**Phần 3 : Mật mã khóa công khai ( 15 tiết)**

**Sử dụng các chương trình tính modulo ở phần 1**

***Bài 1 : Viết chương trình thực hiện thuật giải Knapsack ( Mackle Hellman)***

1. Chọn 1 vecto siêu tăng A’ = (a’1, a’2, ..., a’N), chọn 1 số M > 2 \* a’N, chọn ngẫu nhiên 1 số u < M và (u, M) = 1

2. Xây dưng Vecto S = (s1, s2, ..., sN) trong đó si = (si \* u) mod M

3. Khóa: KP = (S, M), KS = (u, u-1)

4. Không gian các bản rõ là không gian moị dãy N bit

P = (x1, x2, ..., xn).

Mã hóa: *C*

Giải mã: tính C’ = C \* u-1 mod M sau đó giải bài toán xếp ba lô 0/1 với A’, C’ tù đó tìm được P = (x1, x2, ..., xn).

***Bài 2 : Trao đổi khóa bằng*** DIFFE-HELLMAN

#include <iostream>

#include <cstdlib>

using namespace std;

long long Exp(const long long& g, long long exp)

{

long long i = 1;

for (; i<exp; i++)

i \*= g;

return i;

}

int main()

{

long long A, B;

long long g, p;

for (;;)

{

cout << "Chao mung ban den voi thuat giai trao doi khoa Diffe-Hellman" << endl;

cout << "Nhap gia tri so nguyen thuy g(cong khai): " << endl;

cin >> g;

cout << "Nhap gia tri so nguyen to p(cong khai): " << endl;

cin >> p;

cout << "Alice:chon gia tri so mu ngau nhien bat ki(bi mat) " << endl;

cin >> A;

cout << "Bob: chon gia tri so mu ngau nhien bat ki(bi mat) " << endl;

cin >> B;

long long a = Exp(g, A) % p;

long long b = Exp(g, B) % p;

cout << "Gia tri b cua Alice tinh duoc (cong khai): " << a << endl;

cout << "Gia tri b cua Bob tinh duoc (cong khai): " << b << endl;

long long akey = Exp(b, A) % p;

long long bkey = Exp(a, B) % p;

cout << "Khoa chung bi mat(K) cua ALice: " << akey << endl;

cout << "Khoa chung bi mat(K) cua Bob: " << bkey << endl;

}

system("PAUSE");

return EXIT\_SUCCESS;

}

***Bài 3 : Chương trình mã –dich dùng RSA \_ Thuật giải tạo khóa :***

1.Tạo bảng SNT ( hoặc đưa SNT từ KB song phải kiểm tra số NT)

2. Chọn p&q trong bảng

3. Tạo khóa :

* Chương trình tự động tính N=p\*q
* Chương trình tính φ(N) = (p-1)\*(q-1)
* Yêu cầu chọn e (nhập e từ KB)
* Chương trình K/tra (e , φ) = 1
* Nếu (e ,φ) >1 🡪nhập lại e
* Chương trình tính tiếp d ≡ e-1 modφ (Dùng Beazout)
* Xuất cặp khóa (e,N) và (d,N)



***Bài 4 : Chương trình mã –dich dùng RSA \_ Mã dịch trên RSA :***

1. ***Xác thực thông điệp***

* Nhập từ KB một chuỗi ký tư .
* Chuyển ký tự sang số nguyên m
* Nhập khóa từ bảng khóa (d,N) (của tôi)
* Mã xác thực : c = md mod N 🡪 gửi đi
* Bên nhận (cần xác thực) dùng Public Key (của tôi) để xác minh “tôi” chinh là “tôi”.

1. ***Bảo mật thông điệp***

* Nhập thông điệp cần bảo mật là một chuỗi ký tự từ KB
* Chuyển chuỗi ký tự sang số nguyên m.
* Lấy (e,N) của bên nhận thông điệp từ bảng khóa hoặc PK server
* Mã bằng (e,N) của bên nhận : c= me modN gửi c đi.
* Bên nhận dùng (d,N) của mình để giải mật. Nếu giải được 🡪 OK!

