
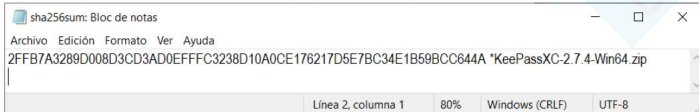


Cifrado ficheros, simétrico y asimétrico

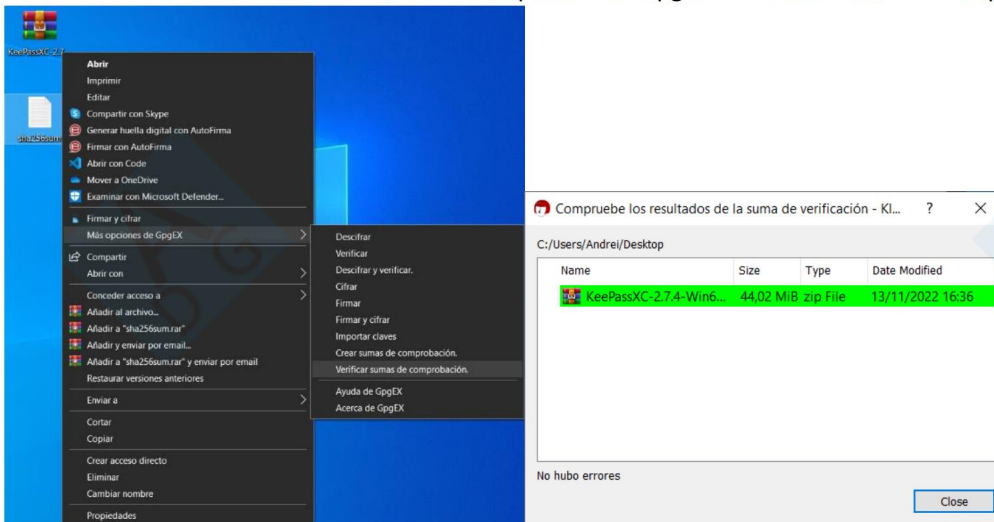
A.D.G.

1) Verificación CRC ficheros de KeePassXC (por ejemplo):

- 1) Entro a la página de descarga de KeePassXC versión Windows: keepassxc.org/download/#windows
- 2) Descargo la versión:  [Portable ZIP archive](#)
- 3) Descargo el algoritmo de hash SHA256: [# SHA-256 digest](#)
- 4) Cambio el nombre y formato del archivo anterior de *KeePassXC-2.7.4-Win64.zip.DIGES* a *sha256sum.txt*
- 5) Dentro, parece ser que hay que añadir una nueva línea para que logre entenderlo/detectarlo al menos en Kleopatra.

