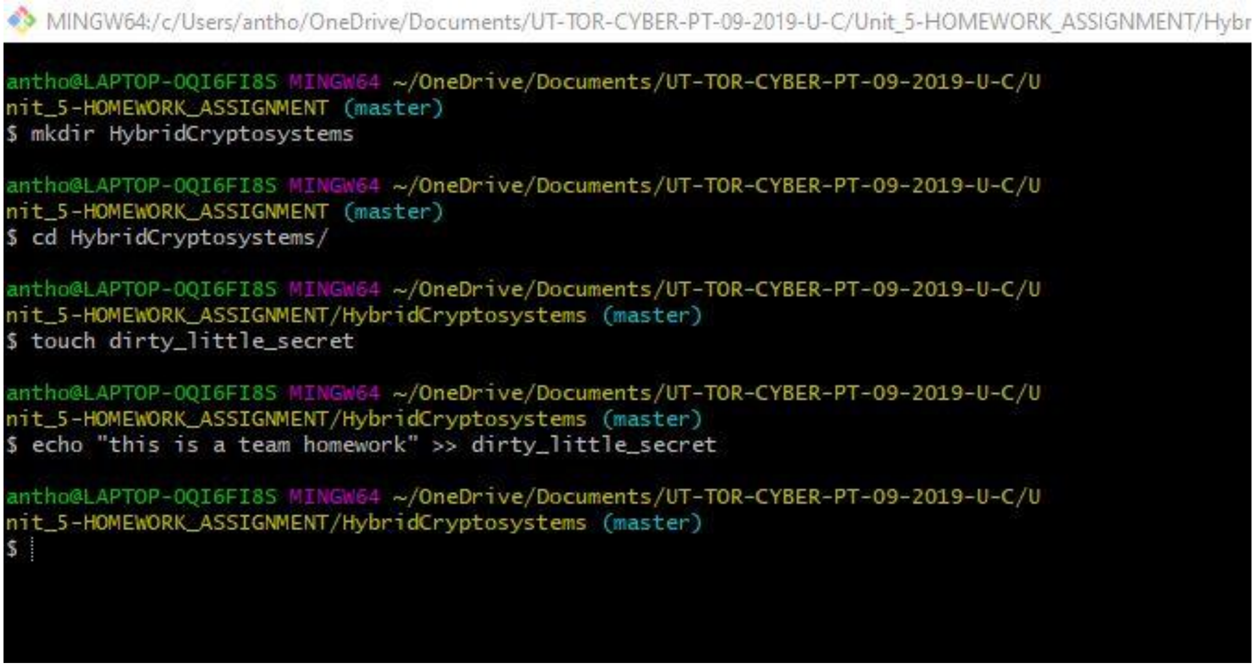
Hybrid Cryptosystems

Use a hybrid cryptosystem to exchange encrypted messages with your partner

Steps:

- Create a folder and file
- Use OpenSSL to generate an RSA keypair. This takes care of the **asymmetric** half of the hybrid system.
- Send your public key to your partner.
- Create a symmetric key so you can encrypt messages with AES.
- Use the symmetric key to encrypt a message.
- Use your asymmetric, _private_ key to encrypt your symmetric key.
- Send _both_ the encrypted message _and_ the encrypted symmetric key to your partner.
- On the other side, your partner will:
  a. Use your public key to decrypt the symmetric key
  b. Use the symmetric key to decrypt the message

