TTY / TLT / J.Koskinen

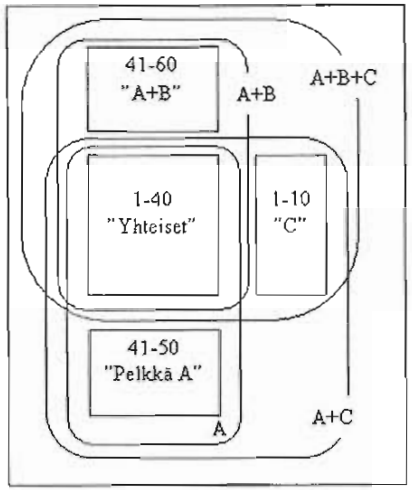
TLT-3100 Tietoturvallisuuden perusteet: A, A+B, A+C, A+B+C
Tentti 23.1.2006

Merkitse vastauksesi A- ja B-osaan oheiselle lomakkeelle. Sille pitää kirjoittaa nimi ja opiskelijanumero, joka pitää merkitä myös rastimalla ao. numeromerkit. Tätä tehtäväpaperia ei tarvitse palauttaa. Jos läpäisit verkkokeskustelun ja tentit myös C-osaa, pyydä valvojalta erillinen tehtäväpaperi sitä varten.

Merkitse enintään yksi rasti tehtävää kohti. Oikeasta vastauksesta tulee 1 piste, tyhjästä 0p. Tosi-epätositehtävissä väärä vastaus poistaa pisteitä yhden, muissa 1/3:n.

Tässä on 70 tehtävää, jotka on lomaketta varten numeroitu 1-60. Samannumeroisten tehtävien asema erottuu otsikoiden perusteella. Numerot, otsikot ja asema on jaoteltu viereisessä kuvassa. Osan C tehtävät ovat siis erikseen ja tässä ovat seuraavat:

- 1-40: yhteiset kaikille tenteille.
- 41-50: pelkkä A tai A+C (älä tee yhtään merkintää tehtäviin 51-60).
- 41-60: A+B tai A+B+C, tehtäviä B-osan materiaaleista (ainakin yksi rasti täytyy merkitä johonkin tehtävistä 51-60)



