

## Proyecto CLCript

Cuadernos de Laboratorio de Criptografía. Entrega nº 14. Última actualización 16/05/19

Autor: Dr. Jorge Ramío Aguirre (@criptored)

### Práctica sobre curiosidades y falsos positivos en ataques por paradoja del cumpleaños a RSA

- Software genRSA v2.1: [https://www.criptored.es/software/sw\\_m001d.htm](https://www.criptored.es/software/sw_m001d.htm)
- Software SAMCrypt: [https://www.criptored.es/software/sw\\_m001t.htm](https://www.criptored.es/software/sw_m001t.htm)

#### Objetivos:

1. Observar la existencia de falsos positivos en los ataques por paradoja de cumpleaños en RSA y comprobar lo que significan.
2. Observar y comprobar que los falsos positivos en un ataque por la paradoja del cumpleaños a RSA tienden a ubicarse en torno a las inmediaciones de los números no cifrables NNC, y que las colisiones producidas en el ataque parecen mostrar un comportamiento peculiar.

#### I. Clave privada y falsos positivos en ataques por la paradoja del cumpleaños

##### Ejercicio 1

- 1.1. Con genRSA, ataca por paradoja del cumpleaños (Ataques -> Paradoja del Cumpleaños) esta clave RSA de 32 bits, usando como Mensaje  $M = 172$  y comprueba que se obtiene el número 19.161.665, que veremos más adelante será un falso positivo.  
Datos públicos Clave1:  $n = 2.934.102.643$ ,  $e = 65.537$ .
- 1.2. Observa que colisiona el primer resultado de la columna  $i$  (valor 1) con un resultado posterior de la columna  $j$ .
- 1.3. Comprueba con SAMCrypt que se cumplen las ecuaciones de ataque:  
 $w = (i - j) / \text{mcd}(e, |i - j|)$        $t = \text{inv}(e, w)$       donde  $t$  es la clave buscada
- 1.4. Con SAMCrypt factoriza el módulo  $n = 2.934.102.643 = p \cdot q =$
- 1.5. Ahora con los primos  $p$  y  $q$ , genera la clave y comprueba que 19.161.665 no es ni la clave privada  $d$  ni una clave privada pareja.
- 1.6. Comprueba con SAMCrypt que la clave encontrada 19.161.665, un falso positivo, que sólo sirve para descifrar el criptograma que da origen la cifra del mensaje usado en el ataque, en este caso  $M = 172$ , y no otros. Comprueba que ese criptograma se descifra también -como es lógico- con la clave privada  $d$  o con cualquier clave privada pareja.
- 1.7. Si hacemos ataques por la paradoja del cumpleaños a esta clave RSA con  $1 < M < 300$ , podemos comprobar que siempre se obtiene la clave privada  $d = 239.511.473$ , excepto cuando  $M = 172$  que aparece el falso positivo 19.161.665. Por ejemplo ataca con  $M = 50$ ,  $M = 100$ ,  $M = 150$ ,  $M = 200$  y  $M = 250$ . ¿Qué conclusión puedes sacar de esto?
- 1.8. Observa que ahora colisiona el primer resultado de la columna  $j$  (valor 1.075.491.957) con un resultado posterior de la columna  $i$ . Puedes comprobar, si lo deseas, que todas las colisiones que entregan la clave privada (un ataque con final exitoso), se producen por la colisión entre un resultado de la columna  $i$  y el primer resultado de la columna  $j$ .
- 1.9. Haz un ataque por paradoja del cumpleaños a esta clave, tomando como valores de entrada  $M = 55.447.904$  y  $M = 55.447.905$ , los dos primeros números no cifrables NNC después del 0 y el 1. ¿Qué ha pasado con el ataque?
- 1.10. Encuentra todos los NCC de esta clave generando el log correspondiente.
- 1.11. Hecho esto, observa esta curiosidad: excepto para los valores 0 y 1, los falsos positivos aparecen en las inmediaciones de los NNC, por ejemplo NNC-2, NNC-1, NNC+1, NNC+2.
- 1.12. Observa además que cuando se obtiene un falso positivo en el ataque por paradoja del cumpleaños, las colisiones pueden producirse ahora entre un resultado de la columna  $j$  con el primer resultado de la columna  $i$ , que es el valor 1.

## Comprueba tu trabajo:

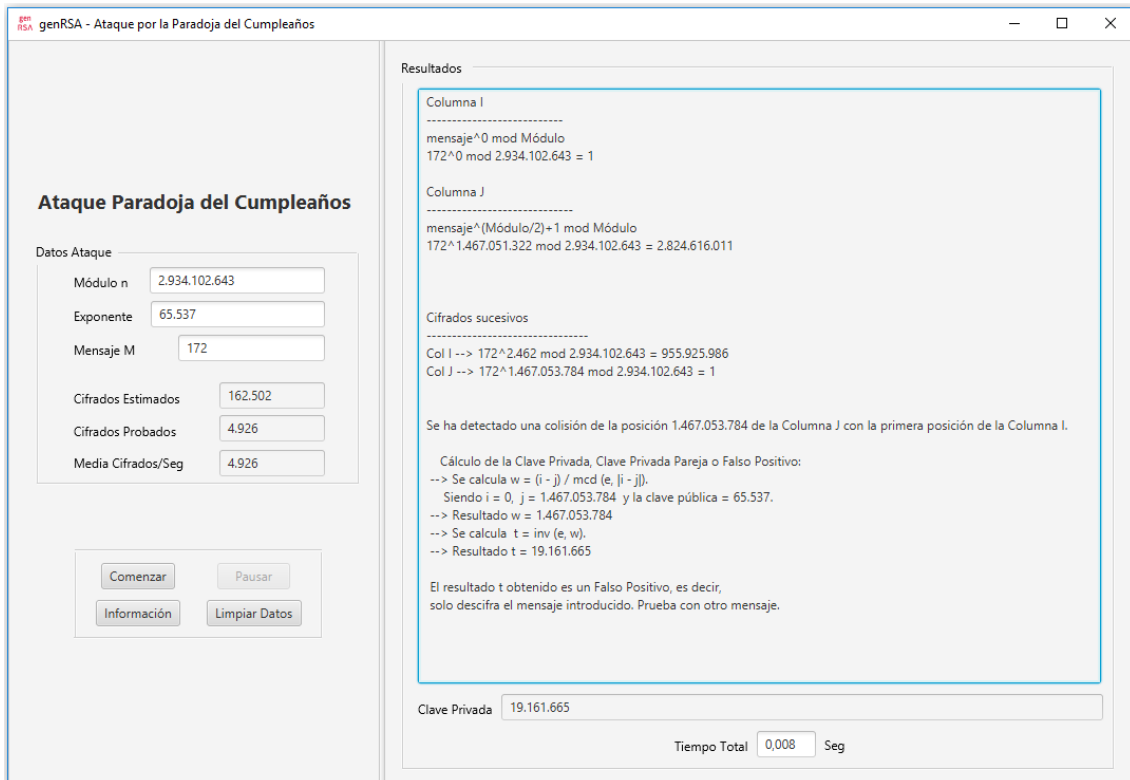


Figura 1. Ataque a la Clave1 con M = 172 que entrega la clave 19.161.665, un falso positivo.

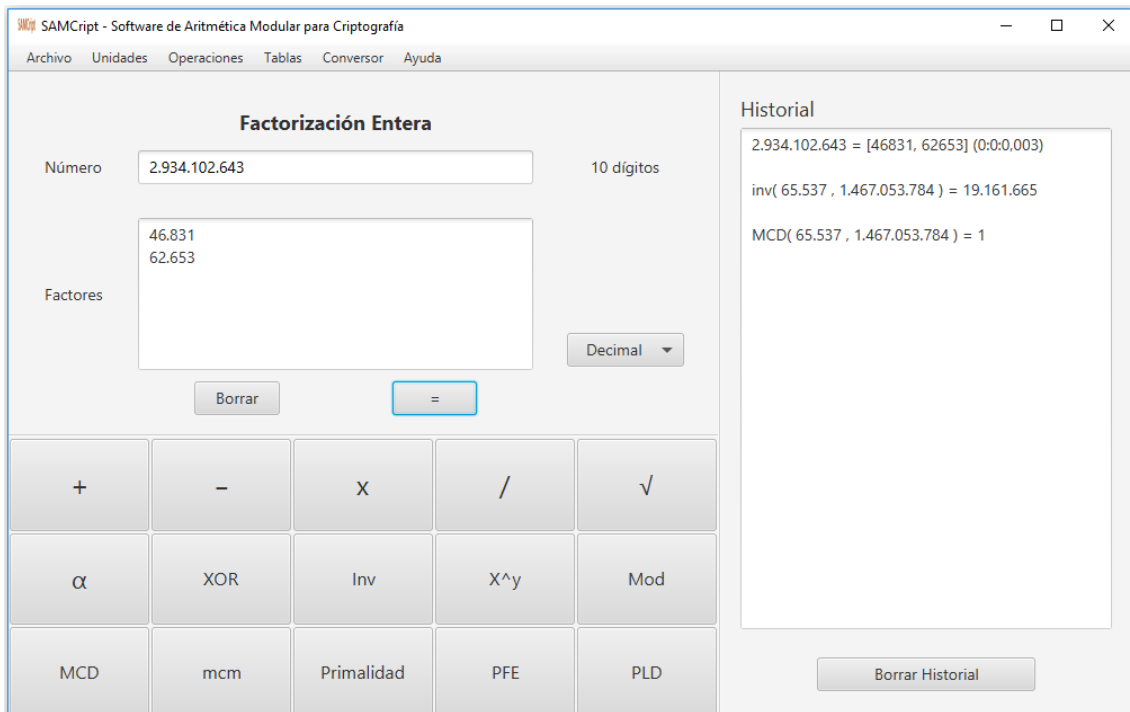


Figura 2. Valores de la ecuación en resultado paradoja del cumpleaños y factorización del módulo n (p = 46.831, q = 62.653).

