/\*

Anudish Jinturkar

H-27

Subject: Network Security (Lab)

Lab5: Implementation of S-RC4 algorithm

\*/

#include <bits/stdc++.h>

#define gc getchar\_unlocked

using namespace std;

void rc4(unsigned char \* ByteInput, unsigned char \* pwd, unsigned char \* &ByteOutput)

{

unsigned char \* temp;

int i,j=0,t,tmp,tmp2,s[256], k[256];

for (tmp=0;tmp<256;tmp++)

{

s[tmp]=tmp;

k[tmp]=pwd[(tmp % strlen((char \*)pwd))];

}

for (i=0;i<256;i++)

{

j = (j + s[i] + k[i]) % 256;

tmp=s[i];

s[i]=s[j];

s[j]=tmp;

}

temp = new unsigned char [ (int)strlen((char \*)ByteInput) + 1 ] ;

i=j=0;

for (tmp=0;tmp<(int)strlen((char \*)ByteInput);tmp++)

{

i = (i + 1) % 256;

j = (j + s[i]) % 256;

tmp2=s[i];

s[i]=s[j];

s[j]=tmp2;

t = (s[i] + s[j]) % 256;

if (s[t]==ByteInput[tmp])

temp[tmp]=ByteInput[tmp];

else

temp[tmp]=s[t]^ByteInput[tmp];

}

temp[tmp]='\0';

ByteOutput=temp;

}

int main(int argc, char\*\* argv)

{

unsigned char \* message;

unsigned char \* pwd;

unsigned char \* encrypted;

unsigned char \* decrypted;

message = (unsigned char \*)malloc(sizeof(char)\*100);

pwd = (unsigned char \*)malloc(sizeof(char)\*100);

cout<<"Enter the plain text"<<endl;

cin>>message;

cout<<"Enter the key"<<endl;

cin>>pwd;

cout<<endl;

rc4(message,pwd,encrypted);

rc4(encrypted,pwd,decrypted);

cout<<"Plain text is: "<<message<<endl;

cout<<"Key is: "<<pwd<<endl;

cout<<"Encrypted message is: "<<encrypted<<endl;

cout<<"Decrypted message is: "<<decrypted<<endl;

return 0;

}

/\*

OUTPUT:

Enter the plain text

ANUDISHJINTURKAR

Enter the key

NILAYKUMAR

Plain text is: ANUDISHJINTURKAR

Key is: NILAYKUMAR

Encrypted message is: ÿ╬ΣΘiP∩≡Rk╦q≈ªa

Decrypted message is: ANUDISHJINTURKAR

\*/