LUNDS UNIVERSITET
Lunds Tekniska Högskola

Kursplan för

Matematisk kryptologi
Mathematical Cryptology

EDI075, 6 högskolepoäng, A (Avancerad nivå)

Gäller för: Läsåret 2012/13
Beslutad av: Utbildningsnämnd 1
Beslutsdatum: 2012-03-19

Allmänna uppgifter

Valfri för: C4, C4-ks, D4, D4-ks, Pi4, Pi4-pv
Undervisningsspråk: Kursen ges på begäran på engelska

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.

Kursinnehåll

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.

Kursens examination

Betygsskala: TH
Prestationsbedömning: Examination sker genom skriftlig tentamen och obligatoriska hemuppgifter. Godkända hemuppgifter är krav för att få tentera. Betyg på tentamen är kursbetyg.

Antagningsuppgifter

Förkunskapskrav:

- EDI051 Kryptoteknik

Förutsatta förkunskaper: FMA410 Endimensionell analys, FMA420 eller FMA425 Linjär algebra, FMA430 eller FMA435 eller FMA025 Flerdimensionell analys.
Begränsat antal platser: Nej
Kursen kan ställas in: Om färre än 8 anmälda.

Kurslitteratur

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

Kontaktinfo och övrigt

Kursansvarig: Professor Thomas Johansson, thomas@eit.lth.se
Hemsida: http://www.eit.lth.se/kurs/edi075
Övrig information: Vid färre än 16 deltagare kan kursen komma att ges med reducerad undervisning och större inslag av självstudier.