CSUA (GBLOCK).

REV-01
MCA/14/18

2022/12

SET A

MASTER OF COMPUTER APPLICATION
THIRD SEMESTER
CRYPTOGRAPH AND NETWORK SECURITY
MCA-302

[USE OMR SHEET FOR OBJECTIVE PART]

Duration: 3 hrs. **Full Marks: 70**

(Objective)

Time: 30 mins. **Marks: 20**

Choose the correct answer from the following: *1×20=20*

1. Use Caesar's Cipher to decipher the following:
   HQFUBSWHG WHAW
   a. ABANDONED LOCK
   b. ENCRYPTED TEXT
   c. ABANDONED TEXT
   d. ENCRYPTED LOCK

2. In which of the following, a person is constantly followed/chased by another person or group of several peoples?
   a. Phishing
   b. Bulling
   c. Stalking
   d. Identity theft

3. Which of the following refers to the violation of the principle if a computer is no more accessible?
   a. Access control
   b. Confidentiality
   c. Availability
   d. All of the above

4. Which one of the following refers to the technique used for verifying the integrity of the message?
   a. Digital signature
   b. Decryption algorithm
   c. Protocol
   d. Message Digest

5. The response time and transit time is used to measure the _____ of a network.
   a. Security
   b. Longevity
   c. Reliability
   d. Performance

6. Which of the following statements is correct about the firewall?
   a. It is a device installed at the boundary of a company to prevent unauthorized physical access.
   b. It is a device installed at the boundary of an incorporate to protect it against the unauthorized access.
   c. It is a kind of wall built to prevent files form damaging the corporate.
   d. None of the above.

7. Which type following UNIX account provides all types of privileges and rights which one can perform administrative functions?
   a. Client
   b. Guest
   c. Root
   d. Administrative

8. If the number of parties involved in a lock-key mechanism is 4, the number of keys needed is_____

a. 2
b. 4
c. 6
d. 8

9. Which of them is not a wireless attack?
a. Eavesdropping
b. MAC Spoofing
c. Wireless Hijacking
d. Phishing

10. In AES, the 16-byte key is expanded into _____
a. 200 bytes
b. 78 bytes
c. 176 bytes
d. 187 bytes

11. There are _____ encryption round in RC5.
a. 18
b. 12
c. 16
d. 20

12. The 4×4 byte matrices in the AES algorithm are called_____
a States
b. Words
c. Transitions
d. Permutations

13. Which of the 4 operations are false for each round in the AES algorithm?
i) Substitute Bytes
ii) Shift Columns
iii) Mix Rows
iv) XOR Round Key
a i) only
b. ii) iii) and iv)
c. ii) and iii)
d. only iv)

14. On comparing AES with DES, which of the following functions from DES does not have an equivalent AES function?
a f function
b. permutation p
c. swapping of halves
d. xor of subkey with function f

15. Which of the following statements are true ?
i) In the CBC mode, the plaintext block is XORed with previous ciphertext block before encryption
ii) The CTR mode does not require an Initialization Vector
iii) The last block in the CBC mode uses an Initialization Vector
iv) In CBC mode repetitions in plaintext do not show up in cipher text
a iii)
b. ii) and iv)
c. i) ii) and iv)
d. All the Statements are true

16. In ECC, elliptic curve € with a point P, Q=dXP. Here d stands for_____
a Prime number
b. Discrete number
c. Random number
d. Even number

17. The man-in-the-middle attack can endanger the security of the Diffie-Hellman method if two parties are not
a. Authenticated
b Joined
c. Submit
d. Separate

18. In the DES algorithm the Round Input is 32 bits, which is expanded to 48 bits via
a. Scaling of the existing bits
b Duplication of the existing bits

c. Addition of zeros
d. Addition of ones

19. A Firewall is a specialized form of a _____
a. Bridge
b. Disk
c. printer
d. router

20. _____ allows reuse of IP addresses.
a. Firewalls
b. IPSec
c. NAT
d. VPN

-- --- --

Descriptive

Time : 2 hrs. 30 mins. **Marks : 50**

[Answer question no.1 & any four (4) from the rest]

1. In NewGen security services agency, few employees become aggressive against administration due to their some HR related issues. Since the employees were core members of their coding team so there are some vulnerability on security and privacy. The management of the organization wants to change their existing security protocol Firewall. What security protocol do you suggest to the management? Discuss your views. 10

2. a. Draw the flow chart to display the steps in the various rounds of AES. 5+5=10
   b. Give a brief comparison between Substitution and Transposition techniques of encryption.

3. a. Why is SHA more secure than MD5? Distinguish between MAC and MD. 5+5=10
   b. Describe the One-time initialization process of AES operation.

4. a. Alice sends a mail to Bob using PGP to ensure security. What steps should Alice follow till the mail has been send completely? 5+5=10
   b. Discuss about the crux of RSA algorithm.

5. a. Explain the role of Proxy server in network security. 5+5=10
   b. Distinguish between Static vs Dynamic WebPages.

6. What is Kerberos? How Kerberos Work in Network security? Explain. 3+7=10

7. What do you understand by user authentication? How Windows operating system maintain user authentication? Write down the different types file privileges in Unix operating system. 2+4+4=10

8. Write short notes on: 5+5=10
   i. Elliptic curve Cryptography
   ii. Intrusion Detection

= = *** = =