

Índice:

Ejercicio 1	2
a) Utilizar en Windows EFS (Encrypted File System). Utilizar PGP en Linux.....	2
• Windows EFS	2
• PGP en Linux.....	3

Ejercicio 1

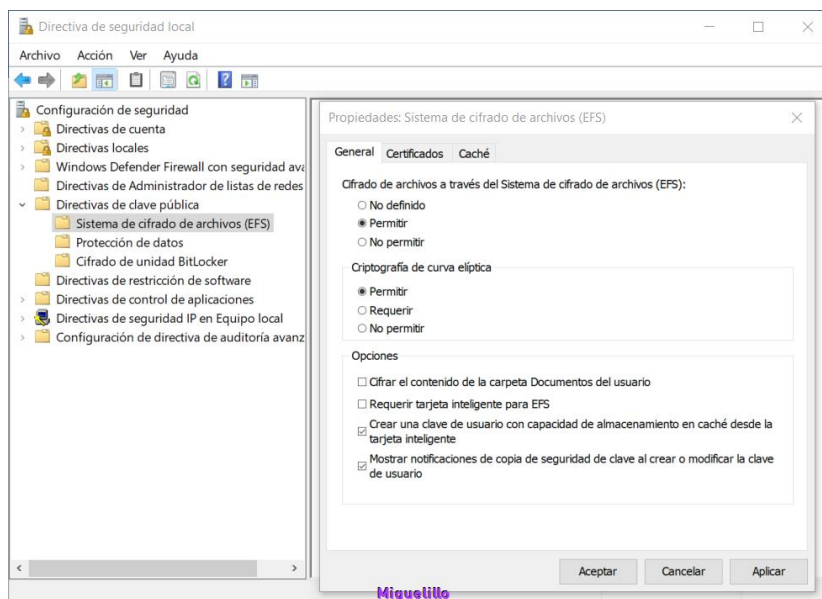
- a) Utilizar en Windows EFS (Encrypted File System).
Utilizar PGP en Linux.

Solución:

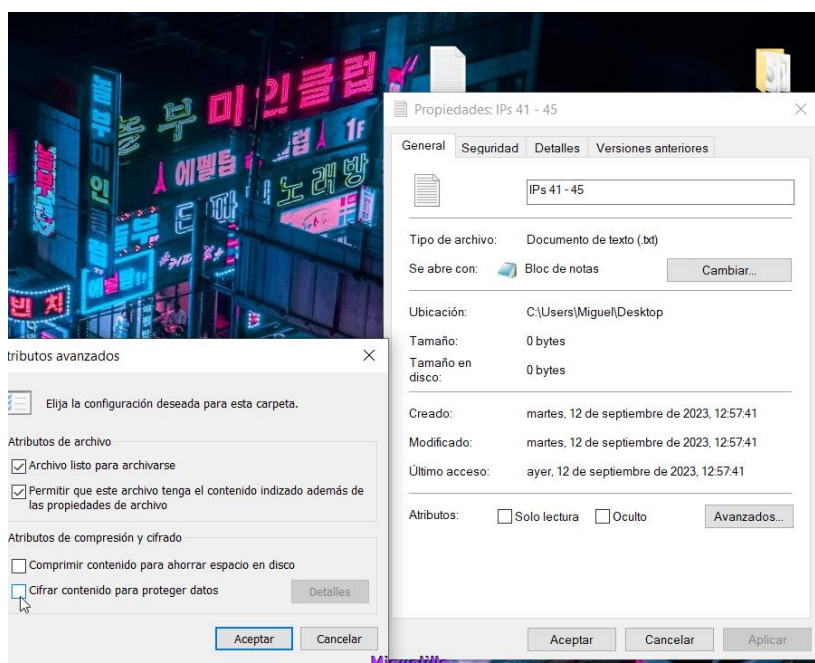
Windows EFS

Primero tendremos que activarla para ello vamos a:

Directiva de seguridad local → Directivas de clave pública → Sistemas de cifrado de archivos (EFS) Clicamos en **Permitir** y por último **Aceptar**.

