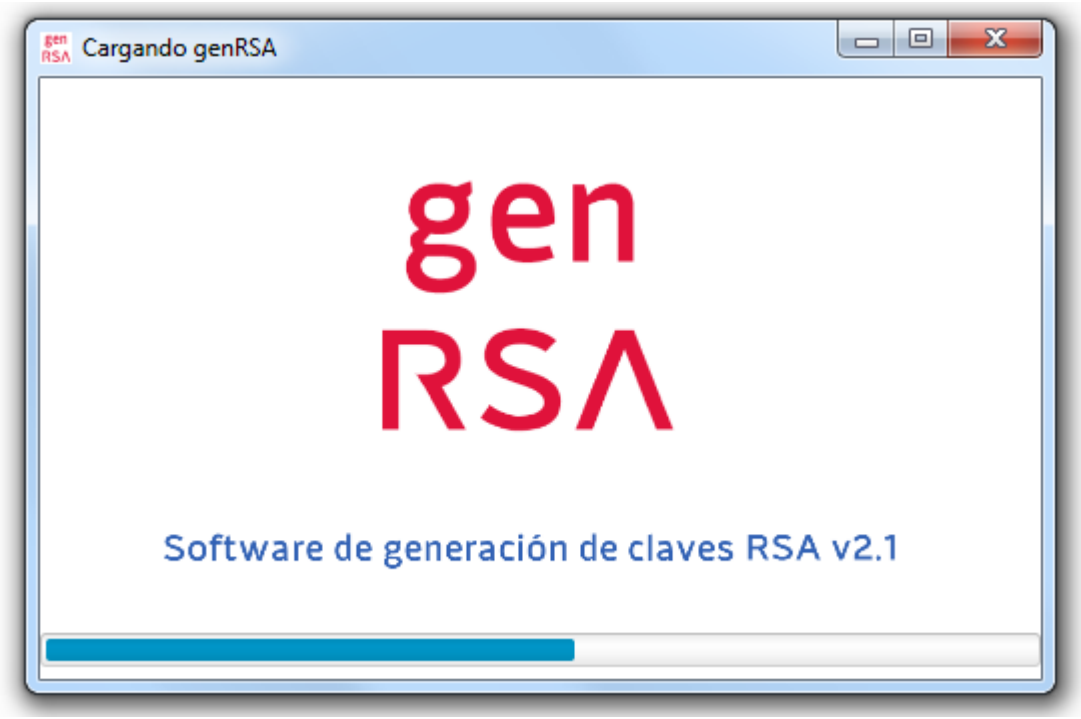


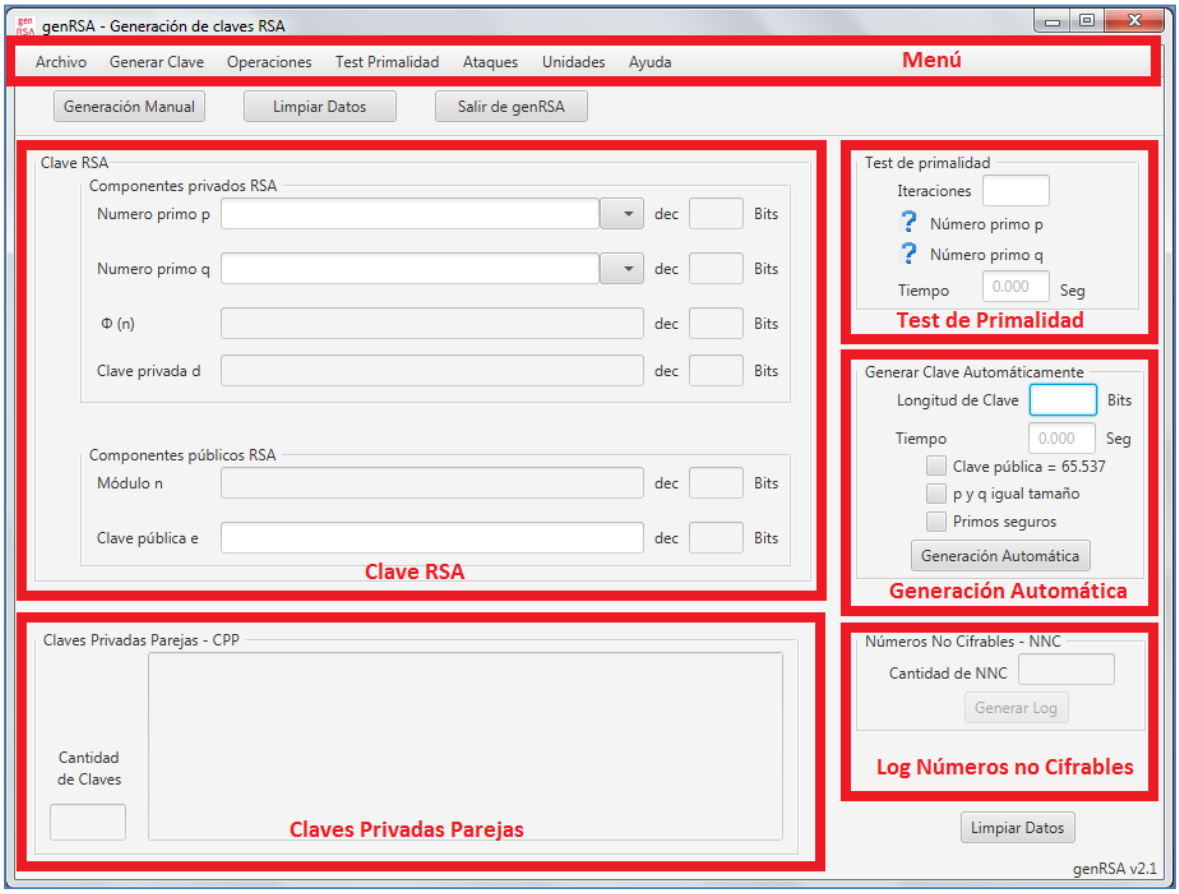
Manual de usuario

Manual de usuario genRSA v2.1

El programa genRSA v2.1 es una aplicación gráfica destinada a facilitar el aprendizaje del algoritmo RSA, un estándar de la criptografía asimétrica.

1. Funcionalidades Ventana Principal

Una vez ejecutado el archivo JAR aparecerá la ventana principal.



La ventana principal está dividida en seis secciones:

- **Menú**: la barra de menú permitirá ejecutar el resto de funcionalidades del programa genRSA. Muchas de estas funcionalidades abrirán pantallas secundarias que se comentarán más adelante.

- **Clave RSA**: en esta sección se visualizarán los componentes de la clave generada, ya sea de forma manual o automática. Se podrán generar claves de forma manual, introduciendo los campos **Número primo p**, **Número Primo q** y **Clave pública e**, pulsando posteriormente el botón **Generación Manual**. Así mismo, se podrán generar claves de forma automática.

