HÖGSKOLAN DALARNA

Kursplan

Kryptografi 7,5 högskolepoäng, Grundnivå

Cryptography 7.5 Credits*, First Cycle

Lärandemål

Efter avslutad kurs ska studenten kunna:

- Förklara kryptografiska begrepp
- Jämföra symmetriska och asymmetriska krypteringsmetoder
- Tillämpa hash algoritmer inom digitalt forensiska situationer och autentiseringstjänster
- Genomföra en enklare kryptoanalytisk attack
- Integrera kryptografiska enheter i mjukvaror på ett säkert sätt
- Tillämpa blockkedje-baserade lösningar
- Bedöma den kryptografiska styrkan i ett system
- Värdera kryptografins samhälleliga roll utifrån såväl ett socialt, etiskt som ekonomiskt perspektiv.

Innehåll

Kursen börjar med en historisk och vetenskapligt introduktion till kryptografi, Kerchoffs princip och det grundläggande arbetet av Shannon och Feistel. De senare etablerade en teoretisk grund för symmetriska krypteringssystem.
Symmetriska krypteringssystem introduceras, med tonvikt på standarder som DES, 3DES, AES och andra kandidat system. Ett symmetriskt krypteringssystem omformas till både ett strömchiffer och en slumpgenerator för nyckelprodukten. Nackdelar hos symmetriska krypteringssystem diskuteras, med fokus på nyckel-distributions problemet. Asymmetriska krypteringssystem visas som en lösning till nyckel-distributions problemet. Alternativa lösningar av Diffie-Hellman och RSA algoritmer utforskas. Asymmetrisk kryptering för autentisering används. Kombinerade symmetriska och asymmetriska krypteringssystem studeras, med PGP-system som praktisk tillämpning. Hash algoritmer studeras, med tillämpning inom digital forensiska situationer. Kryptoanalys introduceras med fokus på “brute force“ attacker, differential- och linjär kryptanalys och side-channel attacker. Olika kryptoanalytiska situationer karakteriseras enligt kvantitet och typ av empiriska data. Blockkjedjor och digitalvalutor introduceras.

* 1 Credit = 1 ECTS

Examinationsformer
Skriftlig hemtentamen som redovisas muntligt 5 hp och laborationsrapporter 2,5 hp.

Arbetsformer
Lektioner och laborationsarbete.

Betyg
Som betygsskala används U–VG.

Betygets nivå fastställs genom tentamen, vilket också blir slutbetyget under förutsättning att laborationer redovisats. Laborationer betygsätts i betygsskalan U/G.

Förkunskapskrav
Grundläggande programmering 7,5 hp

Övrigt
Ersätter DT2017.

Ämnestillhörighet:
Mikrodataanalys

Ämnesgrupp:
Övriga tvärvetenskapliga studier

Utbildningsområde:
Naturvetenskapliga området, 100%

Kursen kan ingå i följande huvudområde(n):
1. Mikrodataanalys

Fördjupningsbeteckning för respektive huvudområde:
1. G1F

Fastställd:
Fastställd 2019-02-21
Kursplanen gäller fr.o.m. 2019-05-06