Proyecto CLCript
Cuadernos de Laboratorio de Criptografía. Entrega nº 11 (última actualización 06/05/19)
Autor: Dr. Jorge Ramió Aguirre (@criptored)
Prácticas con el algoritmo RSA. Anillos en ataque por cifrado cíclico a RSA con RingRSA

- Software RingRSA: https://www.criptored.es/software/sw_m001q.htm
- Software SAMCript: https://www.criptored.es/software/sw_m001t.htm
- Lectura de interés: MOOC Crypt4you, Lección 9: Ataque por cifrado cíclico https://www.criptored.es/crypt4you/temas/RSA/leccion9/leccion09.html

Objetivos:

1. Obtener con el software RingRSA los anillos que se forman en un ataque por cifrado cíclico para claves pequeñas, de 12 hasta 30 bits.
2. Comprobar los valores que componen esos anillos con el software SAMCript.
3. Realizar ataques por cifrado cíclico a un criptograma usando la clave pública de la víctima para descubrir un secreto cifrado con RSA.
4. Comprobar que, aunque las claves sean de igual tamaño y muy similares, el número secreto que se va a cifrar puede encontrarse en anillos de muy diferentes longitudes.

I. Encontrando anillos en el ataque por cifrado cíclico a claves RSA

Ejercicio 1)

1.1. Con RingRSA genera de forma Manual la clave RSA1 de 12 bits con p = 37, q = 61, e = 7. Pulsa luego en Anillos para encontrar todos los anillos que se producen en una cifra cíclica.
1.2. Observa con el *scroll* en la zona central del programa que para los 427 anillos encontrados se muestran todos los valores que los conforman.
1.3. Observa que al final de ese *scroll* se comprueba que los números de todos los anillos conforman el Conjunto Completo de Restos CCR del módulo 2.257.
1.4. Observa que al pinchar en cualquiera de las longitudes de los anillos, se muestran los primeros números (los más pequeños) de la cadena en cuestión.
1.5. Comprueba con SAMCript los 6 valores del anillo que comienza con el número 550. Y, además, que los valores 122, 915 y 1.999 del anillo de longitud 1 son números no cifrables.
1.6. Vuelve a encontrar los anillos si en la clave anterior ahora e = 19. Repite la operación ahora con e = 31. ¿Qué ha pasado con los anillos? ¿Son los mismos o cambian?

Comprueba tu trabajo:

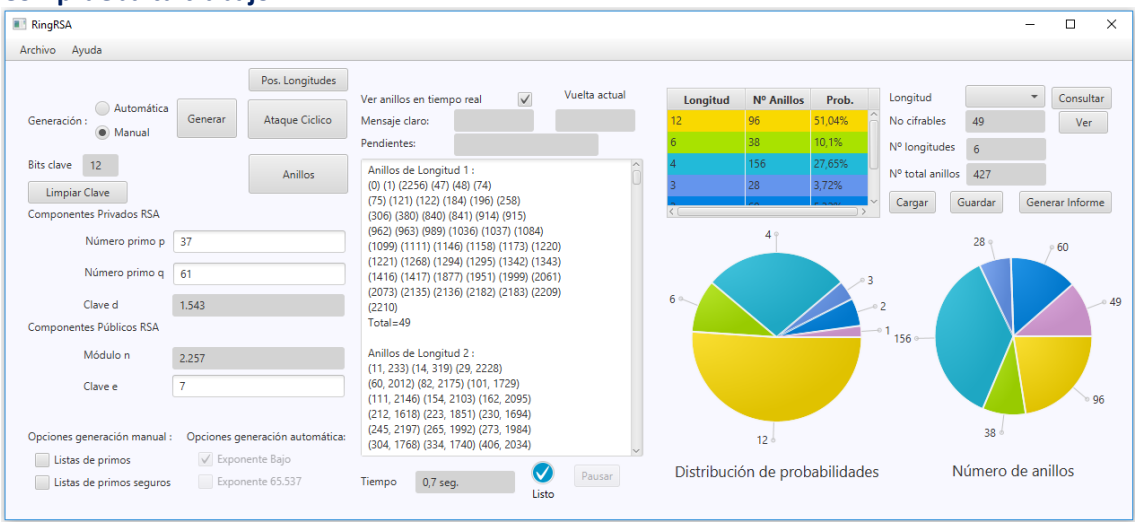

Figura 1. Anillos de la clave RSA1 de 12 bits.

