



KURSPLAN

Tillämpad kryptografi Applied Cryptography 5 högskolepoäng (5 credits)

Kurskod: DV2616

Huvudområde: Datavetenskap, Programvaruteknik

Utbildningsområde: Teknik

Utbildningsnivå: Avancerad nivå

Fördjupning: AIN - Avancerad nivå, har endast kurs/er på grundnivå som förkunskapskrav

Undervisningsspråk: Engelska

Gäller från: 2022-08-29

Fastställd: 2022-03-01

1. Beslut

Denna kurs är inrättad av dekan 2021-11-10. Kursplanen är fastställd av prefekten vid institutionen för datavetenskap 2022-03-01 och gäller från 2022-08-29.

2. Förkunskapskrav

För tillträde till kursen krävs minst 120 hp varav minst 90 hp inom det tekniska området och minst 2 års yrkeserfarenhet inom område som är relaterat till mjukvaruintensiv produkt och/eller tjänsteutveckling (visas exempelvis genom intyg från arbetsgivare).

3. Syfte och innehåll

3.1 Syfte

Kursens huvudsakliga syfte är att lära studenterna tillämpa kryptografiska algoritmer och protokoll för att skydda data i rörelse eller i vila från oönskad påverkan. De kunskaper och färdigheter som förmedlas under kursens gång kommer att hjälpa kursdeltagarna förbättra säkerheten för applikationer och tjänster som används och/eller utvecklas i deras organisation.

3.2 Innehåll

Studenterna kommer att lära sig grundläggande säkerhetsmekanismer som till exempel kryptering, digitala signaturer, integritet, autentisering och behörighet. Kursdeltagarna kommer också att studera hur dessa mekanismer kan kombineras för att bygga säkerhetstjänster såsom IP-säkerhet (IPsec) och säker webbkommunikation (TLS/SSL).

Kursen omfattar följande moment:

- Introduktion till kryptografi
- Överblick av de programmeringsspråk som används i kursen
- Genomgång av ramverk som används för att programmera säkerhetsmekanismer och säkerhetstjänster
- Distribution och hantering av krypteringsnycklar med hjälp av digitala certifikat.
- Grunder i IP-säkerhet (IPsec)
- Grunder i säker webbkommunikation (TLS/SSL)
- Säkerhet för data som lagras i molntjänster

4. Lärandemål

Följande lärandemål examineras i kursen:

4.1 Kunskap och förståelse

Efter genomförd kurs ska studenten kunna:

- Redogöra för vilka typer av hot som kan hanteras respektive inte hanteras med hjälp av kryptografi
- Förklara hur grundläggande säkerhetsmekanismer och tjänster fungerar

4.2 Färdighet och förmåga

Efter genomförd kurs ska studenten kunna:

- Implementera grundläggande säkerhetsmekanismer med hjälp av de ramverk som presenterats under kursens gång.
- Hantera krypteringsnycklar och digitala certifikat
- Konfigurera och driva ett Linux-baserad IP-säkert virtuellt privat nätverk (VPN).
- Övervaka och felsöka IPsec och TLS/SSL-anslutningar

4.3 Värderingsförmåga och förhållningssätt

Efter genomförd kurs ska studenten kunna:

- Avgöra fördelar och nackdelar med specifika säkerhetsramverk baserat på de funktioner de tillhandahåller
- Avgöra vilka säkerhetsmekanismer som behövs för att implementera en specifik säkerhetstjänst

5. Läraktiviteter

Undervisningen sker i form av föreläsningar, inspelat videomaterial, samt egna studier av grundläggande litteratur, forskningslitteratur och annat skrivet material. Under kursens gång kommer kommunikation, feedback och diskussioner med lärare och andra deltagare ske via e-post, kursens lärarplattform och via online-möten.

6. Bedömning och examination

Examinationsmoment för kursen

Kod	Benämning	Omfattning	Betyg
2230	Inlämningsuppgift	5 hp	GU

Kursen bedöms med betygen G Godkänd, UX Underkänd, något mer arbete krävs, U Underkänd.

I kurstillfällets information inför kursstart framgår i vilka examinationsmoment som kursens lärandemål examineras samt gällande bedömningsgrunder.

Examinator kan, efter samråd med högskolans FUNKA-samordnare, fatta beslut om anpassad examinationsform för att en student med varaktig funktionsvariation ska ges en likvärdig examination jämfört med en student utan funktionsvariation.

7. Kursvärdering

Kursvärdering ska göras i enlighet med BTH:s beslut om frågeställning i kursvärderingar och beslut om process för hantering och uppföljning av kursvärderingar.

8. Begränsningar i examen

Kursen kan ingå i examen men inte tillsammans med annan kurs vars innehåll, helt eller delvis, överensstämmer med innehållet i denna kurs.

9. Kurslitteratur och övriga lärresurser

Material såsom forskningsartiklar och annat kursmaterial tillhandahålls på kursens lärplattform och via BTHs biblioteksresurser, samt rekommendationer för vidare läsning.