TTY / TLT / J.Koskinen

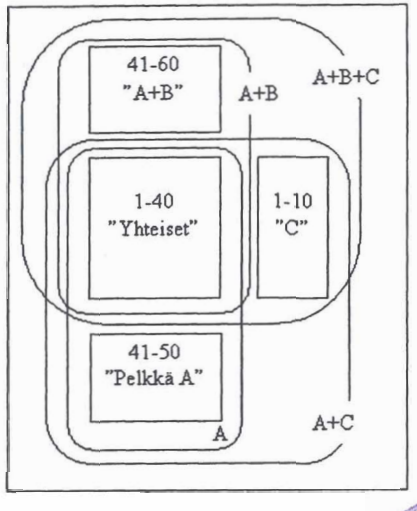
8306001 Tietoturvallisuuden perusteet: A, A+B, A+C, A+B+C
Tentti 31.1.2005

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/(n-1), missä n on vaihtoehtojen määrä.

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. **GSM-puhelinverkko ei autentikoidu puhelimelle.**
   a. ( ) Tosi b. ( ) Epätosi
2. **EDI on sähköisen maksunvälityksen tietoturvastandardi.**
   a. ( ) Tosi b. ( ) Epätosi
3. **HST-kortin varmenteen myöntäjän pitää noudattaa Varmennepolitiikkaa, joka on osa Suomen lainsäädäntöä.**
   a. ( ) Tosi b. ( ) Epätosi
4. **PICS-järjestelmä ei ota kantaa sivujen varsinaiseen luokitukseen vaan tarjoaa vain kielen sitä varten.**
   a. ( ) Tosi b. ( ) Epätosi
5. **Tietosuojan keskeinen merkitys on yksityisten ihmisten salaisten tietojen suojaamisessa.**
   a. ( ) Tosi b. ( ) Epätosi
6. **Omistajan kannattaa soveltaa omaan järjestelmäänsä automaattisia hyökkäystyökaluja.**
   a. ( ) Tosi b. ( ) Epätosi
7. **Varmuuskopioinnissa on tärkeää, että varmassa ja helposti palautettavassa tallessa on mahdollisimman uusi versio tiedoista: Jos se olisi kopioitu useana kappaleena eri paikkoihin, niin vanhemmat kopiot voisi hävittää.**
   a. ( ) Tosi b. ( ) Epätosi
8. **Vain viranomaisilla on oikeus ottaa selville, mitä joku tekee tai on aiemmin tehnyt tietokoneellaan.**
   a. ( ) Tosi b. ( ) Epätosi
9. **Tiedoston pääsynvalvonnassa kirjoitusoikeus tarkoittaa aina myös lukuoikeutta, mutta ei päinvastoin.**
   a. ( ) Tosi b. ( ) Epätosi
10. **Kriittisten tehtävien dokumentointi on tarpeen, jotta joku toinen pystyy ilman koulutusta tai harjoitusta suorittamaan kyseiset tehtävät.**
    a. ( ) Tosi b. ( ) Epätosi
11. **Rich Text Format (RTF) ei kykene levittämään makroviruksia.**
    a. ( ) Tosi b. ( ) Epätosi
12. **Myös pöly ja lika voivat aiheuttaa tietoturvauhkia.**
    a. ( ) Tosi b. ( ) Epätosi
13. **Laitteen näkökulmasta ainoat ikävyydet, joita siihen fyysisesti käsiksi pääsevä voi aiheuttaa, ovat särkeminen, varkaus ja resurssien käyttö.**
    a. ( ) Tosi b. ( ) Epätosi
14. **Merkkijonossa `=:-D)` on enemmän salasanalta vaadittavaa entropiaa kuin jonossa `Sá7a5ANä-2`.**
    a. ( ) Tosi b. ( ) Epätosi
15. **Pakettisuodatin tarkastelee IP-otsikoiden lisäksi TCP:n ja UDP:n porttinumeroita, ja niitä se voi myös vaihtaa.**
    a. ( ) Tosi b. ( ) Epätosi
16. **"Tietoturvallisuus on prosessi" tarkoittaa mm. seuraavaa: Ei tarvitse huolestua, vaikka arkaluonteista tietoa vuotaisi jatkuvasti ja tärkeän tiedon eheys heikkenisi kaiken aikaa, kunhan samoin ovat koko ajan käynnissä parhaat mahdolliset suojaavat ja korjaavat toimenpiteet.**
    a. ( ) Tosi b. ( ) Epätosi
17. **Jos tietoverkossa viestillä on väärä osoite, tuloksena on saatavuuden heikkeneminen, mutta se ei ole tietoturvan kannalta suurin huolenaihe.**
    a. ( ) Tosi b. ( ) Epätosi
18. **Jos salasanan unohtamisen varalle täytyy (esim. seittipalvelussa) muotoilla kysymys ja siihen vastaus, on vastauksen muotoiluun kiinnitettävä enemmän huomiota kuin kysymyksen.**
    a. ( ) Tosi b. ( ) Epätosi
19. **Jos luottaa ohjelmiston valmistajaan, uuden version voi huoletta ladata verkosta, kunhan mukana seuraavan tarkistussumman avulla varmistaa, ettei se ole muuttunut matkalla.**
    a. ( ) Tosi b. ( ) Epätosi
20. **Henkilötietolain mukaan arkaluonteisten henkilötietojen käsittely on joissain tapauksissa sallittua.**
    a. ( ) Tosi b. ( ) Epätosi
21. **Jos ohjelma ei toteuta täsmällisesti määrityksiään, se ei ole myöskään tietoturvallinen.**
    a. ( ) Tosi b. ( ) Epätosi
22. **Termi redundanssi mainitaan tietoturvamekanismeja esittelevässä käsitekartassa.**
    a. ( ) Tosi b. ( ) Epätosi
23. **Työntekijöiden tekemisten seurantaa ei voi lakien mukaan tehdä siinä määrin, että sillä voisi mainittavasti vähentää heidän aiheuttamiaan tietoturvariskejä.**
    a. ( ) Tosi b. ( ) Epätosi
24. **Toimikorttien prosessoreilla on kykyä sekä julkisen avaimen systeemin luomiseen että sen operaatioihin.**
    a. ( ) Tosi b. ( ) Epätosi

