Teoría de Números y Criptografía

F. J. Lobillo

2021/2022

Parte II

Criptografía y Curvas Elípticas

Índice general

Capítulo 3

Criptosistema de Rivest-Shamir-Adleman

3.1 Función unidireccional

Sean p, q dos primos impares, $n = pq$, e un entero primo relativo con $\varphi(n)$, i.e. $(e, \varphi(n)) = 1$ y d su inverso, es decir

$$ed \equiv 1 \mod \varphi(n).$$

Definimos la función

$$\mathrm{RSA}_{n,e} : \mathbb{Z}_n \to \mathbb{Z}_n \left[\mathrm{RSA}_{n,e}(m) = m^e \bmod n\right].$$

Teorema 3.1. *La función* $\mathrm{RSA}_{n,e}$ *es biyectiva con inversa* $\mathrm{RSA}_{n,e}^{-1} = \mathrm{RSA}_{n,d}$.

Demostración. Por la simetría de la construcción, basta comprobar que $m = \mathrm{RSA}_{n,d}(\mathrm{RSA}_{n,e}(m)) = m^{ed} \mod n$ para cualquier $m \in \mathbb{Z}_n$. Sea

$$\begin{aligned} \chi : \mathbb{Z}_n &\to \mathbb{Z}_p \times \mathbb{Z}_q \\ x &\mapsto (x \bmod p, x \bmod q) \end{aligned} \tag{3.1}$$

el isomorfismo de anillos canónico dado por el Teorema Chino del Resto (CRT). Sea $m \in \mathbb{Z}_n$, entonces

$$\chi(m)^{ed} = (m^{ed} \bmod p, m^{ed} \bmod q).$$

Dado que

$$ed = 1 + t\varphi(n) = 1 + t(p-1)(q-1),$$

si $(m, p) = 1$, se deduce del Teorema Pequeño de Fermat que

$$m^{ed} = m(m^{p-1})^{t(q-1)} \equiv m \mod p,$$

y si $m = ap$, obviamente $m^{ed} \equiv m \mod p$, de donde

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

para cualquier $m \in \mathbb{Z}_n$. Análogamente

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

para cualquier $m \in \mathbb{Z}_n$, por lo que concluimos que

$$\chi(m)^{ed} = \chi(m)$$

para todo $m \in \mathbb{Z}_n$. Como χ es isomorfismo de anillos, tenemos que

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

para todo $m \in \mathbb{Z}_n$. □

Por la Proposición 1.8, la función $RSA_{n,e}$ es una función rápida de calcular. Concretamente, el cálculo

$$m^e \bmod n$$

está en $\mathcal{O}\left((\log n)^3\right)$, ya que $\varphi(n) < n$.

El Teorema 3.1 nos dice que, conocido d, $\mathrm{RSA}_{n,e}^{-1}$ también es fácil de calcular. No hay publicados algoritmos de complejidad polinomial para el cálculo de $\mathrm{RSA}_{n,e}^{-1}(m) = \sqrt[e]{m} \bmod n$ sin el conocimiento de d.

Por la Proposición 1.7, es computacionalmente eficiente conocer d si se conoce $\varphi(n)$, concretamente, dicho cálculo es también $\mathcal{O}\left((\log n)^3\right)$.

Proposición 3.2. *Supongamos que es sabido que n es el producto de dos primos p, q. Dados p, q podemos calcular $\varphi(n)$ en $\mathcal{O}(\log n)$ operaciones. Dados n y $\varphi(n)$, se pueden calcular p, q en $\mathcal{O}\left((\log n)^2\right)$ operaciones.*

Demostración. Dado que $\varphi(n) = (p-1)(q-1) = n+1-(p+q)$, calcular $\varphi(n)$ requiere una suma y una resta, por tanto estamos en $\mathcal{O}(\log n)$.

Supongamos que conocemos n y $\varphi(n)$. Podemos suponer que n es impar, pues el caso par es trivial. Como

$$\begin{aligned}(x-p)(x-q) &= x^2-(p+q)x+pq\\ &= x^2-(n+1-\varphi(n))x-n,\end{aligned}$$

tenemos que p y q son raíces del polinomio anterior, es decir, $p, q = b \pm \sqrt{b^2-n}$, donde $p+q = 2b$. Como el cálculo de raíces cuadradas es $\mathcal{O}\left(\left(\log(b^2-n)\right)^2\right) = \mathcal{O}\left((\log n)^2\right)$, tenemos el resultado. □

Ejemplo 3.3. Vamos a descomponer $n = 1189$ sabiendo que $\varphi(n) = 1120$. Tenemos que $2b = p+q = n+1-\varphi(n) = 1189+1-1120 = 70$, luego $b \pm \sqrt{b^2-n} = 35 \pm \sqrt{35^2-1189} = 35 \pm \sqrt{1225-1189} = 35 \pm \sqrt{36} = 35 \pm 6 = 41,\ 29$.