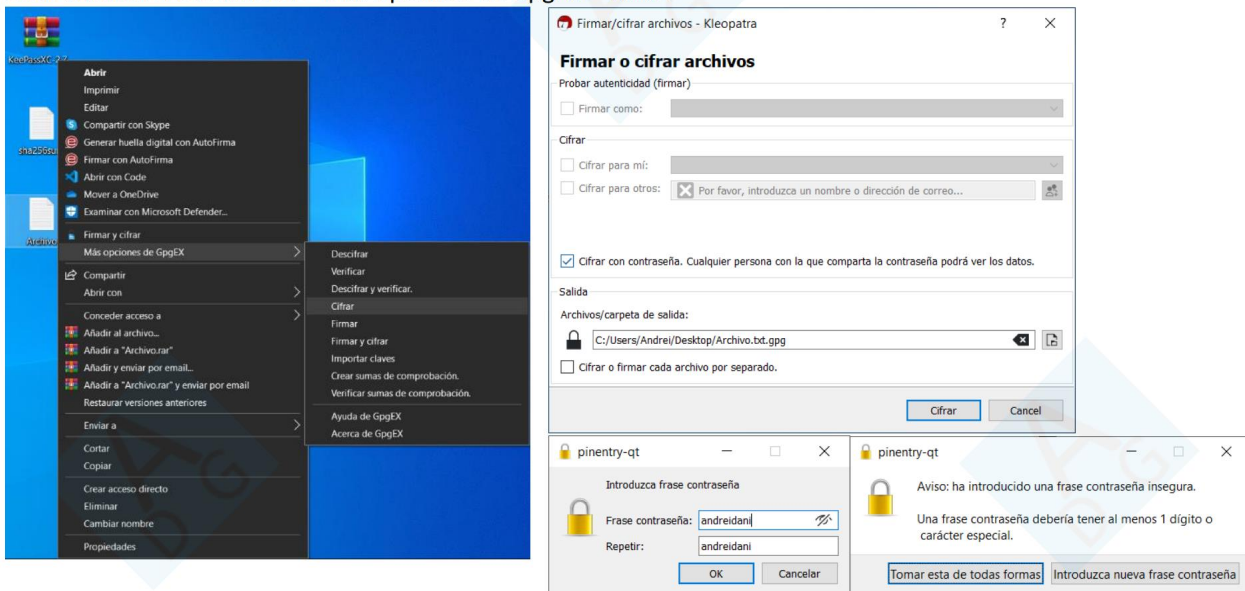


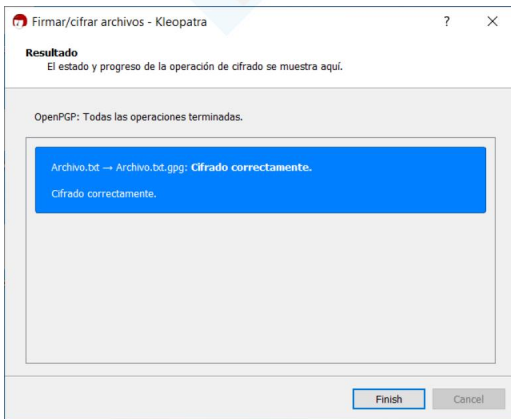
- 6) Click derecho al archivo *sha256sum.txt* > Más opciones de GpgEX > Verificar sumas de comprobación:



2) Crear un archivo de cifrado simétrico:

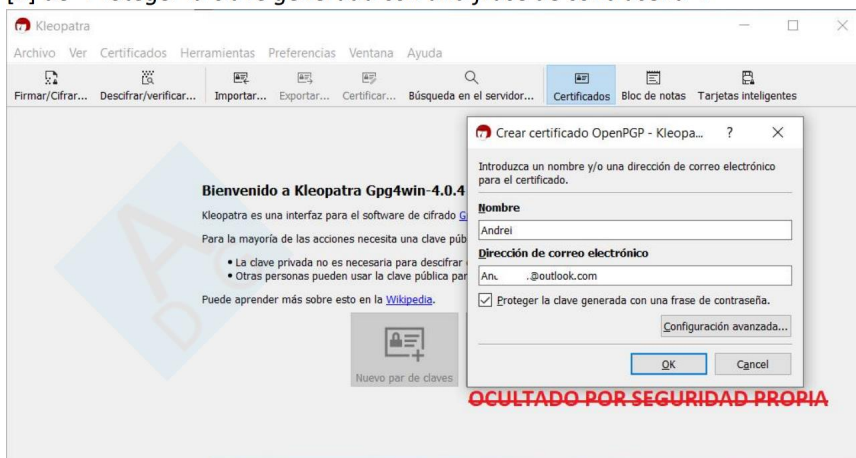
- 1) Creo un archivo cualquiera (Archivo.txt mismamente)
- 2) Click derecho a ese archivo > Más opciones de GpgEX > Cifrar:



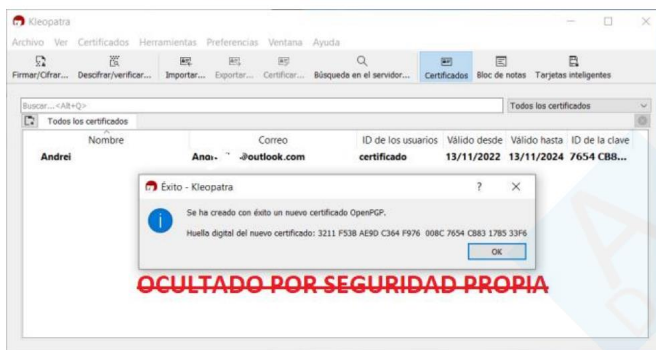
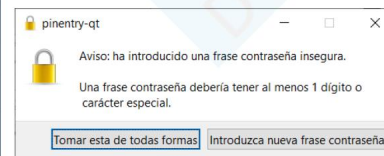
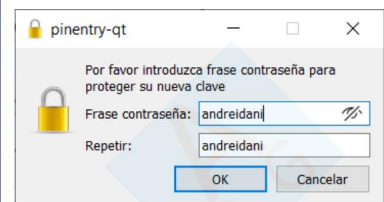


