Programming Project

1. Description

In this project, you will add one more cryptographic algorithm, DES, in the program implemented for Project 1. The program simulates the communication between Client and Server using shift cipher and DES, and works as follows:

1) Client connects to the Server using a socket.
2) Upon a successful connection, Server sends two options (1. Shift cipher and 2. DES) to Client so that the client can choose one of them for future communication.
3) If Client chooses "Shift cipher", then the programs should process shift encryption.In this case, the program takes a set of letters as a string transmitted to the Server.
4) If Client chooses "DES", it must follow the steps below.
5) Client program reads a file (in plain text format; .txt) consisting of several lines of hexadecimal numbers. The length of each line will be a multiple of 64 in binary, such as 64, 128, 192, …)
   0000000000000000
   211ACB937827FC63 783920AB3DE82938
   9283028BC233A3CC
   2938A783CAD3EF29 BCDF2039482029A3
   32918ACDEC9C37AD 1129283113131239
   ……
6) After reading each line from the file, the Client encrypts each block of 64 bits by using DES; please refer to https://en.wikipedia.org/wiki/DES_supplementary_material for IP, IP^{-1}, E, P, PC-1, PC-2 and S-boxes. You can simply hard-code these in your program.
7) After encrypting the plaintext (lines from the file), the Client transmits the data out to the Server through socket.
8) For encryption and decryption, we assume that $C30950FA36CF58CF_{(16)}$ in hexadecimal number is used as a shared key.
9) When Sever receives ciphertext, each block of 64 bits in the ciphertext is decrypted by using DES.
10) For each message, server also sends acknowledgement message to the Client.
11) Client and Server display plaintext and ciphertext before it transmits ciphertext out through the socket.
12) Client and Server display ciphertext and plaintext after it receives ciphertext through the socket and decrypts it.