Proyecto CLCript
Cuadernos de Laboratorio de Criptografía. Entrega nº 10 Última actualización 29/11/18
Autor: Dr. Jorge Ramió Aguirre (@criptored)
Prácticas con el algoritmo RSA: ataque por cifrado cíclico a RSA con genRSA v2.1

- Software genRSA v2.1: http://www.criptored.upm.es/software/sw_m001d.htm
- Software SAMCript: http://www.criptored.upm.es/software/sw_m001t.htm
- Lectura de interés: MOOC Crypt4you, Lección 9: Ataque por cifrado cíclico http://www.criptored.upm.es/crypt4you/temas/RSA/leccion9/leccion09.html

Objetivos:

1. Comprobar con el software genRSA que el ataque mediante el cifrado cíclico permite descubrir un secreto cifrado con RSA, conociendo solamente la clave pública de la víctima.
2. Observar la generación de anillos durante el ataque por cifrado cíclico con genRSA.
3. Comprobar la existencia de esos anillos con el software SAMCript.
4. Comprobar que, para claves similares, un número secreto al azar que se va a cifrar puede encontrarse en anillos de muy diferentes longitudes.

I. Ataques por cifrado cíclico a claves RSA

Ejercicio 1)

1. Con genRSA v2.1, genera de forma Manual las claves RSA decimales que se indican en cada apartado y realiza los ataques por cifrado cíclico.

1.1. **Clave RSA1**: p = 37, q = 61, e = 7, n = 2.257.

1.1.1. Realiza un ataque por cifrado cíclico a esta clave RSA1 con estos cuatro valores de criptograma C, con Número de cifrados 10 y pulsando Continuar si fuese necesario: C = 10, C = 11, C = 12, C = 13.

1.1.2. ¿Qué longitudes tienen los anillos en los cuatro ataques anteriores?

1.1.3. Comprueba con SAMCript los valores del anillo de longitud 6 que has encontrado.

Comprueba tu trabajo:

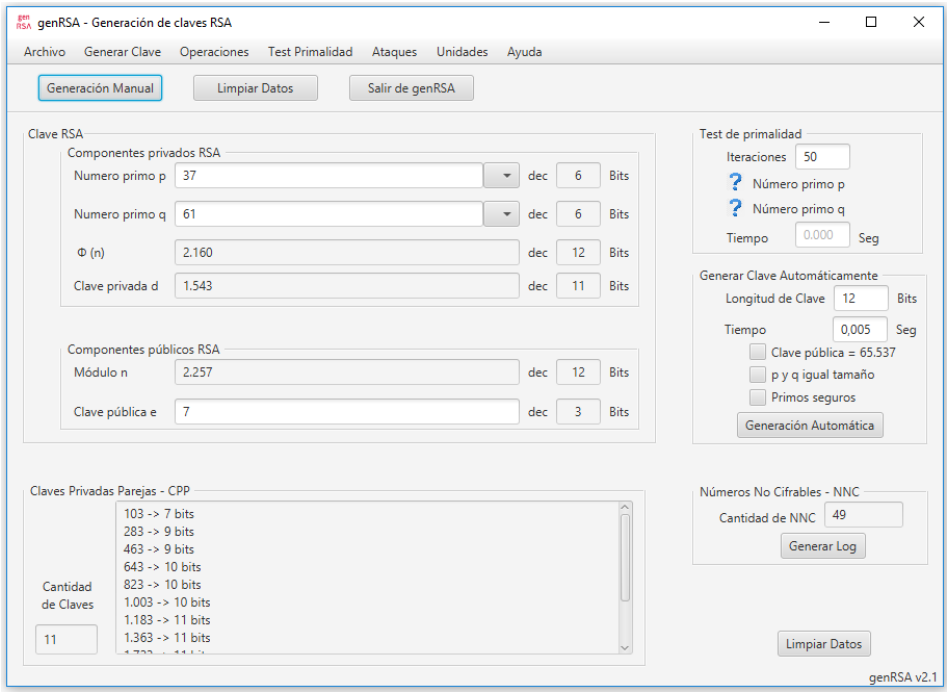

Figura 1. Clave RSA1 de 12 bits.

