

Modulverantwortliche/r	Prof. Dr. Osmanbey Uzunkol				
	<table border="0"> <tr> <td>Dauer des Moduls ein Semester</td> <td>ECTS 5</td> <td>Workload 150 Stunden</td> <td>Häufigkeit in jedem Wintersemester</td> </tr> </table>	Dauer des Moduls ein Semester	ECTS 5	Workload 150 Stunden	Häufigkeit in jedem Wintersemester
Dauer des Moduls ein Semester	ECTS 5	Workload 150 Stunden	Häufigkeit in jedem Wintersemester		
Lehrveranstaltung(en)	Seminar Angewandte Kryptographie				
Detaillierter Zeitaufwand	<p>Themenauswahl: 10 Stunden</p> <p>Erarbeiten der vorgegebenen Literatur und weitere Literaturrecherche, Lesen weiterer Artikel: 40 Stunden</p> <p>Erstellen der schriftlichen Ausarbeitung: 40 Stunden</p> <p>Erstellen der Präsentation, Üben des Vortrags: 40 Stunden</p> <p>Präsenzphase: 20 Stunden</p>				
Qualifikationsziele	<p>Nach erfolgreicher Bearbeitung der Themen sind die Studierende in der Lage:</p> <ul style="list-style-type: none"> - 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	<p>Im Seminar werden aktuelle Themen aus dem Bereich angewandte Kryptographie behandelt. Dabei liegt das Hauptaugenmerk auf aktuellen Gebieten und Anwendungen wie:</p> <ul style="list-style-type: none"> - 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	<p>Zusatzmaterial</p> <p>Betreuung und Beratung durch Lehrende</p> <p>Video-Meetings</p> <p>internetgestütztes Diskussionsforum</p>				
Anmerkung	<p>Für die Teilnahme an einem Seminar ist ein gesondertes Anmeldeverfahren im Vorsemester über folgenden Link erforderlich:</p> <p>https://webregis.fernuni-hagen.de.</p>				
Formale Voraussetzung	mindestens neun Pflichtmodulprüfungen sind bestanden				
Verwendung des Moduls	<p>B.Sc. Informatik</p> <p>B.Sc. Wirtschaftsinformatik</p>				

Prüfungsformen

Prüfung

Stellenwert
der Note

s. PO

Art der Prüfungsleistung

benotete Seminarteilnahme
(Ausarbeitung und Vortrag)

Voraussetzung

Keine