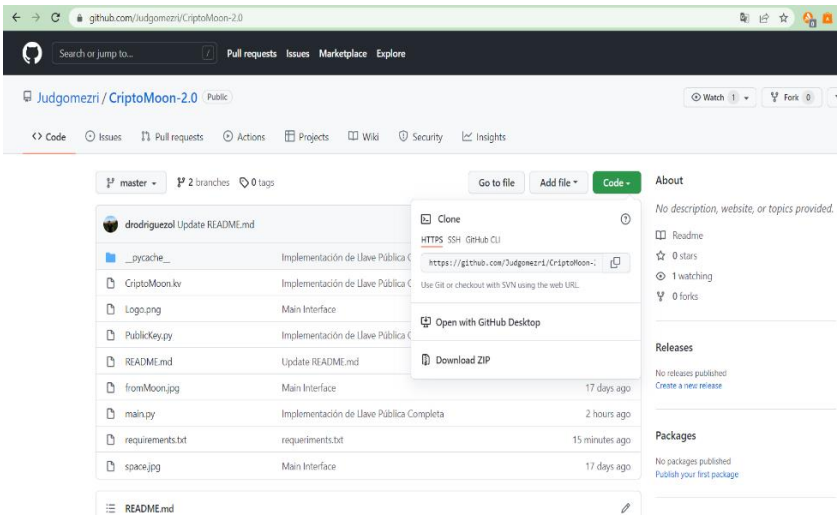
Manual de uso

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.

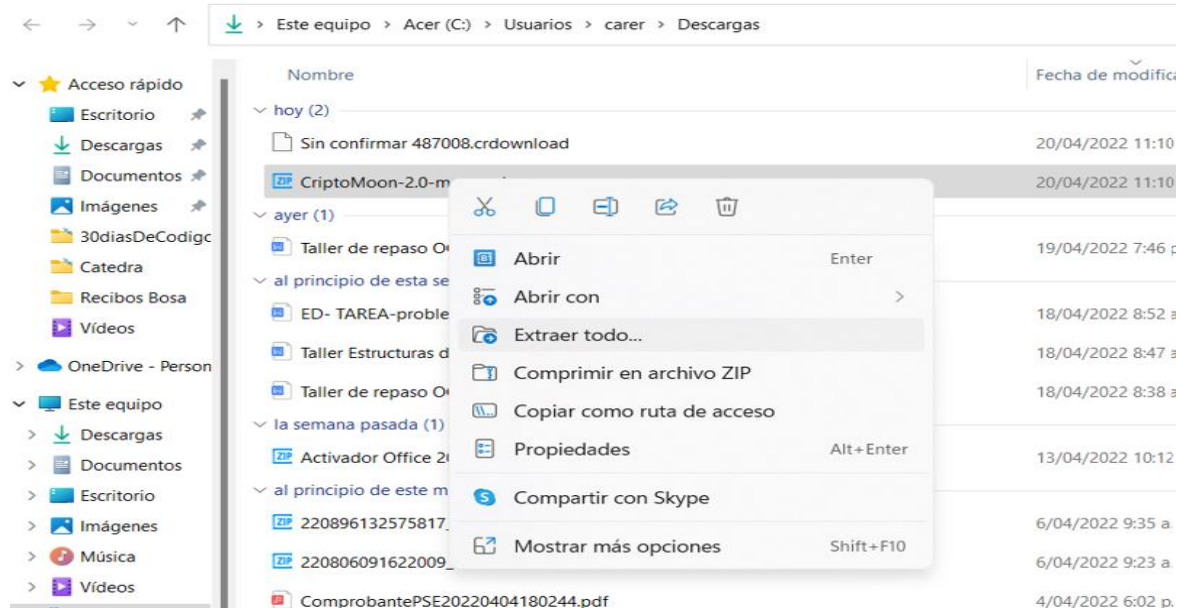
⚠️ IMPORTANTE Asegúrese que su computador tenga instalado Python 3.0 o superior.

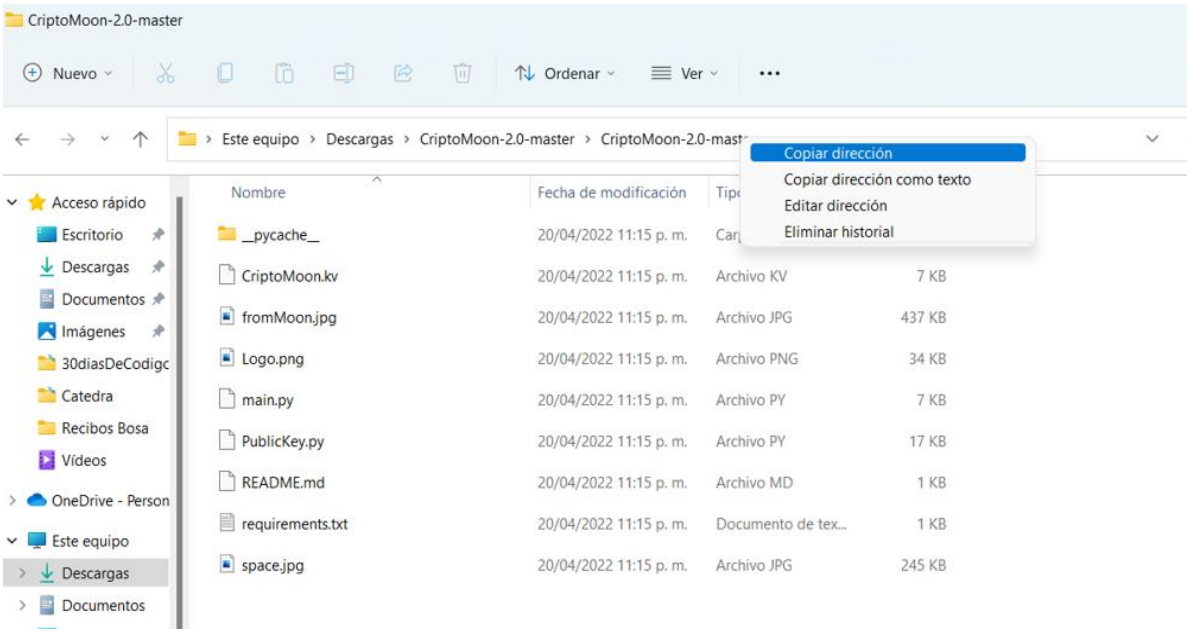
1. Instalación

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

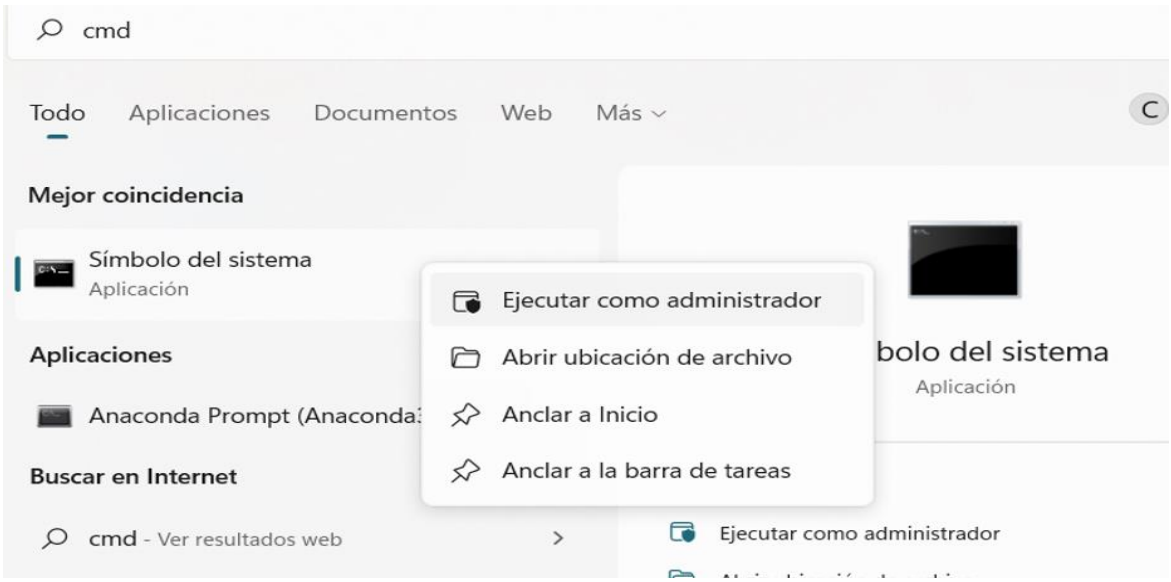


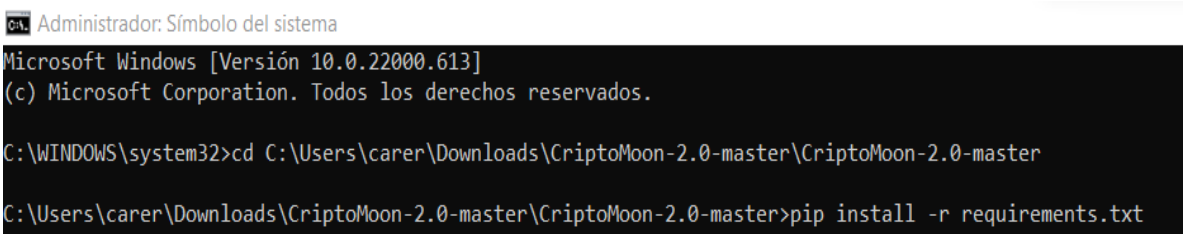
Descomprima el archivo descargado y copie la dirección de su ubicación.





