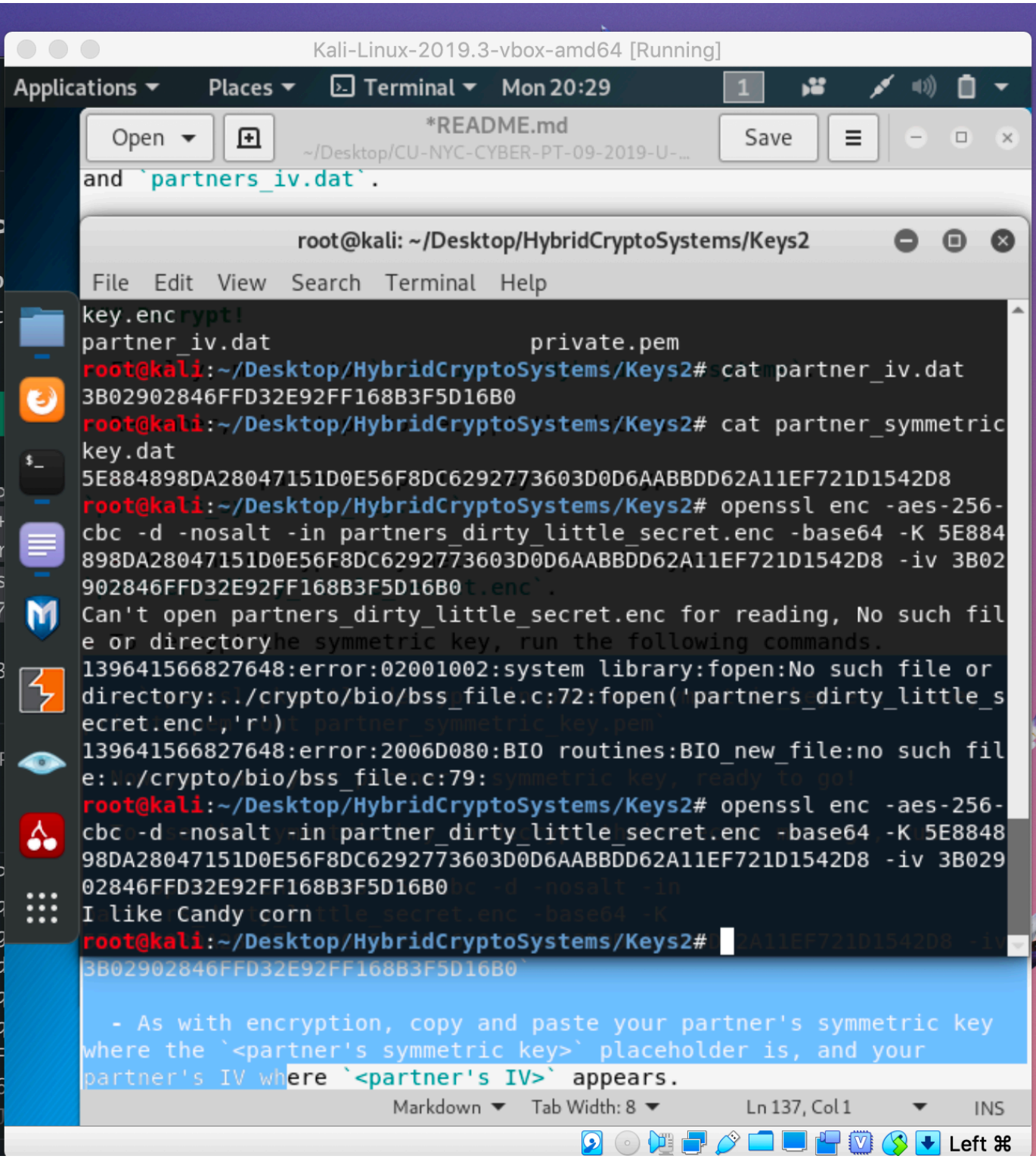

Kali-Linux-2019.3-vbox-amd64 [Running]
Applications
Places
Terminal
Mon 20:29
Open
*README.md
~/Desktop/CU-NYC-CYBER-PT-09-2019-U-...
