



Kungliga Tekniska högskolan  
STH Teknik och hälsa

FREDRIK ÅKERSTRÖM  
KOLDINGGATAN 3 3TR  
164 46 KISTA

Studieintyg för

800105-8257 FREDRIK ÅKERSTRÖM

Avslutade kurser

-----	Hp	Betyg	Datum
IT-säkerhet I	7.5	A	2007-12-20
Projektuppgift	( 1.5)	P	2007-12-20
Projektuppgift	( 1.5)	P	2007-12-20
Projektuppgift	( 1.5)	P	2007-12-20
Tentamen	( 3.0)	A	2007-12-20

-----  
Summa totalt: 7.5 högskolepoäng

Ovanstående är ett utdrag ur registret för studiedokumentation.

Stockholm den 15 januari 2008

  
.....  
Therese Röstlund

60 högskolepoäng motsvarar ett års heltidsstudier.

**Kungl. Tekniska Högskolan**  
KTH Teknik och hälsa  
Marinens väg 30  
136 40 Haninge

## HI117V IT-säkerhet I 7,5 hp

IT-Security I Kursnivå (A-D) C Huvudområde  
Utbildningsnivå Grundnivå Betygsskala A, B, C, D, E, FX, F

Visa tillfällen då kursen ges

Kursmål

Efter genomgången kurs skall deltagarna ha god kännedom om modern IT-säkerhet. I kursen ingår bl a IPSec, kryptering av e-post och filer, VPN, WEP, kryptoalgoritmer och kryptoanalys. Kursen är praktiskt orienterad och analyserar verklighetsbaserade hotbilder mot typiska system och applikationer. Under vårterminen kommer det sedan att erbjudas möjlighet att bygga på denna kurs med IT-säkerhet II: undersökningar, med kurskod HI119V, även den på 7,5 hp.

Kursinnehåll

Overview; Classical Encryption Techniques, Block Ciphers and the Data Encryptions Standard; Introduction to Finite Fields, Advanced Encryption Standard; Contemporary Symmetric Ciphers; Confidentiality using Symmetric Encryption; Introduction to Number Theory; Public-Key Cryptography; Message Authentication and Hash Functions; Hash and Mac Algorithms; Digital Signatures and Authentication Protocols; Authentication Applications; Electronic Mail Security; IP Security; Web Security; Intruders and Viruses; Firewalls; Standards and Standard-setting Organizations; Project for Teaching Cryptography and Network Security.

Kursupplägg

Kursen är en distanskurs som ges på ca halvtid. Under kursen erbjuds frivilliga kursmöten i form av heldagslaborationer i Haninge fem lördagar. Allt kursmaterial är på engelska. Det är fullt möjligt att genomföra hela kursen på distans. En kursdeltagare bör reservera ca 20-30 timmar/vecka för denna kurs, inkl. projektuppgifter och laborationer, lite beroende på tidigare utbildning och yrkeserfarenhet. Som extra kursstöd genomförs de frivilliga kursmötena utan närvaroplikt på lördagar (09-16) på Campus Haninge.

Behörighet

Grundläggande behörighet (avslutad gymnasieutbildning el motsv inkl svenska och engelska) krävs.

Rekommenderade förkunskaper

Inga speciella förkunskaper krävs.

Litteratur

Kursmaterial kan rekvireras från Högskolans Bokservice på KTH Syd, Campus Haninge, telefon: 08-790 4885; e-post: bokservice@sth.kth.se. Kursbok: Cryptology and Network Security, 3:e upplagan, William Stallings, Prentice-Hall, ISBN 0-13-091429-0 (inbunden). Kurskompendium HI117V på CD-ROM med föreläsningmaterial, studieanvisningar och övningsuppgifter, programvara och referensmaterial. Förf. L.O. Strömberg.

Utrustningskrav

Tillgång till dator (PC med Windows 2000 eller XP), browser och Internetanslutning krävs. Två fungerande e-postadresser är obligatoriska och måste anges i ansökan. Kursinformation utsändes endast per e-post. Inlämning av projektuppgifter kan endast ske via e-post. Vi använder SSS - Student Support System - i denna kurs. Detta Internetbaserade kurssupportsystem är skräddarsytt för yrkesverksamma studenter, som på ett säkrat sätt behöver kunna komma åt kursmaterial inifrån företag, myndigheter och länder med

restriktiva brandväggar, vilka oftast omöjliggör användning av traditionella utbildningsprogram, som kräver specifika öppna portar i organisationens brandvägg.

Examination

ANN1 - Projektuppgift, 1,5 hp, betygsskala: P, F

ANN2 - Projektuppgift, 1,5 hp, betygsskala: P, F

ANN3 - Projektuppgift, 1,5 hp, betygsskala: P, F

TEN1 - Tentamen, 3,0 hp, betygsskala: A, B, C, D, E, FX, F

Tentamen ges i början av december, med möjlighet till omtenta i maj och i augusti. Tentamen, som är datorbaserad och på engelska, består av ca 60 flervalsfrågor och ca 8 beräknings/textfrågor. Tentamen kan avläggas på KTH i Haninge eller, på begäran, på annat svenskt eller internationellt universitet eller svensk ambassad. Tentamen är på 3 poäng med betygsskala A-F. Resterande poäng är för projektuppgifter.

Ges av

STH/Datateknik och telekommunikation

Kontaktperson

Maria Nihlén, tel: 08-7909811, fax: 08-7904800, e-post: maria.nihlen@sth.kth.se

Examinator

Lars-Olov Strömberg, tel: 08-7909800, 0706-388239, fax: 0706-158239, e-post: los@kth.se

Övrig information

Textbok och kurskompendium säljs i Haninge i samband med första kursmötet, men kan även beställas per e-post (bokservice@sth.kth.se). Undervisningen är avgiftsfri, men kursmaterialet betalas, ca 1000 kr (textbok, kurskompendium på CD-ROM skivor). Textboken och kursmaterialet är på engelska. För att kunna närvara på de frivilliga kursmötena på lördagar krävs ett inpasseringskort till KTH Campus Haninge, som säljs i anslutning till det första lördagsmötet till de kursantagna som bekräftat sitt kursdeltagande senast 10 dagar före kursstarten. Detta inpasseringskort måste hämtas personligen i samband med kursstarten. För att vi så snabbt som möjligt ska kunna skicka ut ytterligare kursinformation till dig per e-post, ber vi dig skicka oss en e-post med ditt namn och två alternativa e-postadresser, samtidigt som du skickar in din kursansökan till KTH. Skicka din e-post till sss@sth.kth.se. Skriv "HI117V kursansökan" i rubriken. Detaljerad kursinformation utsändes per e-post några veckor före kursstarten. Denna kurs erbjuds även som en kundanpassad kontraktsutbildning, som kan genomföras i uppdragsgivarens lokaler. I mån av plats kommer vi att anta nya sökande även efter sista ansökningsdag.

Versionsinformation

Kursplan giltig från och med HT07

Senast ändrad: 2008-05-22