Chair of Security in Information Technology
TUM Department of Electrical and Computer Engineering
Technical University of Munich

Assistant (Student)

Tutor/in: Sichere Implementierung kryptographischer Verfahren

Die Vorlesung Sichere Implementierung kryptographischer Verfahren (SIKA) wird durch eine Übung begleitet, in der vier Programmieraufgaben durchgeführt werden. Zur Unterstützung der Studierenden, zur Betreuung des Seitenkanalmessplatzes und zum Testen der Abgabe-Umgebung wird ein/e Tutor/in gesucht.

Die Programmierübungen beinhalten die Implementierung von AES in C und die Entwicklung verschiedener Angriffe auf RSA und AES in Python. Im Rahmen des Differential Power Analysis(DPA)-Angriffs wird der Stromverbrauch einer Implementierung mit dem Oszilloskop aufgezeichnet. Für die Abgabe und Auswertung der Progammieraufgaben wird dabei die Coderunner-Umgebung aus Moodle verwendet.

Im Rahmen der Tätigkeit können für die Unterstützungbei den Progammieraufgaben feste Sprechzeiten am Lehrstuhl für Sicherheit in der Informationstechnik eingerichtet werden. Zum Testen von der Coderunner-Umgebung sollten die Aufgaben jeweils eine Woche vor dem Übungstermin eigenständig gelöst und abgegeben werden, um mögliche Probleme der Umgebung aufzudecken.

Zeitraum und Stundenanzahl:

Ab 15. Oktober 2020 bis 31. Januar 2021 mit 8-10 Stunden pro Woche, geringfügige Anpassung des Zeitraums und der Stundenzahl möglich.

Prerequisites

- Programmierkenntnisse in C und Python
- Grundverständnis im Umgang mit Messgeräten, z.B. Oszilloskop
- Idealerweise Belegung der SIKA-Vorlesung in einem vorhergehenden Semester
- Eigenständige Arbeitsweise Semester

Contact

Technische Universität München
Lehrstuhl für Sicherheit in der Informationstechnik
Lars Tebelmann
Theresientr. 90, N1010
E-Mail: lars.tebelmann@tum.de

Advisors

Lars Tebelmann