

Elgamal Crypto System

Prashanth.S 19MID0020

```
In [1]: import pandas as pd
import numpy as np
```

```
In [2]: ## Alice
Xa = 50 ## private_key
Ya = 14 ## public key

## Bob
Xb = 39 ## private_key
Yb = 53 ## public key

## general
prime_number = 61
generator = 6

message = 4
```

```
In [3]: ## Bob sends message to Alice
cipher_text = ( ( Ya**Xb ) * message ) % prime_number
cipher_text
```

Out[3]: 57

```
In [4]: Xa = -1 * Xa
if (Xa<=0):
    Xa = prime_number - 1 + Xa
Xa
```

Out[4]: 10

```
In [5]: decrypt_text = ((cipher_text%prime_number) * (Yb**Xa)%prime_number)%prime_number
```

```
In [6]: print("Plain Text : ", message)
print("Encrypted Plain Text : ", cipher_text)
print("Decrypted Cipher Text : ",decrypt_text)
```

```
Plain Text : 4
Encrypted Plain Text : 57
Decrypted Cipher Text : 4
```