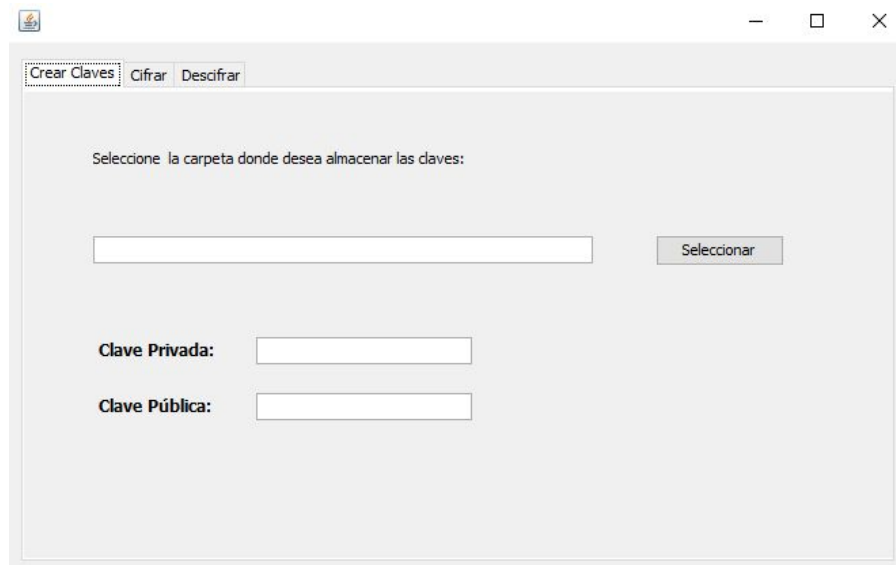


## MANUAL USUARIO PROGRAMA CIFRADO Y DESCIFRADO CON INFRAESTRUCTURA DE CLAVE PÚBLICA

Programa aplicación de concepto de infraestructura de clave pública, implementando la confidencialidad mediante el uso del cifrado RSA para cifrar y descifrar mensajes de corta longitud (117 bytes), con una longitud de clave de 1024 bits. Como nota, para cifrar archivos de cualquier tamaño, se usa RSA en conjunto con otros algoritmos como AES que dividen el tamaño del archivo en bloques y RSA se usaría para encriptar/desenciptar las claves de este cifrador de bloque.

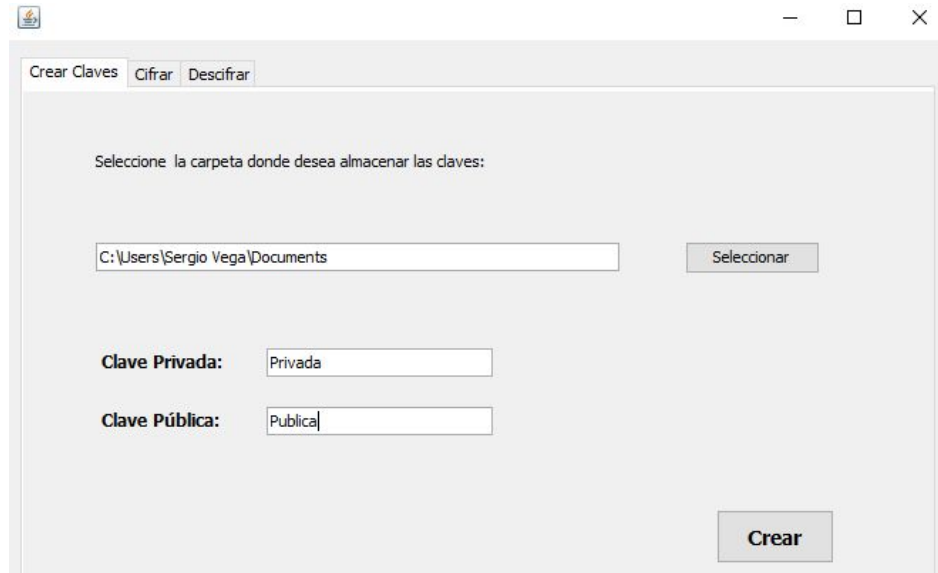
### 1. Generación de claves.

- a. En la pestaña “Crear Claves” seleccionar el directorio donde desea almacenar los archivos de clave pública y privada.

