**Chapter 19:** **Electronic Mail Security**

**TRUE OR FALSE**

T F 1. PGP incorporates tools for developing public-key certificate

management and a public-key trust model.

T F 2. PGP provides confidentiality through the use of asymmetric block

encryption.

T F 3. E-mail is the most common distributed application that is widely

used across all architectures and vendor platforms.

T F 4. As a default, PGP compresses the message after applying the

signature but before encryption.

T F 5. Each PGP entity must maintain a file of its own public/private key

pairs as well as a file of private keys of correspondents.

T F 6. A means of generating predictable PGP session keys is needed.

T F 7. To enhance security an encrypted message is not accompanied by

an encrypted form of the session key that was used for message

encryption.

T F 8. A message component includes the actual data to be stored or

transmitted as well as a filename and a timestamp that specifies

the time of creation.

T F 9. PGP has a very rigid public-key management scheme.

T F 10. The key legitimacy field is derived from the collection of signature

trust fields in the entry.

T F 11. Only single user IDs may be associated with a single public key on

the public-key ring.

T F 12. The MIME-Version field must have the parameter value 1.0 in

order for the message to conform to RFCs 2045 and 2046.

T F 13. For the text type of body no special software is required to get the

full meaning of the text aside from support of the indicated

character set.

T F 14. The objective of MIME Transfer Encodings is to provide reliable

delivery across the largest range of environments.

T F 15. Native form is a format, appropriate to the content type, that is

standardized for use between systems.

**MULTIPLE CHOICE**

1. \_\_\_\_\_\_\_\_\_\_ is an Internet standard approach to e-mail security that incorporates the same functionality as PGP.

A. S/MIME B. MIME

C. DKIM D. HTTPS

1. PGP provides authentication through the use of \_\_\_\_\_\_\_\_\_ .

A. asymmetric block encryption B. symmetric block encryption

C. radix-64 D. digital signatures

1. PGP provides e-mail compatibility using the \_\_\_\_\_\_\_\_\_\_ encoding scheme.

A. radix-64 B. MIME

C. digital signature D. symmetric block

1. The \_\_\_\_\_\_\_\_\_\_ enables the recipient to determine if the correct public key was used to decrypt the message digest for authentication.

A. key ID of the sender's public key

B. timestamp

C. filename

D. leading two octets of message digest

1. Key IDs are critical to the operation of PGP and \_\_\_\_\_\_\_\_\_\_ key IDs are included in any PGP message that provides both confidentiality and authentication.

A. two B. four

C. six D. three

1. MIME is an extension to the \_\_\_\_\_\_\_\_ framework that is intended to address some of the problems and limitations of the use of SMTP.

A. RFC 821 B. RFC 5322

C. RFC 3852 D. RFC 4871

1. The \_\_\_\_\_\_\_\_ MIME field is a text description of the object with the body which is useful when the object is not readable as in the case of audio data.

A. Content-Type B. Content-Description

C. Content-ID D. Content-Transfer-Encoding

1. The \_\_\_\_\_\_\_\_\_\_ field is used to identify MIME entities uniquely in multiple contexts.

A. Content-Transfer- Encoding B. Content-ID

C. Content-Description D. Content-Type

1. Video content will be identified as \_\_\_\_\_\_\_\_\_ type.

A. GIF B. MPEG

C. BMP D. JPEG

1. The \_\_\_\_\_\_\_\_\_\_ subtype is used when the different parts are independent but are to be transmitted together. They should be presented to the receiver in the order that they appear in the mail message.

A. multipart/digest B. multipart/parallel

C. multipart/mixed D. multipart/alternative

1. For the \_\_\_\_\_\_\_\_\_\_ subtype the order of the parts is not significant.

A. multipart/mixed B. multipart/digest

C. multipart/alternative D. multipart/parallel

1. S/MIME cryptographic algorithms use \_\_\_\_\_\_\_\_\_\_ to specify requirement level.

A. CAN and MUST B. SHOULD and CAN

C. SHOULD and MIGHT D. SHOULD and MUST

1. E-banking, personal banking, e-commerce server, software validation and membership-based online services all fall into the VeriSign Digital ID \_\_\_\_\_\_\_\_\_ .

A. Class 4 B. Class 3

C. Class 1 D. Class 2

1. 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. Message Store B. Mail Submission Agent

C. Message Transfer Agent D. Mail Delivery Agent

1. Typically housed in the user's computer, a \_\_\_\_\_\_\_\_\_ is referred to as a client e-mail program or a local network e-mail server.

A. Mail Submission Agent B. Message Transfer Agent

C. Message Store D. Message User Agent

**SHORT ANSWER**

1. \_\_\_\_\_\_\_\_\_\_\_ is an open-source, freely available software package for e-mail security.
2. The key legitimacy field, the signature trust field and the owner trust field are each contained in a structure referred to as a \_\_\_\_\_\_\_\_\_\_\_ .
3. PGP provides compression using the \_\_\_\_\_\_\_\_\_\_ algorithm.
4. To provide transparency for e-mail applications, an encrypted message may be converted to an ASCII string using \_\_\_\_\_\_\_\_\_ conversion.
5. PGP makes use of four types of keys: public keys, private keys, one-time session keys, and \_\_\_\_\_\_\_\_\_\_\_ symmetric keys.
6. Computed by PGP, a \_\_\_\_\_\_\_\_\_ field indicates the extent to which PGP will trust that this is a valid public key for this user; the higher the level of trust, the stronger the binding of this user ID to this key.
7. \_\_\_\_\_\_\_\_\_\_ is a security enhancement to the MIME Internet e-mail format standard based on technology from RSA Data Security.
8. The \_\_\_\_\_\_\_\_\_\_ MIME field describes the data contained in the body with sufficient detail that the receiving user agent can pick an appropriate agent or mechanism to represent the data to the user or otherwise deal with the data in an appropriate manner.
9. The \_\_\_\_\_\_\_\_\_ type refers to other kinds of data, typically either uninterpreted binary data or information to be processed by a mail-based application.
10. The \_\_\_\_\_\_\_\_\_ transfer encoding is useful when the data consists largely of octets that correspond to printable ASCII characters.
11. The \_\_\_\_\_\_\_\_\_ transfer encoding, also known as radix-64 encoding, is a common one for encoding arbitrary binary data in such a way as to be invulnerable to the processing by mail-transport programs.
12. 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, which is then encoded using base64 encoding.
13. S/MIME provides the following functions: enveloped data, signed data, clear signed data, and \_\_\_\_\_\_\_\_ .
14. A specification for cryptographically signing e-mail messages permitting a signing domain to claim responsibility for a message in the mail stream, \_\_\_\_\_\_\_\_\_ allow message recipients to verify the signature by querying the signer's domain directly to retrieve the appropriate public key and thereby confirming that the message was attested to by a party in possession of the private key for the signing domain.
15. The \_\_\_\_\_\_\_\_\_\_ is a directory lookup service that provides a mapping between the name of a host on the Internet and its numerical address.