H **786A3** Total Pages: **2**

Register No.: .... Name: ....

SAINTGITS COLLEGE OF ENGINEERING (AUTONOMOUS)

(AFFILIATED TO APJ ABDUL KALAM TECHNOLOGICAL UNIVERSITY, THIRUVANANTHAPURAM)

FIFTH SEMESTER B.TECH DEGREE EXAMINATION (R), DECEMBER 2023
COMPUTER SCIENCE AND ENGINEERING
(2020 SCHEME)

Course Code : **20CST391**

Course Name: **Cryptographic Algorithms**

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

PART A

(Answer all questions. Each question carries 3 marks)

1. Use an exhaustive key search and decrypt the Caesar cipher “UVACLYFZLJBYL”.
2. Differentiate between passive and active attack.
3. Illustrate the key expansion procedure of IDEA algorithm.
4. Compare stream cipher and block cipher with suitable example.
5. In a public key system using RSA, you intercept the cipher text C=2 sent to a user whose public key is e=17, n=33. What is the plain text M?
6. Illustrate man in the middle attack on Diffie-Hellman key exchange algorithm.
7. Identify the various techniques used for distribution of public keys.
8. What are backup keys and compromised keys?
9. Compare the strength of MAC and hash functions.
10. Distinguish between HMAC and CMAC.

PART B

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

MODULE I

11. a) Using transposition cipher, encrypt the message "attack postponed until two a m" with the key "4312567". (4)

    b) Briefly discuss the security services and mechanisms provided by ITU-T. (10)

OR

12. a) Explain the different types of cryptanalytic attacks. (6)

    b) Use Playfair cipher with keyword “guidance” to encrypt the message “The key is hidden under the doorpad”. (8)

MODULE II

13. a) Explain the RC4 stream cipher. (6)

    b) With a neat sketch, explain single round in DES. (8)

OR

14. a) Explain the key expansion in AES algorithm. (6)

b) Describe the various block cipher modes of operation. (8)

MODULE III

15. a) Demonstrate the Elliptic curve encryption/decryption procedure. (6)

b) Illustrate knapsack cryptosystem. Explain how knapsack system is cracked. (8)

OR

16. a) Consider a Diffie Hellman scheme with a common prime $q = 11$ and primitive root $\alpha = 2$. If user A has public key $Y_A = 9$, what is A's private key? If user B has public key $Y_B = 3$, what is the shared secret key K shared with A? (6)

b) Briefly explain RSA cryptosystem. Prove that the RSA decryption indeed recovers the original plaintext. (8)

MODULE IV

17. a) Demonstrate how simple secret key distribution is prone to man in the middle attack. (5)

b) Explain the key distribution scenario in symmetric key distribution using symmetric encryption. (9)

OR

18. a) Discuss the core components of Public Key Infrastructure. (5)

b) Briefly explain the public-key distribution scenario. (9)

MODULE V

19. a) What are the security requirements for cryptographic hash functions? (6)

b) Demonstrate the working of SHA-512 with necessary diagram. (8)

OR

20. a) Explain X.509 authentication services. (6)

b) Describe MD-5 hash algorithm with a neat diagram. (8)

****