**ACHARYA BANGALORE B SCHOOL**

**DEPARTMENT OF COMPUTER SCIENCE – BCA**

**Online Assessment -- April 2020**

**BCA 6 semester**

**Cryptography and Network Security**

***Choose and write the correct answer.***

1. \_\_\_\_\_\_\_\_ is the science and art of transforming messages

to make them secure and immune to attacks.

A. Cryptography

B. Cryptanalysis

C. either (a) or (b)

D. neither (a) nor (b)

2. The \_\_\_\_\_\_\_\_is the original message before transform ation

A. cipher text

B. plaintext

C. secret-text

D. none of the above 

3. The \_\_\_\_\_\_\_\_ is the message after transformation

A. ciphertext

B. plaintext

C. secret-text

D. none of the above

4. A(n) \_\_\_\_\_\_\_ algoritthm transforms plaintext to ciphertext

1. encryption
2. decryption
3. either (a) or (b)
4. neither (a) nor (b)

5. A(n) \_\_\_\_\_\_ algorithhm transforms ciphertext to plainttext

1. encryption
2. decryption
3. either (a) or (b)
4. neither (a) nor (b)

6. A combination of an encryption algorithm and a decryption algorithm is called a \_\_\_\_\_\_\_\_.

1. Cipher
2. secret
3. key
4. none of the above

7. The \_\_\_\_\_\_\_ is a number or a set of numbers on which the cipher

operates

1. cipher
2. secret
3. key
4. none of the above

8. In a(n) \_\_\_\_\_\_\_\_ cipher, the same key is used by both the sender

and receiver.

A. symmetric-key

1. asymmetric-key
2. either (a) or (b)
3. neither (a) nor (b)

9. In a(n) \_\_\_\_\_\_\_\_, the key is called the secret key.

1. symmetric-key
2. asymmetric-key
3. either (a) or (b)
4. neither (a) nor (b)

10. In a(n) \_\_\_\_\_\_\_\_ cipher, a pair of keys is used.

1. symmetric-key
2. asymmetric-key
3. either (a) or (b)
4. neither (a) nor (b)

***Answer all the questions.***

1. Explain active and passive attack with example?
2. Differentiate symmetric and asymmetric encryption?
3. Define cryptanalysis
4. Compare stream cipher with block cipher with example.
5. Define steganography
6. Define Encryption.
7. Specify the components of encryption algorithm.
8. Define confidentiality and authentication
9. Define cryptography.
10. What are the design parameters of Feistel cipher network
11. Define Product cipher.
12. Give the five modes of operation of Block cipher.
13. State advantages of counter mode.
14. Define Multiple Encryption.
15. Specify the design criteria of block cipher.

------------------------------