Aldel Education Trust's

St. John College of Engineering and Management, Palghar

(A Christian Religious Minority Institution)

Approved by AICTE and DTE, Affiliated to University of Mumbai/MSBTE

St. John Technical Campus, Vevoor, Manor Road, Palghar (E), Dist. Palghar, Maharashtra-401404

NAAC Accredited with Grade 'A'

DEPARTMENT OF COMPUTER ENGINEERING

Lab code: CSL602 **Class:** T.E./COMP/A2 & A3

Course name: Cryptography & System Security Lab

EXPERIMENT 3

Aim: Implementation of Diffie Hellman Key exchange algorithm [LO2].

Theory:

Following points have to be included:

1. What is symmetric key cryptography?
2. Block diagram of Diffie–Hellman key exchange algorithm
3. Description of Diffie–Hellman key exchange algorithm
4. Theoretically solve Diffie–Hellman key exchange algorithm ***[theoretical result and code attached should match]***.

Implementation:

Students are required to implement the logic in Java or Python.

Conclusion:

The famous key exchange algorithm, i.e., Diffie–Hellman key exchange algorithm/agreement algorithm is studied and implemented, which is used to establish a shared secret between two parties (i.e., Alice and Bob).

References: Mention your references here.

Viva Questions:

1. Explain the working of Diffie–Hellman key exchange algorithm.
2. Why is Diffie–Hellman key exchange algorithm called an agreement algorithm?
3. What is a primitive root?

Faculty In-charge:

Mr. Vivian Lobo