



## Kursplan

Fakulteten för teknik

Institutionen för matematik

4MA433 Matematisk kryptering, 7,5 högskolepoäng

Mathematical cryptography, 7.5 credits

### Huvudområde

Matematik

### Ämnesgrupp

Matematik

### Nivå

Avancerad nivå

### Fördjupning

A1N

### Fastställande

Fastställd 2024-07-01.

Kursplanen gäller från och med hösttermin 2024.

### Förkunskaper

60 hp i matematik inkluderande kursen Algebraiska strukturer I, 2MA405, 7,5 hp eller motsvarande.

### Mål

Efter genomgången kurs förväntas studenten kunna:

- redogöra för hur några moderna kryptosystem och digitala signaturer fungerar samt kunna redogöra för deras begränsningar och effektivitet [THE]
- med hjälp av abstrakt algebra redogöra för den matematiska grunden till moderna krypteringssystem [MAT]
- lösa problem och utföra beräkningar inom kryptologi såväl med som utan beräkningsverktyg[COM]
- analysera och diskutera kryptologins roll i samhället och dess etiska

## Innehåll

Diskreta logaritmer; ElGamals krypto, Diffie-Hellmans protokoll. RSA-kryptot; primtalsgenerering, faktoriseringsmetoder. Digitala signaturer. Kryptering med elliptiska kurvor. Gitterbaserad kryptering. Kryptologins roll i samhället.

## Undervisningsformer

Föreläsningar och seminarier.

Deltagande på seminarier är obligatoriskt.

## Examination

Kursen bedöms med betygen A, B, C, D, E 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 består av

- individuella skriftliga inlämningsuppgifter, av vilka några har laborativa inslag; 4 hp Lärandemål THE, COM och MAT. (betygsskala A-F)
- seminarier (diskussion och presentation av inlämningsuppgifter); 1,5 hp. Lärandemål THE, COM och SOC. (betygsskala U/G)
- individuell muntlig tentamen (berör teorin samt innehåll av inlämningsuppgifter); 2 hp. Lärandemål THE och MAT. (betygsskala A-F)

Slutbetyget är en sammanvägning av betyget på den muntliga tentamen och de skriftliga inlämningsuppgifterna

Omexamination ges i enlighet med Lokala regler för kurs och examination på grundnivå och avancerad nivå vid Linnéuniversitetet. I det fall student med funktionsnedsättning har rätt till särskilt pedagogiskt stöd beslutar examinator om anpassad eller alternativ examination.

## Kursvärdering

Kursvärdering genomförs under kursen eller i nära anslutning till kursens avslutning. Resultat och analys av genomförd kursvärdering ska skyndsamt återkopplas till de studenter som genomfört kursen. Studenter som deltar vid nästa kurstillfälle ska senast vid kursstart informeras om föregående kursvärderingsresultat och genomförda förändringar i kursen.

## Överlappning

Kursen kan inte ingå i examen med annan kurs, vars innehåll helt eller delvis överensstämmer med innehållet i följande kurs/kurser:

Matematisk kryptering, 4MA423/4MA123, 5 hp

Kryptering, 4MA923, 5 hp

## Övrigt

Betygskriterier för A-F-skalan kommuniceras till studenten via särskilt dokument. Studenten informeras om kursens betygs-kriterier senast i samband med kursstart.

## Kurslitteratur och övriga läromedel

Jeffrey Hoffstein, Jill Pipher & Joseph H. Silverman, *An Introduction to Mathematical Cryptography*, Springer, senaste upplagan. 350 (523) sidor.