Proyecto CLCript
Cuadernos de Laboratorio de Criptografía. Entrega nº 7 Última actualización 24/10/18
Autor: Dr. Jorge Ramió Aguirre (@criptored)
Prácticas con el algoritmo RSA: ataque por paradoja del cumpleaños con genRSA v2.1

- Software genRSA v2.1: http://www.criptored.upm.es/software/sw_m001d.htm
- Lectura de interés: http://www.criptored.upm.es/crypt4you/temas/RSA/leccion10/leccion10.html
- Tablas y códigos: http://www.criptored.upm.es/descarga/Codigos_y_tablas_de_uso_frecuente_en_criptografia.pdf

Objetivos:

1. Comprobar que si un ataque a RSA por la paradoja del cumpleaños prospera, éste encuentra la clave privada, una clave privada pareja o bien un falso positivo.
2. Comprobar el punto anterior para una clave RSA pequeña, introduciendo todos los posibles valores de entrada.
3. Observar cómo se realiza un ataque por la paradoja del cumpleaños a claves RSA de hasta 50 bits con el software genRSA v2.1.

I. Ataque a clave RSA pequeña que entrega preferentemente la clave privada

Ejercicio 1)

1.1. Con genRSA v2.1 genera de forma Manual una clave RSA con p = 7, q = 13, e = 5 en formato decimal. Guarda la clave como RSA_CLC06_punto11.html y apunta los valores de la clave privada.

1.2. Limpia los Datos. Elige la opción Ataques y selecciona Paradoja del Cumpleaños. Realiza el ataque para el Módulo 91 y la Clave Pública 5 con todos los Mensajes M de entrada posibles, desde M = 1 hasta M = 90.

1.3. Comprueba que se obtienen estos resultados para 0 < M < n:

a) No es posible el ataque porque M es un Número No Cifrable para M = 1, 8, 13, 14, 21, 27, 34, 57, 64, 70, 77, 78, 83, 90.

b) Se obtiene de clave privada d = 29 para M = 2, 3, 4, 5, 6, 7, 10, 11, 12, 15, 16, 17, 19, 20, 21, 23, 24, 25, 28, 30, 31, 32, 33, 36, 37, 38, 40, 41, 43, 44, 45, 46, 47, 48, 50, 51, 52, 54, 55, 58, 59, 60, 61, 62, 36, 66, 67, 68, 69, 71, 72, 73, 75, 76, 80, 82, 84, 85, 86, 87, 88, 89.

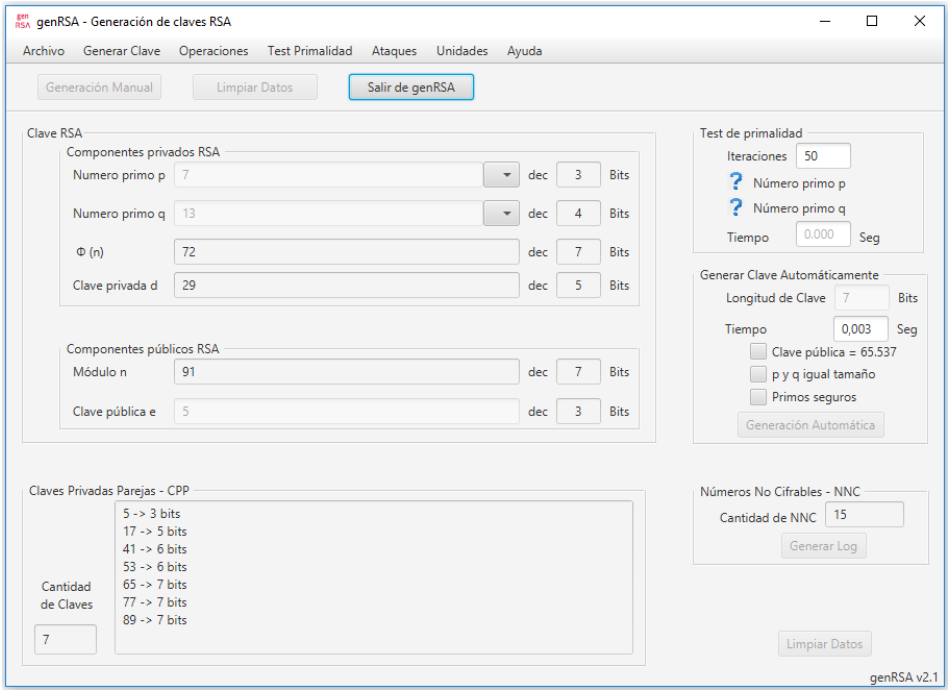
c) Se obtiene la clave privada pareja d_i = 17 para M = 26, 49, 52, 56.

d) Se obtiene un falso positivo d_{FP} = 2 para M = 9, 18, 22, 29, 35, 39, 42, 53, 65, 74, 79, 81.

