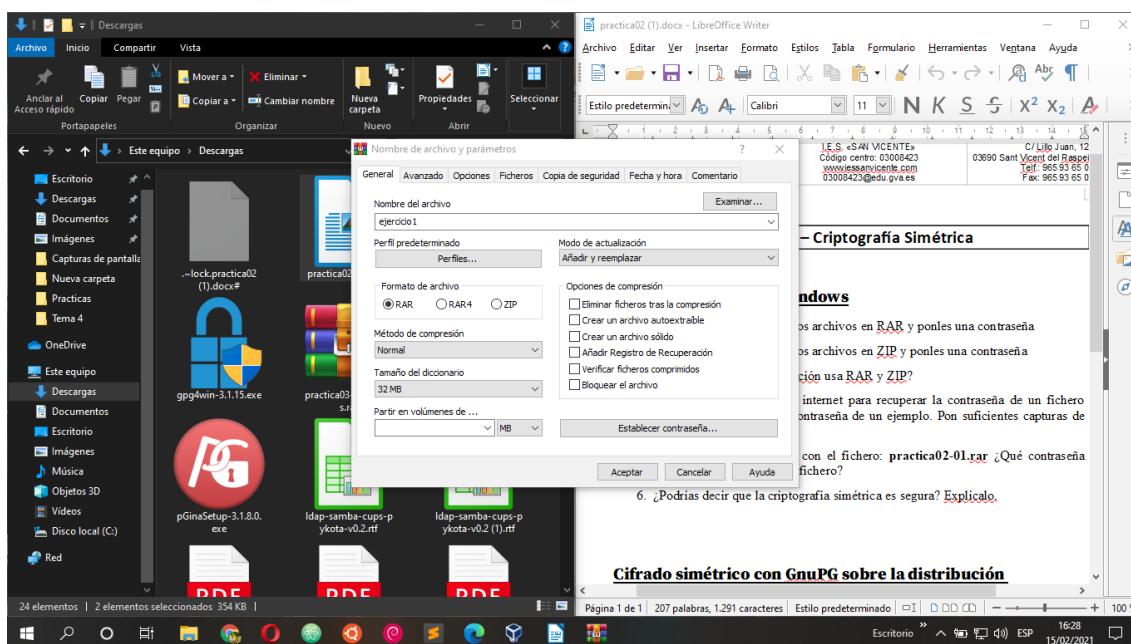
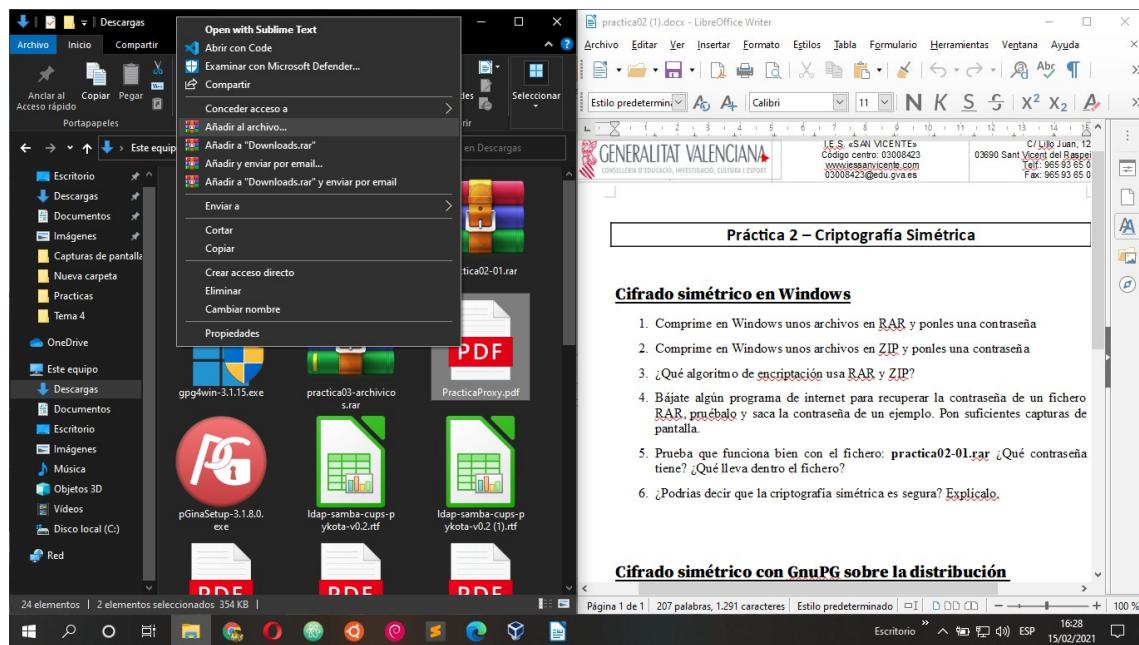