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

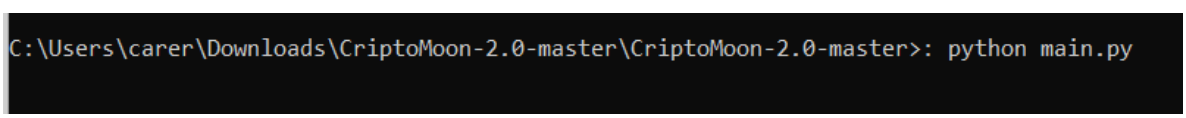




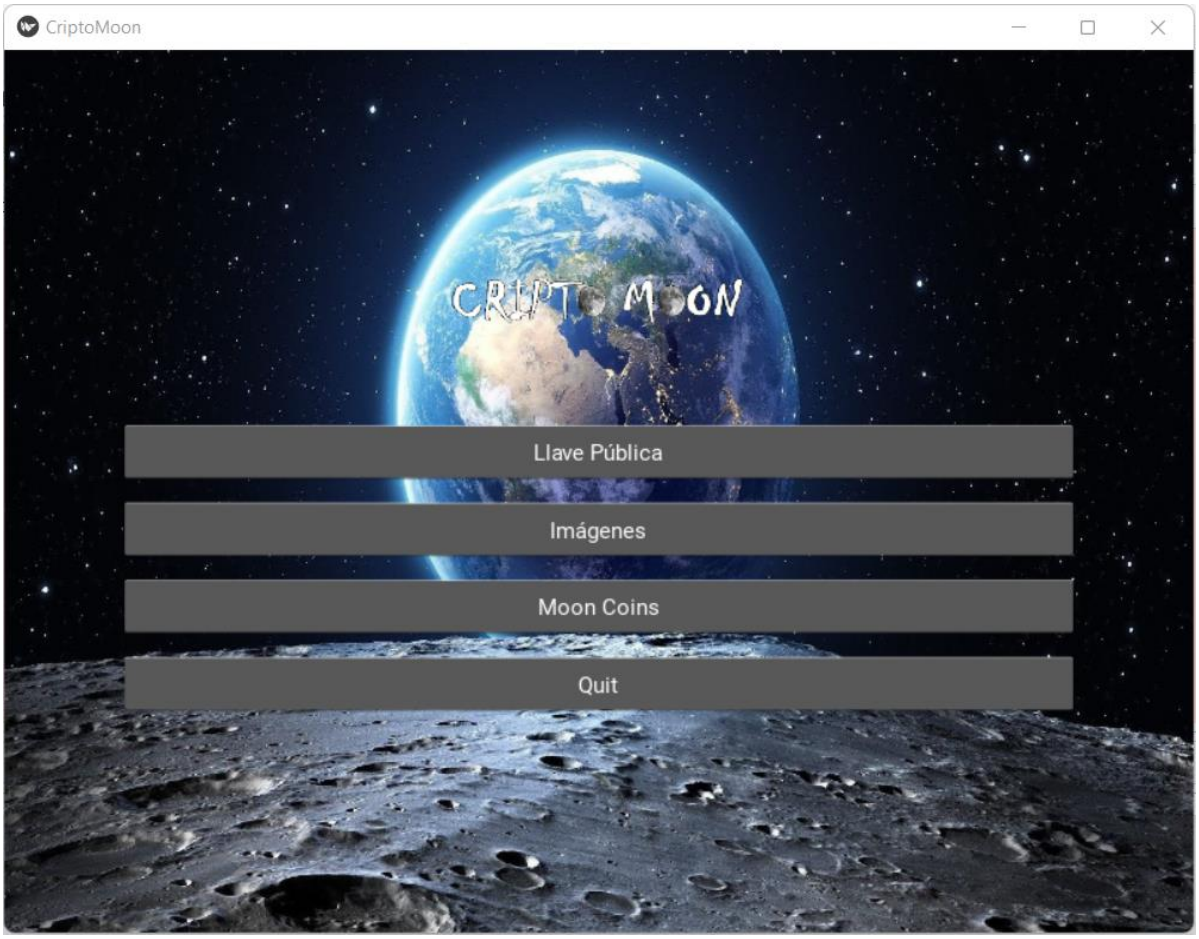
Una vez instalados los requerimientos puede empezar a usar la aplicación.

2. Utilizar la aplicación

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

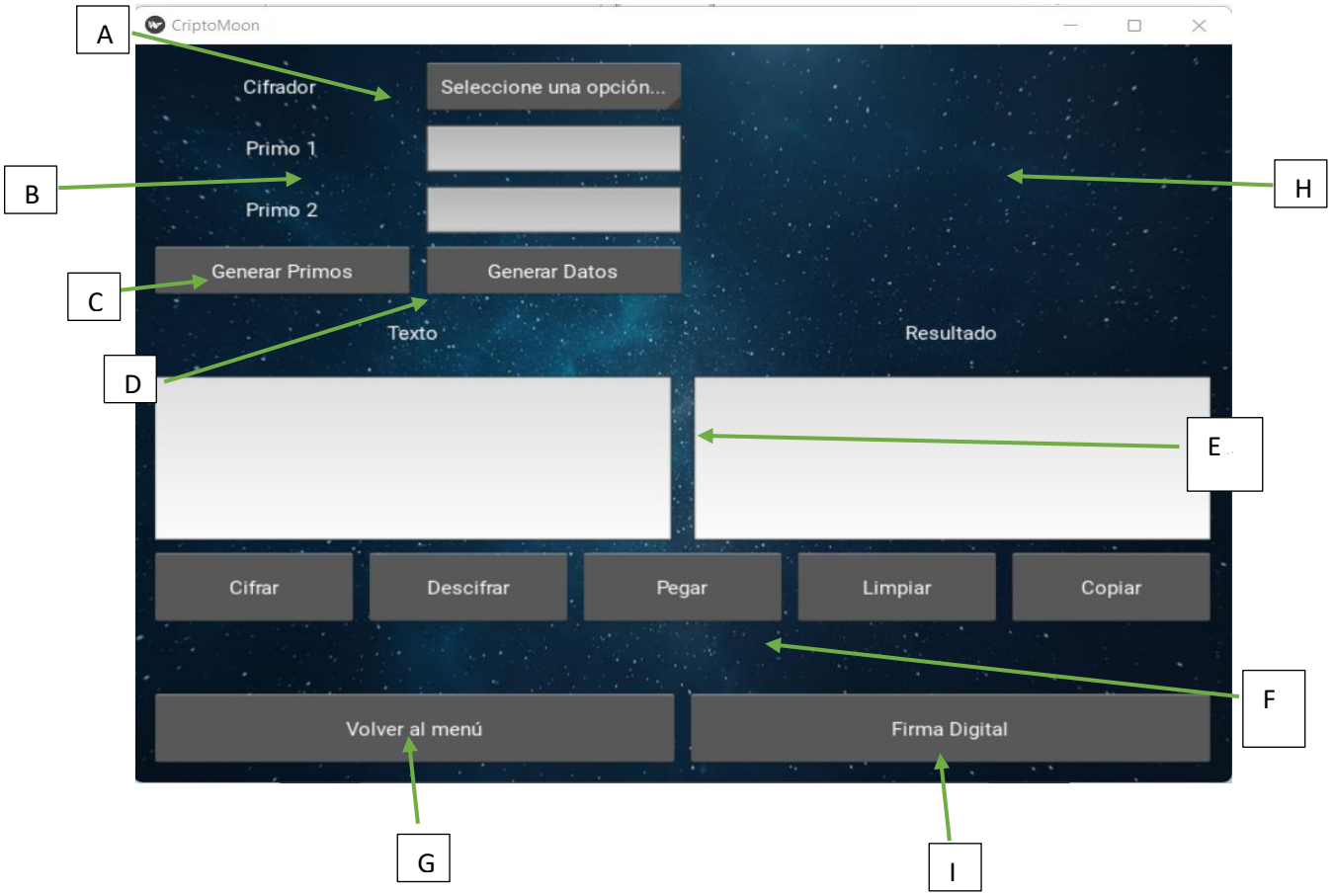


Así, se desplegará la aplicación. Puede pinchar en “Llave Pública” para empezar a cifrar mensajes y firmar documentos digitales; en “Imágenes” para cifrar imágenes; en “Moon Coins” para simular una criptomoneda o en “Quit” para salir.



