DIGITAL SIGNATURES & KEY DISTRIBUTION

TRUE OR FALSE

T F 1. A digital signature can guarantee the integrity but not the source of the message.

T F 2. It must be computationally infeasible to forge a digital signature, either by constructing a new message for an existing digital signature or by constructing a fraudulent digital signature for a given message.

T F 3. The most important development from the work on public-key cryptography is the digital signature.

T F 4. Message authentication protects two parties who exchange messages from any third party, however, it does not protect the two parties against each other.

T F 5. The digital signature function does not include the authentication function.

T F 6. Unlike RSA, the DSA cannot be used for encryption or key exchange.

T F 7. Some sort of mechanism or protocol is needed to provide for the secure distribution of keys.

T F 8. A public-key certificate scheme alone does not provide the necessary security to authenticate the public key.

T F 9. 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 10. The topics of cryptographic key management and cryptographic key distribution are complex, involving cryptographic, protocol, and management considerations.

T F 11. Frequent key changes are usually desirable to limit the amount of data compromised if an attacker learns the key.

T F 12. Each user must share a unique key with the key distribution center for purposes of key distribution.

T F 13. 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 14. Master keys can be distributed in some non-cryptographic way such as physical delivery.

MULTIPLE CHOICE

1. The _____ is formed by taking the hash of the message and encrypting the message with the creator's private key.

   A. timestamp B. message digest

   C. hash code D. digital signature

2. _____ is where the attacker forges a signature for a particular message chosen by the attacker.

   A. Total break B. Universal forgery

   C. Existential forgery D. Selective forgery

3. The digital signature standard is a _____ standard that uses the secure hash algorithm.

   A. IEEE B. NIST

   C. ISO D. ITIL

4. With a _____ attack the attacker is given access to a set of messages and their signatures.

   A. known message B. key-only

   C. directed chosen message D. generic chosen message

5. A _____ is where the attacker determines the user's private key.

   A. universal forgery B. selective forgery

   C. existential forgery D. total break

6. 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

7. _____ key encryption schemes are secure if the public key is authenticated.

   A. Message B. Management

   C. Public D. Private

8. A _____ defines the procedures needed to revoke digital certificates.

   A. KDC B. digital key

   C. cryptographic key encryption D. public key infrastructure

9. 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

10. 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

11. Communication between end systems is encrypted using a _____ key.

    A. session B. master

    C. permanent D. message

12. 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

13. 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

SHORT ANSWER

1. The attacker finds an efficient signing algorithm that provides an equivalent way of constructing signatures on arbitrary messages is a _____ .

2. A digital signature must have the following properties: it must verify the author and the date and time of the signature; it must authenticate the contents at the time of the signature; and it must _____ to resolve disputes.

3. The DSS makes use of the Secure Hash Algorithm and presents a new digital signature technique known as the _____ .

4. The _____ attack is where the attacker chooses a list of messages before attempting to break the user's signature scheme, independent of the user's public key. The attacker then obtains from the user valid signatures for the chosen messages.

5. The term _____ refers to a digital signature scheme that involves only the

communicating parties.

6. _____ is the function that delivers a key to two parties who wish to exchange secure encrypted data.

7. 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.

8. Used in a variety of applications, _____ defines the format for public-key certificates.

9. Public-key encryption schemes are secure only if the authenticity of the _____ is assured.

10. If encryption is done at the _____ level a key is needed for every pair of users or processes that require communication.

11. 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 _____ is responsible for distributing keys to pairs of users as needed.

12. Session keys are transmitted in encrypted form using a _____ that is shared by the key distribution center and an end system or user.