GÖTEBORGS UNIVERSITET

DATA- OCH INFORMATIONSTEKNIK

DIT250 Cryptography, 7,5 högskolepoäng

Cryptography, 7.5 credits

Avancerad nivå / Second Cycle

Fastställande

Kursplanen är fastställd av IT-fakultetsnämnden 2006-11-17 och senast reviderad 2017-06-16 av Institutionen för data- och informationsteknik. Den reviderade kursplanen gäller från och med 2017-08-20, höstterminen 2017.

Utbildningsområde: Naturvetenskapligt 100 %
Ansvarig institution: 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*
Computer Science-Secure and Depend Compr Systems	A1N, Avancerad nivå, har endast kurs/er på grundnivå som förkunskapskrav
Datavetenskap	A1N, Avancerad nivå, har endast kurs/er på grundnivå som förkunskapskrav

Förkunskapskrav

För att vara behörig till kursen ska studenten ha avklarade kurser om 60 hp inom ämnet Datavetenskap eller matematik, inkluderat

• 7,5 hp diskret matematik (till exempel DIT980 Diskret matematik för datavetare, delkursen Inledande algebra i MMG200 Matematik 1, eller motsvarande).
• 7,5 hp programmering (till exempel DIT142 Functional programming, DIT012 Imperativ programmering med grundläggande objektorientering, MVG300

Programmering med MatLab eller motsvarande).

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

• sammanfatta de viktigaste målen för kryptografi och illustrera dessa med ett antal exempel på hur kryptografiska tjänster är integrerade i aktuella tillämpningar, både i mjukvara och hårdvara

Färdigheter och förmåga

• beskriva mål, konstruktionsprinciper och gemensamma strukturer för att skapa hemliga nycklar, t.ex. block- och ström-chiffer och meddelandeautentiseringskoder.
• identifiera, analysera och förklara olika former av attacker som baserats på felaktig användning av primitiver, tillstånd eller protokoll
• förklara hur grundläggande primitiver för öppna nyckar kan definieras utifrån svårlösliga matematiska problem som t.ex. diskreta logaritmer eller faktorisering, samt analysera varianter av dessa system.
• förklara hashfunktioners olika användningsområden i andra kryptografiska primitiver och protokoll, samt de krav detta ställer på hashfunktioner.

Värderingsförmåga och förhållningssätt

• exemplifiera när olika säkerhetskoncept, såsom informationsteoretiska, beräkningsbara, bevisbara och praktisk säkerhet, är tillämpliga samt beskriva de säkerhetsgarantier som de erbjuder.
• förklara grundläggande tekniker för kryptering med såväl hemlig som öppen nyckel.

Innehåll

Grundläggande begrepp inom kryptografi (sekretess, autentisering, oavvislighet). Kryptering med symmetrisk nyckel: block- och strömchiffer, konstruktionsprinciper, exempel, och meddelandeautentiseringskoder. Kryptering med öppen nyckel: asymmetriska chiffer, signaturer. Attackmodeller och säkerhetskoncept. Protokoll för nyckelhantering, autentisering och andra tjänster.

Delkurser

1. **Tentamen** *(Written exam),* 6 hp
   Betygsskala: Väl godkänd (VG), Godkänd (G) 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 individuella heminlämningsuppgifter och en individuell skriftlig salstentamen.

Om student som underkänts två gånger på samma examinerande moment önskar byte av examinator inför nästa examinationstillfälle, ska sådan begäran inlämnas skriftligt till kursansvarig institution 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 studenten i normalfallet garanteras tillgång till minst tre provtillfällen (inklusive ordinarie provtillfälle) under en tid av åtminstone ett år med utgångspunkt i kursens tidigare uppläggning.

Betyg

På kursen ges något av betygen Väl godkänd (VG), Godkänd (G) och Underkänd (U).
För att erhålla betyget Godkänd på hela kursen ska studenten vara godkänd på både salstentamen och inlämningsuppgifterna.
För att erhålla betyget Väl godkänd på hela kursen måste studenten vara godkänd på inlämningsuppgifterna och fått betyget Väl godkänd på 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

Det rekommenderas att i förväg ha läst en kurs i statistik och/eller sannorlikhetslära.

Kursen är samläst med Chalmers.