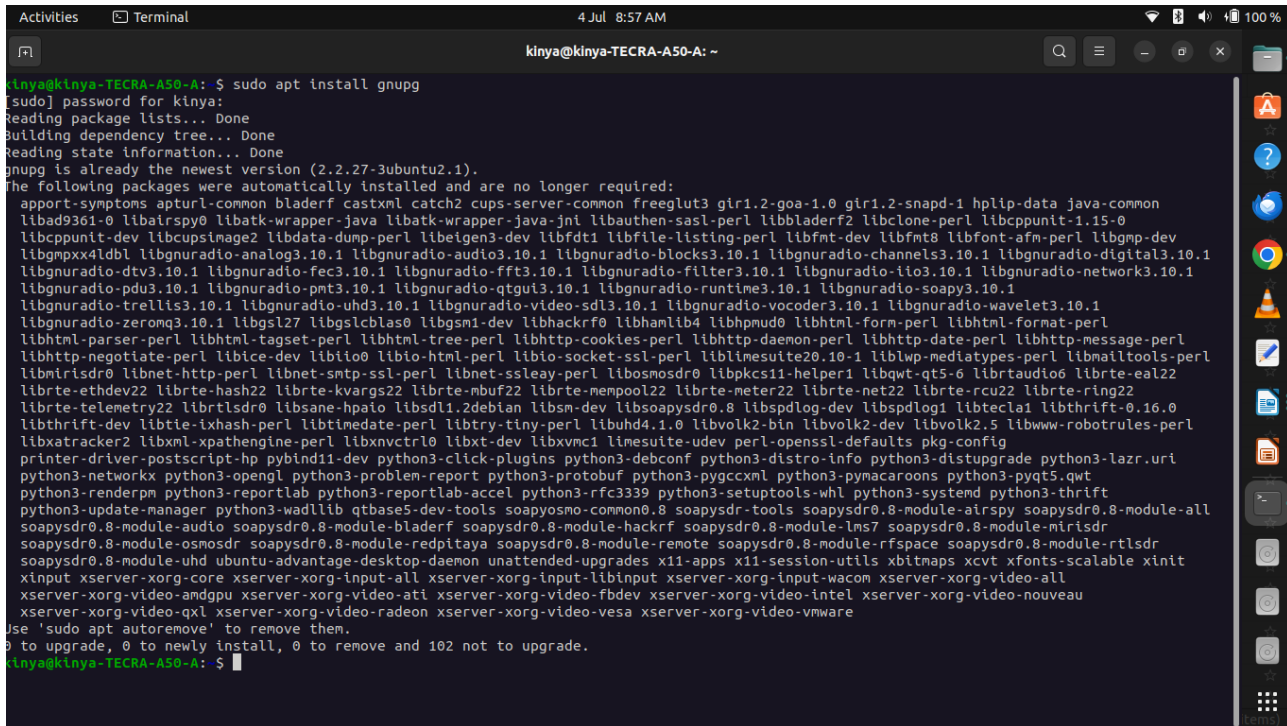


# COMPUTER SECURITY LAB MANUAL

## CRYPTOGRAPHY 101

prepared by  
**Samson Mainah**  
sammainah98@gmail.com

### Installing PGP in linux



```
Activities Terminal 4 Jul 8:57 AM
kinya@kinya-TECRA-A50-A: ~

kinya@kinya-TECRA-A50-A:~$ sudo apt install gnupg
[sudo] password for kinya:
Reading package lists... Done
Building dependency tree... Done
Reading state information... Done
gnupg is already the newest version (2.2.27-3ubuntu2.1).
The following packages were automatically installed and are no longer required:
  apport-symptoms apturl-common bladerf castxml catch2 cups-server-common freeglut3 gir1.2-goa-1.0 gir1.2-snapd-1 hplip-data java-common
  libad9361-0 libatrspp0 libatk-wrapper-java libatk-wrapper-java-jni libauthen-sasl-perl libbladerf2 libclone-perl libcppunit-1.15-0
  libcppunit-dev libcupshimage2 libdata-dump-perl libeigen3-dev libfdt1 libfile-listing-perl libfmt-dev libfmt8 libfont-afm-perl libgmp-dev
  libgmpxx4ldbl libgnuradio-analog3.10.1 libgnuradio-audio3.10.1 libgnuradio-blocks3.10.1 libgnuradio-channels3.10.1 libgnuradio-digital3.10.1
  libgnuradio-dtv3.10.1 libgnuradio-fec3.10.1 libgnuradio-fft3.10.1 libgnuradio-filter3.10.1 libgnuradio-fft3.10.1 libgnuradio-fft3.10.1 libgnuradio-network3.10.1
  libgnuradio-pdu3.10.1 libgnuradio-pmt3.10.1 libgnuradio-qgui3.10.1 libgnuradio-runtime3.10.1 libgnuradio-soapy3.10.1
  libgnuradio-trellis3.10.1 libgnuradio-uhd3.10.1 libgnuradio-video-sdl3.10.1 libgnuradio-vocoder3.10.1 libgnuradio-wavelet3.10.1
  libgnuradio-zero3.10.1 libgsl27 libgslcblas0 libgsm1-dev libhackrf0 libhamlib4 libhpmud0 libhtml-form-perl libhtml-format-perl
  libhtml-parser-perl libhtml-tagset-perl libhtml-tree-perl libhttp-cookies-perl libhttp-daemon-perl libhttp-date-perl libhttp-message-perl
  libhttp-negotiate-perl libice-dev libio0 libio-html-perl libio-socket-ssl-perl liblinesuite20.10-1 liblwp-mediatypes-perl libmailtools-perl
  libmirisdr0 libnet-http-perl libnet-smtp-ssl-perl libnet-ssleay-perl libosmosdr0 libpkcs11-helper1 libqwt-qt5-6 librtaudio6 librt-eal22
