12 Wahrscheinlichkeitsrechnung und Kryptographie

Probability Calculation and Cryptography

Semester	2
Credit Points	5
Pflicht/ Wahlpflicht	Pflicht
Häufigkeit des Angebotes/ Verwendbarkeit	Jedes Semester nach Bedarf der Hochschulen im VFH-Verbund
Modulverantwortliche(r)	Sören Werth
Lerngebiet	Grundlagen der Informatik
Teilnahmevoraussetzungen	empfohlen: Erfolgreiche Abschlüsse der Mathematikkurse des Bachelorstudiengangs oder vergleichbare Leistungsnachweise sind wünschenswert.
Lernergebnisse	Die Studierenden können, • die meisten typischerweise in der Informatik auftretenden kombinatorischen Probleme und Fragestellungen lösen. • mit den vermittelten Grundlagen erste zufällige Phänomene modellieren. • auch sehr komplexe Fragestellungen in kleinere Teilprobleme zerlegen und deren Lösungen zu einer Antwort auf die ursprüngliche Frage zusammenfügen. • erklären, wie die heute aktuell eingesetzten kryptographischen Verfahren funktionieren und deren mathematischen Hintergrund, insbesondere der Public-Key-Kryptographie, erläutern. • verschiedene Verschlüsselungsverfahren vergleichend bewerten.
Prüfungsvorleistung	Einsendeaufgabe
Medien-/ Lernform	Multimedial aufbereitetes Online-Studienmodul zum Selbststudium mit zeitlich parallel laufender Online-Betreuung (E-Mail, Foren, Chat, Webkonferenzen, Einsendeaufgaben u. a.)
Arbeitsaufwand	Prüfung: 120 Minuten Selbststudium: 108 h Betreutes Lernen: 30 h Vorbereitung PVL: 12 h
Präsenzinhalte	Zwei Präsenzveranstaltungen zu je 4 Stunden werden als Übungen abgehalten und dienen dazu, den gelernten Stoff durch Lösen anwendungsorientierter Aufgaben zu vertiefen.
Prüfungsform	Klausur (120 min.)

Literatur	Aigner, Martin (2009): Diskrete Mathematik. Mit 600 Übungsaufgaben. 6., korr. Aufl., Nachdr. Wiesbaden: Vieweg + Teubner. Bauer, Friedrich L. (2000): Entzifferte Geheimnisse. Methoden und Maximen der Kryptologie. Berlin, Heidelberg: Springer Berlin Heidelberg. Ertel, Wolfgang; Löhmann, Ekkehard (2018): Angewandte Kryptographie. 5., überarbeitete und erweiterte Auflage. München: Hanser. Paar, Christof; Pelzl, Jan (2016): Kryptographie verständlich. Springer Berlin Heidelberg. Schickinger, Thomas; Steger, Angelika (2002): Diskrete Strukturen 2. Wahrscheinlichkeitstheorie und Statistik. Berlin, Heidelberg: Springer. Stöcker, Horst (1999): "Mathematik, Der Grundkurs, Bd.3, Lineare Algebra, Optimierung, Wahrscheinlichkeitsrechnung und Statistik. Frankfurt am Main: Verlag Harri Deutsch
weitere Hinweise	Dieses Modul wird auf Deutsch angeboten

Studieninhalte
LE 01 Wiederholung mathematischer Grundlagen Die für das vorliegende Modul wichtigsten mathematischen Grundlagen aus dem Bachelorstudiengang werden wiederholt: Mengenlehre: Mengenoperationen, kartesisches Produkt, Multimengen; Relationen und Funktionen, Binomialkoeffizienten und binomischer Lehrsatz. LE 02 Kombinatorik Grundaufgaben der Kombinatorik: Permutationen, Kombinationen, Variationen; Permutationen von Multimengen, Schubfachprinzip, Siebformel. LE 03 Wahrscheinlichkeitsrechnung 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

Überblick: Kryptographie, Kryptoanalyse, symmetrische und Public-Key-Verfahren, digitale Unterschriften; Grundlegende Begriffe: Chiffrierung, Algorithmus, Schlüssel, monoalphabetische/ polyalphabetische Chiffrierungen, monographische/polygraphische Chiffrierungen, Blockchiffrierung und Stromchiffrierung; Symmetrische Chiffrierverfahren: Substitution und Transposition, Redundanz der Sprache, Häufigkeitsanalyse, Einfluss der Schlüssellänge, Zufallszahlengeneratoren, DES: Data Encryption Standard, AES: Advanced Encryption Standard; Primzahlen und Modulo-Arithmetik: Euklidischer Algorithmus, Eulersche Phi-Funktion, Modulo-Arithmetik, Theoreme von Fermat und Euler, Primzahlentests; Public-Key-Chiffrierverfahren: Einwegfunktionen mit/ohne Falltür, Diffie-Hellman-Verfahren, ElGamal-Verfahren, RSA-Verfahren, digitale Unterschriften, Schlüsselmanagement.