D I E N S T B L A T T
DER HOCHSCHULEN DES SAARLANDES

2021	ausgegeben zu Saarbrücken, 20. August 2021	Nr. 67

UNIVERSITÄT DES SAARLANDES Seite

Fachspezifische Bestimmungen für den Master-Studiengang Cybersecurity der Universität des Saarlandes zur Gemeinsamen Prüfungsordnung für die Bachelor- und Master-Studiengänge der Fakultät für Mathematik und Informatik

Vom 25. Februar 2021

Die Fakultät für Mathematik und Informatik der Universität des Saarlandes hat auf Grund des § 64 Saarländisches Hochschulgesetz (Amtsbl. I S. 1080), geändert durch Gesetz vom 8./9. Dezember 2020 (Amtsbl. I 2021 S. 53) und auf der Grundlage der Gemeinsame Prüfungsordnung für die Bachelor- und Master-Studiengänge der Fakultät für Mathematik und Informatik an der Universität des Saarlandes vom 25. Februar 2021 (Dienstbl. S. 580) folgende fachspezifischen Bestimmungen für den Master-Studiengang Cybersecurity der Fachrichtung Informatik erlassen, die nach Zustimmung des Senats der Universität des Saarlandes und des Universitätspräsidiums hiermit verkündet wird.

§ 27
Geltungsbereich
(vgl. § 1 Gemeinsame Prüfungsordnung)

Dieser fachspezifische Anhang gilt für den Master-Studiengang Cybersecurity der Universität des Saarlandes.

§ 28
Grundsätze
(vgl. § 2 Gemeinsame Prüfungsordnung)

Der Master-Studiengang Cybersecurity ist stärker forschungsorientiert.

§ 29
Studiengang-Formen
(vgl. § 3 Gemeinsame Prüfungsordnung)

Der Master-Studiengang Cybersecurity ist ein Kernbereich-Studiengang im Sinne der Rahmenprüfungsordnung der Universität des Saarlandes.

§ 30
Studienaufwand
(vgl. § 4 Gemeinsame Prüfungsordnung)

Für Seminare, Projektseminare, Übungen und Praktika kann eine Anwesenheitspflicht bestehen, die der Dozent zu Beginn der Veranstaltung bekannt gibt. Die Pflicht der Anwesenheit ist erfüllt, wenn i.d.R. mindestens 85 % des zeitlichen Umfangs der Veranstaltung wahrgenommen wurde. Bei Fehlen aus triftigen Gründen können den Studierenden Ersatzleistungen angeboten werden.

§ 31
Prüfer und Prüferinnen; Betreuer und Betreuerinnen; Beisitzer und Beisitzerinnen
(vgl. § 8 Gemeinsame Prüfungsordnung)

(1) Der Prüfungsausschuss bestellt Prüfer und Prüferinnen sowie Gutachter und Gutachterinnen bzw. Betreuer und Betreuerinnen der Master-Arbeit aus den Gruppen nach Artikel 8 Absatz 1 Nr. 1 bis 7 der gemeinsamen Prüfungsordnung für die Bachelor- und Master-Studiengänge der Fakultät für Mathematik und Informatik sowie zusätzlich aus der Gruppe der

wissenschaftlichen Mitarbeiter und Mitarbeiterinnen mit Promotionsrecht.

(2) Zusätzlich zu den in Artikel 8 Absatz 2 der gemeinsamen Prüfungsordnung genannten Prüfern und Prüferinnen und Gutachtern sowie Gutachterinnen bzw. Betreuern und Betreuerinnen einer Master-Arbeit kann der Prüfungsausschuss im Einvernehmen mit den das betreffende Fachgebiet vertretenden Professoren und Professorinnen in besonderen Fällen Leiter und Leiterinnen selbstständiger Nachwuchsgruppen und promovierte Mitglieder der Gruppe der akademischen Mitarbeiter und Mitarbeiterinnen sowie promovierte Mitarbeiter und Mitarbeiterinnen der An-Institutionen CISPA Helmholtz-Zentrum für Informationssicherheit, Deutsches Forschungszentrum für Künstliche Intelligenz und der Max-Planck-Institute für Informatik und Softwaresysteme sowie qualifizierte, in der beruflichen Praxis erfahrene Personen bestellen.

