B **376B2** **Total pages: 2**

Register No: …… Name: .....

SAINTGITS COLLEGE OF ENGINEERING (AUTONOMOUS)

(AFFILIATED TO APJ ABDUL KALAM TECHNOLOGICAL UNIVERSITY, THIRUVANANTHAPURAM)

EIGHTH SEMESTER B.TECH DEGREE EXAMINATION(R), MAY 2024

Computer Science and Engineering

(2020 SCHEME)

Course Code : 20CST432

Course Name : Cryptography

Max. Marks : 100 **Duration:3 Hours**

Scientific calculator is allowed in the examination hall.

PART A

(Answer all questions. Each question carries 3 marks)

1. Explain the fundamental difference between public key cryptosystems and symmetric key cryptosystems?
2. Differentiate between a DoS (Denial of Service) attack and a DDoS (Distributed Denial of Service) attack
3. What is the advantage of RC4 Algorithm?
4. Explain the block cipher operation and components?
5. Using the superincreasing knapsack sequence [2, 7, 11, 21, 42], demonstrate how the knapsack algorithm can be applied to encrypt the message 'HELLO'. Show the step-by-step process of encryption, including the calculation of the ciphertext?
6. Illustrate Elliptic Curve Decryption?
7. What is the role of backup keys in assymmetric encryption ?
8. Write a note on man-in-the-middle attack during the Simple Secret Key Distribution in Symmetric key distribution using asymmetric encryption
9. How do authentication functions contribute to ensuring the security and integrity of cryptographic systems?
10. List the types of Authentication required in cryptography?

PART B

(Answer one full question from each module, each question carries 14 marks)

MODULE I

11. Discuss the key components and processes involved in public key cryptography? 14

OR

12. Discuss the fundamental principles and practical applications of block ciphers in modern cryptography? Encrypt the following Plaintext Block: 01101110 (8 bits) using a 64-bit key: Key: 1010101010111100101101001101111110001101101011111001101101011110 14

MODULE II

13. Explain the operation of the RC4 stream cipher, including its key scheduling algorithm and pseudorandom generation process? 14

OR

14. Explain in detail the steps of DES Algorithm? 14

MODULE III

15. Consider a Diffie-Hellman key exchange with the following parameters:Shared prime modulus (p): 17. Primitive root modulo (g): 3.Alice chooses a private key (a) = 5, and Bob chooses a private key (b) = 8. Calculate the shared secret key that Alice and Bob will generate using the Diffie-Hellman key exchange algorithm. 14

OR

16. Explain in detail the encryption and decryption procedures using Elliptic Curve Cryptography? 14

MODULE IV

17. List out the steps involved in the Symmetric key distribution using symmetric encryption and explain with an example? 14

OR

18. Explain the architecture of Key Distribution Scenario in symmetric encryption? 14

MODULE V

19. Discuss the construction and operation of CMAC, including its utilization of block cipher algorithms for message authentication? 14

OR

20. Illustrate the working of SHA-1 algorithm with diagram ? 14

****