



Linnéuniversitetet

Kalmar Växjö

Kursplan

Fakultetsnämnden för naturvetenskap och teknik

Institutionen för datavetenskap, fysik och matematik

1MA164 Kryptering och kodningsteori, 7,5 högskolepoäng

Cryptography and Coding Theory, 7.5 credits

Huvudområde

Matematik

Ämnesgrupp

Matematik

Nivå

Grundnivå

Fördjupning

G1F

Fastställande

Fastställd av Organisationskommittén 2009-08-11

Kursplanen gäller från och med vårterminen 2010

Förkunskaper

Ett års universitetsstudier i matematik (motsvarande 60 hp), inkluderande kurser i grundläggande matematik och vektorgeometri eller motsvarande.

Förväntade studieresultat

Efter genomgången kurs förväntas studenten kunna:

- beskriva några vanliga krypterings- och kodningsalgoritmer
- redogöra för olika kryptosystems styrkor och svagheter
- använda kryptoanalys till att forcera klassiska krypton
- förstå principerna för kodning och avkodning hos felrättande koder.

Innehåll

Kryptering:

Några klassiska krypton som t.ex. affina krypton, substitutionskrypton, Vigenèrekryptot och Hillkryptot.

Data Encryption Standard (DES). Advanced Encryption Standard (AES).
Asymmetriska krypton, speciellt RSA-kryptot och ElGamals krypto. Digitala signaturer.
Diffie-Hellmans protokoll.

Kodning:

Felrättande koder. Linjära koder. Hammingkoder. Cykliska koder. CRC-algoritmen

Undervisningsformer

Föreläsningar, övningar och laborationer. 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 skriftlig kursvärdering enligt universitetets riktlinjer. Kursvärderingen diarieförs på institutionen.

Kurslitteratur och övriga läromedel

Obligatorisk litteratur

Trappe, W & Washington, L. C. *Introduction to Cryptography with Coding Theory*, 2nd Ed., Pearson Education, 2006 eller senare. 250 (577) sidor.

MSI:Utdelat material, Växjö universitet, aktuellt år, 30 sidor.