

CS447 –Networks and Data Communications

Quiz #6, July 23, 2026

SOLUTIONS

Note 1: please provide your solutions to the “solution template”

Note 2: answer the questions by including only the option symbols (i.e., (a), (b), (c), and (d)). Please do NOT answer the questions by copying the actual options for each question.

#1: Which of the following statements is a correct description for “passive attacks” (select one)?

- (a) Passive attacks are any harmful activities performed by attackers who have some malicious intentions to legitimate users and/or legitimate organizations who use computer networks.
- (b) Passive attacks are any harmful activities performed not only by attackers who have some malicious intentions to legitimate users and/or legitimate organizations who use computer networks but also by careless users who accidentally perform any harmful activities without malicious intents.
- (c) Passive attacks are any harmful activities performed by attackers who actively look for opportunities for exploiting weaknesses in computer networks.
- (d) None of the above.

Solution: (c)

#2: Which of the following statement is a correct description for “masquerading attacks” (select one – one you think the best fit)?

- (a) Masquerading attacks are those attacks attackers perform to cause some harmful consequences to legitimate users by repeating some actions using network applications.

As long as the repeated actions do not duplicate the legitimate messages, they are not “replay”.

- (b) masquerading attacks are those attacks attackers perform to cause some harmful consequences to legitimate users by creating bogus messages (attackers falsify bogus messages).

“Masquerading attacks”

- (c) Masquerading attacks are those attacks attackers perform to cause some harmful consequences to legitimate users by duplicating messages (packets) legitimate users created (and transmitted to their intended receivers).

Replay attacks

- (d) Replay attacks are those attacks attackers perform to cause some harmful consequences to legitimate users by capturing messages (packets) from legitimate users followed by diverting them to users the legitimate transmitting users do not intend.

“Masquerading attacks”

- (e) None of the above

Solution: (b) or (d)

#3: Which of the following statement is a correct description for “traffic analysis attacks” (select one)?

- (a) Traffic analysis attacks are those attacks attackers perform by modifying the contents of messages (packets) from a sender to a receiver to analyze the weaknesses (or vulnerabilities) in the computer systems the users (senders’ and receivers’) are using.

FALSE traffic analyses will not modify the contents of the transmitted messages

- (b) Traffic analysis attacks are those attacks attackers perform to eavesdrop the contents of the messages from a transmitting host computer to a receiving host computer in a computer network.

FALSE: Attackers do not have to see/understand the contents of the transmitted messages for “traffic analysis”.

- (c) Traffic analysis attacks are those attacks attackers perform by modifying the contents of messages (packets) from a sender to a receiver to observe (analyze) how the modifications by attackers affect the users (senders’ and receivers’) activities after the modifications.

FALSE (it’s “MIM attacks”)

- (d) For attackers to successfully perform traffic analysis attacks, attackers need to know the sender (transmitting users, transmitting organizations, transmitting host computers, or transmitting domains) and the receiver.

TRUE

- (e) None of the above.

Solution(s): (d) (or (e))

#4: Which of the following statement is a correct description for “denial of service attacks” (select one)?

- (a) By performing denial of service attacks, attackers can divert messages (packets) to the receivers senders do not intend.

- (b) By performing denial of service attacks, attackers can falsify the identities of users who transmit messages (packets) to their receivers.

- (c) By performing denial of service attacks, attackers can modify the contents of messages (packets) senders transmit to receivers.

- (d) By performing denial of service attacks, attackers can eavesdrop the contents of messages (packets) senders transmit to receivers.

- (e) None of the above.

Solution: (e)

#5: Which of the following statements is correct for comparing the advantages and the disadvantages of asymmetric cryptographies to those of symmetric cryptographies (select all that apply)?

- (a) Asymmetric cryptographies are more scalable in terms of their execution overhead, but less scalable in terms of the number of users (the number of host computers a host computer needs to communicate with) compared with symmetric cryptographies.
- (b) Asymmetric cryptographies are more scalable in terms of the number of users (the number of host computers a host computer needs to communicate with) but less scalable in terms of their execution overhead compared with symmetric cryptographies.
- (c) Sharing keys (encryption and decryption keys) is easier for asymmetric cryptographies than symmetric cryptographies.
- (d) There is no difference (in terms of the difficulties) between symmetric and asymmetric cryptographies for sharing keys.
- (e) None of the above.

Solution: (b) and (c)

#6: Suppose that a user 'A' is the owner of a pair of a private key ('S') and a public key ('P') and that 'B' is one of the users who obtained P from A.

Which of the following statements is correct for a description of asymmetric cryptographies (select all that apply)?

- (a) If B encrypts its messages to A using P, A is the only one who can correctly see the contents and the meaning of the messages from B.

TRUE

- (b) If B encrypts its messages to A using P, A can tell the meaning in the contents (not just "contents" in a sense that whatever appear in the messages) in the messages are from B but not from anyone else.

FALSE

- (c) If A encrypts its messages to B using S, B is the only one who can correctly see the contents and the meaning of the messages from A.

