Department of Computer Science and Engineering

University of Dhaka

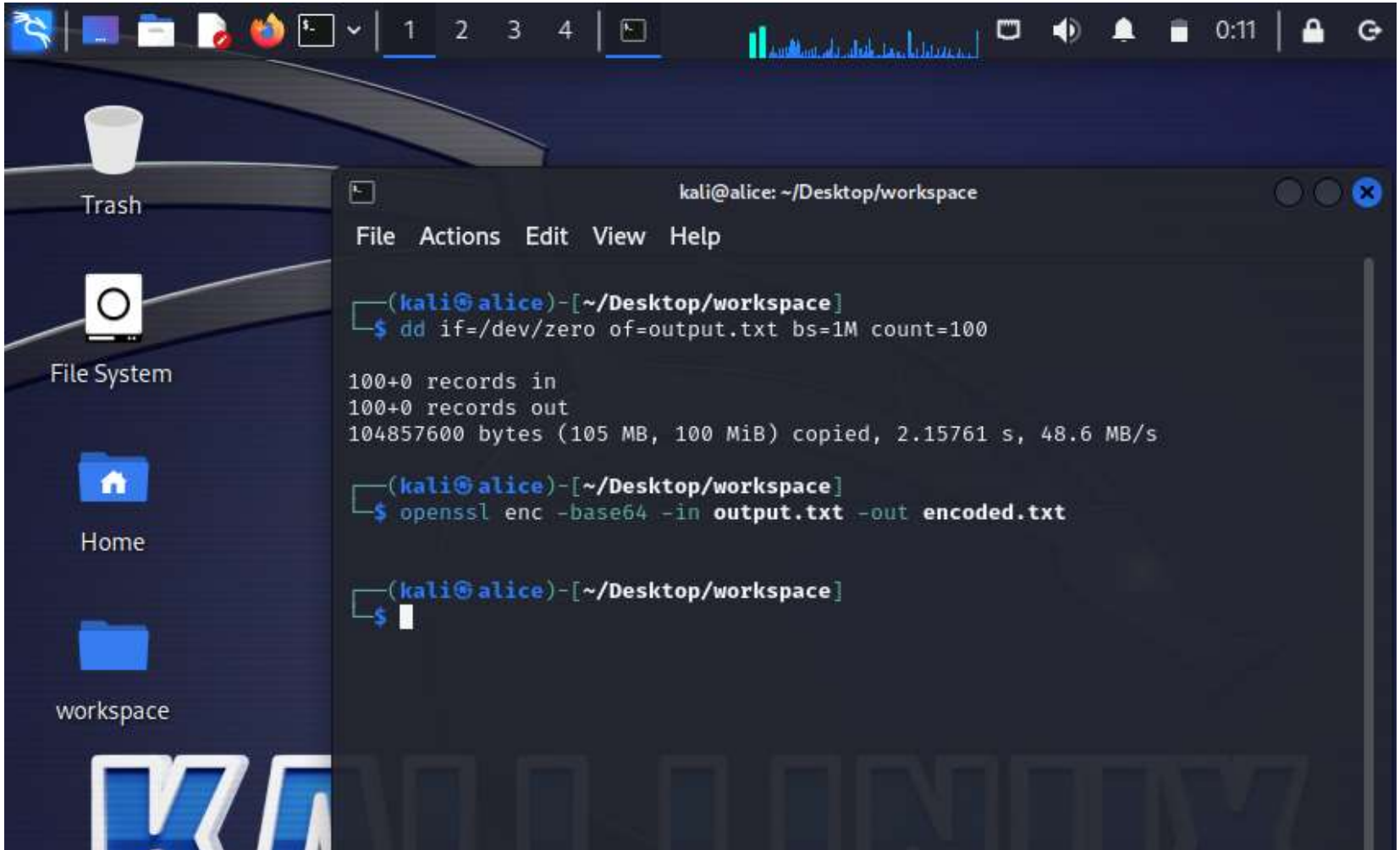
Dhaka-1000
Professional Masters in Information and Cyber Security

