DD2448 Kryptografins grunder 7,5 hp

Foundations of Cryptography

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

Fastställande

Kursplan för DD2448 gäller från och med HT09

Betygsskala

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

Utbildningsnivå

Avancerad nivå

Huvudområden

Datalogi och datateknik

Särskild behörighet

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 asymetrisk kryptering, digitala signaturer, kryptografiska hashfunktioner, samt starka pseudoslumptalsgenerator. 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 Schnorrsignaturer. Kryptografiskt säkra hashfunktioner i teori och praktik (SHA). Egenskaper för och exempel på pseudoslumptalsgeneratorer. Anknytningar till komplexitetsteori.

Kurslitteratur

Stinson, Cryptography; theory and practice, Chapman & Hall.

Examination

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.

I denna kurs tillämpas skolans hederskodex, se: http://www.kth.se/csc/student/hederskodex.

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.