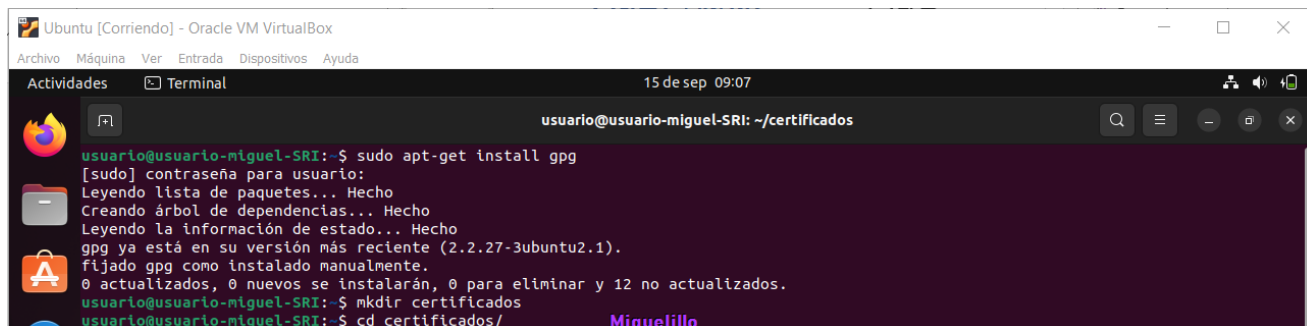


Clicamos en el archivo **Propiedades → Avanzados → Cifrar contenido para proteger datos**



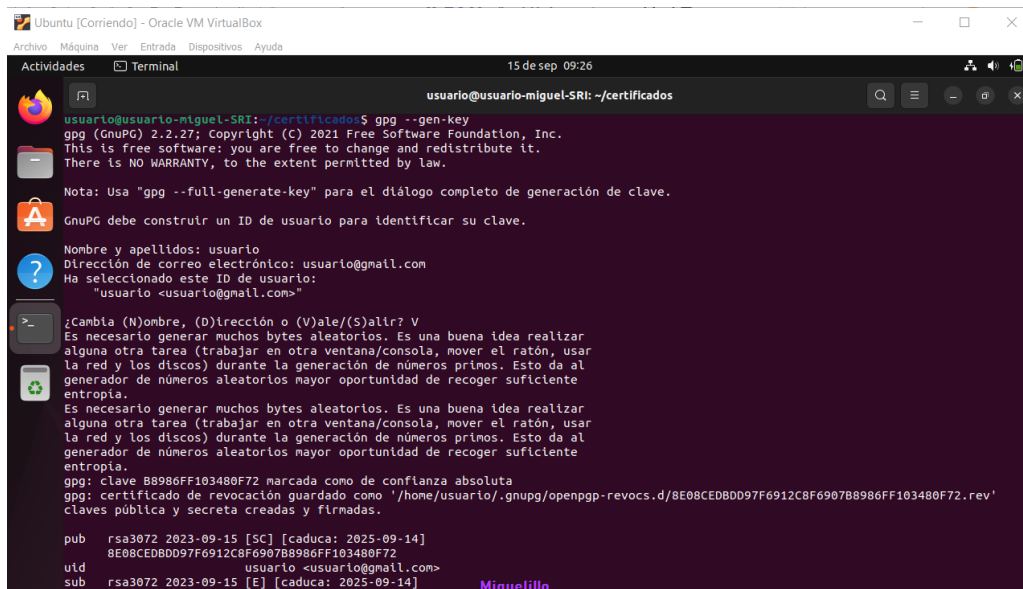
PGP en Linux

Primero instalamos el programa (PGP) → Creamos una carpeta para guardar los certificados (la clave pública y la privada). Con la privada nos permitirá descifrar y con la pública encriptaremos



```
usuario@usuario-miguel-SRI: ~/certificados
usuario@usuario-miguel-SRI:~$ sudo apt-get install gpg
[sudo] contraseña para usuario:
Leyendo lista de paquetes... Hecho
Creando árbol de dependencias... Hecho
Leyendo la información de estado... Hecho
gpg ya está en su versión más reciente (2.2.27-3ubuntu2.1).
fijado gpg como instalado manualmente.
0 actualizados, 0 nuevos se instalarán, 0 para eliminar y 12 no actualizados.
usuario@usuario-miguel-SRI:~$ mkdir certificados
usuario@usuario-miguel-SRI:~$ cd certificados/
```