Subject: Applied Cryptography Course Code: 806

Class Test

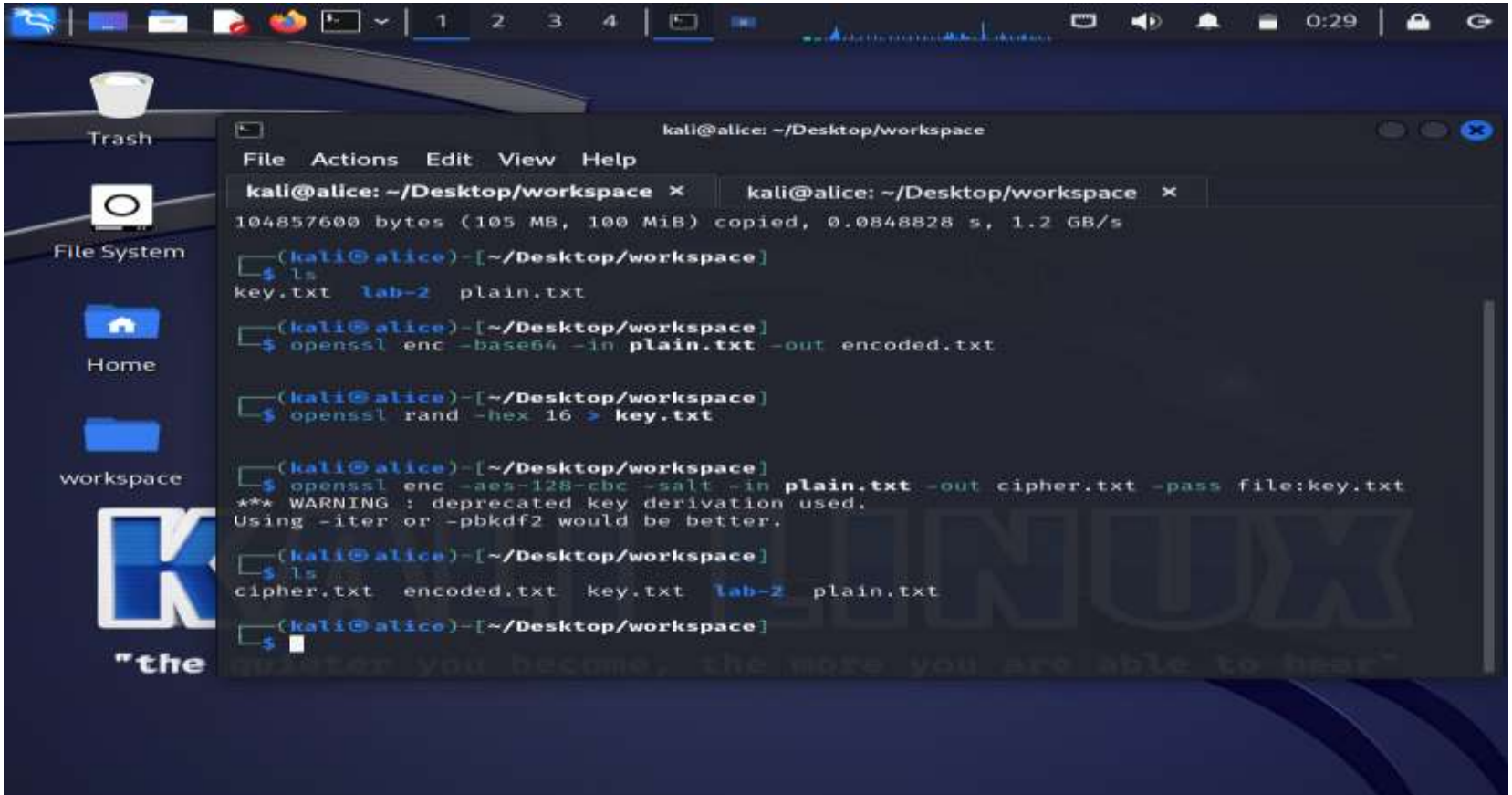
Name: Abu Syeed Sajid Ahmed
Roll: 30023

1/a)


1 2 3 4
0:11
Trash
File System
Home
workspace
kali@alice: ~/Desktop/workspace
File Actions Edit View Help
(kali㉿alice)-[~/Desktop/workspace]
$ dd if=/dev/zero of=output.txt bs=1M count=100
100+0 records in
100+0 records out
104857600 bytes (105 MB, 100 MiB) copied, 2.15761 s, 48.6 MB/s
(kali㉿alice)-[~/Desktop/workspace]
$ openssl enc -base64 -in output.txt -out encoded.txt
(kali㉿alice)-[~/Desktop/workspace]
$