- **Generación Automática**: esta sección sirve para generar claves RSA de forma automática. Para ello debe introducirse la **Longitud de la Clave** en bits que se quiere generar, elegir la clave pública e como el menor valor posible o bien el estándar F4, número 4 de Fermat, elegir si los primos p y q tendrán o no igual longitud de bits, y elegir si se desea trabajar con primos seguros. Finalmente se pulsa el botón **Generación Automática**.

- **Test de Primalidad**: muestra el resultado de la ejecución de los test de primalidad de Miller Rabin o de Fermat sobre el primo p y el primo q.

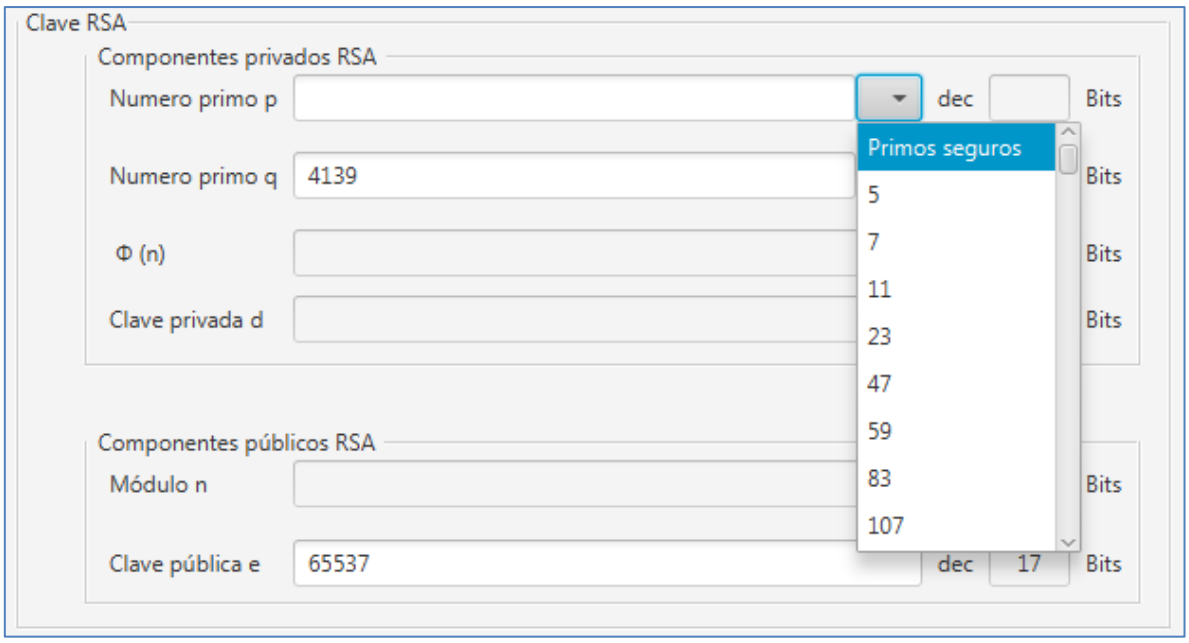
- **Claves Privadas Parejas CPP**: generada la clave, se mostrará la cantidad de claves privadas parejas asociadas a dicha clave, así como sus valores hasta un máximo de 300 claves. Cada una de estas CPP será mostrada informando de su longitud en bits. Si existen más CPP, se puede conocer todos sus valores guardando la clave y abriéndola con un navegador.

