



Universidad Autónoma del Estado de México

Centro Universitario UAEM Zumpango

Ingeniería en Computación

Sistemas Operativos

Trabajo.

Llaves en Linux

Presenta:

Yesenia Martínez Galván

Docente:

Hazem Álvarez Rodríguez

Zumpango, Estado de México a 10 de noviembre de 2025

- Como primer Paso es crear una llave publica. Con el comando **gpg --full-gen-key**
- después seleccionamos **RSA and RSA**
- Le dimos un limite de 1 semana, colocando **1w** y enter

```

Ubuntu 14@Redes14: ~ $ gpg --full-gen-key
gpg (GnuPG) 2.4.5; Copyright (C) 2020 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
(2) DSA and Elgamal
(3) RSA (sign only)
(4) RSA (sign only)
(9) ECC (sign and encrypt) *default*
(10) ECC (sign only)
(14) Existing key from card
Your selection? 1

RSA Keysizes must be between 1024 and 4096 bits long.
What keysize do you want? (3072) 3072
Requested keysize is 3072 bits

Please specify how long the key should be valid.
 0 = key does not expire
 <n>M = key expires in n years
 <n>W = key expires in n weeks
 <n>M = key expires in n months
 <n>D = key expires in n days
Key is valid for? (0) 1w
Key expires at Fri Nov 14 16:36:06 2025 CST
Is this correct? (y/N) y

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

Real name: Yesenia
Email address: y@gmail.com
Comment: trabajo en clase
You selected this USER-ID:
  "Yesenia (trabajo en clase) <y@gmail.com>"

Change (N)ame, (C)omment, (E)mail or (Q)uit? o
We need to generate a lot of random bytes. It is a good idea to perform
other action like move the mouse, utilize the
disks) during the key 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 key generation; this gives the random number
generator a better chance to gain enough entropy.
gpg: revocation certificate stored as '/home/edes_14/.gnupg/openpgp-revocs.d/0B2392A09995463EF938069936F308885D7053BE.rev'
public and secret key created and signed

pub  rsa3072 2025-11-07 [SC] {expires: 2025-11-14}
      0B2392A09995463EF938069936F308885D7053BE
uid  Yesenia (trabajo en Clase) <y@gmail.com>
sub  rsa3072 2025-11-07 [E] {expires: 2025-11-14}

Ubuntu 14@Redes14: ~ $ ls -l
total 316
drwxr-xr-x 2 root root 4096 Sep 26 15:46 Documentos
drwxr-xr-x 2 root root 4096 Aug 21 16:04 Graficas
drwxr-xr-x 2 root root 4096 Aug 21 16:02 IO
-rw-r--r-- 1 edes_14 edes_14 259 Oct 16 16:46 IdUnico.txt
-rw-r--r-- 1 root root 24 Nov 6 16:07 MyPer.txt
-rw-r--r-- 1 root root 183 Nov 6 16:10 MyPer.txt.gpg
drwxr-xr-x 2 root root 4096 Aug 21 16:04 MiCarpeta
