

Engineering Cryptographic Software

General information about this course

Radboud University, Nijmegen, The Netherlands



Winter 2022

Some basic information

- ▶ Teacher: **Peter Schwabe**
Office: Mercator I, 3.10 (but most of the time at MPI-SP)
peter@cryptojedi.org
- ▶ Assistants:
 - ▶ **Ronny Wichers-Schreur** <ronny@cs.ru.nl>
 - ▶ **Ciske Harsema** <C.Harsema@student.ru.nl>
- ▶ Lectures from Nov. 8 until Dec. 20
- ▶ Deadline for assignment: January 20
- ▶ Resit deadline for assignment: March 31

More information about the course

- ▶ Course code NWI-IMC064
- ▶ Lectures: Tuesday, 15:30–17:15 in Transitorium 00.005
- ▶ Lab sessions: Thursday 13:30–15:15 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 8	Lecture	Start SW Assignment
Nov 10	Lab session	
Nov 15	Lecture	
Nov 17	Lab session	
Nov 22	Lecture	
Nov 24	Lab session	
Nov 29	Lecture over Zoom	
Dec 1	Lab session	
Dec 6	Lecture over Zoom	
Dec 8	Lab session	
Dec 13	Lecture	
Dec 16	Lab session	
Dec 20	Lecture	
Jan 20		
Mar 31		Resit Deadline SW Assignment