**Chapter 22 – Internet Security Protocols and Standards**

**TRUE/FALSE QUESTIONS:**

T F 1. MIME is an extension to the old RFC 822 specification of an Internet

mail format.

T F 2. MIME provides the ability to sign and/or encrypt e-mail messages.

T F 3. Recipients without S/MIME capability can view the message content,

although they cannot verify the signature.

T F 4. The recipient of a message can decrypt the signature using DSS and the

sender’s public DSS key.

T F 5. As an alternative the RSA public-key encryption algorithm can be used

with either the SHA-1 or the MD5 message digest algorithm for forming signatures.

T F 6. In S/MIME each conventional key is used a total of three times.

T F 7. DKIM has been widely adopted by a range of e-mail providers and

many Internet service providers.

T F 8. SMTP is used between the message user agent and the mail submission

agent.

T F 9. A message store cannot be located on the same machine as the MUA.

T F 10. An ADMD is an Internet e-mail provider.

T F 11. DKIM is designed to provide an e-mail authentication technique that

is transparent to the end user.

T F 12. Most browsers come equipped with SSL and most Web servers have

implemented the protocol.

T F 13. Search engines support HTTPS.

T F 14. The IAB included authentication and encryption as necessary security

features in IPv6.

T F 15. Transport mode provides protection primarily for lower-layer

protocols.

**MULTIPLE CHOICE QUESTIONS:**

1. \_\_\_\_\_ defines a number of content formats, which standardize representations for the support of multimedia e-mail.

A. MEM B. MIME

C. MSC D. DKIM

2. The \_\_\_\_\_\_\_\_ function consists of encrypted content of any type and encrypted-content encryption keys for one or more recipients.

A. clear-signed data B. signed data

C. enveloped data D. signed and enveloped data

3. In the case of \_\_\_\_\_\_\_\_ only the digital signature is encoded using base64.

A. enveloped data B. signed and enveloped data

C. signed data D. clear-signed data

4. The result of S/MIME encrypting the digest using DSS and the sender’s private DSS key is the \_\_\_\_\_\_\_\_.

A. digital signature B. envelope

C. digest code D. mail extension

5. To protect the data, either the signature alone or the signature plus the message are mapped into printable ASCII characters using a scheme known as \_\_\_\_\_\_\_\_ or base64mapping.

A. radix-64 B. ASCII-64

C. ESP-64 D. safe mapping

6. The basic tool that permits widespread use of S/MIME is \_\_\_\_\_\_\_\_.

A. the domain key B. the public-key certificate

C. the MIME security payload D. radix-64

7. At its most fundamental level the Internet mail architecture consists of a user world in the form of \_\_\_\_\_\_\_\_\_.

A. MHS B. MSA

C. MUA D. MDA

8. The \_\_\_\_\_\_ is responsible for transferring the message from the MHS to the MS.

A. MDA B. MS

C. MUA D. MSA

9. The \_\_\_\_\_\_\_\_ accepts the message submitted by a message user agent and enforces the policies of the hosting domain and the requirements of Internet standards.

A. mail submission agent B. message user agent

C. mail delivery agent D. message transfer agent

10. The most complex part of TLS is the \_\_\_\_\_\_\_\_\_\_.

A. signature B. message header

C. payload D. handshake protocol

11. \_\_\_\_\_\_\_ is a list that contains the combinations of cryptographic algorithms supported by the client.

A. Compression method B. Session ID

C. CipherSuite D. All of the above

12. ESP supports two modes of use: transport and \_\_\_\_\_\_\_\_\_.

A. padding B. tunnel

C. payload D. sequence

13. IPsec can assure that \_\_\_\_\_\_\_\_\_.

A. a router advertisement comes from an authorized router

B. a routing update is not forged

C. a redirect message comes from the router to which the initial packet was sent

D. all of the above

14. A benefit of IPsec is \_\_\_\_\_\_\_\_\_\_.

A. that it is below the transport layer and transparent to applications

B. there is no need to revoke keying material when users leave the organization

C. it can provide security for individual users if needed

D. all of the above

15. The \_\_\_\_\_\_\_ field in the outer IP header indicates whether the association is an AH or ESP security association.

A. protocol identifier B. security parameter index

C. IP destination address D. sequence path counter

**SHORT ANSWER QUESTIONS:**

1. \_\_\_\_\_\_\_\_ is a security enhancement to the MIME Internet e-mail format standard, based on technology from RSA Data Security.
2. S/MIME content-types support four new functions: enveloped data, \_\_\_\_\_\_\_\_\_\_, clear-signed data, and signed and enveloped data.
3. A \_\_\_\_\_\_\_\_\_ is formed by taking the message digest of the content to be signed and then encrypting that with the private key of the signer.
4. A signed data message can only be viewed by a recipient with \_\_\_\_\_\_\_\_\_\_ capability.
5. The default algorithms used for signing S/MIME messages are SHA-1 and the \_\_\_\_\_\_\_\_\_.
6. The default algorithms used for encrypting S/MIME messages are the triple DES and a public-key scheme known as \_\_\_\_\_\_\_.
7. If encryption is used alone, \_\_\_\_\_\_\_ is used to convert the ciphertext to ASCII format.
8. \_\_\_\_\_\_\_\_\_ is a specification for cryptographically signing e-mail messages, permitting a signing domain to claim responsibility for a message in the mail stream.
9. The \_\_\_\_\_\_\_\_ is housed in the user’s computer and is referred to as a client e-mail program or a local network e-mail server.
10. The \_\_\_\_\_\_\_ is a directory lookup service that provides a mapping between the name of a host on the Internet and its numerical address.
11. The SSL record protocol provides two services for SSL connection: message integrity and \_\_\_\_\_\_\_\_\_.
12. The \_\_\_\_\_\_\_\_\_ is used to convey SSL-related alerts to the peer entity.
13. A security association is uniquely identified by three parameters: security parameter index, protocol identifier, and \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_.
14. IP-level security encompasses three functional areas: authentication, confidentiality, and \_\_\_\_\_\_\_\_\_.
15. IPsec provides two main functions: a combined authentication/encryption function called \_\_\_\_\_\_\_\_\_\_\_ and a key exchange function.