**Chapter 21 – Public-Key Cryptography and Message Authentication**

**TRUE/FALSE QUESTIONS:**

T F 1. The one-way hash function is important not only in message

authentication but also in digital signatures.

T F 2. SHA is perhaps the most widely used family of hash functions.

T F 3. SHA-1 is considered to be very secure.

T F 4. SHA-2 shares the same structure and mathematical operations as its

predecessors and this is a cause for concern.

T F 5. HMAC can be proven secure provided that the embedded hash function

has some reasonable cryptographic strengths.

T F 6. The appeal of HMAC is that its designers have been able to prove an

exact relationship between the strength of the embedded hash function and the strength of HMAC.

T F 7. RSA is a block cipher in which the plaintext and ciphertext are integers

between 0 and *n* – 1 for some *n.*

T F 8. Timing attacks are only applicable to RSA.

T F 9. The Diffie-Hellman algorithm depends for its effectiveness on the

difficulty of computing discrete logarithms.

T F 10. The key exchange protocol is vulnerable to a man-in-the-middle

attack because it does not authenticate the participants.

T F 11. Unlike RSA, DSS cannot be used for encryption or key exchange.

T F 12. The operations performed during a round consist of circular

shifts, and primitive Boolean functions based on DSS, MD5, SHA, and RSA.

T F 13. SHA-3 algorithms must be designed to resist any potentially

successful attack on SHA-2 functions.

T F 14. Cryptographic hash functions generally execute faster in software

than conventional encryption algorithms such as DES.

T F 15. A hash function such as SHA-1 was not designed for use as a MAC

and cannot be used directly for that purpose because it does not rely on a secret key.

**MULTIPLE CHOICE QUESTIONS:**

1. SHA-1 produces a hash value of \_\_\_\_\_\_\_\_\_\_ bits.

A. 256 B. 160

C. 384 D. 180

2. In 2005, NIST announced the intention to phase out approval of \_\_\_\_\_\_\_ and move to a reliance on the other SHA versions by 2010.

A. SHA-1 B. SHA-512

C. SHA-256 D. SHA-2

3. Issued as RFC 2104, \_\_\_\_\_\_\_\_\_\_ has been chosen as the mandatory-to-implement MAC for IP Security.

A. RSA B. SHA-3

C. DSS D. HMAC

4. The \_\_\_\_\_\_\_\_\_ scheme has reigned supreme as the most widely accepted and implemented approach to public-key encryption.

A. SHA-1 B. HMAC

C. MD5 D. RSA

5. A \_\_\_\_\_\_\_\_ attack involves trying all possible private keys.

A. mathematical B. timing

C. brute-force D. chosen ciphertext

6. \_\_\_\_\_\_\_\_\_ attacks have several approaches, all equivalent in effort to factoring the product of two primes.

A. Mathematical B. Brute-force

C. Chosen ciphertext D. Timing

7. \_\_\_\_\_\_\_\_\_ are analogous to a burglar guessing a safe combination by observing how long it takes to turn the dial from number to number.

A. Digital standards B. Mathematical attacks

C. Ciphers D. Timing attacks

8. The \_\_\_\_\_\_\_\_\_ attack exploits the common use of a modular exponentiation algorithm in RSA encryption and decryption, but can be adapted to work with any implementation that does not run in fixed time.

A. mathematical B. timing

C. chosen ciphertext D. brute-force

9. A \_\_\_\_\_\_\_\_\_\_ type of attack exploits properties of the RSA algorithm.

A. timing B. brute-force

C. chosen ciphertext D. mathematical

10. Although the \_\_\_\_\_\_\_\_\_ attack is a serious threat, there are simple countermeasures that can be used such as constant time calcs, random delays or blinding computations.

A. timing B. chosen ciphertext

C. mathematical D. none of the above

11. \_\_\_\_\_\_\_\_\_\_\_ was the first published public-key algorithm.

A. NIST B. Diffie-Hellman

C. RC4 D. RSA

12. The National Institute of Standards and Technology has published Federal Information Processing Standard FIPS PUB 186, known as the \_\_\_\_\_\_\_\_\_\_.

A. XOR B. MD5

C. MAC D. DSS

13. The \_\_\_\_\_\_\_\_\_\_ uses an algorithm that is designed to provide only the digital signature function and cannot be used for encryption or key exchange.

A. ECC B. RSA

C. DSS D. XOR

14. The principal attraction of \_\_\_\_\_\_\_\_\_\_ compared to RSA is that it appears to offer equal security for a far smaller bit size, thereby reducing processing overhead.

A. ECC B. MD5

C. Diffie-Hellman D. none of the above

15. The DSS makes use of the \_\_\_\_\_\_\_\_\_ and presents a new digital signature technique, the Digital Signature Algorithm (DSA).

A. HMAC B. XOR

C. RSA D. SHA-1

**SHORT ANSWER QUESTIONS:**

1. The Secure Hash Algorithm (SHA) was developed by the \_\_\_\_\_\_\_\_\_ and published as a federal information processing standard (FIPS 180) in 1993.
2. Versions of SHA, with hash value lengths of 256, 384, and 512 bits, (SHA-256, SHA-384, and SHA 512) are collectively known as \_\_\_\_\_\_\_\_\_.
3. The evaluation criteria for the new hash function are: security, \_\_\_\_\_\_\_, and algorithm and implementation characteristics.
4. \_\_\_\_\_\_ has been issued as RFC 2014, has been chosen as the mandatory-to-implement MAC for IP Security, and is used in other Internet protocols, such as Transport Layer Security.
5. One of the first public-key schemes, \_\_\_\_\_\_\_, was developed in 1977 by Ron Rivest, Adi Shamir, and Len Adleman.
6. \_\_\_\_\_\_\_\_\_\_ are alarming for two reasons: they come from a completely unexpected direction and they are a ciphertext-only attack.
7. Four possible approaches to attacking the RSA algorithm are: brute force, timing attacks, \_\_\_\_\_\_\_\_\_ attacks, and chosen ciphertext attacks.
8. NIST has published FIPS PUB 186, which is known as the \_\_\_\_\_\_\_\_\_\_\_.
9. The purpose of the \_\_\_\_\_\_\_\_\_\_ algorithm is to enable two users to exchange a secret key securely that can then be used for subsequent encryption of messages.
10. One of the simplest hash functions is the \_\_\_\_\_\_\_\_ of every block.
11. “Must support hash value lengths of 224, 256,384, and 512 bits” and “algorithm must process small blocks at a time instead of requiring the entire message to be buffered in memory before processing it” are requirements for \_\_\_\_\_\_\_\_.
12. If speed is a concern, it is fully acceptable to use \_\_\_\_\_\_\_\_\_ rather than SHA as the embedded hash function for HMAC.
13. The purpose of the algorithm is to enable two users to exchange a \_\_\_\_\_\_\_\_\_\_ securely that can then be used for subsequent encryption of messages.
14. The security of any MAC function based on an embedded hash function depends in some way on the \_\_\_\_\_\_\_\_\_ strength of the underlying hash function.
15. Perhaps the most widely used public-key algorithms are \_\_\_\_\_\_\_\_\_ and Diffie-Hellman.