2. Lave Pública

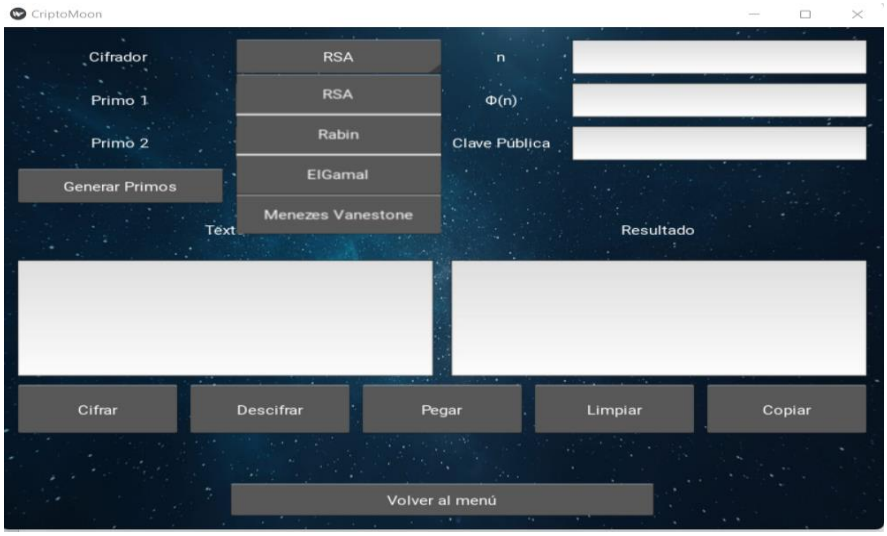
Al pinchar en “Llave Pública” tendrá las siguientes funcionalidades.



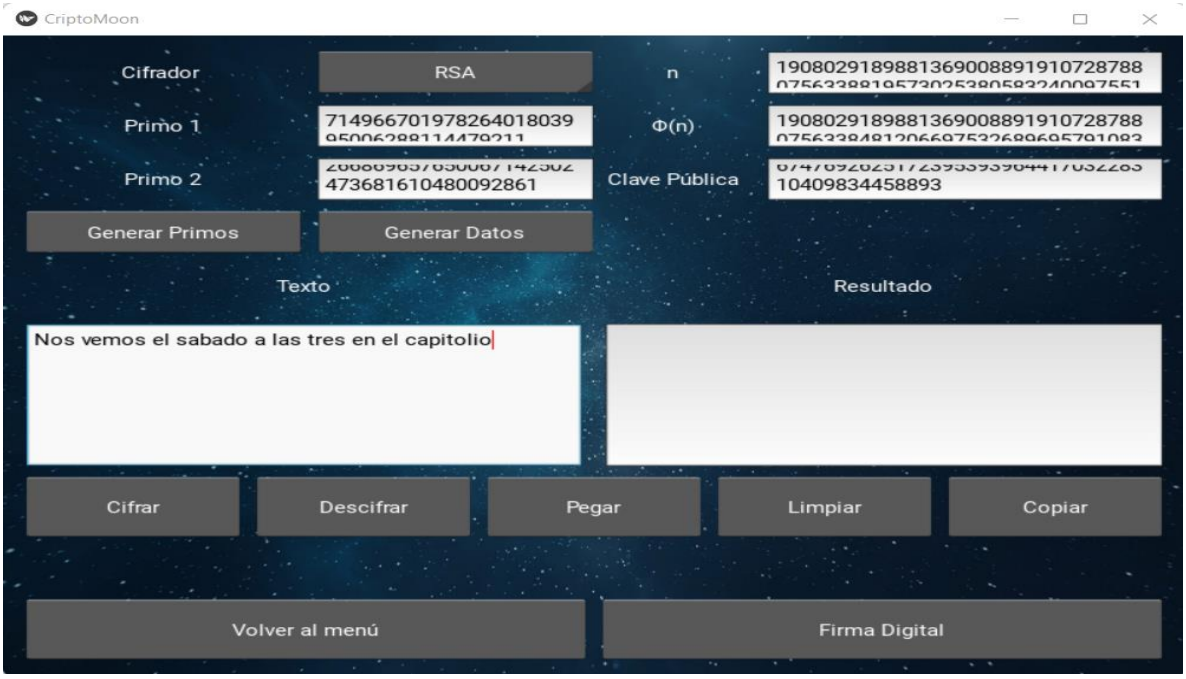
A. En este desplegable puede elegir entre 4 diferentes formas de cifrar.
B. En esta parte están las casillas donde se ingresan los números que son la base para poder cifrar y descifrar. Si conoce de criptografía puede ingresarlos usted mismo, o puede generarlos automáticamente.
C. Con este botón puede 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

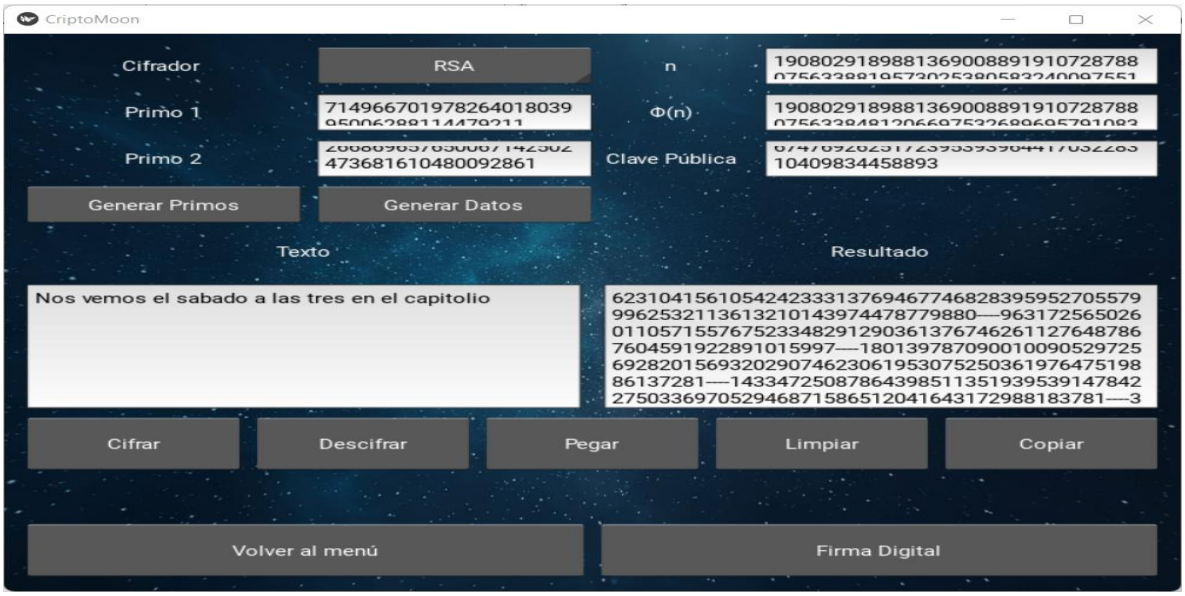
Vamos a cifrar con el método RSA. En A Seleccionamos RSA.



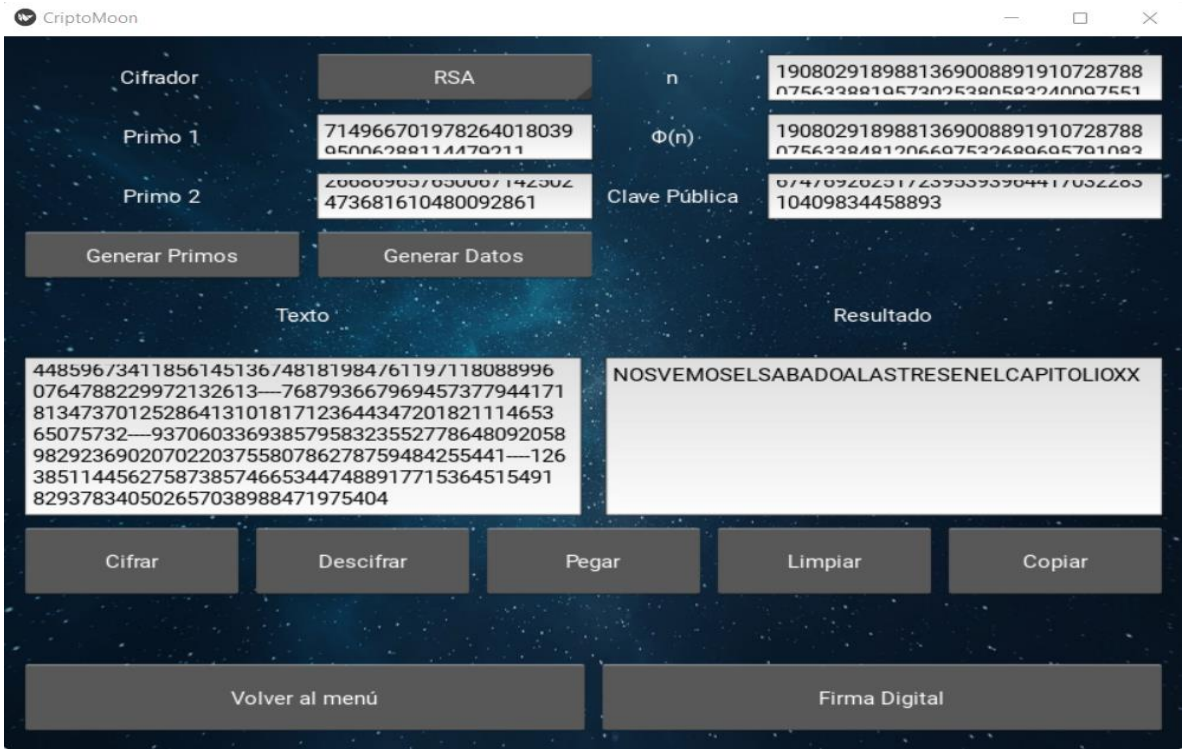
Le damos a genera primos, generar datos e ingresamos el mensaje a cifrar.