25. **Toimikortin valmistuksessa tapahtuva sulakkeen polttaminen estää loogiset muistiviittaukset, minkä jälkeen vain fyysinen viittaus on mahdollista.**
    a. ( ) Tosi b. ( ) Epätosi
26. **RAID-levytekniikassa voidaan parantaa tietoturvallisuutta lisäämällä redundanssia.**
    a. ( ) Tosi b. ( ) Epätosi
27. **Nimitystä skriptipentu käytetään tietynlaisista hyökkääjistä. Mikä heille on tyypillistä puolustajan näkökulmasta?**
    a. ( ) Alaikäisyys, jonka vuoksi heitä ei saa korvausvastuuseen.
    b. ( ) Oleellisesti samanlaiset komentojonot kuin useilla muillakin hyökkääjillä.
    c. ( ) Nuoruus ja taitamattomuus, jonka vuoksi heidän hyökkäyksensä eivät ole kovin vaarallisia.
    d. ( ) Arvaamattomilla tavoilla muunnetut komentojonot, jotka voivat sen vuoksi olla erityisen vaarallisia.
28. **Common Criteria-standardin ehdottamassa prosessissa tietojärjestelmän T turvallisuuden työstämisen *alkulähtökohtiin* kuuluu mm.**
    a. ( ) organisaation tietoturvapolitiikka ja oletukset, jotka T:n ympäristölle voidaan asettaa.
    b. ( ) T:n arvokas sisältö ja siihen kohdistuvat uhkat.
    c. ( ) T:n tavoite ja fyysinen ympäristö.
    d. ( ) T:n tarkoitus ja sitä koskevat turvavaatimukset.
29. **Yksityistä avainta soveltamalla avaimen haltija pystyy muodostamaan vastaavan julkisen avaimen ja oman identiteettinsä välille kytkennän,**
    a. ( ) joka on välttämätön sen osoittamiseksi, kenen hallussa kyseinen yksityinen avain on.
    b. ( ) jonka perusteella toiset saavuttavat luottamuksen siihen, kenen hallussa kyseistä julkista avainta vastaava yksityinen avain on.
    c. ( ) josta voi olla se hyöty, että toiset tietävät, että kytkennän muodostaja tuntee ko. julkista avainta vastaavan yksityisen avaimen.
    d. ( ) jonka avulla toiset voivat luottaa väitteisiin siitä, kenen hallussa kyseinen julkinen avain on.
    e. ( ) josta ei ole hyötyä, jos pitää kasvattaa luottamusta siihen, kenen hallussa ko. julkista avainta vastaava yksityinen avain on.
30. **Virus ei voi tehdä mitään, jos sen koodia vain luetaan mutta ei ajeta. Miksi Wordin makrovirus sitten käynnistyy, vaikka sen sisältävä dokumentti vain luetaan levyltä Wordiin?**
    a. ( ) Virus on muistinvarainen ja tarttuu avattaviin dokumentteihin.
    b. ( ) Virus on tarttunut myös Wordin ohjelmakoodiin.
    c. ( ) Saastunut dokumentti sisältää ohjelmakoodia, jonka Word ajaa luettuaan dokumentin.
    d. ( ) Saastunut dokumentti sisältää ohjelmakoodia, jonka lukeminen saa Wordissa aikaan puskurin ylivuodon, jolloin koodi kuitenkin päätyy ajettavaksi.
31. **Turvallisuuden pahin vihollinen taitaa kyllä olla ihminen, mutta mikä on toiseksi pahin -- jota usein myös pahimmaksi sanotaan?**
    a. ( ) monikerroksisuus
    b. ( ) yksikerroksisuus
    c. ( ) ketjun heikoin lenkki
    d. ( ) lenkin puuttuminen ketjusta
    e. ( ) ei mikään näistä
32. **Kun laitteistojen turvallisuutta tarkastellaan peukaloinnin näkökulmasta, niin keskeistä on, ettei mikään luvaton toimenpide pääse kohdistumaan niihin ja että käyttäjä voi myös vakuuttua tästä. Tällaisessa tarkastelussa jää huomiotta jotain tärkeää, mitä laitteistojen valmistuksessa pitäisi ottaa huomioon. Mitä?**
    a. ( ) Paloturvallinen sijoittelu laitetiloihin.
    b. ( ) Valmistuksen vaiheistus siten, ettei kukaan saa liikaa tietoa rakenteesta tai pääse asentamaan siihen takaportteja.
    c. ( ) Laitteen fyysinen kestävyys, toimivuus ja muu tietoturvan saatavuusnäkökulma.
    d. ( ) Se, että laitteen pitää ennemmin tuhota siihen valmistuksessa asennettu kryptoavain kuin päästää sitä paljastumaan.
33. **Mikä laki sanoo tähän tapaan: teknisenä välittäjänä toimiva palvelun tarjoaja ei joudu vastuuseen, kunhan hän viipymättä poistaa aineiston, jonka hän on saanut tietää sisältävän lasta, väkivaltaa tai eläimeen sekaantumista esittäviä pornografisia kuvia tai kiihottamista kansanryhmää vastaan ?**
    a. ( ) Sähköisen viestinnän tietosuojalaki
    b. ( ) Julkisuuslaki
    c. ( ) Rikoslaki
    d. ( ) Laki tietoyhteiskunnan palvelujen tarjoamisesta
    e. ( ) Ei mikään näistä
34. **Sähköisen kaupankäynnin aapisen maksutapojen esittelyssä otetaan huomioon,**
    a. ( ) miten tietoturvallinen käyttöympäristö asiakkaan käyttämällä maksuohjelmalla on.
    b. ( ) että maksujärjestelmä täyttää myös verottajan vaatimukset.
    c. ( ) että muitakin asioita kuin puheluita voidaan maksaa puhelinlaskun kautta.
    d. ( ) onko asiakkaalla oikeus käyttää omaa tiliään verkkomaksuihin.
35. **Mitä seuraavista CERT:n laatima tarkistuslista ei kehota ylläpitäjää etsimään/tarkastamaan hyökkäysten havaitsemiseksi?**
    a. ( ) ajastettuina ajettavat ohjelmatiedostot
    b. ( ) piilotetut tiedostot
    c. ( ) allekirjoitetut tiedostot
    d. ( ) suid- ja sgid-tiedostot
36. **Millä seuraavista on vähiten vaikutusta siihen, millaisia odotuksia työhön ottajalla on henkilön luotettavuudesta? Sillä, että henkilö**
    a. ( ) on peliriippuvainen.
    b. ( ) käyttää runsaasti alkoholia.
    c. ( ) edustaa seksuaalista vähemmistöä.
    d. ( ) on elatusvelvollinen usealle taholle.
37. **Työsuhteen päättymiseen liittyvät tietoturvariskit luottamuksellisuuden osalta rajoittuvat siihen tietoon, jonka eroava työntekijä on hankkinut ennen kuin hänen tietovälineensä on palautettu yritykselle ja pääsyoikeutensa on peruutettu. Väite on melko lähellä totuutta, mutta riskinä voi olla myös muiden tietojen vuotaminen työntekijän**
    a. ( ) oman muistin kautta, vaikka tiedot voivatkin olla epätarkkoja tai vanhentuneita.
    b. ( ) jouduttua jättämään työnsä nimenomaan siksi, että hän on ollut yhteistyössä ammattirikollisten kanssa.
    c. ( ) työntekijän tehdessä ulkopuolelta hyökkäyksen jonkin aiemmin asentamansa takaportin kautta.
    d. ( ) Ei mikään edellisistä, vaan alkuperäinen väite on tosi.