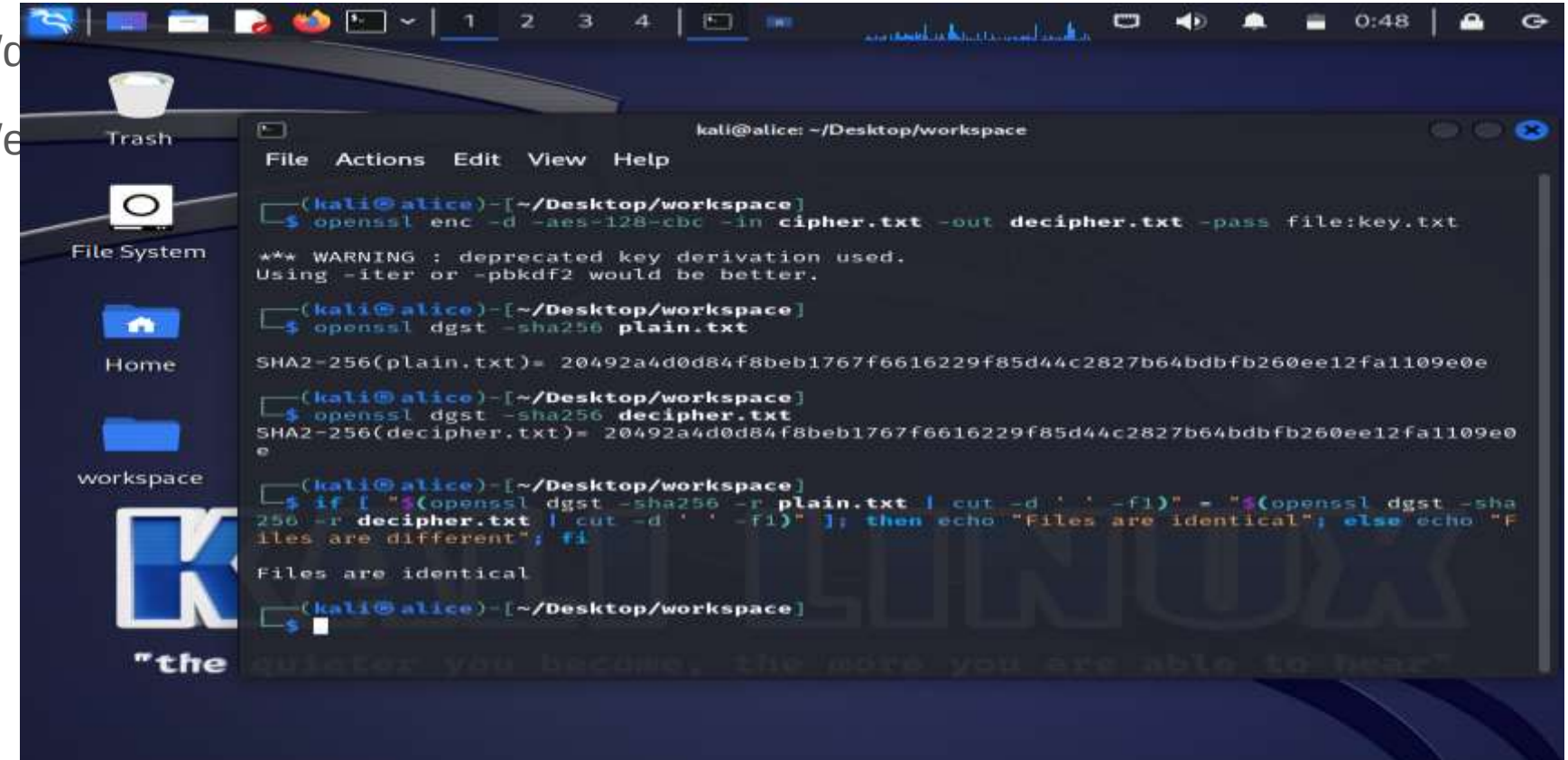
1/b)

1/c)

