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

SAINTGITS COLLEGE OF ENGINEERING (AUTONOMOUS)

(AFFILIATED TO APJ ABDUL KALAM TECHNOLOGICAL UNIVERSITY, THIRUVANANTHAPURAM)

FIFTH SEMESTER B.TECH DEGREE EXAMINATION (Regular), DECEMBER 2022

(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. Differentiate between passive and active attack.
2. Encrypt the message "CRYPTOGRAPHY" using Playfair cipher with key COMPUTER.
3. How is round key generated in DES?
4. Compare stream cipher and block cipher with suitable example.
5. List out the elements of public key cryptosystem.
6. Define elliptic curve crypto system.
7. List ways in which secret keys can be distributed to two communicating parties.
8. What is the difference between a session key and a master key?
9. What is the difference between a message authentication code and a one-way hash function?
10. Give the requirements of MAC function.

PART B

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

MODULE I

11. a) Encrypt the message "we are discovered save yourself" using the following ciphers. Show the calculations. (6)
    i) Vigenère cipher with key= "deceptive".
    ii) Autokey system of Vigenère cipher with key=" deceptive".

    b) Define transposition technique. Explain various transposition technique with suitable examples. (8)

OR

12. a) Encrypt the text "this is an exercise and complete it" using transposition cipher with the key (3, 2, 1, 4, 5). Show decryption of the cipher text to recover the original text back. (6)

b) Define substitution techniques. Explain any four-substitution technique with suitable example. (8)

MODULE II

13. a) Explain the general structure of AES with the help of sketch. (7)

b) Differentiate between linear and differential cryptanalysis. (7)

OR

14. a) Summarize the primitive operations in RC4 algorithm. (7)

b) Differentiate Double DES and Triple DES with neat diagrams. (7)

MODULE III

15. a) Explain RSA cryptosystem. In RSA cryptosystem a participant A uses two prime numbers p=13 and q=17 to generate public key and private key. The public key of A is 35. Find the private key of A. (8)

b) Illustrate El-Gamal cryptosystem. (6)

OR

16. Consider a Diffie-Hellman scheme with a common prime q=11 and a primitive root ∞ = 2.

a) If User A has public key Y_A = 9, what is A's private key X_A ? (7)

b) If User A has public key Y_B = 3, what is the shared secret key shared with A? (7)

MODULE IV

17. a) Explain the four general categories of schemes for the distribution of public keys. (8)

b) Demonstrate how simple secret key distribution is prone to man in the middle attack. (6)

OR

18. a) Describe the following (6)

(i) Updating Keys

(ii) Compromised Keys.

b) Explain the components of Public Key Infrastructure. (8)

MODULE V

19. a) Explain Cipher-Based Message Authentication Code. (6)

b) Describe the working of SHA-512 with diagrams. (8)

OR

20. a) Describe the working of MD5 with diagrams. (8)

b) Define hash function and give the requirements and applications of hash function. (6)

****