3) Crear claves:

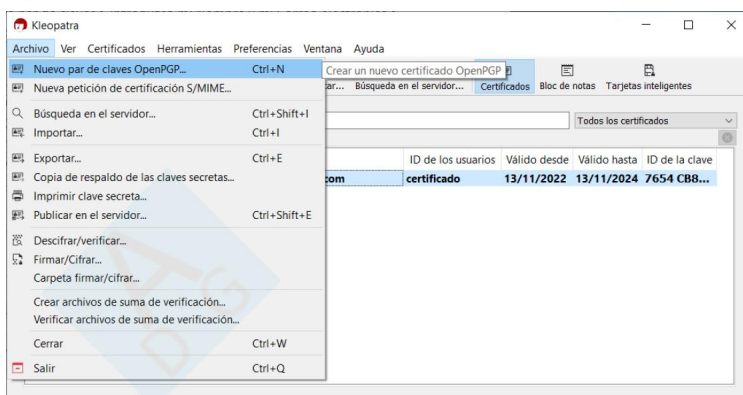
- 1) Entro en Kleopatra > Certificados > Nuevo par de claves > introduzco mi Nombre y mi Correo electrónico > Seleccionar la casilla [X] de "Proteger la clave generada con una frase de contraseña".



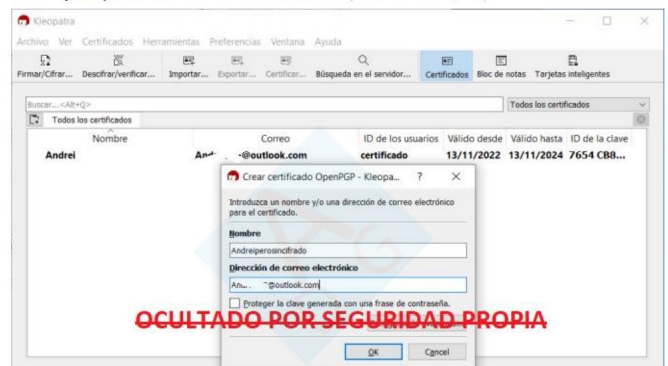
Así ya de paso la dejamos más protegida y cifrada simétricamente:



Ahora creamos otra, para tener varias claves como pide el enunciado, esta vez dirigiéndonos a Archivo > Nuevo par de claves OpenPGP:



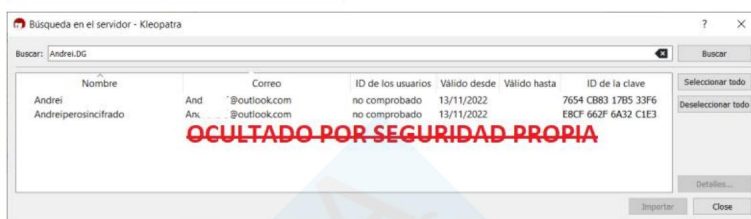
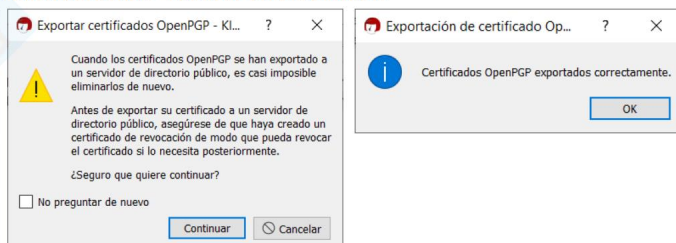
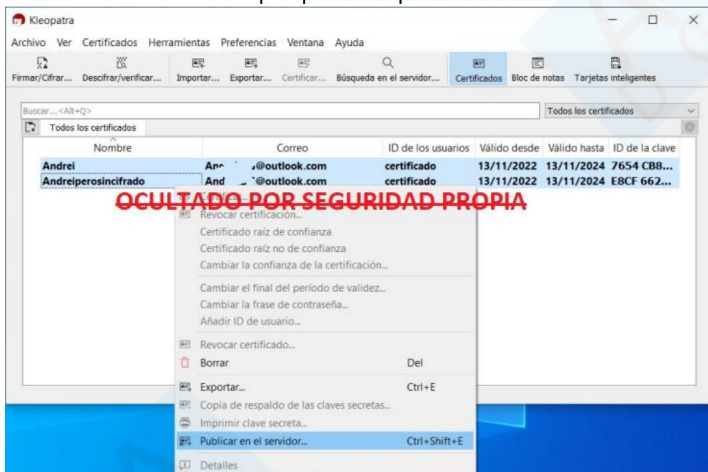
Por ejemplo, sin cifrado simétrico (sin casilla [X]):