§ 32
Zugang zum Master-Studium
(vgl. § 12 Gemeinsame Prüfungsordnung)

(1) Zugangsberechtigt zum Master-Studiengang ist,

1. wer an einer deutschen Hochschule einen Bachelor-Abschluss oder an einer ausländischen Hochschule einen äquivalenten Abschluss in einem Studiengang der Informatik oder einem verwandten Fach erworben hat.
2. und die besondere Eignung (§ 77 Absatz 6 SHSG) nachweist.

(2) Kriterien für die Feststellung der besonderen Eignung sind:

a. der Nachweis englischer Sprachkenntnisse auf fortgeschrittenem Niveau (in der Regel C1)
b. die in der bisherigen akademischen Laufbahn erbrachten Leistungen und der fachliche Inhalt des Bachelor-Abschlusses. Der Kandidat und die Kandidatin sollte dabei Kompetenzen nachweisen, die denen des im Bachelor-Studiengangs Cybersicherheit an der Universität des Saarlandes vermittelten Kompetenzen im Informatik-Kernbereich entsprechen. Vorwissen in fachspezifischen Themen der Cybersicherheit wird explizit nicht erfordert, ist aber auch nicht hinderlich. Erforderliche wesentliche Kompetenzen schließen insbesondere die folgenden Bereiche ein:
   I. Mathematik (diskrete Mathematik, Lineare Algebra, Stochastik, Statistik)
   II. Theoretische Informatik (Komplexitätstheorie, Berechenbarkeit)
   III. Praktische Informatik (funktionale und objektorientierte Programmierung, Datenstrukturen und Algorithmen, Systemarchitektur)
c. das in Form eines Dossiers und zweier qualifizierender Gutachten dokumentierte Studieninteresse

Mit Hilfe der genannten Kriterien wird die studiengangsspezifische Eignung der Bewerberin und des Bewerbers mit dem Profil und den Anforderungen des Master-Studiengangs Cybersecurity abgeglichen. Die Feststellung, ob die Zugangsvoraussetzungen erfüllt sind, trifft der Prüfungsausschuss.

§ 33
Verfahren und Gestaltung
(vgl. § 23 Gemeinsame Prüfungsordnung)

Die selbstständige Ausführung der Master-Arbeit wird in einem 30-minütigen Kolloquium überprüft. Dieses muss spätestens 6 Wochen nach Abgabe der schriftlichen Ausarbeitung der Master-Arbeit abgelegt werden. Eine oder einer der Prüferinnen oder Prüfer soll die oder der Themenstellende der Arbeit sein.

§ 34
Bestehen und Gesamtnote der Master-Prüfung
(vgl. § 24 Gemeinsame Prüfungsordnung)

Das Prädikat „mit Auszeichnung“ wird im Master-Studiengang Cybersecurity bei einer Gesamtnote von 1,1 oder besser vergeben, sofern alle eingebrachten Leistungen in der Regelstudienzeit erbracht wurden.

§ 35
Akademischer Grad und Abschluss-Dokumente
(vgl. § 25 Gemeinsame Prüfungsordnung)

Das Zeugnis kann über die Angaben nach Artikel 25 Absatz 1 der gemeinsamen Prüfungsordnung für die Master-Studiengänge der Fakultät für Mathematik und Informatik hinaus studierte Schwerpunkte sowie weitere erbrachte Leistungen und die jeweils erzielten Ergebnisse enthalten.

§ 36
Inkrafttreten

Diese Ordnung tritt am Tage nach ihrer Bekanntmachung im Dienstblatt der Hochschulen des Saarlandes in Kraft.

