Lab 7

Task 1:

If p=31 q=23, find public and private key. Also show encryption and decryption steps where the message is 4

CODE:

p=31; q=23;

x=4; e=1;

fin=(p-1)*(q-1)

[G,D]=gcd(e,fin)

Y=mod((x^e),fin)

C=D*e

A=mod(C,fin)

X=mod((Y^D),fin)

OUTPUT

```
fin = 660 G = 1 D = 1 Y =
4 C = 1 A = 1 X = 4
```

Task 2:

`

If p=17 q=31 and public key 223, find private key. Also show encryption and decryption steps where the message is 2

CODE

p=17; q=31;

x=2; e=223;

fin=(p-1)*(q-1)

[G,D]=gcd(e,fin)

Y=mod((x^e),n)

C=D*e

A=mod(C,fin)

X=mod((Y^D),n)

OUTPUT:

```
fin = 480 G = 1 D = 127 Y
= 0 C = 28321
A = 1
X = 0
```

`