Lab
Cryptography
Name: Smraddhi Rathore
Roll No: 2021bcy0025

```python
from tinyec import registry
import secrets

def compress(pubKey):
    return hex(pubKey.x) + hex(pubKey.y % 2)[2:]

curve = registry.get_curve('brainpoolP256r1')

alicePrivKey = secrets.randbelow(curve.field.n)
alicePubKey = alicePrivKey * curve.g
print("Alice Public key:", compress(alicePubKey))

bobPrivKey = secrets.randbelow(curve.field.n)
bobPubKey = bobPrivKey * curve.g
print("Bob Public key:", compress(bobPubKey))

print("Exchange the public key through internet")

aliceSharedKey = alicePrivKey * bobPubKey
print("Alice Shared Key:", compress(aliceSharedKey))

bobSharedKey =  bobPrivKey * alicePubKey
print("Bob Shared Key:", compress(bobSharedKey))

print("equal shared key:", aliceSharedKey == bobSharedKey )
```

```
PS C:\Users\IIITK\Documents\codes> & "c:/Program Files/Python311/python.exe" c:/Users/IIITK/Documents/codes/ecdh.py
Alice Public key: 0x22df88e0491a445ebba1689447bf1872416d8b03853af557ccaeb9fc69470bb80
Bob Public key: 0x3e892e8532a931ced034cf492abf530c83076daa25ce0c7d138be348dd3357f91
Now exchange the public key through internet
Alice Shared Key: 0x8693f37e2dd9a852a0bf8926cc67dff7e07f0f5d072c13e2b5ad28a0ec9943330
Bob Shared Key: 0x8693f37e2dd9a852a0bf8926cc67dff7e07f0f5d072c13e2b5ad28a0ec9943330
equal shared key: True
PS C:\Users\IIITK\Documents\codes>
```