

Modulhandbuch MaTIN2012_Kryptographie

Modul

Anerkennbare Lehrveranstaltung (LV)

Organisation

Modulprüfung

Prüfungselemente

Vorlesung / Übung

Praktikum

Verantwortlich: Prof. Dr. Knospe

Modul

Anerkennbare Lehrveranstaltung (LV)

- F07 KRY

Organisation

Bezeichnung		Zuordnung		Einordnung ins Curriculum		Version	
Lang	MaTIN2012_Kryptographie	Studiengang	MaTIN2012	Fachsemester	1	erstellt	2013-06-26
MID	MaTIN2012_KRY	Studienrichtung	alle	Pflicht		VID	1
MPID		Wissensgebiete	VGMT	Wahl	WPMT	gültig ab	WS 2012/13
						gültig bis	

Zeugnistext

de

Kryptographie

en

Cryptography

Unterrichtssprache

Deutsch, Englisch

Modulprüfung

Form der Modulprüfung	
sK	schriftliche Modulprüfung

Beiträge ECTS-CP aus Wissensgebieten	
VGMT	5
Summe	5

Aufwand [h]: 150

Prüfungselemente

Vorlesung / Übung

Form Kompetenznachweis	
bÜA	wöchentlich Übungsaufgaben lösen (Hausaufgaben)

Beitrag zum Modulergebnis	
bÜA	unbenotet

Spezifische Lernziele

Lerninhalte (Kenntnisse)

- Einführung, Begriffe, Definitionen, Geschichte (PFK2, PFK3)
- Grundlagen der Zahlentheorie und Algebra (PFK2)
- Kryptographische Systeme und Klassische Chiffren (PFK2, PFK3)
- Sicherheit von Chiffren, Angriffe, Informationstheorie, perfekte und praktische Sicherheit, Komplexität (PFK2, PFK3, PFK4)
- Symmetrische Chiffren, Blockchiffren, Betriebsmodi, Stromchiffren (PFK2, PFK3, PFK4)
- Public-Key Verfahren, Schlüsselvereinbarung, asymmetrische Verschlüsselung (PFK2, PFK3, PFK4)
- Hashfunktionen, Signaturen, Nachrichtenauthentisierung (PFK2, PFK3)

Fertigkeiten

- Allgemeine Grundlagen (PFK3)
 - Bedeutung und Ziele der Kryptographie erklären
 - Bezug zu Sicherheitszielen herstellen
 - Kryptographische Methoden auswählen
- Mathematische Grundlagen (PFK2)
 - mit Restklassen ganzer Zahlen rechnen
 - Gruppen, Ringe, Restklassenringe verstehen und darstellen
 - Gruppen- und Elementordnungen berechnen
 - Kleinen Satz von Fermat verstehen
 - Polynome und Endliche Körper verwenden
 - Algorithmen verstehen und anwenden
 - Erweiterter Euklidischer Algorithmus
 - Chinesischer Restsatz
 - Polynomdivision über endlichen Körpern
 - Matrizen zur Darstellung von linearen Abbildungen über Ringen verwenden
- Klassische Verfahren kennen und ihre Kryptoanalyse durchführen (PFK2, PFK3)
 - Transposition
 - Monoalphabetisch
 - Polyalphabetisch
 - Vigenere Chiffre
 - Polygramme Substitutionschiffren
 - Affine Chiffren
- Sicherheit von Verfahren bewerten (PFK3, PFK4)
 - Verschiedene Angriffsformen kennen
 - Entropie berechnen
 - Perfekte und praktische Sicherheit, Konfusion, Diffusion analysieren
 - Komplexität von Verfahren und Angriffen gewichten
- Symmetrische Verfahren anwenden (PFK2, PFK3, PFK4)
 - Betriebsmodi unterscheiden und anwenden
 - AES Verfahren verstehen
 - Lineare Operationen
 - S-Box, SubBytes Operation
 - DES Verfahren verstehen
 - Feisteltransformation
 - Feistelfunktion bei DES
 - S-Boxen
 - Schieberegister analysieren
 - Rückkopplungspolynom untersuchen
 - Stromchiffren verwenden
 - Sicherheit der symmetrischen Verfahren bewerten

- Public-Key Verfahren verwenden (PFK2, PFK3, PFK4)
 - Verfahren zur Erzeugung großer Primzahlen kennen
 - RSA und ElGamal Verfahren durchführen
 - Diffie-Hellmann Schlüsselvereinbarung anwenden
 - Grundlagen der Elliptische-Kurven-Kryptographie kennen
 - Voraussetzungen der Public-Key Verfahren kennen und ihre Sicherheit bewerten
- Verfahren der Integritätssicherung verwenden (PFK2, PFK3)
 - Anforderungen an Hashfunktionen verstehen
 - Realisierungen von Hashfunktionen kennen
 - Signaturverfahren anwenden
 - Message Authentication Codes verstehen

Exemplarische inhaltliche Operationalisierung

- Algebraische und zahlentheoretische Grundlagen
- Symmetrische Verschlüsselungsverfahren
- Public-Key Verfahren
- Hashfunktionen, Signaturen, Message Authentication Codes

Praktikum

Form Kompetenznachweis	
bSZ	Testat und individuelle Lernstandsrückmeldung

Beitrag zum Modulergebnis	
bSZ	Voraussetzung für die Teilnahme an der Modulprüfung

Spezifische Lernziele

Fertigkeiten

- Zahlentheoretische Verfahren und Algorithmen umsetzen (PFK2, PFK4)
- Kryptographische Verfahren implementieren und untersuchen (PFK3, PFK4, PFK5, PFK6, PSK3)
 - RSA Verschlüsselung
 - AES Verschlüsselung
 - Operationsmodi vergleichen
 - Sicherheit untersuchen
- Kryptographische Libraries verwenden (PFK4, PFK6)
- Kryptographische Verfahren in C und Java implementieren (PFK4, PFK5)

Handlungskompetenz demonstrieren

- Komplexe Systeme entwickeln (PFK4, PSK3)
- Kryptographische Verfahren einordnen und bewerten (PFK3)

Exemplarische inhaltliche Operationalisierung

- Algorithmen aus Zahlentheorie und Algebra verwenden
- Kryptographische Verfahren implementieren

Das Urheberrecht © liegt bei den mitwirkenden Autoren. Alle Inhalte dieser Kollaborations-Plattform sind Eigentum der Autoren.

Ideen, Anfragen oder Probleme bezüglich Foswiki? Feedback senden

