Kursplan

Fakulteten för teknik

Institutionen för matematik

4MA123 Matematisk kryptering, 7,5 högskolepoäng
4MA123 Mathematical cryptography, 7.5 credits

Huvudområde
Matematik

Ämnesgrupp
Matematik

Nivå
Avancerad nivå

Fördjupning
A1F

Fastställande
Fastställd 2010-12-10
Senast reviderad 2014-09-03 av Fakulteten för teknik. Revidering av förkunskaper, innehåll, mål, examination och undervisningsform.
Kursplanen gäller från och med höstterminen 2015

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 Underkänd, Godkänd eller Väl godkänd.

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.

På begäran kan den studerande få sitt betyg översatt enligt ECTS-skalan. En sådan begäran skall ha inkommit till examinator före betygssättningen.

Kursvärdering
I samband med kursavslutningen genomförs en kursvärdering enligt universitetets riktlinjer. Resultatet av kursvärderingen arkiveras på institutionen.

Kurslitteratur och övriga läromedel
Obligatorisk litteratur
Hoffstein, Pipher & Silverman, *An Introduction to Mathematical Cryptography*, Springer, 2008 eller senare. 350 (523) sidor.