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

2021	ausgegeben zu Saarbrücken, 20. August 2021	Nr. 66

UNIVERSITÄT DES SAARLANDES Seite

Fachspezifische Bestimmungen für den Bachelor-Studiengang Cybersecurity (English) 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), zuletzt geändert durch Gesetz vom 8./9. Dezember 2020 (Amtsbl. I 2021 S. 53 736) und auf der Grundlage der Gemeinsamen 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 Bachelor-Studiengang Cybersecurity (English) 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 Bachelor-Studiengang Cybersecurity (English) der Universität des Saarlandes.

§ 28
Grundsätze
(vgl. § 2 Gemeinsame Prüfungsordnung)

Der Bachelor-Studiengang Cybersecurity (English) ist stärker forschungsorientiert.

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

Der Bachelor-Studiengang Cybersecurity (English) 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/Prüferinnen; Betreuer/Betreuerinnen; Beisitzer/Beisitzerinnen
(vgl. § 8 Gemeinsame Prüfungsordnung)

(1) Der Prüfungsausschuss bestellt die Prüfer und Prüferinnen sowie die Gutachter und Gutachterinnen bzw. Betreuer und Betreuerinnen der Bachelor-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/Mitarbeiterinnen mit Promotionsrecht.

(2) Zusätzlich zu den in Artikel 8 Absatz 2 der gemeinsamen Prüfungsordnung genannten Prüfern und Prüferinnen und Gutachtern/Gutachterinnen bzw. Betreuern und Betreuerinnen einer Bachelor-Arbeit kann der Prüfungsausschuss im Einvernehmen mit den das betreffende Fachgebiet vertretenden Professoren/Professorinnen in besonderen Fällen Leiter oder 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
Verfahren und Gestaltung
(vgl. § 23 Gemeinsame Prüfungsordnung)

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

§ 33
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 Bachelor- und Master-Studiengänge der Fakultät für Mathematik und Informatik hinaus studierte Schwerpunkte sowie weitere erbrachte Leistungen und die jeweils erzielten Ergebnisse enthalten.

§ 34
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 Bachelor-Studiengang Cybersecurity (English)

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 Bachelor-Studiengang Cybersecurity (English) erlassen, die nach Zustimmung des Senats der Universität des Saarlandes hiermit verkündet wird.

§ 1
Geltungsbereich

Diese Studienordnung regelt Inhalt und Aufbau des Bachelor-Studiengangs Cybersecurity (English) auf der Grundlage der 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. Nr. 62, S. 580) sowie der Fachspezifischen Bestimmungen für den Bachelor-Studiengang Cybersecurity (English) vom 25. Februar 2021 (Dienstbl. Nr. 66, S. 626). Zuständig für die Organisation von Lehre, Studium und Prüfungen ist die Fakultät für Mathematik und Informatik.

§ 2
Ziele des Studiums und Berufsfeldbezug

(1) Der Bachelor-Studiengang Cybersecurity (English) verfolgt das Ziel, Studierende in englischer Sprache und in einem internationalen Umfeld, aufbauend auf mathematisch-naturwissenschaftlichen Grundlagen zur Lösung technischer und naturwissenschaftlicher Problemstellungen im Bereich der Cybersicherheit zu befähigen. Darüber hinaus sollen die Absolventinnen und Absolventen des Studiengangs in die Lage versetzt werden, komplexe Fragestellungen auch in allgemeinerem Kontext mit modernen wissenschaftlichen und computergestützten Methoden zu bearbeiten. Neben der wissenschaftlichen Qualifizierung erhalten die Studierenden weiterhin eine praxisorientierte Berufsfähigkeit in Industrie und Wirtschaft. Diese Zielstellungen erfordern eine solide Grundausbildung sowohl in mathematischen Grundlagen als auch in den Grundlagen der Informatik. Zusätzlich wird die Ausbildung durch spezialisierte Veranstaltungen in den verschiedenen Bereichen der Cybersicherheit komplementiert. Ein weiteres wesentliches Element des Studiengangs ist die Anwendung von vermittelten theoretischen Grundlagen im Rahmen von Praktika und Projekten.

