

Name: Yash . Lalit . Sharman
UID: 2023300220
CNS EXP 2

Page No.

Date / /

Aim:- Experiment on Symmetric Ciphers

Problem Definition :- To implement all substitution encryption technique namely Caesar , Monoalphabetic , Playfair, Hill & Polyalphabetic ciphers.

Then perform brute force attack on encryption techniques.

Theory :-

In Network Security Model, encryption and decryption play important role of sending message so that others cannot see them. When encryption and decryption is performed by the same key it is called symmetric cryptosystem. There is class of symmetric encryption cryptosystem where each letter of plain text is substituted to another letter is called as substitution encryption techniques.

My learnings:-

Through this lab , my understanding of diff. substitution & brute force attack technique got increased.