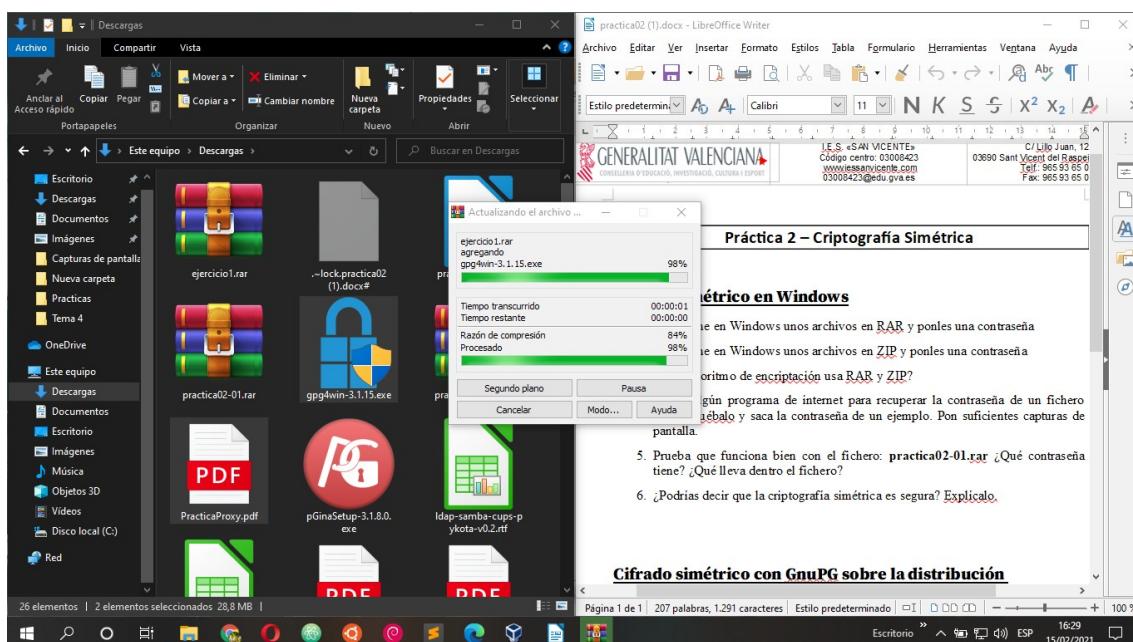
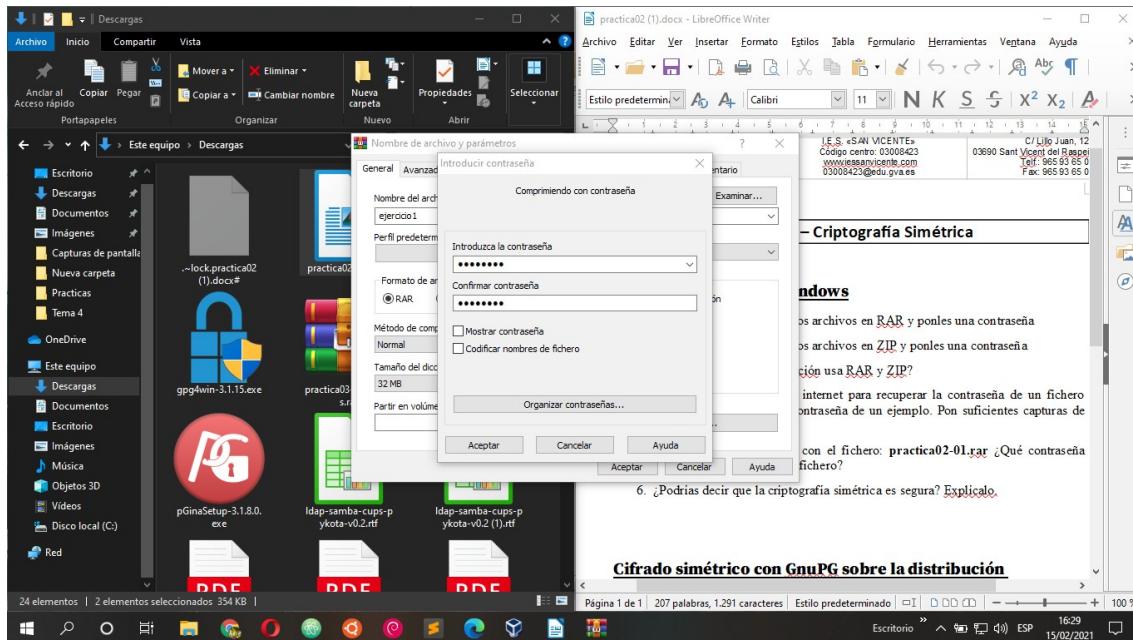