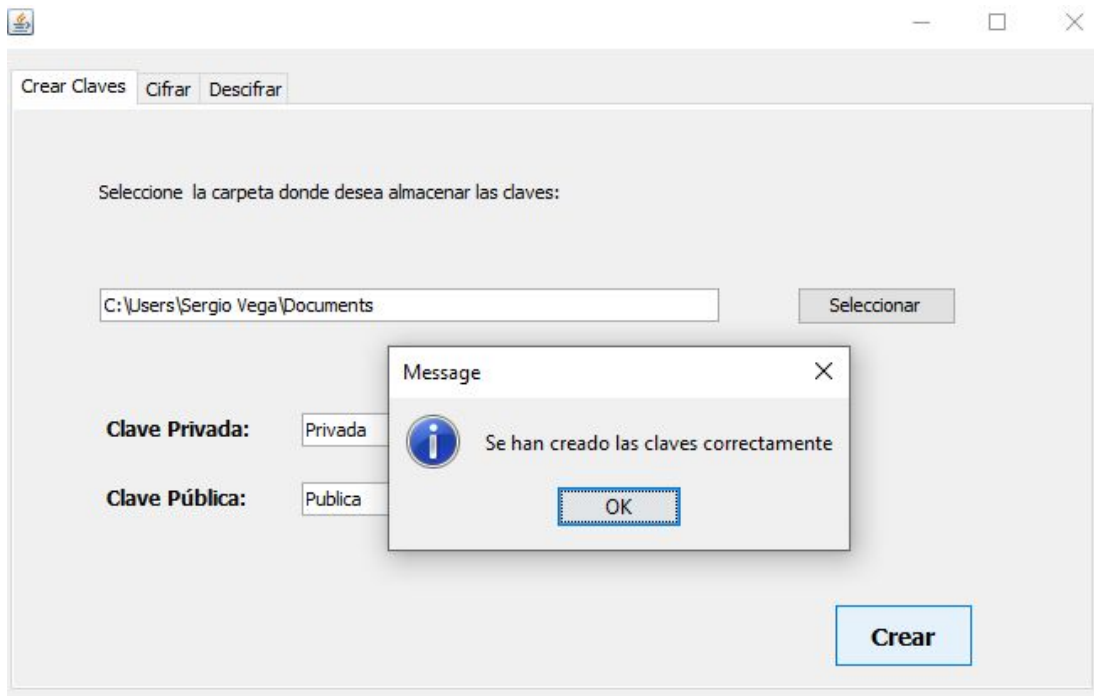


The screenshot shows a window titled "Crear Claves" with three tabs: "Crear Claves", "Cifrar", and "Descifrar". The "Crear Claves" tab is active. Inside the window, there is a text prompt "Seleccione la carpeta donde desea almacenar las claves:" followed by a text input field and a "Seleccionar" button. Below this, there are two more input fields labeled "Clave Privada:" and "Clave Pública:".

- b. En los campos “Clave Privada” y “Clave Pública” escribir el nombre que le quiere dar a cada archivo de clave.