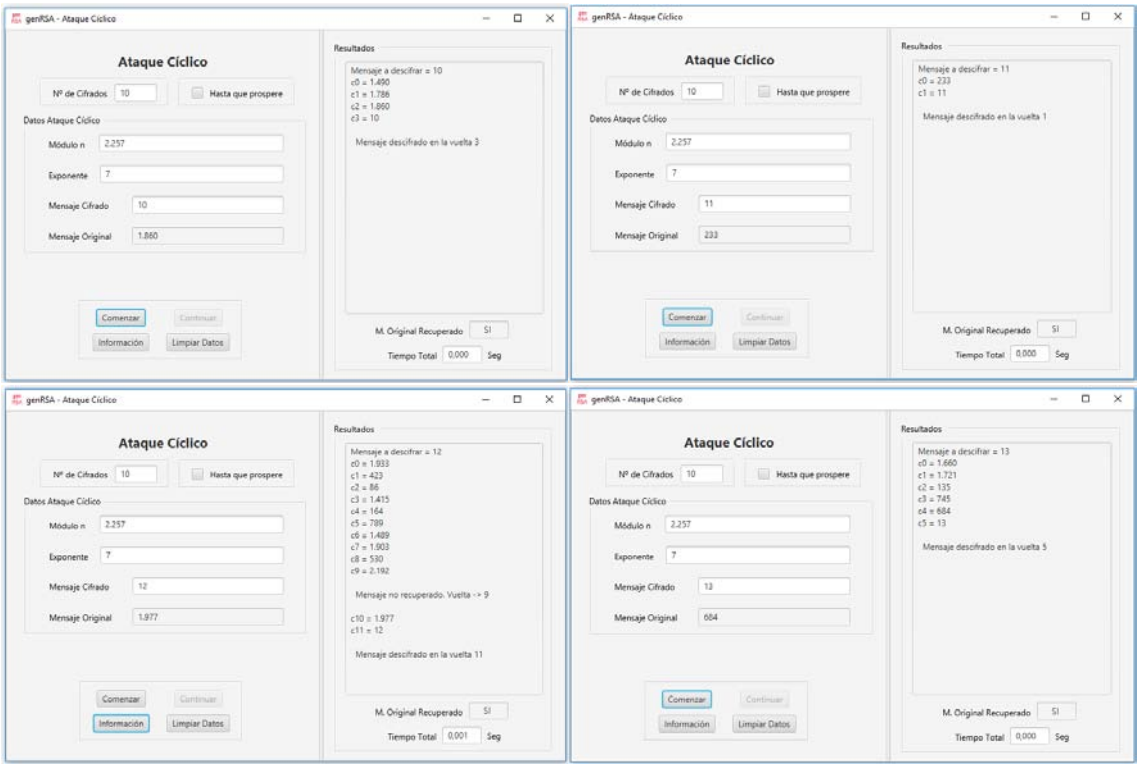

Figura 2. Ataques por cifrado cíclico con valores 10, 11, 12 y 13.

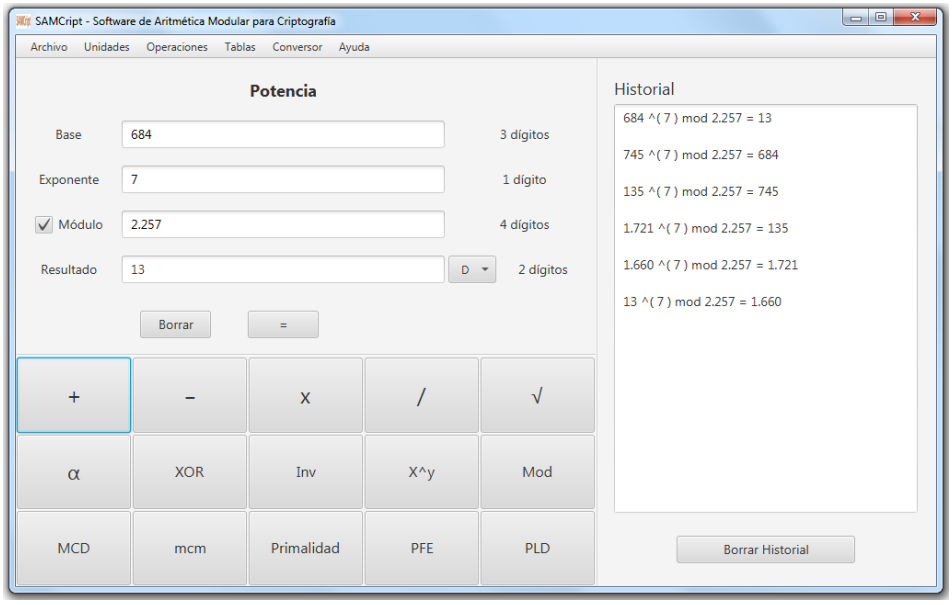

Figura 3. Comprobación con SAMCript de todos los cifrados del anillo de longitud 6.

1.2. **Clave RSA2**: p = 22.481, q = 26.017, e = 7, n = 584.888.177.

