

# CIFRADO SIMETRICO EN LINUX



Juan Carlos Navidad García  
Seguridad Informática

# 1. Cifrar de manera simétrica en Linux:

1. La herramienta **gpg** nos permite utilizar tanto criptografía simétrica como asimétrica. En este ejemplo veremos la simétrica.
2. Nos presentamos en Ubuntu y creamos un directorio llamado **cifrado** donde vamos a trabajar. Lo primero será crear un fichero de prueba.
  - Podemos utilizar la herramienta **fortune**, que ofrece aleatoriamente refranes, chistes, etc.
  - Creamos un archivo de texto cualquiera.
  - Ejecutamos: **"fortune > archivo"**

```
~/cifrado
→ touch mensaje_cifrado

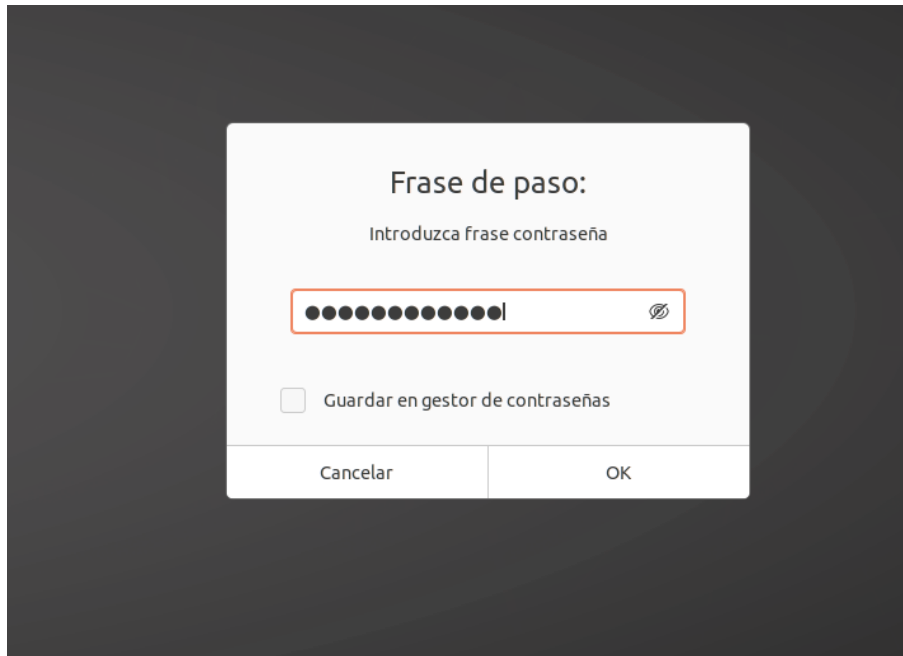
~/cifrado
→ fortune > mensaje_cifrado

~/cifrado
→ cat mensaje_cifrado
You will be divorced within a year.

~/cifrado
→
```

### 3. Para cifrarlo con clave simétrica el comando es:

- `"gpg --symmetric archivo"`
- El comando nos pedirá la clave que queremos utilizar



- El resultado del comando es un nuevo fichero con la extensión. `gpg`. Es un fichero cifrado: si intentamos ver qué hay dentro con el comando `cat`, no aparece nada inteligible.
- Aquí podemos ver que se ha cifrado:

```
~/cifrado
→ ls
mensaje_cifrado  mensaje_cifrado.gpg

~/cifrado
→ cat mensaje_cifrado.gpg
qXWegGi;YRe\U"e^ew1eol:7Zl>^heew{eI~9eV"e$ye
eeeeeeeeeeZlQeCeTe>3cIeh%

~/cifrado
→
```

#### 4. Cuando se necesite leerlo, se descifrá con el comando:

- `"gpg --decrypt documento.gpg"`
- El comando pedirá la clave que habíamos utilizado para cifrar. Si la introducimos correctamente, aparecerá en pantalla el contenido del fichero.

```
~/cifrado
→ ls
mensaje_cifrado  mensaje_cifrado.gpg

~/cifrado
→ cat mensaje_cifrado.gpg
eQeXWegGi;e;eYeR+++u"e^eW1eooHl:7ZL>^heeeW{eeeI~9eeeV"e$ey
+++++ZlQeCeTe>3CIeh

~/cifrado
→ gpg --decrypt mensaje_cifrado.gpg
gpg: datos cifrados AES256
gpg: cifrado con 1 frase contraseña
You will be divorced within a year.

~/cifrado
→
```