Le damos a cifrar y obtenemos el texto cifrado.

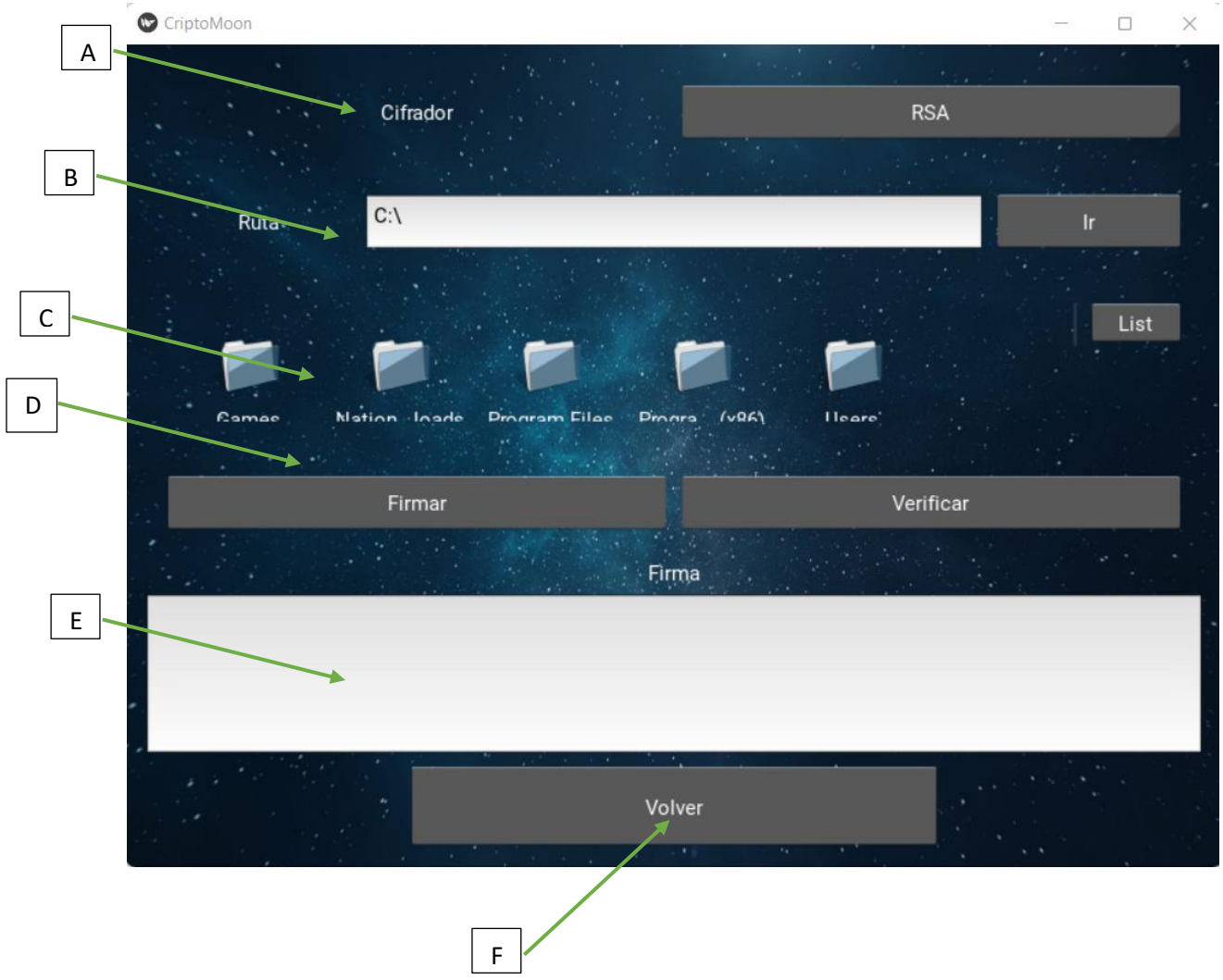


Luego, para descifrar el mensaje, podemos copiar, limpiar pegar y descifrar.



2.2 Firma Digital

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

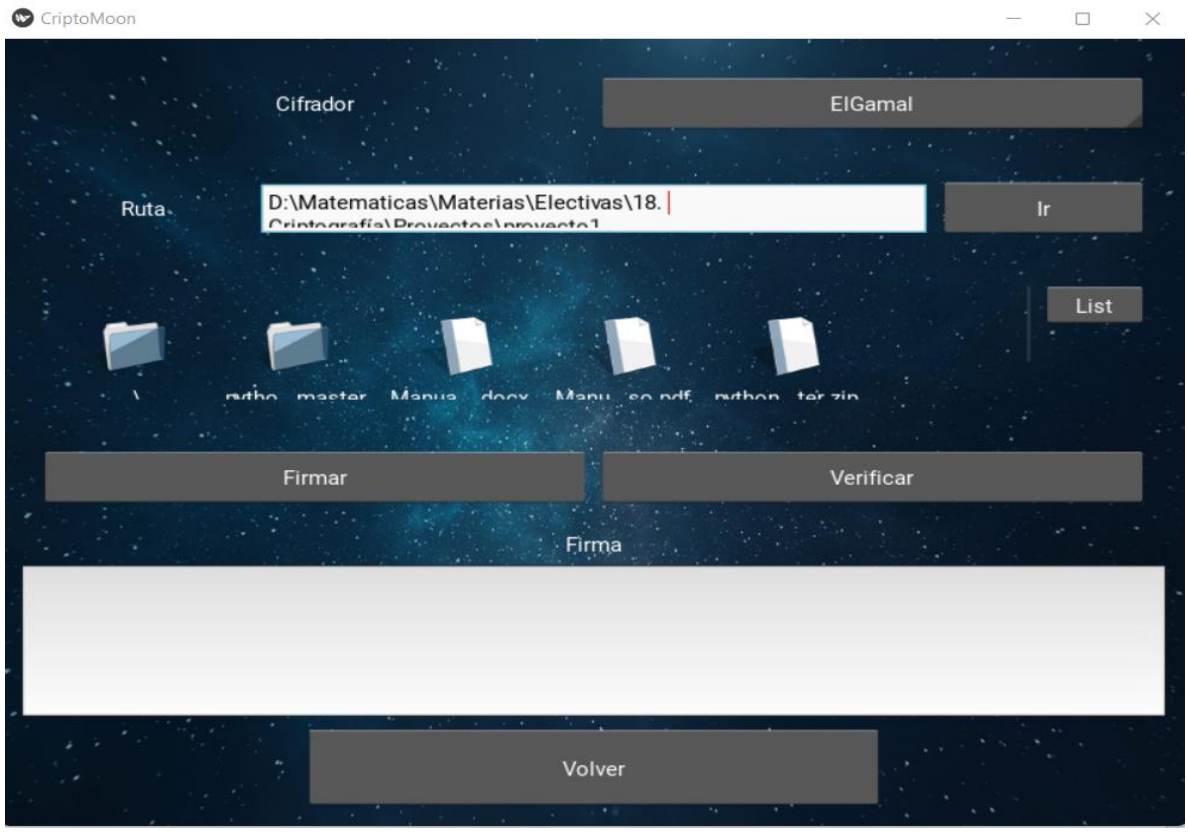


A. Se elije el tipo de cifrador que desea utilizar.
B. Puede copiar o escribir la ruta donde se encuentra el archivo y darle ir para que se carguen en C los archivos que hay en dicha dirección.
C. Puede pinchar en las carpetas para y seleccionar el archivo que desea firmar. Con el botón de “List” puede 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.

