1. Manual de Usuario (versión beta, 2016)

1.1 Longitud de claves

Si la longitud de la clave generada es mayor a 30 no se guardará en memoria todos los números que ya han aparecido en un anillo, ya que se necesita más de un giga de memoria para almacenar esta información. Al no guardar en memoria los números que ya han aparecido en un anillo, no se sabe si un número comprendido entre 1 y el módulo-1 ha aparecido ya en un anillo y habrá que buscar el anillo al que pertenecen todos los números. Mientras que para claves iguales o menores a 30 el número de búsquedas equivale al número de anillos (que no suele sobrepasar los 100.000).

1.2 Generación de claves RSA

Al ejecutar el software se puede generar una clave de manera automática o manual. Si es manual se tendrá que introducir los valores p,q y el exponente, mientras que si es automática sólo la longitud de la clave en bits. Los campos no editables tienen un fondo gris.

Fig. 1.1 Diferencia entre generación manual y automática.

1.3 Opciones de Generación

Manual

Están disponibles las opciones de ver una lista de primos o primos seguros. Los números primos seleccionados se asignarán al valor p o q. Las listas sólo se podrán ver si se está en modo de generación manual.

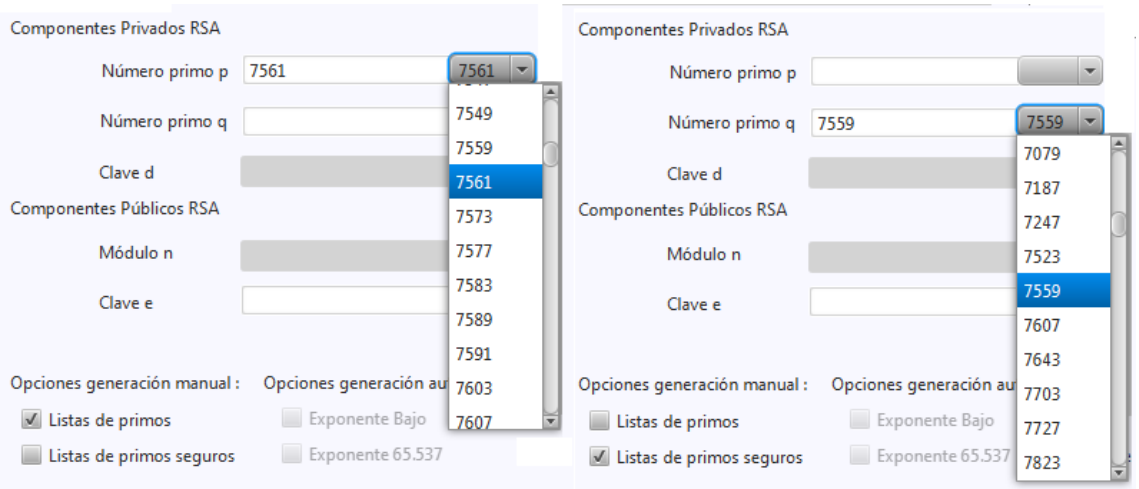

Fig. 1.2 Listas de primos y primos seguros.

Automática

Al generar una clave RSA de una longitud determinada, se puede asignar el menor exponente posible o 65.537 (comúnmente utilizado). Si se desea cambiar los datos de una clave generada automáticamente (p. ej. el exponente) se tendrá que cambiar a modo de generación manual para que los campos se vuelvan editables. Cualquier opción de generación manual que este activada se ignorará si se está en modo automático.

Fig. 1.3 Generando una clave con exponente bajo y con exponente 65.537.

1.4 Generación clave, campos de la interfaz

Botón: Limpiar clave

Limpia todos los campos de la escena, dejando la interfaz como si el programa acabara de arrancar.

Botón: Pos. Longitudes

Calcula las posibles longitudes de los anillos, que son los divisores de lambda(lambda(n)). Las longitudes que aparecerán en el cálculo de los anillos variaran dependiendo del exponente pero siempre serán valores contenidos en esta lista.

Botón: Cálculo de los Anillos

Tras pulsar en el botón "Anillos" se empieza a buscar todos los anillos de la clave RSA. Se muestra diversa información en el transcurso y finalización del cálculo. En la ventana principal la parte izquierda es relativa a la generación de claves y la media y derecha al cálculo de los anillos.

