**Chapter 14:** **Key Management and Distribution**

**TRUE OR FALSE**

T F 1. Some sort of mechanism or protocol is needed to provide for the

secure distribution of keys.

T F 2. A public-key certificate scheme alone does not provide the

necessary security to authenticate the public key.

T F 3. For symmetric encryption to work the two parties to an exchange

must share the same key and that key must be protected from

access by others.

T F 4. X.509 defines the format for private-key certificates.

T F 5. The topics of cryptographic key management and cryptographic

key distribution are complex, involving cryptographic, protocol,

and management considerations.

T F 6. Frequent key changes are usually desirable to limit the amount of

data compromised if an attacker learns the key.

T F 7. For link encryption manual delivery is awkward.

T F 8. Each user must share a unique key with the key distribution center

for purposes of key distribution.

T F 9. Typically the session key is used for the duration of a logical

connection, such as a frame relay connection or transport

connection, and then it is permanently stored.

T F 10. Master keys can be distributed in some noncryptographic way

such as physical delivery.

T F 11. A random number would not be a good choice for a nonce.

T F 12. The distribution of session keys delays the start of any exchange

and places a burden on network capacity.

T F 13. Although public announcement of public keys is convenient,

anyone can forge a public announcement.

T F 14. X.509 is an important standard because the certificate structure

and authentication protocols defined in X.509 are used in a

variety of contexts.

T F 15. Because certificates are forgeable they cannot be placed in a

directory without the need for the directory to make special

efforts to protect them.

**MULTIPLE CHOICE**

1. Key distribution often involves the use of \_\_\_\_\_\_\_\_\_\_ which are infrequently used and are long lasting.

A. private key certificates B. master keys

C. session keys D. public key certificates

1. \_\_\_\_\_\_\_\_\_\_ key encryption schemes are secure if the public key is authenticated.

A. Message B. Management

C. Public D. Private

1. A \_\_\_\_\_\_\_\_\_\_ defines the procedures needed to revoke digital certificates.

A. KDC B. digital key

C. cryptographic key encryption D. public key infrastructure

1. \_\_\_\_\_\_\_\_\_ implementations make use of X.509 certificates.

A. PKI B. CDC

C. HMAC D. KDC

1. Key distribution often involves the use of \_\_\_\_\_\_\_\_\_ which are generated and distributed for temporary use between two parties.

A. public key certificates B. session keys

C. master keys D. private key certificates

1. The strength of any cryptographic system rests with the \_\_\_\_\_\_\_\_\_\_\_ .

A. end encryption B. key distribution technique

C. nonce D. X.509 certificate

1. If \_\_\_\_\_\_\_\_\_\_ is done at a network or IP level a key is needed for each pair of hosts on the network that wish to communicate.

A. end-to-end encryption B. key management

C. key distribution D. link encryption

1. Communication between end systems is encrypted using a \_\_\_\_\_\_\_\_\_ key.

A. session B. master

C. permanent D. message

1. The more frequently session keys are exchanged the more \_\_\_\_\_\_\_\_\_\_ they are because the opponent has less ciphertext to work with for any given session key.

A. insecure B. streamlined

C. secure D. obsolete

1. One of the most important uses of a \_\_\_\_\_\_\_\_\_\_ cryptosystem is to encrypt secret keys for distribution.

A. master key B. KDC

C. public key D. end-to-end

1. With the \_\_\_\_\_\_\_\_\_\_ scheme, if an adversary succeeds in obtaining or computing the private key of the directory authority, the adversary could authoritatively pass out counterfeit public keys and subsequently impersonate any participant and eavesdrop on messages sent to any participant.

A. public key authority B. publicly available directory

C. public key certificates D. public announcement

1. The principal objective for developing a \_\_\_\_\_\_\_\_\_ is to enable secure, convenient and efficient acquisition of public keys.

A. KDC B. IETF

C. PKI D. CRL

1. \_\_\_\_\_\_\_\_\_\_ is an integer value unique within the issuing CA that is unambiguously associated with this certificate.

A. Signature identifier B. Version

C. Serial number D. Issuer unique identifier

1. \_\_\_\_\_\_\_\_\_\_ indicates a restriction imposed as to the purposes for which, and the policies under which, the certified public key may be used.

A. Authority key identifier B. Key usage

C. Subject key identifier D. Certificate policies

1. The \_\_\_\_\_\_\_\_\_\_ is the issuer of certificates and certificate revocation lists and may also support a variety of administrative functions.

A. CRL issuer B. certified user

C. certification authority D. registration authority

**SHORT ANSWER**

1. \_\_\_\_\_\_\_\_\_\_ is the function that delivers a key to two parties who wish to exchange secure encrypted data.
2. A \_\_\_\_\_\_\_\_\_ is defined as the set of hardware, software, people, policies, and procedures needed to create, manage, store, distribute, and revoke digital certificates based on asymmetric cryptography.
3. Used in a variety of applications, \_\_\_\_\_\_\_\_\_\_ defines the format for public-key certificates.
4. Public-key encryption schemes are secure only if the authenticity of the \_\_\_\_\_\_\_\_\_\_\_ is assured.
5. If encryption is done at the \_\_\_\_\_\_\_\_\_\_ level a key is needed for every pair of users or processes that require communication.
6. If A and B each has an encrypted connection to a third party C, C can deliver a key on the encrypted links to A and B. A \_\_\_\_\_\_\_\_\_ center is responsible for distributing keys to pairs of users as needed.
7. Session keys are transmitted in encrypted form using a \_\_\_\_\_\_\_\_\_\_ key that is shared by the key distribution center and an end system or user.
8. A unique identifier for a transaction is a \_\_\_\_\_\_\_\_\_\_ and this identifier may be a timestamp, a counter or a random number, with the minimum requirement being that it differs with each request.
9. A \_\_\_\_\_\_\_\_\_\_ attack is when a protocol is insecure against an adversary who can intercept messages and can either relay the intercepted message or substitute another message.
10. Several techniques have been proposed for the distribution of public keys. The proposals can be grouped into the following four general schemes: public announcement, publicly available directory, public-key certificates, and \_\_\_\_\_\_\_\_\_\_\_\_.
11. A \_\_\_\_\_\_\_\_\_\_ consists of a public key, an identifier of the key owner, and the whole block signed by a trusted third party and can be used by participants to exchange keys without contacting a public key authority in a way that is as reliable as if the keys were obtained directly from a public key authority.
12. \_\_\_\_\_\_\_\_\_\_ certificates are used in most network security applications including IP security, transport layer security and S/MIME.
13. The directory entry for each certification authority includes two types of certificates: forward certificates and \_\_\_\_\_\_\_\_\_\_\_ .
14. \_\_\_\_\_\_\_\_\_\_ is the process whereby a user first makes itself known to a certification authority prior to that certification authority issuing a certificate for that user.
15. A \_\_\_\_\_\_\_\_\_ is a generic term used to denote any method for storing certificates and CRLs so that they can be retrieved by end entities.