MANIPAL INSTITUTE OF TECHNOLOGY
MANIPAL
(A constituent unit of MAHE, Manipal)

DEPARTMENT OF MECHATRONICS

VII SEMESTER B.TECH. (MECHATRONICS)

END SEMESTER (REGULAR) EXAMINATION

SUBJECT: Principles of Cryptography Subject Code: MTE 4058

Date: 02/12/2023

Time: 3 Hrs **Exam Time 2:30PM – 5:30PM** **MAX. MARKS: 50**

Name: ……, Registration No: ……..

Instructions for the Candidates:

- Answer **ALL** questions.
- Data did not provide any, may be suitably assumed.

Q. No.	Questions	M	CO	PO	LO	BL
1A	In DES algorithm, the 32-bit input to E/P (Expansion/Permutation) block and the 48-bit key input to XOR block in hexadecimal format are "c187f457" and "bc923fef20a7," respectively. Generate the E/P output and the XOR output of DES algorithm.	5	1	1	1	3
1B	In a Diffie-Hellman Key Exchange, Alice (Sender) and Bob (Receiver) have chosen prime value q = 11 and primitive root α = 2. If Alice's private key (X_A) is 4 and Bob's private key (X_B) is 7, then generate Alice's secret key K_A and Bob's secret key K_B.	3	3	2	2	3
1C	Develop a message authentication system that offers confidentiality and authenticity but no digital signature. Message authentication must be connected to the ciphertext.	2	4	3	5	6
2A	Generate the final ciphertext *'Y'* using the multiple-round columnar transposition technique when the plaintext *'X'* is "MANIPAL ACADEMY OF HIGHER EDUCATION THE INSTITUTE OF EMINENCE" and the keys *'K1'*, *'K2'*, and *'K3'* are (6 7 4 1 3 5 8 2), (5 1 4 6 3 8 2 7), and (3 1 5 2 8 6 4 7), respectively.	5	1	1	1	3
2B	Compare and contrast the importance of integrity and availability as security goals in critical infrastructure systems. Evaluate the potential consequences and impact of a compromise on each goal.	3	1	2	2	5
2C	Create "Addition Modulo 8," "Multiplication Modulo 8," and "Additive and Multiplicative Inverse Modulo 8" using Arithmetic Modulo 8 operations.	2	2	2	2	3
3A	Analyse how the different keying options in Triple DES impact its security. Discuss the strengths and potential weaknesses associated with using two or three keys in different patterns.	4	1	4	4	4
3B	Compare the CBC and CFB modes of operation. Analyse how they handle error propagation and discuss scenarios where one might be preferred over the other.	4	1	4	4	4

3C	Build a ciphertext using the Rail-Fence transposition technique when the plaintext is "IAMAGOODSTUDENTPLESELIKEME", and the key is 3.	2	1	1	1	3
4A	Propose a modification to the AES structure that enhances its security while maintaining compatibility with existing AES implementations. Justify your design choices.	4	2	3	5	6
4B	Find a solution to the problem 3^{808} *mod* 17 by utilizing Euler's theorem.	3	2	1	1	3
4C	Find a solution to the problem 3^{305} *mod* 7 by employing Fermat's theorem.	3	2	1	1	3
5A	Create a message authentication system that includes digital signatures, confidentiality, and authenticity. The intended authentication should be performed at the plaintext-tied authentication level using the SHA-512 hash algorithm.	4	4	3	5	6
5B	Design a message authentication system that includes authentication and a digital signature but does not include confidentiality. Include in the authentication procedure a mechanism that can internally control the problem, such as unreadable decrypted text. Message authentication can be accomplished using either the SHA hash technique or the MAC algorithm.	3	4	3	5	6
5C	Design a message authentication system that provides authentication but neither confidentiality nor digital signature. Message authentication should be conducted using the MAC algorithm, followed by encryption using the symmetric algorithm.	3	4	3	5	6