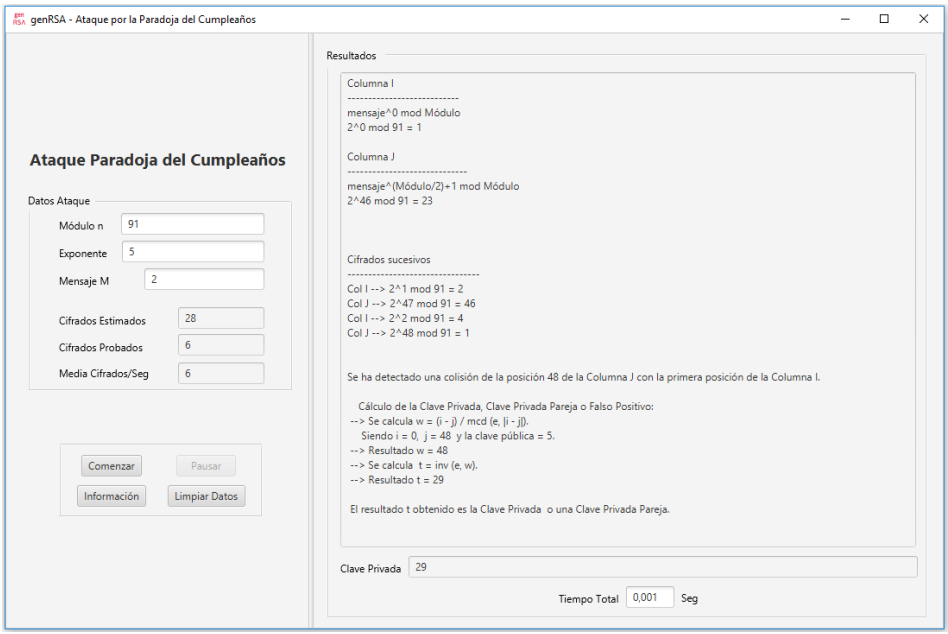
1.4. Comprueba la calculadora de Windows que los valores indicados en el apartado d) son falsos positivos. Es decir, el criptograma resultante de la cifra se descifra con ese valor, que no es la clave privada ni ninguna de las claves privadas parejas. Esto es, que sólo sirve para descifrar el número usado en el ataque pero no es una solución genérica.

1.5. Con las ecuaciones que entrega el programa genRSA v2.1 tras terminar el ataque, comprueba que los resultados son correctos.

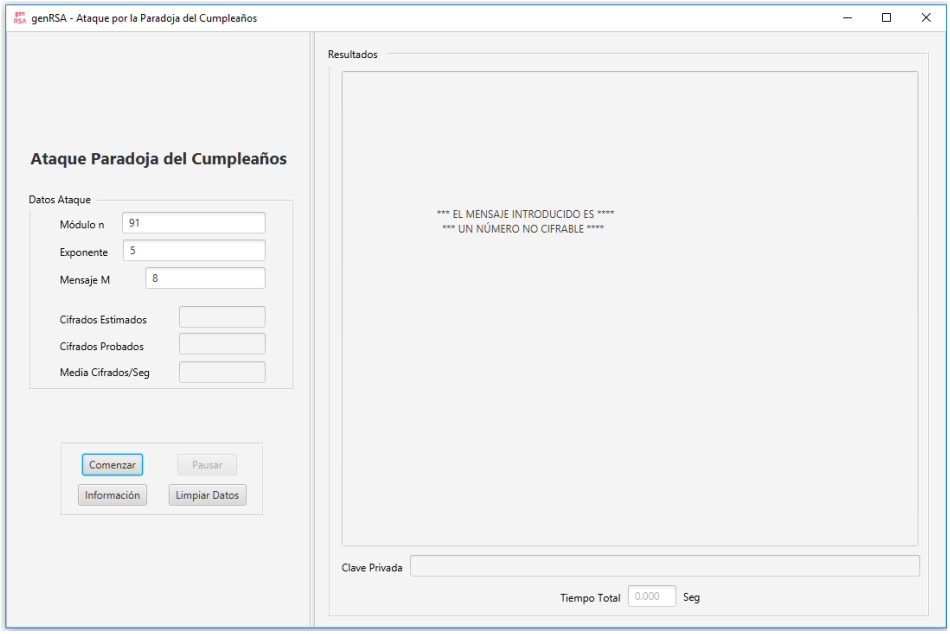
Comprueba tu trabajo:



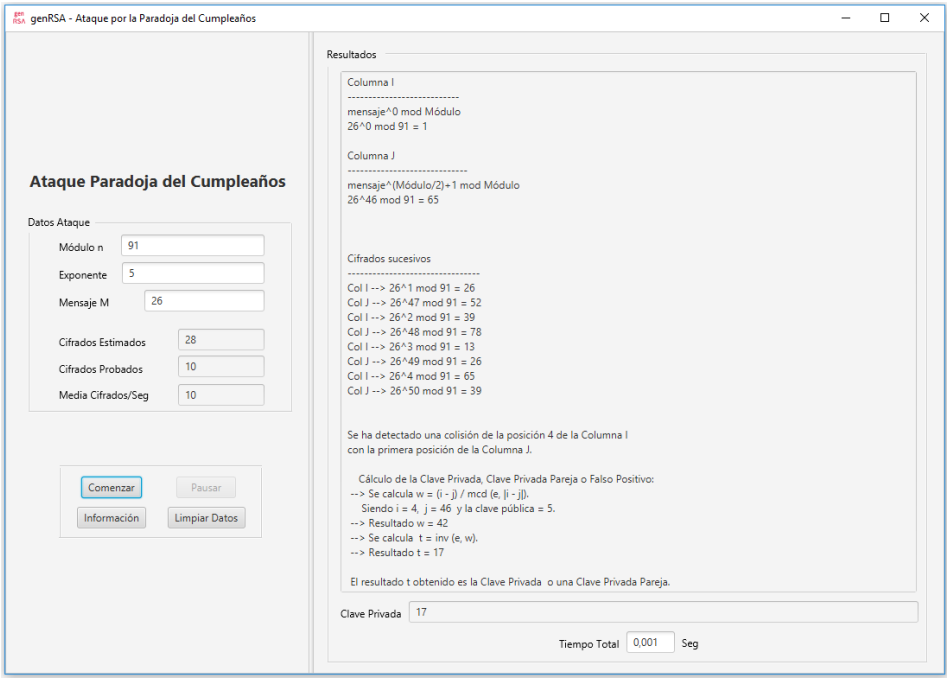
Clave del apartado 1.1.



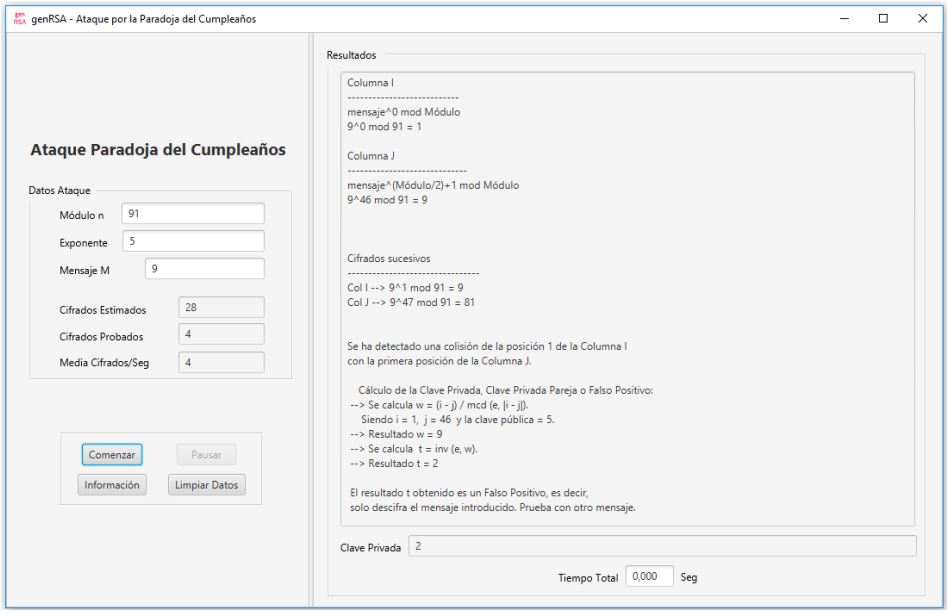
Ataque que encuentra la clave privada 29.



Ataque no posible al ser 8 un número no cifrable.



Ataque que encuentra la clave privada pareja 17.



Ataque que el falso positivo 2.

$9^5 \bmod 91 = 81$

$81^2 \bmod 91 = 9$ (lógicamente $81^d \bmod 91 = 9$ para d = 29, 5, 17,…)

II. Ataque a clave RSA pequeña que entrega preferentemente una clave privada pareja Ejercicio 2)

2.1. Con genRSA v2.1 genera de forma Manual una clave RSA con p = 7, q = 19, e = 5 en formato decimal. Guarda la clave como RSA_CLC06_punto21.html y apunta los valores de la clave privada y de las claves privadas parejas.

