Lab-08

Aim:- write a program to implement Point generation in ECC-Elgamal.

Source code:-

```
#include "functions.h"
#define point pair<int, int>

int a,b;

vector<point> pointGeneration(int a, int b, int p)
{
    vector<point> points;
    for(int x=0; x<p; x++)
    {
        int w = (power(x,3)+(a*x)+b) % p;
        int rem = squareAndMultiply(w, p-1/2, p);

        if( rem == 1)
        {
            while(sqrt(w)*sqrt(w) != w)
                w += p;
            points.push_back(make_pair(x, sqrt(w)));
            points.push_back(make_pair(x, sqrt(-w)
        }
        else if (rem = = 0)
              Points. push-back(make-pair(x, 0);
    }
    return points;
}

int main()
{
    cin>>a>>b>>P;

    vector<point> Points = point Generation(a,b,P);
    for(int i=0; i<points. size(); ++i)
         cout<<"C" <<points[i].first <<"," <<pointssecon
              <<")" <<endl;
    return 0;
}
```

Input

```
1, 1 13
```

Output

```
(0,1)    (4,11)   (8,12)   (12,5)
(0,12)   (5,1)    (10,6)   (12,8)
(1,4)    (5,12)   (10,7)
(1,9)    (7,0)    (11,2)
(4,2)    (8,1)    (11,11)
```