(2) Die akademische Ausbildung mit dem Abschluss Bachlor of Science (B.Sc.) in Cybersecurity liefert eine hinreichende Voraussetzung für weitere fachverwandte Master-Studiengänge.

§ 3
Studienbeginn und Studiendauer

(1) Das Studium kann zum Wintersemester eines Jahres aufgenommen werden.

(2) Das Lehrangebot ist so organisiert, dass das Studium in sechs 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): Sie erweitern die bereits erworbenen Kenntnisse und vermitteln durch das Studium von Fachliteratur und Quellen in Seminargesprächen, Referaten oder Seminararbeiten 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 Bachelorseminar die Grundlage für die Bachelor-Arbeit bilden.

4. Praktika und Projekte (P, Regelgruppengröße = 15): 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 Inhalte des Studiums

(1) Das Studium des Bachelor-Studiengangs Cybersecurity (English) umfasst eine Gesamtleistung von 180 Credit Points (CP) nach dem European Credit Transfer System (ECTS). Pro Semester sind in der Regel 30 CP zu erwerben.

(2) Das Studium umfasst Module aus verschiedenen Bereichen. Die Module und Modulelemente der einzelnen Bereiche, sowie jeweils die Art der Lehrveranstaltung, deren Semesterwochenstunden, Credit Points sowie die Art der Prüfung und Benotung sind in Anhang

A beschrieben. Die angegebene Anzahl an Credit Points in den jeweiligen Bereichen ist zu erbringen. "Wahlpflicht" bedeutet, dass Module/Modulelemente aus einem vorgegebenen Lehrangebot ausgewählt werden können.

1. 18 benotete Credit Points aus dem Pflicht-Bereich der Grundlagen der Mathematik:

a) Mathematics for Computer Scientists 1 (9 CP)
b) Mathematics for Computer Scientists 2 (9 CP)

2. 54 benotete Credit Points aus dem Pflicht-Bereich der Grundlagen der Informatik:

a) Programming 1 (9 CP)
b) Programming 2 (9 CP)
c) Fundamentals of Data Structures and Algorithms (6 CP)
d) Introduction to Theoretical Computer Science (9 CP)
e) System Architecture (9 CP)
f) Statistics Lab (6 CP)
g) Elements of Machine Learning (6 CP)

3. 15 unbenotete Credit Points aus dem Pflicht-Bereich der Praktika:

a) Practical Training "Software Engineering Lab" (9 CP)
b) Practical Training “Cybersecurity Lab” (6 CP)

4. 24 benotete Credit Points aus dem spezialisierten Pflicht-Bereich der Cybersecurity:

a) Foundations of Cybersecurity 1 (9 CP)
b) Foundations of Cybersecurity 2 (6 CP)
c) Cryptography (9 CP)

5. 5 benotete Credit Points aus dem Wahlpflicht-Bereich der Proseminare über Themen der Cybersecurity (je 5 CP)

6. 7 benotete Credit Points aus dem Wahlpflicht-Bereich der Seminare über Themen der Cybersecurity (je 7 CP)

7. Mindestens 12 benotete Credit Points aus dem Wahlpflicht-Bereich “Kernthemen der Cybersicherheit” (üblicherweise 6 CP je Modul)

8. Mindestens 12 benotete Credit Points aus dem Wahlpflicht-Bereich “Komplementäre Themen der Cybersicherheit” (üblicherweise 6 CP je Modul)

9. Mindestens 6 unbenotete Credit Points aus dem Wahlpflicht-Bereich aus Deutsch- oder Englischkursen der Universität des Saarlandes (nicht die Muttersprache); auf Antrag kann der Prüfungsausschuss Sprachkurse für andere Sprachen genehmigen, wenn Studierende nachweisen, dass sie Englisch und Deutsch fließend in Wort und Schrift beherrschen

