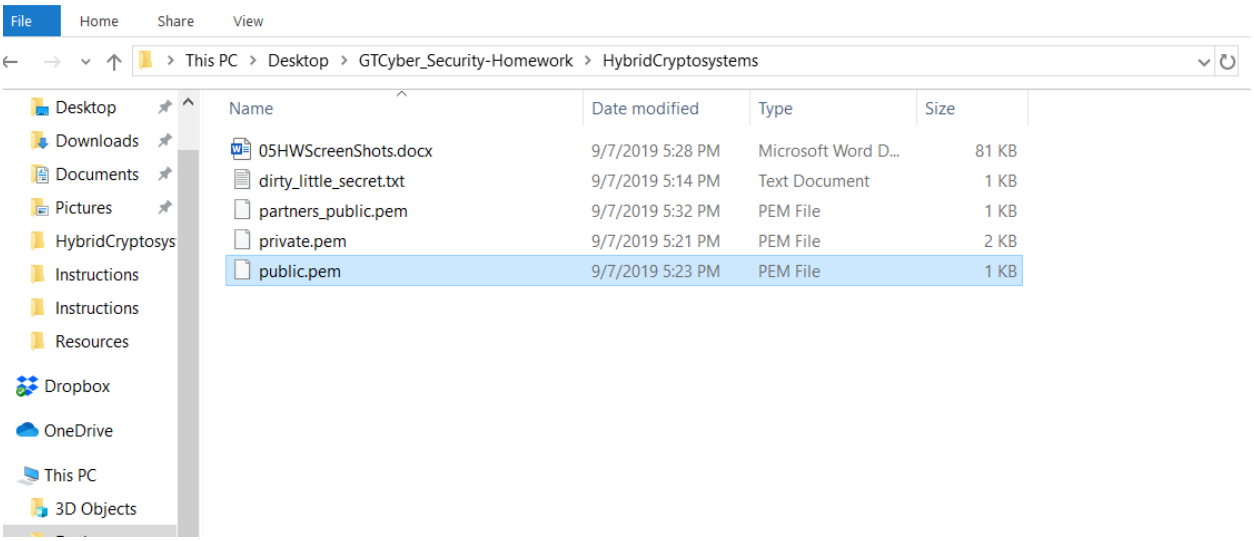
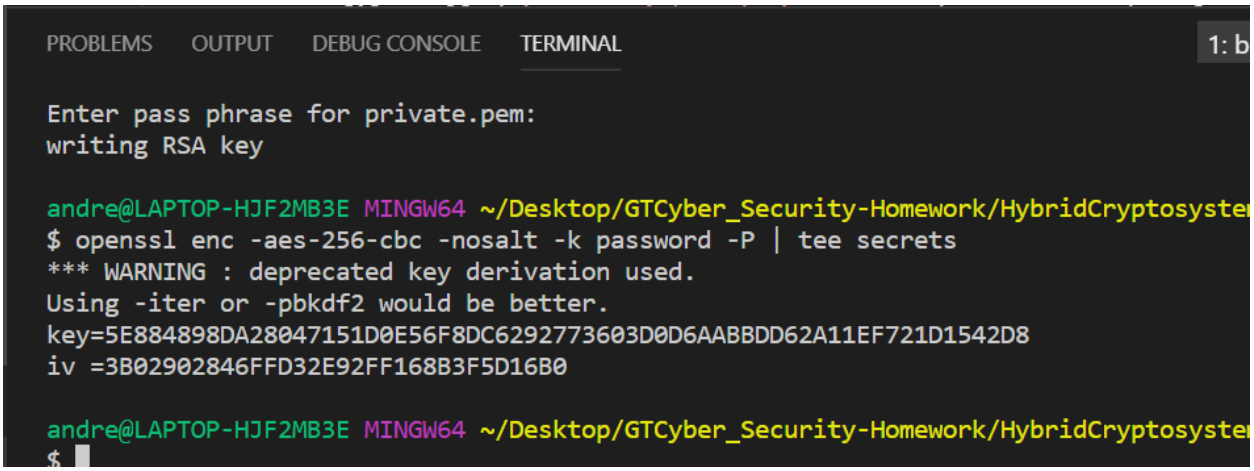
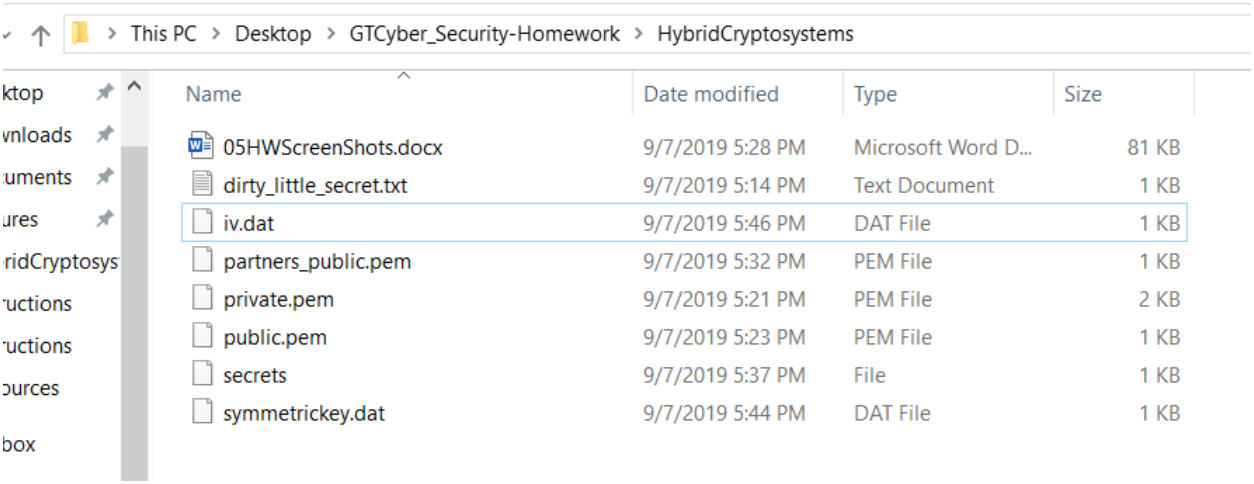
Make a Confession/Generate and RSA Keypair

