**COLLEGE OF COMPUTING & INORMATION TECHNOLOGY**

**Lecturer: Assoc. Prof. Dr. Hisham Dahshan**

**Course Name: Data Security**

**Course Code: CS716** **Time allowed : 15 Minutes.**

**Date: 12/11/2024**

# Quiz1 A

| **Student Name** | |
|---|---|

**Answer the following questions:**

**Question 1:**

Define Perfect secrecy of a cipher.

**Question 2:**

Explain the eavesdropping indistinguishability experiment $PrivK_{A,\Pi}^{eav}(n)$.

**Question 3:**

Explain the Meet in the middle attack in DES.

# COLLEGE OF COMPUTING & INORMATION TECHNOLOGY

**Lecturer: Assoc. Prof. Dr. Hisham Dahshan**

**Course Name: Data Security**

**Course Code: CS716** **Time allowed : 15 Minutes.**

**Date: 12/11/2024**

## Question 4: Choose the right answer:

1) Which of the following is not a principle of CIA triad?
   A. Integrity
   B. Confidentiality
   C. Authentication
   D. Availability

2) Data encryption standard (DES) is a block cipher and encrypts data in blocks of size of _____ each.
   A. 32 bits
   B. 16 bits
   C. 64 bits
   D. All of the mentioned

3) Consider the following steps: Substitution bytes, Shift Rows, Mix columns, and Add round key. The above steps are performed in each round of which of the following ciphers?
   A. Data Encryption Standard (DES)
   C. Rail fence cipher
   B. Advance Encryption Standard (AES)
   D. None of the previous

4) In Cipher block chaining mode, the current plaintext block is added to the ____.
   A. Next ciphertext block
   C. Previous ciphertext block
   B. Next ciphertext block
   D. None of the mentioned

5) In the Advanced Encryption Standard (AES), the highest security will be provided by the algorithm when the number of rounds and key length are:
   A. 14 and 192
   C. 12 and 192
   B. 12 and 256
   D. 14 and 256