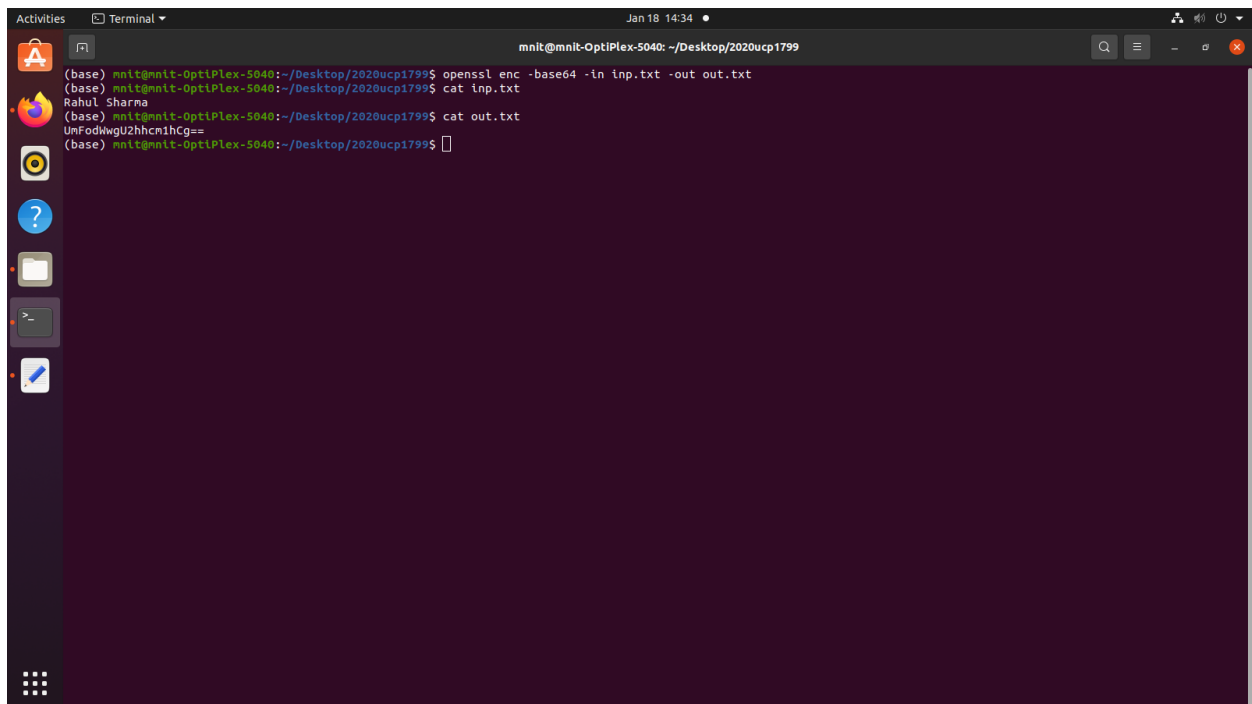


OpenSSL_Assignment 1

Name:- RAHUL SHARMA

ID:- 2020UCP1799

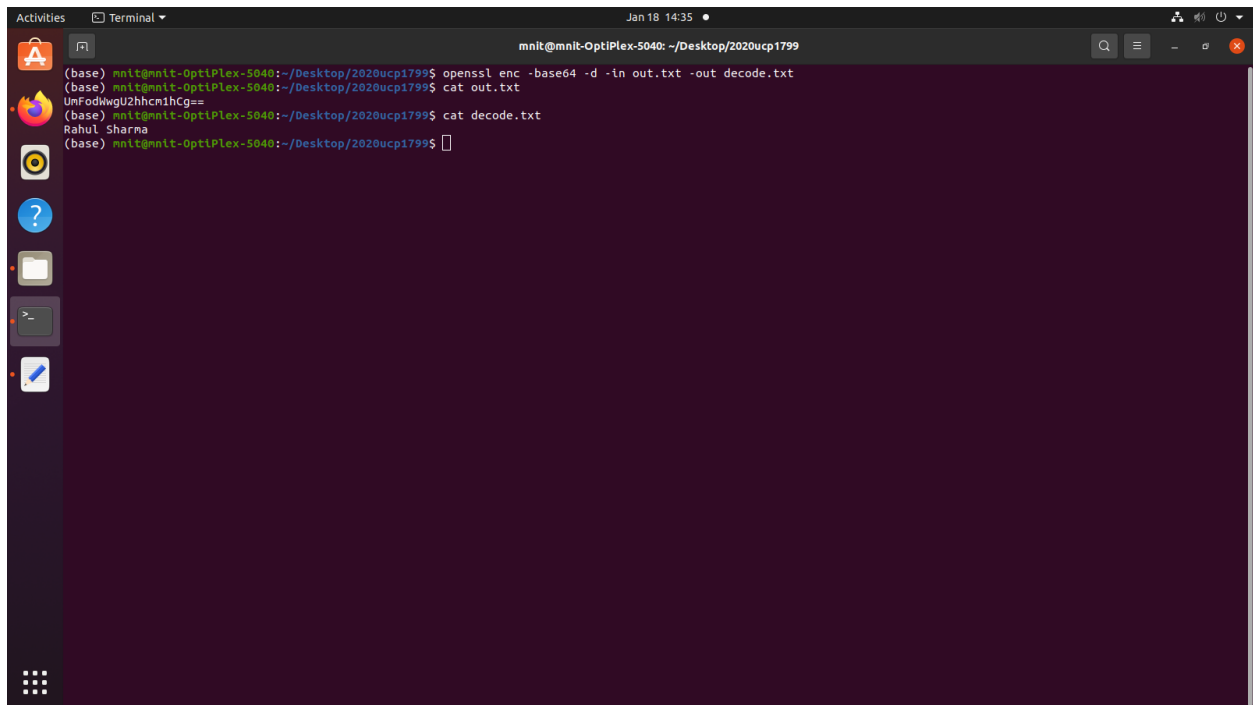
Encoding with base64 definition

A screenshot of a Linux terminal window. The window title is "mnil@mnit-OptiPlex-5040: ~/Desktop/2020ucp1799". The terminal shows the following commands and output:

```
(base) mnil@mnit-OptiPlex-5040:~/Desktop/2020ucp1799$ openssl enc -base64 -in inp.txt -out out.txt
(base) mnil@mnit-OptiPlex-5040:~/Desktop/2020ucp1799$ cat inp.txt
Rahul Sharma
(base) mnil@mnit-OptiPlex-5040:~/Desktop/2020ucp1799$ cat out.txt
UnFodWwGU2hhcm1hCg==
(base) mnil@mnit-OptiPlex-5040:~/Desktop/2020ucp1799$
```

The terminal has a dark purple background. On the left side, there is a vertical dock with several application icons: a red shopping bag (Ubuntu Software), a blue question mark (Help), a white document (Files), a terminal icon, and a blue notepad (Text Editor). The top of the window shows system status icons including network, sound, and power.