-rw-r--r-- 1 root root 32 Nov 6 16:08 WePer.txt
-rw-r--r-- 1 root root 111 Nov 6 16:22 WePer.txt.gpg
-rw-r--r-- 1 root root 29 Nov 6 16:08 YourPer.txt
drwxr-xr-x 2 root root 4096 Aug 21 16:04 MiCarpeta
-rw-r--r-- 1 edes_14 edes_14 61 Nov 6 15:51 cartas.jpeg.Zone.Identifier
drwxr-xr-x 2 root root 4096 Aug 21 15:51 MiCarpeta
-rw-r--r-- 1 root root 145 Oct 17 16:03 cronCF.txt
-rw-r--r-- 1 edes_14 edes_14 78 Nov 6 15:48 documento.txt
-rw-r--r-- 1 edes_14 edes_14 261 Nov 6 15:55 documento.txt.asc
-rw-r--r-- 1 root root 128 Nov 6 15:48 documento.txt.gpg
drwxr-xr-x 13 edes_14 edes_14 4096 Sep 4 10:03 MiCarpeta
-rw-r--r-- 1 root root 29 Oct 17 16:09 fecha.txt
-rw-r--r-- 1 root root 29 Sep 25 15:35 fonseca.txt
-rw-r--r-- 1 root root 24 Nov 6 16:19 gpa
-rw-r--r-- 1 edes_14 edes_14 30 Nov 6 16:03 gpa_mundo.txt
-rw-r--r-- 1 edes_14 edes_14 5261 Nov 6 16:03 keySecretSebas.asc
-rw-r--r-- 1 edes_14 edes_14 25 Nov 7 16:04 keySecretSebas.asc.Zone.Identifier
-rw-r--r-- 1 edes_14 edes_14 2585 Nov 7 15:25 keyFonti.asc
-rw-r--r-- 1 edes_14 edes_14 25 Nov 7 15:26 keyFonti.asc.Zone.Identifier
-rw-r--r-- 1 edes_14 edes_14 4873 Nov 7 15:41 keyYes.asc
-rw-r--r-- 1 edes_14 edes_14 2489 Nov 7 15:41 keyYes.asc.gpg
-rw-r--r-- 1 edes_14 edes_14 251 Oct 16 16:01 llavesHaz.sh
-rw-r--r-- 1 edes_14 edes_14 8 Nov 6 16:45 llaves.asc
-rw-r--r-- 1 edes_14 edes_14 6 Nov 6 16:52 llaves1.asc
-rw-r--r-- 1 edes_14 edes_14 664 Nov 6 16:54 llavesHaz.asc
-rw-r--r-- 1 edes_14 edes_14 25 Nov 6 16:55 llavesHaz.asc.Zone.Identifier
-rw-r--r-- 1 edes_14 edes_14 312 Nov 7 15:34 llavesHaz1.asc
-rw-r--r-- 1 root root 77 Nov 7 15:34 mensaje1.txt
-rw-r--r-- 1 root root 555 Nov 7 15:38 mensaje1.txt.gpg
-rw-r--r-- 1 edes_14 edes_14 975 Nov 7 15:40 mensaje2.txt.gpg
-rw-r--r-- 1 edes_14 edes_14 25 Nov 7 15:42 mensaje2.txt.gpg.Zone.Identifier
-rw-r--r-- 1 root root 27 Sep 25 15:36 monosuario.txt
-rw-r--r-- 1 edes_14 edes_14 76 Nov 7 15:42 nombre.txt
-rw-r--r-- 1 edes_14 edes_14 3098 Oct 16 16:34 programar_usuario.sh
-rw-r--r-- 1 edes_14 edes_14 168 Sep 25 15:45 output
-rw-r--r-- 1 edes_14 edes_14 121298 Aug 29 14:55 packages.txt
-rw-r--r-- 1 edes_14 edes_14 112 Sep 25 15:41 salida.txt
-rw-r--r-- 1 edes_14 edes_14 56 Sep 25 15:44 salidai.txt

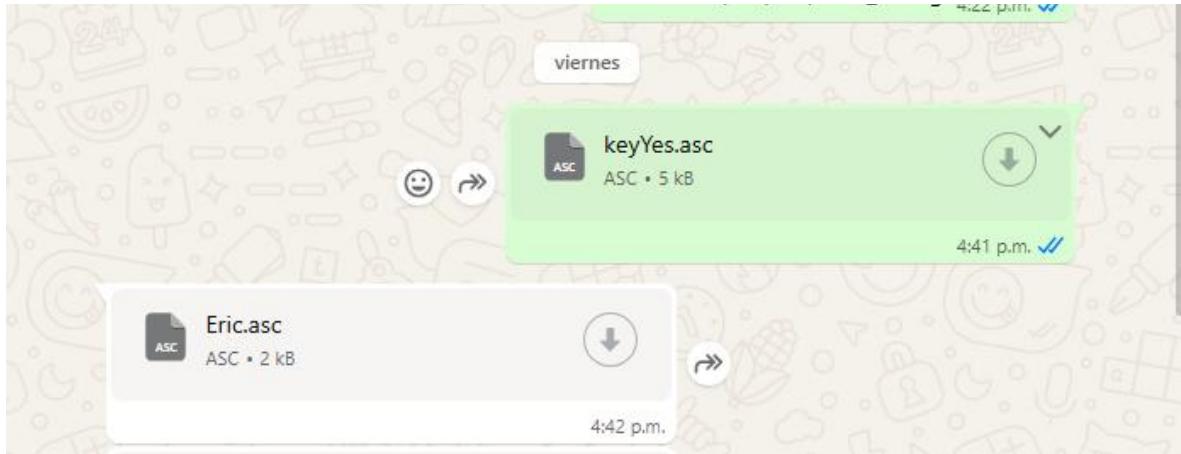
```

```

Ubuntu 14@Redes14: ~ $ gpg --export -a Yesenia > keyYes.asc
Ubuntu 14@Redes14: ~ $ ls -l
total 316
drwxr-xr-x 2 root root 4096 Sep 26 15:46 Documentos
drwxr-xr-x 2 root root 4096 Aug 21 16:04 Graficas
drwxr-xr-x 2 root root 4096 Aug 21 16:02 IO
-rw-r--r-- 1 edes_14 edes_14 259 Oct 16 16:46 IdUnico.txt
-rw-r--r-- 1 root root 24 Nov 6 16:07 MyPer.txt
-rw-r--r-- 1 root root 183 Nov 6 16:10 MyPer.txt.gpg
drwxr-xr-x 2 root root 4096 Aug 21 16:04 MiCarpeta
-rw-r--r-- 1 root root 32 Nov 6 16:08 WePer.txt
-rw-r--r-- 1 root root 111 Nov 6 16:22 WePer.txt.gpg
-rw-r--r-- 1 root root 29 Nov 6 16:08 YourPer.txt
drwxr-xr-x 2 root root 4096 Aug 21 16:04 MiCarpeta
-rw-r--r-- 1 edes_14 edes_14 61 Nov 6 15:51 cartas.jpeg.Zone.Identifier
drwxr-xr-x 2 root root 4096 Aug 21 15:51 MiCarpeta
-rw-r--r-- 1 root root 145 Oct 17 16:03 cronCF.txt
-rw-r--r-- 1 edes_14 edes_14 78 Nov 6 15:48 documento.txt
-rw-r--r-- 1 edes_14 edes_14 261 Nov 6 15:55 documento.txt.asc
-rw-r--r-- 1 root root 128 Nov 6 15:48 documento.txt.gpg
drwxr-xr-x 13 edes_14 edes_14 4096 Sep 4 10:03 MiCarpeta
-rw-r--r-- 1 root root 29 Oct 17 16:09 fecha.txt
-rw-r--r-- 1 root root 29 Sep 25 15:35 fonseca.txt
-rw-r--r-- 1 root root 24 Nov 6 16:19 gpa
-rw-r--r-- 1 edes_14 edes_14 30 Nov 6 16:03 gpa_mundo.txt
-rw-r--r-- 1 edes_14 edes_14 5261 Nov 6 16:03 keySecretSebas.asc
-rw-r--r-- 1 edes_14 edes_14 25 Nov 7 16:04 keySecretSebas.asc.Zone.Identifier
-rw-r--r-- 1 edes_14 edes_14 2585 Nov 7 15:25 keyFonti.asc
-rw-r--r-- 1 edes_14 edes_14 25 Nov 7 15:26 keyFonti.asc.Zone.Identifier
-rw-r--r-- 1 edes_14 edes_14 4873 Nov 7 15:41 keyYes.asc
-rw-r--r-- 1 edes_14 edes_14 2489 Nov 7 15:41 keyYes.asc.gpg
-rw-r--r-- 1 edes_14 edes_14 251 Oct 16 16:01 llavesHaz.sh
-rw-r--r-- 1 edes_14 edes_14 8 Nov 6 16:45 llaves.asc
-rw-r--r-- 1 edes_14 edes_14 6 Nov 6 16:52 llaves1.asc
-rw-r--r-- 1 edes_14 edes_14 664 Nov 6 16:54 llavesHaz.asc
-rw-r--r-- 1 edes_14 edes_14 25 Nov 6 16:55 llavesHaz.asc.Zone.Identifier
-rw-r--r-- 1 edes_14 edes_14 312 Nov 7 15:34 llavesHaz1.asc
-rw-r--r-- 1 root root 77 Nov 7 15:34 mensaje1.txt
-rw-r--r-- 1 root root 555 Nov 7 15:38 mensaje1.txt.gpg
-rw-r--r-- 1 edes_14 edes_14 975 Nov 7 15:40 mensaje2.txt.gpg
-rw-r--r-- 1 edes_14 edes_14 25 Nov 7 15:42 mensaje2.txt.gpg.Zone.Identifier
-rw-r--r-- 1 root root 27 Sep 25 15:36 monosuario.txt
-rw-r--r-- 1 edes_14 edes_14 76 Nov 7 15:42 nombre.txt
-rw-r--r-- 1 edes_14 edes_14 3098 Oct 16 16:34 programar_usuario.sh
-rw-r--r-- 1 edes_14 edes_14 168 Sep 25 15:45 output
-rw-r--r-- 1 edes_14 edes_14 121298 Aug 29 14:55 packages.txt
-rw-r--r-- 1 edes_14 edes_14 112 Sep 25 15:41 salida.txt
-rw-r--r-- 1 edes_14 edes_14 56 Sep 25 15:44 salidai.txt

