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

CLASS: MTech/Pre-PhD **SEMESTER: I**
BRANCH: CSE **SESSION: MO/2025**

SUBJECT: CS541 APPLIED CRYPTOGRAPHY

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)	What do you understand by network security attack? Describe active and passive security attack.	[5]	CO1	2
Q.1(b)	What is zero-knowledge proof, and how does it ensure that no additional information is revealed during the proof process?	[5]	CO1	2
Q.2(a)	Explain Diffie-Hellman Algorithm with an example	[5]	CO2	3
Q.2(b)	Solve the following sets of simultaneous congruences: $x = 5 \pmod{11}$, $x = 14 \pmod{29}$, $x = 15 \pmod{31}$	[5]	CO2	3
Q.3(a)	State and proof Euler's theorem, and how does it relate to Fermat's little theorem?	[5]	CO3	1
Q.3(b)	Discuss RSA with computations for public key cryptography. Also perform the encryption and decryption for $p = 7$, $q = 11$, $e = 17$ and $m = 8$.	[5]	CO3	3
Q.4(a)	How be a threshold cryptosystem used to create a trusted setup? How to relate threshold cryptosystem with signature schemes?	[5]	CO4	2
Q.4(b)	Explain the steps involved in Digital Certificate. How can we verify a Digital Certificate?	[5]	CO4	2
Q.5(a)	What do you mean by Public Key Cryptography Standards (PKCS)? Explain with the help of an example.	[5]	CO5	2
Q.5(b)	Write short notes on any two of the followings: i. Lightweight Cryptography ii. Quantum Computing iii. Cryptocurrencies	[5]	CO5	1

:::::24/11/2025:::::E