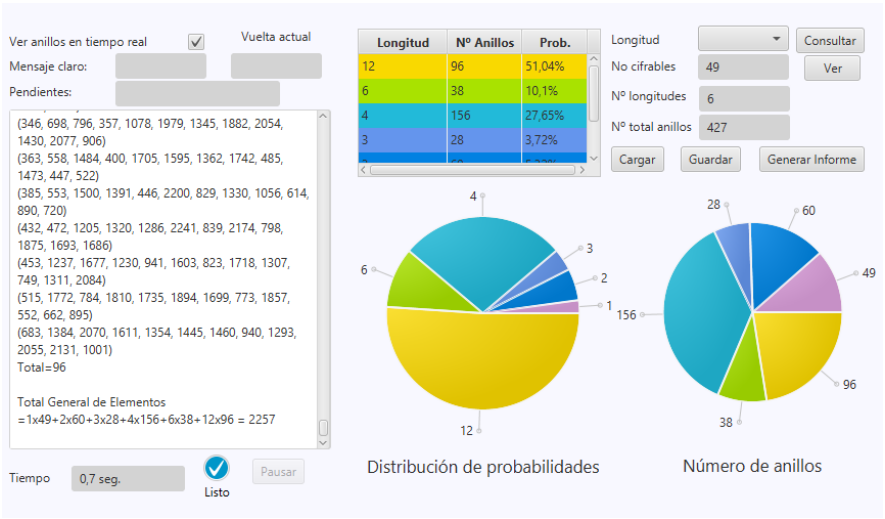

Figura 2. Los 2.257 valores de los 427 anillos de la clave RSA1 (a la izquierda abajo).

Figura 3. Primeros valores de los 36 anillos de longitud 6 de la clave RSA1.

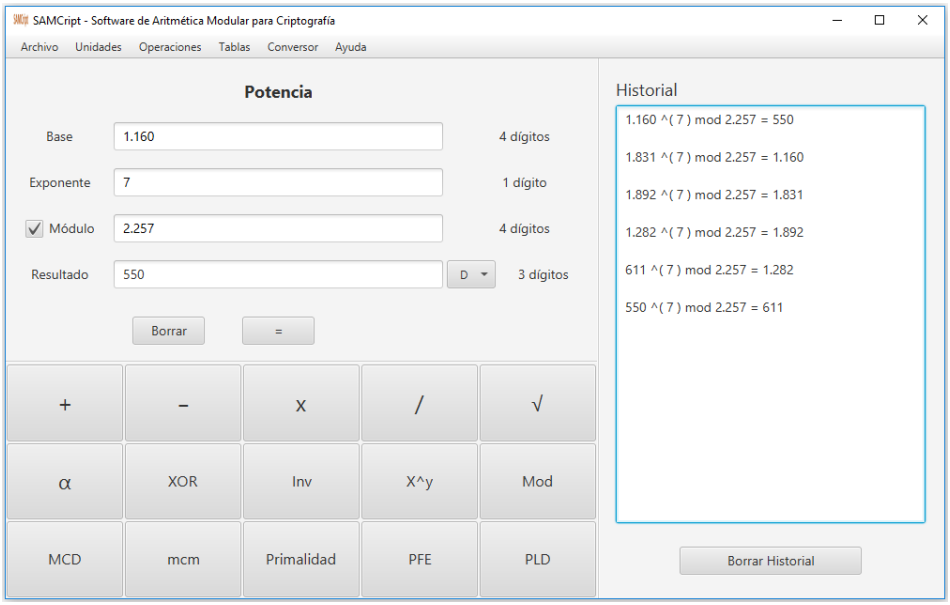

Figura 4. Comprobación del anillo {550 - 611 - 1.282 - 1.892 - 1.831 - 1.160} de RSA1.