Yhteiset tehtävät 1-40

1. **Varmuuskopiointi on turhaa, jos kopioita tehdään vain kerran viikossa.**
   a. ( ) Tosi b. (X) Epätosi
2. **Etäyhteyden turvaavia tunneleita voidaan muodostaa sekä verkkoyhteyksien sisään että sovelluksen viestien ympärille.**
   a. ( ) Tosi b. ( ) Epätosi
3. **Jos toimikortin varastanut hyökkääjä saa myös PIN-luvun haltuunsa, hän pystyy normaalinkaltaisessa käyttöympäristössä lukemaan kortilla olevat salaiset avaimet.**
   a. ( ) Tosi b. (X) Epätosi
4. **PICS-järjestelmä ei ota kantaa sivujen varsinaiseen luokitukseen vaan tarjoaa vain kielen sitä varten.**
   a. (X) Tosi b. ( ) Epätosi
5. **Yksi *yleinen turvaperiaate* on, että kaikkien pääsy-yritysten oikeutus tulee tarkistaa.**
   a. (X) Tosi b. ( ) Epätosi
6. **Jos tiedosto sisältää pelkästään dataa eikä mitään ajettavaa ohjelmakoodia, graafisen käyttöliittymän käyttäjä tietää tiedostoa avatessaan, mitä ohjelmia silloin käynnistyy.**
   a. ( ) Tosi b. (X) Epätosi
7. **Jotkin asiayhteydet, joissa tietoa suojataan ihmisiltä, liittyvät vain siihen, ettei tietoon haluta antaa pääsyä ilmaiseksi.**
   a. (X) Tosi b. ( ) Epätosi
8. **Peukaloinnin sietokyky (tamper resistance) tarkoittaa, että laitetta ei voi muokata ilman, että siitä jää fyysisiä jälkiä.**
   a. ( ) Tosi b. (X) Epätosi
9. **Muistinvarainen virusten etsintäohjelma on jatkuvasti käynnissä ja tarkistaa ohjelmat ennen niiden käynnistymistä.**
   a. ( ) Tosi b. ( ) Epätosi
10. **Yksi tiedostonhallinnan periaatteita on, että jos tiedostoon on write-oikeus, niin silloin on oikeus myös muuttaa kyseisen tiedoston oikeuksia eli pääsylistaa.**
    a. ( ) Tosi b. (X) Epätosi
11. **Käyttöjärjestelmä tarjoaa riittävän hienojakoisen pääsynvalvonnan tietokantojenkin tarpeisiin.**
    a. ( ) Tosi b. (X) Epätosi
12. **Työntekijän asema organisaatiossa on määräävä tekijä tietojenkäsittelyyn liittyvien käyttöoikeuksien kannalta.**
    a. ( ) Tosi b. (X) Epätosi
13. **Hiekkalaatikko- ja wrapper-toteutukset avustavat käyttöjärjestelmää pääsynvalvonnassa kysymällä ajoittain käyttäjältä salasanaa.**
    a. ( ) Tosi b. (X) Epätosi
14. **Tietoaineiston turvaluokitus on luontevaa tehdä samoihin luokkiin sekä luottamuksellisuuden että käytettävyyden suhteen.**
    a. ( ) Tosi b. (X) Epätosi
15. **Samanlaisia työkaluja, joita käytetään tunkeutumisten havainnointiin, voi myös käyttää tietojärjestelmään tunkeutumiseen.**
    a. ( ) Tosi b. (X) Epätosi
16. **EDI tarkoittaa 'enterprise data interface' ja sama on suomeksi OVT, joka tarkoittaa 'organisaatioiden välinen tiedotusrajapinta'.**
    a. (X) Tosi b. ( ) Epätosi
17. **Yrityksen tietojenkäsittelyn turvattomin osatekijä on Internet-yhteys.**
    a. ( ) Tosi b. (X) Epätosi
18. **Jos luottokortin tiedot eivät joudu asiattomille verkossa tapahtuvan liikennöinnin takia, verkkokauppiaan kanssa asiointi noiden tietojen osalta on yhtä turvallista kuin jos asioisit saman kauppiaan kanssa paikan päällä.**
    a. ( ) Tosi b. (X) Epätosi
19. **Sähköisestä asioinnista viranomaistoiminnassa annetun lain mukaan viranomainen on vastuussa siitä, että sille osoitetut sähköiset viestit tulevat perille.**
    a. ( ) Tosi b. (X) Epätosi
20. **Kun *tietoturvallisuuden olemusta* kartoitetaan kysymyksillä, niin eniten vastauksia -- ainakin kurssimateriaaliin -- tuottaa kysymys,**
    a. ( ) kuinka arvokkaita tietojärjestelmän sisällöt ovat omistajalle.
    b. ( ) mitä tietojenkäsittelyssä pitäisi tapahtua.
    c. (X) mitä tietojenkäsittelyssä ei saisi tapahtua.
    d. ( ) mikä tietojärjestelmässä on arvokasta muille kuin omistajalle.
21. **Tiedon ja datan yleistä olemusta jäsennetään materiaalin käsitekartassa viiteen pääsuuntaan. Yksi pääsuunnista on kartassa muita yksinkertaisempi, vaikka sekin sisältää tietoturvaan liittyviä tekijöitä. Mikä? (Viidentenä suuntana kartassa on 'vaihe'.)**
    a. ( ) suhde ihmiseen
    b. (X) muoto
    c. ( ) suhde muihin tietoihin
    d. ( ) sijainti