2.2. Limpia los Datos. Elige la opción Ataques y selecciona Paradoja del Cumpleaños. Realiza el ataque para el Módulo 133 y la Clave Pública 5 con todos los Mensajes M de entrada posibles, desde M = 1 hasta M = 132.

2.3. Comprueba que se obtienen estos resultados para 0 < M < n:

a) No es posible el ataque porque M es un Número No Cifrable para M = 1, 20, 56, 57, 76, 77, 113, 132.

b) Se obtiene la clave privada pareja $d_i = 29$ para M = 2, 3, 5, 6, 10, 13, 15, 17, 22, 24, 29, 32, 33, 34, 40, 41, 47, 48, 51, 52, 53, 54, 55, 59, 60, 61, 62, 66, 67, 71, 72, 73, 78, 79, 80, 82, 86, 89, 90, 97, 101, 104, 108, 109, 110, 111, 116, 117, 118, 124, 127, 128, 129, 131.

c) Se obtiene la clave privada pareja $d_i = 11$ para M = 14, 21, 70, 91, 98, 105,

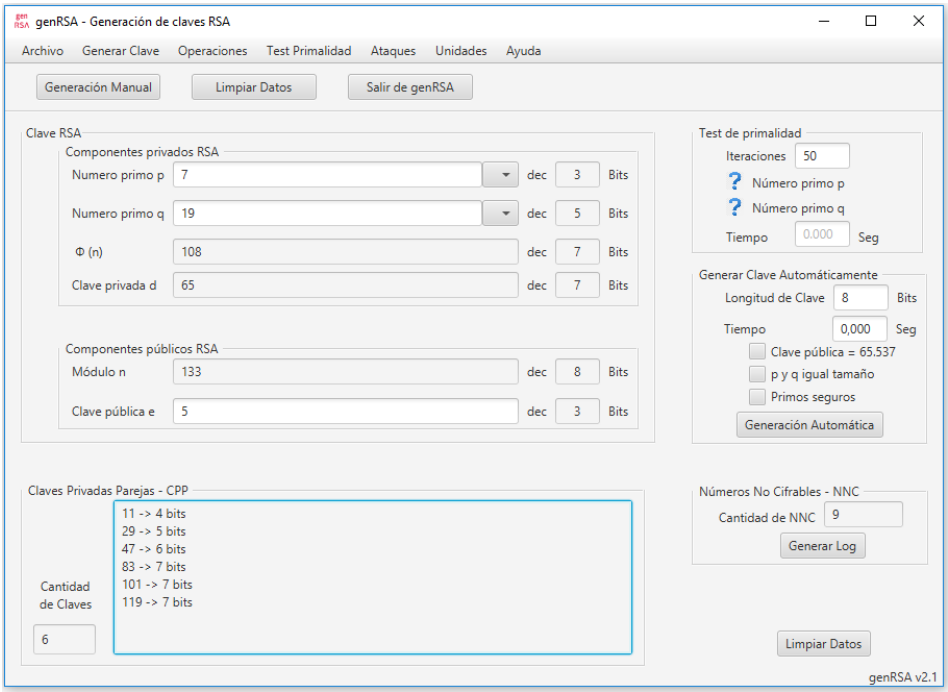
d) Se obtiene un falso positivo $d_{FP} = 38$ para M = 4, 9, 16, 23, 25, 28, 35, 36, 42, 43, 44, 63, 74, 81, 85, 92, 93, 99, 100, 112, 119, 120, 123, 130.

e) Se obtiene un falso positivo $d_{FP} = 53$ para M = 7, 8, 11, 12, 18, 19, 26, 27, 30, 31, 37, 38, 39, 45, 46, 49, 50, 58, 64, 65, 68, 69, 75, 83, 84, 87, 88, 94, 95, 96, 102, 103, 106, 107, 114, 115, 121, 122, 125, 126.

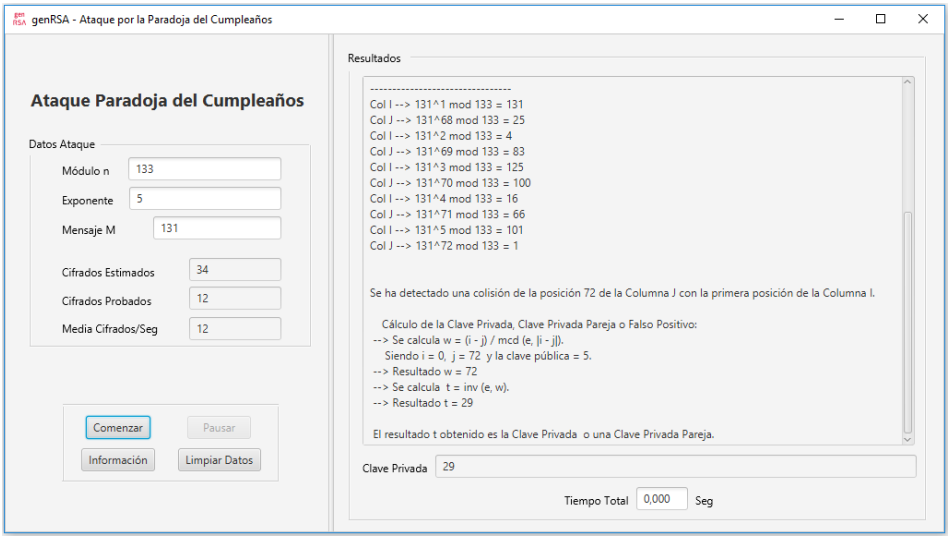
2.4. Comprueba los falsos positivos del apartado d).