Computacionalmente, calcular $\varphi(n)$ y factorizar n son problemas equivalentes. ¿Es la ruptura de RSA equivalente a factorizar n? Es decir, ¿hay algún algoritmo polinomial que permita calcular un factor de n si somos capaces de calcular $\mathrm{RSA}_{n,e}^{-1}$? No conocemos una respuesta a dicha pregunta, pero podemos dar resultados parciales. Por ejemplo, una forma de romper RSA sin factorizar n pasa por calcular d tal que

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

para cualquier $m \in \mathbb{Z}_n$ primo con n. Vía el isomorfismo χ en (3.1), tenemos que $k = ed - 1$ es múltiplo de $[p-1, q-1]$. Supongamos que conocemos k tal que $a^k \equiv 1 \mod n$ para cualquier a primo con n. En particular k es par porque $(-1)^k \equiv 1 \mod n$.

Lema 3.4. *Supongamos que existe* $a_0 \in \mathcal{U}(\mathbb{Z}_n)$ *tal que* $a_0^{k/2} \not\equiv 1 \mod n$. *Entonces*

$$\left|\left\{a \in \mathcal{U}(\mathbb{Z}_n) \mid a^{k/2} \not\equiv 1 \mod n\right\}\right| \geq \frac{\varphi(n)}{2}.$$

Demostración. Sean

$$A_+ = \{a \in \mathcal{U}(\mathbb{Z}_n) \mid a^{k/2} \equiv 1 \mod n\}$$
$$A_- = \{a \in \mathcal{U}(\mathbb{Z}_n) \mid a^{k/2} \not\equiv 1 \mod n\}$$

Tenemos que $a_0 \in A_-$. La aplicación

$$a_0 \cdot : \mathcal{U}(\mathbb{Z}_n) \to \mathcal{U}(\mathbb{Z}_n)$$

es una biyección que satisface

$$a_0 A_+ \subseteq A_-,$$

por lo que $|A_+| \leq |A_-|$. Como $\mathcal{U}(\mathbb{Z}_n) = A_+ \cup A_-$ siendo la unión disjunta, tenemos

$$\varphi(n) = |\mathcal{U}(\mathbb{Z}_n)| = |A_+| + |A_-| \leq 2|A_-|,$$

lo que implica $|A_-| \geq \frac{\varphi(n)}{2}$. □

Por tanto, calculando $a^{k/2} \bmod n$ para suficientes $a \in \mathcal{U}(\mathbb{Z}_n)$, podemos comprobar que $A_- \neq \varnothing$ o afirmar con probabilidad tan alta como queramos que $a^{k/2} \equiv 1 \mod n$ para todo $a \in \mathcal{U}(\mathbb{Z}_n)$. En este último caso reemplazamos k por $k/2$ y volvemos a empezar.

Tras los reemplazos necesarios, podemos suponer que $A_- \neq \varnothing$, es decir,

$$\forall a \in \mathcal{U}(\mathbb{Z}_n), \quad a^k \equiv 1 \mod n$$

y

$$\exists a_0 \in \mathcal{U}(\mathbb{Z}_n), \quad a_0^{k/2} \not\equiv 1 \mod n.$$

Tenemos dos posibilidades

(I) $\frac{k}{2}$ es múltiplo de $p-1$ o $q-1$ pero no de ambos, pongamos $p-1$. En este caso $a^{k/2} \equiv 1 \mod p$ para todo $a \in \mathcal{U}(\mathbb{Z}_n)$ y existe $a_0 \in \mathcal{U}(\mathbb{Z}_n)$ tal que

$$a_0^{k/2} \not\equiv 1 \mod n$$

o, equivalentemente,

$$a_0^{k/2} \equiv -1 \mod q.$$

Usando (3.1), la multiplicación

$$a_0 \cdot : \mathcal{U}(\mathbb{Z}_n) \to \mathcal{U}(\mathbb{Z}_n)$$

es una biyección que satisface

$$a_0 \left\{ a \in \mathcal{U}(\mathbb{Z}_n) \mid a^{k/2} \equiv 1 \mod q \right\} = \left\{ a \in \mathcal{U}(\mathbb{Z}_n) \mid a^{k/2} \equiv -1 \mod q \right\}.$$

En consecuencia

$$\left| \left\{ a \in \mathcal{U}(\mathbb{Z}_n) \mid a^{k/2} \equiv -1 \mod q \right\} \right| = \frac{\varphi(n)}{2}.$$

