Matematiska institutionen

Stockholms universitet

Kursplan

för kurs på avancerad nivå

Krypteringsmatematik **7.5 Högskolepoäng**

Mathematics of cryptography **7.5 ECTS credits**

Kurskod:	MM7029
Gäller från:	VT 2021
Fastställd:	2020-08-17
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 vid Stockholms universitet 2020-08-17.

Förkunskapskrav och andra villkor för tillträde till kursen

För tillträde till kursen krävs kunskaper motsvarande

1. Matematik II - Algebra och kombinatorik , 7,5 hp (MM5013) och Programmeringsteknik för matematiker GN, 7,5 hp (DA2004).

eller

2. Kandidatexamen där minst 60 hp i matematik, matematisk statistik eller datalogi ska ingå.

Engelska 6 eller motsvarande.

Kursens uppläggning

Provkod	Benämning	Högskolepoäng
LABO	Datorlaborationer	2.5
TENT	Teori	5

Kursens innehåll

Kursen behandlar grundläggande begrepp inom kryptering och de matematiska problem, med tillhörande matematisk teori, som ligger till grund för tillämpningar inom asymmetrisk kryptologi som RSA (både som krypto och som digital signatur), DH, El Gamal, ECDH, ECDSA och Miller-Rabin.
Olika algoritmer (för att lösa dessa matematiska problem) studeras med fokus på komplexitet.
Algoritmer som behandlas inkluderar binär exponentiering, Shanks baby-step giant-step, Pohlig-Hellman, Pollards p-1, QS, indexkalkyl, Pollards rho och Lenstras ECM.

Förväntade studieresultat

Efter att ha genomgått kursen förväntas studenten kunna

Del 1, Teori, 5 hp:
-förklara grundläggande begrepp inom kryptologi
-förklara de matematiska problem och den tillhörande matematiska teori som ligger till grund för de asymmetriska kryptologiska tillämpningar som behandlas i kursen, samt kunna använda denna teori för att lösa problem

-förklara de algoritmer som behandlas i kursen, samt redogöra för och bevisa deras komplexitet

Del 2, Datorlaborationer, 2,5 hp:
-implementera de enklare av dessa algoritmer med matematisk mjukvara samt göra enklare analyser av deras komplexitet i praktiken.

Undervisning

Undervisningen består av föreläsningar, övningar och datorlaborationer. Kursen ges på engelska.

Kunskapskontroll och examination

a. Kursen examineras på följande vis:

Kunskapskontroll för del 1, Teori, sker genom skriftligt tentamen
Kunskapskontroll för del 2, Datorlaborationer, sker genom skriftlig redovisning

För godkänt slutbetyg krävs godkänt betyg på samtliga ingående delar.

Examinationen sker på engelska.

Examinator har möjlighet att besluta om anpassad eller alternativ examination för studenter med funktionsnedsättning.

b. Kursen har ingen obligatorisk undervisning.

c. Kursens slutbetyg sätts genom sjugradig målrelaterad skala:
A = Utmärkt
B = Mycket bra
C = Bra
D = Tillfredsställande
E = Tillräckligt
Fx = Underkänd, något mer arbete krävs
F = Underkänd, mycket mer arbete krävs

Betygsättning av del 1, Teori, görs enligt sjugradig målrelaterad skala.
Betygsättning av del 2, Datorlaborationer, görs enligt tvågradig skala: godkänd (G) eller underkänd (U).

d. Kursens betygskriterier delas ut vid kursstart.

e. Studerande som underkänts i ordinarie prov har rätt att genomgå ytterligare prov så länge kursen ges. Antalet provtillfällen är inte begränsat. Med prov jämställs också andra obligatoriska kursdelar. Studerande som godkänts på prov får inte genomgå förnyat prov för högre betyg. En student, som utan godkänt resultat har genomgått två prov för en kurs eller en del av en kurs, har rätt att få en annan examinator utsedd, om inte särskilda skäl talar mot det. Framställan härom ska göras till institutionsstyrelsen. Kursen har minst tre examinationstillfällen per läsår de år då undervisning ges. För de läsår som kursen inte ges erbjuds minst ett examinationstillfälle.

f. Möjlighet till komplettering av betyget Fx upp till godkänt betyg ges inte på denna kurs.

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 kursen har avvecklats. Framställan härom ska göras till institutionsstyrelsen. Bestämmelsen gäller även vid revidering av kursplanen och revidering av kurslitteratur.

Begränsningar

Kursen kan ej ingå i examen tillsammans med kursen Krypteringsmatematik (MM7018).

Kurslitteratur

Kurslitteratur beslutas av institutionsstyrelsen och publiceras på Matematiska institutionens webbplats senast 2 månader före kursstart.