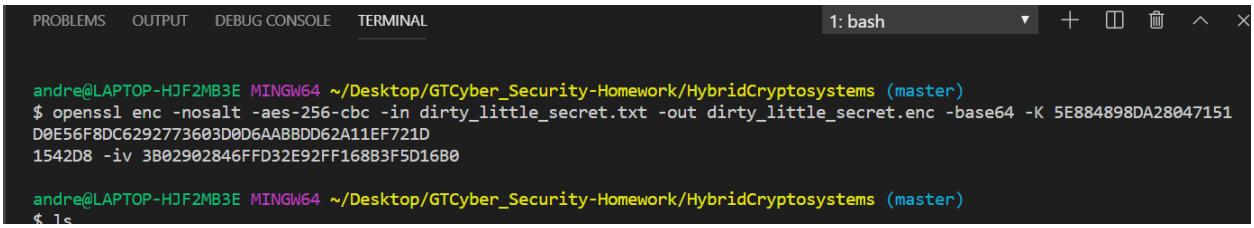
```
$ touch dirty_little_secret.txt

andre@LAPTOP-HJF2MB3E MINGW64 ~/Desktop/GTCyber_Security-Homework/HybridCryptosystems (master)
$ openssl genrsa -des3 -out private.pem 2048
Generating RSA private key, 2048 bit long modulus (2 primes)
...........+++++
...................+++++
e is 65537 (0x010001)
Enter pass phrase for private.pem:
Verifying - Enter pass phrase for private.pem:

andre@LAPTOP-HJF2MB3E MINGW64 ~/Desktop/GTCyber_Security-Homework/HybridCryptosystems (master)
$ openssl rsa -in private.pem -outform PEM -pubout -out public.pem
Enter pass phrase for private.pem:
writing RSA key

andre@LAPTOP-HJF2MB3E MINGW64 ~/Desktop/GTCyber_Security-Homework/HybridCryptosystems (master)
$
```



