Course Code: **CSL602**	Course Name: **Cryptography & System Security Lab**	
Class: **TE (CSE-AIML)**	Semester:**VI (CBCS)**	Academic year: **2024-25**
Roll No: 29	Name of Student: GiriPrasath K	
Practical No: 03	Quiz Score: 4	

Title : Implementation of Diffie Hellman Key Exchange algorithm.

Lab Objective applicable: LOB1: To be able to analyze and implement public key algorithms.

Lab Outcome applicable: LO2: Analyze and implement public key algorithms.

Practical applications of the assignment/experiment:- Implement Diffie Hellman Key exchange algorithm.

Details of Quiz:

Q. No.	Question	Correct Answer	Given Answer
1	Diffie-Hellman algorithm is widely known as_____	both a and b	both a and b
2	How many bytes of the secret key is generated using Diffie-Hellman encryption/decryption scheme?	256	256
3	Which key is used in Diffie Hellman algorithm?	private-public key pair	private-public key pair
4	Is Diffie Hellman key exchange symmetric or asymmetric?	Assymetric	Assymetric
5	The man-in-the-middle attack can endanger the security of the Diffie-Hellman method if two parties are not	authenticated	authenticated
6	Because the users share a common secret key S, the Diffie-Hellman scheme is an example of an asymmetric key exchange protocol. True/False	True	False

Assignment/Experiment Evaluation:

Sr. No.	Parameters	Marks Obtained	Out of
1	Technical Understanding (Assessment based on Q and A through online quiz)	4	6
2	Neatness/Presentation		2
3	Punctuality		2
Date of Execution (DOE)	/2025	Total Marks Obtained	10
Date of Assessment (DOA)	/2025	Signature of Teacher	