1.2.1. Ataca con C = 275.814.113, con la opción Hasta que prospere.

1.2.2. Ataca con C = 185.935.226, con la opción Hasta que prospere.

1.2.3. Ataca con C = 451.126.228, con la opción Hasta que prospere.

1.2.4. Ataca con C = 199.049.171, con la opción Hasta que prospere.

1.2.5. Ataca con C = 180.017.398, con la opción Hasta que prospere.

1.2.6. Ataca con C = 540.492.593, con la opción Hasta que prospere.

1.2.7. Ataca con C = 217.503.676, con la opción Hasta que prospere.

1.2.8. ¿Qué significa que el número 217.503.676 esté en un anillo de longitud 1?

Comprueba tu trabajo:

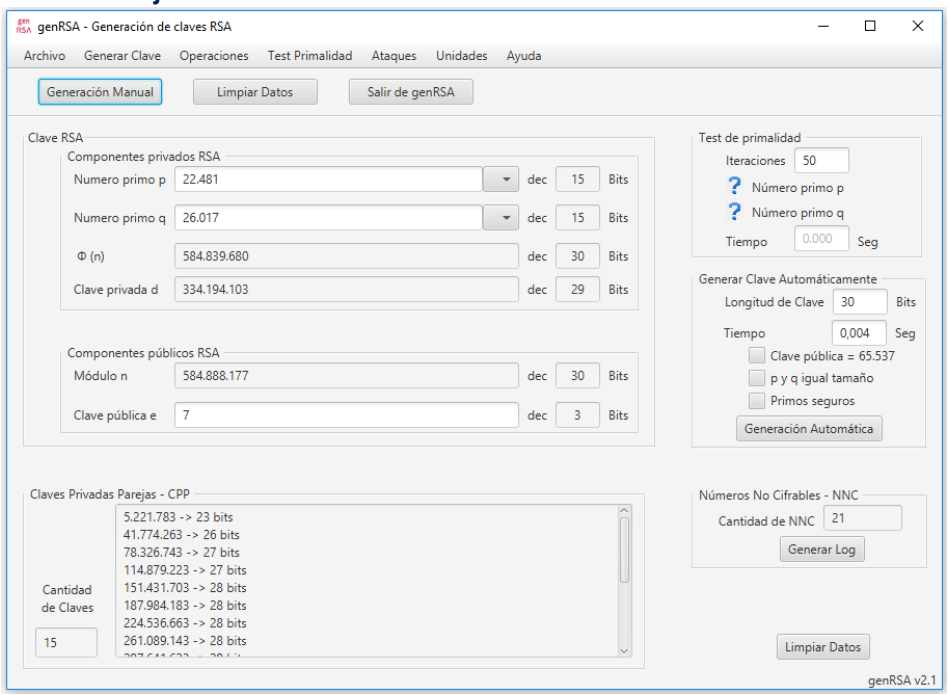

Figura 4. Clave RSA2 de 30 bits.

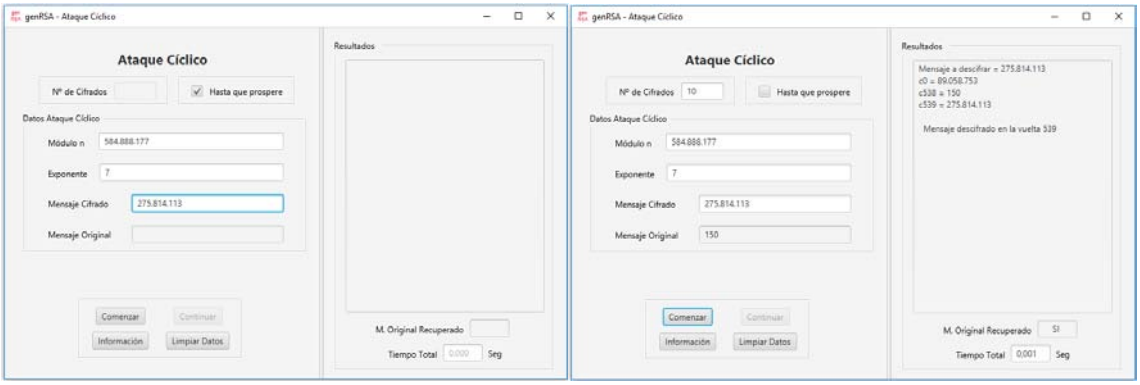

Figura 5. Ataque con cifrado cíclico con entrada 275.814.113 a la clave RSA2, en un anillo de longitud 540, recuperando el secreto 150 (los demás ataques son similares).

1.3. Claves RSA3, RSA4, RSA5, RSA6 y RSA7 de 48 bits cada una.

RSA3: p = 11.869.057, q = 13.597.697, e = 65.537, n = 161.391.840.761.729.

