Reg. No.										

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

DEPARTMENT OF MECHATRONICS

VII SEMESTER B.TECH. (MECHATRONICS)

END SEMESTER EXAMINATIONS (PART-B), December 2021

SUBJECT: PRINCIPLES OF CRYPTOGRAPHY [MTE 4058]

(Date: December 27, 2021)

Time: 75 + 10 Minutes **MAX. MARKS: 20**

Instructions to Candidates:

- Answer **ALL** the questions.
- Missing data if any can be suitably assumed.

Q. No		M	CO	PO	LO	BL
Descriptive Type Questions (10 × 2 = 20)						
1A.	Generate a ciphertext by applying the Hill cipher technique when the plaintext = "SECURITY", and the key = $\begin{pmatrix} 9 & 4 \\ 5 & 7 \end{pmatrix}$.	**5**	**1**	**1**	**1**	**3**
1B.	Generate a ciphertext, when the plaintext = "MECHATRONICS", and the key = "SECTION", by utilizing the Playfair cipher technique.	**3**	**1**	**1**	**1**	**3**
1C.	Generate a ciphertext, when the plaintext = "IAMAGOODSTUDENT" and the encryption key = 'Z', by utilizing the Caesar cipher technique.	**2**	**1**	**1**	**1**	**3**
2A.	Solve $3^{302}\ mod\ 5005$ using CRT (Chinese Remainder Theorem) to build a number of libraries for computations on large numbers.	**5**	**2**	**2**	**2**	**3**
2B.	Consider a Diffie-Hellman scheme with a common prime of $q = 11$ and a primitive root of $\alpha = 2$. Show that 2 is a primitive root of 11. If user A has public key $Y_A = 9$, determine A's private key X_A. If user B has public key $Y_B = 3$, determine the shared secret key K with A.	**3**	**3**	**2**	**2**	**2, 3**
2C.	Design a cryptographic cipher (using hash functions) which provides Confidentiality, Authenticity, and also Digital Signature.	**2**	**4**	**3**	**3**	**6**