

Kennan Lyle Seno
D14123582
Lab 8

Question 1

To run the python script, type 'python lab8-part1.py' in the terminal.

Output

```
Prime:23 Base:5

Alice Sends Over Public Channel: 8
Bob Sends Over Public Channel: 19

Alice Shared Secret: 2
Bob Shared Secret: 2
```

The screenshot above implement Diffie-Hellman key agreement.

Question 2

To run the python script, type 'python lab8-part2.py' in the terminal.

```
Ciphertext: aa19985cf15a2d9c7a817d1b2f9ce1c6ab47d31743f09958dd577fec5eea8c1235bc39514eae1bf7ca0c5369feb7da7c1da4c25f7b4f504977cacc22d7c
ac6f99abdabae13686cbc59b28520c8266cb1a03aa30a1c9fb6dd78c0344a98be9821b5fc3694aad9e5f9699bdcc0ae93125817ef4c72558748f74b07e2e08a51a816
Decrypted text: Hello World!
```

The screenshot above shows the 'Hello World!' message being encrypted a public key and then decrypted back using a private key.