Práctica 2 – Criptografía Simétrica

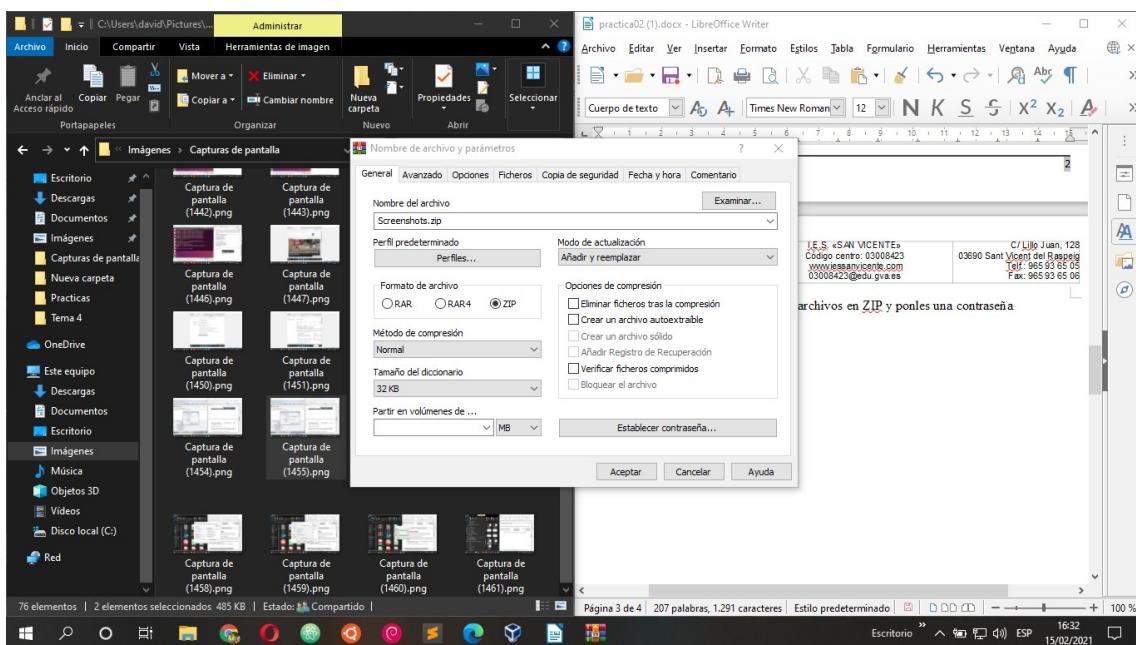
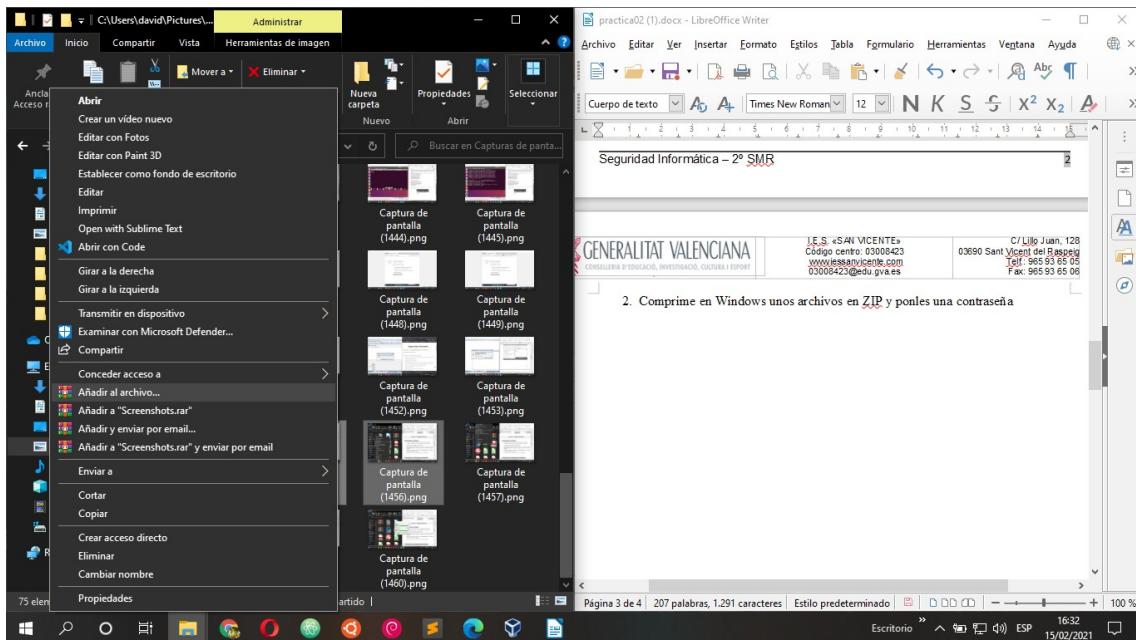
Cifrado simétrico en Windows

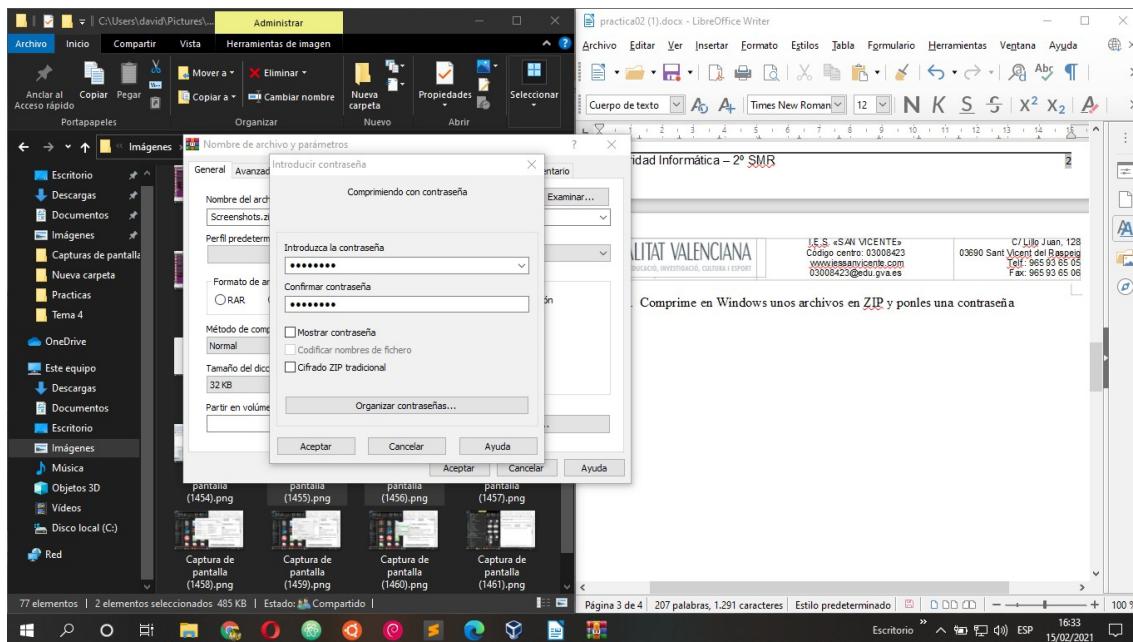
1. Comprime en Windows unos archivos en RAR y ponles una contraseña