38. **Kurssiaineistossa kartoitettiin tietojenkäsittelyn tulosten uskottavuuden merkitystä. Millainen suhde uskottavuudella käyttäjän näkökulmasta on tietoturvaan?**
    a. ( ) Jos uskottavuudella ei ole väliä, ei ole tietoturvallakaan.
    b. ( ) Jos tietoturvalla ei ole väliä, ei ole uskottavuudellakaan.
    c. ( ) Ei ole sellaista tietojenkäsittelyä, jonka uskottavuudella tai tietoturvalla ei olisi väliä.
    d. ( ) Mitään edellistä väitteistä ei esitetty eikä olisi voitukaan, koska käsitteet eivät ole noin yksinkertaisia.
39. **Tietoturvallisuuden osa-alueena mainitaan joissain yhteyksissä tietosodankäynti, mutta yrityksen näkökulmasta sen voi sisällyttää yleisemmän turvallisuusjaottelun osa-alueeseen**
    a. ( ) turvallisuusjohtaminen.
    b. ( ) valmiussuunnittelu.
    c. ( ) force majeure -uhkien torjunta.
    d. ( ) ulkomaantoimintojen turvallisuus.
40. **Voiko sähköpostiviestin loppuun lisätyllä lähettäjän nimellä olla oikeudellista merkitystä?**
    a. ( ) Ei, sillä laki sähköisistä allekirjoituksista määrittelee vain varmenteeseen perustuvan allekirjoituksen.
    b. ( ) Ei, sillä sen voi helposti väärentää.
    c. ( ) Kyllä, sillä laki sähköisistä allekirjoituksista rinnastaa sen faxitse lähetettyyn käsinkirjoitettuun allekirjoitukseen.
    d. ( ) Kyllä, sopimusvapauden ja vapaan todistusharkinnan periaatteiden mukaan.

