2024-05-17-file-2

Hoang Nguyen

5/17/2024

```
from sage.all import *

m = 661
a = 3
b = 1


e = EllipticCurve(GF(m), [a, b])

p = e(2,26)

print("p order is ",p.order())
print("e order is ",e.order())

x = 10
y = 22


# Message to be encrypted
M = e(2, 26)

# Encryption
k = 456  # Random integer
C1 = k * p
C2 = M + k * Q

# Decryption
decrypted_M = C2 - d * C1

print("Original Message:", M)
print("Encrypted Message:", (C1, C2))
print("Decrypted Message:", decrypted_M)
```

```
p order is  108
e order is  648
Original Message: (2 : 26 : 1)
```

Encrypted Message: ((509 : 397 : 1), (344 : 386 : 1))
Decrypted Message: (2 : 26 : 1)