Saarbrücken, 12. August 2021

Der Universitätspräsident
(Univ.-Prof. Dr. Manfred Schmitt)

In Vertretung

Der Vizepräsident für Verwaltung und Wirtschaftsführung
(Dr. Roland Rolles)

Studienordnung der Universität des Saarlandes für den Master-Studiengang Cybersecurity

Vom 25. Februar 2021

Die Fakultät für Mathematik und Informatik der Universität des Saarlandes hat auf Grund von § 60 Saarländisches Hochschulgesetz vom 30. November 2016 (Amtsbl. I S. 1080), zuletzt geändert durch Gesetz vom 8./9. Dezember 2020 (Amtsbl. I 2021 S. 53) und auf der Grundlage der Gemeinsame Prüfungsordnung für die Bachelor- und Master-Studiengänge der Fakultät für Mathematik und Informatik an der Universität des Saarlandes vom 25. Februar 2021 (Dienstbl. S. 580) folgende Studienordnung für den Master-Studiengang Cybersecurity erlassen, die nach Zustimmung des Senats der Universität des Saarlandes hiermit verkündet wird.

§ 1
Geltungsbereich

Diese Studienordnung regelt Inhalt und Aufbau des Master-Studiengangs Cybersecurity und auf der Grundlage der Gemeinsame Prüfungsordnung für die Bachelor- und Master-Studiengänge der Fakultät für Mathematik und Informatik an der Universität des Saarlandes vom 25. Februar 2021 (Dienstbl. S. 580) sowie der Fachspezifischen Bestimmungen für den Master-Studiengang Cybersecurity vom 25. Februar 2021 (Dienstbl. Nr. 67, S. 638). Zuständig für die Organisation von Lehre, Studium und Prüfungen ist die Fakultät für Mathematik und Informatik.

§ 2
Ziele des Studiums und Berufsfeldbezug

Ziel dieses Master-Studiengangs ist es, auf eine anspruchsvolle nationale und internationale Forschungs- und Entwicklungstätigkeit im Bereich der Cybersecurity vorzubereiten. Der Master-Studiengang Cybersecurity zielt darauf ab, den Studierenden unterschiedliche und sich ergänzende Möglichkeiten zur Vertiefung des Themenfelds der Cybersicherheit zu bieten. Studierende können sich in den Bereichen der Kryptographie, Privatsphäre, Sicherheit von Software, Systemen und Netzwerken, formalen Methoden oder rechtlichen Aspekte der Cybersicherheit vertiefen, und dabei gleichzeitig gezielte verwandte Themenblöcke der Informatik erarbeiten. Der Abschluss ermöglicht einen direkten Einstieg in Cybersicherheitsforschung, und vermittelt gleichzeitig tiefes Wissen, um nicht-wissenschaftliche Tätigkeiten im Kontext der Cybersicherheit in der Privatwirtschaft oder im öffentlichen Bereich aufnehmen zu können.

§ 3
Studienbeginn und Studiendauer

(1) Das Studium kann jeweils zum Winter- und Sommersemester eines Jahres aufgenommen werden.

(2) Das Lehrangebot ist so organisiert, dass das Studium in vier Semestern abgeschlossen werden kann (Regelstudienzeit).

§ 4
Art der Lehrveranstaltungen

Das Lehrangebot wird durch Lehrveranstaltungen folgender Art vermittelt:

1. Vorlesungen (V, Regelgruppengröße = 100): Sie dienen zur Einführung in ein Fachgebiet und vermitteln u. a. einen Überblick über fachtypische theoretische Konzepte und Prinzipien, Methoden und Fertigkeiten, Technologien und praktische Realisierungen. Vorlesungen geben Hinweise auf weiterführende Literatur und eröffnen den Weg zur Vertiefung der Kenntnisse durch Übungen, Praktika und ergänzendes Selbststudium.

2. Übungen (Ü, Regelgruppengröße = 20): Sie finden überwiegend als Ergänzungsveranstaltungen zu Vorlesungen bevorzugt in kleineren Gruppen statt. Sie sollen den Studierenden durch Bearbeitung exemplarischer Probleme die Gelegenheit zur Anwendung und Vertiefung der in der Vorlesung vermittelten Lehrinhalte sowie zur Selbstkontrolle des Wissensstandes ggf. durch eigene Fragestellung geben.

3. Seminare (S, Regelgruppengröße = 15) erweitern die bereits erworbenen Kenntnisse und vermitteln durch das Studium von Fachliteratur und Quellen in Seminargesprächen, Referaten oder Seminar-Arbeiten einen vertieften Einblick in einen Forschungsbereich. Sie dienen darüber hinaus dem Erlernen wissenschaftlicher Darstellungs- und Vortragstechniken sowie der Anleitung zu kritischer Sachdiskussion von Forschungsergebnissen. Zusätzlich können projektbezogene Arbeiten zu aktuellen wissenschaftlichen Diskussionen vorgesehen sein. Die dabei vertieften Inhalte können in einem Master-Seminar die Grundlage für die Master-Arbeit bilden.

