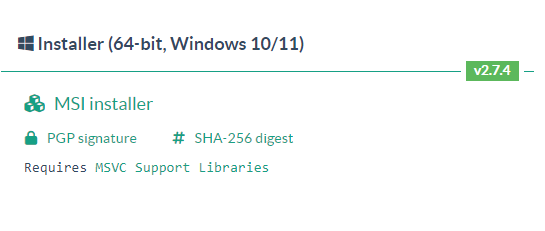
Cifrado ficheros

Para toda la practica usaremos la aplicación Kleopatra, que no es mas que un programa para verificar ficheros y almacenar claves de cifrado, tanto simétrico como asimétrico

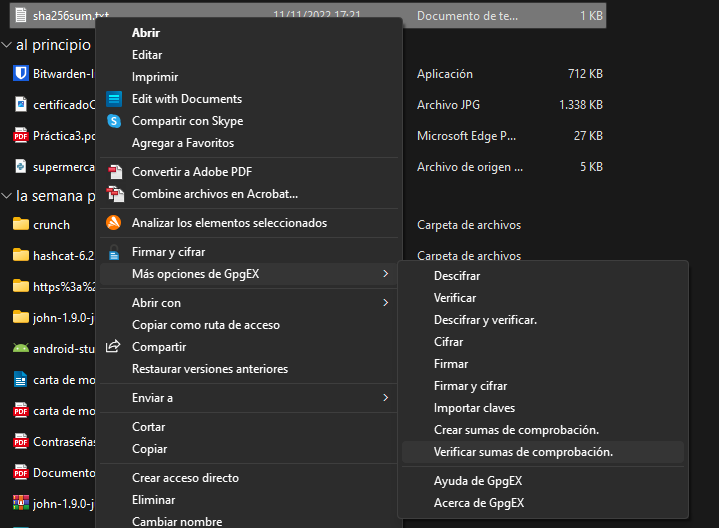
1º: Verificacion CRC ficheros (pj KeePass)

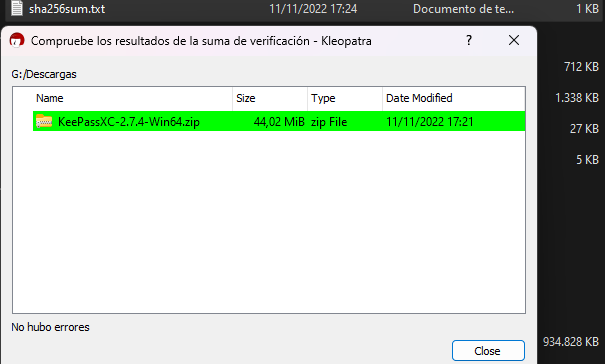
**Lo primero es descargar KeepassXC y su correspondiente archivo checksum.**

**Antes de comprobar el archivo, hay que renombrarlo a sha256sum.txt para que gpgEx puede leerlo, si no nos dará error.**

****

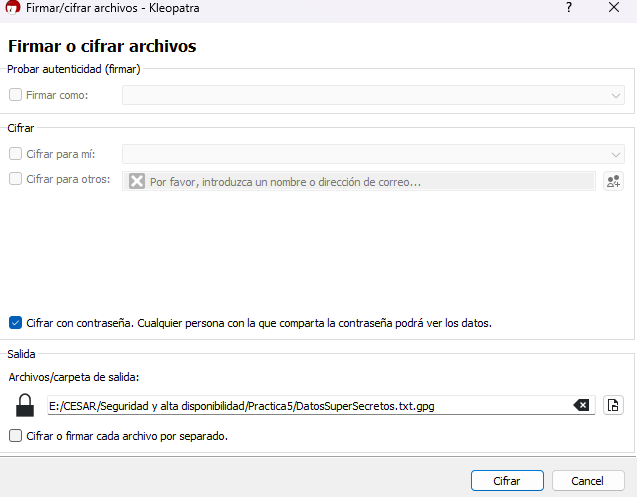
****

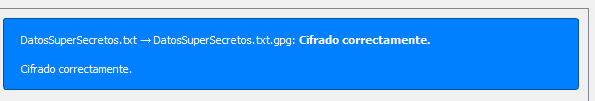
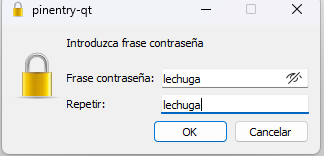
****

