**Blekinge Tekniska Högskola**
Institutionen för matematik och naturvetenskap

**Revision**: 2
**Dnr**: BTH-4-1-14-0038-2025

# KURSPLAN

## Introduktion till kodningsteori och kryptering

Introduction to Coding Theory and Cryptography

7,5 högskolepoäng (7.5 credits)

**Kurskod**: MA1508
**Huvudområde**: Matematik
**Utbildningsområde**: Naturvetenskapliga området
**Utbildningsnivå**: Grundnivå
**Fördjupning**: G1F - Grundnivå, har mindre än 60 hp kurs/er på grundnivå som förkunskapskrav

**Undervisningsspråk**: Svenska
**Gäller från**: 2025-03-04
**Fastställd**: 2025-03-04

### 1. Beslut

Denna kurs är inrättad av dekan 2023-08-18. Kursplanen är fastställd av prefekten vid institutionen för matematik och naturvetenskap 2025-03-04 och gäller från 2025-03-04.

### 2. Förkunskapskrav

För tillträde till kursen krävs avklarad kurs i Diskret matematik och algoritmer 7,5 hp.

### 3. Syfte och innehåll

#### 3.1 Syfte

Syftet med kursen är att studenten ska förvärva grundläggande kunskaper inom sannolikhetsteori, kodningsteori och kryptologi, främst för användning inom kommunikation och säkerhet.

#### 3.2 Innehåll

1. Sannolikhetsteori och matematisk statistik
   - Diskreta stokastiska variabler
   - Väntevärde, varians och standardavvikelse
   - Stora talens lag
   - Introduktion till centrala gränsvärdessatsen
2. Kodningsteori (felrättande koder och komprimering)
   - Blockkoder
   - Matrismetoder för felrättande koder
   - Faltningskoder
   - Kanalmodeller
   - Hammings gräns och liknande övre gränser på kodstorlek
   - Gilbert–Varshamovs sats och liknande resultat
   - Koder för komprimering
   - Definition av entropi
   - Shannons sats för källkodning
3. Kryptologi
   - Blankettchiffer
   - Kort orientering om symmetriska krypton
   - Definition av asymmetriska krypton
   - RSA-metoden för kryptering
   - Praktisk användning av RSA-metoder (paddning)
   - Elliptic Curve Cryptography
   - Digitala signaturer
4. Matematisk programvara/programmering
   - Implementering av kursens algoritmer i Python eller liknande

### 4. Lärandemål

Följande lärandemål examineras i kursen:

#### 4.1. Kunskap och förståelse

Efter genomförd kurs ska studenten kunna:

- visa förståelse för begrepp och satser inom det som ingår i kursinnehållet.

#### 4.2. Färdighet och förmåga

Efter genomförd kurs ska studenten kunna:

- lösa beräkningsuppgifter och problem inom det som ingår i kursinnehållet.

### 4.3. Värderingsförmåga och förhållningssätt

Efter genomförd kurs ska studenten kunna:

- beskriva behandlade metoders användbarhet och begränsningar i ingenjörsvetenskap.

## 5. Läraktiviteter

Kursen undervisas genom föreläsningar och övningar.

## 6. Bedömning och examination

Examinationsmoment för kursen

| Kod | Benämning | Omf. | Betyg |
|---|---|---|---|
| 2510 | Salstentamen [1] | 5,5 hp | AF |
| 2520 | Inlämningsuppgift 1 | 1 hp | GU |
| 2530 | Inlämningsuppgift 2 | 1 hp | GU |

[1] Bestämmer kursens slutbetyg vilket utfärdas först när samtliga moment godkänts.

Kursen bedöms med betygen A Utmärkt, B Mycket bra, C Bra, D Tillfredställande, E Tillräckligt, FX Underkänd, något mer arbete krävs, F Underkänd.

Examinator har möjlighet att muntligen följa upp skriftliga examinationer.

I kurstillfällets information inför kursstart framgår i vilka examinationsmoment som kursens lärandemål examineras samt gällande bedömningsgrunder.

Examinator kan, efter samråd med högskolans FUNKA-samordnare, fatta beslut om anpassad examinationsform för att en student med varaktig funktionsvariation ska ges en likvärdig examination jämfört med en student utan funktionsvariation.

## 7. Kursvärdering

Kursvärdering ska göras i enlighet med BTH:s beslut om frågeställning i kursvärderingar och beslut om process för hantering och uppföljning av kursvärderingar.

## 8. Begränsningar i examen

Kursen kan ingå i examen men inte tillsammans med annan kurs vars innehåll, helt eller delvis, överensstämmer med innehållet i denna kurs.

## 9. Kurslitteratur och övriga lärresurser

Moser, Stefan M. and Chen, Po-Ning (2012), *A Student's Guide to Coding and Information Theory*, Cambridge University Press. ISBN 978-1-107-60196-3.

Material på lärplattformen.

Övriga lärresurser
Läraren är en central lärresurs i kursen. Under schemalagda undervisningstillfällen förmedlas en mängd information om exempelvis lösningsstrategier, matematiska konventioner och kursnivå som inte kan förväntas erhållas på annat sätt än genom deltagande i klassrummet.