

Krypteringsmetoder och säkring av datasystem 7,5 hp

Cryptography Methods and Computer Security 7.5 credits

Grundnivå

Progression: 61-90

Huvudområde: Digital forensik, grundnivå, har mindre än 60 hp kurs/er på grundnivå som förkunskapskrav (GIF)

Kursplanen är fastställd av Forsknings- och utbildningsnämnden (2018-11-14) och gäller studenter antagna vårterminen 2020.

Kursens inplacering i utbildningssystemet

Kursen ingår i programmet IT-forensik och informationssäkerhet 180 hp.

Behörighetskrav

Nätverkssäkerhet 7,5 hp, Riskanalys och IT-säkerhetssystem 7,5 hp och Tillämpad matematik och statistik för IT-forensik 15 hp.

Kursens mål

Kursen syftar till att ge en introduktion till hantering av kryptering och andra aspekter av säker datorkommunikation.

Efter avslutad kurs ska studenten kunna:

Kunskap och förståelse

- ange viktiga egenskaper för säker och tillförlitlig dator-kommunikation

Färdighet och förmåga

- konstruera system för kommunikation med publika nycklar
- genomföra frekvensanalys och resträkning
- beräkna sannolikhet för lyckad överföring av information
- använda algoritmer för faktorisering, diskret exponering och för beräkning av diskret logaritm

Värderingsförmåga och förhållningssätt

- ange svagheter och styrkeområden med vanliga krypterings- och dechiffereringsmetoder
- bedöma lämplighet vid val av nyckelprotokoll i kombination med krypteringslösningar i datornätverk.

Kursens huvudsakliga innehåll

Moduloräkning, digital signering, RSA-kryptot. Autentisering, Kerberos, Publika nycklar. Symmetriska krypton som AES och XOR. Postkvantkryptering som NTRU. Nyckelöverföring. Säkerhetsprinciper. Hashfunktioner. Steganografi. Överföringskvalitet. Detektering av krypterad kod.

Undervisning

Föreläsningar, övningar och datorlaborationer.

Undervisningen bedrivs normalt på svenska men undervisning på engelska kan förekomma.

Examination

Som betyg för hel kurs används något av uttrycken Underkänd, 3, 4 eller 5.

Skriftlig tentamen och rapportering av resultat från datorlaborationer.

Examinationsmoment		Betyg
Laboration 1	1,5 hp	U/G
Laboration 2	1,5 hp	U/G
Laboration 3	1,5 hp	U/G
Tentamen	3 hp	U/3/4/5

Om studenten har fått beslut från Högskolan i Halmstad om särskilt pedagogiskt stöd på grund av funktionsnedsättning, har examinator rätt att besluta om ett anpassat examinationsmoment eller låta studenten genomföra examinationen på ett alternativt sätt.

Kursvärdering

I kursen ingår kursvärdering. Denna ska vara vägledande för utveckling och planering av kursen. Kursvärderingen ska dokumenteras och redovisas för studenterna.

Kurslitteratur och övriga läromedel

Järpe, Eric *Räkna med rester - matematik att tillämpas inom kryptologi*. Studentlitteratur, 2013.

Gollmann, D. *Computer Security*, 3:e upplagan, Wiley, 2011.

Singh, Simon. *The Code Book*. Fourth Estate Ltd, 2000.