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:

15 parties want to exchange messages securely using a symmetric key encryption algorithm. The number of distinct key values required will be:

a. 30
b. 225
c. 210
d. 105

Correct Answer: d

Detail Solution: In symmetric encryption, every pair of communicating parties must have a separate key. For N parties, the number of keys will be ${}^{N}C_2$. For N = 15, ${}^{15}C_2 = 15 \times 14 / 2 = 105$.

The correct option is (d).

QUESTION 2:

200 parties want to exchange messages securely using some public key encryption technique like RSA. The number of distinct key values required will be ___________

Correct Answer: 400

Detail Solution: In public-key or asymmetric encryption, every party is in possession of two keys, a public key and a private key. For N parties, the number of keys will be 2N. For N = 200, the number of distinct keys required will be 200 x 2 = 400.

QUESTION 3:

What are the effective key lengths used in DES and triple-DES symmetric key encryption algorithms in bits?

a. 56 and 168
b. 56 and 112

c. 56 and 56
d. 64 and 128
e. None of these

Correct Answer: a

Detail Solution: In the DES algorithm, the key size is 56 bits. In triple-DES, we have three sequential runs of the DES algorithm. Hence, in triple-DES, the effective key size will be 56 × 3 = 168 bits. Thus, the correct option is (a).

QUESTION 4:

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

a. Discrete logarithm problem.
b. Testing whether a given number if prime or not.
c. Prime factorization problem.
d. The RSA threshold detection.
e. All of these.

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 5:

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 6:

Which of the following terms concern verifying the identity of the sender?

a. Encryption.
b. Authentication.
c. Decryption.
d. None of these.

Correct Answer: b

Detail Solution: Authentication refers to the process of verifying the identity of the sender of a message. Hence, the correct option is (b).

QUESTION 7:

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

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

What will be the encrypted form of the message "W I N D O W" ?

a. W E N D H W
b. S K N G H S
c. S E N D O S
d. None of these.

Correct Answer: c

Detail Solution: According to the specified key, the letter 'W' maps to 'S', 'I' maps to 'E', 'N' maps to 'N', 'D' maps to 'D', and 'O' maps to 'O'. Hence the encrypted form of "WINDOW" will be "SENDOS".

Hence, the correct option is (c).

QUESTION 8:

How many AES rounds are required for 128-bit key size?

a. 10
b. 11
c. 12
d. 14

Correct Answer: a

Detail Solution: 10 rounds are required in the AES algorithm for 128-bit key size.

The correct answer is (a).

QUESTION 9:

For encryption using public-key cryptography, we use the

a. Receiver's public key
b. Receiver's private key
c. Sender's public key
d. Sender's private key

Correct Answer: a

Detail Solution: If a sender A wants to carry out encryption on a message and send it to receiver B using public-key cryptography, A will encrypt the given message using B's public key, so that it can be correctly decrypted by the receiver B using B's private key.

Hence, the correct option is (a).

QUESTION 10:

Which of the following techniques is/are vulnerable to man-in-the-middle attack?

a. AES
b. RSA
c. Diffie-Hellman key exchange
d. None of these.

Correct Answer: c

Detail Solution: Diffie-Hellman key exchange protocol is vulnerable to the man-in-the-middle attack.

Hence, the correct option is (c).

***********END*******