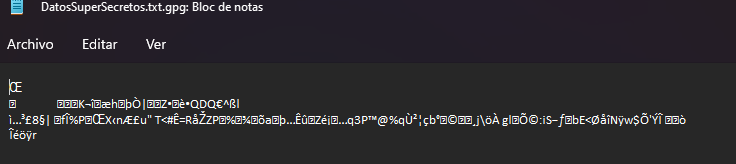
****

2º:Cifrado simétrico

Para cifrar un fichero simétricamente hay que elegir el fichero y decidir que clave simétrica usar. Es bastante intuitivo con este programa.

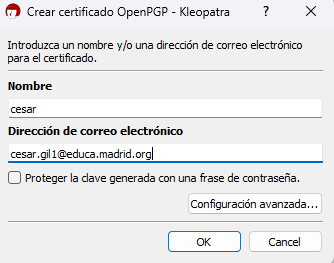




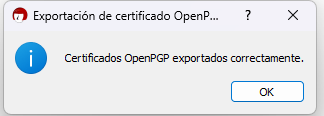
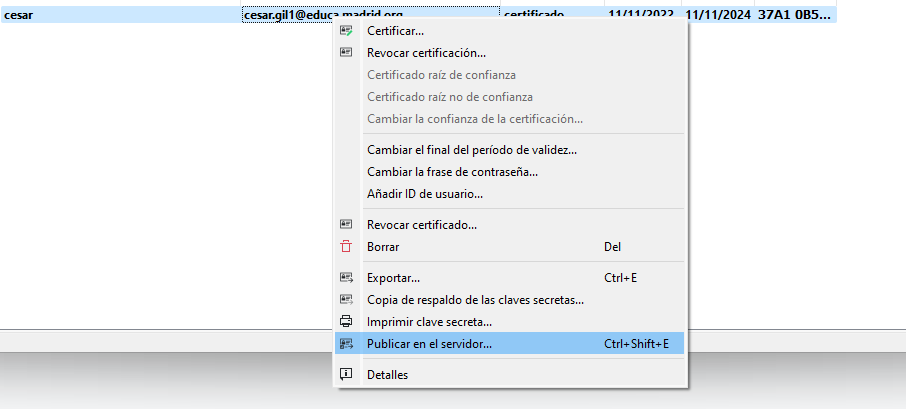
Podemos comprobar que el archivo es ilegible a menos que los descifremos con la clave simétrica.

3º:Crear clave y exportarla al servidor

Para crear la clave y que quede registrada es necesario declarar un nombre y un correo al que vincular dicha clave. También esta la opción de establecer una contraseña para la clave, añadiendo aun mas seguridad al asunto.

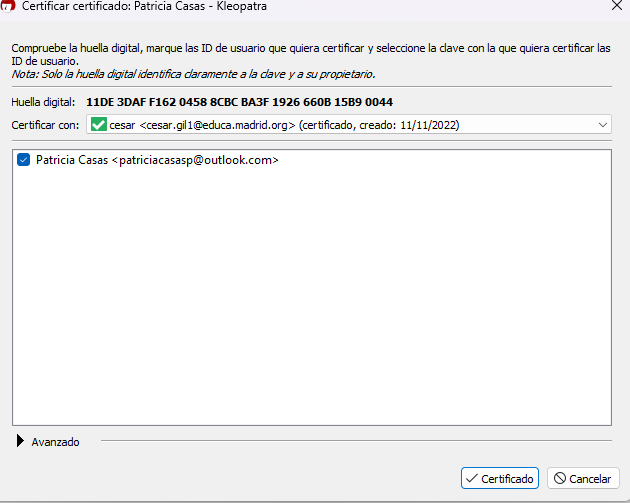
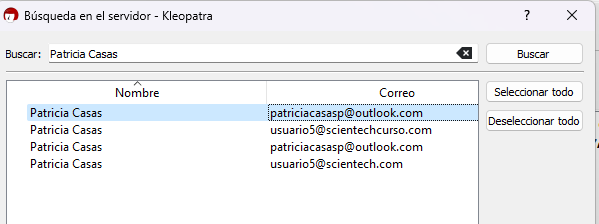