1.5 Cálculo de los anillos

La ventana principal del software se puede dividir en 3 zonas. En la izquierda se generan las claves y selecciona la opción de realizar un ataque cíclico o calcular los anillos, y en la media y derecha se muestran datos relativos al cálculo de los anillos.

Se muestran todos los campos de la zona izquierda y media en la siguiente figura, en la que se ha pausado el cálculo de los anillos en una clave de 22 bits.

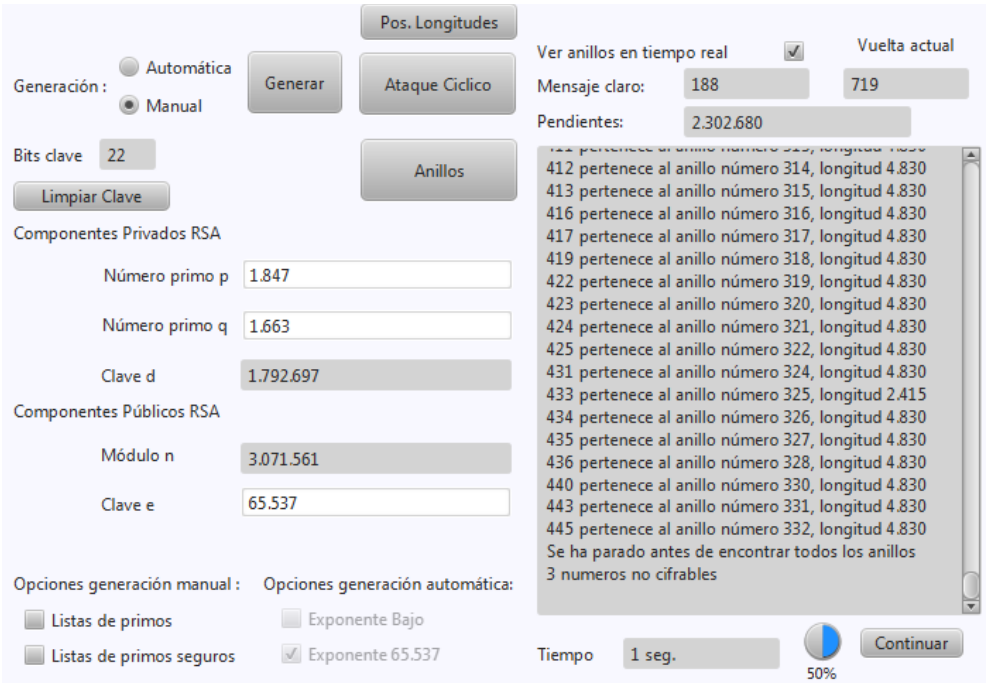

Fig. 1.4 Fracción de la ventana principal (falta zona derecha).

1.5.1 Cálculo de los anillos, Campos de la Interfaz 1/2

CheckBox: Ver anillos en tiempo real

Si se selecciona permite ver los anillos encontrados en tiempo real. Por ejemplo:

2 pertenece al anillo número 4, longitud 4.830

Mensaje claro

Muestra el número sobre el que se está realizando un ataque cíclico. Al finalizar el ataque cíclico se clasifica este número, junto con todos los números que han aparecido en el transcurso del ataque cíclico, en un anillo. La longitud de este anillo es la cantidad de números que contiene.

Vuelta actual

Vuelta del ataque cíclico en el que se encuentra para el respectivo número en claro.

Pendientes

Números que aún no se han aparecido en un anillo.

Botón: Pausar/Continuar

Se puede pausar el ataque para continuarlo posteriormente. Al pausar no se pierde ningún tipo de progreso y se actualizan los diagramas.

Zona media y derecha, únicamente no se ve la parte relativa a la generación de la clave.