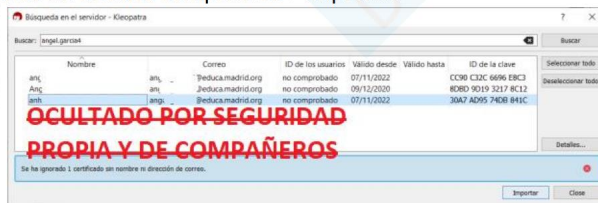


4) Exportar al servidor las claves, e Importar del servidor una clave de unos compis:

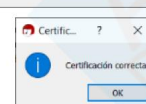
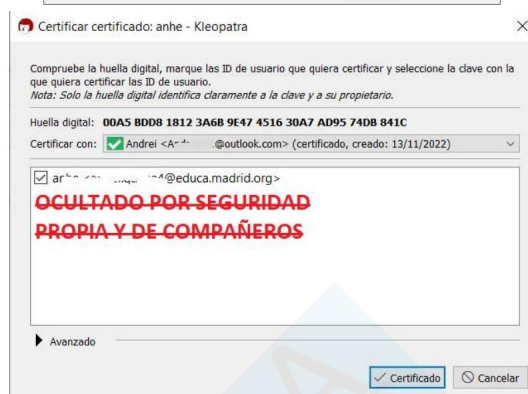
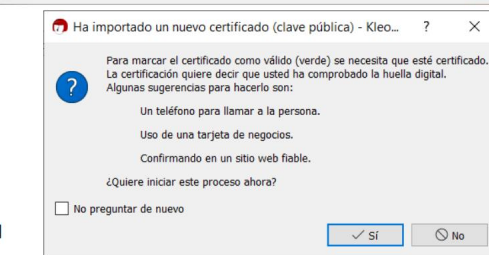
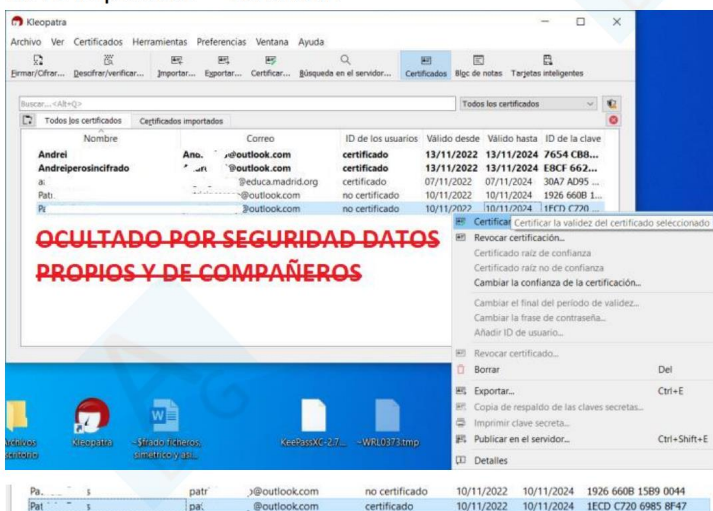
- 1) Seleccionamos las claves que queremos publicar en el servidor con CTRL > Click derecho > Publicar en el servidor:



- 2) Click en Búsqueda en el servidor, introduzco algunos datos para encontrarles las de unos compañeros > Importar:



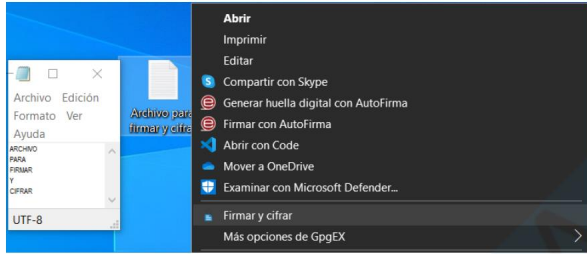
En la primera importación para Patricia, no me ha solicitado nada y por tanto el ID de usuario me aparece como "no certificado". Puedo hacer el certificado con Click derecho en su clave importada > Certificar:



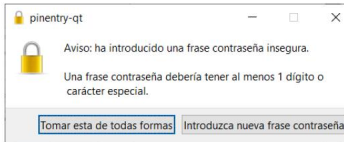
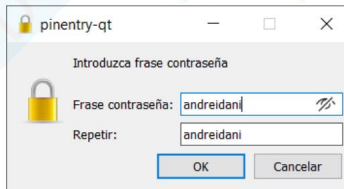
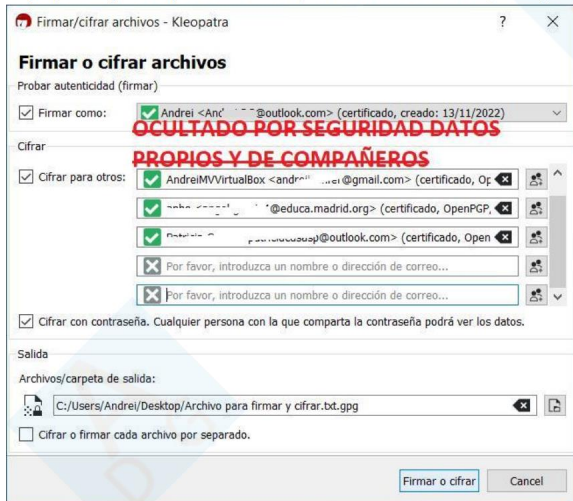
Pedía la clave nuestra después de este paso <

5) Firmar y cifrar fichero para varios compañeros:

- 1) Creo un archivo de texto por ejemplo > Click derecho > Firmar y cifrar:

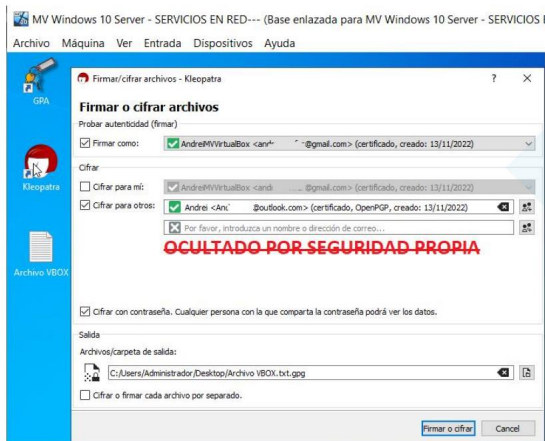


- 2) Elijo para quién quiero firmar y cifrar ese archivo (incluyo otra mía de una máquina virtual para la siguiente tarea):

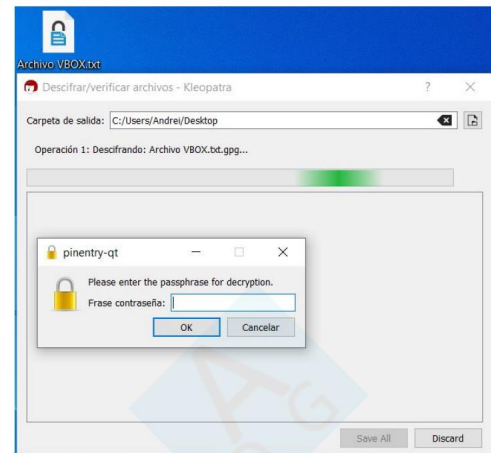
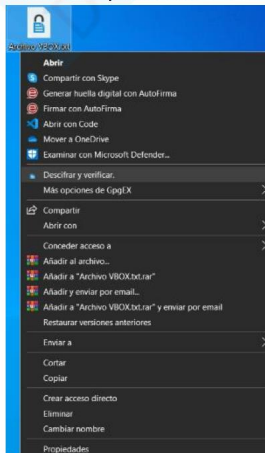


6) Verificación del fichero de otra persona (de la cuenta de mi VirtualBox):

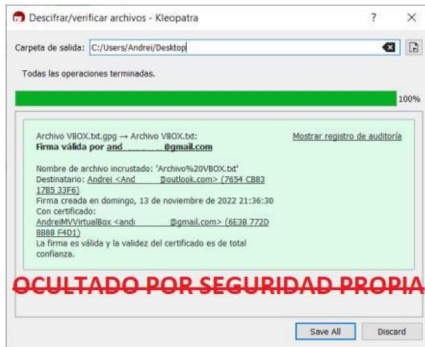
- 1) Simulo crear un archivo cifrado y firmado en VirtualBox para mandarmelo a mí (para poder volver a usarlo esa persona con clave de VirtualBox tendría que seleccionar "Cifrar para mí" también, pero como es una prueba solamente lo dejo sólo para otros que es como se pide:



