NWI-IMC061 Applied Cryptography – Course Manual

Bart Mennink (coordinator), Mercator 1 03.05, b.mennink@cs.ru.nl
Simona Samardjiska (lecturer), Mercator 1 03.18, simonas@cs.ru.nl
Krijn Reijnders (tutorial coordinator), Mercator 1 03.11b, krijn@cs.ru.nl

January 29, 2022

This document serves as a guide for the course of NWI-IMC061 Applied Cryptography (prospectus).

1 Basic Information

Prerequisites. Prerequisite for the course of Applied Cryptography is the course NWI-IBC023 "Introduction to Cryptography."

Obligatory Course Material. The main course material consists of the slides of the lectures. The slides will become available on Brightspace, right after each lecture.

Optional Course Material. The lecture notes for the course "Introduction to Cryptography" serve as optional course material. These lecture notes will be available on Brightspace.

Discord Server. There will be a Discord server set-up for the course; in part as support of the lectures, in part as support for the assignments.

2 Lectures

The course consists of 14 lectures, given by Bart Mennink, Simona Samardjiska, and a couple of guest lecturers (details to be completed). The lectures will be on Wednesdays 10.30–12.15, HG00.071. A detailed course schedule can be found in Section 7. A **tentative** overview of the lectures is given below.

	Date	Topic	Matter
1	Wed 2 Feb 2022	Recap of I2C	security strength, stream ciphers, random oracle, indistinguishability, block ciphers and modes, standardization
2	Wed 9 Feb 2022	Disk Encryption and Message Authentication	disk encryption, MAC functions, universal hash, Wegman-Carter, examples
3	Wed 16 Feb 2022	Authenticated Encryption	authenticated encryption, GCM and intuitive proof, examples
4	Wed 23 Feb 2022	Hash Functions and KDFs	hash functions, history, indifferentiability, sponges, Keccak, NIST standards, KDFs
5	Wed 2 Mar 2022	Keyed Sponges	keyed sponge/duplex, SpongeWrap, examples
6	Wed 9 Mar 2022	Encryption and Signing	Encryption, IND-CPA, IND-CCA, classical CPA secure schemes, Fujisaki-Okamoto transform and proof idea, classical signature schemes, ECDSA
7	Wed 16 Mar 2022	Cryptographic Protocols I	commitment schemes, properties (hiding, binding), examples, challenge-response protocols, zero-knowledge proofs of knowledge, examples
8	Wed 13 Apr 2022	Cryptographic Protocols II	Sigma-protocols, Graph-isomorphism identification protocols, non-interactive zero-knowledge, digital signatures from Fiat-Shamir, examples
9	Wed 20 Apr 2022	Post-Quantum Cryptography I	post-quantum cryptography, key encapsulation mechanisms (KEMs), generic constructions, examples (McEliece, NTRU), hybrid KEMs
10	Wed 11 May 2022	Post-Quantum Cryptography II	signature schemes, examples, one-time signatures, multivariate quadratic signatures
11	Wed 18 May 2022	Selected Topics I	public-key infrastructures
12	Wed 25 May 2022	Selected Topics II	secure messaging, secure video conferencing
13	Wed 1 Jun 2022	Selected Topics III	secure communication
14	Wed 8 Jun 2022	Back-up/Q&A	—

3 Assignments

There will be *no* tutorials for the course. However, there will be assignments at a regular basis. The current plan is to have two assignments regarding symmetric cryptography (lectures 1–5), two assignments regarding public-key and post-quantum cryptography (lectures 6–10), and one assignment regarding the selected topics (lectures 11–13). Coordinator for the assignments is Krijn Reijnders.

The assignments will become available on Brightspace at appropriate moments. Work should be handed in at latest two weeks after availability of the assignment **at 23.59 sharp**, as a single PDF via the assignment module in Brightspace. You are encouraged to work and submit *in pairs*. Detailed information about the availability and deadlines for the assignments can be found in Section 7.

4 Exam

There will be an open-book at-home exam. The exam will be made available before the back-up/Q&A lecture, and the work should be handed in at latest three weeks after the availability of the at-home exam **at 23.59 sharp**, as a single PDF via the assignment module in Brightspace. You have to submit *individually (not in pairs)*.

5 Assessment

Your final grade F for this course will be composed from your assignment grade A (your average score over all assignments) and an open-book (at-home) exam grade E:

$$F = E + \frac{A}{10},$$

with a maximum of 10. To pass the course, E must be at least 5 and F must be at least 6. In other words, E counts as your final grade, with a bonus of at most 1 depending on your assignment grade.

6 Fraud and Plagiarism

The 'Regulations on fraud' of the Radboud University apply to the final written (re-)exam as well as the homework assignments of the course. Homework assignments are to be made and handed in individually. You are allowed to discuss concepts from the course with fellow students, but should not provide or take possession of assignments from last year, answer keys, or model solutions, prior to the deadline of the assignment.

7 Detailed Course Schedule

A detailed schedule for the course is given below. This schedule is tentative, and **changes might occur**. These changes will be clearly communicated.

Week	Date	Time	Room	Event
5	Wed 2 Feb 2022	10.30–12.15	HG00.071	Lecture 1
6	Wed 9 Feb 2022	10.30–12.15	HG00.071	Lecture 2
7	Wed 16 Feb 2022	10.30–12.15	HG00.071	Lecture 3
	Wed 16 Feb 2022	23.59	—	Assignment 1 available
8	Wed 23 Feb 2022	10.30–12.15	HG00.071	Lecture 4
9	Wed 2 Mar 2022	10.30–12.15	HG00.071	Lecture 5
	Wed 2 Mar 2022	23.59	—	Assignment 1 due
	Wed 2 Mar 2022	23.59	—	Assignment 2 available
10	Wed 9 Mar 2022	10.30–12.15	HG00.071	Lecture 6
11	Wed 16 Mar 2022	10.30–12.15	HG00.071	Lecture 7
	Wed 16 Mar 2022	23.59	—	Assignment 2 due
15	Wed 13 Apr 2022	10.30–12.15	HG00.071	Lecture 8
	Wed 13 Apr 2022	23.59	—	Assignment 3 available
16	Wed 20 Apr 2022	10.30–12.15	HG00.071	Lecture 9
19	Wed 11 May 2022	10.30–12.15	HG00.071	Lecture 10
	Wed 11 May 2022	23.59	—	Assignment 3 due
	Wed 11 May 2022	23.59	—	Assignment 4 available
20	Wed 18 May 2022	10.30–12.15	HG00.071	Lecture 11
21	Wed 25 May 2022	10.30–12.15	HG00.071	Lecture 12
	Wed 25 May 2022	23.59	—	Assignment 4 due
	Wed 25 May 2022	23.59	—	Assignment 5 available
22	Wed 1 Jun 2022	10.30–12.15	HG00.071	Lecture 13
23	Wed 8 Jun 2022	10.30–12.15	HG00.071	Lecture 14
	Wed 8 Jun 2022	23.59	—	Assignment 5 due
	Wed 8 Jun 2022	23.59	—	**At-home exam available**
26	Wed 29 Jun 2022	23.59	—	**At-home exam due**