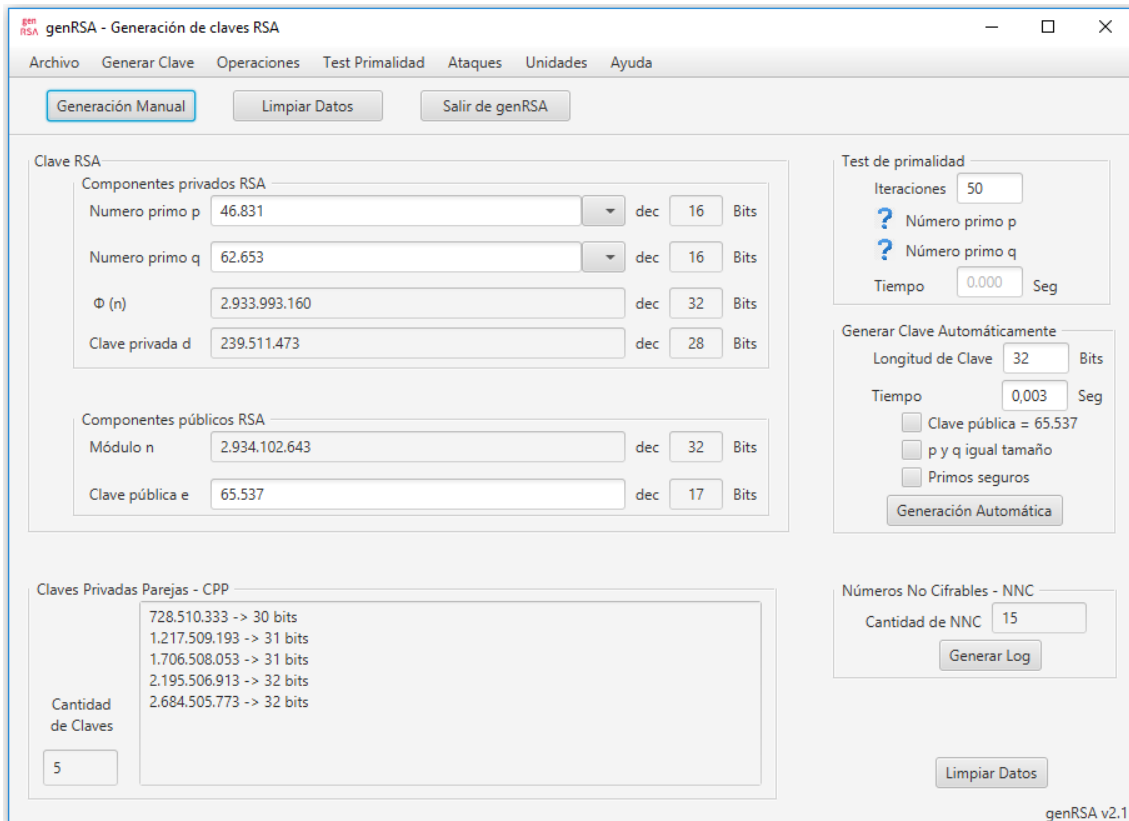


Figura 3. Generación de la Clave1, en que 19.161.665 no es la clave privada d, ni tampoco ninguna de las 5 claves privadas parejas.

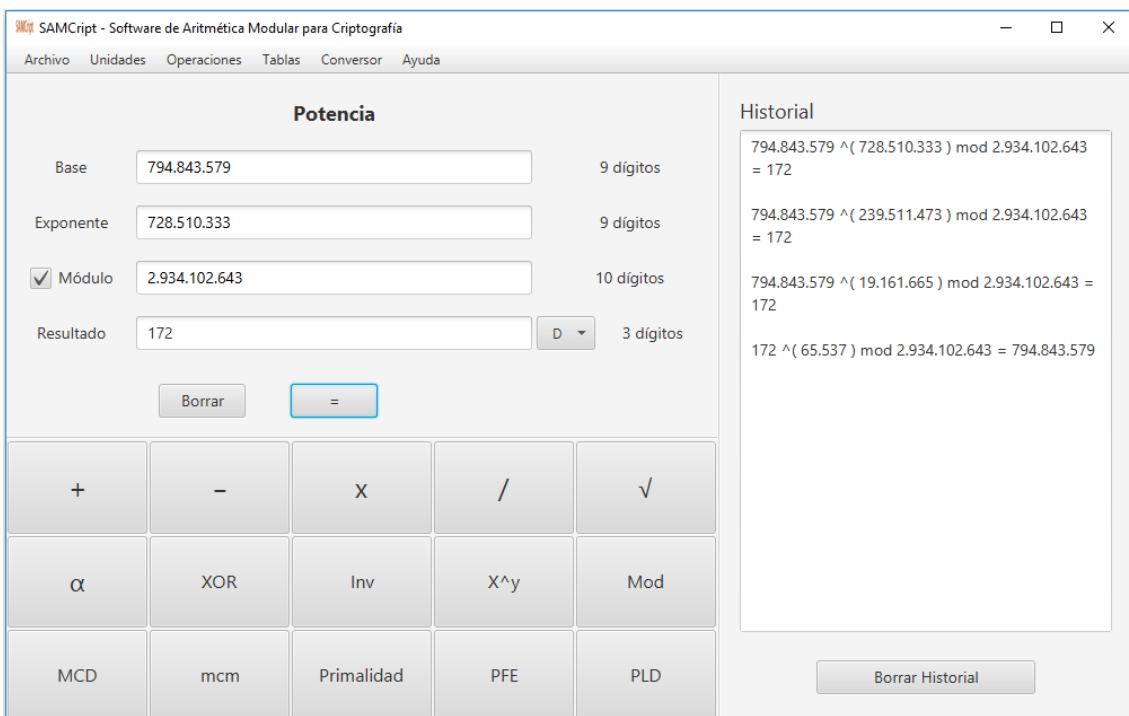


Figura 4. Comprobación que la cifra del número 172 (794.843.579) se descifra con el falso positivo 19.161.665, como también se descifra con la clave privada (239.511.473) y con la primera clave privada pareja (728.510.333).

