Aportes para el estudio de anillos en ataques cíclicos al criptosistema RSA

Juan Pedro Hecht, *Universidad de Buenos Aires,* Jorge Ramió Aguirre, Abel Casado,
Universidad Politécnica de Madrid

***Resumen*—Se aporta un análisis teórico sobre un software desarrollado para analizar experimentalmente los anillos o ciclos de recifrado en el algoritmo RSA. La idea es predecir analíticamente las longitudes de anillos observadas y en casos particulares predecir la frecuencia de aparición de las distintas longitudes cuando se aplica el método a los mensajes $m \in Z_n$. También se discuten consideraciones vinculadas a la potencial factorización del módulo y la obtención de la clave privada a partir de la clave pública.**

***Palabras clave*—Aritmética modular *(modular arithmetics)*, ataque cíclico *(cycle attack)*, campos finitos *(finite fields)*, criptografía de clave pública *(public key cryptography)*, criptosistema RSA *(RSA cryptosystem)*, grupos cíclicos *(cyclic groups)*, generadores congruenciales modulares *(modular congruential generators)*, teoría de números *(number theory)*.**

I. Nomenclatura

Adoptamos la siguiente nomenclatura:

p, **q** primos
n = **pq** módulo del cifrado RSA
φ(n) = **(p-1)(q-1)** función indicador de Euler
λ(n) = **φ(n)/(p-1, q-1)** =**[p-1, q-1]**
donde **λ()** es la función de Carmichael
e coprimo con **λ(n)**
exponente público de cifrado RSA
d exponente privado de cifrado RSA
donde **ed** ≡ **1** mod **λ (n)**
m (entero, (**0** ≤ **m** ≤ **n-1**) mensaje a cifrar
c (cifrado) = $\mathbf{m^e}$ (mod **n**)
k longitud de anillo o período de ciclo
$\mathbf{Z_n}$ enteros módulo n
$\mathbf{Z_n^*}$ enteros módulo n coprimos con n
a|**b** a divide a b
(a, b) máximo común divisor de a y b
[a,b] mínimo común múltiplo de a y b
{**A**}conjunto A
|**A**|cardinal u orden del conjunto A
$<g>$ grupo cíclico generado por g
$\mathbf{ord_m}\,(\mathbf{e})$ orden multiplicativo de e módulo m

II. Introducción

Fruto de la investigación realizada durante los últimos meses de 2013 e inicio de 2014 en el Proyecto Fin de Grado de título "Software para el estudio del comportamiento de los ataques por cifrado cíclico en RSA" [1] en la Escuela Técnica Superior de Ingeniería de Sistemas Informáticos de la Universidad Politécnica de Madrid, su director presenta en [2] unos primeros resultados sobre la generación de anillos que se producen en dicho ataque, utilizando el software educacional RingRSA desarrollado en el proyecto que será próximamente de dominio público, planteándose un interesante tema algebraico vinculado a dos aplicaciones criptográficas; a saber, el orden de los generadores congruenciales modulares (ver Blum-Blum-Shub [3]) y el ataque cíclico al criptosistema RSA [3, 4, 5, 6, 7, 8, 9, 10, 11, 12, 13]. Ambos han sido estudiados de manera extensa a lo largo de los años; basta consultar la bibliografía citada en las referencias arriba indicadas.

Para el caso del ataque a RSA, está demostrado que este método de cifrado cíclico permite descifrar un criptograma que cuenta con confidencialidad, es decir un mensaje secreto que se ha cifrado con la clave pública de destino, contando para ello solamente con los datos públicos de la clave en cuestión de la víctima, esto es los valores n y e. En teoría, permite además quebrar el criptosistema ya que brinda un método para obtener la clave privada d a partir de la clave pública e a través de la factorización del módulo [3, 4]. El objetivo del presente trabajo es:

a. Computar analíticamente las posibles longitudes de los anillos generados por el programa RingRSA.

b. Para determinados casos, calcular analíticamente las frecuencias de aparición de las distintas longitudes de los anillos generados por el programa RingRSA.

Como se demuestra más adelante, ambos objetivos se cumplen satisfactoriamente.

III. Planteamiento del problema

El problema central consiste en computar sucesivamente cifrados iterados (mod n) hasta completar un ciclo u órbita del exponente.

$$m^e,\ m^{e^2},\ m^{e^3},...,\ m^{e^k} \equiv m\ \ (mod\ n)$$

$$m\ \in Z_n\ y\ \ (e, \lambda\,(n)) = 1$$

Dado que las referencias a las ecuaciones serán siempre locales, éstas no se enumerarán.

La existencia de k está asegurada [3, 9, 12]; existe un exponente de cifrado para el cual se recupera el mensaje m, exactamente una iteración previa al volver al cifrado original c [3].

Queda claro que los sucesivos exponentes de recifrado forman un grupo multiplicativo cíclico cuyo generador es el exponente e:

$$< e > \ : \left\{e^1,\ e^2,\ e^3,\ e^4, ..., e^k \equiv 1\right\}\ \ mod\ \lambda\,(n)$$

ISBN: 978-84-9717-323-0

$$k = ord_{\lambda(n)}(e)$$

Donde k es el orden multiplicativo de e módulo $\lambda(n)$. El máximo valor de k, la cota superior de recifrados necesarios para recuperar el mensaje, está dada por:

$$\left|Z^*_{\lambda(n)}\right| = max(k) \;=\; \lambda(\lambda(n))$$

Los posibles valores de k son divisores de max (k) [12]:

$$k \mid \lambda(\lambda(n))$$

ya que los órdenes de los subgrupos son divisores del orden de un grupo [10].

IV. Distribución estadística de valores $Z^*_{\lambda(n)}$

Para el estudio de la distribución estadística, se buscan primos p, q al azar y sin estructura.

Sabemos que los posibles valores de k son divisores de $\lambda(\lambda(n))$. Se puede estudiar su distribución analítica o estadísticamente según cómo se elijan los valores de los primos p, q.

Desde el punto de vista estadístico, si se define r el mayor factor primo del indicador (y de lambda) de uno de los primos, digamos p, entonces r es un divisor de p-1. Acorde a lo demostrado en [9] respecto a la factorización típica y el mayor factor primo, r tendrá un tamaño cercano al 63 % del tamaño de p-1. O sea para n de 1.024 bits, r será del orden de 322 bits (el 63 % de 512 bits). Según [4] esto implica que:

1. *Si se elige al azar un e cuyo k es múltiplo de r, la longitud del ciclo será al menos de tamaño r, lo que hace inviable el ataque cíclico.*
2. *La probabilidad de elegir al azar un e con un orden multiplicativo que no sea múltiplo de r es 1/r, lo que resulta despreciable (para n de 1024 bits p˜10^{-322}). La deducción de esta consecuencia puede obtenerse de la discusión planteada en [4].*
3. *Debe quedar en claro que lo antedicho es válido para todo valor e.*

En conclusión, la inmensa mayoría de pares de los valores (m,e,p) elegidos para el ataque cíclico resultan ser extremadamente costosos en tiempo [4]. Obviamente, los ensayos computacionales con RingRSA así lo ilustran. Dado que el generador congruencial modular representa un generador pseudoaleatorio de calidad criptográfica [3] y que no parece haber regularidad en la distribución de divisores de $\lambda(n)$, no tiene sentido buscar una función de densidad de probabilidades a priori cuando los primos se eligen al azar y son desconocidos [7]. Sin embargo, para ciertos valores especiales de primos p, q es posible dar una respuesta. Para dar sustento analítico a lo antedicho, en el siguiente apartado se deduce que es posible obtener la función de densidad de longitudes de anillos si se conoce la factorización del módulo n en sus primos componentes.

V. Distribución analítica de longitudes de ciclos en $Z^*_{\lambda(n)}$

Formalizando el análisis de los generadores congruenciales modulares, se parte de

$$m_y \equiv {m_{y-1}}^e \,(mod\ n) \qquad 0 \le m_y \le n-1$$

$$y = 1, 2, 3, ...$$

Donde m_0 el valor inicial debe ser coprimo con n y el exponente $e \ge 2$. Se demuestra [6] que si $(e,\ \lambda(n)) = 1$ la secuencia resulta periódica pura (sin fase aperiódica inicial) con período k, entonces

$$k = ord_x(e) \;\; donde\ x = ord_n(m_0)$$

Evidentemente esta última relación [6] permite calcular, para cada m_0 coprimo con n y cada e coprimo con $\lambda(n)$, la longitud del período multiplicativo o longitud del anillo, con lo cual se cumple uno de los objetivos del trabajo. Obviamente cada resultado obtenido con RingRSA así lo verifica.

De aquí en adelante consideramos que m y e se ajustan a las condiciones que generan secuencias periódicas puras. Para estudiar la distribución analítica, se buscan primos p, q con estructura especial.

Sea n = pq donde p, q son primos de Sophie Germain. Entonces p = 2r+1 y q = 2s+1 donde r, s son primos, que si también fuesen de Sophie Germain, r = 2t+1 y s = 2u+1 donde t, u son primos. Ambos conjuntos de primos (t, r, p) y (u, s, q) constituyen cadenas de Cunningham de primera especie.

Los órdenes multiplicativos posibles de los integrantes del grupo multiplicativo Z*$_n$ de cifrados RSA [9, 10] son los divisores de:

$$\lambda(n) = \frac{\varphi(n)}{MCD(p-1, q-1)} = \frac{(p-1)(q-1)}{2} = 2rs$$

De las propiedades bien conocidas de los grupos cíclicos (por ejemplo ver 2.172 y 2.173 de [3]) surge claramente que cada divisor d | 2rs define un único subgrupo cíclico de orden φ(d). Obviamente se cumple el conocido teorema [10]

$$\varphi(n) = \sum_{d|\varphi(n)} \varphi(d)$$

y el cardinal del grupo es:

$$|Z^*_n| = \varphi(n) = 4rs$$

Así resulta que φ(d) es la multiplicidad de veces con las cuales se presenta cada divisor d, o sea cuántos elementos tienen un orden determinado. A su vez, los órdenes multiplicativos de los integrantes del grupo multiplicativo $Z^*_{\lambda(n)}$ de exponentes de cifrados RSA [5, 6, 7, 8] son los divisores de:

$$\lambda(\lambda(n)) = [\lambda(2), \lambda(r), \lambda(s)] = [1, 2t, 2u] = 2tu$$

Y el cardinal del grupo en cuestión es [12]:

$$|Z^*_{\lambda(n)}| = \varphi(\lambda(n)) = \varphi(2)\,\varphi(r)\,\varphi(s) =$$

$$= 1\,(2t)\,(2u) = 4tu$$

También los exponentes forman un grupo multiplicativo cíclico, por lo tanto vale lo expresado antes (2.172 y 2.173 de [3]), por lo cual es evidente que cada divisor d $\mid \lambda(\lambda(n))$ define un único subgrupo cíclico de orden φ(d) y se cumple [10]:

$$\lambda(\lambda(n)) = \sum_{d|\lambda(\lambda(n))} \varphi(d)$$

Para $\lambda(n) = 2rs$, resulta:

$$c \in \ Z^*_{\lambda(n)},\ donde\ c \equiv a\ \ (mod\ r)\ \ y\ \ \ c \equiv b\ \ (mod\ s)$$

y se cumple la siguiente relación entre los órdenes de ciclos de potencias modulares:

$$ord\,(c,\ \lambda(n)) = [ord\,(a,\ r),\ ord\,(b,s)]$$

Y se generan los siguientes subgrupos de exponentes para Z^*_r y Z^*_s:

Cuadro I: SUBGRUPOS DE EXPONENTES PARA Z^*_r

Orden	Multiplicidad	Detalle
1	1	=$\varphi(1)$
2	1	=$\varphi(2)$
t	t-1	=$\varphi(t)$
2t	t-1	=$\varphi(2t)$
Suma	2t	=$\lvert Z^*_r \rvert$

Cuadro II: SUBGRUPOS DE EXPONENTES PARA Z^*_s

Orden	Multiplicidad	Detalle
1	1	=$\varphi(1)$
2	1	=$\varphi(2)$
u	u-1	=$\varphi(u)$
2u	u-1	=$\varphi(2u)$
Suma	2u	=$\lvert Z^*_s \rvert$

Cuando se computan las multiplicidades de los órdenes en $Z^*_{\lambda\ (n)}$ hay que considerar las combinaciones de órdenes de Z^*_r y Z^*_s .

Por ejemplo, para el orden 2 en $Z^*_{\lambda\ (n)}$ es necesario que la combinación de órdenes en Z^*_r y Z^*_s genere un mcm cuyo resultado sea 2. En este caso, hay tres combinaciones posibles con ese resultado : [1,2], [2,1] y [2,2]. La multiplicidad de 2 en $Z^*_{\lambda\ (n)}$ resulta en la suma de los productos de las multiplicidades de estas tres combinaciones:

$$Multiplicidad\ \left(orden\ 2\ \ en\ \ Z^*_{\lambda(n)}\right)$$

$$= \varphi(1)\,\varphi(2) + \varphi(2)\,\varphi(1) + \varphi(2)\,\varphi(2) = 3$$

Finalmente, los divisores de $\lambda(\lambda(n)) = 2tu$ resultan ser:

$$\{1,\ 2, t,\ u,\ 2t,\ 2u,\ tu,\ 2tu\}$$

y generan los siguientes subgrupos de exponentes que se presentan en la siguiente tabla.

Cuadro III: SUBGRUPOS DE EXPONENTES EN $Z^*_{\lambda(n)}$

Orden	Multiplicidad	Detalle
1	1	=$\varphi(1)\varphi(1)$
2	3	=$\varphi(1)\varphi(2) + \varphi(2)\varphi(1) + \varphi(2)\varphi(2)$
t	t-1	=$\varphi(t)$
u	u-1	=$\varphi(u)$
2t	3t-3	=$\varphi(2t)\varphi(1) + \varphi(t)\varphi(2) + \varphi(2t)\varphi(2)$
2u	3u-3	=$\varphi(1)\varphi(2u) + \varphi(2)\varphi(u) + \varphi(2)\varphi(2u)$
tu	tu-t-u+1	=$\varphi(t)\varphi(u)$
2tu	3tu-3t-3u+3	=$\varphi(2t)\varphi(u) + \varphi(t)\varphi(2u) + \varphi(2t)\varphi(2u)$
Suma	4tu	=$\lvert Z^*_{\lambda(n)} \rvert$

Disponiendo de esta tabla y su segunda columna, verdadero aporte de este trabajo al no existir antecedentes publicados, se posee la distribución estadística de las frecuencias de aparición de los ocho órdenes posibles, cualesquiera sean los primos t, u y el valor del mensaje m y exponente e al aplicar el ataque cíclico al RSA. A continuación se ilustra su aplicación a un ejemplo numérico sobre dos cadenas de Cunningham de primera especie.

VI. Ejemplo numérico de la distribución analítica de valores de longitudes de ciclos en $Z^*_{\lambda(n)}$

Adoptando los símbolos del apartado previo, sean:

t = 5, r = 11, p = 23 y u = 89, s = 179, q = 359 cadenas de primos Cunningham de primera especie. Así resulta:

n = pq = 8.257

$|Z^*_n| = \varphi(n) = (p-1)(q-1) = (2r)(2s) = 4rs = 7.876$

$\lambda(n) = \varphi(n)/2 = 2rs = 3.938$

$|Z^*_{\lambda(n)}| = \varphi(\lambda(n)) = \varphi(2rs) = \varphi(2)\varphi(r)\varphi(s)$
$= 1*2t*2u = 4tu = 1.780$

$\lambda(\lambda(n)) = [\lambda(2), \lambda(r), \lambda(s)] = [1, 2t, 2u] = 2tu = 890$
Divisores de λ (λ(n)) = {1, 2, t, u, 2t, 2u, tu, 2tu} = {1, 2, 5, 89, 10, 178, 445, 890]

Y se generan los siguientes ciclos de anillos:

Cuadro IV: SUBGRUPOS DE EXPONENTES EN $Z^*_{\lambda(n)}$

Orden	Multiplicidad	Detalle del cómputo
1	1	$=1$
2	3	$=3$
5	4	$=t-1$
89	88	$=u-1$
10	12	$=3t-3$
178	264	$=3u-3$
445	352	$=tu-t-u+1$
890	1056	$=3tu-3t-3u+3$
Suma	1780	$=\|Z^*_{\lambda(n)}\|$

Es menester aclarar que esta tabla emplea las mismas fórmulas deducidas para la tabla final del apartado previo. Cualquiera sea m^e (mod n), la longitud del ciclo de recifrado será un miembro de la lista de la primera columna. La función de densidad de longitudes se desprende de la segunda columna. Analizando dicha columna, se observa que la mayoría de longitudes de ciclo son relativamente grandes. Así de las ocho longitudes de ciclo disponibles para combinaciones de (m, e) tomadas al azar, el 60 % posee la máxima longitud posible.

En la figura 1 se genera esta clave con RingRSA eligiendo un exponente válido al azar.

Una vez generada la clave, puede comprobarse de manera experimental que las longitudes de los ciclos de recifrado son miembros divisores de $\lambda(\lambda(n))$, que están reflejados en la lista de la primera columna.

Este exponente, al igual que cualquier otro, genera su órbita de valores divisores. En la Figura 2 se ven que están presentes los valores de la primera columna {1, 10, 89, 890}; pero no los valores {2, 5, 178, 445}.

Por ejemplo si ahora elegimos e=31, se generan anillos de longitudes {1, 5, 89, 445} como se nuestra en la figura 3.

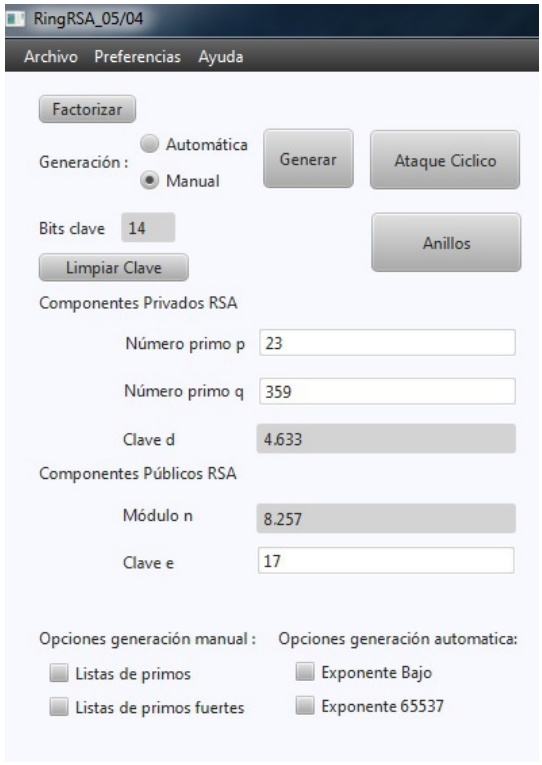

Figura 1: Generación de la clave p=23, q=359, e=17

VII. Trabajos Futuros

1. *El ataque cíclico al RSA como algoritmo de factorización*

   Si se obtiene alguna longitud de anillo (orden k de recifrado), parece ser posible llegar a factorizar [4] y obviamente obtener luego la clave privada. Este tema está siendo analizado por nosotros. También hay evidencia de que es posible factorizar si se obtiene computacionalmente un múltiplo de φ(n) [13]. De todas maneras, cabe añadir que completar experimentalmente un anillo no es tarea fácil si el orden del módulo es suficientemente grande, por lo cual el método de factorización de ataque cíclico es inviable en la práctica. Sin embargo, el ataque siempre es teóricamente exitoso al menos para obtener el mensaje original.

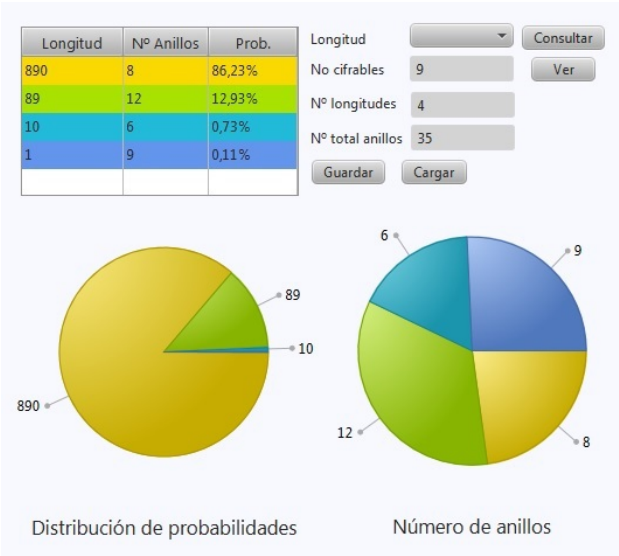

Figura 2: Anillos que se generan en la clave p = 23, q = 359 utilizando e = 17

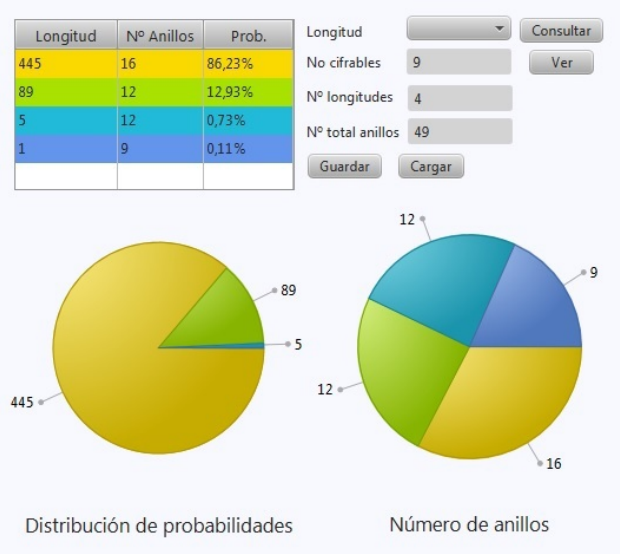

Figura 3: Anillos que se generan en la clave p = 23, q = 359 utilizando e = 31

2. *Cómo prevenir el ataque cíclico al RSA*

Para prevenir o dificultar que prospere el quiebre de RSA a través de un ataque cíclico [12] se debe cumplir, dados los recursos actuales, que:

$$\lambda(\lambda(n)) \quad y \quad ord_{\lambda(n)}(e) > 10^{200}$$

Esta condición se logra con primos fuertes p, q tales que:

$$\frac{p-1}{2} \quad y \quad \frac{p-3}{4} \; sean \; primos$$

Y lo mismo para q. Si p y q lo fuesen, se verifica:

$$\lambda(n) = 2\frac{p-1}{2}\frac{q-1}{2}$$

$$\lambda(\lambda(n)) = mcm\left(2, \frac{p-3}{2}, \frac{q-3}{2}\right) = (p-3)(q-3)/8$$

Sin embargo hay opinión fundada que la primera condición $\frac{p-1}{2}$ sería suficiente para bloquear el ataque cíclico [3].

3. *Complejidad computacional del ataque cíclico*

Este ataque, a pesar de ser teóricamente eficaz, parece pertenecer a la clase de complejidad NP, es decir un problema de tanta dificultad como el propio problema de la factorización de enteros [3, 12]. La evidencia empírica de lo antedicho es que si n se incrementa lo suficiente, el ataque cíclico se vuelve inútil con los recursos computacionales actuales. De hecho, en [6] se demuestra que si se consideran primos tomados al azar, el ataque cíclico es de complejidad $O(\sqrt{n})$, lo que lo hace equivalente al método de factorización por división de primos menores a la raíz cuadrada [9].

No obstante, la aparición de anillos basados en el cifrado cíclico y comentado en este artículo, presenta interesantes aspectos para un posterior estudio. A modo de ejemplo, una clave RSA de 50 bits con primos p y q de 25 bits cada uno (n = pq = 29.221.417 x 24.917.353 = 728.120.362.549.201) para e=15.131 encuentra el mensaje secreto 2 en 300 milisegundos, realizando tan sólo 259.956 cálculos; pero si la clave pública es e=65.537, el mismo ataque tardará 21 segundos al necesitar ahora realizar 13.777.668 cálculos.

En la figura 4 se muestra el resultado del ataque cíclico al mensaje 2 para dicha clave con exponente 65.537 en 21 segundos.

Más aún. Con RingRSA elegimos otra clave de dimensiones similares pero con un tamaño un 20 % menor (n = pq = 20.713.829 x 28.164.079 = 583.385.916.348.491) usando e=65.537 y se buscan los anillos de la clave comenzando como siempre por el número 2. Después de mil minutos, se detiene la búsqueda y con 48.040.766.272 valores ya obtenidos no se encuentra aún ese primer anillo. Queda por tanto la posibilidad de que el número 2 se encuentre en uno de estos cuatro divisores de Carmichael: 54.452.402.235, 72.603.202.980, 108.904.804.470 o bien 217.809.608.940 [14]. Para el mayor divisor de Carmichael de esta clave, a una tasa de 800.000 cifrados por segundo, el programa tardaría más de 75 horas en encontrar ese anillo.

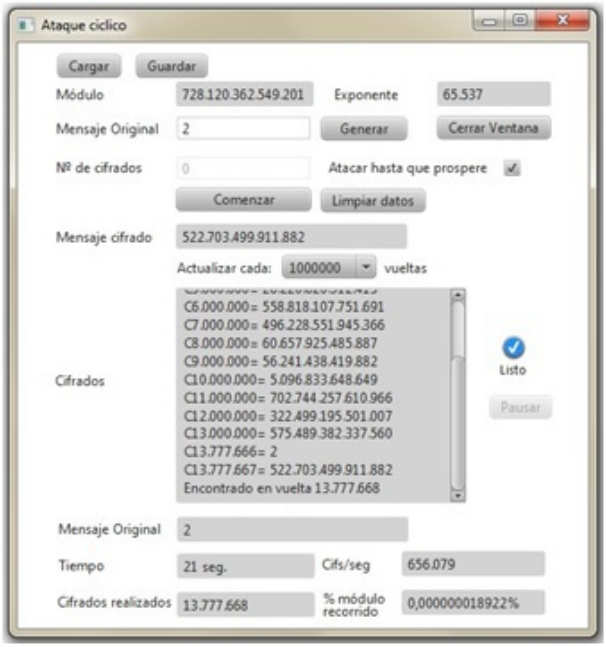

Figura 4: Ataque al valor secreto 2 para la clave con datos públicos n = 728.120.362.549.201 y e = 65.537

En otras palabras, para un par de claves muy similares, en el primer caso el ataque por cifrado cíclico requerirá un cómputo y un tiempo casi un millón de veces menor que en el segundo, siendo incluso la primera clave un 20 % mayor que la segunda. Otro aspecto interesante a estudiar en el futuro.

VIII. Conclusiones

Se ilustra que es factible calcular las longitudes de ciclos (anillos), las frecuencias de longitudes de ciclos de recifrado en el método de ataque cíclico al RSA para elecciones determinadas de valores n, m, e y que a partir de un único ataque cíclico exitoso al RSA sería posible, en teoría, hallar la clave privada a partir de la pública.

Este trabajo plantea algunos temas abiertos como trabajo futuro, entre los que se encuentran los presentados en el apartado anterior: la deducción práctica de la clave privada d mediante este tipo de ataques cíclicos completando un solo anillo, la posibilidad de dificultar o bloquear este ataque si se utilizan primos seguros en el diseño de las claves, todo ello con el soporte del mencionado software y el correspondiente desarrollo analítico.

Referencias

[1] A. Casado, J Ramió, Software para el estudio del comportamiento de los ataques por cifrado cíclico en RSA, programa RingRSA de próxima publicación en Internet, Proyecto Fin de Grado de Abel Casado Gimeno, ETSISI-UPM, 2014.

[2] J Ramió, , RSA cumple 36 años y se le ha caducado el carné joven, Rooted CON Madrid,Marzo 2014. http://www.criptored.upm.es/guiateoria/gt_m001k1.htm

[3] A. J. Menezes, P. C. van Oorschot and S. A. Vanstone, Handbook of Applied Cryptography, CRC Press, Boca Raton, FL, 1996.

[4] T. Pornin, Cycle Attack on RSA, http://crypto.stackexchange.com/questions/1572/cycle-attack-on-rsa

[5] T. W. Cusick, Properties of the x2 mod N pseudorandom number generator, IEEE Trans. Inform. Theory, 41 (1995), 1155?1159.

[6] J. B. Friedlander, C. Pomerance, and I. E. Shparlinski Period of the power generator and small values of Carmichael's function, Math. Comp., 70 (2001), 1591.1605.Corrigendum.Math.Comp., 71 (2002), 1803.1806.

[7] M. Gysin and J. Seberrye, Generalized cycling attacks on RSA and strong RSA primes, Chapter 3, J. Pieprzyk, R. Safavi-Naini, and J. Seberry (Eds.): ACISP'99, LNCS 1587, pp. 149-163, 1999. Springer-Verlag Berlin Heidelberg, 1999.

[8] H. Riesel, Prime Numbers and Computer Methods for Factorization, Progress in Mathematics, 2nd Ed., Birkhäuser, Boston, 1994.

[9] R. Lidl and H. Niederreiter, Finite Fields, Cambridge University Press, Cambridge, 1997.

[10] N. J. A. Sloane, Sequence A181776 a(n) = lambda(lambda(n)), where lambda(n) is the Carmichael lambda function, The On-Line Encyclopedia of Integer Sequences, http://oeis.org/A181776

[11] G. L. Miller Riemann's hypothesis and tests for primality, Journal of Computer and System Sciences, 13:3, 300-317, 1976.

[12] Divisores de Carmichael para el módulo n=583.385.916.348.491. https://www.wolframalpha.com/input/?i=Divisors[Carmichael[CarmichaelLambda[583385916348491]]]

Pedro Hecht (M 2012) nació en Buenos Aires, Argentina, el 14 de Julio de 1944. Se graduó como Licenciado en Análisis de Sistemas (ESIO-DIGID) y como Doctor de la Universidad de Buenos Aires. Actualmente es Profesor Titular de Criptografía I y II de la Maestría en Seguridad Informática dependiente de las Facultades de Cs. Económicas, Cs. Exactas y Naturales y de Ingeniería de la Universidad de Buenos Aires (UBA) e idéntico cargo en la Facultad de Ingeniería del Ejército (EST). Además es el Coordinador Académico de la citada Maestría (UBA) y es investigador en modelos matemáticos en UBACyT (UBA). Es miembro de Criptored, IEEE Argentina, ACM SIGCSE, ACM SIGITE y otras. Áreas de interés actual: álgebra no conmutativa aplicada a la criptografía.

Jorge Ramió Jorge Ramió nació en Barcelona, España, el 22 de Enero de 1952. Doctor en Sistemas Inteligentes en la Ingeniería por la Universidad de León (2013), Máster en Ingeniería de Sistemas y Servicios Accesibles para la Sociedad de la Información por la Universidad Politécnica de Madrid (2011) y Doctor Ingeniero de Telecomunicación Diplomado por la Universidad Politécnica de Madrid (1983). Creador de Criptored y sus proyectos derivados intypedia y crypt4you, así como el Congreso Iberoamericano CIBSI y el Taller de Enseñanza TIBETS. Imparte asignaturas de seguridad y criptografía en la UPM desde el año 1994.

Profesor invitado en posgrados de España y Latinoamérica, actualmente se encuentra desarrollando los proyectos de píldoras formativas Thoth y Mapa de Enseñanza de la Seguridad de la Información MESI.

Abel Casado nació en Madrid, España, el 2 de Noviembre de 1989. Está finalizando los estudios de Grado de Ingeniera de Computadores en la Escuela Técnica Superior de Ingeniería de Sistemas Informáticos, (ETSISI-UPM), a falta de entregar el PFG. Actualmente se encuentra trabajando como becario para el Departamento de Matemática Aplicada de la ETSISI, llevando a cabo labores relativas a geometría computacional y renderizado en 3D en la empresa ACA España. Áreas de interés actual: Computación Gráfica, Desarrollo de aplicaciones Java, Criptografía y Seguridad de la Información.