***Code tham khảo***

/\* m là một số nguyên \*/

#include <stdio.h>

#include <math.h>

#include <conio.h>

#define I 4

#include<time.h>

long Q[40];

int n,N,M;

typedef long vector[I+1];

long MP(long long x,long y,long z);

long inverse(long x,long m),ME(long x,long y,long z);

long BR(long s);

void main()

{/\*main\*/

clrscr();

long q1,p1,M1,x1,phi1,e1,d1,xx,xx1,xx2,xx3,

p2,q2,M2,phi2,e2,d2,yy,yy1,yy2,yy3,now0,now,user\_time;

now0=time(NULL);

p1=2699;q1=795659;

M1=p1\*q1;

printf("p1=%ld q1=%ld M1=%ld ",p1,q1,M1);

phi1=(p1-1)\*(q1-1);e1=3674911;

d1=inverse(e1,phi1);

printf("phi1=%ld e1=%ld d1=%ld \n",phi1,e1,d1);printf("");

p2=5843;q2=367531;M2=p2\*q2;phi2=(p2-1)\*(q2-1);

e2=3674911;printf("p2=%ld q2=%ld M2=%ld ",p2,q2,M2);

d2=inverse(e2,phi2);

printf("phi2=%ld e2=%ld d2=%ld \n",phi2,e2,d2);printf("");

xx=12345;

xx1=ME(xx,M1,e1);xx2=ME(xx1,M1,e1);xx3=ME(xx2,M1,e1);

yy1=ME(xx3,M2,e2);yy2=ME(yy1,M2,e2);yy3=ME(yy2,M2,e2);

cprintf("\n KET QUA MA : ",yy3);

printf("xx=%ld \n\nxx1=%ld xx2=%ld xx3=%ld \n",xx,xx1,xx2,xx3);

printf("yy1=%ld yy2=%ld yy3=%ld \n",yy1,yy2,yy3);

yy2=ME(yy3,M2,d2);yy1=ME(yy2,M2,d2);xx3=ME(yy1,M2,d2);

xx2=ME(xx3,M1,d1);xx1=ME(xx2,M1,d1);xx=ME(xx1,M1,d1);/\* m=c^d modNN=RO \*/

cprintf("\n KET QUA DICH : ",xx);

printf("xx=%ld \n\nxx1=%ld xx2=%ld xx3=%ld \n",xx,xx1,xx2,xx3);

printf("yy1=%ld yy2=%ld yy3=%ld \n",yy1,yy2,yy3);

now=time(NULL);user\_time=now-now0;

printf("\nuser\_time = %d seconds ",user\_time,"seconds");getchar();

}/\*main\*/

long x0,m0,p0;

long ME(long x0,long m0,long p0)

{

long A0,p1,Z[40];int i1;

BR(p0);N=n;for (i1=0;i1<=N;i1++) Z[i1]=Q[i1];

/\*for (i1=0;i1<=N;i1++)

printf("Q[%d]=%ld \n",i1,Q[i1]);getchar();\*/

A0=x0%m0;p1=1;/\* A0=x1modMM B pesentation of x1\*/

if(p0>0);

{

if (Z[0]>0) p1=A0;

for(i1=1;i1<=N;i1++)

{

A0=MP(A0,A0,m0);

if(Z[i1]>0) p1=MP(A0,p1,m0);

}/\*i1\*/

}

return (p1);

}/\*phep tinh luy thua modulo\*/

long s;

long BR(long s)

{

int ii;

long x,q;

ii=0;x=s;q=(x>>1);Q[ii]=x-(q<<1);

while (q>0)

{

ii++;x=q;q=(x>>1);Q[ii]=x-(q<<1);

}

n=ii;

}/\*Bit-Representation,bieu dien x theo bimary\*/

long x,y,k;

long MP(long x,long y,long k)

