CS 519
Cryptography and Network Security
Instructor: Ali Aydın Selçuk
Department of Computer Engineering, Bilkent University

Homework #3

Due October 18, 2012, beginning of the class

1. Answer the following questions regarding the WEP protocol:
   (a) Describe the challenge-response authentication protocol used in WEP. Why is this protocol not secure when implemented with a stream cipher like RC4?
   (b) Describe the message authentication mechanism used in the WEP protocol. Why is this not secure as a MAC? How can an attacker inject arbitrary packets into the user's connection?
   (c) Describe how an active attacker can completely bypass WEP encryption and read WEP-encrypted messages by breaking the MAC scheme used.
2. Question 2, the midterm exam of Fall 2006.
3. Question 4, the midterm exam of Fall 2009.