BIRLA INSTITUTE OF TECHNOLOGY, MESRA, RANCHI
(MID SEMESTER EXAMINATION MO2023)

CLASS: BTECH **SEMESTER: MO/2023**
BRANCH: CSE **SESSION: MORNING**

SUBJECT: IT349 CRYPTOGRAPHY AND NETWORK SECURITY

TIME: 02 Hours **FULL MARKS: 25**

INSTRUCTIONS:
1. The question paper contains 5 questions each of 5 marks and total 25 marks.
2. Attempt all questions.
3. The missing data, if any, may be assumed suitably.
***4*. Tables/Data handbook/Graph paper etc., if applicable, will be supplied to the candidates**

			CO	BL
Q.1	What do you mean by Cryptography? Explain the goals of Cryptography.	[5]	CO1	2
Q.2	Use the Playfair cipher to encipher the message "The key is hidden under the door Pad." The secret key can be made by filling the first and part of the second row with the word "GUIDANCE" and filling the rest of the matrix with the rest of the alphabet.	[5]	CO2	3
Q.3	Explain the concept of Groups and Fields. What do you mean by Galois Field. For the group G = $<Z_{6^*}, \times>$: a. Prove that it is an abelian group. b. Show the result of 5×1 and $1 \div 5$. c. Show that why we should not worry about division by zero in this group	[5]	CO1	3
Q.4	Find the multiplicative inverse of each of the following integers in Z_{180} using the Extended Euclidean algorithm. a. 38 b. 7 c. 132	[5]	CO1	3
Q.5	John is reading a mystery book involving cryptography. In one part of the book, the author gives a ciphertext "CIW" and two paragraphs later the author tells the reader that this is an additive cipher and the plaintext is "yes". In the next chapter, the hero found a tablet in a cave with "XVIEWVWI" engraved on it. John immediately found the actual meaning of the ciphertext. What type of attack did John launch here? What is the plaintext?	[5]	CO2	4

:::::27/09/2023 M:::::