Cryptography (CS362)

Assignment - 2

U19CS012

Aim: To demonstrate working of **Diffie Hellman Key Agreement protocol**.

Library Used: *OpenSSL*

To Show: Same key is shared between two users i.e. User A and User B.

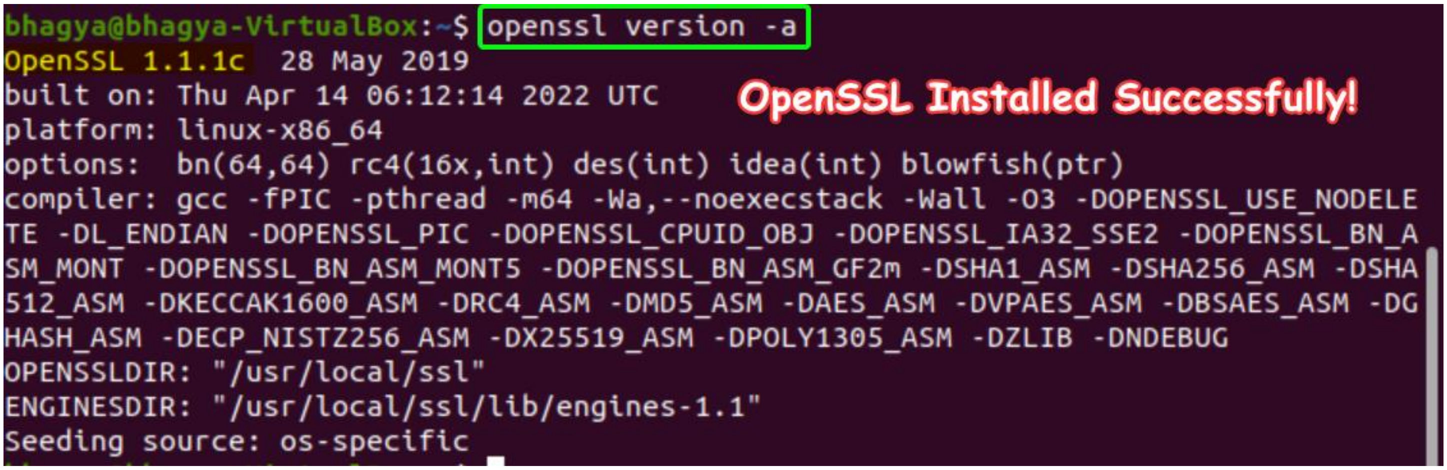
To Generate Below Mentioned Files:

1) Global Parameter file

2) Public key Private key files for User A and User B

3) Shared key file for User A and User B

1.) Check if **OpenSSL** is installed in your Linux system or not. If not, go to this link to install OpenSSL in your system.



```
bhagya@bhagya-VirtualBox:~$ openssl version -a
OpenSSL 1.1.1c  28 May 2019
built on: Thu Apr 14 06:12:14 2022 UTC
platform: linux-x86_64
options:  bn(64,64) rc4(16x,int) des(int) idea(int) blowfish(ptr)
compiler: gcc -fPIC -pthread -m64 -Wa,--noexecstack -Wall -O3 -DOPENSSL_USE_NODELE
TE -DL_ENDIAN -DOPENSSL_PIC -DOPENSSL_CPUID_OBJ -DOPENSSL_IA32_SSE2 -DOPENSSL_BN_A
SM_MONT -DOPENSSL_BN_ASM_MONT5 -DOPENSSL_BN_ASM_GF2m -DSHA1_ASM -DSHA256_ASM -DSHA
512_ASM -DKECCAK1600_ASM -DRC4_ASM -DMD5_ASM -DAES_ASM -DVPAES_ASM -DBSAES_ASM -DG
HASH_ASM -DECP_NISTZ256_ASM -DX25519_ASM -DPOLY1305_ASM -DZLIB -DNDEBUG
OPENSSLDIR: "/usr/local/ssl"
ENGINESDIR: "/usr/local/ssl/lib/engines-1.1"
Seeding source: os-specific
```

Reference - https://fedingo.com/how-to-install-OpenSSL-in-ubuntu/

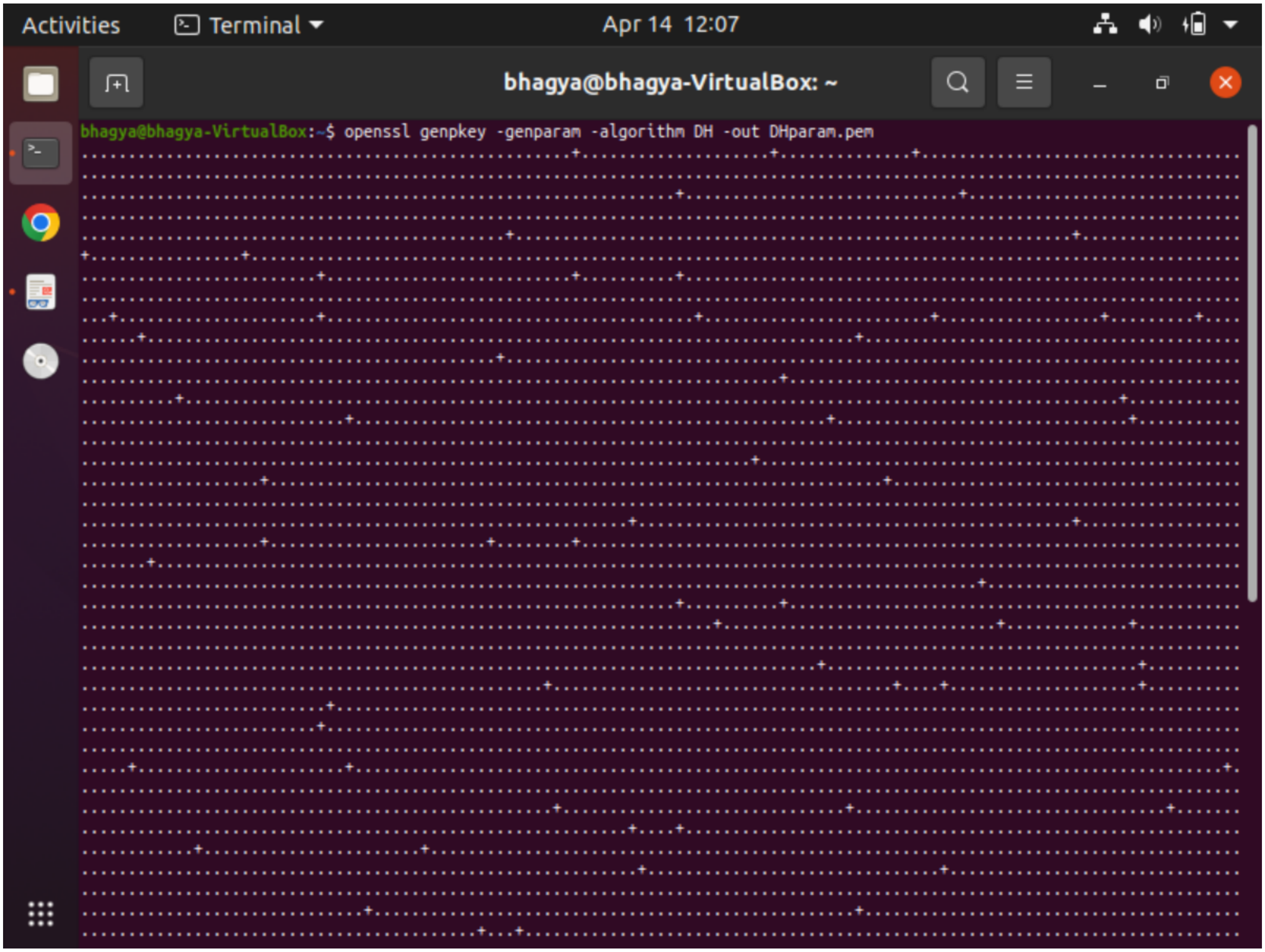
2.) Generate a Diffie-Hellman **Global Domain** Parameters and save it in a file `DHparam.pem`

Use the command:

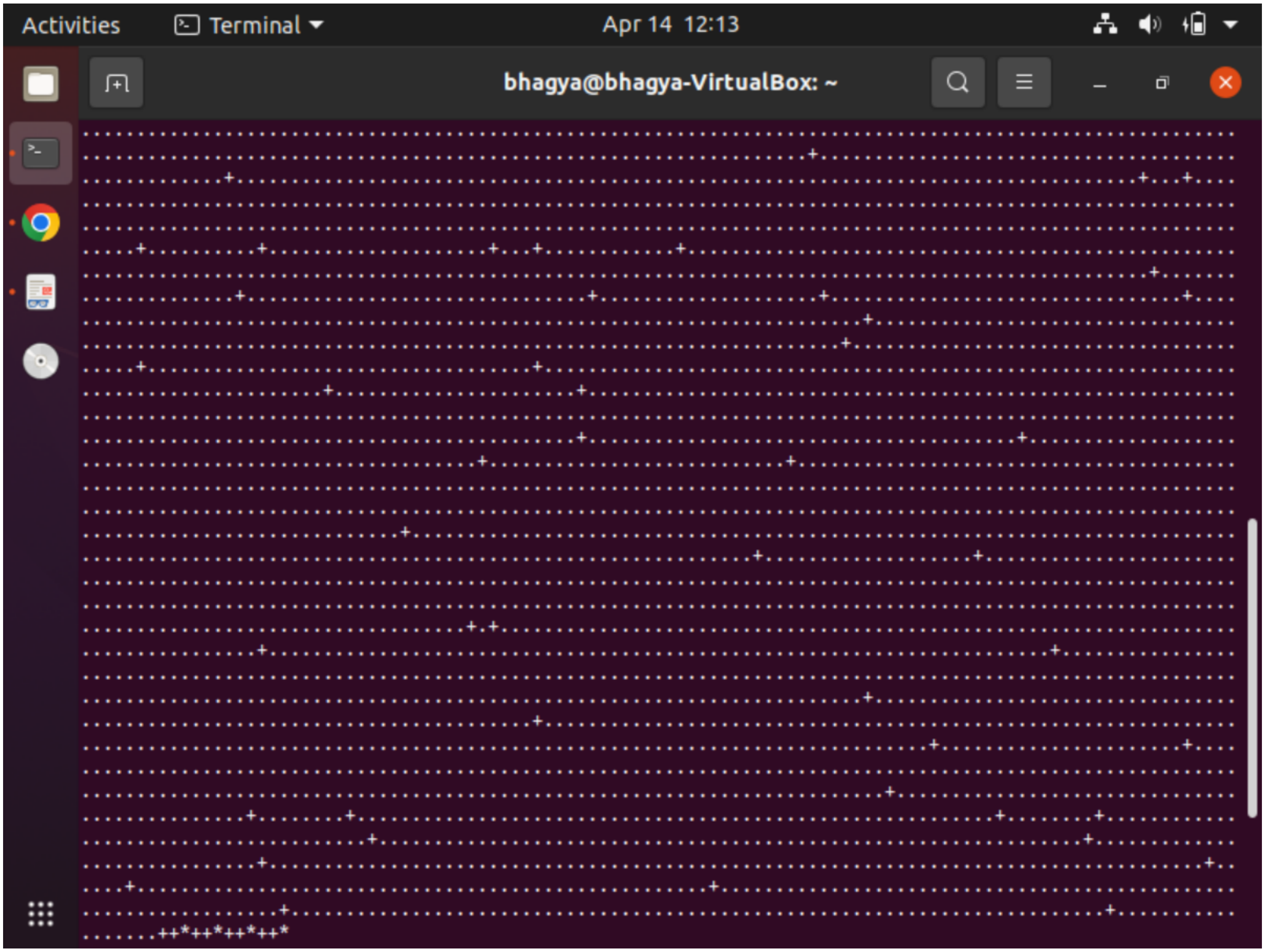
```
openssl genpkey -genparam -algorithm DH -out DHparam.pem
```

Meaning –

Command	Meaning
`openssl`	OpenSSL command line tool
`genpkey`	Generates a Private key
`-genparam`	Generate a set of parameters instead of a private key.
`-algorithm DH`	Using Diffie Hellman Algorithm
`-out DHparam.pem`	Output saved to DHparam.pem



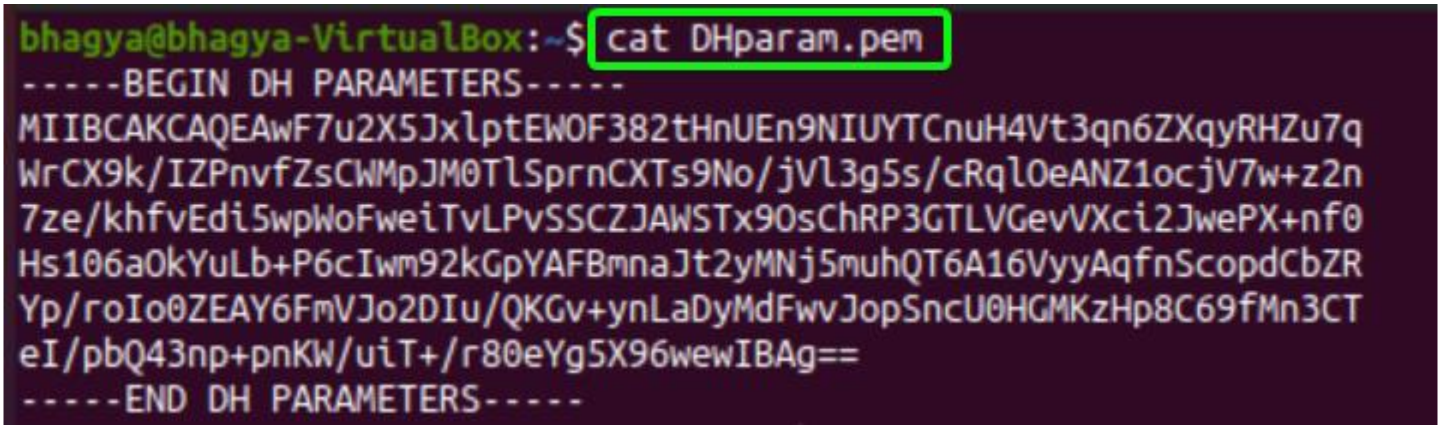
```
bhagya@bhagya-VirtualBox:~$ openssl genpkey -genparam -algorithm DH -out DHparam.pem
```



```
.......++*++*++*++*
```

3.) Display the generated global public parameters, using the following commands. See the difference between both the commands.

```
cat DHparam.pem
```

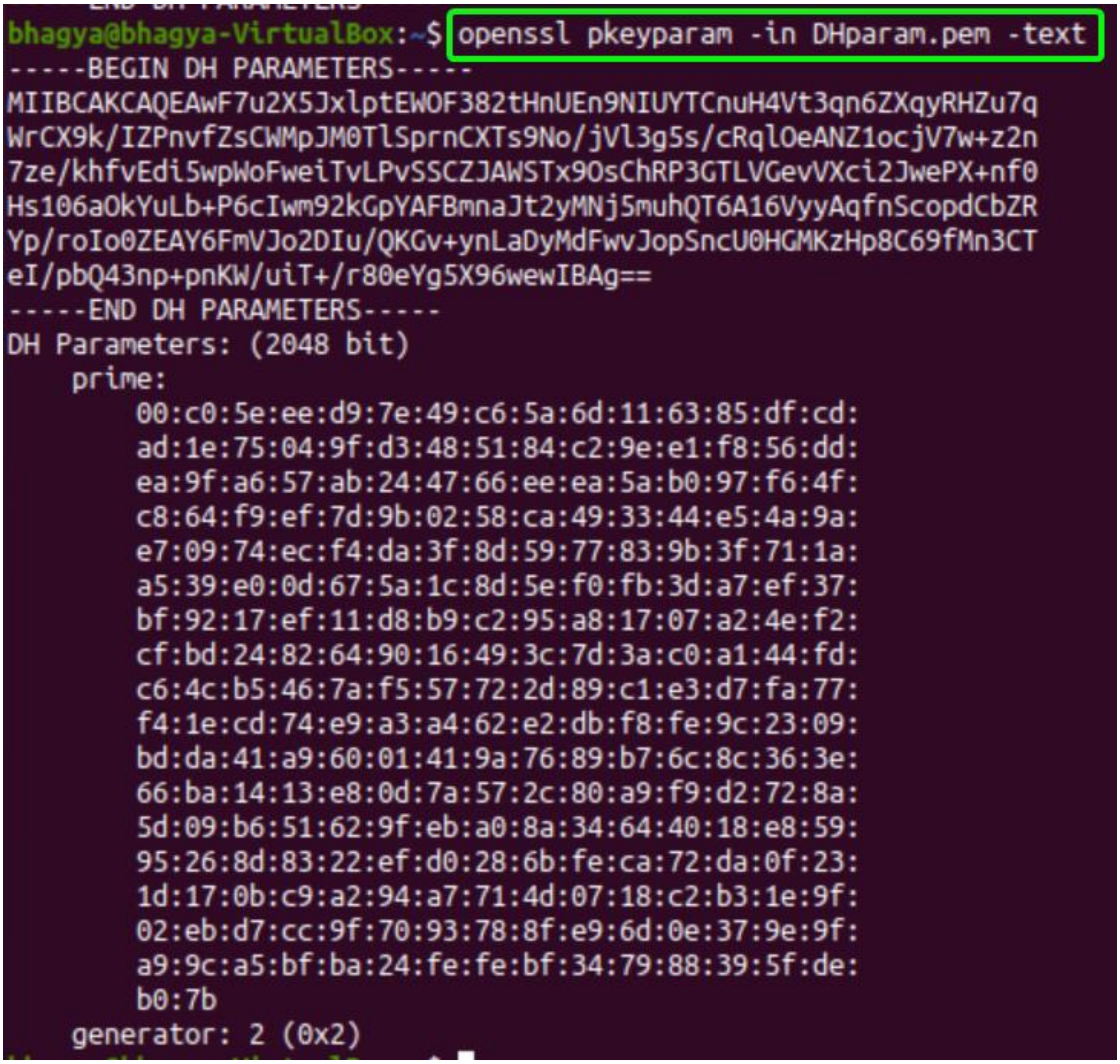


```
bhagya@bhagya-VirtualBox:~$ cat DHparam.pem
-----BEGIN DH PARAMETERS-----
MIIBCAKCAQEAwF7u2X5JxlptEWOF382tHnUEn9NIUYTCnuH4Vt3qn6ZXqyRHZu7q
WrCX9k/IZPnvfZsCWMpJM0TlSprnCXTs9No/jVl3g5s/cRql0eANZ1ocjV7w+z2n
7ze/khfvEdi5wpWoFweiTvLPvSSCZJAWSTx9OsChRP3GTLVGevVXci2JwePX+nf0
Hs106aOkYuLb+P6cIwm92kGpYAFBmnaJt2yMNj5muhQT6A16VyyAqfnScopdCbZR
Yp/roIo0ZEAY6FmVJo2DIu/QKGv+ynLaDyMdFwvJopSncU0HGMKzHp8C69fMn3CT
eI/pbQ43np+pnKW/uiT+/r80eYg5X96wewIBAg==
-----END DH PARAMETERS-----
```

Print out text version of parameters

```
openssl pkeyparam -in DHparam.pem –text
```

Command	Meaning
`openssl`	OpenSSL command line tool
`pkeyparam`	Public key algorithm parameter management
`-in DHparam.pem`	Input File to Read Parameters
`-text`	Print an (unencrypted) text representation of private and public keys and parameters along with the PEM or DER structure. {Certificates}



```
bhagya@bhagya-VirtualBox:~$ openssl pkeyparam -in DHparam.pem -text
-----BEGIN DH PARAMETERS-----
MIIBCAKCAQEAwF7u2X5JxlptEWOF382tHnUEn9NIUYTCnuH4Vt3qn6ZXqyRHZu7q
WrCX9k/IZPnvfZsCWMpJM0TlSprnCXTs9No/jVl3g5s/cRql0eANZ1ocjV7w+z2n
7ze/khfvEdi5wpWoFweiTvLPvSSCZJAWSTx9OsChRP3GTLVGevVXci2JwePX+nf0
Hs106aOkYuLb+P6cIwm92kGpYAFBmnaJt2yMNj5muhQT6A16VyyAqfnScopdCbZR
Yp/roIo0ZEAY6FmVJo2DIu/QKGv+ynLaDyMdFwvJopSncU0HGMKzHp8C69fMn3CT
eI/pbQ43np+pnKW/uiT+/r80eYg5X96wewIBAg==
-----END DH PARAMETERS-----
DH Parameters: (2048 bit)
    prime:
        00:c0:5e:ee:d9:7e:49:c6:5a:6d:11:63:85:df:cd:
        ad:1e:75:04:9f:d3:48:51:84:c2:9e:e1:f8:56:dd:
        ea:9f:a6:57:ab:24:47:66:ee:ea:5a:b0:97:f6:4f:
        c8:64:f9:ef:7d:9b:02:58:ca:49:33:44:e5:4a:9a:
        e7:09:74:ec:f4:da:3f:8d:59:77:83:9b:3f:71:1a:
        a5:39:e0:0d:67:5a:1c:8d:5e:f0:fb:3d:a7:ef:37:
        bf:92:17:ef:11:d8:b9:c2:95:a8:17:07:a2:4e:f2:
        cf:bd:24:82:64:90:16:49:3c:7d:3a:c0:a1:44:fd:
        c6:4c:b5:46:7a:f5:57:72:2d:89:c1:e3:d7:fa:77:
        f4:1e:cd:74:e9:a3:a4:62:e2:db:f8:fe:9c:23:09:
        bd:da:41:a9:60:01:41:9a:76:89:b7:6c:8c:36:3e:
        66:ba:14:13:e8:0d:7a:57:2c:80:a9:f9:d2:72:8a:
        5d:09:b6:51:62:9f:eb:a0:8a:34:64:40:18:e8:59:
        95:26:8d:83:22:ef:d0:28:6b:fe:ca:72:da:0f:23:
        1d:17:0b:c9:a2:94:a7:71:4d:07:18:c2:b3:1e:9f:
        02:eb:d7:cc:9f:70:93:78:8f:e9:6d:0e:37:9e:9f:
        a9:9c:a5:bf:ba:24:fe:fe:bf:34:79:88:39:5f:de:
        b0:7b
    generator: 2 (0x2)
```

We can observe the **Prime** and the **Generator** along with DH Parameters.

4.) The global public parameters generated in above steps can now be used by User A and User B in the protocol to generate their own **Public** and **Private** key.

Save the keys in files `DHkeyA.pem` and `DHkeyB.pem` for User A and B respectively.

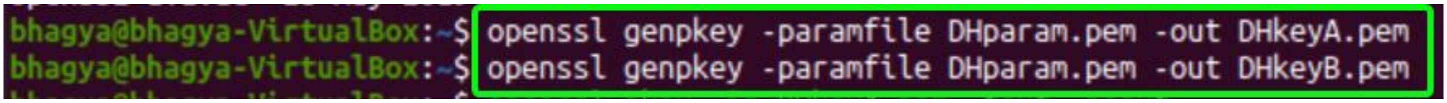
Use the following **commands** for this step.

For User A:

```
OpenSSL genpkey -paramfile DHparam.pem -out DHkeyA.pem
```

For User B:

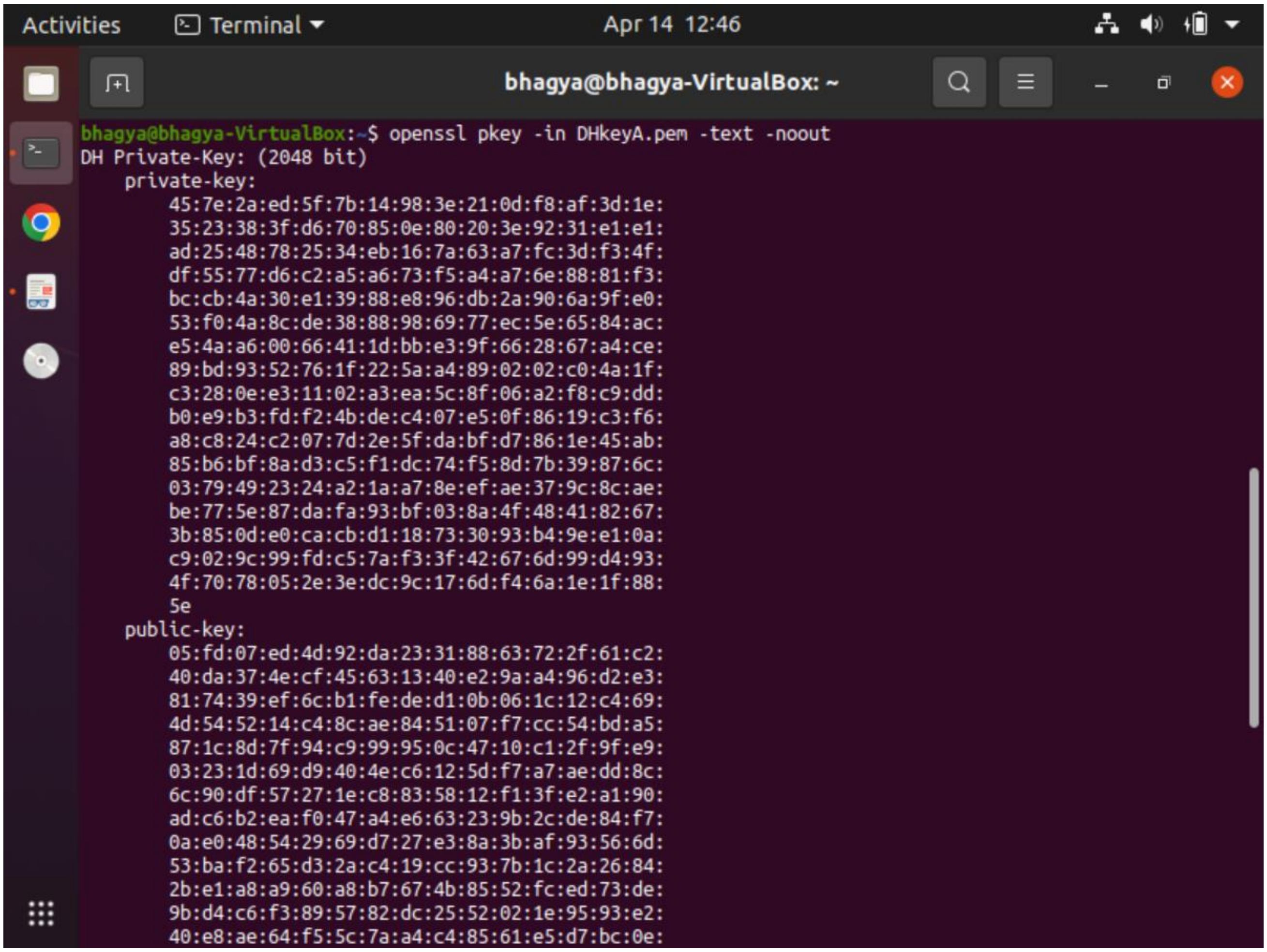
```
OpenSSL genpkey -paramfile DHparam.pem -out DHkeyB.pem
```



