EXPONENTES DE CIFRADO PEQUEÑOS EN RSA Y CRIPTOANÁLISIS DE WIENER

Araceli Queiruga Dios

División de Telecom
Sema
maraceli.queiruga@sema.es

Luis Hernández Encinas

Tratamiento de la Información y Codificación
C.S.I.C.
luis@iec.csic.es

RESUMEN

Es sabido que si en el criptosistema RSA la longitud en bits del exponente de descifrado es menor que la cuarta parte de la longitud en bits del módulo, dicho exponente se puede calcular en tiempo polinómico y el RSA queda roto. En este artículo se demuestra que si se considera el exponente de cifrado $e = 3$, el criptosistema RSA es seguro contra el ataque anterior. Además, se presenta una fórmula explícita para determinar el exponente de descifrado, d, conocido el valor de $\phi(n)$.

1. INTRODUCCIÓN

Debido a la masiva proliferación del intercambio de información mediante el uso de redes de ordenadores, se hace necesario analizar y determinar bajo qué condiciones este intercambio se puede llevar a cabo de forma segura. El procedimiento habitual para asegurar la confidencialidad de la información que se intercambia en Internet, ya sea de carácter general (mensajes), relacionada con movimientos bursátiles (órdenes de compra o venta de valores), de comercio electrónico (transmisión de números de tarjetas de crédito, de sus PIN, o de cuentas bancarias), etc., consiste en utilizar algún criptosistema que cifre la información en origen y la descifre en destino.

1.1. Criptosistema RSA

El criptosistema de clave pública más utilizado hoy en día es el RSA [1], que garantiza la confidencialidad y autenticidad tanto de la información como del remitente.
La clave pública del criptosistema RSA se denota por (n,e), siendo el módulo RSA $n = pq$, el producto de dos primos grandes y e el exponente de cifrado, con $1 < e < \phi(n)$, y primo con $\phi(n) = (p-1)(q-1)$. La clave privada es el exponente de descifrado, es decir, el inverso de e módulo $\phi(n)$: $1 < d < \phi(n)$. La operación más costosa en este criptosistema (computacionalmente hablando) es la exponenciación [2].
Es fundamental que el usuario que va a enviar información a través de Internet (por ejemplo, su número de tarjeta de crédito) sepa que ésta va a ser cifrada; pero a la vez, es importante que este proceso sea transparente para el usuario. Para que este supuesto se verifique, el procedimiento de cifrado debe ser lo suficientemente rápido como para que no se aprecie demora en las comunicaciones. La garantía de esta rapidez se basa en la utilización de un exponente de cifrado, e, pequeño que asegure rapidez computacional, pero que no ponga en peligro la seguridad del criptosistema, para lo que se debe mantener (entre otras precauciones) un módulo RSA, n, de tamaño adecuado según la seguridad requerida (entre 1024 y 2048 bits). Los exponentes de cifrado que se suelen recomendar [3] con este propósito son dos: $e = 3$, y $e = 2^{16} + 1 = 65537$, cuya corta expresión en binario hace que la exponenciación sea muy rápida.
El receptor de la información (en general, empresas) la descifrará con ordenadores de propósito específico o más potentes que los utilizados por los remitentes, por lo que no es tan fundamental que el proceso de descifrado sea tan rápido.

1.2. Criptoanálisis del criptosistema RSA

Para garantizar la seguridad del criptosistema RSA se deben analizar sus debilidades. Hasta la fecha el criptoanálisis que más atención ha suscitado ha sido el de tratar de romper el RSA mediante la factorización de su módulo. Es evidente que si se conocieran los factores primos p y q de n, el RSA quedaría roto. Hoy en día la hipótesis más extendida (aún sin demostrar) es que su seguridad es equivalente a la dificultad de factorizar números.
Por otra parte, es posible atacar el RSA mediante el criptoanálisis de Wiener, estudiando el exponente de descifrado [4]. Así, en [5] se prueba que si $d < 1/3\ n^{1/4}$, es decir, si la longitud en bits del exponente de descifrado es menor que la cuarta parte de la longitud en bits del módulo RSA, entonces, d se puede determinar en tiempo polinómico. El algoritmo que se utiliza hace uso de las fracciones continuas. Recientemente, se ha demostrado que si $d < n^{0.292}$, entonces el criptosistema es inseguro [6]. En la actualidad, la hipótesis más verosímil es que si $d < n^{0.5}$, el RSA puede ser roto.
En este artículo se prueba, en particular, que el exponente de cifrado $e = 3$ no compromete la seguridad del RSA por el criptoanálisis de Wiener, es decir, se demuestra que para $e = 3$, la longitud en bits del exponente de descifrado, d, es mayor que la cuarta parte del número de bits de n, de hecho, de verifica que el número de bits de d es, aproximadamente el mismo que el de n.