```

- Como siguiente paso le enviamos nuestro **.asc** exportado a nuestro compañero y él nos envía la suya

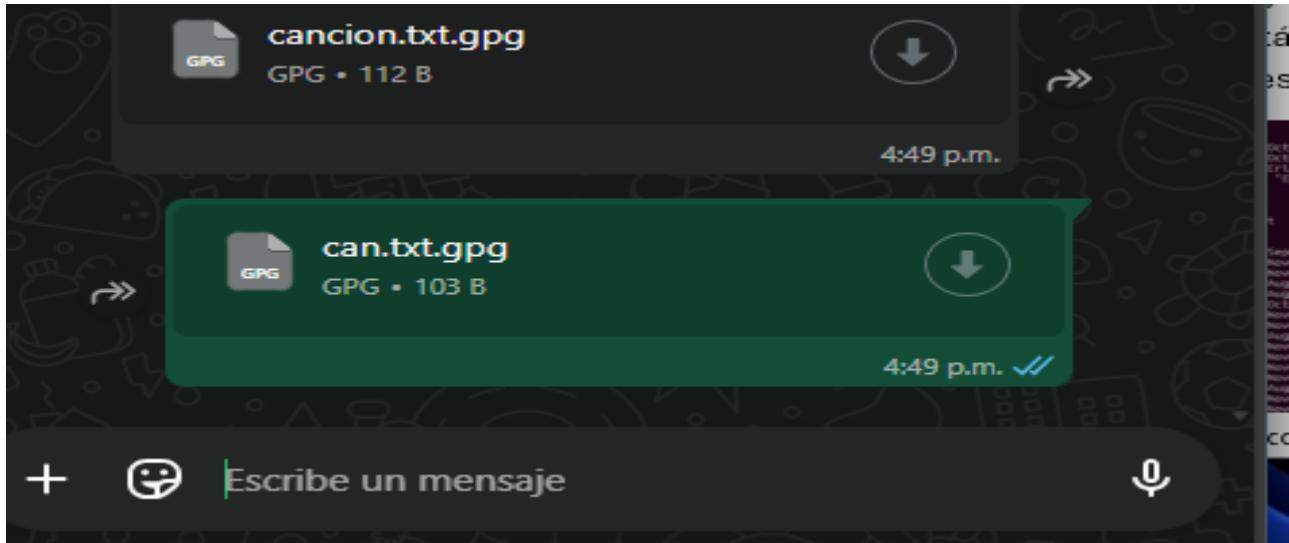


- El siguiente paso es importar la llave de nuestro compañero. Para este paso se descarga y se coloca en /home/usuario.
- Ya que está en esa ubicación se ingresa el comando **gpg -import Eric.asc** (Eric.asc es el nombre que le puso a su llave)

```
Ubuntu          Ubuntu
-rw-r--r-- 1 root    root      496 Sep 26 15:46 update.txt
-rw-r--r-- 1 root    root      3134 Oct 16 16:32 usuario.sh
gpg: key 82442C6B94A86CC4: public key "Eric (Trabajo en clase) <eric@gmail.com>" imported
gpg: Total number of keys imported: 1
999:          imported: 1
edes_14Redes14: $ sudo nano can.txt
edes_14Redes14: $ sudo gpg -c can.txt
edes_14Redes14: $ ls -l
total 332
drwxr-xr-x  2 root    root      496 Sep 26 15:46 Documentos
-rw-r--r--  1 edes_14 edes_14   2468 Nov  7 16:42 Eric.asc
-rw-r--r--  1 edes_14 edes_14   25 Nov  7 16:43 Eric.asc:Zone.Identifier
drwxr-xr-x  2 root    root      496 Aug 21 15:57 calculo
drwxr-xr-x  2 root    root      496 Sep 26 15:46 IdUnico
-rw-r--r--  1 edes_14 edes_14   259 Oct 16 16:46 IdUnico.txt
-rw-r--r--  1 root    root      24 Nov  6 16:07 MyPer.txt
-rw-r--r--  1 root    root     103 Nov  6 16:10 MyPer.txt.gpg
drwxr-xr-x  2 root    root      496 Aug 21 15:08
drwxr-xr-x  2 root    root      30 Nov  6 16:08 MyPer.txt
-rw-r--r--  1 root    root     111 Nov  6 16:22 MePer.txt.gpg
-rw-r--r--  1 root    root      29 Nov  6 16:08 YourPer.txt
-rw-r--r--  1 root    root     212 Nov  6 16:11 YourPer.txt.asc
drwxr-xr-x  2 root    root      496 Aug 21 15:57 calculo
-rw-r--r--  1 root    root      26 Nov  7 16:45 can.txt
