**Chapter 12:** **Message Authentication Codes**

**TRUE OR FALSE**

T F 1. Message authentication is a mechanism or service used to verify

the integrity of a message.

T F 2. The order in which the frame check sequence and encryption

functions are performed is not critical for authentication.

T F 3. The MAC does not provide a digital signature because both sender

and receiver share the same key.

T F 4. A recipient in possession of the secret key cannot generate an

authentication code to verify the integrity of the message.

T F 5. One means of forming a MAC is to combine a cryptographic hash

function in some fashion with a secret key.

T F 6. A brute-force attack on a MAC is easier than a brute-force attack

on a hash function.

T F 7. Message authentication may also verify sequencing and timeliness.

T F 8. The security of any MAC function based on an embedded hash

function depends in some way on the cryptographic strength of

the underlying hash function.

T F 9. Message encryption by itself cannot provide a measure of

authentication.

T F 10. If the calculated frame check sequence is equal to the incoming

frame check sequence the message is considered authentic.

T F 11. The straightforward use of public-key encryption provides

confidentiality and authentication.

T F 12. A CTR-based authenticated encryption approach is the most

efficient mode of operation for high-speed packet networks.

T F 13. An important characteristic of the MAC algorithm is that it needs

to be reversible.

T F 14. As with encryption algorithms and hash functions cryptanalytic

attacks on MAC algorithms seek to exploit some property of the

algorithm to perform some attack other than an exhaustive

search.

T F 15. To attack MD5, the attacker can choose any set of messages and

work on these offline on a dedicated computing facility to find a

collision.

**MULTIPLE CHOICE**

1. \_\_\_\_\_\_\_\_\_ encryption provides authentication among those who share the secret key.

A. Message B. Asymmetric

C. Symmetric D. Authenticated

1. The \_\_\_\_\_\_\_\_\_\_ mode of operation is designed to be parallelizable so that it can provide high throughput with low cost and low latency.

A. DAA B. CCM

C. GCM D. CTR

1. Insertion of messages into the network from a fraudulent source is a \_\_\_\_\_\_\_\_\_\_ attack.

A. content modification B. masquerade

C. source repudiation D. sequence modification

1. Confidentiality can be provided by performing message encryption \_\_\_\_\_\_\_\_\_\_ the MAC algorithm.

A. before B. before or after

C. after D. during

1. A \_\_\_\_\_\_\_\_\_\_ is an algorithm that requires the use of a secret key.

A. DAA B. SHA

C. GCM D. MAC

1. "Release of message contents to any person or process not possessing the appropriate cryptographic key" is a \_\_\_\_\_\_\_\_\_\_ attack.

A. content modification B. source repudiation

C. disclosure D. sequence modification

1. With \_\_\_\_\_\_\_\_\_ authentication an opponent would have difficulty generating ciphertext that when decrypted would have valid error control bits.

A. checksum B. CMAC

C. cipher block chaining D. internal error control

1. The MAC function is a \_\_\_\_\_\_\_\_\_\_ function.

A. one-to-many B. many-to-one

C. one-to-one D. one-to-two

1. The appeal of \_\_\_\_\_\_\_\_\_\_ is that its designers have been able to prove an exact relationship between the strength of the embedded hash function and the strength of this form of authentication.

A. MAC B. HMAC

C. GMAC D. CMAC

1. The \_\_\_\_\_\_\_\_\_ attack is when the attacker is looking for two messages *M* and *M1* that produce the same hash: H(*M*) = H(*M1*)

A. birthday B. chaining

C. MAC D. hash

1. Two MACs that are based on the use of a block cipher mode of operation are Data Authentication Algorithm and \_\_\_\_\_\_\_\_\_\_ .

A. GMAC B. DMAC

C. TMAC D. CMAC

1. The key algorithmic ingredients of \_\_\_\_\_\_\_\_\_ are the AES encryption algorithm, the CTR mode of operation, and the CMAC authentication algorithm.

A. DAA B. GCM

C. CCM D. CMA

1. The GCM mode makes use of two functions: \_\_\_\_\_\_\_\_\_\_, which is a keyed hash function, and GCTR.

A. CTR B. HMAC

C. GHASH D. CCM

1. The essential elements of any pseudorandom number generator are a \_\_\_\_\_\_\_\_\_\_ and a deterministic algorithm for generating a stream of pseudorandom bits.

A. secret key B. session key

C. seed value D. stream encryption function

1. The approach taken by the Transport Layer Security protocol and the Wireless Transport Layer Security Protocol involve invoking HMAC \_\_\_\_\_\_\_\_\_ for each block of output *wi*.

A. zero times B. twice

C. three times D. once

**SHORT ANSWER**

1. \_\_\_\_\_\_\_\_\_\_ message authentication assures that data received are exactly as sent and that the purposed identity of the sender is valid.
2. Discovery of the pattern of traffic between parties is a \_\_\_\_\_\_\_\_\_\_ traffic analysis attack.
3. A \_\_\_\_\_\_\_\_\_\_ message authentication code (MAC) takes a variable length message and a secret key as input and produces an authentication code.
4. One approach to constructing a MAC is to use a symmetric block cipher in such a way that it produces a \_\_\_\_\_\_\_\_\_\_ fixed length output for a variable length input.
5. Any modification to a sequence of messages between parties, including insertion, deletion, and reordering is a \_\_\_\_\_\_\_\_\_\_ sequence modification attack.
6. The types of functions that may be used to produce an authenticator are grouped into three classes: hash function, message authentication code, and message encryption \_\_\_\_\_\_\_\_\_\_\_ .
7. An alternative authentication technique involves the use of a secret key to generate a small fixed size block of data known as a \_\_\_\_\_\_\_\_\_\_cryp chechsum or MAC that is appended to the message.
8. When an entire message is encrypted for confidentiality using either symmetric or asymmetric encryption the security of the scheme generally depends on the \_\_\_\_\_\_\_\_\_\_ bit length of the key.
9. Attacks on MACs can be grouped into two categories: brute-force attacks and cryptoanalysis\_\_\_\_\_\_\_\_\_\_ .
10. The \_\_\_\_\_\_\_\_\_\_ DATA AUTHUNTICATION algorithm can be defined as using the cipher block chaining mode of operation of DES with an initialization vector of zero.
11. \_\_\_\_\_\_\_\_\_\_\_ Authunticated Encryption (EA) is a term used to describe encryption systems that simultaneously protect confidentiality and authenticity of communications.
12. The HtE approach is used in the \_\_\_\_\_\_\_\_\_\_ Wired Equiavalent privacy protocol to protect WiFi networks.
13. The \_\_\_\_\_\_\_\_\_\_CCM mode of operation was standardized by NIST specifically to support the security requirements of IEEE 802.1 WiFi wireless local area networks but can be used in any networking application requiring authenticated encryption.
14. NIST SP 800-90, IEEE 802.11i, and TLS/WTLS are three \_\_\_\_\_\_\_\_\_\_\_\_PRNGs based on HMAC.
15. HMAC is a widely used standardized \_\_\_\_\_\_\_\_\_MAC function and is implemented in many protocols and applications.