# Lab 1: Implementation and Application of DES

Although DES has been proved to be insecure and obsolete, it's 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

Two students in a group. One student A generates a key. Use DES algorithm to encrypt a message, send ciphertext to student B. Student B decrypts the ciphertext and get the plaintext. Then student B encrypts and sends a message to student A. Student A decrypts the message.

## Steps

1. A and B should share a symmetric key for DES. Suppose A generates the key for DES.
    a) A generates a key for DES and dumps the key to a file;
    b) A sends the key file to B via an offline channel, e.g., email.
2. A and B set up a simple chat program. (Socket)
3. A and B both load DES key from the shared key file on startup of their programs.
4. A and B exchange messages. The messages should be entered by you in the console/graphical UI, NOT by hardcoding. 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.

## Languages and Libraries

No restriction. Pick up whatever you are familiar with.

## Submission

Demo your program to the TA (70);

Submit a lab report via email with the subject "cis3319 lab1-<your name>", including two parts: 1. what you have learned about DES (10); 2. steps of your work (e.g., the language and library you used, code and comment, problems you encountered and how you solved them, etc.) Screen captures is recommended (20).

## Due

Demo: 5pm on Feb. 7

Report: 5pm on Feb. 14