03 RSA
Fracciones continuas
Criptanálisis
Exponente pequeño

Quebrando RSA con fracciones continuas

Pablo Gabriel Celayes.

Profesor: Daniel Penazzi
Facultad de Matemática, Astronomía y Física — U.N.C.

22 de diciembre de 2011

Resumen

Describimos el esquema de encriptación de clave pública RSA, y como vulnerarlo en el caso en que el exponente de desencriptación (clave privada) sea pequeño. También adaptaremos este ataque para el caso en el que el exponente sea muy grande (i.e.: negativo pequeño). Para tal fin, introduciremos nociones de desarrollo en fracciones continuas y veremos como emplearlas para recuperar la clave privada d a partir de la clave pública (n, e).

Índice

1. RSA

RSA es un algoritmo de encriptación de clave pública-privada, cuya seguridad se basa en la dificultad para resolver del siguiente problema:

Definición 1 (Problema RSA)**.** Dados $n = pq \in \mathbb{N}$, con p, q dos primos impares distintos, $e \in \mathbb{N}$ tal que $mcd(e, (p-1)(q-1)) = 1$, $c \in \mathbb{Z}$, hallar m tal que $m^e \equiv c \mod n$.

El algoritmo se describe como sigue

Algoritmo 1 (Generación de claves RSA)**.**

Resumen *Cada entidad A crea una clave pública RSA y su correspondiente clave privada. Cada entidad debe hacer lo siguiente:*

1. *Generar dos números primos aleatorios grandes (y distintos) p y q, "del mismo tamaño".*
2. *Calcular $n := pq$ y $\phi(n) = (p-1)(q-1)$.*
3. *Elegir un entero e aleatorio, $1 < e < \phi(n)$, tal que $(e, \phi) = 1$.*
4. *Calcular el $d := e^{-1} \mod \phi$*
5. *La clave pública de A es (n, e); la clave privada de A es d.*

Definición 2. Los enteros e y d se denominan el **exponente de encriptación** y el **exponente de desencriptación**, respectivamente, y n es el **módulo**.

Algoritmo 2 (Encriptación de clave pública RSA)**.**
Resumen *B encripta un mensaje m para A, el cual A desencripta.*

Encriptación *B debe hacer lo siguiente:*

(a) *Obtener la clave pública de A, (n, e).*
(b) *Representar su mensaje como un entero en el intervalo $[0, n-1]$.*
(c) *Calcular $c = m^e \mod n$*
(d) *Enviar el texto encriptado c a A.*

Desencriptación *Para recuperar m a partir de c, A simplemente debe hacer*

(a) *Usar la clave privada d para recuperar $m = c^d \mod n$*

Teorema 3. *La desencriptación RSA funciona correctamente*

Prueba. Como $ed \equiv 1 \mod \phi$, hay un entero k tal que $ed = 1 + k\phi$. Ahora, si $(m, p) = 1$, por el teorema de Fermat se tiene

$$m^{p-1} \equiv 1 \mod p$$

elevando ambos lados a la potencia $k(q-1)$ y luego multiplicando por m, se obtiene

$$m^{1+k(p-1)(q-1)} \equiv m \mod p$$

Por otro lado, si fuera $(m, p) = p$, esta última congruencia sería trivialmente válida pues ambos lados serían $0 \mod p$. Por lo tanto, para cualquier m, se cumple

$$m^{ed} \equiv m \mod p$$

Por el mismo argumento se tiene

$$m^{ed} \equiv m \mod q$$

y como p y q son primos distintos, se verifica

$$m^{ed} \equiv m \mod n$$

Luego

$$c^d \equiv (m^e)^d \equiv m^{ed} \equiv m \mod n$$

□

2. Fracciones continuas finitas

Llamaremos a la expresión

$$a_0 + \cfrac{1}{a_1 + \cfrac{1}{a_2 + \cfrac{1}{a_3 + \cfrac{\cdots}{\cdots + \cfrac{1}{a_N}}}}} \tag{1}$$

sobre las $N+1$ variables $a_0, a_1, \ldots, a_N$, una **fracción continua finita** o, si no hay ambigüedad, simplemente una **fracción continua**.

Llamamos a $a_0, \ldots, a_N$ los **cocientes parciales**, o simplemente los cocientes, de la fracción continua.