(II) $\frac{k}{2}$ no es múltiplo de $p-1$ ni $q-1$. Sean

$$A_{\pm\pm} = \{ a \in \mathcal{U}(\mathbb{Z}_n) \mid a^{k/2} \equiv \pm 1 \mod p, \; a^{k/2} \equiv \pm 1 \mod q \}.$$

Como $p-1 \nmid \frac{k}{2}$, existe $a_0 \in \mathcal{U}(\mathbb{Z}_n)$ tal que

$$a_0^{k/2} \equiv -1 \mod p.$$

Reemplazando eventualmente a_0 por la solución del sistema

$$\begin{aligned} x &\equiv a_0 \mod p \\ x &\equiv 1 \mod q \end{aligned}$$

podemos suponer que

$$a_0^{k/2} \equiv 1 \mod q.$$

Análogamente, existe $a_1 \in \mathcal{U}(\mathbb{Z}_n)$ tal que

$$a_1^{k/2} \equiv -1 \mod q \quad \text{y} \quad a_1^{k/2} \equiv 1 \mod p.$$

Las aplicaciones $a_0\cdot, a_1\cdot : \mathcal{U}(\mathbb{Z}_n) \to \mathcal{U}(\mathbb{Z}_n)$ son biyectivas. Dado que $a_0 A_{++} = A_{-+}$, $a_0 A_{--} = A_{+-}$, $a_1 A_{++} = A_{+-}$ y $a_1 A_{--} = A_{-+}$, tenemos que

$$|A_{++}| = |A_{+-}| = |A_{-+}| = |A_{--}|,$$

lo que implica

$$|A_{+-} \cup A_{-+}| = \frac{\varphi(n)}{2}.$$

En cualquiera de las dos posibilidades, encontramos con probabilidad $\frac{1}{2}$ un $a \in \mathbb{Z}_n$ tal que

$$a^{k/2} \equiv 1 \mod p \quad \text{y} \quad a^{k/2} \equiv -1 \mod q$$

o

$$a^{k/2} \equiv -1 \mod p \quad \text{y} \quad a^{k/2} \equiv 1 \mod q.$$

En este caso $\left(a^{k/2} - 1, n\right)$ es un factor propio de n. En consecuencia, si fuésemos capaces de calcular d tal que

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

para cualquier $m \in \mathbb{Z}_n$ primo con n, podríamos factorizar n con probabilidad tan alta como quisiéramos. Por este motivo se asume que el coste de calcular $\mathrm{RSA}_{n,e}^{-1}$ es equivalente al coste de descomponer $n = pq$.

Ejemplo 3.5. Consideremos la clave pública $(n, e) = (1189, 257)$. Si $d = 353$, podemos encontrar una descomposición de n. Para ello, llamemos $k = ed - 1 = 90720$.

Probamos distintos valores $a \in \mathbb{Z}_{1189}$. Primero comprobamos si $(a, n) = 1$, ya que en caso contrario habríamos hallado un factor de n. Para los valores de n empleados en RSA, la probabilidad de hallar un a no primo con n es tan baja que podemos suponer que nunca lo encontraremos. Como siguiente paso comprobamos que

$$a^{90720} \equiv 1 \mod 1189$$

para $a = 2, 3, 5, 7, 11, 13, 17, 19$. Este paso se realiza en la práctica tomando valores aleatorios de a, pero en este ejemplo vamos a probar con dichos para simplificar los cálculos. Si hubiese un valor a_0 tal que $a_0^{90720} \not\equiv 1 \mod 1189$, habríamos observado un suceso con probabilidad $\frac{1}{2^8} \approx 0{,}004$, por lo que suponemos que no existe dicho a_0.

Reemplazamos k por $k/2 = 45360$ y repetimos el proceso. Volvemos a encontrar que

$$a^{45360} \equiv 1 \mod 1189$$

para $a = 2, 3, 5, 7, 11, 13, 17, 19$, con lo que suponemos de nuevo que $a^{45360} \equiv 1 \mod 1189$ para cualquier a primo con n.

Reemplazamos k por $k/2 = 22680$ y repetimos el proceso. Una vez más

$$a^{22680} \equiv 1 \mod 1189$$

para $a = 2, 3, 5, 7, 11, 13, 17, 19$, con lo que volvemos a asumir que $a^{22680} \equiv 1 \mod 1189$ para cualquier a primo con n.

Reemplazamos k por $k/2 = 11340$ y repetimos el proceso. En este caso tenemos que

$$3^{11340} \equiv 204 \mod 1189.$$

Calculamos $\left(1189, (3^{11340} - 1) \bmod 1189\right) = 29$, lo que nos da un factor de 1189.

3.2

Descripción de RSA

Generación de claves. Para generar su pareja de claves, Alicia realiza los siguientes pasos.

