

Langattomat lähiverkot 2003, syksy. 2. välitentti. 4.12.2003
klo 16:00-18:00, E26/27.

1. Mitä asioita tulisi ottaa huomioon sopivaa WLAN-laitteistoa valittaessa? (6p)

2. Mitä asioita tulisi ottaa huomioon, kun suunnitellaan WLAN-verkkoa kotiin? (7p)

3. Luodaan 4-tavuinen jono S_i , joka sisältää numerot nollassa kolmeen:

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

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

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

Muodosta salausavain S_t . Salaa ilmaitse lähetettävä teksti "HI" (H on binäärimuodossa 01001000 ja I on binäärimuodossa 01001001). Pura salaus vastaanottopäässä ja tarkista, että sait saman salaamattoman tekstin! (7p)

4. Millaisia heikkouksia WEP-salauksessa on ja miten hakkeri voi yrittää hyödyntää niitä? Miten tietoturvaaukia vastaan voidaan suojautua? (7p)

Tentissä saa olla mukana kynä, kumi ja opiskelijakortti.