

Kursplan för

Avancerad kryptografi Advanced Cryptography

**ETIN85, 7,5 högskolepoäng, A
(Avancerad nivå)**

Gäller för: Läsåret 2022/23

Fakultet: Lunds tekniska högskola

Beslutad av: Programledning C/D

Beslutsdatum: 2022-04-07

Allmänna uppgifter

Valfri för: C4-sec, D4-ns, E4, F4, MSOC2, MWIR2, Pi4

Undervisningsspråk: Kursen ges på engelska

Syfte

Syftet med kursen är att visa på hur avancerade algoritmer och protokoll inom kryptologi fungerar och att de har stora praktiska tillämpningar inom datasäkerhet.

Mål

Kunskap och förståelse

För godkänd kurs skall studenten

- beskriva definition och funktion för ett antal avancerade primitiver och protokoll inom kryptologi som tas upp i kursen.
- förklara matematiska principer bakom avancerade kryptografiska byggstenar.
- beskriva modeller för säkerhet samt bevisföring för kryptografiska primitiver.

Färdighet och förmåga

För godkänd kurs skall studenten

- identifiera och formulera matematiska problem relevanta för avancerade algoritmer inom kryptologi.

- matematiskt analysera olika möjliga konstruktioner ur ett säkerhetsperspektiv.
- implementera relevanta primitiver eller attacker för simulering

Värderingsförmåga och förhållningssätt
För godkänd kurs skall studenten

- på egen hand kunna klassificera hur olika primitiver och dess parametrar är kopplade till olika modeller och nivåer inom säkerhet.

Kursinnehåll

Innehållsmässigt ger kursen ett antal avancerade verktyg inom kryptologi som har många tillämpningar inom datasäkerhet. De flesta av de system som tas upp i kursen används i olika kommunikationssystem, exempelvis kryptosystem konstruerade via elliptiska kurvor. Vi går igenom den matematiska bakgrunden som behövs 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 problem; Avancerade typer av symmetriska kryptosystem, digitala signaturer och hashfunktioner, autentisering och secret sharing; Komplexitetsteori, Bevisbar säkerhet, Random-oracle-model; MPC primitiver och homomorfisk kryptering; Post-kvant kryptologi.

Kursens examination

Betygsskala: TH - (U,3,4,5) - (Underkänd, Tre, Fyra, Fem)

Prestationsbedömning: För godkänd kurs krävs godkända projekt och hemuppgifter. Utöver detta krävs godkänd tentamen, där resultatet ger betyget i kursen. Godkända hemuppgifter är ett krav för att få skriva tentamen.

Om så krävs för att en student med varaktig funktionsnedsättning ska ges ett likvärdigt examinationsalternativ jämfört med en student utan funktionsnedsättning, så kan examinator efter samråd med universitetets avdelning för pedagogiskt stöd fatta beslut om alternativ examinationsform för berörd student.

Delmoment

Kod: 0121. **Benämning:** Projekt.

Antal högskolepoäng: 3. **Betygsskala:** UG. **Prestationsbedömning:** Godkända projekt och hemuppgifter.

Kod: 0221. **Benämning:** Tentamen.

Antal högskolepoäng: 4,5. **Betygsskala:** TH. **Prestationsbedömning:** Skriftlig tentamen.

Antagningsuppgifter

Förkunskapskrav:

- EDI051 Kryptoteknik eller EDIN01 Kryptoteknik

Begränsat antal platser: Nej

Kursen överlappar följande kurser: EDIN05

Kurslitteratur

- Nigel Smart: Cryptography Made Simple, (Information Security and Cryptography). Springer, 2016, ISBN: 978-3319219356.

Kontaktinfo och övrigt

Kursansvarig: Thomas Johansson, thomas@eit.lth.se