Seguidamente generamos los certificados



```
usuario@usuario-miguel-SRI:~/certificados$ gpg --gen-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.

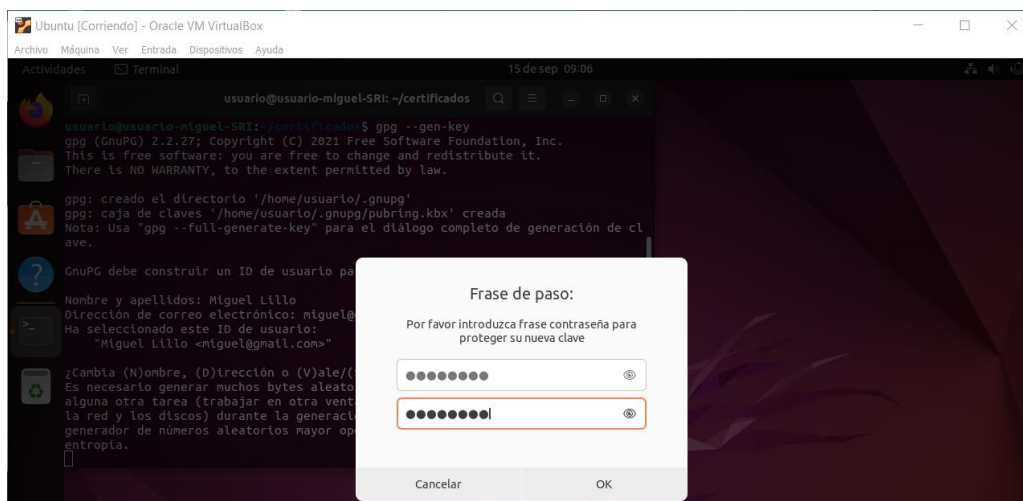
Nota: Usa "gpg --full-generate-key" para el diálogo completo de generación de clave.
GnuPG debe construir un ID de usuario para identificar su clave.

Nombre y apellidos: usuario
Dirección de correo electrónico: usuario@gmail.com
Ha seleccionado este ID de usuario:
"usuario <usuario@gmail.com>"

¿Cambia (N)ombre, (D)irección o (V)ale/(S)alir? V
Es necesario generar muchos bytes aleatorios. Es una buena idea realizar
alguna otra tarea (trabajar en otra ventana/console, mover el ratón, usar
la red y los discos) durante la generación de números primos. Esto da al
generador de números aleatorios mayor oportunidad de recoger suficiente
entropía.
Es necesario generar muchos bytes aleatorios. Es una buena idea realizar
alguna otra tarea (trabajar en otra ventana/console, mover el ratón, usar
la red y los discos) durante la generación de números primos. Esto da al
generador de números aleatorios mayor oportunidad de recoger suficiente
entropía.
gpg: clave B8986FF103480F72 marcada como de confianza absoluta
gpg: certificado de revocación guardado como '/home/usuario/.gnupg/openpgp-revocs.d/8E08CEDBDD97F6912C8F6907B8986FF103480F72.rev'
claves pública y secreta creadas y firmadas.

pub   rsa3072 2023-09-15 [SC] [caduca: 2025-09-14]
      8E08CEDBDD97F6912C8F6907B8986FF103480F72
uid    usuario <usuario@gmail.com>
sub    rsa3072 2023-09-15 [E] [caduca: 2025-09-14]
```

