Part 2 – Nguyễn Thị Thu Hà - 1411010

**Ngôn ngữ sử dụng**: C#

**Các hàm/phương thức trong chương trình**:

* File BinAndDec.cs gồm hai phương thức:

+ DecToBinArr với đầu vào là một số chuyển sang dãy int gồm các ký tự bit 0 và 1

+ BinToDec đầu vào là dãy bit chuyển thành số tự nhiên

* En-De-cryptions.cs có các phương thức chính để thực hiện mã hóa hoặc giải mã

+ InitialPermutation là hàm IP tương ứng trong S-Des

+ functionFk đầu vào là dãy bit cùng hai khóa được tạo từ KeyGeneration

+ switchSW hàm hoán đổi

+ InverseInitialPermutation IP-1 trong SDES

+ encrypt để mã hóa hoặc giả mã nếu đầu vào 2 khóa thích hợp

* KeyGeneration.cs gồm 4 hàm chính để tạo khóa

+ permutationP10 hàm P10 trong SDES

+ leftshiftLS1 xoay vòng trái 5 bit

+ permutationP8 hàm P8 trong SDES

+ leftshiftLS2 dịch vòng trái hai bit

* Chương trình chính Form1.cs

**Hướng dẫn cài**

* Chạy file setup.exe sau đó chọn Install, khi chương trình cài đặt xong chạy file S-DES.application

**Hướng dẫn sử dụng**:

* Đầu vào của dữ liệu dạng text, đầu ra của dữ liệu dạng bit đối với việc encryption
* Đầu vào của dữ liệu dạng bit, đầu ra của dữ liệu dạng text đối với việc decryption
* Chọn mode tương ứng decryption hoặc encryption -> bước thứ 2 nhập key -> bước 3 nhập file bằng cách ấn vào file input, chọn file cần giải mã -> bước thứ 4 chọn button dưới cùng để hiện thực.
* Sau khi mã hóa và giải mã quá trình thực hiện được.

**Đã làm được**: dữ liệu được mã hóa SDES đúng giải thuật,

**Chưa làm được**:

* Chưa sử dụng được mode CBC
* Đối với dữ liệu dạng bit trong việc decryption, nếu đầu vào không phải bội số cho 8 thì bị lỗi khi chạy chương trình.
* Chưa đổi được dãy ciphertext bit cuối cùng sang dạng text, các kí tự còn ở dạng bit thô.
* Giải mã cần có key thích hợp.