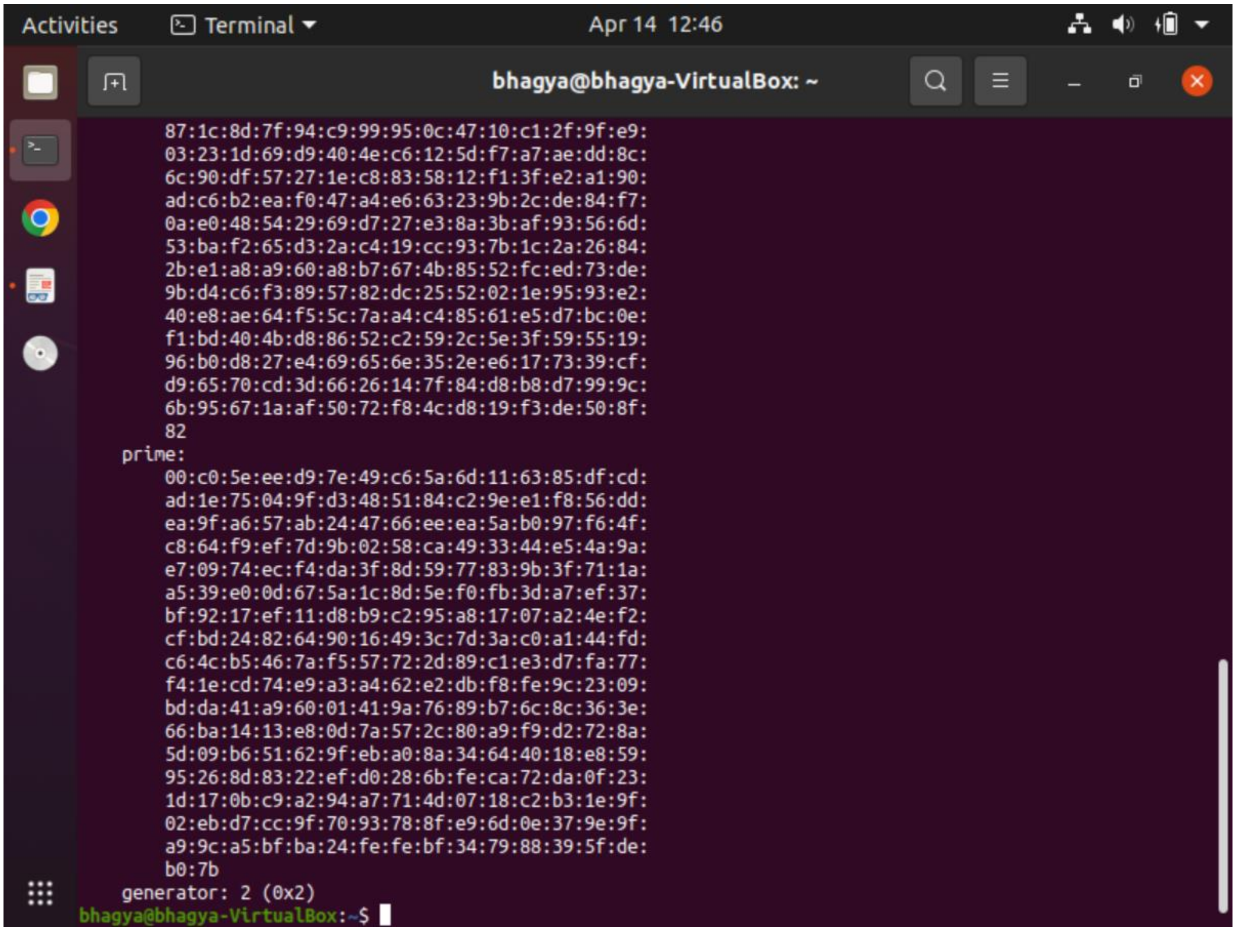
```
bhagya@bhagya-VirtualBox:~$ openssl genpkey -paramfile DHparam.pem -out DHkeyA.pem
bhagya@bhagya-VirtualBox:~$ openssl genpkey -paramfile DHparam.pem -out DHkeyB.pem
```

5.) Display the public and private key using following command

```
OpenSSL pkey -in DHkeyA.pem -text -noout
```

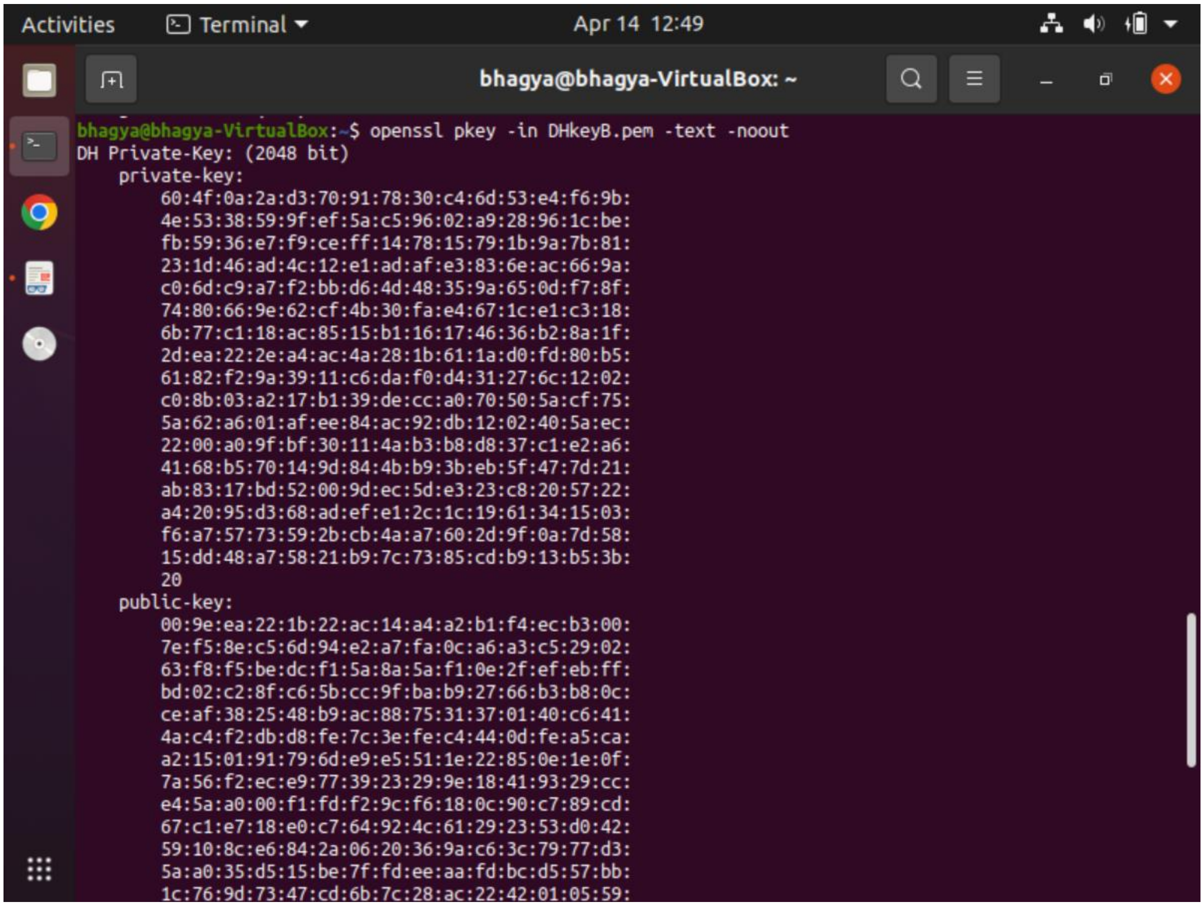


```
bhagya@bhagya-VirtualBox:~$ openssl pkey -in DHkeyA.pem -text -noout
DH Private-Key: (2048 bit)
    private-key:
        45:7e:2a:ed:5f:7b:14:98:3e:21:0d:f8:af:3d:1e:
        35:23:38:3f:d6:70:85:0e:80:20:3e:92:31:e1:e1:
        ad:25:48:78:25:34:eb:16:7a:63:a7:fc:3d:f3:4f:
        df:55:77:d6:c2:a5:a6:73:f5:a4:a7:6e:88:81:f3:
        bc:cb:4a:30:e1:39:88:e8:96:db:2a:90:6a:9f:e0:
        53:f0:4a:8c:de:38:88:98:69:77:ec:5e:65:84:ac:
        e5:4a:a6:00:66:41:1d:bb:e3:9f:66:28:67:a4:ce:
        89:bd:93:52:76:1f:22:5a:a4:89:02:02:c0:4a:1f:
        c3:28:0e:e3:11:02:a3:ea:5c:8f:06:a2:f8:c9:dd:
        b0:e9:b3:fd:f2:4b:de:c4:07:e5:0f:86:19:c3:f6:
        a8:c8:24:c2:07:7d:2e:5f:da:bf:d7:86:1e:45:ab:
        85:b6:bf:8a:d3:c5:f1:dc:74:f5:8d:7b:39:87:6c:
        03:79:49:23:24:a2:1a:a7:8e:ef:ae:37:9c:8c:ae:
        be:77:5e:87:da:fa:93:bf:03:8a:4f:48:41:82:67:
        3b:85:0d:e0:ca:cb:d1:18:73:30:93:b4:9e:e1:0a:
        c9:02:9c:99:fd:c5:7a:f3:3f:42:67:6d:99:d4:93:
        4f:70:78:05:2e:3e:dc:9c:17:6d:f4:6a:1e:1f:88:
        5e
    public-key:
        05:fd:07:ed:4d:92:da:23:31:88:63:72:2f:61:c2:
        40:da:37:4e:cf:45:63:13:40:e2:9a:a4:96:d2:e3:
        81:74:39:ef:6c:b1:fe:de:d1:0b:06:1c:12:c4:69:
        4d:54:52:14:c4:8c:ae:84:51:07:f7:cc:54:bd:a5:
        87:1c:8d:7f:94:c9:99:95:0c:47:10:c1:2f:9f:e9:
        03:23:1d:69:d9:40:4e:c6:12:5d:f7:a7:ae:dd:8c:
        6c:90:df:57:27:1e:c8:83:58:12:f1:3f:e2:a1:90:
        ad:c6:b2:ea:f0:47:a4:e6:63:23:9b:2c:de:84:f7:
        0a:e0:48:54:29:69:d7:27:e3:8a:3b:af:93:56:6d:
        53:ba:f2:65:d3:2a:c4:19:cc:93:7b:1c:2a:26:84:
        2b:e1:a8:a9:60:a8:b7:67:4b:85:52:fc:ed:73:de:
        9b:d4:c6:f3:89:57:82:dc:25:52:02:1e:95:93:e2:
        40:e8:ae:64:f5:5c:7a:a4:c4:85:61:e5:d7:bc:0e:
```

