



# Manual de uso

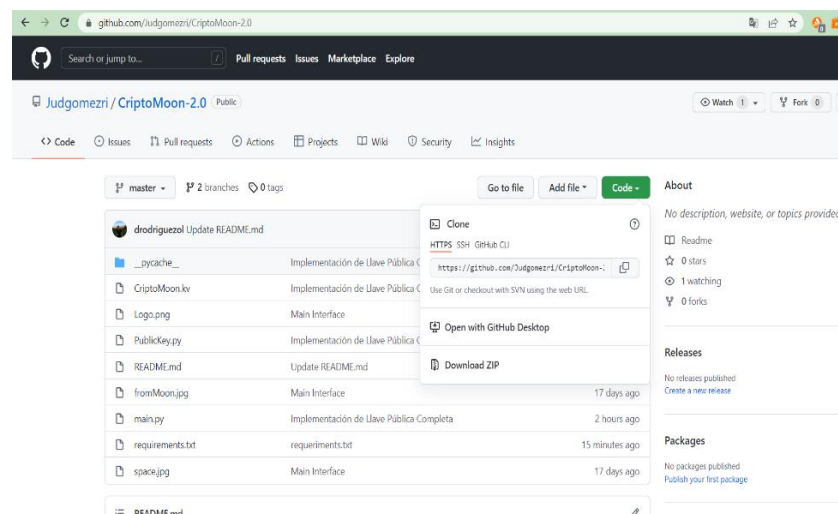
Con esta aplicación de computador puede encriptar mensajes escritos en forma de números enteros, como también descifrar mensajes ya encriptados. Además puede encriptar imágenes y simular una criptomoneda.



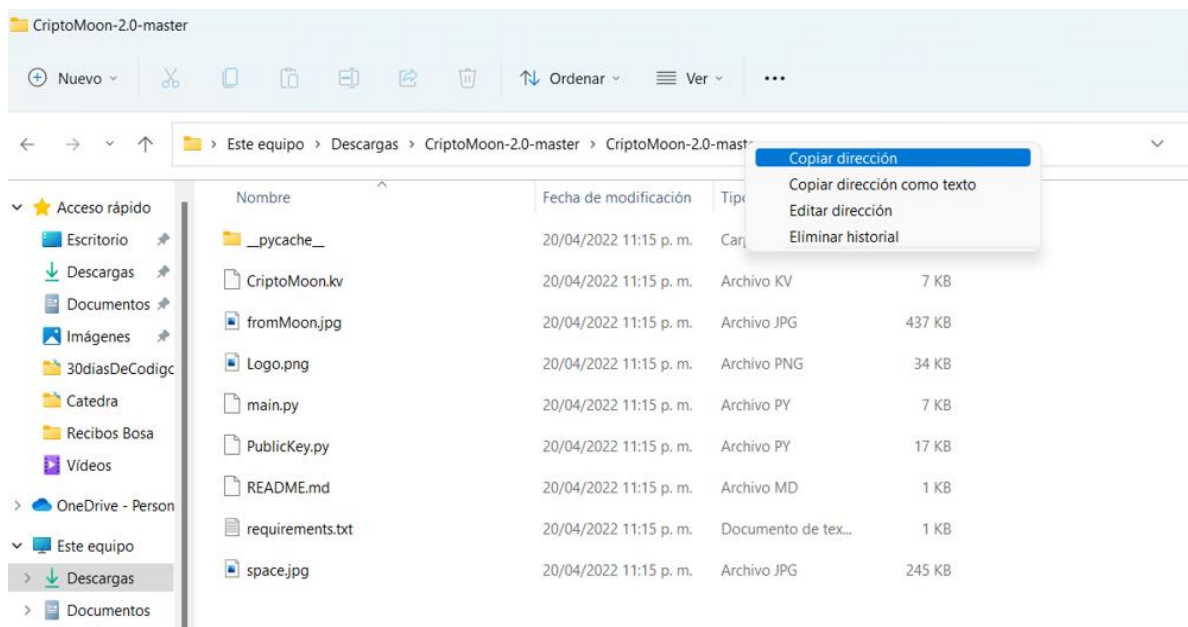
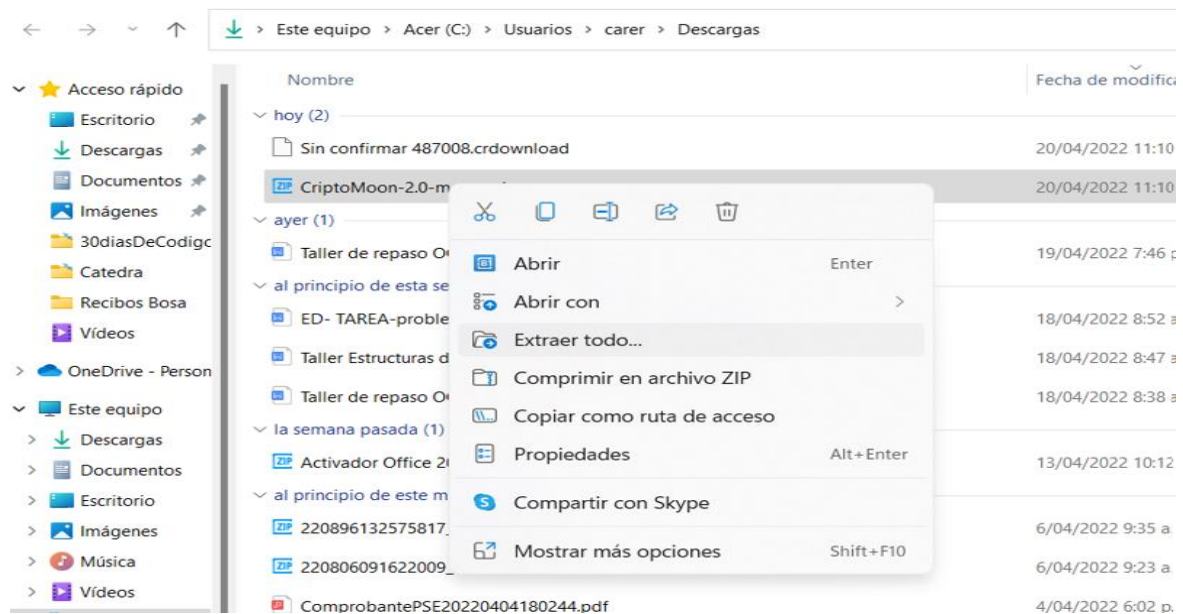
**IMPORTANTE** Asegúrese que su computador tenga instalado Python 3.0 o superior.

## 1. Instalación

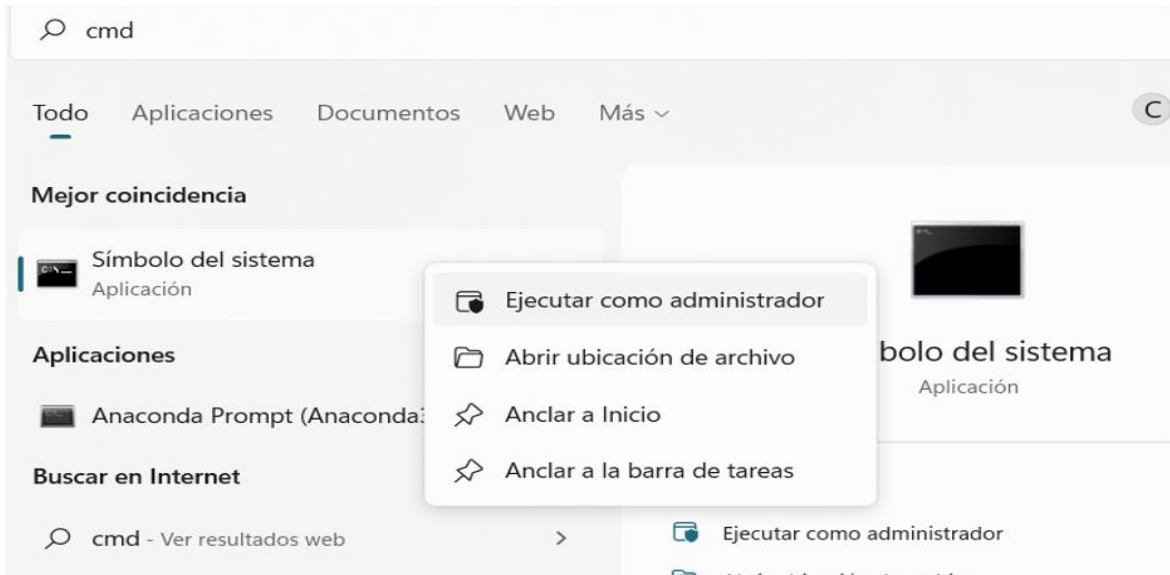
Ingresa a <https://github.com/Judgomezri/CriptoMoon-2.0> y descargue el archivo punto zip de la aplicación y siga las siguientes instrucciones:



Descomprima el archivo descargado y copie la dirección de su ubicación.



