14 Angewandte Kryptographie

Applied Cryptography

Semester	3
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. Patrick Felke
Teilnahmevoraussetzungen	Grundlagen der Kryptographie
Lernergebnisse	Nach Abschluss des Moduls sind die Studierenden in der Lage • Algorithmen zur symmetrischen und asymmetrischenm zu verstehen und anzuwenden. • Sicherheitsmodelle zu verstehen und zur Einschätzung der kryptologischen Wertigkeit von asymmetrischen und symmetrischen Verfahren anzuwenden. • moderate Fragestellungen zur Krytologie selbstständig zu verstehen bzw. zu lösen. • den kryptoanalytischen Kern von kryptologischen Fragestellungen zu extrahieren und deren Einfluss auf die Umsetzung zu verstehen. • geeignete Sicherheitsparameter für den jeweiligen praktischen Einsatz auszuwählen. • kryptographische Verfahren und Protokolle zu implementieren und Fallstricke bei der Umsetzung zu erkennen. • sich in weiterführende Gebiete der Kryptologie einzuarbeiten.
Prüfungsvorleistung	Präsenzteilnahme ist verpflichtend für 2 Termine (i.d.R. werden 3 Angeboten)
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. 20 h Präsenzteilnahme: ca. 8 h Prüfung: 120 Minuten
Präsenzart	erfordert physische Anwesenheit

Präsenzinhalte	Inhaltliche Klärung, Klausurvorbereitung, Besprechung von Übungsaufgaben
Prüfungsform	Klausur (120 min.) oder ggf. andere Prüfungsform
Literatur	Kryptografie verständlich: Ein Lehrbuch für Studierende und Anwender; Christof Paar und Jan Pelzl; 2016 eXamen.press; ISBN 3662492962 Cryptography, Theory and Practice; D. Stinson; Chapman and Hall/CRC Press 2005; ISBN 9781584885085 Post-Quantum Cryptography; D. Bernstein, J. Buchmann, E. Dahmen 2008; Springer ISBN 978-3-540-88701-0 Einführung in die Kryptographie, Johannes Buchmann, 2016 Springer Spektrum; 6. Auflage; ISBN 3642397743
weitere Hinweise	Dieses Modul wird auf Deutsch angeboten

Studieninhalte

In dem Modul werden die wesentlichen Grundlagen der angewandten Kryptographie vermittelt und geübt. Die symmetrische und asymmetrische Kryptographie einschließlich der Grundlagen von Hashfunktionen werden vermittelt und geübt. Die mathematischen, algorithmischen und kryptoanalytischen Aspekte werden vorgestellt und diskutiert.
Nach dem erfolgreichen Abschluss sind die Teilnehmenden befähigt kryptographische Bausteine und Verfahren zum Verschlüsseln und Signieren von Daten zu verstehen, deren Sicherheit einzuschätzen und
diese umzusetzen bzw. einzusetzen. Ferner sind sie in der Lage einzelne Angriffe auf Kryptosysteme zu verstehen und diese ggf. umzusetzen.

Lehreinheiten

Einführung in Kryptographie
Zufallszahlengeneratoren
Symmetrische Kryptographie
- Stromchiffren
- Blockchiffren
- Kryptoanalyse

Asymmetrische Kryptographie
- Verschlüsselungsverfahren
- Ausblick Post-Quantum Kryptographie
- Kryptoanalyse

Authentizierung

- Hashfunktionen
- Digitale Signaturen

- Message Authentication Codes (MACs)
- Kryptoanalyse

Schlüsselverteilung/erzeugung
- Symmetrische Verteilung
- Public Key Infrastructure (PKI)
- Zertifikate