



DD2520 Tillämpad kryptografi

7,5 hp

Applied Cryptography

Fastställande

Kursplan för DD2520 gäller från och med HT19

Betygsskala

A, B, C, D, E, FX, F

Utbildningsnivå

Avancerad nivå

Huvudområden

Datalogi och datateknik

Särskild behörighet

Slutförd kurs DD2395 Datasäkerhet 6 hp, eller motsvarande kurs.

Undervisningsspråk

Undervisningsspråk anges i kurstillfällesinformationen i kurs- och programkatalogen.

Lärandemål

Efter godkänd kurs ska studenten kunna:

- använda grundläggande terminologi inom datasäkerhet och kryptografi korrekt,
- beskriva kryptografiska koncept och förklara deras säkerhetsegenskaper,
- identifiera och kategorisera hot mot ett IT system på en konceptuell nivå,
- hitta och använda dokumentation av kryptografiska bibliotek och standarder,
- analysera beskrivningar av kryptografiska system och protokoll i termer av svartlådekryptografiska primitiver från ett programvaruutvecklingsperspektiv,
- identifiera sårbarheter utifrån systembeskrivningar, uppskatta hotbilden, föreslå motåtgärder mot identifierade hot, samt visa att de är effektiva,
- jämföra motåtgärder, utvärdera deras sidoeffekter, och presentera resonemangen för andra

i syfte att

- som samhällsmedborgare och ingenjör kunna resonera om tillämpad kryptografi i allmänhet och risker med att använda/utveckla kryptografi i synnerhet,
- i arbetslivet och/eller forsknings- och utvecklingsprojekt kunna utvärdera utmaningar inom programvaruutveckling relaterade till kryptografi.

Kursinnehåll

Grundläggande koncept och principer, intuition om säkerhet, implementations- och ingenjörsaspekter samt påverkan på samhället, svartlådeanalys, användande av kryptografiska primitiver som symmetrisk och asymmetrisk kryptering i tillämpningar, digitala signaturer, kryptografiska hashfunktioner, och enklare kryptosystem och protokoll.

Kurslitteratur

Uppgift om kurslitteratur meddelas i kurs-PM.

Examination

- TEN1 - Skriftlig tentamen, 2,5 hp, betygsskala: A, B, C, D, E, FX, F
- LAB1 - Laborationer, 5,0 hp, betygsskala: A, B, C, D, E, FX, F

Examinator beslutar, baserat på rekommendation från KTH:s handläggare av stöd till studenter med funktionsnedsättning, om eventuell anpassad examination för studenter med dokumenterad, varaktig funktionsnedsättning.

Examinator får medge annan examinationsform vid omexamination av enstaka studenter.

När kurs inte längre ges har student möjlighet att examineras under ytterligare två läsår.

Examinator beslutar, i samråd med KTH:s samordnare för funktionsnedsättning (Funka), om eventuell anpassad examination för studenter med dokumenterad, varaktig funktionsnedsättning. Examinator får medge annan examinationsform vid omexamination av enskilda studenter.

Etiskt förhållningssätt

- Vid grupparbete har alla i gruppen ansvar för gruppens arbete.
- Vid examination ska varje student ärligt redovisa hjälp som erhållits och källor som använts.
- Vid muntlig examination ska varje student kunna redogöra för hela uppgiften och hela lösningen.