

Cifrado simétrico con GnuPG

GnuPG es una implementación completa, gratuita y abierta de **OpenPGP**. Es un estándar para el cifrado en muchas distribuciones de Linux y se usa principalmente a través de la línea de comandos.

GnuPG no es una herramienta sofisticada de ninguna manera, y no podrá usarla para cifrar un disco duro completo o configurar una caja de seguridad. Aun así, si tiene algunos datos por ahí, o tal vez un mensaje para enviar, esta aplicación es imprescindible en Linux.

Características notables

- El cifrado de **GnuPG** admite múltiples algoritmos, como **RSA, ECDH, ECDSA, EdDSA, Elgamal, DSA, AES, Camellia, 3DES, Twofish, SHA2** y más.
- Es multiplataforma y se ejecuta en **Mac, Windows** y todos los sistemas similares a Unix como **Linux y BSD**.
- Se puede utilizar para encriptar comunicaciones o archivos de datos.



Instalación Linux

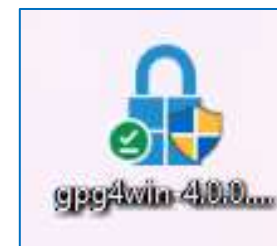
```
sudo apt update && sudo apt upgrade  
sudo apt-get install gnupg  
sudo apt-get install kleopatra
```

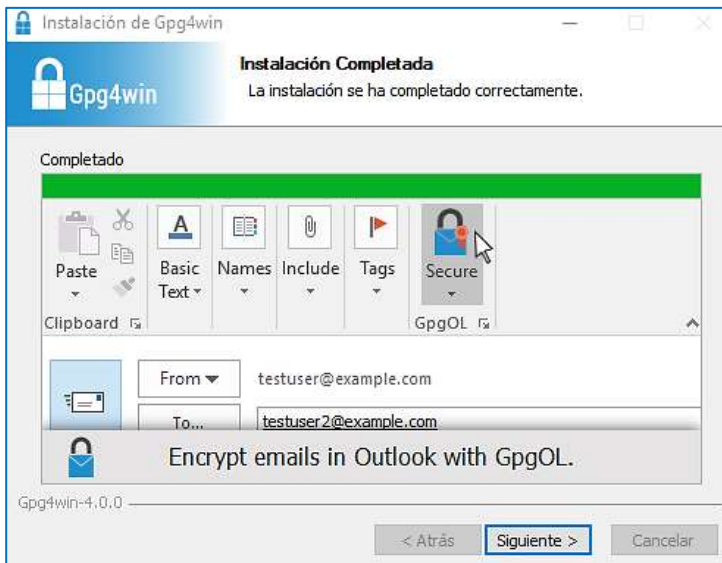
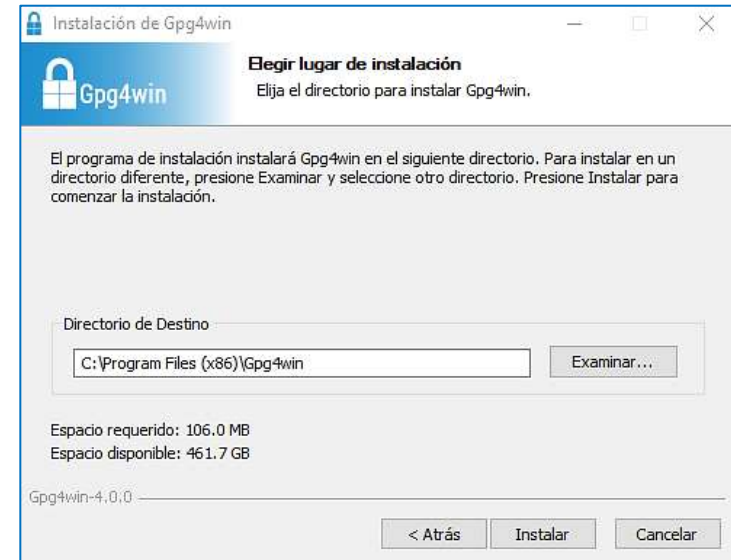
Instalación Windows

