

Manual de Usuario genRSA v2.1

GenRSA v2.1 es una aplicación gráfica destinada a facilitar el aprendizaje del algoritmo RSA estudiado en el marco de la criptografía asimétrica.

1. Funcionalidades Ventana Principal

Una vez ejecutado el archivo JAR aparecerá la ventana principal.

The screenshot shows the main window of the genRSA v2.1 application. The title bar reads "genRSA - Generación de claves RSA". The menu bar includes "Archivo", "Generar Clave", "Operaciones", "Test Primalidad", "Ataques", "Unidades", "Ayuda", and "Menú". Below the menu bar are three buttons: "Generación Manual", "Limpiar Datos", and "Salir de genRSA".

The main interface is divided into several sections:

- Clave RSA:** This section contains two groups of input fields. The first group, "Componentes privados RSA", includes "Numero primo p", "Numero primo q", " $\Phi(n)$ ", and "Clave privada d". The second group, "Componentes públicos RSA", includes "Módulo n" and "Clave pública e". Each input field has a "dec" (decimal) button and a "Bits" button.
- Test de primalidad:** This section includes "Iteraciones", "Número primo p", "Número primo q", and "Tiempo" (0.000 Seg). It features a red "Test de Primalidad" button.
- Generar Clave Automática:** This section includes "Longitud de Clave", "Tiempo" (0.000 Seg), and checkboxes for "Clave Pública = 65537" and "p y q igual tamaño". It features a red "Generación Automática" button.
- Claves Privadas Parejas:** This section includes a "Cantidad de Claves" input field and a large text area. It features a red "Claves Privadas Parejas" button.
- Log Números No Cifrables:** This section includes "Números No Cifrables - NNC", "Cantidad de NNC", and a "Generar Log" button. It features a red "Log Números No Cifrables" button.

At the bottom of the window, there is a "Limpiar Datos" button and the text "Universidad Politécnica de Madrid" and "Generación RSA v2.1".

La ventana principal está dividida en seis secciones:

- Generación Automática: esta sección sirve para generar claves RSA de forma automática. Para ello solo se debe introducir la Longitud de la Clave que se quiere generar y pulsar el botón Generación Automática.
- Clave RSA: en ella se visualizarán los componentes de la clave generada, ya sea de forma manual o automática. En ella también se podrán generar claves de forma manual introduciendo los campos Número primo p , Número Primo q y Clave pública e y pulsando el botón "Generación Manual".
- Claves Privadas Parejas: una vez generada la clave se mostrarán la cantidad de claves privadas parejas asociadas a dicha clave. También se mostrarán hasta un máximo de 300 de estas claves. Cada una de ellas será mostrada informando de su longitud en bits.
- 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.
- Test de Primalidad: muestra el resultado de la ejecución de los test de primalidad sobre el primo p y el primo q .
- 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.

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.

The screenshot shows a window titled "Clave RSA" with two main sections: "Componentes privados RSA" and "Componentes públicos RSA".

Componentes privados RSA:

- "Número primo p": An empty text field.
- "Número primo q": A text field containing the value "4139".
- " Φ (n)": An empty text field.
- "Clave privada d": An empty text field.

Componentes públicos RSA:

- "Módulo n": An empty text field.
- "Clave pública e": A text field containing the value "65537".

On the right side of the "Número primo q" field, there is a dropdown menu labeled "Primos seguros" which is currently open. It displays a list of prime numbers: 5, 7, 11, 23, 47, 59, 83, and 107. To the right of the dropdown, there are labels "dec" and "Bits" for the private components, and "dec" and "17 Bits" for the public components.

A continuación se pulsará el botón "Generación Manual" o bien se podrán pulsar la combinación de teclas "Ctrl+Shift+M".

Como resultado de estas acciones se obtendrá una clave RSA, es decir, se rellenarán los campos " Φ (n)", "Clave privada d", "Módulo N". Además, también se mostrarán las claves privadas parejas y la cantidad de NNC asociados a la clave recién 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). Y se pulsará el botón "Generación Automática" o la combinación de teclas "Ctrl+Shift+A".

Alternativamente, se pueden realizar otros tipos de generación automática. Estos tipos son los resultantes de seleccionar o no las opciones "Clave Pública=65.537" y "p y q igual tamaño".

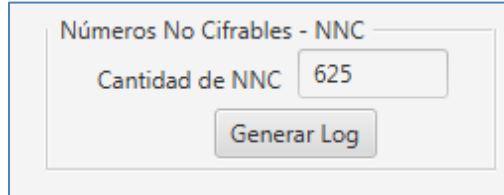
- La primera opción, generará una clave cuya clave pública será el valor más usado en certificados digitales(65.537). Para ello la longitud de clave mínima es 19. Si no se selecciona esta opción, la clave pública tomará el valor más pequeño posible.
- La segunda opción generará una clave cuyos primos p y q sean de 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.

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 ejecutado 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". 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.



Números No Cifrables - NNC

Cantidad de NNC 625

Generar Log

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

El log de NNC se generará 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 en generarse (a partir de los 50 bits de longitud de clave la generación puede alargarse bastantes minutos).