Save
and `partners_iv.dat`.
root@kali: ~/Desktop/HybridCryptoSystems/Keys2
File Edit View Search Terminal Help
key.encrypt!
partner_iv.dat private.pem
root@kali:~/Desktop/HybridCryptoSystems/Keys2# cat partner_iv.dat
3B02902846FFD32E92FF168B3F5D16B0
root@kali:~/Desktop/HybridCryptoSystems/Keys2# cat partner_symmetric
key.dat
5E884898DA28047151D0E56F8DC6292773603D0D6AABBDD62A11EF721D1542D8
root@kali:~/Desktop/HybridCryptoSystems/Keys2# openssl enc -aes-256-
cbc -d -nosalt -in partners_dirty_little_secret.enc -base64 -K 5E884
898DA28047151D0E56F8DC6292773603D0D6AABBDD62A11EF721D1542D8 -iv 3B02
902846FFD32E92FF168B3F5D16B0
Can't open partners_dirty_little_secret.enc for reading, No such fil
e or directory
139641566827648:error:02001002:system library:fopen:No such file or
directory:../crypto/bio/bss_file.c:72:fopen('partners_dirty_little_s
ecret.enc','r')
139641566827648:error:2006D080:BIO routines:BIO_new_file:no such fil
e:../crypto/bio/bss_file.c:79:
root@kali:~/Desktop/HybridCryptoSystems/Keys2# openssl enc -aes-256-
cbc -d -nosalt -in partner_dirty_little_secret.enc -base64 -K 5E8848
98DA28047151D0E56F8DC6292773603D0D6AABBDD62A11EF721D1542D8 -iv 3B029
02846FFD32E92FF168B3F5D16B0
I like Candy corn
root@kali:~/Desktop/HybridCryptoSystems/Keys2#
3B02902846FFD32E92FF168B3F5D16B0`
- As with encryption, copy and paste your partner's symmetric key
where the `<partner's symmetric key>` placeholder is, and your
partner's IV where `<partner's IV>` appears.
Markdown
Tab Width: 8
Ln 137, Col 1
INS
Left ⌘

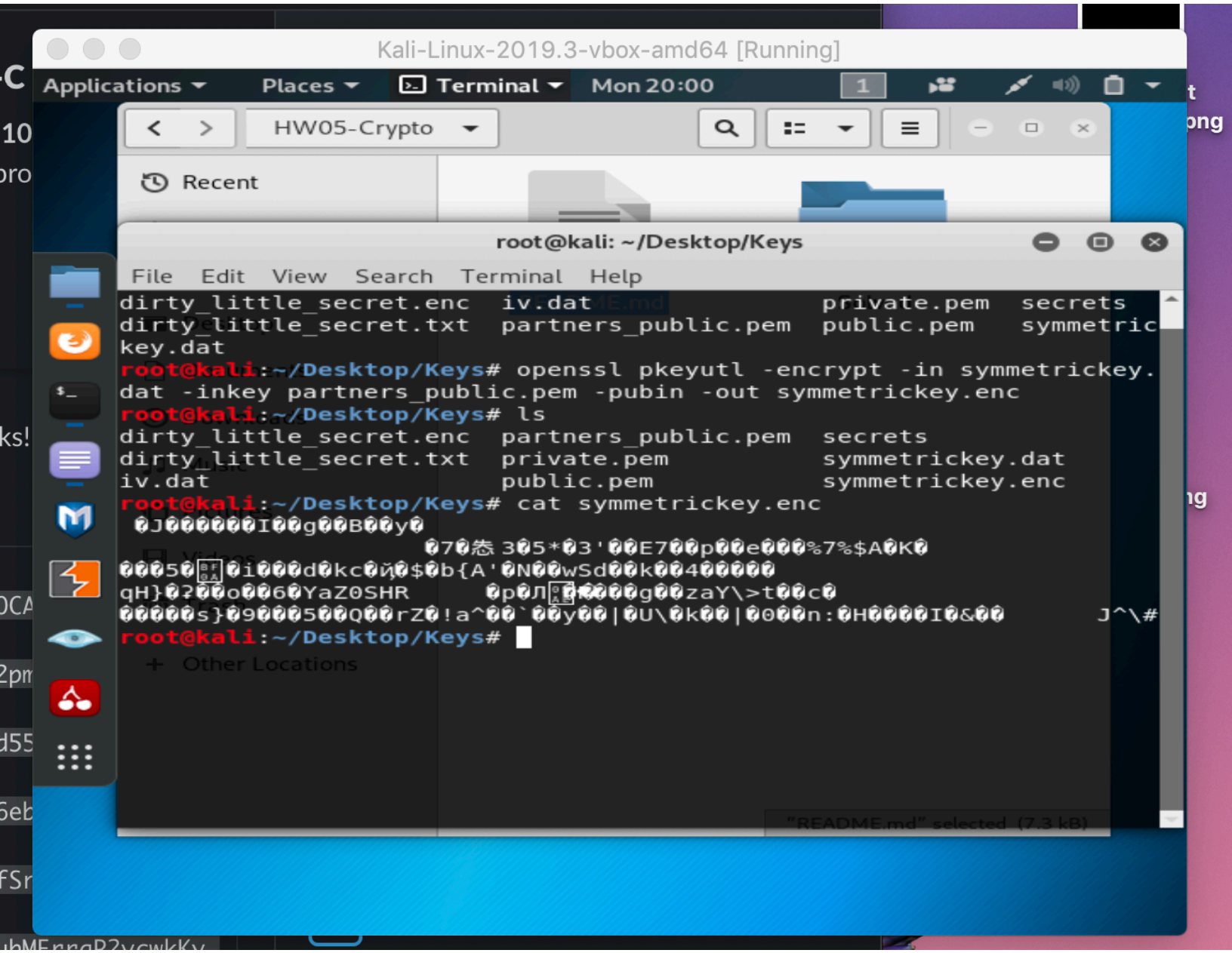
```
Rebeccas-MacBook-Pro:EncryptionAssignment rebeccabartels$ ls
Key1    Key2
Rebeccas-MacBook-Pro:EncryptionAssignment rebeccabartels$ cd Key2/
Rebeccas-MacBook-Pro:Key2 rebeccabartels$ ls
