GHARDA FOUNDATION'S
GHARDA INSTITUTE OF TECHNOLOGY
Department of Computer Engineering

Evaluation Sheet

Class: T.E Computer Engineering **Sem:** VI

Subject: Cryptography and System Security

Experiment No: 14

Date:

Title of Experiment: Explore the GPG tool of Linux to implement email security.

Sr. No.	Evaluation Criteria	Max Marks	Marks Obtained
1	Practical Performance	12	
2	Oral	2	
3	Timely Submission	1	
	Total	15	

Signature of Subject Teacher
[Vijesh M.Nair]

Output –

```
student@student-HP-Desktop-Pro-G1-MT:~/Documents/68_TE$ sudo apt install gnupg
[sudo] password for student:
Reading package lists... Done
Building dependency tree
Reading state information... Done
gnupg is already the newest version (2.2.19-3ubuntu2.2).
gnupg set to manually installed.
The following package was automatically installed and is no longer required:
  gir1.2-goa-1.0
Use 'sudo apt autoremove' to remove it.
0 upgraded, 0 newly installed, 0 to remove and 124 not upgraded.
```

```
student@student-HP-Desktop-Pro-G1-MT:~/Documents/68_TE$ 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: Niraj
Email address: dse21123406@git-india.edu.in
You selected this USER-ID:
    "Niraj <dse21123406@git-india.edu.in>"

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 79A8509F6B1EA7C4 marked as ultimately trusted
gpg: directory '/home/student/.gnupg/openpgp-revocs.d' created
gpg: revocation certificate stored as '/home/student/.gnupg/openpgp-revocs.d/0E1577
5C82425340D52B24DB79A8509F6B1EA7C4.rev'
public and secret key created and signed.

pub   rsa3072 2023-04-11 [SC] [expires: 2025-04-10]
      0E15775C82425340D52B24DB79A8509F6B1EA7C4
uid                      Niraj <dse21123406@git-india.edu.in>
sub   rsa3072 2023-04-11 [E] [expires: 2025-04-10]
```

```
student@student-HP-Desktop-Pro-G1-MT:~/Documents/68_TE$ gpg --list-keys
/home/student/.gnupg/pubring.kbx
--------------------------------
pub   rsa3072 2023-04-11 [SC] [expires: 2025-04-10]
      0E15775C82425340D52B24DB79A8509F6B1EA7C4
uid           [ultimate] Niraj <dse21123406@git-india.edu.in>
sub   rsa3072 2023-04-11 [E] [expires: 2025-04-10]

student@student-HP-Desktop-Pro-G1-MT:~/Documents/68_TE$ gpg --armor --export dse211
23406@git-india.edu.in>mypk
student@student-HP-Desktop-Pro-G1-MT:~/Documents/68_TE$ cat mypk
-----BEGIN PGP PUBLIC KEY BLOCK-----

mQGNBGQ1PvwBDACguQQcaGlKcDuoqY3Mg2SdXoUzdpWCKB49aqaw3yBVD4AcXHGj
zUE3T7LgKSA0VEtOIltoeSIy5oo/Rf85Yix1L6nQ/k5CgI4D1qnMRZ+ylQdqucsM
YSFRvqWefQiG4ZzzBqywX6L8XwopqI/LClajgDt/KK5g9FAO1HThYWe4+ufsYydM
cT/Bq/ayiSFnT6h1LJDaDh+crdenUdWUkVZMWY8LuBE9gEh5SqSuP0IpPkJdfanS
MSVstFS+KralSOEZZlDTwYKwSAfrMrBiboq0LKDRczLfRzbyFFE1pGKsI43wUuLa
UdgEewpDJXRFOyXOUo2WGuD1HY05qNRW2fNzIcGqG0kvOkhm6rtwZa4f7wdRtKIe
CDAJVaF85UmWePL8JSem/WQf0Bm9ytXy4plVp9/5uLKpunyvSm4Pwb5YdwgHLKeV
zNuvF/dJEubM1cFyz0G22kecAMr5FNfYWcwJJAaWBgqO7jj+ltRez7/jGL6YwuQ+
yZW42xAmcevhvp8AEQEAAbQkTmlyYWogPGRzZTIxMTIzNDA2QGdpdC1pbmRpYS5l
ZHUuaW4+iQHUBBMBCgA+FiEEDhV3XIJCU0DVKyTbeahQn2sep8QFAmQ1PvwCGwMF
CQPCZwAFCwkIBwIGFQoJCAsCBBYCAwECHgECF4AACgkQeahQn2sep8Sn6AwAhGX7
o8mPPh2hmWTBE21MF6ktVBTl0hIpGsBaL3yA5gCTGc3s9OPXiuh+FtmVkF/g6b7v
9jVry9Y5biTWhh3m87LsHVWZnI78s5d0XXcVBMCFpH3tZjFF7zztEeV2V/03Fhte
WOz2DdyneCpQwqsBt21ZTfcreaC8nXgYC/VIlprSRthI1H7MOgvS61cGTB0fMyxr
gVG68tdyBWAvpKP0VXBvfhHQY3Xww+ER2fX3R8GzyNMSti3Qe/bU8ZvJWu36O9rv
bHXRWKH0I7WQGXSRU5QQ+YZhxFayws/wmqcgB/+2mFq6U790vKMMFXuykprWHWpk
wTqwYVHXNRyu562UMK+iE3OTGq7haPDtLtv/GcYOe067Zilaal4d0BWXAIV/Jtkf
AGRsG5atr9mupUFf9+SSRtuQqunkqEvTJQ/edLP/iCV8VHCGHYdGk0f5k88sM6Mi
