DD2448 Kryptografins grunder 7,5 hp

Foundations of Cryptography

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-2023-1556.Beslutsdatum: 2023-06-07

Betygsskala

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

Utbildningsnivå

Avancerad nivå

Huvudområden

Datalogi och datateknik

Särskild behörighet

Kunskaper i algoritmer och komplexitet, 7,5 hp, motsvarande slutförd kurs DD2350/DD2352.

Kunskaper i diskret matematik, 7,5 hp, motsvarande slutförd kurs SF1610/SF1630/SF1662/SF1679/SF1688.

Kunskaper i sannolikhetslära och statistik, 6 hp, motsvarande slutförd kurs SF1912/SF1914/SF1915/SF1916/SF1920/SF1921/SF1922/SF1923/SF1924.

Kunskaper i algebra och geometri, 7,5 hp, motsvarande slutförd kurs SF1624/SF1672.

Kunskaper i envariabelanalys, 7,5 hp, motsvarande slutförd kurs SF1625/SF1673.

Gymnasiekursen Engelska B/6.

Undervisningsspråk

Undervisningsspråk anges i kurstillfällesinformationen i kurs- och programkatalogen.

Lärandemål

Efter godkänd kurs ska studenten kunna

- diskutera följande grundläggande begrepp inom kryptografi: symmetrisk och asymmetrisk kryptering, digitala signaturer, kryptografiska hashfunktioner, samt starka pseudoslumptalsgenerator
- redogöra för exempel på ovanstående begrepp
- genomföra enkla egna analyser av kryptografiska konstruktioner såsom kryptosystem och kryptografiska protokoll
- avgöra tillförlitligheten hos analyser av kryptografiska konstruktioner såsom kryptosystem och kryptografiska protokoll
- sammanfatta innehållet i tekniska artiklar om kryptografi och kryptografiska protokoll

i syfte att kunna arbeta med analys och utveckling av kryptografiska protokoll och system.

Kursinnehåll

Klassiska kryptosystem. Vad innebär säker kryptering? Bakgrund inom informationsteori, entropi. Symmetriska krypteringsalgoritmer som t.ex. Advanced Encryption Standard (AES). Öppna nyckelsystem för kryptering och digitala signaturer t.ex. RSA-, ElGamal- och Schnorrsignaturer. Kryptografiskt säkra hashfunktioner i teori och praktik (SHA). Egenskaper för och exempel på pseudoslumptalsgeneratorer. Anknytningar till komplexitetsteori.

Examination

- GRU1 - Grupparbete, 2,5 hp, betygsskala: P, F
- INDA - Individuell hemuppgift, 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.

GRU1 är ett utredande grupparbete om ett ämne som beskrivs i vetenskapliga artiklar och/eller föreslagna eller fastställda standarder. Det examineras genom en skriftlig rapport och/eller muntlig presentation.

INDA är en uppsättning problem som löses individuellt och examineras både skriftligt och muntligt.

Övergångsbestämmelser

Den utgångna modulen ÖVN1 har ersatts av GRU1 och INDA.

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.