

Ruhr-Universität Bochum (RUB)

Mikromodulnummer	3025																			
Studienprogramm	Zertifikatsprogramm																			
Mikromodulbezeichnung:	Digitale Signaturen																			
Modulverantwortliche(r):	Prof. Dr. Christof Paar																			
Dozent(in):	Prof. Dr. Christof Paar, Christopher Späth, Sebastian Lauer																			
Sprache:	Deutsch																			
Zeitaufwand insgesamt für Selbststudium, Lehre, Übungsaufgaben etc.	<table border="1"> <tr> <td>Präsenzstudium: davon Prüfung und Prüfungsvorbereitung:</td> <td>0</td> <td>Zeitstunden Zeitstunden</td> </tr> <tr> <td>Fernstudienanteil:</td> <td>30</td> <td>Zeitstunden</td> </tr> <tr> <td> davon Selbststudium:</td> <td>20</td> <td>Zeitstunden</td> </tr> <tr> <td> davon Aufgaben:</td> <td>8</td> <td>Zeitstunden</td> </tr> <tr> <td> davon Online-Betreuung:</td> <td>2</td> <td>Zeitstunden</td> </tr> <tr> <td>Summe:</td> <td>30</td> <td>Zeitstunden</td> </tr> </table>		Präsenzstudium: davon Prüfung und Prüfungsvorbereitung:	0	Zeitstunden Zeitstunden	Fernstudienanteil:	30	Zeitstunden	davon Selbststudium:	20	Zeitstunden	davon Aufgaben:	8	Zeitstunden	davon Online-Betreuung:	2	Zeitstunden	Summe:	30	Zeitstunden
Präsenzstudium: davon Prüfung und Prüfungsvorbereitung:	0	Zeitstunden Zeitstunden																		
Fernstudienanteil:	30	Zeitstunden																		
davon Selbststudium:	20	Zeitstunden																		
davon Aufgaben:	8	Zeitstunden																		
davon Online-Betreuung:	2	Zeitstunden																		
Summe:	30	Zeitstunden																		
Leistungspunkte (ETCS)	keine																			
Voraussetzungen:	Einleitungskapitel „Einführung in die Kryptographie“ (Thema: Kryptographie)																			
Lernziele/Kompetenzen	<p>Fachkompetenz: Die Studierenden erlernen die notwendigen mathematischen Grundlagen von modernen kryptographischen Verfahren, die in Folgemodulen vorausgesetzt werden.</p> <p>Methodenkompetenz: Die Studierenden beherrschen den Umgang mit Fachliteratur und können wichtige Informationen eigenständig entnehmen.</p> <p>Sozialkompetenz: Die Studenten tauschen sich über Probleme beim Erarbeiten und Anwenden von neuen Inhalten aus und können problemorientiert diskutieren.</p>																			
Lehrinhalt	Einführung in Digitale Signaturen RSA Signaturen Elgamal Signaturen Digital Signature Algorithmus (DSA) Elliptic Curve Digital Signature Algorithmus (ECDSA)																			
Studien- und Prüfungsleistungen:	keine																			
Medienformen:	Onlineveranstaltung: Vorlesung, flexible Vertiefung wichtiger Themen, Lernen im Dialog, Übung, Schriftlicher und elektronischer Studienbrief																			
Literatur:	Weitere Literatur wird in der Lehrveranstaltung bekannt gegeben.																			