HÖGSKOLAN
I SKÖVDE

KURSPLAN

Praktisk kryptologi A1N

7,5 högskolepoäng

Kurskod: IT754A
Revisionsnummer: 5.1
Gäller från: 2023-07-01
Beslutad av: Utbildningskommittén för informationsteknologi
Beslutsdatum: 2023-03-16

1. Allmänt om kursen

Kursen ges av Högskolan i Skövde och benämns Praktisk kryptologi A1N (Practical Cryptology A1N). Omfattningen är 7,5 högskolepoäng (hp). Kursen är på avancerad nivå och har fördjupningsnivå A1N.

Kursen ingår i huvudområdet informationsteknologi. Kursens utbildningsområde är teknik.

2. Behörighetskrav

För att vara behörig till kursen krävs en kandidatexamen inom informationsteknologi, datavetenskap eller datalogi (eller motsvarande).

Vidare krävs godkänt betyg i gymnasiekursen Engelska 6/Engelska B (eller motsvarande). Motsvarande kunskaper visas normalt genom ett internationellt erkänt språktest, till exempel IELTS eller TOEFL.

3. Innehåll

Moderna IT-system ställer höga krav på säkerhet och kryptografiska tekniker är en förutsättning för att säkerställa konfidentialitet och integritet. I denna kurs presenteras kryptografiska primitiver och algoritmer samt formella modeller för säkerhet. Övergripande aspekter av vanligt förekommande begrepp såsom elliptiska kurvor, blockchain, digital vattenmärkning och stegonografi behandlas också. Vidare diskuteras aspekter relaterade till hur kryptosystem implementeras och används och studenterna får själva, utifrån sin egen bakgrund, implementera och utvärdera ett kryptosystem.

4. Mål

Efter avslutad kurs ska studenten kunna:

- beskriva och kritiskt reflektera kring kryptografiska primitiver och algoritmer,
- beskriva och kritiskt reflektera kring formella modeller för säkerhet,
- tillämpa olika kryptografiska verktyg i praktiska sammanhang samt
- implementera och kritiskt utvärdera kryptografiska system.

5. Examination

Kursen bedöms med betygen A (Utmärkt), B (Mycket bra), C (Bra), D (Tillfredställande), E (Tillräcklig) eller F (Underkänd).

Kursen har följande examinationsmoment:

- **Hemtentamen**
  4,5 hp, betyg: A/B/C/D/E/F (bestämmer betyg på hel kurs)
- **Inlämningsuppgift**
  3 hp, betyg: G/U

Studenter med varaktig funktionsnedsättning som har fått beslut om riktat pedagogiskt stöd kan erbjudas anpassad eller alternativ examination.

6. Undervisningsformer och undervisningsspråk

Undervisningen består av föreläsningar och laborationer.

Undervisningen bedrivs på engelska.

7. Kurslitteratur och övriga läromedel

Piper, F. & Murphy, S. (2002). *Cryptography: A very short introduction*. Oxford University Press. ISBN 9780192803153.

Artiklar och rapporter enligt anvisningar på kursens sida på lärplattformen.

8. Studentinflytande

Studentinflytande i kursen säkerställs genom kursvärdering. Studenterna informeras om resultatet av kursvärderingen och eventuella åtgärder som genomförts eller planeras, grundat på kursvärderingen.

9. Övrigt

På Högskolan i Skövdes webbplats finns ytterligare information om kursen samt nationella och lokala styrdokument för högskoleutbildning.