien- und Prüfungsleistungen:	Schriftliche Prüfung: 120 min.
Berechnung der Modulnote:	Schriftliche Prüfung
Turnus des Angebots:	Jedes Semester
Wiederholung der Prüfungen:	
Anerkannte Module:	
Anerkannte Lernergebnisse:	
Generelle Zielsetzung des Moduls:	Modul zum Aufbau von Kenntnissen und Erfahrungen in einem Spezialgebiet
Arbeitsaufwand bzw. Gesamtworkload:	Summe: 150 h Präsenzzeit: 2 h • Prüfung: 2h Eigenstudium: 148 h • Durcharbeiten der Studienbriefe: 85 h • Durcharbeiten des Online-Lernmaterials: 15 h • Wahrnehmen der Online Betreuung und Beratung: 10 h • Ausarbeiten von Aufgaben: 30 h • Individuelle Prüfungsvorbereitung der Studierenden: 8 h
Lerninhalt und Niveau:	Das Niveau der Lerninhalte liegt gemessen am DQR-Niveau bei 6 (Bachelor)
Leistungspunkte:	5 ECTS
Moduldauer:	1 Semester
Unterrichtssprache:	Deutsch, aktuelle Facharktikel in englischer Sprache

Medienformen:	Studienbriefe in schriflicher und elektronischer Form, Online-material in Lernplattform, Übungen über Lernplattform, Online-Konferenzen, Chat und Forum
Literatur:	• Moderne Verfahren der Kryptographie, Beutelsbacher, Schwenk, Wolfenstetter, 2000 • Protocols for Authentication and Key Esteblishment, Boyd, Maturia, 2003 • Understanding Cryptography, Christof Paar, Jan Pelzl, 2010 • Sicherheit und Kryptographie im Internet, Jörg Schwenk, 2005 Weitere Literatur wird in der Lehrveranstaltung bekannt gegeben.

Modulbeschreibung

Studiengang:	Bachelor IT-Sicherheit
Modulbezeichnung:	Netzsicherheit 3
Lehrveranstaltungen:	Netzsicherheit 3
Dozent(in):	Prof. Dr. Jörg Schwenk
Modulverantwortliche(r):	Prof. Dr. Jörg Schwenk
Modulentwickler(in):	
Inhalt:	Kryptographie wird eingesetzt, um die Vertraulichkeit und Integrität von Daten zu schützen, die über Datennetze übertragen werden. Hierbei werden sowohl symmetrische Verfahren (Mobilfunk, WLAN), als auch asymmetrische bzw. hybride Verfahren (E-Mail, WWW, VPN) eingesetzt. In diesem Modul werden konkrete kryptographische Systeme zur Absicherung des World Wide Web (www) betrachtet und von allen Seiten auf ihre Sicherheit hin beleuchtet. Dieses Modul umfasst folgende Themen: • Same Origin Policy • Cross Site Scripting • Cross Site Request Forgery • XML • Web Services Neben den Systemen selbst werden dabei auch publizierte Angriffe auf diese Systeme besprochen; die Studenten werden aufgefordert, selbst wissenschaftliche Überlegungen zur Verbesserung der Sicherheit anzustellen.
Lernziele/Kompetenzen:	*Fachkompetenz:* Die Studierenden erwerben grundlegendes Wissen im Bereich der Sicherheit von Webanwendung. Sie sind in der Lage die Sicherheit einer Webanwendung einzuschätzen und Angriffspunkte offenzulegen. *Methodenkompetenz:* Die Studierenden beherrschen den Umgang mit Fachliteratur und können ihr wichtige Informationen eigenständig entnehmen. Weiterhin sind die Studierenden mit verschiedenen Angriffstechniken vertraut, welche auf neue Protokolle und Verfahren übertragen werden können. *Sozialkompetenz:* Die Studenten tauschen sich über Probleme beim Erarbeiten und Anwenden von neuen Inhalten aus und können problemorientiert diskutieren. Die Studenten erlangen die Fähigkeit, sich eine Meinung über die Sicherheit von Protokollen zu bilden. Darüber hinaus besitzen sie die Kompetenz, neue Angriffe aus der aktuellen Fachliteratur zu verstehen und ihre Bedeutungen zu evaluieren. Die Studenten entwickeln ein "gesundes Misstrauen"gegenüber vorgegebenen Sicherheitskonzepten.

