Hochschule
Albstadt-Sigmaringen
Albstadt-Sigmaringen University

Wahlpflichtmodul-Katalog

Fakultät Informatik
Studiengang
Advanced IT Security M.Sc.

StuPO 21.2
ab Wintersemester 2021/22
Ersteller: Prof. Dr. German Nemirovski, Studiendekan
Verantwortlich: Prof. Dr. German Nemirovski, Studiendekan

Inhaltsverzeichnis

1 Übersicht der Modulbeschreibungen

1.1 Wintersemester

- Business Intelligence
- Electronic System-Level Design
- File System Forensics
- Funktionale Programmierung
- Highly Optimized Hardware Cryptography
- Post-Quantum Cryptography and Quantum Key Exchange
- Semantic Web

1.2 Sommersemester

- Advanced Network and Internet Security
- Advanced Programming
- Blockchain Technology and Crypto Currencies
- Distributed Enterprise Applications
- Electronic Design Automation
- Finanical Risk & Financial Management
- Innovation and Transfer Competence
- IT Sicherheit und IT-Angriffe

2 Modulbeschreibungen

2.1 Wintersemester

2.1.1 51100 – Business Intelligence

Studiengang: Advanced IT Security M.Sc. **Semester**: WS 2021/22
StuPO-Version: 21.2 **Letzte Bearbeitung**: 14.04.21

<table>
<tr><td colspan="8">Modul: Business Inteligence</td></tr>
<tr><td colspan="2">Kennnummer
51100</td><td>Workload
180 h</td><td>Modulart
WPM</td><td colspan="2">Studiensemester
1</td><td>Dauer
1 Semester</td><td>Häufigkeit
WS und SS</td></tr>
<tr><td>1</td><td colspan="2">Lehrveranstaltung(en)
Vorlesung Business Intelligence
Project Business Intelligence</td><td colspan="2">Sprache
Deutsch oder Englisch, wenn von den Modulteil-nehmern gewünscht (deutsches und englisches Literatur-studium erforderlich)</td><td>Kontakt-zeit
60 h</td><td>Selbst-studium
120</td><td>Credits (ECTS)
6</td></tr>
<tr><td>2</td><td colspan="7">Lehrform(en) / SWS:
Vorlesung: 2 SWS
Projekt: 2 SWS</td></tr>
<tr><td>3</td><td colspan="7">Lernergebnisse (learning outcomes), Kompetenzen:

Kompetenz Wissen
Die Studierenden kennen den elementaren Aufbau von Data Warehouse Systemen und sind mit den zentralen Konzepten der Informationsvisualisierung vertraut [Wissen, 7]
Kompetenz Fertigkeiten
Die Studierenden sind in der Lage, die Konzepte des Data Warehousing in realen Anwendungsszenarien konzeptionell und operativ umzusetzen. Sie können Kennzahlen mittels geeigneter Methoden visualisieren. [Instrumentelle Fertigkeiten, 7]
Sozialkompetenz
Die Studierenden erarbeiten gemeinsam Lösungsansätze zu vorgegebenen Fragestellungen [Mitgestaltung, 7]</td></tr>
</table>

	Selbstständigkeit Konzeption und Aufbau von Szenarien zur Erfassung, Aufbereitung und Analyse von Kennzahlen wird in Bezug auf die jeweiligen Anforderungen kritisch diskutiert. *[Reflexivität, 7]*
4	**Inhalte*:*** Abgrenzung dispositive vs. operative Datenbestände (OLTP / OLAP) Data Warehouse Architekturen ETL-Prozesse (Datenqualität, Datenbereinigung, Transformation, etc. Logische und semantische Datenmodelle für Data Warehouses (Star-/Snowflake-Schema,…) Implementierung von Data Warehouses (MOLAP, ROLAP,..) spezielle Aspekte im Zusammenhang mit Data Warehouses (slowly changing dimensions,…) Date Warehouse Projekte (agiles Vorgehen) Aufbau eines Data Warehousing Prozesses mittels SAP BW on HANA Visualisierung von Kennzahlen Konzeption und Aufbau von Dashoards Visual Analytics (Reduktion von Darstellungsdimensionen, Visualisierung von Objekten auf Grundlage von Unähnlichkeitsmaßen…)
	Empfohlene Literaturangaben: Bauer, A, Günzel, H (Hrsg): Data Warehouse Systeme – Architekur, Entwickung, Anwendung, dpunkt verlag, 2013 Müller, R.M., Lenz, H.-J.: Business Intelligence, Springer Vieweg, 2013 Kemper, H. G., Mehanna, W., & Unger, C. : Business Intelligence– Grundlagen und praktische Anwendungen, Vieweg, Wiesbaden, 2004, ISBN:3834807192 Klein, A., Gräf, J.: Reporting und Business Intelligence, Haufe-Lexware, 2014, ISBN: 364804771X Sharda, T. Aronson, King, A.:Business Intelligence: A Managerial Approach, Pearson Verlag, 2008, ISBN: 013610066X Kohlhammer, J., Proff, D.U., Wiener, A.: Visual Business Analytics: Effektiver Zugang zu Daten und Informationen. dpunkt.verlag GmbH, 2014, ISBN: 3864900441
5	**Teilnahmevoraussetzungen:** Empfohlen: Datenbank-Grundlagen
6	**Prüfungsformen***:* Klausur 90 min., benotet Praktische Arbeit, unbenotet
7	***Voraussetzungen für die Vergabe von Kreditpunkten:*** Bestandene schriftliche Modulprüfung; erfolgreiche Bearbeitung der Aufgaben im Praktikum
8	***Verwendbarkeit des Moduls:*** Business and Security Analytics, M.Sc., Advanced IT Security M.Sc., Systems Engineering M.Eng.

9	***Modulverantwortliche(r):*** Prof. Dr. Bernd Stauß Dozenten: Prof. Dr. Bernd Stauß, N.N.
10	***Optionale Informationen:*** Studiengangsspezifische, zusätzliche Informationen zum Modul

2.1.2 53160 - Electronic System-Level Design

Studiengang: Advanced IT Security M.Sc. **Semester**: WS 2021/22
StuPO-Version: 21.2 **Letzte Bearbeitung**: 14.04.21

<table>
<tr><td colspan="7">Modul: Electronic System-Level (ESL) Design</td></tr>
<tr><td colspan="2">Kennnummer
53160</td><td>Work-load
180</td><td>Modulart
WPM</td><td>Studiensemester
1. Semester</td><td>Dauer
1 Semester</td><td>Häufigkeit
WS</td></tr>
<tr><td>1</td><td colspan="2">Lehrveranstaltung(en)
LV 53165 ESL Design 1
LV 53166 ESL Design 2</td><td>Sprache
Deutsch</td><td>Kontakt-zeit
4 SWS / 60 h</td><td>Selbst-studium
120 h</td><td>Credits (ECTS)
6</td></tr>
<tr><td>2</td><td colspan="6">Lehrform(en) / SWS:
Vorlesung + Übung ESL Design 1, Umfang 15 x 2 = 30 SWS
Vorlesung + Übung ESL Design 2, Umfang 15 x 2 = 30 SWS</td></tr>
<tr><td>3</td><td colspan="6">Lernergebnisse (learning outcomes), Kompetenzen:
Kompetenz Wissen
Kenntnis und Verständnis der Entwurfsebene ESL und deren Methoden und Werkzeuge. [Wissen, 7]
Kompetenz Fertigkeiten
Fähigkeit zur Modellierung und Simulation von Systemen unter Anwendung von ESL-Methoden. [Instrumentelle Fertigkeiten, 7]
Sozialkompetenz
Diskussion und Konsolidierung der selbständig erarbeiteten Lösungen der Übungsaufgaben. [Kommunikation, 2]
Selbstständigkeit
Transfer der Vorlesungsinhalte in die praktische Anwendung im Rahmen der Übungen. [Lernkompetenz, 4]</td></tr>
<tr><td>4</td><td colspan="6">Inhalte:
Der Entwurf mikroelektronischer Systeme ist durch einen kontinuierlichen Anstieg der Systemkomplexität einhergehend mit sich stetig verschärfenden Systemanforderungen, etwa hinsichtlich Sicherheit, Zuverlässigkeit oder Performanz, geprägt. Um dieser Entwicklung nachzukommen, wurde in den letzten Jahren eine neue höhere Abstraktionsebene des Systementwurfs mit Bezeichnung "Electronic System-Level" ("ESL") etabliert. Die Lehrveranstaltungen des Moduls "Electronic System-Level Design" liefern eine Einführung in diese neue Systemsicht und geben einen Überblick über deren Entwurfsmethoden und -werkzeuge. Anhand der eng mit der Entwicklung von ESL verwobenen C++-basierten Systembeschreibungssprache SystemC werden die wesentlichen Konzepte und Techniken des ESL Designs vorgestellt und neue Mechanismen dieser Ebene, etwa das Prinzip der transaktionsbasierten Modellierung (Transaction-Level Modeling, TLM), vermittelt (Teil Vorlesung) und im Rahmen von praktischen Übungen am Rechner vertieft (Teil Übung).</td></tr>
</table>

