GÖTEBORGS UNIVERSITET

INSTITUTIONEN FÖR DATA- OCH INFORMATIONSTEKNIK

DIT352 Kryptografi, 7,5 högskolepoäng

Cryptography, 7.5 credits

Avancerad nivå / Second Cycle

Fastställande

Kursplanen är fastställd av Institutionen för data- och informationsteknik 2023-11-13 att gälla från och med 2024-09-02, höstterminen 2024.

Utbildningsområde: Naturvetenskapligt 100 %
Ansvarig institution: Institutionen för data- och informationsteknik

Inplacering

Kursen ges inom ett antal program. Den ges även som fristående kurs vid Göteborgs universitet.

Kursen kan ingå i följande program: 1) Datavetenskapligt program (N1COS), 2) Computer Science, Master's Programme (N2COS), 3) Matematikprogrammet (N1MAT) och 4) Applied Data Science masterprogram (N2ADS)

Huvudområde	*Fördjupning*
Datavetenskap	A1N, Avancerad nivå, har endast kurs/er på grundnivå som förkunskapskrav

Förkunskapskrav

För att vara behörig till kursen ska studenten med godkänt resultat ha genomgått kurser motsvarande 90 hp i ämnet datavetenskap eller matematik, inklusive:

- 7,5 hp i algebra eller diskret matematik (som täcker ämnena: kongruensräkning, och grundläggande sannolikhetsteori)
- 7,5 hp programmering

Studenten måste uppvisa kunskaper i Engelska: Engelska 6/Engelska B eller motsvarande nivå från ett internationell erkänt test, till exempel TOEFL, IELTS

Lärandemål

Efter godkänd kurs ska studenten kunna:

Kunskap och förståelse

- Känna igen väletablerade kryptografiska system och identifiera situationer där de kan användas för att förbättra säkerheten för ett givet system
- Demonstrera kunskap om principerna bakom bevisbar säkerhet
- Förstå de teoretiska grunderna för kryptografi

Färdigheter och förmåga

- Beskriva ändamål och designprinciper för gemensamma strukturer mellan flera kryptografiska primitiver och bevissystem
- Identifiera, analysera och förklara olika former av attacker baserade på felaktig användning av kryptografiska byggstenar, blockchiffer eller protokoll
- Reproducera säkerhetsbevis

Värderingsförmåga och förhållningssätt

- Exemplifiera när olika begrepp om säkerhet, såsom informationsteori, beräkningsmässig, bevisbar och praktisk säkerhet, är tillämpliga och beskriv de säkerhetsgarantier som tillhandahålls
- Tillämpa den förvärvade kunskapen i nya situationer.

Innehåll

- Grundläggande och avancerade ändamål för kryptografi (sekretess, autentisering, anonymitet, nollkunskap)
- Symmetrisk kryptografi: blockchiffer, designprinciper och exempel, meddelandeautentiseringskoder.
- Asymetrisk kryptografi: nyckelöverföring, asymmetriska chiffer, signaturer. Attackmodeller och säkerhetsbegrepp.
- Kryptografiska protokoll: hemlighetsdelning "secret sharing", nollkunskapsbevis.

Delkurser

1. **Skriftlig salstentamen** *(Written hall exam),* 6 hp
   Betygsskala: Mycket väl godkänd (5), Väl godkänd (4), Godkänd (3) och Underkänd (U)
2. **Inlämningsuppgifter** *(Assignments),* 1,5 hp
   Betygsskala: Godkänd (G) och Underkänd (U)

Former för undervisning

Kursen är uppbyggd av föreläsningar, övningstillfällen och inlämningsuppgifter.

Undervisningsspråk: engelska

Former för bedömning

Kursen examineras genom hemuppgifter gjorda individuellt eller i grupp, samt skriftlig tentamen gjord individuellt i tentamenssal.

Om student som underkänts två gånger på samma examinerande moment önskar byte av examinator inför nästa examinationstillfälle, ska sådan begäran inlämnas skriftligt till institutionen och bifallas om det inte finns särskilda skäl däremot (HF 6 kap § 22).

I det fall en kurs har upphört eller genomgått större förändringar ska student garanteras minst tre examinationstillfällen (inklusive ordinarie examinationstillfälle) under en tid av minst ett år, dock som längst två år efter det att kursen upphört/förändrats. Vad avser praktik och VFU gäller motsvarande, men med begränsning till endast ett ytterligare examinationstillfälle.

Betyg

På kursen ges något av betygen Mycket väl godkänd (5), Väl godkänd (4), Godkänd (3) och Underkänd (U).
För att bli godkänd på kursen krävs att både inlämningsuppgifterna och tentamen är godkända. Betyget för hela kursen avgörs av den skriftliga salstentamen.

Kursvärdering

Kursen utvärderas genom möten både under och efter kursen mellan lärare och studentrepresentanter. Därutöver används en anonym enkät för att få skriftlig information. Resultatet av utvärderingen används för att förbättra kursen genom att visa på delar som kan läggas till, förbättras, ändras eller tas bort.

Övrigt

Kursen är samläst med Chalmers.

Kurslitteratur kommer att publiceras senast 8 veckor innan kursstart.

Kursen ersätter kursen DIT250, 7,5 hp. Den här kursen kan inte ingå i en examen som innehåller DIT250. Den kan inte heller ingå i en examen som bygger på en annan examen där DIT250 ingår.