Abstract: Building a Client-Server Application with Caesar Cipher Encryption

The **Caesar cipher** is a simple yet effective encryption technique that has been used for centuries to secure messages. In this project, we develop a client-server application that allows secure communication between a client and a server by encrypting messages using the Caesar cipher.

Objectives:

1. **Secure Communication**: Our goal is to establish a secure channel for exchanging messages between a client and a server over an untrusted network.
2. **Encryption**: We implement the Caesar cipher algorithm to transform plaintext messages into ciphertext. The Caesar cipher involves shifting each letter in the message by a fixed key (the "shift value").
3. **Decryption**: The server can decrypt received ciphertext back to plaintext using the same key.

Implementation Details:

- **Client-Side**:
  - The client initiates communication with the server.
  - User input (plaintext) is encrypted using the Caesar cipher.
  - The encrypted message is sent to the server.
- **Server-Side**:
  - The server receives the ciphertext from the client.
  - The server decrypts the ciphertext using the shared key.
  - The decrypted message is displayed or processed as needed.

Key Features:

- **Key Management**: The client and server share a secret key (the shift value) for encryption and decryption.
- **Robustness**: We handle edge cases such as non-alphabetic characters and wraparound (e.g., shifting 'z' by 1 results in 'a').
- **Network Communication**: We use sockets or APIs for communication between the client and server.

Conclusion:

By implementing the Caesar cipher in our client-server application, we achieve a basic level of message security. However, we acknowledge that the Caesar cipher is vulnerable to brute-force attacks due to its limited key space. Future work could explore more robust encryption methods.

Team members:

Y Guru Prerana Reddy – BU21CSEN0100831

K Shirisha – BU21CSEN0100833

M Bhanuprakash Reddy –BU21CSEN0102032

Thota Tarun Reddy – BU21CSEN0100811