Decoding with base64 definition

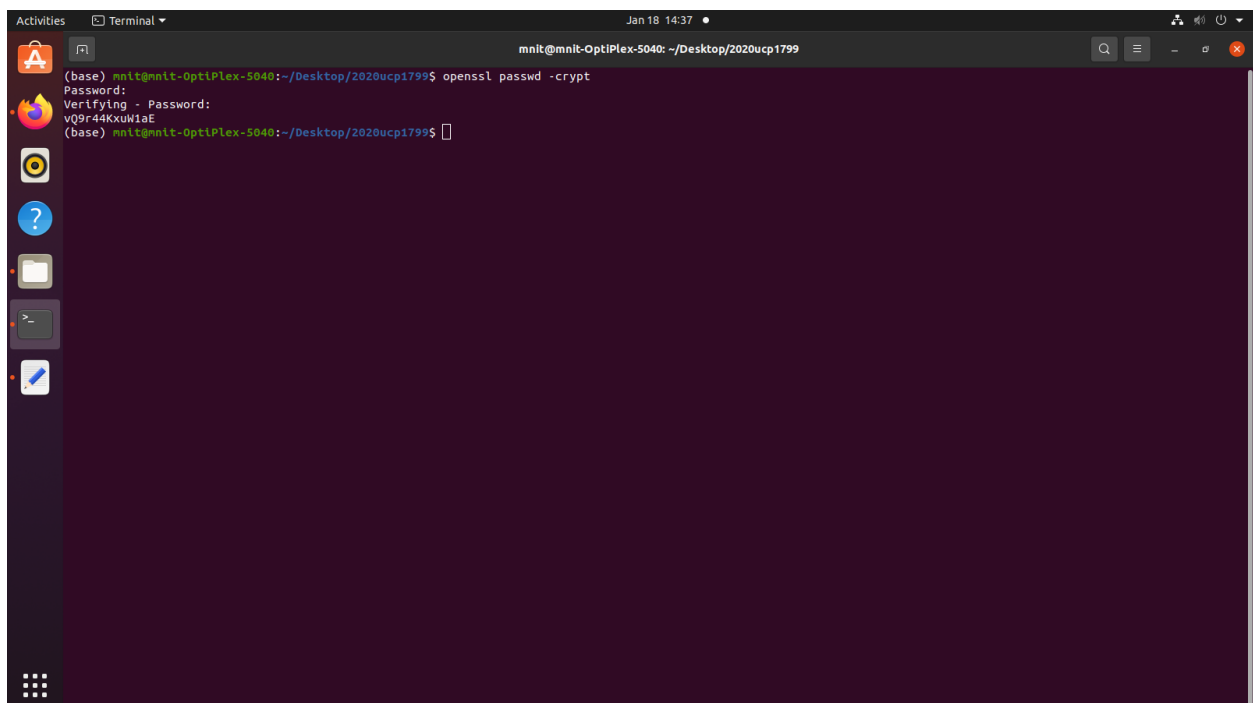


A terminal window titled 'Terminal' with a search bar and window controls. The prompt is 'mnit@mnit-OptiPlex-5040: ~/Desktop/2020ucp1799'. The user enters the command 'openssl enc -base64 -d -in out.txt -out decode.txt'. The prompt changes to '(base)'. The user then enters 'cat out.txt', and the output 'UnFodWwGU2hhcn1hCg==' is displayed. The user enters 'cat decode.txt', and the output 'Rahul Sharma' is displayed. The prompt returns to '(base) mnit@mnit-OptiPlex-5040:~/Desktop/2020ucp1799\$'.

```
(base) mnit@mnit-OptiPlex-5040:~/Desktop/2020ucp1799$ openssl enc -base64 -d -in out.txt -out decode.txt
(base) mnit@mnit-OptiPlex-5040:~/Desktop/2020ucp1799$ cat out.txt
UnFodWwGU2hhcn1hCg==
(base) mnit@mnit-OptiPlex-5040:~/Desktop/2020ucp1799$ cat decode.txt
Rahul Sharma
(base) mnit@mnit-OptiPlex-5040:~/Desktop/2020ucp1799$
```

Password files definition

- passwd



A terminal window titled 'Terminal' with a search bar and window controls. The prompt is 'mnit@mnit-OptiPlex-5040: ~/Desktop/2020ucp1799'. The user enters the command 'openssl passwd -crypt'. The prompt changes to '(base)'. The user is prompted 'Password:' and enters 'vQ9r44KxuW1aE'. The prompt changes to 'Verifying - Password:'. The user enters 'vQ9r44KxuW1aE' again. The prompt changes to '(base) mnit@mnit-OptiPlex-5040:~/Desktop/2020ucp1799\$'.

```
(base) mnit@mnit-OptiPlex-5040:~/Desktop/2020ucp1799$ openssl passwd -crypt
Password:
Verifying - Password:
vQ9r44KxuW1aE
(base) mnit@mnit-OptiPlex-5040:~/Desktop/2020ucp1799$
```

A terminal window titled "Terminal" with a search icon and window controls. The prompt is "mnil@mnil-OptiPlex-5040: ~/Desktop/2020ucp1799". The user enters the command "(base) mnil@mnil-OptiPlex-5040:~/Desktop/2020ucp1799\$ openssl passwd -crypt -salt 2002". The output shows "Password:" followed by "20xyuwopfdQR." and a new prompt "(base) mnil@mnil-OptiPlex-5040:~/Desktop/2020ucp1799\$".

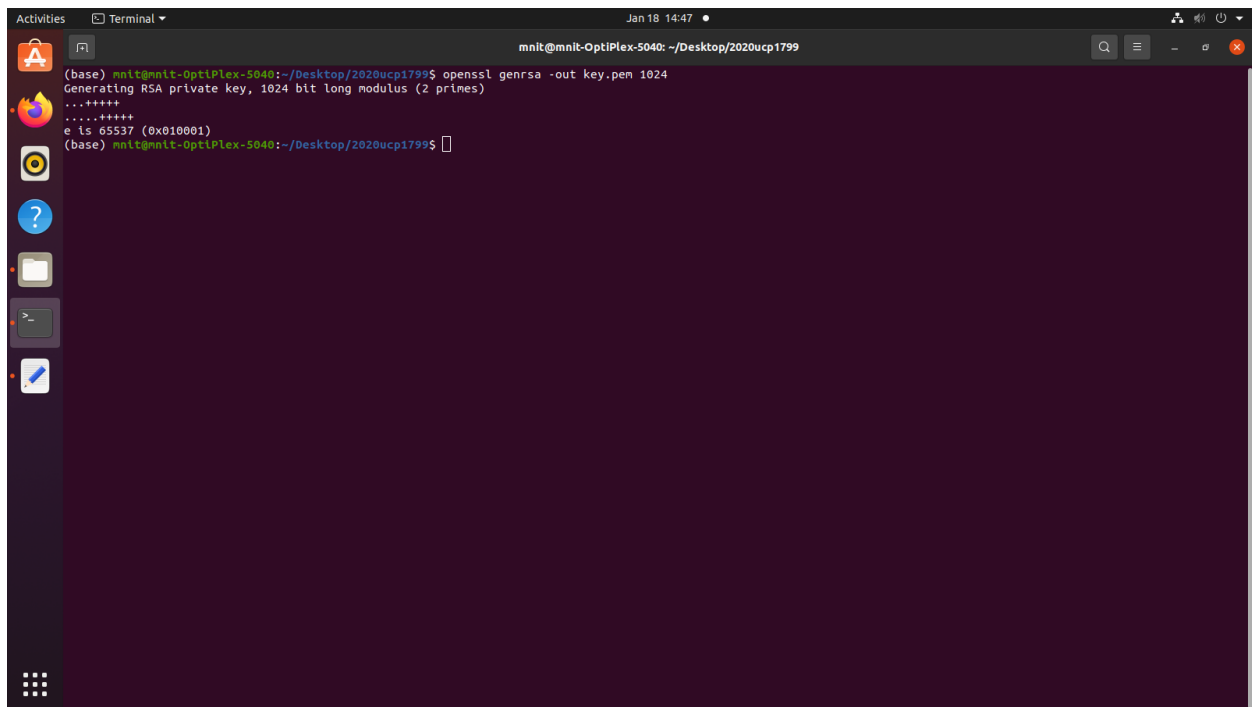
```
(base) mnil@mnil-OptiPlex-5040:~/Desktop/2020ucp1799$ openssl passwd -crypt -salt 2002
Password:
20xyuwopfdQR.
(base) mnil@mnil-OptiPlex-5040:~/Desktop/2020ucp1799$
```

A terminal window titled "Terminal" with a search icon and window controls. The prompt is "mnil@mnil-OptiPlex-5040: ~/Desktop/2020ucp1799". The user enters the command "(base) mnil@mnil-OptiPlex-5040:~/Desktop/2020ucp1799\$ openssl passwd -1". The output shows "Password:", "Verifying - Password:", and the hash "S1\$vlqptkKcShgNA.NfgpJPa9KqQg28k7." followed by a new prompt "(base) mnil@mnil-OptiPlex-5040:~/Desktop/2020ucp1799\$".

```
(base) mnil@mnil-OptiPlex-5040:~/Desktop/2020ucp1799$ openssl passwd -1
Password:
Verifying - Password:
S1$vlqptkKcShgNA.NfgpJPa9KqQg28k7.
(base) mnil@mnil-OptiPlex-5040:~/Desktop/2020ucp1799$
```