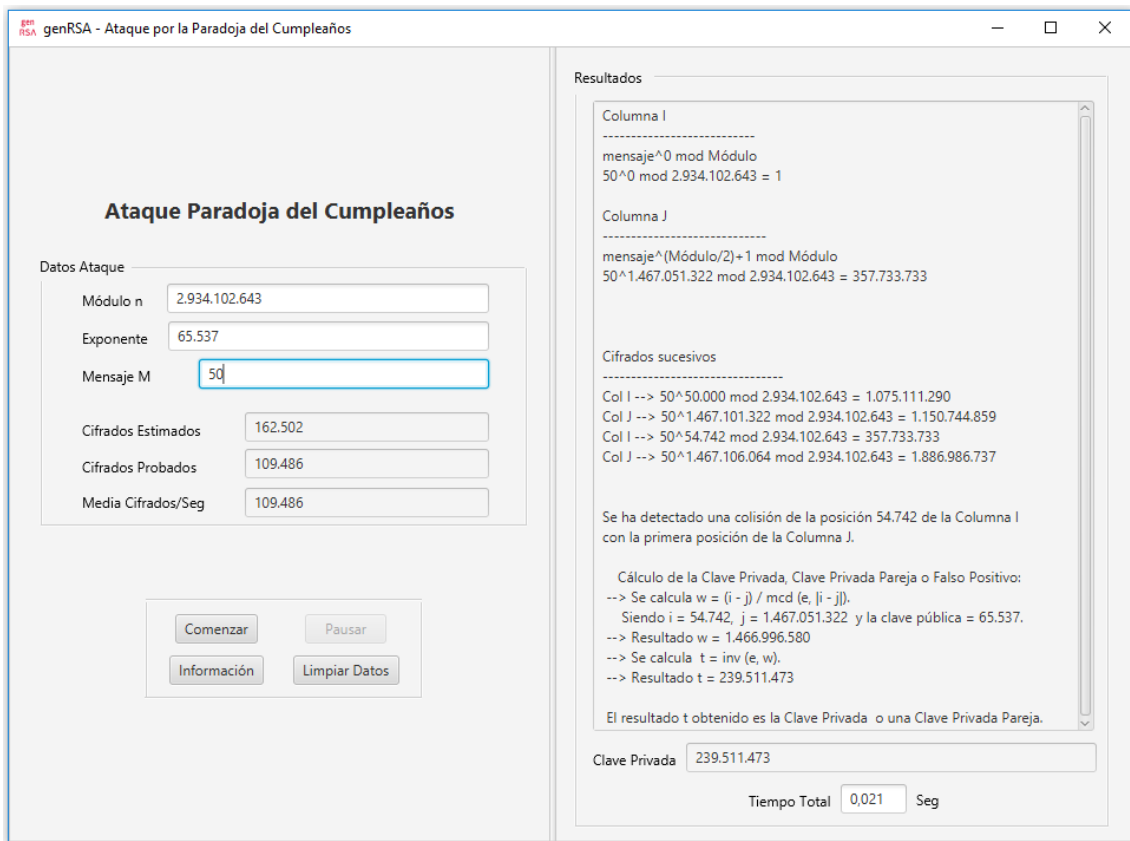


Figura 4. Ataque por la paradoja del cumpleaños con M = 50

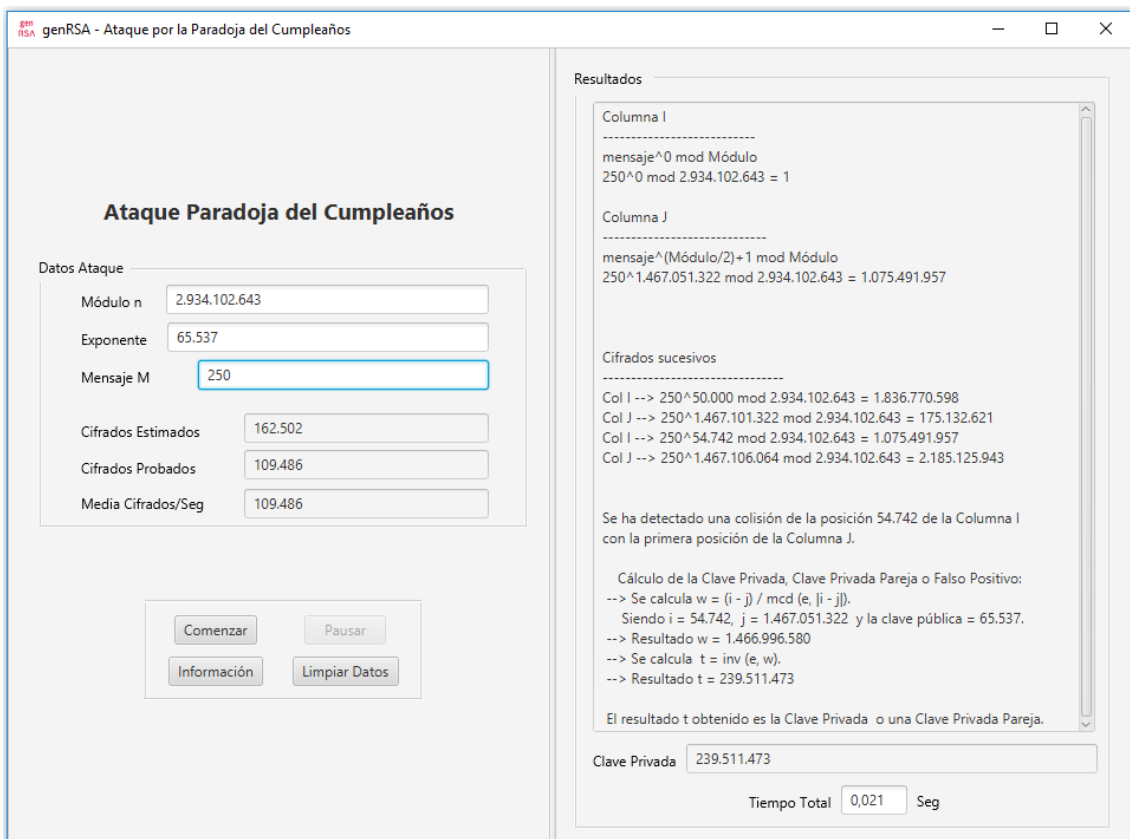


Figura 5. Ataque por la paradoja del cumpleaños con M = 250

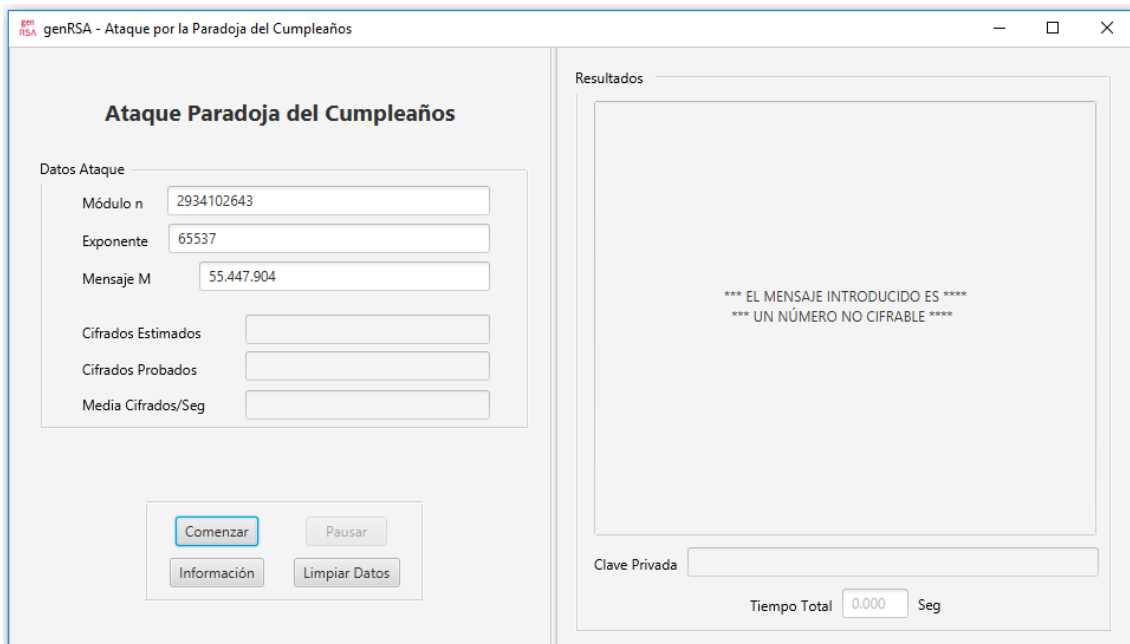


Figura 6. Ataque por la paradoja del cumpleaños con  $M = 55.447.904$ , un número no cifrable.

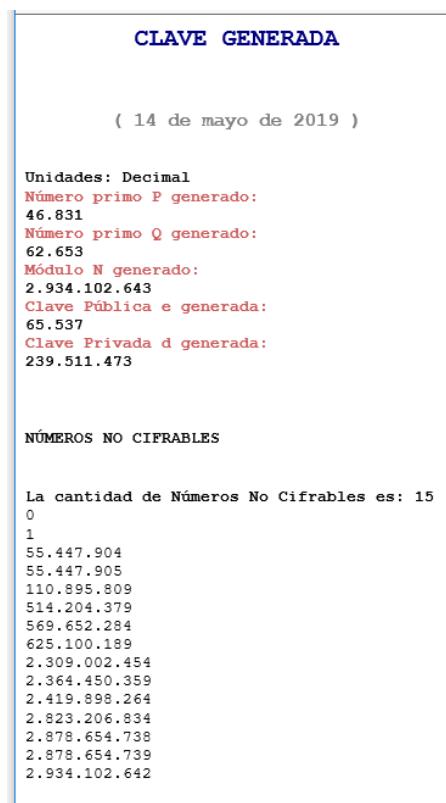


Figura 7. Los 15 números no cifrables de la clave.

Para NNC = 55.447.904, con M = 55.447.903 (-1) obtenemos 510.919.937, un FP
Para NNC = 55.447.905, con M = 55.447.906 (+1) obtenemos 1.068.238.568, un FP
Para NNC = 110.895.809, con M = 110.895.807 (-2) obtenemos 510.919.937, un FP
Para NNC = 110.895.809, con M = 110.895.810 (+1) obtenemos 1.068.238.568, un FP
Para NNC = 110.895.809, con M = 110.895.811 (+2) obtenemos 953.107.013, un FP
Para NNC = 514.204.379, con M = 514.204.381 (+2) obtenemos 510.919.937, un FP
Para NNC = 569.652.284, con M = 569.652.283 (-1) obtenemos 510.919.937, un FP
Para NNC = 569.652.284, con M = 569.652.285 (+1) obtenemos 510.919.937, un FP
Para NNC = 2.309.002.454, con M = 2.309.002.455 (+1) obtenemos 85.622.498, un FP
Para NNC = 2.309.002.454, con M = 2.309.002.456 (+2) obtenemos 510.919.937, un FP
Para NNC = 2.364.450.359, con M = 2.364.450.358 (-1) obtenemos 510.919.937, un FP
Para NNC = 2.364.450.359, con M = 2.364.450.360 (+1) obtenemos 85.622.498, un FP
Para NNC = 2.419.898.264, con M = 2.419.898.262 (+2) obtenemos 510.919.937, un FP
Para NNC = 2.823.206.834, con M = 2.823.206.833 (-1) obtenemos 953.107.013, un FP
Para NNC = 2.823.206.834, con M = 2.823.206.832 (-2) obtenemos 953.107.013, un FP
Para NNC = 2.823.206.834, con M = 2.823.206.836 (+2) obtenemos 85.622.498, un FP

Figura 8. Ejemplos de falsos positivos en ataques por paradoja del cumpleaños para valores de M en las inmediaciones de un NNC de Clave1 (n = \*\*, e = 65.537).

