**Chapter 11:** **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. Limited characteristics make it impossible for hash functions to be

used to determine whether or not data has changed.

T F 4. Hash functions can be used for intrusion and virus detections.

T F 5. Whirlpool is a popular cryptographic hash function.

T F 6. The cryptographic hash function is not a versatile cryptographic

algorithm.

T F 7. It is possible to use a hash function but no encryption for message

authentication.

T F 8. Encryption hardware is optimized toward smaller data sizes.

T F 9. Hash functions are commonly used to create a one-way password

file.

T F 10. 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 11. 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 12. It can be shown that some form of birthday attack will succeed

against any hash scheme involving the use of cipher block

chaining without a secret key, provided that either the resulting

hash code is small enough or that a larger hash code can be

decomposed into independent subcodes.

T F 13. The most widely used hash function has been the Whirlpool.

T F 14. Big-endian format is the most significant byte of a word in the

low-address byte position.

T F 15. 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

1. 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

1. The Secure Hash Algorithm design closely models, and is based on, the hash function \_\_\_\_\_\_\_\_\_\_ .

A. MD5 B. FIPS 180

C. RFC 4634 D. MD4

1. 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

1. 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. preimage resistant D. second preimage resistant

1. \_\_\_\_\_\_\_\_\_\_ 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

1. Message authentication is achieved using a \_\_\_\_\_\_\_\_\_\_ .

A. DES B. MDF

C. SHA D. MAC

1. \_\_\_\_\_\_\_\_\_\_ are measures of the number of potential collisions for a given hash value.

A. MACs B. Primitives

C. Hash codes D. Preimages

1. 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

1. 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

1. 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

1. The Secure Hash Algorithm was developed by the \_\_\_\_\_\_\_\_\_\_\_ .

A. ITIL B. IEEE

C. ISO D. NIST

1. SHA-1 produces a hash value of \_\_\_\_\_\_\_\_\_\_ bits.

A. 224 B. 160

C. 384 D. 256

1. "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

1. 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 \_\_\_\_\_\_\_\_\_\_\_ symmetric block cipher.
2. A \_\_\_\_\_\_\_\_\_\_ cryptanalysis is an attack based on weaknesses in a particular cryptographic algorithm.
3. The \_\_\_\_\_\_\_\_\_\_ second preimage 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 \_\_\_\_\_\_\_\_\_\_ cryptographic hash function.
5. The most important and widely used family of cryptographic hash functions is the \_\_\_\_\_\_\_\_\_\_ SHA family.
6. When a hash function is used to provide message authentication, the hash function value is often referred to as a \_\_\_\_\_\_\_\_\_\_\_ message digest.
7. Requirements for a cryptographic hash function include \_\_\_\_\_\_\_\_\_\_\_ preimage resistant 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 \_\_\_\_\_\_\_\_\_\_ collision resistant is referred to as a strong hash function.
9. The two categories of attacks on hash functions are \_\_\_\_\_\_\_\_\_\_ brute-force attacks and cryptanalysis.
10. If collision resistance is required the value \_\_\_\_\_\_\_\_\_ 2*m*/2 determines the strength of the hash code against brute-force attacks.
11. The hash algorithm involves repeated use of a \_\_\_\_\_\_\_\_\_\_ compression function, f, that takes two inputs (an *n*-bit input and a *b*-bit block) and produces an *n*-bit output.
12. SHA-1 is very similiar in structure and in the basic mathematical operations used to \_\_\_\_\_\_\_\_\_\_ MD5 and SHA-0.
13. The evaluation criteria for SHA-3 are security, \_\_\_\_\_\_\_\_\_\_\_ cost, and algorithm and implementation characteristics.
14. A message authentication code is also known as a \_\_\_\_\_\_\_\_\_\_ keyed hash function.
15. The hash value of a message in the \_\_\_\_\_\_\_\_\_\_ digital signature application is encrypted with a user's private key.