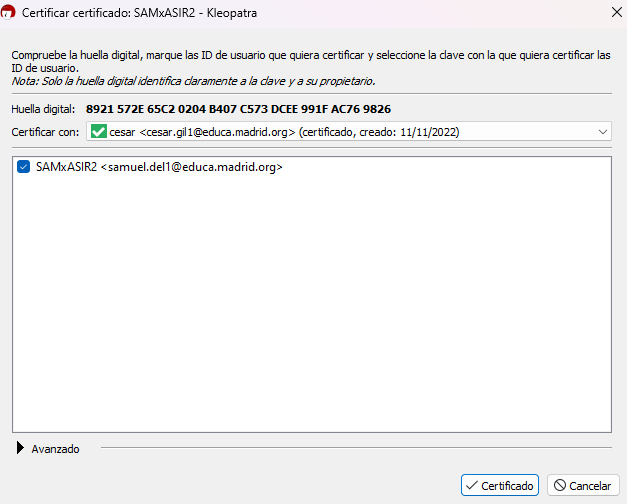
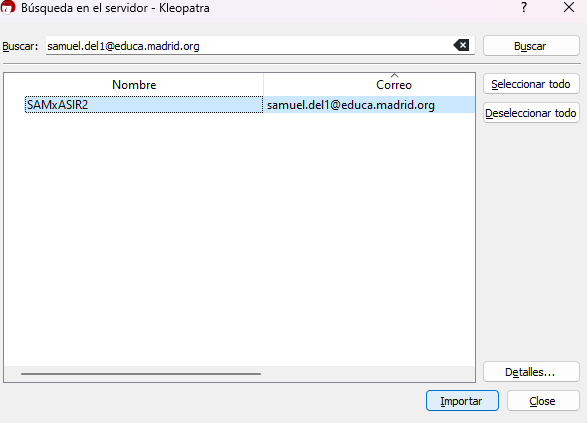
La exportamos al servidor



4º:Importar claves publicas de varios compañeros

Para importar las claves publicas de otra persona necesitamos saber el correo con el que la ha generado, una vez lo sabemos, basta con buscar dicho correo en el servidor, o en caso de que no la haya exportado, pedírsela personalmente, así nos aseguramos que sea de quien dice ser.

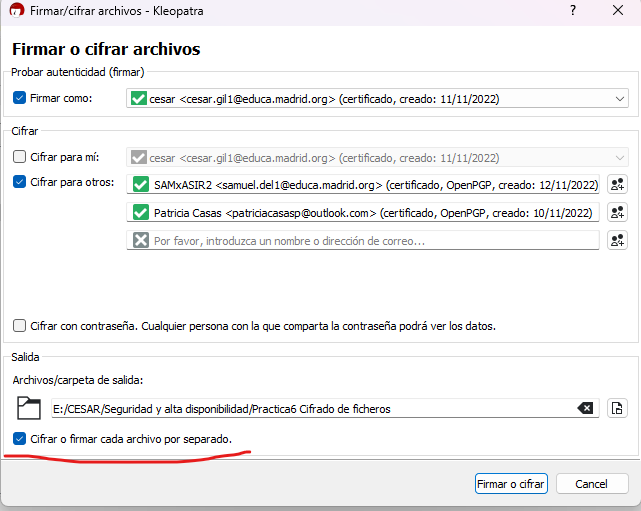
Clave publica de patricia:

Clave publica de samuel:

5º: firmar y cifrar fichero para varios compañeros

**Firmado y cifrado asimétricamente**

Con este metido de cifrado solo aquellas personas a las que este destinado pueden ver en contenido del mensaje.

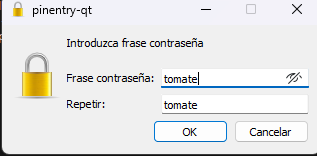
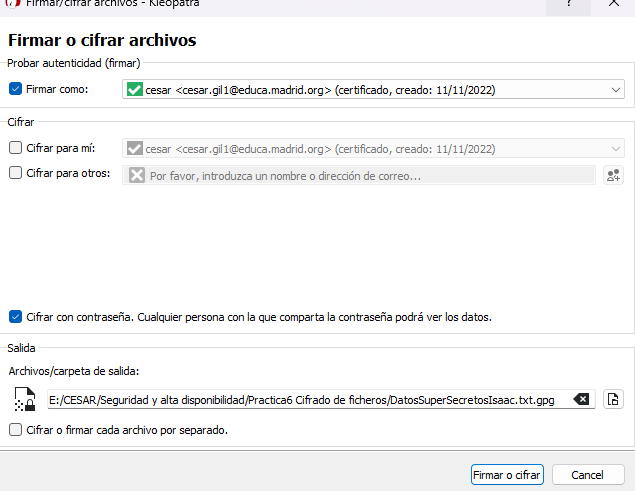


Decir que no tengo muy claro para que sirve la opción de cifrar los archivos por separado, porque aunque la marque, solo me genera un único archivo.