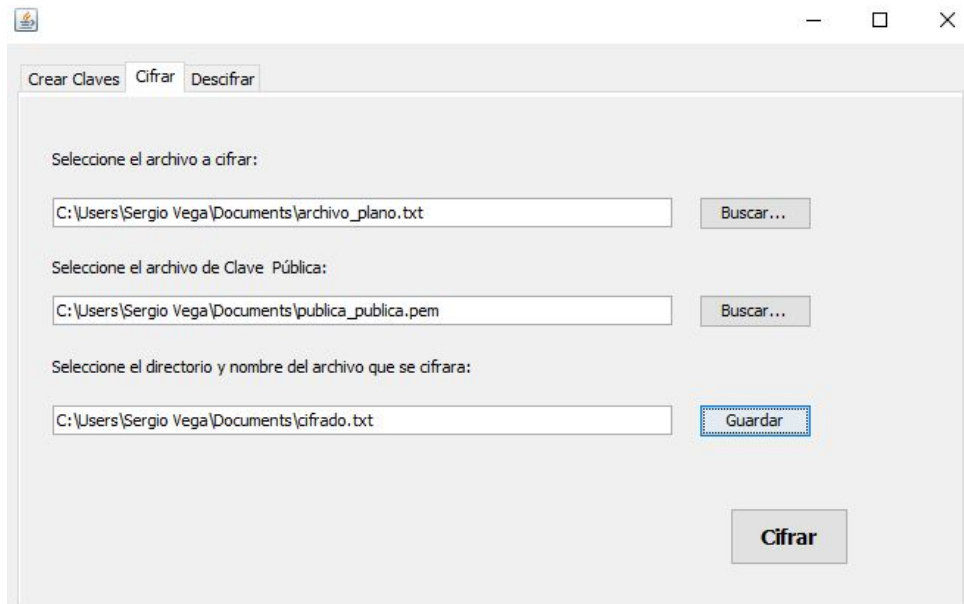


- c. Click en el botón “Crear” y se crearán las claves.(El botón “Crear” solo se habilitará una vez complete los pasos mencionados anteriormente”).

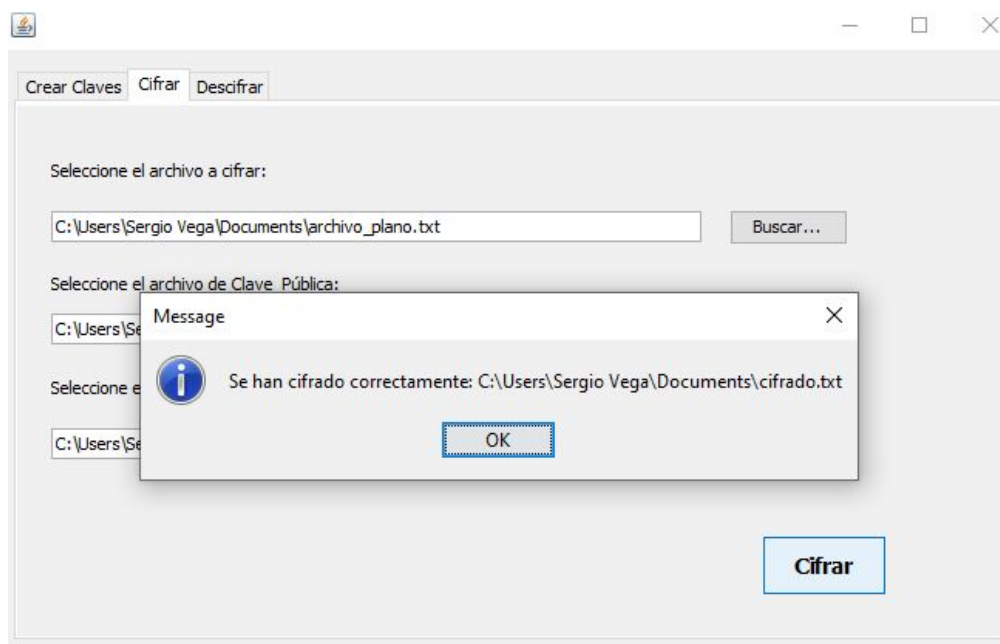


## 2. Cifrado de archivos.

- En la pestaña “Cifrar” seleccione el archivo que desea cifrar.
- Seleccione el archivo de clave pública creado en el paso 1.



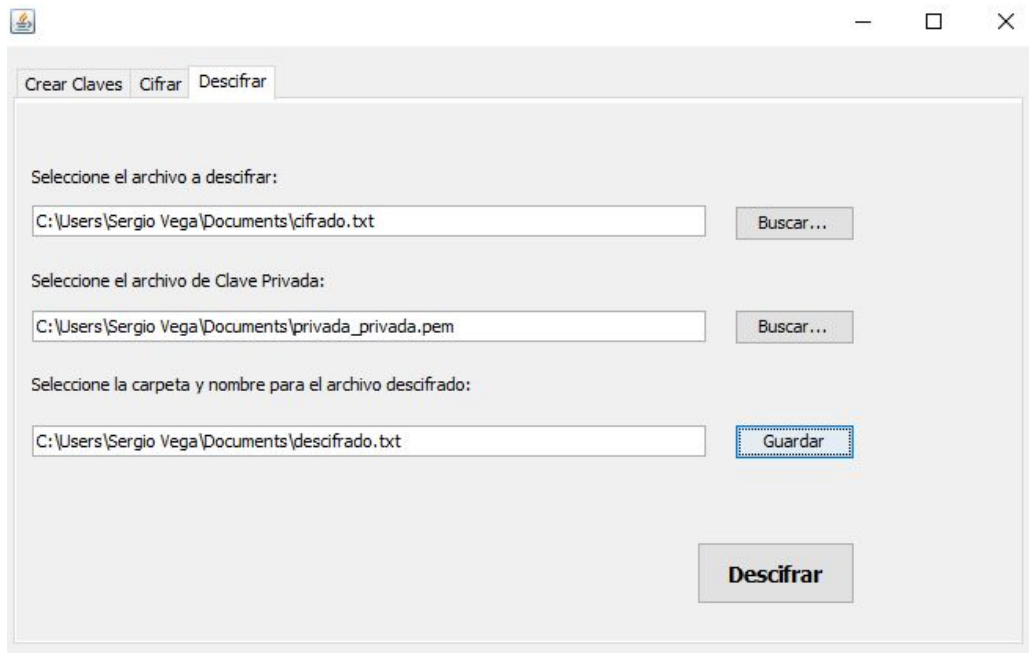
- c. Seleccione el directorio donde desea almacenar el archivo cifrado.
- d. Click en el botón “Cifrar” para cifrar el archivo.



