63050 Bachelorseminar Angewandte Kryptographie

Lehrende/r	Prof. Dr. Osmanbey Uzunkol	Modulverantwortliche/r	Prof. Dr. Osmanbey Uzunkol

Dauer des Moduls	ECTS	Workload	Häufigkeit
ein Semester	5	150 Stunden	in jedem Wintersemester

Lehrveranstaltung(en)
Seminar Angewandte Kryptographie

Detaillierter Zeitaufwand
Themenauswahl: 10 Stunden
Erarbeiten der vorgegebenen Literatur und weitere Literaturrecherche, Lesen weiterer Artikel: 40 Stunden
Erstellen der schriftlichen Ausarbeitung: 40 Stunden
Erstellen der Präsentation, Üben des Vortrags: 40 Stunden
Präsenzphase: 20 Stunden

Qualifikationsziele
Nach erfolgreicher Bearbeitung der Themen sind die Studierende in der Lage:
- ein wissenschaftliches Thema aus dem Bereich Kryptographie anhand vorgegebener Literaturhinweise und der evtl. Implementierungen zu erarbeiten,
- selbstständig weitere Literatur zum Thema zu suchen,
- die neuesten praktischen sowie (noch) theoretischen Lösungsansätze zu Problemen der digitalen Sicherheit zu verstehen,
- einige noch nicht effizient lösbare Fragestellungen (open problems) kennenzulernen,
- englische Informatik-Artikel zu lesen und zu verstehen,
- Inhalte strukturieren und mit eigenen Beispielen darzustellen,
- eine schriftliche Ausarbeitung zu erstellen,
- eine Bildschirmpräsentation zu erstellen,
- technische Inhalte vor einem Publikum zu erklären,
- auf Fragen aus dem Publikum angemessen einzugehen.

Inhalte
Im Seminar werden aktuelle Themen aus dem Bereich angewandte Kryptographie behandelt. Dabei liegt das Hauptaugenmerk auf aktuellen Gebieten und Anwendungen wie:
- Post-Quanten-Kryptographie
- Homomorphe Verschlüsselung
- Effizienz und Skalierbarkeit kryptographischer Algorithmen und Protokolle

Inhaltliche Voraussetzung
Modul 63512 "Sicherheit im Internet" und Grundkenntnisse über Mathematik und Programmierung

Lehr- und Betreuungsformen
Zusatzmaterial

Betreuung und Beratung durch Lehrende

Video-Meetings

internetgestütztes Diskussionsforum

Anmerkung
Für die Teilnahme an einem Seminar ist ein gesondertes Anmeldeverfahren im Vorsemester über folgenden Link erforderlich:
https://webregis.fernuni-hagen.de.

Formale Voraussetzung
mindestens neun Pflichtmodulprüfungen sind bestanden

Verwendung des Moduls
B.Sc. Informatik

B.Sc. Wirtschaftsinformatik

Prüfungsformen	Art der Prüfungsleistung	Voraussetzung
Prüfung	benotete Seminarteilnahme (Ausarbeitung und Vortrag)	Keine
Stellenwert der Note	s. PO	