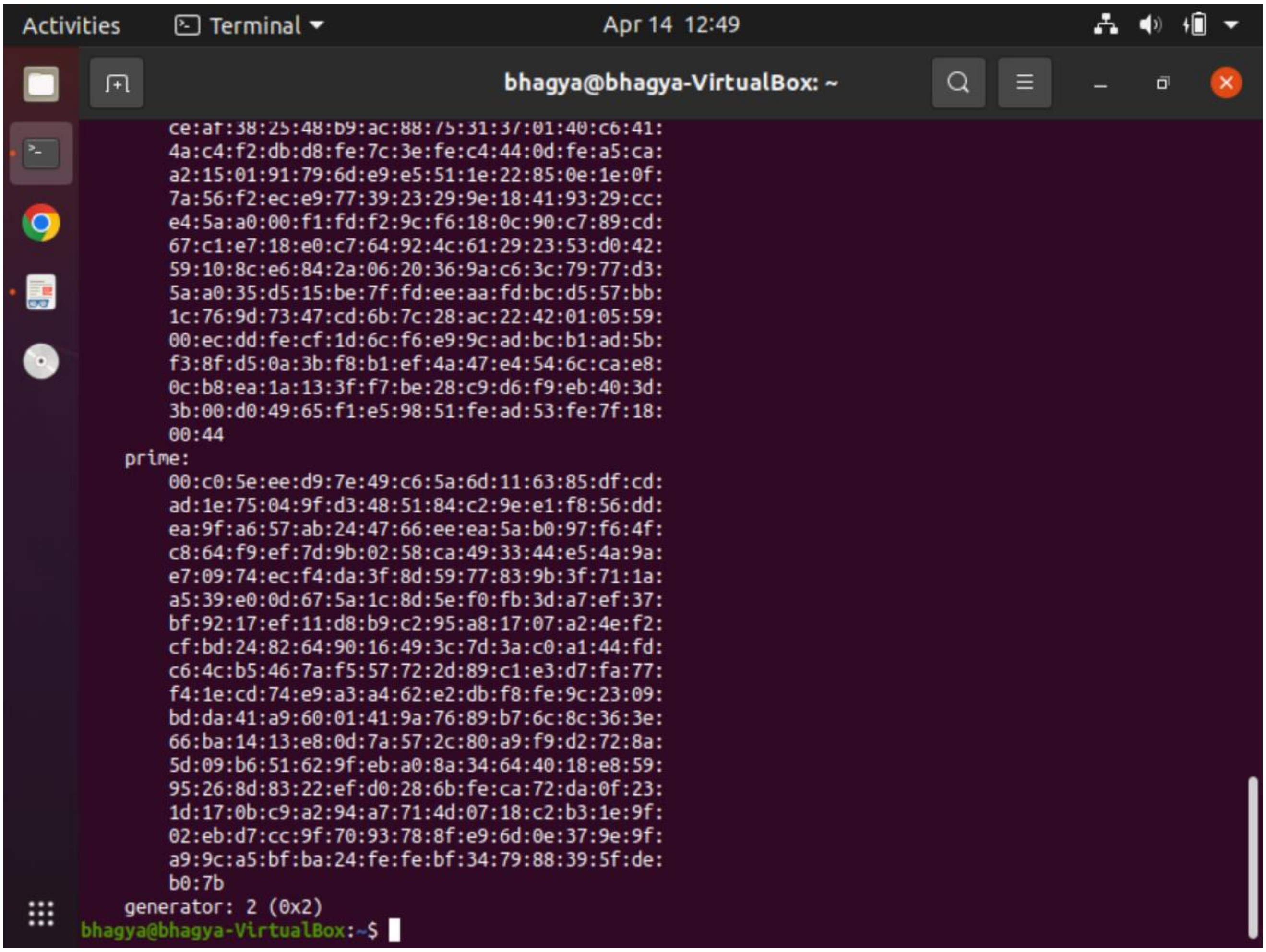


```
        87:1c:8d:7f:94:c9:99:95:0c:47:10:c1:2f:9f:e9:
        03:23:1d:69:d9:40:4e:c6:12:5d:f7:a7:ae:dd:8c:
        6c:90:df:57:27:1e:c8:83:58:12:f1:3f:e2:a1:90:
        ad:c6:b2:ea:f0:47:a4:e6:63:23:9b:2c:de:84:f7:
        0a:e0:48:54:29:69:d7:27:e3:8a:3b:af:93:56:6d:
        53:ba:f2:65:d3:2a:c4:19:cc:93:7b:1c:2a:26:84:
        2b:e1:a8:a9:60:a8:b7:67:4b:85:52:fc:ed:73:de:
        9b:d4:c6:f3:89:57:82:dc:25:52:02:1e:95:93:e2:
        40:e8:ae:64:f5:5c:7a:a4:c4:85:61:e5:d7:bc:0e:
        f1:bd:40:4b:d8:86:52:c2:59:2c:5e:3f:59:55:19:
        96:b0:d8:27:e4:69:65:6e:35:2e:e6:17:73:39:cf:
        d9:65:70:cd:3d:66:26:14:7f:84:d8:b8:d7:99:9c:
        6b:95:67:1a:af:50:72:f8:4c:d8:19:f3:de:50:8f:
        82
    prime:
        00:c0:5e:ee:d9:7e:49:c6:5a:6d:11:63:85:df:cd:
        ad:1e:75:04:9f:d3:48:51:84:c2:9e:e1:f8:56:dd:
        ea:9f:a6:57:ab:24:47:66:ee:ea:5a:b0:97:f6:4f:
        c8:64:f9:ef:7d:9b:02:58:ca:49:33:44:e5:4a:9a:
        e7:09:74:ec:f4:da:3f:8d:59:77:83:9b:3f:71:1a:
        a5:39:e0:0d:67:5a:1c:8d:5e:f0:fb:3d:a7:ef:37:
        bf:92:17:ef:11:d8:b9:c2:95:a8:17:07:a2:4e:f2:
        cf:bd:24:82:64:90:16:49:3c:7d:3a:c0:a1:44:fd:
        c6:4c:b5:46:7a:f5:57:72:2d:89:c1:e3:d7:fa:77:
        f4:1e:cd:74:e9:a3:a4:62:e2:db:f8:fe:9c:23:09:
        bd:da:41:a9:60:01:41:9a:76:89:b7:6c:8c:36:3e:
        66:ba:14:13:e8:0d:7a:57:2c:80:a9:f9:d2:72:8a:
        5d:09:b6:51:62:9f:eb:a0:8a:34:64:40:18:e8:59:
        95:26:8d:83:22:ef:d0:28:6b:fe:ca:72:da:0f:23:
        1d:17:0b:c9:a2:94:a7:71:4d:07:18:c2:b3:1e:9f:
        02:eb:d7:cc:9f:70:93:78:8f:e9:6d:0e:37:9e:9f:
        a9:9c:a5:bf:ba:24:fe:fe:bf:34:79:88:39:5f:de:
        b0:7b
    generator: 2 (0x2)
bhagya@bhagya-VirtualBox:~$ 
```

```
OpenSSL pkey -in DHkeyB.pem -text -noout
```



```
bhagya@bhagya-VirtualBox:~$ openssl pkey -in DHkeyB.pem -text -noout
DH Private-Key: (2048 bit)
    private-key:
        60:4f:0a:2a:d3:70:91:78:30:c4:6d:53:e4:f6:9b:
        4e:53:38:59:9f:ef:5a:c5:96:02:a9:28:96:1c:be:
        fb:59:36:e7:f9:ce:ff:14:78:15:79:1b:9a:7b:81:
        23:1d:46:ad:4c:12:e1:ad:af:e3:83:6e:ac:66:9a:
        c0:6d:c9:a7:f2:bb:d6:4d:48:35:9a:65:0d:f7:8f:
        74:80:66:9e:62:cf:4b:30:fa:e4:67:1c:e1:c3:18:
        6b:77:c1:18:ac:85:15:b1:16:17:46:36:b2:8a:1f:
        2d:ea:22:2e:a4:ac:4a:28:1b:61:1a:d0:fd:80:b5:
        61:82:f2:9a:39:11:c6:da:f0:d4:31:27:6c:12:02:
        c0:8b:03:a2:17:b1:39:de:cc:a0:70:50:5a:cf:75:
        5a:62:a6:01:af:ee:84:ac:92:db:12:02:40:5a:ec:
        22:00:a0:9f:bf:30:11:4a:b3:b8:d8:37:c1:e2:a6:
        41:68:b5:70:14:9d:84:4b:b9:3b:eb:5f:47:7d:21:
        ab:83:17:bd:52:00:9d:ec:5d:e3:23:c8:20:57:22:
        a4:20:95:d3:68:ad:ef:e1:2c:1c:19:61:34:15:03:
        f6:a7:57:73:59:2b:cb:4a:a7:60:2d:9f:0a:7d:58:
        15:dd:48:a7:58:21:b9:7c:73:85:cd:b9:13:b5:3b:
        20
    public-key:
        00:9e:ea:22:1b:22:ac:14:a4:a2:b1:f4:ec:b3:00:
        7e:f5:8e:c5:6d:94:e2:a7:fa:0c:a6:a3:c5:29:02:
        63:f8:f5:be:dc:f1:5a:8a:5a:f1:0e:2f:ef:eb:ff:
        bd:02:c2:8f:c6:5b:cc:9f:ba:b9:27:66:b3:b8:0c:
        ce:af:38:25:48:b9:ac:88:75:31:37:01:40:c6:41:
        4a:c4:f2:db:d8:fe:7c:3e:fe:c4:44:0d:fe:a5:ca:
        a2:15:01:91:79:6d:e9:e5:51:1e:22:85:0e:1e:0f:
        7a:56:f2:ec:e9:77:39:23:29:9e:18:41:93:29:cc:
        e4:5a:a0:00:f1:fd:f2:9c:f6:18:0c:90:c7:89:cd:
        67:c1:e7:18:e0:c7:64:92:4c:61:29:23:53:d0:42:
        59:10:8c:e6:84:2a:06:20:36:9a:c6:3c:79:77:d3:
        5a:a0:35:d5:15:be:7f:fd:ee:aa:fd:bc:d5:57:bb:
        1c:76:9d:73:47:cd:6b:7c:28:ac:22:42:01:05:59:
```



```
        ce:af:38:25:48:b9:ac:88:75:31:37:01:40:c6:41:
        4a:c4:f2:db:d8:fe:7c:3e:fe:c4:44:0d:fe:a5:ca:
        a2:15:01:91:79:6d:e9:e5:51:1e:22:85:0e:1e:0f:
        7a:56:f2:ec:e9:77:39:23:29:9e:18:41:93:29:cc:
        e4:5a:a0:00:f1:fd:f2:9c:f6:18:0c:90:c7:89:cd:
        67:c1:e7:18:e0:c7:64:92:4c:61:29:23:53:d0:42:
        59:10:8c:e6:84:2a:06:20:36:9a:c6:3c:79:77:d3:
        5a:a0:35:d5:15:be:7f:fd:ee:aa:fd:bc:d5:57:bb:
        1c:76:9d:73:47:cd:6b:7c:28:ac:22:42:01:05:59:
        00:ec:dd:fe:cf:1d:6c:f6:e9:9c:ad:bc:b1:ad:5b:
        f3:8f:d5:0a:3b:f8:b1:ef:4a:47:e4:54:6c:ca:e8:
        0c:b8:ea:1a:13:3f:f7:be:28:c9:d6:f9:eb:40:3d:
        3b:00:d0:49:65:f1:e5:98:51:fe:ad:53:fe:7f:18:
        00:44
    prime:
        00:c0:5e:ee:d9:7e:49:c6:5a:6d:11:63:85:df:cd:
        ad:1e:75:04:9f:d3:48:51:84:c2:9e:e1:f8:56:dd:
        ea:9f:a6:57:ab:24:47:66:ee:ea:5a:b0:97:f6:4f:
        c8:64:f9:ef:7d:9b:02:58:ca:49:33:44:e5:4a:9a:
        e7:09:74:ec:f4:da:3f:8d:59:77:83:9b:3f:71:1a:
        a5:39:e0:0d:67:5a:1c:8d:5e:f0:fb:3d:a7:ef:37:
        bf:92:17:ef:11:d8:b9:c2:95:a8:17:07:a2:4e:f2:
        cf:bd:24:82:64:90:16:49:3c:7d:3a:c0:a1:44:fd:
        c6:4c:b5:46:7a:f5:57:72:2d:89:c1:e3:d7:fa:77:
        f4:1e:cd:74:e9:a3:a4:62:e2:db:f8:fe:9c:23:09:
        bd:da:41:a9:60:01:41:9a:76:89:b7:6c:8c:36:3e:
        66:ba:14:13:e8:0d:7a:57:2c:80:a9:f9:d2:72:8a:
        5d:09:b6:51:62:9f:eb:a0:8a:34:64:40:18:e8:59:
        95:26:8d:83:22:ef:d0:28:6b:fe:ca:72:da:0f:23:
        1d:17:0b:c9:a2:94:a7:71:4d:07:18:c2:b3:1e:9f:
        02:eb:d7:cc:9f:70:93:78:8f:e9:6d:0e:37:9e:9f:
        a9:9c:a5:bf:ba:24:fe:fe:bf:34:79:88:39:5f:de:
        b0:7b
    generator: 2 (0x2)
bhagya@bhagya-VirtualBox:~$ 
```

