

Engineering Cryptographic Software

General information about this course

Radboud University, Nijmegen, The Netherlands



Winter 2023/24

Some basic information

- ▶ Teacher: **Peter Schwabe**
Office: Mercator I, 3.10 (but most of the time at MPI-SP)
peter@cryptojedi.org
- ▶ Assistant:
 - ▶ **Ronny Wichers-Schreur** <ronny@cs.ru.nl>
- ▶ Lectures from Nov. 7 until Dec. 19
- ▶ Deadline for assignment: Friday, January 19, 2024
- ▶ Resit deadline for assignment: Friday, March 29, 2024

More information about the course

- ▶ Course code NWI-IMC064
- ▶ Lectures: Tuesday, 15:30–17:15 in HG00.616
- ▶ Lab sessions: Thursday 10:30–12:15 in HFML0220
- ▶ No exam
- ▶ 3 EC points
- ▶ Material (slides etc.) online on Brightspace
- ▶ Recommended prerequisite knowledge:
 - ▶ C programming
 - ▶ Course on cryptology

Assignment

- ▶ Programming assignment on embedded CPU
- ▶ Work in groups of 2
- ▶ Assignment grade = course grade
- ▶ More details later...

Course schedule

Date	Lecture/Lab sessions	Assignment
Nov 7	Lecture	Start SW Assignment
Nov 9	Lab session	
Nov 14	Lecture	
Nov 16	Lab session	
Nov 21	Lecture	
Nov 23	Lab session	
Nov 28	Lecture over Zoom	
Nov 30	Lab session	
Dec 5	Lecture	
Dec 7	Lab session	
Dec 12	Lecture (by Amber Sprenkels)	
Dec 14	Lab session	
Dec 19	Lecture	
Jan 19		
Mar 29		