-rw-r--r--  1 root    root      183 Nov  7 16:45 can.txt.gpg
-rw-r--r--  1 edes_14 edes_14   61 Nov 22 16:51 cartas.jpeg:Zone.Identifier
drwxr-xr-x  2 root    root      496 Aug 21 15:53
-rw-r--r--  1 root    root     145 Oct 17 16:03 cronCF.txt
-rw-r--r--  1 edes_14 edes_14   78 Nov  6 15:48 documento.txt
-rw-r--r--  1 edes_14 edes_14   261 Nov  6 15:55 documento.txt.asc
-rw-r--r--  1 root    root      6 Nov  6 16:05 documento.txt.gpg
-rw-r--r--  1 edes_14 edes_14   239 Nov  7 16:05 documento.txt.gpg.gpg
drwxr-xr-x 13 edes_14 edes_14  4096 Sep  4 10:03
-rw-r--r--  1 root    root     29 Oct 17 16:09 fecha.txt
-rw-r--r--  1 root    root     29 Sep 25 15:35 fonseca.txt
-rw-r--r--  1 root    root     24 Nov  6 16:19 gpg
-rw-r--r--  1 edes_14 edes_14   30 Nov  6 16:03 gpg_mundo.txt
-rw-r--r--  1 edes_14 edes_14   5263 Nov  7 16:03 keySecretSebas.asc
-rw-r--r--  1 edes_14 edes_14   25 Nov  7 16:04 keySecretSebas.asc:Zone.Identifier
-rw-r--r--  1 edes_14 edes_14   2585 Nov  7 15:25 keyFont.asc
-rw-r--r--  1 edes_14 edes_14   25 Nov  7 15:26 keyFont.asc:Zone.Identifier
-rw-r--r--  1 edes_14 edes_14   489 Nov  7 15:41 keyYes.asc
-rw-r--r--  1 edes_14 edes_14   2493 Nov  7 15:41 keyYes.asc
-rw-r--r--  1 edes_14 edes_14   251 Oct 16 16:03 llavesHaz.sh
-rw-r--r--  1 edes_14 edes_14   6 Nov  6 16:45 llaves.asc
-rw-r--r--  1 edes_14 edes_14   6 Nov  6 16:45 llaves1.asc
-rw-r--r--  1 edes_14 edes_14   664 Nov  6 16:54 llavesHaz.asc
-rw-r--r--  1 edes_14 edes_14   25 Nov  6 16:55 llavesHaz.asc:Zone.Identifier
-rw-r--r--  1 edes_14 edes_14   3138 Nov  6 16:53 llaves.asc
-rw-r--r--  1 root    root      77 Nov  7 15:34 menseje1.txt
```