2. Comprime en Windows unos archivos en ZIP y ponles una contraseña



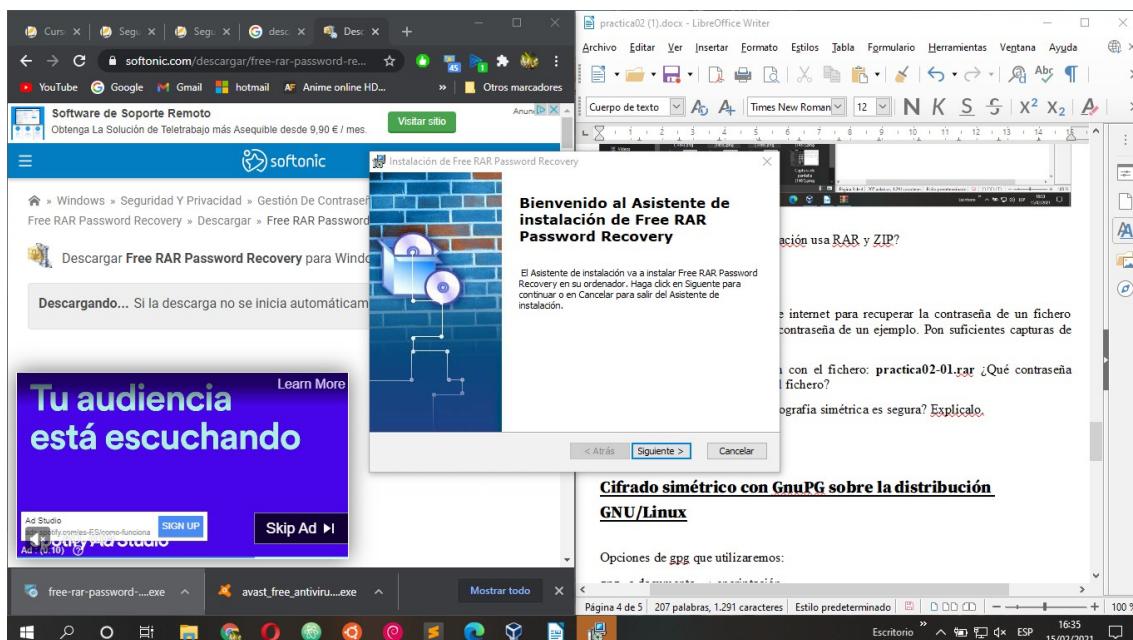


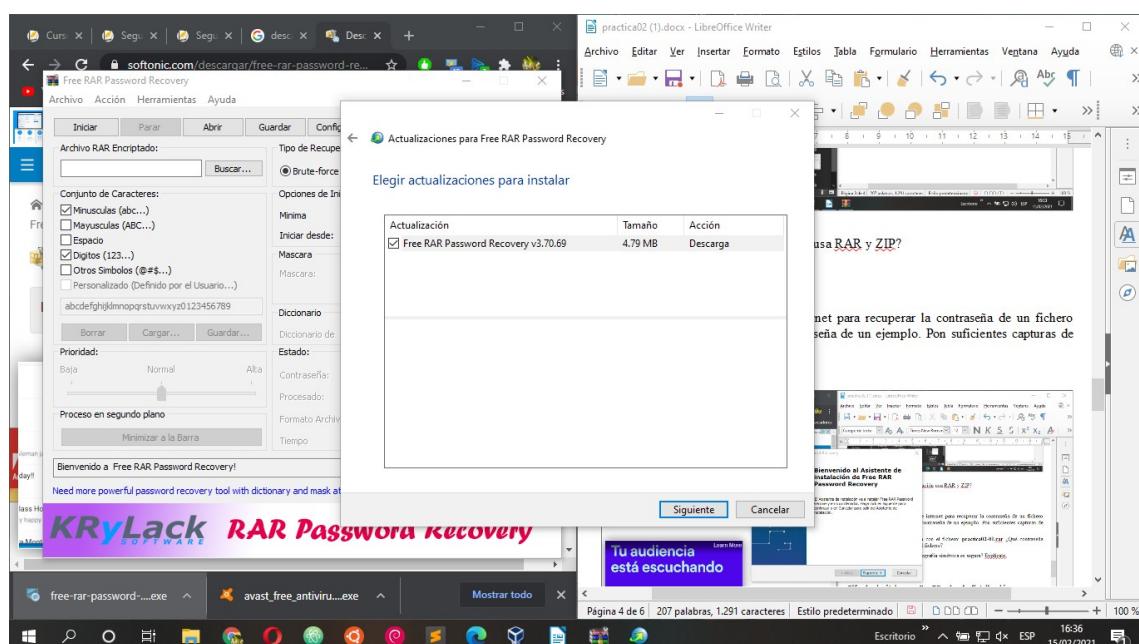
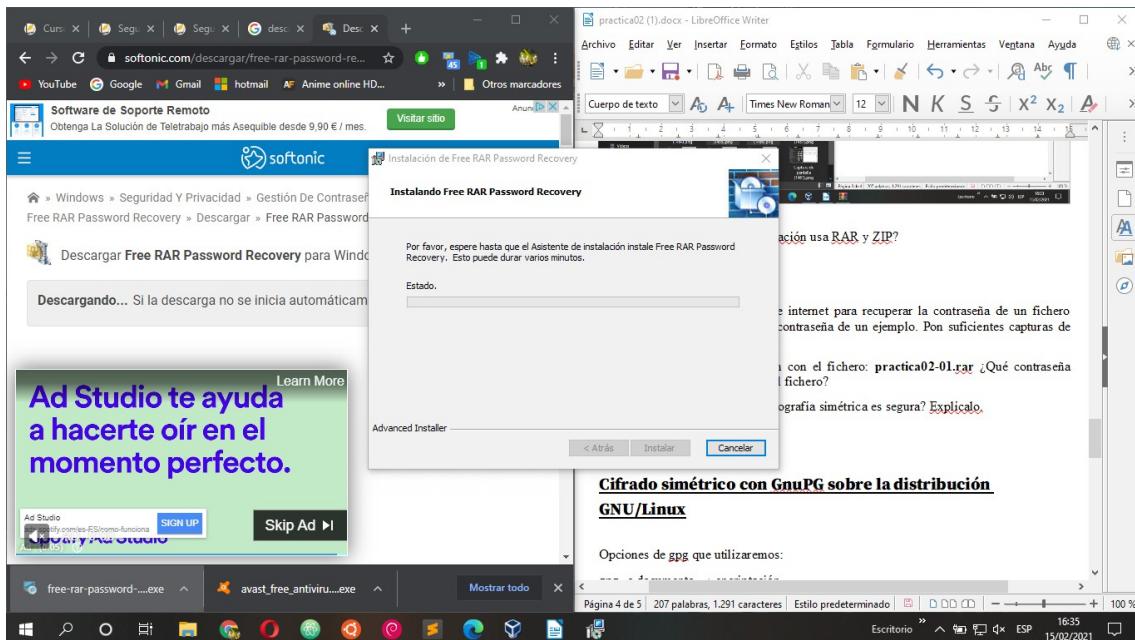
3. ¿Qué algoritmo de encriptación usa RAR y ZIP?