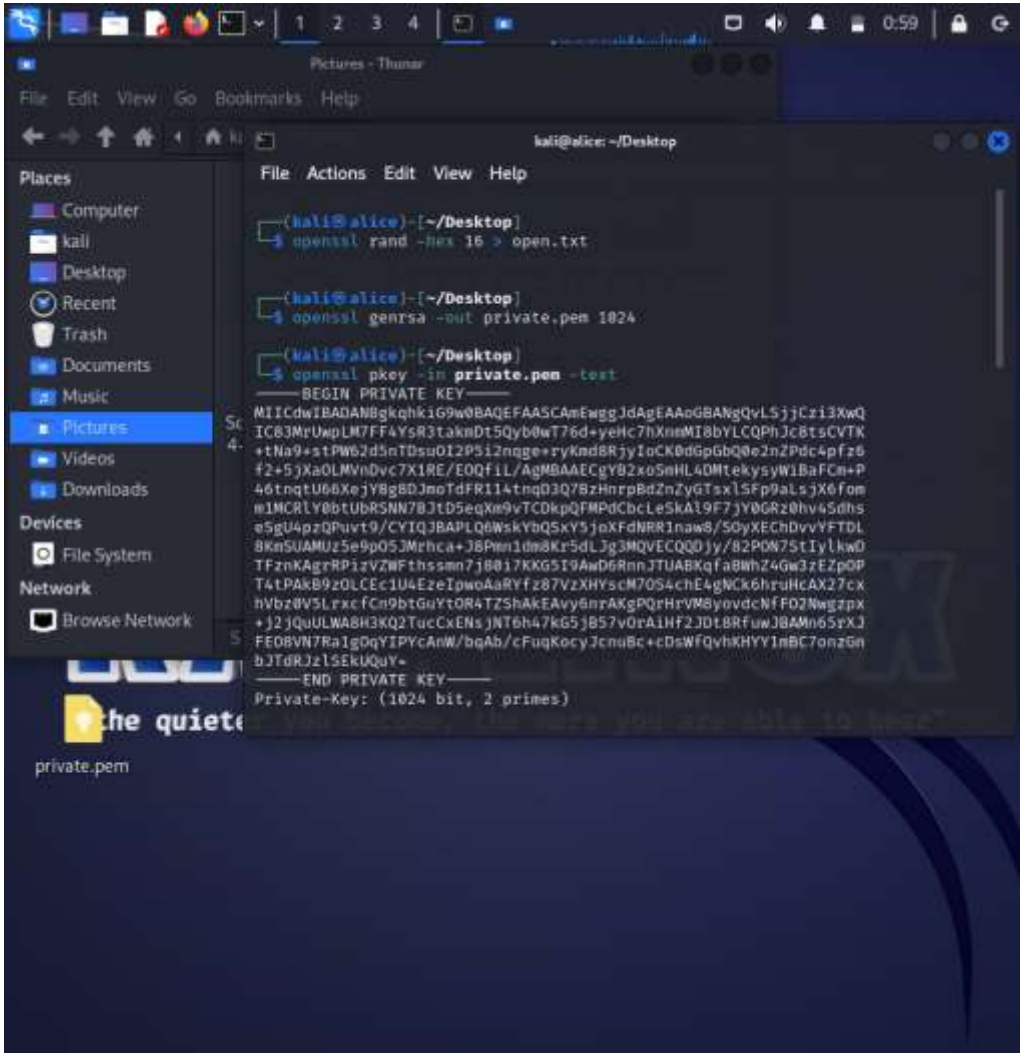

1 2 3 4
0:29
Trash
File System
Home
workspace
"the
kali@alice: ~/Desktop/workspace
File Actions Edit View Help
kali@alice: ~/Desktop/workspace
kali@alice: ~/Desktop/workspace
104857600 bytes (105 MB, 100 MiB) copied, 0.0848828 s, 1.2 GB/s
(kali㉿alice)-[~/Desktop/workspace]
$ ls
key.txt lab-2 plain.txt
(kali㉿alice)-[~/Desktop/workspace]
$ openssl enc -base64 -in plain.txt -out encoded.txt
(kali㉿alice)-[~/Desktop/workspace]
$ openssl rand -hex 16 > key.txt
(kali㉿alice)-[~/Desktop/workspace]
$ openssl enc -aes-128-cbc -salt -in plain.txt -out cipher.txt -pass file:key.txt
*** WARNING : deprecated key derivation used.
Using -iter or -pbkdf2 would be better.
(kali㉿alice)-[~/Desktop/workspace]
$ ls
cipher.txt encoded.txt key.txt lab-2 plain.txt
(kali㉿alice)-[~/Desktop/workspace]
$

