BIRLA INSTITUTE OF TECHNOLOGY, MESRA, RANCHI
(MID SEMESTER EXAMINATION SP/2025)

CLASS: BTECH **SEMESTER : VI**
BRANCH: CSE **SESSION : SP/2025**

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(a)	Explain the network security model and its important parameters with a neat block diagram.	[2]	CO2	2
Q.1(b)	Describe the encryption process of the Row Transposition Cipher. Explain how the key is used to reorder plaintext into ciphertext and provide a step-by-step example to illustrate the method.	[3]	CO3	3
Q.2(a)	Distinguish between active and passive attacks with a pictorial representation. Also provide some examples for each type of attack.	[2]	CO2	2,4
Q.2(b)	Use a Hill cipher to encipher the message "We live in an insecure world". Use the following key: K = $\begin{pmatrix} 03 & 02 \\ 05 & 07 \end{pmatrix}$	[3]	CO1	2,3
Q.3(a)	Define a ring and distinguish between a ring and a commutative ring.	[2]	CO1	1,2
Q.3(b)	Find the results of the following, using Fermat's little theorem: (i) 5^15 mod 13 (ii) 15^18 mod 17	[3]	CO2	2,4
Q.4(a)	What is a finite field of the form GF(2^n)? Explain its structure and how elements are represented.	[2]	CO2	2
Q.4(b)	Explain the working mechanism of the Playfair cipher, including the process of encryption with a given key matrix. Provide an example to illustrate the steps involved.	[3]	CO3	3
Q.5(a)	Find GCD(1970, 1066) using Euclid's algorithm.	[2]	CO2	2
Q.5(b)	What is the Chinese Remainder Theorem (CRT), and how does it help in solving simultaneous modular equations? Explain with an example.	[3]	CO3	3

::::::28/02/2025::::::E