

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.


 Installer (64-bit, Windows 10/11)

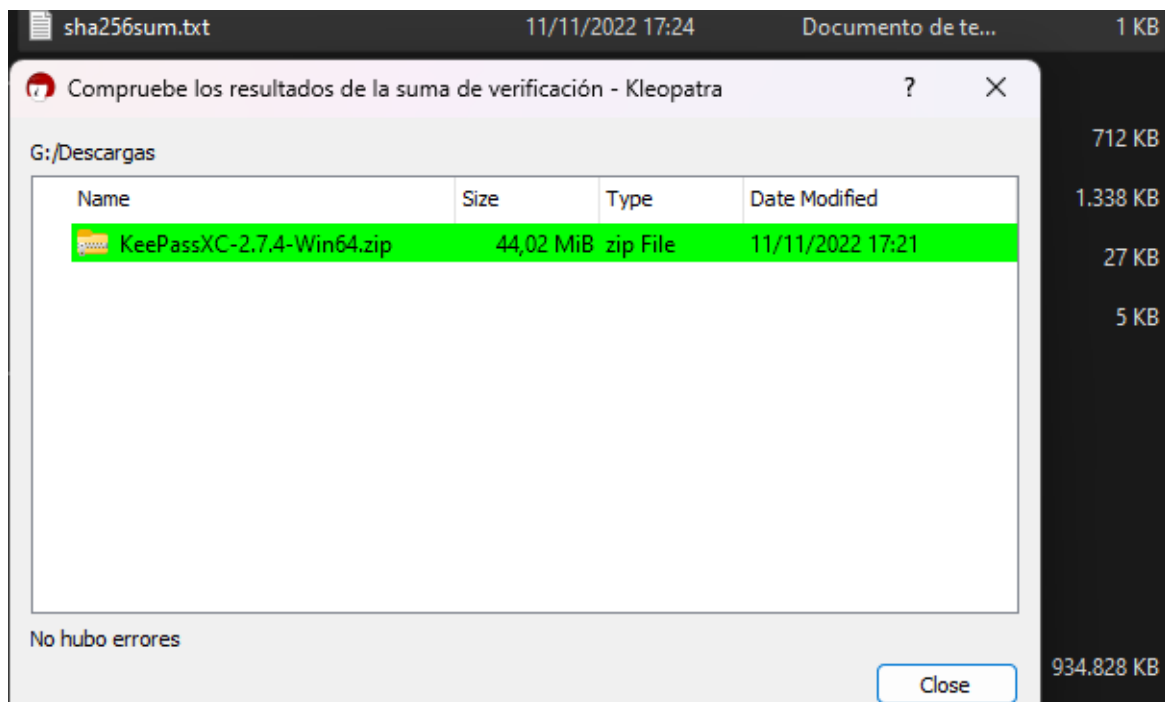
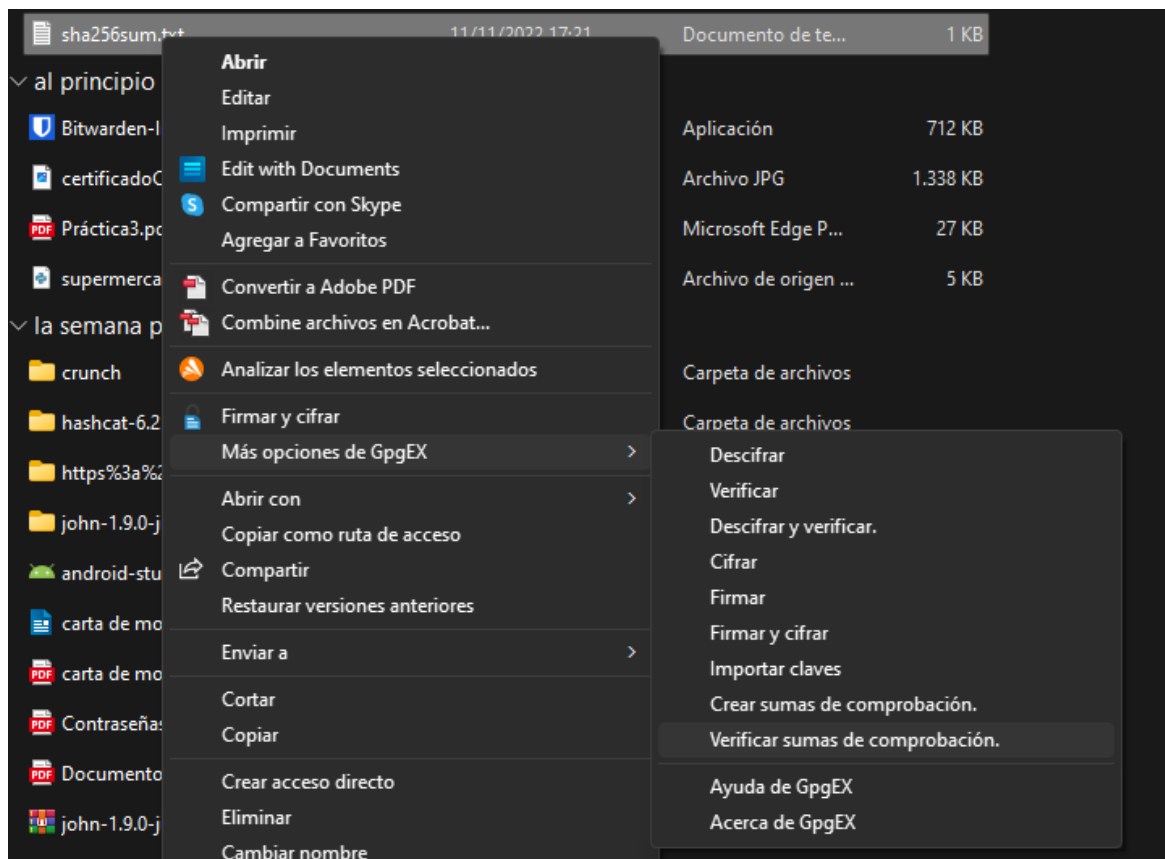
v2.7.4