Abra el cmd de su computador y con el comando “cd” vaya a la dirección copiada anteriormente. Luego, ejecute el siguiente comando: `pip install -r requirements.txt`



```
Administrator: Símbolo del sistema
Microsoft Windows [Versión 10.0.22000.613]
(c) Microsoft Corporation. Todos los derechos reservados.

C:\WINDOWS\system32>cd C:\Users\carer\Downloads\CriptoMoon-2.0-master\CriptoMoon-2.0-master
C:\Users\carer\Downloads\CriptoMoon-2.0-master\CriptoMoon-2.0-master>pip install -r requirements.txt
```

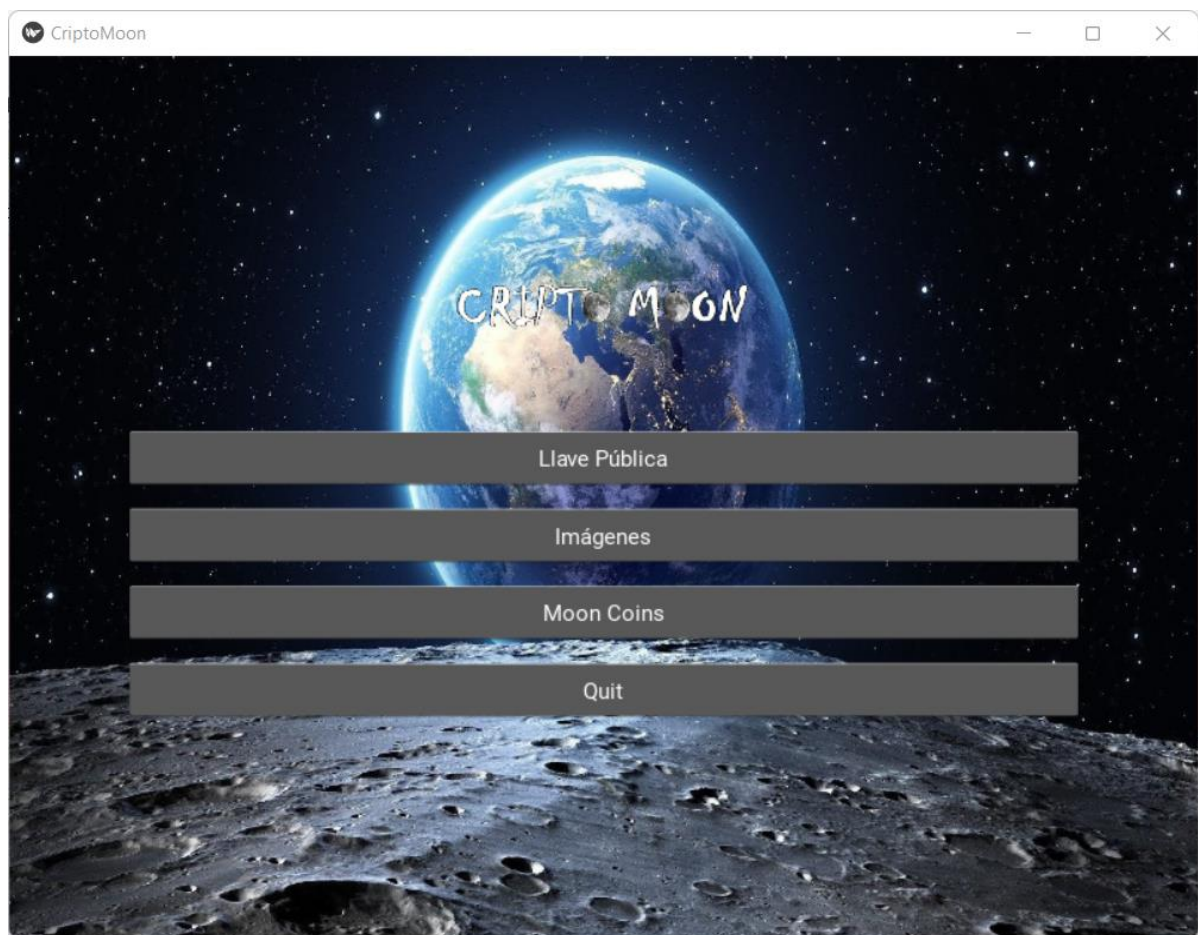
Una vez instalados los requerimientos puede empezar a usar la aplicación.

## 2. Utilizar la aplicación

En la pantalla cmd en de la dirección de la carpeta de la aplicación, ejecute el comando:  
`python main.py`

```
C:\Users\carer\Downloads\CriptoMoon-2.0-master\CriptoMoon-2.0-master>: python main.py
```

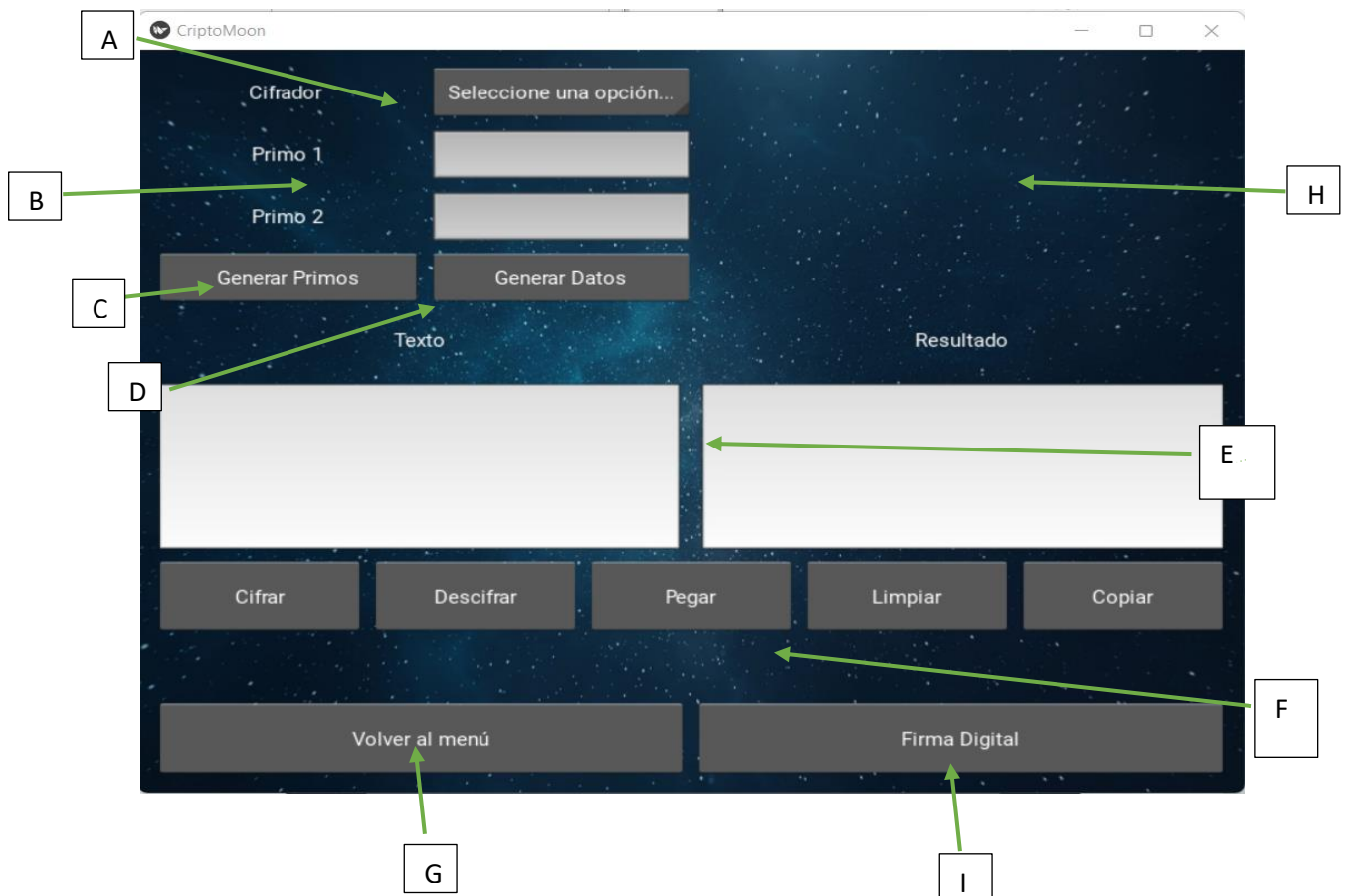
Así, se desplegará la aplicación. Puede pinchar en “Llave Pública” para empezar a cifrar mensajes y firmar documentos digitales; en “Imágenes” para cifrar imágenes; en “Moon Coins” para simular una criptomoneda o en “Quit” para salir.





