┌──(kali㉿kali)-[~]

└─$ cd Desktop

┌──(kali㉿kali)-[~/Desktop]

└─$ ls

rsa

┌──(kali㉿kali)-[~/Desktop]

└─$ cd rsa

┌──(kali㉿kali)-[~/Desktop/rsa]

└─$ LS

LS: command not found

┌──(kali㉿kali)-[~/Desktop/rsa]

└─$ ls

enc.txt exploit.py pubkey.pem

┌──(kali㉿kali)-[~/Desktop/rsa]

└─$ cat enc.txt

��▒��&����"�

��E��U� 2��0>��X\*mm�TO�ŀ�������P�u�м����b�gIҾ)���

┌──(kali㉿kali)-[~/Desktop/rsa]

└─$ cat pubkey.pem

-----BEGIN PUBLIC KEY-----

MGQwDQYJKoZIhvcNAQEBBQADUwAwUAJJAMLLsk/b+SO2Emjj8Ro4lt5FdLO6WHMM

vWUpOIZOIiPu63BKF8/QjRa0aJGmFHR1mTnG5Jqv5/JZVUjHTB1/uNJM0VyyO0zQ

owIDAQAB

-----END PUBLIC KEY-----

┌──(kali㉿kali)-[~/Desktop/rsa]

└─$ openssl rsa -pubin -inform PEM -text -noout <pubkey.pem

Public-Key: (576 bit)

Modulus:

00:c2:cb:b2:4f:db:f9:23:b6:12:68:e3:f1:1a:38:

96:de:45:74:b3:ba:58:73:0c:bd:65:29:38:86:4e:

22:23:ee:eb:70:4a:17:cf:d0:8d:16:b4:68:91:a6:

14:74:75:99:39:c6:e4:9a:af:e7:f2:59:55:48:c7:

4c:1d:7f:b8:d2:4c:d1:5c:b2:3b:4c:d0:a3

Exponent: 65537 (0x10001)

┌──(kali㉿kali)-[~/Desktop/rsa]

└─$

┌──(kali㉿kali)-[~/Desktop/rsa]

└─$

┌──(kali㉿kali)-[~/Desktop/rsa]

└─$ touch exploit.py

┌──(kali㉿kali)-[~/Desktop/rsa]

└─$ pip install pycryptodome

Defaulting to user installation because normal site-packages is not writeable

Collecting pycryptodome

Obtaining dependency information for pycryptodome from https://files.pythonhosted.org/packages/af/20/5f29ec45462360e7f61e8688af9fe4a0afae057edfabdada662e11bf97e7/pycryptodome-3.20.0-cp35-abi3-manylinux\_2\_17\_x86\_64.manylinux2014\_x86\_64.whl.metadata

Downloading pycryptodome-3.20.0-cp35-abi3-manylinux\_2\_17\_x86\_64.manylinux2014\_x86\_64.whl.metadata (3.4 kB)

Downloading pycryptodome-3.20.0-cp35-abi3-manylinux\_2\_17\_x86\_64.manylinux2014\_x86\_64.whl (2.1 MB)

━━━━━━━━━━━━━━━━━━━━━━━━━━━━━━━━━━━━━━━━ 2.1/2.1 MB 4.2 MB/s eta 0:00:00

Installing collected packages: pycryptodome

Successfully installed pycryptodome-3.20.0

┌──(kali㉿kali)-[~/Desktop/rsa]

└─$ python exploit.py

┌──(kali㉿kali)-[~/Desktop/rsa]

└─$ touch dec.txt

┌──(kali㉿kali)-[~/Desktop/rsa]

└─$ openssl pkeyutl -decrypt -in enc.txt -out dec.txt -inkey private.pem

┌──(kali㉿kali)-[~/Desktop/rsa]

└─$ cat dec.txt

RSAisEasy