

Cryptographic Engineering

General information about this course

Radboud University, Nijmegen, The Netherlands



Spring 2020

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 Feb. 3 until Mar. 9
- ▶ Deadline for assignment: May. 8
- ▶ Resit deadline for assignment: Jul. 10

Two parts to this course

Part II: Engineering crypto hardware

- ▶ Teacher: **Lejla Batina**
Office: Mercator I, 3.10
lejla@cs.ru.nl
- ▶ Guest Professor: **Patrick Schaumont**
Office: Mercator I, 3.02
Patrick.Schaumont@ru.nl
- ▶ Assistant: **Léo Weissbart**
Office: Mercator I, 3.11
L.Weissbart@cs.ru.nl
- ▶ Lectures from Mar. 16 until Jun. 8
- ▶ Deadline for assignment: Jun. 26
- ▶ Resit deadline for assignment: Jul. 10

About this course

- ▶ **Coordinator: Lejla Batina**
- ▶ Lecture/Tutorial: Monday, 15:30–19:15 in HG00.071
- ▶ Most Mondays only one lecture, i.e., until 17:15
- ▶ No exam
- ▶ 6 EC points
- ▶ Material (slides etc.) online on Brightspace
- ▶ Recommended prerequisite 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	
Feb 3	2 Lectures	Start SW Assignment
Feb 10	2 Lectures	
Feb 17	Lecture (Lejla)	
Feb 24	No Lecture (Carnival)	
Mar 2	Lecture/Tutorial (Matthias)	
Mar 9	Tutorial (Matthias)	
May 8		Deadline SW Assignment
Jul 10		Resit Deadline SW Assignment