{

int ii;long P,t1,t2,Y[40];double tem;t1=x;t2=y;

if(x<0) {x=-x;x=k-(x%k);} else x=x%k;

if(y<0) {y=-y;y=k-(y%k);} else y=y%k;

if ((x==0)||(y==0)) {P=0;goto label1;}

BR(y); M=n;

for(ii=0;ii<=M;ii++) Y[ii]=Q[ii];

if(Y[0]>0) P=x; else P=0;

for(ii=1;ii<=M;ii++)

{

tem=2.0\*x;

if(tem>=k) tem-=k;

x=(long)tem;

if(Y[ii]>0)

{

tem+=P;

if(tem>=k) P=(long)(tem-k);

else P=(long)tem;

}

}/\*ii\*/

x=t1;

y=t2;

label1:return(P);

}/\*phep nhan modulo\*/

long b,a;/\*0<b<a,Multicative inverce of b mod a\*/

long inverse(long b,long a)

{

long A,B,d,q,r,x,x1,x2,y,y1,y2,tem;

A=a;B=b; /\*Dung Beazout\*/

if(b==0)

{

d=a;x=1;y=0;

}/\*if\*/

else

{

x2=1;x1=0;y2=0;y1=1;

while (b>0)

{

q=a/b;

r=a-q\*b;

x=x2-q\*x1;

y=y2-q\*y1;

a=b;b=r;x2=x1;x1=x;y2=y1;y1=y;

}/\*while\*/

d=a;x=x2;y=y2;

}/\*else\*/

tem=A\*x+B\*y-d;

if(y<0)

y=A+y;

return(y);

}/\*inverse\*/

***/\* plain text  ’m’ được nhập vào dưới dạng một chuỗi ký tự***

#include <iostream.h>

#include <conio.h>

#include <math.h>

#include <stdlib.h>

#include <stdio.h>

#include<string.h>

#include<iomanip.h>

long MP(long long ,long ,long ); //Nhan luy thua

long inverse(long ,long ); //Modulo nghich dao

long ME(long ,long ,long ); //Luy thua modulo

void BR(long ); //Doi sang dang bit (co so 2)

int SNT(long);

int snt( long);

long Bezout (long a, long b);//tinh gcd

long Q[40];

int n,N,M;

long MP(long long x,long y,long k){ //Nhan luy thua

int ii;

long P,t1,t2,Y[40];

double tem;

t1=x; t2=y;

if(x<0){

x = -x;

x = k - (x%k);

}

else x = x%k;

if(y<0){

y = -y;

y = k - (y%k);

}

else y = y%k;

if(x==0 || y==0){

P=0;

return P;

}

BR(y); M=n;

for(ii=0;ii<=M;ii++)

Y[ii]=Q[ii];

if(Y[0]>0)

P = x;

else P = 0;

for(ii=1;ii<=M;ii++){

tem=2.0\*x;

if(tem>=k)

tem -= k;

x = (long)tem;

if(Y[ii] > 0){

tem +=P;

if(tem>=k) P = (long)(tem-k);

else P = (long)tem;

}

}

x = t1;

y = t2;

return P;

}

long inverse(long b,long a){ //Modulo nghich dao

long A,q,r,x,x1,x2,y,y1,y2;

A = a;

if(b == 0){

x = 1; y = 0;

}

else{

x2 = 1; x1 = 0; y2 = 0; y1 = 1;

while(b>0){

q = a/b;

r = a - q\*b;

x = x2 - q\*x1;

y = y2 - q\*y1;

a = b;b = r;x2 = x1; x1 = x; y2 = y1; y1 = y;

}

x = x2; y = y2;

}

if(y<0)

y = A + y;

return y;

}

long ME(long x0,long m0,long p0){

//Tính Luy thua Modulo

long A0,p1,Z[40];

int i1;

BR(p0);

N=n;

for(i1=0;i1<=N;i1++)