 MSI installer

 PGP signature # SHA-256 digest

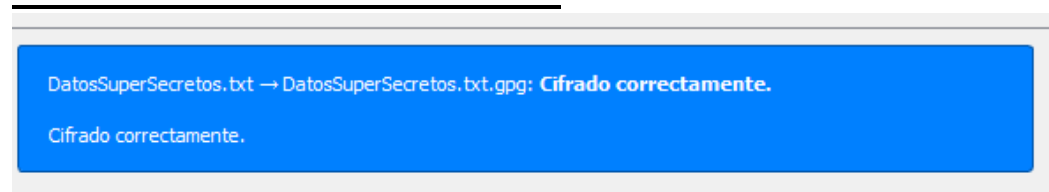
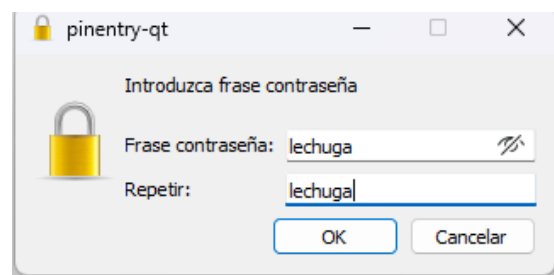
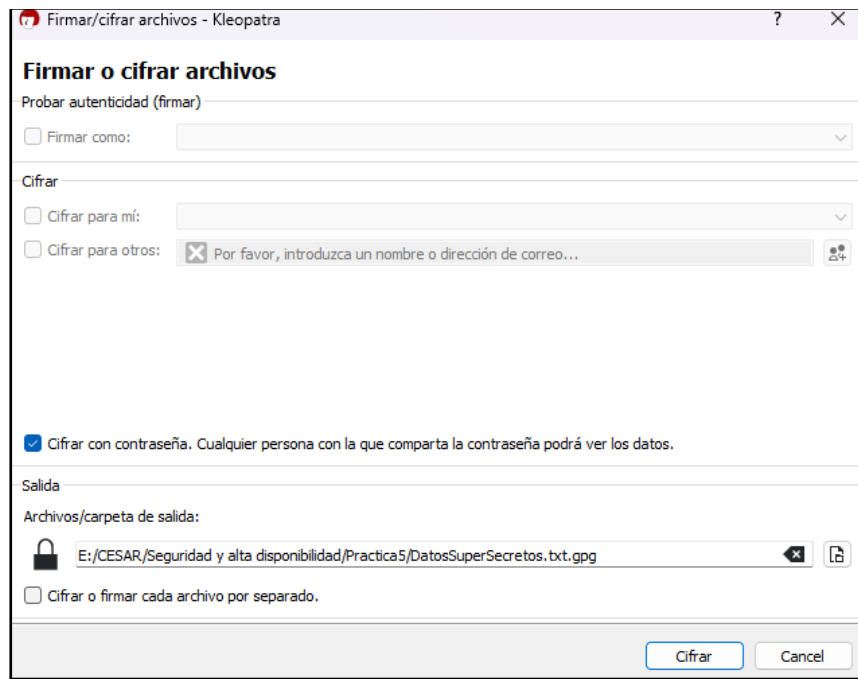
Requires MSVC Support Libraries