## 2. Llave Pública

Al pinchar en “Llave Pública” tendrá las siguientes funcionalidades.



- A. En éste desplegable puede elegir entre 4 diferentes formas de cifrar.
- B. En esta parte están las casillas donde se ingresan los números que son la base para poder cifrar y descifrar. Si conoce de criptografía puede ingresarlos usted mismo, o puede generarlos automáticamente.
- C. Con este botón puede generar automáticamente los números necesarios para cifrar.
- D. Calcula internamente los datos necesarios que la aplicación funcione, algunos de ellos aparecerán en la parte H.
- E. En el cuadro de texto puede digitar el mensaje a encriptar o cifrar. En el cuadro de resultado aparecerá el texto cifrado en forma de números enteros, este texto es el que puede utilizar para comunicarse de forma secreta.
- F. Estos botones le permiten interactuar con los cuadros de texto de la parte E. Una vez ingresado el mensaje a cifrar, puede pinchar en cifrar. Luego, aparecerá el texto cifrado. Con el botón de copiar puede copiar el texto cifrado. Con el botón de limpiar puede borrar el texto en ambos cuadros. Con el botón de pegar se ingresa la el texto anteriormente pegado; y con el botón de descifrado puede recuperar el mensaje original.
- G. Con este botón puede regresar al menú anterior para salir de la aplicación.
- H. Después generar datos con la parte D, aparecerán algunos datos que utiliza el programa para cifrar, esta parte solo le interesará si sabe un poco de criptografía.
- I. Con este botón puede ir al menú para firmar documentos digitales.

## 2.1 Ejemplo

Vamos a cifrar con el método RSA. En A Seleccionamos RSA.

The screenshot shows the 'CriptoMoon' application window. On the left, under 'Cifrador', there are input fields for 'Primo 1' and 'Primo 2', and a 'Generar Primos' button. In the center, a vertical stack of buttons allows selecting a cipher method: 'RSA' (selected), 'Rabin', 'ElGamal', and 'Menezes Vanestone'. To the right, there are input fields for 'n', ' $\Phi(n)$ ', and 'Clave Pública'. Below these are two large text areas labeled 'Text' and 'Resultado'. At the bottom, a row of buttons includes 'Cifrar', 'Descifrar', 'Pegar', 'Limpiar', and 'Copiar', followed by a 'Volver al menú' button.

Le damos a genera primos, generar datos e ingresamos el mensaje a cifrar.

The screenshot shows the 'CriptoMoon' application interface. The 'Cifrador' is set to 'RSA'. The 'Primo 1' is 714966701978264018039 and 'Primo 2' is 2008090370300071423042. The 'Clave Pública' is 074/0920231/23733737041/03220310409834458893. The 'Texto' field contains 'Nos vemos el sabado a las tres en el capitolio'. The 'Resultado' field is empty. The interface includes buttons for 'Generar Primos', 'Generar Datos', 'Cifrar', 'Descifrar', 'Pegar', 'Limpiar', 'Copiar', 'Volver al menú', and 'Firma Digital'.

Primo 1	Primo 2	Clave Pública
714966701978264018039	2008090370300071423042	074/0920231/23733737041/03220310409834458893

Texto: Nos vemos el sabado a las tres en el capitolio

Resultado:

Le damos a cifrar y obtenemos el texto cifrado.

The screenshot shows the 'CriptoMoon' application interface after encryption. The 'Cifrador' is set to 'RSA'. The 'Primo 1' is 714966701978264018039 and 'Primo 2' is 2008090370300071423042. The 'Clave Pública' is 074/0920231/23733737041/03220310409834458893. The 'Texto' field contains 'Nos vemos el sabado a las tres en el capitolio'. The 'Resultado' field contains the encrypted text: 623104156105424233313769467746828395952705579962532113613210143974478779880—9631725650260110571557675233482912903613767462611276487867604591922891015997—18013978709001009052972569282015693202907462306195307525036197647519886137281—14334725087864398511351939539147842275033697052946871586512041643172988183781—3. The interface includes buttons for 'Cifrar', 'Descifrar', 'Pegar', 'Limpiar', 'Copiar', 'Volver al menú', and 'Firma Digital'.

Primo 1	Primo 2	Clave Pública
714966701978264018039	2008090370300071423042	074/0920231/23733737041/03220310409834458893

Texto: Nos vemos el sabado a las tres en el capitolio

Resultado: 623104156105424233313769467746828395952705579962532113613210143974478779880—9631725650260110571557675233482912903613767462611276487867604591922891015997—18013978709001009052972569282015693202907462306195307525036197647519886137281—14334725087864398511351939539147842275033697052946871586512041643172988183781—3



Luego, para descifrar el mensaje, podemos copiar, limpiar pegar y descifrar.

CriptoMoon

Cifrador	RSA	n	1908029189881369008891910728788 0756238810572075280582740007551
Primo 1	714966701978264018039 05006288114470211	$\Phi(n)$	1908029189881369008891910728788 0756238810572075280582740007551
Primo 2	200009037030007142302 473681610480092861	Clave Pública	0747092023172393393904417032263 10409834458893

Generar Primos Generar Datos

Texto	Resultado
448596/3411856145136/48181984/6119/118088996 0764788229972132613—768793667969457377944171 81347370125286413101817123644347201821114653 65075732—93706033693857958323552778648092058 9829236902070220375580786278759484255441—126 38511445627587385746653447488917715364515491 829378340502657038988471975404	NOSVEMOSELSABADOALASTRESENELCAPITOLIOXX