Z[i1] = Q[i1];

A0 = x0%m0;

p1 = 1;

if(p0>0);{

if(Z[0]>0)

p1=A0;

for(i1=1;i1<=N;i1++){

A0=MP(A0,A0,m0);

if(Z[i1]>0)

p1=MP(A0,p1,m0);

}

}

return p1;

}

void BR(long s){ //Doi sang dang bit (co so 2)

int ii;

long x,q;

ii = 0; x = s; q = (x>>1); Q[ii] = x - (q<<1);

while(q>0){

ii++; x = q;

q = (x>>1); Q[ii] = x - (q<<1);

}

n = ii;

}

int SNT(long n){

if(n == 1 || n == 2)

return 1;

int i=3;while(n%i!=0)i++;i--;

if(n == i)

return -1;

return 1;

}

void main(){

clrscr();

long q1,p1,M1,phi1,e1,d1,xx[25]={0},xx1[25]={0},xx2[25]={0},xx3[25]={0};

//tao ngau nhien SNT

randomize();

long arr[30]={0},z,y,x;

cout<<"\n Day so nguyen to(Ban co the chon!):";

int i=0;

for( int j=0;j<50;j++)

{

if((z=snt(random(10000)))!=0)

{

arr[i]=z;i++;

}

}

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

cout<<setw(10)<<arr[j];

cout<<"\nNHAP CAP SO NGUYEN TO THU NHAT:";

do{

cout<<"\nNhap so nguyen to thu nhat p1 = "; cin>>p1;

}while(SNT(p1)<0);

do{

cout<<"\nNhap so nguyen to thu hai q1 = "; cin>>q1;

}while(SNT(q1)<0);

M1 = p1\*q1;

cout<<"p1 = "<<p1<<" q1 = "<<q1<<" M1 = "<<M1<<endl;

phi1 = (p1-1)\*(q1-1);

do{

cout<<"\n nhap vao so e1:";cin>>e1;

}while(Bezout(e1,phi1)!=1);

d1=inverse(e1,phi1);

cout<<" phi1 = "<<phi1<<" e1 = "<<e1<<" d1 = "<<d1;

char a[25];

cout<<"\nNHAP VAN BAN CAN MA HOA: "; gets(a);

int n= strlen(a);

cout<<"chieu dai chuoi = "<<n<<endl;

cout<<"\nVAN BAN CAN MA HOA "<<a;

for(int ii=0;ii<n;ii++) [/\*chuyen](file:///\\chuyen) kt sang so \*/

{

if((a[ii]!=' '))

{

xx[ii]= (a[ii] - '0');

}

else

xx[ii]=a[ii];

}

cout<<"\n chuoi sau khi doi thanh so: "<<xx;

//Ma hoa

for( ii=0;ii<n;ii++)

xx1[ii]=ME(xx[ii],M1,e1);

for( ii=0;ii<n;ii++)

xx2[ii]=ME(xx1[ii],M1,e1);

for( ii=0;ii<n;ii++)

xx3[ii]=ME(xx2[ii],M1,e1);

cout<<"\nKET QUA MA (van ban ma):"<<xx3<<endl;

getch();

//giai ma

for( ii=0;ii<n;ii++)

xx2[ii]=ME(xx3[ii],M1,d1);

for( ii=0;ii<n;ii++)

xx1[ii]=ME(xx2[ii],M1,d1);

for( ii=0;ii<n;ii++)

xx[ii]=ME(xx1[ii],M1,d1);

// cout<<"\n Sau giai ma (chua doi thanh ky tu):"<<xx;

for(ii=0;ii<n;ii++)

{

if(xx[ii]!=32)

a[ii]= char(xx[ii] + '0');

else

a[ii]=' ';

}

cout<<"\nKET QUA DICH (BANG RO): "<<a;

getch();

}

long Bezout (long a, long b)

{

long d,q,r,x,x1,x2,y,y1,y2;

if (b==0) {

d=a; x=1; y=0;

