Name: **Mareena Fernandes**
Roll No.: **8669**
Class: **TE IT**
Batch: **B**

EXPERIMENT NO: 10

1)

```
mareenalinux@mareenalinux:~/Desktop$ sudo apt install gnupg2
[sudo] password for mareenalinux:
Reading package lists... Done
Building dependency tree
Reading state information... Done
The following package was automatically installed and is no longer required:
  libfprint-2-tod1
Use 'sudo apt autoremove' to remove it.
The following NEW packages will be installed:
  gnupg2
0 upgraded, 1 newly installed, 0 to remove and 0 not upgraded.
Need to get 5,316 B of archives.
After this operation, 51.2 kB of additional disk space will be used.
Get:1 http://in.archive.ubuntu.com/ubuntu focal/universe amd64 gnupg2 all 2.2.19-3ubuntu2 [5,316 B]
Fetched 5,316 B in 0s (44.5 kB/s)
Selecting previously unselected package gnupg2.
(Reading database ... 187739 files and directories currently installed.)
Preparing to unpack .../gnupg2_2.2.19-3ubuntu2_all.deb ...
Unpacking gnupg2 (2.2.19-3ubuntu2) ...
Setting up gnupg2 (2.2.19-3ubuntu2) ...
Processing triggers for man-db (2.9.1-1) ...
```

2)

```
mareenalinux@mareenalinux:~/Desktop$ touch mareenatext.txt
```

3)

```
mareenalinux@mareenalinux:~/Desktop$ gpg --pinentry-mode loopback --passphrase 88bottlesOfBeer --symmetric mareenatext.txt
File 'mareenatext.txt.gpg' exists. Overwrite? (y/N) y
```

4)

```
mareenalinux@mareenalinux:~/Desktop$ ls -l
total 4
-rw-rw-r-- 1 mareenalinux mareenalinux  0 Nov 20 12:40 mareenatext.txt
-rw-rw-r-- 1 mareenalinux mareenalinux 81 Nov 20 12:41 mareenatext.txt.gpg
```

5)

```
mareenalinux@mareenalinux:~/Desktop$  ls -l mareenatext.txt.*
-rw-rw-r-- 1 mareenalinux mareenalinux 81 Nov 15 22:53 mareenatext.txt.gpg
```

6)

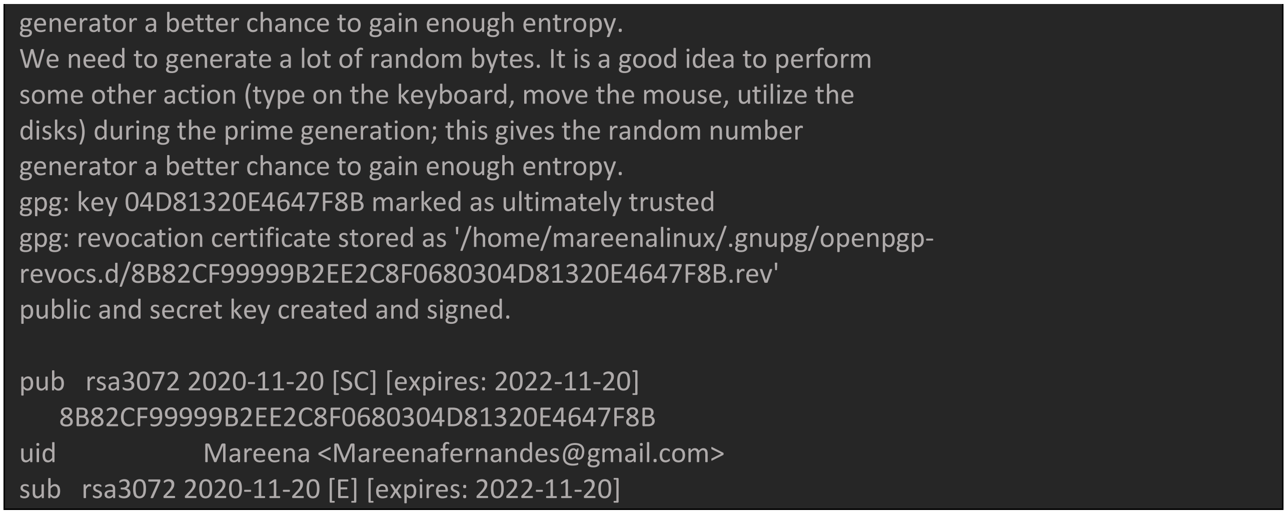
```
mareenalinux@mareenalinux:~/Desktop$ gpg2 --symmetric mareenatext.txt
File 'mareenatext.txt.gpg' exists. Overwrite? (y/N) y
```