- **Log Números No Cifrables**: en esta sección se mostrará la cantidad de Números No Cifrables NNC asociados a la clave. Además, se podrá pulsar el botón **Generar Log** para crear un archivo HTML donde se visualicen los componentes de la clave y todos los NNC asociados.

Las funcionalidades que se pueden ejecutar sin necesidad de abandonar la ventana principal son las siguientes (todas ellas podrán ser ejecutadas para claves decimales y hexadecimales).

1.1. Generación Manual

Para generar una clave RSA se han de rellenar los campos **Número primo p**, **Número primo q** y **Clave pública e**. En los campos de los números primos se pueden introducir los valores directamente o hacer uso de los desplegables en los que se pueden seleccionar números primos seguros.



A continuación, se pulsará el botón **Generación Manual** o bien se podrán pulsar una combinación de teclas, como en todas las demás operaciones, y que se indican al final de este Manual.

Como resultado de estas acciones se obtendrá una clave RSA, es decir, se rellenarán los campos del Indicador de Euler Φ(n), de la Clave privada d y del Módulo n. Además, se mostrarán también las claves privadas parejas CPP y la cantidad de Números No Cifrables NNC asociados a la clave generada.

No obstante, la generación de una clave, tanto de forma manual como automática, supondrá desbloquear las siguientes funcionalidades del programa:

- Guardar la clave recién generada en un archivo HTML.
- Realizar operaciones de Cifrado-Descifrado y de Firma-Validación.
- Generar el Log de Números No Cifrables.
- Realizar los tres tipos de ataque con los datos de la clave.

1.2. Generación Automática

Para generar una clave de forma automática simplemente se introducirá la longitud que se quiere que tenga la clave (entre 6 y 8.192 bits).

Alternativamente, se pueden realizar otros tipos de generación automática. Estos tipos son el resultado de seleccionar o no una de estas tres opciones: Clave pública = 65.537; p y q igual tamaño; Primos seguros.

- La primera opción **Clave pública = 65.537**, generará una clave RSA cuya clave pública e será el valor estándar 65.537. Para ello la longitud de clave mínima es 19. Si no se selecciona esta opción, la clave pública e tomará el valor más pequeño posible.

- La segunda opción **p y q igual tamaño**, generará una clave cuyos primos p y q tendrán la misma longitud de bits. Si no se selecciona esta opción, la diferencia máxima de bits se dará en claves mayores a 40 bits, donde la diferencia serán 8 bits.

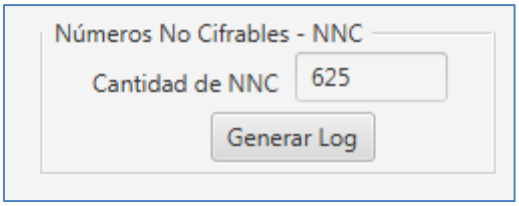
- La tercera opción **Primos seguros**, permite usar este tipo de primos que minimiza las CPP y los NNC en la clave generada. En este caso, para valores grandes del módulo la clave tardará más tiempo en generarse, pues un primo seguro r es el resultado de r = 2xs + 1, siendo s primo.

No obstante, las claves inferiores a 19 bits y de longitud par tendrán los primos p y q de igual cantidad de bits.

Finalmente, una vez ejecutada cualquiera de las diferentes combinaciones de generación automática, se obtendrá como resultado una clave RSA cuya longitud en bits del módulo n será igual al número introducido. De este modo, al igual que en la generación manual, se rellenarán las secciones Clave RSA, Claves Privadas Parejas y Log Números No Cifrables. Además, también se desbloquearán las mismas funcionalidades que en la generación manual.

1.3. Generar Log Números No Cifrables

Una vez generada una clave se obtendrá la cantidad de NNC y se habilitará el botón **Generar Log**. Este botón se tendrá que pulsar para generar estos números no cifrables.



Una vez pulsado el botón, se abrirá una ventana donde se podrá seleccionar dónde guardar el fichero de log y el nombre que tendrá.

El log de NNC generará un archivo en formato HTML. En él se guardarán los componentes de la clave y una lista con todos los NNC asociados a dicha clave. Dependiendo del tamaño de la clave, el fichero puede tardar más o menos tiempo en generarse (a partir de los 50 bits de longitud de clave, la generación de este archivo puede alargarse bastantes minutos).

