Quiz 6

Due Feb 9 at 11:59pm **Points** 15 **Questions** 10
Available Feb 8 at 12pm - Feb 9 at 11:59pm **Time Limit** 30 Minutes

Instructions

This quiz covers the following module objectives:

- MO 11. Recall Diffie-Hellman protocol and the man-in-the-middle attack against it (CO 5)
- MO 12. Identify the contents of a public key certificate (CO 4)
- MO 13. Apply forward search attack in a given scenario (CO 5)
- MO 14. Define major steps in key distribution protocols (CO 4)

It will also cover password storage.

This quiz is no longer available as the course has been concluded.

Attempt History

	Attempt	Time	Score
LATEST	Attempt 1	8 minutes	15 out of 15

ⓘ Correct answers are hidden.

Score for this quiz: **15** out of 15
Submitted Feb 8 at 12:40pm
This attempt took 8 minutes.

Question 1

1 / 1 pts

Which of the following is specifically used to verify that message has not been altered?

○ Message authentication code (MAC)

○ RSA

○ Public key

○ Secure Shell

Question 2

2 / 2 pts

Which of the following is defined as a temporary encryption key used between two principals?

○ Key Distribution Center

○ Primary Key

● Session Key

○ Long-Term Key

Question 3

1 / 1 pts

(True/False): If the public keys of the nodes do not have a certificate, they can be fake.

● True

○ False

Question 4

2 / 2 pts

Which of the following is NOT a property of a secure hash function?

○ Second pre-image resistance

● Load balance by a trusted third party

○ Pre-image resistance (or One Way)

○ Collision resistance

Question 5

2 / 2 pts

Suppose Alice and Bob use the Diffie-Hellman protocol to establish a symmetric session key. They choose a large prime number p and a smaller integer $g \in \{2, \ldots, p-2\}$ for the protocol. Suppose Alice chooses a random number a and Bob chooses a random number b . Alice sends A = $g^a \mod p$ to Bob, while Bob sends B = $g^b \mod p$ to Alice. What would be the shared session key?

● $g^{ab} \mod p$

○ $A^a \mod p$

○ $A^B \mod p$

○ $B^A \mod p$

Question 6

1 / 1 pts

Suppose Alice and Bob use the Diffie-Hellman protocol to establish a symmetric session key. They choose a large prime number p and a smaller integer $g \in \{2, \ldots p-2\}$ for the protocol. Suppose Alice chooses a random number a and Bob chooses a random number b. Alice sends $A = g^a \mod p$ to Bob, while Bob sends $B = g^b \mod p$ to Alice. Now suppose Mallory is a man-in-the-middle attacker. Which of the following is true about Mallory?

○ Mallory will forward A to Bob and try to figure out a from A

○ Mallory does not know p or g

○ Mallory will compute $g^{A \cdot B}$

● Mallory will generate a random number mb and send $g^{mb} \mod p$ to Alice

Question 7

1 / 1 pts

We have discussed a scheme to store the hash result of user passwords in a computer. Which of the following is NOT true about this scheme?

● The plaintext password needs to be stored.

○ To log in, a user has to type in the plaintext password.

○ This scheme is susceptible to the Rainbow attack.

○ The user name needs to be stored.

Question 8

2 / 2 pts

Alice’s age is between 26 and 35 (inclusive). Now Alice needs to send her birthday to her lawyer, Bob. Bob has a public/private key pair, Alice knows Bob’s public key (pubkey-Bob), but she does not know Bob's private key (privkey-Bob). Alice plans to send the message as $E_{\text{pubkey-Bob}}$ (mm/dd/yyyy) to Bob. Here she will encrypt the month, day, and year of her birthday with Bob’s public key. Carol is another customer of Bob’s law firm and she knows Bob’s public key as well. Carol can eavesdrop on the encrypted packet that Alice sends to Bob.

Suppose today is October 1, 2019, and Carol wants to employ a forward search attack to guess Alice's birthday. Which of the following is a possible entry in Carol's forward search table?

● < 08/31/1993, $E_{pubkey-Bob}$(08/31/1993) >

○ < 09/30/1983, $E_{pubkey-Bob}$(09/30/1983) >

○ < 10/06/1994, $E_{pubkey-Bob}$(10/06/1994) >

○ < 10/06/1994, $E_{privkey-Bob}$(10/06/1994) >

Question 9

2 / 2 pts

An X.509 certificate can contain the following information except

○ Subject public key information

● Subject private key

○ Certificate signature algorithm

○ Serial number

Question 10

1 / 1 pts

True/False: Alice and Bob rely on a trusted third party (TTP) to establish a shared key using the toy protocol discussed in video segment 31. Alice shares secret key $k_A$with TTP, and Bob shares secret key $k_B$with TTP. Suppose TTP chooses k_{AB} as the shared key between Alice and Bob, it generates a ticket that is equal to $E\left(k_B,\ A \parallel k_{AB}\right) \parallel B$.

○ True

● False

Quiz Score: **15** out of 15