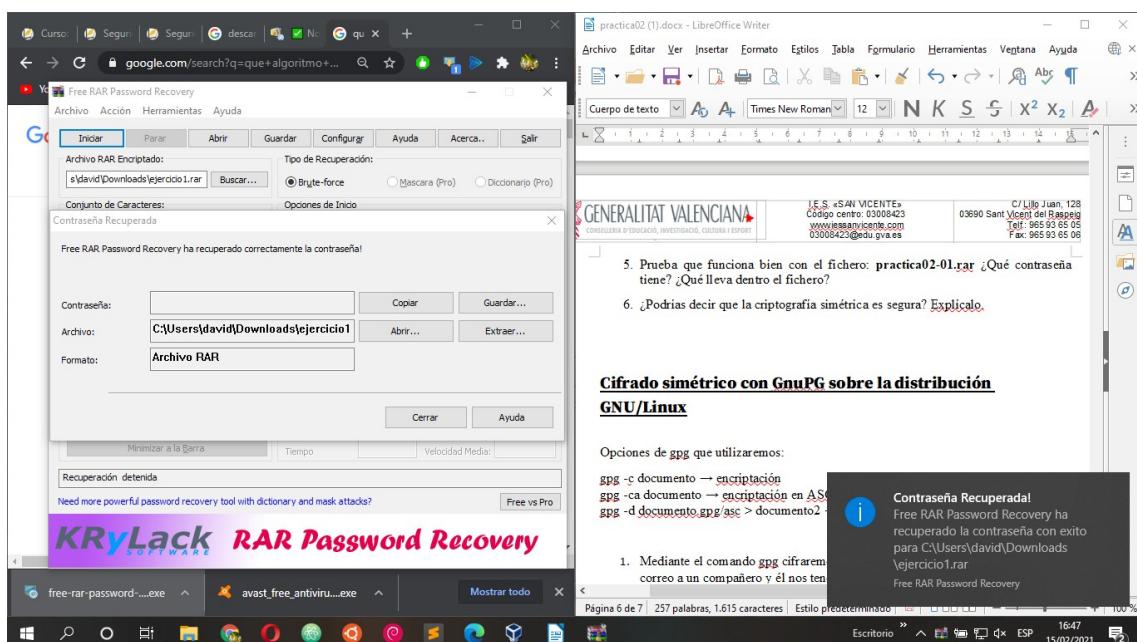
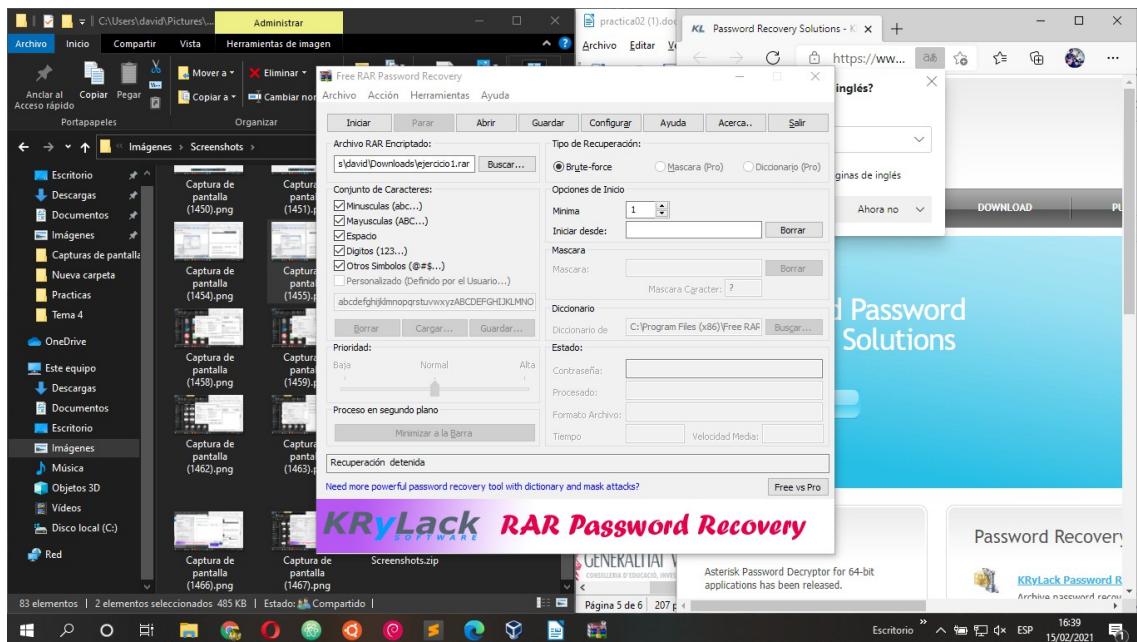
Por defecto, WinRAR usa AES-256 en modo CTR para cifrar archivos ZIP. Aunque AES-256 es significativamente más seguro que el algoritmo de cifrado ZIP 2.0 tradicional, puede ser incompatible con algunas herramientas antiguas.

Cifrado basado en el algoritmo AES-256, que es teóricamente más seguro que el AES-128 del RAR 4.x.