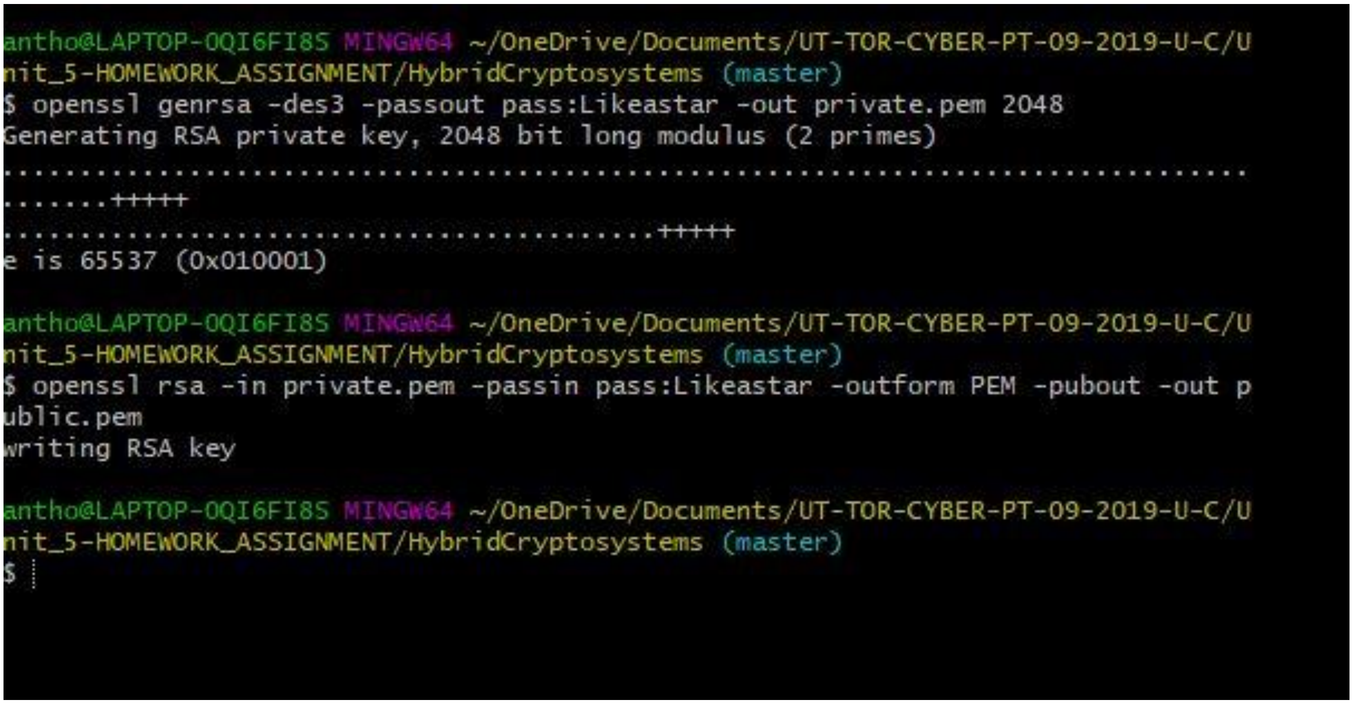
Step 1:



MINGW64:/c/Users/antho/OneDrive/Documents/UT-TOR-CYBER-PT-09-2019-U-C/Unit_5-HOMEWORK_ASSIGNMENT/Hybr

