Assignment 8

The due date for submitting this assignment has passed. Due on 2019-03-27, 23:59 IST.
As per our records you have not submitted this assignment.

1) To check integrity of a message, or document, receiver creates the
   A. hash-table
   B. hash tag
   C. hyper text
   D. finger print

   Accepted Answers: B

2) A session symmetric key is used between two parties for ______.
   A. twice
   B. only once
   C. multiple times
   D. recovering previously sent data

   Accepted Answers: C

3) Digital signature provides
   A. authentication
   B. non-repudiation
   C. both (A) and (B)
   D. neither (A) nor (B)

   Accepted Answers: C

4) Authentication means ______.
   A. verification of user's identification
A sender must not be able to deny sending a message that was sent, is known as
A. message non-repudiation
B. message integrity
C. message confidentiality
D. message sending

When data must arrive at receiver exactly as they were sent, it is called
A. message confidentiality.
B. message integrity.
C. message splashing.
D. message sending.

In Diffie-Hellman key exchange protocol, if two parties are not authenticated to each other then __________ can harm the security of the protocol.
A. man-in-the-front attack
B. ciphertext attack
C. plaintext attack
D. man-in-the-middle attack

The goal of key distribution center is
A. to sustain privacy of plaintext.
B. to distribute ciphertexts among users.
C. to reduce the risk in exchanging keys.
D. to maintain secrecy of signed messages.
9) When prime $p$ used in ElGamal signature and composite $n$ used in RSA signature are of same which of the following is true?
   - A. Elgamal signatures are shorter than RSA signatures
   - B. Elgamal signatures are more efficient to verify than RSA signatures
   - C. RSA signature is faster than Elgamal signature
   - D. None of the above

   No, the answer is incorrect.
   Score: 0
   Accepted Answers: C

10) What is a hash table?
   - A. A structure that maps values to keys
   - B. A structure that maps keys to values
   - C. A structure used to attack symmetric cipher
   - D. A structure used to implement stack and queue

   No, the answer is incorrect.
   Score: 0
   Accepted Answers: B