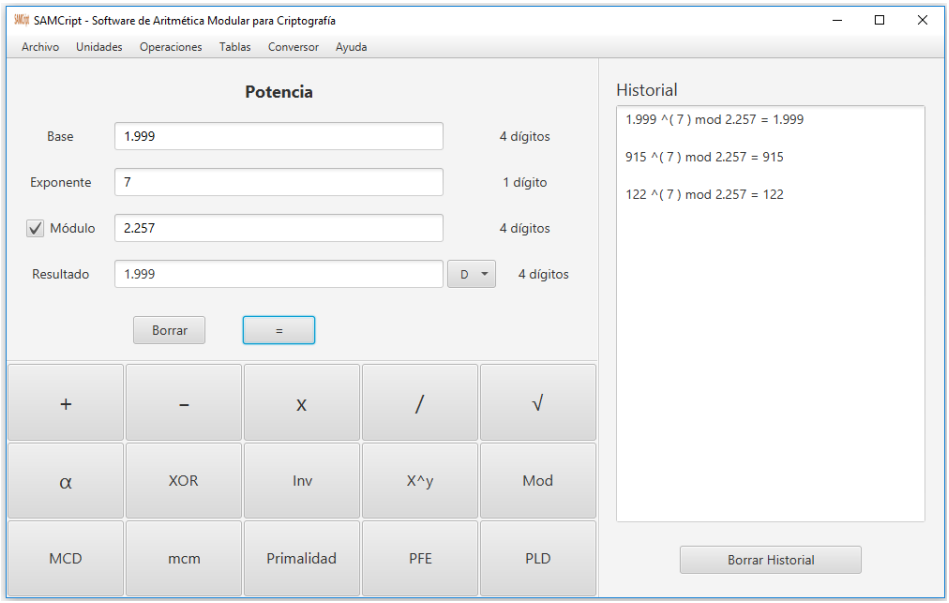

Figura 5. Comprobación con SAMCript que los números 122, 915 y 1.999 son no cifrables.

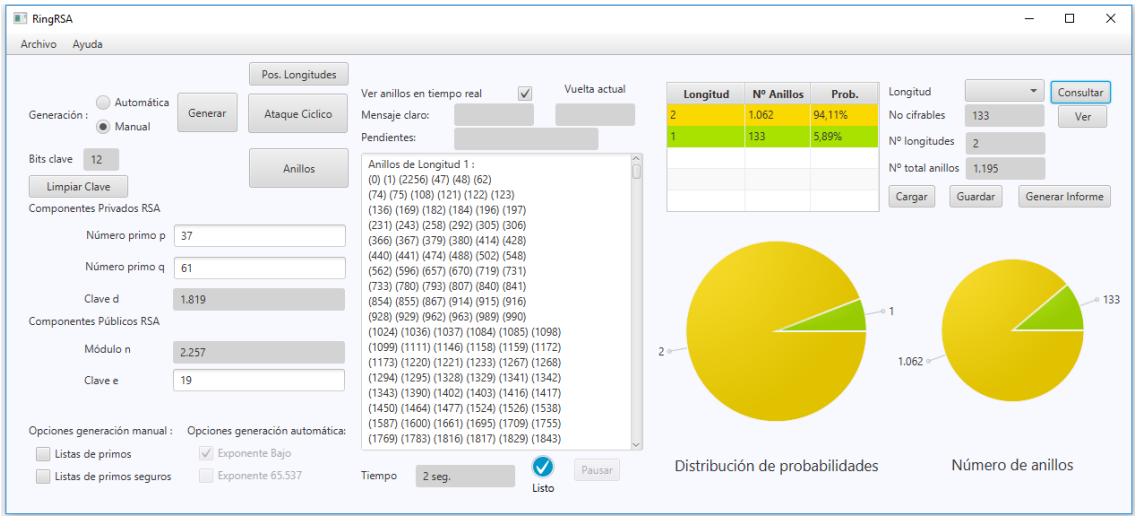

Figura 6. Modificación de anillos al cambiar la clave pública e = 7 por e = 19.

