H Roll No. .....

TCS–491

B. TECH. (CSE)
(FOURTH SEMESTER)
END SEMESTER
EXAMINATION, June, 2023

INTRODUCTION TO CRYPTOGRAPHY

Time : Three Hours

Maximum Marks : 100

Note : (i) All questions are compulsory.

(ii) Answer any *two* sub-questions among (a), (b) and (c) in each main question.

(iii) Total marks in each main question are **twenty**.

(iv) Each sub-question carries 10 marks.

1. (a) What do you mean by Brute Force attack in cryptography ? State the various ways of conducting Brute Force attack. State the various solutions to solve the problem of Brute force attack. (CO1)

P. T. O.

(b) What do you mean byX.800 security architecture ? Write about the various security services and mechanisms stated in the X.800 architecture. (CO1)

(c) Decrypt the sequence : "PQFVCKFUFB" using Playfair classical cipher using the key = 'PAYMENT". Write the appropriate steps for Decryption. (CO1)

2. (a) Calculate the values of round keysK1, K2 using S-DES symmetric algorithm. Given that the value of key K = 1111100000 and the values of P10 = {3, 5, 2, 7, 4, 10, 1, 9, 8, 6} and P8 = {6, 3, 7, 4, 8, 5, 10, 9}. Explain the steps involved and draw the block diagram. (CO2)

(b) State the importance of pseudo random number generators in a Stream Cipher. State the properties of a true random number. (CO2)

(c) State how modern block ciphers converts a plain text into cipher text with the help of suitable block diagrams. State how cryptographic strength is increased in a modern block cipher. (CO2)

3. (a) Calculate the values of the following using the Fermet's Theorem : (CO3)

(i) $2^{246} \bmod 11$

(ii) $2^{50} \bmod 17$

(iii) $13^{32} \bmod 17$

(iv) $13^{40} \bmod 17$

(b) Explain with suitable diagram the key distribution techniques available in symmetric key distribution in symmetric encryption. (CO3)

(c) Users A and B want to share a secret key 'K' using Diffie-Hellman key exchange protocol using a common prime q = 353, a primitive root α = 3, A's secret key X_A = 97 and B's secret key X_B = 233.

Compute (i) A's public key, Y_A (ii) B's public key, Y_B (iii) A's and B's common secret key, K. (CO3)

4. (a) Explain with the help of suitable block diagram how confidentiality and authentications achieved in message authentication using message encryption technique. (CO4)

(b) What do you mean by message authentication ? State how message authentication is implemented using Message Authentication Code (MAC). (CO4)

(c) Calculate the value of private and public key pair using RSA algorithm, given that p = 17; q = 13. Also show the encryption and decryption steps using the plain text value of M = 7. Write all the steps involved. (CO4)

5. (a) What do you mean by Email Security ? Explain how confidentiality, integrity and authentication is offered by PGP (Pretty Good Privacy). (CO5)

(b) Explain the following terms : (CO5)

(i) Intrusion Detection System (IDS)

(ii) Firewall

(iii) Distributed Denial of Service Attack (DDoS)

(iv) S/MIME

(c) Explain the following terms : (CO5)

(i) Rootkit

(ii) Phishing

(iii) Cryptojacking

(iv) Keystroke logging