RSA4: p = 10.862.081, q = 14.602.633, e = 65.537, n = 158.614.982.459.273.

RSA5: p = 14.865.967, q = 15.107.707, e = 65.537, n = 224.590.673.707.669.

RSA6: p = 12.272.033, q = 12.968.533, e = 65.537, n = 159.150.264.937.589.

RSA7: p = 10.272.413, q = 15.365.137, e = 65.537, n = 157.837.033.065.581.

1.3.1. Para estas 5 claves, realiza un ataque por cifrado cíclico tomando como criptograma C el resultado de cifrar el valor secreto M = 123.456.789, con la opción Hasta que prospere. Nota: el último ataque tardará más de un día en prosperar.

1.3.2. Observa que aunque las cinco claves tienen 48 bits y son muy similares, el secreto 123.456.789 que se ataca en RSA3, RSA4, RSA5 y RSA6, se encuentra en anillos de muy diferentes longitudes: 3.245.130, 14.664.594, 198.181.620 y 607.594.680.

1.3.3. Observa además que en la clave de menor tamaño (RSA7), el secreto M = 123.456.789 se encontrará en un anillo inmenso, mayor que 32.000.000.000, en donde se ha detenido el programa, después de más de un día realizando cálculos.

1.3.4. Si lo deseas, puedes encontrar este último anillo y notificármelo vía email, adjuntando una captura de pantalla del ataque cíclico que has realizado. Lo incluiré (con tu nombre y adecuado agradecimiento) en una próxima actualización de esta práctica.

1.3.5. Según el número de cifrados realizados y el tiempo empleado en el ataque, ¿qué tasa de cifra tiene aproximadamente el programa genRSA?

Comprueba tu trabajo:

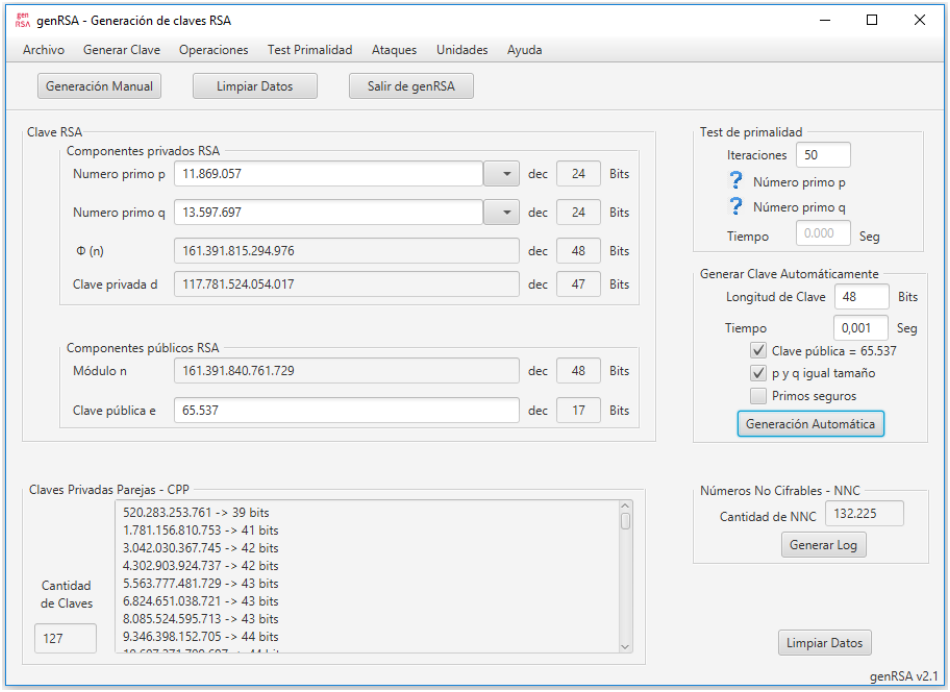

Figura 6. Clave RSA3 de 48 bits con n = 161.391.840.761.729.

