TRƯỜNG ĐẠI HỌC BÁCH KHOA TP.HỒ CHÍ MINH
KHOA KHOA HỌC KỸ THUẬT VÀ MÁY TÍNH

*

tháng

LAB 1

MÔN: *MẬT MÃ VÀ AN NINH MẠNG*

Simplified-DES

Sinh Viên Thực Hiện : **TRẦN VĂN LẮM**

MSSV: **51201830**

Nhóm: **A03-**

Giáo Viên Hướng Dẫn: **NGUYỄN NHẬT NAM**

TP.HỒ CHÍ MINH, tháng 9 năm 2015

I. NGÔN NGỮ SỬ DỤNG:

Ngôn ngữ : C++

II. CÁC HÀM VÀ PHƯƠNG THỨC SỬ DỤNG TRONG CHƯƠNG TRÌNH:

`char_to_int(char _ch)&& in_to_char(int num)`: Hàm chuyển ký tự thành số và ngược lại.

`decimal2binstr(int num)&& binstr2decimal(string binstr)` : hàm chuyển số thập phân thành số nhị phân và ngược lại.

`derive_key()`: hàm tự động sinh key.

`sconvert(const char *pCh, int arraySize)`: hàm chuyển ký tự thành chuỗi.

`circular_left_shift(string input_1, string input_2)` : hàm dịch trái 1bit.

`Xor(char a, char b)`: Hàm xor.

`P10(string input) && P8(string input) && P4(string input) && IP(string input) && R_IP(string input) && EP(string input_1, string input_2) && Ex_Xor(string input_1, string input_2) && S_Boxs(string input_1, string input_2) && Swith(string input) && FK(string input, string key)` : là các hàm của giải thuật S-DES.

`encrypt(string key)`: hàm mã hóa plaintext từ file plaintext.txt thành ciphertext chứa trong file result_ciphertext.txt.

`decrypt(string key)`: hàm giải mã ciphertext từ file result_ciphertext.txt ra plaintext chứa trong file plaintext_1.txt

III. HƯỚNG DẪN CÀI ĐẶT VÀ CHẠY CHƯƠNG TRÌNH:

Bước 1: Mở file Lab 1.exe

Bước 2: Nhập đoạn text cần mã hóa vào file plaintext.txt

Bước 3: Ở giao diện consoles : Nhấn 1 để sinh key tự động và tiến trình mã hóa và giải mã bắt đầu.

Nhấn 2 để nhập key (key có chiều dài 10bit), enter để quá trình mã hóa và giải mã bắt đầu.