}

else {

x2=1;x1=0;y2=0;y1=1;

while (b>0) {

q=a/b;r=a-q\*b;x=x2-q\*x1;y=y2-q\*y1;

a=b; b=r; x2=x1;x1=x;y2=y1; y1=y;

}

d=a; x=x2;y=y2;

}

return d;

}

int snt(long n)

{

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

{

if((n%i)==0)

{ n=0;

break;

} }

return n;

}

=================================================

***/\* Mã hóa một file text (thu1.txt) dùng RSA\*/***

#include <stdio.h>

#include <math.h>

#include <conio.h>

#define I 4

#include<time.h>

long Q[40];

FILE \*fp1;

int n,N,M;

long q1,p1,M1,x1,phi1,e1,d1,xx,xx1,xx2,xx3,

p2,q2,M2,phi2,e2,d2,yy,yy1,yy2,yy3;

typedef long vector[I+1];

long MP(long long x,long y,long z);

long inverse(long x,long m),ME(long x,long y,long z);

long BR(long s);/\*long codage(long x,long y,long z,long t,long v);\*/

void main()

{/\*main\*/

long now0,now,user\_time,i2=0;

clrscr();

now0=time(NULL);

p1=2699;q1=795659;

M1=p1\*q1;

printf("p1=%ld q1=%ld M1=%ld ",p1,q1,M1);

phi1=(p1-1)\*(q1-1);e1=3674911;

d1=inverse(e1,phi1);

printf("phi1=%ld e1=%ld d1=%ld \n",phi1,e1,d1);printf("");

p2=5843;q2=367531;M2=p2\*q2;phi2=(p2-1)\*(q2-1);

e2=3674911;

printf("p2=%ld q2=%ld M2=%ld ",p2,q2,M2);

d2=inverse(e2,phi2);

printf("phi2=%ld e2=%ld d2=%ld \n",phi2,e2,d2);printf("");

fp1=fopen("a:\thu1.txt","rb");

printf("KET QUA MA : \n");

while(fread(&xx,sizeof(xx),1,fp1)==1)

{

/\*codage(xx,M1,e1,M2,e2);\*/

xx1=ME(xx,M1,e1);

xx2=ME(xx1,M1,e1);xx3=ME(xx2,M1,e1);

yy1=ME(xx3,M2,e2);

yy2=ME(yy1,M2,e2);yy3=ME(yy2,M2,e2);

i2++;printf("%lx ",yy3);

if(i2%7==0)printf("");

}

fclose(fp1);

now=time(NULL);user\_time=now-now0;

printf("\n user\_time = %d seconds ",user\_time,"seconds");getchar();

}/\*main\*/

long x0,m0,p0;

long ME(long x0,long m0,long p0)

{

long A0,p1,Z[40];int i1;

BR(p0);N=n;for (i1=0;i1<=N;i1++) Z[i1]=Q[i1];

/\*for (i1=0;i1<=N;i1++)

printf("Q[%d]=%ld \n",i1,Q[i1]);getchar();\*/

A0=x0%m0;p1=1;/\*printf ("A0=%ld N=%d ",A0,N);getchar();/\* A0=x1modMM B pesentation of x1\*/

if(p0>0);

{

if (Z[0]>0) p1=A0;

for(i1=1;i1<=N;i1++)

{

A0=MP(A0,A0,m0);

if(Z[i1]>0) p1=MP(A0,p1,m0);

/\*printf("i1=%d A0=%ld p1=%ld \n",i1,A0,p1);\*/

}/\*i1\*/

}/\* printf("p1=%ld ",p1); getchar();\*/

return (p1);

}/\*phep tinh luy thua modulo\*/

long s;

long BR(long s)

{

int ii;

long x,q;

ii=0;x=s;q=(x>>1);Q[ii]=x-(q<<1);

while (q>0)

{

ii++;x=q;q=(x>>1);Q[ii]=x-(q<<1);

}

n=ii;