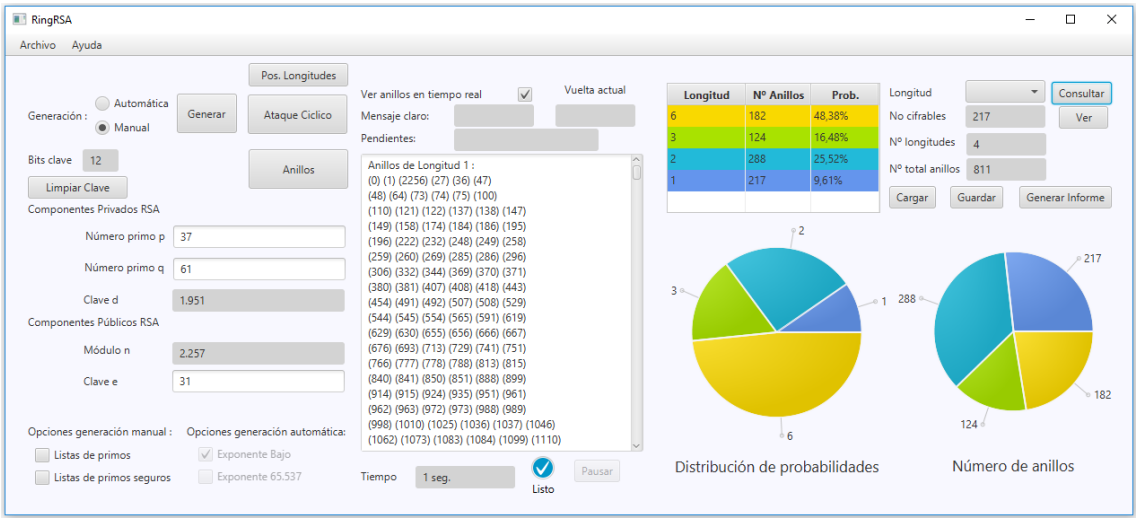

Figura 7. Modificación de anillos al cambiar la clave pública e = 7 por e = 31.

Ejercicio 2)

2.1. Con RingRSA, genera de forma Manual las claves RSA2 y RSA3 y encuentra sus anillos.
Observación: estas operaciones con claves de 30 bits pueden tardar más de 10 minutos.
RSA2: p = 25.933, q = 23.539, e = 5.
RSA3: p = 26.017, q = 22.481, e = 7.

2.2. Guarda un informe de estas dos claves con la opción Generar Informe.
Observación: el programa no notifica que se ha guardado el informe. Por lo tanto, nada más pinchar en esa opción, mira el archivo InformeNUM.html guardado en la carpeta donde reside el programa RingRSA.

2.3. Guarda la clave con la opción Guardar y ponle cualquier nombre al archivo. Hecho esto, elige la opción Limpiar Clave. Para tener todos los datos otra vez de esa clave, pulsa en Cargar y elige ese archivo.

2.4. ¿En qué clave tienes una mayor probabilidad de que un número secreto que hayas cifrado sea más fácil de atacar por un tercero mediante cifrado cíclico, RSA2 o RSA3?

2.5. ¿Cuál crees que es el algoritmo que usa RingRSA para encontrar estos anillos?

Comprueba tu trabajo:

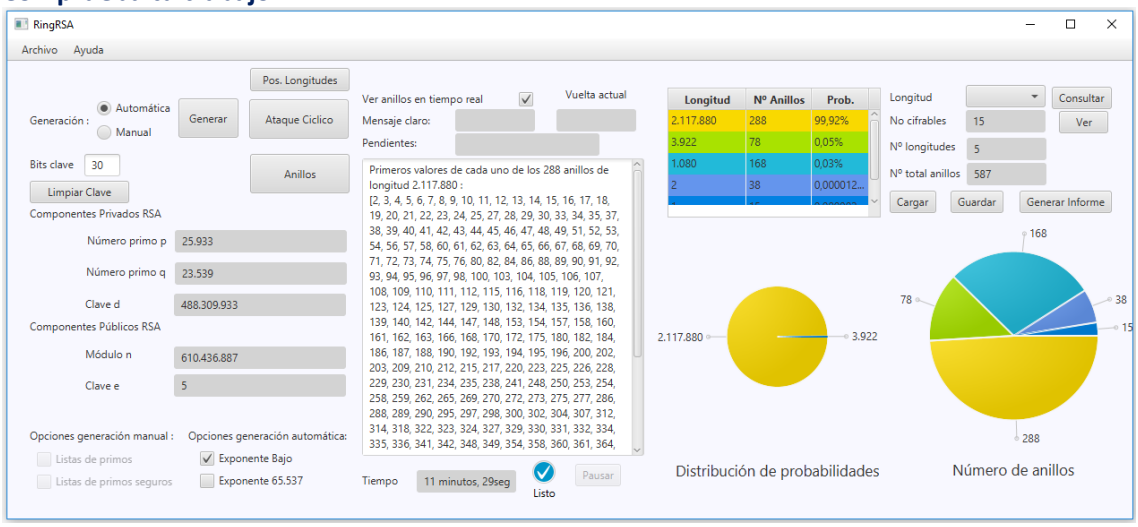

Figura 8. Anillos de longitud grande en la clave RSA2 con n = 610.436.887 y e = 5 (288 anillos de longitud 2.117.880, el 99,9% de los restos de n están en esos anillos).

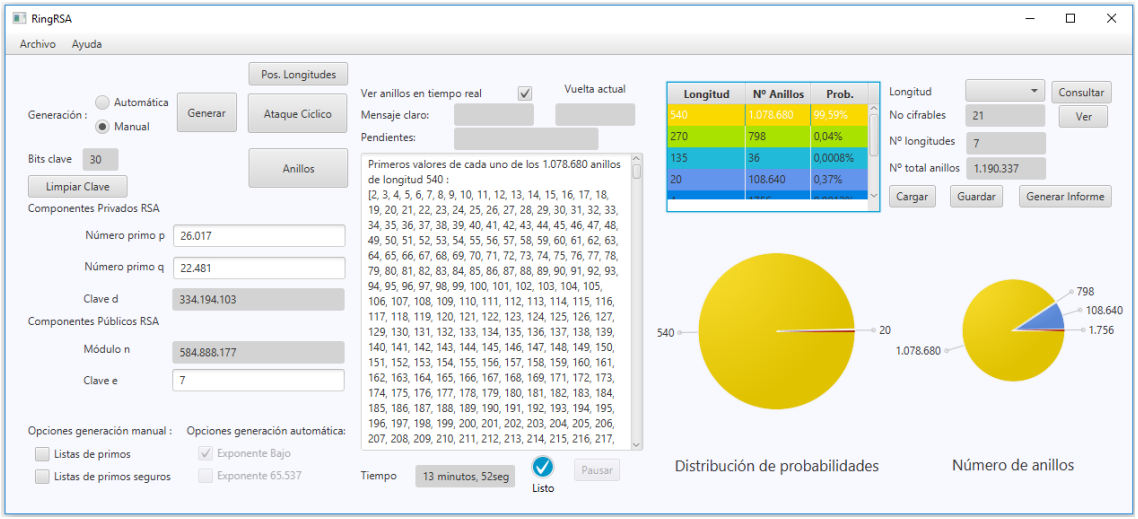

Figura 9. Anillos de longitud pequeña en la clave RSA3 con n = 584.888.177 y e = 7 (1.078.680 anillos de longitud 540, el 99,6% de los restos de n están en esos anillos).