Una vez completada la información que nos pedía que en este caso era el correo y el nombre y apellido, nos pedirá que le pongamos una contraseña.



```
usuario@usuario-miguel-SRI:~/certificados$ gpg --gen-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.

gpg: creado el directorio '/home/usuario/.gnupg'
gpg: caja de claves '/home/usuario/.gnupg/pubring.kbx' creada
Nota: Usa "gpg --full-generate-key" para el diálogo completo de generación de clave.
GnuPG debe construir un ID de usuario para identificar su clave.

Nombre y apellidos: Miguel Lillo
Dirección de correo electrónico: miguel@gmail.com
Ha seleccionado este ID de usuario:
"Miguel Lillo <miguel@gmail.com>"

¿Cambia (N)ombre, (D)irección o (V)ale/(S)alir? V
Es necesario generar muchos bytes aleatorios. Es una buena idea realizar
alguna otra tarea (trabajar en otra ventana/console, mover el ratón, usar
la red y los discos) durante la generación de números primos. Esto da al
generador de números aleatorios mayor oportunidad de recoger suficiente
entropía.
```

Frase de paso:

Por favor introduzca frase contraseña para proteger su nueva clave

●●●●●●●●

●●●●●●●●

Cancelar OK

Una vez hecho esto nos pedirá comprobar la información y en caso de ser correcta escribir V, de este modo ya se habrían creado la clave pública y la privada.

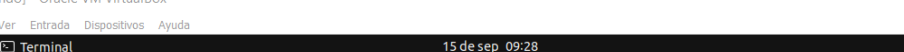
```

>_> ¿Cambia (N)ombre, (D)irección o (V)ale/(S)alir? V
Es necesario generar muchos bytes aleatorios. Es una buena idea realizar
alguna otra tarea (trabajar en otra ventana/consola, mover el ratón, usar
la red y los discos) durante la generación de números primos. Esto da al
generador de números aleatorios mayor oportunidad de recoger suficiente
entropía.
Es necesario generar muchos bytes aleatorios. Es una buena idea realizar
alguna otra tarea (trabajar en otra ventana/consola, mover el ratón, usar
la red y los discos) durante la generación de números primos. Esto da al
generador de números aleatorios mayor oportunidad de recoger suficiente
entropía.
gpg: clave B8986FF103480F72 marcada como de confianza absoluta
gpg: certificado de revocación guardado como '/home/usuario/.gnupg/openpgp-revocs.d/8E08CEDBD097F6912C8F6907B8986FF103480F72.rev'
claves pública y secreta creadas y firmadas.

pub   rsa3072 2023-09-15 [SC] [caduca: 2025-09-14]
      8E08CEDBD097F6912C8F6907B8986FF103480F72
uid          usuario <usuario@gmail.com>
sub       rsa3072 2023-09-15 [E] [caduca: 2025-09-14]

```

Exporto la clave publica a un documento la importo para poder usarla y creo un archivo para cifrarlo.



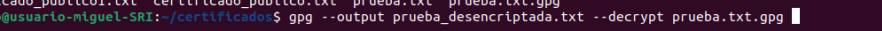
The screenshot shows a terminal window titled "Ubuntu [Corriendo] - Oracle VM VirtualBox". The terminal output is as follows:

```
usuario@usuario-miguel-SRI: ~/certificados
usuario@usuario-miguel-SRI:~/certificados$ gpg --export -a -o certificado_publico1.txt usuario
usuario@usuario-miguel-SRI:~/certificados$ gpg --import certificado_publico1.txt
gpg: clave B8986FF03480F72: "usuario <usuario@gmail.com>" sin cambios
gpg: Cantidad total procesada: 1
gpg:      sin cambios: 1
Miguelillo
usuario@usuario-miguel-SRI:~/certificados$ nano prueba.txt
usuario@usuario-miguel-SRI:~/certificados$ cat prueba.txt
hola buenas esto e sun mensaje cifrado
Miguelillo
```

Encripto el archivo y compruebo que esta encriptado y no se puede leer

[illegible]

Desencriptaremos con la clave privada el archivo cifrado, como esta clave no la vamos a compartir no hace falta exportarla en un documento.

