

CIFRADO SIMETRICO EN WINDOWS



Juan Carlos Navidad García
Seguridad Informática

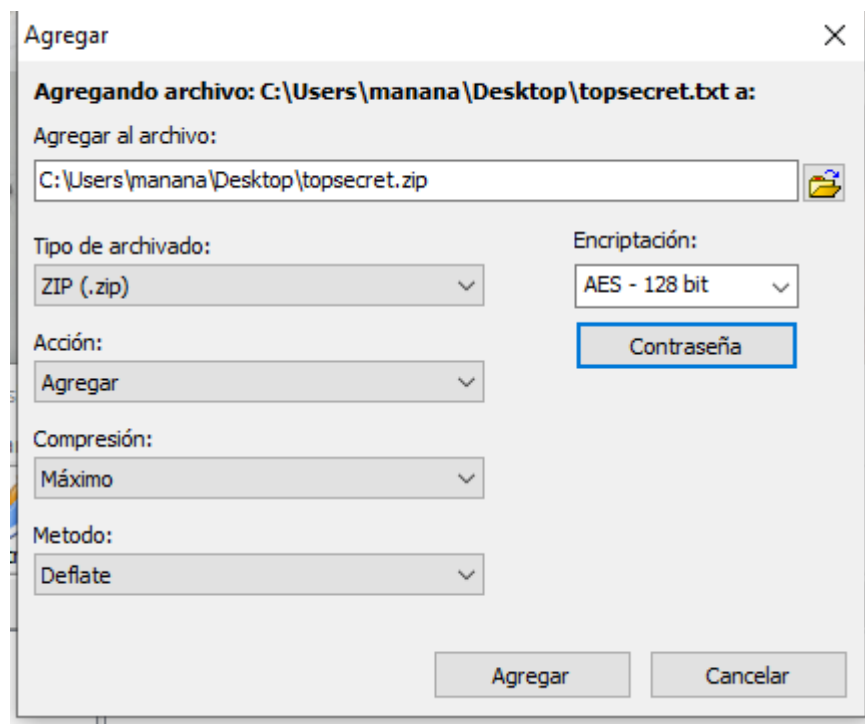
1. Cifrar de manera simétrica en Windows:

1. En un ordenador con Windows descargamos la herramienta de la web oficial IZArc. Realmente es un compresor de ficheros, pero como además tiene la opción de cifrar el fichero comprimido, podemos utilizarlo para las dos cosas. Por ejemplo, podemos cifrar muchos ficheros, incluso una estructura de carpetas, en un solo fichero fácil de transportar.

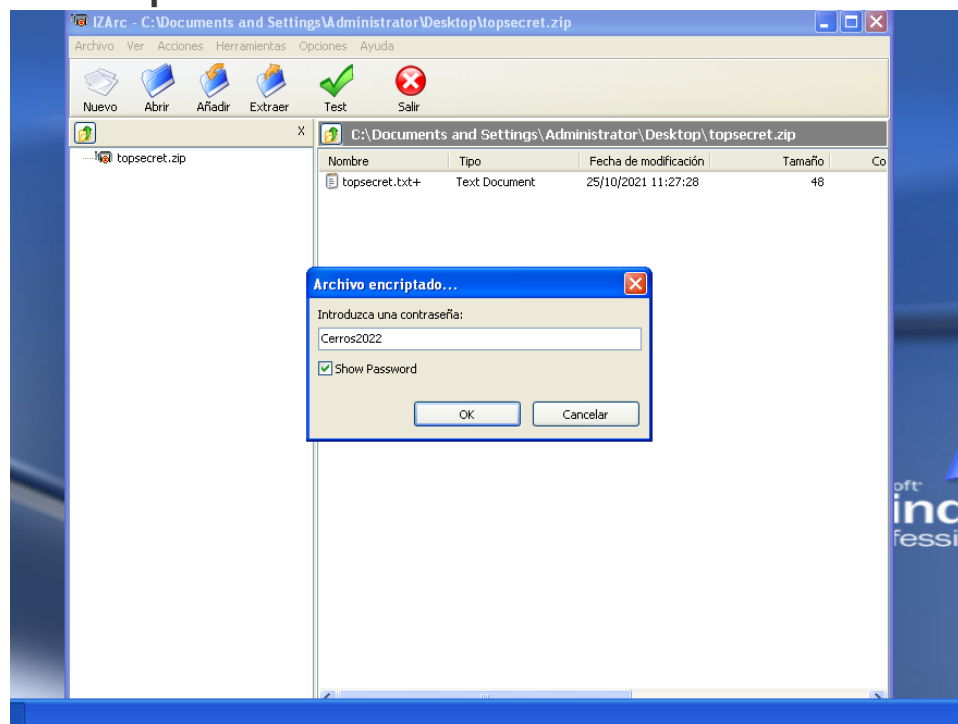


2. Durante la instalación nos indicará qué tipos de cifrado queremos manejar con IZArc. Están los habituales (.zip,.rar) y algunos interesantes (.tar, .7z).

3. Una vez instalado, podemos situarnos sobre cualquier fichero o carpeta y acceder al menú del botón derecho. En este ejemplo hemos creado el fichero de texto top secret y en la opción IZArc elegiremos la operación Agregar a top secret.zip (el nombre se genera automáticamente). Aparecerá la ventana de la herramienta, donde podremos elegir el algoritmo de encriptación. En nuestro caso será AES de 128bits.
4. La opción por defecto es None porque estamos trabajando con un programa que es fundamentalmente un compresor de ficheros. En encriptación lo ponemos como AES – 128 bit y terminaremos pulsando en Agregar. En ese momento nos preguntará la clave que queremos utilizar en el cifrado. La preguntará una segunda vez para confirmar que la hemos tecleado bien. Si es así, estará disponible el fichero cifrado topsecret.zip.



5. Ese fichero .zip lo podemos llevar a otra máquina que también tenga IZArc y descifrarlo allí (en este ejemplo, un XP). Nos situamos sobre el fichero .zip y desde el menú del botón derecho recuperamos los ficheros pulsando en Extract Here.
6. Nos preguntará la clave. Si la introducimos bien, habremos conseguido el fichero de texto que almacenaba el fichero **zip**.



Finalmente, se descomprime:

