



LUNDS UNIVERSITET  
Lunds Tekniska Högskola

*Kursplan för*

## Kryptoteknik Cryptography

**EDIN01, 7,5 högskolepoäng, A (Avancerad nivå)**

Gäller för: Läsåret 2013/14

Beslutad av: Utbildningsnämnd A

Beslutsdatum: 2013-04-15

### Allmänna uppgifter

Valfri för: C4, C4-ks, D4, D4-ks, E4, E4-ks, F4, MWIR2, Pi4, Pi4-pv

Undervisningsspråk: Kursen ges på begäran på engelska

### Syfte

Syftet med kursen är att ge en orientering om klassiska kryptosystem samt att ge ingående kunskaper om moderna kryptosystem.

### Mål

*Kunskap och förståelse*

För godkänd kurs skall studenten

- beskriva de olika byggstenar som området kryptologi tillhandahåller,
- förklara principer bakom olika kryptografiska funktioner,
- beskriva de generella problemen inom området kryptologi.

*Färdighet och förmåga*

För godkänd kurs skall studenten

- identifiera och formulera problem inom området kryptologi
- göra översiktliga beskrivningar av hur kryptografiska funktioner kan användas i system som syftar till att erbjuda någon typ av säkerhet
- göra val av lämpliga parametrar till kryptografiska funktioner samt analysera olika möjliga konstruktioner ur ett säkerhetsperspektiv.

### Kursinnehåll

*Klassiska kryptosystem:* Inledning och grundläggande begrepp. Caesarkrypto, enkel

substitution, polyalfabetssystem (Vigenére, Vernam), transposition, rotormaskiner (Enigma).

*Shannons teori för sekretess:* Nyckelentropier och meddelanden, redundans och entydighetslängd, perfekt sekretess.

*Skiftregister och strömchiffer:* Ändliga kroppar, linjärt återkopplade skiftregister och skiftregistersekvenser, perioder och cykelkarakteristiker, skiftregistersyntes, olinjära kombinationer av skiftregistersekvenser, attacker på strömchiffer.

*Blockchiffer:* Data Encryption Standard (DES), Advanced Encryption Standard (AES).

*Öppen-nyckel-kryptosystem:* Enkel talteori, RSA-systemet, Diffie-Hellman nyckelutbyte, faktorisering, primtalstestning, digitala signaturer.

*Hashfunktioner:* egenskaper, kollisionss attacker, födelsedagsparadoxen

*Simmons' teori för autentisering:* Imitation och substitution.

*Secret sharing:* Shamirs tröskelschema, allmän secret sharing, perfekta och ideala system.

**Projekt:** 1. Faktorisering algoritmer. 2. Studium av skiftregister. 3. Korrelations attacker.

## Kursens examination

**Betygsskala:** TH

**Prestationsbedömning:** Examination sker genom skriftlig tentamen och tre projektuppgifter. Godkända projektuppgifter är krav för att få tentera. Betyg på tentamen är kursbetyg.

## Antagningsuppgifter

**Förutsatta förkunskaper:** EDA011 eller EDA016 Programmeringsteknik.

**Begränsat antal platser:** Nej

**Kursen överlappar följande kurser:** EDI051

## Kurslitteratur

- Föreläsning anteckningar i kryptoteknik, utges av institutionen.
- Alternativ litteratur: Stinson, D., Cryptography, Theory and Practice, CRC Press, ISBN 1-58488-206-9 eller Smart, N., Cryptography: An Introduction, McGraw-Hill, ISBN 0077099877.

## Kontaktinfo och övrigt

**Kursansvarig:** Professor Thomas Johansson, thomas@eit.lth.se

**Hemsida:** <http://www.eit.lth.se/kurs/edin01>