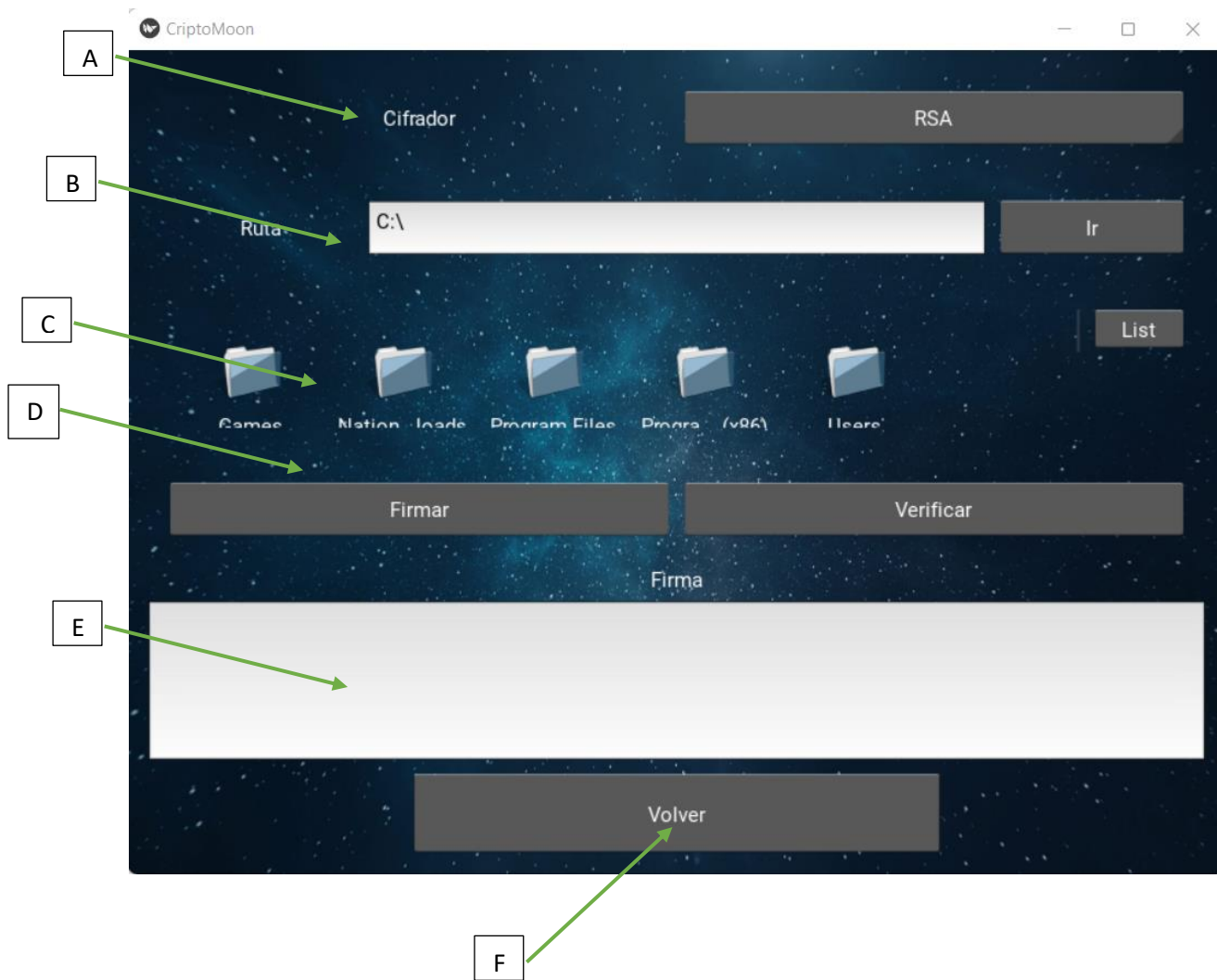
Cifrar Descifrar Pegar Limpiar Copiar

Volver al menú Firma Digital

## 2.2 Firma Digital

Al pinchar en “Firma Digital” podrá la siguiente interfaz para firmar documentos.



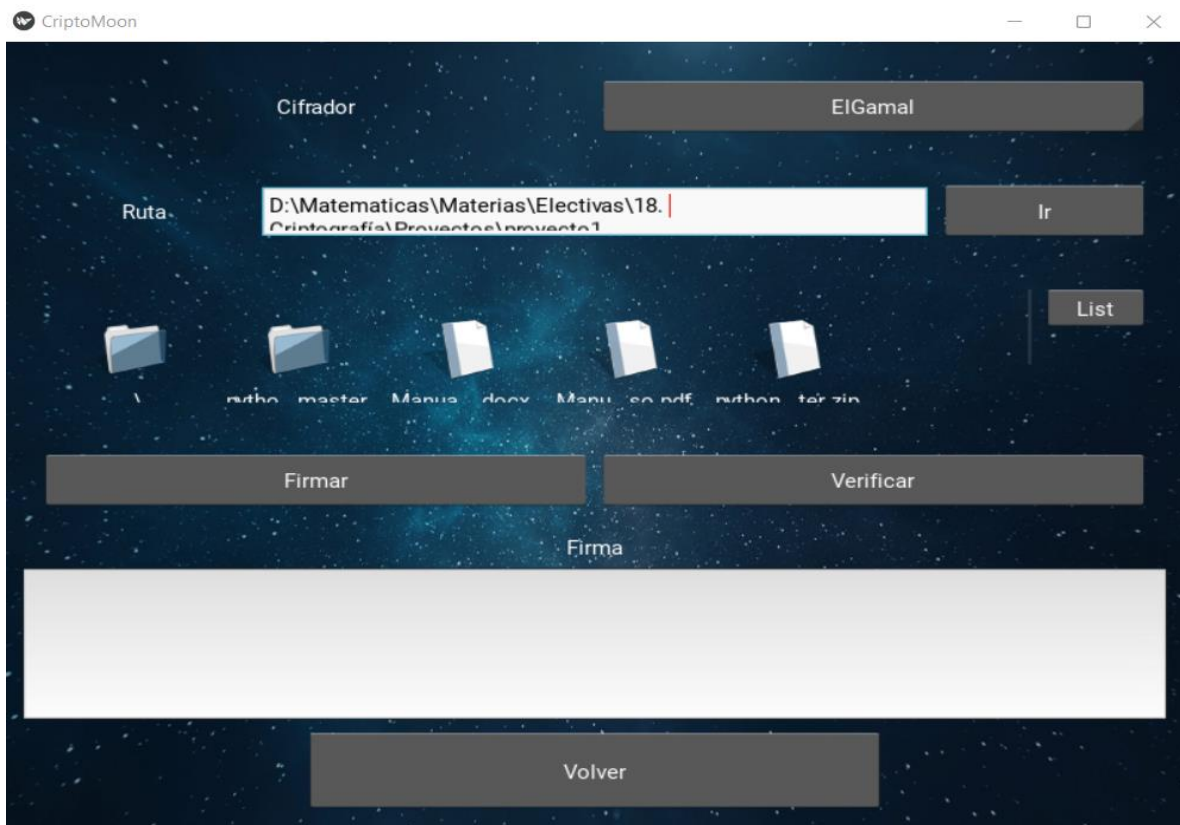


- A. Se elije el tipo de cifrador que desea utilizar.
- B. Puede copiar o escribir la ruta donde se encuentra el archivo y darle ir para que se carguen en C los archivos que hay en dicha dirección.
- C. Puede pinchar en las carpetas para y seleccionar el archivo que desea firmar. Con el botón de "List" puede cambiar a ver los archivos en forma de lista.
- D. Con el botón de "Firma" se genera una firma digital del documento. Una vez seleccionado el documento, con el botón de "Verificar" puede revisar que sea el documento anteriormente firmado.
- E. Se muestra el hash del documento firmado.
- F. Con este botón puede regresar al menú anterior.

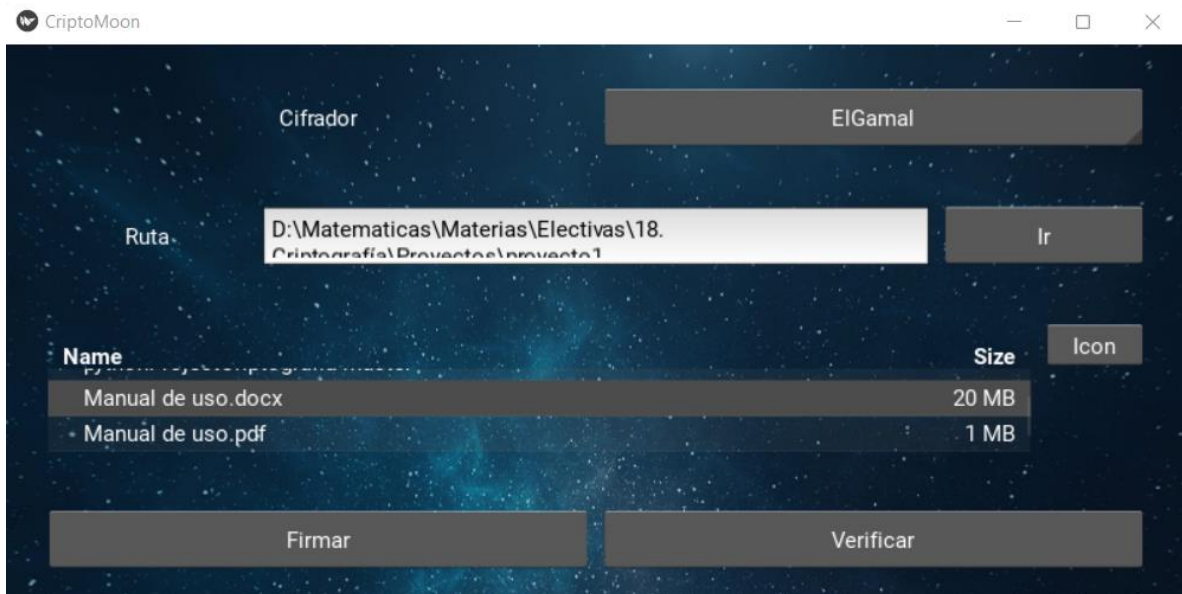
## 2.3 Ejemplo Firma Digital

Vamos a utilizar el método de ElGamal para firmar un documento.