7)

```
mareenalinux@mareenalinux:~/Desktop$ ls -l
total 8
-rw-rw-r-- 1 mareenalinux mareenalinux  8 Nov 20 12:43 mareenatext.txt
-rw-rw-r-- 1 mareenalinux mareenalinux 89 Nov 20 12:44 mareenatext.txt.gpg
```

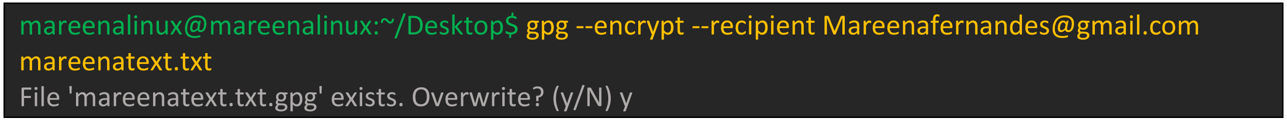
8)

```
mareenalinux@mareenalinux:~/Desktop$  gpg --gen-key
gpg (GnuPG) 2.2.19; Copyright (C) 2019 Free Software Foundation, Inc.
This is free software: you are free to change and redistribute it.
There is NO WARRANTY, to the extent permitted by law.

Note: Use "gpg --full-generate-key" for a full featured key generation dialog.

GnuPG needs to construct a user ID to identify your key.

Real name: Mareena
Email address: Mareenafernandes@gmail.com
You selected this USER-ID:
    "Mareena <Mareenafernandes@gmail.com>"

Change (N)ame, (E)mail, or (O)kay/(Q)uit? o
We need to generate a lot of random bytes. It is a good idea to perform
some other action (type on the keyboard, move the mouse, utilize the
disks) during the prime generation; this gives the random number
```



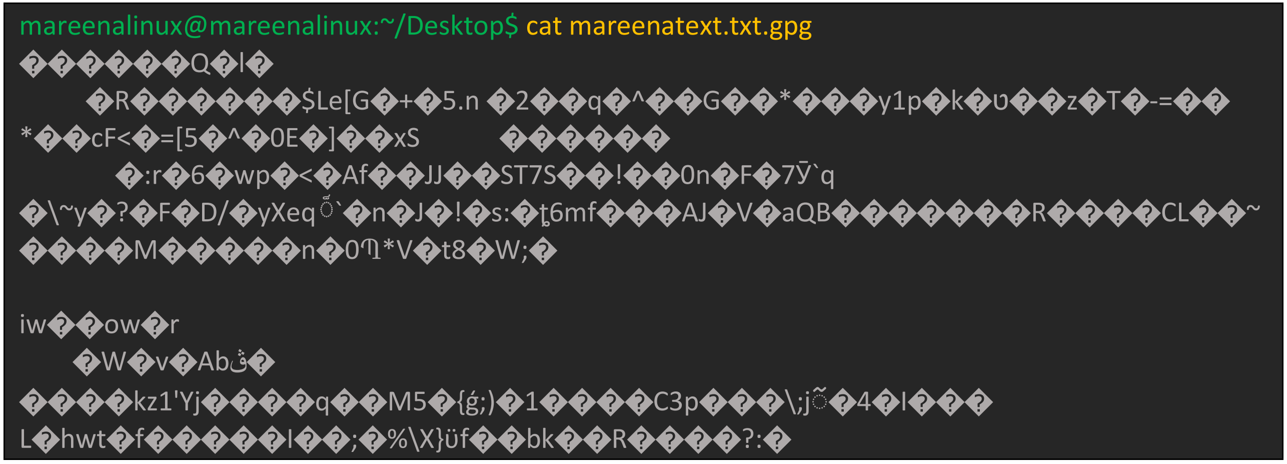
```
generator a better chance to gain enough entropy.
We need to generate a lot of random bytes. It is a good idea to perform
some other action (type on the keyboard, move the mouse, utilize the
disks) during the prime generation; this gives the random number
generator a better chance to gain enough entropy.
gpg: key 04D81320E4647F8B marked as ultimately trusted
gpg: revocation certificate stored as '/home/mareenalinux/.gnupg/openpgp-
revocs.d/8B82CF99999B2EE2C8F0680304D81320E4647F8B.rev'
public and secret key created and signed.

pub   rsa3072 2020-11-20 [SC] [expires: 2022-11-20]
      8B82CF99999B2EE2C8F0680304D81320E4647F8B
uid                      Mareena <Mareenafernandes@gmail.com>
sub   rsa3072 2020-11-20 [E] [expires: 2022-11-20]
```

9)



```
mareenalinux@mareenalinux:~/Desktop$ gpg --encrypt --recipient Mareenafernandes@gmail.com
mareenatext.txt
File 'mareenatext.txt.gpg' exists. Overwrite? (y/N) y
```

10)



```
mareenalinux@mareenalinux:~/Desktop$ cat mareenatext.txt.gpg
�������Q�I�
        �R��������$Le[G�+�5.n �2��q�^��G��*���y1p�k�ʊ��z�T�-=��
*��cF<�=[5�^�0E�]��xS          �������
           �:r�6�wp�<�Af��JJ��ST7S��!��0n�F�7Ȳ`q
�\~y�?�F�D/�yXeq ő`�n�J�!�s:�ţ6mf���AJ�V�aQB���������R�����CL��~
����M�������n�0Ղ*V�t8�W;�

iw��ow�r
       �W�v�Abڤ�
�����kz1'Yj�����q��M5�{ǵ;)�1�����C3p���\;j̃�4�I���
L�hwt�f�������I��;�%\X}üf��bk��R������?:�
```

11)

```
mareenalinux@mareenalinux:~/Desktop$ gpg --cipher-algo AES256 --symmetric mareenatext.txt
File 'mareenatext.txt.gpg' exists. Overwrite? (y/N) y

gpg --gen-key
gpg (GnuPG) 2.2.19; Copyright (C) 2019 Free Software Foundation, Inc.
This is free software: you are free to change and redistribute it.
There is NO WARRANTY, to the extent permitted by law.

Note: Use "gpg --full-generate-key" for a full featured key generation dialog.

GnuPG needs to construct a user ID to identify your key.

Real name: Mareena1
Email address: mareena@gmail.com
You selected this USER-ID:
   "Mareena1 <mareena@gmail.com>"

Change (N)ame, (E)mail, or (O)kay/(Q)uit? o
We need to generate a lot of random bytes. It is a good idea to perform
some other action (type on the keyboard, move the mouse, utilize the
disks) during the prime generation; this gives the random number
generator a better chance to gain enough entropy.
We need to generate a lot of random bytes. It is a good idea to perform
some other action (type on the keyboard, move the mouse, utilize the
disks) during the prime generation; this gives the random number
generator a better chance to gain enough entropy.
gpg: key E10A6DF1EB99E87B marked as ultimately trusted
gpg: revocation certificate stored as '/home/mareenalinux/.gnupg/openpgp-
revocs.d/AEBF015330870E8D7EBCF065E10A6DF1EB99E87B.rev'
public and secret key created and signed.

pub   rsa3072 2020-11-20 [SC] [expires: 2022-11-20]
      AEBF015330870E8D7EBCF065E10A6DF1EB99E87B
uid                      Mareena1 <mareena@gmail.com>
sub   rsa3072 2020-11-20 [E] [expires: 2022-11-20]
```

