Tietoturvallisuuden jatkokurssi, osa A

Välikoe 8.12.2010

---

1. **Jos joku keksii samasta tekstistä kaksi variaatiota, joilla on sama tiiviste, hän voi luoda niille digitaalisen allekirjoituksen tuntematta yksityistä avainta.**
   a. ( ) Tosi b. ( ) Epätosi

2. **Käyttäjien autentikointiin on suppeassa tietoverkossa luontevampaa käyttää julkista avainta ja laajassa verkossa jotain symmetristä menetelmää.**
   a. ( ) Tosi b. ( ) Epätosi

3. **Kryptologisessa hierarkiassa algoritmista ihmiseen on mahdollista, että kryptoprotokolla esiintyy toisen kryptoprotokollan osana.**
   a. ( ) Tosi b. ( ) Epätosi

4. **Sokean allekirjoituksen vastaanottajan on ensin purettava pois sokaisutekijä ennen kuin hän voi tarkistaa onko allekirjoitus oikea.**
   a. ( ) Tosi b. ( ) Epätosi

5. **Jos RSA-salauksen purkueksponentti on f, niin RSA-salauksen purkava ohjelma joutuu tekemään f-1 kappaletta modulaarisia kertolaskuja.**
   a. ( ) Tosi b. ( ) Epätosi

6. **Olet lähettämässä luottamuksellista viestiä jollekulle A:lle, jonka PGP-avainrenkaasta löytyy sinun julkinen avaimesi. Väittämä: A:n avainrenkaassa tätä avainta varmentamassa olevat allekirjoitukset vaikuttavat siihen, miten hyvin A uskoo viestin voineen pysyä vain sinun ja A:n välisenä, mutta eivät vaikuta siihen, miten sinä voit suhtautua tähän seikkaan.**
   a. ( ) Tosi b. ( ) Epätosi

7. **ElGamalin salausalgoritmissa salateksti saadaan kertomalla selkoteksti satunnaisella avaimella modulo p ja ilmoittamalla avain Diffie-Hellman -tyyppisesti samassa viestissä.**
   a. ( ) Tosi b. ( ) Epätosi

8. **Avaimensalausavaimen kryptoperiodi on lyhyempi kuin istuntoavaimen.**
   a. ( ) Tosi b. ( ) Epätosi

9. **Jos kryptoanalyytikko haluaa murtaa jonkin salatekstin hänelle ei ole apua muista samalla avaimella salatuista teksteistä, jos hän ei tiedä niidenkään selkotekstiä.**
   a. ( ) Tosi b. ( ) Epätosi

10. **Luotettu tietojenkäsittelyjärjestelmä, TCB, on sellainen laitteiston ja ohjelmiston kokoelma, että sen ulkopuoliset osat voisi periaatteessa antaa vaikka hyökkääjän rakennettaviksi, eikä tietoturvapolitiikasta silti tarvitsisi tinkiä.**
    a. ( ) Tosi b. ( ) Epätosi

17. **Mikä seuraavista on välttämätöntä julkisen avaimen K varmenteessa X.509:n mukaan? Tieto**
    a. ( ) algoritmista, jolla K:ta käytetään
    b. ( ) varmennepolitiikasta
    c. ( ) sulkulistan sijainnista
    d. ( ) K:n käyttötarkoituksesta

18. **Jos A:n pitäisi sitoutua bittijonoon s lähettämällä B:lle salattu viesti E_k(s) ja tarkistusvaiheessa avain k sekä s, niin mikä olisi protokollan pahin heikkous?**
    a. ( ) Tarkistusvaiheessa A voisi kertoa väärät tiedot, jolloin k:lla purkaminen ei tuottaisi väitettyä s:ää.
    b. ( ) Jo ennen tarkistusvaihetta B voisi löytää s:n käyttämällä syntymäpäivähyökkäystä.
    c. ( ) B ei voi ennen tarkistusvaihetta testata, onko A:lta saatu viesti oikean muotoinen, eikä esim. satunnainen bittijono.
    d. ( ) A on voinut etsiä syntymäpäivähyökkäyksellä kaksi avainta, joilla hän saa saman salatekstin kahdesta erilaisesta s:stä.

19. **Hanoin torni -systeemi varmuuskopionnissa**
    a. ( ) tuottaa tietyllä tavalla epätasaisen ikäjakauman kulloinkin tallessa oleville kopioille.
    b. ( ) edellyttää levyjen käyttöä tallennusvälineenä.
    c. ( ) edellyttää, että täyskopioiden välissä tehdään inkrementaali- eikä differentiaalikopioita.
    d. ( ) kuluttaa rotaatioon osallistuvia tallennusvälineitä tasaisesti.