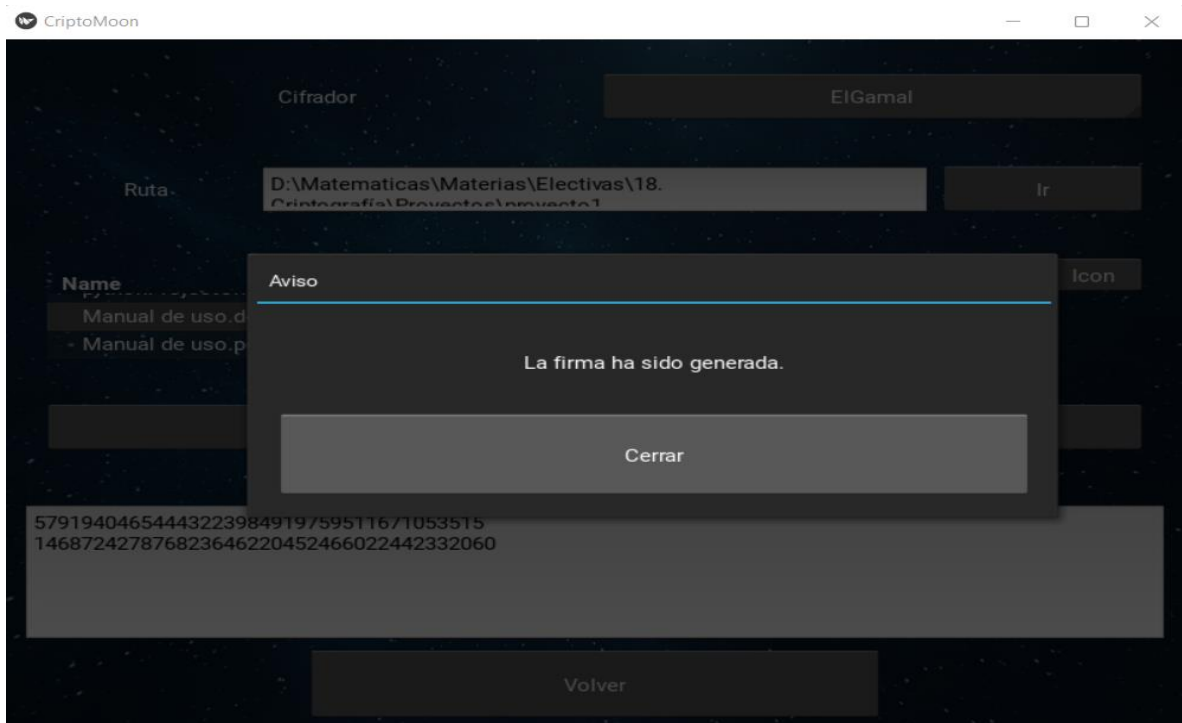
Copiamos la dirección donde se encuentra el documento y le damos a ir.



Pinchamos "List" y seleccionamos el archivo deseado. En este caso, seleccionamos es documento.



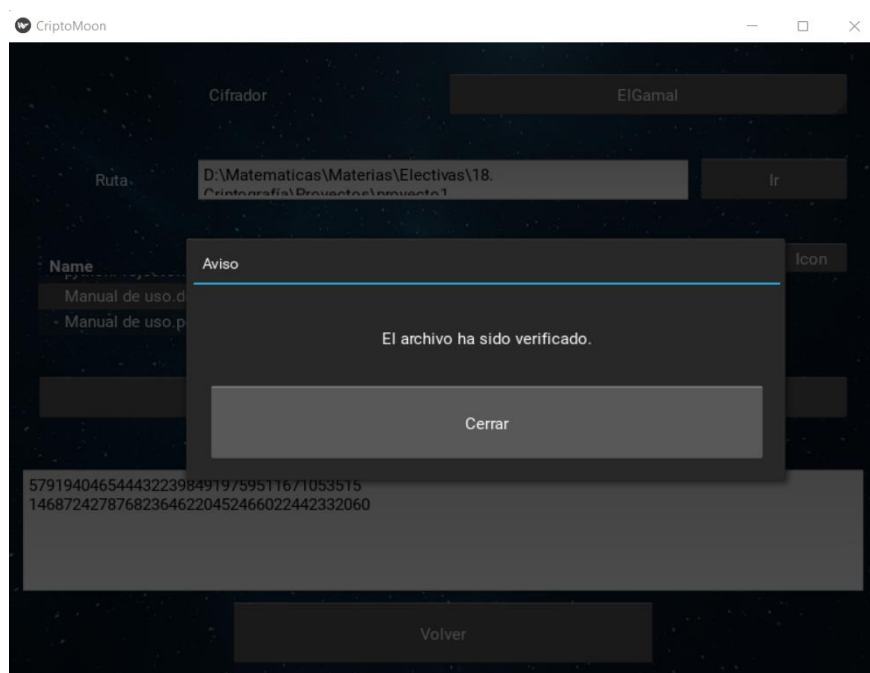
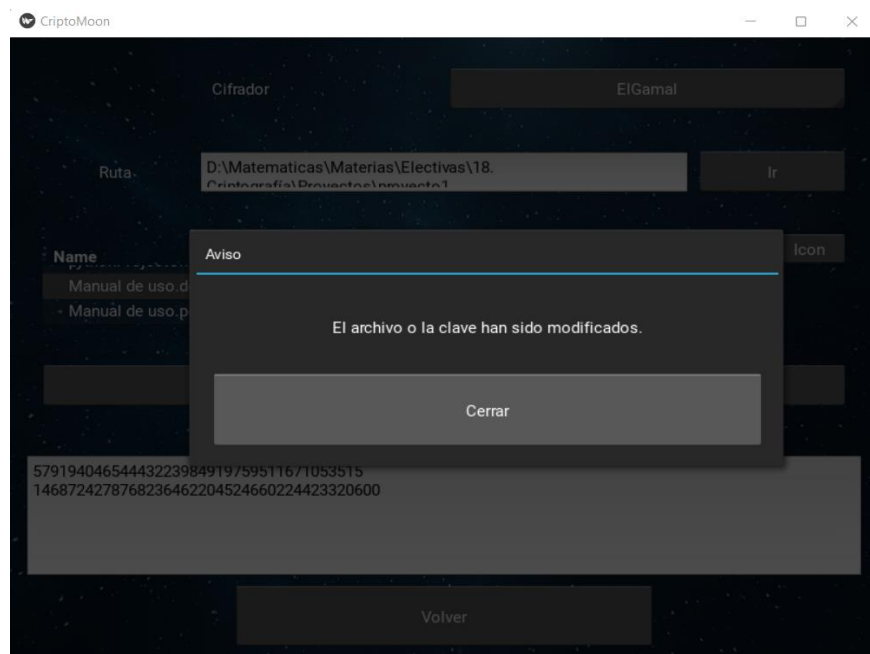
Al darle firmar sale una ventana emergente y se muestra el hash del documento.