1.4. Test de Primalidad

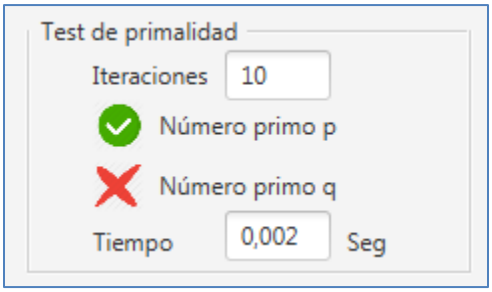
En esta aplicación se pueden realizar dos tests de primalidad, el de Fermat y el de Miller Rabin. Para ejecutar cualquiera de ellos, se han de introducir con anterioridad dos números a comprobar su primalidad en las cajas **Número Primo p** y **Número primo q**. Además, se indicará el número de **Iteraciones** a ejecutar en el test, valor que oscila entre 1 y 300. A mayor número de vueltas, mayor certeza de que el resultado sea correcto.

Para realizar el test de Fermat, se pulsará el botón **Test de Primalidad > Fermat** situado en la barra de menú.

Para ejecutar el test de Miller Rabin, se pulsará el botón **Test de Primalidad > Miller Rabin** situado en la barra de menú.

En ambos casos se obtendrá el resultado de la ejecución y el tiempo empleado para la misma. Como se muestra en la imagen inferior, el resultado se mostrará mediante imágenes.

Para aplicar esta funcionalidad no es necesario generar una clave previamente.



1.5. Guardar una clave generada

Para guardar una clave generada, simplemente se pulsará el botón **Archivo > Guardar Clave** situado en la barra de menú. Esto abrirá una ventana con un explorador de archivos donde se tendrá que indicar dónde se guardará la clave.

1.6. Abrir una clave generada

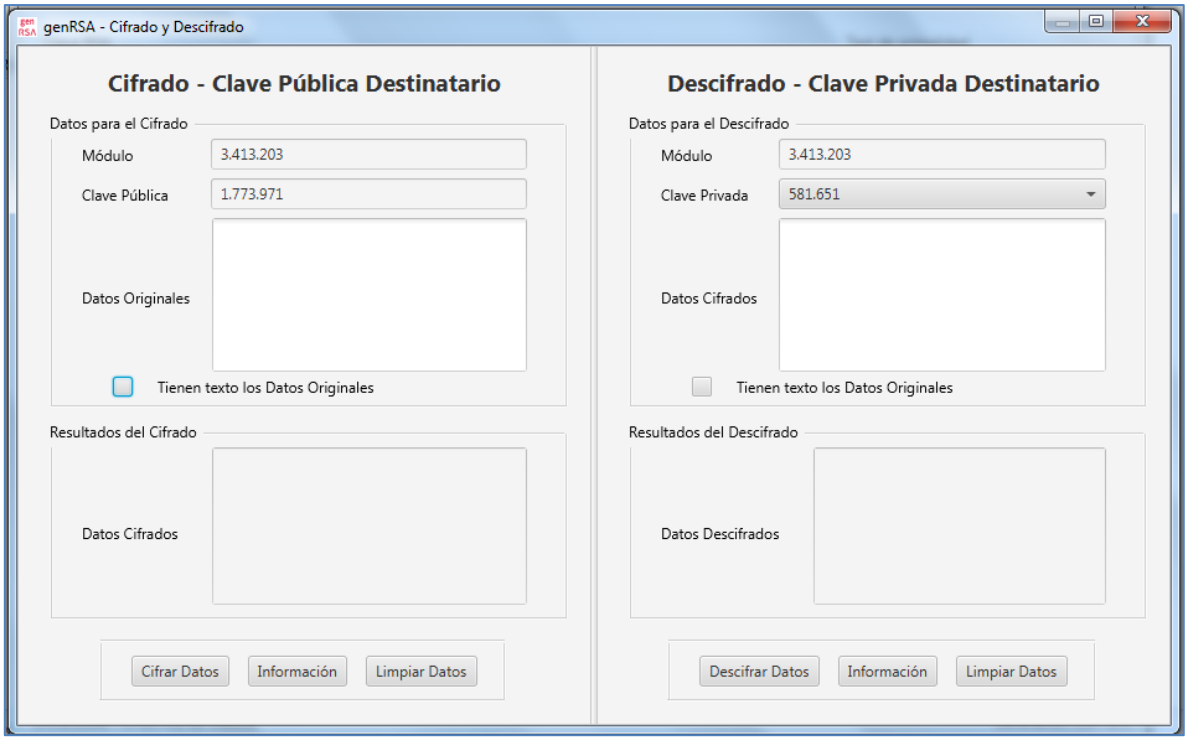
Para abrir una clave guardada, simplemente se pulsará el botón **Archivo > Abrir Clave** situado en la barra de menú. Esto abrirá una ventana con un explorador de archivos, donde se tendrá que indicar dónde se encuentra el archivo guardado con la clave. Una vez abierto, el resultado será el mismo que al generar una clave de forma manual o automática.

2. Funcionalidades Secundarias

Las funcionalidades secundarias son cinco. A todas ellas se accede desde la barra de menú.

2.1. Operación Cifrar – Descifrar

Para poder acceder a esta funcionalidad, previamente se debe haber generado una clave. Una vez generada, se pulsará el botón **Operaciones > Cifrar Descifrar** situado en la barra de menú. Entonces se abrirá la siguiente ventana.