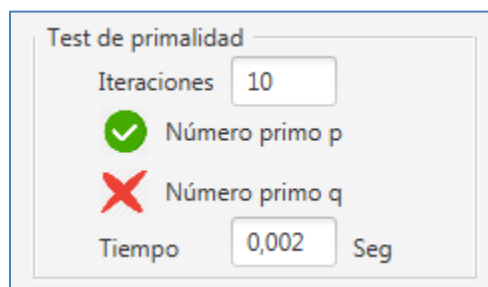
1.4. Test de Primalidad

En esta aplicación se pueden realizar dos tests de primalidad, el de Fermat y el de Miller Rabin y Lucas-Lehmer. Para ejecutar cualquiera de ellos se han de introducir con anterioridad dos números a comprobar su primalidad en las cajas de "Número Primo p" y "Número primo q". Además se indicará el número de iteraciones a ejecutar 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. De forma alternativa, una vez introducidos los datos se puede pulsar la combinación de teclas "Ctrl+F".

Para ejecutar el test de Miller Rabin y Lucas-Lehmer se pulsará el botón "Test de Primalidad>Miller Rabin" situado en la barra de menú. De forma alternativa, una vez introducidos los datos se puede pulsar la combinación de teclas "Ctrl+M".

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.



Test de primalidad	
Iteraciones	10
✓	Número primo p
✗	Número primo q
Tiempo	0,002 Seg

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 donde 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 donde 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. Todas ellas se acceden 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.

The screenshot shows a software window titled "genRSA - Cifrado y Descifrado". It is divided into two main sections: "Cifrado - Clave Pública Destinatario" on the left and "Descifrado - Clave Privada Destinatario" on the right. Each section contains input fields for "Módulo" and "Clave" (Publica/Privada), a large text area for "Datos Originales" or "Datos Cifrados", a checkbox for "Tienen texto los Datos Originales", and a section for "Resultados del Cifrado" or "Resultados del Descifrado" with a "Datos Cifrados" or "Datos Descifrados" field. At the bottom of each panel are buttons for "Cifrar Datos" or "Descifrar Datos", "Información", and "Limpiar Datos".

Esta ventana está dividida 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, el número introducido se va partiendo en números lo más cercanos al módulo posible. Es decir, se parte el en números de igual cantidad de bits que el modulo o de un bit menos. Un ejemplo: si el módulo es 65.537 y se introduce el número 5883364551 para cifrar, este se partirá en los números 58833 y 64551.

Para evitar confusiones una vez procesados todos los números introducidos se formatea el campo donde se han introducido y se muestran cada número procesado en una línea. De este modo se muestra claramente cómo se deberían haber introducido los datos y cuáles son los datos que realmente se van a cifrar descifrar. Además se mostrará un mensaje indicando que se han modificado los valores introducidos.

En el caso de introducir texto a cifrar se debe marcar la opción "Tienen texto los Datos Originales". El texto se codificará a números usando el 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. Pero al igual que en el caso anterior, si al codificar los datos se obtienen números mayores que el módulo estos se partirán.

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 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.

The screenshot shows a software window titled "genRSA - Firma y Validación". It is divided into two panels. The left panel, titled "Firma - Clave Privada Emisor", contains a section "Datos para la Firma" with a "Clave Privada" dropdown menu showing a long hexadecimal string, a "Módulo" text box with another long hexadecimal string, and a large empty text area for "Datos Originales". Below this is a checkbox labeled "Tienen texto los Datos Originales". At the bottom of the left panel is a section "Resultados de la Firma" with a text box for "Datos Firmados" and three buttons: "Firmar Datos", "Información", and "Limpiar Datos". The right panel, titled "Validar firma - Clave Pública Emisor", has a similar layout with "Clave Pública" and "Módulo" fields, a text area for "Datos Firmados", a checkbox for "Tienen texto los Datos Originales", a "Resultados de la validación" section with a "Datos Validados" text box, and buttons for "Validar Firma", "Información", and "Limpiar Datos".

Esta ventana está dividida 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, el número introducido se va partiendo en números lo más cercanos al módulo posible. Es decir, se parte el en números de igual cantidad de bits que el modulo o de un bit menos. Un ejemplo: si el módulo es 65.537 y se introduce el número 5883364551 para firmar, este se partirá en los números 58833 y 64551.

Para evitar confusiones una vez procesados todos los números introducidos se formatea el campo donde se han introducido y se muestran cada número procesado en una línea. De este modo se muestra claramente cómo se deberían haber introducido los datos y

cuáles son los datos que realmente se van a firmar. Además se mostrará un mensaje indicando que se han modificado los valores introducidos.

En el caso de introducir texto a firmar se debe marcar la opción "Tienen texto los Datos Originales". El texto se codificará a números usando el 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. Pero al igual que en el caso anterior, si al codificar los datos se obtienen números mayores que el módulo estos se partirán.

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 validen.

2.3 Ataque por la Paradoja del Cumpleaños

Para acceder a la ventana de este ataque no es necesario generar una clave, simplemente se pulsará el botón "Ataques > Paradoja del Cumpleaños" de la barra de menú.

