63518 Angewandte Kryptografie und Implementierung von Kryptografie

Modulverantwortliche/r	Prof. Dr. Jörg Keller

Dauer des Moduls	ECTS	Workload	Häufigkeit
ein Semester	10	300 Stunden	in jedem Sommersemester

Lehrveranstaltung(en)	Angewandte Kryptografie und Implementierung von Kryptografie
Detaillierter Zeitaufwand	Lektionen: 100 Stunden Einsendearbeiten: 150 Stunden Prüfungsvorbereitung: 50 Stunden
Qualifikationsziele	Studierende kennen die grundlegenden kryptografischen Verfahren, ihre Implementierung sowie die Grenzen solcher Verfahren. Studierende können in Anwendungen geeignete kryptografische Verfahren durch Vergleich auswählen bzw. in Anwendungen vorhandene kryptografische Verfahren bezüglich ihrer Leistung und ihrer Sicherheit beurteilen.
Inhalte	In der angewandten Kryptografie werden kryptografische Primitive wie asymmetrische Verschlüsselung, digitale Signaturen oder kryptografische Protokollen eingesetzt, um für Anwendungsfälle sichere Realisierungen zu finden. Implementiert man kryptografische Algorithmen, so tauchen durch ihre Besonderheiten eine Reihe von Herausforderungen auf, die von Seitenkanälen über lange Zahlendarstellungen bis zu mangelnder Ausnutzung der Breite heutiger Architekturen reicht. Das Modul liefert in beiden Bereichen Grundlagen und zeigt wegen der großen Breite exemplarisch Lösungen auf, die auch in weiteren Anwendungsfällen nützlich oder übertragbar sind.
Inhaltliche Voraussetzung	Modul 63512 "Sicherheit im Internet", 63017 "Datenbanken und Sicherheit im Internet" oder äquivalente Inhalte
Lehr- und Betreuungsformen	Betreuung und Beratung durch Lehrende Lehrveranstaltungsmaterial Einsendeaufgaben mit Korrektur und/oder Musterlösung Internetgestütztes Diskussionsforum Zusatzmaterial Video-Meetings
Anmerkung	Keine
Formale Voraussetzung	keine
Verwendung des Moduls	B.Sc. Informatik M.Sc. Informatik M.Sc. Praktische Informatik

Prüfungsformen	Art der Prüfungsleistung	Voraussetzung
Prüfung	benotete zweistündige Prüfungsklausur	keine
Stellenwert der Note	1/8	