2.5. Con las ecuaciones que entrega el programa genRSA v2.1 tras finalizar el ataque, comprueba que todos los resultados son correctos.

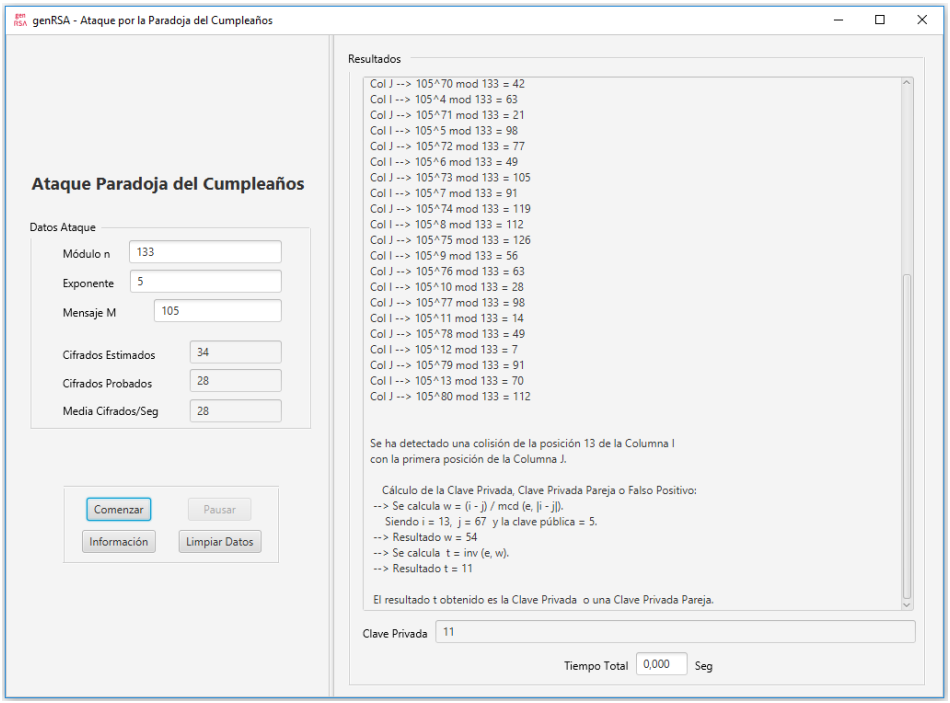
Comprueba tu trabajo:



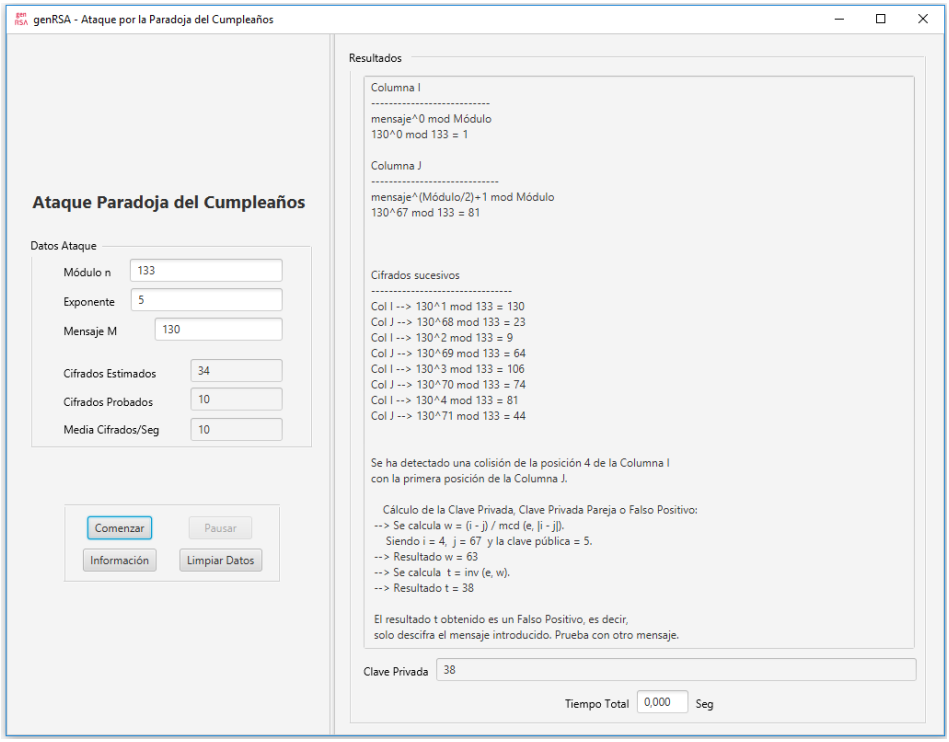
Clave del apartado 2.1.