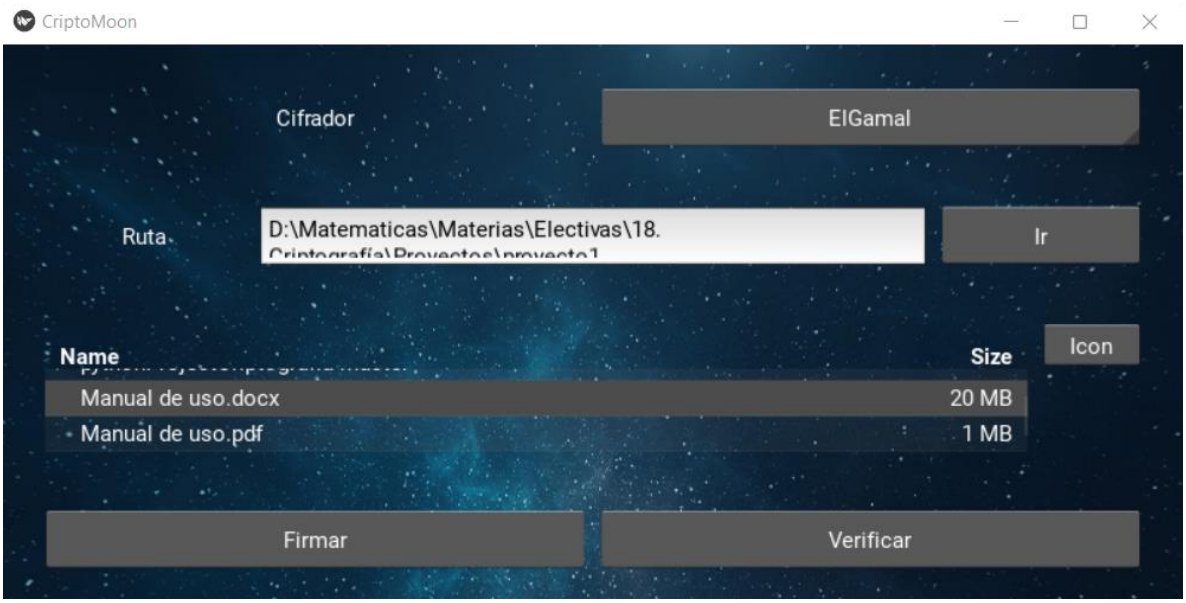
2.3 Ejemplo Firma Digital

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

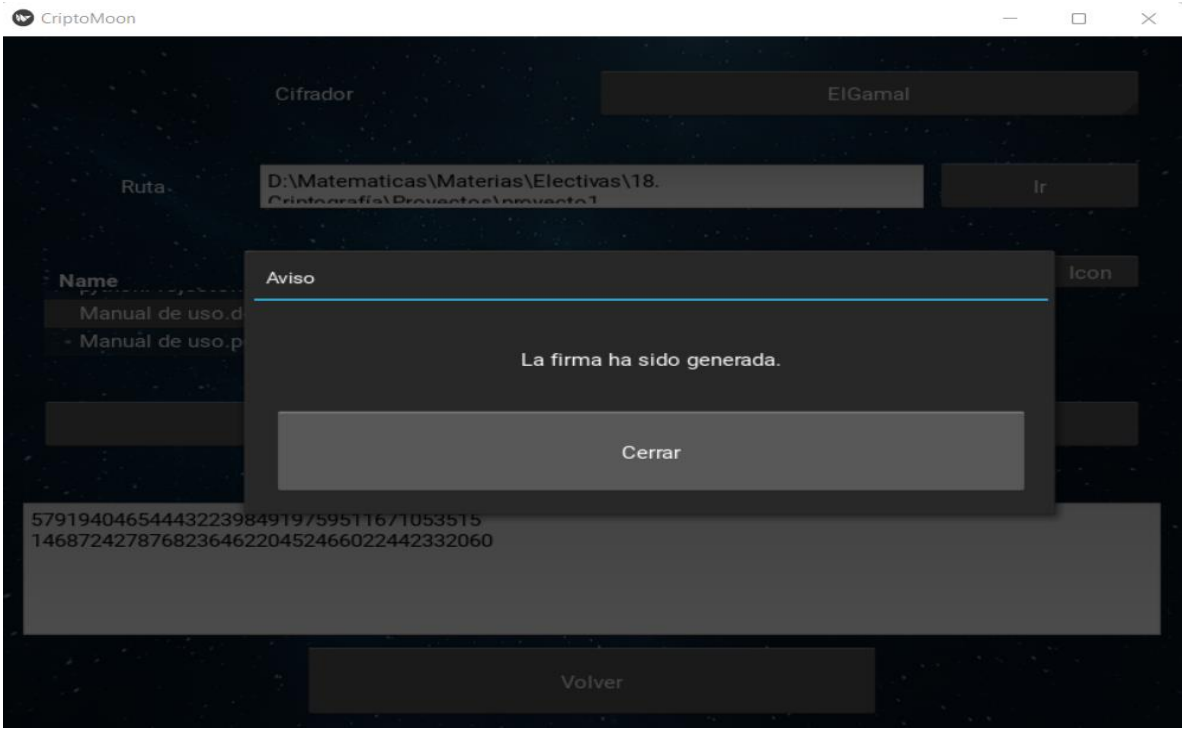
Copiamos la dirección donde se encuentra el documento y le damos a ir.



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

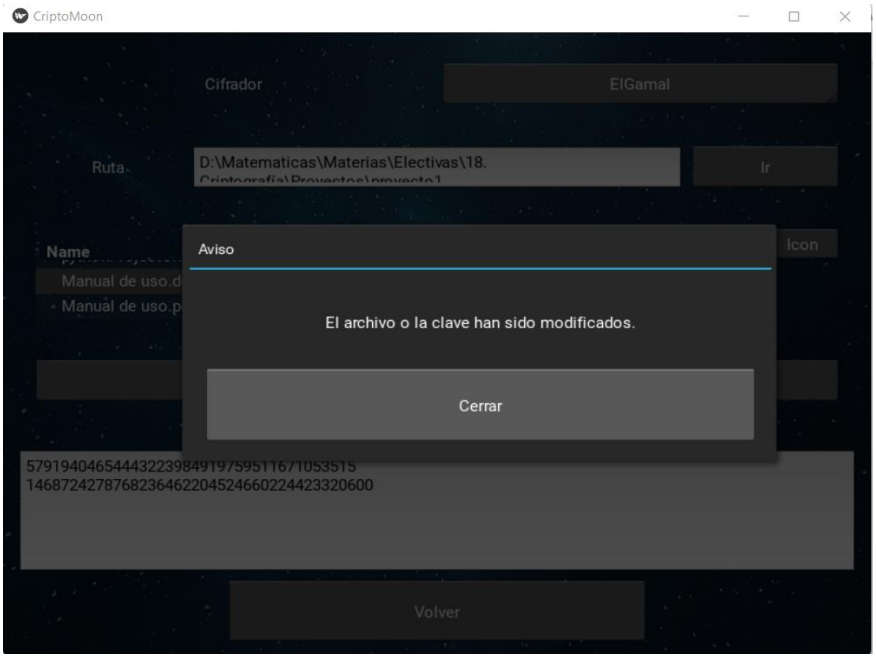


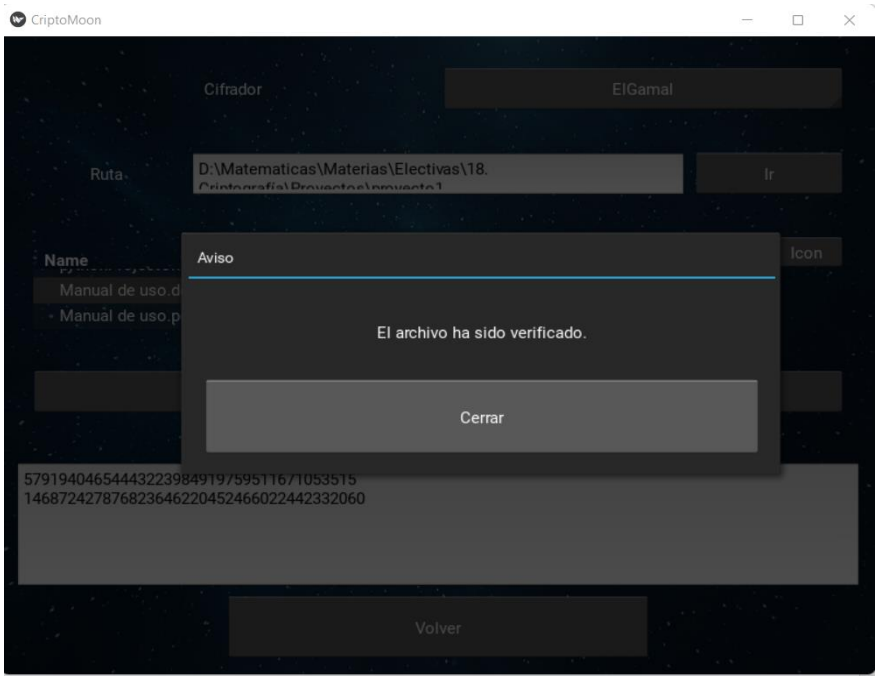
Al darle firmar sale una ventana emergente y se muestra el hash del documento.