Encryption with RSA key generation

- Generating Keys



A terminal window titled "Terminal" with a dark background. The window shows the command `openssl genrsa -out key.pem 1024` being executed. The output indicates that a 1024-bit RSA private key is being generated. The terminal also shows the hexadecimal value of the exponent `e` as `65537 (0x010001)`. The prompt is `(base) mnit@mnit-OptiPlex-5040: ~/Desktop/2020ucp1799$`.

```
(base) mnit@mnit-OptiPlex-5040:~/Desktop/2020ucp1799$ openssl genrsa -out key.pem 1024
Generating RSA private key, 1024 bit long modulus (2 primes)
.....+++++
.....+++++
e is 65537 (0x010001)
(base) mnit@mnit-OptiPlex-5040:~/Desktop/2020ucp1799$
```

```
Activities Terminal Jan 18 14:49 mnit@mnit-OptiPlex-5040: ~/Desktop/2020ucp1799
(base) mnit@mnit-OptiPlex-5040:~/Desktop/2020ucp1799$ openssl genrsa -out mySmall.pem 1024
Generating RSA private key, 1024 bit long modulus (2 primes)
.....+++++
e is 65537 (0x010001)
(base) mnit@mnit-OptiPlex-5040:~/Desktop/2020ucp1799$
```

```
Activities Terminal Jan 18 14:53 mnit@mnit-OptiPlex-5040: ~/Desktop/2020ucp1799
(base) mnit@mnit-OptiPlex-5040:~/Desktop/2020ucp1799$ openssl rsa -in mySmall.pem -text -noout
RSA Private-Key: (1024 bit, 2 primes)
modulus:
00:e5:db:0c:1c:7e:e2:82:81:2d:1d:7a:b6:58:4e:
0d:ef:56:63:7e:36:d2:c0:b7:a1:62:e1:8e:4d:4d:
a2:98:de:c4:3a:fc:b1:0b:c5:af:4c:16:ee:95:4b:
35:e7:34:ef:bb:f6:a9:9d:03:95:b7:6f:3d:13:93:
95:0a:b5:d7:d7:e6:5b:17:ab:04:0d:4f:38:d1:2b:
0e:09:dd:bd:ac:5e:31:05:00:c8:56:c7:5e:05:00:
25:8c:3d:29:0e:1d:73:99:2d:0d:06:bc:e0:cc:9e:
93:da:fc:85:0c:23:5e:c2:5e:a8:24:1f:0f:f5:fb:
79:a3:54:4f:b9:55:e5:f4:f3
publicExponent: 65537 (0x10001)
privateExponent:
6d:0e:0e:a2:fe:78:8d:9e:a8:3f:12:57:ad:71:eb:
1e:a1:08:37:7b:df:66:5c:39:8f:e6:a0:53:81:00:
22:33:0f:3a:b5:65:72:c6:6a:33:59:b5:fc:d3:00:
51:c0:45:f6:12:43:cb:21:46:49:6f:d7:b4:90:13:
16:3c:0c:99:96:9c:0e:5e:a4:63:2c:87:6c:b5:a7:
58:97:60:ff:ab:ee:66:35:c5:9c:d6:22:c9:2c:22:
c3:f1:3d:ba:2e:6a:4f:8b:94:bc:86:b1:b0:ca:ef:
52:10:ab:72:57:78:bc:2d:c4:6d:13:d5:32:f0:6d:
71:46:8b:91:73:5e:d6:c1
primes:
00:f3:8a:7f:e5:d0:6d:f6:27:f4:d9:20:4d:bd:1a:
0a:1f:6f:e1:ee:ac:a8:01:df:47:30:36:4a:af:70:
44:09:6b:13:da:82:9a:6d:75:2a:68:47:99:f8:84:
0a:78:c1:ab:ac:a2:19:75:20:50:a7:56:f9:cb:83:
9e:fd:55:60:c3
prime2:
00:f2:1c:91:6b:c4:da:24:aa:5d:64:42:d6:a1:d1:
65:27:f6:f2:86:e7:83:45:14:8b:d2:4e:c5:a9:ee:
ce:4a:dc:96:dc:1d:0d:bf:e1:ff:35:42:72:c6:cd:
97:38:ac:d5:4d:ca:61:56:fa:25:17:cc:d3:0e:63:
8a:e6:b2:d8:11
exponent1:
00:c2:7d:6b:7e:1f:fe:6f:16:e8:84:7c:aa:59:23:
0c:d7:3d:74:62:c8:3e:26:49:64:31:7b:b0:e6:9c:
6a:6d:d3:07:6f:3c:46:92:43:49:ad:6b:67:16:8d:
ab:c7:98:cc:65:f8:ce:40:81:9c:a9:5d:1b:c6:b5:
cc:9c:54:1f:7b
exponent2:
00:d4:a4:72:b4:8c:78:6b:ab:95:ca:f1:49:41:66:
7f:c9:d2:02:c0:a9:a5:89:8e:ba:1f:43:eb:d6:8c:
7f:73:10:bb:0f:28:15:63:6a:42:93:ac:80:d2:4a:
cf:7e:5f:8e:18:7c:9f:71:9c:d1:e7:4d:66:a1:b0:
```

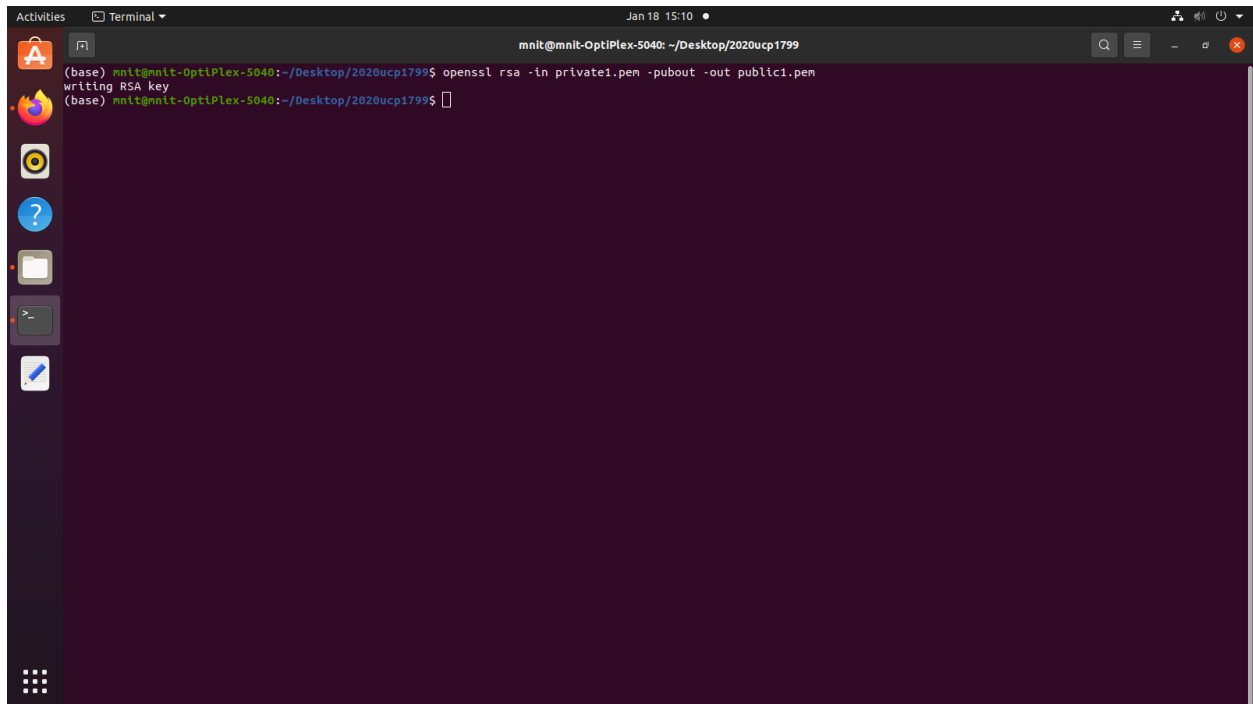
```
Activities Terminal Jan 18 14:53 mnlit@mnit-OptiPlex-5040: ~/Desktop/2020ucp1799
25:8c:3d:29:0e:1d:73:99:2d:0d:06:bc:e0:cc:9e:
93:da:fc:85:0c:23:5e:c2:5e:a0:24:1f:0f:f5:fb:
79:a3:54:4f:b9:55:e5:f4:f3
publicExponent: 65537 (0x10001)
privateExponent:
6d:0e:0e:a2:fe:78:8d:9e:a8:3f:12:57:ad:71:eb:
1e:a1:08:37:7b:df:66:5c:39:8f:e6:a0:53:81:00:
22:33:9f:3a:b5:65:72:c6:6a:33:59:b5:fc:d3:60:
51:c0:45:f6:12:43:cb:21:40:49:0f:d7:b4:90:13:
16:3c:0c:99:96:9c:8e:5e:a4:63:2c:07:6c:b5:a7:
58:97:60:ff:ab:ee:6e:35:c5:9c:d6:22:c9:2c:22:
c3:f1:3d:ba:2e:6a:4f:8b:94:bc:86:b1:b0:ca:ef:
52:10:ab:72:57:78:bc:2d:c4:6d:13:d5:32:f0:6d:
71:46:8b:91:73:5e:d6:c1
prime1:
00:f3:0a:7f:e5:d0:6d:f6:27:f4:d9:20:4d:bd:1a:
8a:1f:6f:e1:ee:ac:a8:01:df:47:30:36:4a:af:78:
44:09:6b:13:da:82:9a:6d:75:2a:60:47:99:f8:84:
8a:78:c1:ab:ac:a2:19:75:20:50:a7:56:f9:cb:83:
9e:fd:55:60:c3
prime2:
00:f2:1c:91:6b:c4:da:24:aa:5d:64:42:d6:a1:d1:
65:27:f6:f2:86:e7:83:45:14:8b:d2:4e:65:a9:ee:
ce:4a:dc:96:dc:1d:0d:bf:e1:ff:35:42:72:c6:cd:
97:38:ac:d5:4d:ca:61:56:fa:25:17:cc:d3:8e:63:
8a:e0:b2:d8:11
exponent1:
00:c2:7d:6b:7e:1f:fe:6f:16:e8:84:7c:aa:59:23:
0c:d7:3d:74:62:c8:3e:26:49:64:31:7b:b0:e6:9c:
6a:6d:d3:07:6f:3c:46:92:43:49:ad:6b:c7:16:8d:
ab:c7:98:cc:65:f8:ce:40:81:9c:a9:5d:1b:c6:b5:
cc:9c:54:1f:7b
exponent2:
00:d4:e4:72:b4:8c:78:6b:ab:95:ca:f1:49:41:66:
7f:c9:d2:02:c0:a9:a8:80:8e:ba:1f:43:eb:d6:dc:
7f:73:10:bb:0f:28:15:63:6a:42:93:ac:80:d2:4a:
cf:7e:5f:8e:18:7c:9f:71:9c:d1:e7:4d:66:a1:b0:
9b:d6:73:4d:81
coefficient:
00:d0:63:10:ae:fe:4b:e2:34:5c:1e:2c:ef:e8:bb:
0e:08:a2:c9:e2:61:f1:d2:69:11:e5:6c:63:86:1b:
34:f7:57:d0:4f:26:52:1d:45:e2:f9:7f:43:ed:24:
12:08:ed:29:95:08:ee:8d:0b:d9:e4:a2:3f:c7:7d:
4f:8a:3c:5d:83
(base) mnlit@mnit-OptiPlex-5040:~/Desktop/2020ucp1799$
```