22. **Etäkäytössä täytyy autentikoida kohdekone, jotta se ei voisi**
    a. ( ) kohdistaa DoS-hyökkäystä käyttäjään.
    b. ( ) joutua palvelunestohyökkäyksen kohteeksi.
    c. ( ) lähettää käyttäjän koneelle haittaohjelmia.
    d. (x) antaa käyttäjän autentikointitietoja hyökkääjälle.
23. **Oletetaan, että pääsynvalvontaa varten on jo luotu tietty ryhmärakenne toimijoille ja kohteille: kaikki oliot kuuluvat yhteen tai useampaan joukkoon. Mikä seuraavista malleista sallii eniten pääsyjä? Toimijan pääsy kohteeseen sallitaan, jos**
    a. ( ) toimija kuuluu tarkalleen samoihin ryhmiin kuin kohde.
    b. ( ) toimija kuuluu ainakin yhteen kohteen ryhmistä.
    c. (x) kohteen ryhmitys on toimijan ryhmityksen osajoukko.
    d. ( ) toimijan ryhmitys on kohteen ryhmityksen osajoukko.
24. **Minkä seuraavista Työelämän tietosuojalaki kieltää?**
    a. ( ) viranomaistarkistuksen yrityksen sisäpuolisen työnhakijan tapauksessa
    b. (x) geneettiset testit
    c. ( ) huumetestit
    d. ( ) älykkyystestit
25. **Paketinnuuskijan ('packet sniffer') tarkoituksena on**
    a. (x) kaapata (kopioida) verkkoliikennettä myöhempää analyysia varten.
    b. ( ) poistaa verkkoliikenteestä asiaankuulumattomia paketteja.
    c. ( ) jäljittää verkkoyhteyksiä ulkoisiin kohteisiin.
    d. ( ) skannata verkon segmenttejä kaapelointivaurioiden varalta.
26. **Jos palomuuri hylkää jonkin paketin,**
    a. ( ) se kirjoitetaan lokitiedostoon.
    b. ( ) sen kryptografinen tiiviste kirjoitetaan lokitiedostoon.
    c. ( ) se lähetetään takaisin sinne, mistä se tulikin.
    d. (x) voidaan jättää lokimerkintä myös tekemättä.
27. **Millainen vaikutus tekstinkäsittelyohjelman "undo"-toiminnolla muutoslokeincen on eheyden ja luottamuksellisuuden kannalta?**
    a. ( ) ei auta tahallisia eheysrikkeitä vastaan mutta voi auttaa luottamuksellisuusrikkeitä vastaan.
    b. ( ) auttaa sekä eheys- että luottamuksellisuusongelmissa.
    c. ( ) auttaa tahallisia eheysrikkeitä vastaan mutta ei vaikuta luottamuksellisuuteen.
    d. (x) auttaa tahattomia eheysrikkeitä vastaan mutta voi olla ongelma luottamuksellisuuden kannalta.
28. **Kertakirjautumisen mekanismeja on/ovat**
    a. ( ) kertakäyttöiset salasanat.
    b. ( ) VPN ja IPSec.
    c. ( ) SSL ja TLS.
    d. (x) Kerberos ja Passport.
29. **Eräässä suomalaisyritysten tietoturvaa tarkastelevassa tutkielmassa on tällainen toteamus: "Tietosuojalainsäädännön puutteiden vuoksi piratismi on riski Venäjällä, erityisesti Pietarin ja Moskovan alueilla toimiville yrityksille." Mikä seuraavista pohdinnoista on eniten oikeassa?**
    a. ( ) Piratismi on suomalaisyritykselle riski vasta, kun se tuo Venäjältä hankkimiaan laittomia kopioita Suomeen.
    b. ( ) Piratismin riski päinvastoin on melko pieni, kun siitä kerran on säädetty Venäjän laissa puutteellisesti.
    c. (x) Mainitulla lainsäädännön puutteella ei ole mitään tekemistä mainitun riskin kanssa.