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.

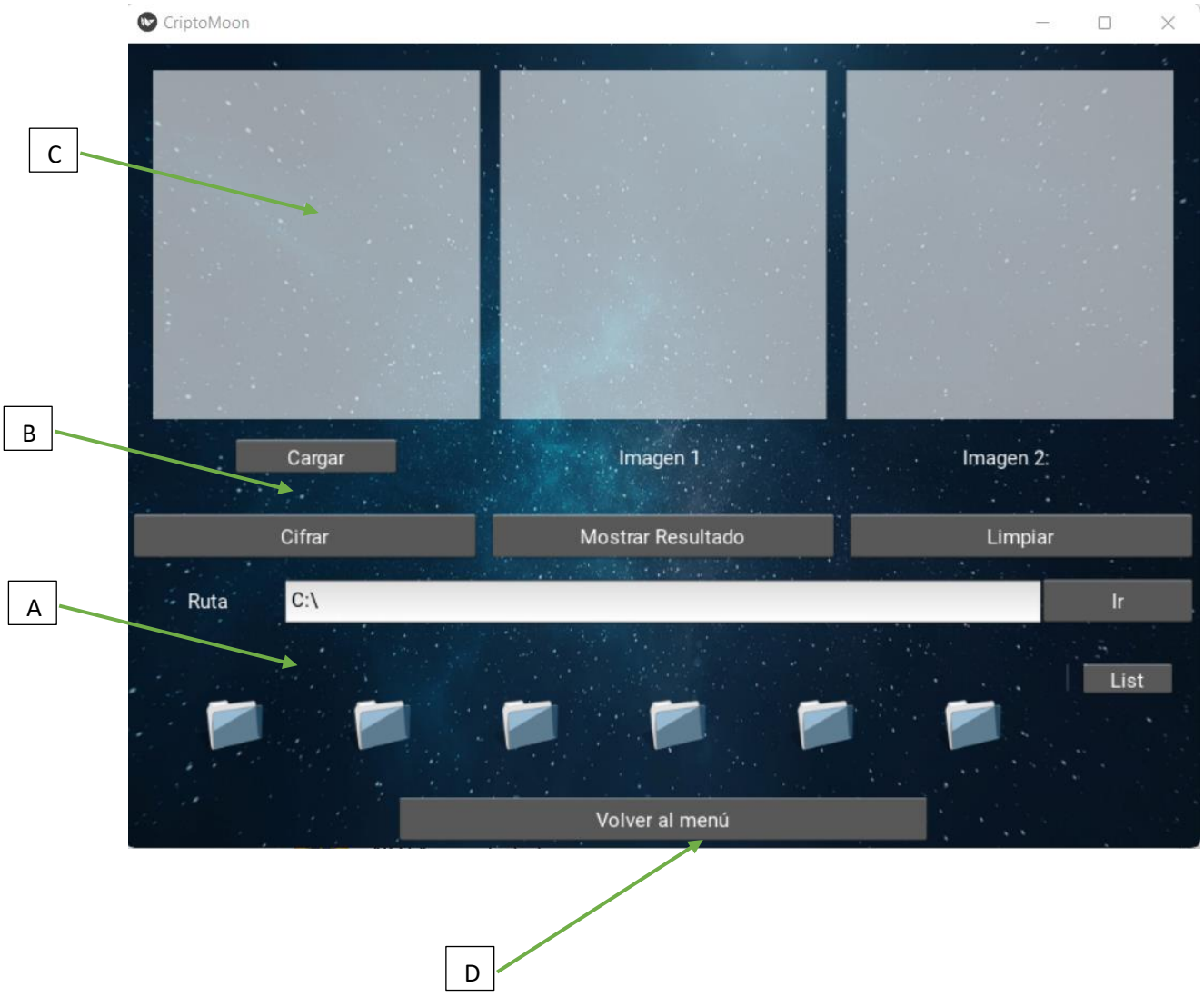
Si tanto el documento seleccionado como el hash es el correcto sale aviso de verificación correcta.





3 Imágenes

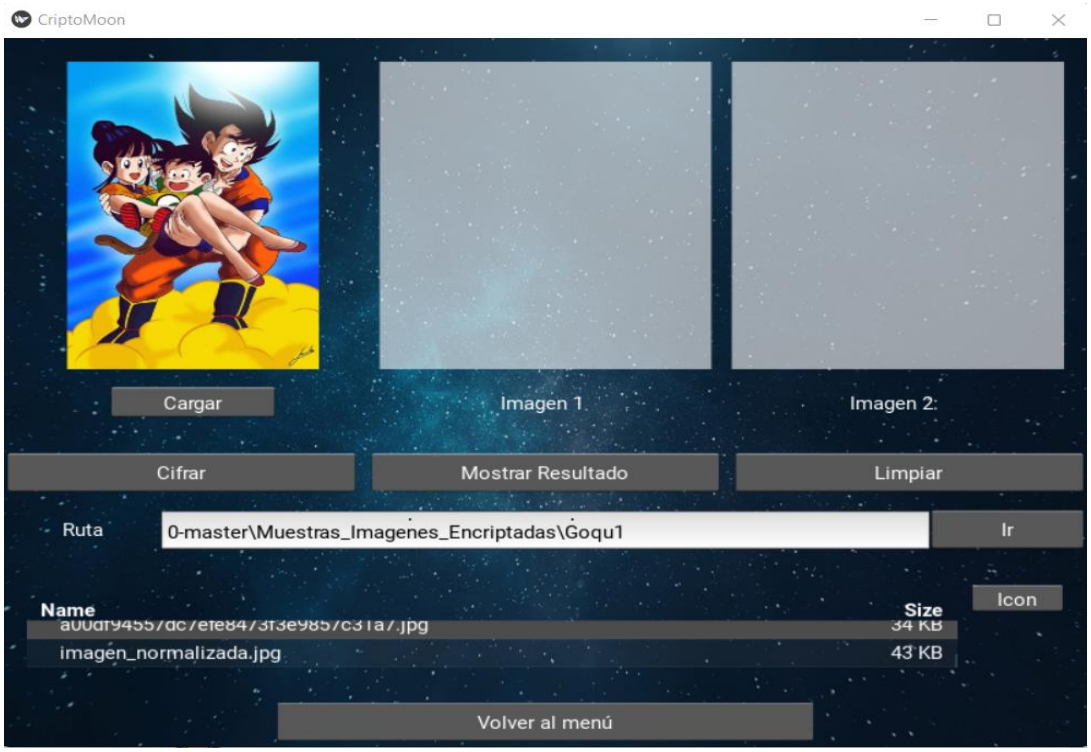
Para cifrar imágenes se tiene la siguiente interfaz.