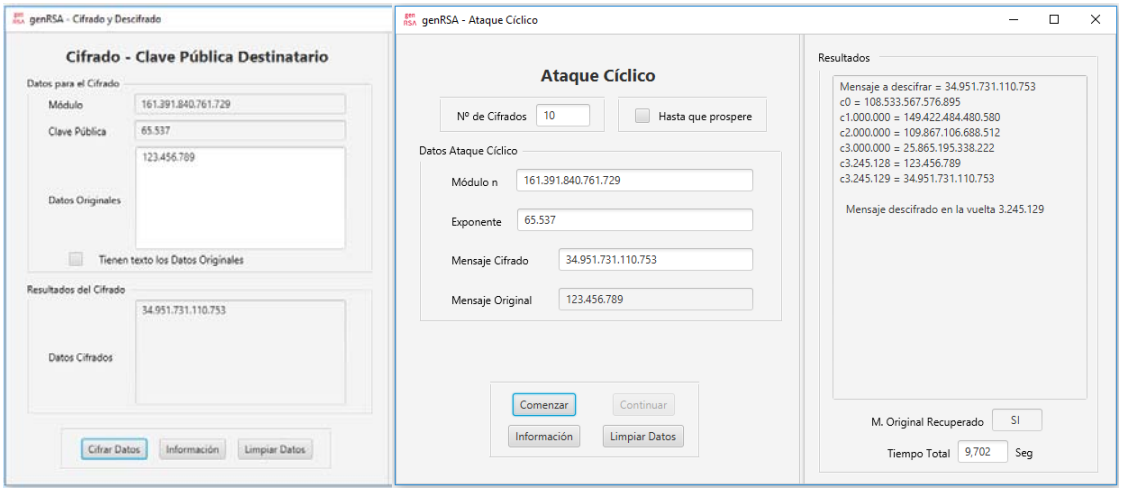

Figura 7. Ataque cíclico a la clave RSA3 con criptograma C = 34.951.731.110.753 y mensaje secreto M = 123.456.789 encontrado en anillo de longitud 3.245.130 en 10 segundos.

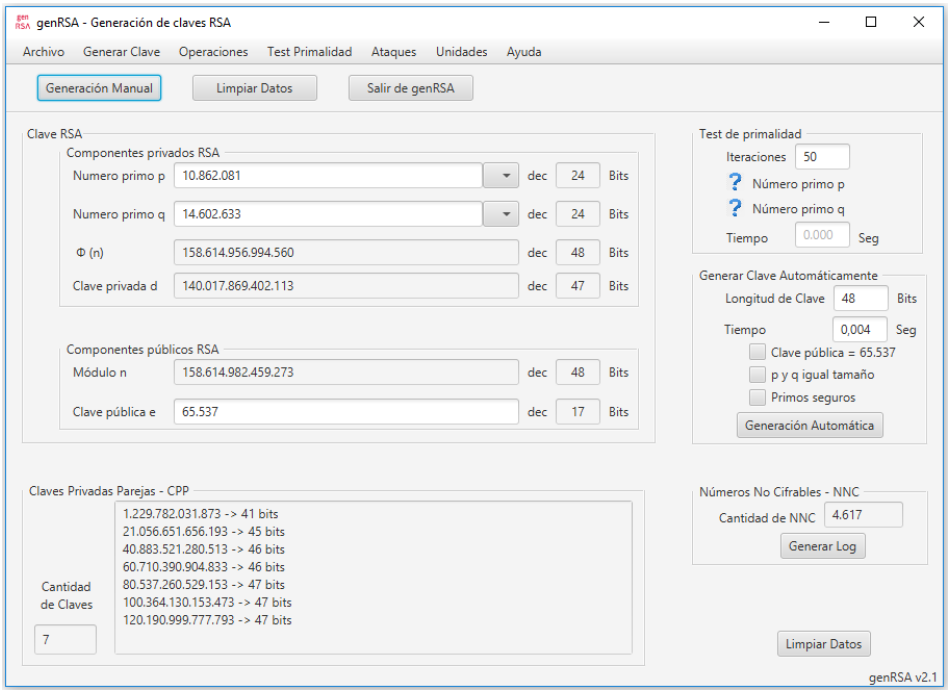

Figura 8. Clave RSA4 de 48 bits con n = 158.614.982.459.273.

