NPTEL Online Certification Courses

Indian Institute of Technology Kharagpur

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:

Two messages M1 and M2 are fed to a hash function HASH to generate the hash values:

H1 = HASH (M1)

H2 = HASH (M2)

When do we say there is a collision?

a. H1 = H2.
b. M1 = M2.
c. H1 = HASH (H2).
d. None of these.

Correct Answer: a

Detail Solution: With respect to hashing, collision refers to the situation where more than one messages (here M1 and M2) map to the same hash value. The correct option is (a).

QUESTION 2:

What do you mean by first preimage resistance in the context of hash functions?

a. Except for few hash values H, it is difficult to find a message M such that HASH(M) = 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) = HASH(M2).
d. None of these.

Correct Answer: a

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 option is (a).

QUESTION 3:

What kind of mapping does a hash function implement?

a. One-to-one mapping.
b. Many-to-one mapping.
c. One-to-many mapping.
d. Many-to-many mapping.

Correct Answer: b

Detail Solution: A hash function is one that maps a larger-size message to a smaller-size hash value. Several different messages may map to the same hash value, but the converse is not true. The correct option is (b).

QUESTION 4:

Which of the following is/are not hash functions?

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

Correct Answer: b, d

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

QUESTION 5:

Which of the following algorithms are the slowest and the fastest?

Symmetric-key encryption, public-key encryption, hash function

a. Hash function, Symmetric-key encryption
b. Public-key encryption, Symmetric-key encryption
c. Symmetric-key encryption, Hash function

d. None of these.

Correct Answer: d

Detail Solution: Computation of hash function is the fastest, which computation of public-key encryption is the slowest. Symmetric-key encryption lies in between the two. Hence, the correct option is (d).

QUESTION 6:

What are the block size of DES algorithm and the hash digest size of MD5 algorithm?

a. 64 bits, 64 bits
b. 56 bits, 128 bits
c. 64 bits, 128 bits
d. 64 bits, 256 bits

Correct Answer: c

Detail Solution: In the DES algorithm, the block size is 64 bits and the key size is 56 bits. The hash digest size of the MD5 algorithm is 128 bits. The correct option is (c).

QUESTION 7:

On which cryptographic algorithm can the birthday attack be mounted?

a. Cryptographic hash function.
b. Symmetric-key cryptography.
c. Public-key cryptography.
d. Diffie-Hellman key exchange.
e. None of these.

Correct Answer: a

Detail Solution: Birthday attack utilizes some statistical properties to mount attacks on cryptographic hash functions. The correct option is (a).

QUESTION 8:

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

a. Cryptographic hash function.

b. Symmetric-key encryption.
c. Public-key encryption.
d. All of these

Correct Answer: a, c

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

QUESTION 9:

The SSL record protocol is responsible for

a. Data encryption
b. Data authentication
c. Non repudiation
d. All of these

Correct Answer: a

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 (a).

QUESTION 10:

Which of the following security protocols work above the IP layer in the TCP/IP protocol stack?

a. IPSec
b. TLS
c. SSL
d. HTTPS

Correct Answer: b, c, d

Detail Solution: The TLS, SSL and HTTPS protocols work above the IP layer, whereas IPSec protocol makes the IP layer secure. The correct options are (b), (c) and (d).

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