- Generating key with Des3 encryption

```
Activities Terminal Jan 18 14:57 mnlit@mnit-OptiPlex-5040: ~/Desktop/2020ucp1799
(base) mnlit@mnit-OptiPlex-5040:~/Desktop/2020ucp1799$ openssl genrsa -des3 -out private.pem 1024
Generating RSA private key, 1024 bit long modulus (2 primes)
.....+++++
e is 65537 (0x10001)
Enter pass phrase for private.pem:
Verifying - Enter pass phrase for private.pem:
(base) mnlit@mnit-OptiPlex-5040:~/Desktop/2020ucp1799$
```

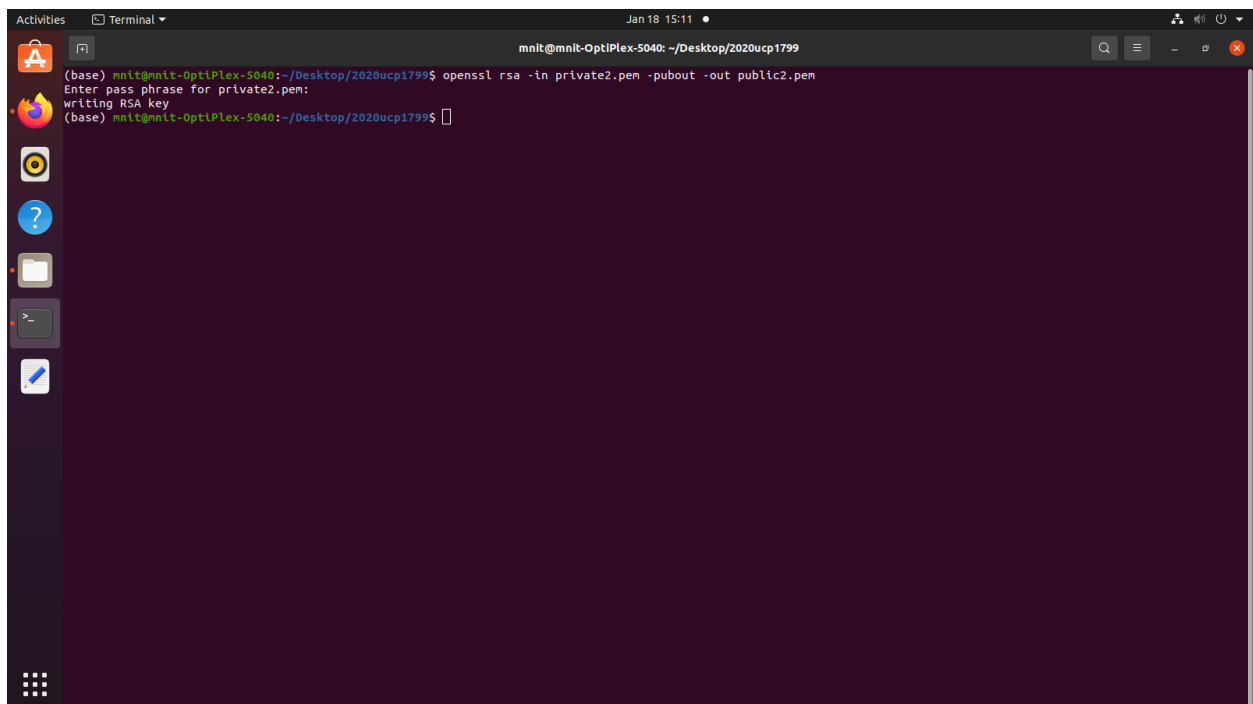
```
Activities Terminal Jan 18 15:07 mnit@mnit-OptiPlex-5040: ~/Desktop/2020ucp1799
(base) mnit@mnit-OptiPlex-5040:~/Desktop/2020ucp1799$ openssl genrsa -out private1.pem 1024
Generating RSA private key, 1024 bit long modulus (2 primes)
.....+++++
e is 65537 (0x010001)
(base) mnit@mnit-OptiPlex-5040:~/Desktop/2020ucp1799$
```

```
Activities Terminal Jan 18 15:08 mnit@mnit-OptiPlex-5040: ~/Desktop/2020ucp1799
(base) mnit@mnit-OptiPlex-5040:~/Desktop/2020ucp1799$ openssl genrsa -des3 -out private2.pem 1024
Generating RSA private key, 1024 bit long modulus (2 primes)
.....+++++
e is 65537 (0x010001)
Enter pass phrase for private2.pem:
Verify - Enter pass phrase for private2.pem:
(base) mnit@mnit-OptiPlex-5040:~/Desktop/2020ucp1799$
```



A terminal window titled "Terminal" with a search icon and window controls. The prompt is "mnlit@mnit-OptiPlex-5040: ~/Desktop/2020ucp1799". The command entered is `openssl rsa -in private1.pem -pubout -out public1.pem`. The output shows the command being executed and the RSA key being written.

```
(base) mnlit@mnit-OptiPlex-5040:~/Desktop/2020ucp1799$ openssl rsa -in private1.pem -pubout -out public1.pem
writing RSA key
(base) mnlit@mnit-OptiPlex-5040:~/Desktop/2020ucp1799$
```



A terminal window titled "Terminal" with a search icon and window controls. The prompt is "mnlit@mnit-OptiPlex-5040: ~/Desktop/2020ucp1799". The command entered is `openssl rsa -in private2.pem -pubout -out public2.pem`. The output shows the command being executed, a password prompt, the password being entered, and the RSA key being written.

```
(base) mnlit@mnit-OptiPlex-5040:~/Desktop/2020ucp1799$ openssl rsa -in private2.pem -pubout -out public2.pem
Enter pass phrase for private2.pem:
writing RSA key
(base) mnlit@mnit-OptiPlex-5040:~/Desktop/2020ucp1799$
```


- Encryption and Decryption using rsa key

The screenshot shows a terminal window titled "Terminal" with the user "mnlt" on host "mnlt-OptiPlex-5040". The terminal displays the following commands and output:

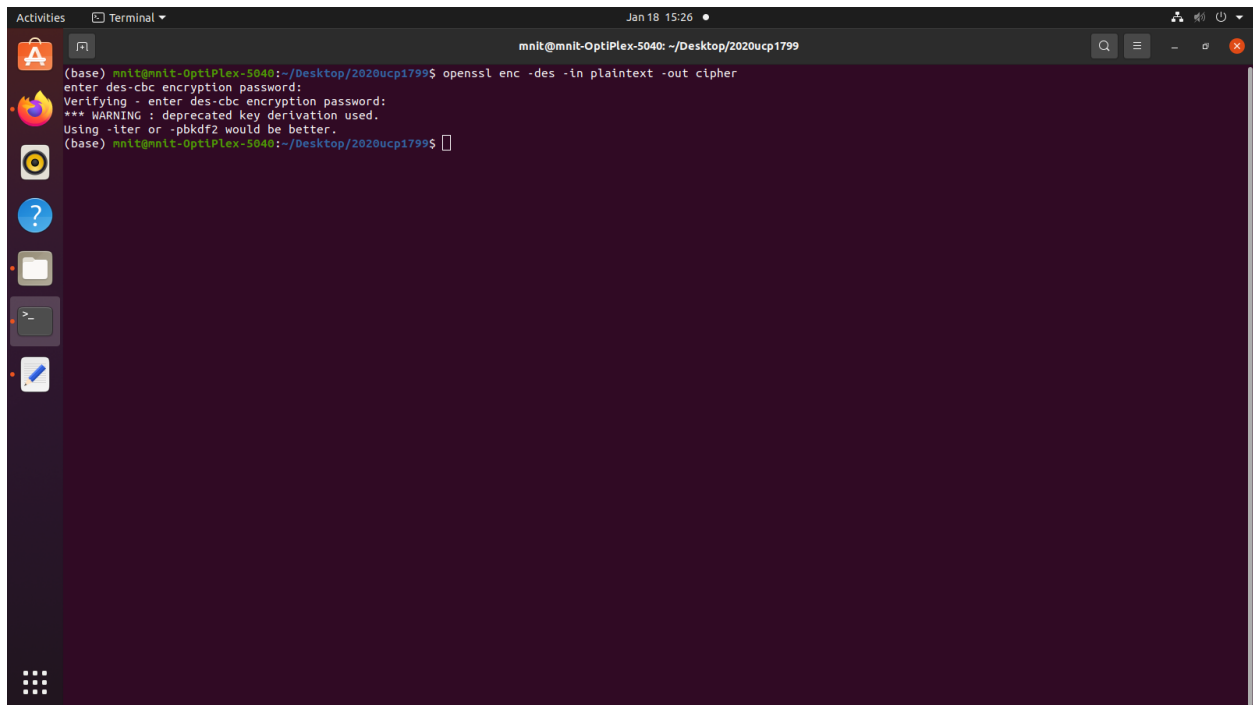
```

(base) mnlt@mnlt-OptiPlex-5040: ~/Desktop/2020ucp1799$ openssl rsautl -encrypt -in inp.txt -inkey public1.pem -pubin -out cipher.txt
(base) mnlt@mnlt-OptiPlex-5040: ~/Desktop/2020ucp1799$ cat cipher.txt
-----YnIXe1e3gG3*peo>e
U+Yr 7e<eySocgegeeeHw--]w(e=eneg4#FecbeY449Gw\5^Eg>--eUg>e)eeuu#(base) mnlt@mnlt-OptiPlex-5040: ~/Desktop/2020ucp1799$

```

Using des3 algorithm

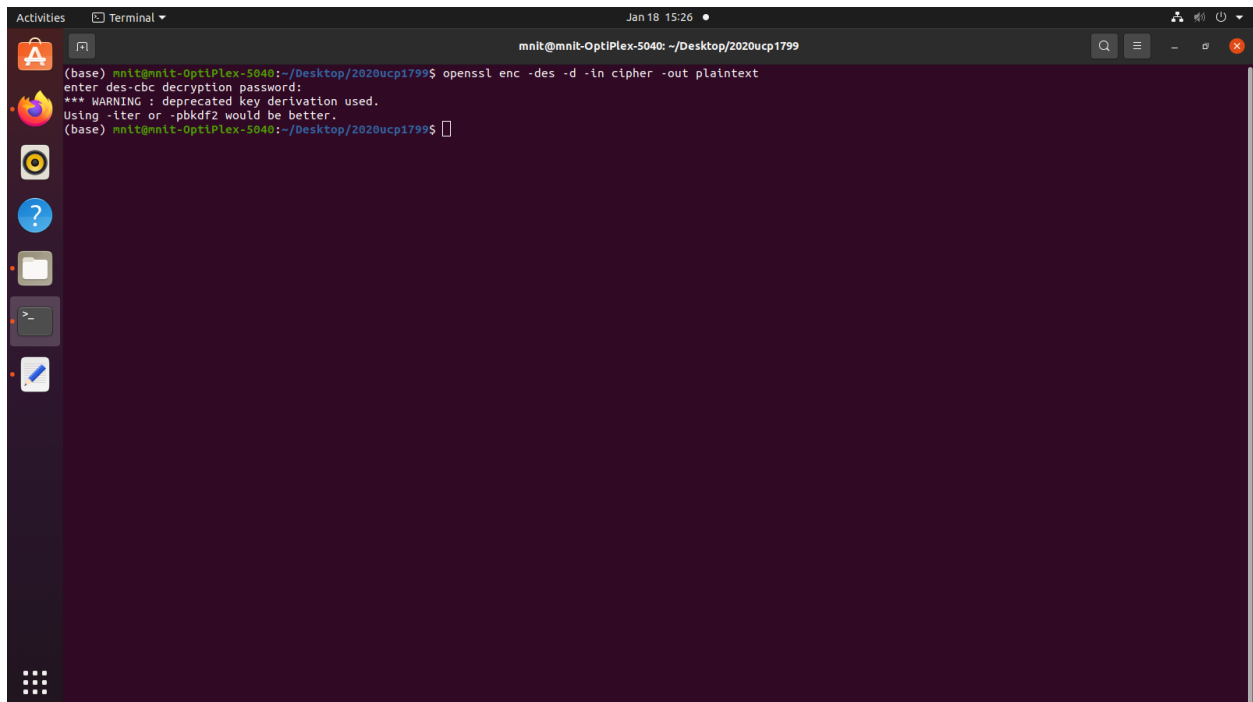
- Encryption



A terminal window titled "Terminal" with a dark background. The prompt is "mnit@mnit-OptiPlex-5040: ~/Desktop/2020ucp1799". The user enters the command "openssl enc -des -in plaintext -out cipher". The output shows the command being executed, followed by a password prompt, a verification prompt, a warning about deprecated key derivation, and a suggestion to use -iter or -pbkdf2. The prompt returns to the shell.

```
(base) mnit@mnit-OptiPlex-5040:~/Desktop/2020ucp1799$ openssl enc -des -in plaintext -out cipher
enter des-cbc encryption password:
Verifying - enter des-cbc encryption password:
*** WARNING : deprecated key derivation used.
Using -iter or -pbkdf2 would be better.
(base) mnit@mnit-OptiPlex-5040:~/Desktop/2020ucp1799$
```

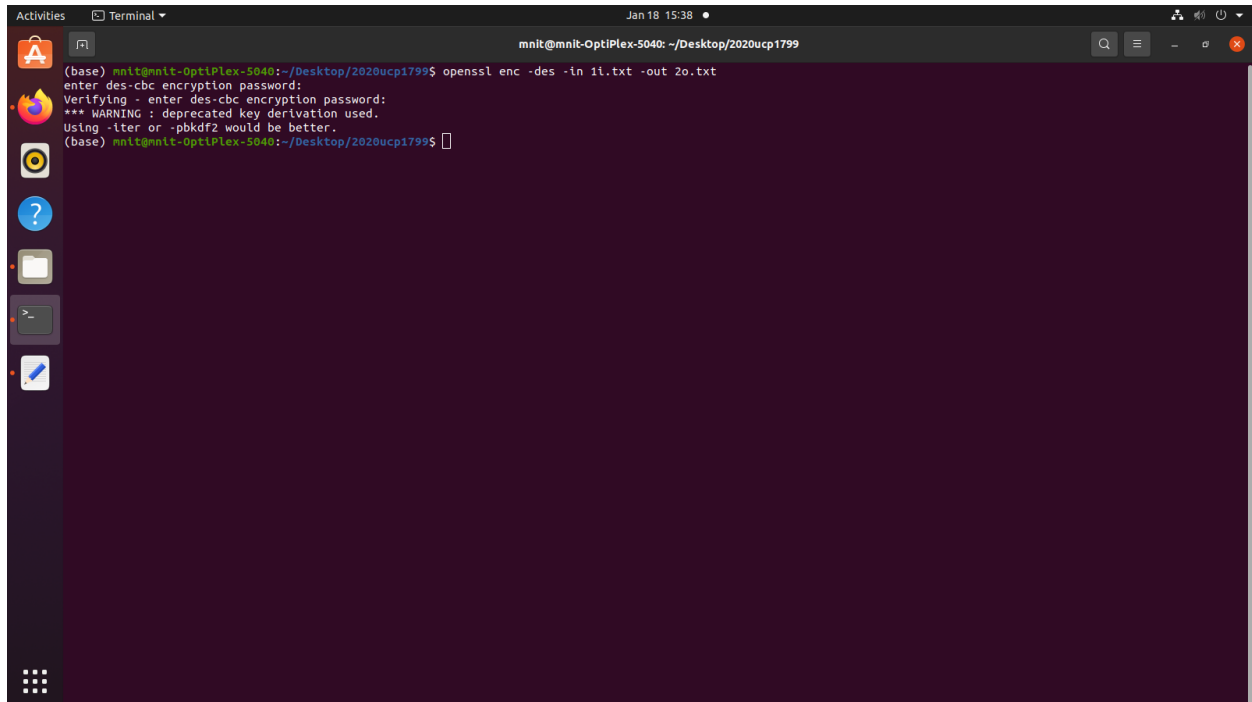
- Decryption



A terminal window titled "Terminal" with a dark background. The prompt is "mnit@mnit-OptiPlex-5040: ~/Desktop/2020ucp1799". The user enters the command "openssl enc -des -d -in cipher -out plaintext". The output shows the command being executed, followed by a password prompt, a verification prompt, a warning about deprecated key derivation, and a suggestion to use -iter or -pbkdf2. The prompt returns to the shell.