10. Mindestens 6 unbenotete Credit Points aus dem Wahlpflicht-Bereich der "Freien Punkte" durch wählbare Module/Modulelemente aus:

a) Beliebig wählbare Module aus dem Kursangebot der Informatik, nicht jedoch die Stammvorlesung "Security"
b) Betreuung von Übungsgruppen (Tutortätigkeit); in der Regel je 4 CP, wobei eine mehrfache Erbringung dieser Leistungen möglich ist, sofern die Übungsgruppen unterschiedlichen Modulen angehören.
c) Weitere Sprachkurse (maximal 6 CP; lebende Sprachen; nicht die Muttersprache)

d) Industrie-Praktikum (maximal 6 CP), das auf Antrag an den Prüfungsausschuss genehmigt wurde.
e) Module/Modulelemente, 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.

11. 9 benotete Credit Points aus dem Bachelor-Seminar über Themen der Cybersecurity oder Informatik und
12 benotete Credit Points aus der Bachelor-Arbeit über Themen der Cybersecurity oder Informatik

(3) Von den 180 CP des Bachelor-Studiengangs Cybersecurity (English) werden 153 CP als benotete Leistungen erbracht.

(4) Im Pflicht-Bereich sind alle in § 5 Absatz 2 Nr. 1, Nr. 2, Nr. 3, Nr. 4, und Nr. 11 genannten Module zu belegen (insgesamt 132 CP). Im Wahlpflicht-Bereich können Module oder Modulelemente aus einem vorgegebenen Lehrangebot ausgewählt und gemäß ihren Zulassungsvoraussetzungen belegt werden (insgesamt mindestens 48 CP).

(5) In Modulen aus den Bereichen Praktikum, Proseminar, Seminar, Tutortätigkeit und Sprachkurs sowie gegebenenfalls in anderen oben genannten Bereichen können begrenzte Teilnehmerplätze zur Verfügung stehen. 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) Für Module nach § 5 Absatz 2 Nr. 1, Nr. 2, Nr. 3, Nr. 4 a und b wird einmalig eine nicht bestandene Prüfungsleistung, die beim erstmöglichen Prüfungstermin und vor Ablauf des Regelstudiensemesters abgelegt wird, als "Freiversuch" gewertet (vgl. § 17 Absatz 4 der Prüfungsordnung), falls die Prüfungsleistung unmittelbar, d.h. im gleichen Prüfungszeitraum (vgl. § 13 Absatz 4 der Prüfungsordnung) wiederholt wird. Das Regelstudiensemester für die hier genannten Module beträgt 6.

(8) Eine bestandene Prüfungsleistung der Module nach § 5 Absatz 2 Nr. 1, Nr. 2, Nr. 3, Nr. 4 a-c sowie der Module der Stammvorlesungen (vgl. § 5 Absatz 2 Nr. 10a) kann in der Regelstudienzeit einmalig zur Notenverbesserung im gleichen Prüfungszeitraum (vgl. § 13 Absatz 4 der Prüfungsordnung) wiederholt werden. Bestandene Prüfungsleistungen der Module der Vertiefungsvorlesungen können einmalig zur Notenverbesserung im gleichen Prüfungszeitraum wiederholt werden, falls der Dozent/die Dozentin zu Beginn der Veranstaltung die jeweilige Prüfungsleistung als verbesserbar ausweist. Dabei zählt das bessere Ergebnis. Ansonsten ist die Wiederholung einer bestandenen Prüfungsleistung nicht zulässig.

(9) Die Module der Pflicht-Bereiche werden mindestens einmal im Jahr angeboten. Die Module der Stammvorlesungen im Wahlpflicht-Bereich werden mindestens einmal alle zwei Jahre angeboten. Proseminare, Seminare, sowie die Module aus den Wahlpflichtbereichen "Komplementäre Vorlesungen der Cybersicherheit" und "Kernthemen der Cybersicherheit" können einmalig angeboten werden. Der Studiendekan/Die Studiendekanin stellt in jedem Studienjahr ein hinreichendes Angebot sicher.