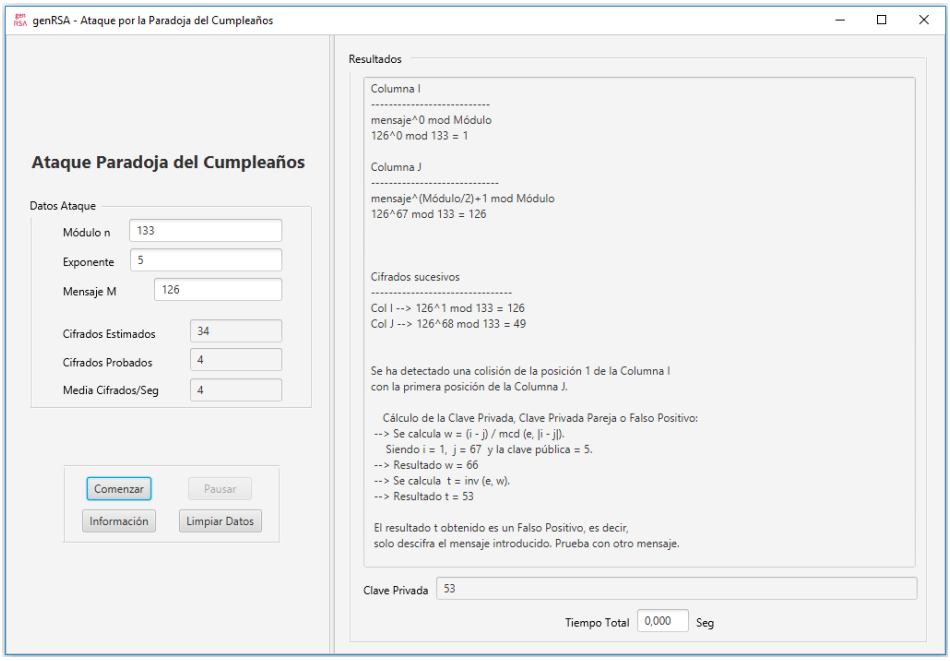
Ataque que encuentra la clave privada pareja 29.



Ataque que encuentra la clave privada pareja 11.



Ataque que encuentra el falso positivo 38.



Ataque que encuentra el falso positivo 53.

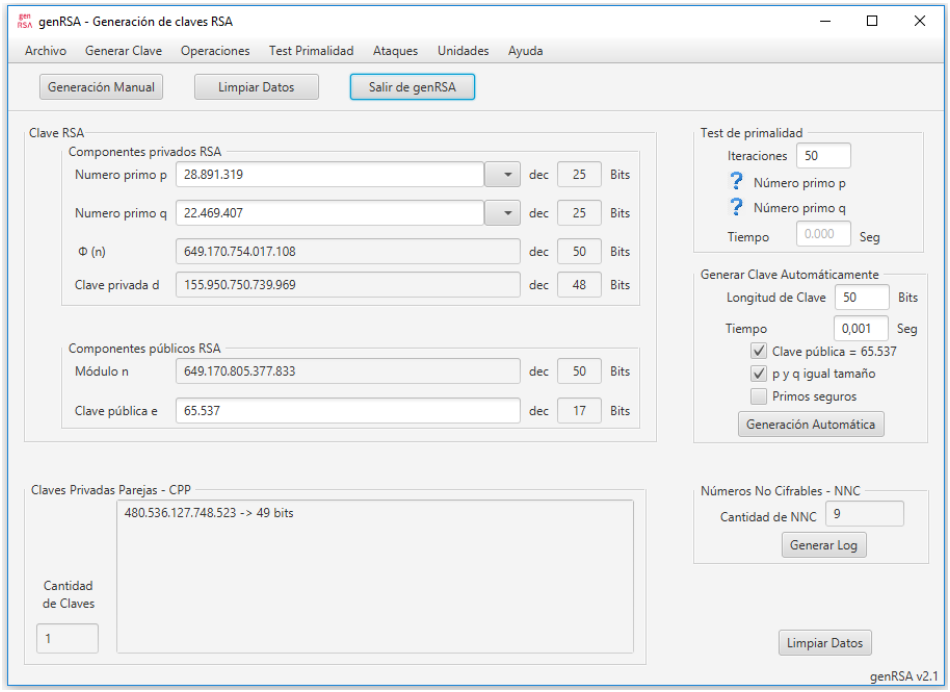
$$126^{5} \bmod 133 = 84$$

$84^{53} \bmod 133 = 126$ (lógicamente $84^{d} \bmod 133 = 126$ para d = 65, 11, 29,…)

