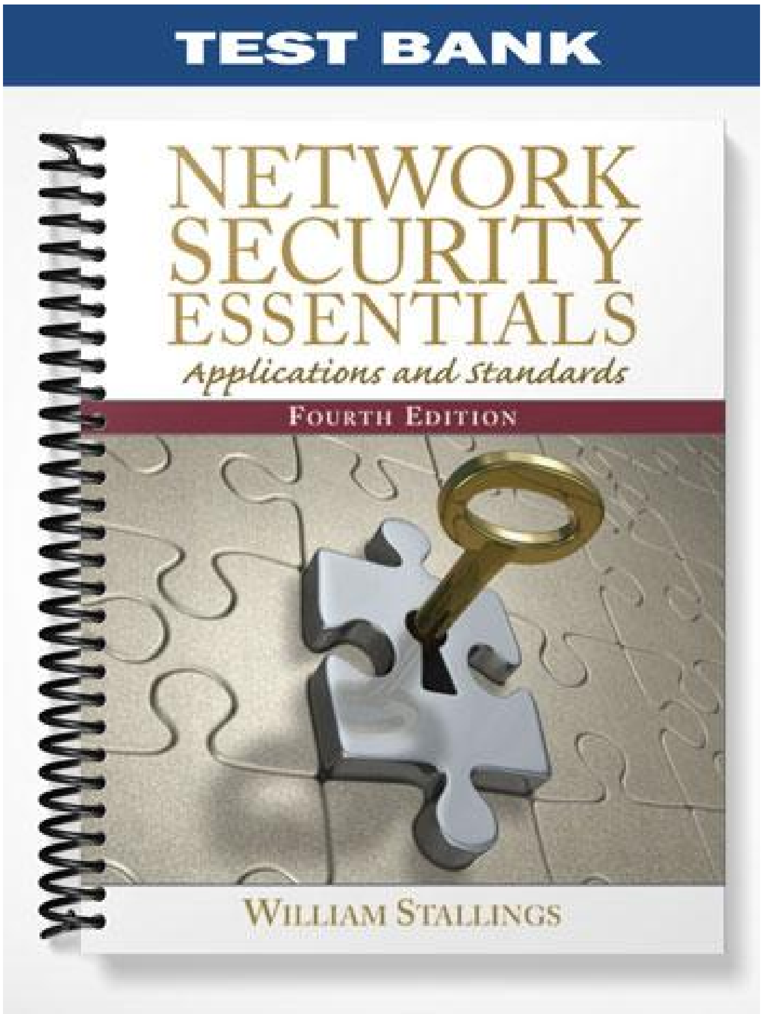

# TEST BANK

# NETWORK SECURITY ESSENTIALS

*Applications and Standards*

FOURTH EDITION

WILLIAM STALLINGS

**TRUE/FALSE. Write 'T' if the statement is true and 'F' if the statement is false.**

1) Public-key encryption is also referred to as conventional encryption, secret-key, or single-key encryption. 1) _______

2) The advantage of a block cipher is that you can reuse keys. 2) _______

3) Ciphertext is the scrambled message produced as output. 3) _______

4) The security of symmetric encryption depends on the secrecy of the algorithm, not the secrecy of the key. 4) _______

5) The ciphertext-only attack is the easiest to defend against because the opponent has the least amount of information to work with. 5) _______

6) The Feistel structure is a particular example of the more general structure used by all symmetric block ciphers. 6) _______

7) Smaller block sizes mean greater security but reduced encryption/decryption speed. 7) _______

8) The essence of a symmetric block cipher is that a single round offers inadequate security but that multiple rounds offer increasing security. 8) _______

9) Triple DES was first standardized for use in financial applications in ANSI standard X9.17 in 1985. 9) _______

10) The most commonly used symmetric encryption algorithms are stream ciphers. 10) ______

11) The principal drawback of 3DES is that the algorithm is relatively sluggish in software. 11) ______

12) AES uses a Feistel structure. 12) ______

13) Random numbers play an important role in the use of encryption for various network security applications. 13) ______

14) The primary advantage of a stream cipher is that stream ciphers are almost always faster and use far less code than do block ciphers. 14) ______

15) One desirable property of a stream cipher is that the ciphertext be longer in length than the plaintext. 15) ______

**MULTIPLE CHOICE. Choose the one alternative that best completes the statement or answers the question.**

16) A symmetric encryption scheme has _________ ingredients. 16) ______

A) five B) three C) four D) six

17) _________ is the original message or data that is fed into the algorithm as input. 17) ______

A) DES B) Ciphertext

C) Plaintext D) Encryption key

18) _________ mode requires only the implementation of the encryption algorithm and not the decryption algorithm. 18) ______

