



Universidad Autónoma del Estado de México

Centro Universitario UAEM Zumpango

Ingeniería en Computación

Sistemas Digitales

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

```

edes_14@edes14: $ gpg --full-gen-key
gpg (GnuPG) 2.4.4; Copyright (C) 2024 g10 Code GmbH
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) DSA (sign only)
(4) RSA (sign only)
(5) ECC (sign and encrypt) *default*
(10) ECC (sign only)
(14) Existing key from card
Your selection? 1
RSA keys may be between 1024 and 4096 bits long.
What keysizes do you want? (3072) 3072
Requested keysizes is 3072 bits
Please specify how long the key should be valid.
0 = key does not expire
<no> = key expires in n days
<nw> = key expires in n weeks
<mon> = key expires in n months
<eny> = key expires in n years
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 (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: revocation certificate stored as '/home/edes_14/.gnupg/openpgp-revocs.d/0B2392A09995A63EF938D6936F3D8885D7D53BE.rev'
public and secret key created and signed.

pub  rsa3072 2025-11-07 [SC] [expires: 2025-11-14]
     0B2392A09995A63EF938D6936F3D8885D7D53BE
uid          Yesenia (trabajo en clase) <y@gmail.com>
sub  rsa3072 2025-11-07 [E] [expires: 2025-11-14]

```

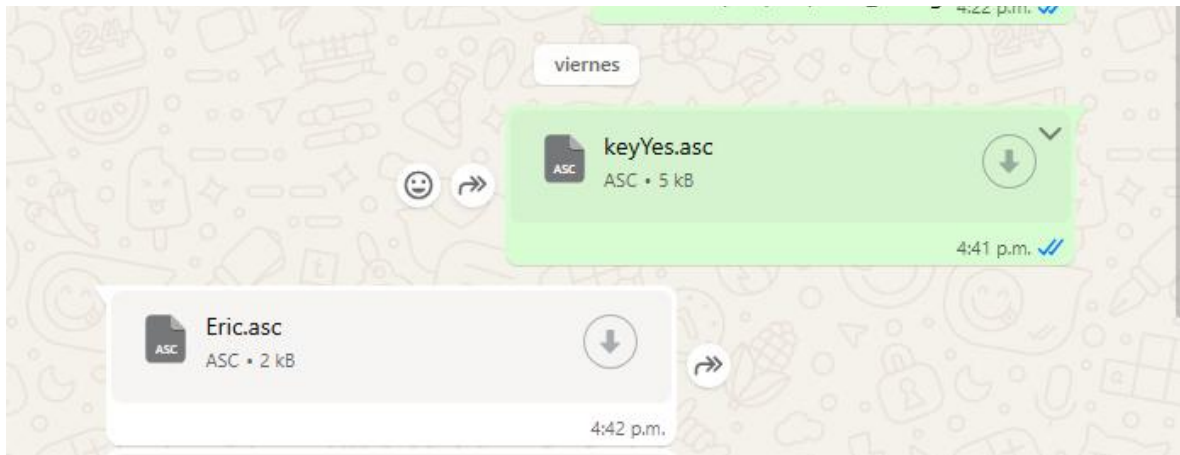
- Exportamos la llave con el comando **gpg --export -a Yesenia > keyYes.asc**
- Y ponemos el comando **ls -l** para verificar que se encuentra exportada

```

edes_14@edes14: $ gpg --export -a Yesenia > keyYes.asc
edes_14@edes14: $ 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 --fixaction
