Langattomat lähiverkot, kevät 2005. 2. välitentti. 22.3.2005 klo 14:00-16:00, MTA.

1. Vastaa **vain** kohtaan 1a, jos olet jo pitänyt/tehnyt oman harjoitustyöesityksesi. Muussa tapauksessa vastaa **vain** kohtaan 1b. (molempiin kohtiin vastaaminen on kielletty)
a) Kerro kaikki mitä tiedät ja ymmärrät omasta harjoitustyöstäsi (Jokaiselle pakollinen LAN-kurssin 1. harjoitustyö)? (6p)
b) Kerro kaikki mitä tiedät ja ymmärrät IEEE 802.1X:stä. (6p)

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

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

$S_i =$	0	1	2	3
	S_0	S_1	S_2	S_3

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

$K_i =$	2	5	2	5
	K_0	K_1	K_2	K_3

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

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

Tentissä saa olla mukana kynä, kumi ja opiskelijakortti.