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:

Consider a hash function H that generates hash values h1 and h2, when fed with messages m1 and m2 respectively. Which of the following options can **never be true**?

a. h1 and h2 are equal, but m1 and m2 are unequal.

b. m1 and m2 are equal, but h1 and h2 are unequal.

c. None of these.

Correct Answer: b

Detail Solution: A hash function maps a given message m to generate some particular hash value h. Two different messages m1 and m2 can, however, generate the same hash value, which is called collision. The same message always generates the same hash value. The correct option is (b).

QUESTION 2:

What is meant by collision in the context of hashing?

a. More than one different message can generate the same hash value.

b. After encryption, the ciphertexts corresponding to two or more plaintexts are the same.

c. The hash function generates the all zero string as the hash value.

d. None of these.

Correct Answer: a

Detail Solution: In a hash function, collision refers to the situation where more than one different message generate the same hash value. It has nothing to do with encryption. The correct option is (a).

QUESTION 3:

A message M is fed to a hash function HASH to generate the hash value H:

H = HASH (M)

Which of the following statements is **true**?

a. The number of bits in H is much larger than the number of bits in M.
b. The number of bits in H and M are almost equal.
c. The number of bits in M is much larger than the number of bits in H.
d. None of these.

Correct Answer: c

Detail Solution: A hash function maps a very large number to a relatively much smaller number. The correct option is (c).

QUESTION 4:

What of the following does not correspond to the first preimage resistance in the context of hash functions?

a. It is difficult to find a message M such that HASH(M) = H, except for a few hash values H.
b. Given a message M1, it is difficult to find another message M2 such that HASH(M1) = HASH(M2).
c. It is difficult to find two messages M1 and M2 such that HASH(M1) and HASH(M2) and unequal.
d. None of these.

Correct Answer: b, c

Detail Solution: This follows from the definition of the desirable properties of a hash function. First preimage resistance refers to the condition that we are given a hash value H, and are trying to find out some message M such that HASH(M) = H. This should be difficult to do. The correct options are (b) and (c).

QUESTION 5:

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

a. Hashing realizes a one-to-one mapping.

b. Encryption realizes a one-to-one mapping.
c. Hashing realizes a many-to-one mapping.
d. Encryption realizes a many-to-one mapping.

Correct Answer: b, c

Detail Solution: A hash function by definition realizes a many-to-one mapping, where more than one message can get mapped to the same hash function. In contrast, encryption realizes a one-to-one function, where a given plaintext maps to a unique ciphertext, and vice versa. The correct options are (b) and (c).

QUESTION 6:

Which of the following are hash functions?

a. MD5
b. Triple-DES
c. SHA-1
d. AES

Correct Answer: a, c

Detail Solution: MD5 and SHA-1 are examples of hash function, while Triple-DES and AES are examples of symmetric key encryption algorithm. The correct options are (a) and (c).

QUESTION 7:

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

a. Computing a hash function is faster than computing symmetric-key encryption.
b. Computing public-key encryption is slower than computing symmetric-key encryption.
c. Computing public-key encryption is slower than computing hash function.
d. Both public-key and symmetric-key encryption take approximately the same time.

Correct Answer: a, b, c

Detail Solution: Public-key encryption is the slowest, while hash function computation is the fastest. Hence, the correct options are (a), (b) and (c).

QUESTION 8:

What are the block size and key size of the DES algorithm?

a. 64 bits, 56 bits
b. 56 bits, 64 bits
c. 64 bits, 64 bits
d. 64 bits, 128 bits

Correct Answer: a

Detail Solution: In the DES algorithm, the block size is 64 bits and the key size is 56 bits. The correct option is (a).

QUESTION 9:

What kinds of algorithms are typically used in the computation of digital signature?

a. Cryptographic hash function.
b. Symmetric-key encryption.
c. Biometric authentication.
d. All of these

Correct Answer: a

Detail Solution: Digital signature is the electronic equivalent of pen-and-paper signature, and typically uses a combination of hashing and public-key cryptography. A hash function is first computed on the given message, and the hash value is encrypted using public-key cryptography, with the sender's private key. It does not reply on biometric authentication. The correct option is (a).

QUESTION 10:

The SSL record protocol is responsible for

a. High-speed data transmission
b. Data authentication
c. Non repudiation
d. None of these

Correct Answer: d

Detail Solution: The SSL Record protocol uses a combination of various cryptographic techniques to provide secure data transmission over a network. It ensures data encryption and also data integrity (using a hash function). However, it does not provide authentication service or non-repudiation guarantee. The correct option is (d).

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