Kryptographische Implementierungen

Implementation of Cryptography

Modulnummer: ME-707.07

Master

Pflicht/Wahl ☐
Wahl ☒ Basis ☐ Ergänzung ☒
Sonderfall ☐

Zugeordnet zu Masterprofil

	Basis	Ergänzung
Sicherheit und Qualität (SQ)	☐	☒
KI, Kognition, Robotik (KIKR)	☐	☐
Digitale Medien und Interaktion (DMI)	☐	☐

Modulbereich: Praktische und Technische Informatik

Modulteilbereich: 707 Sichere Systeme

Anzahl der SWS

V	UE	K	S	Prak.	Proj.	Σ
2	2	0	0	0	0	4

Kreditpunkte: 6

Turnus: wird i.d.R. alle 2 Semester angeboten

Formale Voraussetzungen: Technische Informatik

Inhaltliche Voraussetzungen: Programmierkenntnisse, Mathematische Grundlagen, Einführung in die Kryptographie

Vorgesehenes Semester: ab 1. Semester

Sprache: Deutsch/Englisch

Ziele:

- Technische Herausforderungen der symmetrischen und asymmetrischen Kryptographie verstehen
- Anforderungen für die Kryptographie praktische Systeme in Hardware und Software (z.B. Server, Smart Cards, RFIDs) kennen
- Effiziente Programmiertechniken für bitorientierte Blockchiffren (symmetrische Kryptographie) erlernen
- Effiziente Algorithmen für Langzahlarithmetik (asymmetrische Kryptographie) erlernen
- Sichere Realisierung kryptographischer Implementierungen gegen physikalische Angreifer gewährleisten können
- Grundlegende und erweiterte Sicherheitsdienste der Kryptographie erlernen

Inhalte:

- Grundlegende Verfahren der symmetrischen und asymmetrischen Kryptographie (Kurzdarstellung)
- Effiziente Implementierung des Data Encryption Standard in Software via Tabellen und Bit-Slicing
- Mathematische Grundlagen (modulare Arithmetik, endliche Körper)
- Effiziente Implementierung des Advanced Encryption Standard (T-Table Implementierung)
- Effiziente Umsetzung von modularer Langzahlarithmetik für RSA und Kryptographie über elliptischen Kurven
- Erweiterte Verfahren zur schnellen Exponentiation und Skalarmultiplikation
- Physikalische Angriffe (Seitenkanalanalyse und Fehlerinjektionsangriffe)
- Gegenmaßnahmen und Programmiertechniken zur Verhinderung physikalischer Angriffe

Unterlagen (Skripte, Literatur, Programme usw.):

- Christof Paar, Jan Pelzl: Understanding Crpytography, Springer-Verlag, 2010.
- Jonathan Katz,Yehuda Lindell, Introduction to Modern Cryptography, CRC PRESS, Boca Raton.

Form der Prüfung:
Die theoretisch erarbeiteten Inhalte der Vorlesung werden in Kleingruppen in vorlesungsbegleitenden Projekten/Workshops auf praktische Weise umgesetzt. Die Ergebnisse dieser Projekte gehen mit 40% in die Gesamtnote jedes Teilnehmers ein. Weiterhin ist ein Fachgespräch (Gewichtung: 60% der Gesamtnote) erfolgreich zu absolvieren.

Arbeitsaufwand

Präsenz	56 h
Übung/Projekte/Prüfungsvorbereitung	124 h
Summe	180 h

Lehrende: Prof. Dr.-Ing. Tim Güneysu	Verantwortlich: Prof. Dr.-Ing. Tim Güneysu