import math

import random

def point(a, b):

if (4\*(a\*\*3) + 27\*(b\*\*2)) != 0:

x = 1

while True:

rhs = (x\*\*3) + (a\*x) + b

y = int(math.sqrt(rhs))

lhs = (y\*\*2)

if lhs == rhs:

return [x, y]

else:

x += 1

else:

print("Enter another coefficients.")

a = int(input("Enter the coefficient 'a' of curve: "))

b = int(input("Enter the coefficient 'b' of curve: "))

private\_A = 13

private\_B = 15

generator = point(a, b)

print("Generator point: ", generator)

m = int(input("Enter the plaintext integer: "))

public\_key\_A = [private\_A\*generator[0], private\_A\*generator[1]]

print("Public Key of A: ", public\_key\_A)

public\_key\_B = [private\_B\*generator[0], private\_B\*generator[1]]

print("Public Key of B: ", public\_key\_B)

k = random.randint(0, 10)

print(k)

c1 = k \* (generator[0] + generator[1]) # same as K\* gen[0] + K\*gen[1]

c2 = m + ((k\*public\_key\_B[0]) + (k\*public\_key\_B[1]))

ciphertext = [c1, c2]

print("Ciphertext: ", ciphertext)

plaintext = c2 - (c1\*private\_B)

print("Decrypted Plaintext: ", plaintext)