**Chapter 13: digital signatures**

**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 global public key components for DSA are *p, q,* and *h.*

T F 4. The most important development from the work on public-key

cryptography is the digital signature.

T F 5. The ElGamal signature scheme involves the use of the public key

for encryption and the private key for decryption.

T F 6. It is important in a direct digital signature to perform an outer

confidentiality function first and then the signature function.

**T** F 7. 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 8. The digital signature function does not include the authentication

function.

T F 9. The DSS approach makes use of a hash function.

T F 10. It must be relatively difficult to recognize and verify the digital

signature.

T F 11. The Schnorr signature scheme is based on discrete logarithms.

T F 12. The main work for signature generation depends on the message

and is done during the idle time of the processor.

T F 13. Unlike RSA, DSS cannot be used for encryption or key exchange.

T F 14. The global public key components of DSA are the same as for the

Schnorr signature scheme.

T F 15. The first part of the Schnorr digital signature scheme is the

generation of a private/public key pair.

**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

1. \_\_\_\_\_\_\_\_\_\_ 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

1. The digital signature standard is a \_\_\_\_\_\_\_\_\_\_ standard that uses the secure hash algorithm.

A. IEEE B. NIST

C. ISO D. ITIL

1. 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

1. Similar to the generic attack, except that the list of messages to be signed is chosen after the attacker knows the user's public key but before any signatures are seen, is the \_\_\_\_\_\_\_\_\_\_ attack.

A. directed chosen B. key-only

C. adaptive chosen D. known message

1. A \_\_\_\_\_\_\_\_\_\_ is where the attacker determines the user's private key.

A. universal forgery B. selective forgery

C. existential forgery D. total break

1. As with ElGamal encryption, the global elements of \_\_\_\_\_\_\_\_\_\_ are a prime number *q* and *a*, which is a primitive root of *q*.

A. ElGamal digital signature B. digital signature standard

C. digital signature D. direct digital signature

1. The \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_, which is the latest of the RSA schemes, is the one that RSA Laboratories recommends as the most secure of the RSA schemes.

A. RSA-PSS B. ECDSA

C. DSA-SDS D. EDSDS

1. The digital signature approach uses an algorithm that is designed to provide only the \_\_\_\_\_\_\_\_\_ function.

A. digital signature B. ElGamal

C. DSA D. timestamp

1. In the \_\_\_\_\_\_\_\_\_\_ approach only the sender knows the private key so only the sender could have produced a valid signature.

A. EDS B. DSA

C. DSS D. RSA

1. The \_\_\_\_\_\_\_\_\_\_\_\_ components of DSA are the same as in the Schnorr

signature scheme.

A. private key B. EDS

C. global public key D. message digest

1. To create a \_\_\_\_\_\_\_\_\_\_ a user calculates two quantities, r and s, that are functions of the public key components (p, q, g), the user's private key (x), the hash code of the message H(M), and an additional integer k that should be generated randomly or pseudorandomly and be unique for each signing.

A. signature B. hash authentication

C. secret key D. global key

1. The \_\_\_\_\_\_\_\_\_\_ scheme minimizes the message dependent amount of computation required to generate a signature.

A. Rabin B. SHA-1

C. ElGamal D. Schnorr

1. With a \_\_\_\_\_\_\_\_\_\_ attack the attacker is allowed to use the user as an "oracle". This means that the user may request signatures of messages that depend on previously obtained message-signature pairs.

A. adaptive chosen message B. generic chosen

C. directed chosen message D. known message

1. In the digital signature algorithm the user's \_\_\_\_\_\_\_\_\_\_ is represented by x, which is a random or pseudorandom integer with 0 < x < q.

A. per message secret number B. private key

C. global key D. public key

**SHORT ANSWER**

1. A \_\_\_\_\_\_\_\_\_ is an authentication mechanism that enables the creator of a message to attach a code that acts as a signature.
2. The first stage in generating an RSA-PSS signature of a message

*M* is to generate from *M* a fixed-length message digest, called an \_\_\_\_\_\_\_\_\_\_\_\_\_\_.

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. \_\_\_\_\_\_\_\_\_ specifies that if the signature generation process results in a value of *s* = 0 a new value of *k* should be generated and the signature should be recalculated.
6. The term \_\_\_\_\_\_\_\_\_\_ refers to a digital signature scheme that involves only the communicating parties.
7. The \_\_\_\_\_\_\_\_\_\_ encryption scheme is designed to enable encryption by a user's public key with decryption by the user's private key.
8. The \_\_\_\_\_\_\_\_\_\_ scheme minimizes the message dependent amount of computation required to generate a signature.
9. The message dependent part of the Schnorr digital signature generation requires multiplying a \_\_\_\_\_\_\_\_\_\_ with an *n*-bit integer.
10. In addition to the NIST Digital Signature Algorithm and ECDSA, the 2009 version of FIPS 186 also includes several techniques based on \_\_\_\_\_\_\_\_\_ , all of which were developed by RSA Laboratories and are in wide use.
11. The \_\_\_\_\_\_\_\_\_ is based on the difficulty of computing discrete logarithms and is based on schemes originally presented by ElGamal and Schnorr.
12. FIPS 186 -3 incorporates digital signature algorithms based on RSA and on \_\_\_\_\_\_\_\_\_\_ cryptography.
13. Administrative controls relating to the security of private keys can be employed by including a \_\_\_\_\_\_\_\_\_\_ (which includes date and time) and to require prompt reporting of compromised keys to a central authority.