20. **Jos kolmois-DES:iä sovelletaan salaukseen kahdella avaimella, niin salaukset (Ei) ja purut (Di) menevät avaimilla i=1,2 näin:**
    a. ( ) c = E1 (D2 (E1 (p)))
    b. ( ) c = E2 (E1 (E1 (p)))
    c. ( ) c = E2 (D1 (E1 (p)))
    d. ( ) c = E1 (E2 (E1 (p)))

21. **Mitä tarkoittaa DMA, direct memory access?**
    a. ( ) Laitteen ja keskusmuistin välinen siirräntä on sillä tavoin suoraa, että CPU voi samalla suorittaa jotain muuta prosessia.
    b. ( ) Kääntäjä ja linkittäjä tekevät ohjelman muistiviittauksista sillä tavoin absoluuttiset, ettei käyttöjärjestelmän tarvitse muuntaa niitä.
    c. ( ) Virtuaalimuisti toteutetaan nopean väylän avulla ohi levyajurin.
    d. ( ) Sovellusohjelmaa käynnistäessään käyttöjärjestelmä tarkistaa ohjelman muistiviittaukset eikä tarkistuksia enää tarvita ajon aikana.

22. **Mikä ero on IPSecin ESP:n ja AH:n tarjoamalla autentikoinnilla?**
    a. ( ) AH voi käyttää autentikointiin myös allekirjoitusta.
    b. ( ) Tunnelimoodissa ESP ei tarjoa autentikointia alkuperäiselle paketille ollenkaan.
    c. ( ) ESP:stä on luontevaa jättää autentikointi poiskin.
    d. ( ) ESP autentikoi paketista suuremman osan kuin AH.

23. **Baseline-menettelylle tietoturvan rakentamisessa on tyypillistä**
    a. ( ) passiivisuus.
    b. ( ) reaktiivisuus.
    c. ( ) proaktiivisuus.
    d. ( ) kvantitatiivisuus.

30. **Koska samalle viestille joissain järjestelmissä tehdään erikseen (eri alustusvektorilla) CBC-salaus ja CBC-MAC, voidaan päätellä, että on löytynyt hyökkäys, jossa**
    a. ( ) CBC-salaus kyseisellä lohkoalgoritmilla ei säilytä luottamuksellisuutta.
    b. ( ) CBC-salaus ja CBC-MAC samalla alustusvektorilla ovat jossain lohkossa tuottaneet saman tuloksen.
    c. ( ) samalla kerralla tuotetut CBC-salaus ja CBC-MAC ovat paljastaneet ainakin osan alustusvektorista tai avaimesta.
    d. ( ) CBC-salauksen viimeinen lohko saadaan menemään oikein, vaikka aiempia lohkoja on peukaloitu.

31. **Sovellusohjelmien ja levyn pinnalle tallettuvien bittien välillä on monta kerrosta, joilla bitit voidaan salata. Mitä ylemmällä tasolla salaus tehdään sitä**
    a. ( ) vähemmän tietoa biteistä (metatietoa) jää näkyville.
    b. ( ) heikommin järjestelmä sopii yhteen verkkolevyjen ja varmuuskopioinnin kanssa.
    c. ( ) enemmän käyttäjä joutuu huolehtimaan salauksesta ja avaimista.
    d. ( ) hitaampaa se on.

32. **Feistelin periaatteessa yhden kierroksen sisällä lohkon puolikkaille tapahtuu seuraavaa:**
    a. ( ) toinen puolikas kopioidaan eteenpäin sellaisenaan eikä se vaikuta toisen puoliskon tuottamaan tulokseen.
    b. ( ) kumpikin vaikuttaa molempiin seuraavan vaiheen puolikkaisiin.
    c. ( ) salausavain ei vaikuta lainkaan toisen puoliskon seuraavalle kierrokselle tuottamaan tulokseen.
    d. ( ) molemmille tehdään jokin muunnos ennen sijoitusta seuraavan vaiheen lähtökohdaksi.

33. **GSM-järjestelmässä puhelin ei autentikoi verkkoa, mutta verkko autentikoi puhelimen tai oikeastaan siinä olevan SIM-kortin. Mikä mekanismi tässä on käytössä?**
    a. ( ) Haaste-vaste -menetelmä, symmetrisen avaimen systeemillä.
    b. ( ) Haaste-vaste -menetelmä, jossa sovelletaan julkisen avaimen systeemiä.
    c. ( ) Kiinteä salasana
    d. ( ) Kertakäyttösalasana

34. **PGP:ssä oikea järjestys on (kun tiivistys tarkoittaa "ZIPpausta" ja koodaus radix-64:ää):**
    a. ( ) allekirjoitus, salaus, tiivistys ja koodaus
    b. ( ) koodaus, allekirjoitus, salaus ja tiivistys
    c. ( ) salaus, allekirjoitus, tiivistys ja koodaus
    d. ( ) allekirjoitus, tiivistys, salaus ja koodaus

35. **Luvuilla modulo 5 on kaksi generaattoria eli primitiivialkiota. Ne ovat**
    a. ( ) 2 ja 4
    b. ( ) 1 ja 4
    c. ( ) 2 ja 3
    d. ( ) 3 ja 4

36. **Mitä tekemistä ohjelmalaskurilla (program counter) on käyttöjärjestelmän (KJ) kanssa?**
    a. ( ) Se on KJ:n sovellusohjelmalle tarjoama ympäristömuuttuja.
    b. ( ) Sen avulla KJ hallinnoi kaikkien samanaikaisesti ajossa olevien ohjelmien resurssien kulutusta.
    c. ( ) Jos se osoittaa väärään kohtaan, KJ voi estää ohjelman suorituksen.
    d. ( ) Sen avulla KJ hallinnoi kyseisen ohjelman resurssien kulutusta.