NTNU
Det skapende universitet

Reference group report

Date: 13.11.14

Course code and title: TMA4160 Cryptography

Dates of reference group meetings held: 27.08.14; 08.10.14; 11.11.14

Students who have participated in the reference group. Name and programme of study:

Petter Nyland, MMA
Ludwig Lahmeyer, BMAT
Karianne Sørum, MLREAL

The reference group's report on the quality of the course:

Lectures

- Room switch at the beginning of the semester from S265 to K25 was a good decision as the former room was unsuitable (e.g. no projcetor)
- Writing the theorem/definiton nr. used by the book when lecturing was positively received by the students once it was implicated
- There was a fitting amount of curriculum
- Lecturer responded well when asked questions
- Choosing exam exercises from sets without available solutions was appreciated
- Lectures and blackboard were well structured

Exercises

- A mix of computer and writtene exercises worked well, computer exercises gave some hand on experience
- The intial room (used for exercise classes) F2 was unsuitable as it was an auditorium and change to R4 was appreciated by the students
- Positive that the exercises were always available one week prior to exercise class
- The intial 1 hour exercise class was extended to 2 hours
- A reasonable amount of exercises were given relevant to the current topic(s)

Other

- Well organized webpage and up to date
- Detailed lecture plan made it easy to follow along with the course in case of absence
- The posted guide to Python was useful for students unfamiliar with Python

NTNU
Det skapende universitet

Measures proposed by the reference group:

- Consider changing the exam format, i.e. a short appendix instead of the whole book, in order to evaluate the understanding of the students more easily
- (Continue to) linclude 1-2 motivational speeches (preferably during the semester) to motivate further study in cryptography
- Possibly include more examples (i.e. calculate encryption/decryption) of the different cryptosystems especially classic crypto
- Make sure to avoid long silences while writing long passages on the board
- Consider making a Norwegian to Englisgh dictionary of terms used in the course
- Selected exercises had hints (No solution manuals were given), these hints could be given on more exercises
- Topics in the curriculum not included in the book were for the most part covered by documents posted on the webpage, except for Sigma protocols. It would be nice if all the curriculum was available in a written format.