# Experiment 9: Mono-alphabetic Substitution Cipher using TCP Sockets

**Aim:** To use TCP Sockets to implement mono-alphabetic substitution ciphers

**Objective:** After carrying out this experiment, students will be able to:

* Apply mono-alphabetic substitution cipher techniques to encrypt and decrypt text messages

**Problem statement:** You are required to write programs for a TCP client-server system that performs simple encryption and decryption using mono-alphabetic substitution ciphers. The client should first authenticate a user using a pre-defined password. Then the client (user) sends a message to the server. The server will encrypt the message using mono-alphabetic substitution cipher and store it in a file. Subsequently, when a user asks for the message he has entered previously, the message should be decrypted and transmitted back to the client.

**Analysis:** While analyzing your program, you are required to address the following points:

* Difference between alphanumeric and mono-alphabetic substitution ciphers.
* What are the vulnerabilities of mono-alphabetic substitution ciphers?

**MARKS DISTRIBUTION**

|  |  |  |
| --- | --- | --- |
| **Component** | **Maximum Marks** | **Marks Obtained** |
| Preparation of Document | 7 |  |
| Results | 7 |  |
| Viva | 6 |  |
| **Total** | **20** |  |

Submitted by:

Register No:

1. Algorithm/Flowchart
2. Program
3. Results
4. Analysis and Discussions
5. Conclusions
6. Comments
   1. Limitations of the experiment
   2. Limitations of the results obtained
   3. Learning
   4. Recommendations