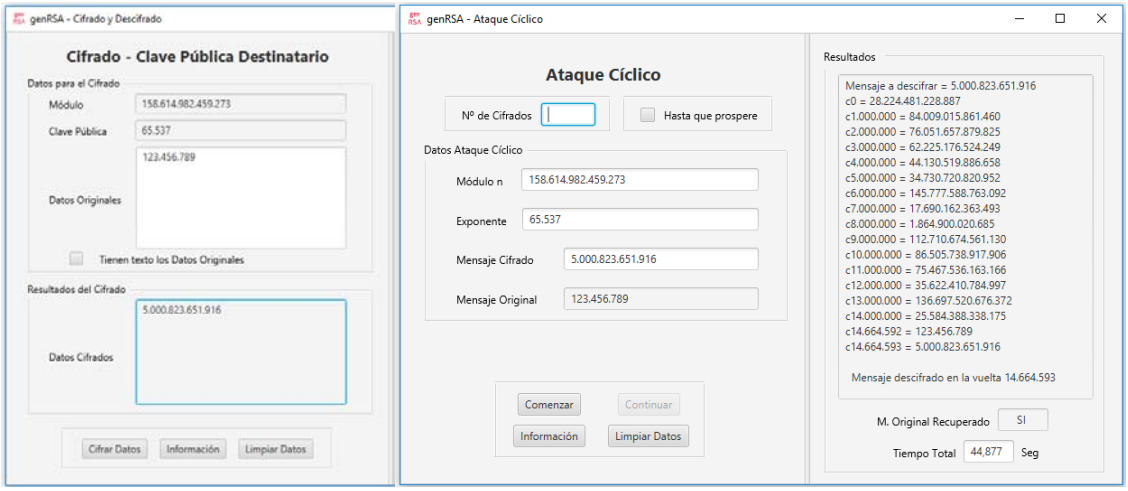

Figura 9. Ataque cíclico a la clave RSA4 con criptograma C = 5.000.823.651.916 y mensaje secreto M = 123.456.789 encontrado en anillo de longitud 14.664.594 en 45 segundos.

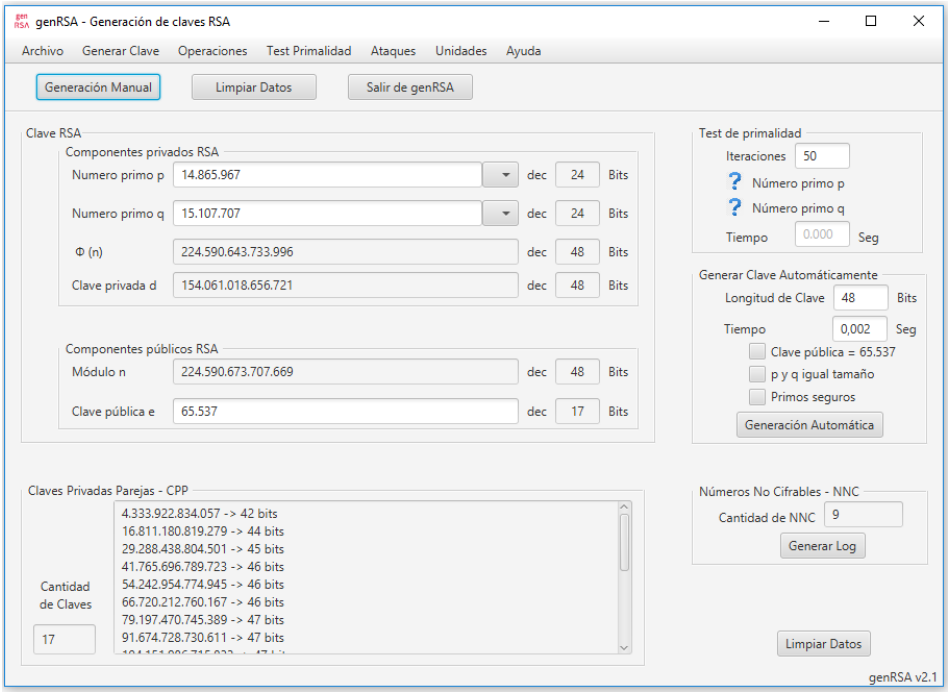

Figura 10. Clave RSA5 de 48 bits con n = 224.590.673.707.669.

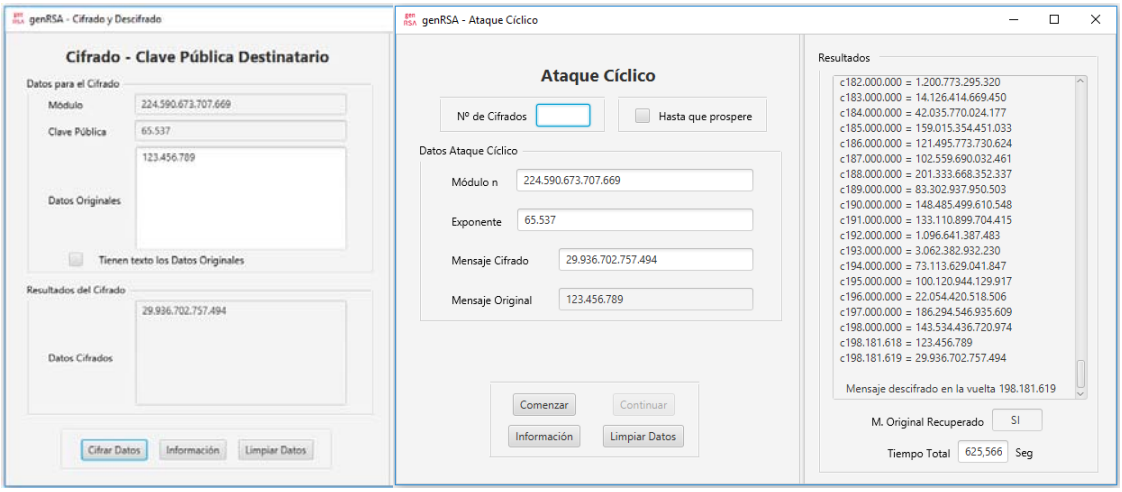

Figura 11. Ataque cíclico a la clave RSA5 con criptograma C = 29.936.702.757.494 y mensaje secreto M = 123.456.789 encontrado en anillo de longitud 198.181.620 en 625 segundos.