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

41. **Kerta-avainjärjestelmässä tarvitaan yhtä pitkä avain kuin on selkotekstikin.**
    a. ( ) Tosi b. ( ) Epätosi
42. **Yksi mahdollinen toiminta IPSecillä on, että se lisää datapakettiin kentän, jossa on paketista laskettu avaimellinen tiiviste.**
    a. ( ) Tosi b. ( ) Epätosi
43. **SSL:n turvallisuus perustuu siihen oletukseen, että kumpikin osapuoli voi luottaa toisen osapuolen julkiseen avaimeen.**
    a. ( ) Tosi b. ( ) Epätosi
44. **Jos haaste-vaste -menetelmä perustuu kryptografisen tiivistefunktion käyttöön, käyttäjän salasanan riittää olla todentajalla tallessa tiivistetyssä muodossa.**
    a. ( ) Tosi b. ( ) Epätosi
45. **Kahden suuren alkuluvun p ja q tulosta pitää ensin laskea jakojäännös kolmannen alkuluvun suhteen, jotta tuloksen voi julkaista ilman, että p ja q paljastuvat.**
    a. ( ) Tosi b. ( ) Epätosi
46. **Kryptoalgoritmien turvallisuuden kannalta on keskeistä, että hyökkääjä ei tunne algoritmin rakennetta.**
    a. ( ) Tosi b. ( ) Epätosi
47. **PGP-ohjelmalle on ominaista, että se määrittelee avainrenkaassa olevien julkisten avainten luotettavuutta hakemistoista tai muualta tietoverkosta hakemiensa varmenneketjujen avulla.**
    a. ( ) Tosi b. ( ) Epätosi
48. **Jos lohkosalausalgoritmissa syöte olisi pitempi kuin kryptoteksti, salausta ei välttämättä voisi purkaa.**
    a. ( ) Tosi b. ( ) Epätosi
49. **Autentikoinnin yleisen perustavoitteen kannalta voivat olla järkeviä muut paitsi yksi seuraavista erikoisista järjestelyistä. Mikä?**
    a. ( ) kertaalleen hyväksytyn autentikaation vaatiminen uudestaan jonkin ajan kuluttua.
    b. ( ) sama todennustieto (esim. salasana) usealla eri oliolla.
    c. ( ) ei tiedetä todennettavan olion oikeaa identiteettiä.
    d. ( ) todennustietojen toimittaminen oliolle, jolla ei ole mitään oikeuksia järjestelmään.
50. **Mikä seuraavista on lähinnä sellainen tehtävä, jonka hoitamiseen voidaan käyttää kryptografista protokollaa?**
    a. ( ) sähköpostiviestin muuttaminen salatekstiksi
    b. ( ) salausavaimesta sopiminen
    c. ( ) salausavaimen turvallinen säilytys
    d. ( ) salausavaimen generointi hyvien satunnaislukujen perusteella