(10) Die Unterrichtssprache des Studiengangs ist in der Regel Englisch. Sollte die

Unterrichtssprache abweichen, so wird dies zu Beginn des Moduls/Modulelements bekannt gegeben.

(11) Das Studienangebot in den verschiedenen Wahlpflicht-Bereichen kann für ein oder mehrere Semester modifiziert werden, wobei dies vom Prüfungsausschuss zu genehmigen ist. Diese Module/Modulelemente, ihr Gewicht in CP und ihre Zugehörigkeit zu den Modulbereichen werden jeweils vor Semesterbeginn bekannt gegeben.

(12) 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.

(13) Für Proseminare, Seminare, Übungen 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.

(14) 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 oder die Studiendekanin erstellt auf der Grundlage dieser Studienordnung einen Studienplan, der nähere Angaben über Art und Umfang der Module/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 Lehrangebot in den verschiedenen Bereichen 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 Studiengang Cybersecurity (English).

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

§ 8
Auslandsaufenthalt

Es besteht die Möglichkeit, ein Auslandsstudium zu absolvieren. Der Auslandsaufenthalt sollte nach dem Erbringen der Module der Grundlagen-Bereiche absolviert werden. 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 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
Bachelor-Arbeit und Bachelor-Seminar

(1) Durch die Anfertigung einer Bachelorarbeit soll der Studierende nachweisen, dass er/sie theoretisch-konzeptuelle und/oder angewandte Aufgabenstellungen aus dem Bereich der Cybersicherheit oder verwandten Bereichen eigenständig bearbeiten kann. Die Bearbeitungszeit beträgt drei Monate. Der mit der Bachelor-Arbeit verbundene Aufwand wird mit 12 CP kreditiert.

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

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

§ 10
Inkrafttreten

(1) 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

Wahlpflicht-Bereich "Freie Punkte"				
Tutortätigkeit	Tutortätigkeit	u	4	0
Sprachkurse (max. 6 CP)	mündlich, schriftlich	u	3 / 6	0
Industriepraktikum (max. 6 CP)		u	6	0
Weitere Vorlesungen aus dem Kursangebot der Informatik				
Der Prüfungsausschuss kann das Studienangebot modifizieren.				

Wahlpflicht-Bereich "Kernthemen der Cybersicherheit"				
Advanced Public Key Cryptography	Klausur(en), PVL	b	0	6
Algorithms in Cryptanalysis	Klausur(en), PVL	b	0	6
Generating 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
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.				

Wahlpflicht-Bereich "Komplementäre Themen der Cybersicherheit"				
Automated Debugging	Klausur(en), PVL	b	0	6
Big Data Engineering	Klausur(en), PVL	b	0	6
Elements of Statistical Learning	Klausur(en), PVL	b	0	6
Ethics for Nerds	Klausur(en), PVL	b	0	6
Nebenläufige Programmierung	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
Topics in Algorithmic Data Analysis	Klausur(en), PVL	b	0	6
Der Prüfungsausschuss kann das Studienangebot modifizieren.				

Studienplan

Bachelor-Studiengang Cybersecurity (English)

