Linnéuniversitetet
Kalmar Växjö

Dnr: 2022/200-3.1.2.2

Kursplan

Fakulteten för teknik
Institutionen för matematik

1MA464 Kryptering och kodningsteori, 7,5 högskolepoäng
Cryptography and Coding Theory, 7.5 credits

Huvudområde
Matematik

Ämnesgrupp
Matematik

Nivå
Grundnivå

Fördjupning
G1F

Fastställande
Fastställd 2015-05-22
Senast reviderad 2022-01-24 av Fakulteten för teknik. Revidering av litteraturen.
Kursplanen gäller från och med vårterminen 2022

Förkunskaper
1MA462 Diskret matematik, 7,5 hp eller motsvarande

Mål

Efter genomgången kurs förväntas studenten kunna

- lösa problem, utföra beräkningar och föra resonemang inom den del av matematiken som omfattas av kursen samt skriftligt kunna kommunicera dessa lösningar, beräkningar och resonemang
- identifiera och formulera frågeställningar inom kursens ämnesområde samt genomföra uppgifter inom givna tidsramar.

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 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 sker med skriftlig tentamen, samt en datorlaboration.

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 en examen tillsammans med följande kurser som helt eller delvis överlappar innehållet i denna kurs: 1MA164 Kryptering och kodningsteori, 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

Christof Paar & Jan Pelzl: *Understanding Cryptography*, Springer, senaste upplagan. 140 (350) sidor.

Simon Rubinstein-Salzedo: *Cryptography*, Springer, senaste upplagan. 65 (250) sidor

FTK: Utdelat material, Linnéuniversitetet, aktuellt år, 58 sidor.