8 Grundlagen der Kryptographie

Principles of Cryptography

Semester	2
Dauer (Semester)	einsemestrig
Credit Points	5
Pflicht/ Wahlpflicht	Pflicht
Häufigkeit des Angebotes/ Verwendbarkeit	Jedes Semester nach Bedarf der Hochschulen des VFH-Verbundes.
Modulverantwortliche(r)	Prof. Dr. Christian Forler; Jeweils betreuender Professor/ betreuende Professorin
Teilnahmevoraussetzungen	Grundlagen der Mathematik
Lernergebnisse	In dem Modul werden die mathematischen Grundlagen der Kryptographie vermittelt und geübt. Nach dem erfolgreichen Abschluss sind die Teilnehmenden befähigt kryptographische Bausteine und Verfahren zum Verschlüsseln und Signieren von Daten zu verstehen und deren Sicherheit einzuschätzen. Nach Abschluss des Moduls sind die Studierenden in der Lage • formale Notationen zu verstehen und anzuwenden. • elementare kombinatorische Problemstellungen zu lösen. • grundlegende Algorithmen zur Ganzzahlarithmetik anzuwenden. • den Umgang mit Operationen in Gruppen und Körpern zu beherrschen. • die Funktionsweise von elementaren Verfahren der asymmetrischen Kryptographie zu verstehen. • die mathematische Kernidee von elementaren kryptographischen Verfahren zu erkennen. • sich in weiterführende Gebiete der Kryptographie einzuarbeiten. • grundlegende kryptographische Problemstellungen und Lösungsansätze zu verstehen.
Prüfungsvorleistung	Einsendeaufgabe, Präsenzteilnahme
Medien-/ Lernform	Multimedial aufbereitetes Online-Studienmodul zum Selbststudium mit zeitlich parallel laufender Online-Betreuung (E-Mail, Web-Konferenz, Einsendeaufgaben u. a.) sowie Präsenzphasen
Arbeitsaufwand	Selbststudium: ca. 120 h Webkonferenzteilnahme: ca. 26 h

	Präsenzteilnahme: ca. 4 h Prüfung: 120 Minuten
Präsenzart	erfordert physische Anwesenheit
Präsenzinhalte	Inhaltliche Klärung, Klausurvorbereitung, Besprechung von Übungsaufgaben
Prüfungsform	Klausur (120 min.) oder ggf. mündliche Prüfung
Literatur	Einführung in die Kryptographie, Johannes Buchmann, 2016 Springer Spektrum; 6. Auflage; ISBN 3642397743 Kryptografie verständlich: Ein Lehrbuch für Studierende und Anwender; Christof Paar und Jan Pelzl; 2016 eXamen.press; ISBN 3662492962
weitere Hinweise	Dieses Modul wird auf Deutsch angeboten

Studieninhalte
Teil A: Grundlagen Kapitel 1: Ganze Zahlen Kapitel 2: Algorithmen für Ganzzahlen Kapitel 3: Polynome und Permutationen Kapitel 4: Primzahlen Kapitel 5: Diskrete Wahrscheinlichkeiten und Kombinatorik **Teil B: Kongruenzen und Restklassenringe** Kapitel 6: Restklassen Kapitel 7: Gruppen Kapitel 8: Textbook-RSA und DH-Schlüsselaustausch Kapitel 9: Endliche Körper