FALSE

- (d) If A encrypts its messages to B using S, B can correctly tell the meaning in the contents* (not just "contents" in a sense that whatever appear in the messages) in the messages are from A but not from anyone else.

TRUE

- (e) None of the above.

Solutions: (a) and (d)

#7: Suppose the following assumptions (i, ii, and iii):

- i: A user 'A' is the owner of a pair of a private key ('S') and a public key ('P') and a user 'B' is one of the users who obtained P from A.
- ii: A encrypts its message ('M') that contains only one numeric parameter (e.g., '100') but nothing else.
- iii: Any information in the headers of any network protocol (especially the network-layer protocol that carries the identity information about the sender) can be modified or falsified any time.

Question: Which of the following statements is correct (select one)?

- (a) When B receives a message from A, B is sure that no one else except A sent the contents* in the message (assuming that B decrypts the message from A using P).

FALSE

NOTE: "the contents" means that that is the number A sent.

- (b) When B receives a message from A, B is sure that no one else except B can see the contents* in the message and that no one else except A sent the contents* in the message (assuming that B decrypts the message from A using P).

FALSE

NOTE: "the contents" means that that is the number A sent.

- (c) When B receives a message from A, B is sure that no one else except B can see the contents A sent in the message (assuming that B decrypts the message from A using P).

FALSE

- (d) None of the above.

Solution: (d)

#8: Which of the following statements is correct about “digital signature” (select one)?

- (a) Digital signatures are message digests encrypted by the private key of senders to make sure that receivers are sure that the attached message digest is never duplicated after the digest was calculated at the sender side.

FALSE*

Receivers cannot tell if the message is an original copy or a duplicated copy using message digests.

- (b) Digital signatures are message digests encrypted by the private key of senders to make sure that only the receivers who are supposed receive messages from the sender can see the contents (values) of the message digests.

FALSE*

Since anyone has the public key, anyone can decrypt the message digest encrypted by the private key of the sender.

- (c) Digital signatures are message digests encrypted by the public key of senders to make sure that receivers are sure that the attached message digest is never modified after the digest was calculated at the sender side.

FALSE

- (d) Digital signatures are message digests encrypted by the public key of senders to make sure that only the receivers who are supposed receive messages from the sender can see the contents (values) of the message digests.

FALSE

- (e) None of the above.

TRUE

Solution: (e)

#9: Suppose the following assumptions (i, ii, and iii):

i: 'A' is a merchant who sells product using its website in the Internet.

ii: 'B' is a user in the Internet, who visited the website of A trying to buy some products from A through A's website.

iii: 'C' is the CA user A contacted for the digital certificate of A.

Question: Which of the following statements about digital certificates is the best statement for a description of digital certificate (select the best one)?

(a) B can confirm that the contents in A's website are genuine (i.e., none of contents in the website is falsified by anyone), because B can be sure that the contents in the website are encrypted by the public key of C.

FALSE*

The contents in the website are NOT encrypted by the public key of C

(b) B can confirm that the contents in A's website are genuine (i.e., none of contents in the website is falsified by anyone), because B can be sure that the contents in the website are encrypted by the public key of A.

FALSE*

The contents in the website are NOT encrypted by the public key of A

(c) B can confirm that the contents in A's website are genuine (i.e., none of contents in the website is falsified by anyone), because B can be sure that the contents in the website are decrypted by the public key of A.

TRUE

(d) B can confirm that the contents in A's website are genuine (i.e., none of contents in the website is falsified by anyone), because B can be sure that the contents in the website are encrypted by the private key of C.

FALSE*

The contents in the website are NOT encrypted by the private key of C.

(e) None of the above.

Solution: (c)

#10: Suppose the following assumptions (i, ii, iii, and iv):

- i: 'A' is a merchant who sells product using its website in the Internet.
- ii: 'B' is a user in the Internet, who visited the website of A trying to buy some products from A through A's website.
- iii: 'C' is the CA user A contacted for the digital certificate of A.
- iv: 'C' is not a root CA.

Question: Which of the following statements about 'C' (select the best one)?

- (a) C needs a root CA for the root CA to authenticate the private key of A (i.e., for proving the genuineness of the key to B).

FALSE the underlined phrase

- (b) C needs a root CA for the root CA to authenticate the public key of A (i.e., for proving the genuineness of the key to B).

FALSE the underlined phrase

- (c) C needs a root CA for the root CA to to authenticate the private key of C (i.e., for proving the genuineness of the key to B).

FALSE the underlined phrase

- (d) C needs a root CA for the root CA to authenticate the public key of the root CA (i.e., for proving the genuineness of the key to B).

FALSE the underlined phrase

- (e) C needs a root CA for the root CA to authenticate the private key of the root CA (i.e., for proving the genuineness of the key to B).

FALSE the underlined phrase

- (f) C needs a root CA for the root CA to authenticate the public key of C (i.e., for proving the genuineness of the key to B).

TRUE

- (g) None of the above.

Solution: (f)