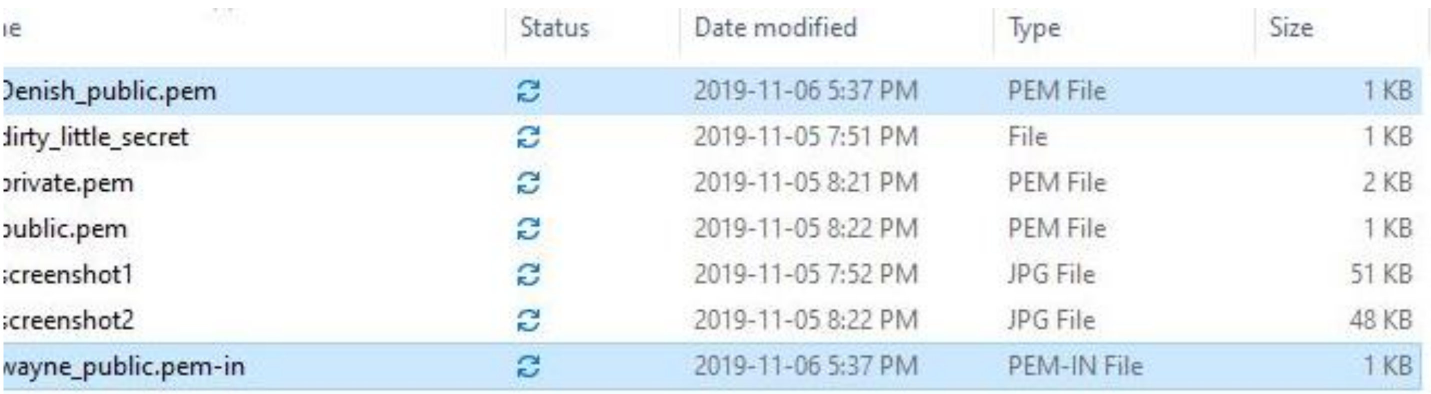
```
antho@LAPTOP-0QI6FI8S MINGW64 ~/OneDrive/Documents/UT-TOR-CYBER-PT-09-2019-U-C/U
nit_5-HOMEWORK_ASSIGNMENT (master)
$ mkdir HybridCryptosystems

antho@LAPTOP-0QI6FI8S MINGW64 ~/OneDrive/Documents/UT-TOR-CYBER-PT-09-2019-U-C/U
nit_5-HOMEWORK_ASSIGNMENT (master)
$ cd HybridCryptosystems/

antho@LAPTOP-0QI6FI8S MINGW64 ~/OneDrive/Documents/UT-TOR-CYBER-PT-09-2019-U-C/U
nit_5-HOMEWORK_ASSIGNMENT/HybridCryptosystems (master)
$ touch dirty_little_secret

antho@LAPTOP-0QI6FI8S MINGW64 ~/OneDrive/Documents/UT-TOR-CYBER-PT-09-2019-U-C/U
nit_5-HOMEWORK_ASSIGNMENT/HybridCryptosystems (master)
$ echo "this is a team homework" >> dirty_little_secret

antho@LAPTOP-0QI6FI8S MINGW64 ~/OneDrive/Documents/UT-TOR-CYBER-PT-09-2019-U-C/U
nit_5-HOMEWORK_ASSIGNMENT/HybridCryptosystems (master)
$
```

Step 2:



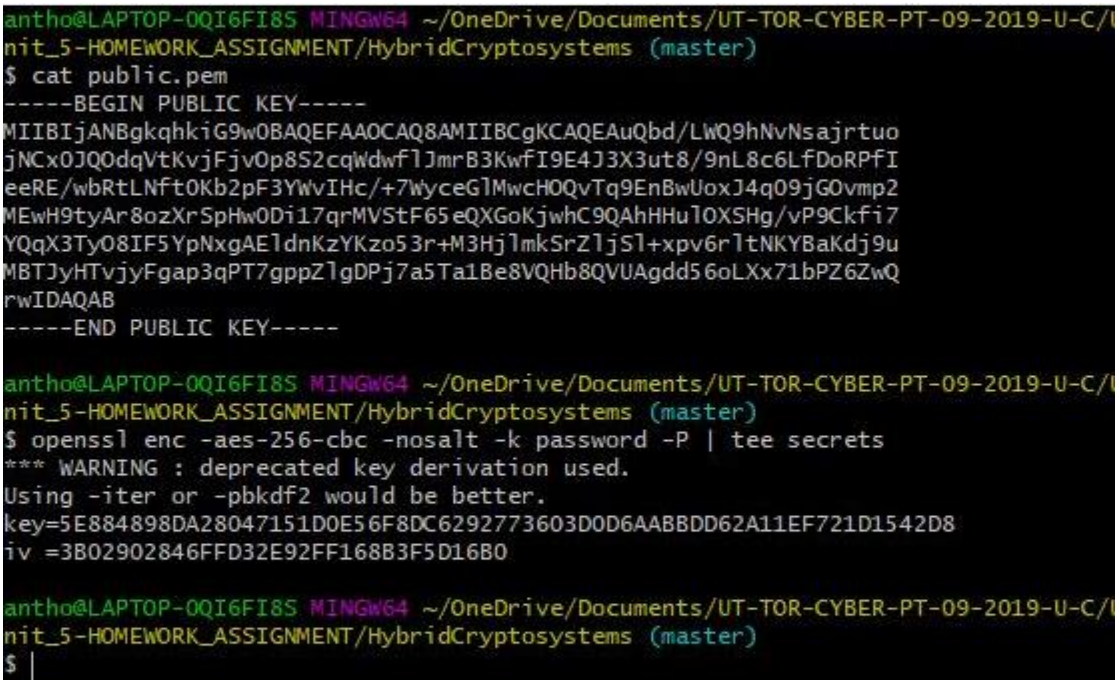
```
antho@LAPTOP-0QI6FI8S MINGW64 ~/OneDrive/Documents/UT-TOR-CYBER-PT-09-2019-U-C/U
nit_5-HOMEWORK_ASSIGNMENT/HybridCryptosystems (master)
$ openssl genrsa -des3 -passout pass:Likeastar -out private.pem 2048
Generating RSA private key, 2048 bit long modulus (2 primes)
...............................................................................
.......+++++
.........................................+++++
e is 65537 (0x010001)

antho@LAPTOP-0QI6FI8S MINGW64 ~/OneDrive/Documents/UT-TOR-CYBER-PT-09-2019-U-C/U
nit_5-HOMEWORK_ASSIGNMENT/HybridCryptosystems (master)
$ openssl rsa -in private.pem -passin pass:Likeastar -outform PEM -pubout -out p
ublic.pem
writing RSA key

antho@LAPTOP-0QI6FI8S MINGW64 ~/OneDrive/Documents/UT-TOR-CYBER-PT-09-2019-U-C/U
nit_5-HOMEWORK_ASSIGNMENT/HybridCryptosystems (master)
$
```