Version	Geändert von Ammann/am 14.04.2021	Dokument	Freigabe am/von	Gültig ab WS 2021/22
1.0		WPM-Katalog_Advanced IT Security_Version1.0_Stand 20210414_FINAL		

	ESL Design 1: - Einführung in ESL Design - Grundlagen des Systementwurfs - Die Systembeschreibungssprache SystemC ESL Design 2: - Advanced SystemC: Transaction Level Modeling - ESL Entwurfsmethoden
	Empfohlene Literaturangaben: - Kesel F.: Modellierung von digitalen Systemen mit SystemC: Von der RTL- zur Transaction-Level-Modellierung. Oldenbourg Wissenschaftsverlag. - Grötker T., Swan S., Martin G., Liao S.: System Design with SystemC. Springer-Verlag. - Accellera Systems Initiative: SystemC Download-Package (Simulator + Dokumentation). https://www.accellera.org/downloads/standards/systemc - IEEE Standard 1666-2011: Standard SystemC Language Reference Manual. https://ieeexplore.ieee.org/document/6134619
5	**Teilnahmevoraussetzungen:** Grundlagen der Programmierung und Programmentwicklung in C/C++. ESL Design 2 setzt inhaltlich auf ESL Design 1 auf, die beiden Lehrveranstaltungen finden daher innerhalb des Semesters nicht nebenläufig sondern in sequentieller Abfolge statt (ESL Design 1 in der ersten Semesterhälfte, daran anschließend ESL Design 2 in der zweiten Semesterhälfte).
6	**Prüfungsformen***:* ESL Design 1: Klausur 45 Minuten, benotet ESL Design 2: Klausur 45 Minuten, benotet
7	***Voraussetzungen für die Vergabe von Kreditpunkten:*** ESL Design 1: Bestandene Klausur (3 ECTS) ESL Design 2: Bestandene Klausur (3 ECTS)
8	***Verwendbarkeit des Moduls:*** Systems Engineering M.Eng., Advanced IT Security M.Sc., Business and Security Analytics M.Sc.
9	***Modulverantwortliche(r):*** Prof. Dr. Joachim Gerlach Dozenten: Prof. Dr. Joachim Gerlach
10	***Optionale Informationen:***

2.1.3 Xxxxx - File System Forensics

Studiengang: Advanced Internet Security M.Sc. **Semester**: WS 2021/22

StuPO-Version: 21.2 **Letzte Bearbeitung**: 16.03.21

<table>
<tr><td colspan="7">Modul: Dateisystemforensik / File System Forensics</td></tr>
<tr><td colspan="2">52600</td><td>Workload
180 h</td><td>Modulart
WPM</td><td>Studiensemester
2</td><td>Dauer
1 Semester</td><td>Häufigkeit
SoSe</td></tr>
<tr><td>1</td><td colspan="2">Lehrveranstaltung(en)
Vorlesung Dateisystemforensik
Praktikum Dateisystem-forensik</td><td>Sprache
Deutsch oder Englisch (Literaturstudium in Deutsch und Englisch erforderlich)</td><td>Kontakt-zeit
4 SWS / 60 h</td><td>Selbst-studium
120</td><td>Credits (ECTS)
6</td></tr>
<tr><td>2</td><td colspan="6">Lehrform(en) / SWS:
Vorlesung, Übungen, Seminar: 2 SWS
Praktikum: 2 SWS</td></tr>
<tr><td>3</td><td colspan="6">Lernergebnisse (learning outcomes), Kompetenzen:

Kompetenz Wissen
Die Studierenden verfügen über ein breites Wissen über die technischen Grundlagen des Aufbaus von Dateisystemen. [Wissen, 7]
Die Studierenden verfügen über ein tiefes Wissen über ausgewählte und relevante Dateisysteme. [Wissen, 7]
Kompetenz Fertigkeiten
Die Studierenden können Werkzeuge nutzen um Partitions- und Dateisysteme forensisch zu analysieren. [Instrumentelle Fertigkeiten, 7]
Die Studierenden können den Aufbau von Dateisystemen vergleichen und somit auch unbekannte Dateisysteme einordnen. [Beurteilungsfähigkeit, 7]
Sozialkompetenz
Studierende können sich auf tiefer Expertenebene mit der Fachcommunity unterhalten, Erkenntnisse und Methoden diskutieren und Ergebnisse für forensisches Zielpublikum (z.B. Juristen) darstellen. [Kommunikation, 7]
Selbstständigkeit
Studierende können selbstständig Dateisysteme analysieren, die Ergebnisse analysieren und das Ergebnis zielgruppengerecht darstellen. [Eigenständigkeit/Verantwortung, 7]</td></tr>
</table>

4	**Inhalte*:*** Vorlesung, Praktikum • Auffrischung relevanter Grundlagen der IT-Sicherheit und der digitalen Forensik • Technische Grundlagen und Sicherungsprozess • Grundlagen ausgewählter Partitionssysteme (z.B. MBR) • Grundlagen der Dateisystemforensik • Detaillierte Betrachtung ausgewählter Dateisysteme (z.B. NTFS und FAT) • Weitere aktuelle Inhalte aus dem Bereich der Dateisystemforensik
	Empfohlene Literaturangaben: Carrier, Brian (2005). File System Forensic Analysis. Boston/USA: Addison Wesley. Casey, Eoghan (2011). Digital Evidence and Computer Crime. London: Elsevier/AP. Dewald, Andreas und Felix Freiling (2015). Forensische Informatik. Norderstedt: BoD (Books on Demand). Weitere Literatur wird in der Vorlesung vorgestellt.
5	**Teilnahmevoraussetzungen:** Grundlagen IT Sicherheit und Digitaler Forensik, Programmierung in einer Skriptsprache
6	**Prüfungsformen***:* Klausur 90 min., benotet Laborarbeit, unbenotet
7	**Voraussetzungen für die Vergabe von Kreditpunkten:** Mindestens ausreichend bewertete Klausur Erfolgreiche Teilnahme am Praktikum
8	**Verwendbarkeit des Moduls:** Systems Engineering M.Eng., Advanced IT Security M.Sc., Business and Security Analytics M.Sc.
9	**Modulverantwortliche(r):** Prof. Dr. Fein Prof. Morgenstern Dozenten: Prof. Morgenstern, Prof. Dr. Fein
10	**Optionale Informationen:** Studiengangsspezifische, zusätzliche Informationen zum Modul

2.1.4 56000 - Funktionale Programmierung

Studiengang: Advanced IT Security M.Sc. **Semester**: WS 21/22
StuPO-Version: 21.2 **Letzte Bearbeitung**: 14.04.21

<table>
<tr><td colspan="7">Modul: Funktionale Programmierung</td></tr>
<tr><td colspan="2">Kennnummer
56000</td><td>Work-load
180</td><td>Modulart
WPM</td><td>Studiensemester
1</td><td>Dauer
1</td><td>Häufigkeit
WS</td></tr>
<tr><td>1</td><td colspan="2">Lehrveranstaltung(en)
Funktionale Programmierung</td><td>Sprache
Deutsch</td><td>Kontakt-zeit
4 SWS / 60 h</td><td>Selbst-studium
120</td><td>Credits (ECTS)
6</td></tr>
<tr><td>2</td><td colspan="6">Lehrform(en) / SWS:
Vorlesung mit Übung</td></tr>
<tr><td>3</td><td colspan="6">Lernergebnisse (learning outcomes), Kompetenzen:

Kompetenz Wissen
Die Studierenden kennen funktionale Programmierkonzepte, die Beziehung zu Konzepten der Kategorientheorie (Morphismen) sowie deren Umsetzungen in Haskell [Wissen, 7]
Weiter haben die Studierenden Kenntnisse der streng statischen Typisierung am Beispiel des Hindley-Millner Typsystems [Wissen, 7]

Kompetenz Fertigkeiten
Selbständiges entwickeln und schreiben funktionaler Programme unter Einsatz des gewonnenen Wissens [Instrumentelle Fertigkeiten, 7]

Sozialkompetenz
Nicht relevant

Selbstständigkeit
Studierende verstehen das Lernen als einen komplexen Prozess, der individuelle sowie auch soziale Kompetenzen umfasst; Sie verfügen über Motivation und Ausdauer, um komplexe Inhalte zu erlernen und verwenden dabei Ansätze des wissenschaftlichen Forschens [Eigenständigkeit/Verantwortung, 7]</td></tr>
<tr><td>4</td><td colspan="6">Inhalte:
- Funktionen (Extensionalität, Currying, Operatoren, Sections, Funktionskomposition)
- Datentypen (Aufzählungstypen, Summentypen, Produkttypen, rekursive Datentypen)
- Listen (Konkatenation, Homomorphismen und Katamorphismen auf Listen)
- Bäume (Homomorphismen und Katamorphismen auf Bäumen)
- Typisierung (Typsystem, Typklassen, Konstruktorklassen)
- Monaden</td></tr>
</table>

