Forslag om ny studieretning i MAMI:

Matematikk og informasjonssikkerhet

Studieretningen gir et bredt og solid fundament i matematikk, programmering og informasjonssikkerhet og dermed et godt grunnlag for videre læring i både studie- og i arbeidssammenheng.

Studieretningen gir grunnlag for masterstudier i matematikk og i informasjonssikkerhet.

Oppbygging.

Obligatoriske fellesemner (90 studiepoeng) MAT 1100, MAT-INF 1100, IN 1900, MAT 1110, MEK 1100, STK 1100, MAT 1120, IN 1910, EXPHIL03

Obligatoriske fordypningsemner (40 studiepoeng) MAT 2200, MAT 2250, IN2120, MAT 2100/MAT 2400/MAT 2410/MAT 2500

Utviklingssemester/frie emner (50 studiepoeng)

For å kvalifisere til Ifi's masterprogram i informasjonssikkerhet må de 50 frie studiepoengene velges blant IN-emner: IN 1010, og fire emner til hvorav minst ett på 2000 eller 3000 nivå.

Bakgrunnen for forslaget: Studieretningen gir spesielt grunnlag for masterstudier i kryptografi innenfor masterprogrammene i matematikk og informasjonssikkerhet. Den er imidlertid beregnet til å kvalifisere for flere spesialiseringer innenfor disse programmene. (se vedlagte notat med kommentarer)

Oslo, Februar 2019

Kristian Ranestad og Kristin Shaw

Vedlegg:

-Notat om "Cryptography and mathematics- a new line of study"
-Kommentarer til notatet fra tidligere studenter /forelesere ved MI som arbeider med kryptering/informasjonssikkerhet
-Kommentar fra utdanningsleder IFI

Cryptography and mathematics - a new line of study

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 MAT 2100/MAT 2400/MAT 2410/MAT 2500
. 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 data 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:

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

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

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.

The comments, below, from Maers, Larsen and Gregersen (all working data-security and crypto) 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 could be included as a recommended option.
On algorithms and complexity we would naturally rely on IN-courses (see above plan), but this should also be discussed with the IN-department.

Kristian Ranestad and Kristin Shaw (September/October 2018)

Kommentarer:

Rafael Lukas Maers: Hva angår det nye kurset, så er det (som allerede nevnt) vanskelig å gi tilbakemelding på bakgrunn av en skisse og uten tilgang til den foretrukne pensumboken; men jeg prøver likevel. Erfaringsvis gir MAT2200 gode forkunnskaper for TEK4500, noe som trolig skyldes at begge kursene er innføringsemner. Etterhvert som man graver seg dypere i kryptografien, så vil man fort få behov for både bredere og dypere matematikkunnskaper. Dybden dekkes i stor grad av påfølgende masterkurs i algebra, mens jeg mistenker og håper at hensikten med det nye kurset er å dekke i bredden.

Jeg hadde utvilsomt hatt nytte av bedre forkunnskaper i endelige kropper og snublet faktisk over kodeteori underveis i arbeidet masteroppgaven min. Således virker emnevalget relevant for meg, men det eneste jeg savner er mer klassisk tallteori. Det gir en dypere forståelse av kryptografien, og er så vidt meg bekjent ikke dekket nevneverdig i noen av emnene i den foreslåtte planen.

Med vennlig hilsen
Rafael Lukas Maers

Leif Nilsen: Først av alt, flott med dette initiativet! Jeg er sikker på at dette vil gi et godt teoretisk grunnlag for studenter som ønsker å fordype seg i kryptografi. Jeg sendte eposten også til Thomas Gregersen, og kopierer også inn hans svar.
Min første reaksjon var at jeg gjerne skulle sett litt mer av:

- Algoritmer og kompleksitet, litt om kompleksitetsklasser/automata/Turingmaskiner/reduserbarhet
- Grunnleggende tallteori
- Litt mer om endelige kropper enn det som man vanligvis finner i innføringskurs i algebra (er vel tenkt inn i det nye emnet?)

Thomas sin kommentar om elliptiske kurver er relevant, men for meg er dette fortsatt et interessant område for kryptoanvendelser. Fokus på kvanteresistent krypto har jo endret på dette, men vi ser anvendelser innen isogenibaserte løsninger, primtallstesting og faktorisering. Skulle vi ta hensyn til post-kvantekrypto burde en første innføring i latticeteori være nyttig (geometrisk tallteori)?

Har så vidt "googlet" litt rundt læreboka som er foreslått i Diskret Matematikk. Kan se ut som Aigner har fått litt mer blandet mottagelse enn Biggs.

Hold meg gjerne inne i diskusjonen videre rundt denne studieretningen!

mvh
Leif

Thomas Gregersen: Mitt første innfall var kanskje at det mangler et kurs i algoritmer/kompleksitetsteori i masterretningen for kryptografi. Det er vel strengt tatt en god idé at man behersker dette litt før man tar fatt på videre studier. Kanskje er det derfor å anbefale at kursene IN2010/3130 inngår. Det er i alle fall en tanke.

Når det gjelder kurset om elliptiske kurver er det selvfølgelig fint å kjenne til, men med tanke på hvor dagens kryptosystemer er på vei, tviler jeg på at dette blir nødvendig. I praksis er det mange som unngår å bruke ECC som primitiv av historiske grunner og noen (viktige organer) anbefaler alle som planla et skifte fra RSA til ECC å vente til PQC-primitivene er ferdige. Jeg ville ha tenkt på dette som et spesialfelt som eventuelt spares til en som vil studere SIDH. Men dette er fortsatt marginalt i praksis.

Mvh,
Thomas G

Ragnhild Kobro Runde (Utdanningsleder, IFI): Jeg har sett på forslaget deres.
Har jeg oppfattet det riktig at dere foreslår en bachelor studieretning i kryptografi som ikke egentlig inneholder noe kryptografi? Det virker noe spesielt, hva er eventuelt begrunnelsen for det?

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.

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.

Hilsen Ragnhild.