**An toàn bảo mật thông tin**

**Chương 1:**

1. **Hiện 1 chuỗi từ bàn phím , cộng mỗi phần tử vs 3, giải mã**

#include <iostream>

Using namespace std;

Int main()

{ string s;

//ma hoa

Cout<<”Nhap chuoi:” ; getline(cin,s);

For (int[i]=0; i<s.size(); i++;

{ s[i]=s[i]+3; }

Cout<<”Chuoi ma hoa la:”<<s<<endl;

// giai ma

for(int i=0; i<s.size(); i++) { s[i]= s[i]-3; } cout<<"chuoi giai ma la: "<<s;}

**Chương 2: Mật mã cổ điển**

**1-1**

**2.1)Nhập một chuỗi kí tự từ bàn phím , mã hóa chuỗi bằng Caeser tổng quát vs K, giải mã**

#include<iostream> //mat ma caeser

using namespace std;

int Kt\_so(char c)

{ return c-'A';}

char So\_kt(int n)

{ return 'A'+n;}

int main()

{

string P, C; int K;

cout<<"Nhap chuoi :";getline(cin,P); C=P;

cout<<"Nhap K ="; cin>>K;

// Ma hoa

for(int i=0; i<P.size(); i++)

{

int m ; m =Kt\_so(P[i]);

m=(m+K)%26;

C[i]=So\_kt(m);

}

cout<<"Chuoi ma hoa la"<<C<<endl;

// GIAI MA

for(int i=0; i<C.size(); i++)

{

int m ; m =Kt\_so(C[i]);

m=(m-K+26)%26;

P[i]=So\_kt(m);

}

cout<<"Chuoi ma hoa la"<<P;

}

**2.2) Lập trình bẻ khóa bằng BRUTE-force (Đầu vào là một chuỗi kí tự từ b1, xác định K đã sử dụng và nội dung ban đầu)**

#include<iostream> //mat ma caeser

using namespace std;

int Kt\_so(char c)

{ return c-'A';}

char So\_kt(int n)

{ return 'A'+n;}

int main()

{

string P, C; int K;

cout<<"Nhap chuoi :";getline(cin,C); P=C;

for(K=1; K<=25; K++)

{

// giai ma

for(int i=0; i<C.size(); i++)

{

int m ; m =Kt\_so(C[i]);

m=(m-K+26)%26;

P[i]=So\_kt(m);

}

cout<<K<<':'<<P<< endl;

}

}

**-Nhập một chuỗi , mã hóa bằng affine với cặp số {a,b} từ bàn phím. Hiện chuỗi**

#include<iostream> //mat ma Affine

using namespace std;

int Kt\_so(char c)

{ return c-'A';}

char So\_kt(int n)

{ return 'A'+n;}

int main()

{

string P, C; int a=0,b;

cout<<"Nhap chuoi :";getline(cin,P); C=P;

while (a<1|| a>25|| a%2==0||a==13)

{

cout<<"Nhap a= "; cin>>a;

}

cout<<"Nhap b= "; cin>>b;

// ma hoa

for(int i=0; i<P.size(); i++)

{

int m ; m =Kt\_so(P[i]);

m=(a\*m+b)%26;

C[i]=So\_kt(m);

}

cout<<"chuoi ma hoa: "<<C<< endl;

//GIAI MA

int a1;

for( int i=1; i<=25; i++)

if( (i\*a)%26==1) {a1=i; break;}

for(int i=0; i<C.size(); i++)

{

int m ; m =Kt\_so(C[i]);

m=a1\*(m-b+26)%26;

P[i]=So\_kt(m);

}

cout<<"Chuoi giai ma: "<<P;

}

**-Bẻ khóa Affine**

#include<iostream> //giai mat ma Affine

using namespace std;

int Kt\_so(char c)

{ return c-'A';}

char So\_kt(int n)

{ return 'A'+n;}

int main()

{

string P, C; int a=0,b;

cout<<"Nhap chuoi :";getline(cin,C); P=C;

for(a=1;a<=25 ;a=a+2 )

if(a!=13)

{

int a1;

for( int i=1; i<=25; i++)

if( (i\*a)%26==1) {a1=i; break;}

for(b=0; b<=25; b++)

{

for(int i=0; i<C.size(); i++)

{

int m ; m =Kt\_so(C[i]);

m=a1\*(m-b+26)%26;

P[i]=So\_kt(m);

}

cout<<a<<","<<b<<":"<<P<<endl;

}

}

}

**2.3) ma hoa monoalphabetic, giải mã**

#include<iostream>

using namespace std;

int main()