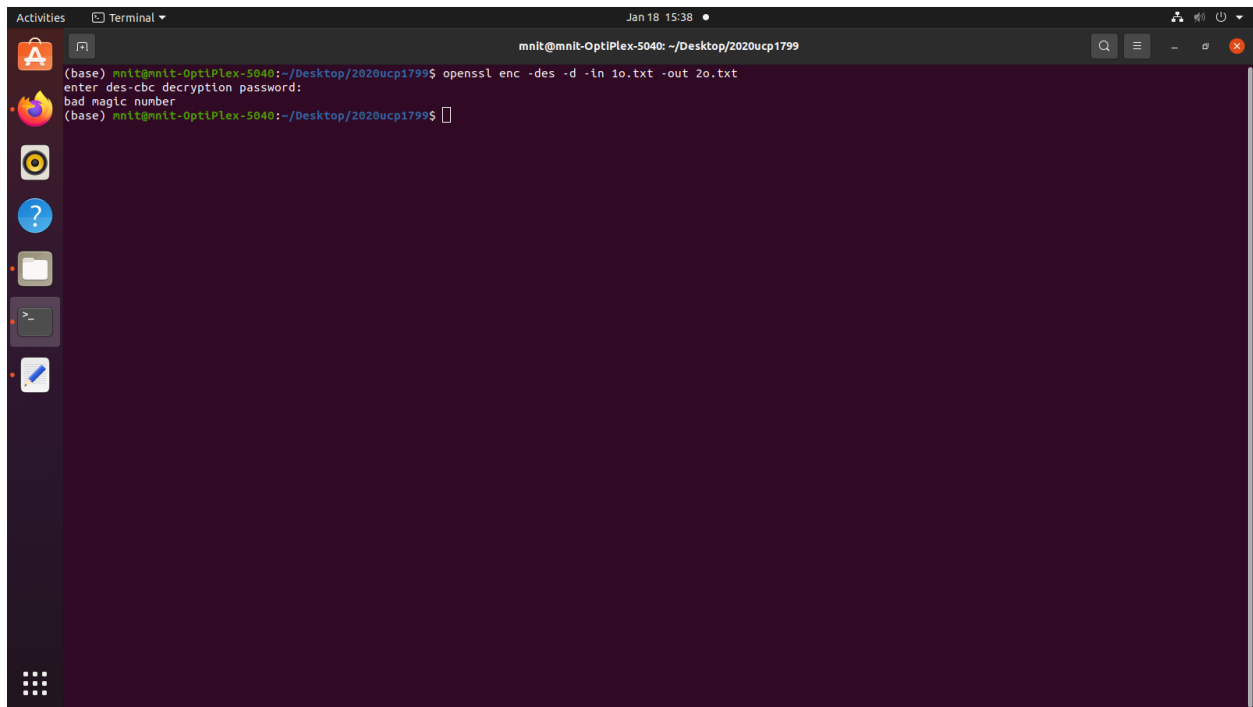
```
(base) mnit@mnit-OptiPlex-5040:~/Desktop/2020ucp1799$ openssl enc -des -d -in cipher -out plaintext
enter des-cbc decryption password:
*** WARNING : deprecated key derivation used.
Using -iter or -pbkdf2 would be better.
(base) mnit@mnit-OptiPlex-5040:~/Desktop/2020ucp1799$
```

Encryption and decryption Syntax:



A terminal window titled "Terminal" with a dark background. The window shows the execution of an OpenSSL command to encrypt a file. The prompt is "(base) mnit@mnit-OptiPlex-5040: ~/Desktop/2020ucp1799\$". The command entered is "openssl enc -des -in 11.txt -out 20.txt". The output shows the command being executed, a password prompt, a verification prompt, a warning about deprecated key derivation, and the use of a specific cipher and mode. The prompt returns to the shell.

```
(base) mnit@mnit-OptiPlex-5040:~/Desktop/2020ucp1799$ openssl enc -des -in 11.txt -out 20.txt
enter des-cbc encryption password:
Verifying - enter des-cbc encryption password:
*** WARNING : deprecated key derivation used.
Using -iter or -pbkdf2 would be better.
(base) mnit@mnit-OptiPlex-5040:~/Desktop/2020ucp1799$
```



A terminal window titled "Terminal" with a dark background. The prompt is "mnit@mnit-OptiPlex-5040: ~/Desktop/2020ucp1799". The user enters the command "openssl enc -des -d -in 1o.txt -out 2o.txt". The terminal displays the following output: "enter des-cbc decryption password:", "bad magic number", and then returns to the prompt "(base) mnit@mnit-OptiPlex-5040:~/Desktop/2020ucp1799\$". The left sidebar shows application icons for Activities, Home, Files, and others. The top bar shows the date "Jan 18 15:38" and system status icons.

```
(base) mnit@mnit-OptiPlex-5040:~/Desktop/2020ucp1799$ openssl enc -des -d -in 1o.txt -out 2o.txt
enter des-cbc decryption password:
bad magic number
(base) mnit@mnit-OptiPlex-5040:~/Desktop/2020ucp1799$
```