	Empfohlene Literaturangaben: http://book.realworldhaskell.org/
5	**Teilnahmevoraussetzungen:** Grundkenntnisse in Programmierkonzepten und Paradigmen (wie z.B. Iterative oder Objektorientiert Programmierung) Vorlesungen Software Entwicklung, Programmieren I und II
6	**Prüfungsformen***:* Klausur 90 Minuten
7	***Voraussetzungen für die Vergabe von Kreditpunkten:*** Bestehen der Klausur
8	***Verwendbarkeit des Moduls:*** Systems Engineering M.Eng., Advanced IT Security M.Sc., Business and Security Analytics M.Sc.
9	***Modulverantwortliche(r):*** Prof. Dr. Häberlein Dozenten: Herr Brettschneider, N.N.
10	***Optionale Informationen:*** Studiengangsspezifische, zusätzliche Informationen zum Modul

-

2.1.5 Xxxxx - Highly Optimized Hardware Cryptography

Studiengang: Advanced IT Security M.Sc. **Semester**: WS 21/22
StuPO-Version: 21.2 **Letzte Bearbeitung**: 14.04.21

Modul: Highly Optimized Hardware Cryptography						
Kennnummer z.B. 15100	**Workload** 180 h	**Modulart** WP	**Studiensemester** 1	**Dauer** 1 Semester	**Häufigkeit** WS	
1	**Lehrveranstaltung(en)** Vorlesung Highly Optimized Hardware Cryptography Projekt Highly Optimized Hardware Cryptography	**Sprache** Deutsch oder Englisch	**Kontakt-zeit** Vorlesung 2 SWS / 30h Projekt 2 SWS / 30h	**Selbst-studium** 120	**Credits (ECTS)** 6	
2	**Lehrform(en) / SWS:** Vorlesung Highly Optimized Hardware Cryptography Projekt Highly Optimized Hardware Cryptography					
3	**Lernergebnisse (learning outcomes), Kompetenzen:** *Kompetenz Wissen* Die Studierenden verstehen verschiedene Optimierungs-Strategien für die effiziente Implementierung von kryptografischen Algorithmen in Hardware. *[Wissen, 7]* *Kompetenz Fertigkeiten* Die Studierenden können kryptografische Algorithmen effizient in Hardware umsetzen und auf bestimmte Zielvorgaben hin optimieren. *[Instrumentelle Fertigkeiten, 7]* Die Studierenden können die Auswirkungen von Optimierungen auf Systeme bzgl. unterschiedlichen Kriterien, wie z.B. Gesamtsystemperformance, Kosten, oder Angriffs-Anfälligkeit beurteilen und geeignete Maßnahmen herleiten und umsetzen. *[Beurteilungsfähigkeit, 7]* *Sozialkompetenz* Die Studierenden können komplexe Themenfelder der Hardware-Kryptografie mit anderen Experten diskutieren und im Team weiterentwickeln. *[Team-/Führungsfähigkeit, 7]* *Selbstständigkeit* Die Studierenden können selbstständig und anwendungsorientiert Entscheidungen zur Optimierung komplexer Sachverhalte treffen. *[Eigenständigkeit/Verantwortung, 7]*					
4	**Inhalte*:*** Vorlesung - Einführung in die RTL-Programmierung mit VHDL - Grundlagen zur Programmierung von FPGAs und ASICs					

Version	Geändert von Ammann/am 14.04.2021	Dokument	Freigabe am/von	Gültig ab WS 2021/22
1.0		WPM-Katalog_Advanced IT Security_Version1.0_Stand 20210414_FINAL		

	- Optimierungsstrategien für hochperformante, ressourcensparende, oder energiesparende Implementierungen - Optimierungs-Strategien mit Software/Hardware Co-Design - Anwendung der Optimierungsstrategien für unterschiedliche kryptgrafische Algorithmen - Effiziente Algorithmen für Public Key Kryptografie Projektarbeit - Einführung in die FPGA-Programmierung mit VHDL - Implementierung und Optimierung eines Algorithmus auf einem FPGA - Erprobung unterschiedlicher Optimierungsstrategien
	Empfohlene Literaturangaben: Koç, C. K. - Cryptographic Engineering, Springer-Verlag, 2010 Ashenden, J. P. - The Designer's Guide to VHDL, Morgan Kaufmann, 2010
5	**Teilnahmevoraussetzungen:** Grundlagen der Kryptologie, Programmierkenntnisse (C, optional ARM Assembly oder VHDL)
6	**Prüfungsformen***:* Wissenschaftliche Ausarbeitung zur Projektarbeit, benotet Referet 20 min., Diskussion, benotet
7	***Voraussetzungen für die Vergabe von Kreditpunkten:*** Ausreichend bewertete Ausarbeitung Ausreichend bewertetes Referat
8	***Verwendbarkeit des Moduls:*** Systems Engineering M.Eng., Advanced IT Security M.Sc., Business and Security Analytics M.Sc.
9	***Modulverantwortliche(r):*** Prof. Dr. Bernhard Jungk
10	***Optionale Informationen:*** Studiengangsspezifische, zusätzliche Informationen zum Modul

2.1.6 Xxxxx - Post-Quantum Cryptography and Quantum Key Distribution

Studiengang: Advanced IT Security M.Sc. **Semester**: WS 2021/22
StuPO-Version:.21.2 **Letzte Bearbeitung**: 18.03.2021

<table>
<tr><td colspan="7">Modul: Post-Quantum Cryptography and Quantum Key Distribution</td></tr>
<tr><td colspan="2">Kennnummer
z.B. 15100</td><td>Work-load
180 h</td><td>Modulart
WP</td><td colspan="2">Studiensemester
1. Semester</td><td>Dauer
1 Semester</td><td>Häufigkeit
WS</td></tr>
<tr><td>1</td><td colspan="2">Lehrveranstaltung(en)
a. Vorlesung, Praktikum Post-Quantum Cryptography
b. Vorlesung Quantum Key Distribution</td><td>Sprache
Englisch (Literaturstudium in Deutsch und Englisch erforderlich)</td><td>Kontakt-zeit
4 SWS / 60 h</td><td>Selbst-studium
120 h</td><td>Credits (ECTS)
6</td></tr>
<tr><td>2</td><td colspan="6">Lehrform(en) / SWS:
Vorlesung, Praktikum Post-Quantum Cryptography: 3 SWS
Vorlesung Quantum Key Distribution: 1 SWS</td></tr>
<tr><td>3</td><td colspan="6">Lernergebnisse (learning outcomes), Kompetenzen:

Kompetenz Wissen
Die Studierenden können die Gefahren von Quantencomputern für etablierte kryptographische Verfahren erklären und quantensichere Verfahren aufzählen, die nicht betroffen sind. [Wissen, 7]

Die Studierenden können Funktionsweise, Voraussetzungen und Vor- und Nachteile von Quantum Key Distribution aufzählen. [Wissen, 7]

Kompetenz Fertigkeiten
Die Studierenden können quantensichere kryptographische Verfahren für eine Anwendung auswählen und implementieren. [Instrumentelle Fertigkeiten, 7]

Die Studierenden können die Eignung von Quantum Key Distribution für eine Anwendung bewerten. [Beurteilungsfähigkeit, 7]

Sozialkompetenz
Die Studierenden können sich auf Expertenebene mit der Fachcommunity über Post-Quatum Cryptography und Quantum Key Distribution unterhalten, Erkenntnisse und Methoden diskutieren und ihr Expertenwissen auch Fachabteilungen vermitteln [Kommunikation, 7]

Die Studierenden können mögliche gesellschaftliche Auswirkungen von aktuellen und neuen Entwicklungen im Quantencomputing für die IT-Sicherheit erkennen, bewerten und mit Laien- und Fachpublikum diskutieren. [Kommunikation, 7]</td></tr>
</table>

Version	Geändert von Ammann/am 14.04.2021	Dokument	Freigabe am/von	Gültig ab WS 2021/22
1.0		WPM-Katalog_Advanced IT Security_Version1.0_Stand 20210414_FINAL		

	Selbstständigkeit Die Studierenden können neue Anwendungen für Post-Quatum Cryptography und Quantum Key Distribution selbstständig identifizieren und erforschen sowie mit der Fachcommunity diskutieren. /Kompetenzausprägung wählen /Niveaustufe wählen Die Studierenden können neue Aufgabenstellungen und Probleme aus den Bereichen Post-Quatum Cryptography und Quantum Key Distribution selbstständig anhand der aktuellen Forschungsergebnisse erarbeiten. /Kompetenzausprägung wählen /Niveaustufe wählen
4	**Inhalte*:*** Vorlesung, Praktikum Post-Quantum Cryptography: • Auffrischung relevanter Grundlagen der Kryptologie, IT Sicherheit und Mathematik • Einführung in Quantum Computing • Gefahren durch Quantencomputer für etablierte Verschlüsselungsverfahren • Prinzipien für Post-Quantum Cryptography • Implementierung konkreter Post-Quatum-Verschlüsselungsverfahren Vorlesung Quantum Key Distribution: • Auffrischung relevanter Grundlagen der Kryptologie und IT Sicherheit • Grundlagen der Quantenmechanik • Quantum Key Distribution • Angriffsszenarien *Empfohlene Literaturangaben:* Empfohlene Literaturangaben
5	**Teilnahmevoraussetzungen:** Grundlagen der Kryptologie (insbesondere Public Key Cryptography), IT-Sicherheit, Programmierkenntnisse
6	**Prüfungsformen***:* Wissenschaftliche Ausarbeitung inkl. Kurzpräsentation, benotet Referat 20 min., Diskussion, benotet
7	**Voraussetzungen für die Vergabe von Kreditpunkten:** Ausreichend bewertete Ausarbeitung Ausreichend bewertetes Referat
8	**Verwendbarkeit des Moduls:** Systems Engineering M.Eng., Advanced IT Security M.Sc., Business and Security Analytics M.Sc.
9	**Modulverantwortliche(r):** Prof. Dr. Henrich.
10	**Optionale Informationen:** Studiengangsspezifische, zusätzliche Informationen zum Modul

