2. Semester: Wahrscheinlichkeitsrechnung und Kryptografie

Modul-Bezeichnung MSc Curriculum 2012	überarbeitet: Mündemann, 20.4.13	Stufen nach Bloom	Wahrscheinlichkeitsrechnung und Kryptografie
englische Modulbezeichnung			Probability calculus and cryptography
Abkürzung			WRK
Beschreibung erstellt	am		18.10.2011
	durch		Schiffer
Niveaustufe			Master
Studiensemester			2
Kreditpunkte			5
Status	Pflichtmodul		Pflichtmodul
	Wahlpflichtmodul		
	Wahlmodul		
Häufigkeit des Angebotes			jedes Semester nach Bedarf der Hochschulen des VFH-Verbundes
Lehrsprache			Deutsch
Autoren			Prof. Dr. Ralf Schiffer (FH Lübeck)
Verantwortliche Hochschule			FH Lübeck
Fachverbunds-leiter(in)			Prof. Dr. Ralf Schiffer (FH Lübeck)
Verantwortliche(r) Lehrende(r) am Standort nach dem Meister-Geselle-Prinzip: ein Lehrender für alle Standorte	Beuth-Hs Berlin		Prof. Dr. Ralf Schiffer (FH Lübeck)
	FH Brandenburg		Prof. Dr. Ralf Schiffer (FH Lübeck)
	FH Emden / Leer		Prof. Dr. Ralf Schiffer (FH Lübeck)
	FH Lübeck		Prof. Dr. Ralf Schiffer (FH Lübeck)
	Ostfalia Hochschule Wolfenbüttel		Prof. Dr. Ralf Schiffer (FH Lübeck)
Lerngebiet			Mathematische und naturwiss.-technische Grundlagen
Erworbene Kenntnisse, Fertigkeiten, Kompetenzen	Formale, algorithmische, mathematische Kompetenzen	Wissen	wissen, wie die heute aktuell eingesetzten kryptographischen Verfahren funktionieren
		Verstehen	verstehen des mathematischen Hintergrunds insbesondere der Public-Key-Kryptographie
		Anwenden	In der Lage sein, für die meisten typischerweise in der Informatik auftretenden Probleme und Fragestellungen aus diesem Bereich sinnvolle Lösungswege zu erkennen und schnell zu den entsprechenden Lösungen zu gelangen.
		Analysieren	
		Synthetisieren	
		Evaluieren, Bewerten	
	Analyse-, Design- und Realisierungs-Kompetenzen	Wissen	
		Verstehen	
		Anwenden	
		Analysieren	
		Synthetisieren	
		Evaluieren, Bewerten	
	Technologische Kompetenzen	Wissen	
		Verstehen	
		Anwenden	
		Analysieren	
		Synthetisieren	
		Evaluieren, Bewerten	

	Fachübergreifende Kompetenzen	Wissen	
		Verstehen	
		Anwenden	
		Analysieren	
		Synthetisieren	
		Evaluieren, Bewerten	
	Methodenkompetenzen	Wissen	
		Verstehen	
		Anwenden	
		Analysieren	
		Synthetisieren	
		Evaluieren, Bewerten	
	Projektmanagement-Kompetenz	Wissen	
		Verstehen	
		Anwenden	
		Analysieren	
		Synthetisieren	
		Evaluieren, Bewerten	
	Soziale Kompetenz und Selbstkompetenz	Wissen	
		Verstehen	
		Anwenden	
		Analysieren	
		Synthetisieren	
		Evaluieren, Bewerten	
Obligatorische Teilnahmevoraussetzungen (nach Prüfungsordnung)			
Fakultative Teilnahmevoraussetzungen			
Medien-/ Lernform			Multimedial aufbereitetes Online-Studienmodul mit zahlreichen interaktiven Anteilen zum Selbststudium mit zeitlich parallel laufender Online-Betreuung (E-Mail, Discussion Board, Chat).
Arbeitsaufwand / work load (jeweils in Zeitstunden summiert)	Pflicht-Präsenzstudium	Vorlesung, Übung, Labor, Seminar u.a.	8h
		Modulprüfung	2h
	Online-Studium (Chat, Audio- / Videokonf. u.a.) incl. studentische Lerngruppen und fakultative Präsenzen		16h
	Erarbeiten der Prüfungsvorleistungen		18h
	Eigenstudium einschl. Prüfungs-vorbereitung		106h
Summe Workload in Stunden			150h
Präsenzinhalte			Zwei Präsenzveranstaltungen zu je 4 Stunden werden als Übungen abgehalten und dienen dazu, den gelernten Stoff durch Lösen anwendungsorientierter Aufgaben zu vertiefen.
Präsenzart	obligatorisch		obligatorisch
	fakultativ		
Präsenzteilnahme	erfordert physische Anwesenheit		Die Vermittlung der Präsenzinhalte sollte möglichst mit physischer Anwesenheit verbunden sein,