4. Praktika und Projekte (P, Regelgruppengröße = 15, Masterpraktikum, Regelgruppengröße = 6): In einem Praktikum oder Projekt werden fachpraktische Themen angeboten, die in die spezifische Arbeitsweise der betreffenden Studienfächer einführen. Die den Themen zugrundeliegenden theoretischen Kenntnisse erwirbt man durch Vorlesungen und Literaturstudien. Ein weiteres Ziel der Praktika ist die Vermittlung computergestützter Methoden durch praktische Anwendung. In Projekten werden in der Regel fachübergreifende Themen behandelt. Die Bearbeitung eines Themas bietet den Studierenden die Gelegenheit, in Gruppen unter Anleitung themenspezifische Aufgabenstellungen von der Konzeption bis hin zur praktischen Realisierung zu lösen. Man lernt hier einerseits die Zusammenhänge zwischen Theorie und Praxis durch eigene selbstständige Arbeit kennen, andererseits wird die Gruppenarbeit in Projekten gefördert. Die Teilnahme an Praktika oder Projekten kann vom Nachweis über die erfolgreiche Teilnahme an zugehörigen Vorlesungen und Übungen abhängig gemacht werden.

§ 5
Aufbau und Inhalt des Studiums

(1) Das Studium des Master-Studiengangs Cybersecurity umfasst eine Gesamtleistung von 120 Credit Points (CP) nach dem European Credit Transfer System (ECTS). Davon müssen mindestens 106 CP und maximal 110 CP als benotete Leistungen erbracht werden. Pro Semester sind in der Regel 30 CP zu erwerben.

(2) Das Studium umfasst Module zu folgenden Teilbereichen. Die Module und Modulelemente der einzelnen Teilbereiche, sowie jeweils die Art der Lehrveranstaltung, deren Semesterwochenstunden und Credit Points, Zyklus, sowie die Art der Prüfung und Benotung sind in Anhang A beschrieben.

1. 27 benotete Credit Points aus dem Bereich der Stammvorlesungen (je 9 CP, Wahlpflicht). Aus diesem Katalog sind verpflichtend die beiden Stammvorlesungen “Cryptography” und

"Security" zu bestehen, sofern keine äquivalenten Vorleistungen aus einem vorangegangenen Studium nachgewiesen werden.

Studierende, welche die beiden Bachelor-Grundvorlesungen "Grundlagen der Cybersicherheit I" und "Grundlagen der Cybersicherheit II" in einem grundständigen Studium bereits bestanden haben, müssen die Stammvorlesung "Security" durch eine andere Stammvorlesung ersetzen.

2. Mindestens 30 und maximal 34 benotete Credit Points aus dem Bereich der Stammvorlesungen (je 9 CP), der Vertiefungsvorlesungen Cybersecurity (variable Anzahl an CP, zumeist jedoch 6 CP) oder der Seminare Cybersecurity (je 7 CP) (Wahlpflicht). Darin darf maximal ein weiteres Seminar (vgl. § 5 Absatz 2, Nr. 3) und eine weitere Stammvorlesung (vgl. § 5 Absatz 2, Nr. 1) enthalten sein.

3. 7 benotete Credit Points aus dem Bereich der Seminare Cybersecurity (je 7 CP, Wahlpflicht)

4. 12 benotete Credit Points des Master-Seminars (12 CP)

5. 30 benotete Credit Points der Master-Arbeit (30 CP)

