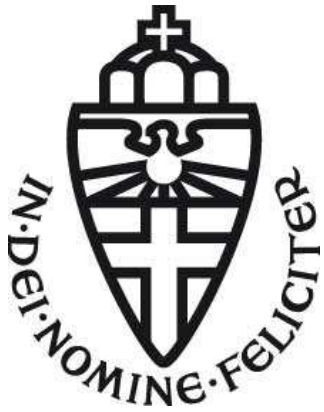
Cryptographic Engineering

General information about this course

Radboud University, Nijmegen, The Netherlands



Spring 2019

Two parts to this course

Part I: Engineering crypto software

- Teacher: **Peter Schwabe**
  Office: Mercator I, 3.02
  peter@cryptojedi.org
- Assistant: **Matthias Kannwischer**
  Office: Mercator I, 3.11b
  matthias@kannwischer.eu
- Lectures from Jan. 28 until Mar. 11
- Deadline for assignment: Apr. 5

Part II: Engineering crypto hardware

- Teacher: **Lejla Batina**
  Office: Mercator I, 3.15
  lejla@cs.ru.nl
- Assistants: **Pedro Massolino** and **Léo Weissbart**
  Office: Mercator I, 3.17
  P.Massolino@cs.ru.nl

About this course

- Lecture/Tutorial: Monday, 15:30–17:15 in HG00.616
- 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**	
Jan 28	Lecture	Start SW Assignment
Feb 4	Tutorial	
Feb 11	Lecture	
Feb 18	Lecture	
Feb 25	Lecture	
Mar 4	No Lecture (Carnival)	
Mar 11	Lecture	
Apr 5		Deadline SW Assigment