2.1.7 51400 – Semantic Web

Studiengang: Advanced IT Security M.Sc. **Semester**: WS 2021/22
StuPO-Version: 21.2 **Letzte Bearbeitung**: 14.04.211

<table>
<tr><td colspan="8">Modul: Semantic Web</td></tr>
<tr><td colspan="2">Kennnummer
51400</td><td>Workload
180</td><td>Modulart
WP</td><td colspan="2">Studiensemester
1</td><td>Dauer
1</td><td>Häufigkeit
WS</td></tr>
<tr><td>1</td><td colspan="3">Lehrveranstaltung(en)
a. 51405 Semantic Web
b. 51420 Proj. Semantic Web</td><td>Sprache
a.,b., deutsch oder englisch</td><td>Kontakt-zeit
a. 30
b. 30</td><td>Selbst-studium
120</td><td>Credits (ECTS)
6</td></tr>
<tr><td>2</td><td colspan="7">Lehrform(en) / SWS:
a. Vorlesung, b. Projektarbeit</td></tr>
<tr><td>3</td><td colspan="7">Lernergebnisse (learning outcomes), Kompetenzen:

Kompetenz Wissen
Vertieftes verstehen Formaler Logiken und Reasoning-Aufgaben [Wissen, 7]
Vertieftes Verstehen von Semantic Web -Technologien als Instrument für interoperable Wissensbeschreibung [Wissen, 7]
Kompetenz Fertigkeiten
Können Ontologien mit Hilfe von Tools wie Editoren und Reasoner entwickeln und Anwenden [Instrumentelle Fertigkeiten, 6]
Können Wissensstrukturen von Komplexen Wissensdomains analysieren und formal beschreiben [Systemische Fertigkeiten, 7]
Sozialkompetenz
Sind in der Lage komplexe Formalismen zu kommunizieren und Diskussion auf Grundlage der Formalismen und mit Anwendung des formallogischen Vokabular zu führen [Kommunikation, 7]
Selbstständigkeit
Sind in der Lage komplexe Fragestellungen selbständig zu Bearbeiten und eigenen Fortschritt adäquat zu bemessen
[Lernkompetenz, 7]</td></tr>
<tr><td>4</td><td colspan="7">Inhalte:
Die Grundlagen:
- Definition und Begriffsklärung
- Security Analytics Use Cases
- Data Sourcess und Methoden der Datensammlung
- Real time Data Harvesting
- Anwendung der Security Analytics Ergebnissen und ihr Impact
- Basic Security Analytics Costs</td></tr>
</table>

	- Advanced persistent threats - Security Analytics und Digitale Forensics Security Analytics Tools and Services, u.a.: - Blue Coat Security Analytics Platform, - Lancope Stealth Watch System - JuniperNetworks JSA Series Secure Analytics - EMC RSASecurity Analytics NetWitness - FireEye Threat Analytics Platform - Arbor Networks Security Analytics - Click Security Click Commander - Hexis Cyber Solutions' NeatBeat MON - Sumo Logics' cloud service. - Security Onion - Splunk - Elastic Stack
	Empfohlene Literaturangaben: Lehto, Martti, and Pekka Neittaanmäki, eds. Cyber security: Analytics, technology and automation. Vol. 78. Springer, 2015. Talabis, Mark, et al. Information Security Analytics: Finding Security Insights, Patterns, and Anomalies in Big Data. Syngress, 2014. THOMAS, TONY P. VIJAYARAGHAVAN, Athira P. Vijayaraghavan, and Sabu Emmanuel. MACHINE LEARNING APPROACHES IN CYBER SECURITY ANALYTICS. SPRINGER VERLAG, SINGAPOR, 2020.
5	**Teilnahmevoraussetzungen:** Kenntnisse in IT Security (DQR 6), Praktische Fertigkeiten in Netzwerken und Programmierung (DQR 6)
6	**Prüfungsformen***:* Klausur 90 Min. (Modulprüfung)
7	***Voraussetzungen für die Vergabe von Kreditpunkten:*** Bestandene Klausur
8	***Verwendbarkeit des Moduls:*** Systems Engineering M.Eng., Advanced IT Security M.Sc., Business and Security Analytics M.Sc.
9	***Modulverantwortliche(r):*** Prof. Dr. German Nemirovski
10	***Optionale Informationen:*** Studiengangsspezifische, zusätzliche Informationen zum Modul

2.2 Sommersemester

2.2.1 52600 – Advanced Network and Internet Security

Studiengang: Advanced IT Security M.Sc. **Semester**: WS 2021/22
StuPO-Version: 21.2 **Letzte Bearbeitung**: 14.04.21

Modul: Advanced Network and Internet Security (ANIS)					
Kennnummer 52600	**Workload** 180 h	**Modulart** WPM	**Studiensemester** 2	**Dauer** 1 Semester	**Häufigkeit** WS und SS

1	**Lehrveranstaltung(en)** Vorlesung, Seminar, Projekt	**Sprache** Englisch	**Kontakt-zeit** 4 SWS / 60 h	**Selbst-studium** 120	**Credits (ECTS)** 6

2	**Lehrform(en) / SWS:** Vorlesung: 1 SWS Seminar: 1,5 SWS Projekt: 1,5 SWS
3	**Lernergebnisse (learning outcomes), Kompetenzen:** *Kompetenz Wissen* Die Studierenden kennen den aktuellen Forschungsstand ausgewählter Forschungsbereiche in der Netzwerksicherheit *[Wissen, 7]* *Kompetenz Fertigkeiten* Die Studierenden können Forschungsfragestellungen der Netzwerksicherheit mit geeigneten Mechanismen und Methoden in Verbindung setzen und diese zur Bearbeitung der Fragestellung anwenden [Instrumentelle Fertigkeiten, 7] Die Studierenden können eine Forschungsfragestellung bearbeiten und die erzielten Ergebnisse adäquat [Systemische Fertigkeiten, 7] *Sozialkompetenz* Die Studierenden sind in der Lage die Ergebnisse ihrer Tätigkeit im Bereich Network Security auf einem Master-Niveau einem fachkundigen Experten zu erläutern. *[Kommunikation, 7]* *Selbstständigkeit* Die Studierenden können im Rahmen einer eigenständigen Arbeit neue Systeme im Bereich Netzwerksicherheit entwickeln und bestehende Systeme bewerten erweitern und analysieren [Eigenständigkeit/Verantwortung, *7]*
4	**Inhalte*:*** Die Vorlesung gliedert sich in drei Teile auf, die z.T. zeitlich überlappend durchgeführt werden: - Wiederholung und Vertiefung der Grundlagen und fortgeschrittenen Aspekte der Netzwerksicherheit. Dieser Teil wird im Rahmen einer Vorlesung absolviert und dient

	dazu, Informatik-Studierenden ohne spezifischen IT Security-Hintergrund die Grundlagen für die Bearbeitung des Referats und des Projekts zu vermitteln. - Ausarbeitung eines Referats über ein aktuelles Thema der Netzwerksicherheit (basierend auf aktuellen Konferenz- oder Journal Veröffentlichungen aus dem Bereich der Netzwerksicherheit). Dieser Teil dient dazu, an einem konkreten Beispiel den Aufbau einer wissenschaftlichen Arbeit zu erarbeiten und diese zu bewerten. Die Referate werden im Peer-Review Prozess von jeweils zwei Kommilitonen korrigiert und ähnlich zu einem Konferenzformat gehalten (1-tägige Blockveranstaltung). - Bearbeitung eines eigenen Projekts zu einer ausgewählten Forschungsfragestellung aus dem Bereich der Netzwerk- und Internetsicherheit. Dabei werden sowohl Ingenieursmethoden als auch analytische Methoden verwendet um die Fragestellung zu beantworten. Die Projektbearbeitung schließt mit einem Vortrag über die Ergebnisse ab (erneut im Konferenz-Format als Blockveranstaltung). Hier sollen selbständig wissenschaftliche Fragestellungen bearbeitet werden. Beispiele für die zu behandelnden Themen • Sicherheit moderner Kommunikationsprotokolle (HTTP/2, QUIC, P2P Protokolle, etc.) • Aktuelle Angriffe gegen Kommunikationsprotokolle • Protokolle zur Erreichung spezifischer Sicherheitsziele (Vertraulichkeit, Integrität, Verfügbarkeit, Anonymität, Pseudonymität) • Authentifikations- und Authorisierungsprotokolle • Sicherheit im industriellen Umfeld (Fertigung, Steuerung) • Analyse von Kommunikationsdaten zur Erkennung von Sicherheitsproblemen • Analyse verschlüsselter Verbindungen zur Klassifikation von Verkehr • Analyse von Log- Einträgen und anderweitig erfassten Ereignissen zur Erkennung und Klassifikation von Angriffen
	Empfohlene Literaturangaben: R. Anderson, Security Engineering, Wiley, 2009G. Schäfer, M. Roßberg, Netzssicherheit, dpunkt.verlag, 2014 Ausgewählte Literatur bekannter Top-Tier Konferenzen im Bereich Sicherheit und Netzwerksicherheit z.B. ACM CCS, Usenix Security, Defcon, Balckhat, etc.
5	**Teilnahmevoraussetzungen:** Bestandenes Referat
6	**Prüfungsformen***:* Referat 20 min. mit Ausarbeitung, benotet Laborarbeit, unbenotet
7	***Voraussetzungen für die Vergabe von Kreditpunkten:*** Bestandenes Referat und bestandene Laborarbeit
8	***Verwendbarkeit des Moduls:*** Systems Engineering M.Eng., Advanced IT Security M.Sc., Business and Security Analytics M.Sc.
9	***Modulverantwortliche(r):*** Prof. Dr. German Nemirovski Dozenten: Prof. Dr. German Nemirovski