Step 3:



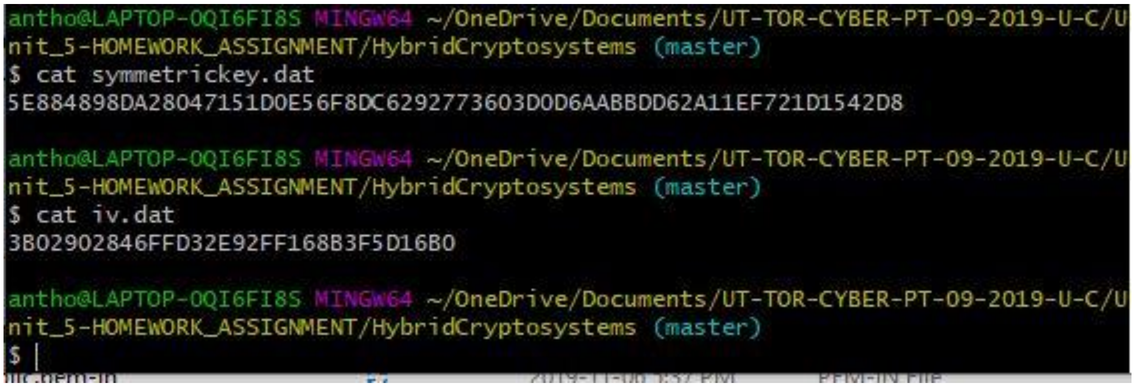
ıe	Status	Date modified	Type	Size
Denish_public.pem	⟳	2019-11-06 5:37 PM	PEM File	1 KB
dirty_little_secret	⟳	2019-11-05 7:51 PM	File	1 KB
private.pem	⟳	2019-11-05 8:21 PM	PEM File	2 KB
public.pem	⟳	2019-11-05 8:22 PM	PEM File	1 KB
screenshot1	⟳	2019-11-05 7:52 PM	JPG File	51 KB
screenshot2	⟳	2019-11-05 8:22 PM	JPG File	48 KB
wayne_public.pem-in	⟳	2019-11-06 5:37 PM	PEM-IN File	1 KB

Step 4:



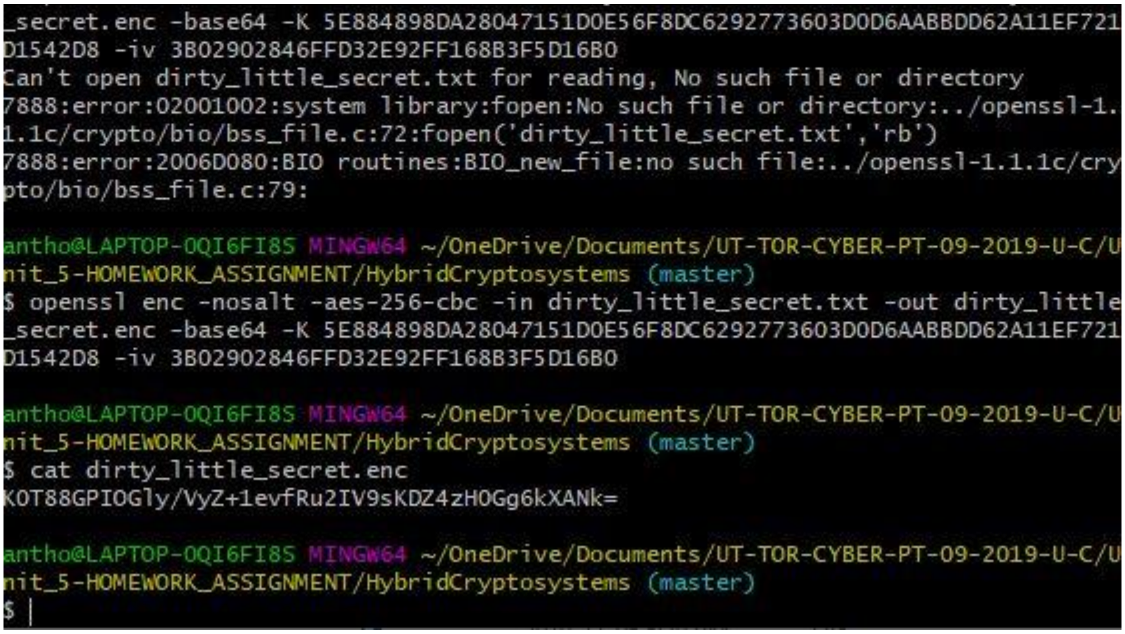
```
antho@LAPTOP-OQI6FI8S MINGW64 ~/OneDrive/Documents/UT-TOR-CYBER-PT-09-2019-U-C/U
nit_5-HOMEWORK_ASSIGNMENT/HybridCryptosystems (master)
$ cat public.pem
-----BEGIN PUBLIC KEY-----
MIIBIjANBgkqhkiG9w0BAQEFAAOCAQ8AMIIBCgKCAQEAuQbd/LWQ9hNvNsajrtuo
jNCx0JQOdqVtKvjFjvOp8S2cqWdwflJmrB3KwfI9E4J3X3ut8/9nL8c6LfDoRPfI
eeRE/wbRtLNft0Kb2pF3YWvIHc/+7WyceGlMwcHOQvTq9EnBwUoxJ4q09jGOvmp2
MEwH9tyAr8ozXrSpHwODi17qrMVStF65eQXGoKjwhC9QAhHHulOXSHg/vP9Ckfi7
YQqX3TyO8IF5YpNxgAEldnKzYKzo53r+M3HjlmkSrZljSl+xpv6rltNKYBaKdj9u
MBTJyHTvjyFgap3qPT7gppZlgDPj7a5Ta1Be8VQHb8QVUAgdd56oLXx71bPZ6ZwQ
rwIDAQAB
-----END PUBLIC KEY-----

antho@LAPTOP-OQI6FI8S MINGW64 ~/OneDrive/Documents/UT-TOR-CYBER-PT-09-2019-U-C/U
nit_5-HOMEWORK_ASSIGNMENT/HybridCryptosystems (master)
$ openssl enc -aes-256-cbc -nosalt -k password -P | tee secrets
*** WARNING : deprecated key derivation used.
Using -iter or -pbkdf2 would be better.
key=5E884898DA28047151D0E56F8DC6292773603D0D6AABBDD62A11EF721D1542D8
iv =3B02902846FFD32E92FF168B3F5D16B0

antho@LAPTOP-OQI6FI8S MINGW64 ~/OneDrive/Documents/UT-TOR-CYBER-PT-09-2019-U-C/U
nit_5-HOMEWORK_ASSIGNMENT/HybridCryptosystems (master)
$ |
```

Step 5:



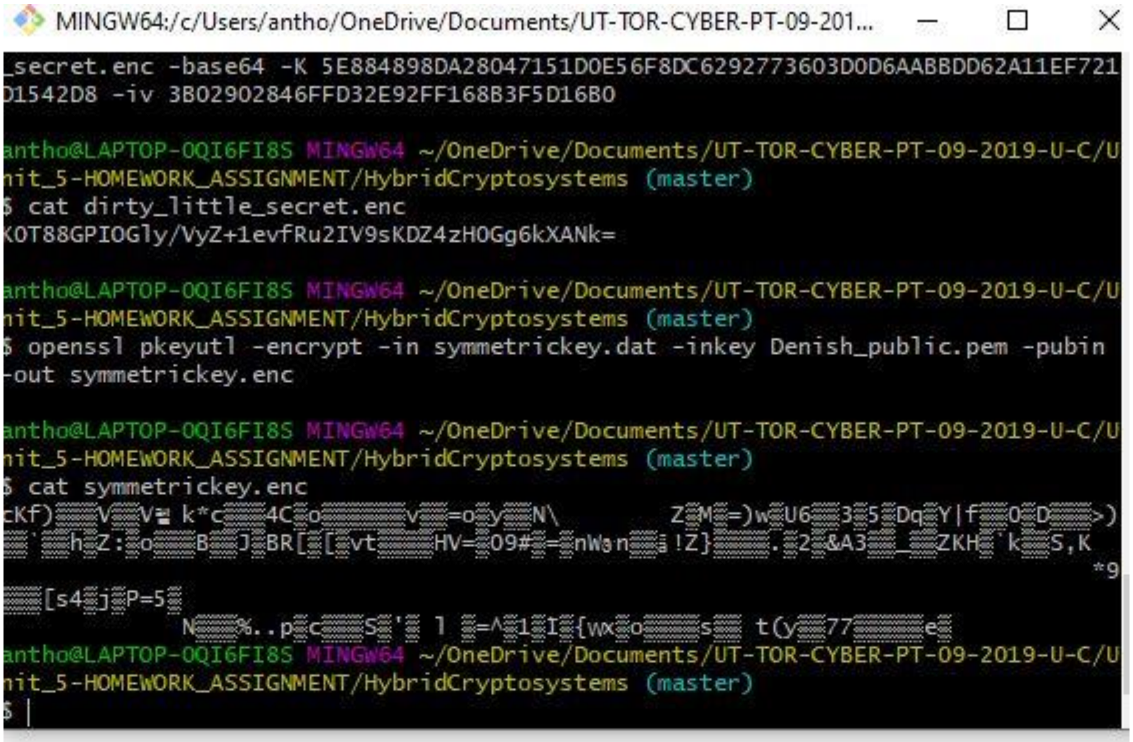
```
antho@LAPTOP-OQI6FI8S MINGW64 ~/OneDrive/Documents/UT-TOR-CYBER-PT-09-2019-U-C/U
nit_5-HOMEWORK_ASSIGNMENT/HybridCryptosystems (master)
$ cat symmetrickey.dat
5E884898DA28047151D0E56F8DC6292773603D0D6AABBDD62A11EF721D1542D8

antho@LAPTOP-OQI6FI8S MINGW64 ~/OneDrive/Documents/UT-TOR-CYBER-PT-09-2019-U-C/U
nit_5-HOMEWORK_ASSIGNMENT/HybridCryptosystems (master)
$ cat iv.dat
3B02902846FFD32E92FF168B3F5D16B0

antho@LAPTOP-OQI6FI8S MINGW64 ~/OneDrive/Documents/UT-TOR-CYBER-PT-09-2019-U-C/U
nit_5-HOMEWORK_ASSIGNMENT/HybridCryptosystems (master)
$ |
```

