

Kursplan för läsåret 2001/2002

KRYPTOTEKNIK

EDI050

Cryptography

Poäng: 4.0 **Betygskala:** TH. **Valfri för:** D4, E4, F4.

Kursansvarig: Professor Thomas Johansson. **Rekommenderade**

förkunskaper: Informationsteori (EDI030), Digitalteknik

(EIT020). **Prestationsbedömning:** Godkänd laboration och godkänt projekt är krav för att få tentera. Tentamen (5 tim) är skriftlig och av problemlösningstyp. **Webbsida:**

<http://www.it.lth.se/cryptology>

Mål:

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

Innehåll:

Klassiska kryptosystem: Inledning och grundläggande begrepp. Caesarkrypto, enkel substitution, polyalfabetssystem (Vigenère, Kasiskis forceringsmetod, Vernam), bigramsubstitution, transposition.

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

Kryptomaskiner: Hagelins M-209 maskin, Transvertex HC-9, rotormaskiner (Enigma).

Skiftregister: Något om ändliga kroppar, linjärt återkopplade

skiftregister och skiftregistersekvenser, perioder och cykelkaraktistiker, skiftregistersyntes, olinjära kombinationer av skiftregistersekvenser, skiftregisterfiltrering.

Elektroniska kryptosystem: Forcering med skiftregistersyntes.

Data Encryption Standard: Historik, konstruktionsfilosofi, DES, Hellmans kritik.

Öppen-nyckel-distribution: Logaritmproblemet, Pohlig-Hellman-systemet.

Öppen-nyckel-kryptosystem: Något om talteori, RSA-systemet, Rabins ekvivalenssats, Herlestams kritik.

Simmons' teori för autentisering: Imitation och substitution, Simmons' gräns.

Secret sharing. Historik: Laboration: Studium av skiftregister.

Projekt: Learning about DES.

Litteratur:

Johannesson, R.: Något om kryptering. (Kompedium, utges av institutionen).