  librt-ethdev22 librt-hash22 librt-kvargs22 librt-mbuf22 librt-mempool22 librt-meter22 librt-net22 librt-rcu22 librt-ring22
  librt-telemetry22 librtlsdr0 librsane-hpaio libstd1.2debian libsm-dev libsoapsdr0.8 libspdl-dev libspdl-log1 libtecla1 libthrift-0.16.0
  libthrift-dev libtie-ixhash-perl libtimedate-perl libtiny-perl libuhd4.1.0 libvolk2-bin libvolk2-dev libvolk2.5 libwww-robotrules-perl
  libxatracker2 libxml-xpathengine-perl libxnvctrl0 libxt-dev libxvmc1 limesuite-udev perl-openssl-defaults pkg-config
  printer-driver-postscript-hp pybind11-dev python3-click-plugins python3-debconf python3-distro-info python3-distupgrader python3-lazr.uri
  python3-networkx python3-opengl python3-problem-report python3-protobuf python3-pygccxml python3-pymacaroons python3-pyqt5.qwt
  python3-renderpm python3-reportlab python3-reportlab-accel python3-rfc3339 python3-setuptools-whl python3-systemd python3-thrift
  python3-update-manager python3-wadllib qtbase5-dev-tools soapysdr0.8-module-all soapysdr0.8-module-airspy soapysdr0.8-module-ads1
  soapysdr0.8-module-audio soapysdr0.8-module-bladerf soapysdr0.8-module-hackrf soapysdr0.8-module-lms7 soapysdr0.8-module-mirisdr
  soapysdr0.8-module-osmosdr soapysdr0.8-module-redpitaya soapysdr0.8-module-remote soapysdr0.8-module-rfspace soapysdr0.8-module-rtlsdr
  soapysdr0.8-module-uhd ubuntu-advantage-desktop-daemon unattended-upgrades x11-apps x11-session-utils xbitmaps xcvr xfonts-scalable xinit
  xinput xserver-xorg-core xserver-xorg-input-all xserver-xorg-input-libinput xserver-xorg-input-wacom xserver-xorg-video-all
  xserver-xorg-video-amdgpu xserver-xorg-video-ati xserver-xorg-video-fbdev xserver-xorg-video-intel xserver-xorg-video-nouveau
  xserver-xorg-video-qxl xserver-xorg-video-radeon xserver-xorg-video-vesa xserver-xorg-video-vmware
Use 'sudo apt autoremove' to remove them.
0 to upgrade, 0 to newly install, 0 to remove and 102 not to upgrade.
kinya@kinya-TECRA-A50-A:~$
```

