Linnéuniversitetet
Kalmar Växjö

Kursplan

Fakultetsnämnden för naturvetenskap och teknik
Institutionen för datavetenskap, fysik och matematik

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

Huvudområde
Matematik

Ämnesgrupp
Matematik

Nivå
Avancerad nivå

Fördjupning
A1N

Fastställande
Fastställd av institutionsstyrelsen vid Institutionen för datavetenskap, fysik och matematik 2010-12-10

Senast reviderad 2012-08-17. Revidering av förkunskaper.

Kursplanen gäller från och med vårterminen 2013

Förkunskaper
Algebraiska strukturer I 7,5 hp (2MA105) och Elementär talteori 7,5 hp (2MA106), eller motsvarande.

Mål
Efter genomgången kurs förväntas studenten kunna:

- redogöra för hur man krypterar och dekrypterar meddelanden med hjälp diverse olika moderna kryptosystem
- redogöra för några matematiska resultat som är av relevans när det gäller tillämpningar i kryptologi.

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

Undervisningsformer
Föreläsningar och övningar. Grupparbeten och obligatoriska moment kan förekomma.

Examinationsformer
Kursen bedöms med betygen Underkänd, Godkänd eller Väl godkänd.

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

Examinationen sker med skriftlig och/eller muntlig tentamen. Kontinuerlig examination genom skriftliga och/eller muntliga redovisningar kan dessutom förekomma. Den huvudsakliga formen för examination bestäms vid kursstart.

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.