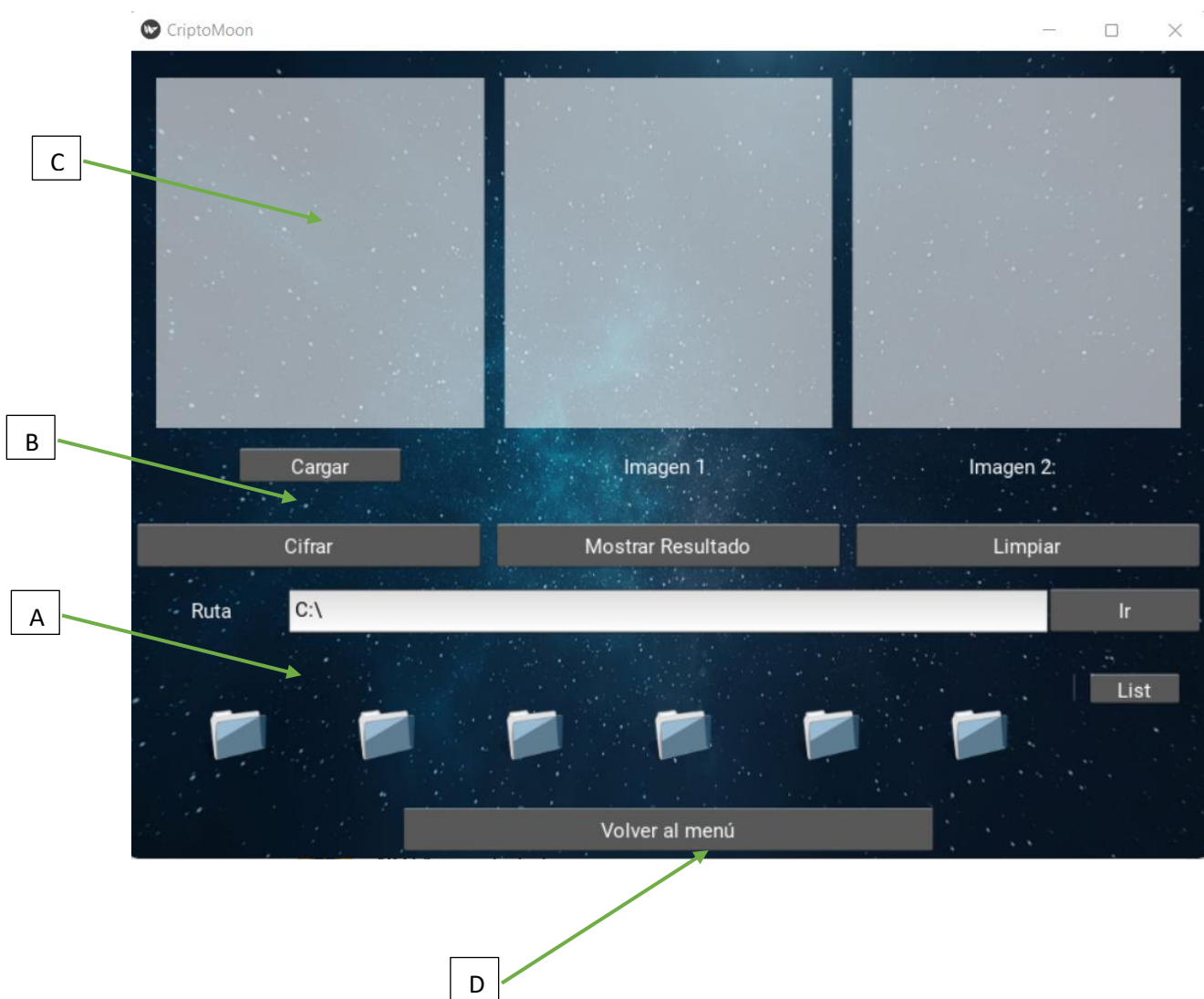
Para verificar el documento, se selecciona el documento y se le da “Verificar”, si el documento no es el correcto o si se modifica el hash sale el aviso de error.

Si tanto el documento seleccionado como el hash es el correcto sale aviso de verificación correcta.



### 3 Imágenes

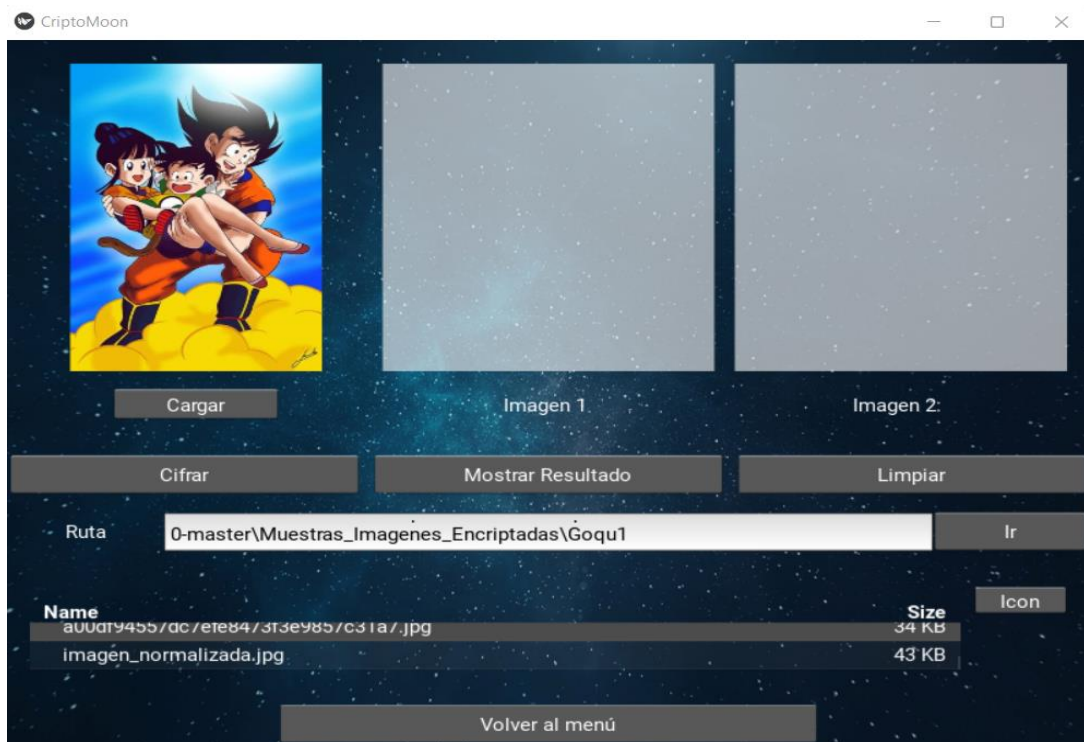
Para cifrar imágenes se tiene la siguiente interfaz.



- A. Se selecciona la imagen que desea cifrar.
- B. Al darle “Cargar” se muestra la imagen original. Al darle “Cifrar” se muestra la imagen normalizada a 8 colores y las transparencias con que queda cifrada la imagen. Al darle “Mostrar Resultado” se muestra, en vez de la imagen normalizada, la imagen producto de sobreponer las dos transparencias.
- C. Recuadros donde se cargan las imágenes.
- D. Para volver al menú.

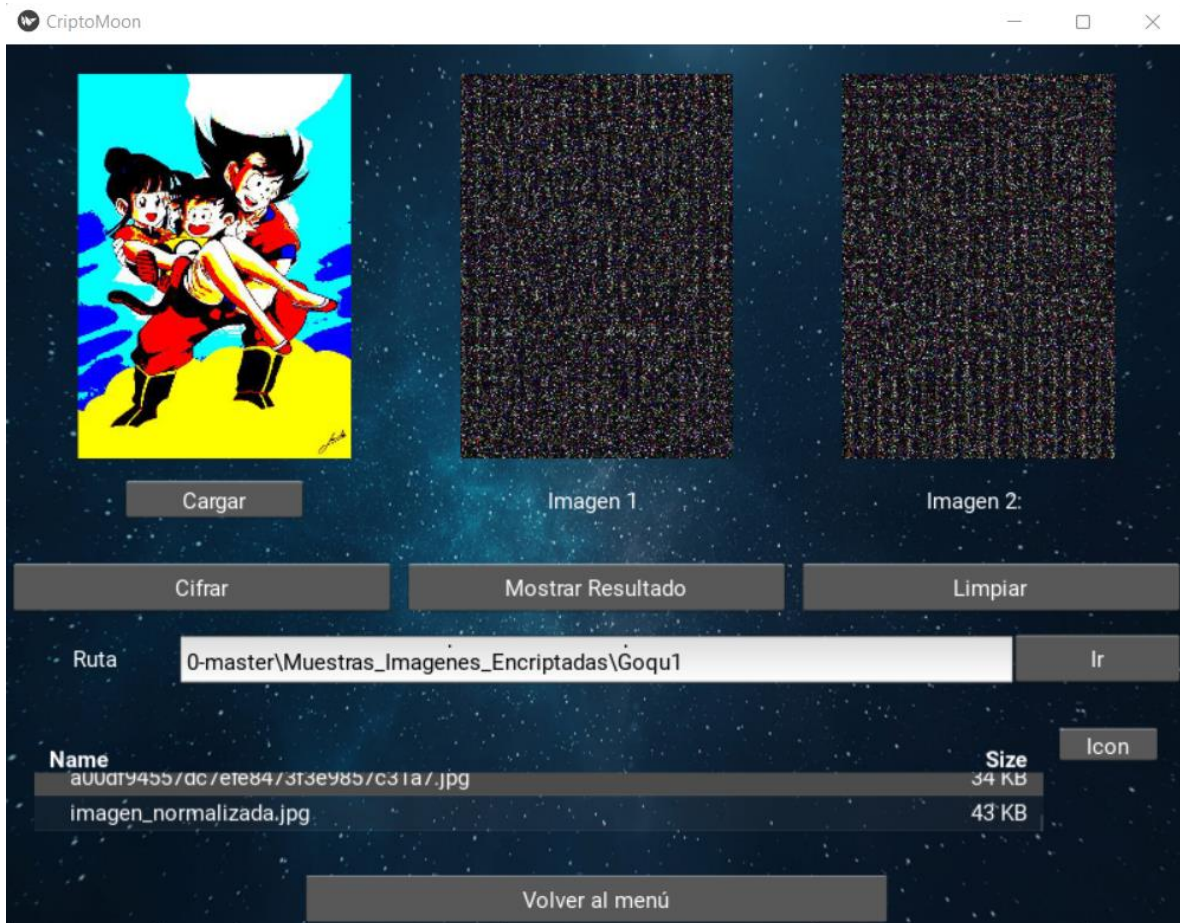
## 3.1 Ejemplo Imágenes

A continuación, se muestra la encriptación de una imagen. Primero se selecciona y se carga la imagen a encriptar.