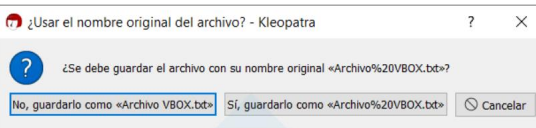
- 2) Con el archivo copiado desde la máquina a mi Windows, hago Click derecho > Descifrar y verificar > Y se introduce la contraseña:



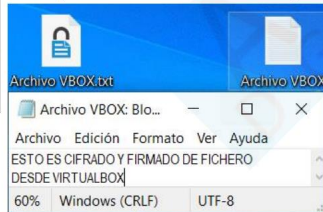
Y tendremos el mensaje de que ha sido correcta la firma y el descifrado. Le damos a “Save All” para guardarlo.



Lo guardamos como “Archivo VBox.txt” para no salirnos con caracteres distintos a lo que se tenía originalmente (por el tema del espacio):

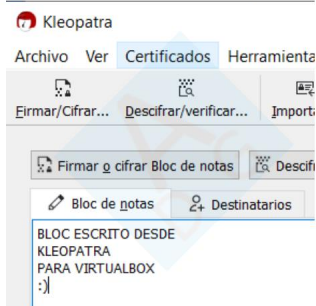


Y aquí tenemos el resultado, el documento de texto de VirtualBox que previamente se cifró y firmó:

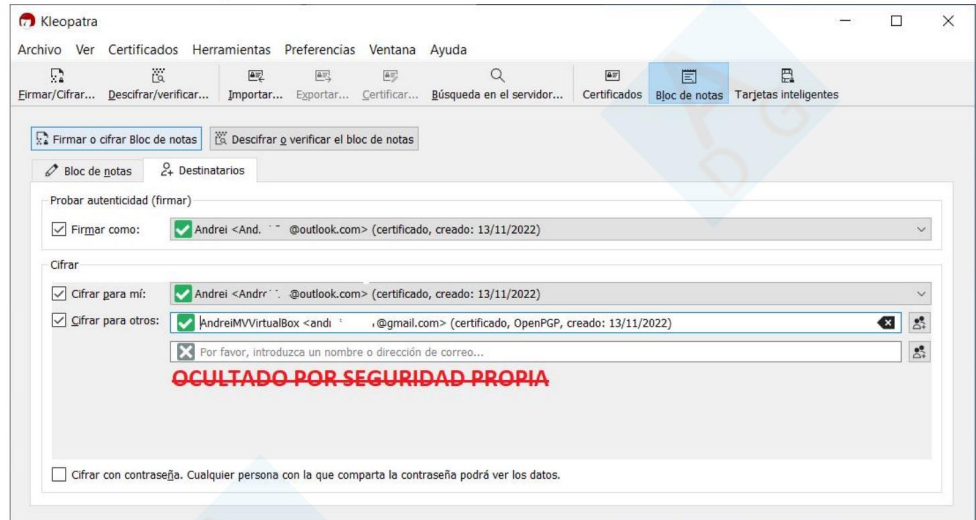


7) Enviar fichero a otra persona (a la máquina Virtual otra vez vale)

1) Creo el archivo, también puedo desde Kleopatra para crear documentos de texto clickando en Bloc Notas:



2) En Destinatarios se dejaría sin seleccionar lo de “Cifrar con contraseña” para ser asimétrico.



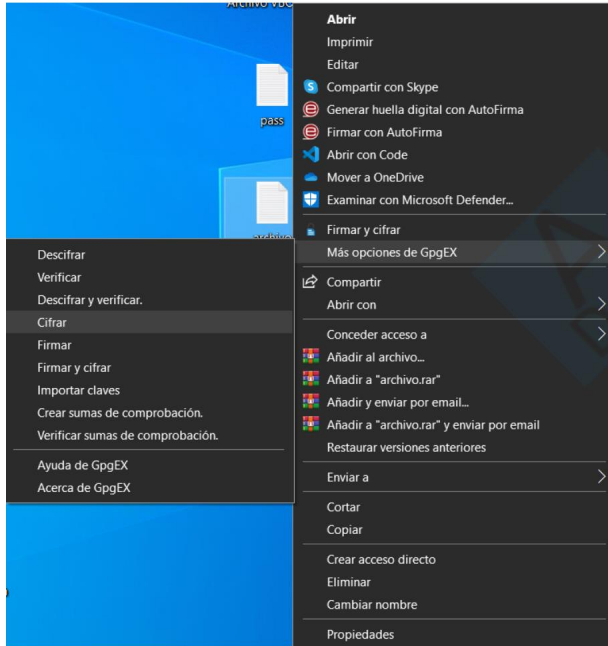
Se introduciría la contraseña que se tendrá que usar para descifrar el archivo (ya la puse pero no hice captura), y luego aparecería:

