



## SÄKERHET

EDA625

### Data Security

**Antal poäng:** 5. **Betygskala:** TH. **Obligatorisk för:** IDA3, IMM3. **Kursansvarig:** Rolf Björkman, rolf.bjorkman@hbg.lth.se, Ingenjörshögskolan i Helsingborg.

**Prestationsbedömning:** Skriftlig tentamen. **Hemsida:** <http://www.hbg.lth.se>.

#### Mål

I en värld där kommunicerande datorer är geografiskt utspridda är det viktigt att man säkerställer att rätt information når rätt och endast rätt mottagare. Det är av största vikt att IT-ingenjören är väl förtrogen med de säkerhetsproblem som behöver lösas kring och i datorsystem för att en betryggande kommunikation skall kunna upprättas. Kryptering, autenticering, nyckelhantering och certifikat är exempel på begrepp som klargörs och exemplifieras i kursen.

#### Innehåll

- Strukturering och nomenklatur. Tillförlitlig drift. Grundanalyser. Säkra operativsystem. Identitetsverifiering. Behörighetskontroll. Kryptering. Nätsäkerhet.
- Skyddsbehov vid lagring och kommunikation av information.
- Kryptering som informationsskydd. Kryptoteori.
- Perfekta krypton och begreppet slumpmässighet. Pseudoslumpföljder. Blockkrypton. DES.
- System för öppen krypteringsnyckel och öppen nyckeldistribution.
- Kryptobaserade kontrollsummor, signaturer.
- Standardlösningar för Internet typ SSL, SET.

#### Litteratur

Gollman, D: Computer Security. John Wiley And Sons Ltd, UK, 1998. ISBN: 0-471-97844-2.