LUNDS UNIVERSITET
Lunds Tekniska Högskola

Kursplan för kalenderåret 2005

MATEMATISK KRYPTOLOGI EDI075

Mathematical Cryptology

Antal poäng: 4. **Betygskala:** TH. **Valfri för:** C4, D4, E4. **Kursansvarig:** Professor Thomas Johansson, thomas@it.lth.se, Inst f informationsteknologi. **Förkunskapskrav:** EDI051 Kryptoteknik. **Rekommenderade förkunskaper:** FMA410 Endimensionell analys, FMA420 eller FMA425 Linjär algebra, FMA430 eller FMA435 eller FMA025 Flerdimensionell analys. **Prestationsbedömning:** Obligatoriska projektuppgifter samt skriftlig tentamen. **Hemsida:** http://www.it.lth.se.

Mål
Syftet med kursen är att visa på hur avancerad matematisk teori har stora praktiska tillämpningar inom områdena kryptologi och datasäkerhet.

Innehåll
Innehållsmässigt ger kursen ett antal matematiska verktyg som har många applikationer, inte enbart inom krypto och säkerhet. De flesta av de system som tas upp i kursen är standard i olika kommunikationssystem, till exempel kryptosystem konstruerade via elliptiska kurvor. Få har dock den matematiska bakgrunden att kunna förstå hur sådana system fungerar. Vi tittar också på hur man matematiskt bevisar att system eller protokoll är säkra och de modeller som finns.

Mer specifikt de flesta av följande områden: Diskreta logaritmer och dess kryptosystem; Elliptiska kurvor och dess kryptosystem; Gröbnerbaser och dess användning i attacker på kryptosystem; Faktorisering och diskret log problemen; Projektiv geometri över ändliga kroppar, autentisering och secret sharing; Komplexitetsteori, bevisbar säkerhet, random-oracle-model; Protokollanalys

Litteratur
Smart N: Cryptography, an introduction, McGraw-Hill.
Föreläsningsanteckningar.