6. Mindestens 14 unbenotete Credit Points ("freie Punkte") durch wählbare Module aus den Bereichen (Wahlpflichtbereich):
   a. Masterpraktika (je 6 CP)
   b. beliebig wählbare Module aus dem Bereich der Stammvorlesungen, Vertiefungsvorlesungen Cybersecurity oder Seminare Cybersecurity oder der entsprechenden Modulkategorien des Master-Studiengangs Informatik
   c. Betreuung von Übungsgruppen (Tutorentätigkeit); in der Regel je 4 CP, wobei eine mehrfache Erbringung dieser Leistungen möglich ist, sofern die Übungsgruppen unterschiedlichen Modulen angehören.
   d. Sprachkurse (maximal 6 CP; lebende Sprachen; nicht die Muttersprache)
   e. Soft Skill Seminar
   f. Industrie-Praktikum (maximal 6 CP), das auf Antrag an den Prüfungsausschuss genehmigt wurde.
   g. Module, die auf Antrag an den Prüfungsausschuss genehmigt wurden. Studierende haben beispielsweise die Möglichkeit, einen Antrag an den Prüfungsausschuss auf Anerkennung des geleisteten studentischen Engagements (insbesondere Mitarbeit bei der akademischen Selbstverwaltung) sowie Veranstaltungen zu Schlüsselqualifikationen im Umfang von jeweils maximal 3 CP zu stellen.

(3) Im Wahlpflichtbereich können gesamte Module oder einzelne Lehrveranstaltungen belegt werden. Prüfungsleistungen, die bereits in die Bachelor-Prüfung eingegangen sind, können prinzipiell nicht in die Master-Prüfung eingebracht werden. Prüfungsleistungen aus dem Bachelor-Studium, die nicht in der Bachelor-Prüfung berücksichtigt wurden und einen Gesamtumfang von 30 CP nicht überschreiten, können in die Master-Prüfung eingebracht werden.

(4) Im Pflichtbereich werden insgesamt 42 CP erworben (30 CP davon entfallen auf das Modul "Master-Arbeit" und 12 CP auf das Modul "Master-Seminar") und im Wahlpflichtbereich sind mindestens 78 CP zu erwerben.

(5) Bei Veranstaltungen aus den Bereichen "Praktikum", "Seminar" sowie "Tutor", "Soft Skill Seminar" und "Sprachkurse" aus dem Wahlpflichtbereich stehen begrenzte Teilnehmerplätze, abhängig von der entsprechenden Veranstaltung zur Verfügung. Die Zulassung wird durch den Modulverantwortlichen geregelt.

(6) Eine Prüfungsleistung ist entweder benotet oder unbenotet einzubringen. Die Teilung einer benoteten Prüfungsleistung in unbenotete und benotete Credit Points ist nicht möglich.

(7) Eine bestandene Prüfungsleistung der Stammvorlesungen Cybersecurity und Informatik kann in der Regelstudienzeit einmalig zur Notenverbesserung im gleichen Prüfungszeitraum (vgl. § 13 Abs. 4 der Prüfungsordnung) wiederholt werden. Bestandene Prüfungsleistungen der Vertiefungsvorlesungen Cybersecurity können einmalig zur Notenverbesserung im gleichen Prüfungszeitraum wiederholt werden, falls der Dozent zu Beginn der Veranstaltung die jeweilige Prüfungsleistung als verbesserbar ausweist. Dabei zählt das bessere Ergebnis. Ansonsten ist die Wiederholung einer bestandenen Prüfungsleistung nicht zulässig.

(8) Die Module der Stammvorlesungen im Wahlpflichtbereich werden mindestens einmal alle zwei Jahre angeboten. Seminare und Vertiefungsvorlesungen können einmalig angeboten werden. Der Studiendekan/Die Studiendekanin stellt in jedem Studienjahr ein hinreichendes Angebot sicher.

(9) Die Unterrichtssprache ist in der Regel Englisch und wird zu Beginn der Veranstaltung bekannt gegeben. Es wird gewährleistet, dass das Studium auch mit ausschließlich englischsprachigen Veranstaltungen erfolgreich abgeschlossen werden kann.

(10) Das Studienangebot in den verschiedenen Wahlpflichtbereichen kann modifiziert werden, wobei Änderungen vom Prüfungsausschuss zu genehmigen sind. Neue bzw. modifizierte Veranstaltungen, ihr Gewicht in CP und ihre Zugehörigkeit zu den Modulbereichen werden jeweils vor Semesterbeginn bekannt gegeben.

