Cryptographic Engineering

General information about this course

Radboud University, Nijmegen, The Netherlands

Spring 2021

Two parts to this course

Part I: Engineering crypto software

- Teacher: **Peter Schwabe**
  Office: Mercator I, 3.11b
  peter@cryptojedi.org
- Assistant: **Denisa Greconici**
  Office: Mercator I, 3.11b
  D.Greconici@cs.ru.nl
- Lectures from Jan. 25 until Mar. 8
- Deadline for assignment: Apr. 9
- Resit deadline for assignment: Jul. 9

Two parts to this course

Part II: Engineering crypto hardware

- Teacher: **Lejla Batina**
  Office: Mercator I, 3.10
  lejla@cs.ru.nl
- Assistant: **Konstantina Miteloudi**
  Office: Mercator I, 3.11
  konstantina.miteloudi@ru.nl
- Lectures from Apr. 12 until May 31
- Deadline for assignment: Jun. 18
- Resit deadline for assignment: Jul. 9

About this course

- **Coordinator: Lejla Batina**
- Lecture/Tutorial: Monday, 15:30–17:30 on Zoom
- No exam
- 6 EC points
- Material (slides etc.) online on Brightspace
- Recommended prerequesite knowledge:
  - C programming
  - TRU/e Cryptology (or similar course)

Computation of final grade

- Two assignments:
  - Software assignment (in Part I)
  - Hardware assignment (in Part II)
- Work on assignments in **groups of 2**
- Final grade $= 0.5SW + 0.5HW$, where
  - $SW =$ grade of the software assignment
  - $HW =$ grade of the hardware assignment
- Additional requirement for passing the course: $SW \geq 5$ and $HW \geq 5$

Schedule for Part I

Date	Lecture/Tutorial	Assignment
Jan 25	Lecture	Start SW Assignment
Feb 1	Lecture/Tutorial	
Feb 8	Lecture	
Feb 15	No Lecture (Carnival)	
Feb 22	Lecture	
Mar 1	Lecture	
Mar 8	Lecture	
Apr 9		Deadline SW Assigment
Jul 9		Resit Deadline SW Assigment

Distribution of Hardware

- SW Assignment needs STM32F4 Discovery board
- Two options for obtaining one

Distribution of Hardware

- SW Assignment needs STM32F4 Discovery board
- Two options for obtaining one

Pick it up on Thursday, Jan. 28

- Enter Mercator I, one student at a time
- Denisa and Konstantina will be around from 10:00 to 16:00
- Pick up board from desk in the reception area
- Return board after the end of the course

Distribution of Hardware

- SW Assignment needs STM32F4 Discovery board
- Two options for obtaining one

Pick it up on Thursday, Jan. 28

- Enter Mercator I, one student at a time
- Denisa and Konstantina will be around from 10:00 to 16:00
- Pick up board from desk in the reception area
- Return board after the end of the course

Buy one yourself

- For example, at RS-Components: `https://nl.rs-online.com/web/p/microcontroller-development-tools/9107951/`
- Additionally need Mini-USB cable and USB-TTL converter, e.g., `https://www.amazon.nl/dp/B089QJZ51Z/ref=sspa_dk_detail_1`