18. (a) Illustrate kerberos.

Or

(b) Explain x.509 authentication service.

19. (a) Write a short note on secure socket layer.

Or

(b) Explain basic concepts of SNMP.

20. (a) Write a short note intrusion detection.

Or

(b) Elaborate password management.

PART C — (3 × 10 = 30)

Answer any THREE questions.

21. Give a detailed explanation in classical encryption techniques.

22. Briefly explain about chiper block modes of operation.

23. Explain in detail about public key infrastructure.

24. Discuss briefly about IP security architecture.

25. Write detailed about distributed firewalls.

S.No. 7280 **P 22 MCAE 2 A**

(For candidates admitted from 2022–2023 onwards)

M.C.A. DEGREE EXAMINATION, NOVEMBER 2023

Computer Applications — Elective

CRYPTOGRAPHY AND NETWORK SECURITY

Time : Three hours Maximum : 75 marks

PART A — (20 marks)

Answer ALL questions

I. (A) Multiple choice questions: (5 × 1 = 5)

1. Which of the following is an example of data-link layer vulnerability?

(a) MAC Address Spoofing

(b) Physical Theft of Data

(c) Route spoofing

(d) Weak or non-existent authentication

2. How many keys does the Triple DES algorithm use?

(a) 2 (b) 3

(c) 2 or 3 (d) 3 or 4

3. Linux systems can store Kerberos authentication keys for a service principal in ———— files.

(a) Client

(b) Server

(c) Keytab

(d) All of the mentioned

4. WPA2 is used for security in ————.

(a) Ethernet (b) Bluetooth

(c) Wi-Fi (d) Email

5. The intent of a ———— is to overkill the targeted server's bandwidth and other resources of the target website.

(a) Phishing attack (b) DoS attack

(c) Website attack (d) MiTM attack

(B) Fill in the blanks : (5 × 1 = 5)

6. ———— may be forced for flooding traffic to all VLAN ports allowing interception of data through any device that is connected to a VLAN.

7. SSM stands for ————.

8. On Linux, MongoDB clients can use Kerberos's ———— program to initialize a credential cache for authenticating the user principal to servers.

9. An attempt to make a computer resource unavailable to its intended users is called ————.

10. DoS is abbreviated as ————.

II. Answer ALL questions : (5 × 2 = 10)

11. State the concept of security policies.

12. Expand HMAC.

13. List out any two advantages of PGP.

14. Define authentication header.

15. How Intruders are defined?

PART B — (5 × 5 = 25)

Answer ALL questions, choosing either (a) or (b)

16. (a) Explain product cryptosystem.

Or

(b) Discuss a note on security attacks.

17. (a) Elaborate about stream ciphers and RC4.

Or

(b) Discuss a note on secure hash functions.