LUNDS UNIVERSITET
Lunds Tekniska Högskola

Kursplan för kalenderåret 2005

SÄKRA SYSTEM OCH APPLIKATIONER EIT015

Secure Systems and Applications

Antal poäng: 5. **Betygskala:** TH. **Valfri för:** C4, D4, E4. **Kursansvarig:** Professor Ben Smeets, Inst f informationsteknologi. **Rekommenderade förkunskaper:** EIT060 Datasäkerhet (5p) eller EDI051 Kryptoteknik (5p). **Prestationsbedömning:** Obligatoriska hemuppgifter och projektuppgifter samt laborationer som ger betyg 3 eller 4. Efter betyg 4 på kursarbetet sker skriftlig tentamen för betyg 5. **Övrigt:** Kursen kan komma att ges på engelska. **Hemsida:** http://www.it.lth.se.

Mål
Målet med kursen är att visa hur olika säkerhets protokoll och kryptografiska metoder tillämpas för att skapa säkra applikationer samt att visa hur man ska analysera system där datorintrång har förekommit. Studenten kommer att bli förtrogen med de viktigaste grundmekanismer och får insikt hur man använder dessa mekanismer på ett korrekt sätt för att få en säker applikation.

Innehåll
Public Key Infrastructure (PKI) (certifikat, revokering, CA, RA, X509), XML-signaturer, E-commerce (Amazon.com, SET, E-cash), DRM (ebook, OMA DRM Phase 2), Smarta kort (grund koncept, ISO standard, attacker, GSM/WIM, bank/cash kort, token), Säkra nätverk (revisit: IPSEC/VPN, TLS, SSL och GSM/UMTS, Computer Forensics

Litteratur
Föreläsningsanteckningar samt artiklar.