BIRLA INSTITUTE OF TECHNOLOGY, MESRA, RANCHI
(MID SEMESTER EXAMINATION)

CLASS: B.TECH. **SEMESTER: V**
BRANCH: CSE/IT **SESSION: MO/2022**

SUBJECT: IT330 CRYPTOGRAPHY AND NETWORK SECURITY

TIME: 2 HOURS **FULL MARKS: 25**

INSTRUCTIONS:
1. The total marks of the questions are 25.
2. Candidates attempt for all 25 marks.
3. Before attempting the question paper, be sure that you have got the correct question paper.
4. The missing data, if any, may be assumed suitably.
5. Tables/Data hand book/Graph paper etc. to be supplied to the candidates in the examination hall.

				CO	BL
Q1	(a)	Differentiate between symmetric cryptography and asymmetric cryptography.	[2]	CO1	2
Q1	(b)	Explain the security requirement CIA (Confidentiality, Integrity and Availability) triad in details.	[3]	CO1	1
Q2	(a)	Differentiate between stream cipher and block cipher.	[2]	CO2	2
Q2	(b)	Consider Plaintext="Algorithm" and Key="Playfair". Using Playfair Cryptographic Algorithm, compute Cyphertext.	[3]	CO3	3
Q3	(a)	Explain Euclidean Algorithm with the help of an example.	[2]	CO2	2
Q3	(b)	With the help of a diagram explain DES encryption algorithm	[3]	CO3	2
Q4	(a)	For GF(5^2) find finite field Z_5^2.	[2]	CO3	3
Q4	(b)	Find out additive inverse and multiplicative inverse for GF(2^3).	[3]	CO3	3
Q5	(a)	Define Euler's Totient Function and Euler's Theorem.	[2]	CO2	1
Q5	(b)	Find out the public key and private key using RSA algorithm for the following problem: Two prime numbers are p=11 and q=13. Select other values suitably, if required.	[3]	CO4	4

:::::: 01/10/2022 ::::::M