2. RESULTADOS

A continuación se presentarán los principales resultados obtenidos:
Teorema 1. Sean p y q dos primos tales que $\phi(pq)$ es primo con 3, entonces $\phi(pq)-1$ es un múltiplo de 3.
Demostración. Podemos escribir $p = 2^r p'+1$ y $q = 2^s q'+1$, siendo $r, s \geq 1$, y $p' = 2p''+1$ y $q' = 2q''+1$ impares. Entonces,

$$p'q' = 4p''q'' + 2p'' + 2q'' + 1 \quad (1)$$

Teniendo en cuenta que p y q juegan un papel simétrico (y por tanto, también p', q' y p'', q''), según la expresión (1) y los posibles valores de p'' y q'' al hacer módulo 3, se tienen las siguientes posibilidades para $p'q'$ (mod 3):

casos	p'' (mod 3)	q'' (mod 3)	$p'q'$ (mod 3)
a	1	0	0
b	1	1	0
c	1	–1	0
d	0	0	1
e	–1	–1	1
f	0	–1	–1

Para los casos ***a***, ***b*** y ***c***, se tiene que $p'' = 3k+1$, es decir, $p' = 6k+3$, con lo que p' no sería primo con 3 y por tanto tampoco lo sería

$$\phi(pq) = (p-1)(q-1) = 2^{r+s} p'q' \quad (2)$$

en contra de la hipótesis. Teniendo en cuenta que

$$2^r \equiv \begin{cases} 1 (\mathrm{mod}\, 3) & \text{si } r \text{ es par} \\ -1 (\mathrm{mod}\, 3) & \text{si } r \text{ es impar} \end{cases} \quad (3)$$

resulta que en el caso ***d***, es $p'' = 3k$, es decir, $p' = 6k+1$, con lo que $p = 2^{r+1}3k+2^r+1$, que sólo puede ser primo si r es par. De forma análoga, $q = 2^{s+1}3l+2^s+1$, que sólo puede ser primo para s par. Así pues, el caso ***d*** sólo puede darse cuando r y s sean pares.

En el caso ***e*** se tiene que $p'' = 3k+2$, por lo que $p' = 6k+5$, y entonces $p = 2^{r+1}3k+2^{r+2}+2^r+1$, que sólo puede ser primo si r es impar por (3). Análogamente, $q = 2^{s+1}3l+2^{s+2}+2^s+1$ sólo puede ser primo para s impar. Por tanto, el caso ***e*** sólo puede presentarse cuando r y s sean impares.

Finalmente, en el caso ***f*** se tiene que $p'' = 3k$ y $q'' = 3k+2$, por lo que $p = 2^{r+1}3k+2^r+1$ y $q = 2^{s+1}3l+2^{s+2}+2^s+1$, que sólo pueden ser primos en el caso que r sea par y s impar.

Por tanto, las únicas posibilidades son:

$$p'q' \equiv \begin{cases} 1 (\mathrm{mod}\, 3) & \text{si } r \text{ y } s \text{ son de la misma paridad} \\ -1 (\mathrm{mod}\, 3) & \text{si } r \text{ y } s \text{ son de distinta paridad} \end{cases} \quad (4)$$

Así pues, de (2) y (4) se sigue que si r y s son de la misma paridad, se tiene que $\phi(pq) = 2^{2k}p'q' \equiv p'q' \equiv 1$ (mod 3), y si son de distinta paridad, es $\phi(pq) = 2^{2l+1}p'q' \equiv -p'q' \equiv 1$ (mod 3), con lo que se concluye. □

Corolario 2. Si p y q son primos seguros mayores que 7 (es decir, $p = 2p'+1$ y $q = 2q'+1$, con p' y q' primos), entonces $\phi(pq)-1$ es múltiplo de 3.

Teorema 3. Sean p y q dos primos tales que $\phi(pq)$ es primo con 3, entonces el inverso de 3 módulo $\phi(pq)$ es

$$\frac{1+2\phi(pq)}{3} \quad (5)$$

Demostración. Por el Teorema 1, $\phi(pq) \equiv 1$ (mod 3), es decir, $1+2\phi(pq) \equiv 0$ (mod 3), lo que implica que $(1+2\phi(pq))/3$ es un número entero. Como

$$3\frac{1+2\phi(pq)}{3} = 1+2\phi(pq) \equiv 1 (\mathrm{mod}\, \phi(pq)) \quad (6)$$

se concluye. □

Corolario 4. Si $n = pq$ es el módulo del criptosistema RSA, con exponente de cifrado $e = 3$ y exponente de descifrado d, la longitud en bits de d es aproximadamente la misma que la longitud en bits de n.

Demostración. Por definición, es $ed \equiv 1$ (mod $\phi(n)$), pero por el Teorema 3, se tiene que $3d = 1+2\phi(n)$, es decir,

$$d = \frac{1+2\phi(n)}{3} \quad (7)$$

Tomando logaritmos en base 2, se verifica que

$$\log(d) \simeq \log(2/3) + \log(\phi(n)) \simeq \log(\phi(n)) \simeq \log(n) \quad (8)$$

con lo que las longitudes en bits de d y n son, aproximadamente, iguales. □

Según el Corolario 4, si se considera como exponente de cifrado en el criptosistema RSA $e = 3$, se obtiene un criptosistema que es seguro contra los criptoanálisis de Wiener y de Boneh, dado que $d > n^{0.292} > 1/3\, n^{1/4}$.

Como resultado particular se observa que con la notación del criptosistema RSA ya señalada, la condición $ed \equiv 1$ (mod $\phi(n)$), es decir, $ed = 1+k\phi(n)$, implica que para $e = 3$ se tiene que $k = 2$. De forma más general se demuestra el siguiente

Teorema 5. Si (n,e) es la clave pública del RSA con exponente de descifrado d, siendo $ed = 1+k\phi(n)$, se tiene que $k < e$.

Demostración. En efecto, dado que $d < \phi(n)$, se verifica que

$$d = \frac{1+k\phi(n)}{e} < \phi(n) \quad (9)$$

es decir,

$$k < \frac{\phi(n)e-1}{\phi(n)} = e - \frac{1}{\phi(n)} < e \quad (10)$$

con lo que $k < e$. □

3. CONCLUSIONES

En este artículo se ha estudiado el criptoanálisis del criptosistema RSA mediante la determinación del exponente de descifrado, utilizando los ataques de Wiener [4] y Boneh [6] y se ha demostrado que si se considera como exponente de cifrado $e = 3$, que es uno de los más recomendados porque permite un proceso de cifrado muy rápido, el criptosistema RSA es seguro debido a que la longitud en bits del exponente de descifrado es, aproximadamente, la misma que la del módulo RSA que se utilice.

4. REFERENCIAS

[1] Rivest, R., Shamir, A. and Adleman, L., "A method for obtaining digital signatures and public-key cryptosystems", Comm. ACM 21: 120-126, 1978.

[2] Fúster, A., Guía, D., Hernández, L., Montoya, F. y Muñoz J., *Técnicas criptográficas de protección de datos*, RA-MA, Madrid, 2000.

[3] Menezes, A., Oorschot, P. and Vanstone, S., *Handbook of applied cryptography*, CRC Press, Boca Raton, FL., 1997.

[4] Boneh, D., "Twenty years of attacks on the RSA cryptosystem", Notices of The AMS, 46(2): 203-213, 1999.

[5] Wiener, M. J., "Cryptanalysis of short RSA secret exponents", IEEE Trans. Inform. Theory, 36(3): 553-558, 1990.

[6] Boneh, D., and Durfee, G, "Cryptanalysis of RSA with private key d less than $n^{0.292}$", IEEE Trans. Inform. Theory, 46(4): 1339-1349, 2000.