CS 447-001 Networks and Data Communications  
Fall 2019  
Quiz #12 on December 3, 2019 (SOLUTIONS)

Your Last Three Digits: ________________ 
(please do NOT write all of your student ID or your name) 
Grade: ______

*********************************************************

(1) What is “authentication”? 

Authentication is the act of confirming the identity of a user as he (she) claims to be.

(2) What is (are) the major protection(s) against replay attacks? 

To prevent replay attacks, a hard-to-guess message (packet) sequence number, which is unique to each message is required. The unique sequence number should be protected by unauthorized modification to prevent the sequence numbers from being modified by attackers.
(3) What is (are) the major protection(s) against modification of message attacks?

Digital signature (a message digest encrypted by the sender’s private key)

(4) Why is it necessary to encrypt the message digest by the private (secret) key of a sender?

Otherwise, attackers can attach the recalculated message digest after the attackers modify the message body.

(5) What does “digital certificate” certify?

Public key