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 is not an example of active security attack?

a. Masquerade
b. Replay
c. Traffic analysis
d. Modification
e. Denial of Service.

Correct Answer: c

Detail Solution: Analyzing the network traffic refers to passive attack. Masquerade, replay, modification, denial of service are active attacks.

Thus the correct option is (c).

QUESTION 2:

Consider the following statements:

(i) In symmetric key cryptography, single shared key is used by sender and receiver.
(ii) In Asymmetric key cryptography, separate keys are used by sender and receiver.

a. Only (i) is true
b. Only (ii) is true
c. Both (i) and (ii) are true.
d. Both (i) and (ii) are false.

Correct Answer: c

Detail Solution: In symmetric key (private key) cryptography, a single key is shared and used by sender and receiver, whereas in public key cryptography separate keys are used by sender and receiver.

Thus correct option is (c).

QUESTION 3:

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

Correct Answer: 105

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, ${}^{15}C_2 = 15 \times 14 / 2 = 105$.

QUESTION 4:

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 5:

How many AES rounds are required for 192-bit key size?

a. 10
b. 11

c. 12
d. 14

Correct Answer: c

Detail Solution: 12 rounds are required in the AES algorithm for 192-bit key size.

The correct answer is (c).

QUESTION 6:

What is the key length in data encryption standard (DES)?

a. 56
b. 64
c. 128
d. 192

Correct Answer: a

Detail Solution: The DES encryption algorithm is a "block cipher" that encrypts information in blocks of 64 bits (8 bytes). Using a 56-bit key, DES encrypts each block in 16 identical rounds.

The correct answer is (a).

QUESTION 7:

100 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: 200

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 = 100, the number of distinct keys required will be 100 x 2 = 200.

QUESTION 8:

In Digital signature sender signs a message with its:

a. Private key
b. Public key

Correct Answer: a

Detail Solution: For digital signature or authentication sender signs a message with its private key that is authenticated by the corresponding public key.

Thus the correct option is (a).

QUESTION 9:

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 10:

Which of the following statement(s) is/are **true** for Diffie-Hellman Key Exchange algorithm?

a. It allows group of users to agree on secret key over insecure channel.
b. The security of the algorithm depends on prime factorization problem.
c. The algorithm is vulnerable to man-in-the-middle attack.
d. It does not require any prior communication between sender and receiver.
e. All of these.

Correct Answer: a, c, d

Detail solution: D-H algorithm is mainly used for key exchange between users over an insecure channel; it does not require any prior communication between sender and receiver for key exchange. As the communication is done over insecure channel it is vulnerable to man-in-the-middle attack. The complexity of the algorithm depends on that of cracking the discrete logarithm problem.

The correct options are (a), (c) and (d).

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