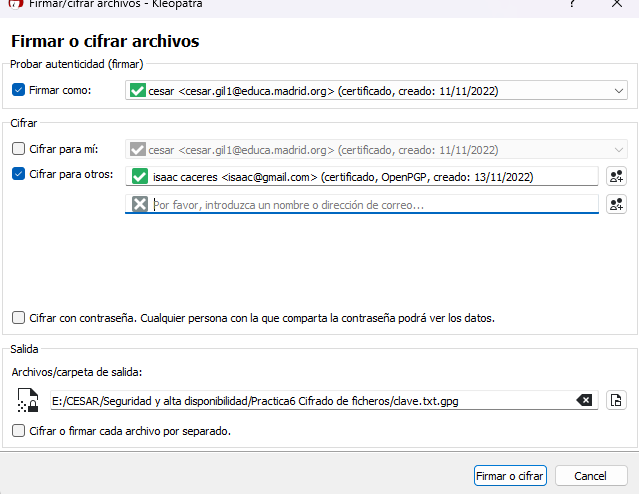
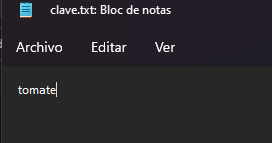
Quiero pensar que vale para que tanto uno como otro puedan descifrar el archivo sin necesidad del segundo. Y que si por el contrario no lo cifras por separado, hace falta la clave privada de ambos, pero repito, no se si es que el programa hace lo que le da la gana o qué.

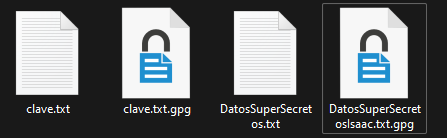
**Firmado y cifrado simétricamente y la clave cifrada asimétricamente**

Con este metido de cifrado cualquier persona que conozca la clave simétrica puede ver el contenido del mensaje, pero ya que hemos cifrado la clave asimétricamente, solo aquellas personas a las que este destinado pueden ver cual es la clave simétrica para descifrar el mensaje.

Cifrado simétrico del archivo:

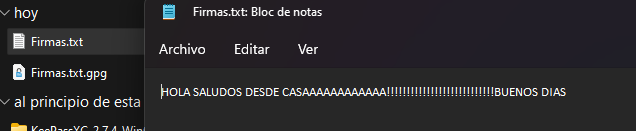
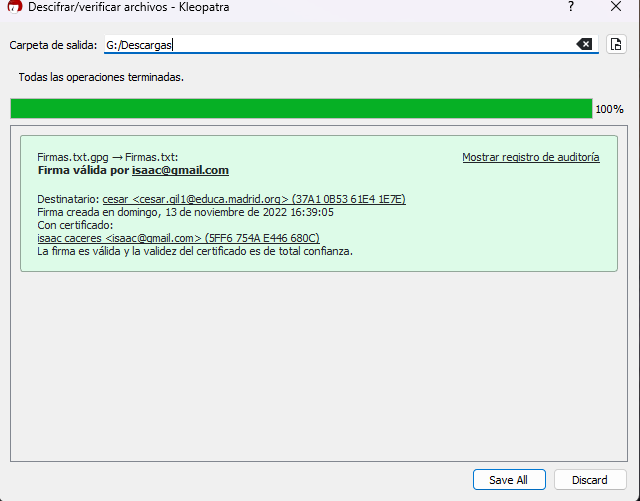
Cifrado asimétrico de la clave simétrica:



Aquí tenemos los 2 archivos cifrados que mandaremos a nuestro compañero.

6º:verificación del fichero del compañero

**Cifrado asimétricamente:**



**Firmado y cifrado simétricamente y la clave cifrada asimétricamente:**

Descifrado asimétrico de la clave simétrica:

Descifrado simétrico con la clave obtenida: