In [1]:

```
import math
import random

def point(a, b):

    if (4*(a**3) + 27*(b**2)) != 0:
        x = 1
        print("generating")
        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)

c1 = k * (generator[0] + generator[1])

c2 = m + ((k*public_key_B[0]) + (k*public_key_B[1]))

ciphertext = [c1, c2]
print("Ciphertext: ", ciphertext)

r = private_B*c1

plaintext = c2 - r
print("Decrypted Plaintext: ", plaintext)
```

```
Enter the coefficient 'a' of curve: 3
Enter the coefficient 'b' of curve: 4
generating
Generator point:  [5, 12]
Enter the plaintext integer: 10001010
Public Key of A:  [65, 156]
Public Key of B:  [75, 180]
```

```
Ciphertext:  [102, 10002540]
Decrypted Plaintext:  10001010
```

In [ ]: