

Course Name: ETHICAL HACKING

Assignment- Week 6

TYPE OF QUESTION: MCQ/MSQ/SA

Number of questions: 10

Total mark: 10 x 1 = 10

QUESTION 1:

Which of the following types of attack can the DoS attack be categorized into?

- a. Interruption
- b. Interception
- c. Modification
- d. Fabrication

Correct Answer: a

Detail Solution: In the denial-of-service (DoS) attack, the attacker makes a system/service inaccessible from legitimate users. This is a type of interruption attack.

The correct option is (a).

QUESTION 2:

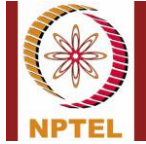
Which of the following statement(s) is/are **false**?

- a. In symmetric key cryptography, separate keys are used by sender and receiver.
- b. In symmetric key cryptography, a single key is used by sender and receiver.
- c. In asymmetric key cryptography, separate keys are used by sender and receiver.
- d. In asymmetric key cryptography, a single key is used by sender and receiver.

Correct Answer: a, d

Detail Solution: Encryption is the most important concept for network security, and typically two types of encryptions are used. Private key (symmetric): where the sender and receiver uses same key for encryption/decryption of the message. Public key (asymmetric): where separate keys are used for encryption and decryption of the message.

Thus the false options are (a) and (d).



QUESTION 3:

On which difficult mathematical problem does the security of RSA algorithm depend on?

- a. Discrete logarithm problem.
- b. Testing whether a given number is prime or not.
- c. Prime factorization problem.
- d. The RSA threshold detection.

Correct Answer: c

Detail solution: The security of the RSA algorithm depends on the complexity of factoring the product of two large prime numbers.

The correct option is (c).

QUESTION 4:

100 parties want to exchange messages securely using public-key cryptography (like RSA). The number of distinct key values required will be _____.

Correct Answer: 200

Detail Solution: In asymmetric encryption, every party has two keys (private and public). For N parties, the number of keys will be $2N = 2 \times 100 = 200$.

QUESTION 5:

20 parties want to exchange messages securely using symmetric key cryptography. The number of distinct key values required will be _____.

Correct Answer: 190

Detail Solution: In symmetric encryption, every pair of communicating parties must have a separate key. For N parties, the number of keys will be NC_2 . For $N = 20$, ${}^{20}C_2 = 20 \times 19 / 2 = 190$.



QUESTION 6:

We want to encrypt the plain text “CRYPTOGRAPHY” using a substitution cipher, where each letter is replaced by the k-th next letter, with the following assumptions:

- (i) The alphabets are wrapped around, i.e. Z is followed by A.
- (ii) Each alphabet (A to Z) is assigned a number (1 to 26).
- (iii) The value of secret key k is 4.

What will be the cipher text?

- a. GWCUXSKWETMC
- b. GVCTXSKVETLC
- c. HTDZAXLYIXPG
- d. KZRVUOCPJQNA
- e. None of these.

Correct Answer: b

Detail Solution: k=4 indicates that for encryption, each letter is replaced by its 4th following letter (C → G, R → V, Y → C, P → T, T → X, O → S, G → K, R → V, A → E, P → T, H → L, Y → C.) If we encrypt the message we will get the cipher text as GVCTXSKVETLC.

Thus the correct option is (b).

QUESTION 7:

Consider a mono-alphabetic cipher with the following key value:

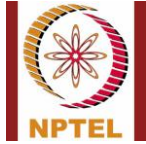
(A B W X E F S T I J O P M N K L Q R G H U V C D Y Z)

What will be the encrypted form of the message “SWAYAM” ?

- a. GCAYAM
- b. SWAYAM
- c. WCAYAM
- d. None of these.

Correct Answer: a

Detail Solution: According to the specified mapping the encrypted message will be GCAYAM.



Hence, the correct option is (a).

QUESTION 8:

If a receiver A wants to carry out decryption on a message received from B using public-key cryptography, which of the following key will be used for decryption by A?

- a. A's public key
- b. A's private key
- c. B's public key
- d. B's private key

Correct Answer: b

Detail Solution: If a receiver A wants to carry out decryption on a message received from B, using public-key cryptography, that means B must have encrypted the message using A's public key which can be decrypted using A's private key.

Thus the correct option is (b).

QUESTION 9:

AES uses an effective key length of _____ bits?

- a. 64 bit
- b. 128 bit
- c. 192 bit
- d. 256 bit
- e. 513 bit.

Correct Answer: b, c, d

Detail Solution: In AES the block length is limited to 128-bit; however, the key length can be 128, 192 or 256 bits.

Thus the correct options are (b), (c) and (d).



QUESTION 10:

Which cryptographic algorithms uses the same key for encryption and decryption?

- a. RSA
- b. Diffie-Hellman
- c. DES
- d. AES

Correct Answer: c, d

Detail Solution: both DES and AES are symmetric key algorithms which uses same key for encryption and decryption.

Thus the correct options are (c) and (d).

*****END*****