Bloc de notas → Bloc de notas: **Firmado y cifrado correctamente.**

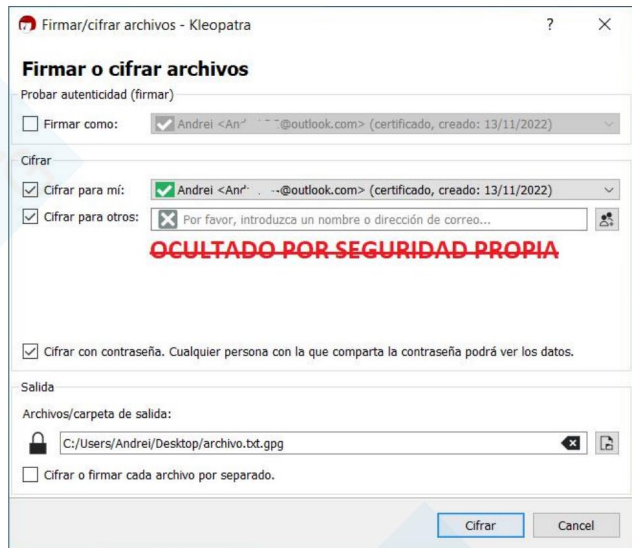
Cerrar

8) Con una contraseña simétrica cifrada asimétricamente cifrar un fichero simétricamente:

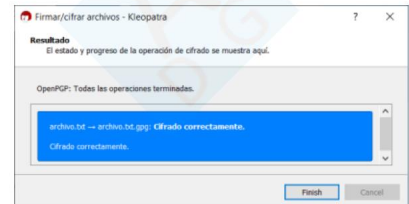
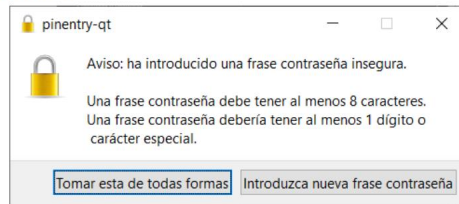
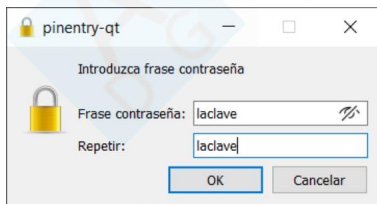
- 1) Creo un archivo de documento de texto en el que lo cifro simétricamente con la contraseña "laclave":



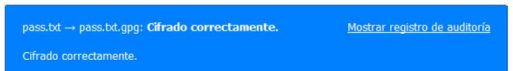
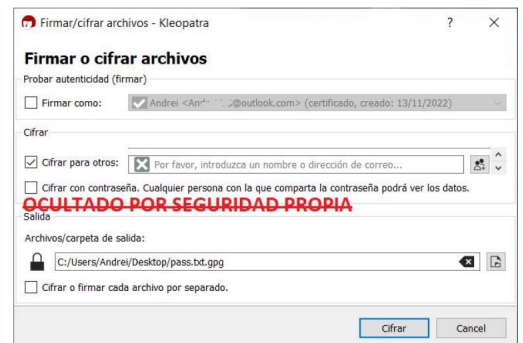
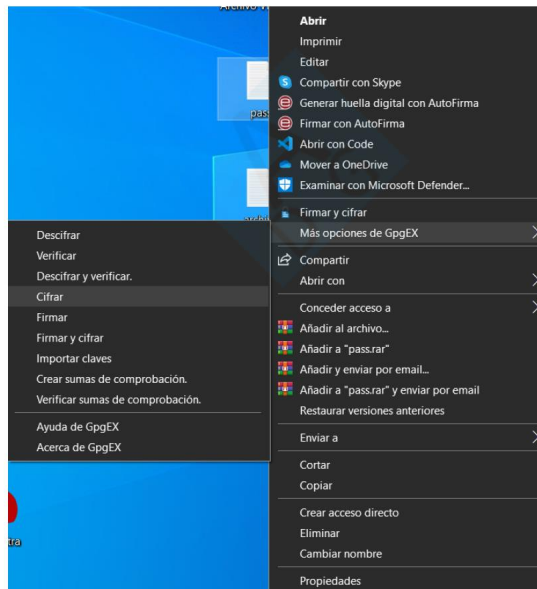
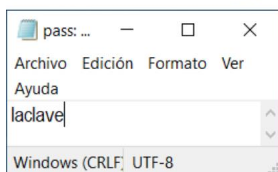
- 2) Le añado una contraseña (activando la casilla [X] Cifrar con contraseña) y por tanto se hará simétricamente:



- 3) Añado la contraseña para descifrar ese fichero:

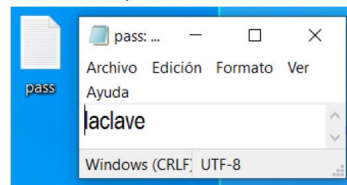
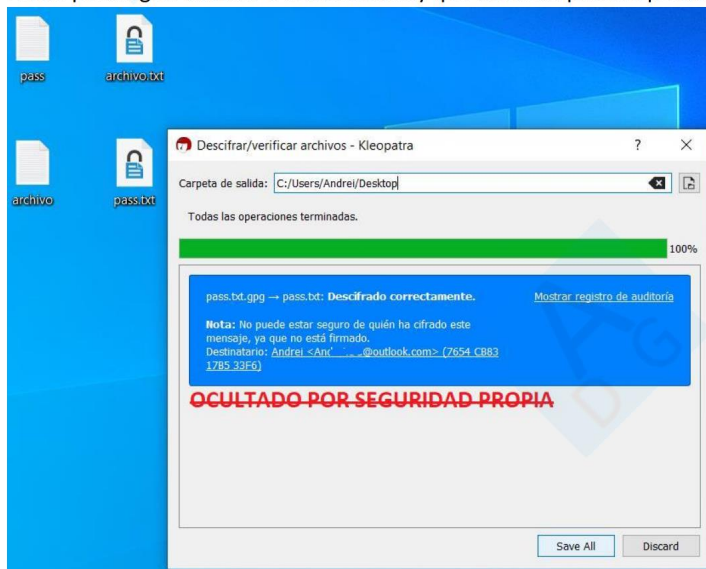


- 4) Añado la contraseña que he usado para descifrar el archivo.txt en el documento de texto pass.txt y lo cifro asimétricamente (desactivando la casilla [X] Cifrar con contraseña):



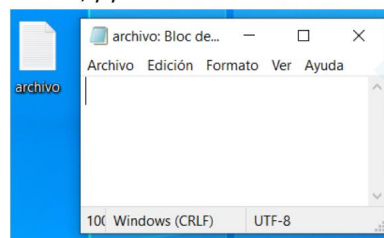
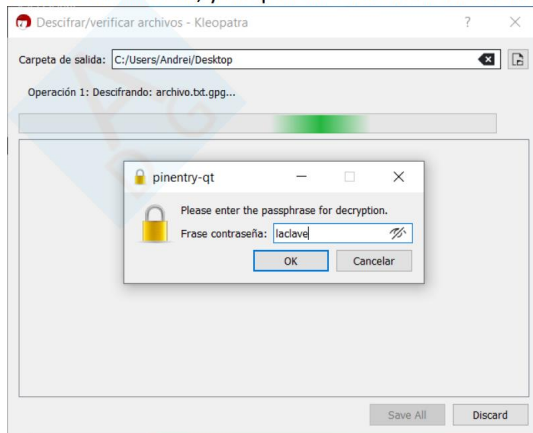
Ahora para lograr acceder a archivo.txt hay que descifrar pass.txt primero que lo tengo sin contraseña por estar cifrado asimétricamente, solamente tendré que ingresar mi contraseña que tengo de una clave pública que tengo publicada en el servidor, en mi caso "andreidani".

Guardamos, nos da el archivo:



Descifro archivo.txt, y me pide la contraseña del archivo para descifrarlo, introduzco la clave que conseguí anteriormente:

Guardo, y ya tendría mi archivo.txt:



(No se perdió ni un bit por el camino, lo dejé en blanco 😊)