LUNDS UNIVERSITET
Lunds Tekniska Högskola

SÄKERHET EDA625

Data Security

Poäng: 5.0 **Betygskala:** TH **Obligatorisk för:** MMH3 **Kursansvarig:** Lärare vid LTH Ingenjörshögskolan **Prestationsbedömning:** Skriftlig tentamen. För slutbetyg fordras även godkända laborationer.

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 multimediaingenjören är väl förtrogen med de säkerhetsproblem som behöver lösas kring och i datorsystem för att en betryggande kommunikation skall kunna upprättas. Kryptering, autentisering, nyckelhantering och certifikat är exempel på begrepp som klargörs och exemplifieras i kursen.
Kursen förmedlar också nödvändiga kunskaper från talteorin och från algebran.

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 krytpteringsnyckel och öppen nyckeldistribution.
· Kryptobaserade kontrollsummor, signaturer.
· Standardlösningar för Internet typ SSl, SET.

Litteratur:
Meddelas senare.