

Wireless Local Area Networks, spring 2005. 2. test. 31.3.2005 8:00-12:00 at SL.

You can make FINAL EXAM, 1. TEST, 2. TEST, or BOTH 1. AND 2. TESTS. You can't retake 1. and 2. tests, so if you already have made 1. or 2. test, YOU CAN'T RETAKE IT NOW! You also can't make FINAL EXAM and (1. OR 2.) TEST AT THE SAME TIME. You have 4 hours for final exam, 2 hours for 1. test, and 2 hours for 2. test.

1. Write everything you know and understand about your practical assignment. (1. practical assignment of LAN course, that is mandatory for everyone) (6p)

2. Let's create 4-byte sequence  $S_i$ , which consist of numbers from zero to three:

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

We also create 4-byte keysequence  $K_i$ , where we repeat the key as long as  $K_i$  is full (let's select bytes 2 and 5):

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

Generate encryption key  $S_i$ . Encrypt text "HI" ("H" is 01001000 and "I" is 01001001 in binary form). Decrypt text in the receiving end and check that you got the same "HI" that was sent! (7p)

3. What WPA and WPA2 are? How do they work? What benefits do they offer to WLANs? (7p)

4. What kind of vulnerabilities are there in WEP? How hacker can take advantage of them? How can you protect your network against these security threats? (7p)

You can use pencil, rubber and student-card.