**ECC**

ECC stands for Elliptical Curve Cryptography. It takes point on a curve drawn and extract public and private key from that curve.

In step 1 the message is input, in our case, the message is

Step 2 is the key generation step where private and public key pair is extracted according to the curve. We have selected a random curve that is according to the secp256r1 standard. This outputs those curves that are not a Koblitz curve. Using the initial values as,

"p": 0xffffffff00000001000000000000000000000000ffffffffffffffffffffffff,

"a": 0xffffffff00000001000000000000000000000000fffffffffffffffffffffffc,

"b": 0x5ac635d8aa3a93e7b3ebbd55769886bc651d06b0cc53b0f63bce3c3e27d2604b,

"g":(0x6b17d1f2e12c4247f8bce6e563a440f277037d812deb33a0f4a13945d898c296,0x4fe342e2fe1a7f9b8ee7eb4a7c0f9e162bce33576b315ececbb6406837bf51f5),

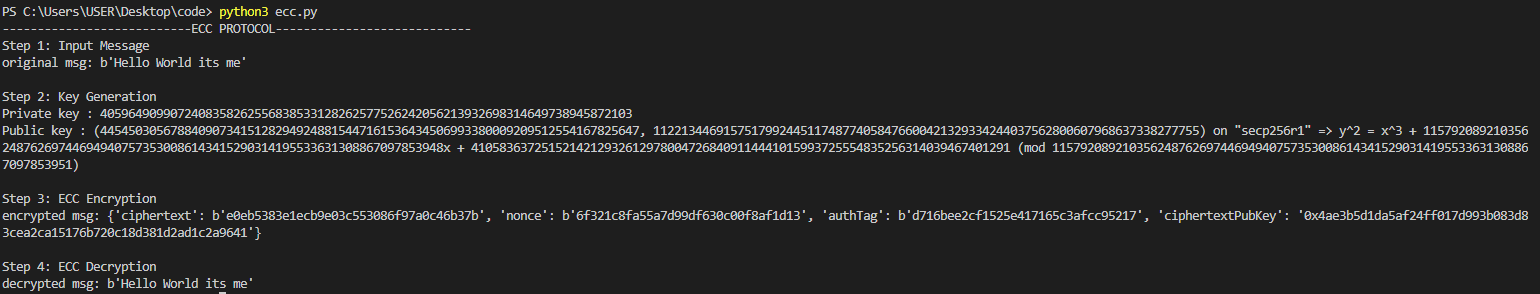
"n": 0xffffffff00000000ffffffffffffffffbce6faada7179e84f3b9cac2fc632551,

"h": 0x1},

For AES to encrypt we need a 256-bit key. The function ecc\_point\_to\_256\_bit\_key converts the point to a 256-bit key.

After that a function to encrypt the input message using the gcm mode of aes is used to encrypt. Similarly, a function to decrypt the cipher text message using the gcm mode of aes is used to decrypt.

**Output of the code**

****