**Ataque Paradoja del Cumpleaños**

Datos Ataque

Módulo n: 2.934.102.643  
Exponente: 65.537  
Mensaje M: 55.447.903

Cifrados Estimados: 162.502  
Cifrados Probados: 15.822  
Media Cifrados/Seg: 15.822

Comenzar Pausar  
Información Limpiar Datos

**Resultados**

Columna I  
-----  
mensaje<sup>0</sup> mod Módulo  
55.447.903<sup>0</sup> mod 2.934.102.643 = 1

Columna J  
-----  
mensaje<sup>(Módulo/2)+1</sup> mod Módulo  
55.447.903<sup>1.467.051.322</sup> mod 2.934.102.643 = 1.492.082.492

Cifrados sucesivos  
-----  
Col I --> 55.447.903<sup>7.910</sup> mod 2.934.102.643 = 1.917.214.310  
Col J --> 55.447.903<sup>1.467.059.232</sup> mod 2.934.102.643 = 1

Se ha detectado una colisión de la posición 1.467.059.232 de la Columna J con la primera posición de la Columna I.

Cálculo de la Clave Privada, Clave Privada Pareja o Falso Positivo:  
--> Se calcula w = (i - j) / mcd(e, |i - j|).  
Siendo i = 0, j = 1.467.059.232 y la clave pública = 65.537.  
--> Resultado w = 1.467.059.232  
--> Se calcula t = inv(e, w).  
--> Resultado t = 510.919.937

El resultado t obtenido es un Falso Positivo, es decir, solo descifra el mensaje introducido. Prueba con otro mensaje.

Clave Privada: 510.919.937

Tiempo Total: 0,005 Seg

Figura 9. Comprobando que las colisiones por falsos positivos pueden producirse entre el primer resultado de la columna i (valor 1) y un resultado de la columna j.

## II. Claves privadas parejas y falsos positivos en ataques por la paradoja del cumpleaños

### Ejercicio 2

- 2.1. Con genRSA realiza un ataque por paradoja del cumpleaños a la clave RSA de 40 bits que se indica siendo  $M = 2$ . Datos públicos Clave2:  $n = 549.876.895.021$  y  $e = 65.537$ .
- 2.2. Comprueba que en la vuelta  $i = 767.465$  la cifra de la columna  $i$  colisiona con el primer valor de la columna  $j$ , entregando como resultado del ataque el valor  $113.365.593.907$ .
- 2.3. Con SAMCrypt, cifra  $N = 123.456$  con esta clave RSA ( $e = 65.537$ ;  $n = 549.876.895.021$ ) y comprueba que el criptograma  $C$  lo descifras con  $113.365.593.907$ .
- 2.4. Con SAMCrypt factoriza  $n = 549.876.895.021 = p * q$  y luego genera con genRSA la clave Clave2. Comprueba que  $113.365.593.907$  es la clave privada pareja  $d'$ .
- 2.5. Comprueba que desde  $M = 2$  hasta  $M = 10$  el ataque por la paradoja del cumpleaños siempre devuelve la clave privada pareja  $d' = 113.365.593.907$ .
- 2.6. Con genRSA encuentra los 9 números no cifrables NNC y realiza ataques por paradoja del cumpleaños con los valores NNC-2, NNC-1, NNC+1 y NNC+2 de estos números (excepto el 0 y el 1). Comprueba que en muchos casos se obtiene un falso positivo FP y que la colisión puede ser entre un resultado de  $j$  con el primer resultado de  $i$ , que es 1.

### Comprueba tu trabajo:

**Ataque Paradoja del Cumpleaños**

Datos Ataque

Módulo n: 549.876.895.021  
Exponente: 65.537  
Mensaje M: 2

Cifrados Estimados: 2.224.610  
Cifrados Probados: 1.534.932  
Media Cifrados/Seg: 1.534.932

Comenzar Pausar  
Información Limpiar Datos

**Resultados**

Columna I  
-----  
mensaje<sup>0</sup> mod Módulo  
2<sup>0</sup> mod 549.876.895.021 = 1

Columna J  
-----  
mensaje<sup>^(Módulo/2)+1</sup> mod Módulo  
2<sup>274.938.447.511</sup> mod 549.876.895.021 = 112.702.169.096

Cifrados sucesivos  
-----  
Col I --> 2<sup>100.000</sup> mod 549.876.895.021 = 268.497.021.317  
Col J --> 2<sup>274.938.547.511</sup> mod 549.876.895.021 = 468.337.400.477  
Col I --> 2<sup>200.000</sup> mod 549.876.895.021 = 31.172.967.110  
Col J --> 2<sup>274.938.647.511</sup> mod 549.876.895.021 = 350.365.822.937  
Col I --> 2<sup>300.000</sup> mod 549.876.895.021 = 173.359.692.390  
Col J --> 2<sup>274.938.747.511</sup> mod 549.876.895.021 = 315.373.333.672  
Col I --> 2<sup>400.000</sup> mod 549.876.895.021 = 368.767.540.615  
Col J --> 2<sup>274.938.847.511</sup> mod 549.876.895.021 = 515.176.406.714  
Col I --> 2<sup>500.000</sup> mod 549.876.895.021 = 187.114.110.350  
Col J --> 2<sup>274.938.947.511</sup> mod 549.876.895.021 = 438.877.767.038  
Col I --> 2<sup>600.000</sup> mod 549.876.895.021 = 144.716.998.015  
Col J --> 2<sup>274.939.047.511</sup> mod 549.876.895.021 = 535.032.072.534  
Col I --> 2<sup>700.000</sup> mod 549.876.895.021 = 468.953.014.682  
Col J --> 2<sup>274.939.147.511</sup> mod 549.876.895.021 = 91.608.493.092  
Col I --> 2<sup>767.465</sup> mod 549.876.895.021 = 112.702.169.096  
Col J --> 2<sup>274.939.214.976</sup> mod 549.876.895.021 = 276.746.988.592

Se ha detectado una colisión de la posición 767.465 de la Columna I con la primera posición de la Columna J.

Cálculo de la Clave Privada, Clave Privada Pareja o Falso Positivo:  
--> Se calcula  $w = (i - j) / \text{mcd}(e, |i - j|)$ .  
Siendo  $i = 767.465$ ,  $j = 274.938.447.511$  y la clave pública = 65.537.  
--> Resultado  $w = 274.937.680.046$   
--> Se calcula  $t = \text{inv}(e, w)$ .  
--> Resultado  $t = 113.365.593.907$

El resultado  $t$  obtenido es la Clave Privada o una Clave Privada Pareja.

Clave Privada: 113.365.593.907

Tiempo Total: 0,335 Seg

Figura 10. Ataque a la Clave2 con  $M = 2$  que entrega la clave 19.161.665.

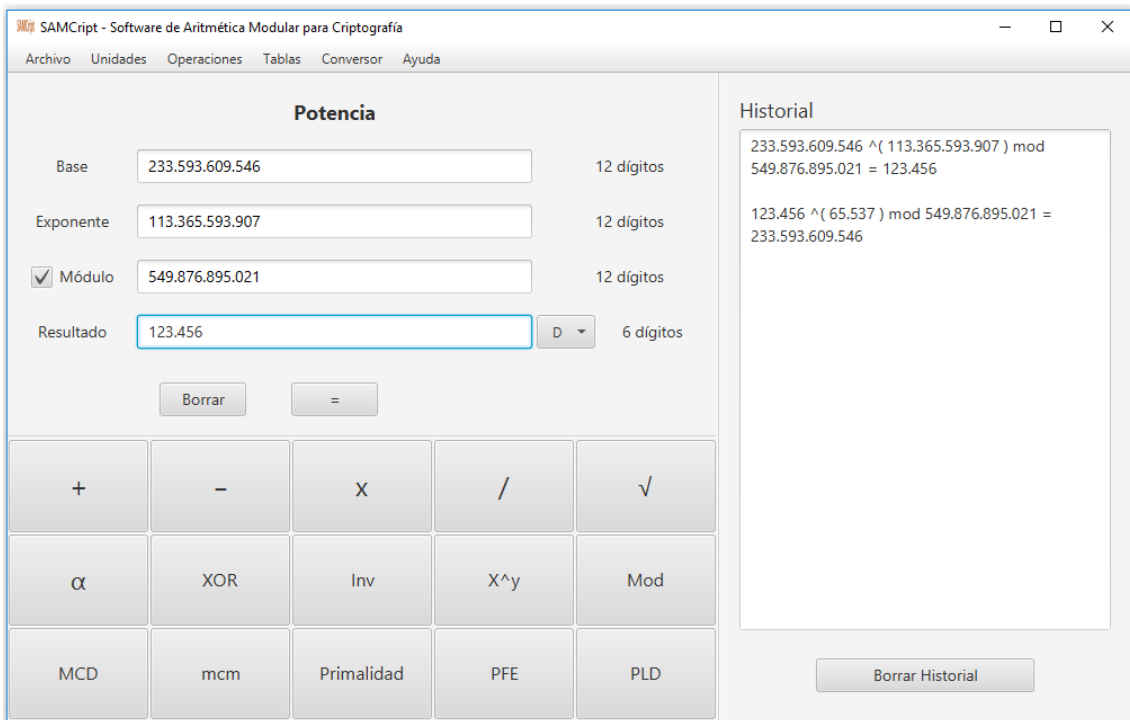


Figura 11. La clave 19.161.665 descifra el criptograma 233.593.609.546.