Step 6:



```
_secret.enc -base64 -K 5E884898DA28047151D0E56F8DC6292773603D0D6AABBDD62A11EF721
D1542D8 -iv 3B02902846FFD32E92FF168B3F5D16B0
Can't open dirty_little_secret.txt for reading, No such file or directory
7888:error:02001002:system library:fopen:No such file or directory:../openssl-1.
1.1c/crypto/bio/bss_file.c:72:fopen('dirty_little_secret.txt','rb')
7888:error:2006D080:BIO routines:BIO_new_file:no such file:../openssl-1.1.1c/cry
pto/bio/bss_file.c:79:

antho@LAPTOP-0QI6FI8S MINGW64 ~/OneDrive/Documents/UT-TOR-CYBER-PT-09-2019-U-C/U
nit_5-HOMEWORK_ASSIGNMENT/HybridCryptosystems (master)
$ openssl enc -nosalt -aes-256-cbc -in dirty_little_secret.txt -out dirty_little
_secret.enc -base64 -K 5E884898DA28047151D0E56F8DC6292773603D0D6AABBDD62A11EF721
D1542D8 -iv 3B02902846FFD32E92FF168B3F5D16B0

antho@LAPTOP-0QI6FI8S MINGW64 ~/OneDrive/Documents/UT-TOR-CYBER-PT-09-2019-U-C/U
nit_5-HOMEWORK_ASSIGNMENT/HybridCryptosystems (master)
$ cat dirty_little_secret.enc
KOT88GPIOGly/VyZ+1evfRu2IV9sKDZ4zHOGg6kXANk=

antho@LAPTOP-0QI6FI8S MINGW64 ~/OneDrive/Documents/UT-TOR-CYBER-PT-09-2019-U-C/U
nit_5-HOMEWORK_ASSIGNMENT/HybridCryptosystems (master)
$ |
```

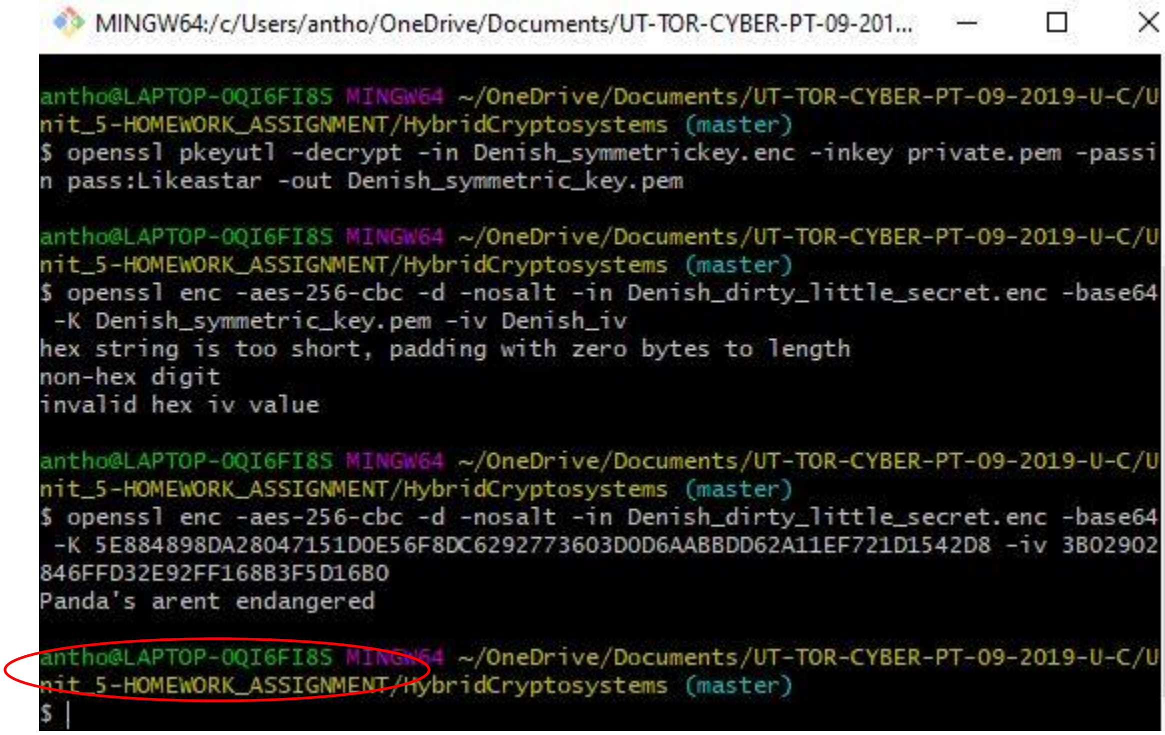
Step 7:



