# Lab 1: Implementation and Application of DES

Although DES has been proved to be insecure and obsolete, it is still a good material for study and research since the DES algorithm exploits the Feistel block cipher structure that many modern symmetric ciphers are based on. Its enhanced version 3-DES is still widely used by industry and government. In this lab, we implement the basic version, DES.

## Task

This is an **individual** work. Firstly, you need to generate a key and store it in a file (e.g., txt file). Then a simple chat program (socket programing) should be created to exchange messages between a Server ***S*** and a Client ***C***. Once the connection between ***S*** and ***C*** is successfully established, we can start exchanging messages. The client ***C*** uses DES algorithm to encrypt a message and sends the corresponding ciphertext to the server ***S***. The server ***S*** decrypts the received ciphertext to obtain the plaintext. Then the server ***S*** encrypts a new message and sends it back to the client ***C***. The client ***C*** receives the message from ***S*** and decrypts the received ciphertext to get the new message.

## Steps

1. ***S*** and ***C*** should share a symmetric key for DES. Suppose ***C*** generates the key for DES and dumps the key to a file. Since we run the server and the client on the same computer here, we simply assume the server ***S*** has access to the key file.

2. ***S*** and ***C*** set up a simple chat program. (Socket)

3. ***S*** and ***C*** both load DES key from the key file on startup of their programs.

4. ***S*** and ***C*** exchange messages. The messages should be entered by you through keyboard in the console, **NOT** by hardcoding. All messages are encrypted before being sent.

5. The programs on both sides should display *the shared key, the plaintext message to be sent, the ciphertext after encryption, the received ciphertext, and the plaintext after decryption*.

## Submission

Submit a lab.zip to Canvas including two parts:

a) All the code you have for completing the task.

b) What you have learned about this lab.

c) Steps of your work (e.g., the language and library you used, problems you encountered and how you solved them, etc.). Screen captures are recommended.