{

string P,C,K;

string B="ABCDEFGHIJKLMNOPQRSTUWXYZ";

cout<<"Nhap plaintext: ";cin>>P; C=P;

cout<<"Nhap chuoi K="; cin>>K;

//ma hoa

for(int i=0; i<P.size(); i++)

for(int j=0; j<26; j++)

if(P[i]==B[j]) C[i]=K[j];

cout<<"Chuoi ma hoa :"<<C;

//Giai ma

for(int i=0; i<C.size(); i++)

for(int j=0; j<26; j++)

if(C[i]==K[j]) P[i]=B[j];

cout<<endl<<"Chuoi giai ma :"<<P;

}

**n-n: Mã hóa đa kí tự**

**Mã playfair**

Loại các kí tự trùng lặp trong dãy:

#include<iostream>

using namespace std;

int main()

{

string K;

cout<<"Nhap chuoi khoa:"; getline(cin,K);

// xoa trung lap

for (int i=0; i<K.size();i++)

for (int j=i+1; j<K.size(); j++)

if(K[j]==K[i]) {K.erase(j,i); j--;}

cout<<"Chuoi vua xoa :"<<K;

}

Bài gộp:

#include<iostream>

using namespace std;

int main()

{

string K;

string B="ABCDEFGHIKLMNOPQRSTUWXYZ";

cout<<"Nhap chuoi khoa:"; getline(cin,K);

K=K+B;

// xoa trung lap

for (int i=0; i<K.size();i++)

for (int j=i+1; j<K.size(); j++)

if(K[j]==K[i]) {K.erase(j,i); j--;}

cout<<"Chuoi vua xoa :"<<K<<endl;

char A[5][5]; int t=0;

for(int i=0; i<5; i++)

for(int j=0; j<5; j++)

{A[i][j]=K[t]; t++;}

//hien ma tran

cout<<"ma tran khoa :"<<endl;

for(int i=0; i<5; i++)

{ for(int j=0; j<5; j++) cout<<A[i][j]<<" ";

cout<<endl;}

}

Mật mã HILL: (giải tay)

Pay mor emo ney

P1p2p3

P1=’p’=15 ; p2=’a’=0 ; p3=’y’=24

C1= 17.p1+17.p2+5.p3= 375=11 (17,17,5 là khóa K) l

C2= 21.p1+18.p2+21.p3=819=13 n

C3= 2.p1+2.p2+19.p3=486=18 (mod26) s

Giải mã

P1= c1\*4+c2\*9+c3\*15= 11\*4+13\*9+18\*15=431=15

P2= c1\*15+c2\*17+c3\*6=...=494=0

P3=c1\*24+c2\*0+c3\*17=...=570=24

**1-n: Mật mã polyalphabetic**

**-Vigenere**

Lập trình mã hóa:

#include <iostream>

using namespace std;

int Kt\_so(char c)

{return c-'A';}

int So\_kt(int n)

{return 'A'+n;}

int main()

{

string P,C,K;

cout<<"Nhap chuoi plaintext: "; cin>>P; C=P;

cout<<endl<<"Nhap chuoi K; "; cin>>K;

//ma hoa

int j=0;

for (int i=0; i<P.size(); i++)

{

int m; m=Kt\_so(P[i]);

int k; k=Kt\_so(K[j]);

m=(m+k)%26;

C[i]=So\_kt(m);

j=j+1;

if(j==K.size()) j=0;

}

cout<<"Chuoi ma hoa :"<<C;

//giai ma

j=0;

for (int i=0; i<P.size(); i++)

{

int m; m=Kt\_so(C[i]);

int k; k=Kt\_so(K[j]);

m=(m-k+26)%26;

P[i]=So\_kt(m);

j=j+1;

if(j==K.size()) j=0;

}

cout<<"Chuoi giai ma :"<<P;

}

**Mã ver man**

B1)

#include<iostream>

using namespace std;

int main()

{

string P,C; char K;

cout<<"Nhap chuoi plantext :"; getline(cin,P); C=P;

cout<<"Nhap khoa K: "; cin>>K;

// ma hoa

for(int i=0; i<P.size() ; i++) C[i]=P[i]^K;

cout<<"Chuoi ma hoa :"<<C;

//giai ma

for(int i=0; i<C.size() ; i++) P[i]=C[i]^K;

cout<<endl<<"Chuoi giai ma :"<<P;

}

B2)

#include<iostream>

using namespace std;

int main()

{

string P,C,K;

cout<<"Nhap chuoi plantext :"; getline(cin,P); C=P;

cout<<"Nhap khoa K: "; getline(cin,K);

// ma hoa

int j=0;

for(int i=0; i<P.size() ; i++)

{ C[i]=P[i]^K[j];

j++;

if (j==K.size() ) j=0;

