

1. **Selitä lyhyesti** seuraavaat tietoliikenteeseen ja tietoturvaan liittyvät käsitteet ja lyhenteet (6p)
  - a. Hajautettu järjestelmä
  - b. CIA-malli
  - c. Reitin
  - d. DNS
  - e. CIDR
  - f. Socket API
  
2. **Perustele** lyhyesti mitkä seuraavista väitteistä pitävät paikkansa ja mitkä eivät (pisteet tulevat perusteluista) (6p)
  - a. WLANissa käytetään törmäysten havaitsemiseen perustuvaa monipääsyprotokollaa
  - b. Modernilla, hyvällä salausalgoritmilla salattu viesti on käytännössä murtamaton
  - c. Fyysisellä kerroksella tapahtuvat tietoliikennevirheet johtuvat liki aina huonolaatuisista komponenteista
  - d. Palvelinohjelman ohjelmointi on haastavampaa kuin asiakasohjelman
  - e. 196.236.260.1 on toimiva IP-osoite
  - f. IP tarjoaa luotettavaa tiedonsiirtoa
  
3. **AJAX & TCP**
  - a. Määrittele AJAX (kurssin kontekstissa). Mitä sillä pyritään tekemään? Minkälaisia teknologioita siinä käytetään? (3p)
  - b. Miten TCP-yhteys avataan? Miten se suljetaan? Miksi? (3p)
  
4. **Tietoturva**
  - a. Selaat Webiä ja huomaat, että verkkosivun siirtämiseen on käytetty HTTPS-protokollaa. Miten selaimesi on varmistunut siitä, että verkkosivu on peräisin siltä palvelimelta, jonka nimi lukee selaimen osoitekentässä? (4p)
  - b. Lue oheinen artikkeli nettikaupan tietoturvasta. Mitkä käsitteet toimittaja sekoittaa artikkelissaan? Miten kritisoisit artikkelia? (2p)
  
5. **Protokollapino (6p)**

Ohessa on kuva Ethernet-kehyksestä. Mille TCP/IP-protokollapinon kerroksille otsakkeet A,B,C ja D sijoittuvat? Mikä kunkin kerroksen tehtävä on ja mitä tietoja kerroksen otsakkeessa pitää olla tehtävän toteuttamiseksi?

A	B	C	D	Data	A
---	---	---	---	------	---