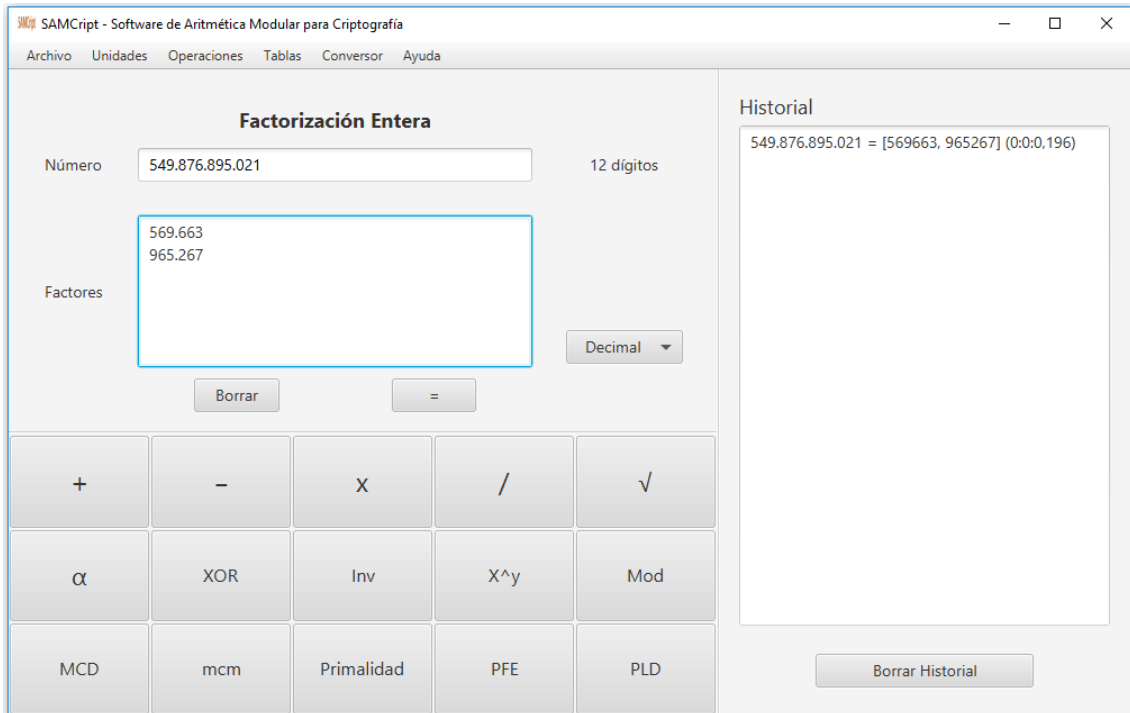


Figura 12. Factorización de  $549.876.895.021 = 569.663 * 965.267$ .



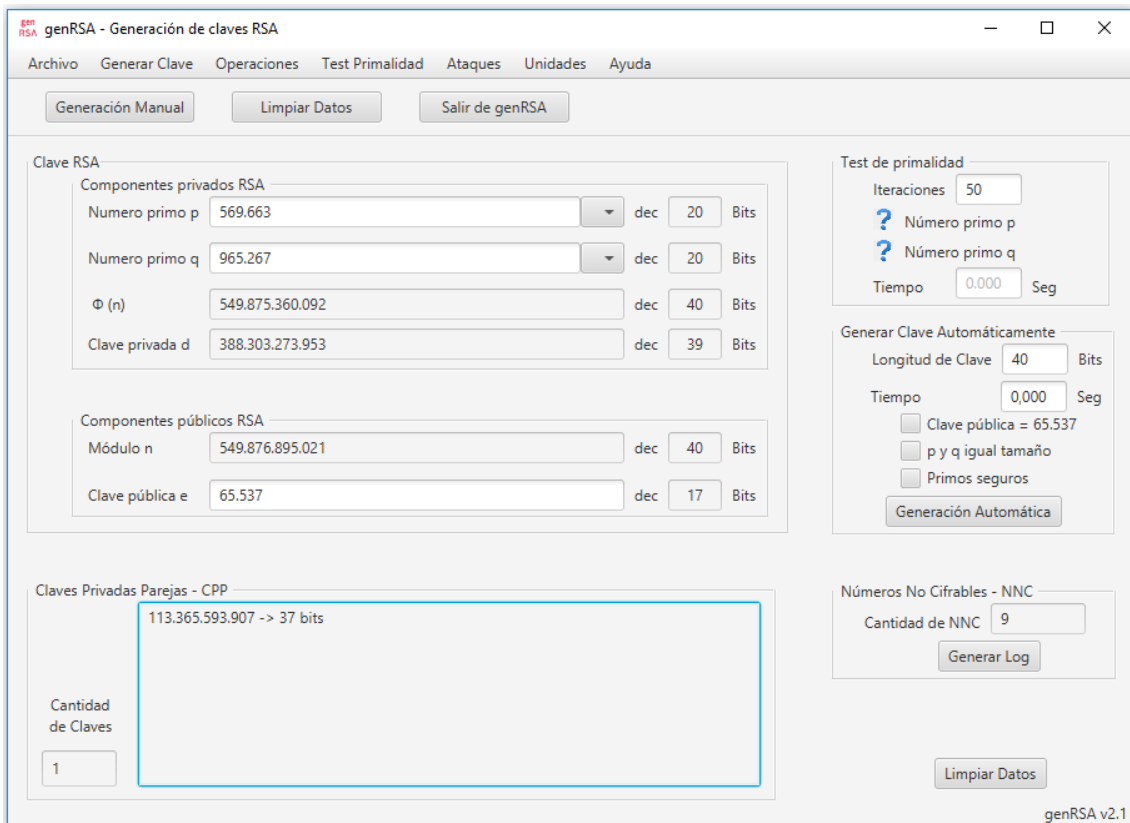


Figura 13. Generación de la Clave2, en la que 113.365.593.907 es su única clave privada pareja.

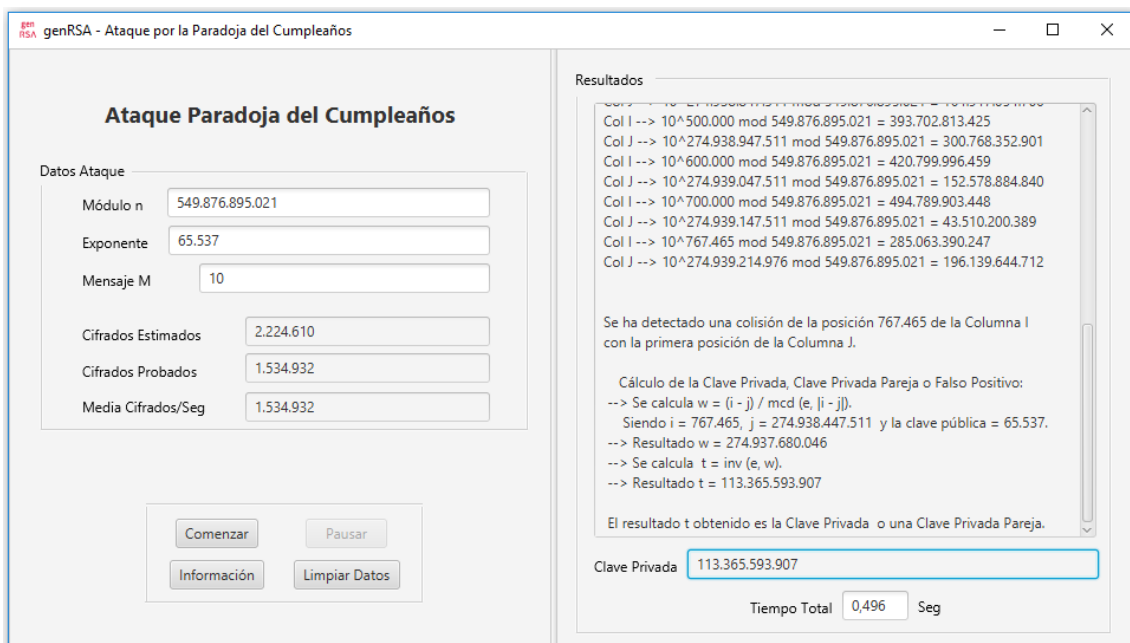


Figura 14. Ataque con  $M = 10$  con resultado  $d' = 113.365.593.907$ .