(11) Detaillierte Informationen zu den Inhalten der Module und Modulelemente werden im Modulhandbuch beschrieben, das in geeigneter Form bekannt gegeben wird. Änderungen an den Festlegungen des Modulhandbuchs, die nicht in dieser Studienordnung geregelt sind, sind dem zuständigen Studiendekan/der zuständigen Studiendekanin anzuzeigen und in geeigneter Form zu dokumentieren.

(12) Für Seminare und Praktika kann eine Anwesenheitspflicht bestehen, die der Dozent/die Dozentin zu Beginn des Moduls/Modulelements bekannt gibt. Die Pflicht der Anwesenheit ist erfüllt, wenn i.d.R. mindestens 85 % des zeitlichen Umfangs der Veranstaltung wahrgenommen wurde. Bei Fehlen aus triftigen Gründen können den Studierenden Ersatzleistungen angeboten werden.

(13) Inhaltsgleiche Module, die lediglich in verschiedenen Sprachen angeboten werden, gelten als ein Modul hinsichtlich der Anzahl der Prüfungsversuche sowie der Regelungen des Freiversuchs bzw. der Notenverbesserung, falls die Studienordnung diese vorsieht.

§ 6
Studienplan

Der Studiendekan/die Studiendekanin erstellt auf der Grundlage dieser Studienordnung einen Studienplan, der nähere Angaben über Art und Umfang der Modulelemente (Anhang A) enthält sowie Empfehlungen für einen zweckmäßigen Aufbau des Studiums gibt (Anhang B). Dieser wird in geeigneter Form bekannt gegeben. Das jeweils aktuelle Angebot in den verschiedenen Modulkategorien wird im Vorlesungsverzeichnis des jeweiligen Semesters bekannt gegeben.

§ 7
Studienberatung

(1) Die Zentrale Studienberatung der Universität des Saarlandes berät Interessierte und Studierende über Inhalt, Aufbau und Anforderungen eines Studiums. Darüber hinaus gibt es Beratungsangebote bei Entscheidungsproblemen, bei Fragen der Studienplanung und Studienorganisation.

(2) Fragen zu Studienanforderungen und Zulassungsvoraussetzungen, zur Studienplanung und -organisation beantwortet der Fachstudienberater/die Fachstudienberaterin für den Master-Studiengang Cybersecurity.

(3) Für spezifische Rückfragen zu einzelnen Modulen stehen die Modulverantwortlichen zur Verfügung.

§ 8
Auslandsaufenthalt

Es besteht die Möglichkeit, ein Auslandsstudium zu absolvieren. Die Studierenden sollten an einer Beratung zur Durchführung des Auslandsstudiums teilnehmen, ggf. vorbereitende Sprachkurse belegen und im Vorfeld über ein Learning Agreement die Anerkennung von Studienleistungen gemäß der einschlägigen Prüfungsordnung klären. Über Studienmöglichkeiten, Austauschprogramme, Stipendien und Formalitäten informieren sowohl das International Office als auch die Fachvertreter des entsprechenden Schwerpunktfachs. Aufgrund langer Antragsfristen und Bearbeitungszeiten bei ausländischen Universitäten wie Stipendiengebern sollte die Anmeldung für ein Auslandsstudium in der Regel ein Jahr vor Antritt des Auslandaufenthalts im Prüfungssekretariat erfolgen.

§ 9
Master-Arbeit und Master-Seminar

(1) Durch die Anfertigung einer Master-Arbeit soll der/die Studierende nachweisen, dass er/sie Aufgabenstellungen aus den Bereichen der Cybersicherheit eigenständig bearbeiten kann. Die Arbeit entstammt einem der genannten Teilgebiete und wird individuell von einem Lehrenden des Master-Studiengangs Cybersecurity betreut. Die Bearbeitungszeit beträgt sechs Monate. Der mit der Master-Arbeit verbundene Aufwand wird mit 30 CP kreditiert.

(2) Jeder und jede Studierende muss vor Abschluss der Master-Arbeit erfolgreich ein Master-Seminar mit direktem Bezug zum Thema der Master-Arbeit abgeschlossen haben. Dieses beinhaltet sowohl einen Vortrag über die geplante Themenstellung als auch eine schriftliche Beschreibung der geplanten Aufgabenstellung der Master-Arbeit.