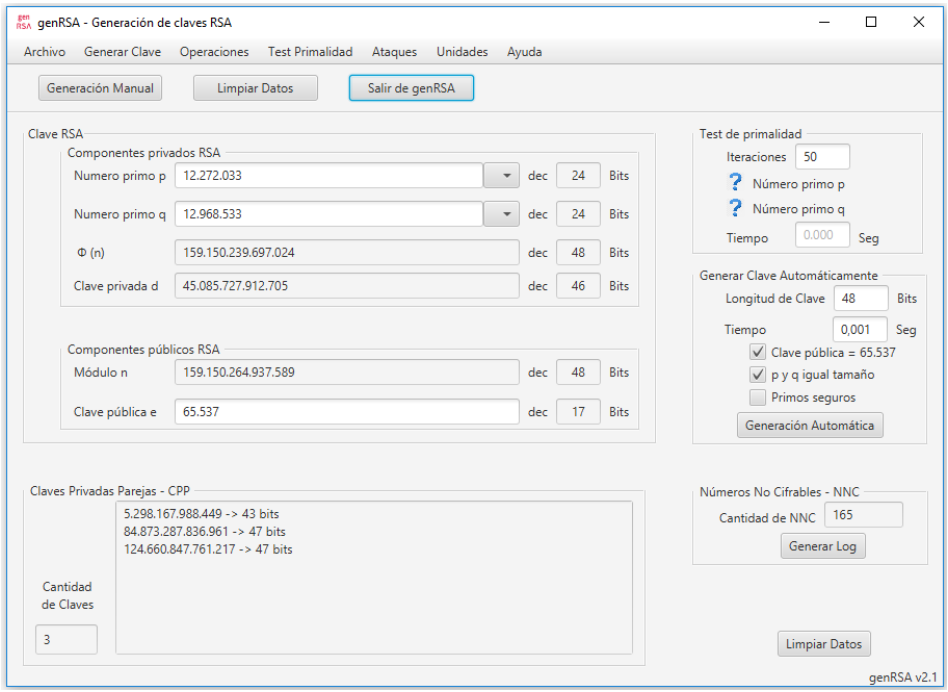

Figura 12. Clave RSA6 de 48 bits con n = 159.150.264.937.589.

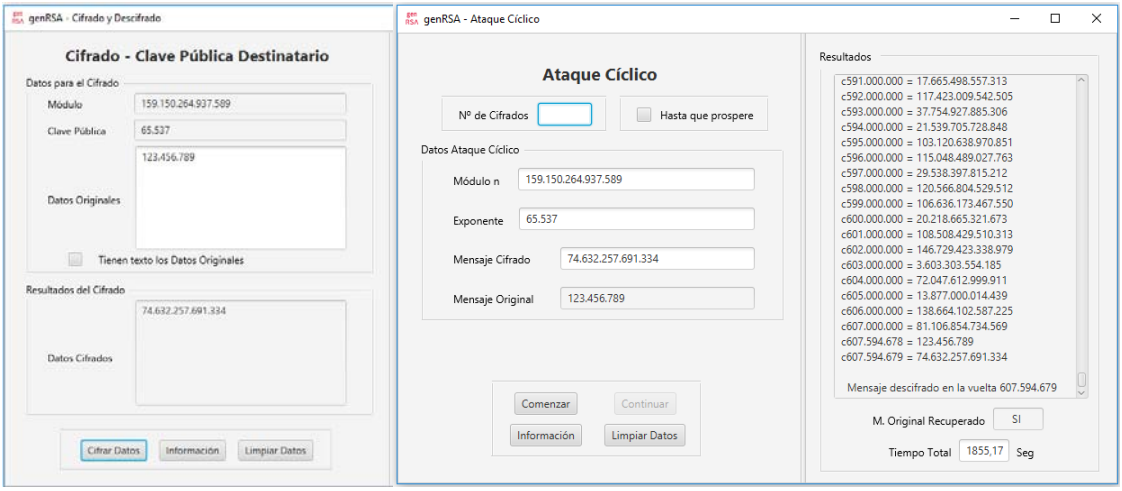

Figura 13. Ataque cíclico a la clave RSA6 con criptograma C = 74.632.257.691.334 y mensaje secreto M = 123.456.789 encontrado en anillo de longitud 607.594.680 en 1.855 segundos (31 minutos).

