Cryptography and mathematics - a new line of study

Kristian Ranestad and Kristin Shaw, december 2018

After discussions with Geir Dahl and Arne B Sletsjøe, we suggest that a new line of study (studieretning) is opened in the MAMI-bachelorprogram. It would contain a number of existing courses, and one new one.

The underlined courses are required in the MAMI-program.
https://www.uio.no/studier/program/matematikk-informatikk/index.html
Additional compulsory courses for the study line are in boldface.

This line of study is meant to qualify for masterprograms in mathematics and in informatics. With the required choices it should qualify for a new line of study in cryptography in the master program in mathematics. Depending on the choice of optionals, it should also qualify for any line of study in the master program in mathematics and in the master programs in information security at IFI.

Bachelor:

1. semester: MAT1100, MAT-INF 1100, INF 1900
2. semester: MAT 1110, STK 1100, MEK1100
3. semester: MAT 1120, IN 1910, **IN2120**
4. semester: **MAT 2200, MAT 2250** (new)

In addition we ask the students to take at least one of the following:
MAT 2100/MAT 2400/MAT 2410/MAT 2500

Other relevant, but optional courses are
IN 1150 Logiske emner
MAT 1140 Strukturer og argumenter
MAT 3100 Lineær optimering

IN2010 Algoritmer og datastrukturer
IN 3130 Algoritmer design og effektivitetet
IN2080 Beregninger og kompleksitet

A line of study in cryptography in the master program in mathematics would contain
MAT 4250 Elliptic curves (new)
TEK 4500 Innføring i kryptografi
TEK 5550 Avanserte områder innen kryptologi

Comments:

Maers, Nilsen and Gregersen, all working data-security and crypto, have been asked to comment on the plan (see separate emails). Their answers may be summarized as: Include enough number theory, and preferably also algorithms and complexity in the program.

Elementary number theory appears a bit in several courses. I guess some must be included as part of "finite fields" in MAT2250.
The existing master course in cryptography (TEK 4500) could be included as a recommended option.
On algorithms and complexity we naturally rely on IN-courses (see above plan). This has been discussed with IFI.

Utdanningsleder ved IFI: Forslaget om IN2120 Informasjonssikkerhet som obligatorisk på denne retningen virker fornuftig for at studentene skal få en breddeinnføring i sikkerhet. Både IN1150 og de to algoritme-emnene fremstår også som gode valg. I tillegg kan eventuelt emnet IN2080 Beregninger og kompleksitet vurderes. Eventuelle øvrige informatikkemner avhenger av hvilken profil dere ønsker på programmet.

Requirements for masterprograms at IFI has also been discussed.

Utdanningsleder ved IFI: Skal dette kvalifisere for masterprogrammet i programmering og systemarkitektur, studieretning informasjonssikkerhet, må studentene ha 80 studiepoeng informatikk som inkluderer 30 studiepoeng programmering/algoritmer med minst ett kurs i algoritmer. Det vil si at studentene vil måtte ta IN2010, og ellers fylle alle eller nesten alle valgfrie emner med informatikk. Med dette vil de også kvalifisere til studieretningen programvare. Vi diskuterer om et emne i sikkerhet (IN2120) burde være opptakskrav til informasjonssikkerhet eller ikke.

A new undergraduate discrete mathematics course

For the new undergraduate discrete math course,

"MAT 2250 Discrete mathematics"

we suggest the topics "graph theory, networks, enumerative combinatorics, modular arithmetic, finite fields and coding theory"

and the book

Martin Aigner/ David Kramer: Discrete mathematics.

We have looked at other books, including
Biggs: Discrete mathematics , but find the Aigner/Kramer book clearly better in treatment of our key topics. Biggs is more comprehensive, covering more topics, but less of each.

The Aigner/Kramer book seems to have a reasonable level for a 4th semester course.

Aigner/Kramer contents:

- Pt. 1. Counting
- Ch. 1. Fundamentals
- Ch. 2. Summation
- Ch. 3. Generating functions
- Ch. 4. Counting patterns
- Ch. 5. Asymptotic analysis
- Pt. 2. Graphs and algorithms
- Ch. 6. Graphs
- Ch. 7. Trees
- Ch. 8. Matchings and networks
- Ch. 9. Searching and sorting
- Ch. 10. General optimization methods
- Pt. 3. Algebraic systems
- Ch. 11. Boolean algebras
- Ch. 12. Modular arithmetic
- Ch. 13. Coding
- Ch. 14. Cryptography
- Ch. 15. Linear optimization.