CRYPTOGRAPHIC HASH FUNCTIONS

TRUE OR FALSE

T F 1. Virtually all cryptographic hash functions involve the iterative use of a compression function.

T F 2. A good hash function has the property that the results of applying the function to a large set of inputs will produce outputs that are evenly distributed and apparently random.

T F 3. Hash functions can be used for intrusion and virus detections.

T F 4. The cryptographic hash function is not a versatile cryptographic algorithm.

T F 5. It is possible to use a hash function but no encryption for message authentication.

T F 6. Hash functions are commonly used to create a one-way password file.

T F 7. A weak hash function is sufficient to protect against an attack in which one party generates a message for another party to sign.

T F 8. The way to measure the resistance of a hash algorithm to cryptanalysis is to compare its strength to the effort required for a brute-force attack.

T F 9. Big-endian format is the most significant byte of a word in the low-address byte position.

T F 10. The SHA-512 algorithm has the property that every bit of the hash code is a function of every bit of the input.

MULTIPLE CHOICE

1. The principal object of a hash function is _____ .

   A. data integrity B. compression

C. collision resistance D. mapping messages

2. A _____ accepts a variable length block of data as input and produces a fixed size hash value h = H(M).

   A. hash resistance B. hash value

   C. hash function D. hash code

3. A _____ is an algorithm for which it is computationally infeasible to find either (a) a data object that maps to a pre-specified hash result or (b) two data objects that map to the same hash result.

   A. cryptographic hash function B. strong collision resistance

   C. one-way hash function D. compression function

4. The cryptographic hash function requirement that guarantees that it is impossible to find an alternative message with the same hash value as a given message and prevents forgery when an encrypted hash code is used is the _____ .

   A. collision resistant B. pseudorandomness

   C. pre-image resistant D. second pre-image resistant

5. _____ is a mechanism or service used to verify the integrity of a message.

   A. Message authentication B. Data compression

   C. Data mapping D. Message digest

6. Message authentication is achieved using a _____ .

   A. DES B. MDF

   C. SHA D. MAC

7. _____ are measures of the number of potential collisions for a given hash value.

A. MACs B. Primitives

C. Hash codes D. Preimages

8. A hash function that satisfies the properties of variable input size, fixed output size, efficiency, preimage resistant and second preimage resistant is referred to as a _____.

A. strong hash function B. collision resistant function

C. weak hash function D. preimage resistant function

9. The effort required for a collision resistant attack is explained by a mathematical result referred to as the _____ .

A. Whirlpool B. birthday paradox

C. hash value D. message authentication code

10. An ideal hash algorithm will require a cryptanalytic effort _____ the brute-force effort.

A. less than or equal to B. greater than or equal to

C. less than D. greater than

11. SHA-1 produces a hash value of _____ bits.

A. 224 B. 160

C. 384 D. 256

12. "Given a hash function H, with n possible outputs and a specific value H(x), if H is applied to k random inputs, what must be the value of k so that the probability that at least one input y satisfies H(y) = H(x) is 0.5?" is a reference to the _____ .

A. authentication code B. collision resistant

C. big endian D. birthday attack

13. Three new versions of SHA with hash value lengths of 256, 384, and 512 bits are collectively known as _____ .

    A. SHA-3 B. SHA-1

    C. SHA-2 D. SHA-0

SHORT ANSWER

1. The compression function used in secure hash algorithms falls into one of two categories: a function specifically designed for the hash function or an algorithm based on a _____ .

2. A _____ is an attack based on weaknesses in a particular cryptographic algorithm.

3. The _____ resistant guarantees that it is impossible to find an alternative message with the same hash value as a given message.

4. The kind of hash function needed for security applications is referred to as a _____ hash function.

5. The most important and widely used family of cryptographic hash functions is the _____ family.

6. When a hash function is used to provide message authentication, the hash function value is often referred to as a _____ .

7. Requirements for a cryptographic hash function include _____ which is the one-way property.

8. A hash function that satisfies the properties of variable input size, fixed output size, efficiency, preimage resistant, second preimage resistant and _____ is referred to as a strong hash function.

9. The two categories of attacks on hash functions are _____ attacks and cryptanalysis.

10. The evaluation criteria for SHA-3 are security, _____, and algorithm and implementation characteristics.

11. A message authentication code is also known as a _____ hash function.

12. The hash value of a message in the _____ application is encrypted with a user's private key.

Questions

1. What are some approaches to producing message authentication?
2. Compare message hashes and MACs