10	***Optionale Informationen:*** Studiengangsspezifische, zusätzliche Informationen zum Modul

2.2.2 Xxxxx - Advanced Programming

Studiengang: Advanced IT Security M.Sc. **Semester**: WS 2021/22
StuPO-Version: 21.2 **Letzte Bearbeitung**: 14.04.21

<table>
<tr><td colspan="7">Modul: Advanced Programming</td></tr>
<tr><td colspan="2"></td><td>Workload
90 h</td><td>Modulart
Projekt</td><td>Studiensemester
1</td><td>Dauer
1 Semester</td><td>Häufigkeit
SS</td></tr>
<tr><td>1</td><td colspan="2">Lehrveranstaltung(en)
Advanced Programming</td><td>Sprache
Deutsch</td><td>Kontakt-zeit
2 SWS/
30 h</td><td>Selbst-studium
60 h</td><td>Credits (ECTS)
3</td></tr>
<tr><td>2</td><td colspan="6">Lehrform(en) / SWS:
Vorlesung, Umfang 15x2 = 30 SWS</td></tr>
<tr><td>3</td><td colspan="6">Lernergebnisse (learning outcomes), Kompetenzen:

Kompetenz Wissen
Kenntnis von Komponenten eingebetteter Systeme und Wissen über Zusammenstellung zu einem Gesamtsystem. [Wissen, 7]
Kompetenz Fertigkeiten
Erstellung eines Designs mit Auswahl von Komponenten für eingebettete Systeme. [Instrumentelle Fertigkeiten, 2]
Sozialkompetenz
Fragen während Lehrveranstaltung und Klausurvorbereitung. Präsentation der Praktikumsergebnisse vor Publikum. [Kommunikation, 3]
Selbstständigkeit
Selbständiges Erlernen der Komponenten und Designmethoden. [Lernkompetenz, 4]</td></tr>
<tr><td>4</td><td colspan="6">Inhalte:
Planung eines über das Netzwerk verteilten Systems.
Anwendungsprogrammierung mit Authentifizierung.
Sichere Netzwerkkommunikation über Middleware.
Einsatz einer Datenbank zur Sicherung von Daten.
Integration der Systemkomponenten.
Image-Container Programmierung.

Empfohlene Literaturangaben</td></tr>
<tr><td>5</td><td colspan="6">Teilnahmevoraussetzungen:
Der Studierende muss die Programmiersprache Python oder Java beherrschen (Modul Programmieren I u. II).</td></tr>
</table>

Version	Geändert von Ammann/am 14.04.2021	Dokument	Freigabe am/von	Gültig ab WS 2021/22
1.0		WPM-Katalog_Advanced IT Security_Version1.0_Stand 20210414_FINAL		

6	**Prüfungsformen***:* Laborarbeit, benotet
7	***Voraussetzungen für die Vergabe von Kreditpunkten:*** Der Studierende soll in der Lage sein, ein Authentifizierungsfenster mit GUI programmieren. Der Studierende soll aus einer Reihe von zur Verfügung stehenden Middleware's (MQTT, DDS etc.) ein passendes finden und daraus eine verteiltes System programmieren. Der Studierende soll Daten über das Netzwerk sicher zugreifen und verarbeiten. Der Studierende soll alle programmierten Teilkomponenten zu einer kompletten Lösung integrieren. Der Studierende soll Teilkomponenten seiner Lösung mit Hilfe von Container-Techniken verpacken, um die Installation und Wartbarkeit zu vereinfachen.
8	***Verwendbarkeit des Moduls:*** Systems Engineering M.Eng., Advanced IT Security M.Sc., Business and Security Analytics M.Sc.
9	***Modulverantwortliche(r):*** Prof. Dr. Derk Rembold Dozenten: Prof. Dr. Rembold
10	***Optionale Informationen:*** keine

2.2.3 Xxxxx - Blockchain Technology and Crypto Currencies

Studiengang: Advanced IT Security M.Sc. **Semester**: WS 2021/22
StuPO-Version: 21.2 **Letzte Bearbeitung**: 18.03.2021

<table>
<tr><td colspan="7">Modul: Blockchain Technology and Crypto Currencies</td></tr>
<tr><td colspan="2">Kennnummer
z.B. 15100</td><td>Work-load
180 h</td><td>Modulart
WP</td><td colspan="2">Studiensemester
1. Semester</td><td>Dauer
1 Semester</td><td>Häufigkeit
WS</td></tr>
<tr><td>1</td><td colspan="2">Lehrveranstaltung(en)
a. Vorlesung Blockchain Technology
b. Vorlesung Crypto Currencies</td><td colspan="2">Sprache
Englisch (Literatur-studium in Deutsch und Englisch erforderlich)</td><td>Kontakt-zeit
a. 2 SWS / 30 h
b. 2 SWS / 30 h</td><td>Selbst-studium
120 h</td><td>Credits (ECTS)
6</td></tr>
<tr><td>2</td><td colspan="7">Lehrform(en) / SWS:
Vorlesung, Übung Blockchain Technology: 2SWS
Vorlesung, Seminar Crypto Currencies: 2 SWS</td></tr>
<tr><td>3</td><td colspan="7">Lernergebnisse (learning outcomes), Kompetenzen:

Kompetenz Wissen
Die Studierenden können die grundlegenden Prinzipien einer Blockchain erklären und verschiedene Anwendungsgebiete aufzählen. [Wissen, 7]

Die Studierenden können verschiedene Crypto Currencies aufzählen und deren Eigenschaften und Unterschiede erläutern. [Wissen, 7]

Kompetenz Fertigkeiten
Die Studierenden können die Eignung von Blockchain Technology für ein neues Anwendungsgebiet bewerten und eine geeignete Blockchain Technology auswählen. [Beurteilungsfähigkeit, 7]

Die Studierenden können eine Blockchain Technology unter Berücksichtigung der anwendungsspezifischen Anforderungen implementieren. [Instrumentelle Fertigkeiten, 7]

Sozialkompetenz
Die Studierenden können sich auf Expertenebene mit der Fachcommunity über Blockchain Technology und Crypto Currencies unterhalten, Erkenntnisse und Methoden diskutieren und ihr Expertenwissen auch Fachabteilungen vermitteln [Kommunikation, 7]

Die Studierenden können mögliche gesellschaftliche Auswirkungen von aktuellen und neuen Entwicklungen in den Bereichen Blockchain Technology und Crypto Currencies</td></tr>
</table>

	erkennen, bewerten und mit Laien- und Fachpublikum diskutieren. [Kommunikation, 7]
	Selbstständigkeit Die Studierenden können neue Anwendungen für Blockchain Technology und Crypto Currencies selbstständig identifizieren und erforschen sowie mit der Fachcommunity diskutieren. [Eigenständigkeit/Verantwortung, 7] Die Studierenden können neue Aufgabenstellungen und Probleme aus den Bereichen Blockchain Technology und Crypto Currencies selbstständig anhand der aktuellen Forschungsergebnisse erarbeiten. [Eigenständigkeit/Verantwortung, 7]
4	**Inhalte*:*** Vorlesung, Übung Blockchain Technology: • Auffrischung relevanter Grundlagen der Kryptologie und IT Sicherheit • Datenstrukturen von Blockchains • Mechanismen zur Konsensfindung (Proof of Work, Proof of Stake) • Angriffsszenarien • Beispielanwendungen (Bitcoin, Smart Contracts) Vorlesung, Seminar Crypto Currencies: • Auffrischung relevanter Grundlagen der Kryptologie und IT Sicherheit • praktische und rechtliche Rahmenbedingungen • Konkrete Crypto Currencies (Bitcoin, Ethereum)
	Empfohlene Literaturangaben: Empfohlene Literaturangaben
5	**Teilnahmevoraussetzungen:** Grundlagen der IT-Sicherheit, Programmierkenntnisse
6	**Prüfungsformen***:* Wissenschaftliche Ausarbeitung inkl. Kurzpräsentation, benotet Referat 20 min., Diskussion, benotet
7	**Voraussetzungen für die Vergabe von Kreditpunkten:** Ausreichend bewertete Ausarbeitung Ausreichend bewertetes Referat
8	**Verwendbarkeit des Moduls:** Systems Engineering M.Eng., Advanced IT Security M.Sc., Business and Security Analytics M.Sc.
9	**Modulverantwortliche(r):** Prof. Dr. Henrich Dozenten: Prof. Dr. Henrich
10	**Optionale Informationen:** Studiengangsspezifische, zusätzliche Informationen zum Modul

