Read chapter 20 in Computer Security: Principles and Practice

TRUE/FALSE QUESTIONS:

T F 1. Symmetric encryption is also referred to as secret-key or single-key encryption.

T F 2. Plaintext is the scrambled message produced as output.

T F 3. If both sender and receiver use the same key the system is referred to as asymmetric.

T F 4. The ciphertext-only attack is the easiest to defend against.

T F 5. A brute-force approach involves trying every possible key until an intelligible translation of the ciphertext into plaintext is obtained.

T F 6. AES uses a Feistel structure.

T F 7. Stream ciphers are far more common than block ciphers.

T F 8. "Each block of 64 plaintext bits is encoded independently using the same key" is a description of the CBC mode of operation.

T F 9. It is possible to convert any block cipher into a stream cipher by using the cipher feedback (CFB) mode.

T F 10. One desirable property of a stream cipher is that the ciphertext be of the same length as the plaintext.

T F 11. In using encryption, we need to decide what to encrypt and where the encryption gear should be located.

T F 12. One disadvantage of the link encryption approach is that the message must be decrypted each time it enters a frame switch.

T F 13. "The plaintext is 64 bits in length and the key is 56 bits in length; longer plaintext amounts are processed in 64-bit blocks" is a description of the DES algorithm.

T F 14. The National Bureau of Standards is now the National Institute of Standards and Technology.

T F 15. Key distribution can be achieved for two parties A and B by a third party selecting the key and physically delivering it to A and B.

MULTIPLE CHOICE QUESTIONS:

1. _____ is the original message or data that is fed into the algorithm as input.

Read chapter 20 in Computer Security: Principles and Practice

A. Plaintext B. Encryption algorithm

C. Decryption algorithm D. Ciphertext

2. The exact substitutions and transformations performed by the algorithm depend on the _____.

A. ciphertext B. decryption algorithm

C. secret key D. encryption algorithm

3. The _____ is the encryption algorithm run in reverse.

A. decryption algorithm B. ciphertext

C. plaintext D. secret key

4. If the analyst is able to get the source system to insert into the system a message chosen by the analyst, then a _____ attack is possible.

A. known-plaintext B. chosen-plaintext

C. chosen ciphertext D. chosen text

5. The most widely used encryption scheme is based on the _____ adopted in 1977 by the National Bureau of Standards.

A. AES B. 3DES

C. CES D. DES

6. There are _____ modes of operation defined by NIST that are intended to cover virtually all the possible applications of encryption for which a block cipher could be used.

A. three B. five

C. seven D. nine

7. For stream-oriented transmission over noisy channel you would typically use _____ mode.

A. ECB B. CTR

C. OFB D. CBC

Read chapter 20 in Computer Security: Principles and Practice

8. For general-purpose block-oriented transmission you would typically use _____ mode.

A. CBC B. CTR

C. CFB D. OFB

9. For general-purpose stream-oriented transmission you would typically use _____ mode.

A. CTR B. CFB

C. ECB D. CBC

10. _____ mode is typically used for a general-purpose block-oriented transmission and is useful for high-speed requirements.

A. ECB B. OFB

C. CFB D. CTR

11. _____ is a term that refers to the means of delivering a key to two parties that wish to exchange data without allowing others to see the key.

A. Session key B. Subkey

C. Key distribution technique D. Ciphertext key

12. A _____ is a key used between entities for the purpose of distributing session keys.

A. permanent key B. session key

C. distribution key D. all of the above

13. The _____ module performs end-to-end encryption and obtains session keys on behalf of users.

A. PKM B. RCM

C. SSM D. CCM

14. Public-key encryption was developed in the late _____.

A. 1950s B. 1970s

C. 1960s D. 1980s

15. Cryptographic systems are generically classified by _____.

Read chapter 20 in Computer Security: Principles and Practice

A. the type of operations used for transforming plaintext to ciphertext

B. the number of keys used

C. the way in which the plaintext is processed

D. all of the above

SHORT ANSWER QUESTIONS:

1. A symmetric encryption scheme has five ingredients: plaintext, encryption algorithm, ciphertext, decryption algorithm and _____.

2. _____ is the process of attempting to discover the plaintext or key.

3. A _____ cipher processes the input one block of elements at a time, producing an output block for each input block.

4. A _____ cipher processes the input elements continuously, producing output one element at a time as it goes along.

5. An encryption scheme is _____ if the cost of breaking the cipher exceeds the value of the encrypted information and/or the time required to break the cipher exceeds the useful lifetime of the information.

6. The _____ was issued as a federal information-processing standard and is intended to replace DES and 3DES with an algorithm that is more secure and efficient.

7. _____ was designed in 1987 by Ron Rivest and is a variable key-size stream cipher with byte-oriented operations.

8. "The input to the encryption algorithm is the XOR of the next 64 bits of plaintext and the preceding 64 bits of ciphertext" is a description of the _____ mode of operation.

9. Unlike ECB and CBC modes, _____ mode requires only the implementation of the encryption algorithm and not the decryption algorithm.

10. The most powerful, and most common, approach to countering the threats to network security is _____.

11. With _____ encryption the encryption process is carried out at the two end systems.

Read chapter 20 in Computer Security: Principles and Practice

12. With _____ encryption each vulnerable communications link is equipped on both ends with an encryption device.

13. For symmetric encryption to work the two parties to an exchange must share the same _____, which must be protected from access by others.

14. All encryption algorithms are based on two general principles: substitution and _____.

15. The three most important symmetric block ciphers are: 3DES, AES, and _____.