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

CLASS: BTECH **SEMESTER : VI**
BRANCH: ECE/EEE/CE/MECH **SESSION : SP/2025**

SUBJECT: IT363 CRYPTOGRAPHY & 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 security requirement CIA (Confidentiality, Integrity and Availability) triad in details.	[2]	1	1
Q.1(b)	Briefly explain the active and passive attacks with suitable examples and differentiate between them.	[3]	2	4
Q.2(a)	Explain Playfair cryptographic algorithm and encrypt the message: "THE EMEMY ATTACKS IN THE DAY" using key as "JOCKER".	[2]	4	2
Q.2(b)	Use the Playfair cipher to encrypt the message "THE SUN SETS IN THE WEST" The secret key word is "UPDATE".	[3]	4	3
Q.3(a)	Explain Euclidean Algorithm and use it to determine gcd (2470,1760).	[2]	3	2
Q.3(b)	Calculate the multiplicative inverse of each of the following integers using the Extended Euclidean algorithm. a. 23 in Z_{100} b. 11 in Z_{26} c. 132 in Z_{180}	[3]	3	3
Q.4(a)	What is Euler's Totient Function. Find the value of $\Phi(1000)$.	[2]	1	1
Q.4(b)	Using Chinese remainder theorem solve the following equations. $X \equiv 2 \pmod 3$ $X \equiv 3 \pmod 5$ $X \equiv 2 \pmod 7$	[3]	1	3
Q.5(a)	Explain what Symmetric key and Asymmetric key encryptions are and the differences between them.	[2]	2	4
Q.5(b)	Generate the elements of the field $GF(2^3)$ using the irreducible polynomial $f(x)= x^3+x+1$	[3]	5	6

::::::04/03/2025::::::E