Private Key, **Public Key**, **Prime** and **Generator** can be Clearly Seen for Both A & B.

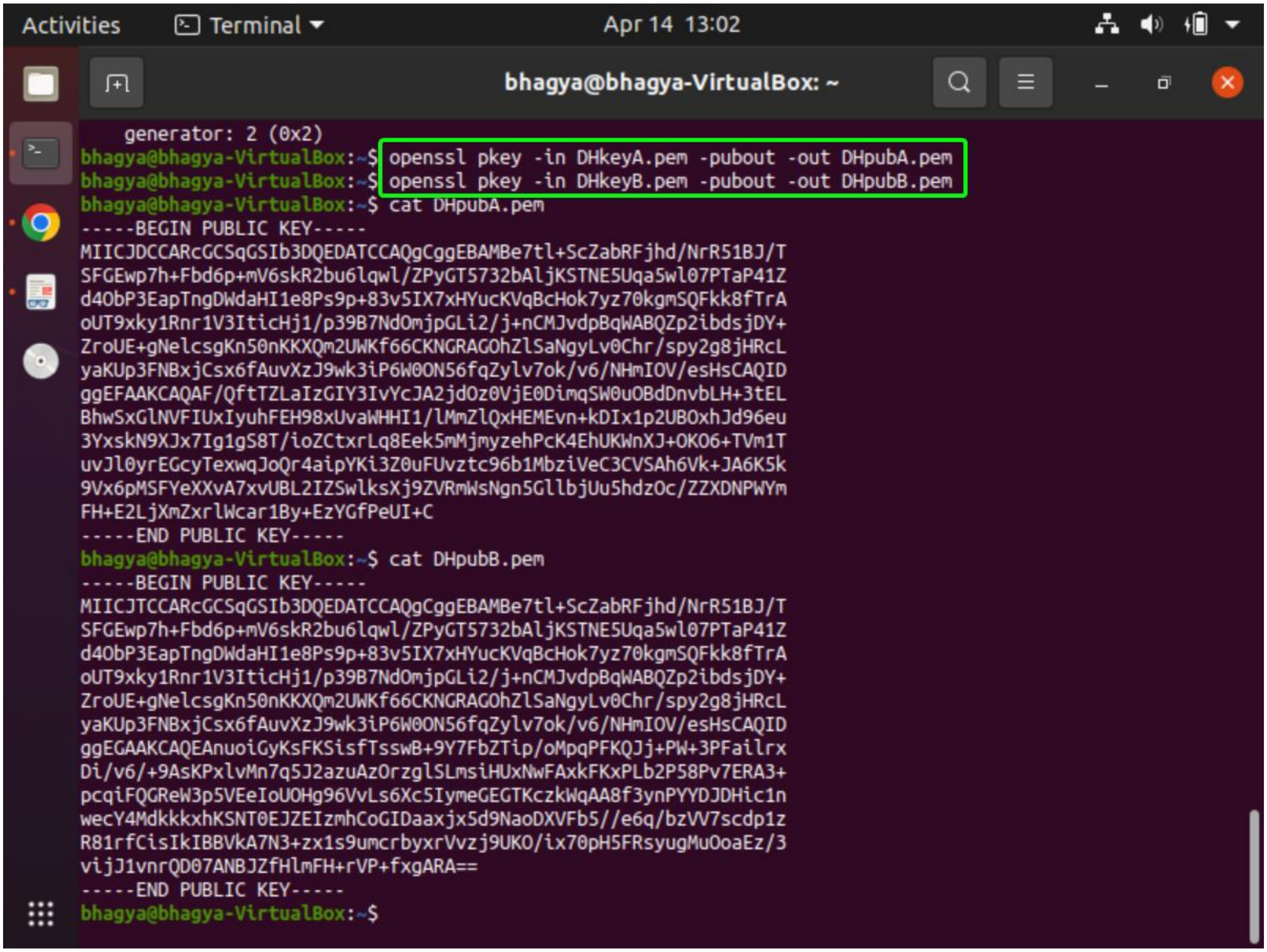
6.) Extract the public keys of user A and user B into separate file viz., `DHpubA.pem` and `DHpubB.pem`.