}/\*Bit-Representation,bieu dien bit\*/

long x,y,k;

long MP(long x,long y,long k)

{

int ii;

long P,t1,t2,Y[40];

double tem;

t1=x;

t2=y;

if(x<0) {x=-x;x=k-(x%k);

} else x=x%k;

if(y<0) {y=-y;y=k-(y%k);

} else y=y%k;

if ((x==0)||(y==0))

{

P=0;

goto label1;

}

BR(y); M=n;

for(ii=0;ii<=M;ii++) Y[ii]=Q[ii];

if(Y[0]>0) P=x; else P=0;

for(ii=1;ii<=M;ii++)

{

tem=2.0\*x;

if(tem>=k) tem-=k;

x=(long)tem;

if(Y[ii]>0)

{

tem+=P;

if(tem>=k) P=(long)(tem-k);

else P=(long)tem;

}

}/\*ii\*/

x=t1;

y=t2;

label1:

return(P);

}/\*phep nhan modulo\*/

long b,a;/\*0<b<a,Multicative inverse of b mod a\*/

long inverse(long b,long a)

{

long A,B,d,q,r,x,x1,x2,y,y1,y2,tem;

A=a;B=b;

if(b==0)

{

d=a;x=1;y=0;

}/\*if\*/

else

{

x2=1;x1=0;y2=0;y1=1;

while (b>0)

{

q=a/b;

r=a-q\*b;

x=x2-q\*x1;

y=y2-q\*y1;

a=b;b=r;x2=x1;x1=x;y2=y1;y1=y;

}/\*while\*/

d=a;x=x2;y=y2;

}/\*else\*/

tem=A\*x+B\*y-d;

if(y<0)

y=A+y;

return(y);

}/\*inverse\*/

/\* long codage(long x, long y ,long z,long t,long v)

{

}/\*codage\*/

*Bài 5. Bài tổng hợp :* HIỆN THỰC CHƯƠNG TRÌNH HỆ BẢO MẬT – XÁC THỰC DÙNG RSA



Bấm (K) –tạo khóa :

**Menu tạo khóa :**

1.Tạo bảng SNT ( hoặc đưa SNT từ BF song phải kiểm tra số NT)

2. Chọn p&q trong bảng

3. Tạo khóa :

Chương trình tự động tính N=p\*q

Chương trình tính Fi = (p-1)\*(q-1)

Yêu cầu chọn e (nhập e từ KB)

Chương trình K/tra e có NTCN với Fi

Nếu e không là số NT cùng nhau với Fi🡪nhập lại e

Chương trình tính tiếp d = e-1 modFi (Dùng Beazout)

Xuất cặp khóa (e,N) và (d,N)

Ví dụ p=3,q=5;p\*q=15 ; Fi=(p-1)\*(q-1)=8

Chọn e = 3 d =38mod15 = 6561mod15

Xuất (3,15) và (6,15)

Thoát về main menu

🟔Bấm A ( Authenticate)

1.Yêu cầu nhập văn bản gốc cần xác thực

- Nhập từ KB số nguyên m

Trong thực tế : Nhập text 🡪 chuyển khối dữ liệu thành số nguyên

* Nhập khóa từ bảng khóa (d,N) (của tôi)
* Mã xác thực : c = md mod N 🡪 gửi đi
* Bên nhận (cần xác thực) dùng Public Key của “tôi” để giải .--> giả được “tôi” đúng là tôi.

🟔Bấm C ( bảo mật thông điệp).

Nhập thông điệp cần bảo mật “m” từ KB

Lấy (e,N) của bên nhận thông điệp từ bang khóa hoặc PK server

Mã bằng (e,N) của bên nhận : c= me modN gửi c đi.

Bên nhận dùng (d,N) của mình để giải mật. Nếu giải được 🡪 OK!

Thoát ra menu chính

Hỏi có tiếp tục Ko???

Yes ! Trở về menu chính

No ! Bye bye!

Thoát ra HĐH