Kursplan

Fakulteten för teknik

Institutionen för matematik

1MA164 Kryptering och kodningsteori, 7,5 högskolepoäng
1MA164 Cryptography and Coding Theory, 7.5 credits

Huvudområde
Matematik

Ämnesgrupp
Matematik

Nivå
Grundnivå

Fördjupning
G1F

Fastställande
Fastställd 2009-08-11
Senast reviderad 2014-09-03 av Fakulteten för teknik. Revidering av mål, innehåll, examination och undervisningsform.
Kursplanen gäller från och med vårterminen 2015

Förkunskaper
1MA101 Grundläggande matematik, 7,5 hp och 1MA103 Vektorgeometri, 7,5 hp eller 1MA141 Grundläggande matematik för dataloger, 7,5 hp

Mål
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.

Orientering om aktuella forskningsfrågor

Kodning:

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

Undervisningsformer
Föreläsningar, övningar och laborationer.

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

Examinationen sker med skriftlig salstentamen och skriftlig redovisning av datorlaboration.

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

DFM:Utdelat material, Linnéuniversitetet, aktuellt år, 30 sidor.