Reg. No.										

MANIPAL INSTITUTE OF TECHNOLOGY

MANIPAL

(A constituent unit of MAHE, Manipal)

SEVENTH SEMESTER BTECH. (E & C) DEGREE END SEMESTER EXAMINATION
DECEMBER 2021-JANUARY 2022
SUBJECT: CIPHER SYSTEM (ECE - 4069)

TIME: 75 minutes **MAX. MARKS: 20**

Instructions to candidates

- Answer **ALL** questions.
- Missing data may be suitably assumed.

Q. No.	Questions	Marks
1A.	Calculate the inverse of 12652 mod 13159. Show the steps.	3
1B.	Calculate the 191^{171} mod 311 using repeated squaring technique.	3
1C	In Merkle Hellman public cryptosystem, the public key is **(10, 305, 486, 16, 525)** and the private encryption key is **(57, 731)** Decrypt the cipher text "**RTKPQWAQSD**". Use **A to Z as 0 to 25** for plain text and Cipher text are digram	4
3C.	The input state given to mix column transformation in one of the encryption round of AES is $A = \begin{bmatrix} 51 & A6 & 20 & 18 \\ 6E & 87 & 32 & 20 \\ 12 & 6E & 23 & 81 \\ EF & 46 & F1 & 41 \end{bmatrix}$ Calculate the byte located in the **second row, second column** of the output state after mix column transformation.	2
4A.	Illustrate computation of function ***g* ( )** in **5th round AES** key expansion. Given 4th round key as $\begin{bmatrix} 51 & A6 & 20 & 18 \\ 6E & 87 & 32 & 20 \\ 12 & 6E & 23 & 81 \\ EF & 46 & F1 & 41 \end{bmatrix}$, Determine the **output word of g ( ).**	3
4B.	Detect the plain text observing the cipher text {**TAXDDOM-ƀ?C**} that was encrypted using digram **affine** cipher with keys **(324, 191).** The alphabet used is numbered as {A=0,B=1,….Z=25, . (dot)=26, ƀ (is Space)=27, ?=28}	5