



Kursplan för läsåret 2008/2009  
(Genererad 2008-07-17.)

---

## KRYPTOTEKNIK Cryptography

EDI051

**Antal högskolepoäng:** 7,5. **Betygskala:** TH. **Nivå:** G2 (Grundnivå, fördjupad).  
**Undervisningspråk:** Kursen ges på svenska. **Valfri för:** C4, C4ks, C4sd, D4, D4ks, E4, E4ks, F4, MWIR2, Pi4, RH4. **Kursansvarig:** Professor Thomas Johansson, thomas@eit.lth.se, Inst för elektro- och informationsteknik. **Förutsatta förkunskaper:** EDA011 eller EDA016 Programmeringsteknik. **Prestationsbedömning:** Examination sker genom skriftlig tentamen och fyra mindre projektuppgifter. Godkända projektuppgifter är krav för att få tentera. Betyg på tentamen är kursbetyg. **Hemsida:** <http://www.eit.lth.se/kurs/edi051>.

### 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

Efter genomgången kurs skall studenten på egen hand kunna:

- 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

Efter genomgången kurs skall studenten på egen hand kunna:

- 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.

### Innehåll

*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.

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

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

**Projekt:** 1. Faktoriseringsalgoritmer. 2. Studium av skiftregister. 3. Korrelationsattacker. 4. Learning about DES.

#### **Litteratur**

Kompendium 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