**Assignment 3 ( Implementation of Diffie-Hellman key exchange)**

# Public Values (Everyone can see this)

q = 353

alpha = 3

def calculate\_y\_value(X: int) -> int:

Y = (alpha \*\* X) % q

return Y

# User A

Xa = 97 # user selection

Ya = calculate\_y\_value(Xa)

print(Ya)

# User A sends values (q = 353, alpha = 3, Ya = 40) to User B

# Anyone can know these values

# User B

Xb = 233

Yb = calculate\_y\_value(Xb)

print(Yb)

# Send public value back (Yb = 248)

def generate\_key(X: int, Y: int) -> int:

K = (Y \*\* X) % q

return K

# User A

Ka = generate\_key(Xa, Yb)

print(Ka)

# User B

Kb = generate\_key(Xb, Ya)

print(Kb)

assert Ka == Kb

**Output:**

40

248

160

160