Theoretische Informatik (W3WI_SE301)

Formale Angaben zum Modul		
Studiengang	**Studienrichtung**	**Vertiefung**
-	Software Engineering	-

Modulbezeichnung	Sprache	Nummer	Version	Modulverantwortlicher
Theoretische Informatik	Deutsch/Englisch	W3WI_SE301	1	Baum, Prof. Dr. Ulrich; Lörrach Ratz, Prof. Dr. Dietmar; Karlsruhe

Verortung des Moduls im Studienverlauf			
Semester	**Voraussetzungen für die Teilnahme**	**Modulart**	**Moduldauer**
2. Stj.		Studienrichtungskernmodul	2

Eingesetzte Lehr- und Prüfungsformen	
Lehrformen	Vorlesung, Übung, Laborübung
Lehrmethoden	-

Prüfungsleistung	Prüfungsumfang (in min)
Klausur oder Mündliche Prüfung	-
Bestandteile Kombinierte Prüfungsleistung	
-	

Workload und ECTS			
Workload insgesamt (in h)	**davon Präsenzzeit (in h)**	**davon Selbststudium (in h)**	**ECTS-Punkte**
150,0	55,0	95,0	5

Qualifikationsziele und Kompetenzen	
Fachkompetenz	Die Studierenden kennen grundlegende Konzepte, Begriffe und Zusammenhänge aus den Teilgebieten formale Sprachen, Automaten, Berechenbarkeit und Komplexität. Sie haben grundlegende Kenntnisse in den Bereichen IT-Sicherheit und Kryptographie, Verschlüsselungstechniken und Netzwerksicherheit.
Methodenkompetenz	Die Studierenden können mit formalen Sprachen umgehen, reguläre Ausdrücke erstellen und anwenden, Automaten verstehen und programmieren, die Komplexität von Problemen bestimmen bzw. berechnen. Außerdem können sie Szenarien zur IT-Sicherheit beurteilen und geeignete Schutzmaßnahmen auswählen und anwenden.
Personale und Soziale Kompetenz	Die Studierenden erkennen die Stärken und Grenzen der vorgestellten Formalisierungen und können Probleme selbständig analysieren und bewerten. Sie sind mit den Grundzügen der IT-Sicherheit vertraut und in der Lage, für den Einsatz an geeigneten sicherheitstechnischen Verfahren gegen Angriffe zu argumentieren.
Übergreifende Handlungskompetenz	Die Studierenden können Formalisierungen auf Probleme in der Praxis anwenden sowie Probleme auf ihre Komplexität und Berechenbarkeit prüfen. Sie können Konzepte der Informatik mit theoretischen Modellen analysieren und IT-Sicherheit einschätzen sowie Lösungswege finden, um Angriffe zu verhindern.

Lerneinheiten und Inhalte		
Lehr- und Lerneinheiten	**Präsenz**	**Selbststudium**
Einführung in die Theoretische Informatik	**28,0**	**47,0**
- Formale Sprachen: Sprache und Grammatik (reguläre, kontextfreie, kontextsensitive Sprachen), reguläre Ausdrücke - Automaten: endliche Automaten, Kellerautomaten, Automaten und reguläre Sprachen - Berechenbarkeit: Berechnungsmodelle (z.B. Turing-Maschinen), berechenbare und nicht berechenbare Funktionen, primitiv-rekursive Funktionen. - Komplexitätstheorie: Komplexität von Problemen, Entscheidungsprobleme, NP-vollständige Probleme.		
IT-Sicherheit und Kryptographie	**27,0**	**48,0**
- Grundbegriffe der IT-Sicherheit: Schutzziele, Angreifer und Angriffe, ökonomische Aspekte - Netzwerk- und Softwaresicherheit, Sicherheitsmodelle - Grundlegende kryptographische Verfahren - Hashfunktionen, digitale Signaturen und Zertifikate - Schlüsselmanagement und Schlüsselaustausch - Authentifikation, digitale Identität, Zugriffskontrolle		

Besonderheiten und Voraussetzungen

Besonderheiten

-

Voraussetzungen

-

Literatur

- Eckert, C.: IT-Sicherheit: Konzepte –Verfahren –Protokolle, De Gruyter Oldenbourg, München.
- Hoffmann, D. W.: Theoretische Informatik, Hanser, München.
- Hromkovic, J.: Theoretische Informatik, Springer-Vieweg, Wien.
- Kappes, M.: Netzwerk-und Datensicherheit, Springer, Wien.
- Schöning, U.: Theoretische Informatik – kurzgefasst, Spektrum, Heidelberg.
- Schwenk, J.: Sicherheit und Kryptographie im Internet, Springer-Vieweg, Wien.
- Stallings, W.: Network Security Essentials, Pearson, London., Springer-Vieweg, Wien.
- Stallings, W.: Network Security Essentials, Pearson, London.