| | |
|---|---|
| Modulbezeichnung | **Kryptographische Implementierungen** |
| Modulverantwortliche(r) | Prof. Dr.-Ing. Tim Güneysu |
| Modulart | Pflicht/Wahl ☐<br>Wahlpflicht ☒ |
| Spezialisierungsbereich | Systemsoftware / Eingebettete Systeme |
| Dauer des Moduls | 1 Semester |
| Kreditpunkte | 6 CP |
| Arbeitsaufwand | Berechnung des Workloads<br>Präsenz 56 h<br>Übung/Projekte/Prüfungsvorbereitung 124 h<br>Summe 180 h |
| Turnus des Moduls | wird i.d.R. alle 2 Semester angeboten |
| Voraussetzung für die Teilnahme | Keine ☐<br>Folgende: Formale Voraussetzungen: Technische InformatikInhaltliche Voraussetzungen: Programmierkenntnisse, Mathematische Grundlagen, Einführung in die Kryptographie |
| Lehr- und Lernformen | Seminar ☐<br>Vorlesung ☒<br>Tutorium ☒<br>Praktikum ☐<br>Projekt ☐ |
| Lernziele | • Technische Herausforderungen der symmetrischen und asymmetrischen Kryptographie verstehen<br>• Anforderungen für die Kryptographie praktische Systeme in Hardware und Software (z.B. Server, Smart Cards, RFIDs) kennen<br>• Effiziente Programmiertechniken für bitorientierte Blockchiffren (symmetrische Kryptographie) erlernen<br>• Effiziente Algorithmen für Langzahlarithmetik (asymmetrische Kryptographie) erlernen<br>• Sichere Realisierung kryptographischer Implementierungen gegen physikalische Angreifer gewährleisten können<br>• Grundlegende und erweiterte Sicherheitsdienste der Kryptographie erlernen |
| Lerninhalte | • Grundlegende Verfahren der symmetrischen und asymmetrischen Kryptographie (Kurzdarstellung)<br>• Effiziente Implementierung des Data Encryption Standard in Software via Tabellen und Bit-Slicing<br>• Mathematische Grundlagen (modulare Arithmetik, endliche Körper)<br>• Effiziente Implementierung des Advanced Encryption Standard (T-Table Implementierung)<br>• Effiziente Umsetzung von modularer Langzahlarithmetik für RSA und Kryptographie über elliptischen Kurven<br>• Erweiterte Verfahren zur schnellen Exponentiation und Skalarmultiplikation<br>• Physikalische Angriffe (Seitenkanalanalyse und Fehlerinjektionsangriffe)<br>• Gegenmaßnahmen und Programmiertechniken zur Verhinderung physikalischer Angriffe |
| Prüfungsformen | 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. |

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