**CLAVE GENERADA**

( 14 de mayo de 2019 )

Unidades: Decimal  
**Número primo P generado:**  
569.663  
**Número primo Q generado:**  
965.267  
**Módulo N generado:**  
549.876.895.021  
**Clave Pública e generada:**  
65.537  
**Clave Privada d generada:**  
388.303.273.953

**NÚMEROS NO CIFRABLES**

La cantidad de Números No Cifrables es: 9  
0  
1  
3.253.915.056  
3.253.915.057  
6.507.830.113  
543.369.064.908  
546.622.979.964  
546.622.979.965  
549.876.895.020

Figura 15. Números no cifrables de la Clave2.

NNC = 3.253.915.056: con M = 3.253.915.055 (-1) obtenemos 27.633.563.585, FP
NNC = 3.253.915.057: con M = 3.253.915.058 (+1) obtenemos 258.212.411.323, FP
NNC = 6.507.830.113: con M = 6.507.830.114 (+1) obtenemos 172.425.301.757, FP
NNC = 6.507.830.113: con M = 6.507.830.115 (+2) obtenemos 258.212.411.323, FP
NNC = 543.369.064.908: con M = 543.369.064.906 (-2) obtenemos 172.425.301.757, FP
NNC = 543.369.064.908: con M = 543.369.064.907 (-1) obtenemos 172.425.301.757, FP
NNC = 543.369.064.908: con M = 543.369.064.910 (+2) obtenemos 27.633.563.585, FP
NNC = 546.622.979.964: con M = 546.622.979.963 (-1) obtenemos 172.425.301.757, FP
NNC = 546.622.979.965: con M = 546.622.979.966 (+1) obtenemos 27.633.563.585, FP

Figura 15. Ejemplos de falsos positivos en ataques por paradoja del cumpleaños para valores de M en las intermediaciones de un NNC de Clave2.

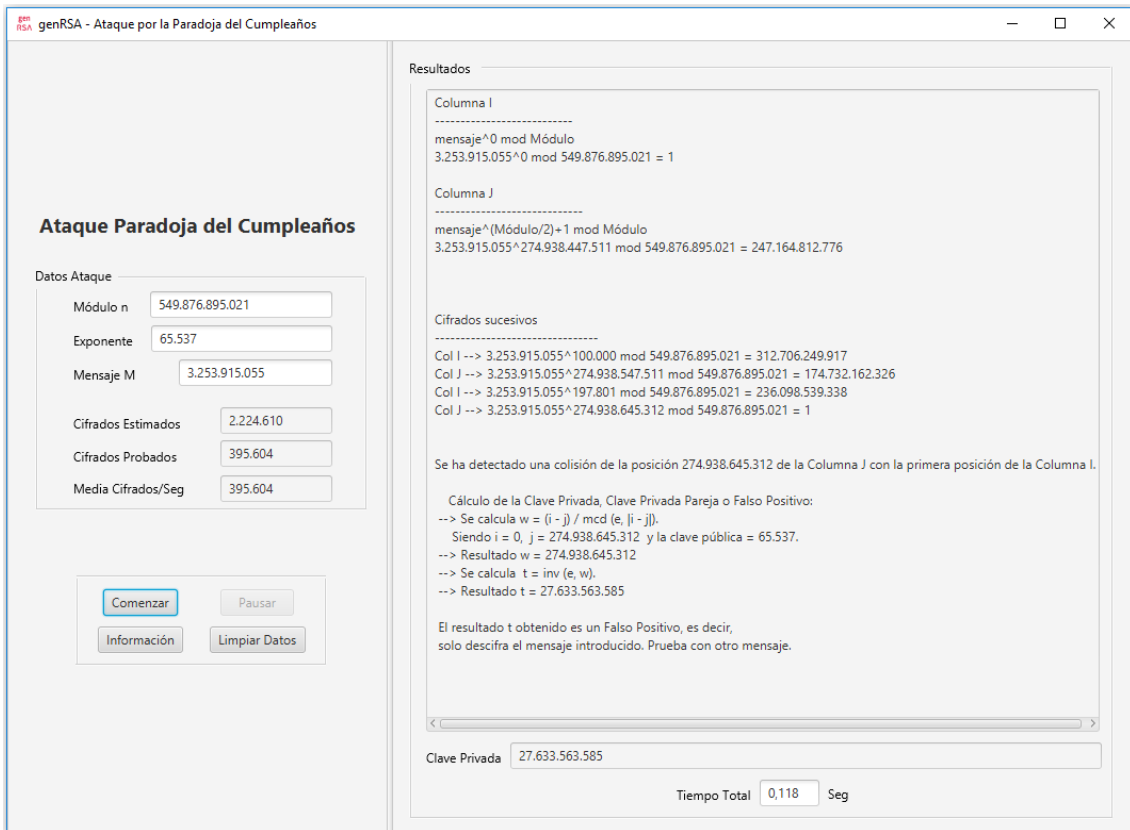


Figura 16. Colisión entre valor de la columna j y el primer valor de la columna i (1)

**Nota y curiosidad:**

Parece ser que lo común que la colisión que entrega un resultado positivo del ataque por la paradoja del cumpleaños, es decir que encuentra la clave privada o una clave privada pareja, se produzca entre una cifra de la columna i con la primera cifra de la columna j. Al menos para una gran cantidad de casos se ha podido comprobar que así sucede, sin poder determinar a qué puede deberse. No obstante, cuando se obtiene un falso positivo, se observa que en muchas ocasiones la colisión se produce entre el primer valor de la columna i (cuyo resultado es siempre 1 dado que  $i = 0$ ) y un resultado de la columna j. Algo digno de estudio...

Sin embargo, sí hay ejemplos de colisiones al revés (resultado de j que colisiona con primer valor de i) y que entregan resultados positivos. Por ejemplo, puede comprobar que:

- Con  $p = 41$ ,  $q = 61$ ,  $e = 7$ , si  $M = 2$  se obtiene una CPP y la colisión se da en  $i=0$ ,  $j=1.260$ .
- Con  $p = 37$ ,  $q = 73$ ,  $e = 5$ , si  $M = 2$  se obtiene una CPP y la colisión se da en  $i=0$ ,  $j=1.368$ .

**III. Incidencia de la clave pública en el resultado del ataque por la paradoja del cumpleaños**  
**Ejercicio 3**

- 3.1. Con genRSA genera la Clave3 de 32 bits Clave3:  $p = 51.287$ ,  $q = 64.763$ ,  $e = 3$ .
- 3.2. Realiza un ataque por paradoja del cumpleaños a la Clave3 con los valores  $1 < M < 11$ .
- 3.3. Comprueba que en todos los ataques se obtiene siempre  $d' = 553.563.989$ , la única clave privada pareja, y que la colisión se produce siempre entre el primer valor de la columna j ( $j = 1.660.749.991$ ) y un valor de la columna i ( $i = 58.025$ ).