MINGW64:/c/Users/antho/OneDrive/Documents/UT-TOR-CYBER-PT-09-201...

```
_secret.enc -base64 -K 5E884898DA28047151D0E56F8DC6292773603D0D6AABBDD62A11EF721
D1542D8 -iv 3B02902846FFD32E92FF168B3F5D16B0

antho@LAPTOP-0QI6FI8S MINGW64 ~/OneDrive/Documents/UT-TOR-CYBER-PT-09-2019-U-C/U
nit_5-HOMEWORK_ASSIGNMENT/HybridCryptosystems (master)
$ cat dirty_little_secret.enc
KOT88GPIOGly/VyZ+1evfRu2IV9sKDZ4zHOGg6kXANk=

antho@LAPTOP-0QI6FI8S MINGW64 ~/OneDrive/Documents/UT-TOR-CYBER-PT-09-2019-U-C/U
nit_5-HOMEWORK_ASSIGNMENT/HybridCryptosystems (master)
$ openssl pkeyutl -encrypt -in symmetrickey.dat -inkey Denish_public.pem -pubin
-out symmetrickey.enc

antho@LAPTOP-0QI6FI8S MINGW64 ~/OneDrive/Documents/UT-TOR-CYBER-PT-09-2019-U-C/U
nit_5-HOMEWORK_ASSIGNMENT/HybridCryptosystems (master)
$ cat symmetrickey.enc
cKf)▒▒V▒V▒ k*c▒▒4C▒o▒▒▒▒v▒=o▒y▒N\        Z▒M▒=)w▒U6▒3▒5▒Dq▒Y|f▒0▒D▒▒>)
▒▒`▒▒h▒Z:▒o▒▒B▒J▒BR[▒[▒vt▒▒▒HV=▒09#▒=▒nW▒n▒▒!Z}▒▒▒▒.▒2▒&A3▒▒_▒▒ZKH▒`k▒▒S,K
                                                                          *9
▒▒[s4▒j▒P=5▒
            N▒▒%..p▒c▒▒S▒'▒ l ▒=^▒1▒I▒{wx▒o▒▒▒s▒▒ t(y▒77▒▒▒▒e▒
antho@LAPTOP-0QI6FI8S MINGW64 ~/OneDrive/Documents/UT-TOR-CYBER-PT-09-2019-U-C/U
nit_5-HOMEWORK_ASSIGNMENT/HybridCryptosystems (master)
$ |
```

Step 8:



MINGW64:/c/Users/antho/OneDrive/Documents/UT-TOR-CYBER-PT-09-201...

```
antho@LAPTOP-0QI6FI8S MINGW64 ~/OneDrive/Documents/UT-TOR-CYBER-PT-09-2019-U-C/U
nit_5-HOMEWORK_ASSIGNMENT/HybridCryptosystems (master)
$ openssl pkeyutl -decrypt -in Denish_symmetrickey.enc -inkey private.pem -passi
n pass:Likeastar -out Denish_symmetric_key.pem

antho@LAPTOP-0QI6FI8S MINGW64 ~/OneDrive/Documents/UT-TOR-CYBER-PT-09-2019-U-C/U
nit_5-HOMEWORK_ASSIGNMENT/HybridCryptosystems (master)
$ openssl enc -aes-256-cbc -d -nosalt -in Denish_dirty_little_secret.enc -base64
 -K Denish_symmetric_key.pem -iv Denish_iv
hex string is too short, padding with zero bytes to length
non-hex digit
invalid hex iv value

antho@LAPTOP-0QI6FI8S MINGW64 ~/OneDrive/Documents/UT-TOR-CYBER-PT-09-2019-U-C/U
nit_5-HOMEWORK_ASSIGNMENT/HybridCryptosystems (master)
$ openssl enc -aes-256-cbc -d -nosalt -in Denish_dirty_little_secret.enc -base64
 -K 5E884898DA28047151D0E56F8DC6292773603D0D6AABBDD62A11EF721D1542D8 -iv 3B02902
846FFD32E92FF168B3F5D16B0
Panda's arent endangered

antho@LAPTOP-0QI6FI8S MINGW64 ~/OneDrive/Documents/UT-TOR-CYBER-PT-09-2019-U-C/U
nit_5-HOMEWORK_ASSIGNMENT/HybridCryptosystems (master)
$ |
```