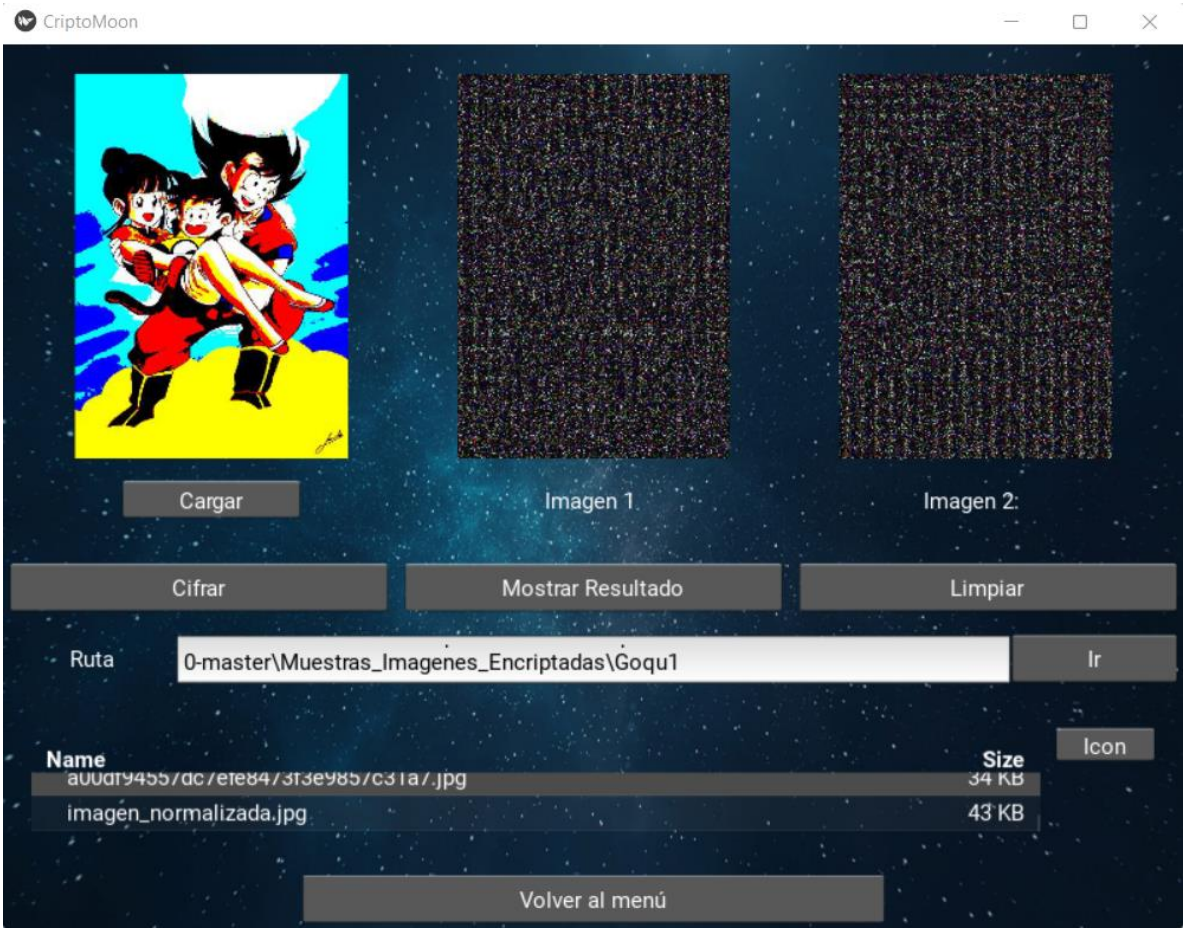
A. Se selecciona la imagen que desea cifrar.
B. Al darle “Cargar” se muestra la imagen original. Al darle “Cifrar” se muestra la imagen normalizada a 8 colores y las trasparencias con que queda cifrada la imagen. Al darle “Mostrar Resultado” se muestra, en vez de la imagen normalizada, la imagen producto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

3.1 Ejemplo Imágenes

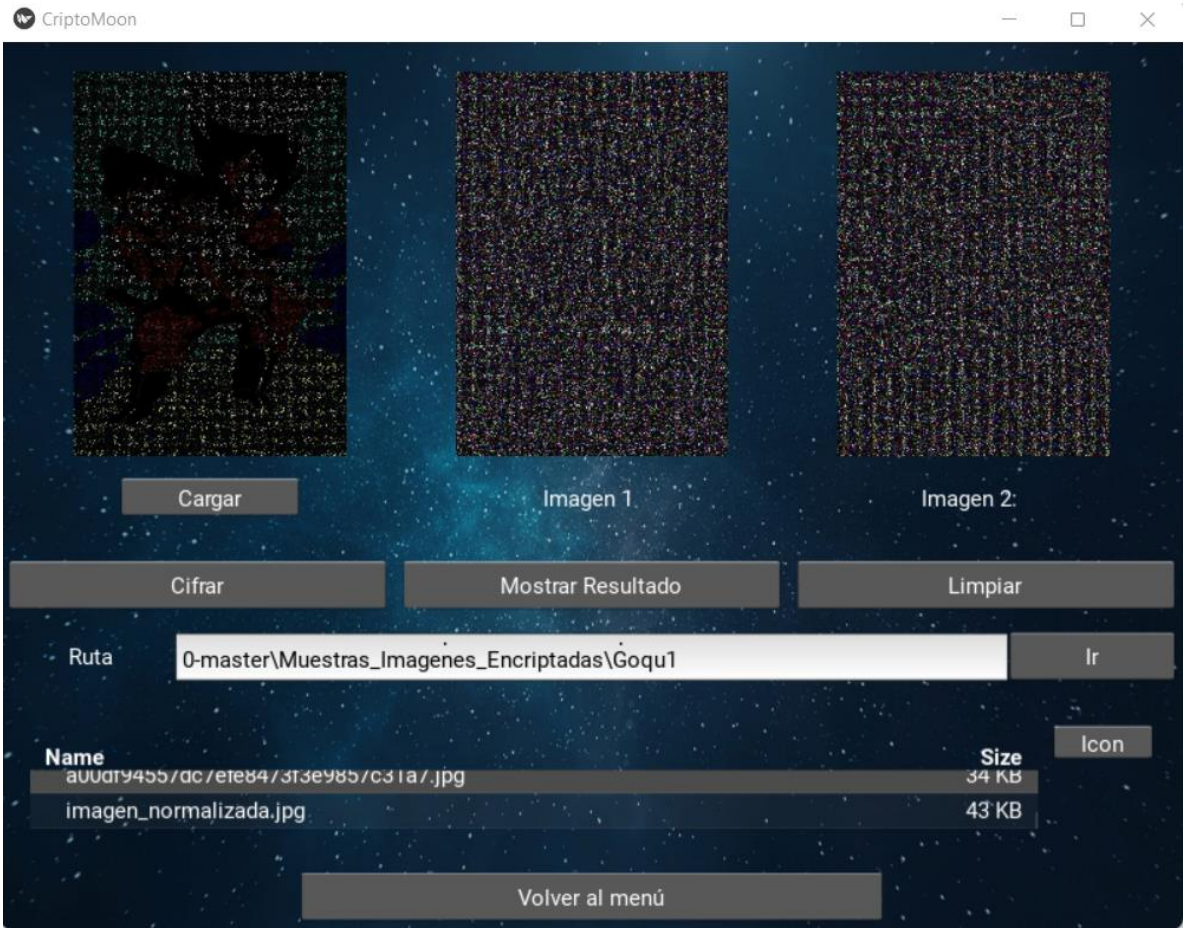
A continuación, se muestra la encriptación de una imagen. Primero se selecciona y se carga la imagen a encriptar.



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



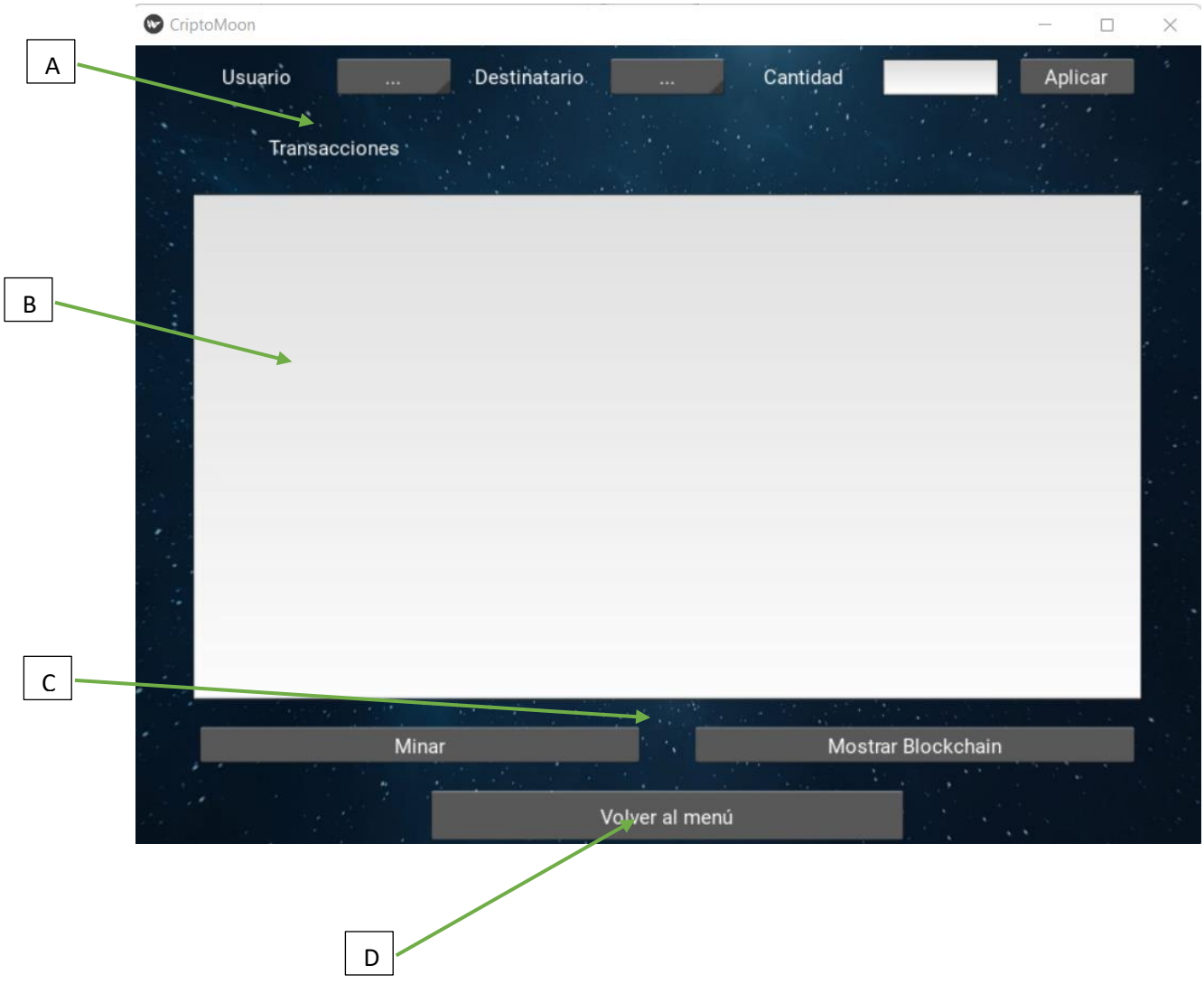
Al darle “Mostrar resultado”, en el primer recuadro se carga la imagen descifrada.