    d. ( ) Lainsäädännön puutteella tarkoitetaan Suomen lainsäädännössä olevaa puutetta.
30. **Eräässä arvovaltaisessa tietoturvaesitelmässä lainataan Germaine Greerin tokaisua: "There is no such thing as security." Olettaen, että tässä on tosiaan tolkkua, mikä on tokaisun keskeinen oppi?**
    a. ( ) Tietoturvakäsitteen *sisältö* on niin monitahoinen, ettei siihen pitäisi viitata yhdellä sanalla.
    b. ( ) Tietoturva liittyy niin moneen *asiaan*, ettei sitä voi määritellä.
    c. (x) Tietoturvallisuus ei ole absoluuttinen suure, vain suhteellinen.
    d. ( ) Mikään järjestelmä ei ole tietoturvallinen edes politiikkansa puitteissa.
31. **Mikä seuraavista on yhteistä maksujärjestelmille Digiraha, Mobiiliraha ja PayPal?**
    a. ( ) luotto, eli varsinainen maksu tapahtuu myöhemmin
    b. ( ) tilisiirto omasta pankista maksun saajan pankkiin
    c. ( ) toimii vain matkapuhelimella
    d. (x) ei mikään näistä
32. **Mikä piirre yleisessä tietoturvatavoitteessa "saatavuus" (eli käytettävyys eli availability) poikkeaa sekä luottamuksellisuudesta että eheydestä?**
    a. ( ) Tavoite ottaa huomioon sekä vahingossa että tahallaan syntyneet ongelmat.
    b. (x) Tavoitetta ei voi saavuttaa ilman, että molemmat muut on ensin saavutettu.
    c. ( ) Tavoitteessa on mukana aikaraja, jonka puitteissa asioiden pitäisi tapahtua.
    d. ( ) Tavoite ei riipu siitä, kenen näkökulmasta asioita tarkastellaan.
33. **Mistä vuodesta asti sähköinen henkilökortti on ollut Suomessa käytössä?**
    a. ( ) 1990
    b. ( ) 1995
    c. ( ) 2000
    d. (x) 2005
34. **Skriptipennuiksi kutsutuille hyökkääjille on ominaista**
    a. ( ) toiminta kokeneempien tekijöiden oppipoikina ja avustajina.
    b. ( ) hyökkäysohjelmien asentaminen useiden muiden käyttäjien koneisiin, joista hyökkäys jatkuu automaattisesti.
    c. ( ) alaikäisyys ja kehittymätön moraali.
    d. (x) muiden kirjoittamien komentojonojen käyttäminen.
35. **Yksi mahdollinen toiminta IPSecillä on, että se lisää datapakettiin kentän, jossa on**
    a. ( ) pakettia varten generoitu julkinen avain ja sen varmenne.
    b. ( ) paketista ja symmetriscstä avaimesta laskettu tiiviste.
    c. ( ) paketin otsikkokentistä laskettu varmenne.
    d. ( ) paketista lähettäjän avaimella laskettu allekirjoitus.
36. **Jos sähköisen viranomaisasioinnin vaiheet jaotellaan kolmeen, niin ne ovat**
    a. ( ) oikeuksien tarkistus – palvelun toteuttaminen – lokitietojen kirjaaminen.
    b. ( ) vireillepano – käsittely – päätöksen tiedoksianto.
    c. ( ) tuotteiden valinta – maksaminen – toimitus.
    d. ( ) aikomus – oikeuksien tarkistus – päätös.
37. **Sähköisen kaupankäynnin aapisen maksutapojen esittelyssä ei oteta huomioon,**
    a. ( ) onko luottoriski myyjällä, ostajalla vai jollakulla muulla.
    b. ( ) miten asiakkaan tietosuojasta huolehditaan.
    c. ( ) että kertamaksu voi olla niin pieni, ettei sitä kannattaisi maksaa erikseen.
    d. (x) onko myyjällä oikeus tehdä kauppaa tuotteillaan.

