

Register No.: Name:

SAINTGITS COLLEGE OF ENGINEERING (AUTONOMOUS)

(AFFILIATED TO APJ ABDUL KALAM TECHNOLOGICAL UNIVERSITY, THIRUVANANTHAPURAM)

THIRD SEMESTER M.C.A DEGREE EXAMINATION (S), MAY 2022

(2020 SCHEME)

Course Code: 20MCAT221

Course Name: Cyber Security and Cryptography

Max. Marks: 60

Duration: 3 Hours

Special instructions – Calculator is allowed to use

PART A

(Answer all questions. Each question carries 3 marks)

1. Which are the various cryptographic services used in cyber security ?
2. State the encryption and decryption technique behind playfair cipher.
3. With the help of a diagram, write the algorithm to perform encryption operation in CBC mode.
4. Express the function of a D-box using a diagram.
5. Distinguish between message integrity and message authentication.
6. Discuss the idea behind blind signatures.
7. How can we enhance the security feature of an e-mail ?
8. Identify the protocol(s) used in SSL.
9. List the various web application security vulnerabilities as defined by OWASP.
10. Write a short note on SQL injection attack.

PART B

(Answer one full question from each module, each question carries 6 marks)

MODULE I

11. a) Analyze the various security mechanisms used in cyber security. (3)
- b) Encrypt the plaintext 'security' using Affine cipher method for key pairs (5, 13). (3)

OR

12. a) Use a Hill cipher to encrypt the message "we live in an insecure world". Use the following key $K = \begin{pmatrix} 03 & 02 \\ 05 & 07 \end{pmatrix}$ (3)
- b) Encrypt the message "enemy attacks tonight" using Transposition cipher with the help of the key matrix [3 1 4 5 2]. (3)

MODULE II

13. Discuss the working of DES algorithm using a neat sketch. (6)

OR

14. Describe the technique behind Diffie Hellman key exchange algorithm. (6)

MODULE III

15. a) Define a cryptographic hash function. (3)
b) What are the properties of a good hash function? (3)

OR

16. a) Distinguish between HMAC and CMAC. (3)
b) Using a block diagram, prepare a write up on RSA digital signature scheme. (3)

MODULE IV

17. What is the idea behind PGP? Explain the various functionalities inherent in PGP to implement security. (6)

OR

Outline the concept of

18. i) Encapsulation Security Payload. (3)
ii) Secure Electronic Transactions. (3)

MODULE V

19. Give an account of the following terms. (3)
i) Broken Authentication (3)
ii) XML External Entities

OR

20. Write notes on the following terms. (3)
i) Broken Access Control (3)
ii) Cross Site Scripting
