Kursplan

Fakulteten för teknik
Institutionen för matematik

4MA423 Matematisk kryptering, 7,5 högskolepoäng
Mathematical cryptography, 7.5 credits

Huvudområde
Matematik

Ämnesgrupp
Matematik

Nivå
Avancerad nivå

Fördjupning
A1F

Fastställande
Fastställd av Fakulteten för teknik 2015-05-22
Kursplanen gäller från och med vårterminen 2016

Förkunskaper
4MA121 Algebraiska strukturer II, 7,5 hp eller motsvarande.

Mål
Efter genomgången kurs förväntas studenten kunna:

- redogöra för hur man krypterar och dekrypterar meddelanden med hjälp av några olika moderna kryptosystem
- redogöra för några matematiska resultat som är av relevans när det gäller tillämpningar i kryptologi
- lösa problem och utföra beräkningar inom kryptologi och implementera kryptologiska algoritmer med hjälp av matematisk programvara
- analysera och diskutera kryptologins roll i samhället och dess etiska konsekvenser
- visa fördjupad kunskap inom något område av kryptologin.

Innehåll
Några historiska krypton. Diskreta logaritmer; ElGamals krypto, Diffie-Hellmans protokoll. RSA-kryptot; primtalsgenerering, faktoriseringsmetoder. Informationsteori. Kryptering med elliptiska kurvor. Gitterbaserad kryptering. Generering av pseudoslumptal. Kryptologins roll i samhället.

Undervisningsformer
Föreläsningar och övningar.

Examination
Kursen bedöms med betygen A, B, C, D, E, Fx 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 skriftliga inlämningsuppgifter (4,5 hp), av vilka några har laborativa inslag (datorprogrammering), samt ett projektarbete (3 hp) som ska redovisas såväl skriftligt som muntligt vid ett seminarium.

För ett godkänt betyg avkrävs att de förväntade studieresultaten ska vara uppnådda.

Kursvärdering

Under kursens genomförande eller i nära anslutning till kursen genomförs en kursvärdering. Resultat och analys av kursvärderingen ska återkopplas till de studenter som genomfört kursen och de studenter som deltar vid nästa kurstillfälle. Kursvärderingen genomförs anonymt. Den sammanställda rapporten arkiveras vid fakulteten.

Överlappning

Kursen kan inte ingå i examen med annan kurs, vars innehåll helt eller delvis överensstämmer med innehållet i denna kurs: 4MA123 Matematisk kryptering, 7,5 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

Obligatorisk litteratur

Hoffstein, Pipher & Silverman, *An Introduction to Mathematical Cryptography*, Springer, 2008 eller senare. 350 (523) sidor.