#### 5. Si no queremos verlo por pantalla, sino volcarlo a un fichero, podemos redirigir la salida estándar con el comando:

- `"gpg --decrypt documento.gpg > documento2"`

```
~/cifrado
→ gpg --decrypt mensaje_cifrado.gpg > mensaje_descifrado
gpg: datos cifrados AES256
gpg: cifrado con 1 frase contraseña

~/cifrado
→ ls
mensaje_cifrado  mensaje_cifrado.gpg  mensaje_descifrado

~/cifrado
→ cat mensaje_descifrado
You will be divorced within a year.

~/cifrado
→
```

**6. Los ficheros binarios.gpg no siempre son adecuados. No sirven para incluirlos dentro de un texto. Para resolverlo tenemos el parámetro `-a`, que genera un fichero cifrado pero compuesto solo de caracteres ASCII. Estos ficheros ya no tienen extensión.gpg, sino .asc. El comando en cuestión sería:**

- *"gpg -a --symmetric mensaje"*

```
~/cifrado
+ gpg -a --symmetric mensaje_cifrado
~/cifrado took 3s
+ ls
mensaje_cifrado  mensaje_cifrado.asc  mensaje_cifrado.gpg  mensaje_descifrado

~/cifrado
+ cat mensaje_cifrado.asc
-----BEGIN PGP MESSAGE-----
jA0EQQMcbndhTU3hW8z/0mcBM2PkmmiJRNRvffxrEgYLry1/bPzqv3UEloVM2Wt
3mvQBFSnWGeLEtMTJy7jrZwv1r53vYfWF9QIt0J+RjYJgSjXvYnS0HQ4FtlreSRP
/ucmrFAasJ901Y4fiELdF91FJjC+NYC7
sVTU
-----END PGP MESSAGE-----

~/cifrado
+ 
```

**7. El fichero .asc ofrece las mismas garantías que el .gpg y se utiliza igual. Para descifrar sería:**

- *"gpg --decrypt mensaje.asc"*

```
~/cifrado
+ gpg --decrypt mensaje_cifrado.asc
gpg: datos cifrados ASCII
gpg: cifrado con 1 frase contraseña
You will be divorced within a year.

~/cifrado
+ 
```

8. La herramienta por defecto utiliza el algoritmo de cifrado **CAST5**. Podemos cambiarlo con el parámetro **cipher-alg**. Por ejemplo, para utilizar **AES** ejecutaríamos:

- *"gpg -a --symmetric --cipher-alg AES -o mensaje.aes mensaje"*
- En este ejemplo hemos utilizado **-a** para tener el fichero en ASCII y el parámetro **-o** para indicar el fichero de salida (es equivalente a redirigir la salida estándar).

```

jnav@Juan...

/cifrado
➤ gpg -a --symmetric --cipher-alg AES -o mensaje_cifrado_aes mensaje_cifrado

/cifrado took 4s
➤ ls
mensaje_cifrado  mensaje_cifrado_aes  mensaje_cifrado.asc  mensaje_cifrado.gpg  mensaje_descifrado

/cifrado
➤ cat mensaje_cifrado_aes
-----BEGIN PGP MESSAGE-----

A0EBwMCR0zGSci/ZCD/0mcBdXlXsBkJaLkPkcxawK/znmGaFJwH1RZgekW4tEu
NkW3+DaAwdzCvcP0Fd3zxN+LxP1tXKwmNmW6/JnTq1R09C0xn3spulvad/LZmWB
OfRsNIULsPeTSiSlQu8Uc0i1Cnz7kt3
T2Xl
-----END PGP MESSAGE-----

/cifrado
➤