II. Ataque por cifrado cíclico a claves RSA

Ejercicio 3)

3.1 Genera otra vez las claves RSA2 y RSA3.
RSA2: p = 25.933, q = 23.539, e = 5.
RSA3: p = 26.017, q = 22.481, e = 7.

3.2 Realiza un ataque por cifrado cíclico a ambas claves teniendo como valor secreto o Mensaje Original 999.

3.3 Observa los anillos en donde ha caído el secreto 999.

3.4 ¿Qué conclusiones puedes sacar de lo visto en este ejercicio 3?

Comprueba tu trabajo:

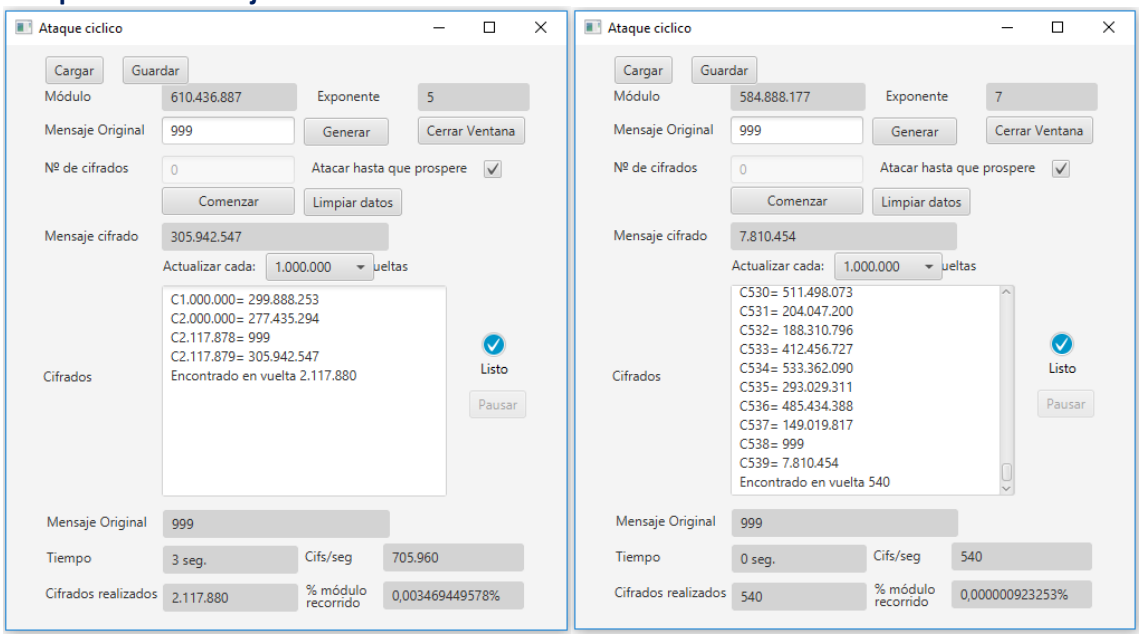

Figura 10. Ataque cíclico al Mensaje Original 999 en claves RSA2 y RSA3.

Ejercicio 4)

4.1. Crea esta clave RSA4 de 40 bits con p = 795.763, q = 700.171, e = 65.537.

4.2. Inicia un Ataque Cíclico con el Mensaje Original = 12.345, pero cuando el ataque vaya por 8.000.000 de cifrados (unos 30 segundos), pulsa en Pausa y luego pulsa en Guardar.

4.3. Guarda el archivo como AtaqueClaveRSA4Detenido.

4.4. Limpia la clave, vuelve a cargar los datos p = 795.763, q = 700.171, e = 65.537 generando la clave y pulsa en Generación Manual.

4.5. Accede a Ataque Cíclico y selecciona Cargar. Carga el archivo AtaqueClaveRSA4Detenido y pulsa a continuación en Continuar.

4.6. Observa que el ataque continúa desde el lugar donde se dejó y se guardó en un archivo, y que al final en el cifrado C13.396.010 aparece el secreto 12.345.

4.7. Vamos a realizar un ataque a K = 241.883.621.666.832.960.334.593.886.516.012.967.689, una clave secreta de 128 bits que queremos enviar con RSA en un intercambio de clave. Genera de forma Automática una clave de 1.024 bits con e = 65.537.

