

FR. CONCEICAO RODRIGUES COLLEGE OF ENGINEERING
Department of Computer Engineering

1. Course , Subject & Experiment Details

Academic Year	2017-18	Estimated Time	03 - Hours
Course & Semester	B.E. (CMPN)- Sem VII	Subject Name & Code	CSS - (CPC702)
Chapter No.	02 – Mapped to CO- 1	Chapter Title	Basics of Cryptography

Practical No:	1
Title:	To study and implement different types of substitution ciphers.
Date of Performance:	
Date of Submission:	
Roll No:	7371
Name of the Student:	Flavion D'sa

Evaluation:

Sr. No	Rubric	Grade
1	On time submission Or completion (2)	
2	Preparedness(2)	
3	Skill (4)	
4	Output (2)	

Signature of the Teacher:

Date:

Practical & Real-Time Application

- Encryption and decryption of stream cipher

Conclusion:

The program was tested for different sets of inputs.

Program is working SATISFACTORY NOT SATISFACTORY
(Tick appropriate outcome)

Post Lab :

1. Explain why Modular arithmetic has been used in cryptography.
2. To break the Caesar cipher using brute force attack, how many attempts are needed?
3. Compare Substitution and Transposition techniques.