Esta ventana está divida en dos: la parte de cifrado y la parte de descifrado.

- **Cifrado**: en la caja **Datos Originales** se pueden introducir números decimales o hexadecimales, según sea la clave generada. Estos números deben tener un valor positivo y menor que el módulo. En el caso de introducir un número mayor que el módulo, éste se reducirá mod n y se informará de ello al usuario.

  En el caso de introducir texto a cifrar, se debe marcar la opción **Tienen texto los Datos Originales**. El texto se codificará como números usando el valor decimal del código ASCII, en el cual cada carácter se convierte en números de 8 bits. En este caso será necesario que la clave generada tenga una longitud mínima de 12 bits. Si al codificar los datos se obtienen números mayores que el módulo, el texto de entrada se dividirá en el máximo bloques de bytes menores que el módulo n.

  Una vez introducidos los números o el texto, se pulsará el botón **Cifrar** y se obtendrán los datos cifrados en la caja de nombre **Datos Cifrados**.

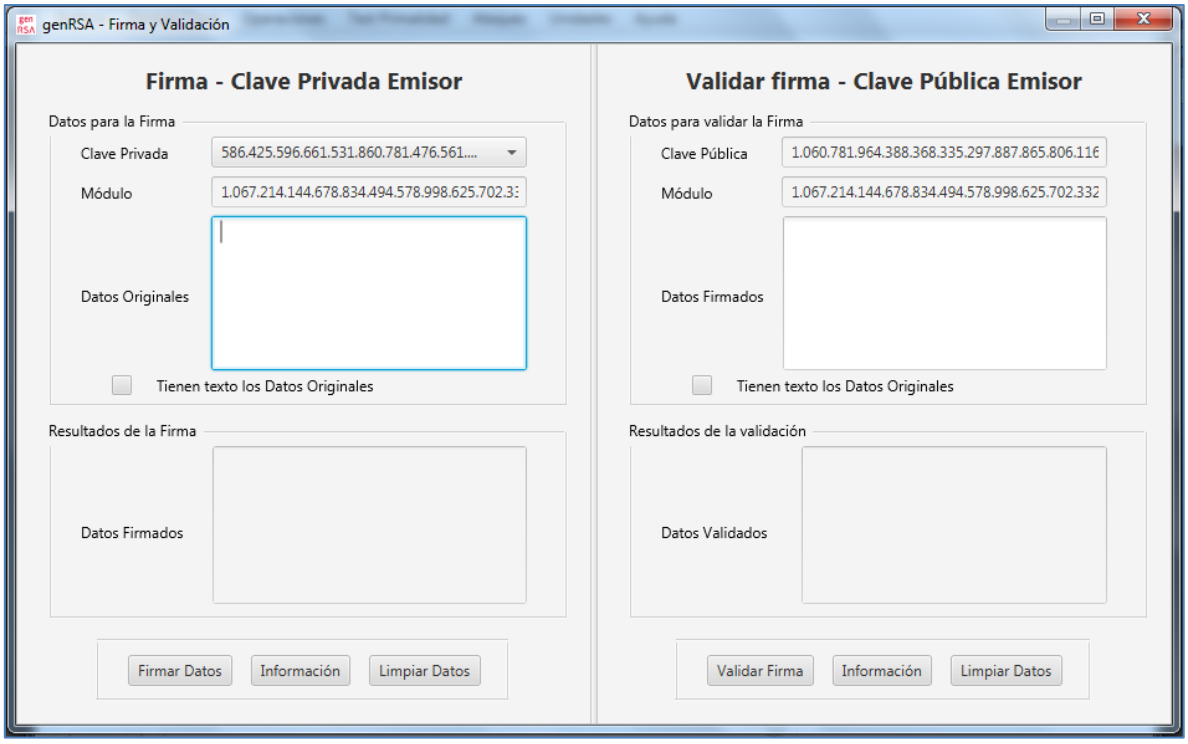
- **Descifrado**: se introducirán los datos cifrados en la caja con el mismo nombre. Si los datos cifrados eran originalmente texto, se ha de marcar la opción **Tienen texto los Datos Originales**. Además, se puede usar

cualquiera de las claves privadas parejas aparte de la clave privada para descifrar los datos.

A continuación, se pulsará el botón **Descifrar** y se obtendrán los datos originales en la caja **Datos Descifrados**.

2.2. Operación Firmar – Validar

Para poder acceder a esta funcionalidad previamente se debe haber generado una clave. Una vez generada se pulsará el botón **Operaciones > Firmar Validar** situado en la barra de menú. Entonces se abrirá la siguiente ventana.



Esta ventana está divida en dos: la parte de Firma y la parte de Validación.

- **Firma**: en la caja **Datos Originales** se pueden introducir números decimales o hexadecimales, según sea la clave generada. Estos números deben tener un valor positivo y menor que el módulo. En el caso de introducir un número mayor que el módulo, éste se reducirá mod n y se informará de ello al usuario.