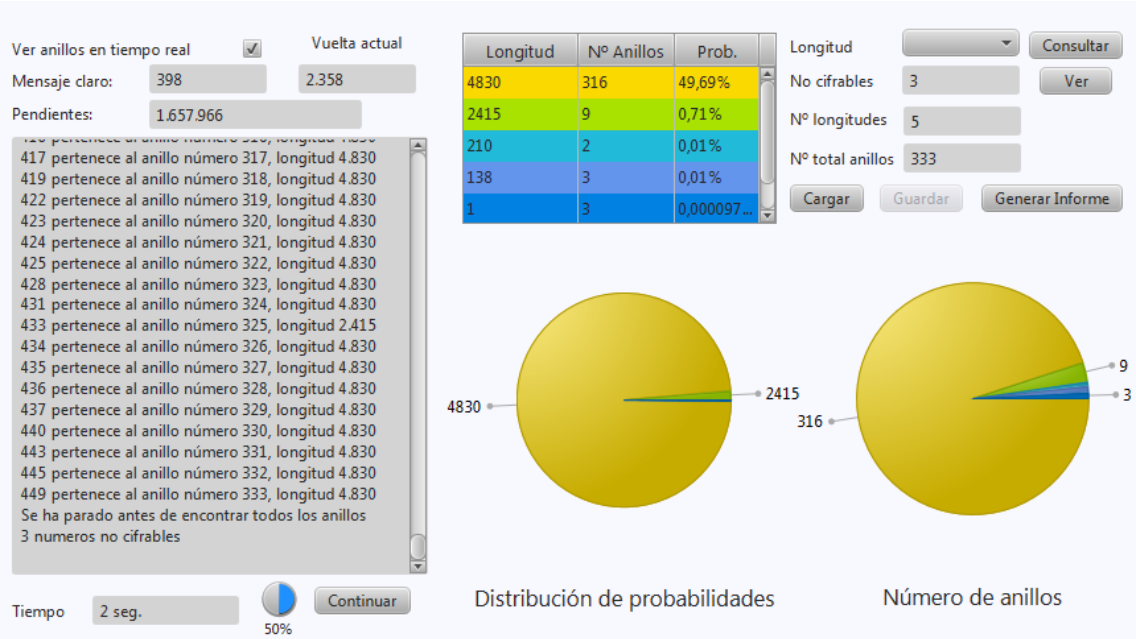

Fig. 1.5 Fracción de la ventana principal (falta zona izquierda).

1.5.1 Cálculo de los anillos, Campos de la Interfaz 2/2

Tiempo
Tiempo que lleva realizando el cálculo de los anillos

Indicador de progreso
El 100% equivale al valor del módulo. Si el módulo es 3.071.561 y hay 1.657.966 pendientes se han clasificado en un anillo aproximadamente el 50%, como muestra la figura 1.5.

TextArea
Zona en la que se escriben los anillos encontrados en tiempo real o las longitudes consultadas de los anillos. En el caso de consultar una longitud sólo se escribirán los 100.000 primeros números que pertenezcan a ese anillo:

En la figura 1.5 una de las líneas presentes en el TextArea es:

449 pertenece al anillo número 333, longitud 4.830

Tabla de Anillos
Muestra las longitudes de los anillos encontradas, el número de anillos con esa longitud, y el porcentaje de números del módulo que está contenido en un anillo con esa longitud.

Al hacer clic en la fila de una longitud se cargará un Piechart secundario si hay 15 o menos anillos con esa longitud. El mismo comportamiento se observa al consultar una longitud mediante el botón “Consultar” o al hacer clic en una sección del primer Piechart.

Piecharts
Hay un color diferente asociado a cada longitud única del anillo. Hay dos Piecharts: Distribución de probabilidades y Número de Anillos.

Longitud
Lista desplegable con todas las longitudes encontradas de los anillos. Seleccionar una y pulsar en el botón consultar para ver los primeros valores de todos los anillos que tengan esa longitud.

Nº longitudes
Número total de longitudes diferentes.

Nº total anillos
Suma total del número de anillos.

Botón: Cargar/Guardar

Se pueden guardar los ataques ya finalizados. En el caso de una búsqueda de anillos en progreso sólo se puede guardar si la longitud de la clave es mayor a 30 (no se guarda en memoria los anillos que ya han aparecido previamente). En caso contrario sería necesario guardar todos los números que ya han aparecido en un anillo, y esta información ocuparía cientos de megas. Para claves con una longitud menor o igual a 30 el cálculo completo no suele llevar más de 10 o 15 minutos.

Botón: Pausar/Continuar

Pausar y continuar el cálculo de los anillos. Al pausar se actualizan los anillos encontrados en la Tabla y Piecharts.

