#include<iostream>

#include<bits/stdc++.h>

using namespace std;

int P[2],Q[2],E[2],p;

int delta1,delta2;

int r1,r2,res1,res2,s1,s2;

int R[2];

int G[2],Ep[2],q,na,nb,binary[10],Gnext[2];int rem[10];

int\* bin1;int\* bin2;

//int arr[10][10];

int\* temp;int\* temp1;

int delta;

int\* pa; int\* pb;

int\* k1; int\* k2;

void accept\_inputs(){

cout<<"Enter the coordinates of P: ";

cin>>P[0]>>P[1];

cout<<"Enter the coordinates of Q: ";

cin>>Q[0]>>Q[1];

cout<<"Enter the coordinates of E: ";

cin>>E[0]>>E[1];

cout<<"Enter the value of p: ";

cin>>p;

}

int multiplicative\_inverse(int num,int p){

int temp;

for(int m=0;m<p;m++){

if((num\*m)%p == 1){

temp = m;

break;

}

}

return temp;

}

int calculate\_delta\_equal(int M[],int N[],int p){

s1 = 3\*(M[0]\*M[0])+N[0] ;

s2 = (2\*M[1]) ;

cout<<"s1: "<<s1<<" s2: "<<s2;

if(s2 > 0)

res2 = multiplicative\_inverse(s2,p);

else{

p = s2%p;

res2 = p + s2;

res2 = multiplicative\_inverse(res2,p);

}

if(s1 > 0)

res1 = s1 % p;

else

res1 = (p + s1) % p;

delta1 = (res1\*res2) % p;

//cout<<"Delta for P=Q is: "<<delta1;

return delta1;

}

int calculate\_delta\_not\_equal(int X[],int Y[],int p){

r1 = (Y[1] - X[1]);

r2 = (Y[0] - X[0]);

if(r2 > 0)

res2 = multiplicative\_inverse(r2,p);

else{

//p=r2%p;

//res2 = p + r2;

r2 = r2\*(-1);

res2 = r2%p;

res2 = p - res2;

res2 = multiplicative\_inverse(res2,p);

}

if(r1 > 0)

res1 = r1 % p;

else{

//res1 = (p + r1) % p;

r1 = r1\*(-1);

res1 = r1%p;

res1 = p - res1;

}

delta2 = (res1\*res2) % p;

//cout<<"Delta for P!=Q is: "<<delta2;

return delta2;

}

int\* calculate\_P\_plus\_Q(int S[],int T[],int p,int delta){

int xr,yr;

if(S[0]!=T[0] && S[1]!=T[1]) //P!=Q

{

xr = ((delta\*delta) - S[0] - T[0]) % p;

yr = (((-1)\*S[1]) + delta \* (S[0] - xr)) % p;

}

else //P=Q

{

xr = ((delta\*delta) - S[0] - T[0]) % p;

yr = (((-1)\*S[1]) + delta\* (S[0] - xr)) % p;

}

if(xr < 0)

xr = p + xr;

if(yr < 0)

yr = p + yr;

R[0] = xr; R[1] = yr;

cout<<endl<<" P+Q: "<<R[0] <<" "<<R[1] ;

return R;

}

void accept\_inputs\_DHKE(){

cout<<"Enter nA and nB: ";

cin>>na>>nb;

cout<<"Enter coordinate of G: ";

cin>>G[0]>>G[1];

cout<<"Enter coordinate of Ep: ";

cin>>Ep[0]>>Ep[1];

cout<<"Enter the value of P: ";

cin>>q;

}

int\* convert\_to\_binary(int num1){

int i=0;

for(int i=0;i<10;i++){

rem[i] = 0;

binary[i] = 0;

}

while(num1 != 0){

rem[i] = num1%2;

num1 = num1/2;

i++;

}

i--;

int j=0;

for(i=9;i>=0;i--){

binary[j] = rem[i];

j++;

}

cout<<"Binary of na: ";

for(int i=0;i<10;i++)

cout<<binary[i];

return rem;

}

int\* calculate\_public\_key(int\* bin1,int n1){

int k=1;

int cnt=0;

while(n1>k){

k = k+k;

cnt++;

}

cout<<endl<<"cnt is: "<<cnt;

int arr[cnt][2];

//cout<<"hello ";

//calculate\_delta\_equal(G,Ep,q);

arr[0][0] = G[0];

arr[0][1] = G[1];

for(int i=1;i<cnt;i++){

delta = calculate\_delta\_equal(G,Ep,q);

cout<<"G is: ";

for(int a=0;a<2;a++)

cout<<" "<< G[a];

temp = calculate\_P\_plus\_Q(G,G,q,delta);

for(int j=0;j<2;j++){

arr[i][j] = temp[j];