drwxr-xr-x 2 root root 4096 Aug 21 16:02 id
-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 4096 Aug 21 16:00 n
-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 16:06 YourPer.txt
-rw-r--r-- 1 root root 212 Nov 6 16:11 YourPer.txt.asc
drwxr-xr-x 2 root root 4096 Aug 21 15:57
-rw-r--r-- 1 edes_14 edes_14 61 Aug 22 15:51 cartas_peg:Zone.Identifier
drwxr-xr-x 2 root root 4096 Aug 21 15:53 fecha
-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 148 Nov 6 16:04 documento.txt.gpg
-rw-r--r-- 1 root root 239 Nov 6 16:05 documento.txt.gpg.gpg
drwxr-xr-x 13 edes_14 edes_14 4096 Sep 4 18:03
-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 Oct 16 16:12 hola_mundo.txt
-rw-r--r-- 1 edes_14 edes_14 5261 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 keyTonI.asc
-rw-r--r-- 1 edes_14 edes_14 25 Nov 7 15:26 keyTonI.asc:Zone.Identifier
-rw-r--r-- 1 edes_14 edes_14 4873 Nov 7 16:41 keyYes.asc
-rw-r--r-- 1 edes_14 edes_14 2493 Nov 7 15:23 keyYesenia.asc
-rwxr-xr-x 1 root root 251 Oct 16 16:01 leer_smbios.sh
-rw-r--r-- 1 edes_14 edes_14 0 Nov 6 16:45 llaves.asc
-rw-r--r-- 1 edes_14 edes_14 0 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 3130 Nov 6 16:53 llavess.asc
-rw-r--r-- 1 root root 77 Nov 7 15:34 mensaje1.txt
-rw-r--r-- 1 root root 535 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 monosaurio.txt
-rw-r--r-- 1 root root 76 Oct 16 16:15 name.sh
-rwxr-xr-x 1 edes_14 edes_14 3898 Oct 16 16:34 nuevo_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 salida1.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)

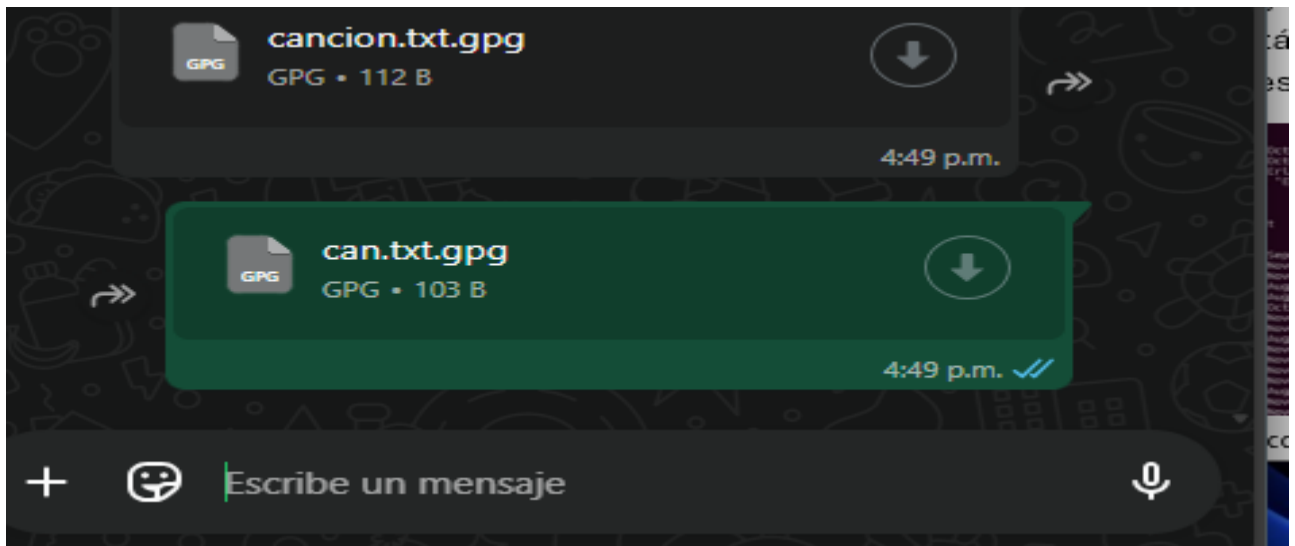
```

