

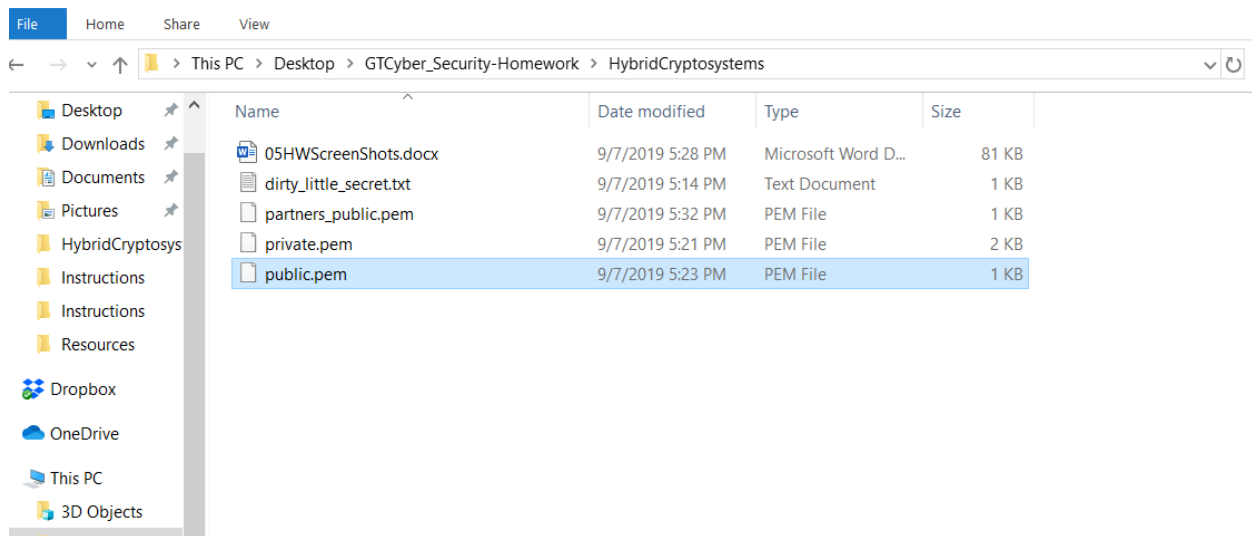
Make a Confession/Generate and RSA Keypair

```
$ 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

```
PROBLEMS  OUTPUT  DEBUG CONSOLE  TERMINAL  1: b

Enter pass phrase for private.pem:
writing RSA key

andre@LAPTOP-HJF2MB3E MINGW64 ~/Desktop/GTCyber_Security-Homework/HybridCryptosystems
$ openssl enc -aes-256-cbc -nosalt -k password -P | tee secrets
*** WARNING : deprecated key derivation used.
Using -iter or -pbkdf2 would be better.
key=5E884898DA28047151D0E56F8DC6292773603D0D6AABDD62A11EF721D1542D8
iv =3B02902846FFD32E92FF168B3F5D16B0

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

✓ ↑ > This PC > Desktop > GTCyber_Security-Homework > HybridCryptosystems

	Name	Date modified	Type	Size
ktop				
vnloads				
uments				
ures				
ridCryptosys				
uctions				
uctions				
ources				
box				
	05HWScreenShots.docx	9/7/2019 5:28 PM	Microsoft Word D...	81 KB
	dirty_little_secret.txt	9/7/2019 5:14 PM	Text Document	1 KB
	iv.dat	9/7/2019 5:46 PM	DAT File	1 KB
	partners_public.pem	9/7/2019 5:32 PM	PEM File	1 KB
	private.pem	9/7/2019 5:21 PM	PEM File	2 KB
	public.pem	9/7/2019 5:23 PM	PEM File	1 KB
	secrets	9/7/2019 5:37 PM	File	1 KB
	symmetrickey.dat	9/7/2019 5:44 PM	DAT File	1 KB

```
PROBLEMS  OUTPUT  DEBUG CONSOLE  TERMINAL  1: bash

andre@LAPTOP-HJF2MB3E MINGW64 ~/Desktop/GTCyber_Security-Homework/HybridCryptosystems (master)
$ openssl enc -nosalt -aes-256-cbc -in dirty_little_secret.txt -out dirty_little_secret.enc -base64 -K 5E884898DA28047151
D0E56F8DC6292773603D0D6AABDD62A11EF721D
1542D8 -iv 3B02902846FFD32E92FF168B3F5D16B0

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

```

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
xBu0mrcHw0e7pWg7JJJa6AmMFTTrAYS6fZTUpX3CPDxKAwUHb+hDC/4yzcXiXq3ka
/LuNXQofQ2P5PK83Z88I2u1AhXwma3HwsIe8YZHrHYD5PrRn9ERHJPCNGTjhPwqp
L3ccUd49JFQBVPwK6pIgy73AlaLTEovdz6w5lwy8E=

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"l" < [! V 戚 (w l , l TO l k j | * ; J - F F6 Y Y A } _ \ I _ q & || j / r I ] n Ooe Fc

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

```

File Explorer view of the directory: This PC > Desktop > GTCyber_Security-Homework > HybridCryptosystems

Name	Date modified	Type	Size
05HWScreenShots.docx	9/7/2019 5:47 PM	Microsoft Word D...	211 KB
dirty_little_secret.enc	9/7/2019 8:24 PM	Wireshark capture ...	1 KB
dirty_little_secret.txt	9/7/2019 5:14 PM	Text Document	1 KB
iv.dat	9/7/2019 6:16 PM	DAT File	1 KB
partners_public.pem	9/7/2019 5:32 PM	PEM File	1 KB
private.pem	9/7/2019 5:21 PM	PEM File	2 KB
public.pem	9/7/2019 5:23 PM	PEM File	1 KB
secrets	9/7/2019 5:37 PM	File	1 KB
symmetrickey.dat	9/7/2019 5:44 PM	DAT File	1 KB
symmetrickey.enc	9/7/2019 8:30 PM	Wireshark capture ...	1 KB
partners_iv.dat	9/9/2019 8:49 AM	DAT File	1 KB
partners_symmetrickey.enc	9/9/2019 8:49 AM	Wireshark capture ...	1 KB
partners_dirty_little_secret.enc	9/9/2019 8:49 AM	Wireshark capture ...	1 KB

```
~$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 5E884898DA28047151D0E56F603D0D6AABDD62A11EF721D1542D8 -iv 3B02902846FFD32E92FF168B3F5D16B0
Taylor Swift ROCKS!
```

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

```
$ █
```