En el caso de introducir texto a firmar, se debe marcar la opción **Tienen texto los Datos Originales**. El texto se codificará como números usando el valor decimal del código ASCII, en el cual cada carácter se convierte en números de 8 bits. En este caso será necesario que la clave generada tenga una longitud mínima de 12 bits. Si al codificar los datos se obtienen números mayores que el módulo, el texto de entrada se dividirá en el máximo bloques de bytes menores que el módulo n.

Una vez introducidos los números o el texto, se pulsará el botón **Firmar** y se obtendrán los datos firmados en la caja de nombre **Datos Firmados**.

- **Descifrado**: se introducirán datos firmados en la caja con el mismo nombre. Si los datos cifrados eran originalmente texto, se ha de marcar la opción **Tienen texto los Datos Originales**.

  A continuación, se pulsará el botón **Descifrar** y se obtendrán los datos originales para que se valide la firma.

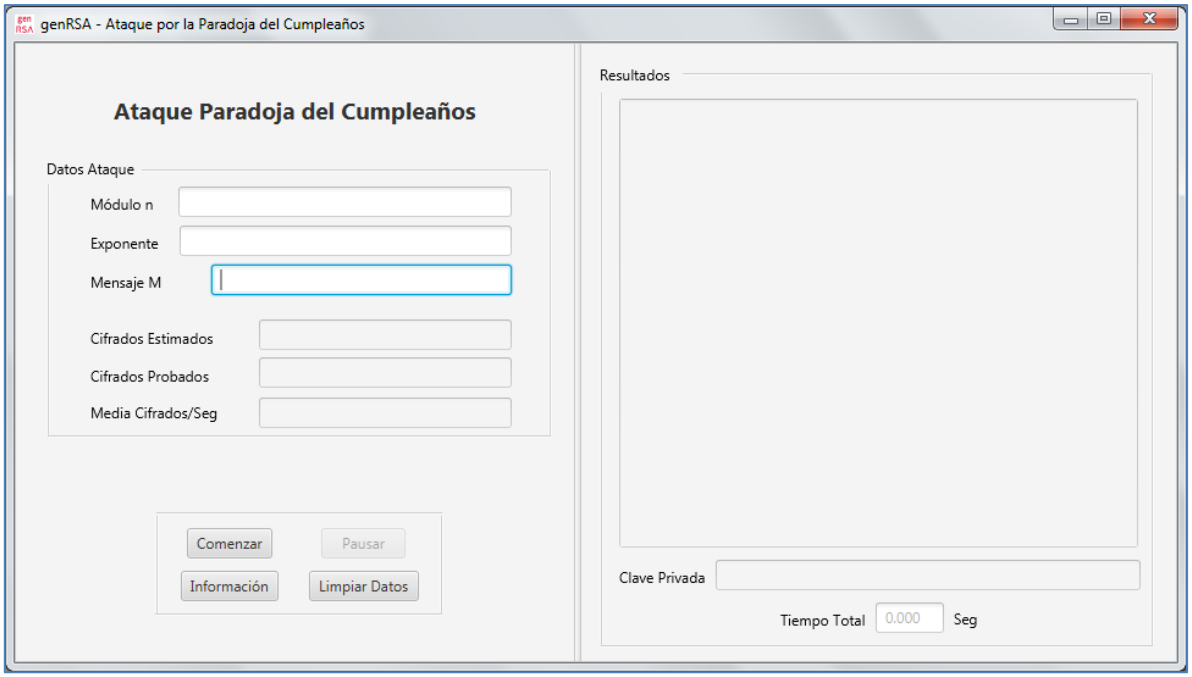
2.3. Ataque por la Paradoja del Cumpleaños

Para acceder a la ventana de este ataque no es necesario generar una clave, aunque puede hacerse también sobre ella. Simplemente se pulsará el botón **Ataques > Paradoja del Cumpleaños** de la barra de menú.

Se debe introducir un mensaje M (número) para realizar el ataque. En caso de no haber generado previamente una clave, será necesario rellenar los datos **Módulo n** y **Exponente**.

A continuación, se pulsará el botón **Comenzar** y el ataque dará inicio. Durante el ataque se mostrará la media de cifrados realizados por segundo en la caja **Media Cifrados/Seg** y se irán mostrando los resultados del ataque en la parte derecha de la ventana.

No obstante, también se mostrará una estimación de los cifrados necesarios (aproximación empírica $3\sqrt{n}$) para resolver el ataque y el número de cifrados probados que se están realizando durante el ataque.



Durante su ejecución, se habilitará el botón **Pausar** para que el ataque pueda ser pausado y, si se desea, continuar el ataque.

Finalmente, cuando termina el ataque se mostrará la clave privada y el tiempo total empleado para encontrarla.