-#w-r--r-- 1 root root 0 Oct 17 16:45 update.txt
-#w-r--r-- 1 root root 3134 Oct 16 16:32 usuario.sh
edes_14@edes14:~$ sudo gpg --import Eric.asc
gpg: key B2442C8B4460C4: public key "Eric (Trabajo en clase) <eric@gmail.com>" imported
gpg: Total number processed: 1
gpg:   imported: 1
edes_14@edes14:~$ sudo nano can.txt
edes_14@edes14:~$ ls -l
total 332
drwxr-xr-x 2 root root 4896 Sep 26 15:46 .
drwxr-xr-x 1 edes_14 edes_14 2468 Nov 7 16:42 Eric.asc
drwxr-xr-x 1 edes_14 edes_14 25 Nov 7 16:43 Eric.asc:Zone.Identifier
drwxr-xr-x 2 root root 4896 Aug 21 16:04 .Trash-1000
drwxr-xr-x 2 root root 4896 Aug 21 16:02 .
drwxr-xr-x 1 edes_14 edes_14 259 Oct 16 16:46 IdUnico.txt
drwxr-xr-x 1 root root 24 Nov 6 16:07 MyPer.txt
drwxr-xr-x 1 root root 103 Nov 6 16:10 MyPer.txt.gpg
drwxr-xr-x 2 root root 4896 Aug 21 16:08 .
drwxr-xr-x 1 root root 32 Nov 6 16:08 WePer.txt
drwxr-xr-x 1 root root 111 Nov 6 16:22 WePer.txt.gpg
drwxr-xr-x 1 root root 29 Nov 6 16:08 YourPer.txt
drwxr-xr-x 1 root root 212 Nov 6 16:11 YourPer.txt.asc
drwxr-xr-x 2 root root 4896 Aug 21 15:57 .
drwxr-xr-x 1 root root 26 Nov 7 16:45 can.txt
drwxr-xr-x 1 root root 103 Nov 7 16:49 can.txt.gpg
drwxr-xr-x 1 edes_14 edes_14 61 Aug 22 15:51 cartas.jpeg:Zone.Identifier
drwxr-xr-x 2 root root 4896 Aug 21 15:53 .
drwxr-xr-x 1 root root 145 Oct 17 16:03 cronCF.txt
drwxr-xr-x 1 edes_14 edes_14 78 Nov 6 15:48 documento.txt
drwxr-xr-x 1 edes_14 edes_14 261 Nov 6 15:55 documento.txt.asc
drwxr-xr-x 1 root root 148 Nov 6 16:04 documento.txt.gpg
drwxr-xr-x 1 root root 239 Nov 6 16:05 documento.txt.gpg.gpg
drwxr-xr-x 13 edes_14 edes_14 4896 Sep 4 10:03 .
drwxr-xr-x 1 root root 29 Oct 17 16:09 fecha.txt
drwxr-xr-x 1 root root 29 Sep 25 15:35 fonseca.txt
drwxr-xr-x 1 root root 24 Nov 6 16:19 gpg
drwxr-xr-x 1 edes_14 edes_14 30 Oct 16 16:12 hola_mundo.txt
drwxr-xr-x 1 edes_14 edes_14 5261 Nov 7 16:03 keySecretSebas.asc
drwxr-xr-x 1 edes_14 edes_14 25 Nov 7 16:04 keySecretSebas.asc:Zone.Identifier
drwxr-xr-x 1 edes_14 edes_14 2595 Nov 7 15:25 keyFont.asc
drwxr-xr-x 1 edes_14 edes_14 25 Nov 7 15:26 keyFont.asc:Zone.Identifier
drwxr-xr-x 1 edes_14 edes_14 4873 Nov 7 16:41 keyYes.asc
drwxr-xr-x 1 edes_14 edes_14 2493 Nov 7 15:23 keyYesEnLa.asc
drwxr-xr-x 1 edes_14 edes_14 251 Oct 16 16:01 llave-fairas.sh
drwxr-xr-x 1 edes_14 edes_14 0 Nov 6 16:45 llaves.asc
drwxr-xr-x 1 edes_14 edes_14 664 Nov 6 16:54 llavesH2.asc
drwxr-xr-x 1 edes_14 edes_14 25 Nov 6 16:55 llavesH2.asc:Zone.Identifier
drwxr-xr-x 1 edes_14 edes_14 3130 Nov 6 16:53 llavesH3.asc
drwxr-xr-x 1 root root 77 Nov 7 15:34 mensaje1.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 continuó 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.
- Desencriptamos 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.

```

-#-#-#-#-#-# 1 edes_14 edes_14 2493 Nov 7 15:23 keyYesenta.asc
-#-#-#-#-#-# 1 edes_14 edes_14 251 Oct 16 16:01 user=eduardo.sh
-#-#-#-#-#-# 1 edes_14 edes_14 0 Nov 6 16:45 llaves.asc
-#-#-#-#-#-# 1 edes_14 edes_14 0 Nov 6 16:52 llaves1.asc
-#-#-#-#-#-# 1 edes_14 edes_14 664 Nov 6 16:54 llavesHaz.asc
-#-#-#-#-#-# 1 edes_14 edes_14 25 Nov 6 16:55 llavesHaz.asc:Zone.Identifier
-#-#-#-#-#-# 1 edes_14 edes_14 3130 Nov 6 16:53 llaves2.asc
-#-#-#-#-#-# 1 root root 77 Nov 7 15:34 mensaje1.txt
-#-#-#-#-#-# 1 root root 555 Nov 7 15:38 mensaje1.txt.gpg
-#-#-#-#-#-# 1 edes_14 edes_14 975 Nov 7 15:40 mensaje2.txt.gpg
-#-#-#-#-#-# 1 edes_14 edes_14 25 Nov 7 15:42 mensaje2.txt.gpg:Zone.Identifier
-#-#-#-#-#-# 1 root root 27 Sep 25 15:36 monosaurio.txt
-#-#-#-#-#-# 1 root root 76 Oct 16 16:15 name.sh
-#-#-#-#-#-# 1 edes_14 edes_14 3098 Oct 16 16:34 nemo_usuario.sh
-#-#-#-#-#-# 1 edes_14 edes_14 168 Sep 25 15:45 output
-#-#-#-#-#-# 1 edes_14 edes_14 121298 Aug 29 14:55 packages.txt
-#-#-#-#-#-# 1 edes_14 edes_14 112 Sep 25 15:41 salida.txt
-#-#-#-#-#-# 1 edes_14 edes_14 56 Sep 25 15:44 salida1.txt
-#-#-#-#-#-# 1 root root 6 Oct 24 16:59 saludos.txt
-#-#-#-#-#-# 1 edes_14 edes_14 65 Oct 16 16:02 to-do.txt
-#-#-#-#-#-# 1 root root 0 Oct 17 16:45 update.txt
-#-#-#-#-#-# 1 root root 3134 Oct 16 16:32 usuario.sh
edes_14@edes14: $ sudo gpg 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@edes14: $ cat cancion.txt
La balada del perdon
Rosalia
edes_14@edes14: $

```