2.2.4 52300 - Distributed Enterprise Applications

Studiengang: Advanced IT Security M.Sc. **Semester**: WS 2021/22
StuPO-Version: 21.2 **Letzte Bearbeitung**: 14.04.21

<table>
<tr><td colspan="7">Modul: Distributed Enterprise Applications</td></tr>
<tr><td colspan="2">Kennnummer
51300</td><td>Workload
180 h</td><td>Modulart
WPM</td><td colspan="2">Studiensemester
2</td><td>Dauer
1 Semester</td><td>Häufigkeit
WS und SS</td></tr>
<tr><td>1</td><td colspan="3">Lehrveranstaltung(en)
Vorlesung Distributed Enterprise Applications
Projekt Distributed Enterprise Applications</td><td>Sprache
Deutsch, bei Bedarf Englisch (muss vor Semester-beginn geäußert werden)</td><td>Kontakt-zeit
4 SWS / 60 h</td><td>Selbst-studium
120</td><td>Credits (ECTS)
6</td></tr>
<tr><td>2</td><td colspan="7">Lehrform(en) / SWS:
Vorlesung: 2 SWS
Übungen: 2 SWS</td></tr>
<tr><td>3</td><td colspan="7">Lernergebnisse (learning outcomes), Kompetenzen:

Kompetenz Wissen
Die Studierenden kennen
die Bedeutung und Notwendigkeit der Betrachtung und Entwicklung von Software-Architekturen für komplexe und vor allem verteilter Software-Produkte,
Architekturmuster zur Implementierung verteilter Anwendungen,
Techniken zur Implementierung komponentenbasierter Software-Entwicklung auf Basis von Applikationsservern
[Wissen, 7]

Kompetenz Fertigkeiten
Die Studierenden sind in der Lage
Komponenten im Sinne einer Applikationsserver-orientierten Architektur zu entwerfen und zu implementieren,
verteilte Transaktionsarchitekturen zu entwerfen und zu implementieren,
verschiedene Frontend- und Backend-Architekturen zu entwickeln und zu implementieren [Instrumentelle Fertigkeiten, 7]

Sozialkompetenz
Nicht relevant
/Kompetenzausprägung wählen /Niveaustufe wählen</td></tr>
</table>

Version	Geändert von Ammann/am 14.04.2021	Dokument	Freigabe am/von	Gültig ab WS 2021/22
1.0		WPM-Katalog_Advanced IT Security_Version1.0_Stand 20210414_FINAL		

	Selbstständigkeit Die Studierenden sind fähig selbständig komplexere Aufgabenstellungen im Sinne einer komponentenorientierten Software-Architektur zu modellieren und umzusetzen *[Eigenständigkeit/Verantwortung, 7]*
4	**Inhalte*:*** Aufbau eines komponentenorientierten, TP-Monitor-basierten Applikationsservers Implementierung komplexer (Datenbank-) Anwendungen auf Basis der Java Persistence Architektur
	Empfohlene Literaturangaben: https://www.tutorialspoint.com/software_architecture_design/component_based_architecture.htm Syperski, C.: Component Software: Beyond Object-Oriented Programming (Addison-Wesley Component Software), 2011 Andresen, A.: Komponentenbasierte Softwareentwicklung mit MDA, UML 2 und XML. Hanser, 2. Auflage, 2004,ISBN-13: 978-3446229150 Eilebrecht, K., Starke, G.: Patterns kompakt: Entwurfsmuster für effektive Software-Entwicklung. Spektrum Akademischer Verlag, 3. Auflage, 2010, ISBN-13: 978-3827425256 Erl, T.: SOA: Design Patterns. Prentice Hall International, 2008, ISBN-13: 978-0136135166Erl, T.: SOA: Entwurfsprinzipien für service-orientierte Architektur. Addison-Wesley, 2008, ISBN-13: 978-3827326515 Fowler, M. et al.: Patterns of Enterprise Application Architecture. mitp, 2003, ISBN-13: 978-3826613784 Gamma et al.: Entwurfsmuster: Elemente wiederverwendbarer objektorientierter Software. Addison-Wesley, Neuauflage, 2010, ISBN-13: 978-3827330437 Gharbi, M.: Basiswissen für Softwarearchitekten: Aus- und Weiterbildung nach iSAQB-Standard zum Certified Professional for Software Architecture - Foundation Level. dpunkt.verlag, 1. Auflage, 2012, ISBN-13: 978-3898647915 Wieken, J.-H.: SQL -Einstieg für Fortgeschrittene, Addison Wesley, 2008 Kroenke, D.M.; Auer, D.: Database Processing, Prentice Hall, 2010 Wehr, H., Müller, B.: Java Persistence API mit Hibernate, Addison Wesley, 2007Bauer, Chr.; King, G.: Hibernate in Action. Manning Pub., 2004 http://jbossts.blogspot.de/2014/01/narayana-transaction-analyser-100alpha1.htmlhttp://www.redhat.com/products/jbossenterprisemiddleware/data-grid/
5	**Teilnahmevoraussetzungen:** Teilnahmevoraussetzungen: Zulassung zumeinem Master-Studiengang an der HS Albstadt Sigmaringen
6	**Prüfungsformen***:* Mündliche Prüfung 20 min., benotet Praktische Arbeit, unbenotet
7	***Voraussetzungen für die Vergabe von Kreditpunkten:*** Erfolgreiche Teilnahme an der mündlichen Prüfung
8	***Verwendbarkeit des Moduls:*** Systems Engineering M.Eng., Advanced IT Security M.Sc., Business and Security Analytics M.Sc.

9	***Modulverantwortliche(r):*** Prof. Dr. J. Röhrle Dozenten: Prof. Dr. J. Röhrle
10	***Optionale Informationen:*** Studiengangsspezifische, zusätzliche Informationen zum Modul

2.2.5 53150 - Electronic Design Automation

Studiengang: Advanced IT Security M.Sc. **Semester**: WS 2021/22
StuPO-Version: 21.2 **Letzte Bearbeitung**: 09.03.2021

<table>
<tr><td colspan="7">Modul: Electronic Design Automation (EDA)</td></tr>
<tr><td colspan="2">Kennnummer
53150</td><td>Work-load
180</td><td>Modulart
WPM</td><td>Studiensemester
2. Semester</td><td>Dauer
1 Semester</td><td>Häufigkeit
SS</td></tr>
<tr><td>1</td><td colspan="2">Lehrveranstaltung(en)
LV 53155 EDA - Entwurf & Optimierung
LV 53156 EDA - Verifikation & Test</td><td>Sprache
Deutsch</td><td>Kontakt-zeit
4 SWS / 60 h</td><td>Selbst-studium
120 h</td><td>Credits (ECTS)
6</td></tr>
<tr><td>2</td><td colspan="6">Lehrform(en) / SWS:
Vorlesung + Übung EDA - Entwurf & Optimierung, Umfang 15 x 2 = 30 SWS
Vorlesung + Übung EDA - Verifikation & Test, Umfang 15 x 2 = 30 SWS</td></tr>
<tr><td>3</td><td colspan="6">Lernergebnisse (learning outcomes), Kompetenzen:
Kompetenz Wissen
Kenntnis und Verständnis der theoretischen Grundlagen, Wirkungsweise und Anwendung von EDA-Werkzeugen im Systementwurf. [Wissen, 7]
Kompetenz Fertigkeiten
Fähigkeit zur Anwendung von EDA-Werkzeugen im Systementwurfsprozess. [Instrumentelle Fertigkeiten, 7]
Sozialkompetenz
Diskussion und Konsolidierung der selbständig erarbeiteten Lösungen der Übungsaufgaben. [Kommunikation, 2]
Selbstständigkeit
Transfer der Vorlesungsinhalte in die praktische Anwendung im Rahmen der Übungen. [Lernkompetenz, 4]</td></tr>
<tr><td>4</td><td colspan="6">Inhalte:
Die Entwicklung hochkomplexer Mikrochips ist nur mit Unterstützung leistungsfähiger Software-Werkzeuge zu bewerkstelligen, die eine teilweise oder vollständige Automatisierung von Entwurfs- und Validierungsschritten ermöglichen. Derartige Verfahren und Werkzeuge werden unter dem Begriff "EDA" ("Electronic Design Automation") zusammengefasst.
Die Lehrveranstaltungen des Moduls "Electronic Design Automation" liefern einen Überblick über die heutige EDA-Landschaft und geben einerseits Einblicke in das algorithmische Vorgehen von EDA-Verfahren (Wie funktionieren EDA-Werkzeuge unter der Haube? Was sind sie in der Lage zu leisten …und was nicht? – Teil Vorlesung) und andererseits in deren praktische Anwendung (eigenes Arbeiten mit State-of-the-Art EDA-Werkzeugen am Rechner – Teil Übung).
Das Modul umfasst zwei Lehrveranstaltungen, die sich einerseits mit dem strukturierten Entwurf mikroelektronischer Systemlösungen (Teil "Entwurf &</td></tr>
</table>

	Optimierung") und andererseits mit der systematischen Validierung und Absicherung des Systemverhaltens (Teil "Verifikation & Test") beschäftigen.
	