Gpg4win



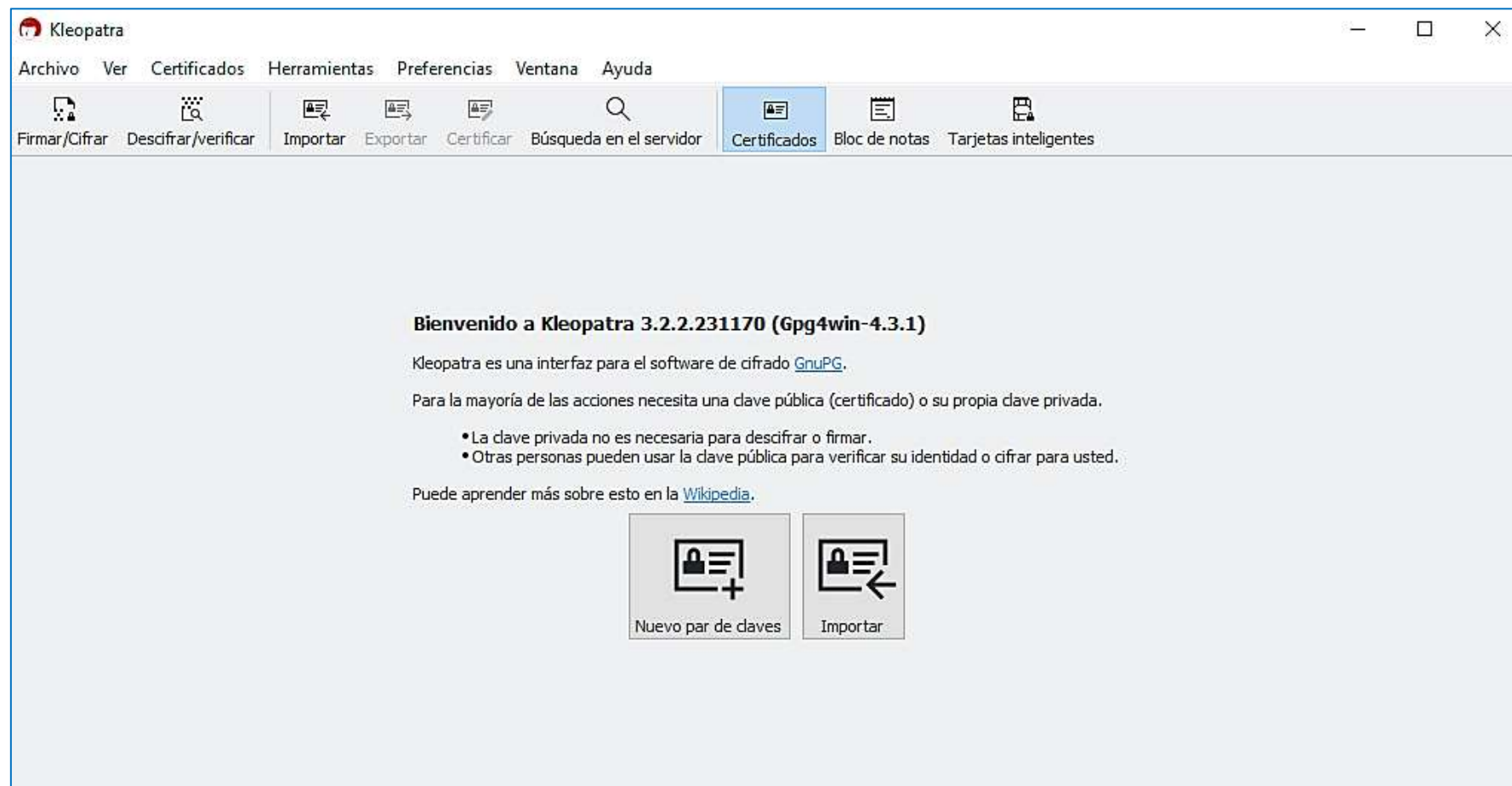
Comenzamos la instalación. Descargamos y ejecutamos el instalador:





Termina la instalación

Se abre el programa **Kleopatra**, La interfaz para el software de cifrado **GnuPG**:



Cifrar archivo (simétrico)

