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

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

SUBJECT: IT349 CRYPTOGRAPHY AND NETWORK SECURITY

TIME: 3 Hours **FULL MARKS: 50**

INSTRUCTIONS:
1. The question paper contains 5 questions each of 10 marks and total 50 marks.
2. Attempt all questions.
3. The missing data, if any, may be assumed suitably.
***4*. Before attempting the question paper, be sure that you have got the correct question paper.**
5. Tables/Data hand book/Graph paper etc. to be supplied to the candidates in the examination hall.

			CO	BL
Q.1(a)	Illustrate the model for network security and explain each of its components.	[5]	CO1	2
Q.1(b)	Discuss the rules for encryption using the Playfair cipher. Given the following matrix:	[5]	CO1	3

J/K	C	D	E	F
U	N	P	Q	S
Z	V	W	X	Y
R	A	L	G	O
B	I	T	H	M

Encrypt the message "I only regret that I have but one life to give for my country."

Q.2(a)	Differentiate between GF(p) and GF(2^n). Explain how finite fields are constructed.	[5]	CO2	4
Q.2(b)	Prove the Following	[5]	CO2	5
	(i) If 'p' is a prime and 'a' is a positive integer relatively prime to 'p', then $a^{p-1} \equiv 1 \pmod p$			
	(ii) If 'p' is a prime and 'a' is a positive integer, then $a^p \equiv a \pmod p$.			
Q.3(a)	Explain the working of the DES algorithm, including its key structure and encryption process.	[5]	CO3	2
Q.3(b)	Explain the working principle of Elliptic Curve Cryptography (ECC) encryption and decryption process.	[5]	CO3	2
Q.4(a)	Elaborate on how secure electronic transaction (SET) protocol enable e-transactions securely. Explain the different components involved.	[5]	CO4	2
Q.4(b)	Elaborate the four protocols used in SSL and highlight the interactions between them.	[5]	CO4	4
Q.5(a)	What is a firewall and why is it needed? Differentiate between the various types of firewalls briefly. Also explain the working principles of Firewalls	[5]	CO5	4
Q.5(b)	Write a short note on Buffer Overflow Attack and Malicious Program	[5]	CO5	1

::::::30/04/2025::::::M