Command to Extract Public Key for A:

```
openssl pkey -in DHkeyA.pem -pubout -out DHpubA.pem
```

Command to Extract Public Key for B:

```
openssl pkey -in DHkeyB.pem -pubout -out DHpubB.pem
```



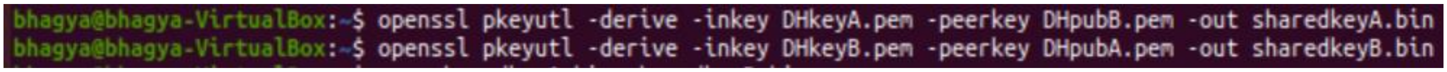
```
    generator: 2 (0x2)
bhagya@bhagya-VirtualBox:~$ openssl pkey -in DHkeyA.pem -pubout -out DHpubA.pem
bhagya@bhagya-VirtualBox:~$ openssl pkey -in DHkeyB.pem -pubout -out DHpubB.pem
bhagya@bhagya-VirtualBox:~$ cat DHpubA.pem
-----BEGIN PUBLIC KEY-----
MIICJDCCARcGCSqGSIb3DQEDATCCAQgCggEBAMBe7tl+ScZabRFjhd/NrR51BJ/T
SFGEwp7h+Fbd6p+mV6skR2bu6lqwl/ZPyGT5732bAljKSTNE5Uqa5wl07PTaP41Z
d40bP3EapTngDWdaHI1e8Ps9p+83v5IX7xHYucKVqBcHok7yz70kgmSQFkk8fTrA
oUT9xky1Rnr1V3IticHj1/p39B7NdOmjpGLi2/j+nCMJvdpBqWABQZp2ibdsjDY+
ZroUE+gNelcsgKn50nKKXQm2UWKf66CKNGRAGOhZlSaNgyLv0Chr/spy2g8jHRcL
yaKUp3FNBxjCsx6fAuvXzJ9wk3iP6W0ON56fqZylv7ok/v6/NHmIOV/esHsCAQID
ggEFAAKCAQAF/QftTZLaIzGIY3IvYcJA2jdOz0VjE0DimqSW0uOBdDnvbLH+3tEL
BhwSxGlNVFIUxIyuhFEH98xUvaWHHI1/lMmZlQxHEMEvn+kDIx1p2UBOxhJd96eu
3YxskN9XJx7Ig1gS8T/ioZCtxrLq8Eek5mMjmyzehPcK4EhUKWnXJ+OKO6+TVm1T
uvJl0yrEGcyTexwqJoQr4aipYKi3Z0uFUvztc96b1MbziVeC3CVSAh6Vk+JA6K5k
9Vx6pMSFYeXXvA7xvUBL2IZSwlksXj9ZVRmWsNgn5GllbjUu5hdzOc/ZZXDNPWYm
FH+E2LjXmZxrlWcar1By+EzYGfPeUI+C
-----END PUBLIC KEY-----
bhagya@bhagya-VirtualBox:~$ cat DHpubB.pem
-----BEGIN PUBLIC KEY-----
MIICJTCCARcGCSqGSIb3DQEDATCCAQgCggEBAMBe7tl+ScZabRFjhd/NrR51BJ/T
SFGEwp7h+Fbd6p+mV6skR2bu6lqwl/ZPyGT5732bAljKSTNE5Uqa5wl07PTaP41Z
d40bP3EapTngDWdaHI1e8Ps9p+83v5IX7xHYucKVqBcHok7yz70kgmSQFkk8fTrA
oUT9xky1Rnr1V3IticHj1/p39B7NdOmjpGLi2/j+nCMJvdpBqWABQZp2ibdsjDY+
ZroUE+gNelcsgKn50nKKXQm2UWKf66CKNGRAGOhZlSaNgyLv0Chr/spy2g8jHRcL
yaKUp3FNBxjCsx6fAuvXzJ9wk3iP6W0ON56fqZylv7ok/v6/NHmIOV/esHsCAQID
ggEGAAKCAQEAnuoiGyKsFKSisfTsswB+9Y7FbZTip/oMpqPFKQJj+PW+3PFailrx
Di/v6/+9AsKPxlvMn7q5J2azuAzOrzglSLmsiHUxNwFAxkFKxPLb2P58Pv7ERA3+
pcqiFQGReW3p5VEeIoUOHg96VvLs6Xc5IymeGEGTKczkWqAA8f3ynPYYDJDHic1n
wecY4MdkkkxhKSNT0EJZEIzmhCoGIDaaxjx5d9NaoDXVFb5//e6q/bzVV7scdp1z
R81rfCisIkIBBVkA7N3+zx1s9umcrbyxrVvzj9UKO/ix70pH5FRsyugMuOoaEz/3
vijJ1vnrQD07ANBJZfHlmFH+rVP+fxgARA==
-----END PUBLIC KEY-----
bhagya@bhagya-VirtualBox:~$
```

7.) Let us consider, both the users have exchanged their public keys with each other. That means, user A has `DHpubB.pem` and user B has `DHpubA.pem`.

Using this keys, generate a shared secret key (128 bit binary file) at both sides using following command.

```
OpenSSL pkeyutl -derive -inkey DHkeyA.pem -peerkey DHpubB.pem -out sharedkeyA.bin
```

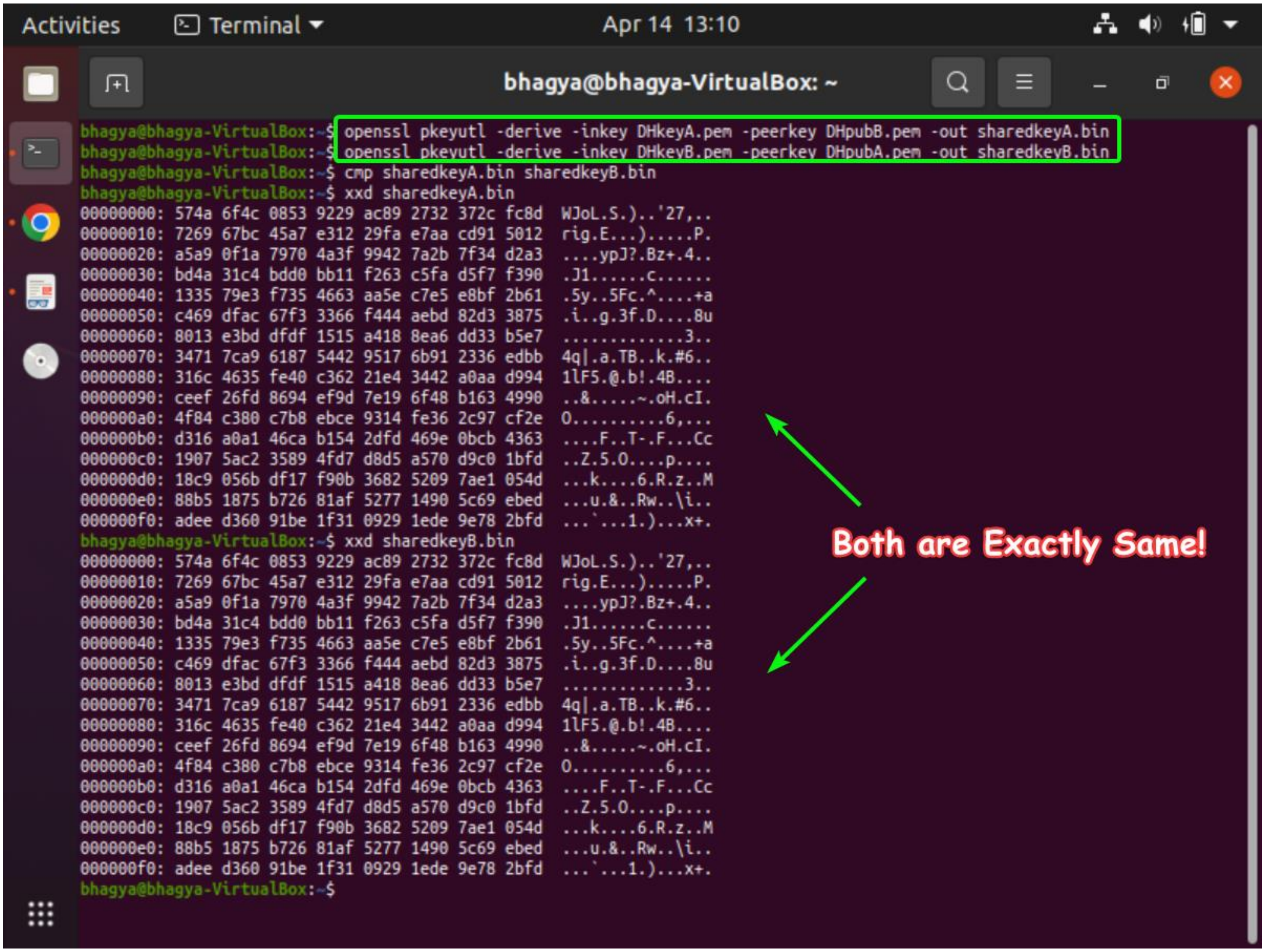
```
OpenSSL pkeyutl -derive -inkey DHkeyB.pem -peerkey DHpubA.pem -out sharedkeyB.bin
```



```
bhagya@bhagya-VirtualBox:~$ openssl pkeyutl -derive -inkey DHkeyA.pem -peerkey DHpubB.pem -out sharedkeyA.bin
bhagya@bhagya-VirtualBox:~$ openssl pkeyutl -derive -inkey DHkeyB.pem -peerkey DHpubA.pem -out sharedkeyB.bin
```