(3) Die Master-Arbeit muss spätestens ein Semester nach erfolgreicher Teilnahme am Master-Seminar beim Prüfungssekretariat angemeldet werden. Nach Ablauf dieser Frist muss erneut ein Master-Seminar erfolgreich absolviert werden.

§ 10
Inkrafttreten

Diese Ordnung tritt am Tage nach ihrer Bekanntmachung im Dienstblatt der Hochschulen des Saarlandes in Kraft.

Saarbrücken, 12. August 2021

Der Universitätspräsident
(Univ.-Prof. Dr. Manfred Schmitt)

In Vertretung

Der Vizepräsident für Verwaltung und Wirtschaftsführung
(Dr. Roland Rolles)

Anhang A: Modulliste

Stammvorlesungen				
Cryptography **(obligatorisch)**	Klausur(en), PVL	b	0	9
Security **(obligatorisch)**	Klausur(en), PVL	b	0	9
Algorithms and Data Structures	Klausur(en), PVL	b	0	9
Artificial Intelligence	Klausur(en), PVL	b	0	9
Audio/Visual Communication and Networks	Klausur(en), PVL	b	0	9
Automated Reasoning	Klausur(en), PVL	b	0	9
Compiler Construction	Klausur(en), PVL	b	0	9
Complexity Theory	Klausur(en), PVL	b	0	9
Computer Algebra	Klausur(en), PVL	b	0	9
Computer Graphics	Klausur(en), PVL	b	0	9
Data Networks	Klausur(en), PVL	b	0	9
Database Systems	Klausur(en), PVL	b	0	9
Digital Transmission, Signal Processing	Klausur(en), PVL	b	0	9
Distributed Systems	Klausur(en), PVL	b	0	9
Embedded Systems	Klausur(en), PVL	b	0	9
Geometric Modeling	Klausur(en), PVL	b	0	9
Human Computer Interaction	Klausur(en), PVL	b	0	9
Image Processing and Computer Vision	Klausur(en), PVL	b	0	9
Information Retrieval and Data Mining	Klausur(en), PVL	b	0	9
Introduction to Computational Logic	Klausur(en), PVL	b	0	9
Machine Learning	Klausur(en), PVL	b	0	9
Multimedia Transport	Klausur(en), PVL	b	0	9
Operating Systems	Klausur(en), PVL	b	0	9
Optimization	Klausur(en), PVL	b	0	9
Semantics	Klausur(en), PVL	b	0	9
Software Engineering	Klausur(en), PVL	b	0	9
Verification	Klausur(en), PVL	b	0	9
Der Prüfungsausschuss kann das Studienangebot modifizieren.				
Vertiefungsvorlesungen Cybersicherheit				
Das Angebot an Vertiefungsvorlesungen Cybersicherheit kann jedes Semester variieren				
Advanced Public Key Cryptography	Klausur(en), PVL	b	0	6
Algorithms in Cryptanalysis	Klausur(en), PVL	b	0	6
Automated Debugging	Klausur(en), PVL	b	0	6
Ethics for Nerds	Klausur(en), PVL	b	0	6
Generated Software Tests	Klausur(en), PVL	b	0	6
Machine Learning in Cybersecurity	Klausur(en), PVL	b	0	6
Mobile Security	Klausur(en), PVL	b	0	6
Obfuscation	Klausur(en), PVL	b	0	6
Parameterized Verification	Klausur(en), PVL	b	0	6
Physical-Layer Security	Klausur(en), PVL	b	0	6
Privacy Enhancing Technologies	Klausur(en), PVL	b	0	6
Reactive Synthesis	Klausur(en), PVL	b	0	6
Recht der Cybersicherheit - Datenschutzrechtliche Aspekte	Klausur(en), PVL	b	0	6
Recht der Cybersicherheit - Strafrechtliche Aspekte	Klausur(en), PVL	b	0	6
Secure Web Development	Klausur(en), PVL	b	0	6
Side-Channels Attacks & Defenses	Klausur(en), PVL	b	0	6
Usable Security	Klausur(en), PVL	b	0	6
Web Security	Klausur(en), PVL	b	0	6
Der Prüfungsausschuss kann das Studienangebot modifizieren.				
Seminare Cybersicherheit				
Das Angebot an Seminaren Cybersicherheit kann jedes Semester variieren.	mündlich, schriftlich	b	0	7
Der Prüfungsausschuss kann das Studienangebot modifizieren.				
Wahlpflichtbereich				
Tutor	Tutorentätigkeit	u	4	0
Soft Skill Seminar	mündlich, schriftlich	u	variabel	0
Sprachkurse (max. 6 CP)	mündlich, schriftlich	u	3 oder 6	0
Industriepraktikum (max. 6 CP)		u	6	0
Masterpraktika (je 6 CP)		u	6	0
Weitere Module aus dem Bereich Cybersicherheit oder Informatik	Klausur(en), PVL	u	variabel	0
Der Prüfungsausschuss kann das Studienangebot modifizieren.				

