Information page for written examinations at Linköping University

Examination date	2019-03-01
Room (1)	TER2(18)
Time	14-18
Edu. code	TDDD82
Module	TEN1
Edu. code name **Module name**	Project Semester including Bachelor Thesis Project: Secure, Mobile Systems (Projekttermin inklusive kandidatprojekt: Säkra, mobila system) Written examination in information security (Informationssäkerhet: Skriftlig tentamen)
Department	IDA
Number of questions in the examination	10
Teacher responsible/contact person during the exam time	Niklas Carlsson (+extra)
Contact number during the exam time	013-282644
Visit to the examination room approximately	ca 16:00
Name and contact details to the course administrator (name + phone nr + mail)	Veronica Kindeland Gunnarsson veronica.kindeland.gunnarsson@liu.se 013-285634
Equipment permitted	None.
Other important information	
Number of exams in the bag	

TEN 1

Skriftlig tentamen

TDDD82 Projekttermin inklusive kandidatprojekt: Säkra, mobila system

2019-03-01

Tillåtna hjälpmedel
Inga

Jourhavande lärare
Niklas Carlsson

Betyg
Ditt betyg på säkerhetsdelen av kursen avgörs av hur många poäng du får på tentamen. Nedanstående betygsgränser är preliminära.

Betyg	3	4	5
Poäng	33	40	46

Instruktioner
För varje fråga står det i fetstil hur många poäng frågan är värd. För varje deluppgift står det sedan hur många poäng man maximalt kan få för deluppgiften. Se exemplet nedan (exemplet ingår inte i tentamen). Totalt ger uppgiften 4 poäng, och man kan svara på de två första deluppgifterna för att få 2 av dessa 4 poäng.

Fråga 0: Historia (4p)

(a) I vilket land föddes Alan Turing? (1p)

(b) Var Alan Turing aktiv vid Bletchley Park? (1p)

(c) Förklara vad man menar med en *Turing Machine*. (2p)

Fråga 1: Säkerhetsbegrepp, policy och mekanism (5p)

(a) Rita en bild och förklara vad det innebär att en säkerhetsmekanism är säker, exakt, och bred? (3p)

(b) Man brukar tala om två olika typer av integritet, namnge och förklara dessa. (2p)

Fråga 2: Kryptoteknik (10p)

(a) Använd punktlista/bild (med tydliga steg) och ekvationer till att förklara hur man tar fram de publika och privata nycklarna i RSA, samt hur man krypterar och dekrypterar meddelanden. (3p)

(b) Använd bild (med meddelanden) och ekvationer till att förklara hur man tar fram en gemensam hemlig nyckel med hjälp av Diffie-Hellman. (3p)

(c) Varför används en initialisation vector (IV)? (2p)

(d) Rita två diagram, ett som visar hur ECB mode fungerar och ett som visar hur CBC mode fungerar. Ge en kort förklaring till diagrammen. (2p)

Fråga 3: Accesskontroll (4p)

Givet tre klienter C_1, C_2 och C_3 (subjekt) samt fyra servrar S_1, S_2, S_3, S_4 (objekt), skapa en accesskontrollmatris och en access control list för detta system så att policyn nedan uppfylls. (4p)

- C_1 får läsa (r), skriva (w) och exekvera (x) kod på S_1.
- C_2 får läsa och skriva kod på S_4.
- C_2 får skriva kod på S_2.
- C_3 får läsa och exekvera kod på S_2.
- C_3 får skriva kod på S_1.
- Om inget annat anges så ges inga rättigheter.

Fråga 4: Policymodeller (5p)

Förklara Biba integrity model när *strict integrity policy* används. Förklara med ett exempel så att det är tydligt vilka koncept som ingår och vilka funktioner som används. Det skall bland annat vara tydligt vilka regler som gäller för läsning och skrivning och hur dessa regler är definierade. (5p)

Fråga 5: Hash-funktioner (6p)

(a) Antag att A och B har en hemlig nyckel k. Redogör för hur A och B kan garantera att meddelanden de skickar till varandra inte ändras under transport utan att det upptäcks. (3p)

(b) Låt m_1 och m_2 vara klartext-meddelanden och H en hash-funktion. För varje egenskap nedan, **motivera kort** om egenskapen är önskvärd eller icke-önskvärd av H.

(1) Om $m_1 = m_2 + m_2$ så ska $H(m_1) = H(m_2) + H(m_2)$. (1p)

(2) Antalet bitar i $H(m_1)$ ska vara exakt lika många som i m_1. (1p)

(3) Det måste existera en funktion H^{-1} sådan att $m_1 = H^{-1}(H(m_1))$. (1p)

Fråga 6: Autentisering (4p)

(a) Beskriv hur en man-in-the-middle attack går till under nyckelutbyte med RSA. (2p)

(b) Förklara hur tidsbaserade lösenord fungerar. (2p)

Fråga 7: Certifikat (4p)

(a) I ett X.509 certifikat, vad finns i fältet *subject*? (1p)

(b) Hur avgör man om ett certifikat är giltigt? Förklara i steg-för-steg hela processen. (3p)

Fråga 8: Designprinciper (4p)

Förklara följande designprinciper:

(a) Principle of open design. (2p)

(b) Principle of psychological acceptability. (2p)

Fråga 9: Riskanalys (10p)

(a) Med en kort mening per steg, tydligt namnge och förklara de sju stegen som används av CORAS. (2p)

(b) Trots att CORAS är en kvalitativ metod så kan man ändå estimera risk genom de två faktorerna sannolikhet och konsekvens. Hur? (2p)

(c) Förklara genom ett exempel hur man skapar attack träd (alla byggstenar som vi diskuterat i kursen skall förklaras). (2p)

(d) För ovan scenario, tydligt klargör antaganden om den potentiella "attacker" (i.e., your "threat model"), och beskriv de "CIA" som är applicerbara här och förklara varför. (2p)

(e) Förklara begreppet *analysis paralysis*. (2p)

Bonus Fråga 10 [endast orginaltenta]: Random topic (4p)

(a) Redogör för algoritmen som används när man beräknar ett HMAC värde? (3p)

(b) Ska output från en hash-funktion vara det samma om man använder den på samma input två gånger (motivera kort)? (1p)