1/d

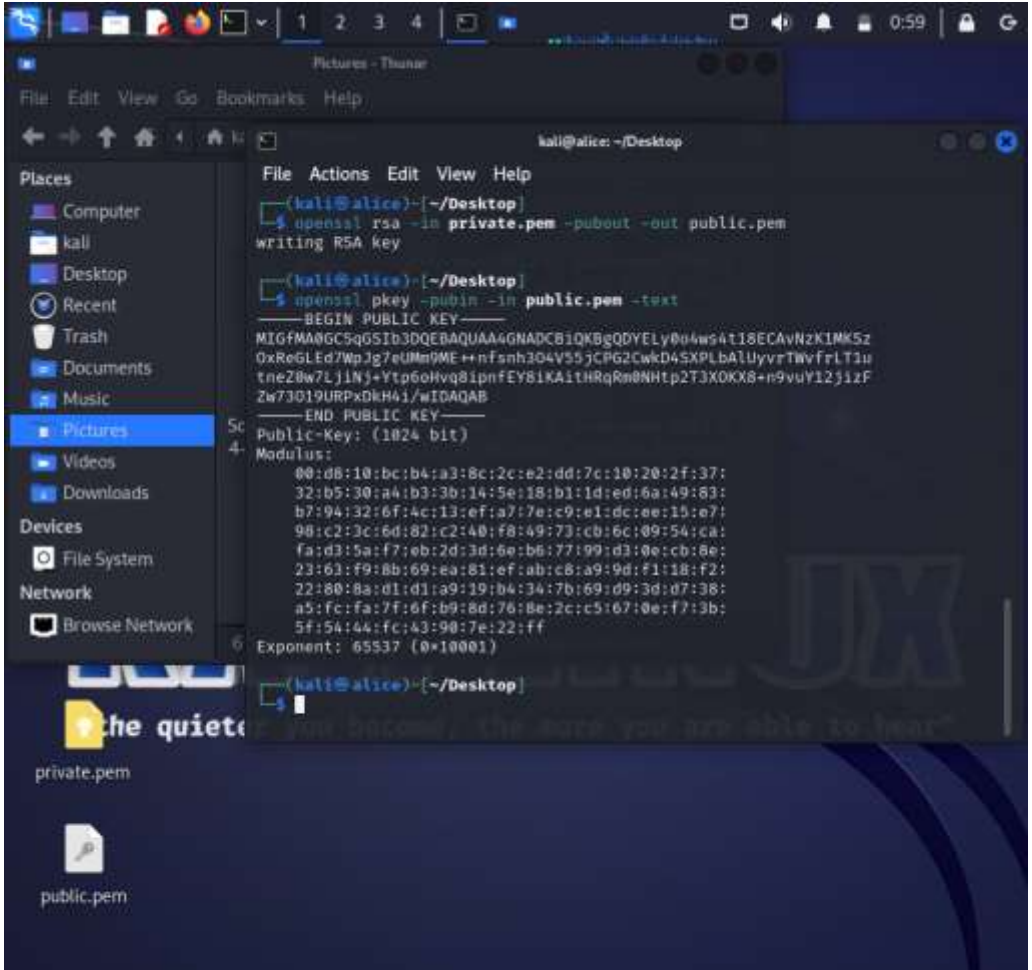
1/e


1 2 3 4
0:48
Trash
File System
Home
workspace
"the
kali@alice: ~/Desktop/workspace
File Actions Edit View Help
(kali㉿alice)-[~/Desktop/workspace]
$ openssl enc -d -aes-128-cbc -in cipher.txt -out decipher.txt -pass file:key.txt
*** WARNING : deprecated key derivation used.
Using -iter or -pbkdf2 would be better.
(kali㉿alice)-[~/Desktop/workspace]
$ openssl dgst -sha256 plain.txt
SHA2-256(plain.txt)= 20492a4d0d84f8beb1767f6616229f85d44c2827b64bdbfb260ee12fa1109e0e
(kali㉿alice)-[~/Desktop/workspace]
$ openssl dgst -sha256 decipher.txt
SHA2-256(decipher.txt)= 20492a4d0d84f8beb1767f6616229f85d44c2827b64bdbfb260ee12fa1109e0
e
(kali㉿alice)-[~/Desktop/workspace]
$ if ["$(openssl dgst -sha256 -r plain.txt | cut -d ' ' -f1)" = "$(openssl dgst -sha
256 -r decipher.txt | cut -d ' ' -f1)"]; then echo "Files are identical"; else echo "F
iles are different"; fi
Files are identical
(kali㉿alice)-[~/Desktop/workspace]
$

2/a)