12)

```
mareenalinux@mareenalinux:~/Desktop$ gpg --list-keys
gpg: checking the trustdb
gpg: marginals needed: 3  completes needed: 1  trust model: pgp
gpg: depth: 0  valid:   5  signed:   0  trust: 0-, 0q, 0n, 0m, 0f, 5u
gpg: next trustdb check due at 2022-11-13
/home/mareenalinux/.gnupg/pubring.kbx
---------------------------------
pub   rsa3072 2020-11-13 [SC] [expires: 2022-11-13]
      CA33D67F75B151BEAA93F6C9C33FD276D2555420
uid           [ultimate] Mareena Lobo <mareenafernandes2001@gmail.com>
sub   rsa3072 2020-11-13 [E] [expires: 2022-11-13]

pub   rsa3072 2020-11-15 [SC] [expires: 2022-11-15]
      19AA5B4E86EE6B88C7EAE190676B87553558804D
uid           [ultimate] Mareena <mareenafernandes2001@gmail.com>
sub   rsa3072 2020-11-15 [E] [expires: 2022-11-15]

pub   rsa3072 2020-11-16 [SC] [expires: 2022-11-16]
      04B0EB7B62CD106B88DEF336E36AA8439FB18F5C
uid           [ultimate] Mareena Lobo <mareenafernandes2001@gmail.com>
sub   rsa3072 2020-11-16 [E] [expires: 2022-11-16]

pub   rsa3072 2020-11-20 [SC] [expires: 2022-11-20]
      8B82CF99999B2EE2C8F0680304D81320E4647F8B
uid           [ultimate] Mareena <Mareenafernandes@gmail.com>
sub   rsa3072 2020-11-20 [E] [expires: 2022-11-20]

pub   rsa3072 2020-11-20 [SC] [expires: 2022-11-20]
      AEBF015330870E8D7EBCF065E10A6DF1EB99E87B
uid           [ultimate] Mareena1 <mareena@gmail.com>
sub   rsa3072 2020-11-20 [E] [expires: 2022-11-20]
```

13)

```
mareenalinux@mareenalinux:~/Desktop$ gpg --encrypt --recipient mareenafernandes2001@gmail.com
mareenatext.txt
File 'mareenatext.txt.gpg' exists. Overwrite? (y/N) y
```

14)

```
mareenalinux@mareenalinux:~/Desktop$ ls -l mareenatext.txt.gpg
-rw-rw-r-- 1 mareenalinux mareenalinux 478 Nov 20 12:54 mareenatext.txt.gpg
```

15)

```
mareenalinux@mareenalinux:~/Desktop$ gpg --fingerprint mareenafernandes2001@gmail.com
pub   rsa3072 2020-11-13 [SC] [expires: 2022-11-13]
      CA33 D67F 75B1 51BE AA93  F6C9 C33F D276 D255 5420
uid           [ultimate] Mareena Lobo <mareenafernandes2001@gmail.com>
sub   rsa3072 2020-11-13 [E] [expires: 2022-11-13]

pub   rsa3072 2020-11-15 [SC] [expires: 2022-11-15]
      19AA 5B4E 86EE 6B88 C7EA  E190 676B 8755 3558 804D
uid           [ultimate] Mareena <mareenafernandes2001@gmail.com>
sub   rsa3072 2020-11-15 [E] [expires: 2022-11-15]

pub   rsa3072 2020-11-16 [SC] [expires: 2022-11-16]
      04B0 EB7B 62CD 106B 88DE  F336 E36A A843 9FB1 8F5C
uid           [ultimate] Mareena Lobo <mareenafernandes2001@gmail.com>
sub   rsa3072 2020-11-16 [E] [expires: 2022-11-16]
```

16)

```
mareenalinux@mareenalinux:~/Desktop$ gpg --fingerprint Mareenafernandes@gmail.com
pub   rsa3072 2020-11-20 [SC] [expires: 2022-11-20]
      8B82 CF99 999B 2EE2 C8F0  6803 04D8 1320 E464 7F8B
uid           [ultimate] Mareena <Mareenafernandes@gmail.com>
sub   rsa3072 2020-11-20 [E] [expires: 2022-11-20]
```

17)

```
mareenalinux@mareenalinux:~/Desktop$ touch mareena.txt

mareenalinux@mareenalinux:~/Desktop$ gpg -c mareena.txt

mareenalinux@mareenalinux:~/Desktop$ cat mareena.txt.gpg
�      h��₊L���K���f���=D���P�:�⁾�����CC₊e旂
�X�{��*�c�X0�̀@##��r �uJLl��N;�
```

18)

```
mareenalinux@mareenalinux:~/Desktop$ gpg -o mareena.txt -d mareena.txt.gpg
gpg: AES256 encrypted data
gpg: encrypted with 1 passphrase
File 'mareena.txt' exists. Overwrite? (y/N) y
```

19)

```
mareenalinux@mareenalinux:~/Desktop$ cat mareena.txt.gpg
�     h��₊L���K���f���=D���P�:�⁾�����CC·e斺
�X�{��*�c�X0�̀@##��r �uJLI��N;�
```

20)

```
mareenalinux@mareenalinux:~/Desktop$ rm mareena.txt
```

21)

```
mareenalinux@mareenalinux:~/Desktop$ gpg -o mareena.txt -d mareena.txt.gpg
gpg: AES256 encrypted data
gpg: encrypted with 1 passphrase
```

22)

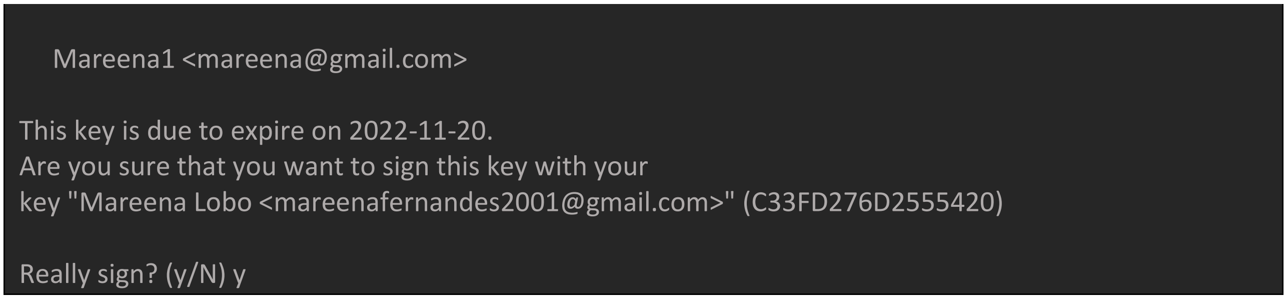
```
mareenalinux@mareenalinux:~/Desktop$ ls
mareenatext.txt  mareenatext.txt.gpg  mareena.txt  mareena.txt.gpg
```

23)

```
mareenalinux@mareenalinux:~/Desktop$ cat mareena.txt
hello i'm Mareena
```

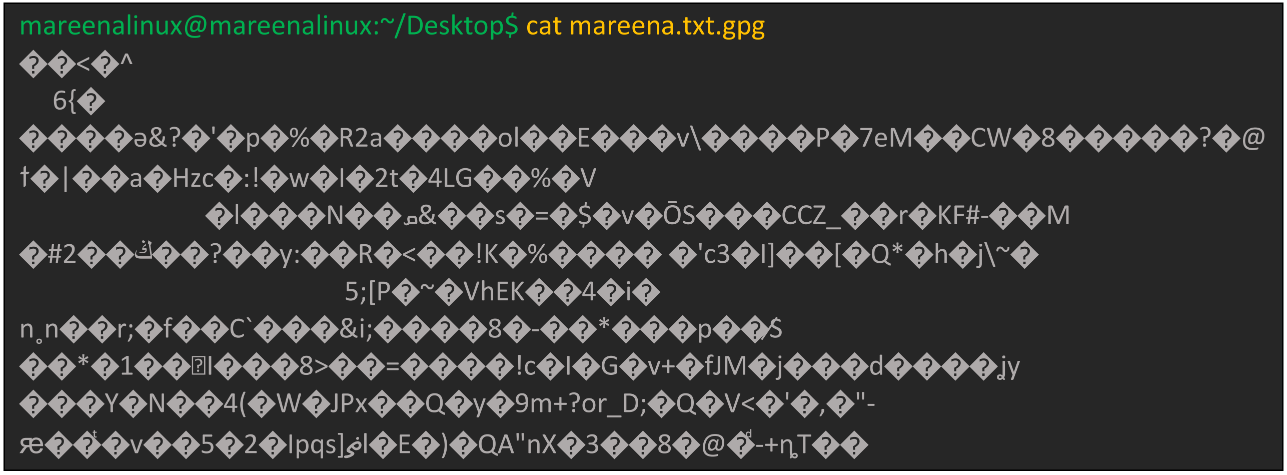
24)

```
mareenalinux@mareenalinux:~/Desktop$ gpg --sign-key mareena@gmail.com

sec  rsa3072/E10A6DF1EB99E87B
     created: 2020-11-20  expires: 2022-11-20  usage: SC
     trust: ultimate      validity: ultimate
ssb  rsa3072/8BC35079EF1E80FC
     created: 2020-11-20  expires: 2022-11-20  usage: E
[ultimate] (1). Mareena1 <mareena@gmail.com>


sec  rsa3072/E10A6DF1EB99E87B
     created: 2020-11-20  expires: 2022-11-20  usage: SC
     trust: ultimate      validity: ultimate
 Primary key fingerprint: AEBF 0153 3087 0E8D 7EBC  F065 E10A 6DF1 EB99 E87B
```



```
    Mareena1 <mareena@gmail.com>

This key is due to expire on 2022-11-20.
Are you sure that you want to sign this key with your
key "Mareena Lobo <mareenafernandes2001@gmail.com>" (C33FD276D2555420)

Really sign? (y/N) y
```

25)



```
mareenalinux@mareenalinux:~/Desktop$ cat mareena.txt.gpg
��<�^
    6{�
�����ə&?�'�p�%�R2a����ol��E���v\�����P�7eM��CW�8�������?�@
ϯ�|��a�Hzc�:!�w�l�2t�4LG��%�V
                        �l���N��ﻣ&��s�=�$�v�ŌS���CCZ_��r�KF#-��M
�#2��ڭ��?��y:��R�<��!K�%����� �'c3�l]��[�Q*�h�j\~�
                                        5;[P�~�VhEK��4�i�
n̥n��r;�f��C`���&i;�����8�-��*���p��$
��*�1���l����8>��=�����!c�l�G�v+�fJM�j���d�����ȷy
���Y�N��4(�W�JPx��Q�y�9m+?or_D;�Q�V<�'�,�"-
 footer��ͭ�v��5�2�lpqs]ۼl�E�)�QA"nX�3��8�@�ͩ-+ŋ̥T��
```

Post labs:

1. Which are different tools used for checking various SSL services? Explain in brief.

Ans:
SSL Certificate Checker
Online Free SSL checker tool helps to learn about SSL certificate that is installed on a particular domain. With the help of this free SSL certificate checker tool, it is easier to find below information about domain and SSL certificate:

- SSL validation type and expiration information
- You can learn about IP and server
- SSL certificate issuer, strength, signature and algorithm type (sha1RSA, etc.)
- Key root length and other important information

SSL Checker

SSL Checker is helpful to quickly diagnose pmareenalems with your SSL certificate installation. You can verify the SSL certificate on your web server to make sure it is correctly installed, valid, trusted and doesn't give any errors to any of your users.

SSL Server Test
This free online service performs a deep analysis of the configuration of any SSL web server on the public Internet.

SSL Labs:
With the SSL Labs powered by Qualys, you can check your website certificate and configurations and your browser's SSL installation. It runs a top to bottom output and gives you a point-by-point examination report.

SSL Lab offers a wide scope of services including SSL Labs APIs, SSL server test, SSL customer test, SSL Server Rating Guide, HTTP Client Fingerprinting, and SLL Threat Model. You can begin the investigation by simply entering the domain name or the IP address of the objective server. You will discover small insights concerning your SSL testament here like OCSP status, TLS rendition, root declaration, and halfway endorsement data, by and large appraising, diverse convention subtleties, and different incidental subtleties.