Kursplan

för kurs på avancerad nivå

Krypteringsmatematik **7.5 Högskolepoäng**
Mathematics of cryptography **7.5 ECTS credits**

Kurskod:	MM7018
Gäller från:	HT 2019
Fastställd:	2010-05-17
Ändrad:	2010-05-17
Institution	Matematiska institutionen
Huvudområde:	Matematik
Fördjupning:	A1N - Avancerad nivå, har endast kurs/er på grundnivå som förkunskapskrav

Beslut
Denna kursplan är fastställd av Naturvetenskapliga fakultetsnämnden 2010-05-17.
Teknisk revidering av Studentavdelningen 2019-04-25.

Förkunskapskrav och andra villkor för tillträde till kursen
Kunskaper motsvarande 60 högskolepoäng i matematik där Linjär algebra II GN 7,5 hp och Matematisk analys III GN 7,5 hp ingår. Engelska 6.

Kursens uppläggning

Provkod	Benämning	Högskolepoäng
F718	Krypteringsmatematik	7.5

Kursens innehåll
Kursen behandlar de moderna metoder för kryptering som är basen för säker elektronisk kommunikation, samt metoder för att forcera dessa. Fokus är på de matematiska grunderna inom talteori, algebraisk geometri och statistik och hur dessa används för kryptering. Kursen är av intresse för den som sysslar med säkerhetsaspekter på elektronisk kommunikation, men även för den som vill se en av de mer spektakulära moderna tillämpningarna av matematik.

Förväntade studieresultat
Efter att ha genomgått kursen förväntas studenten kunna
• redogöra för ett antal kryptosystem som RSA och ElGamal, kryptering med elliptiska kurvor och de olika metoder som används för att dekryptera dessa
• redogöra för väsentliga tekniker och resultat i elementär talteori, kombinatorik, informationsteori, statistik och algebraisk geometri och dessas relevans för tillämpningar i kryptologi.

Undervisning
Undervisningen består huvudsakligen av föreläsningar. Inlämningsuppgifter och gruppseminarier kan förekomma. Deltagande i eventuella seminarier är obligatoriskt. Om särskilda skäl föreligger kan examinator efter samråd med vederbörande lärare medge den studerande befrielse från skyldigheten att delta i vissa obligatoriska moment.

Kunskapskontroll och examination
a. Kursen examineras på följande vis: Kunskapskontroll sker genom skriftligt och/eller muntligt prov. Skriftliga och/eller muntliga redovisningar av gruppuppgifter och övningar.

b. Betygssättning sker enligt sjugradig målrelaterad betygsskala:
A = Utmärkt
B = Mycket bra
C = Bra
D = Tillfredsställande
E = Tillräckligt
Fx = Otillräckligt
F = Helt Otillräckligt

c. Kursens betygskriterier delas ut vid kursstart.

d. För godkänt krävs lägst betygsgraden E samt godkända inlämningsuppgifter, seminarier och laborationer (om dessa används).

e. Studerande som underkänts i ordinarie prov har rätt att genomgå minst fyra ytterligare prov så länge kursen ges. Med prov jämställs också andra obligatoriska kursdelar. Studerande som godkänts på prov får inte genomgå förnyat prov för högre betyg. Studerande som underkänts på prov två gånger har rätt att begära att annan lärare utses för att bestämma betyg på kursen. Framställan härom ska göras till institutionsstyrelsen.

Övergångsbestämmelser

Studerande kan begära att examination genomförs enligt denna kursplan även efter det att den upphört att gälla, dock högst tre gånger under en tvåårsperiod efter det att undervisning på kursen upphört. Framställan härom ska göras till institutionsstyrelsen.

Övrigt

Kursen ges som fristående kurs.

Kurslitteratur

Kurslitteratur beslutas av institutionsstyrelsen och redovisas därefter i bilaga till kursplanen.