	EDA - Entwurf & Optimierung:
	- Einführung in EDA
	- EDA im Entwurfsprozess
	- Automatisierung von Entwurfsschritten
	  - Algorithmen-Synthese
	  - Register-Transfer-Synthese
	  - Logik-Optimierung
	  - Technologie-Abbildung
	
	EDA - Verifikation & Test:
	- Einführung in EDA
	- EDA im Entwurfsprozess
	- Validierung von funktionalem Verhalten
	  - Simulation
	  - Formale Verifikation
	  - Property Checking

	Empfohlene Literaturangaben: - Jansen D.: Handbuch der Electronic Design Automation. Fachbuchverlag Leipzig. - Bringmann O., Lange W., Bogdan M.: Eingebettete Systeme: Entwurf, Modellierung und Synthese. De Gruyter Studium. - Barke E.: Entwurfsautomatisierung in der Mikroelektronik (Online-Skript). http://edascript.ims.uni-hannover.de - Teich J., Haubelt C. Digitale Hardware/Software-Systeme: Synthese und Optimierung. Springer-Verlag. - Haubelt C., Teich J.: Digitale Hardware/Software-Systeme: Spezifikation und Verifikation. Springer-Verlag.
5	**Teilnahmevoraussetzungen:** Grundlagen der digitalen Schaltungstechnik und der Funktionsweise digitaler Rechnersysteme. Die beiden Lehrveranstaltungen ergänzen sich sinnvoll, bauen inhaltlich aber nicht aufeinander auf und können somit einzeln oder kombiniert bzw. in beliebiger Reihenfolge besucht werden.
6	**Prüfungsformen***:* EDA - Entwurf & Optimierung: Klausur 45 Minuten, benotet EDA - Verifikation & Test: Klausur 45 Minuten, benotet
7	***Voraussetzungen für die Vergabe von Kreditpunkten:*** EDA - Entwurf & Optimierung: Bestandene Klausur (3 ECTS) EDA - Verifikation & Test: Bestandene Klausur (3 ECTS)
8	***Verwendbarkeit des Moduls:*** Systems Engineering M.Eng., Advanced IT Security M.Sc., Business and Security Analytics M.Sc.

9	***Modulverantwortliche(r):*** Prof. Dr. Joachim Gerlach Dozent: Prof. Dr. Joachim Gerlach
10	***Optionale Informationen:***

2.2.6 52400 – Financial Risks and Financial Management

Studiengang: Advanced IT Security M.Sc. **Semester**: WS 2021/22
StuPO-Version: 21.2 **Letzte Bearbeitung**: 14.04.211

<table>
<tr><td colspan="8">Modul: Financial Risks & Financial Management</td></tr>
<tr><td colspan="2">Kennnummer
52400</td><td>Workload
180 h</td><td>Modulart
WPM</td><td colspan="2">Studiensemester
2</td><td>Dauer
1 Semester</td><td>Häufigkeit
WS und SS</td></tr>
<tr><td>1</td><td colspan="2">Lehrveranstaltung(en)
Vorlesung; Übungen & Fallstudien Financial Risks & Financial Management</td><td colspan="2">Sprache
Deutsch und Englisch (deutsches und englisches Literatur-studium erforderlich)</td><td>Kontakt-zeit
4 SWS / 60 h</td><td>Selbst-studium
120</td><td>Credits (ECTS)
6</td></tr>
<tr><td>2</td><td colspan="7">Lehrform(en) / SWS:
Vorlesung: 2 SWS
Übungen / Fallstudien: 2 SWS</td></tr>
<tr><td>3</td><td colspan="7">Lernergebnisse (learning outcomes), Kompetenzen:

Kompetenz Wissen
Die Studierenden:
• sind mit zentralen Aspekten des Kapitalstrukturmanagements und der Ableitung der relevanten Kapitalkosten vertraut
• kennen die Portfoliotheorie und das CAPM und deren Anwendungsgebiete im Risikomanagement und der Kapitalkostenableitung
• kennen die wesentlichen Verfahren der Unternehmens- sowie der Anleihebewertung
• sind mit den zentralen finanzwirtschaftlichen Risiken vertraut und kennen die gängigen Verfahren des Risikomanagements
• kennen in Grundzügen das Wesen von Derivaten und deren Anwendungs-möglichkeiten im Management von finanzwirtschaftlichen Risiken [Wissen, 7]
Lernergebnisbeschreibung einer bestimmten Kompetenz z.B. Fachwissen mit Niveaustufe /Niveaustufe wählen
Kompetenz Fertigkeiten
Die Studierenden:
• können marktgestützt Kapitalkosten von Unternehmen ableiten
• können die gängige Verfahren zur Unternehmensbewertung anwenden und selbständig Unternehmenswerte ableiten
• können Anleihen bewerten
• können die unterschiedlichen finanzwirtschaftlichen Risiken identifizieren und voneinander abgrenzen
• können gängige Verfahren zum Management finanzwirtschaftlicher Risiken</td></tr>
</table>

	(Value at Risk, Hedging mittels Derivaten, etc.) anwenden • *[Instrumentelle Fertigkeiten, 7]*
	Sozialkompetenz Die Studierenden können Fallstudien im Team bearbeiten und sind in der Lage die Teams selbst zu organisieren; beherrschen Methoden der Präsentation und Dokumentation und können diese zielgruppenorientiert einsetzen *[Team-/Führungsfähigkeit, 7]* Die Studierenden beherrschen Methoden der Präsentation und Dokumentation und können diese zielgruppenorientiert einsetzen *[Kommunikation, 7]*
	Selbstständigkeit Die Studierenden können im Rahmen von Fallstudien Problemstellungen des Finanz- und Risikomanagements selbständig erkennen, nach Lösungen recherchieren, auf das Wesentliche abstrahieren und in einem gestalteten Prozess Aufgaben bezogen lösen *[Eigenständigkeit/Verantwortung, 7]* Durch die fortlaufende Vertiefung des Stoffes durch die selbständige Bearbeitung von Übungsaufgaben und Fallstduien, sind die Studierenden in der Lage, sich ein realistisches Bild ihrer eigenen Kompetenzentwicklung zu machen und entsprechend darauf zu reagieren. *[Lernkompetenz, 7]*
4	**Inhalte*:*** Grundlagen des Finanzmanagements, Finanzanalyse, Value Management und Unternehmenswert, Fremdkapitalmanagement, Finanzielle Risiken und Risikomanagement.
	Empfohlene Literaturangaben: Becker, H. P.: Investition und Finanzierung –Grundlagen der betrieblichen Finanzwirtschaft, 7. Auflage, Springer Verlag, 2015, Brealey, R. A./ Myers, St. C., 2003, Principles of Corporate Finance, 7th. Ed., New York et. al. (Mc Graw Hill International Ed.), Elton, E., Gruber, M., Brown, S. und Goetzmann,W., 2002, Modern Portfolio Theory and Investment Analysis, 6. Aufl., John Wiley and SonsKruschwitz, L.;Husmann, S.: Finanzierung und Investition, 6. Auflage, Oldenbourg Verlag, 2009Hull, J.C.: Options, Futures, and Other Derivatives, 9th Edition, Pearson, 2015Higgins, R.: Analysis for Financial Management, 10thEdition, McGraw-Hill/Irwin, 2011Perridon, L.; Steiner, M.;Rathgeber, A.: Finanzwirtschaft der Unternehmung, 15. Auflage, Vahlen Verlag, 2009Zantow, R.;Dinauer, J.: Finanzwirtschaft der Unternehmens:Die Grundlagen des modernen Finanzmanagements, 3. Auflage,PearsonStudium, 2011
5	**Teilnahmevoraussetzungen:** Empfohlen: Grundlagen der Investition und Finanzierung, Grundlagen der Statistik
6	**Prüfungsformen***:* Klausur 90 min.
7	***Voraussetzungen für die Vergabe von Kreditpunkten:*** Bestandene Klausur

8	***Verwendbarkeit des Moduls:*** Systems Engineering M.Eng., Advanced IT Security M.Sc., Business and Security Analytics M.Sc.
9	***Modulverantwortliche(r):*** Prof. Dr. Philipp Lindenmayer Dozenten: Prof. Dr. Philipp Lindenmayer
10	***Optionale Informationen:*** Studiengangsspezifische, zusätzliche Informationen zum Modul

2.2.7 52500 – Innovation and Transfer Competence

Studiengang: Advanced IT Security M.Sc. **Semester**: WS 2021/22
StuPO-Version: 21.2 **Letzte Bearbeitung**: 14.04.21