Pictures - Thunar
File Edit View Go Bookmarks Help
Places
Computer
kali
Desktop
Recent
Trash
Documents
Music
Pictures
Videos
Downloads
Devices
File System
Network
Browse Network
kali@alice: ~/Desktop
File Actions Edit View Help
(kali㉿alice)-[~/Desktop]
$ openssl rand -hex 16 > open.txt
(kali㉿alice)-[~/Desktop]
$ openssl genrsa -out private.pem 1024
(kali㉿alice)-[~/Desktop]
$ openssl pkey -in private.pem -text
-----BEGIN PRIVATE KEY-----
MIICdwIBADANBgkqhkiG9w0BAQEFAASCAmEwggJdAgEAAoGBANgQvL5jjCzi3XwQ
IC83MrUwpLM7FF4YsR3takmDt5Qyb0wT76d+yeHc7hXnnMI8bYLCQPhJc8tsCVTK
+tNa9+stPW62d5nTDsuOI2P5i2nqge+ryKmd8RjyIoCK0dGpGbQ0e2nZPdc4pfz6
f2+5jXaOLMVnDvc7X1RE/EOQfiL/AgMBAAECgYB2xoSmHL4DMtekysyW1BaFCm+P
46tnqtU66XejYBg8DJmoTdFR114tnqO3Q7BzHnrpBdZnZyGTsxlSFp9aLsjX6fom
m1MCRlY0btUbRSNN78JtD5eqXm9vTCDkpQFMPdCbcLeSkAl9F7jY0GRz0hv4Sdhs
e5gU4pzQPuvt9/CYIQJBAPLQ6WskYbQSxY5joXFdNRR1naw8/SOyXEChDvvYFTDL
8KmSUAMUz5e9pO5JMrhca+JBPmn1dm8Kr5dLJg3MQVECQQDjy/82PON75tIylkwD
TFznKAgrRPizVZWFthssmn7j80i7KKG5I9AwD6RnnJTUABKqfaBWhZ4Gw3zEZpOP
T4tPAkB9zOLCEc1U4EzeIpwoAaRYfz87VzXHYscM7OS4chE4gNCk6hruHcAX27cx
hVbz0V5LrxcfCn9btGuYtOR4TZShAkEAvy6nrAKgPQrHrVM8yovdcNfFO2NwgzpX
+j2jQuULWA8H3KQ2TucCxENsjNT6h47kG5jB57vOrAiHf2JDt8RfuwJ0AMn65rXJ
FEO8VN7Ra1gDqYIPYcAnW/bqAb/cFuqKocyJcnuBc+cDsWfQvhKHYY1mBC7onzGn
bJTdRJzlSEkUQuY=
-----END PRIVATE KEY-----
Private-Key: (1024 bit, 2 primes)
private.pem

2/b)


Pictures - Thunar
File Edit View Go Bookmarks Help
Places
Computer
kali
Desktop
Recent
Trash
Documents
Music
Pictures
Videos
Downloads
Devices
File System
Network
Browse Network
kali@alice: ~/Desktop
File Actions Edit View Help
(kali㉿alice)-[~/Desktop]
$ openssl rsa -in private.pem -pubout -out public.pem
writing RSA key
(kali㉿alice)-[~/Desktop]
$ openssl pkey -pubin -in public.pem -text
-----BEGIN PUBLIC KEY-----
MIGfMA0GCSqGSIb3DQEBAQUAA4GNADCBiQKBgQDYELy0o4ws4t18ECAvNzK1MK5z
OxReGLEd7WpJg7eUMm9ME++nfsnh3O4V55jCPG2CwkD4SXPLbAlUyvrTWvfrLT1u
tneZ0w7LjiNj+Ytp6oHvq8ipnfEY8iKAitHRqRm0NHtp2TJXOKX8+n9vuY12jizF
Zw73O19URPxDkH4i/wIDAQAB
-----END PUBLIC KEY-----
Public-Key: (1024 bit)
Modulus:
00:d8:10:bc:b4:a3:8c:2c:e2:dd:7c:10:20:2f:37:
32:b5:30:a4:b3:3b:14:5e:18:b1:1d:ed:6a:49:83:
b7:94:32:6f:4c:13:ef:a7:7e:c9:e1:dc:ee:15:e7:
98:c2:3c:6d:82:c2:40:f8:49:73:cb:6c:09:54:ca:
fa:d3:5a:f7:eb:2d:3d:6e:b6:77:99:d3:0e:cb:8e:
23:63:f9:8b:69:ea:81:ef:ab:c8:a9:9d:f1:18:f2:
22:80:8a:d1:d1:a9:19:b4:34:7b:69:d9:3d:d7:38:
a5:fc:fa:7f:6f:b9:8d:76:8e:2c:c5:67:0e:f7:3b:
5f:54:44:fc:43:90:7e:22:ff
Exponent: 65537 (0x10001)
(kali㉿alice)-[~/Desktop]
$
private.pem
public.pem

2/c)

2/d)