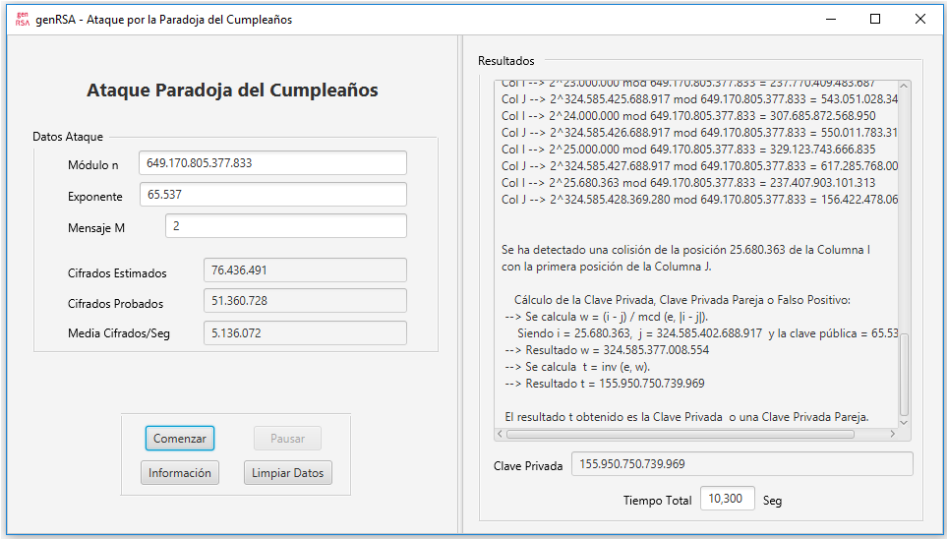
III. Ataque por paradoja del cumpleaños a claves RSA mayores

Ejercicio 3)

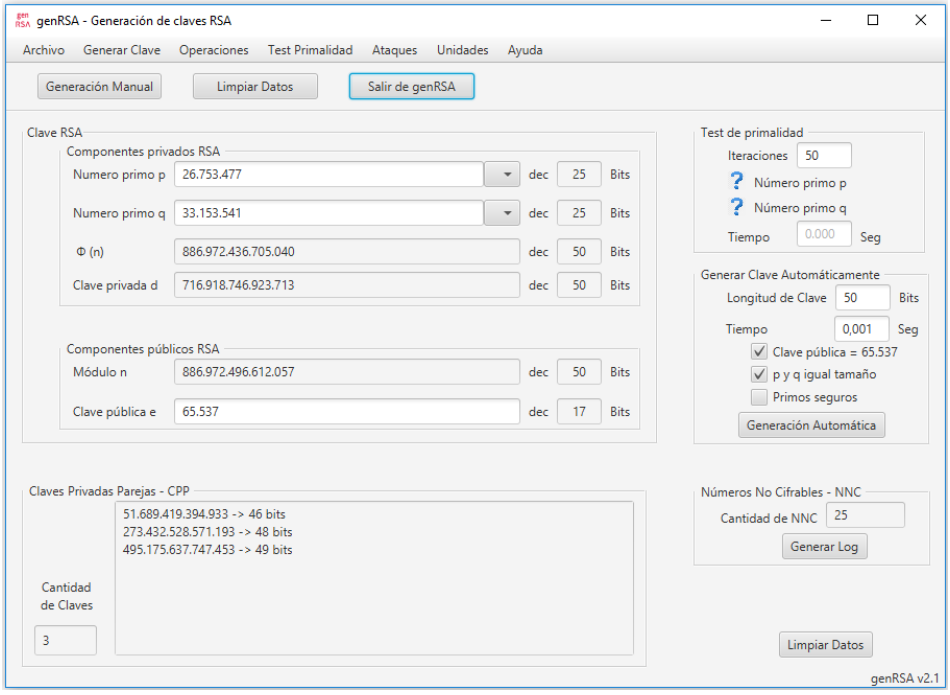
3.1. Con genRSA v2.1 genera de forma Automática claves decimales de 50 bits, con p y q de igual tamaño y clave pública = 65.537. Una de ellas deberá sucumbir ante un ataque por la paradoja del cumpleaños con M = 2 encontrando la clave privada, y la otra con el mismo valor M = 2 encuentre una clave privada pareja.