Notwendige Voraussetzungen:	• Modul Grundlagen der Programmierung
Empfohlene Voraussetzungen:	
Einpassung in den Studienplan:	Ab Studiensemester 7
Verwendbarkeit des Moduls:	Dieses Modul ist verwendbar für • Studierende der IT-Sicherheit • Studierende der Informatik • Studierende der Wirtschaftsinformatik • Studierende der Mathematik und Informatik auf Bachelorniveau. Dieses Modul kann nicht als Wahlpflichtmodul gewählt werden, sondern ist ein Pflichtmodul.
Studien- und Prüfungsleistungen:	Schriftliche Prüfung: 120 min.
Berechnung der Modulnote:	Schriftliche Prüfung
Turnus des Angebots:	Jedes Semester
Wiederholung der Prüfungen:	
Anerkannte Module:	
Anerkannte Lernergebnisse:	
Generelle Zielsetzung des Moduls:	Modul zur Förderung und Verstärkung der Fachkompetenz
Arbeitsaufwand bzw. Gesamtworkload:	Summe: 150 h Präsenzzeit: 2 h • Prüfung: 2h Eigenstudium: 148 h • Durcharbeiten der Studienbriefe: 85 h • Durcharbeiten des Online-Lernmaterials: 15 h • Wahrnehmen der Online Betreuung und Beratung: 10 h • Ausarbeiten von Aufgaben: 30 h • Individuelle Prüfungsvorbereitung der Studierenden: 8 h
Lerninhalt und Niveau:	Das Niveau der Lerninhalte liegt gemessen am DQR-Niveau bei 6 (Bachelor)
Leistungspunkte:	5 ECTS
Moduldauer:	1 Semester
Unterrichtssprache:	Deutsch, aktuelle Facharktikel in englischer Sprache
Medienformen:	Studienbriefe in schriflicher und elektronischer Form, Online-material in Lernplattform, Übungen über Lernplattform, Online-Konferenzen, Chat und Forum

Literatur:	• Understanding Cryptography, Christof Paar, Jan Pelzl, 2010 • Sicherheit und Kryptographie im Internet, Jörg Schwenk, 2005 • Computer Networks, Andrew S. Tanenbaum, 2002 Weitere Literatur wird in der Lehrveranstaltung bekannt gegeben.

Anhang

(1) Beispiel Arbeitsaufwand / Gesamtworkload

Präsenzstudium:	6	Zeitstunden
Fernstudienanteil:	46	Zeitstunden
davon Selbststudium:	30	Zeitstunden
davon Aufgaben:	14	Zeitstunden
davon Online-Betreuung:	2	Zeitstunden
Prüfungszeit inkl. Prüfungsvorbereitung:	8	Zeitstunden
davon Präsenz:	3	Zeitstunden
Summe:	**60**	**Zeitstunden**
	15	% = Präsenz

(2) DQR-Niveaustufen

Niveau 1: Erfüllung einfacher Anforderungen in einem überschaubar und stabil strukturierten Lern- oder Arbeitsbereich. Die Erfüllung der Aufgaben erfolgt unter Anleitung.

Niveau 2: Fachgerechte Erfüllung grundlegender Anforderungen in einem überschaubar und stabil strukturierten Lern- oder Arbeitsbereich. Die Erfüllung der Aufgaben erfolgt weitgehend unter Anleitung.

Niveau 3: Selbständige Erfüllung fachlicher Anforderungen in einem noch überschaubaren und zum Teil offen strukturierten Lernbereich oder beruflichen Tätigkeitsfeld.

Niveau 4: Selbständige Planung und Bearbeitung fachlicher Aufgabenstellungen in einem umfassenden, sich verändernden Lernbereich oder beruflichen Tätigkeitsfeld.

Niveau 5: Selbständige Planung und Bearbeitung umfassender fachlicher Aufgabenstellungen in einem komplexen, spezialisierten, sich verändernden Lernbereich oder beruflichen Tätigkeitsfeld.

Niveau 6: Planung, Bearbeitung und Auswertung von umfassenden fachlichen Aufgaben- und Problemstellungen sowie eigenverantwortliche Steuerung von Prozessen in Teilbereichen eines wissenschaftlichen Faches oder in einem beruflichen Tätigkeitsfeld. Die Anforderungsstruktur ist durch Komplexität und häufige Veränderungen gekennzeichnet.

Niveau 7: Bearbeitung von neuen komplexen Aufgaben- und Problemstellungen sowie eigenverantwortliche Steuerung von Prozessen in einem wissenschaftlichen Fach oder in einem strategieorientierten beruflichen Tätigkeitsfeld. Die Anforderungsstruktur ist durch häufige und unvorhersehbare Veränderungen gekennzeichnet.

Niveau 8: Gewinnung von Forschungserkenntnissen in einem wissenschaftlichen Fach oder Entwicklung innovativer Lösungen und Verfahren in einem beruflichen Tätigkeitsfeld. Die Anforderungsstruktur ist durch neuartige und unklare Problemlagen gekennzeichnet.

(3) Beispiel Lerninhaltsbeschreibung

1.Dienste

1.1 WWW, http: Funktionsweise des WWW auf der Basis von http und HTML, XML und WML
1.2 E-Mail: Transport von E-Mails vom Client über den Server zum Empfänger unter Berücksichtigung der verschiedenen Zeichensetzungen und der Kodierungen; Lesen von Email-Headern
1.3 weitere Dienste: IRC, Telnet, FTP, News
1.4 soziale Netzwerke: Profile, Kontakte, Personensuche
1.5 Peer-to-Peer-Kommunikation: Nutzung des Netzes zur schnellen Verteilung von Daten insbesondere am Beispiel von Tauschbörsen und Skype; Weiterentwicklung insbesondere mit dem Ziel der Anonymisierung
1.6 Neue Dienste wie VoIP, Skype, RSS, Podcast

Übungen: - Mit Wireshark Netzwerkverkehr aufzeichnen;
- Analyse einer HTML-Seite, einer E-Mail und eines sozialen Netzwerks

(4) DQR-Kategorien

Wissen bzw. Kenntnissen, d. h. kennen von Information im Sinne von Theorie und / oder Faktenwissen in einem Lern- oder Arbeitsbereich als Ergebnis von Lernen und Verstehen. Anforderungsstruktur: Tiefe und Breite.

