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

———————————— * ————————————

BÁO CÁO LAB-1
S-DES

MÔN HỌC : MẬT MÃ VÀ AN NINH MẠNG

SINH VIÊN THỰC HIỆN :	NGUYỄN HỒNG PHƯỚC.
MSSV :	51202890.
NHÓM :	A01.
GIÁO VIÊN HƯỚNG DẪN :	Nguyễn Hữu Hiếu.

TP.HỒ CHÍ MINH, tháng 9 năm 2016.

I.NGÔN NGỮ SỬ DỤNG.

- Ngôn ngữ c++.

II.CÁC HÀM VÀ PHƯƠNG THỨC SỬ DỤNG.

① **void readFile(*string* &input, const char* nameFile)**: Đọc file và lưu dữ liệu vào biến input.

② **void wirteFile(*string* input,const char* nameFile)**: Ghi dữ liệu vào file.

③ ***string* xor(*string* a, *string* b)**: XOR hai chuỗi bit bằng nhau về độ dài.

④ **void keyGeneration(*string* key,*string* &k1,*string* &k2)**: Hàm sinh khóa k1 và k2 từ key đầu vào.

⑤ ***string* En_DeCryption(*string* k1,*string* k2, *string* &P)**: Hàm mã hóa (hoặc giải mã nếu đổi vị trí k1 thành k2 và ngược lại) một chuỗi nhị phân P với độ dài 8bit.

⑥ ***string* ECBEncryption(*string* k1, *string* k2, *string* input)**: Hàm mã hóa cho mô hình ECB.

⑦ ***string* ECBDecryption(*string* k1, *string* k2, *string* input)**: Hàm giải mã cho mô hình ECB.

⑧ **void CBCEncryption(*string* IV, *string* &input, *string* k1, *string* k2, *string* key)**: Hàm mã hóa cho mô hình CBC.

⑨ **void CBCDecryption(*string* IV, *string* &input, *string* k1, *string* k2, *string* key)**: Hàm gải mã cho mô hình CBC.

⑩ ***string* P10(*string* input), *string* P8(*string* input), *string* P4(*string* input),*string* IP(*string* input),*string* IP1(*string* input),*string* EP(*string* input)**: là các hàm phục vụ cho quá trình mã hóa và giải mã của giải thuật S-DES.

⑪ ***string* convertStringToBinary(*string* input)**: chuyển đổi chuỗi ký tự thành chuỗi bit.

⑫ **void convertBinarytoString(*string* &data)**: chuyển đổi chuỗi bit thành chuỗi ký tự.

III. MÔ HÌNH MÃ HÓA ĐƯỢC CHỌN.

Cả hai mô hình ECB (Electronic code book) và CBC (Cipher Block Chaining).

IV. HƯỚNG DẪN CÀI ĐẶT VÀ CHẠY CHƯƠNG TRÌNH.

Bước 1: Mở file **Lab1.exe** trong thư mục **"EXE File"**.

Bước 2: Nhập đoạn text cần mã hóa vào file **plaintext.txt** hoặc nếu giải mã nhập chuỗi nhị phân vào file **result_ciphertext.txt**

Bước 3: Ở giao diện consoles : nhấn 1 chọn **ENCRYPTION** hoặc nhấn 2 chọn **DECRYPTION,**sau đó tiếp tục nhấn 1 chọn mô hình **CBC** hoặc nhấn 2 chọn mô hình **ECB.**

Bước 4: Kiểm tra kết quả .