Generate an AES Key

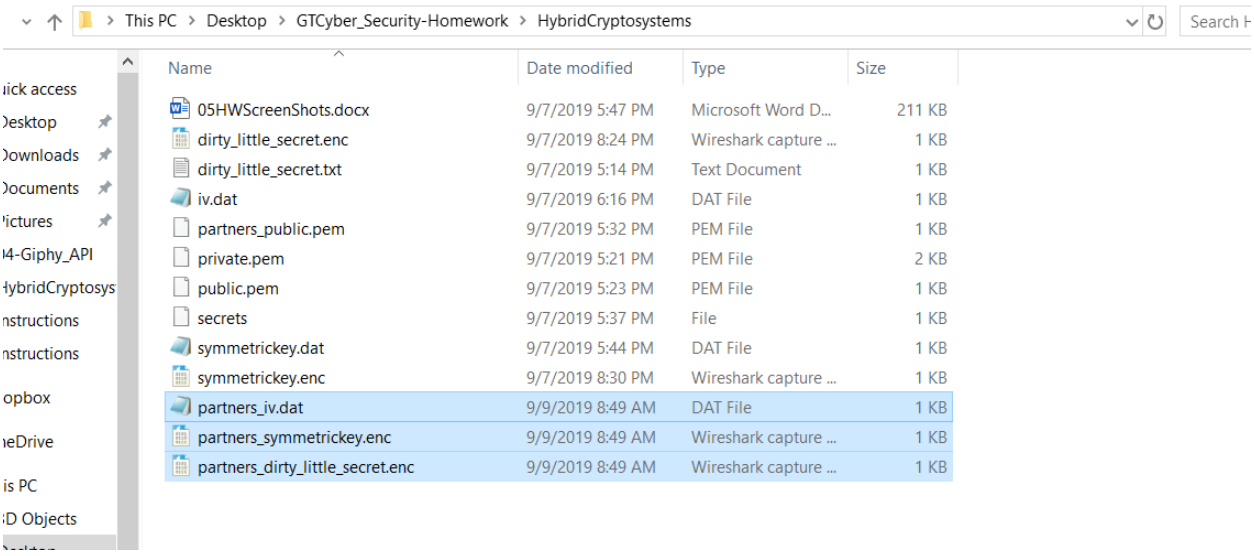


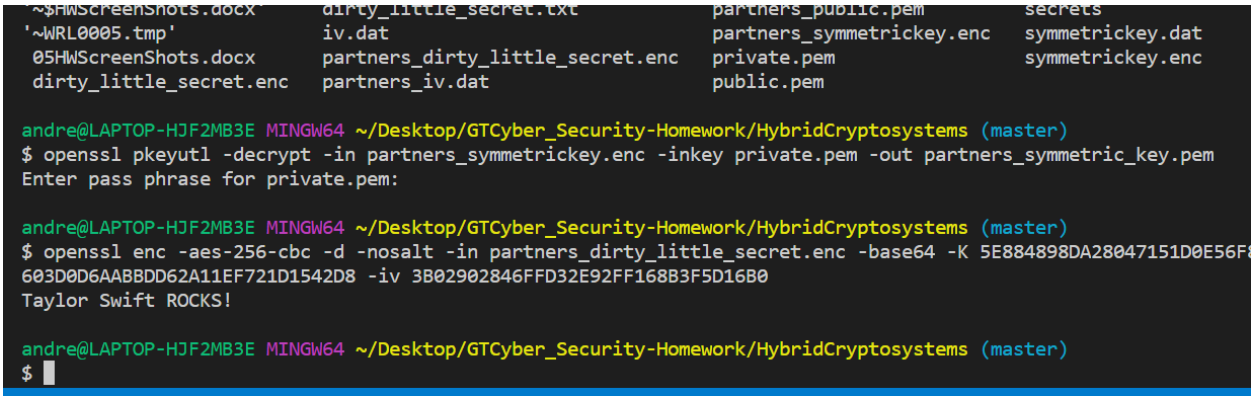




```
andre@LAPTOP-HJF2MB3E MINGW64 ~/Desktop/GTCyber_Security-Homework/HybridCryptosystems (master)
$ cat dirty_little_secret.en
cat: dirty_little_secret.en: No such file or directory

andre@LAPTOP-HJF2MB3E MINGW64 ~/Desktop/GTCyber_Security-Homework/HybridCryptosystems (master)
$ cat dirty_little_secret.enc
xBu0mrcHw0e7pWG7JJa6AmMFTTrAYS6fZTUpx3CPDxKAwUHb+hDC/4yzcXiXq3ka
/LuNXQofQ2P5PK83Z88I2ulAhXwma3HwsIe8YZHrHYD5PrRn9ERHJPCNGTjhPwqp
L3ccUd49JFQBVpHWwK6pIgy73AlaLTEovdz6w5lwy8E=

andre@LAPTOP-HJF2MB3E MINGW64 ~/Desktop/GTCyber_Security-Homework/HybridCryptosystems (master)
$
```

```
andre@LAPTOP-HJF2MB3E MINGW64 ~/Desktop/GTCyber_Security-Homework/HybridCryptosystems (master)
$ openssl pkeyutl -encrypt -in symmetrickey.dat -inkey partners_public.pem -pubin -out symmetrickey.enc

andre@LAPTOP-HJF2MB3E MINGW64 ~/Desktop/GTCyber_Security-Homework/HybridCryptosystems (master)
$ cat symmetrickey.enc
 f"I )<□1!      V 戚(W 1 ,1 TO 1  k j |*  ;J -     F FG Y Y A}  _\I  ,  q &  j/ I ]n 0oe Fc

andre@LAPTOP-HJF2MB3E MINGW64 ~/Desktop/GTCyber_Security-Homework/HybridCryptosystems (master)
```




'~$HWScreenShots.docx' dirty_little_secret.txt partners_public.pem secrets
'~WRL0005.tmp' iv.dat partners_symmetrickey.enc symmetrickey.dat
05HWScreenShots.docx partners_dirty_little_secret.enc private.pem symmetrickey.enc
dirty_little_secret.enc partners_iv.dat public.pem
andre@LAPTOP-HJF2MB3E MINGW64 ~/Desktop/GTCyber_Security-Homework/HybridCryptosystems (master)
$ openssl pkeyutl -decrypt -in partners_symmetrickey.enc -inkey private.pem -out partners_symmetric_key.pem
Enter pass phrase for private.pem:
andre@LAPTOP-HJF2MB3E MINGW64 ~/Desktop/GTCyber_Security-Homework/HybridCryptosystems (master)
$ openssl enc -aes-256-cbc -d -nosalt -in partners_dirty_little_secret.enc -base64 -K 5E884898DA28047151D0E56F
603D0D6AABBDD62A11EF721D1542D8 -iv 3B02902846FFD32E92FF168B3F5D16B0
Taylor Swift ROCKS!
andre@LAPTOP-HJF2MB3E MINGW64 ~/Desktop/GTCyber_Security-Homework/HybridCryptosystems (master)
$