Studienplan

Master-Studiengang Cybersecurity														
Kategorie	**Modulbezeichnung**	**Art der Prüfung**	**Ben.**	**CP (ECTS)** unbenotet	benotet	**WiSe** **Fachsemester 1** V/Ü/P SWS	CP	**SoSe** **2** V/Ü/P SWS	CP	**WiSe** **3** V/Ü/P SWS	CP	**SoSe** **4** V/Ü/P SWS	CP
Stammvorlesung*	(Wechselnde Module, je 9 CP, siehe unten)	Klausur(en), PVL	b	0	27	4/2/0 4/2/0	9 9	4/2/0	9				
Stammvorlesung* oder Vertiefungsvorlesungen Cybersicherheit* oder Seminar Cybersicherheit*; max. eine Stammvorlesung und ein Seminar Cybersicherheit	(Wechselnde Module, Seminar (7 CP), Stamm- (9 CP) oder Vertiefungsvorlesungen (je 6 CP))	Klausur(en), PVL, mündlich, schriftlich	b	0	30 bis 34	2/2/0 2/2/0	6 6	2/2/0	6	2/2/0 2/2/0	6 6		
Seminar Cybersicherheit	(Wechselnde Module, je 7 CP, siehe unten)	mündlich, schriftlich	b	0	7			0/0/3	7				
Wahlpflichtbereich	(Verschiedene Module, variable CP-Zahl, siehe unten)		u	mind. 14	0			4/2/0	8	4/2/0	6		
	Master-Seminar	mündlich, schriftlich	b	0	12						12		
	Master-Arbeit	Master-Arbeit	b	0	30								30
	SUMMEN						30		30		30		30

* Das aktuelle Angebot ist auf der Webseite des Prüfungssekretariates veröffentlicht.

Legende: V = Vorlesung, Ü = Übung, P = Projekt oder Praktikum, PVL = Prüfungsvorleistung, CP = Credit Points, SWS = Semesterwochenstunden, Ben. = Benotung

Anhang B.

Beispielstudienplan Master-Studiengang Cybersecurity (ohne Grundkenntnisse Cybersecurity)

1	Security (9 CP)	Core Lecture (9 CP)	Advanced Lecture Cybersecurity (6 CP)	Advanced Lecture Cybersecurity (6 CP)	30
2	Cryptography (9 CP)	Advanced Lecture Cybersecurity (6 CP)	Seminar CySec (7 CP)	Mandatory Elect (8 CP)	30
3	Advanced Lecture Cybersecurity (6 CP)	Advanced Lecture Cybersecurity (6 CP)	Mandatory Elect (6 CP)	Master's Seminar (12 CP)	30
4	Master's Thesis (30 CP)				30

Beispielstudienplan Master-Studiengang Cybersecurity (nach BSc Cybersicherheit oder BSc Cybersecurity (English))

1	Core Lecture (9 CP)	Core Lecture (9 CP)	Advanced Lecture Cybersecurity (6 CP)	Advanced Lecture Cybersecurity (6 CP)	30
2	Core Lecture (9 CP)	Advanced Lecture Cybersecurity (6 CP)	Seminar CySec (7 CP)	Mandatory Elect (8 CP)	30
3	Advanced Lecture Cybersecurity (6 CP)	Advanced Lecture Cybersecurity (6 CP)	Mandatory Elect (6 CP)	Master's Seminar (12 CP)	30
4	Master's Thesis (30 CP)				30