Practice Set for Class Test – I

Course Name: Cryptography & Network Security

Course Code: MCA304A

Multiple Choice Type Questions:

1. Identify which is not an objective of network security.

A. identification
B. authentication
C. access control
D. lock

2. Identify the process of verifying the identity of a user.

A. authentication
B. identification
C. validation
D. verification

3. Identify which of these is a part of network identification?

A. user id
B. password
C. otp
D. fingerprint

4. Identify the person who enjoys learning details about computers and how to enhance their capabilities.

A. cracker
B. hacker
C. app controller
D. site controller

5. Identify a small program that changes the way a computer operates.

A. worm
B. Trojan
C. bomb
D. virus

6. TCP/IP model does not have _____ layer but OSI model have this layer. Select the right one.

A. session layer
B. transport layer
C. application layer
D. network layer

7. In cryptography, identify what is cipher?

A. algorithm for performing encryption and decryption

B. encrypted message

C. both algorithm for performing encryption and decryption and encrypted message

D. decrypted message

8. Identify Malware is

A. malfunctioned software

B. multipurpose software

C. malicious software

D. malfunctioning of security

12. Select which of them is not an ideal way of spreading the virus?

A. infected website

B. e-mails

C. official antivirus cds

D. usbs

13. Identify which of the following is a non-technical type of intrusion or attack technique?

A. reverse engineering

B. malware analysis

C. social engineering

D. malware writing

14. Identify which of them is not a proper method for email security?

A. use strong password

B. use email encryption

C. spam filters and malware scanners

D. click on unknown links to explore

15. Predict the keys used in cryptography are

A. secret key

B. private key

C. public key

D. all of them

16. Predict the process of writing the text as rows and read it as columns is known as

A. vernam cipher

B. ceaser cipher

C. transposition columnar cipher

D. homophonic substitution cipher

17. Estimate the sub key length at each round of DES is

A. 32

B. 56

C. 48

D. 64

18. Estimate the advantages of Public key encryption over Symmetric Key Cryptography because of

A. speed B. space

C. key exchange D. key length

19. Estimate the sub key length at each round of DES is

A. 32 B. 56

C. 48 D. 64

20. Conclude AES also uses Feistel Structure.

A. true B. false

C. cannot be determined D. none

Short Answer Type Questions:

1. Identify six different principles of security.
2. Define integrity and non-repudiation.
3. Define cryptanalysis.
4. Define Diffusion & Confusion.
5. Define confidentiality and authentication.
6. Discover the design parameters of Feistel cipher network?
7. Explain Traffic analysis.
8. Sketch the differences between Message Authentication Code and Hash function.
9. Write the schemes for the distribution of public keys.
10. Explain Avalanche effect.
11. Predict the attacks to RSA.
12. Summarize the basic task for defining a security service.
13. Find the three classes of message authentication function.
14. Write the five modes of operation of Block cipher.
15. Estimate the evaluation criteria defined by NIST for AES.
16. Distinguish between active attack and passive attack with suitable examples.

17. State what is the difference between MAC and Message Digest.
18. State the term Key Distribution Center (KDC).
19. Write the significance of tunnel mode.
20. Write the three main actions of a packet filter.
21. State the significance of Initialization Vector (IV).
22. Discuss the algorithm of Rail Fence Technique.
23. Briefly explain virus and worms.
24. State the difference between Substitution Cipher and Transposition Cipher.
25. Write the concept of HMAC.
26. State what is Triple DES.
27. Explain Message Digest.
28. Write the significance of tunnel mode.
29. "Authentication can be achieved using DES" --- Comment on it.
30. Write the principle behind One-time pads.