38. **Jos tietoturvapolitiikka on järkevä ja sen mukaan jokin tieto pitää hävittää moninkertaisella päällekirjoituksella, niin mitä muuta pitäisi sen lisäksi tai sijasta tehdä?**
   a. ( ) poistaa tiedon omistajan käyttöoikeudet.
   b. ( ) salata ko. tiedon varmuuskopiot avaimella, jota ei kirjoiteta levylle ja joka pyyhitään muistista käytön jälkeen.
   c. ( ) tehdä kattavat tietokanta- ja www-haut, joilla selviää, onko tieto jo olemassa muualla, josta sitä ei voida hävittää. Tällöin päällekirjoituskin on turhaa.
   d. (X) kohdella samoin kaikkia ko. tiedon kopioita.

39. **Saksan tietoturvaviraston käsikirjan ylivoimaisten uhkien luettelossa on kohta "Ausfall eines Weitverkehrsnetzes / Failure of a wide area network". Millaisten Internet-palvelujen tarjoajien toiminnan laatuun tämä uhka liittyy?**
   a. (X) yhteyspalvelu
   b. ( ) sähköpostipalvelu
   c. ( ) nimipalvelu (DNS)
   d. ( ) haku- tai hakemistopalvelu

40. **Salasanasta on sanottu, että sitä pitäisi kohdella kuin omaa hammasharjaa. Kuinka monta seuraavista salasanaan liittyvistä ominaisuuksista tämä sanonta edustaa? Salasanan (i) entropia, (ii) käytettävyys, (iii) pitäminen vain omassa käytössä, (iv) vaihtaminen riittävän usein.**
   a. ( ) ei yhtään
   b. ( ) yhtä
   c. ( ) kahta
   d. ( ) kaikkia

Pelkän A-osan tehtävät 41-50 (Jos teet A+B:tä, ohita tämä jakso)

41. **Jos kerta-avain on nimensä mukaan ainutkertainen eikä se ole paljastunut kenellekään ulkopuoliselle, niin kerta-avainsalaus antaa parhaan mahdollisen suojan sekä luottamuksellisuudelle että eheydelle.**
   a. ( ) Tosi b. ( ) Epätosi

42. **Toimikorttien prosessorit eivät ole yleensä tarpeeksi älykkäitä symmetriseen salaukseen.**
   a. ( ) Tosi b. ( ) Epätosi

43. **Jos GSM-puhelimesta soittaa lankapuhelimeen, puhelu on salattu tukiasemaan ja ensimmäiseen matkapuhelinverkon keskukseen asti, mutta ei pitemmälle.**
   a. ( ) Tosi b. ( ) Epätosi

44. **Luvun kertominen itsellään on tietynlaisessa kokonaislukujärjestelmässä sillä tavoin yksisuuntainen operaatio, että sitä voidaan käyttää tiedon salaamiseen ja järjestelmän rakenteen tunteva pystyy purkamaan salauksen.**
   a. ( ) Tosi b. ( ) Epätosi

45. **PGP:ssä ei käytetä allekirjoitettuja varmenteita, vaan luottamus julkisiin avaimiin perustuu esittelijöiden antamiin luonnehdintoihin.**
   a. ( ) Tosi b. ( ) Epätosi

46. **Kryptografisen protokollan käyttö edellyttää, että tiedetään etukäteen, mikä versio siitä vastapuolella on käytössä.**
   a. ( ) Tosi b. ( ) Epätosi

47. **Jos salasanan unohtamisen varalle saa esim. seittipalvelussa muotoilla muistutuskysymyksen ja siihen vastauksen, vastaus on oleellisesti toinen salasana.**
   a. ( ) Tosi b. ( ) Epätosi

48. **Mikä seuraavista ei päde, kun tietokannassa on arkaluonteisia tietoja? Voi olla, että**
   a. ( ) niistä laaditut yhteenvetotiedot eivät ole arkaluonteisia.
   b. ( ) niistä saa suojauksista huolimatta tietoa päättelyillä sallittujen kyselyiden avulla.
   c. ( ) suojaukseksi riittää, etteivät sivulliset osaa muodostaa oikeanlaisia kyselyehtoja.
   d. ( ) tiedon olemassaoloakaan ei saa paljastaa.

49. **Materiaalissa sanotaan: "Avaintenvaihto on yksi tärkeimmistä kryptografisista protokollista." Mitä avaintenvaihto, eli 'key exchange' tässä tarkoittaa?**
   a. ( ) Vanha symmetrinen avain päivitetään.
   b. ( ) Symmetrisestä avaimesta sovitaan.
   c. ( ) Julkinen avain peruutetaan ja uusi varmennetaan.
   d. ( ) Päivitetty julkinen avain rekisteröidään.