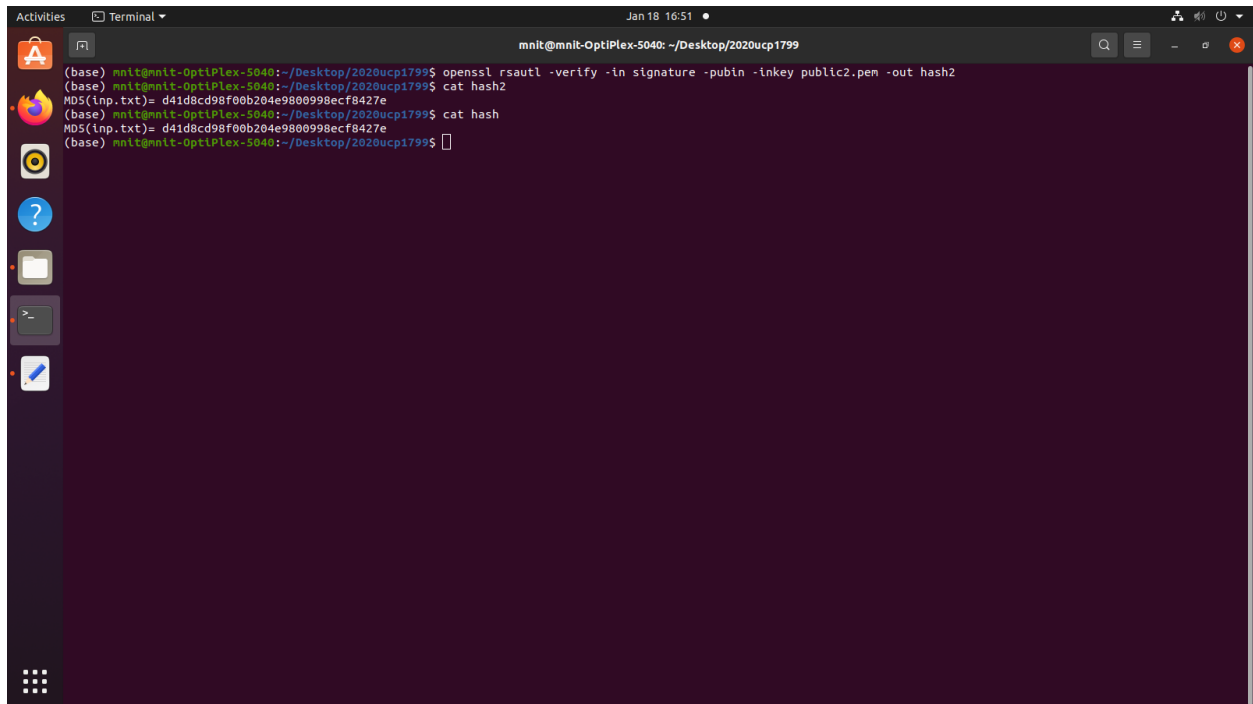
Signature

- Generating hash and signature

```
Activities Terminal Jan 18 16:41 mnit@mnit-OptiPlex-5040: ~/Desktop/2020ucp1799
(base) mnit@mnit-OptiPlex-5040:~/Desktop/2020ucp1799$ openssl dgst -md5 -out hash inp.txt
(base) mnit@mnit-OptiPlex-5040:~/Desktop/2020ucp1799$ cat hash
MD5(inp.txt)= d41d8cd98f00b204e9800998ecf8427e
(base) mnit@mnit-OptiPlex-5040:~/Desktop/2020ucp1799$
```

```
Activities Terminal Jan 18 16:49 mnit@mnit-OptiPlex-5040: ~/Desktop/2020ucp1799
(base) mnit@mnit-OptiPlex-5040:~/Desktop/2020ucp1799$ openssl rsautl -sign -in hash -inkey private2.pem -out signature
Enter pass phrase for private2.pem:
(base) mnit@mnit-OptiPlex-5040:~/Desktop/2020ucp1799$ cat signature
Cs*oebee,"e#+++++er4)eeYxesDY9]eekeeeVeee/-e]EeeeeeJe_eZ.eeH3eeppv<eebeHe eG0'3-f7Woe
eZSUe#eeeeeUeeOe.e*9pr_(base) mnit@mnit-OptiPlex-5040:~/Desktop/2020ucp1799$
```

- Hash for 2 different files



A terminal window titled "Terminal" with a dark background. The window shows a series of commands and their outputs. The first command is `openssl rsautl -verify -in signature -pubin -inkey public2.pem -out hash2`. The second command is `cat hash2`, which outputs `MD5(inp.txt)= d41d8cd98f00b204e9800998ecf8427e`. The third command is `cat hash`, which also outputs `MD5(inp.txt)= d41d8cd98f00b204e9800998ecf8427e`. The terminal window has a sidebar on the left with various application icons and a top bar with system information.

```
(base) mnit@mni-OptiPlex-5040:~/Desktop/2020ucp1799$ openssl rsautl -verify -in signature -pubin -inkey public2.pem -out hash2
(base) mnit@mni-OptiPlex-5040:~/Desktop/2020ucp1799$ cat hash2
MD5(inp.txt)= d41d8cd98f00b204e9800998ecf8427e
(base) mnit@mni-OptiPlex-5040:~/Desktop/2020ucp1799$ cat hash
MD5(inp.txt)= d41d8cd98f00b204e9800998ecf8427e
(base) mnit@mni-OptiPlex-5040:~/Desktop/2020ucp1799$
```

Certificate

- Create a request

```

rahul@rahul-pc:~/Desktop$ openssl req -new -key private.pem -out request
You are about to be asked to enter information that will be incorporated
into your certificate request.
What you are about to enter is what is called a Distinguished Name or a DN.
There are quite a few fields but you can leave some blank
For some fields there will be a default value,
If you enter '.', the field will be left blank.
-----
Country Name (2 letter code) [AU]:
State or Province Name (full name) [Some-State]:
Locality Name (eg, city) []:
Organization Name (eg, company) [Internet Widgits Pty Ltd]:
Organizational Unit Name (eg, section) []:
Common Name (e.g. server FQDN or YOUR name) []:
Email Address []:

Please enter the following 'extra' attributes
to be sent with your certificate request
A challenge password []:
An optional company name []:
rahul@rahul-pc:~/Desktop$
rahul@rahul-pc:~/Desktop$ cat request
-----BEGIN CERTIFICATE REQUEST-----
MIIBhDCB7gIBADBQswCQYDVQQGEwJBVTETMBEGA1UECAwKU29tZS1TdGF0ZTEh
MB8GA1UECgwYSW50ZXJuZuZGUqV2lkZ2l0cyBqdHkgTHRkMIGfMA0GCSqGSIb3DQEB
AQUAA4GNADCBiQKBgQD0ueXG3H/WYL1DHXX2Km1fgJWqmFEf+4LdRnRvS4YlBwZD
EMTB5D09TU+2CeTCRmV0txXp0v5SFFgPYr176c0ny36KUjz0WLZFzQPK/S+mehV8
oJmnEpcKj04sWLFzST72PygPVXPPzq7kC7q8lveS1y6CSHqkUVw0niEYZjGhlwID
AQABoAAwDQYJKoZIhvcNAQELBQADgYEAGXPJYLY7aaTDHRBrE0IN7lTqr+skotn
N/OPL3u8BKDO/Y6V2cPqf7Exm7J8iIM57nRluU3jtsqQwMACf0zJ10A0aavFBknD
77eaerCxb3WK7WP8qt6GhWk63IjsqYi/lonDYhNx3PolyXcfmpnH4/VJHKg+DFwh
0OUrrHp5uPI=
-----END CERTIFICATE REQUEST-----
rahul@rahul-pc:~/Desktop$

```

- Autosign the certificate

```

rahul@rahul-pc:~/Desktop$ openssl x509 -req -in request -signkey private.pem -out certificate
Certificate request self-signature ok
subject=C = AU, ST = Some-State, O = Internet Widgits Pty Ltd
rahul@rahul-pc:~/Desktop$ cat certificate
-----BEGIN CERTIFICATE-----
MIICDDCCAXUCFBsV0dJqBnr/GeSIWSyjj4lapkIMA0GCSqGSIB3DQEBwUAMEUx
CzAJBgNVBAYTAkFVMRMwEQYDVQQIDApTb211LLVN0YXRlMSEwHwYDVQQKDBhJbnRl
cm5ldCBXaWRnaXRzIFB0eSBMdGQwHhcNMjMwMTE4MjIyMDE4WmcNMjMwMjE3MjIy
MDE4WjBFMQswCQYDVQQGEwJBVTETMBEGA1UECAwKU29tZS1TdGF0ZTEhMB8GA1UE
CgwYSW50ZXJuZXQgV2lkZ2l0cyBqdHkgTHRkMIGfMA0GCSqGSIB3DQEBAQUAA4GN
ADCBiQKBggQDOueXG3H/WYL1DHXX2Km1fgJWqmFEf+4LdRnRvS4YlBwZDEMTB5D09
TU+2CeTCRmV0txXp0v5SFFgPYrL76c0ny36KUjz0WlZFzQPK/S+mehV8oJmnEpcK
j04sWLFzST72PygPVXPpzq7kC7q8lveS1y6CShqkUVw0niEYZjGHLwIDAQABMA0G
CSqGSIB3DQEBwUAA4GBAJVRNAL9pWVeNUIGRrZCT/Uo19wDJNuDaBvDVbxBg2y0
q+tvZ88m51/5cIYw0Xu4LqjxfqwiHXJ5L2BMIXNMxaFACQzt2nBt1+0Np/mk2++j
1ez5fQS9IDnWsxVo6Hirirx2+R8LmFKZkoQCXrpEaUH42XIWpzyhK33teEVNNrxV
-----END CERTIFICATE-----
rahul@rahul-pc:~/Desktop$

