CRYPTOGRAPHY.

SNEHA MAGANAHALLI RAJENDRANATH

ROLL NO: CS21M522

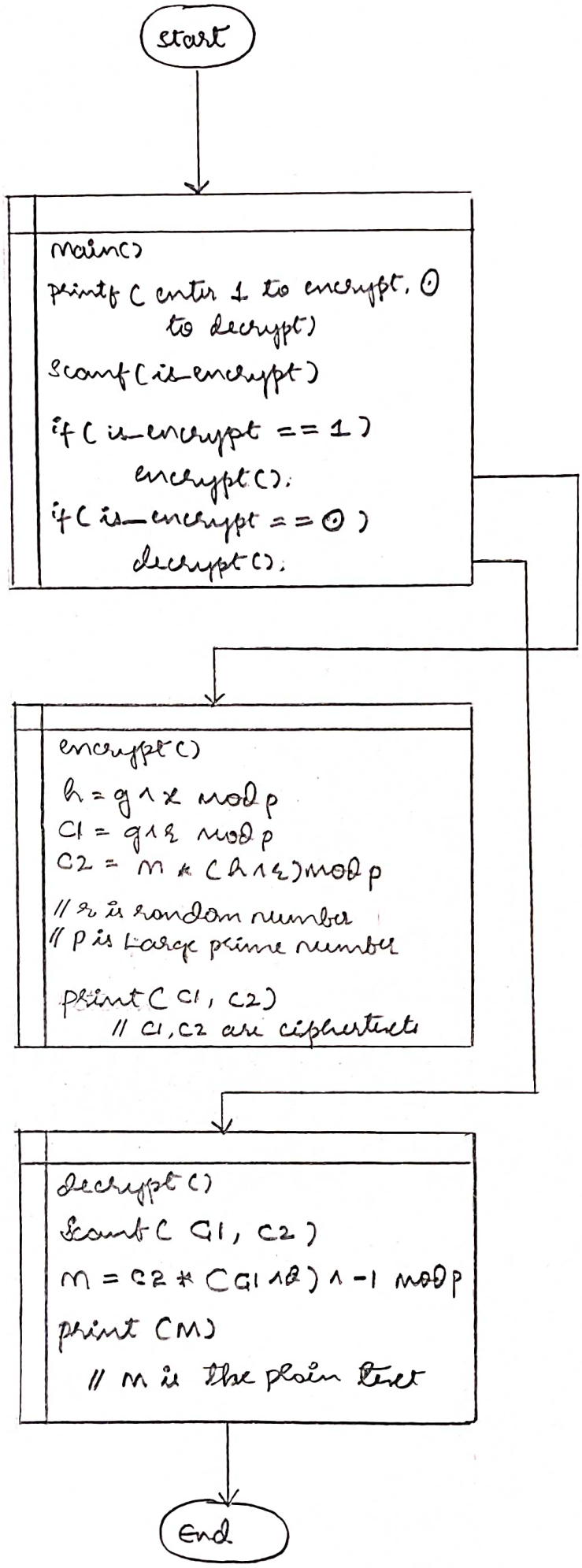
ASSIGNMENT : 04

Algorithm :-

```
Void encrypt()
{
    h = g^x mod p
    c1 = g^r mod p      // g is primitive root mod p
    c2 = m * (h^r) mod p
                        // r is random number.
                        // p is a large prime number.
                        // h is g^x mod p

    c1 and c2 are cipher texts
}

Void decrypt()
{
    Printf ("Enter the value c1, c2")
    gmp_sconf (c1, c2)
    m = c2 * (c1^d)^-1 mod p
    m is the plain text
}
```

```
int main()
{
    printf("Enter 1 to encrypt and 0 to decrypt");
    scanf(input)
    is_encrypt = input;

    if( is_encrypt == 1)
    {
        encrypt();
    }
    if ( is_encrypt == 0)
    {
        decrypt();
    }
return 0;
}
```

Flow chart :-


start
main()
printf(enter 1 to encrypt, 0 to decrypt)
scanf(is_encrypt)
if(is_encrypt == 1)
encrypt();
if(is_encrypt == 0)
decrypt();
encrypt()
h = g^x mod p
c1 = g^r mod p
c2 = m * (h^r) mod p
// r is random number
// p is large prime number
print(c1, c2)
// c1, c2 are ciphertexts
decrypt()
scanf(c1, c2)
m = c2 * (c1^x)^-1 mod p
print (m)
// m is the plain text
End