Linnéuniversitetet
Kalmar Växjö

Dnr: LNU-2024/2771

Kursplan

Fakulteten för teknik
Institutionen för matematik

4MA923 Kryptering, 7,5 högskolepoäng
Cryptography, 7.5 credits

Huvudområde
Matematik

Ämnesgrupp
Matematik

Nivå
Avancerad nivå

Fördjupning
A1N

Fastställande
Fastställd 2024-07-01.
Kursplanen gäller från och med hösttermin 2024.

Förkunskaper
90 hp i matematik eller datavetenskap inklusive kurserna:
Diskret matematik 1MA912/1MA902/1MA405/1MA462, 7,5 hp eller motsvarande,
Linjär algebra 1MA901/1MA406, 7,5 hp eller motsvarande,
Flervariabelanalys och vektoranalys, 1MA906/1MA465, 7,5 hp eller motsvarande
Inledande programmering, 1DT901/1DV901, 7,5 hp eller motsvarande

Mål

Efter genomgången kurs förväntas studenten kunna:

- redogöra för hur några moderna kryptosystem och digitala signaturer fungerar samt kunna redogöra för deras begränsningar och effektivitet [THE]
- lösa problem och utföra beräkningar inom kryptologi såväl med som utan beräkningsverktyg [COM]

- implementera och analysera kryptologiska algoritmer [IMP]
- analysera och diskutera kryptologins roll i samhället och dess etiska konsekvenser [SOC]

Innehåll

Diskreta logaritmer; ElGamals krypto, Diffie-Hellmans protokoll. RSA-kryptot; primtalsgenerering, faktoriseringsmetoder. Digitala signaturer. Kryptering med elliptiska kurvor. Gitterbaserad kryptering. Kryptologins roll i samhället.

Undervisningsformer

Föreläsningar och semiarier.
Deltagande på seminarierna är obligatoriskt.

Examination

Kursen bedöms med betygen A, B, C, D, E eller F.

Betyget A utgör det högsta betygssteget, resterande betyg följer i fallande ordning där betyget E utgör det lägsta betygssteget för att vara godkänd. Betyget F innebär att studentens prestationer bedömts som underkända.
Examinationen består av

- individuella skriftliga inlämningsuppgifter, av vilka några har laborativa inslag; 4 hp. Lärandemål THE, COM och IMP. (betyggskala A-F)
- seminarier; 1,5 hp. Lärandemål THE, COM och SOC. (betygsskala U/G)
- individuell muntlig tentamen; 2 hp. Lärandemål THE och IMP. (betygskala A-F)

Slutbetyget är en sammanvägning av betyget på den muntliga tentamen och de skriftliga inlämningsuppgifterna.
Omexamination ges i enlighet med Lokala regler för kurs och examination på grundnivå och avancerad nivå vid Linnéuniversitetet. I det fall student med funktionsnedsättning har rätt till särskilt pedagogiskt stöd beslutar examinator om anpassad eller alternativ examination.

Kursvärdering

Kursvärdering genomförs under kursen eller i nära anslutning till kursens avslutning. Resultat och analys av genomförd kursvärdering ska skyndsamt återkopplas till de studenter som genomfört kursen. Studenter som deltar vid nästa kurstillfälle ska senast vid kursstart informeras om föregående kursvärderingsresultat och genomförda förändringar i kursen.

Överlappning

Kursen kan inte ingå i examen med annan kurs, vars innehåll helt eller delvis överensstämmer med innehållet i följande kurs/kurser:
Matematisk kryptering 4MA123/4MA432/4MA433, 5 hp

Övrigt

Betygskriterier för A-F-skalan kommuniceras till studenten via särskilt dokument. Studenten informeras om kursens betygskriterier senast i samband med kursstart.

Kurslitteratur och övriga läromedel

Jeffrey Hoffstein, Jill Pipher & Joseph H. Silverman, *An Introduction to Mathematical Cryptography*, Springer, senaste upplagan. 350 (523) sidor.