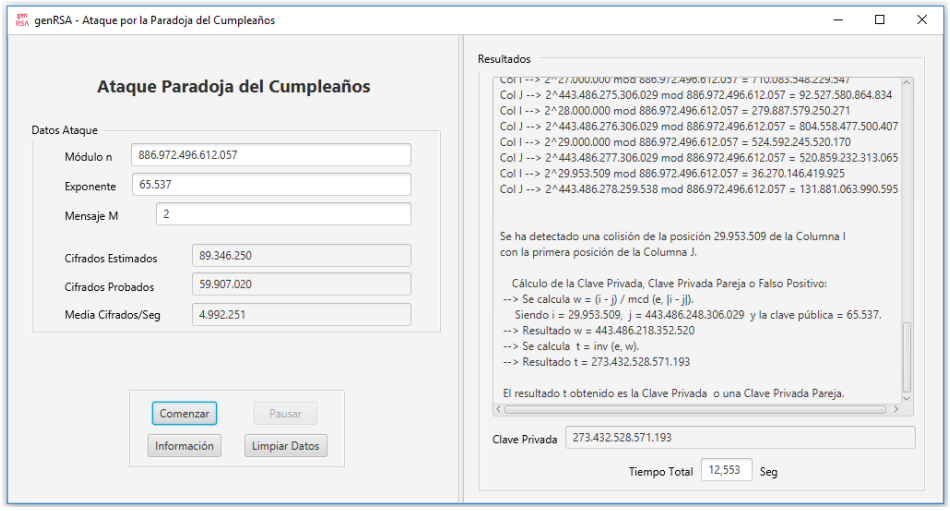
Primera clave de 50 bits del apartado 3.1



Ataque con M = 2 que encuentra la clave privada 155.950.750.739.969.

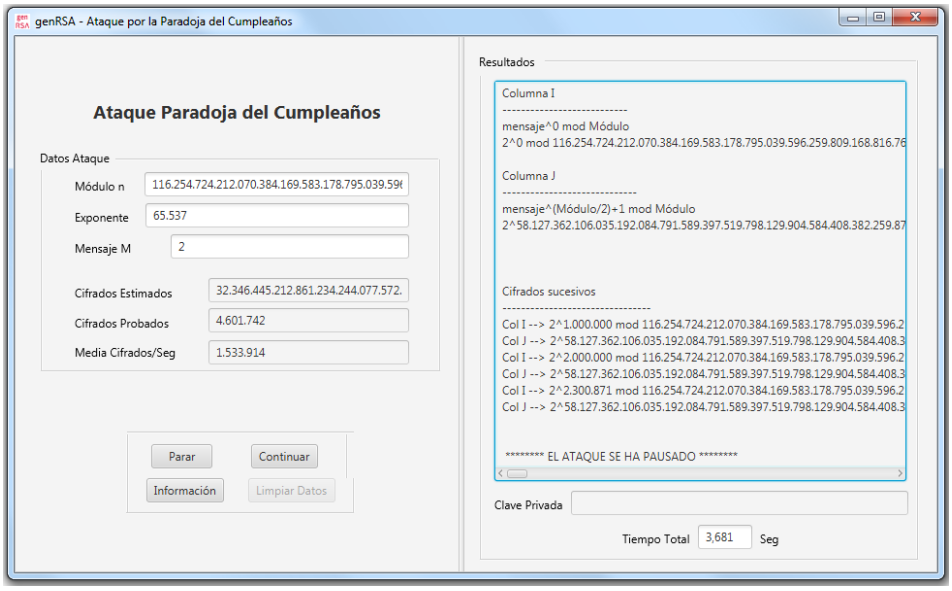


Segunda clave de 50 bits del apartado 3.1



Ataque con M = 2 que encuentra la clave privada pareja 273.432.528.571.193.

Nota: Observa que la tasa de cifra en genRSA v2.1 para claves de tamaño pequeño se encuentra en los 5 millones de cifrados por segundo. Para claves de 2.048 bits, esta tasa baja hasta 1,5 millones de cifrados por segundo.



Ataque por paradoja del cumpleaños a una clave de 1.024 bits, en pausa.

Nota: En una segunda práctica de ataque a RSA mediante la paradoja del cumpleaños, usando ahora el software LegionRSA y que se publicará próximamente, alcanzaremos una tasa de cifra en torno a los 100 millones de cifrados por segundo por cada uno de los procesadores que tenga nuestro PC y permitirá, además, hacer un ataque distribuido en red (divide y vencerás) con un servidor y n clientes.