}

cout<<"Chuoi ma hoa :"<<C;

//giai ma

j=0;

for(int i=0; i<C.size() ; i++)

{

P[i]=C[i]^K[j];

j++;

if(j==K.size() ) j=0;

cout<<endl<<"Chuoi giai ma :"<<P;

}

}

B2)

#include <iostrearainm> // fence

using namespace std;

int main()

{

string P,C;

cout<<"Nhap chuoi plantext: "; getline(cin,P);C=P;

//ma hoa

string h1,h2;

for(int i=0;i<P.size() ; i++)

{

if (i%2==0) h1=h1+P[i];

else h2= h2+P[i];

}

C=h1+h2;

cout<<"Chuoi ma hoa :"<<C;

//giai ma

if (C.size()%2==0)

{

for(int i=0; i<C.size() ; i++)

{

if (i<C.size()/2) h1=h1+C[i];

else h2=h2+C[i];

}

}

else

{

for(int i=0;i<C.size();i++)

{

if(i<=C.size()/2) h1=h1+C[i];

else h2=h2+C[i];

}

}

**Bài tập nhập chuỗi, ma trận 5\*5, lặp lại chuỗi**

#include<iostream>

using namespace std;

int main()

{

string P,C; char A[5][5];

cout<<"Nhap chuoi plantext: "; getline(cin,P);

// ma hoa

int t=0;

for (int i=0; i<5; i++)

for(int j=0; j<5; j++)

{

A[i][j]=P[t];

t++;

if (t==P.size()) t=0;

}

for(int i=0; i<5; i++) // hien ma tran

{

for (int j=0; j<5; j++) cout<<A[i][j]<<" ";

cout<<endl;

}

for(int i=0; i<5; i++)

for(int j=0; j<5; j++)

C=C+A[i][j];

cout<<"Chuoi ma hoa :"<<C<<endl;

//giaia ma

t=0; P="";

for (int i=0; i<5; i++)

for(int j=0; j<5; j++)

{

A[i][j]=C[t];

t++;

if (t==C.size()) t=0;

}

for(int i=0; i<5; i++) // hien ma tran

{

for (int j=0; j<5; j++) cout<<A[i][j]<<" ";

cout<<endl;

}

for(int i=0; i<5; i++)

for(int j=0; j<5; j++)

P=P+A[i][j];

cout<<"Chuoi ma hoa :"<<P;

}

Bài 1)

#include<iostream>

using namespace std;

char F(char R, char Ki)

{return R+Ki;}

int main()

{

string P,C; char K[3], L[3],R[3];

cout<<"Nhap khoi plaintext: "; getline(cin,P); C=P;

cout<<"Nhap khoa K: "; cin>>K[0];

// ma hoa

R[0]=P[0];

L[0]=P[0];

for(int i=1; i<=2; i++)

{

K[i]=K[0]<<i;

R[i]=L[i-1]^F(R[i-1],K[i]);

L[i]=R[i-1];

}

C[0]=L[2];

C[1]=R[2];

cout<<"Khoi ma hoa :"<<C;

}

B2) //chưa chạy đc

#include<iostream>

using namespace std;

char F(char R, char Ki)

{return R+Ki;}

MHKhoi(char P0, char P1, char k)

{

char K[3], L[3],R[3];

string C=" ";

// ma hoa

R[0]=P0;

L[0]=P1;

K[0]=k;

for(int i=1; i<=2; i++)

{

K[i]=K[0]<<i;

R[i]=L[i-1]^F(R[i-1],K[i]);

L[i]=R[i-1];

}

C[0]=L[2];

C[1]=R[2];

return C;

}

int main()

{

string P,C; char k;

cout<<"Nhap chuoi plaintext :";getline(cin, P);

cout<<"Nhap khoa K: "; cin>>k;

if(P.size()%2==1) P=P+'X';

for(int i=0; i<P.size(); i=i+2) C=C+MHKhoi(P[i],P[i+1],k);

cout<<"Chuoi ma hoa :"<<C;

}

**Mã hash**

Ví dụ 1

#include <iostream>

using namespace std;

int main()

{

string M; char H=0;

cout<<"Nhap chuoi:"; getline(cin,M);

for(int i=0; i<M.size(); i++) H=H^M[i];

cout<<"Ma hash: "<<H;

}

Bt2)

#include <iostream>

using namespace std;

int main()

{

string M; char H=0; char n;

cout<<"Nhap chuoi:"; getline(cin,M);

for(int i=0; i<M.size(); i++)

{

if(H%2==1) n=128; else n=0;

H=H<<1; H=H+n; //quay phai

H=H^M[i];

}

cout<<"Ma hash: "<<H;

}