 C-2.7.4-Win64.zip.txt

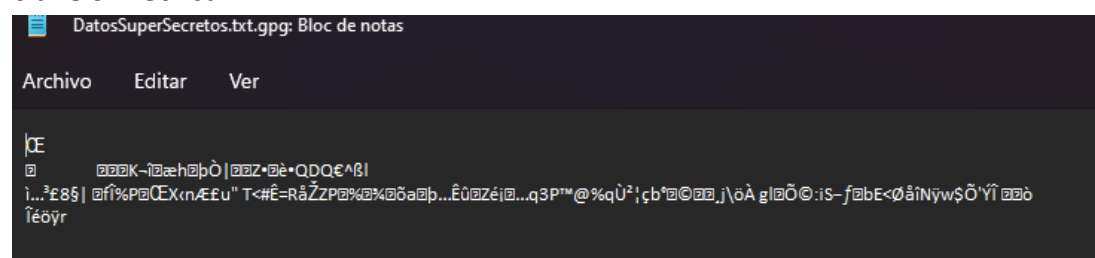


2º: Cifrado simétrico

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

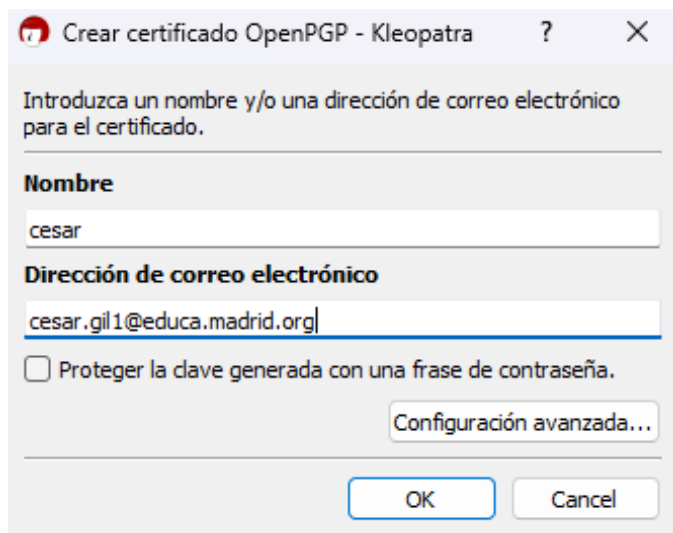


Podemos comprobar que el archivo es ilegible a menos que los descifremos con la clave simétrica.

