

1.

a) Miten IEEE:n WLAN-standardit 802.11, 802.11a, 802.11b, 802.11g ja 802.11n toimivat ja miten ne eroavat toisistaan? Vertaile standardeja keskenään. Kerro lisäksi kaikki mitä tiedät ns. Super-G:stä (samasta asiasta käytetään myös esim. nimityksiä Turbo-G, Speedbooster ja Afterburner). (6p)

b) Mitä Wi-Fi, WPA, WPA2 ja WMM ovat? Miten ne toimivat? Mitä hyötyä niistä on WLAN-verkoille? (5p)

2. Kerro kaikki mitä tiedät ja ymmärrät omasta harjoitustyöstäsi? (Jokaiselle pakollinen LAN-opintojakson 1. harjoitustyö) (10p)

3.

a) Mitä sijaintipaikan kartoituksella tarkoitetaan? Mitkä ovat sijaintipaikan kartoituksen painopisteet? Kerro sijaintipaikan kartoituksen kulku pääpiirteissään (kyseessä suuri yritys). (7p)

b) Mitä asioita tulisi ottaa huomioon, kun suunnitellaan WLAN-verkkoa kotiin? (4p)

4.

a) Luodaan 4-tavuinen jono S_i , joka sisältää numerot nolasta kolmeen:

$$S_i = \begin{matrix} 0 & 1 & 2 & 3 \\ S_0 & S_1 & S_2 & S_3 \end{matrix}$$

Luodaan lisäksi 4-tavuinen avainjono K_i , johon toistetaan avainta niin kauan, kunnes se täyttää koko jonon (valitaan toistettaviksi tavuiksi 2 ja 5):

$$K_i = \begin{matrix} 2 & 5 & 2 & 5 \\ K_0 & K_1 & K_2 & K_3 \end{matrix}$$

Muodosta salausavain S_t . Salaa ilmeisesti lähetettävä teksti "HI" (H on binäärimuodossa 01001000 ja I on binäärimuodossa 01001001). Pura salaus vastaanottopäässä ja tarkista, että sait saman salaamattoman tekstin! (Vinkki: WEP-salaus & RC4) (5p)

b) Mitä BSS, IBSS sekä ESS ovat ja miten ne eroavat toisistaan? Hahmottele selityksesi tueksi kuva jokaisesta erikseen. (6p)

5.

a) Miten tietoturva on hoidettu WLAN-verkoissa? Mitä heikkouksia WLAN-tietoturvassa on? Miten WLAN-tietoturvaa voidaan parantaa? (7p)

b) Miksi WLAN käyttää CSMA/CA-protokollaa? Miten se eroaa Ethernetin käyttämästä CSMA/CD-protokollasta? (4p)