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 B

Student Name	

Answer the following questions:

Question 1 (5 pts): Choose the right answer:

1) 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?

i. Rail fence cipher iii. Advance Encryption Standard (AES)
ii. Data Encryption Standard (DES) iv. None of the previous

2) Which of the following is not a principle of CIA triad?

i. Confidentiality ii. Integrity
iii. Authentication iv. Availability

3) Data encryption standard (DES) is a block cipher and encrypts data in blocks of size of _____ each.

i. 16 bits ii. 32 bits
iii. 64 bits iv. All of the mentioned

4) In Cipher block chaining mode, the current plaintext block is added to the ____.

i. Previous ciphertext block iii. Next ciphertext block
ii. Next ciphertext block iv. 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:

i. 12 and 192 iii. 12 and 256
ii. 14 and 192 iv. 14 and 256

Question 2:

Define Perfect secrecy of a cipher.

Question 3:

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

Question 4:

Explain the Meet in the middle attack in DES.