4.8. Antes de iniciar el ataque, selecciona Actualizar cada 100.000 cifrados. Pulsa Comenzar y detén el ataque cuando hayas superado los 200.000 cifrados. Observa que la velocidad ahora se ve seriamente mermada debido al tamaño de la clave.

4.9. Según lo aprendido, ¿sería vulnerable hoy el algoritmo RSA ante este tipo de ataques?

Comprueba tu trabajo:

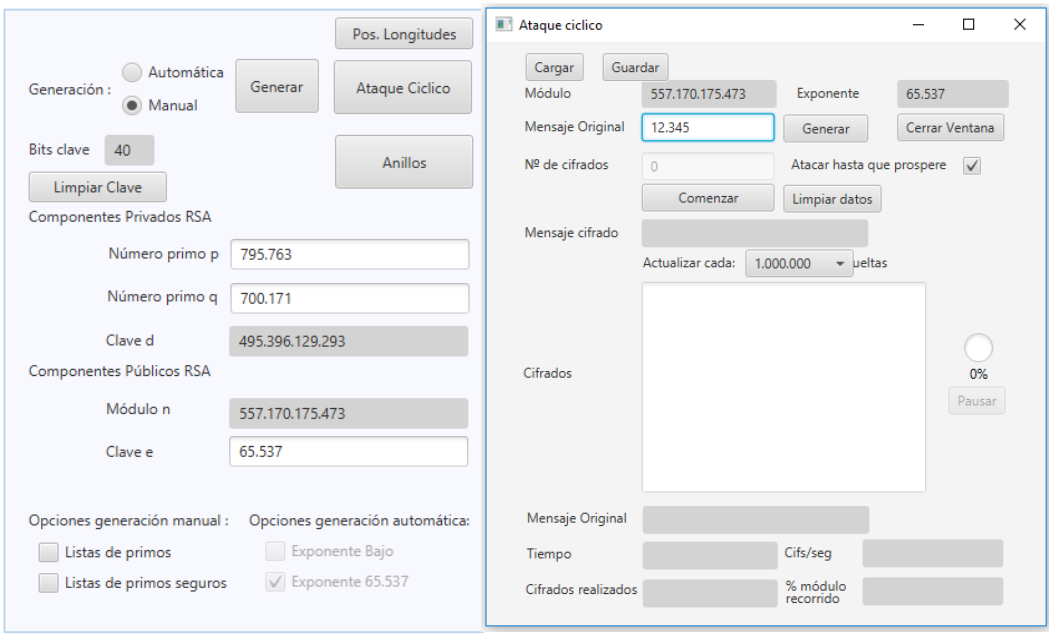

Figura 11. Clave RSA4 y preparación del ataque cíclico.

