Cryptography

Assignment :05.

Elgamal encryption and decryption using elliptic curve cryptography.

NAME: SNEHA MAGANAHALLI RAJENDRANATH

ROLLNO: CS21M522

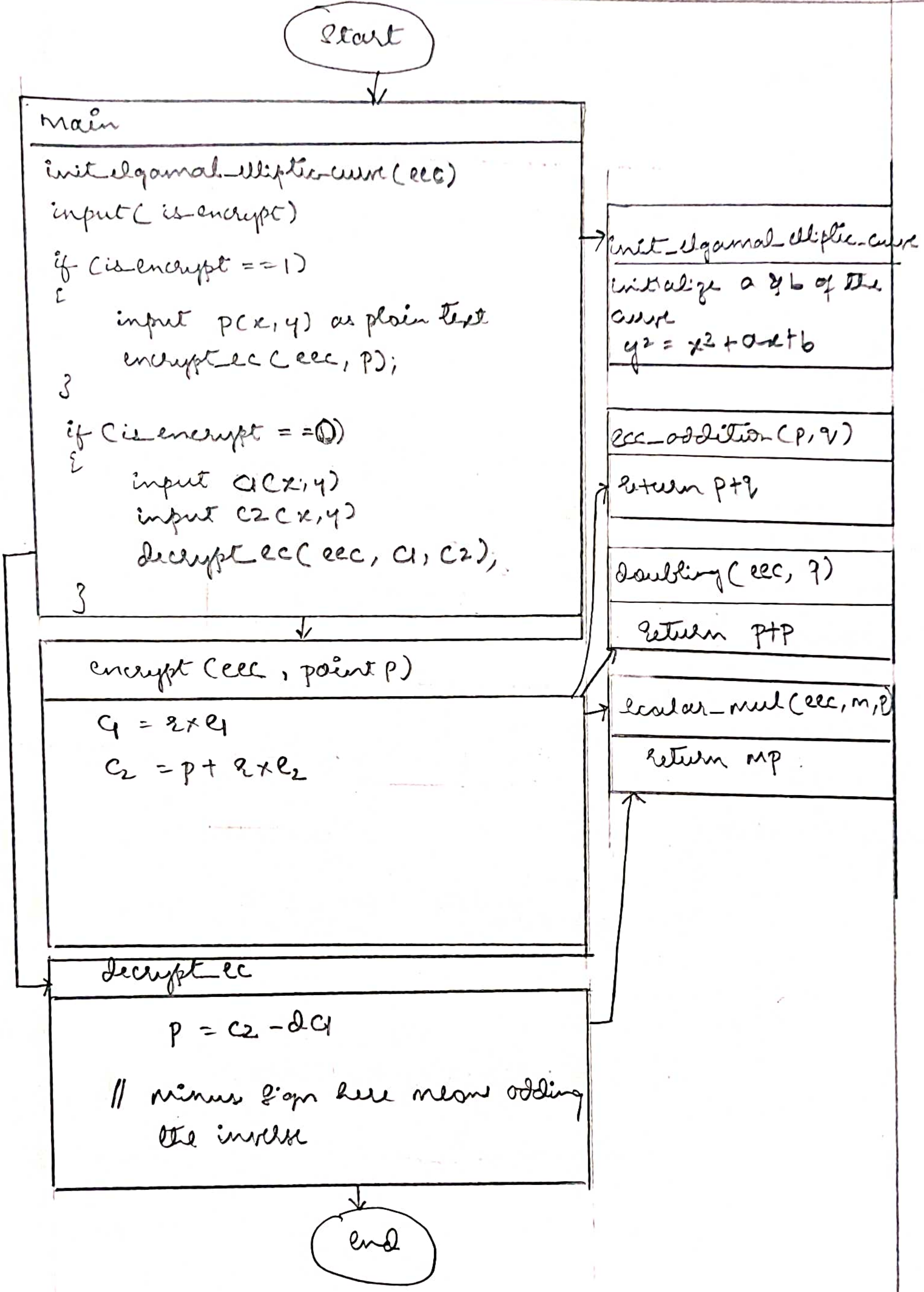
Algorithm :-

library function which will be used often :

```
point ecc_addition ( elgmal_elliptic_curve, ecc , point p, point q)
{
    return p+q;
}

point doubling ( ecc, point p)
{
    return p+p
}

point scalar_mul (ecc, int n, point p)
{
    return np
}

init_elgamal_elliptic_curve
{
    // y^2= x^3+ax+b.
    initialize a,b
}

Void destroy_elgam_ec
{
    free (ecc)
}
```

```
Void  encrypt_ec( eec, point p)
{
        c1 = k x e1
        c2 = p + k x e2
 }

 Void  decrypt_ec (eec,  point c1, point c2)
 {
        p =  c2 -(d x c1)
        // minus sign here means adding with the inverse

  }

int main()
{
     init_elgamal_elliptic_curve(eec);

     input is_encrypt;

     if ( is_encrypt ==1)
     {
          input p(x,y) as plain text
          encrypt_ec( eec, p);
     }

     if( is_encrypt ==0)
     {
          input c1 (x,y)
          input c2 (x,y)
          decrypt_ec ( eec, c1, c2);
     }

     destroy_elgamal_ec (eec
}
```

Flowchart :


Start
main
init_elgamal_elliptic_curve(eec)
input(is_encrypt)
if (is_encrypt ==1)
{
input P(x,y) as plain text
encrypt_ec(eec, P);
}
if (is_encrypt ==0)
{
input C1(x,y)
input C2(x,y)
decrypt_ec(eec, C1, C2);
}
init_elgamal_elliptic_curve
initialize a & b of the curve
y² = x² + ax + b
ecc_addition(p, q)
return p+q
doubling(eec, p)
return P+P
scalar_mul(eec, m, P)
return mP
encrypt(eec, point P)
C1 = k×e1
C2 = P + k×e2
decrypt_ec
P = C2 - dC1
// minus sign here means adding the inverse
end

Example:

$E_{67}(2,3)$ ---> mod is over 67

$a = 2$

$b = 3$

Bob/ ~~Sender~~ Reciever:

$e_1 = (2,22)$

$d = 4$

$e_2 = d \times e_1 = 4(2,22) = (13,45)$

Announce $[E, e_1, e_2]$

Alice /Sender:

Send $P(24,26)$

$r = 2$

$c_1 = (35,1)$ i.e; $c_1 = 2 \times e_1 = 2 \times (2,22) = (35,1)$

$c_2 = P + r \times e_2 = (22,26) + 2 \times (13,35) = (21,44)$

Send (c_1, c_2)

Bob:

$P = c_2 - dc_1$

$dc_1 = 2(35,1) = (22,25)$

dc_1 inverse $= (23,25)$

$P = c_2 + (\text{Inverse of } dc_1)$

$= (21,44) + (23,25)$

$$\boxed{P = (24,26)}$$

—— X ——