```

9. El descifrado se hace como siempre:

- *"gpg --decrypt documento.aes"*
- Ahora, el mensaje de la pantalla nos avisa de que el fichero estaba cifrado con **AES** (ya no es **CAST5**).

```

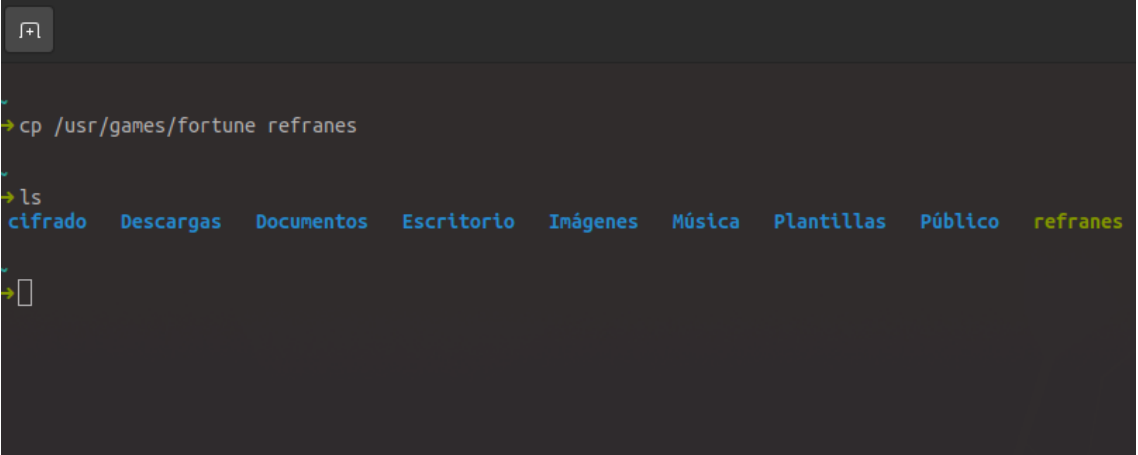
~/cifrado
➔ gpg --decrypt mensaje_cifrado_aes
gpg: datos cifrados AES
gpg: cifrado con 1 frase contraseña
You will be divorced within a year.

~/cifrado
➔

```

**10. Con esta herramienta podemos cifrar ficheros binarios, no solo ficheros de texto. Vamos a trabajar sobre una copia del propio ejecutable fortune y le llamaremos refranes. Los comandos serían:**

- `"cp /usr/games/fortune refranes"`
- `"./refranes"`



```
→ cp /usr/games/fortune refranes
→ ls
cifrado  Descargas  Documentos  Escritorio  Imágenes  Música  Plantillas  Público  refranes
→
```

**11. Lo ciframos en modo ASCII:**

- `"gpg -a --symmetric refranes"`

```

jnav@Juanca-PC:~$ gpg --symmetric refranes
gpg: data cifrados AES256
gpg: cifrado con 1 frase contraseña
El fichero 'dichos' ya existe. ¿Sobreescribir? (s/N) s

jnav@Juanca-PC:~$ cat refranes
Many enraged psychiatrists are inciting a weary butcher. The butcher is
weary and tired because he has cut meat and steak and lamb for hours and
weeks. He does not desire to chant about anything with raving psychiatrists,
but he sings about his gingivectomist, he dreams about a single cosmologist,
he thinks about his dog. The dog is named Herbert.
-- Racter, "The Policeman's Beard is Half-Constructed"

jnav@Juanca-PC:~$ gpg --decrypt -o dichos refranes.asc
gpg: datos cifrados AES256
gpg: cifrado con 1 frase contraseña
El fichero 'dichos' ya existe. ¿Sobreescribir? (s/N) s

jnav@Juanca-PC:~$ cat dichos
Many enraged psychiatrists are inciting a weary butcher. The butcher is
weary and tired because he has cut meat and steak and lamb for hours and
weeks. He does not desire to chant about anything with raving psychiatrists,
but he sings about his gingivectomist, he dreams about a single cosmologist,
he thinks about his dog. The dog is named Herbert.
-- Racter, "The Policeman's Beard is Half-Constructed"

jnav@Juanca-PC:~$ chmod 755 dichos

jnav@Juanca-PC:~$ ./dichos

```

## 12. Podemos recuperarlo descifrando el fichero refranes.asc con las opciones conocidas. Por ejemplo, podemos dejar el resultado en un nuevo fichero dichos. Después de introducir la contraseña, solo necesitamos darle permisos de ejecución y estará disponible. Los comandos son:

- `“gpg --decrypt -o dichos refranes.asc”`
- `“chmod 755 dichos”`

```

jnav@Juanca-PC:~$ gpg --decrypt -o dichos refranes.asc
gpg: datos cifrados AES256
gpg: cifrado con 1 frase contraseña
El fichero 'dichos' ya existe. ¿Sobreescribir? (s/N) s

jnav@Juanca-PC:~$ took 3s
jnav@Juanca-PC:~$ chmod 755 dichos

jnav@Juanca-PC:~$ ./dichos
Many enraged psychiatrists are inciting a weary butcher. The butcher is
weary and tired because he has cut meat and steak and lamb for hours and
weeks. He does not desire to chant about anything with raving psychiatrists,
but he sings about his gingivectomist, he dreams about a single cosmologist,
he thinks about his dog. The dog is named Herbert.
-- Racter, "The Policeman's Beard is Half-Constructed"

jnav@Juanca-PC:~$

```