Linux

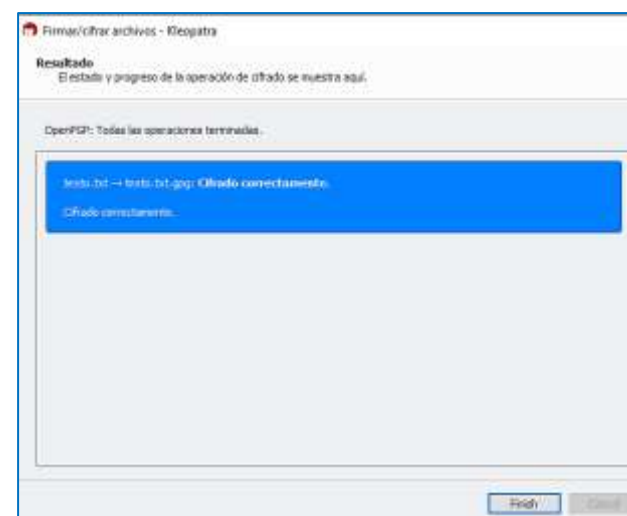
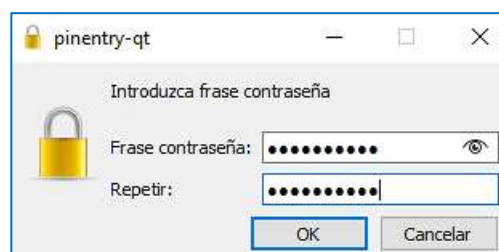
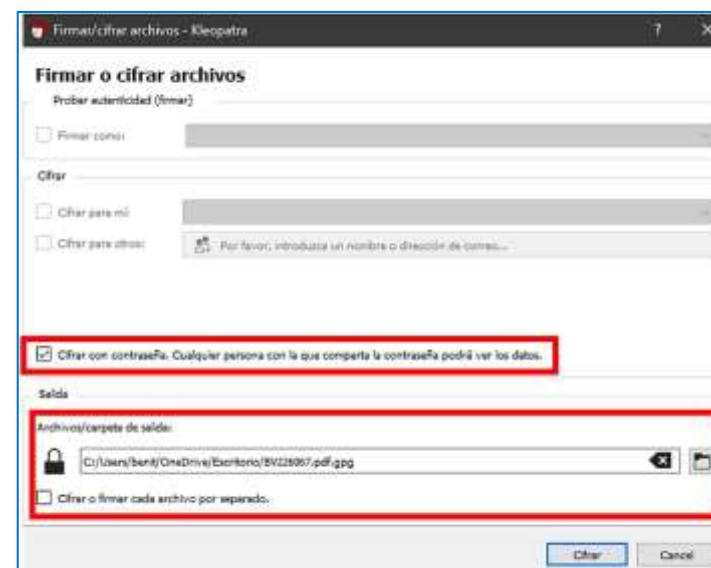
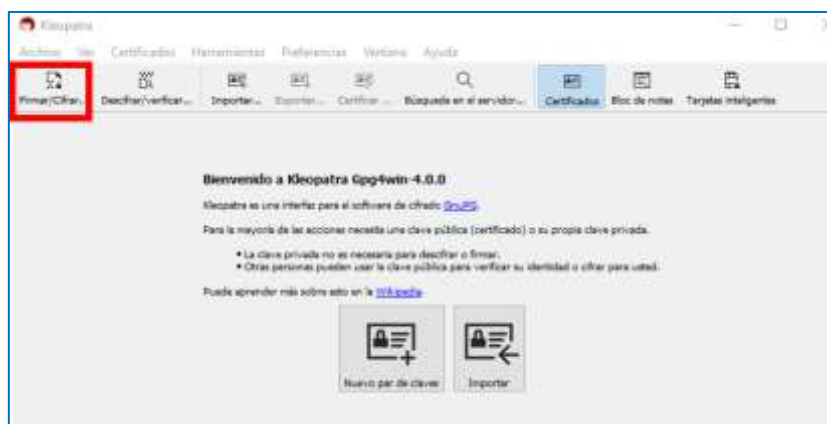
```
gpg -c texto.txt
```



Se ha generado el fichero cifrado **texto.txt.gpg**:

```
(kali㉿kali)-[~]  
$ ls texto*  
texto.txt  texto.txt.gpg  
  
(kali㉿kali)-[~]  
$ cat texto.txt.gpg  
h`kio1_<.B U & M, t}< j; l T8 PWe x  
D b f > ! HE ) Z . j :  
| 3 j { { 9 Z [ ~ ] s a 4 ' A , d S ( 1 ; 1 2  
P ( & l n d * R 3 L ! V M k NSG  
2 . e o : = 6 @
```

Windows (Gp4win. Kleopatra):



Descifrar archivo (simétrico)

Linux

```
gpg -d texto.txt.gpg > texto.descifrado
```



```
(pru@kali)-[~]
$ gpg -d texto.txt.gpg > texto.descifrado
gpg: datos cifrados AES256.CFB
gpg: cifrado con 1 frase contraseña
```

```
(pru@kali)-[~]
$ cat texto.descifrado
```

En un lugar de la Mancha, de cuyo nombre no quiero acordarme, no ha mucho tiempo que vivía un hidalgo de los de lanza en astillero, adarga antigua, rocín flaco y galgo corredor.

Windows (Gp4win. Kelopatra)