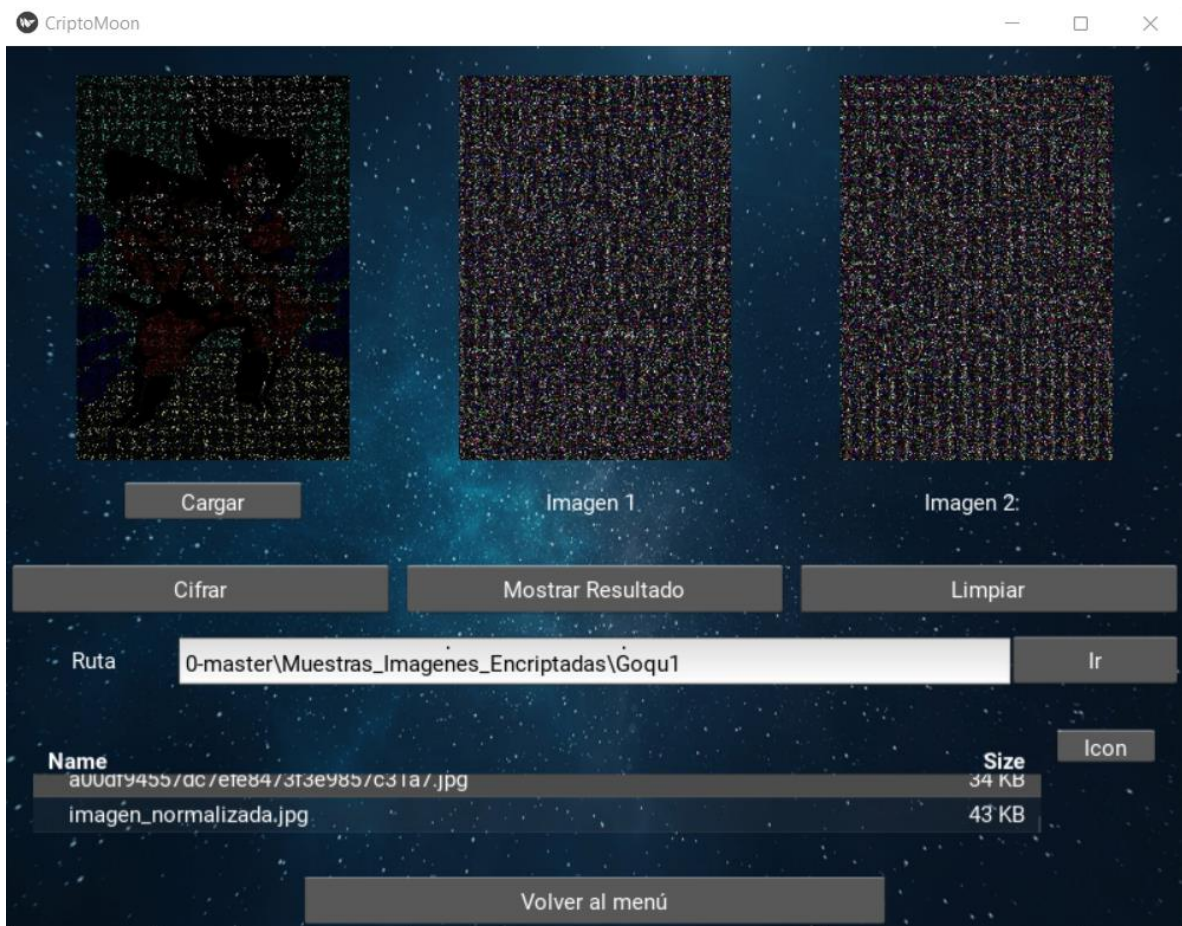




Al darle cifrar, obtenemos los siguientes resultados: la imagen normalizada y las dos transparencias.



Al darle “Mostrar resultado”, en el primer recuadro se carga la imagen descifrada.



Para ver mejor el resultado puede ir a la dirección donde descargo el archivo y allí encontrara una imagen llamada T1T2.

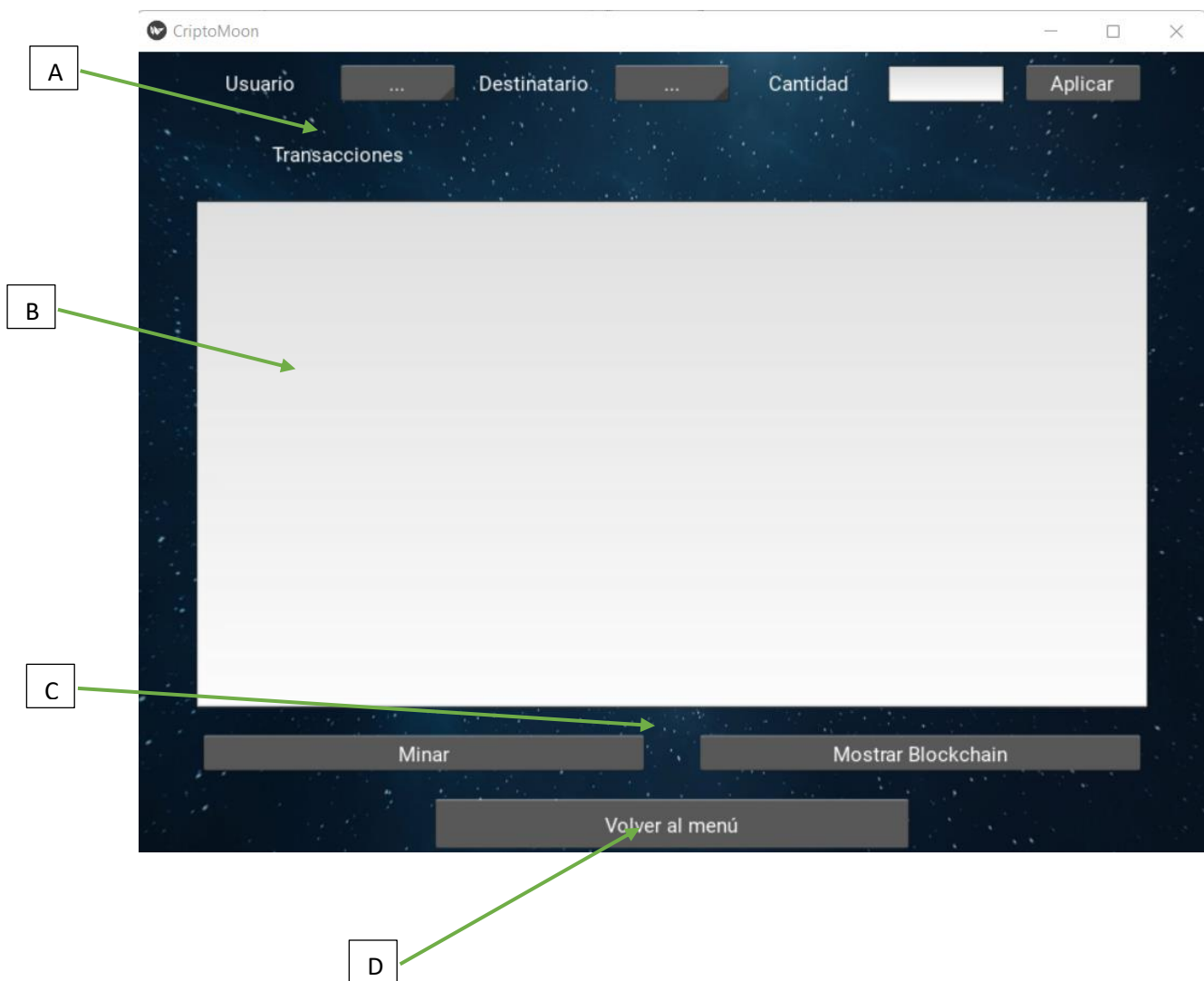






## 4. Moon Coins

A continuación se muestra la interfaz para simular transacciones con una criptomoneda.