A) CTR B) CBC C) ECB D) DKS

19) A __________ processes the input elements continuously, producing output one element at a time, as it goes along. 19) ______

A) stream cipher B) cryptanalysis
C) keystream D) block cipher

20) If both sender and receiver use the same key the system is referred to as _________ encryption. 20) ______

A) asymmetric B) two-key
C) symmetric D) public-key

21) If the sender and receiver each use a different key the system is referred to as __________ encryption. 21) ______

A) asymmetric B) conventional
C) single-key D) secret-key

22) A _________ approach involves trying every possible key until an intelligible translation of the ciphertext into plaintext is obtained. 22) ______

A) brute-force B) block cipher
C) computational D) triple DES

23) With the ________ mode if there is an error in a block of the transmitted ciphertext only the corresponding plaintext block is affected. 23) ______

A) TSR B) CTS C) CBC D) ECB

24) The most common key length in modern algorithms is ________ . 24) ______

A) 128 bits B) 256 bits C) 64 bits D) 32 bits

25) A ________ takes as input a source that is effectively random and is often referred to as an entropy source. 25) ______

A) PRNG B) PRF C) TRNG D) PSRN

26) A symmetric block cipher processes _________ of data at a time. 26) ______

A) three blocks B) two blocks
C) one block D) four blocks

27) In _________ mode a counter equal to the plaintext block size is used. 27) ______

A) CBC B) ECB C) CFB D) CTR

28) The _________ algorithm performs various substitutions and transformations on the plaintext. 28) ______

A) codebook B) encryption
C) keystream D) cipher

29) If the analyst is able to get the source system to insert into the system a message chosen by the analyst, a _________ attack is possible. 29) ______

A) known plaintext B) chosen ciphertext

C) ciphertext only D) chosen plaintext

30) The _________ key size is used with the Data Encryption Standard algorithm. 30) ______

A) 56 bit B) 128 bit C) 168 bit D) 32 bit

**SHORT ANSWER. Write the word or phrase that best completes each statement or answers the question.**

31) The _________ algorithm takes the ciphertext and the same secret key and produces the original plaintext. 31) _____________

32) A _________ cipher processes the plaintext input in fixed sized blocks and produces a block of ciphertext of equal size for each plaintext block. 32) _____________

33) With the use of symmetric encryption, the principal security problem is maintaining the secrecy of the _________ . 33) _____________

34) Three broad categories of cryptographic algorithms are commonly used to create PRNGs: Asymmetric ciphers, Hash functions and message authentication codes, and ___________ . 34) _____________

35) The process of attempting to discover the plaintext or key is known as _________ . 35) _____________

36) 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. 36) _____________

37) The three most important symmetric block ciphers are: triple DES (3DES), the Advanced Encryption Standard (AES), and the ___________ . 37) _____________

38) The ________ source is drawn from the physical environment of the computer and could include things such as keystroke timing patterns, disk electrical activity, mouse movements, and instantaneous values of the system clock. 38) _____________

39) A PRNG takes as input a fixed value called the ________ and produces a sequence of output bits using a deterministic algorithm. 39) _____________

40) __________ is a stream cipher used in the Secure Sockets Layer/Transport Layer Security standards that have been defined for communication between Web browsers and servers and is also used in WEP and WPA protocols. 40) _____________

41) In the _________ mode the input to the encryption algorithm is the XOR of the current plaintext block and the preceeding ciphertext block; the same key is used for each block. 41) _____________

42) Also referred to as conventional encryption, secret-key, or single-key encryption, _________ encryption was the only type of encryption in use prior to the development of public-key encryption in the late 1970's. 42) _____________

43) Two requirements for secure use of symmetric encryption are: sender and receiver must have obtained copies of the secret key in a secure fashion and a strong __________ is needed. 43) _____________

44) All encryption algorithms are based on two general principles: _________, in which each element in the plaintext is mapped into another element, and transposition, in which elements in the plaintext are rearranged. 44) _____________

45) Many symmetric block encryption algorithms including DES have a structure first described by _________ of IBM in 1973. 45) _____________

1) FALSE
2) TRUE
3) TRUE
4) FALSE
5) TRUE
6) TRUE
7) FALSE
8) TRUE
9) TRUE
10) FALSE
11) TRUE
12) FALSE
13) TRUE
14) TRUE
15) FALSE
16) A
17) C
18) A
19) A
20) C
21) A
22) A
23) D
24) A
25) C
26) C
27) D
28) B
29) D
30) A
31) decryption
32) block
33) key
34) Symmetric block ciphers
35) cryptanalysis
36) computationally secure
37) Data Encryption Standard (DES)
38) entropy
39) seed
40) RC4
41) cipher block chaining (CBC)
42) symmetric
43) encryption algorithm
44) substitution
45) Horst Feistel