



## 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 2019-11-10 av Fakulteten för teknik. Revidering av litteraturlistan.

Kursplanen gäller från och med vårterminen 2019

### 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**

Stanoyevitch Alexander. *Introduction to Cryptography with Mathematical Foundations and Computer Implementations*, Chapman & Hall, 2011 eller senare. 250 (649) sidor.

FTK: Utdelat material, Linnéuniversitetet, aktuellt år, 50 sidor.