G[j] = temp[j];

}

}

cout<<endl<<"Array contains: ";

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

for(int j=0;j<2;j++){

cout<<" "<<arr[i][j];

}

cout<<"bin1 in cpk: ";

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

cout<<bin1[i];

int v=0;

for(int i=0;i<cnt;i++){

if(bin1[i]!=0){

v++;

if(v==1){

G[0] = arr[i][0];

G[1] = arr[i][1];

}

else{

Gnext[0] = arr[i][0];

Gnext[1] = arr[i][1];

cout<<"Gnext: ";

for(int j=0;j<2;j++)

cout<<" "<<Gnext[j];

}

//cout<<endl<<"G is: "<<G[0]<<" "<<G[1];

//cout<<endl<<"Gnext is: "<<Gnext[0]<<" "<<Gnext[1];

//cout<<endl<<"p is: "<<q;

if(Gnext[0]!=0){

delta = calculate\_delta\_not\_equal(G,Gnext,q);

cout<<"delta is: "<<delta;

temp1 = calculate\_P\_plus\_Q(G,Gnext,q,delta);

for(int j=0;j<2;j++){

G[j] = temp1[j];

}

}

}

}

cout<<endl<<"Final G: " ;

for(int j=0;j<2;j++){

cout<<" "<<G[j];

}

return G;

}

int main(){

//accept\_inputs();

//calculate\_delta\_equal();

//calculate\_delta\_not\_equal();

//calculate\_P\_plus\_Q();

int n,z;

cout<<"Option Menu: ";

do{

cout<<"1.Calculation P=Q(2P) p+p "<<endl<<"2.Calculation P!=Q P+Q"<<endl<<"3.ECC Over DHKE ";

cout<<endl<<"Enter your choice: ";

cin>>n;

switch(n){

case 2:

accept\_inputs();

delta = calculate\_delta\_not\_equal(P,Q,p);

calculate\_P\_plus\_Q(P,Q,p,delta);

break;

case 1:

accept\_inputs();

delta = calculate\_delta\_equal(P,E,p);

calculate\_P\_plus\_Q(P,P,p,delta);

break;

case 3:

accept\_inputs\_DHKE(); //accept\_inputs\_DHKE;

bin1 = convert\_to\_binary(na);

int G1[2];

G1[0] = G[0];

G1[1] = G[1];

cout<<endl<<"Calculation for pa: ";

pa = calculate\_public\_key(bin1,na);

cout<<endl<<"Pa is: ";

for(int i=0;i<2;i++)

cout<<" "<<pa[i];

G[0] = pa[0]; Gnext[0] = 0;

Gnext[1] =0;

G[1] = pa[1];

bin2 = convert\_to\_binary(nb);

k2 = calculate\_public\_key(bin2,nb);

cout<<endl<<"K2 is: ";

for(int i=0;i<2;i++)

cout<<" "<<k2[i];

bin2 = convert\_to\_binary(nb);

G[0] = G1[0]; Gnext[0] = 0;

Gnext[1] =0;

G[1] = G1[1];

cout<<endl<<"Calculation for pb: ";

pb = calculate\_public\_key(bin2,nb);

cout<<endl<<"pb is: ";

for(int i=0;i<2;i++)

cout<<" "<<pb[i];

G[0] = pb[0]; Gnext[0] = 0;

Gnext[1] =0;

G[1] = pb[1];

bin1 = convert\_to\_binary(na);

k1 = calculate\_public\_key(bin1,na);

cout<<endl<<"K1 is: ";

for(int i=0;i<2;i++)

cout<<" "<<k1[i];

//compare code

cout<<endl<<"Compare K1 and K2: ";

if(k1[0]==k2[0] && k1[1]==k2[1])

cout<<endl<<"Keys are same........!";

else

cout<<endl<<"Keys are not matched..! ";

/\* while(na>k){

k = k+k;

cnt++;

}

cout<<endl<<"cnt is: "<<cnt;

cout<<"hello ";

//calculate\_delta\_equal(G,Ep,q);

for(int i=0;i<cnt-1;i++){

calculate\_delta\_equal(G,Ep,q);

cout<<"G is: ";

for(int a=0;a<2;a++)

cout<<" "<< G[a];

temp = calculate\_P\_plus\_Q(G,G,q);

for(int j=0;j<2;j++){

arr[i][j] = temp[j];

G[j] = temp[j];

}

}\*/

//bin2 = convert\_to\_binary(nb);

//calculate public key

//cacluate keys

//compare the keys

break;

default: exit(0);

break;

}

cout<<"Do you want to continue:(0/1)";

cin>>z;

}while(z!=0);

cout<<endl;

return 0;

}