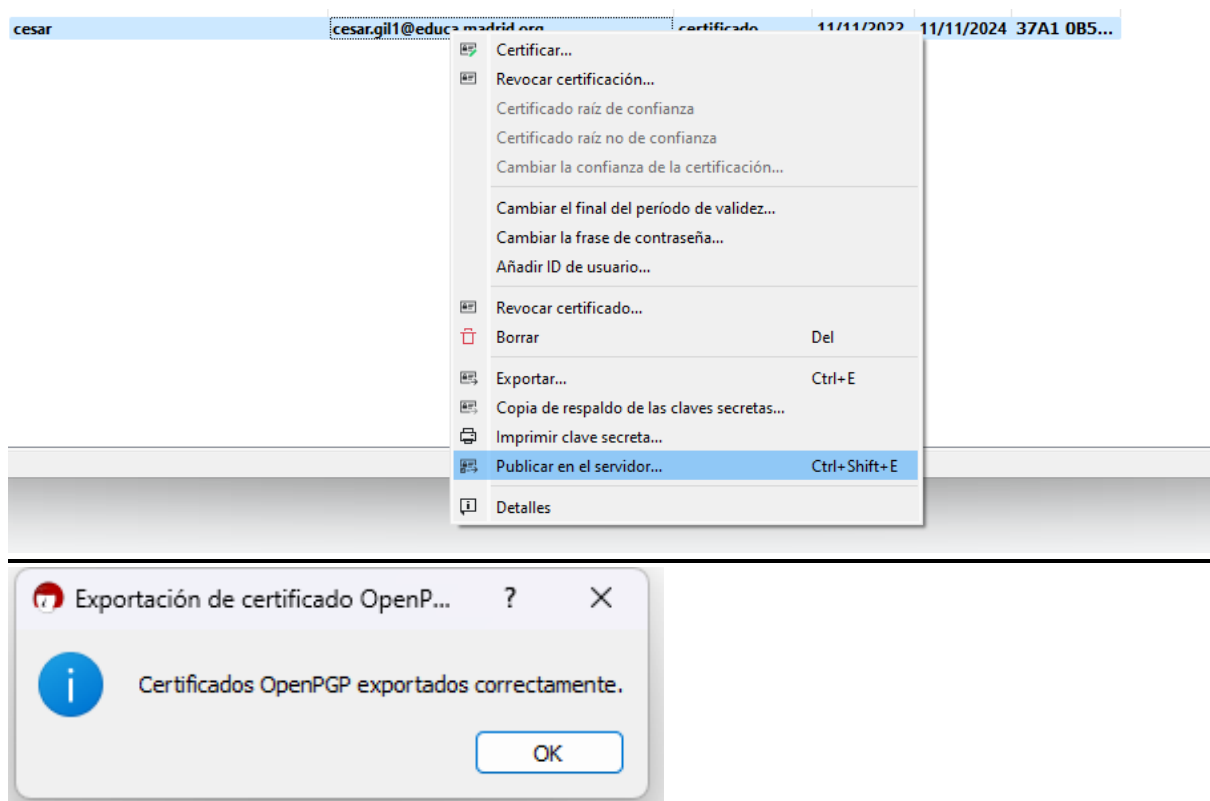


3º: Crear clave y exportarla al servidor

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:

The image shows two screenshots of the Kleopatra application interface. The top window, titled 'Búsqueda en el servidor - Kleopatra', displays a search for 'Patricia Casas'. It contains a table with two columns: 'Nombre' and 'Correo'. The first row is highlighted in blue. To the right of the table are buttons for 'Seleccionar todo' and 'Deseleccionar todo'. The bottom window, titled 'Certificar certificado: Patricia Casas - Kleopatra', shows the digital fingerprint '11DE 3DAF F162 0458 8CBC BA3F 1926 660B 15B9 0044' and a dropdown menu for the certificate authority, currently set to 'cesar <cesar.gil1@educa.madrid.org> (certificado, creado: 11/11/2022)'. Below this, a list shows 'Patricia Casas <patriciacasasp@outlook.com>' with a checked checkbox. At the bottom right, there are buttons for 'Certificado' and 'Cancelar'.

| Nombre | Correo |
|----------------|------------------------------|
| Patricia Casas | patriciacasasp@outlook.com |
| Patricia Casas | usuario5@scientechncurso.com |
| Patricia Casas | patriciacasasp@outlook.com |
| Patricia Casas | usuario5@scientechn.com |

Huella digital: **11DE 3DAF F162 0458 8CBC BA3F 1926 660B 15B9 0044**

Certificar con: ☒ cesar <cesar.gil1@educa.madrid.org> (certificado, creado: 11/11/2022)

☒ Patricia Casas <patriciacasasp@outlook.com>

Avanzado

Clave publica de samuel:

Búsqueda en el servidor - Kleopatra

Buscar: samuel.del1@educa.madrid.org

Buscar

| Nombre | Correo |
|-----------|------------------------------|
| SAMxASIR2 | samuel.del1@educa.madrid.org |

Seleccionar todo

Deseleccionar todo

Certificar certificado: SAMxASIR2 - Kleopatra

Compruebe la huella digital, marque las ID de usuario que quiera certificar y seleccione la clave con la que quiera certificar las ID de usuario.
Nota: Solo la huella digital identifica claramente a la clave y a su propietario.