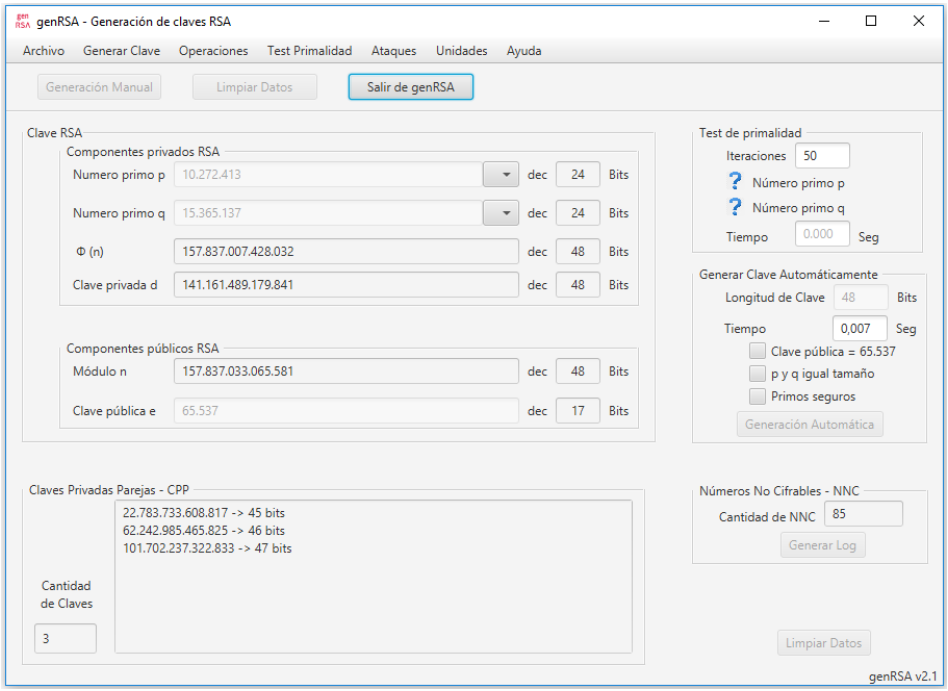

Figura 14. Clave RSA7 de 48 bits con n = 157.837.033.065.581.

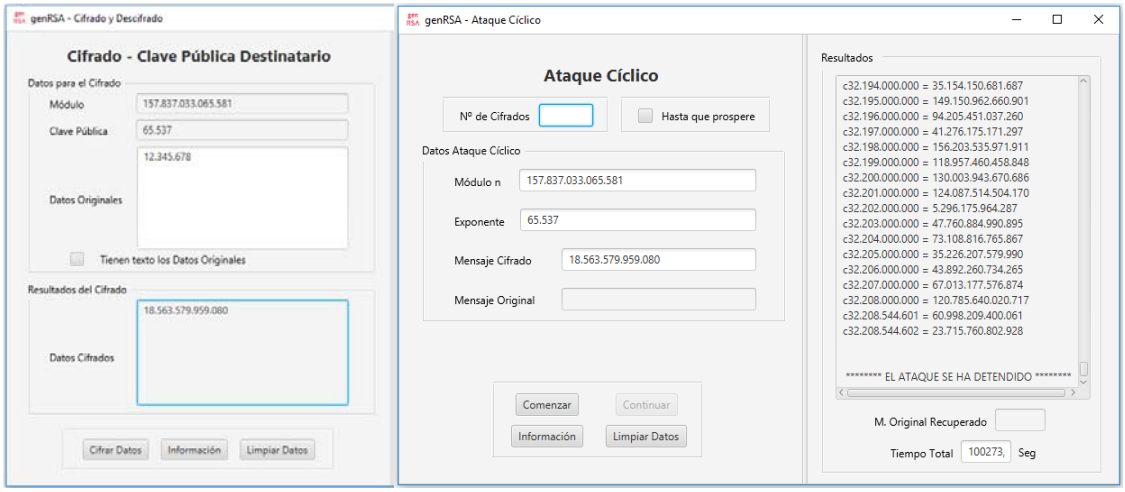

Figura 15. Intento de ataque cíclico a la clave RSA7 con criptograma C = 18.563.579.959.080 y mensaje secreto M = 123.456.789 cuyo anillo es mayor que 32.000.000.000.
Ataque detenido después de 100.273 segundos (28 horas) en ejecución.