50. **Millä seuraavista on vähiten tekemistä perinteisten GSM-puhelujen kanssa?**
   a. ( ) virustorjunta
   b. ( ) tietoturvapolitiikka
   c. ( ) avainten hallinta
   d. ( ) autentikointi

A+B:n tehtävät 41-60 (liittyvät kurssin B-osaan)

41. **Jos yrityksen kahden toimipisteen välinen liikenne salataan ja autentikoidaan niissä olevien palomuurien välillä, kyseessä on silloin SSH-tunneli.**
   a. ( ) Tosi b. (X) Epätosi

42. **Ohjelmistoprosessissa yksi haavoittuvuusanalyysin tekniikoita on konfiguraationhallinta.**
   a. ( ) Tosi b. (X) Epätosi

43. **Jos kryptoprimitiivit luokitellaan avaimellisiin ja avaimettomiin, niin kaikki salausalgoritmit kuuluvat jälkimmäiseen luokkaan.**
   a. ( ) Tosi b. (X) Epätosi

44. **Julkisen avaimen järjestelmä voi ulottua maan rajojen yli tai se voi rajoittua pelkästään tiettyyn yritykseen..**
   a. (X) Tosi b. ( ) Epätosi

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

46. **Lyhimmässäkin AES-avaimessa on yli sata bittiä.**
   a. (X) Tosi b. ( ) Epätosi

47. **Viestistä laskettu kryptografinen tiivistefunktio edustaa koko viestiä sikäli, että on erittäin epätodennäköistä löytää jotain muuta viestiä, jolla olisi sama tiiviste.**
   a. (X) Tosi b. ( ) Epätosi

48. **Kryptografisissa protokollissa viestien tuoreutta voi osoittaa aikaleimojen lisäksi satunnaislukujen käytöllä.**
   a. ( ) Tosi b. (X) Epätosi

49. **Salasanatiedoston suola**
    a. ( ) pakottaa salasana-arvaajan työskentelemään erikseen suurinta osaa käyttäjätunnuksia kohti.
    b. ( ) vaihtuu joka kerta, kun salasanaa käytetään.
    c. ( ) estää salasana-arvausten todentamisen.
    d. ( ) hidastaa tietyn käyttäjän salasanan löytämistä arvaamalla.

50. **Millä seuraavista on vähiten tekemistä niiden menetelmien kanssa, joilla tietokannan luottamuksellisuutta ylläpidetään, kun sieltä kuitenkin annetaan julki kyselyvastauksina tilastollisia tietoja?**
    a. ( ) permutaatio
    b. ( ) vaihteluvälit
    c. ( ) satunnaisotos
    d. ( ) satunnainen muuntelu

51. **Avaintenhallintaa tarvitaan, vaikka mitään kommunikaatiosuhdetta eri osapuolten välillä ei olisi. Jos avainta käytetään työntekijän henkilökohtaisen tietokoneen kiintolevyn salaamiseen, niin mikä seuraavista avaintenhallinnan vaiheista ei kuulu asiaan?**
    a. ( ) key escrow
    b. ( ) varmuuskopiointi
    c. ( ) jakelu
    d. ( ) päivitys

52. **Jos siirtorekisteriä (LFSR:ää) kuvaava rekursioyhtälö on s[i] = s[i-1]+s[i-4] mod 2 ja rekisteri on juuri tulostanut bitit 1, 0, 1 ja viimeisenä vielä 1:n, niin mitkä ovat kaksi seuraava?**
    a. ( ) 0 ja sitten 0
    b. (X) 0 ja sitten 1
    c. ( ) 1 ja sitten 0
    d. ( ) 1 ja sitten 1

53. **Jos presidentinvaali olisi järjestetty Internetissä sopivalla protokollalla, toisen kierroksen äänestystä olisi voitu yksinkertaistaa huomattavasti hoitamalla se vain äänten vaihtamisrutiinilla. Tällöin useimpien ei tarvitsisi tehdä enää mitään toisella kierroksella, koska kuitenkin äänestäisivät samaa ehdokasta. Mikä ongelma tässä olisi?**
    a. ( ) Äänestysprosentti laskisi keinotekoisesti.
    b. (X) Monista äänestäjistä tiedettäisiin, keitä he eivät äänestäneet.
    c. ( ) Ei voisi järjestää ennakkoäänestystä.
    d. ( ) Se ehdokas, joka sai eniten ääniä ensimmäisellä kierroksella voittaisi varmasti.