### creating keys

```
Activities Terminal 4 Jul 9:03 AM kinya@kinya-TECRA-A50-A: ~
kinya@kinya-TECRA-A50-A:~$ mkdir encryption
kinya@kinya-TECRA-A50-A:~$ gpg --full-generate-keys
Invalid option "--full-generate-keys"
kinya@kinya-TECRA-A50-A:~$ gpg --full-generate-key
gpg (GnuPG) 2.2.27; Copyright (C) 2021 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.

Please select what kind of key you want:
  (1) RSA and RSA (default)
  (2) DSA and Elgamal
  (3) DSA (sign only)
  (4) RSA (sign only)
  (14) Existing key from card
Your selection? 1
RSA keys may be between 1024 and 4096 bits long.
What keysize do you want? (3072) 1024
Requested keysize is 1024 bits
Please specify how long the key should be valid.
  0 = key does not expire
  <n> = key expires in n days
  <n>w = key expires in n weeks
  <n>m = key expires in n months
  <n>y = key expires in n years
Key is valid for? (0) 0
Key does not expire at all
Is this correct? (y/N) y

You need a user ID to identify your key; the software constructs the user ID
from the Real Name, Comment and Email Address in this form:
  "Heinrich Heine (Der Dichter) <heinrichh@duesseldorf.de>"

Real name: Samson Mainah
E-mail address: sammainah98@gmail.com
Comment: call me master
You selected this USER-ID:
  "Samson Mainah (call me master) <sammainah98@gmail.com>"
```

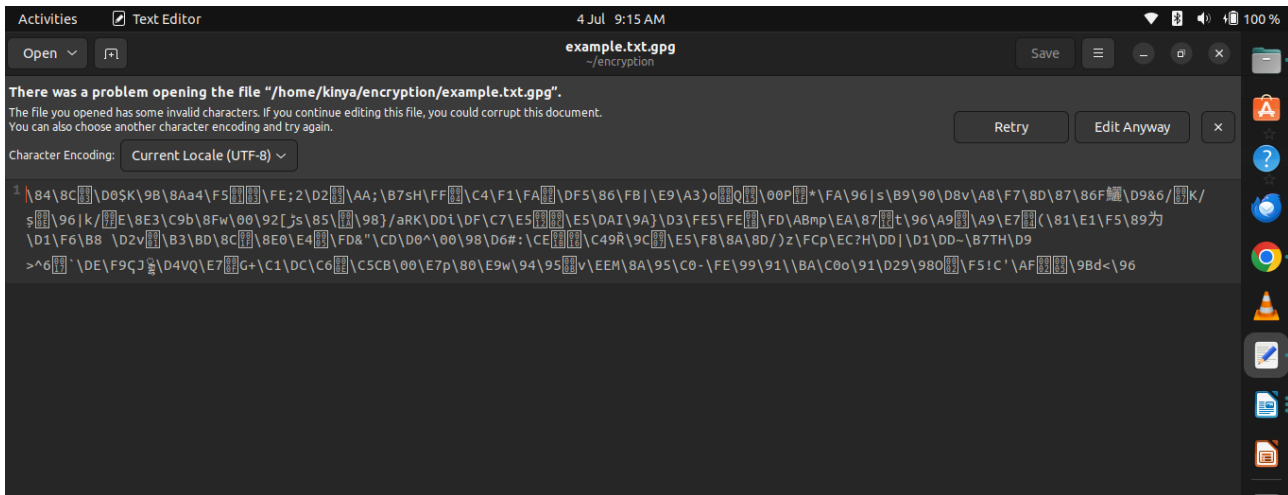
export both public and secret key in the folder you are working on

```
kinya@kinya-TECRA-A50-A:~$ gpg --export -a "Samson Mainah" > encryption/public_key.asc
kinya@kinya-TECRA-A50-A:~$ gpg --export-secret-keys -a "Samson Mainah" > encryption/private_key.asc
kinya@kinya-TECRA-A50-A:~$
```

## Encrypting and decrypting a file

```
kinya@kinya-TECRA-A50-A:~$ gpg --output encryption/example.txt.gpg --encrypt --recipient "Samson Mainah" encryption/example.txt
gpg: checking the trustdb
gpg: marginals needed: 3 completes needed: 1 trust model: pgp
gpg: depth: 0 valid: 3 signed: 0 trust: 0-, 0q, 0n, 0m, 0f, 3u
gpg: next trustdb check due at 2026-07-04
kinya@kinya-TECRA-A50-A:~$ gpg --output encryption/decrypted_example.txt --decrypt encryption/example.txt.gpg
gpg: encrypted with 1024-bit RSA key, ID D0244B9B8A6134F5, created 2024-07-04
  "Samson Mainah (call me master) <sammainah98@gmail.com>"
kinya@kinya-TECRA-A50-A:~$
```

## output of encrypted file



## decrypted file