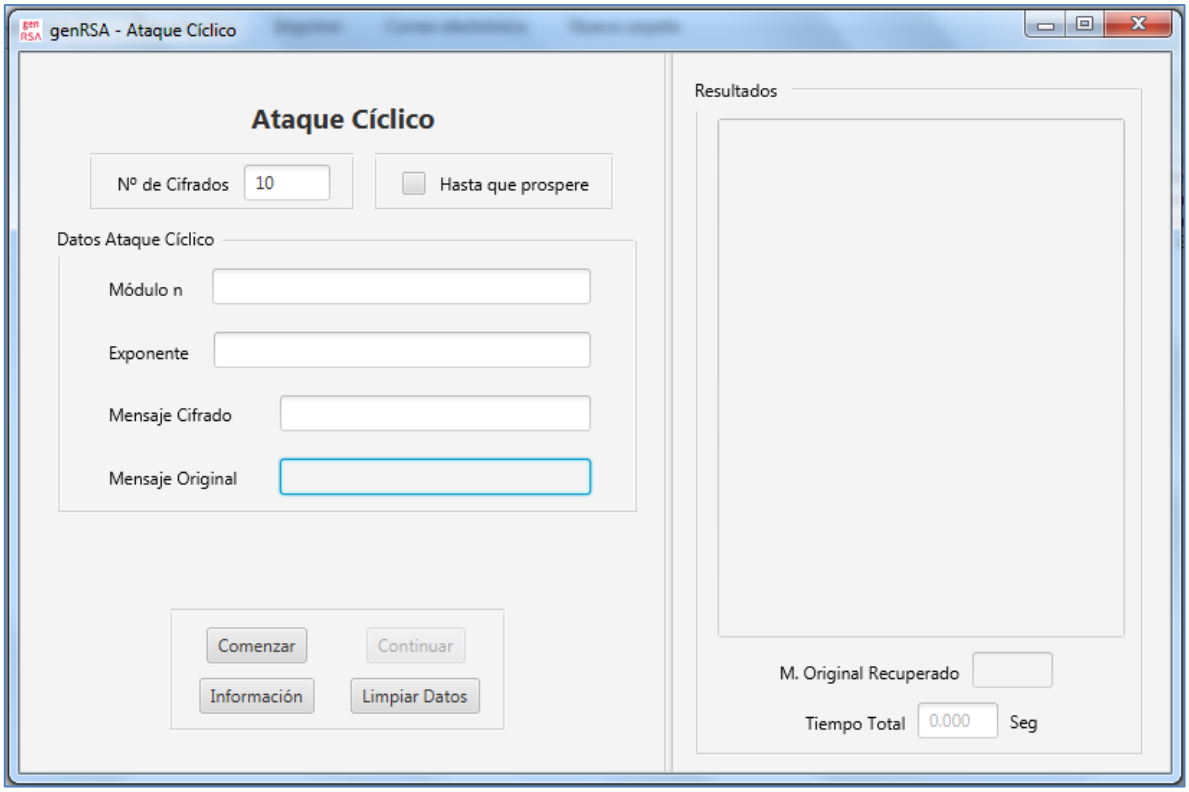
2.4. Ataque Cíclico

Para acceder a la ventana de este ataque no es necesario generar una clave, aunque puede hacerse también sobre ella. Simplemente se pulsará el botón **Ataques > Cíclico** situado en la barra de menú.

Se debe introducir un mensaje cifrado (número) para realizar el ataque. En caso de no haber generado previamente una clave, será necesario rellenar los datos **Módulo n** y **Exponente**.

El ataque se puede ejecutar de dos formas: indicando el **Nº de cifrados** a realizar o marcando la opción **Hasta que prospere**. En el caso de seleccionar la opción hasta que prospere, el ataque no parará hasta que encuentre el mensaje original o bien se pulse el botón **Parar**.

A continuación, se pulsará el botón **Comenzar**. El ataque dará inicio realizando cifrados cíclicos al mensaje cifrado con los componentes públicos de la clave. Una vez comenzado el ataque, se habilitará el botón de **Parar** el ataque.