La fórmula 1 es un poco molesta de escribir, por lo que normalmente usaremos alguna de estas dos notaciones:

$$a_0 + \frac{1}{a_1+} + \frac{1}{a_2+} \cdots \frac{1}{a_N}$$

$$[a_0, a_1, \ldots, a_N]$$

Son inmediatas de la definición las siguientes identidades:

$$[a_0, a_1] = a_0 + \frac{1}{a_1} \tag{2}$$

$$[a_0, a_1, \ldots, a_{n-1}, a_n] = [a_0, a_1, \ldots, a_{n-1} + \frac{1}{a_n}] \tag{3}$$

$$[a_0, a_1, \ldots, a_n] = a_0 + \frac{1}{[a_1, \ldots, a_{n-1}, a_n]} = [a_0, [a_1, \ldots, a_{n-1}, a_n]] \tag{4}$$

Podríamos dar una definición formal recursiva de nuestras fracciones continuas usando 2 y 3 ó 4. Ambas ecuaciones se generalizan a:

$$[a_0, a_1, \ldots, a_n] = [a_0, a_1, \ldots, a_{m-1}, [a_m, a_{m+1}, \ldots, a_n]] \tag{5}$$

para $1 \leq m < n \leq N$.

2.1. Convergentes

Denominamos a

$$[a_0, a_1, \ldots, a_n] \ , \ (0 \leq n \leq N)$$

el n-ésimo **convergente** de $[a_0, a_1, \ldots, a_N]$. Simplifiquemos, a modo de ejemplo, el segundo convergente:

$$a_0 + \frac{1}{a_1 + \frac{1}{a_2}} = a_0 + \frac{1}{\frac{a_1 a_2 + 1}{a_2}} = a_0 + \frac{a_2}{a_1 a_2 + 1} = \frac{a_0(a_1 a_2 + 1) + a_2}{a_1 a_2 + 1} = \frac{a_0 a_1 a_2 + a_0 + a_2}{a_1 a_2 + 1}$$

Podemos calcular fácilmente los convergentes gracias al siguiente teorema:

Teorema 4. *Si p_n y q_n se definen recursivamente como*

$p_0 = a_0$, $p_1 = a_1 a_0 + 1$, $p_n = a_n p_{n-1} + p_{n-2}$ $(2 \leq n \leq N)$,

$q_0 = 1$, $q_1 = a_1$, $q_n = a_n q_{n-1} + q_{n-2}$ $(2 \leq n \leq N)$,

entonces

$$[a_0, a_1, \ldots, a_n] = \frac{p_n}{q_n}$$

Prueba. Se ve fácilmente que $[a_0] = \frac{a_0}{1}$ y $[a_0, a_1] = \frac{a_1 a_0 + 1}{a_1}$. Supongamos ahora el teorema cierto para $n \leq m$, con $m < N$. Entonces

$$[a_0, a_1, \ldots, a_m] = \frac{p_m}{q_m} = \frac{a_m p_{m-1} + p_{m-2}}{a_m q_{m-1} + q_{m-2}}$$

y $p_{m-1}, p_{m-2}, q_{m-1}, q_{m-2}$ dependen solo de $a_0, a_1, \ldots, a_{m-1}$. Luego, usando (3), obtenemos

$$\begin{aligned}
[a_0, a_1, \ldots, a_m, a_{m+1}] &= [a_0, a_1, \ldots, a_m + \frac{1}{a_{m+1}}] \\
&= \frac{\left(a_m + \frac{1}{a_{m+1}}\right) p_{m-1} + p_{m-2}}{\left(a_m + \frac{1}{a_{m+1}}\right) p_{m-1} + p_{m-2}} \\
&= \frac{a_{m+1}(a_m p_{m-1} + p_{m-2}) + p_{m-1}}{a_{m+1}(a_m q_{m-1} + q_{m-2}) + q_{m-1}} \\
&= \frac{a_{m+1} p_m + p_{m-1}}{a_{m+1} q_m + q_{m-1}} = \frac{p_{m+1}}{q_{m+1}}
\end{aligned}$$

y entonces el teorema queda probado por inducción. □

El teorema anterior nos permite probar el siguiente resultado

Teorema 5. *Para todo $n \geq 1$, p_n y q_n satisfacen la ecuación*

$$p_n q_{n-1} - p_{n-1} q_n = (-1)^{n-1} \tag{6}$$

Prueba. Para $n = 1$, tenemos $p_1 q_0 - p_0 q_1 = (a_1 a_0 + 1)(1) - a_0 a_1 = 1$. Probémoslo por inducción para $n \geq 2$, asumiendo que (6) vale para $n - 1$. Por el teorema 4 se tiene

$$\begin{aligned}
p_n q_{n-1} - p_{n-1} q_n &= (a_n p_{n-1} + p_{n-2}) q_{n-1} - p_{n-1}(a_n q_{n-1} + q_{n-2}) \\
&= p_{n-2} q_{n-1} - p_{n-1} q_{n-2} \\
&= -(p_{n-1} q_{n-2} - p_{n-2} q_{n-1}) \\
&= -(-1)^{n-2} = (-1)^{n-1}
\end{aligned}$$

□

2.2. Representación de racionales

Ahora les daremos valores numéricos a las variables a_n, y por lo tanto a la fracción 1 y a sus convergentes. Asumiremos siempre que $a_1 > 0, \ldots, a_N > 0$ y normalmente también que $a_0 \in \mathbb{Z}$, en cuyo caso la fracción continua se denomina **simple**. Denotaremos

$$x_n := \frac{p_n}{q_n}, \quad x := x_N$$

de modo que el valor de la fracción continua es x o x_N.

Se sigue de (5) que

$$\begin{aligned} x &= [a_0, a_1, \ldots, a_N] = [a_0, a_1, \ldots, a_{n-1}, [a_n, a_{n+1}, \ldots, a_N]] \\ &= \frac{[a_n, a_{n+1}, \ldots, a_N]p_{n-1} + p_{n-2}}{[a_n, a_{n+1}, \ldots, a_N]q_{n-1} + q_{n-2}} \end{aligned} \tag{7}$$

para $2 \leq n \leq N$.

De aquí en adelante trabajaremos con fracciones continuas simples y asumiremos que los a_n son todos enteros, de donde por el teorema 4 los p_n y q_n serán enteros, y q_n será siempre positivo. Por (6) tenemos además que $(p_n, q_n) = 1$ y entonces los convergentes p_n/q_n son fracciones irreducibles.

Denotamos

$$a'_n := [a_n, a_{n+1}, \ldots, a_N] \quad (0 \leq n \leq N)$$

y lo denominamos el **n-ésimo cociente completo** de la fracción continua.

Por lo tanto

$$x = a'_0 \quad x = \frac{a'_1 a_0 + 1}{a'_1}$$

y

$$x = \frac{a'_n p_{n-1} + p_{n-2}}{a'_n q_{n-1} + q_{n-2}} \quad (2 \leq n \leq N) \tag{8}$$

Cualquier fracción continua $[a_0, a_1, \ldots, a_N]$ representa a un número racional $x = x_N$. Veremos luego que, recíprocamente, todo número racional positivo x es representable por una fracción continua y que, salvo una pequeña ambigüedad, la representación es única.

Teorema 6. *Si x es representable como una fracción continua con un cantidad impar (par) de convergentes, entonces también es representable por una fracción continua con un cantidad par (impar).*

Prueba. Si $a_n \geq 2$,

$$[a_0, a_1, \ldots, a_n] = [a_0, a_1, \ldots, a_n - 1, 1]$$

y, si $a_n = 1$

$$[a_0, a_1, \ldots, a_{n-1}, 1] = [a_0, a_1, \ldots, a_{n-1} + 1]$$

□

Teorema 7. *$a_n = [a'_n]$ (la parte entera de a'_n), con la única excepción de que $a_{N-1} = [a'_{N-1}] - 1$ cuando $a_N = 1$.*

Prueba. Si $N = 0$, entonces $a_0 = a'_0 = [a'_0]$. Si $N > 0$ entonces

$$a'_n = a_n + \frac{1}{a'_{n+1}} \quad 0 \leq n \leq N$$

ahora, $a'_{n+1} > 1$ salvo cuando $n = N - 1$ y $a_N = 1$. Luego

$$a_n < a'_n < a_n + 1 \Rightarrow a_n = [a'_n]$$

salvo en el caso mencionado. □

Este último teorema nos permitirá probar que, salvo por la ambigüedad observada en el teorema 6, la representación de un racional x como fracción continua es única.

Teorema 8. *Si dos fracciones continuas simples*

$$[a_0, a_1, \ldots, a_N], \quad [b_0, b_1, \ldots, b_M]$$

tienen el mismo valor x, y $a_N > 1$, $b_M > 1$, entonces $M = N$ y $a_n = b_n \ \forall\ 0 \leq n \leq N$.

Prueba. Por el teorema 7, $a_0 = [x] = b_0$. Supongamos que los primeros n cocientes parciales de nuestras fracciones continuas son iguales. Entonces

$$x = [a_0, a_1, \ldots, a_{n-1}, a'_n] = [a_0, a_1, \ldots, a_{n-1}, b'_n]$$

Si $n = 1$, entonces $a_0 + \frac{1}{a'_1} = a_0 + \frac{1}{b'_1}$, y $a'_1 = b'_1$, luego, por el teorema 7, $a_1 = b_1$. Si $n > 1$ entonces, por (8)

$$\frac{a'_n p_{n-1} + p_{n-2}}{a'_n q_{n-1} + q_{n-2}} = \frac{b'_n p_{n-1} + p_{n-2}}{b'_n q_{n-1} + q_{n-2}}$$

$$(a'_n - b'_n)(p_{n-1}q_{n-2} - p_{n-2}q_{n-1}) = 0$$

Pero $p_{n-1}q_{n-2} - p_{n-2}q_{n-1} = (-1)^n$, por el teorema 5, y entonces $a'_n = b'_n$. Se sigue del teorema 7 que $a_n = b_n$.

Supongamos ahora que, por ejemplo, $N \leq M$. Nuestro argumento anterior muestra que $a_n = b_n$ para $n \leq N$. Si $M > N$, entonces

$$\frac{p_N}{q_N} = [a_0, a_1, \ldots, a_N] = [a_0, a_1, \ldots, a_N, b_{N+1}, \ldots, b_M] = \frac{b'_{N+1} p_N + p_{N-1}}{b'_{N+1} q_N + q_{N-1}}$$

pero esto implica $p_N q_{N-1} - p_{N-1} q_N = 0$, lo cual es falso. Luego, $M = N$ y las fracciones son idénticas. □

Podemos dar ahora una prueba constructiva (algorítmica) de

Teorema 9. *Todo número racional x se puede representar como una fracción continua simple finita.*

Prueba. Si x es un entero, no hay nada que probar. Si x no es entero, haciendo $a_0 := [x]$, podemos escribir

$$x = a_0 + \zeta_0, \quad 0 < \zeta_0 < 1$$

Como $\zeta_0 \neq 0$, podemos definir

$$a_1' := \frac{1}{\zeta_0}, \quad a_1 := [a_1'], \quad a_1' = a_1 + \zeta_1, \quad 0 \leq \zeta_1 < 1$$

Si $\zeta_1 \neq 0$, podemos definir

$$\frac{1}{\zeta_1} =: a_2' =: a_2 + \zeta_2, \quad 0 \leq \zeta_1 < 1$$

y así sucesivamente. Notemos que $a_n' = 1/\zeta_{n-1} > 1$, y luego $a_n \geq 1$, para $n \geq 1$. Entonces

$$x = [a_0, a_1'] = [a_0, a_1 + \frac{1}{a_2'}] = [a_0, a_1, a_2'] = [a_0, a_1, a_2, a_3'] = \ldots$$

El proceso de definición de los a_n que acabamos de definir se puede programar como un algoritmo que permita encontrar el desarrollo en fracción continua de un número dado. Pero aún no hemos terminado la prueba, necesitamos ver que si x es racional, este proceso termina en una cantidad finita de pasos. Como x no es entero, se tiene $x = \frac{h}{k}$, con h y k enteros y $k > 1$. Ahora

$$\frac{h}{k} = a_0 + \zeta_0 \Rightarrow h = a_0 k + \zeta_0 k,$$

a_0 es entonces el cociente, y $k_1 := \zeta_0 k$ el resto, en la división de h por k.

Si $\zeta_0 \neq 0$, entonces $a_1' = \frac{1}{\zeta_0} = \frac{k}{k_1}$ y

$$\frac{k}{k_1} = a_1 + \zeta_1, \quad k = a_1 k_1 + \zeta_1 k_1;$$

Luego k_1 es el cociente y $k_2 := \zeta_1 k_1$ el resto en la división de k por k_1. Obtenemos entonces una serie de ecuaciones

$$h = a_0 k + k_1, \quad k = a_1 k_1 + k_2, \quad k_1 = a_2 k_2 + k_3, \quad \ldots$$

que se extiende mientras sea $\zeta_n \neq 0$, o, lo que es lo mismo, mientras $k_{n+1} \neq 0$. Pero $k > k_1 > k_2 > \ldots$ y entonces $k_{N+1} = 0$ para algún N. Se sigue entonces que $\zeta_N = 0$ para algún N y que entonces el algoritmo termina.

Notemos que $\zeta_N = 0$ implica $a_N' = a_N$, y

$$0 < \frac{1}{a_N} = \frac{1}{a_N'} = \zeta_{N-1} < 1$$

y entonces $a_N \geq 2$. Deducimos que el algoritmo encuentra una representación del tipo cuya unicidad demostramos en el teorema 8. Siempre tenemos la posibilidad de utilizar la variante del teorema 6. □

Teorema 10. *Si $x = \frac{P}{Q}$ es un racional positivo, la representación de x como fracción continua puede calcularse en $\mathcal{O}(\log_2(\text{máx}\{P, Q\}))$ pasos.*

Prueba. Por el teorema 4, tenemos que $\{p_n\}$ y $\{q_n\}$ son sucesiones crecientes. Además,

$$\begin{aligned} p_n &\geq p_{n-1} + p_{n-2} \geq 2p_{n-2}, \\ q_n &\geq q_{n-1} + q_{n-2} \geq 2q_{n-2}, \text{ para } n \geq 2 \end{aligned} \tag{9}$$

Como $p_1 \geq 1$ y $q_0 = 1$, tenemos $p_3 \geq p_2 + p_1 \geq 2$ y análogamente $q_2 \geq 2$. Aplicando (9) para $n \geq 5$ tenemos

$$p_n \geq 2p_{n-2} \geq 4p_{n-4} \geq \ldots \geq 2^{[\frac{n-3}{2}]}p_k, \quad k = 3 \text{ ó } 4$$

de donde $p_n \geq 2^{[\frac{n-3}{2}]+1} = 2^{[\frac{n-1}{2}]}$. Análogamente se ve que q_n también crece exponencialmente. Dado que $p_N = P$ y $q_N = Q$, el algoritmo del teorema 9 tiene complejidad $\mathcal{O}(\log_2(\text{máx}\{P, Q\}))$. □

El siguiente teorema nos permite dar una caracterización útil de los convergentes de una fracción continua simple.

Teorema 11. *Si $x = \frac{P\xi+R}{Q\xi+S}$, con $\xi > 1$ y P, Q, R, S enteros tales que*

$$Q > S > 0 \ , \ PS - QR = \pm 1 \ ,$$

entonces R/S y P/Q son dos convergentes consecutivos de la fracción continua simple cuyo valor es x. Si R/S es el $(n-1)$-ésimo convergente y P/Q es el n-ésimo, entonces ξ es el $(n+1)$-ésimo cociente completo.

Prueba. Desarrollamos a P/Q como fracción continua:

$$\frac{P}{Q} = [a_0, a_1, \ldots, a_n] = \frac{p_n}{q_n} \tag{10}$$

Por el teorema 6, podemos asumir n par o impar según nos convenga. Elegimos n tal que

$$PS - QR = \pm 1 = (-1)^{n-1} \tag{11}$$

Ahora, $(P, Q) = 1$ y $Q > 0$, y p_n y q_n satisfacen las mismas condiciones. Entonces, (10) y (11) implican $P = p_n$, $Q = q_n$, y

$$p_nS - q_nR = PS - QR = (-1)^{n-1} = p_nq_{n-1} - p_{n-1}q_n$$

y de aquí sale $p_n(S - q_{n-1}) = q_n(R - p_{n-1})$. Como $(p_n, q_n) = 1$, deducimos que

$$q_n | (S - q_{n-1}) \tag{12}$$

Pero $q_n = Q > S > 0$, y $q_n \geq q_{n-1} > 0$, y entonces $|S - q_{n-1}| < q_n$. Esto, junto con (12) implican $S - q_{n-1} = 0$. Luego,

$$S = q_{n-1} \ , \ R = p_{n-1} \ , \text{ y } \ x = \frac{p_n \xi + p_{n-1}}{q_n \xi + q_{n-1}}$$

, o sea $x = [a_0, a_1, \ldots, a_n, \xi]$.

Si desarrollamos ξ como fracción continua, obtenemos $\xi = [a_{n+1}, a_{n+2}, \ldots]$, con $a_{n+1} = [\xi] \geq 1$. Luego $x = [a_0, a_1, \ldots, a_n, a_{n+1}, a_{n+2}, \ldots]$ es una fracción continua simple, $R/S = p_{n-1}/q_{n-1}$ y $P/Q = p_n/q_n$ son dos convergentes consecutivos de dicha fracción, y ξ es el $(n+1)$-ésimo cociente completo. □

El siguiente teorema nos dice que toda aproximación suficientemente buena tiene que ser un convergente. Este es el resultado que emplearemos luego para ver cómo quebrar RSA.

Teorema 12. *Si*

$$\left| \frac{p}{q} - x \right| < \frac{1}{2q^2} \tag{13}$$

entonces p/q es un convergente.

Prueba. Si (13) es cierta, entonces

$$\frac{p}{q} - x = \frac{\epsilon \theta}{q^2}$$

con $\epsilon = \pm 1$, $0 < \theta < \frac{1}{2}$.

Podemos expresar a p/q como una fracción continua $[a_0, a_1, \ldots, a_n]$, y como por el teorema 6 podemos hacer que n sea par o impar, podemos asumir que $\epsilon = (-1)^{n-1}$.

Sea ω tal que $x = \frac{\omega p_n + p_{n-1}}{\omega q_n + q_{n-1}}$, donde p_n/q_n y p_{n-1}/q_{n-1} son el último y penúltimo convergentes de la fracción continua de p/q. Luego

$$\frac{\epsilon \theta}{q_n^2} = \frac{p_n}{q_n} - x = \frac{p_n q_{n-1} - p_{n-1} q_n}{q_n(\omega q_n + q_{n-1})} = \frac{(-1)^{n-1}}{q_n(\omega q_n + q_{n-1})}$$

y entonces

$$\frac{q_n}{\omega q_n + q_{n-1}} = \theta$$

de donde tenemos

$$\omega = \frac{1}{\theta} - \frac{q_{n-1}}{q_n} > 1$$

(porque $\theta < \frac{1}{2}$ y $q_{n-1} < q_n$), y entonces, por el teorema 11, p_{n-1}/q_{n-1} y p_n/q_n son dos convergentes consecutivos de x. Como era $p_n/q_n = p/q$ hemos probado lo que queríamos. □

3. Quebrando RSA

3.1. exponente d pequeño

Para mejorar la velocidad de desencriptación, puede resultar conveniente escoger d pequeño. Veamos como esto genera vulnerabilidades, viendo que mediante el uso de convergentes de fracciones continuas puede recuperarse d a partir de la clave pública (n, e)

El siguiente ataque fue descripto por Wiener en 1990:

Teorema 13 (Ataque de Wiener para d chico)**.** *Si $n = pq$ es un módulo RSA con $p < q < 2p$ y $d < \frac{\sqrt[4]{n}}{\sqrt{6}}$, entonces d es el denominador de uno de los convergentes del desarrollo en fracción continua de $\frac{e}{n}$ y se recupera en tiempo $\mathcal{O}(\log_2(n))$.*

Prueba. Notemos que $p^2 < pq = n$ y luego $p + q < p + 2p < 3\sqrt{n}$. De aquí se obtiene que $n - \phi(n) = pq - (p-1)(q-1) = p + q - 1 < 3\sqrt{n} - 1$. Ahora, sea k entero tal que $ed - k\phi(n) = 1$. Veamos que se satisface la hipótesis del **teorema 12**:

$$\left|\frac{k}{d} - \frac{e}{n}\right| = \left|\frac{kn - de}{nd}\right| = \left|\frac{k(n - \phi(n)) + (k\phi(n) - de}{nd}\right| = \left|\frac{k(n - \phi(n)) - 1}{nd}\right| < \frac{k3\sqrt{n}}{nd} = \frac{3k}{\sqrt{n}d}$$

Por otra parte, tenemos

$$k(p-1)(q-1) = ed - 1 < ed < (p-1)(q-1)d \Rightarrow k < d$$

y además $d < \frac{\sqrt[4]{n}}{\sqrt{6}}$, implica $6d^2 < \sqrt{n}$. Entonces

$$\frac{3k}{\sqrt{n}d} < \frac{3}{\sqrt{n}} < \frac{3}{6d^2} = \frac{1}{2d^2}$$

Ahora, por el **teorema 12**, $\frac{k}{d}$ es un convergente de $\frac{e}{n}$. Notemos que por el **teorema 10**, se puede recuperar d en tiempo $\mathcal{O}(\log_2(n))$, o sea, en tiempo lineal en la cantidad de bits de n. □

3.2. exponente d muy grande

Normalmente pensamos todos los cálculos de RSA en su representación positiva (i.e.: usando siempre valores positivos). Sin embargo, si los exponentes público y privado se piensan en su representación simétrica, el costo computacional de la exponenciación se puede reducir considerablemente usando exponentes negativos pequeños.

De hecho, si d es un exponente negativo pequeño, el costo de calcular $m^{-d} \mod n$ es el costo de calcular $m^d \mod n$ más el costo de una inversión mod n.

Como ya hemos visto, emplear exponentes positivos pequeños es peligroso. Resultaría tentador entonces tratar de emplear un exponente d negativo pequeño, para acelerar la desencriptación. Veremos a continuación que esto resulta igualmente inseguro.

Teorema 14 (Ataque de Wiener para d grande)**.** *Si $n = pq$ es un módulo RSA con $p < q < 2p$ y $(\phi(n) - d) < \frac{\sqrt[4]{n}}{\sqrt{6}}$, entonces d puede recuperarse en $\mathcal{O}(\log_2(n))$ pasos.*

Prueba. Igual que antes, tenemos $n - \phi(n) < 3\sqrt{n} - 1$.

Como $ed \equiv 1 \mod \phi(n)$, tenemos $e(\phi(n) - d) \equiv -1 \mod \phi(n)$. Definiendo $D := \phi(n) - d$, podemos escribir $eD = k\phi(n) - 1$. Como $e < \phi(n)$, resulta, como antes, $k < D$. Veamos que también se satisface la hipótesis del **teorema 12**:

$$\left|\frac{k}{D} - \frac{e}{n}\right| = \left|\frac{kn - De}{nD}\right| = \left|\frac{kn - (k\phi(n) - 1)}{nD}\right| = \left|\frac{1 + k(n - \phi(n))}{nD}\right| < \frac{1 + k(3\sqrt{n} - 1)}{nD} < \frac{3k}{\sqrt{n}D}$$

Como $k < D$ y $6D^2 < \sqrt{n}$, tenemos

$$\frac{3k}{\sqrt{n}D} < \frac{3}{\sqrt{n}} < \frac{1}{2D^2}$$

y concluimos como antes que $\frac{k}{D}$ es uno de los $\mathcal{O}(\log_2(n))$ convergentes de $\frac{e}{n}$.

Para chequear si un convergente $\frac{k'}{d'}$ cumple $d' = D$, calculamos $\phi' = \frac{ed'+1}{k'}$. Si ϕ' resulta entero, chequeamos que sea $\phi' = \phi(n)$ como sigue. Dado que $\phi(n) - n - 1 = p + q$, y que p y q son raíces de $x^2 - (p + q)x + pq = 0$, definimos $m' := \phi' - n - 1$ y chequeamos si $x^2 - m'x + n = 0$ tiene raíces enteras positivas. Cuando esto se cumpla, habremos obtenido la factorización de n y $d := \phi' - D'$ será el exponente de desencriptación. □

La necesidad de conocer $\phi(n)$ para recuperar d en este último teorema, nos forzó a probar algo más fuerte que antes: no sólo se logra recuperar d, sino que además logramos factorizar n. Esto también puede adaptarse al caso de exponente chico.

Referencias

[75HW] G.H. Hardy, E.M. Wright: "An Introduction to the Theory of Numbers". *Oxford University Press*

[96Men] A. Menezes, P. Van Oorschot, S. Vanstone: "Handbook of Applied Cryptography". *CRC Press*

[Duj] Andrej Dujella: "Continued fractions and RSA with small Secret Exponent".

[04Hin] M. Jason Hinek: "(Very) Large RSA Private Exponent Vulnerabilities". *School of Computer Science, University of Waterloo*

[89Wie] Michael J. Wiener: "Cryptanalysis of Short RSA Secret Exponents".