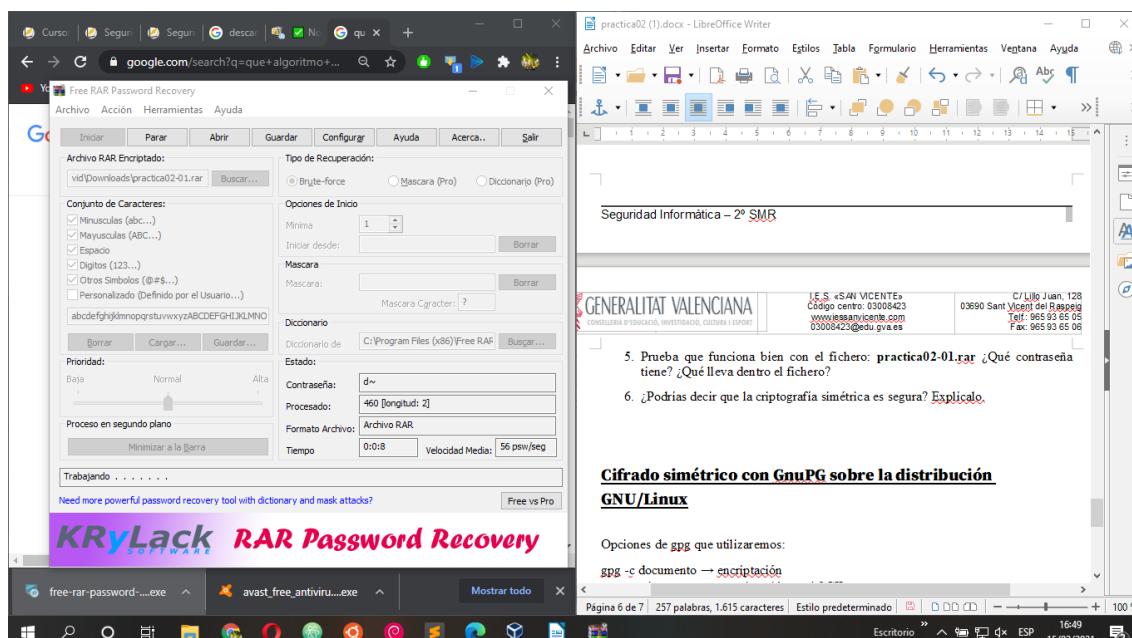
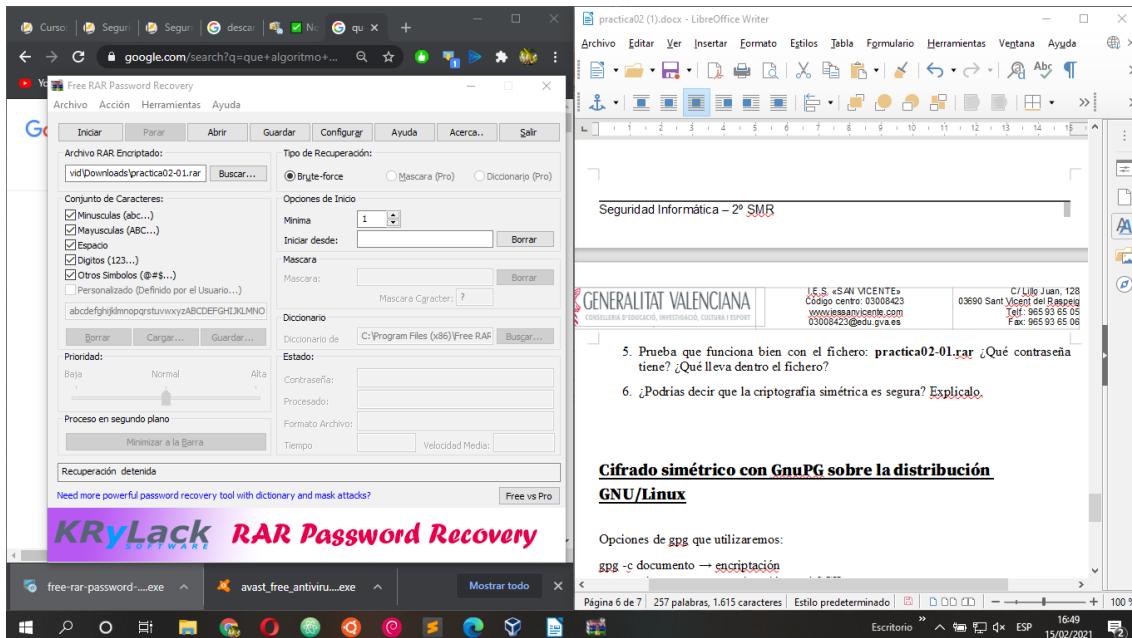
4. Bájate algún programa de internet para recuperar la contraseña de un fichero RAR, pruébalo y saca la contraseña de un ejemplo. Pon suficientes capturas de pantalla.

