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 1

Aim: Design and Implementation of a product cipher using Substitution *(Caesar/Additive/Shift Cipher | Multiplicative Cipher | Affine Cipher)* and Transposition *(Rail fence Cipher)* ciphers [LO1].

Theory:

Following points have to be included:

1. Explain cryptography.
2. Explain the basis of classification of cryptography.
3. Explain substitution cipher technique (Caesar, multiplicative, and Affine) with an example ***[theoretical result and code attached should match]***.
4. Explain transposition cipher technique (rail fence) with an example ***[theoretical result and code attached should match]***.

Implementation:

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

Conclusion:

The basic features of substitution and transposition cipher techniques are studied through this experiment. The features of transposition cipher and its basic differences from substitution cipher are studied.

References: Mention your references here.

Viva Questions:

1. Encrypt a given message using substitution technique.
2. Encrypt a given message using transposition technique.
3. Differentiate between symmetric key and asymmetric key cryptography.

Faculty In-charge:

Mr. Vivian Lobo