Hochschule Aalen	**Fakultät** Elektronik und Informatik	Modulbeschreibung
	Studiengang Informatik	SPO 29
	Modulkoordinator Prof. Dr. Christoph Karg	

Modul-Name	Angewandte Kryptografie	**Modul-Nr : 57937**

CP	SWS	Workload	Kontakt-zeit	Selbst-studium	Angebot Beginn	Sem	Dauer
19	8	300h	120h	180h	☒ Wintersemester ☐ Sommersemester		☐ 1 Semester ☒ 2 Semester Semester

Angestrebter Abschluss	Modultyp (PM/WPM/WM)	Studienabschnitt	Einsatz in Studiengängen
Bachelor of Science	PM - Pflichtmodul	HS - Hauptstudium	

Form der Wissensvermittlung	☒ Vorlesung ☒Übung ☒Labor ☐ Selbststudium ☐Seminar ☐Hausarbeit ☐ Projektarbeit ☐ Sonstiges: Referat, Bericht
Zugangsvoraussetzung	Modul: - Grundlagen der Mathematik - Objektorientierte Programmierung - IT-Sicherheit Prüfung: - erfolgreiches Absolvieren der Praktika - Besuch des Zahlentheorie-Kurses

Enthaltene Teilmodule / Lehrveranstaltungen

Fach-Nr.	Titel des Teilmoduls / Lehrveranstaltung	Lehrende	Art	SWS	CP	Sem	Modul-prüfung Art / Dauer / Benotung
57625	Kryptografische Algorithmen	Prof. Dr. Christoph Karg	V P	4	5	6	PLM 45

Teilmodultyp (PM/WPM/WM)	Studienabschnitt	Einsatz in Studiengängen
PM - Pflichtveranstaltung	HS - Hauptstudium	

Fach-Nr.	Titel des Teilmoduls / Lehrveranstaltung	Lehrende	Art	SWS	CP	Sem
57722	Kryptografische Protokolle	Prof. Dr. Christoph Karg	V L	4	5	7

Teilmodultyp (PM/WPM/WM)	Studienabschnitt	Einsatz in Studiengängen
PM - Pflichtveranstaltung	HS - Hauptstudium	

Zugelassene Hilfsmittel	keine

Lernziele / Kompetenzen

Allgemeines:
Lernziel des Modules ist die Vermittlung der wichtigsten in der Praxis verwendeten kryptografischen Algorithmen und Protokolle. Ein Teilnehmer ist nach Besuch der obigen Lehrveranstaltungen in der Lage, die in einem Produkt eingesetzten Sicherheitsmechanismen zu verstehen und deren Eignung für diverse Einsatzgebiete zu beurteilen.
57722:
Ziel dieser Veranstaltung ist die Vermittlung der Funktionsweise von kryptografischen Protokollen für die Verteilung und Aushandlung von Schlüsseln sowie dem Nachweis der Identität eines Nutzers. Der Besuch dieser Lehrveranstaltung versetzt den Teilnehmer in die Lage, die in der Praxis eingesetzten Verfahren zu verstehen und bezüglich ihrer Tauglichkeit und Sicherheit zu beurteilen.

Fachkompetenz:
Kenntnisse über Aufbau und Funktionen von kryptografischen Verfahren

Methodenkompetenz:
Theoretische und praktische Kenntnisse zu kryptografischen Verfahren erarbeiten und umsetzen

Sozialkompetenz:
Gruppenarbeit bei den Programmierprojekten

Kompetenzbereich	Schwerpunkt	Teilschwerpunkt	In geringen Anteilen
Fachkompetenz	☒	☐	☐
Methodenkompetenz	☒	☐	☐
Sozialkompetenz	☐	☒	☐

Lehrinhalte

• Klassische Verfahren der Kryptografie
· Klassische Kryptosysteme
· Kryptoanalyse klassischer Kryptosysteme
• Symmetrische Kryptosysteme
· Blockchiffren (DES, 3DES, AES, IDEA, Blowfish)
· Stromchiffren (RC4)
• Asymmetrische Kryptosysteme
· Generierung von Primzahlen
· Das RSA-System
· Kryptosysteme auf Basis diskreter Logarithmen
• Authentisierung und Datenintegrität
· Kryptographische Hashfunktionen (SHA2, SHA3)
· Digitale Signaturen (RSA, DSA)
• Generierung von kryptographischen Parametern
-Zufallszahlengeneratoren
-Generierung von Primzahlen
• Grundlagen zur Erstellung von kryptographischen Protokollen
• Schlüsselverteilung
-Vorausverteilung von Schlüsseln
-Pattern zur Verteilung von Schlüsseln
-Verteilung von Sitzungsschlüsseln
• Schlüsselvereinbarung
-Diffie-Hellman Protokoll
-MTI Key Agreement Protokoll
-Vereinbarung mittels selbstzertizierenden Schlüsseln
• Authentisierungsprotokolle
-Challenge Response Verfahren
-Schnorr Verfahren
-Okamoto Verfahren
-Guillou-Quisquater Verfahren

-Zweifaktorauthentisierung • Elektronisches Geld

Sprache	☒ Deutsch ☐ Englisch ☐ Spanisch ☐ Französisch ☐ Chinesisch ☐ Portugiesisch ☐ Russisch
Literatur	Schmeh: Kryptografie: Verfahren, Protokolle, Infrastrukturen, 2009. Stinson: Cryptography: Theory and Practice, 2005. Schneier: Angewandte Kryptografie, 2005. B. Schneier: Angewandte Kryptographie, Addison Wesley, 1996. N. Ferguson, B. Schneier: Practical Cryptography, Wiley, 2003. A. Beutelspacher, J. Schwenk, K. Wolfenstetter: Moderne Verfahren der Kryptographie, Vieweg, 1995. J. Katz, Y. Lindell: Introduction to Modern Cryptography, Chapman & Hall, 2008. D. Stinson: Cryptography (Theory and Practice), CRC Press, 1995. A. Menezes, P. van Oorschot, S. Vanstone: Handbook of Applied Cryptography, CRC Press, 1997. K. Schmeh: Kryptografie und Public-Key Infrastrukturen im Internet, dpunkt.verlag, 2001. T. Cormen, C. Leiserson, R. Rivest, C. Stein: Introduction to Algorithms, MIT Press, 2001.
Zusammensetzung der Endnote	Die Note wird durch eine mündliche Prüfung über 45 Minuten ermittelt. Die Prüfung ist eine Modulprüfung über die Vorlesungen Kryptografische Algorithmen und Kryptografische Protokolle
Bemerkungen / Sonstiges	Zulassungsvoraussetzung für die Prüfung: erfolgreiche Bearbeitung von Praktika, Teilnahme am Kurs "Zahlentheoretische Grundlagen" (auch für die Teilnahme an den Praktika erforderlich)
Letzte Aktualisierung	28.2.2018 Prof. Dr. Christoph Karg