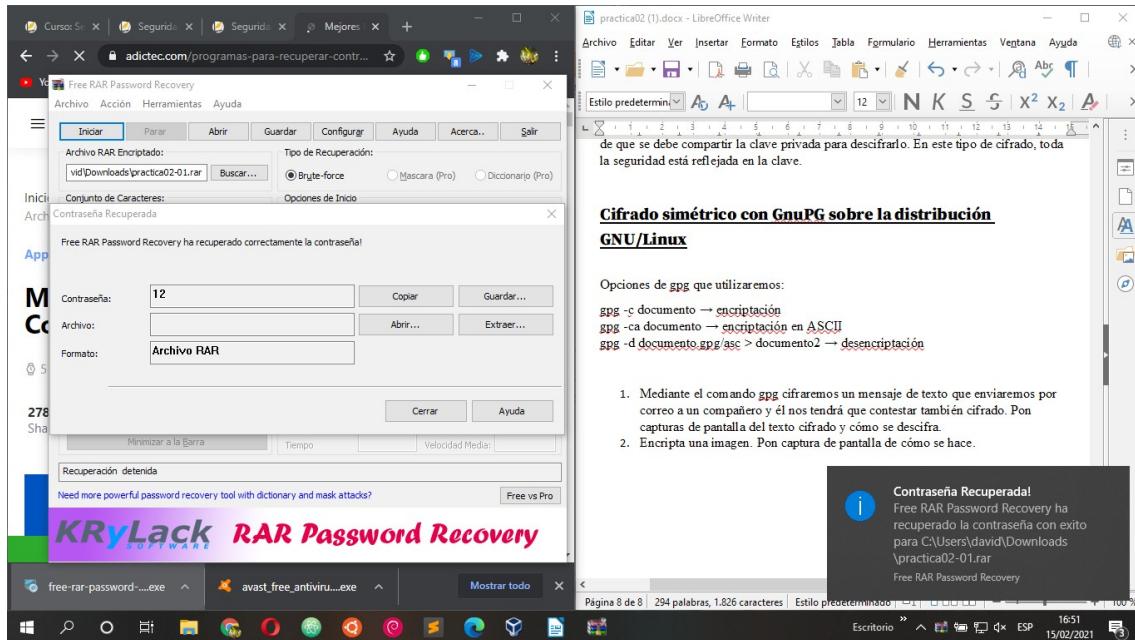






5. Prueba que funciona bien con el fichero: **practica02-01.rar** ¿Qué contraseña tiene? ¿Qué lleva dentro el fichero?



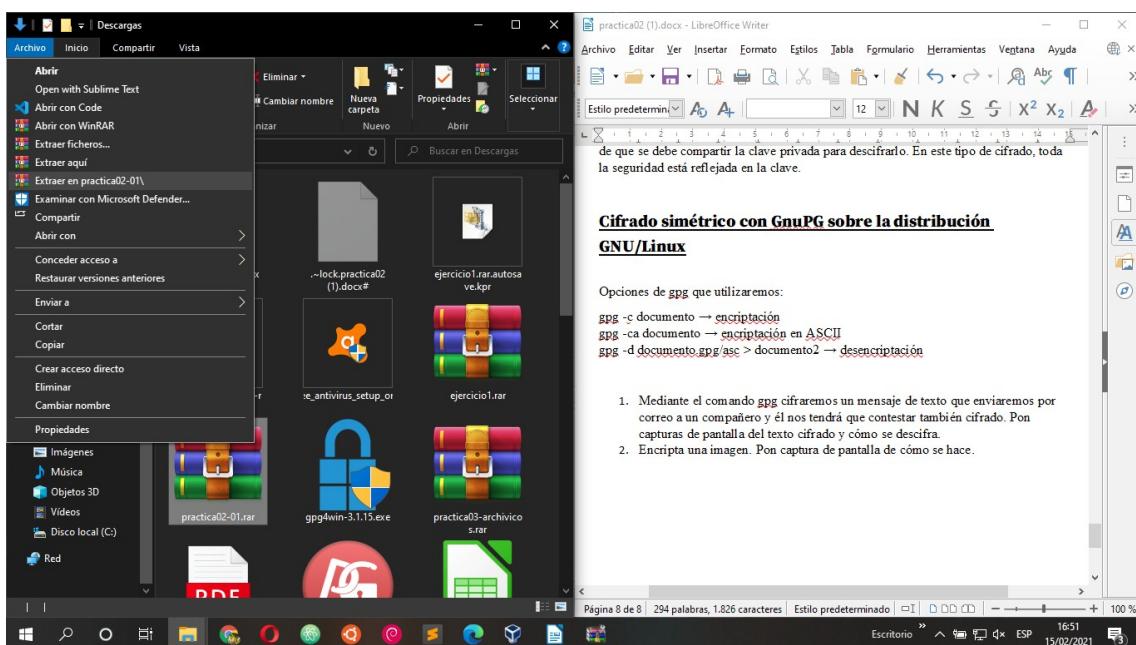


Cifrado simétrico con GnuPG sobre la distribución GNU/Linux

Opciones de gpg que utilizaremos:

gpg -c documento → **encriptación**
 gpg -ca documento → **encriptación en ASCII**
 gpg -d documento.gpg/asc > documento2 → **desencriptación**

1. Mediante el comando gpg cifaremos un mensaje de texto que enviaremos por correo a un compañero y él nos tendrá que contestar también cifrado. Pon capturas de pantalla del texto cifrado y cómo se descifra.
2. Encripta una imagen. Pon captura de pantalla de cómo se hace.

