



DD2520 Tillämpad kryptografi

7,5 hp

Applied Cryptography

Fastställande

Skolchef vid EECS-skolan har 2020-10-13 beslutat att fastställa denna kursplan att gälla från och med VT2021, diarienummer: J-2020-1831.

Betygsskala

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

Utbildningsnivå

Avancerad nivå

Huvudområden

Datalogi och datateknik

Särskild behörighet

Slutförd kurs i datasäkerhet motsvarande DD2395.

Aktivt deltagande i kursomgång vars slutexamination ännu inte är Ladokrapporterad jämförelses med slutförd kurs.

Den som är registrerad anses vara aktivt deltagande. Med slutexamination avses både ordinarie examination och det första omexaminationstillfället.

Undervisningsspråk

Undervisningsspråk anges i kurstillfällesinformationen i kurs- och programkatalogen.

Lärandemål

Efter godkänd kurs ska studenten kunna:

- korrekt använda grundläggande terminologi inom datasäkerhet och kryptografi
- beskriva kryptografiska koncept och förklara deras säkerhetsegenskaper
- hitta och använda dokumentation av kryptografiska bibliotek och standarder
- identifiera och kategorisera hot mot ett kryptografiskt IT-system på en konceptuell nivå, föreslå lämpliga motåtgärder, 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 för kryptografi, 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 samt enklare kryptosystem och protokoll.

Examination

- INL1 - Inlämningsuppgifter, 2,5 hp, betygsskala: P, 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.

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.