54. **Menetelmä jolla tekijänoikeudellisesti suojatun materiaalin levittymistä voi seurata on**
    a. ( ) digitaalinen vesileimaus.
    b. ( ) varmenteeseen perustuva allekirjoitus.
    c. (X) sokea allekirjoitus.
    d. ( ) bittiin sitoutuminen.

55. **Järjestelmässä, jossa pankki myy sokeasti allekirjoittamiaan sähköisiä seteleitä asiakkailleen,**
    a. ( ) asiakas keksii itse sarjanumeron, joka on riittävän pitkä satunnaisluku.
    b. (X) pankki muodostaa seteliin sovitunkaltaista redundanssia sisältävän yksikäsitteisen sarjanumeron.
    c. ( ) ideana on, ettei pankki tiedä, kuka siltä ostaa näitä seteleitä..
    d. ( ) ensimmäinen allekirjoituksen tarkistus tapahtuu, kun setelin ostaja tarkistaa pankista saamansa setelin.

56. **Biometriikan soveltaminen matkapuhelintekniikkaan olisi järkevintä seuraavasti:**
    a. ( ) SIM-kortti sisältää omistajansa biometriikkaa, ja autentikoituu sen perusteella puhelinverkolle.
    b. ( ) Puhelinverkon palvelu autentikoi puhelun osapuolet toisilleen biometrisesti heidän ääntensä perusteella.
    c. (X) Käyttäjä autentikoituu puhelimelleen tai sen SIM-kortille biometrisesti.
    d. ( ) Puhelun osapuolten äänten perusteella generoidaan ja samalla autentikoidaan end-to-end -salaukseen käytettävä salausavain.

57. **Rabinin allekirjoitusalgoritmi on järkevä, vaikka kaikilla viesteillä (= niitä edustavilla luvuilla) ei ole modulaarista neliöjuurta. Selitys tälle on:**
    a. ( ) Allekirjoitusalgoritmin aluksi viesti korotetaan toiseen ja sitä seuraavan muunnoksen jälkeen neliöjuuri on olemassa.
    b. ( ) Allekirjoittaja voi muutamalla yrityksellä saada aikaan neliöjuurellisen muunnoksen viestistään.
    c. ( ) Todennus tapahtuu kuitenkin toiseen korottamalla eikä neliöjuuren laskulla.
    d. ( ) On erittäin epätodennäköistä, että viestillä joka halutaan allekirjoittaa, ei olisi neliöjuurta.

58. **Suurten kokonaislukujen operaatioita käyttävät salausmenetelmät käyttävät modulaarista aritmetiikkaa, koska**
    a. ( ) se nopeuttaa laskentaa.
    b. ( ) se säästää tilaa.
    c. ( ) tiettyjä käänteisoperaatioita ei voisi muuten laskea.
    d. (X) tietyt käänteisoperaatiot olisivat muuten liian helppoja.

59. **Olet lähettämässä viestiä jollekulle A:lle ja A:n julkinen avain löytyy PGP-avainrenkaastasi. Sitä varmentaa muutama allekirjoitus. Mitä vaikutusta näillä allekirjoituksilla voi olla?**
    a. ( ) Sinä uskot, että viesti ei paljastu muille kuin A:lle.
    b. ( ) A uskoo viestin luettuaan, ettei se ole paljastunut muille kuin hänelle.
    c. ( ) A uskoo viestin tekstiä lukemattakin, että sinä lähetit viestin.
    d. ( ) A pystyy vakuuttamaan jonkun muun siitä, että sinä lähetit viestin.

60. **Oletetaan, että tietokannan johonkin kenttään (taulun sarakkeeseen) on rakennettu sellainen eheystarkistus, joka estää väärän tai edes väärin kirjoitetun datan pääsyn tietokantaan. Se tarkoittaisi**
    a. (X) että kyseinen kenttä voitaisiin täyttää automaattisesti.
    b. ( ) että pahantahtoinen käyttäjä voisi särkeä eheyden jättämällä tuon kentän täyttämättä.
    c. ( ) että kyseistä kenttää ei voisi kryptata.
    d. ( ) palvelunestohyökkäystä tuohon kenttään kirjoittavia vastaan.