HI117V IT-säkerhet I 7,5 hp

IT-Security I

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

Fastställande

Kursplan för HI117V gäller från och med HT12

Betygsskala

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

Utbildningsnivå

Grundnivå

Huvudområden

Elektroteknik,Teknik

Särskild behörighet

Grundläggande behörighet. Undantag från kunskaper i svenska ges när undervisningsspråk är engelska.

Undervisningsspråk

Undervisningsspråk anges i kurstillfällesinformationen i kurs- och programkatalogen.

Lärandemål

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

The course consists of the following topics:

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 (beroende på studentens förkunskaper).

Under kursen erbjuds frivilliga kursmöten i form av föreläsningsseminarier samt tentamen under fem lördagar 09-16. Allt kursmaterial är på engelska. Det är fullt möjligt att genomföra hela kursen på distans. En kursdeltagare bör reservera ca 20-35 timmar/vecka för denna kurs, inkl. projektuppgifter och laborationer, lite beroende på tidigare utbildning och yrkeserfarenhet.

Kurslitteratur

Computer Security: Principles and Practice;

William Stallings, Lawrie Brown; 2008, 880 pp. Prentice Hall;

ISBN-10: 0136004245

ISBN-13: 9780136004240

Classical and Contemporary Cryptology;

Richard J. Spillman 2004, 304 pp

Prentice Hall,

ISBN-10: 0131828312

ISBN-13: 978-0131828315

/This book is included in the Digital Course Notes, with author´s permission/

Digital Course Notes IT-Sec I, 3 CDs, 1.5 GB, L.O. Stromberg

Utrustning

Tillgång till dator (PC med Windows Windows XP/ Vista/ 7), browser och Internetanslutning krävs. Två fungerande e-postadresser är obligatoriska. 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

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.

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 minst 30 dagar i förväg, på annat svenskt eller internationellt universitet eller svensk ambassad. Tentamen är på 3 poäng med betygsskala A-F. Resterande poäng är för projektuppgifter.

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.