- Como siguiente se creo un documento donde le llame **can.txt** en ese documento le agregue nombre de canción favorita y artista
- después se continúo encriptando el documento con el comando **sudo gpg -c can.txt** y ingresamos un **ls -l** para verificar que ya esta y debe de aparecer como **can.asc.gpg**

- Como siguiente paso compartimos el documento encriptado.



- Descargamos el documento.
 - Lo guardamos en /home/usuario.
 - Descriptamos el documento con el comando **sudo gpg canción.txt.gpg**
 - Ingresamos el comando **cat.txt** para visualizar lo que escribió el compañero en su documento. Así sabemos su canción favorita y artista que escribió en el documento.

```
Ubuntu          x  Ubuntu          x + 
-W--r--r--  1 edes_14 edes_14  2493 Nov  7 15:23 keyYesenia.asc
-W--r--r-X  1 edes_14 edes_14  251 Oct 16 16:01 leer-tareas.sh
-W--r--r-X  1 edes_14 edes_14     0 Nov  6 16:45 llaves.asc
-W--r--r-X  1 edes_14 edes_14     0 Nov  6 16:45 llavesYes.asc
-W--r--r-X  1 edes_14 edes_14  664 Nov  6 16:54 llavesHd.asc
-W--r--r-X  1 edes_14 edes_14  25 Nov  6 16:55 llavesHaz.asc:Zone.Identifier
-W--r--r-X  1 edes_14 edes_14 3130 Nov  6 16:53 llavesSS.asc
-W--r--r-X  1 root   root      77 Nov  7 15:34 mensaje1.txt
-W--r--r-X  1 root   root     555 Nov  7 15:38 mensaje1.txt.gpg
-W--r--r-X  1 edes_14 edes_14  975 Nov  7 15:42 mensaje2.txt.gpg:Zone.Identifier
-W--r--r-X  1 edes_14 edes_14  23 Nov  7 15:42 mensaje2.txt.gpg:Zone.Identifier
-W--r--r-X  1 root   root      27 Sep 16 16:15 nonosario.txt
-W--r--r-X  1 root   root      76 Oct 16 16:15 name.sh
-W--r--r-X  1 edes_14 edes_14 3698 Oct 16 16:34 nuevo_usuario.sh
-W--r--r-X  1 edes_14 edes_14  168 Sep 29 15:45 output
-W--r--r-X  1 edes_14 edes_14 121298 Aug 29 14:55 packages.txt
-W--r--r-X  1 edes_14 edes_14  100 Sep 25 15:44 salidas1.txt
-W--r--r-X  1 edes_14 edes_14  56 Sep 25 15:44 salidas1.txt
-W--r--r-X  1 root   root      6 Oct 24 16:59 saludos.txt
-W--r--r-X  1 edes_14 edes_14  65 Oct 16 16:02 to-do.txt
-W--r--r-X  1 root   root      0 Oct 17 16:45 update.txt
-W--r--r-X  1 edes_14 edes_14 3134 Oct 16 16:32 usuario.sh
-W--r--r-X  1 root   root      3134 Oct 16 16:32 usuario.sh
[edes_14@Redes14 ~]$ sudoing cancion.txt.gpg
gpg: WARNING: no command supplied. Trying to guess what you mean ...
gpg: AES256.CFB encrypted data
gpg: encrypted with 1 passphrase
edes_14@Redes14: $ cat cancion.txt
La balada del perdon
Rosalia
[edes_14@Redes14: ~]$
```