Rebeccas-MacBook-Pro:Key2 rebeccabartels$ openssl genrsa -des3 -out private.pem 2048
Generating RSA private key, 2048 bit long modulus
..............................+++
...........+++
e is 65537 (0x10001)
Enter pass phrase for private.pem:
Verifying - Enter pass phrase for private.pem:
Rebeccas-MacBook-Pro:Key2 rebeccabartels$ openssl rsa -in private.pem -outform PEM -pubout -out public.pem
Enter pass phrase for private.pem:
writing RSA key
Rebeccas-MacBook-Pro:Key2 rebeccabartels$
```

```
Rebeccas-MacBook-Pro:EncryptionAssignment rebeccabartels$ ls
Key1    Key2
Rebeccas-MacBook-Pro:EncryptionAssignment rebeccabartels$ cd Key2/
Rebeccas-MacBook-Pro:Key2 rebeccabartels$ ls
Rebeccas-MacBook-Pro:Key2 rebeccabartels$ openssl genrsa -des3 -out private.pem 2048
Generating RSA private key, 2048 bit long modulus
..............................+++
...........+++
e is 65537 (0x10001)
Enter pass phrase for private.pem:
Verifying - Enter pass phrase for private.pem:
Rebeccas-MacBook-Pro:Key2 rebeccabartels$ openssl rsa -in private.pem -outform PEM -pubout -out public.pem
Enter pass phrase for private.pem:
writing RSA key
Rebeccas-MacBook-Pro:Key2 rebeccabartels$
```

```
Rebeccas-MacBook-Pro:Key1 rebeccabartels$ ls
secrets.txt
Rebeccas-MacBook-Pro:Key1 rebeccabartels$ openssl enc -aes-256-cbc -nosalt -k password -P | tee secrets
key=5F4DCC3B5AA765D61D8327DEB882CF992B95990A9151374ABD8FF8C5A7A0FE08
iv =B7B4372CDFBCB3D16A2631B59B509E94
Rebeccas-MacBook-Pro:Key1 rebeccabartels$ ls
secrets         secrets.txt
Rebeccas-MacBook-Pro:Key1 rebeccabartels$ cat secrets
key=5F4DCC3B5AA765D61D8327DEB882CF992B95990A9151374ABD8FF8C5A7A0FE08
iv =B7B4372CDFBCB3D16A2631B59B509E94
Rebeccas-MacBook-Pro:Key1 rebeccabartels$
```

```
