KAMARAJ COLLEGE (Autonomous)

Accredited with A+ Grade by NAAC

(Affiliated to Manonmaniam Sundaranar University, Tirunelveli)

THOOTHUKUDI – 628 003

(6 Pages) **Reg. No: ……**

Question Code No : 25O03208 **Course Code : 24PMAI33**

PG Degree - End Semester Examinations, November 2025

Third Semester

M.Sc. COMPUTER SCIENCE WITH ARTIFICIAL INTELLIGENCE

Cryptography and Network Security

(For those who joined in July 2024 onwards)

Time : 3 Hours **Maximum : 75 Marks**

PART– A (10 × 1 = 10 Marks)

Answer ALL Questions

Choose the correct answer:

1. What is the original message before any cryptographic transformation?

   (a) Secret-text (b) Plaintext

   (c) Ciphertext (d) None of the above

2. Which cryptographic method rearranges the order of letters in a message?

   (a) Transposition ciphers (b) Substitution ciphers

(c) Digital signature (d) Quadratic ciphers

3. Which one of the following algorithms is not used in asymmetric-key cryptography?
   (a) DSA algorithm
   (b) Electronic code book algorithm
   (c) Diffie-Hellman algorithm
   (d) RSA algorithm
4. What is the primary purpose of cryptanalysis?
   (a) To find insecurity in a cryptographic scheme (b) To increase speed
   (c) To encrypt the data (d) To make new ciphers
5. Who keeps the private key in asymmetric key cryptography?
   (a) Sender (b) Receiver
   (c) Sender and Receiver (d) All devices on the network
6. Which of the following cannot be achieved using a hash value?
   (a) Password check
   (b) Data integrity check
   (c) Digital signatures

(d) Data retrieval in its original form

7. Which cryptographic protocol is used to protect an HTTP connection?

(a) Resource Reservation Protocol
(b) SCTP
(c) TLS
(d) ECN

8. Which is not an objective of network security?

(a) Identification
(b) Authentication
(c) Access control
(d) Lock

9. What is the main purpose of steganography?

(a) Encrypting messages
(b) Hiding messages within other media
(c) Digital signatures
(d) Firewall management

10. What is digital watermarking primarily used for?

(a) Hiding secret messages
(b) Protecting ownership and copyright of digital content
(c) Encrypting files
(d) Analyzing network traffic

PART – B (5 X 5 = 25 Marks)

Answer ALL Questions choosing either (a) or (b).
Answer should not exceed 250 words.

11. (a) Describe the method of Columnar transposition technique.

(OR)

(b) Describe the key generation process in DES.

12. (a) Explain the steps involved in RSA key generation.

(OR)

(b) Identify the main purpose of using a digital signature.

13. (a) Write down the main components of Kerberos authentication system.

(OR)

(b) What are the techniques used in S/MIME? Explain.

14. (a) Explain the various methods used to prevent and detect viruses.

(OR)

(b) What are the main components of SSL?

15. (a) Write down the main purpose of steganography.

(OR)

(b) Explain the main phases of network forensic investigation.

PART – C (5 X 8 = 40 Marks)

Answer ALL Questions choosing either (a) or (b).
Answer should not exceed 600 words.

16. (a) Explain the OSI security architecture and provide an illustrative diagram.

(OR)

(b) Describe the steps involved in performing a brute-force cryptanalysis on a Caesar cipher.

17. (a) Explain the Diffie – Hellman key exchange Algorithm with a numeric example.

(OR)

(b) Analyze the working of HMAC and describe how it enhances security.

18. (a) Discuss the steps involved in PG Encryption.

(OR)

(b) Describe in detail about the X.509 certificate structure and its purpose of each element.

19. (a) Analyze the roles of the change cipher spec and alert protocols in TLS.

(OR)

(b) What are the strategies of password selection? Explain.

20. (a) Compare and contrast symmetric and asymmetric cryptography algorithm.

(OR)

(b) List the advantages of DNA base cryptography over traditional methods.