Se debe introducir un mensaje M para realizar el ataque y en caso de no haber generado una clave será necesario rellenar los datos "Modulo n" y "Exponente".

genRSA - Ataque por la Paradoja del Cumpleaños

Ataque Paradoja del Cumpleaños

Datos Ataque

Módulo n

Exponente

Mensaje M

Cifrados Estimados

Cifrados Probados

Media Cifrados/Seg

Resultados

Clave Privada

Tiempo Total 0.000 Seg

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 para resolver el ataque y el número de cifrados probados que se están realizando durante el ataque.

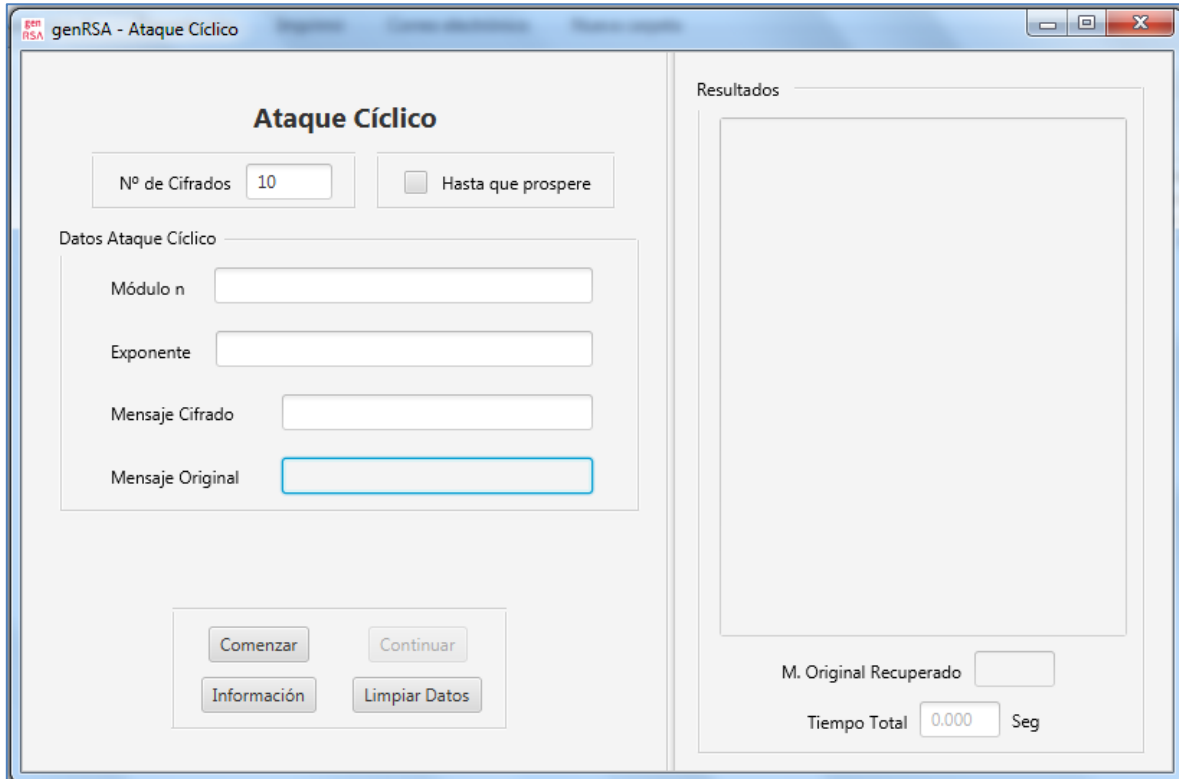
Durante el ataque, se habilitará un botón para que pueda ser parado.

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

2.4 Ataque Cíclico

Para acceder a la ventana de este ataque no es necesario generar una clave, simplemente se pulsará el botón "Ataques > Cíclico" situado en la barra de menú.

Se debe introducir un mensaje cifrado para realizar el ataque y en caso de no haber generado una clave será necesario rellenar los datos "Modulo n " y "Exponente".



El ataque se puede ejecutar de dos formas: indicando el número de cifrados o marcando la opción de hasta que prospere. En el caso de seleccionar la opción hasta que prospere el ataque no parará hasta que encuentre el mensaje original o se pulse el botón de 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.

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

2.5 Ataque por Factorización

Para acceder a la ventana de este ataque no es necesario generar una clave, simplemente se pulsará el botón "Ataques > Factorizar n" situado en la barra de menú.

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

The screenshot shows a software window titled "genRSA - Ataque por Factorización". The main area is titled "Factorización Pollar Rho". It contains a section for "Factorización" with three input fields: "N = p * q", "Primo p", and "Primo q". Above these fields, there is a "Nº de Vueltas" field set to "10" and a checkbox labeled "Obtener p y q". Below the input fields are four buttons: "Comenzar", "Continuar", "Información", and "Limpiar Datos". To the right of the main area is a panel titled "Resultados Parciales" which is currently empty. At the bottom right of the panel, there is a "Tiempo Total" field showing "0.000" and the unit "Seg".

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