The following is a list of possible questions for our quiz on December 5th. Some of the questions will not be asked in the quiz. All the questions that will appear in the quiz will appear exactly as shown below (however, numeric parameters may be changed). The quiz is closed textbook, closed notes and closed neighbors. Note that the questions, which did not appear in this quiz, still may appear in the exams. You will find a solution for these questions during lectures.

#1:   What are “application-level security implementations”? What are “protocol-level security implementations”?

#2:   What are the four security functions IPSec perform?

#3:   What are the primary advantages in using “protocol-level security implementations”? Mention at least three.

#4:   What are the four security issues “data integrity” in IPSec provides protection for?

#5:   What does “Tunnel” in “IPsec Tunnel Mode” mean?

#6:   What are the six different tunnel modes in IPSec?

#7:   What security threats “IPSec Transport-Mode AH” prevent?

#8:   “IPSec AH mode” uses “secret hash key”. What is it for?

#9:   If anything in TCP payload field has been modified (unauthorized modification) after the TCP packet was transmitted, does “IPSec Transport-Mode AH” detect such unauthorized modifications? If no, explain why not. If yes, explain how.

#10:  Is it possible for MIM attackers to change the destination IP address of IP packets that are protected by “IPSec Transport-Mode AH” so that the attackers modify the receiver IP address in IP packets to redirect IP packets to other host computers in the Internet? If no, explain why not. If yes, explain how.

#11:  Is it possible for masquerading attackers to transmit IP packets using a spoofed (bogus) IP address to a receiver (without a receiver detecting the spoofed sender IP address) If no, explain why not. If yes, explain how.