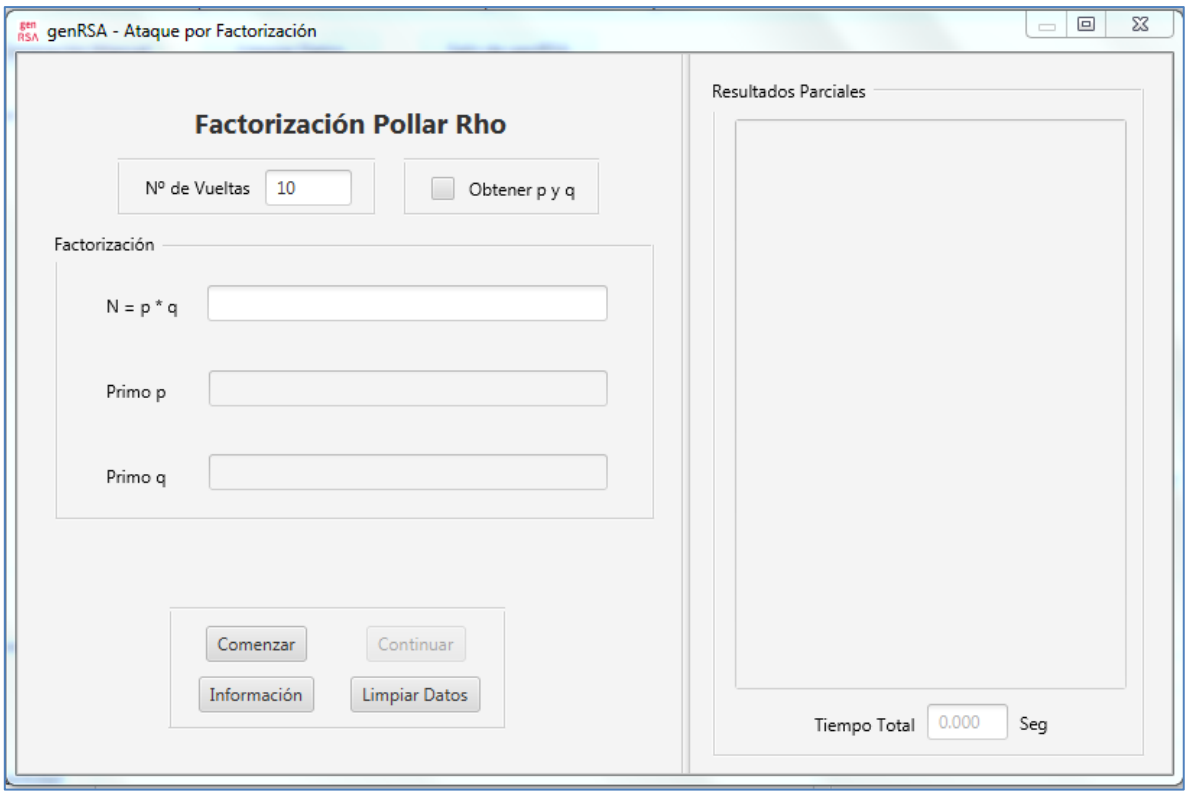
En el caso de no haber recuperado el mensaje original en el número de vueltas indicado, se puede continuar el ataque en el mismo punto donde se dejó con la opción **Continua**r.

Finalmente, cuando termina el ataque, se mostrará el mensaje original recuperado y el tiempo total empleado para encontrarlo.

2.5. Ataque por Factorización

Para acceder a la ventana de este ataque no es necesario generar una clave, aunque puede hacerse también sobre ella. Simplemente se pulsará el botón **Ataques > Factorizar n** situado en la barra de menú.

En caso de no haber generado previamente una clave previamente, se debe introducir el número que se quiere factorizar en el campo **Módulo n**.



El ataque se puede ejecutar de dos formas: indicando el **Nº de vueltas** o marcando la opción **Obtener p y q**. En el caso de seleccionar esta última opción, el ataque no parará hasta que se factorice el módulo o se pulse el botón **Parar**.

A continuación, se pulsará el botón **Comenzar** y se comenzarán a obtener resultados parciales del ataque. Una vez comenzado el ataque se habilitará el botón de **Parar** el ataque.

En el caso de no haber factorizado el módulo en el número de vueltas indicado, se puede continuar el ataque en el mismo punto donde se dejó pulsando el botón **Continuar**.

Finalmente, cuando termina el ataque se mostrarán los primos p y q y el tiempo total empleado para ejecutar el ataque.

3. Información en funcionalidades

Las funcionalidades de genRSAv2.1 **Operaciones**, **Test** y **Ataques** tienen un botón de **Información** que entrega una breve descripción de la operación que se va a realizar.

4. Acceso a funcionalidades mediante teclado

Salir	Ctrl + Shift + X
Guardar clave	Ctrl + S
Abrir clave	Ctrl + O
Borrar clave	Ctrl + D
Generación Manual	Ctrl + Shift + M
Generación de clave automática	Ctrl + Shift + A
Cifrar – Descifrar	Ctrl + Shift + C
Firmar – Validar	Ctrl + Shift + F
Test de primalidad de Miller Rabin	Ctrl + M
Test de primalidad de Fermat	Ctrl + F
Ataque Paradoja del cumpleaños	Ctrl + 1
Ataque Cíclico	Ctrl + 2
Ataque Factorizar n	Ctrl + 3
Unidad decimal	Ctrl + Shift + D
Unidad hexadecimal	Ctrl + Shift + H
Manual de usuario	F1
Banco de pruebas	F2
Acerca de	F10

5. Software de complemento para ataques a RSA

Si desea realizar los ataques por Paradoja del cumpleaños, por Cifrado Cíclico o por Factorización del módulo n a claves RSA de mayor longitud, se recomienda usar los siguientes programas de libre distribución:

a) Ataque por Paradoja del Cumpleaños. Software LegionRSA (CriptoRed)
   Descarga: http://www.criptored.upm.es/software/sw_m001o.htm
b) Ataque por Cifrado Cíclico. Software RingRSA (CriptoRed)
   Descarga: http://www.criptored.upm.es/software/sw_m001q.htm
c) Ataque por Factorización de n. Software msieve153 (sourceforge)
   Descarga: https://sourceforge.net/projects/msieve/