Botón: Consultar longitud

Permite consultar los primeros valores de cada uno de los anillos de una longitud determinada. También se puede hacer clic en la fila de la tabla en la que aparezca la longitud correspondiente o en la sección del Piechart que corresponda a la longitud.

Botón: Ver no cifrables.

Muestra los números no cifrables, aquellos que están en un anillo de longitud 1.

Botón: Generar Informe

Genera un informe con los datos de la clave, los dos Piecharts y la tabla. Hay un límite de 5 informes en la misma carpeta, rebasado este límite se sobrescribirá el archivo “Informe5.html”.

1.6 Ataque Cíclico

Utilizando la misma clave p=1.857, q=1.663, e=65.537, se podrá pulsar sobre el botón "Ataque Cíclico" de la ventana principal para abrir esta ventana secundaria.

En la siguiente figura se ha introducido un Mensaje Original aleatorio al pulsar el botón "Generar" y se ha hecho clic en "Comenzar". El modo seleccionado es "Atacar hasta que prospere".

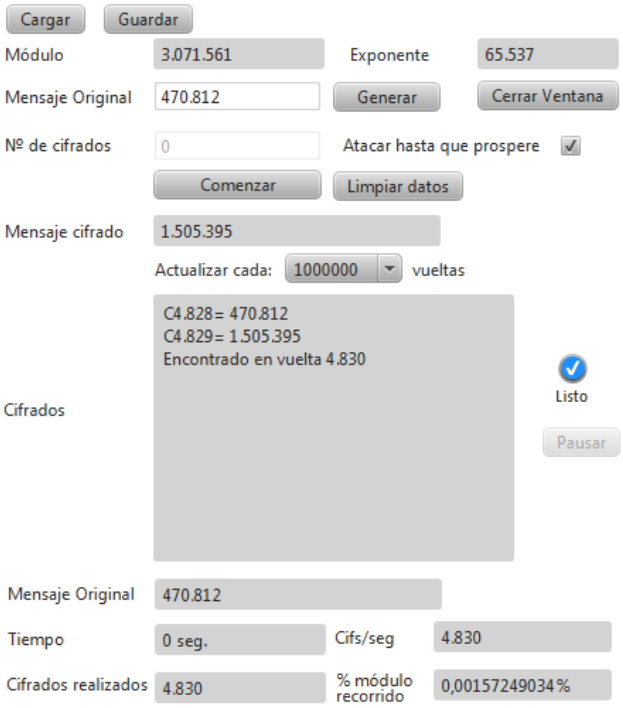

Fig. 16.6 Ataque cíclico finalizado con éxito.

Botón: Comenzar

Si hay un Mensaje original válido y un número de ciclos válido (o "Atacar hasta que prospere" seleccionado) se calcula el Mensaje cifrado y se comienzan los cálculos del ataque cíclico.

Botón: Limpiar datos

Limpia los datos de la ventana.

Botón: Cerrar Ventana

Cierra la ventana del ataque cíclico.

Botón: Cargar/Guardar, Pausar/continuar

Tras pausar el ataque cíclico se puede guardar en un fichero de texto los datos necesarios (datos de la clave, número de cifrados, resultado de la última exponenciación modular, etc). para proseguir el ataque más tarde.

Módulo y exponente

Valores de la clave RSA generada en la ventana principal.

Mensaje Original/Mensaje Cifrado

El mensaje cifrado será el punto de partida del ataque cíclico, una vez que se vuelva a obtener se podrá ver el mensaje en claro en el resultado de la penúltima operación.

Selección: N º de cifrados/Atacar hasta que prospere

En caso de introducir un número de ciclos el algoritmo se pausará tras realizar ese número de cifrados (con opción de continuar). En cambio si se ataque hasta que prospere, sólo se parará tras finalizar el ataque cíclico con éxito.

Selección: Actualizar cada 10000/100000/1000000 vueltas

Por defecto se escribe el valor de $C_i = C^e_{i-1} \bmod n$ cada 1.000.000 vueltas, pero se puede cambiar si la velocidad de cifrado es mucho más lenta.

Tiempo, Cifrados realizados, Cifs/seg, % módulo recorrido.

Se actualizarán cada segundo.