IV1013 Introduktion till datasäkerhet 7,5 hp

Introduction to Computer Security

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

Fastställande

Kursplanen gäller från och med VT 2024 enligt skolchefsbeslut: J-2023-2212.Beslutsdatum: 2023-10-10

Betygsskala

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

Utbildningsnivå

Grundnivå

Huvudområden

Teknik

Särskild behörighet

Kunskaper och färdigheter i Javaprogrammering, 6 hp, motsvarande slutförd kurs ID1018/DD1337 alternativt en slutförd kurs i grundläggande programmering som DD1310-DD1319/DD1321/DD1331/DD100N kombinerad med en slutförd kurs i Javaprogrammering motsvarande DD1380.

Kunskaper i maskinnära programmering, 6 hp, motsvarande slutförd kurs IS1200/IS1500/EP1200.

Kunskaper i nätverk och kommunikation, 6 hp, motsvarande slutförd kurs IK1203/EP1100.

Kunskaper i diskret matematik, 6 hp, motsvarande slutförd kurs IX1500/SF1610/SF1630/SF1662/SF1679/SF1688.

Aktivt deltagande i kursomgång vars slutexamination ännu inte är Ladokrapporterad jämställs 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

- förklara grundläggande mekanismer i och uppbyggnaden av säkra kommunikationsprotokoll
- beskriva svagheter i datorsystem, programvara, nätverk och kommunikationsprotokoll samt förklara attacker som utnyttjar svagheterna
- förklara och jämföra för- och nackdelar med vanliga kryptografiska tekniker
- designa och implementera enklare kryptografiska tillämpningar
- redogöra för och känna igen hot mot informationssäkerhet: konfidentialitet, integritet och tillgänglighet samt välja lämpliga metoder för att skydda sig mot hot
- designa, implementera och utvärdera säkerhet i nätverk

i syfte att få en introduktion till grunderna inom kryptografi, säkerhet inom datorsystem och nätverkssäkerhet

Kursinnehåll

- Grundläggande kryptografi: symmetrisk och assymetrisk kryptografi.
- Kryptografisk hashning och digitala signaturer.
- Säkerhet i Internets protokoll och tjänster.
- Certifikat och infrastrukturer för öppen nyckel-kryptering.
- Säkerhet i nätverkssystem: routrar, brandväggar och system för att detektera intrång.
- Säkerhet i operativsystem.
- Mjukvarusäkerhet: sårbarhet, attacker och skyddsmekanismer.

Examination

- PRO1 - Projektuppgift, 6,0 hp, betygsskala: A, B, C, D, E, FX, F
- TENT - Digital examination, 1,5 hp, betygsskala: P, 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.

TENT genomförs som kontinuerlig digital examination och ges på engelska. Skriftliga lösningar får lämnas på svenska eller engelska.

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.