A+B:n tehtävät 41-60 (ovat B-osan materiaalista)

41. **Kryptografisissa protokollissa viestien tuoreutta voi osoittaa alkaleimoilla tai satunnaisluvuilla.**
    a. ( ) Tosi b. ( ) Epätosi
42. **Avaimen peruuttaminen PGP:ssä onnistuu vain antamalla voimassaoloajan kulua loppuun.**
    a. ( ) Tosi b. ( ) Epätosi
43. **Tiivistefunktiolla toteutetussa kertakäyttöisten salasanojen menetelmässä asiakas voi joka kerta joutua laskemaan monta askelta eteenpäin, mutta palvelimen riittää yleensä tehdä yksi askel.**
    a. ( ) Tosi b. ( ) Epätosi
44. **Edistyneissäkin äänestysprotokollissa, joita aineistossa esitellään, on se ongelma, että vaaliviranomainen voi äänestää niiden puolesta, jotka eivät käytä ääniolkeuttaan.**
    a. ( ) Tosi b. ( ) Epätosi
45. **Tietoverkossa tapahtuvan liikennöinnin eheyttä edistää, jos liikennöintiprotokollat havaitsevat ja toipuvat, kun viestejä tai paketteja katoaa, kopioutuu, muuntuu, pilkkoutuu tai niiden järjestys vaihtuu.**
    a. ( ) Tosi b. ( ) Epätosi
46. **Vaikka ohjelmoinnissa olisi noudatettu modulaarisuuden periaatteita, ohjelmistoprosessiin kuuluva staattinen analyysi voi paljastaa moduuleissa tietoturvattomuuksia.**
    a. ( ) Tosi b. ( ) Epätosi
47. **CBC-salauksen purussa alustusvektorin bitit ovat lohkoalgoritmin syötteenä myös ensimmäisellä kierroksella.**
    a. ( ) Tosi b. ( ) Epätosi
48. **Avaimen pituudesta riippuen AES:ssa tehdään noin 12 Feistel-kierrosta.**
    a. ( ) Tosi b. ( ) Epätosi

