# CYB101 Project 2

## **SSH Encryption and Decryption**

#### Screenshot #1: The appropriate encryption command and its' output

```
codepath@idx-cyb101-idx-1742096851850:~$ openssl pkeyutl -encrypt -pubin -inkey ~/.ssh/publickey.pem -in secret.txt -out secret.txt.encrypted codepath@idx-cyb101-idx-1742096851850:~$ cat secret.txt.
```

## Screenshot #2: The appropriate decryption command

```
codepath@idx-cyb101-idx-1742096851850:-$ openssl pkeyutl -decrypt -inkey ~/.ssh/privatekey.pem -in secret.txt.encrypted -out secret.txt.decrypted codepath@idx-cyb101-idx-1742096851850:~$ cat secret.txt.decrypted
My secret code is CHEESE
```

## Notes (Optional):

### Screenshot #3: The contents of all 3 files: original, encrypted, decrypted

```
codepath@idx-cyb101-idx-1742096851850:~$ openssl genrsa -out ~/.ssh/privatekey.pem 2048
openssl rsa -in ~/.ssh/privatekey.pem -out ~/.ssh/publickey.pem -pubout -outform PEM
writing RSA key
codepath@idx-cyb101-idx-1742096851850:~$ ls ~/.ssh
authorized_keys id_rsa_cyb101 id_rsa_cyb101.pub privatekey.pem publickey.pem ubuntu_key ubuntu_key.pub
codepath@idx-cyb101-idx-1742096851850:~$ echo "My secret code is CHEESE" > secret.txt
codepath@idx-cyb101-idx-1742096851850:~$ cat secret.txt
My secret code is CHEESE
codepath@idx-cyb101-idx-1742096851850:~$ openssl pkeyutl -encrypt -pubin -inkey ~/.ssh/publickey.pem -in secret.txt -out secret.txt.encrypted
codepath@idx-cyb101-idx-1742096851850:~$ cat secret.txt.encrypted
Wêôqê\êôôôT*"êô2"HôôÑ\êôôôxYêW%zk'n'êEôjôôôôôô$$pêU]êôMô
                                                  00 00z"00W0h0000y%000Sa000T
codepath@idx-cyb101-idx-1742096851850:~$ cat secret.txt.decrypted
My secret code is CHEESE
Notes (Optional):
```

# **SSH Git Commit Signing**

## Screenshot #4: The git commit command and its' output

codepath@idx-cyb101-idx-1742096851850:~/DemoProject\$ git commit --allow-empty --message="Did the SSH signing work?"
[master (root-commit) fe288bc] Did the SSH signing work?

Notes (Optional):

**Screenshot #5:** The git show --show-signature command and its' output, showing a successful signature

```
codepath@idx-cyb101-idx-1742096851850:~/DemoProject$ git show --show-signature
commit fe288bc1f227e8aa9a779bf625f71dad480a2815 (HEAD -> master)
Good "git" signature for * with RSA key SHA256:/0L8XIEP4vygzWodTkfNtoCFo0IRQBnRpLo0R5e2mjQ
Author: CYB101NAME <CYB101EMAIL>
Date: Sun Mar 16 04:11:37 2025 +0000

Did the SSH signing work?
codepath@idx-cyb101-idx-1742096851850:~/DemoProject$ []
```

Notes (Optional):