Bereich	Module	Art der Prüfung	Benotung	CP (ECTS) unb.	CP (ECTS) ben.	WiSe 1 V/Ü/P SWS	WiSe 1 CP	SoSe 2 V/Ü/P SWS	SoSe 2 CP	WiSe 3 V/Ü/P SWS	WiSe 3 CP	SoSe 4 V/Ü/P SWS	SoSe 4 CP	VLF V/Ü/P SWS	VLF CP	WiSe 5 V/Ü/P SWS	WiSe 5 CP	SoSe 6 V/Ü/P SWS	SoSe 6 CP
						Fachsemester													
Grundlagen Mathematik	Mathematics for Comp. Scient. 1	Klausur(en), PVL	b	0	9	4/2/0	9												
	Mathematics for Comp. Scient. 2	Klausur(en), PVL	b	0	9			4/2/0	9										
Grundlagen Informatik	Programming 1	Klausur(en), PVL	b	0	9	4/2/0	9												
	Programming 2	Klausur(en), PVL	b	0	9			4/2/0	9										
	Data Structures and Algorithms	Klausur(en), PVL	b	0	6					2/2/0	6								
	Introduction to Theoretical CS	Klausur(en), PVL	b	0	9					4/2/0	9								
	System Architecture	Klausur(en), PVL	b	0	9							4/2/0	9						
	Statistics Lab	Klausur(en), PVL	b	0	6							2/2/0	6						
	Elements of Machine Learning	Klausur(en), PVL	b	0	6											2/2/0	6		
Praktika	Software Engineering Lab	Projektarbeit	u	9	0									2/0/4	9				
	Cybersecurity Lab	Projektarbeit	u	6	0					1/0/3	6								
Cybersecurity	Foundations of Cybersecurity 1	Klausur(en), PVL	b	0	9	2/2/2	9												
	Foundations of Cybersecurity 2	Klausur(en), PVL	b	0	6			2/2/0	6										
	Cryptography	Klausur(en), PVL	b	0	9							4/2/0	9						
Sprachkurs Deutsch oder Englisch	(Module der Sprachkurse, 3 o. 6 CP)	mündlich, schriftlich	u	6	0				6										
Proseminare Cybersecurity*		mündlich, schriftlich	b	0	5					0/0/2	5								
Seminare Cybersecurity*		mündlich, schriftlich	b	0	7											0/0/3	7		
Kernthemen der Cybersicherheit*	(siehe unten)	Klausur(en), PVL	b	0	12											2/2/0	6	2/2/0	6
Komplementäre Themen der Cybersicherheit.*	(siehe unten)	Klausur(en), PVL	b	0	12							2/2/0	6			2/2/0	6		
"Freie Punkte"	(siehe unten)	divers	u	6	0		3												3
	Bachelor's Seminar	mündlich, schriftlich	b	0	9														9
	Bachelor's Thesis	Bachelor-Arbeit	b	0	12														12
SUMMEN				**27**	**153**	**30**		**30**		**26**		**30**		**9**		**25**		**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, u / unb. = unbenotet, b / ben. = benotet

Anhang B.

Beispielstudienplan Bachelor-Studiengang Cybersecurity (English)

← Semester					CP →
1	Programming 1 (9 CP)	Mathematics for Computer Scientists 1 (9 CP)	Foundations of Cybersecurity 1 (9 CP)	Mandatory Elective (e.g., Introduction to Python, 3 CP)	30
2	Programming 2 (9 CP)	Mathematics for Computer Scientists 2 (9 CP)	Foundations of Cybersecurity 2 (6 CP)	Language Course (6 CP)	30
3	Cybersecurity Lab (6 CP)	Introduction to Theoretical Computer Science (9 CP)	Fundamentals of Data Structures and Algorithms (6 CP)	Cybersecurity Proseminar (5 CP)	26
4	Cryptography (9 CP)	System Architecture (9 CP)	Cybersecurity Complementary Lecture (6 CP)	Statistics Lab (6 CP)	30
	"Software Engineering Lab" (9 CP) offered during the break between summer and winter term				9
5	Advanced Lecture Cybersecurity (6 CP)	Elements of Machine Learning (6 CP)	Cybersecurity Complementary Lecture (6 CP)	Cybersecurity Seminar (7 CP)	25
6	Advanced Lecture Cybersecurity (6 CP)	Bachelor's Thesis (12 CP)	Bachelor's Seminar (9 CP)	Mandatory Elective (e.g., language course, 3 CP)	30