	per web-Konferenz möglich		Die Vermittlung der Präsenzinhalte ist per Webkonferenz möglich.
Prüfungsvorleistungen	Präsenzteilnahme		ggf. Teilnahme an der Präsenzveranstaltung.
	Online-Teilnahme		Teilnahme an den Onlineveranstaltungen
	Einsendeaufgaben		Semesterbegleitend werden 3 Einsendeaufgaben gestellt, die im Team als Gruppenaufgaben bearbeitet werden sollen. Eine erfolgreiche Bearbeitung ist Voraussetzung für die Klausurzulassung.
	Hausarbeit / Projektarbeit		
Teilleistungsnachweise			
Prüfungsform	Klausur	(120 Min)	Klausur (120 min)
	Mündliche Prüfung	(30 Min)	
	Hausarbeit mit Kolloquium	(30 Min)	
Benotung			
Literatur			Horst Stöcker (Hrsg.): "Lineare Algebra, Optimierung, Wahrscheinlichkeitstheorie und Statistik", Verlag Harri Deutsch Martin Aigner: „Diskrete Mathematik“, vieweg Thomas Schickinger, Angelika Steger: "Diskrete Strukturen 2", Springer Wolfgang Ertel: "Angewandte Kryptographie", Fachbuchverlag Leipzig Friedrich L. Bauer: "Entzifferte Geheimnisse, Methoden und Maximen der Kryptologie", Springer Evangelos Kranakis: „Primality and Cryptography“, Wiley
Weitere Hinweise			
Studieninhalte des Moduls (Allgemeines zum Modul / Zusammenfassung)			
Kapitelüberschriften / Überschriften der Lerneinheiten			LE 01 Wiederholung mathematischer Grundlagen (5%) Die für das vorliegende Modul wichtigsten Inhalte des Bachelormoduls „Mathematik III“ werden wiederholt und an etlichen Stellen vertieft: Mengenlehre: Mengenoperationen, kartesisches Produkt, Multimengen; Relationen und Funktionen, Binomialkoeffizienten und binomischer Lehrsatz.
			LE 02 Kombinatorik (20%) Grundaufgaben der Kombinatorik: Permutationen, Kombinationen, Variationen; Permutationen von Multimengen, Schubfachprinzip, Siebformel.
			LE 03 Wahrscheinlichkeitsrechnung (45%) Zufall, Ereignisse, Wahrscheinlichkeit, diskrete und kontinuierliche Wahrscheinlichkeitsräume, Prinzip von Laplace, stochastische Unabhängigkeit, bedingte Wahrscheinlichkeiten, Satz von Bayes, Zufallsvariablen, Wahrscheinlichkeitsdichte und verteilung, Erwartungswert, Varianz, Standardabweichung; Diskrete Verteilungen: Bernoulli-Verteilung, Binomialverteilung, geometrische Verteilung, Poisson-Verteilung; Kontinuierliche Verteilungen: Gleichverteilung, Exponentialverteilung, Normalverteilung, zentraler Grenzwertsatz; Anwendungen in Statistik: Statistische Eigenschaften von Stichproben, Standardfehler der Einzelmessung, Standardfehler des Mittelwertes, Schätzfunktionen, Vertrauensintervalle;

		LE 04 Kryptographische Verfahren (30%) Überblick: Kryptographie, Kryptoanalyse, symmetrische und Public-Key-Verfahren, digitale Unterschriften; Grundlegende Begriffe: Chiffrierung, Algorithmus, Schlüssel, monoalphabetische/polyalphabetische Chiffrierungen, monographische/polygraphische Chiffrierungen, Polyphonie, Blockchiffrierung und Stromchiffrierung; Symmetrische Chiffrierverfahren: Substitution und Transposition, Redundanz der Sprache, Häufigkeitsanalyse, Inzidenzindex, Einfluss der Schlüssellänge, Zufallszahlengeneratoren, DES: Data Encryption Standard, AES: Advanced Encryption Standard; Primzahlen und Modulo-Arithmetik: Euklidischer Algorithmus, Eulersche Phi-Funktion, Modulo-Arithmetik, Galois-Felder, Theoreme von Fermat und Euler, Primzahlentests; Public-Key-Chiffrierverfahren: Einwegfunktionen mit/ohne Falltür, Diffie-Hellman-Verfahren, ElGamal-Verfahren, RSA-Verfahren (Rivest/Shamir/Adleman), digitale Unterschriften, PGP: Pretty Good Privacy, Schlüsselmanagement.