Langattomat lähiverkot, kevät 2005. 2. välitentti. 31.3.2005 klo 8:00-12:00, SL.

Voit tehdä joko LOPPUTENTIN, 1. VÄLITENTIN, 2. VÄLITENTIN, tai MOLEMMAT VÄLITENTIT. Välitenttejä ei saa uusia, joten mikäli olet tehnyt jo aiemmin jonkun välitentin, SITÄ EI NYT SAA TEHDÄ UUDESTAAN! Et saa myöskään tehdä LOPPUTENTTIÄ ja VÄLITENTTIÄ SAMALLA KERTAA! Aikaa on 4h/lopputentti ja 2h/välitentti.

1. Kerro kaikki mitä tiedät ja ymmärrät omasta harjoitustyöstäsi (Jokaiselle pakollinen LAN-kurssin 1. harjoitustyö)? (6p)

2. 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)

3. Mitä WPA ja WPA2 ovat? Miten ne toimivat? Mitä hyötyä niistä on WLAN-verkoille? (7p)

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

Tentissä saa olla mukana kynä, kumi ja opiskelijakortti.