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.

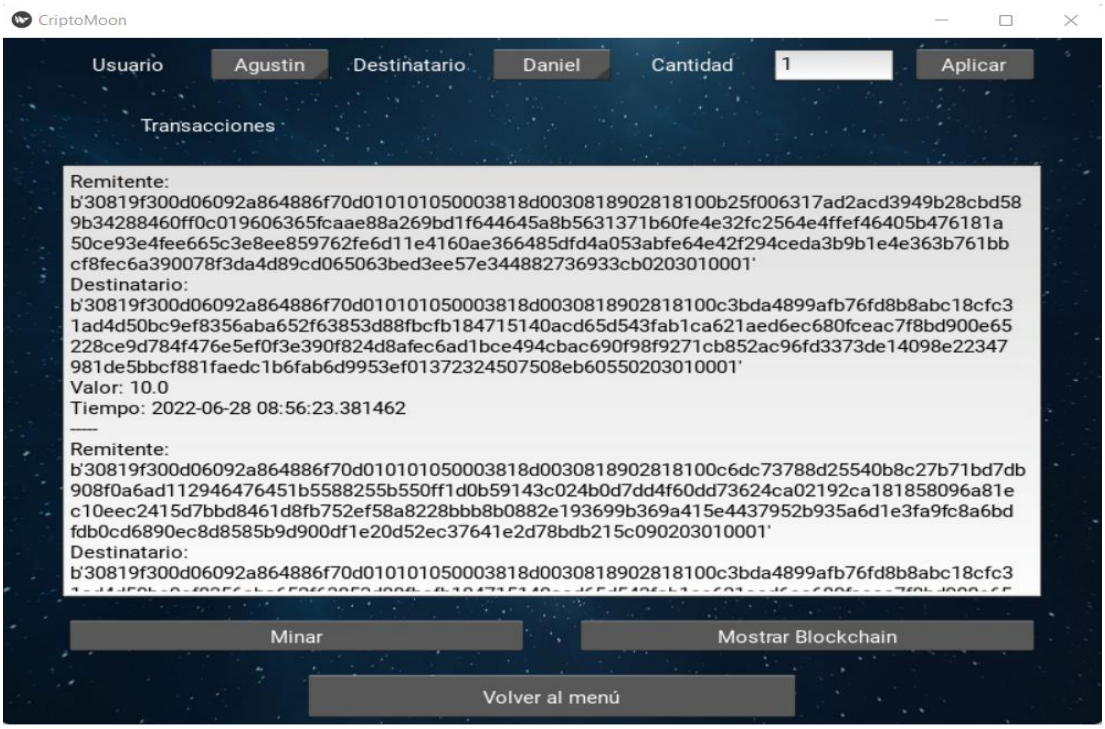


A. De una lista desplegable se puede seleccionar el origen y el destino de la transacción, así como el monto de esta. Al darle “Aplicar” se ejecuta muestra la transacción en pantalla.
B. Se muestra la transacción. Aparece las identidades tanto del remitente como del destinatario, así como el valor y 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 construidos.
D. Para volver al menú anterior.

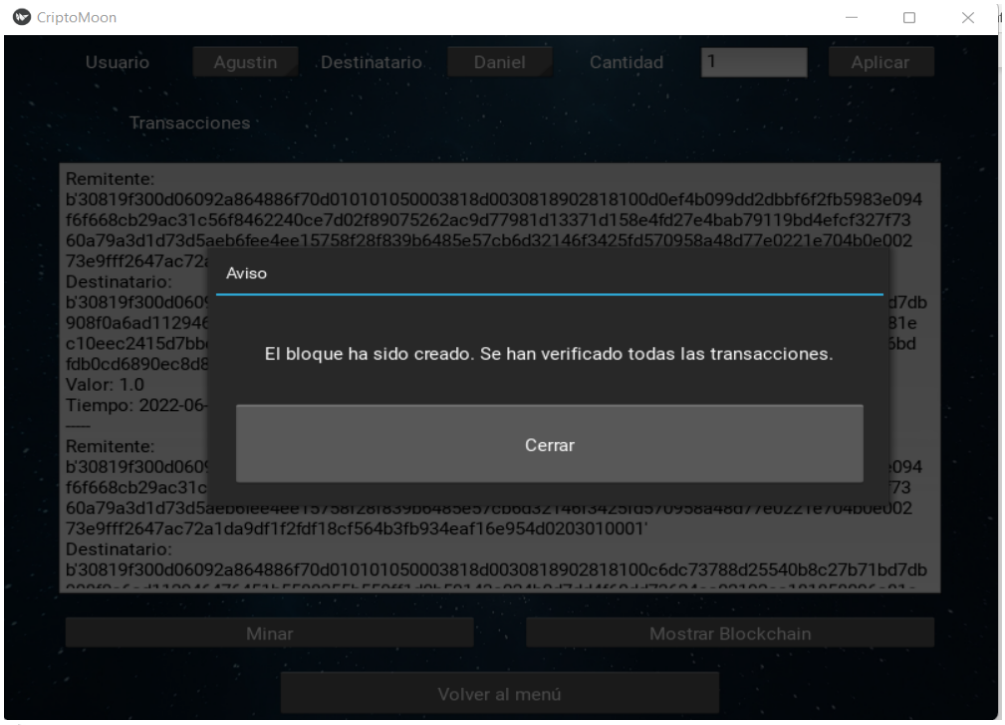
4.1 Ejemplo Moon Coins

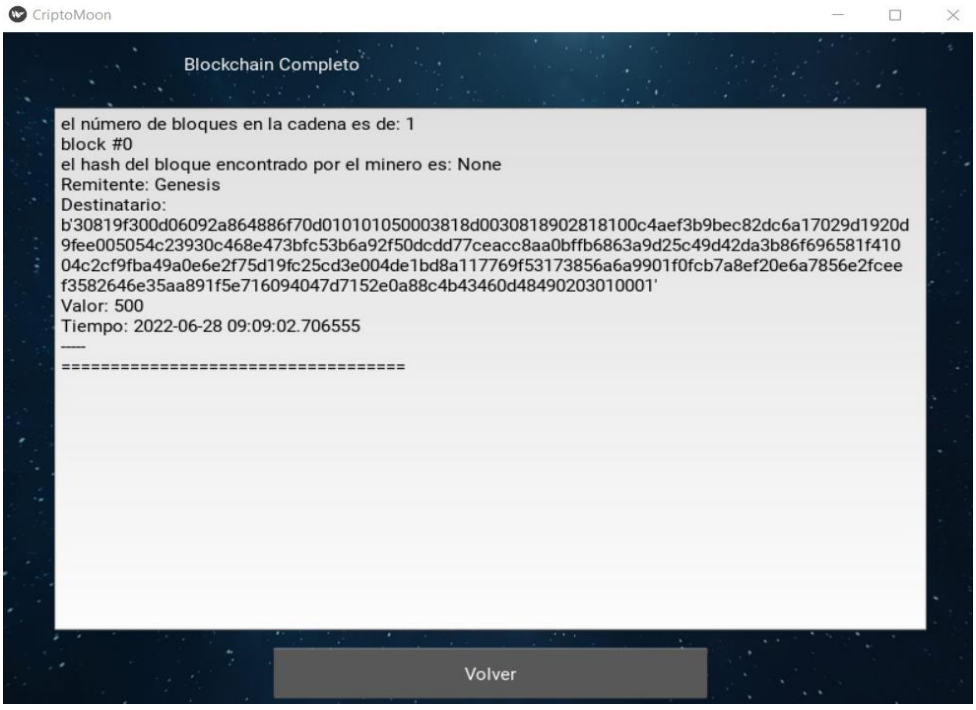
A continuación se muestra como generar transacciones y como minarlas.

Primero se generan 5 transacciones.



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.