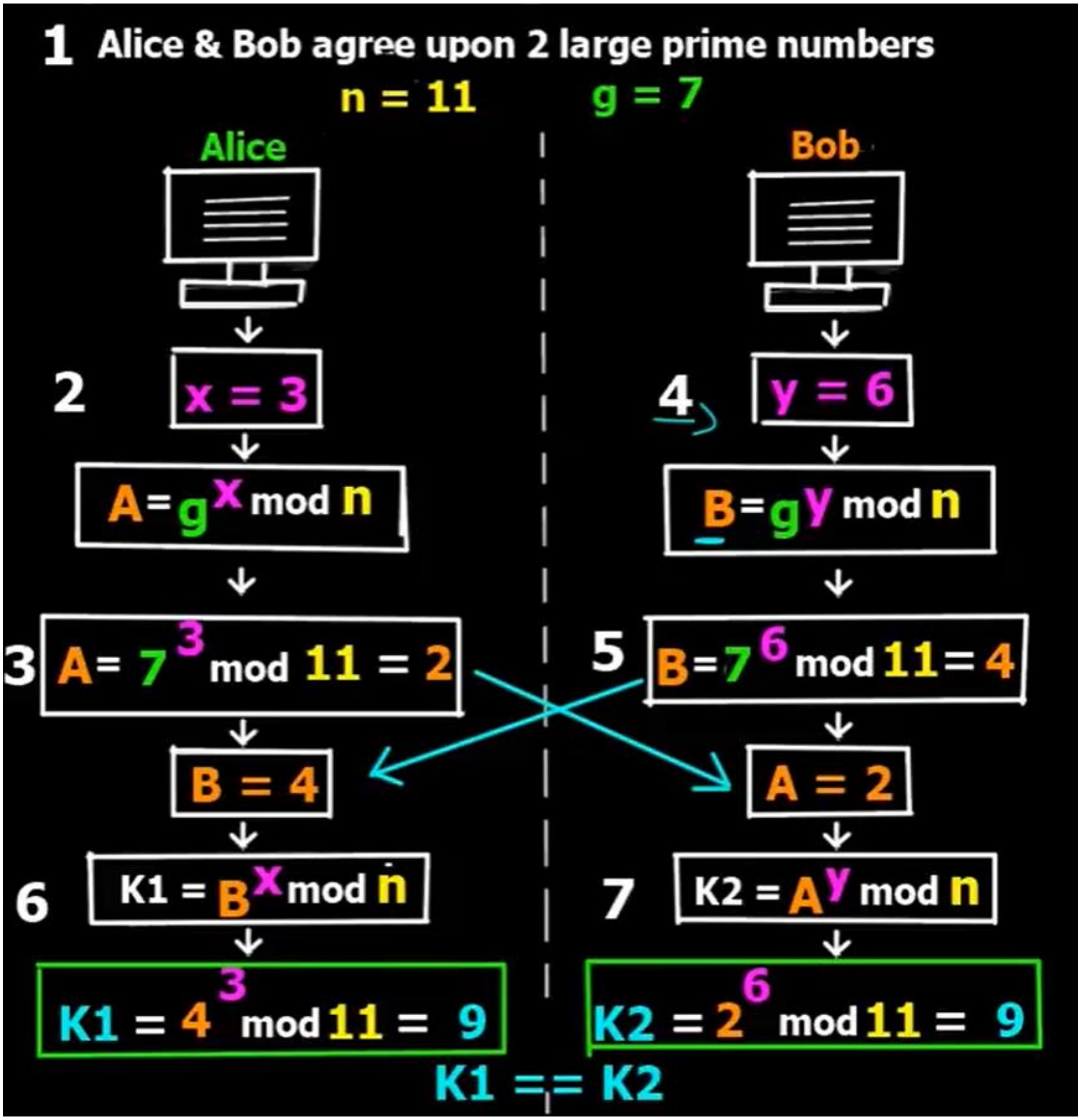
8.) Check if **same key** is generated at both sides.

```
cmp sharedkeyA.bin sharedkeyB.bin

xxd sharedkeyA.bin

xxd sharedkeyB.bin
```



```
bhagya@bhagya-VirtualBox:~$ openssl pkeyutl -derive -inkey DHkeyA.pem -peerkey DHpubB.pem -out sharedkeyA.bin
bhagya@bhagya-VirtualBox:~$ openssl pkeyutl -derive -inkey DHkeyB.pem -peerkey DHpubA.pem -out sharedkeyB.bin
bhagya@bhagya-VirtualBox:~$ cmp sharedkeyA.bin sharedkeyB.bin
bhagya@bhagya-VirtualBox:~$ xxd sharedkeyA.bin
00000000: 574a 6f4c 0853 9229 ac89 2732 372c fc8d  WJoL.S.)..'27,..
00000010: 7269 67bc 45a7 e312 29fa e7aa cd91 5012  rig.E...).....P.
00000020: a5a9 0f1a 7970 4a3f 9942 7a2b 7f34 d2a3  ....ypJ?.Bz+.4..
00000030: bd4a 31c4 bdd0 bb11 f263 c5fa d5f7 f390  .J1......c......
00000040: 1335 79e3 f735 4663 aa5e c7e5 e8bf 2b61  .5y..5Fc.^....+a
00000050: c469 dfac 67f3 3366 f444 aebd 82d3 3875  .i..g.3f.D....8u
00000060: 8013 e3bd dfdf 1515 a418 8ea6 dd33 b5e7  .............3..
00000070: 3471 7ca9 6187 5442 9517 6b91 2336 edbb  4q|.a.TB..k.#6..
00000080: 316c 4635 fe40 c362 21e4 3442 a0aa d994  1lF5.@.b!.4B....
00000090: ceef 26fd 8694 ef9d 7e19 6f48 b163 4990  ..&.....~.oH.cI.
000000a0: 4f84 c380 c7b8 ebce 9314 fe36 2c97 cf2e  O..........6,...
000000b0: d316 a0a1 46ca b154 2dfd 469e 0bcb 4363  ....F..T-.F...Cc
000000c0: 1907 5ac2 3589 4fd7 d8d5 a570 d9c0 1bfd  ..Z.5.O....p....
000000d0: 18c9 056b df17 f90b 3682 5209 7ae1 054d  ...k....6.R.z..M
000000e0: 88b5 1875 b726 81af 5277 1490 5c69 ebed  ...u.&..Rw..\i..
000000f0: adee d360 91be 1f31 0929 1ede 9e78 2bfd  ...`...1.)...x+.
bhagya@bhagya-VirtualBox:~$ xxd sharedkeyB.bin
00000000: 574a 6f4c 0853 9229 ac89 2732 372c fc8d  WJoL.S.)..'27,..
00000010: 7269 67bc 45a7 e312 29fa e7aa cd91 5012  rig.E...).....P.
00000020: a5a9 0f1a 7970 4a3f 9942 7a2b 7f34 d2a3  ....ypJ?.Bz+.4..
00000030: bd4a 31c4 bdd0 bb11 f263 c5fa d5f7 f390  .J1......c......
00000040: 1335 79e3 f735 4663 aa5e c7e5 e8bf 2b61  .5y..5Fc.^....+a
00000050: c469 dfac 67f3 3366 f444 aebd 82d3 3875  .i..g.3f.D....8u
00000060: 8013 e3bd dfdf 1515 a418 8ea6 dd33 b5e7  .............3..
00000070: 3471 7ca9 6187 5442 9517 6b91 2336 edbb  4q|.a.TB..k.#6..
00000080: 316c 4635 fe40 c362 21e4 3442 a0aa d994  1lF5.@.b!.4B....
00000090: ceef 26fd 8694 ef9d 7e19 6f48 b163 4990  ..&.....~.oH.cI.
000000a0: 4f84 c380 c7b8 ebce 9314 fe36 2c97 cf2e  O..........6,...
000000b0: d316 a0a1 46ca b154 2dfd 469e 0bcb 4363  ....F..T-.F...Cc
000000c0: 1907 5ac2 3589 4fd7 d8d5 a570 d9c0 1bfd  ..Z.5.O....p....
000000d0: 18c9 056b df17 f90b 3682 5209 7ae1 054d  ...k....6.R.z..M
000000e0: 88b5 1875 b726 81af 5277 1490 5c69 ebed  ...u.&..Rw..\i..
000000f0: adee d360 91be 1f31 0929 1ede 9e78 2bfd  ...`...1.)...x+.
bhagya@bhagya-VirtualBox:~$
```

Both have the **Exact Same Shared Secret Key** (128 Bit Binary File).



Hence, Using **Diffie Hellman Key Protocol**, we have **Successfully Verified** that Same Key is Shared Between Two Users.

SUBMITTED BY: U19CS012

BHAGYA VINOD RANA