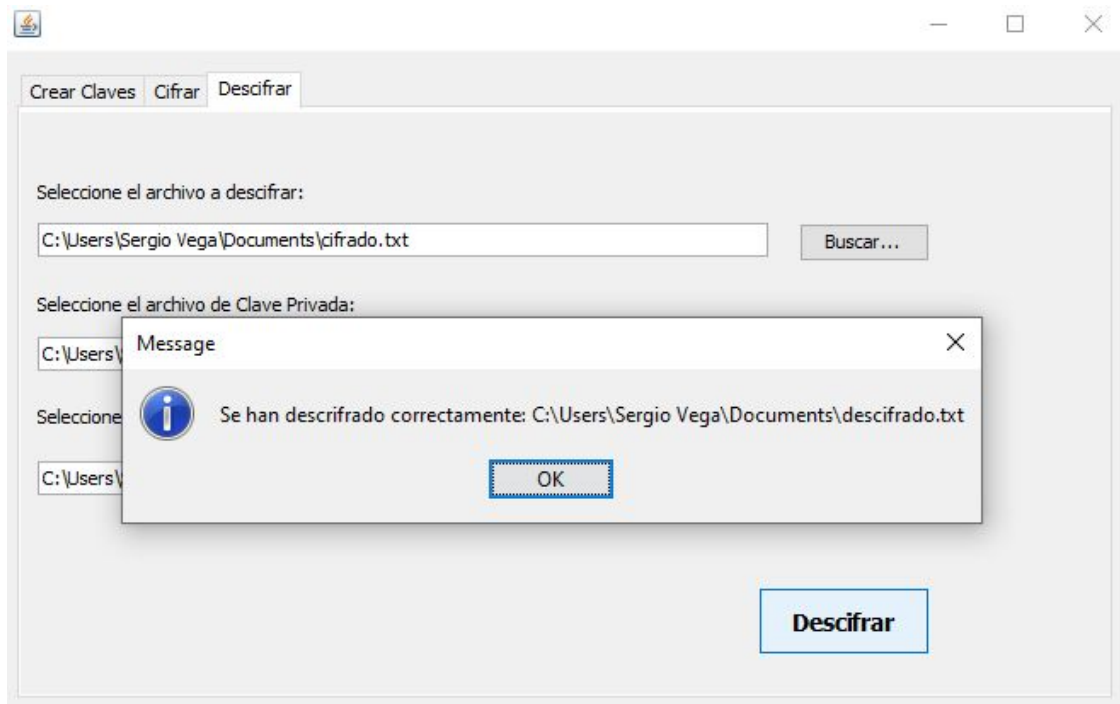
### 3. Descifrado de archivos.

- a. En la pestaña “Descifrar” seleccione el archivo cifrado en paso 2.
- b. Seleccione el archivo de clave Privada creado en el paso 1.

c. Seleccione el directorio donde desea almacenar el archivo Descifrado.



d. Click en el botón “Descifrar” para descifrar el archivo.



Para comprobar el funcionamiento del programa, compare el archivo original contra el archivo descifrado y deberían ser iguales.

**Video funcionalidad:**

<https://youtu.be/CfQuInmkx4E>

**Documentación JavaDoc:**

<https://drive.google.com/open?id=1lg-tvL1HjNJ17NhntMJ10Bjl8LcEBxDb>

**Autores:**

- Robinson Muñoz Muñoz
- Sergio Vega