Fertigkeiten, d. h. kognitive (logisches, intuitives und kreatives Denken) und praktische (Geschicklichkeit und Verwendung von Methoden, Materialien, Werkzeugen und Instrumenten) Fertigkeiten bei denen Wissen bzw. Kenntnisse zur Aufgaben- bzw. Problemlösung eingesetzt werden. Anforderungsstruktur: Instrumentale und systemische Fertigkeiten, Beurteilungsfähigkeit.

Sozialkompetenz ist die Fähigkeit und Bereitschaft, zielorientiert mit anderen zusammenzuarbeiten, ihre Interessen und sozialen Situationen zu erfassen, sich mit ihnen rational und verantwortungsbewusst auseinanderzusetzen und zu verständigen sowie die Arbeits- und Lebenswelt mitzugestalten. Anforderungsstruktur: Team / Führungsfähigkeit, Mitgestaltung und Kommunikation.

Selbständigkeit ist die Fähigkeit und Bereitschaft, eigenständig und verantwortlich zu handeln, eigenes Handeln und das Handeln anderer zu reflektieren, sowie die eigene Handlungsfähigkeit weiterzuentwickeln. Anforderungsstruktur: Eigenständigkeit / Verantwortung, Reflexivität und Lernkompetenz

(5) Lernergebnisorientierte Formulierungshilfen (in Anlehnung an Bloom's Taxonomie)

Lernergebnisse sollten möglichst kurz und präzise beschrieben werden, komplizierte Sätze und unnötiges Fachvokabular sollten nach Möglichkeit vermieden werden. Wenn machbar sollten Lernergebnisse in einem Satz beschrieben werden.

Wissen: auflisten, aufzählen, benennen, beschreiben, bezeichnen, definieren, erinnern, erkennen, feststellen, herausfinden, identifizieren, präsentieren, sammeln, skizzieren, wiedergeben, wiederholen, zeigen, zitieren.

Verstehen: assoziieren, ausdrücken, auseinanderhalten, auswählen, ausweiten, berichten, beschreiben, dekodieren, differenzieren, diskutieren, erkennen, erklären, gegenüberstellen, generalisieren, hinweisen, interpretieren, klären, konstruieren, klassifizieren, lokalisieren, lösen, schätzen, übersetzen, umwandeln, vorhersagen.

Anwenden: anwenden, ausprobieren, auswählen, bedienen, berechnen, beschäftigen, beurteilen, beziehen, demonstrieren, entdecken, entwickeln, erlassen, gebrauchen, interpretieren, konstruieren, lösen, manipulieren, planen, organisieren, produzieren, prüfen, skizzieren, transferieren, voraussagen, wählen, zeigen.

Analysieren: ableiten, analysieren, arrangieren, ausführen, berechnen, bestimmen, beurteilen, beziehen, debattieren, differenzieren, ermitteln, experimentieren, folgern, herausstellen, identifizieren, illustrieren, kategorisieren, klassifizieren, kritisieren, prüfen, untersuchen, vergleichen.

Synthetisieren:
anhäufen, argumentieren, arrangieren, neu arrangieren, aufbauen, ausdenken, beziehen, einrichten, entwickeln, erfinden, erklären, formulieren, generalisieren, generieren, hervorbringen, integrieren, kategorisieren, kombinieren, konstruieren, kreieren, machen, managen, modifizieren, organisieren, planen, rekonstruieren, reorganisieren, sammeln, transferieren, überarbeiten, vorbereiten, vorschlagen, zusammenfassen, zusammenfügen, übertragen.

Evaluieren: argumentieren, benoten, beurteilen, bewerten, beziehen, einschätzen, empfehlen, entscheiden, evaluieren, interpretieren, kontrastieren, kritisieren, messen, rechtfertigen, schließen, überarbeiten, überzeugen, unterscheiden, unterstützen, validieren, vergleichen, versichern, verteidigen, Wert bemessen.

(6) Beispiel Lernergebnisbeschreibung

Nach erfolgreichem Abschluss des Moduls hat der Studierende Kenntnisse über die grundlegenden Strukturen und möglichen Transportwege von Informationen im weltweiten Netz erworben. Er kennt die für den Betrieb des Internets erforderliche Hard- und Software und kann deren Bedeutung für die IT-Sicherheit beurteilen. Er kann die aus dem Informationsfluss resultierenden digitalen Spuren bewerten und Ermittlungsansätze selbstständig ableiten sowie Eigenschaften wichtiger Dienste nachvollziehen und diese einsetzen. Darüber hinaus hat er einen Überblick über die Sicherheitsaspekte der Netze und ist in der Lage, mögliche Tools sowohl bewerten als auch einsetzen zu können. Der Studierende ist fähig …