Huella digital: **8921 572E 65C2 0204 B407 C573 DCEE 991F AC76 9826**

Certificar con: ☒ cesar <cesar.gil1@educa.madrid.org> (certificado, creado: 11/11/2022)

☒ SAMxASIR2 <samuel.del1@educa.madrid.org>

▶ Avanzado

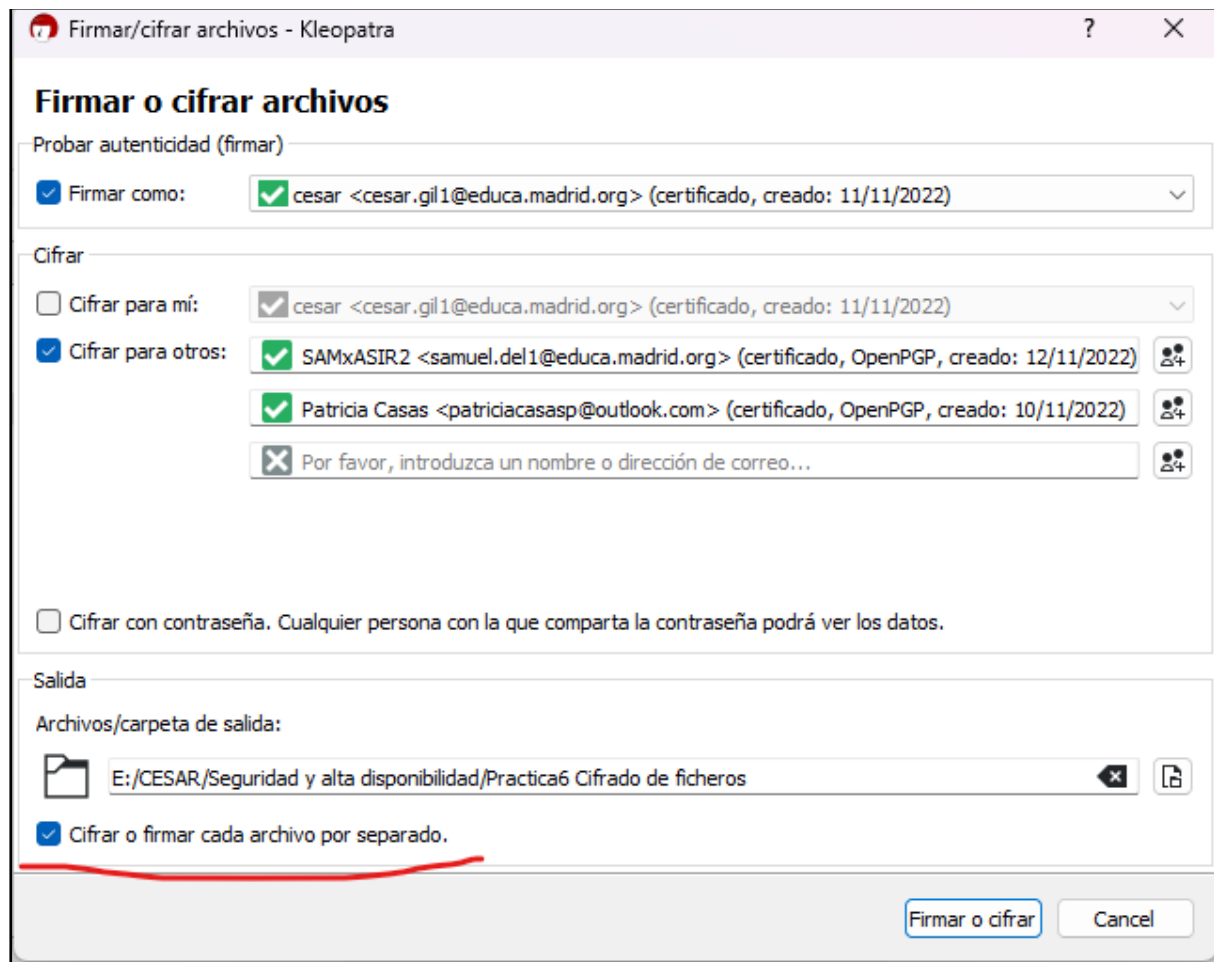
✓ Certificado

⌛ Cancelar

5º: firmar y cifrar fichero para varios compañeros

Firmado y cifrado asimétricamente

Con este metodo 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 metodo 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:

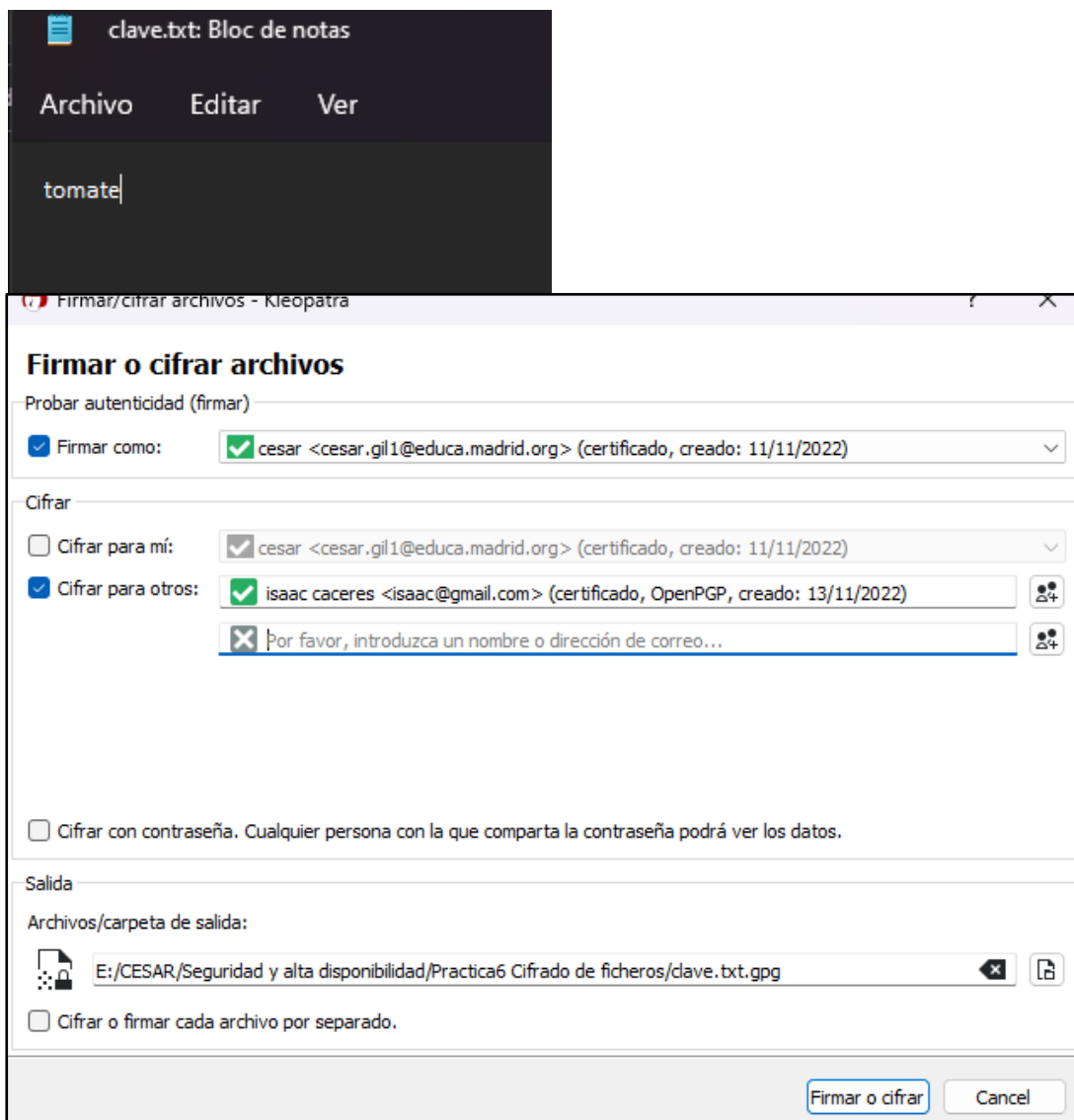
The screenshot shows the 'Firmar o cifrar archivos' (Sign or encrypt files) dialog box in the Kleopatra application. The window title is 'Firmar/cifrar archivos - Kleopatra'. The dialog is divided into several sections:

- Firmar o cifrar archivos**: The main title of the dialog.
- Probar autenticidad (firmar)**: A section for signing. It includes a checked checkbox 'Firmar como:' and a dropdown menu showing 'cesar <cesar.gil1@educa.madrid.org> (certificado, creado: 11/11/2022)'.
- Cifrar**: A section for encryption. It includes two checkboxes: 'Cifrar para mí:' (checked) and 'Cifrar para otros:' (unchecked). The 'Cifrar para mí:' checkbox is associated with the same dropdown menu as the signing section. The 'Cifrar para otros:' checkbox is associated with a text field containing 'Por favor, introduzca un nombre o dirección de correo...'. There is also a small icon of a group of people next to this field.
- Salida**: A section for the output. It includes a checked checkbox 'Cifrar con contraseña. Cualquier persona con la que comparta la contraseña podrá ver los datos.' and a text field for the output path: 'E:/CESAR/Seguridad y alta disponibilidad/Practica6 Cifrado de ficheros/DatosSuperSecretosIsaac.txt.gpg'. There are also icons for file operations (delete and save) next to the path field.
- Archivos/carpeta de salida:**: A section for the output files/folder.
- Cifrar o firmar cada archivo por separado.**: An unchecked checkbox.

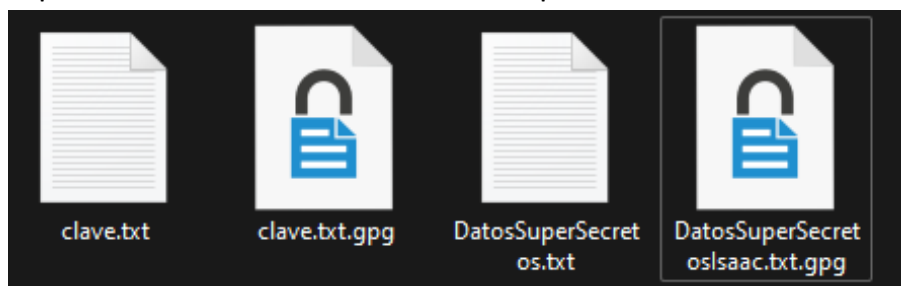
At the bottom right of the dialog are two buttons: 'Firmar o cifrar' and 'Cancelar'.

The screenshot shows the 'pinentry-qt' password prompt dialog box. The window title is 'pinentry-qt'. The dialog has a yellow padlock icon on the left. The text 'Introduzca frase contraseña' (Enter password phrase) is at the top. Below it are two text input fields: 'Frase contraseña:' (Password phrase) and 'Repetir:' (Repeat). Both fields contain the text 'tomate'. At the bottom are two buttons: 'OK' and 'Cancelar'.

Cifrado asimétrico de la clave simétrica:

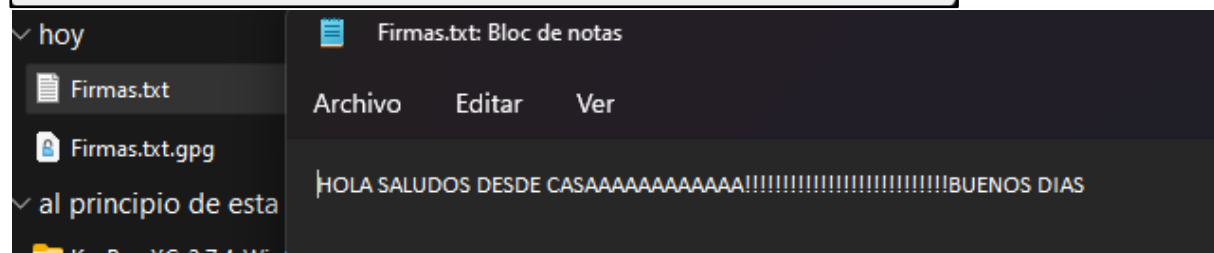
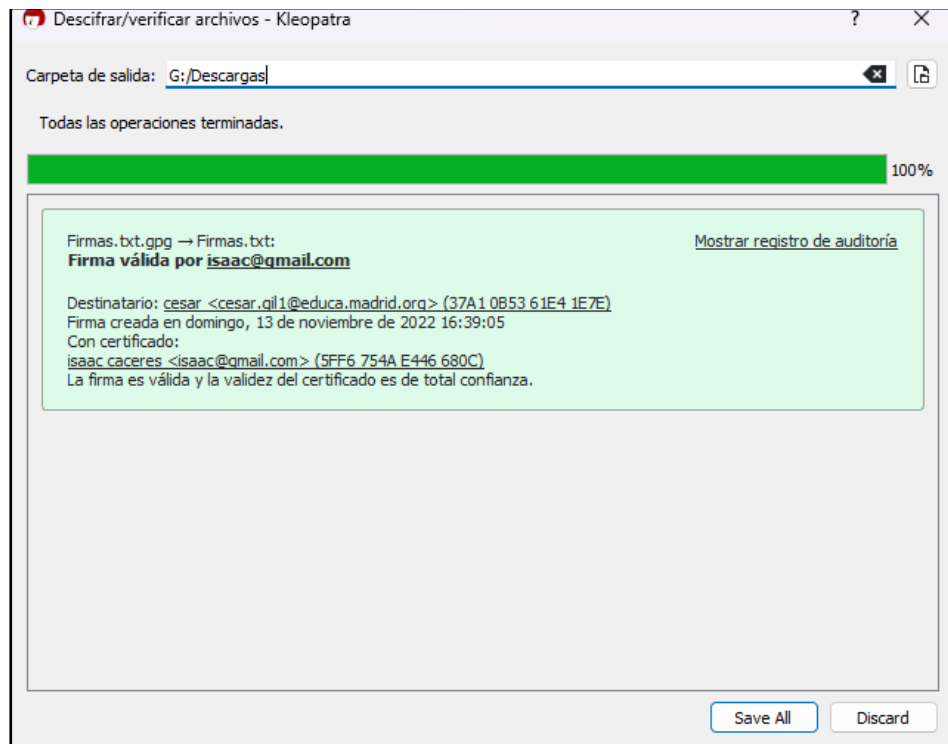


Aquí tenemos los 2 archivos cifrados que mandaremos a nuestro compañero.



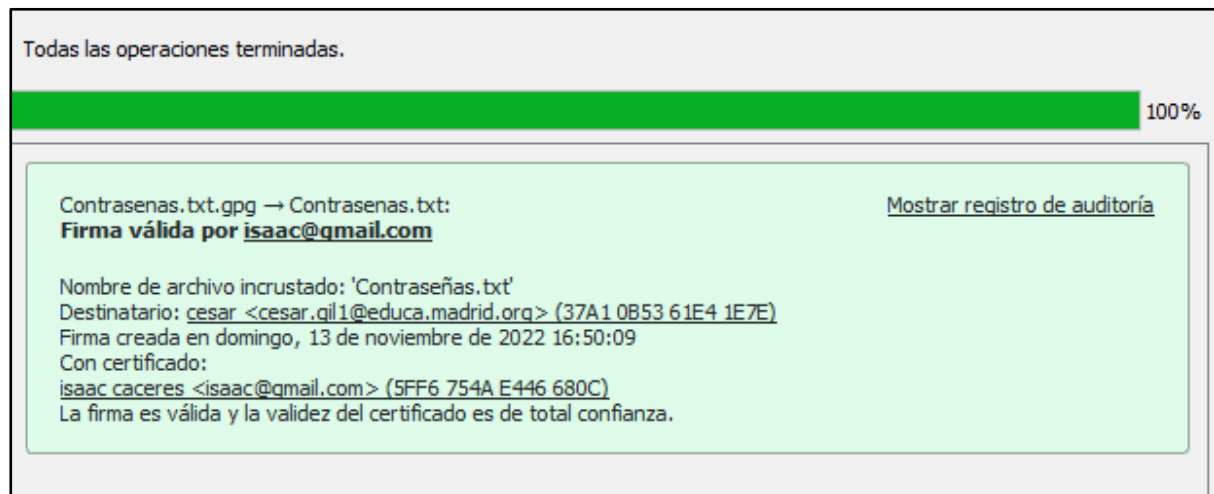
6º:verificación del fichero del compañero

Cifrado asimétricamente:



Firmado y cifrado simétricamente y la clave cifrada asimétricamente:

Descifrado asimétrico de la clave simétrica:



Descifrado simétrico con la clave obtenida:

