CS 447-002 Networks and Data Communications
Spring 2024
Quiz #10 on April 22, 2024 (SOLUTIONS)

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

Grade: _____

****

(1) What are "passive (network security) attacks"?

Passive attacks are (any) malicious activities that do not (a) add new contents or (b) modify the contents of user data (or transmitted data).

Note: This question does not ask an example or "passive attacks", but a definition of "passive attacks". For example, "traffic analysis" is a passive attack, but passive attack is not (necessarily) "traffic analysis". In the same reason, "release of message contents" is not a good solution to this question either.

(2) What is "the symmetric cryptography"? What is its primary weakness (mention the one identified as its primary weakness in the previous CS447 lecture)?

The symmetric cryptography is any cryptography scheme (encryption) for which encryption and decryption use the same key.

(3) If a payload data is encrypted using a private (secret) key (assuming an asymmetric cryptography), what (security) protection does it offer to (legitimate users)?

If a payload data is encrypted using a private (secret) key, receivers who decrypt the encrypted message using the public key of the private key, they (receivers) are sure that the contents in the message must come from the sender (who is the only one who has the private key).

(4) If a payload data is encrypted using a public key (assuming asymmetric cryptography), what (security) protection does it offer to (legitimate users)?

If a payload data is encrypted using a public key, the only one who has its private key can decrypt the encrypted message.

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

To make sure none but the one who has the private key can create a message digest. This makes sure that attackers between a sender and a receiver can not create a message digest, preventing any unauthorized creation or modification of a message digest between a sender and a receiver (i.e., "MIM").