(6 pages)

Reg. No. : .....

Code No. : 7745 **Sub. Code : ZCIM 33**

M.Sc. (CBCS) DEGREE EXAMINATION, NOVEMBER 2023.

Third Semester

Computer Science with Artificial Intelligence – Core

NETWORK SECURITY AND CRYPTOGRAPHY

(For those who joined in July 2022 onwards)

Time : Three hours Maximum : 75 marks

PART A — (10 × 1 = 10 marks)

Answer ALL questions.

Choose the correct answer :

1. Which of the following attacks is a passive attack?
   (a) Masquerade
   (b) Modification of message
   (c) Denial of service
   (d) Traffic analysis

2. A mechanism used to encrypt and decrypt data
   (a) Cryptography
   (b) Algorithm
   (c) Data flow
   (d) None of these

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. The private key in asymmetric key cryptography is kept by _____.
   (a) Sender
   (b) Receiver
   (c) Sender and receiver
   (d) All the connected devices to the network

5. Which of the following ciphers is a block cipher?
   (a) Caesar cipher (b) Vernam cipher
   (c) Playfair cipher (d) None of the above

6. Which of the following is not possible through hash value?
   (a) Password Check
   (b) Data Integrity check
   (c) Digital Signatures
   (d) Data retrieval in its original form

7. Cryptanalysis is used _____.
   (a) to find some insecurity in a cryptographic scheme
   (b) to increase the speed
   (c) to encrypt the data
   (d) to make new ciphers

8. Which is not an objective of network security?
   (a) identification
   (b) authentication
   (c) access control
   (d) lock

9. The process of verifying the identity of a user
   (a) authentication (b) identification
   (c) validation (d) verification

10. A process of making the encrypted text readable again
    (a) decryption (b) encryption
    (c) network security (d) information hiding

PART B — (5 × 5 = 25 marks)

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

Each answer should not exceed 250 words.

11. (a) Summarize the uses of transposition techniques in cryptography.

    Or

    (b) Explain the need for security at multiple levels.

12. (a) Describe the approaches to message authentication.

    Or

    (b) Point out the symmetric block encryption algorithm.

13. (a) Write down the overview of Kerberos.

    Or

    (b) What are the advantages of electronic main security? Explain.

14. (a) Elaborate the basic concept of SNMP.

Or

(b) Bring out the concept of IPSec authentication header with diagram.

15. (a) Highlights the virus and related threats.

Or

(b) Mention the concept of trusted systems.

PART C — (5 × 8 = 40 marks)

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

Each answer should not exceed 600 words.

16. (a) Determine the OSI security architecture with diagram.

Or

(b) Outline the ethical and professional aspects of security.

17. (a) Discuss the secure hash functions and HMAC.

Or

(b) Analysis the key management in cryptography.

18. (a) Draw and explain the key elements of the public-key infrastructure model.

Or

(b) What are the S/MIME messages? Explain.

19. (a) Elucidate the format of an encapsulating security payload packet.

Or

(b) Examine the services of Secure Electronic Transaction.

20. (a) Formulate the design principles of firewall.

Or

(b) Evaluate the distributed denial of service attacks.

———————