LUNDS UNIVERSITET
Lunds Tekniska Högskola

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

MATEMATISK KRYPTOLOGI EDI075

Mathematical Cryptology

Antal högskolepoäng: 6. **Betygskala:** TH. **Nivå:** A (Avancerad nivå). **Undervisningsspråk:** Kursen ges på begäran på engelska. **Valfri för:** C4, C4sd, D4, E4, Pi4. **Kursansvarig:** Professor Thomas Johansson, thomas@eit.lth.se, Inst för elektro- och informationsteknik. **Förkunskapskrav:** EDI051 Kryptoteknik. **Förutsatta förkunskaper:** FMA410 Endimensionell analys, FMA420 eller FMA425 Linjär algebra, FMA430 eller FMA435 eller FMA025 Flerdimensionell analys. **Kan ställas in:** Vid mindre än 10 anmälda. **Prestationsbedömning:** Examination sker genom skriftlig tentamen och obligatoriska hemuppgifter. Godkända hemuppgifter är krav för att få tentera. Betyg på tentamen är kursbetyg. **Hemsida:** http://www.eit.lth.se/kurs/edi075.

Syfte

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

Mål

Kunskap och förståelse
För godkänd kurs skall studenten

- kunna beskriva matematikens roll inom området kryptologi,
- förklara matematiska principer bakom avancerade kryptografiska funktioner,
- beskriva och jämföra olika lösningar till ett givet problem inom området kryptologi.

Färdighet och förmåga
För godkänd kurs skall studenten

- identifiera och formulera matematiska problem relevanta för området kryptologi
- beskriva av hur matematiska problemställningar kan utnyttjas för att konstruera kryptografiska funktioner
- matematiskt analysera olika möjliga konstruktioner ur ett säkerhetsperspektiv.

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 används i olika kommunikationssystem, exempelvis 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 behandlar vi de flesta av följande områden: Diskreta logaritmer och dess kryptosystem; Elliptiska kurvor och dess kryptosystem; Faktorisering och diskret log problemen; Symmetriska kryptosystem, Digitala signaturer och hashfunktioner, Autentisering och secret sharing; Komplexitetsteori, Bevisbar säkerhet, Random-oracle-model.

Litteratur

Smart, N., Cryptography: An Introduction, McGraw-Hill, ISBN 0077099877
samt diverse föreläsningsanteckningar.