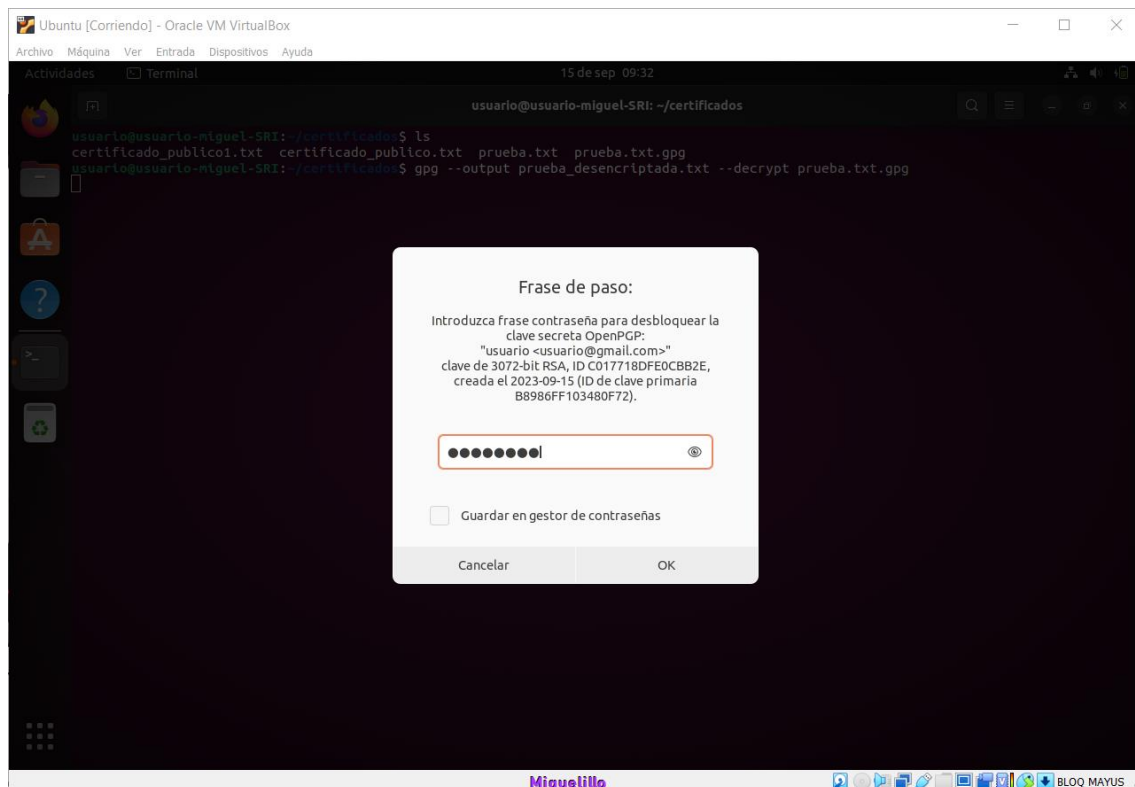


The screenshot shows a terminal window titled "Ubuntu [Corriendo] - Oracle VM VirtualBox". The window has a menu bar with "Archivo", "Máquina", "Ver", "Entrada", "Dispositivos", and "Ayuda". Below the menu bar is a toolbar with icons for "Actividades" and "Terminal". The terminal itself has a title bar "usuario@usuario-miguel-SRI: ~/certificados" and a search bar. The terminal content shows the following commands and output:

```
usuario@usuario-miguel-SRI:~/certificados$ ls
certificado_publico1.txt certificado_publico.txt prueba.txt prueba.txt.gpg
usuario@usuario-miguel-SRI:~/certificados$ gpg --output prueba_desencriptada.txt --decrypt prueba.txt.gpg
```

The terminal window is part of a larger application window titled "Miguelillo".

Introducimos la contraseña que le asignamos anteriormente en la creación de las claves.



Una vez descriptado podremos leerlo perfectamente.