```

- Visualise Certificate


```

rahul@rahul-pc:~/Desktop$ openssl x509 -in certificate -text -noout
Certificate:
    Data:
        Version: 1 (0x0)
        Serial Number:
            1b:15:d1:d2:6a:06:7a:ff:19:e4:88:59:2c:a3:ca:3e:25:6a:99:08
        Signature Algorithm: sha256WithRSAEncryption
        Issuer: C = AU, ST = Some-State, O = Internet Widgits Pty Ltd
        Validity
            Not Before: Jan 18 22:20:18 2023 GMT
            Not After : Feb 17 22:20:18 2023 GMT
        Subject: C = AU, ST = Some-State, O = Internet Widgits Pty Ltd
        Subject Public Key Info:
            Public Key Algorithm: rsaEncryption
                Public-Key: (1024 bit)
                Modulus:
                    00:ce:b9:e5:c6:dc:7f:d6:60:bd:43:1d:75:f6:2a:
                    6d:5f:80:95:aa:98:51:1f:fb:82:dd:46:74:6f:4b:
                    86:25:07:06:43:10:c4:c1:e4:33:bd:4d:4f:b6:09:
                    e4:c2:46:65:4e:b7:15:e9:d2:fe:52:14:58:0f:62:
                    b9:7b:e9:c3:a7:cb:7e:8a:52:3c:f4:5a:56:45:cd:
                    03:ca:fd:2f:a6:7a:15:7c:a0:99:a7:12:97:0a:8c:
                    ee:2c:58:b7:f3:49:3e:f6:3f:28:0f:55:73:e9:ce:
                    ae:e4:0b:ba:bc:96:f7:92:d7:2e:82:4a:1a:a4:51:
                    5c:34:9e:21:18:66:31:87:97
                Exponent: 65537 (0x10001)
            Signature Algorithm: sha256WithRSAEncryption
            Signature Value:
                95:51:34:02:fd:a5:65:5e:35:42:06:46:b6:42:4f:f5:28:d7:
                dc:03:24:db:83:68:1b:c3:55:bc:41:83:6c:8e:ab:eb:55:67:
                cf:26:e7:5f:f9:70:86:30:d1:7b:b8:2e:a8:f1:7e:ac:22:1d:
                72:79:2f:60:4c:23:13:4c:5d:a1:40:09:0c:ed:da:70:6d:d7:
                ed:0d:a7:f9:a4:db:ef:a3:d5:ec:f9:7d:04:bd:20:39:d6:b3:
                15:68:e8:72:2b:8a:bc:76:f9:1f:0b:98:52:99:92:84:02:5e:
                ba:44:69:41:f8:d9:72:16:a7:3c:a1:2b:7d:ed:78:45:4d:36:
                bc:55
rahul@rahul-pc:~/Desktop$

```

Final Assignment

- Making files

```

rahul@rahul-pc:~/Desktop$ cat file.txt
0000000000000000
1111111111111111
2222222222222222
0000000000000000
1111111111111111
2222222222222222
0000000000000000
1111111111111111
2222222222222222
rahul@rahul-pc:~/Desktop$ cat modified_file.txt
0000000000000000
1111111111111111
2222222222222222
0000000100000000
1111111111111111
2222222222222222
0000000000000000
1111111111111111
2222222222222222
rahul@rahul-pc:~/Desktop$

```

- AES encryption on file.txt in ECB mode

```

rahul@rahul-pc:~/Desktop$ openssl aes-256-ecb -e -in file.txt -out cipher_ecb.bin -nosalt
enter AES-256-ECB encryption password:
Verifying - enter AES-256-ECB encryption password:
*** WARNING : deprecated key derivation used.
Using -iter or -pbkdf2 would be better.
rahul@rahul-pc:~/Desktop$ xxd cipher_ecb.bin
00000000: d69b 3162 0522 5aad 2bab 3a1a e8c4 293d  ..1b."Z.+.:...)=
00000010: b3bb 2c98 fcd6 be4b db74 c5d2 bc97 5776  ..,....K.t....Wv
00000020: 9411 7eae 1415 4296 9752 f529 f422 fbf8  ..~...B..R.)."..
00000030: d69b 3162 0522 5aad 2bab 3a1a e8c4 293d  ..1b."Z.+.:...)=
00000040: b3bb 2c98 fcd6 be4b db74 c5d2 bc97 5776  ..,....K.t....Wv
00000050: 9411 7eae 1415 4296 9752 f529 f422 fbf8  ..~...B..R.)."..
00000060: d69b 3162 0522 5aad 2bab 3a1a e8c4 293d  ..1b."Z.+.:...)=
00000070: b3bb 2c98 fcd6 be4b db74 c5d2 bc97 5776  ..,....K.t....Wv
00000080: 9411 7eae 1415 4296 9752 f529 f422 fbf8  ..~...B..R.)."..
00000090: 5434 0bee c2c1 2209 62b7 07be 6bbf 8e0e  T4....".b...k...
rahul@rahul-pc:~/Desktop$

```

- AES encryption on file.txt in CBC mode

```

rahul@rahul-pc:~/Desktop$ openssl aes-256-cbc -e -in file.txt -out cipher_cbc.bin -nosalt
enter AES-256-CBC encryption password:
Verifying - enter AES-256-CBC encryption password:
*** WARNING : deprecated key derivation used.
Using -iter or -pbkdf2 would be better.
rahul@rahul-pc:~/Desktop$ xxd cipher_cbc.bin
00000000: ccc1 5c63 848b 28de 8a5b 74f8 c523 d6bb  ..\c..(..[t..#..
00000010: ff3f 6f0d d96f cda9 5d5f fb2c b632 a23b  .?o...o..]_.,.2.;
00000020: 1ef9 f6f5 badf 2970 c57e db12 00ee 02c1  .....p.~.....
00000030: 0171 b780 26c2 f31c aca3 edcc b4e4 92a5  .q...&.....
00000040: 4b12 8e98 f7ab 1fc1 2902 4bec 5051 dd83  K.....).K.PQ..
00000050: 3f00 af4f 799e 7e21 4c42 3cb9 b6ba 5715  ?.Oy.~!LB<...W.
00000060: e7cf 4bb0 abb4 2eda d82f febe ec61 8bdd  ..K...../...a..
00000070: 6a29 6c93 508e 776a b5aa 415a 426a 934f  j)l.P.wj..AZBj.O
00000080: 898b c202 c248 a7eb df74 0aa2 6d38 4db3  ....H...t..m8M.
00000090: 8715 851e 145b 13f0 bdf0 590d 6fb3 628f  ....[....Y.o.b.
rahul@rahul-pc:~/Desktop$

```

- AES encryption on modified_file.txt in ECB mode

```

rahul@rahul-pc:~/Desktop$ openssl aes-256-ecb -e -in modified_file.txt -out cipher_ecb_modified.b
enter AES-256-ECB encryption password:
Verifying - enter AES-256-ECB encryption password:
*** WARNING : deprecated key derivation used.
Using -iter or -pbkdf2 would be better.
rahul@rahul-pc:~/Desktop$ xxd cipher_ecb_modified.bin
00000000: d69b 3162 0522 5aad 2bab 3a1a e8c4 293d  ..1b."Z.+.:...)=
00000010: b3bb 2c98 fcd6 be4b db74 c5d2 bc97 5776  ..,....K.t....Wv
00000020: 9411 7eae 1415 4296 9752 f529 f422 fbf8  ..~...B..R.)."..
00000030: d359 65d7 daaa ab70 1dad d8bc 49b1 f1e5  .Ye....p....I...
00000040: b3bb 2c98 fcd6 be4b db74 c5d2 bc97 5776  ..,....K.t....Wv
00000050: 9411 7eae 1415 4296 9752 f529 f422 fbf8  ..~...B..R.)."..
00000060: d69b 3162 0522 5aad 2bab 3a1a e8c4 293d  ..1b."Z.+.:...)=
00000070: b3bb 2c98 fcd6 be4b db74 c5d2 bc97 5776  ..,....K.t....Wv
00000080: 9411 7eae 1415 4296 9752 f529 f422 fbf8  ..~...B..R.)."..
00000090: 5434 0bee c2c1 2209 62b7 07be 6bbf 8e0e  T4....".b...k...
rahul@rahul-pc:~/Desktop$

```

- AES encryption on modified_file.txt in CBC mode

```

rahul@rahul-pc:~/Desktop$ openssl aes-256-cbc -e -in modified_file.txt -out cipher_cbc_modified.b
enter AES-256-CBC encryption password:
Verifying - enter AES-256-CBC encryption password:
*** WARNING : deprecated key derivation used.
Using -iter or -pbkdf2 would be better.
rahul@rahul-pc:~/Desktop$ xxd cipher_cbc_modified.bin
00000000: ccc1 5c63 848b 28de 8a5b 74f8 c523 d6bb  ..\c...(.[t..#..
00000010: ff3f 6f0d d96f cda9 5d5f fb2c b632 a23b  .?o..o..]_,.2.;
00000020: 1ef9 f6f5 badf 2970 c57e db12 00ee 02c1  .....)p.~.....
00000030: f46c df16 eaaf a219 10f6 ac22 a0d8 c017  .l.....".....
00000040: b1a9 a1a0 1192 4dff d09f 23f9 2007 7fb5  .....M...#. ...
00000050: 07af 1015 ca04 5ff9 bf33 609b 84e9 2365  ....._...3`...#e
00000060: 3754 9f33 58e5 8956 9d32 e8e5 f819 c1b1  7T.3X..V.2.....
00000070: a604 59fc 7dab 3f18 6062 4568 6862 c005  ..Y.}.?.`bEhnb..
00000080: f71b c1af bf66 efbe d5ed 1344 f65f 70c5  .....f.....D._p.
00000090: d49d 6f9c eeef 5496 e953 3eee 72e3 0059  ..o...T..S>.r..Y
rahul@rahul-pc:~/Desktop$ █

```