Tentamen i Säkerhet (EDA625) för IT-programmen

060426 kl. 8.00 – 12.00

INGA HJÄLPMEDEL

Maxpoängen för provet är totalt 60 poäng. För betyget 3 krävs minst 30 poäng som får vara fördelade godtyckligt mellan uppgifterna. Lycka till !

1. Beskriv dom tänkbara svagheter som kan finnas hos en krypteringsalgoritm. (3p)

2. Beskriv dom svagheter som finns hos krypteringsalgoritmen DES och beskriv dom åtgärder som vidtas för att kompensera för svagheterna hos DES-algoritmen. (3p)

3. Beskriv dom svagheter som finns hos krypteringsalgoritmen RSA och beskriv dom åtgärder som vidtas för att kompensera för svagheterna hos RSA-algoritmen. (3p)

4. Det traditionella syftet med kryptering är sekretesskydd, d.v.s. att hemlighålla meddelanden. Antag nu att vi har ett system utan krav på sekretess, men där korrekthet hos meddelanden, identifiering av avsändare och hög hastighet vid databehandling och överföring är viktiga. Beskriv de verktyg som behövs för att lösa säkerhetsproblemen. (6p)

5. Antag att ett krav på sekretess tillkommer i det system som du diskuterat i uppgift 4. Beskriv dom ändringar som behöver göras då sekretesskravet tillkommit. (3p)

6. Vid symmetrisk kryptering brukar nyckellängden 128 bitar anses fullt tillräcklig. Vid asymmetrisk kryptering däremot anses 512 bitar otillräckligt. Förklara varför asymmetrisk kryptering kräver större nyckellängd än symmetrisk kryptering. (3p)

7. Förklara vad som menas med en envägsfunktion och ge två exempel på situationer då envägsfunktioner används. (3p)

8. Förklara begreppen digital signatur och certifikat (innehåll och användningsområde). (6p)

VÄND!

9. Datorerna i ett sjukhus är uppkopplade mot internet samt mot ett intranet. Externt behöver man, förutom att söka allmänt på webben liksom i olika specialdatabaser, också kontakt med andra intressenter. Det kan vara andra sjukhus, analysföretag, olika leverantörer, kommunala organ inom vård och omsorg mm …

   Du skall utifrån en sårbarhetsanalys, så som du uppfattar det
   a) bedöma i vilken grad de olika säkerhetskriterierna berörs av sjukhusets datorsystem (5p)
   b) föreslå lösningar för hur nätet och trafiken kan struktureras för att skydda sig mot olika tänkbara/sannolika hot. (5p)

10. Redogör för skillnaden på en trojansk häst och ett virus. Hur kan man skydda sig mot dem. (3p)

11. Att skydda sina lösenord är viktigt eftersom ett intrång ofta börjar med att hitta eller k komma runt lösenordsskyddet. Beskriv hur man skall välja ett bra lösenord samt hur ett b bra OP-system kan skydda lösenord och lösenordsfilen. (3p)

12. Bell LaPadula, Biba och Clark-Wilson är tre datasäkerhetsmodeller. Ange vad var och en av dem har för huvudprincip samt vilket/vilka av de tre säkerhetskriterierna respektive modell berör. (4p)

13. Förklara kort begreppen: DoS-attack, Buffer overflow, IP-spoofing och controlled invocation. (4p)

14. Vad är skillnaden mellan en vanlig brandvägg och en proxy-server? Ange några typiska egenskaper hos en proxy-server. (3p)

15. Vad är ett behörighetskontrollsystem? Ange huvuduppgift och principiell funktion. (3p)