The following is a list of possible questions for our quiz on December 3rd. 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 is “authentication”?
#2: What is “authorization”?
#3: What is “access control”?
#4: What is “data confidentiality”?
#5: What is data integrity”?
#6: What is “nonrepudiation”?
#7: What is (are) the major protection(s) against modification of message attacks?
#8: What is (are) the major protection(s) against replay attacks?
#9: What is (are) the major protection(s) against release of message contents attacks?
#10: What is (are) the major protection(s) against masquerade attacks?
#11: What is (are) the major protection(s) against traffic analysis attacks?
#12: What is “message digest”?
#13: Why is it necessary to encrypt the message digest by the private (secret) key of a sender?
#14: What does “digital certificate” certify?
#15: Regarding digital certificates, after your local web browser downloads a digital certificate, describe how the local browser confirms the correctness of the public key (describe the procedure)?
#16: How is the following “certificate error” caused (technically explain how the “certificate error” is caused)?

![Certificate Error Image]

#17: How are “the root CAs” different from “(other) CAs”?

#18: What is (are) the major protection(s) against denial of service (DoS) attacks?

#19: What is (are) the major protection(s) against distributed denial of service (DDoS) attacks?

#20: Why are DoS and DDoS attacks hard to prevent?