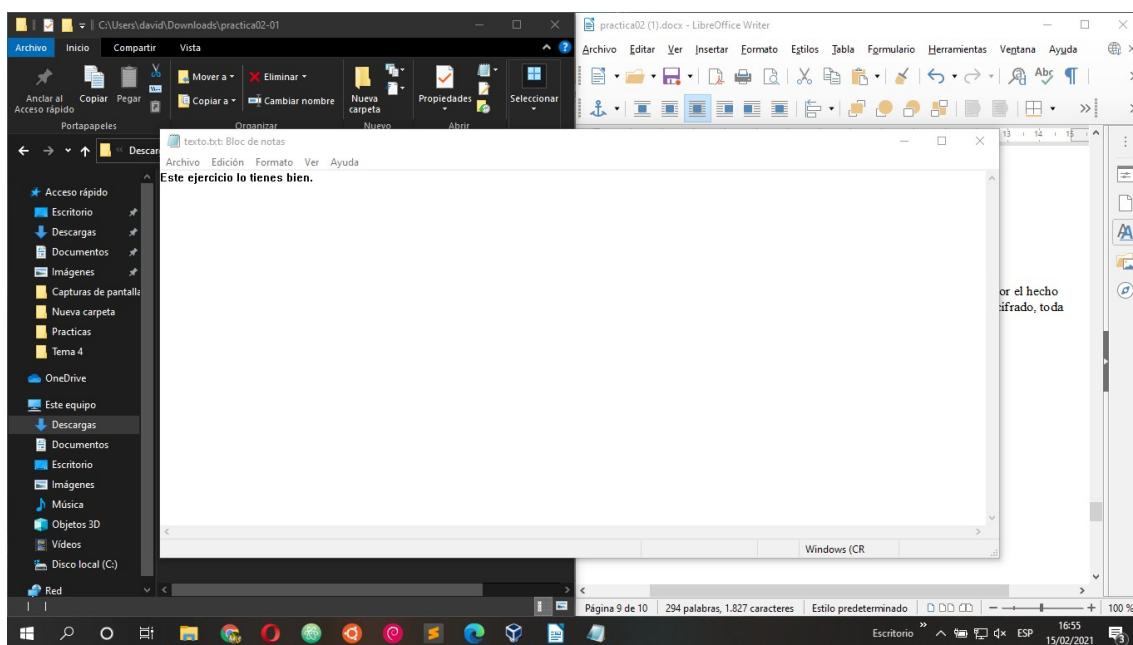
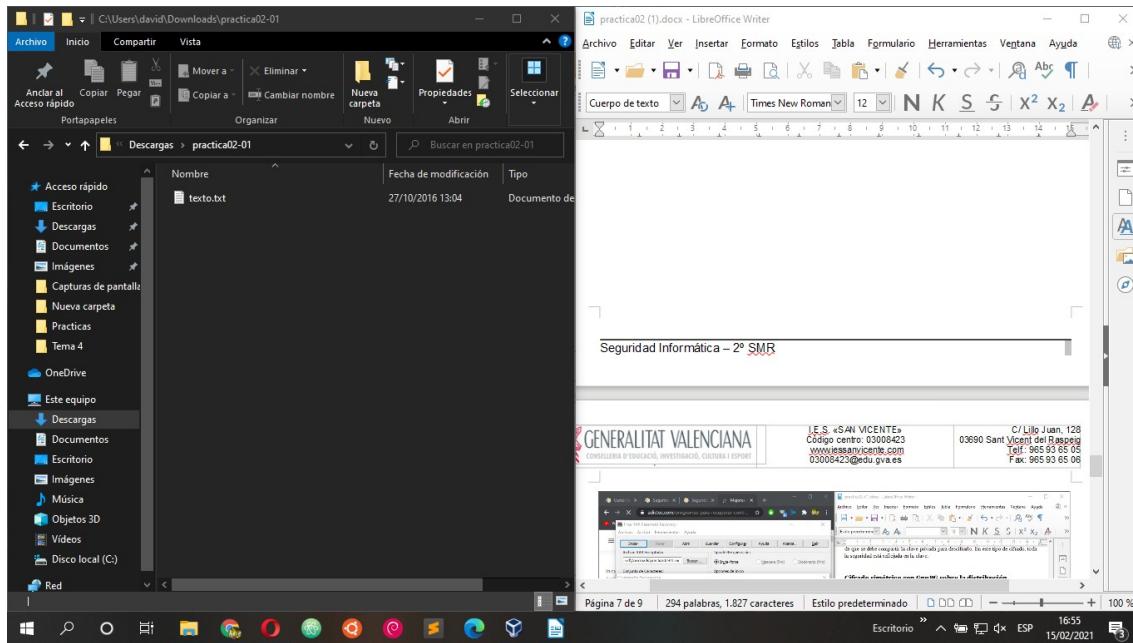


Cifrado simétrico con GnuPG sobre la distribución GNU/Linux

Opciones de gpg que utilizaremos:

gpg -c documento → **encriptación**
 gpg -ca documento → **encriptación en ASCII**
 gpg -d documento.gpg/asc > documento2 → **desencriptación**

1. Mediante el comando gpg cifaremos un mensaje de texto que enviaremos por correo a un compañero y él nos tendrá que contestar también cifrado. Pon capturas de pantalla del texto cifrado y cómo se descifra.
2. Encripta una imagen. Pon captura de pantalla de cómo se hace.



6. ¿Podrías decir que la criptografía simétrica es segura? Explícalo.

En términos de seguridad, el cifrado simétrico no es tan confiable por el hecho de que se debe compartir la clave privada para descifrarlo. En este tipo de cifrado, toda la seguridad está reflejada en la clave.

Cifrado simétrico con GnuPG sobre la distribución GNU/Linux

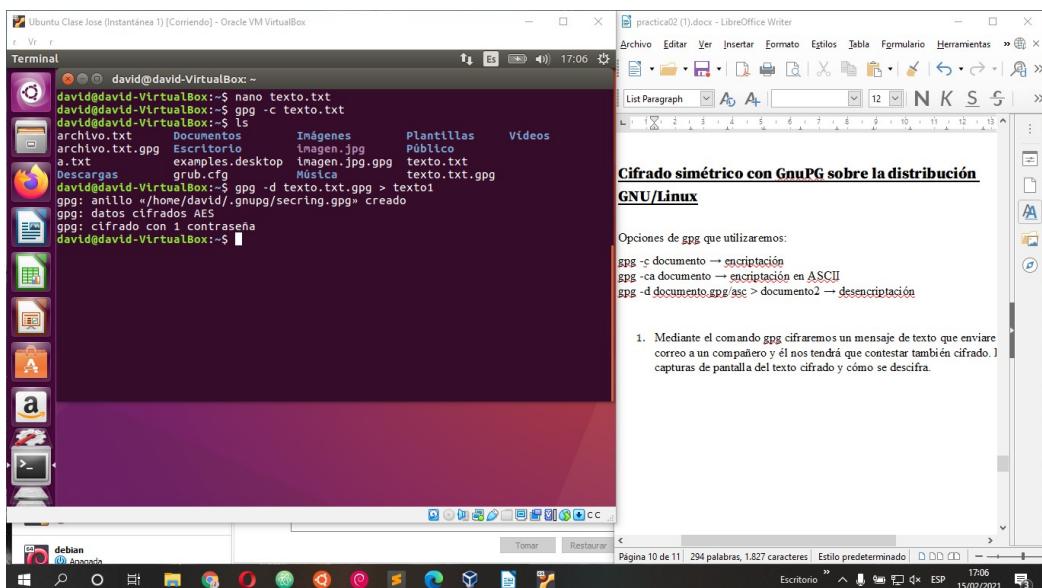
Opciones de gpg que utilizaremos:

gpg -c documento → encriptación

gpg -ca documento → encriptación en ASCII

gpg -d documento.gpg/asc > documento2 → desencriptación

1. Mediante el comando gpg cifraremos un mensaje de texto que enviaremos por correo a un compañero y él nos tendrá que contestar también cifrado. Pon capturas de pantalla del texto cifrado y cómo se descifra.



2. Encripta una imagen. Pon captura de pantalla de cómo se hace.

