



DD2448 Kryptografins grunder

7,5 hp

Foundations of Cryptography

Fastställande

Skolchef vid EECS-skolan har 2020-04-21 beslutat att fastställa denna kursplan att gälla från och med HT 2020, diarienummer: J-2020-0751.

Betygsskala

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

Utbildningsnivå

Avancerad nivå

Huvudområden

Datalogi och datateknik

Särskild behörighet

För fristående kursstuderande:

SF1604 Linjär Algebra, SF1625 Envariabelanalys, SF1626 Flervariabelanalys, SF1901 Sannolikhetsteori och statistik, DD1337 Programmering, DD1338 Algoritmer och Datastrukturer, DD1352 Algoritmer, Datastrukturer och Komplexitet, SF1630 Diskret Matematik eller motsvarande kurser.

Undervisningsspråk

Undervisningsspråk anges i kurstillfällesinformationen i kurs- och programkatalogen.

Lärandemål

Efter genomgången kurs ska en elev kunna

- Diskutera följande grundläggande begrepp inom kryptografi: symmetrisk och asymmetrisk kryptering, digitala signaturer, kryptografiska hashfunktioner, samt starka pseudoslump-talsgenerator. Att kunna redogöra för exempel på samtliga begrepp.
- Genomföra enkla egna analyser av kryptografiska konstruktioner såsom kryptosystem och kryptografiska protokoll.
- Läsa andras analyser av kryptografiska konstruktioner såsom kryptosystem och kryptografiska protokoll och avgöra dessa analysers tillförlitlighet.
- Tillgodogöra sig tekniska artiklar om kryptografi och kryptografiska protokoll.

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 Schnorr-signaturer. Kryptografiskt säkra hashfunktioner i teori och praktik (SHA). Egenskaper för och exempel på pseudoslump-talsgeneratorer. Anknytningar till komplexitetsteori.

Examination

- ÖVN1 - Övningsuppgift, 7,5 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 enskilda studenter.

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

Övriga krav för slutbetyg

Inlämningsuppgifter (ÖVN1; 7,5 hp).

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.