Reg. No.										

MANIPAL INSTITUTE OF TECHNOLOGY

MANIPAL

(A constituent unit of MAHE, Manipal)

SEVENTH SEMESTER BTECH. (E & C) DEGREE

MAKE UP - END SEMESTER EXAMINATION FEBRUARY 2022

SUBJECT: CIPHER SYSTEM (ECE - 4069)

PART B

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

Instructions to candidates

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

Q. No.	Questions	M*	C*	A*	B*
1A	Compute $67^{115} \bmod 215$ using repeated squaring method. Show the computational steps.	3	1	1	4
1B	**Encrypt the message (11011011) using the S-DES with encryption key (1011001101).**	4	1	1	4
1C	Apply Merkle Hellman public cryptosystem, and decrypt the cipher text FNDAJJ knowing the public key is **(67,78, 55, 21, 110)** and the private encryption key is **(67, 123)**. Use **A to Z as 0 to 25** for plain text and Cipher text are di-gram	3	1	1	4
2A	Apply CRT and solve the equations, Show the computations $x \equiv 129 \pmod{211}$ $5x \equiv 3 \pmod{127}$	3			
2B.	Determine the entry in Row 2, column 3 in the output state of Mix Column transformation in AES, if the input state given to mix column transformation of 6^{th} encryption round $State\ Matrix\ A = \begin{bmatrix} EF & A6 & 46 & 18 \\ 6E & 87 & 87 & 20 \\ 21 & 6E & 6E & 32 \\ AC & 46 & A6 & 2A \end{bmatrix}$	2			
2C.	Alice and Bob use Elliptic curve Elgamal cryptosystem $\mathbf{E_{67}}$ **(2,3)**. Bob declares his public key **[e1= (2, 22), e2= (13, 45)].** Calculate the encrypted text for the plain text P (13, 22), that Alice sends to Bob, using her private key as 2.	5			