HÖGSKOLAN
I SKÖVDE

KURSPLAN

Praktisk kryptologi A1N

7,5 högskolepoäng

Kurskod: IT812A
Revisionsnummer: 2.1
Gäller från: 2026-07-01
Beslutad av: Utbildningskommittén för informationsteknologi
Beslutsdatum: 2026-02-05

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 eller Engelska nivå 2. Motsvarande kunskaper visas normalt genom ett internationellt erkänt språktest, till exempel IELTS eller TOEFL.

3. Innehåll

Säkerhet är ett grundläggande krav vid datoranvändning och kryptografiska tekniker är en viktig del av att säkerställa konfidentialitet och integritet. Fokus i denna kurs ligger på hur kryptografi fungerar på en operativ nivå och hur olika kryptoanalytiska attacker kan tillämpas, snarare än på kryptologi som vetenskap. Kursen är organiserad kring tre kategorier av kryptografiska primitiv (symmetriska, asymmetriska och nyckellösa), som diskuteras och sätts in i praktisk kontext.

4. Mål

Efter avslutad kurs ska studenten kunna:

- beskriva och kritiskt reflektera kring kryptografiska primitiver och algoritmer,
- beskriva och på ett fördjupande sätt redogöra för olika centrala begrepp inom kryptologi,
- tillämpa olika kryptografiska verktyg i praktiska sammanhang, samt
- tillämpa och kritiskt reflektera kring olika kryptoanalytiska attacker.

5. Examination

Kursen bedöms med betygen VG (Väl godkänd), G (Godkänd) eller U (Underkänd).

Kursen har följande examinationsmoment:

- **Inlämningsuppgifter**
  3 hp, betyg: G/U
- **Hemtentamen**
  4,5 hp, betyg: VG/G/U (bestämmer betyg på hel kurs)

Studenter med varaktig funktionsnedsättning som har fått beslut om riktat pedagogiskt stöd kan erbjudas anpassad 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

Kursens innehåll överensstämmer helt eller delvis med följande kurs och kan därför inte ingå i examen med denna kurs:

- IT754A - Praktisk kryptologi A1N 7,5 hp

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