Course Name: ETHICAL HACKING

Assignment- Week 7

TYPE OF QUESTION: MCQ/MSQ/SA

Number of questions: 10 **Total mark: 10 x 1 = 10**

QUESTION 1:

Which type of mapping is implemented by cryptographic hash function?

a. One-to-One

b. Many-to-One

c. One-to-Many

d. Many-to-Many

Correct Answer: b

Detail Solution: A hash function takes a message of arbitrary length and generates a fixed length Hash. That means the input set is very large and output set is finite which makes it many to one mapper.
The correct option is (b).

QUESTION 2:

Two messages M_1 and M_2 are fed to a hash function HASH to generate the hash value:

H_1 = HASH (M_1)

H_2 = HASH (M_2)

Which of the following options can **never be true**?

a. $H_1 = H_2$ and $M_1 != M_2$

b. $H_1 != H_2$ and $M_1 = M_2$

c. $H_1 != H_2$ and $M_1 != M_2$

d. $H_1 = H_2$ and $M_1 = M_2$

Correct Answer: b

Detail Solution: A hash function is deterministic (same input always gives same output) Thus if $M_1 = M_2$; H_1 must be equal to H_2. Two different messages M1 and M2 can, however, generate the same hash value, which is called collision.

The correct option is (b).

QUESTION 3:

Which of the following is true for hash function?

a. Hashing can be reversed.
b. Hash function generates a variable length output.
c. It is computationally easy to find collisions
d. None of these.

Correct Answer: d

Detail Solution: A hash function has the following properties: one way → non-reversible, fixed-length output, and collision resistance (computationally hard to detect collision).

The correct option is (d).

QUESTION 4:

Which of the following is provided by Unkeyed hash function (Modification Detection Code)?

a. Integrity
b. Authenticity
c. Confidentiality
d. Availability

Correct Answer: a

Detail Solution: Unkeyed hash function takes an input of variable length and converts it to a fixed-length output. It is designed to detect if the message has been altered during transmission or not. Any change in message will cause change in hash thus it ensures integrity. Since no key is used it does not provide authenticity. As the message is not encrypted it does not provide confidentiality. Availability is not related with hashing.

Thus the correct option is (a).

QUESTION 5:

Which of the following are UNKEYED hash functions?

a. MD5
b. HMAC
c. SHA-256
d. CMAC

Correct Answer: a, c

Detail Solution: MD5 and SHA-256 are examples of Unkeyed hash function, while HMAC and CMAC are example of keyed hash function.

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

QUESTION 6:

SHA-512 processes the message in _____ bits blocks.

Correct Answer: 1024

Detail Solution: SHA-512 process the message in a block of 1024 bits.

QUESTION 7:

Which type of digital signature generates the same signature every time for a given message?

a. Deterministic Signature
b. Probabilistic Signature
c. Blind Signature
d. Undeniable Signature

Correct Answer: a

Detail Solution:

Deterministic signatures → for a given message, the signing algorithm always produces the same signature.
Probabilistic signatures → use randomization, so even for the same message, different runs of the algorithm generate different signatures.
Blind signatures → signer does not see the content of the message being signed.
Undeniable signatures → require the active participation of the signer during verification.

The correct option is (a).

QUESTION 8:

Which property of digital signature ensures that a signer cannot deny a valid signature created by them?

a. Confidentiality
b. Integrity
c. Non-repudiation
d. Availability

Correct Answer: c

Detail Solution: Digital signatures provide three key security services:
Integrity: Ensures the message has not been altered.
Authentication: Confirms the sender's identity.
Non-repudiation: Prevents the sender from denying that they signed the message.

Non-repudiation specifically means → Once a signer digitally signs a message with their private key, they cannot later claim they did not sign it. The signature can be verified by anyone using the signer's public key, proving it was generated by the signer.

The correct option is (c).

QUESTION 9:

Which of the following is not an objective of SSL?

a. Authentication
b. Data Integrity
c. Data Privacy
d. Faster Transmission

Correct Answer: d

Detail Solution: Main objectives of SSL are:
Authentication → the client and server authenticate each other using certificates/keys.
Data Integrity → ensures data is not altered during transmission.
Data Privacy (Confidentiality) → Protects data using encryption so that only intended parties can read it.
Faster transmission is not an objective of SSL.
The correct option is (d).

QUESTION 10:

In IPSec, which mode encapsulates only the transport layer information with protection?

a. Tunnel Mode
b. Transport Mode
c. Replay Mode
d. Confidential Mode

Correct Answer: b

Detail Solution: IPSec provides two modes of protection:
Tunnel Mode → Encapsulates the entire IP packet (header + payload).
Transport Mode → Encapsulates only the transport layer information (payload), while leaving the original IP header intact.
Replay and Confidential are not a mode in IPSec's standard terminology.

The correct answer is (b)

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