ALGORITHM

201133216

정유석

**CODE**

#include<stdio.h>

#include<stdlib.h>

#include<math.h>

int Mod\_Exp(int a,int b,int n){ //Explanation

int i,num,result[50],cnt=0;

int c=0, d=1;

num = b;

for(i=0; num>0; i++){

result[cnt]= num%2; //Store the binary number

num = num/2;

cnt++;

}

for(i=cnt-1; i>=0; i--){ //Check the calculate

c = 2\*c;

d = (d\*d) % n;

if(result[i] == 1){

c = c+1;

d = (d\*a) % n;

}

}

return d; //return mod

}

int Miller\_Rabin(int n){ //Miller\_Rabin function

int k,q,a,i,j,a\_S,a\_L,Last,test;

int k\_S = 1;

int check=0;

//Find integers k and q(q is odd number)

for(k=1; k<100; k++){

k\_S = k\_S \* 2;

for(q=0; q<100; q++){

if((n-1)<k\_S\*q)

break;

if(((n-1)==k\_S\*q) && k>0){

check=1;

break;

}

}

if(check==1)

break;

}

//select a random integer A

while(1){

a = rand()+1;

if(a<n-1 && a>1){

break;

}

}

a\_S=2;

a\_L = 1;

//Find the prime number

for(j=0; j<k-1; j++){

a\_S = a\_S \* 2;

test = Mod\_Exp(a,a\_S+q,n);

if(test != n-1)

return 0;

}

return 1;

}

void main(){

int a1,a2;

int i,j,d1,d2;

while(1){

int p,q,ee=0,dd=0,cipher,nn,PIn,check=0,orign\_M=0;

int message,temp\_message;

int confirm1=1,confirm2=1;

while(1){ //Receive P,Q

printf("Enter the P,Q : ");

scanf("%d %d",&p,&q);

fflush(stdin);

if(p>2 && p<65000 && q>2 && q<65000)

break;

}

if(p>0){ //Find A of P

while(1){

a1 = rand()+1;

if(a1<p && a1>1)

break;

}

}

if(q>0){ //Find A of Q

while(1){

a2 = rand()+1;

if(a2<q && a2>1)

break;

}

}

d1 = Mod\_Exp(a1,p,p);

d2 = Mod\_Exp(a2,q,q);

//Check the Fermat's Little Theorem

if((d1 != a1) || (d2 != a2)){

printf("P or Q are none prime number!\n");

continue;

}

//Confirm the Carmichael number

confirm1 = Miller\_Rabin(p);

confirm2 = Miller\_Rabin(q);

if(confirm1 == 0 || confirm2 == 0){

printf("P or Q is Carmichael number !\n");

printf("\n--Reinput--\n");

continue;

}

//RSA algorithm

//Find n, n of pi

nn = p\*q;

PIn = (p-1)\*(q-1);

//Find e

for(i=2; i<PIn; i++){

if(PIn%i!=0 && i%2!=0){

ee = i;

break;

}

}

//Find d

for(i=1; i<1000; i++){

for(j=1; j<1000; j++){

if(j\*ee > i\*PIn+1)

break;

else if(j\*ee < i\*PIn+1)

continue;

else if(j\*ee == i\*PIn+1){

dd=j;

check=1;

break;

}

}

if(check==1)

break;

}

//Receive message and Print message

printf("Input Message : ");

scanf("%d",&message);

fflush(stdin);

temp\_message = message;

cipher=Mod\_Exp(message,ee,nn);

orign\_M = Mod\_Exp(cipher,dd,nn);

printf("Orignal Message : %d\n",orign\_M);

}

}