- A. De una lista desplegable se puede seleccionar el origen y el destino de la transacción, así como el monto de esta. Al darle “Aplicar” se ejecuta muestra la transacción en pantalla.
- B. Se muestra la transacción. Aparece las identidades tanto del remitente como del destinatario, así como el valor y la fecha de la transacción.
- C. Al minar el programa coje grupo de a tres transacciones para crear un bloque. Las restantes siguen en pantalla hasta completar tres transacciones. En “Mostrar Blockchain” se muestran los bloques contruidos.
- D. Para volver al menú anterior.

## 4.1 Ejemplo Moon Coins

A continuación se muestra como generar transacciones y como minarlas.

Primero se generan 5 transacciones.

The screenshot shows the 'CriptoMoon' application window. At the top, there are input fields for 'Usuario' (Agustin), 'Destinatario' (Daniel), and 'Cantidad' (1), followed by an 'Aplicar' button. Below this, the 'Transacciones' section displays two transaction details. Each detail includes a 'Remitente' address, a 'Destinatario' address, a 'Valor' of 10.0, and a 'Tiempo' of 2022-06-28 08:56:23.381462. At the bottom, there are three buttons: 'Minar', 'Mostrar Blockchain', and 'Volver al menú'.

Usuario: Agustin Destinatario: Daniel Cantidad: 1 Aplicar

Transacciones

Remitente:  
b'30819f300d06092a864886f70d010101050003818d0030818902818100b25f006317ad2acd3949b28cbd589b34288460ff0c019606365fcaae88a269bd1f644645a8b5631371b60fe4e32fc2564e4ffef46405b476181a50ce93e4fee665c3e8ee859762fe6d11e4160ae366485dfd4a053abfe64e42f294ceda3b9b1e4e363b761bbcf8fec6a390078f3da4d89cd065063bed3ee57e344882736933cb0203010001'

Destinatario:  
b'30819f300d06092a864886f70d010101050003818d0030818902818100c3bda4899afb76fd8b8abc18cfc31ad4d50bc9ef8356aba652f63853d88fbcfb184715140acd65d543fab1ca621aed6ec680fceac7f8bd900e65228ce9d784f476e5ef0f3e390f824d8afec6ad1bce494cbac690f98f9271cb852ac96fd3373de14098e22347981de5bbcf881faedc1b6fab6d9953ef01372324507508eb60550203010001'

Valor: 10.0  
Tiempo: 2022-06-28 08:56:23.381462

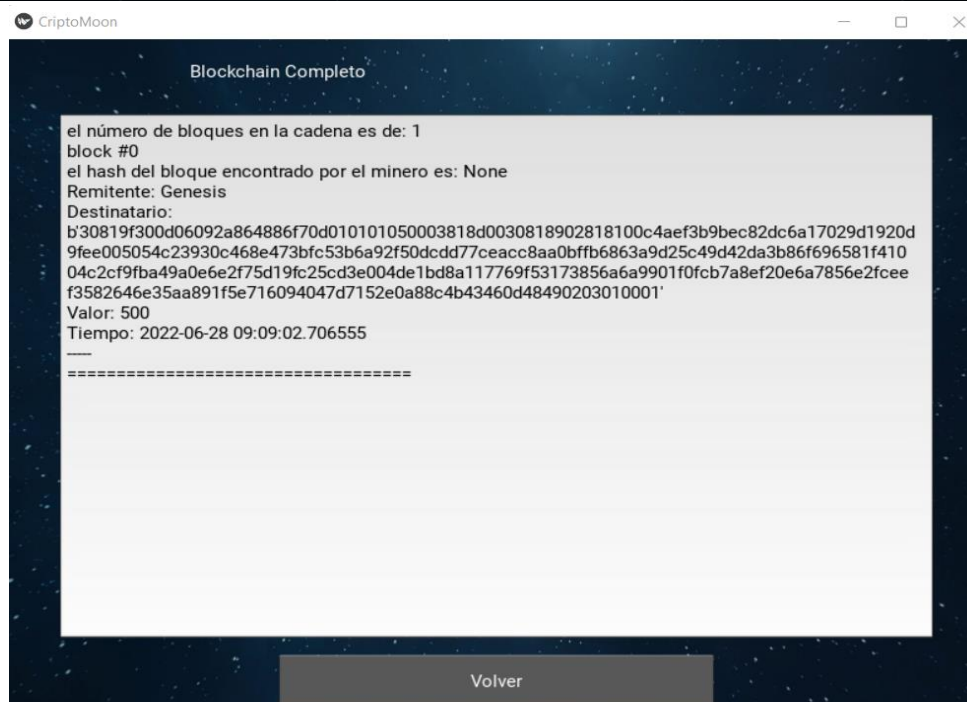
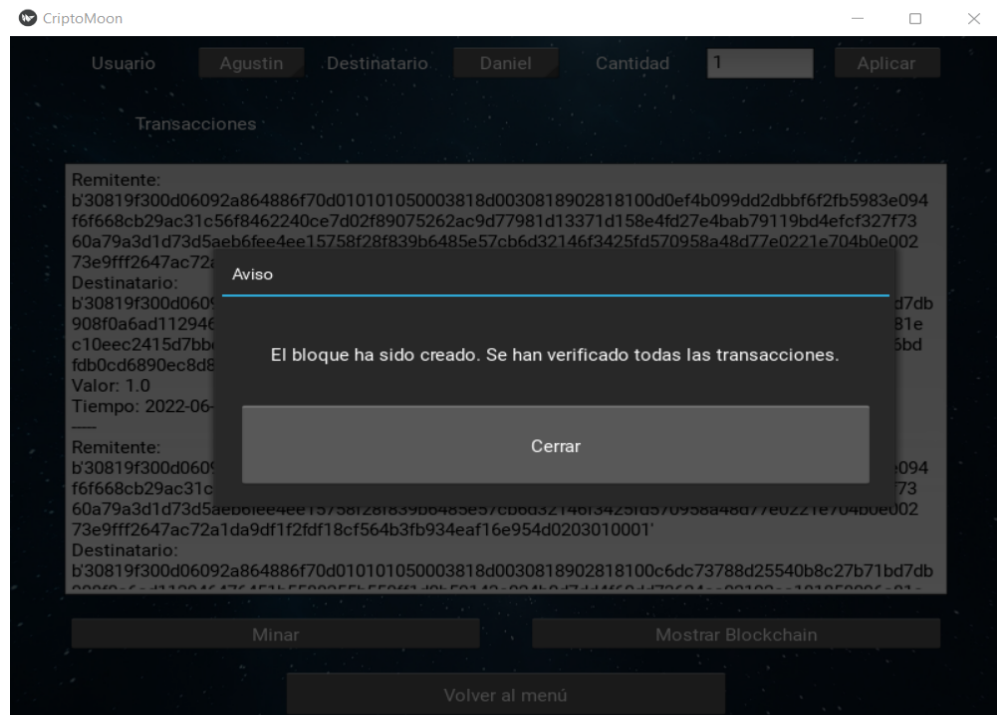
Remitente:  
b'30819f300d06092a864886f70d010101050003818d0030818902818100c6dc73788d25540b8c27b71bd7db908f0a6ad112946476451b5588255b550ff1d0b59143c024b0d7dd4f60dd73624ca02192ca181858096a81ec10eec2415d7bbd8461d8fb752ef58a8228bbb8b0882e193699b369a415e4437952b935a6d1e3fa9fc8a6bdfdb0cd6890ec8d8585b9d900df1e20d52ec37641e2d78bdb215c090203010001'

Destinatario:  
b'30819f300d06092a864886f70d010101050003818d0030818902818100c3bda4899afb76fd8b8abc18cfc31ad4d50bc9ef8356aba652f63853d88fbcfb184715140acd65d543fab1ca621aed6ec680fceac7f8bd900e65228ce9d784f476e5ef0f3e390f824d8afec6ad1bce494cbac690f98f9271cb852ac96fd3373de14098e22347981de5bbcf881faedc1b6fab6d9953ef01372324507508eb60550203010001'

Minar Mostrar Blockchain

Volver al menú

Al darle “Minar” se cogen las primeras 3 transacciones para crear el bloque y se dejan 2 en pantalla, a espera de completar las 3 transacciones para crear un segundo bloque.







NOTA en este link,

<https://www.youtube.com/watch?v=wTKGK0bpsOs>, puede ver un video de su funcionamiento. Gracias por elegirnos.