GdK2XlHZ2s5+tVOkzepUTpwi9DH3AWEb7MRakk3YaDgL7f9QvEL32Nk6OOciuQGN
BGQ1PvwBDADH5+GQZ6KTWZ7rBGtXDqBZw/6rxLbhAhKspkejwOAADbJTG0aMcwJg
fD0zsj3Nf7vriQbWzVF2FQC5NXhQcLvD/Mg4L71loSm3tXPGU9Rg+Yb/FHxrR9SW
ZLwhZSuWiQKDN60IwthH5a8taQiCvcivah+lFBzwqF5m8HN3M1ix21dljPVs4ZTZ
```

```
student@student-HP-Desktop-Pro-G1-MT:~/Documents/68_TE$ 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: Surve
Email address: nirajsurve550@gmail.com
You selected this USER-ID:
    "Surve <nirajsurve550@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 568D658D3F94DC77 marked as ultimately trusted
gpg: revocation certificate stored as '/home/student/.gnupg/openpgp-revocs.d/BF61A3
43B6E0F0CC968A7A93568D658D3F94DC77.rev'
public and secret key created and signed.

pub   rsa3072 2023-04-11 [SC] [expires: 2025-04-10]
      BF61A343B6E0F0CC968A7A93568D658D3F94DC77
uid                      Surve <nirajsurve550@gmail.com>
sub   rsa3072 2023-04-11 [E] [expires: 2025-04-10]
```

```
student@student-HP-Desktop-Pro-G1-MT:~/Documents/68_TE$ gpg --list-keys
/home/student/.gnupg/pubring.kbx
------------------------------
pub   rsa3072 2023-04-11 [SC] [expires: 2025-04-10]
      0E15775C82425340D52B24DB79A8509F6B1EA7C4
uid           [ultimate] Niraj <dse21123406@git-india.edu.in>
sub   rsa3072 2023-04-11 [E] [expires: 2025-04-10]

pub   rsa3072 2023-04-11 [SC] [expires: 2025-04-10]
      BF61A343B6E0F0CC968A7A93568D658D3F94DC77
uid           [ultimate] Surve <nirajsurve550@gmail.com>
sub   rsa3072 2023-04-11 [E] [expires: 2025-04-10]

student@student-HP-Desktop-Pro-G1-MT:~/Documents/68_TE$ gpg --import mypk
gpg: key 79A8509F6B1EA7C4: "Niraj <dse21123406@git-india.edu.in>" not changed
gpg: Total number processed: 1
gpg:              unchanged: 1
student@student-HP-Desktop-Pro-G1-MT:~/Documents/68_TE$ gpg --edit-key dse21123406@
git-india.edu.in
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.

Secret key is available.

sec  rsa3072/79A8509F6B1EA7C4
     created: 2023-04-11  expires: 2025-04-10  usage: SC
     trust: ultimate      validity: ultimate
ssb  rsa3072/766420B75ABE3F96
     created: 2023-04-11  expires: 2025-04-10  usage: E
[ultimate] (1). Niraj <dse21123406@git-india.edu.in>

gpg> fpr
pub   rsa3072/79A8509F6B1EA7C4 2023-04-11 Niraj <dse21123406@git-india.edu.in>
 Primary key fingerprint: 0E15 775C 8242 5340 D52B  24DB 79A8 509F 6B1E A7C4

gpg> sign
"Niraj <dse21123406@git-india.edu.in>" was already signed by key 79A8509F6B1EA7C4
Nothing to sign with key 79A8509F6B1EA7C4

gpg> quit
```

```
student@student-HP-Desktop-Pro-G1-MT:~/Documents/68_TE$ cat > secrets
Hai
Hello!
^C
student@student-HP-Desktop-Pro-G1-MT:~/Documents/68_TE$ cat secrets
Hai
Hello!
student@student-HP-Desktop-Pro-G1-MT:~/Documents/68_TE$ gpg --out secrets_san --enc
rypt secrets
You did not specify a user ID. (you may use "-r")

Current recipients:

Enter the user ID.  End with an empty line: dse21123406@git-india.edu.in

Current recipients:
rsa3072/766420B75ABE3F96 2023-04-11 "Niraj <dse21123406@git-india.edu.in>"

Enter the user ID.  End with an empty line:
gpg: signal Interrupt caught ... exiting

student@student-HP-Desktop-Pro-G1-MT:~/Documents/68_TE$ ls
Expt11_1.png  Expt11_4.png  Expt12_2.png  Expt13_2.png  Expt13_5.png  sample3.c
Expt11_2.png  Expt11_5.png  Expt12_3.png  Expt13_3.png  mypk          sample4.c
Expt11_3.png  Expt12_1.png  Expt13_1.png  Expt13_4.png  sample2.c     secrets
student@student-HP-Desktop-Pro-G1-MT:~/Documents/68_TE$
```