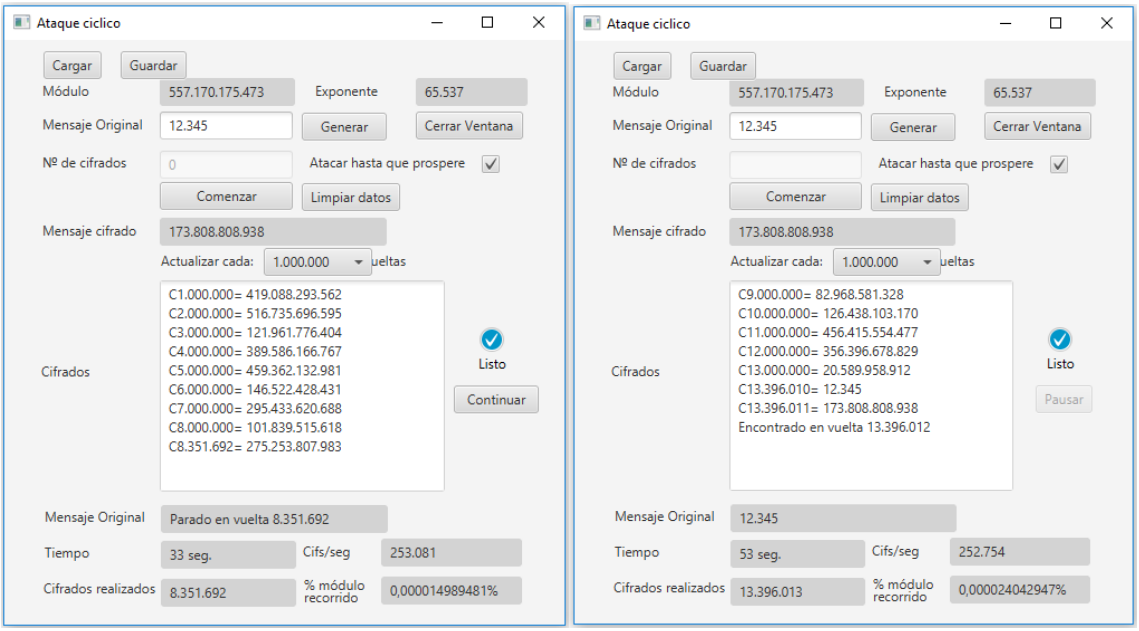

Figura 12. Ataque cíclico a la clave RSA4 detenido a los 33 segundos, guardado en un archivo y posteriormente reanudado desde donde se dejó.

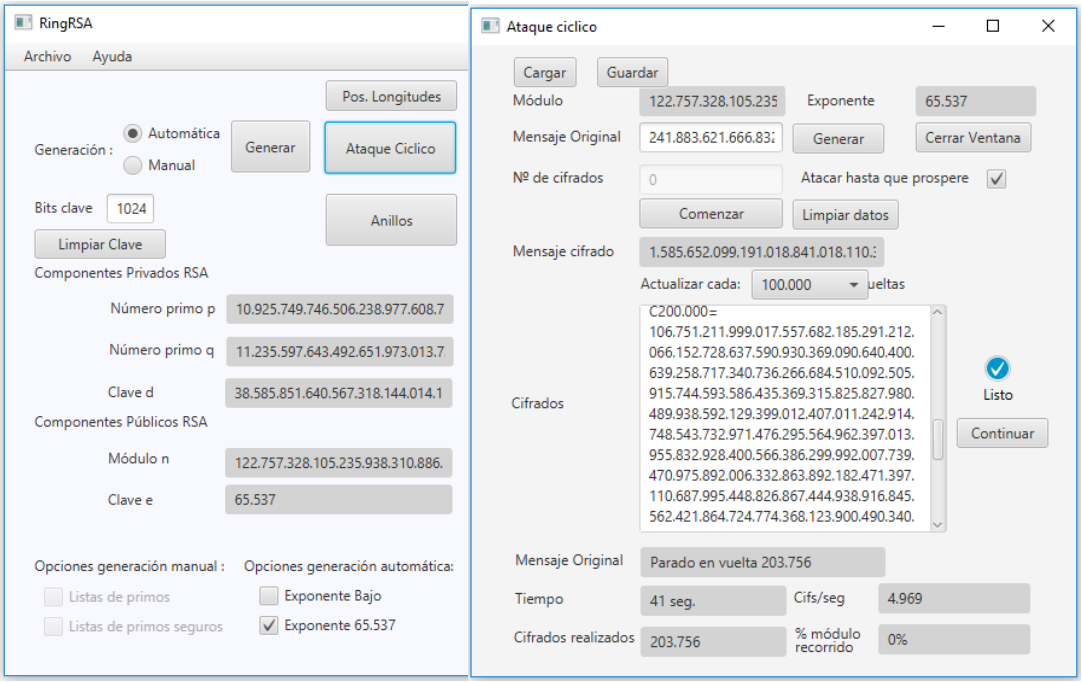

Figura 13. Intento de ataque cíclico a una clave RSA de 1.024 bits detenido en vuelta 203.756.

Madrid, 6 de mayo de 2019
Dr. Jorge Ramió Aguirre