Rebeccas-MacBook-Pro:Key1 rebeccabartels$ ls
iv.dat                  secrets                 secrets.txt             symmetrickey.dat
Rebeccas-MacBook-Pro:Key1 rebeccabartels$ cat iv.dat
B7B4372CDFBCB3D16A2631B59B509E94Rebeccas-MacBook-Pro:Key1 rebeccabartels$ cat symmetrickey.dat
5F4DCC3B5AA765D61D8327DEB882CF992B95990A9151374ABD8FF8C5A7A0FE08Rebeccas-MacBook-Pro:Key1 rebeccabartels$
```

```
Rebeccas-MacBook-Pro:Key1 rebeccabartels$ openssl enc -nosalt -aes-256-cbc -in dirty_little_secret.txt -out dirty_little_secret.enc -base64 -K 5F4DCC3B5AA765D61D8327DEB882CF992B95990A9151374ABD8FF8C5A7A0FE08 -iv B7B4372CDFBCB3D16A2631B59B509E94
Rebeccas-MacBook-Pro:Key1 rebeccabartels$ ls
dirty_little_secret.enc dirty_little_secret.txt iv.dat                  secrets                 symmetrickey.dat
Rebeccas-MacBook-Pro:Key1 rebeccabartels$ cat dirty_little_secret.enc
Pb/15xu4LynnAn/04ASMWNViffqXETsjrS3VskAjQ3Q/oikDMemZG4lRDlFhQlsX
+l6fnVIv/Bm77dhEj8SwGNdx1HU12Rs1zSrLAMCY8meLVTpB9lhzXHZpqdKCzZS/
8ck6SUwIwkYIKKKhaxHfMw==
Rebeccas-MacBook-Pro:Key1 rebeccabartels$
```


Kali-Linux-2019.3-vbox-amd64 [Running]
Applications
Places
Terminal
Mon 20:00
HW05-Crypto
Recent
root@kali: ~/Desktop/Keys
File Edit View Search Terminal Help
dirty_little_secret.enc iv.dat private.pem secrets
dirty_little_secret.txt partners_public.pem public.pem symmetric
key.dat
root@kali:~/Desktop/Keys# openssl pkeyutl -encrypt -in symmetrickey.
dat -inkey partners_public.pem -pubin -out symmetrickey.enc
root@kali:~/Desktop/Keys# ls
dirty_little_secret.enc partners_public.pem secrets
dirty_little_secret.txt private.pem symmetrickey.dat
iv.dat public.pem symmetrickey.enc
root@kali:~/Desktop/Keys# cat symmetrickey.enc
root@kali:~/Desktop/Keys#
Other Locations
"README.md" selected (7.3 kB)