<table>
<tr><td colspan="8">Modul: Innovation and Transfer Competence</td></tr>
<tr><td colspan="2">Kennnummer
52500</td><td>Workload
180</td><td>Modulart
PM</td><td colspan="2">Studiensemester
2</td><td>Dauer
1</td><td>Häufigkeit
SS</td></tr>
<tr><td>1</td><td colspan="3">Lehrveranstaltung(en)
a. 52305 In. and Transfer Competence
b. 52320 Proj. In. and Transfer Competence</td><td>Sprache
a.,b., deutsch oder englisch</td><td>Kontakt-zeit
a. 15
b. 45</td><td>Selbst-studium
120</td><td>Credits (ECTS)
6</td></tr>
<tr><td>2</td><td colspan="7">Lehrform(en) / SWS:
a. Vorlesung, Seminar b. Projektarbeit</td></tr>
<tr><td>3</td><td colspan="7">Lernergebnisse (learning outcomes), Kompetenzen:
Kompetenz Wissen
Methoden zur Integration einen betrieblichen Innovationsmangements in bestehende Betriebe [Wissen, 7]
Planungs-, Organisations-und Qualitätsmanagementsmethoden aus Theorie und Praxis [Wissen, 7]

Kompetenz Fertigkeiten
Wissenschaftliche Grundlagen-und neuere Forschungsergebnisse erfassen, auf deren praktischen Einsatz hin prüfen, ergänzen und zum Einsatz bringen. [Systemische Fertigkeiten, 7]

Zusammenhänge zwischen diversen Theorien und Konzepten zu sehen, diese zu umfassenderen integrierenden praxisorientierten Konzeptionen weiterzuentwickeln und in konkreten entwickelten Anwendungen zum Einsatz zu bringen [Instrumentelle Fertigkeiten, 7]

Geschäftsideen entwickeln, diese bezügliche Realisierbarkeit prüfen und Strategien entwickeln, Forschungsergebnisse zu transferieren und als Innovation umzusetzen [Systemische Fertigkeiten, 7]

Sozialkompetenz
Projekte organisieren, umsetzen, steuern und die Einhaltung nach Gesichtspunkten des Qualitätsmanagements kontrollieren, überwachen. [Team-/Führungsfähigkeit, 7]

Selbstständigkeit
Sind in der Lage in einem konkurrierendem Kontext, eigene Ideen zu reflektieren, diese gegeben Falls anzupassen und durchzusetzen, oder sich Argumenten zu beugen und die Ideen der Wettbewerber zu akzeptieren
[Eigenständigkeit/Verantwortung, 7]</td></tr>
</table>

4	**Inhalte*:*** Vorlesung: - Ideenmanagement - Betriebliches Innovationsmanagement - Transfer Wissenschaft -Praxis Projekt - Entwicklung eines ausführlichen Geschäftsszenarios, eines Qualitätsmanagementplans und einer Risikoabschätzung - Bestimmung, Suche und Auswahl der einzusetzenden wissenschaftlichen Forschungsergebnisse - Entwicklung einer Vermarktungsstrategie - Durchführen der Organisations-und Qualitätsplanung - Vornahme der Projektplanung (Aufgaben, Netzplan, Meilensteine) und Festlegung der Arbeitsverteilung (Rollen, Verantwortlichkeiten, Mitarbeit, Personalführung) - Leitung und Durchführung des Projekts - Betreiben des Projekt-und Risikomanagements - Durchführung von Produkttest, Endfertigung und Qualitätskontrolle
	Empfohlene Literaturangaben: Al-Laham, Andreas. Organisationales Wissensmanagement: Eine strategische Perspektive. Vahlen, 2016. Mertins, Kai, Ina Kohl, and Ronald Orth. "Ein Referenzmodell für Wissensmanagement." Wissensmanagement im Mittelstand. Springer Gabler, Berlin, Heidelberg, 2016. 31-40. Kamiske, Gerd F., and Jörg-Peter Brauer. Qualitätsmanagement von A-Z: Wichtige Begriffe des Qualitätsmanagements und ihre Bedeutung. Carl Hanser Verlag GmbH Co KG, 2016. Neumann, Alexander. Führungsorientiertes Qualitätsmanagement. Carl Hanser Verlag GmbH Co KG, 2017.
5	**Teilnahmevoraussetzungen:** Wissenschaftliches Arbeiten (DQR 6), Projektmanagement (DQR 5)
6	**Prüfungsformen***:* Praktische Arbeit (benotet) als Modulprüfung
7	***Voraussetzungen für die Vergabe von Kreditpunkten:*** Bestandene Praktische Arbeit
8	***Verwendbarkeit des Moduls:*** Systems Engineering M.Eng., Advanced IT Security M.Sc., Business and Security Analytics M.Sc.
9	***Modulverantwortliche(r):*** Prof. Dr. German Nemirovski
10	***Optionale Informationen:*** Studiengangsspezifische, zusätzliche Informationen zum Modul

2.2.8 Xxxxx - IT-Sicherheit und IT-Angriffe

Studiengang: Advanced IT Security M.Sc. **Semester**: WS 2021/22
StuPO-Version: 21.2 **Letzte Bearbeitung**: 14.04.21

<table>
<tr><td colspan="7">Modul: IT-Sicherheit und IT-Angriffe</td></tr>
<tr><td colspan="2">Kennnummer</td><td>Work-load
90 h</td><td>Modulart
WPF</td><td>Studiensemester
1</td><td>Dauer
1 Semester</td><td>Häufigkeit
SS</td></tr>
<tr><td>1</td><td colspan="2">Lehrveranstaltung(en)
Vorlesung IT-Sicherheit und IT-Angriffe</td><td>Sprache
Deutsch</td><td>Kontakt-zeit
2 SWS / 30 h</td><td>Selbst-studium
60 h</td><td>Credits (ECTS)
3</td></tr>
<tr><td>2</td><td colspan="6">Lehrform(en) / SWS:
Vorlesung: 2 SWS</td></tr>
<tr><td>3</td><td colspan="6">Lernergebnisse (learning outcomes), Kompetenzen:

Kompetenz Wissen
Die Studierenden Kennen die Kategorien der Schadsoftware und deren Auswirkung [Wissen, 7]
Kompetenz Fertigkeiten
Die Studierenden Kennen die Kategorien der Schadsoftware und deren Auswirkung /Kompetenzausprägung wählen 7]
Sozialkompetenz
Die Studierenden Kennen die Kategorien der Schadsoftware und deren Auswirkung /Kompetenzausprägung wählen 7]
Selbstständigkeit
Die Studierenden sind in der Lage größere Aufgaben, deren Bearbeitung auch mehrere Tage in Anspruch nimmt, verantwortungsvoll zu erfüllen, realistische Ziele zu definieren und diese konsequent zu verfolgen /Kompetenzausprägung wählen 7]</td></tr>
<tr><td>4</td><td colspan="6">Inhalte:
• Grundlagen der IT-Sicherheit
• IT-Bedrohungen und Abwehrmaßnahmen
• Schadsoftware (Computerviren, Würmer, Trojanisches Pferd)
• Angriff über Pufferüberlauf (Mechanismen, Manipulation des Programmablaufes, Erstellen von Schadcode, Überlegungen zur Abwehr von Schadcode)
• Bedrohungen im Rechnernetz und Abwehrmaßnahmen
• Angriffe auf Schicht 2, 3, und 4) und Abwehrmaßnahmen
• Bedrohungen aus dem Internet und Abwehrmaßnahmen</td></tr>
</table>

Version	Geändert von Ammann/am 14.04.2021	Dokument	Freigabe am/von	Gültig ab WS 2021/22
1.0		WPM-Katalog_Advanced IT Security_Version1.0_Stand 20210414_FINAL		

	• Angriff auf einen Browser • E-Mail-Client Angriffe • Spam-Mails und Phishing-Mails • DoS und DDoS • Python-Hacks (Kelogger, Ransomware, WLAN-Probe-Requestst, Passwortangriff)
	Empfohlene Literaturangaben: Alan J White (Autor), Ben Clark: Blue Team Field Manual. Create Space Independent Publishing Platform (2017); Cameron H. Malin, Eoghan Casey, James M. Aquilina: Malware Forensics Guide for Windows Systems, Digital Forensics Field Guides. Elsevier (2012) Claudia Eckert. IT-Sicherheit - Konzepte - Verfahren - Protokolle. Oldenbourg Verlag, München, überarbeitete und erweiterte Auflage edition, 2008a. ISBN 978-3-486-70687-1. Klein, T. (2003): Buffer Overflows und Format-String-Schwachstellen: Funktionsweisen, Exploits und Gegenmaßnahmen; Heidelberg: dpunkt-Verlag Weitere Literatur, insbesondere aktuelle wissenschaftliche Artikel, warden in der Vorlesung bekannt gegeben.
5	Teilnahmevoraussetzungen: Die Studierenden besitzen Kenntnisse, Fertigkeiten und Erfahrungen in • Betriebssysteme • Netzwerke • Netzwerksicherheit • Programmierung in einer Hochsprache und einer Skriptsprache
6	**Prüfungsformen***:* Klausur 60 Min; benotet
7	***Voraussetzungen für die Vergabe von Kreditpunkten:*** Bestandenes Referat und bestandene Praktische Arbeit
8	***Verwendbarkeit des Moduls:*** Systems Endineering M.Eng.; Business and Security Analytics M.Sc., Advanced IT Security M.Sc.
9	***Modulverantwortliche(r):*** Prof. Dr. Rieger Dozenten: Prof. Dr. Rieger
10	***Optionale Informationen:*** Studiengangsspezifische, zusätzliche Informationen zum Modul