49. **Sovellustason palomuuri on käytännössä sama kuin WWW-proxy.**
    a. ( ) Tosi b. ( ) Epätosi
50. **Valitun selvätekstin skenaario tarkoittaa, että kryptoanalyytikko voi vaikuttaa siihen selvätekstiin, josta hänen murrettavanaan oleva salateksti on tehty.**
    a. ( ) Tosi b. ( ) Epätosi
51. **Feistelin periaatteessa kunkin vaiheen tekstin puolikkaaseen sovellettavan funktion pitää olla injektio, eli kahdesta eri lähtöarvosta ei saa tulla samaa tulosta.**
    a. ( ) Tosi b. ( ) Epätosi
52. **ElGamalin allekirjoitusalgoritmi eroaa RSA:sta siinä, että se ei tuota aina samasta tekstistä samanlaista allekirjoitusta.**
    a. ( ) Tosi b. ( ) Epätosi
53. **ElGamalin julkisen avaimen kryptosysteemin turvallisuus perustuu siihen, että**
    a. ( ) on vaikea laskea logaritmeja modulaarisessa aritmetiikassa.
    b. ( ) on vaikea laskea juuria (käänteispotensseja) modulaarisessa aritmetiikassa.
    c. ( ) viesti salataan kertomalla se satunnaisella luvulla, jota ei liitetä viestiin lähetykseen mukaan.
    d. ( ) kahden suuren alkuluvun tuloa on vaikea jakaa tekijöihin.
54. **Vaikka joku keksisi tekstit X ja Y, joilla on sama tiiviste, tekstille X laadittu digitaalinen allekirjoitus ei toimisi tekstin Y allekirjoituksena, sillä**
    a. ( ) tekstit ovat mukana allekirjoituksissa -- pelkästä tiivisteestähän ei voisi tietää mitä on allekirjoitettu.
    b. ( ) tekstistä lasketaan allekirjoituksia varten aina kaksi tiivistettä eri algoritmeilla.
    c. ( ) satunnaisluku, joka allekirjoitusalgoritmissa generoidaan, osuu äärimmäisen epätodennäköisesti samaksi.
    d. ( ) Edelliset ovat turhia selityksiä, sillä tekstin X:n allekirjoitus todentuu myös tekstille Y.
55. **Mikä on pahin ongelma biometrisessä autentikoinnissa, jonka pitäisi toimia internetin kaltaisen turvattoman verkon yli?**
    a. ( ) Ei tiedetä, kuka on autentikoitumassa.
    b. ( ) Joku voi saada haltuunsa palvelimella olevan vertailudatan.
    c. ( ) Ei tiedetä, onko autentikointidatan syöttäjä sama kuin se, jota data koskee.
    d. ( ) Verkossa kulkevan datan eheys tai salaus voi särkyä matkalla.
56. **Mikä seuraavista ei päde kuvaan liitettävästä digitaalisesta vesileimasta?**
    a. ( ) Se voi näkyä myös paljaalle silmälle.
    b. ( ) Se voidaan tehdä niin, ettei kuva muutu.
    c. ( ) Se voidaan tehdä erilaiseksi kuvan eri kopioihin.
    d. ( ) Se voi sisältää metatietoa kuvasta.
57. **Olkoon n allekirjoittajan julkinen moduuli, ja e julkinen eksponentti. Sokeaa RSA-allekirjoitusta varten lähettäjä kertoo alkuperäisen viestinsä (tiivisteen) X:llä modulo n, missä X on**
    a. ( ) lähettäjän valitsema satunnaisluku.
    b. ( ) allekirjoittajan valitsema satunnaisluku.
    c. ( ) lähettäjän valitsema satunnaisluku potenssiin e.
    d. ( ) e potenssiin lähettäjän valitsema satunnaisluku.
    e. ( ) ei mikään edellisistä, vaan lähettäjä korottaa tiivisteen potenssiin e.

58. **Suppean aineiston sääntönä tietokantakyselyissä voidaan käyttää ns. (n,k)-sääntöä, jonka mukaan kysely hylätään, jos**
    a. ( ) kyselyn tulos perustuu vähintään n tietueeseen, mutta tulos on enintään k % vastaavasta tuloksesta, jossa koko kanta on mukana.
    b. ( ) kyselyn tulos perustuu tietueisiin, joiden joukossa on n:n kokoinen tai pienempi osajoukko, jotka tuottavat vähintään k % kyselyn tuloksesta.
    c. ( ) enintään n tietuetta tuottaa enintään k % kyselyn tuloksesta.
    d. ( ) kyselyn tulos perustuu tietueisiin, joiden joukossa on n:n kokoinen tai suurempi osajoukko, jotka tuottavat vähintään k % kyselyn tuloksesta.
    e. ( ) vähintään n tietuetta tuottaa enintään k % kyselyn tuloksesta.
59. **Mikä seuraavista ei kuulu symmetrisen kryptosysteemin avaimenhallintaan?**
    a. ( ) avaimen varmuuskopiointi/palauttaminen
    b. ( ) avainmateriaalin luonti
    c. ( ) avaimen käyttötarkoituksen kontrolli
    d. ( ) avaimen pakkoluovutus (key escrow)
    e. ( ) avaimen asettaminen sulkulistalle
60. **Mikä seuraavista ei päde bittikäteisestä?**
    a. ( ) Symmetrisiin kryptosysteemeihin perustuvissa järjestelmissä rahabittien omistaja ei pääse näkemään niitä binäärimuodossa edes salattuina.
    b. ( ) Joissain systeemeissä bitit voivat olla sillä tavoin vapaina, että niitä voi kopioida.
    c. ( ) Järjestelmässä, jossa bitit myynyt pankki joutuu tarkastamaan, ettei lunastettavia bittejä ole ennestään lunastettu, ei alkuperäisen ostajan identiteettiä voida piilottaa.
    d. ( ) Toteutuksessa voidaan käyttää sellaista allekirjoitusalgoritmia, jossa pankki ei pysty luomaan allekirjoitusta yksin, vaan hänen täytyy ensin saada sopiva viesti asiakkaalta.