## Comprueba tu trabajo:

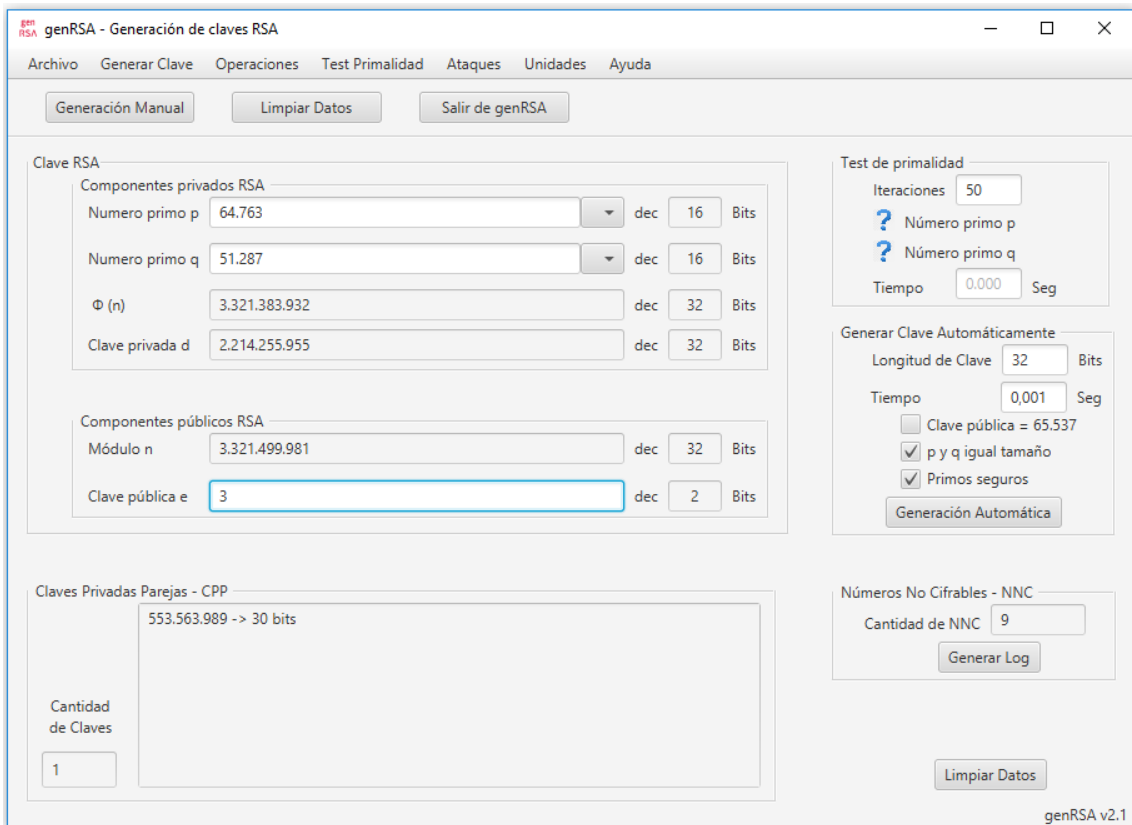


Figura 17. Clave3.

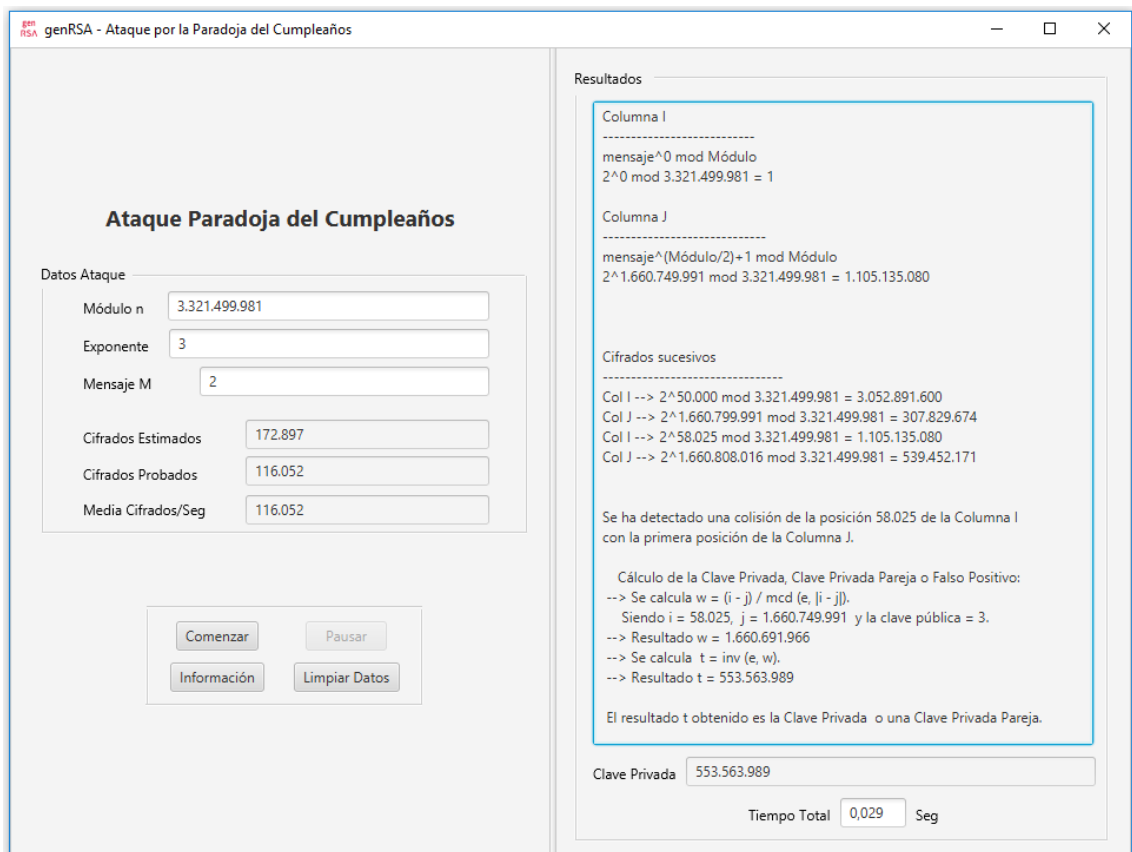


Figura 18. Ataque por paradoja del cumpleaños a Clave3 para M = 2.

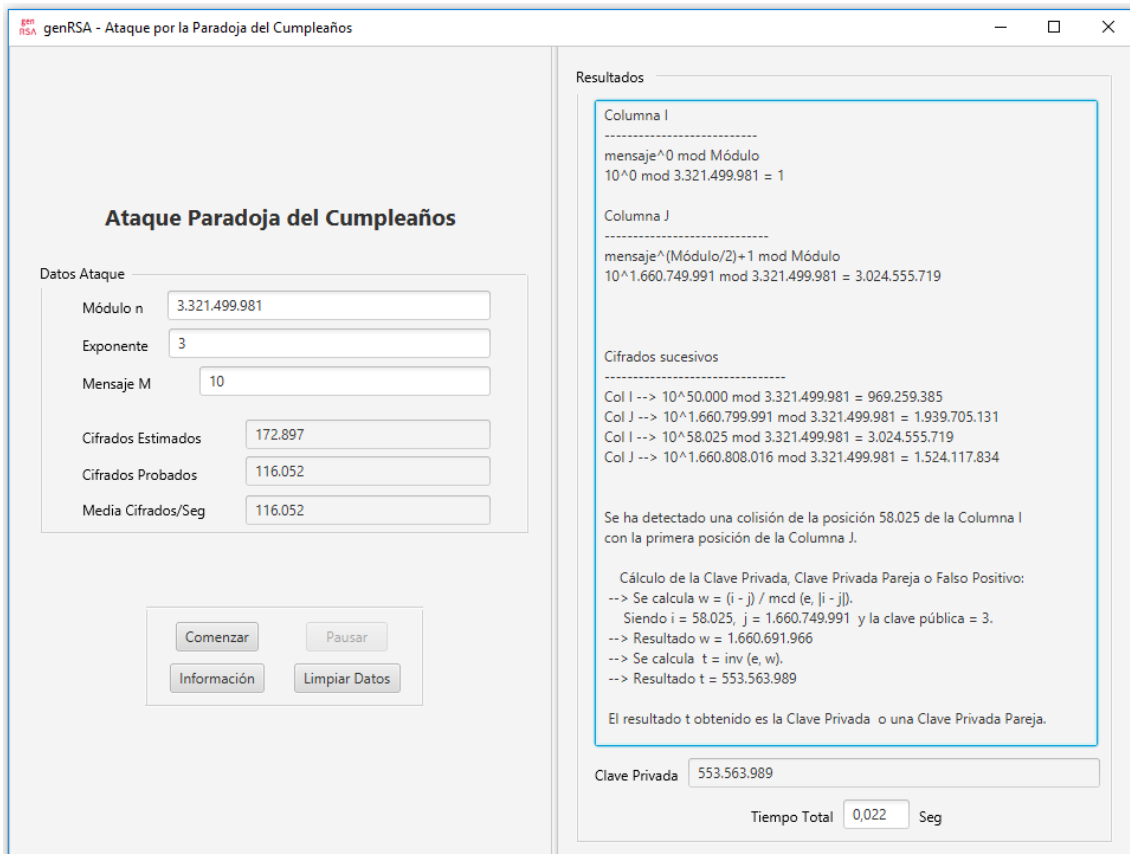


Figura 19. Ataque por paradoja del cumpleaños a Clave3 para M = 10.

#### Ejercicio 4

- 4.1. Con genRSA genera la Clave4 de 32 bits Clave3:  $p = 51.287$ ,  $q = 64.763$ ,  $e = 5$ .
- 4.2. Realiza un ataque por paradoja del cumpleaños a la Clave4 con los valores  $1 < M < 11$ .
- 4.3. Comprueba que en todos los ataques se obtiene siempre  $d = 1.328.553.573$ , la clave privada, y que nuevamente la colisión se produce siempre entre el primer valor de la columna j ( $j = 1.660.749.991$ ) y un valor de la columna i ( $i = 58.025$ ), los mismos valores del caso anterior.

#### Comprueba tu trabajo:

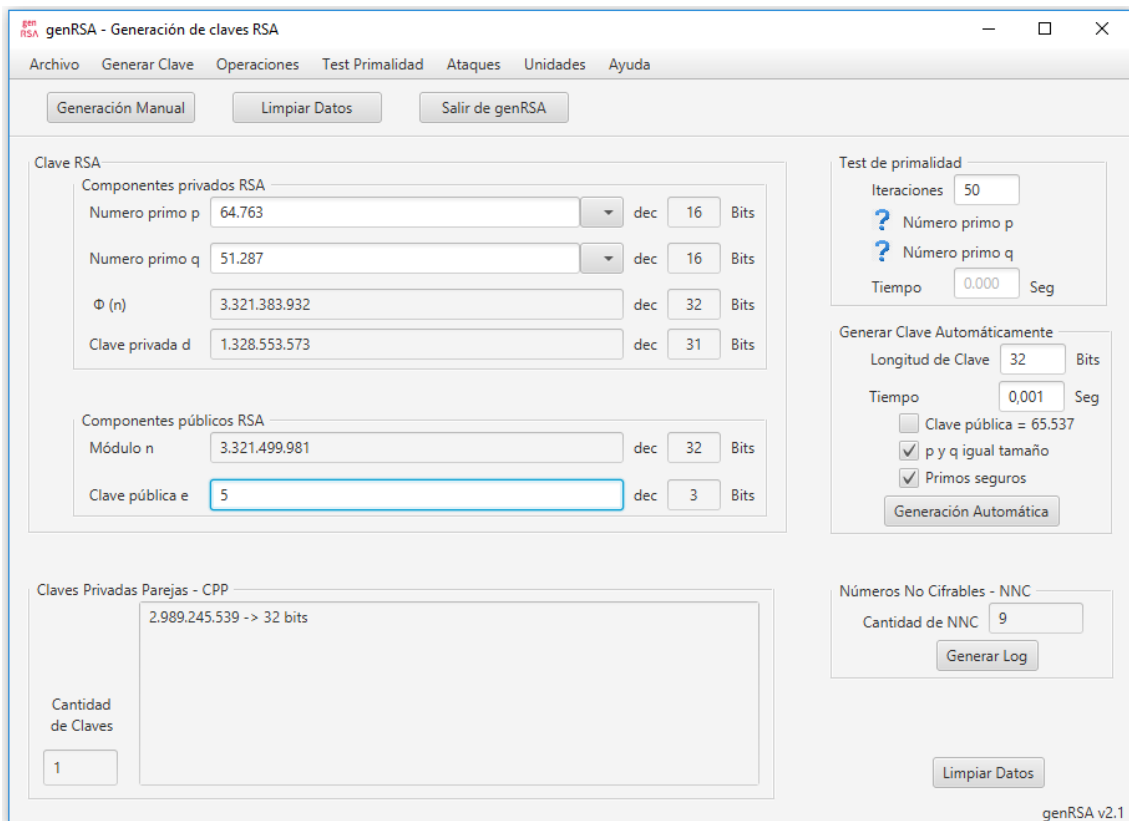


Figura 20. Clave4.

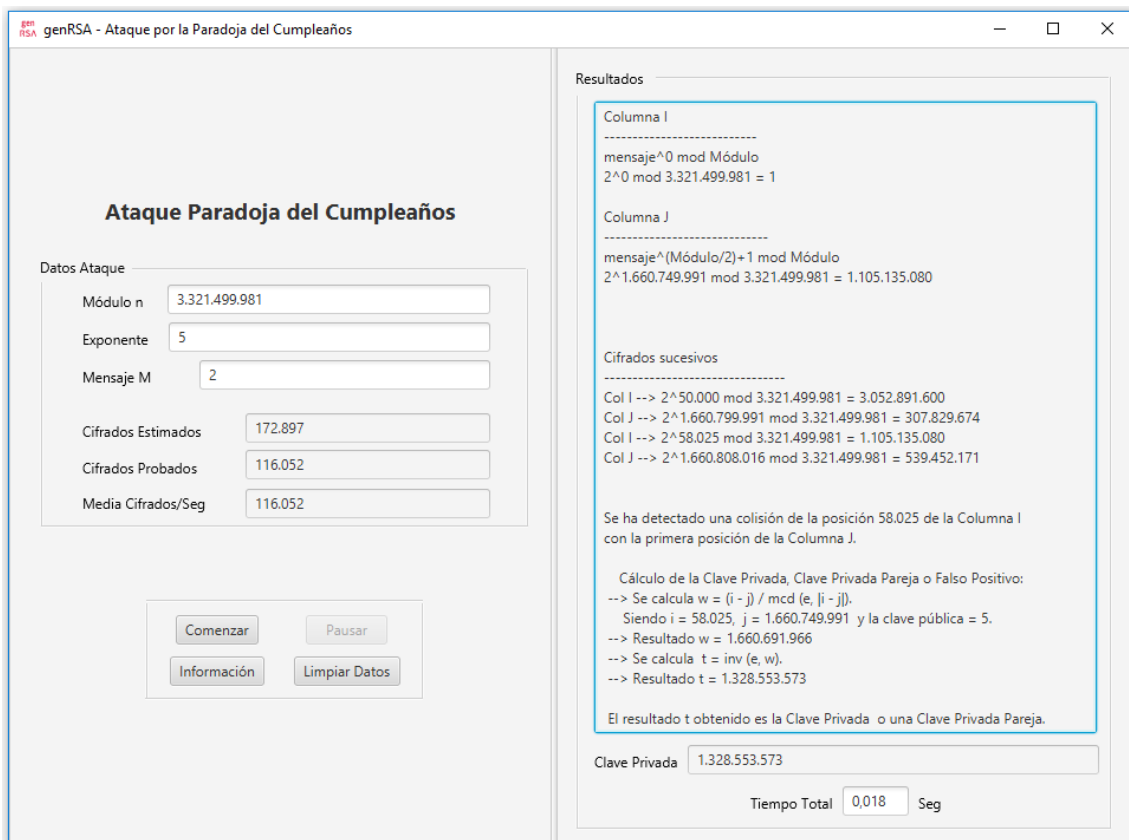


Figura 21. Ataque por paradoja del cumpleaños a Clave4 para M = 2.

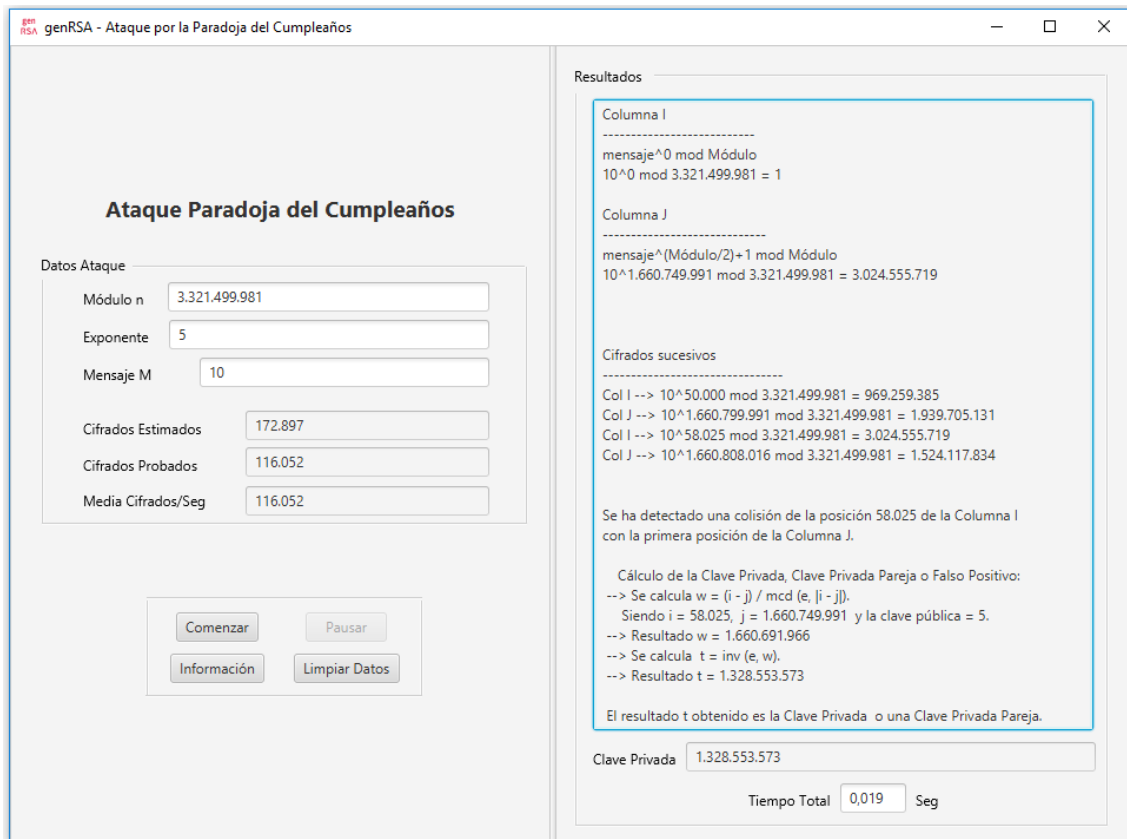


Figura 22. Ataque por paradoja del cumpleaños a Clave4 para M = 10.

Madrid, 16 de mayo de 2019  
 Dr. Jorge Ramió Aguirre