(I) Selecciona aleatoriamente dos primos p_A, q_A de tamaño adecuado. Cada primo lo selecciona de la siguiente forma. Para un primo de b bits seleccionamos aleatoriamente $b-2$ bits, agregamos al principio y al final dos 1 para garantizar que tenemos un número impar de exactamente b bits. Le aplicamos un test de primalidad. Si el resultado es positivo, ya tenemos el primo, En caso contrario sumamos 2 al número obtenido y repetimos el proceso.

(II) Calcula $n_A = p_A q_A$ y $\varphi(n_A) = n_A + 1 - (p_A + q_A)$.

(III) Elige un e_A primo con $\varphi(n_A)$. Esta elección puede hacerse de muchas formas. Una de ellas es proceder de forma análoga a la elección de p_A y q_A, generando aleatoriamente un número impar y comprobando si es primo con $\varphi(n_A)$. Otra forma es elegir un primo entre $\max\{p_A, q_A\}$ y $\varphi(n_A)$, lo que garantiza que será primo con $\varphi(n_A)$.

(IV) Calcula $d_A = e_A^{-1} \bmod \varphi(n_A)$.

(V) La clave pública es la pareja (n_A, e_A).

(VI) La clave privada es (p_A, q_A, d_A).

Función de cifrado. La función de cifrado es

$$\mathrm{RSA}_{n_A,e_A}(m) = m^{e_A} \bmod n_A.$$

La elección de e_A puede acelerar la función de cifrado. Por ejemplo, si $e_A = 65537 = 2^{2^4}+1$, para cifrar hay que realizar 17 multiplicaciones módulo n_A. Consecuentemente, RSA_{n_A,e_A} está en $\mathcal{O}\left((\log n_A)^2\right)$, eliminando el factor $\log e_A$ que aparece en la Proposición 1.8. Otras elecciones como $e_A = 3 = 2^{2^0}+1$, $e_A = 5 = 2^{2^1}+1$ o $e_A = 17 = 2^{2^2}+1$, que también dan implementaciones eficientes, pueden acarrear problemas de seguridad. Para que el cifrado sea eficiente, números de la forma $2^{2^\alpha}+1$ son buenas elecciones, pero no son necesariamente primos si $\alpha \geq 5$.

Función de descifrado. La función de descifrado es

$$\mathrm{RSA}^{-1}_{n_A,e_A}(c) = c^{d_A} \bmod n_A.$$

El Teorema 3.1 garantiza que la función anterior es efectivamente la función de descifrado. Por la Proposición 1.8,

$$\mathrm{RSA}^{-1}_{n_A,e_A} = \mathcal{O}\left((\log n_A)^2(\log d_A)\right).$$

El isomorfismo χ de (3.1), permite acelerar el proceso de descifrado, concretamente,

$$\mathrm{RSA}^{-1}_{n_A,e_A}(c) = \mathrm{RSA}_{n_A,d_A}(c) = \chi^{-1}\left(c^{d_A \bmod (p_A-1)} \bmod p_A, c^{d_A \bmod (q_A-1)} \bmod q_A\right).$$

Aunque la complejidad algorítmica no se ve reducida, en la práctica el tamaño de p_A y q_A es la mitad de n_A, y lo mismo podemos decir de $d_A \bmod p_A - 1$ y $d_A \bmod q_A - 1$ con respecto a d_A, con lo que se suele reducir el tiempo empleado en el descifrado.

Ejemplo 3.6. $p = 31, q = 17, n = 527, \varphi(n) = 480, e = 17, d = 113$. Supongamos que $m = 130$.

$$\begin{aligned} c &= \mathrm{RSA}_{527,17}(130) \\ &= \left(\left((130^2)^2\right)^2\right)^2 130 \bmod 527 \\ &= \left((36^2)^2\right)^2 130 \bmod 527 \\ &= (242^2)^2 130 \bmod 527 \\ &= 67^2 130 \bmod 527 = 273 \cdot 130 \bmod 527 \\ &= 181. \end{aligned}$$

Para descifrar c,

$$
\begin{aligned}
&\mathrm{RSA}_{527,17}^{-1}(c) = \mathrm{RSA}_{527,113}(181) = 181^{113} \bmod 527 \\
&= \left(\left(\left(\left((181^2 181)^2 181\right)^2\right)^2\right)^2\right)^2 181 \bmod 527 \\
&= \left(\left(\left(\left((87 \cdot 181)^2 181\right)^2\right)^2\right)^2\right)^2 181 \bmod 527 \\
&= \left(\left(\left((280^2 181)^2\right)^2\right)^2\right)^2 181 \bmod 527 \\
&= \left(\left(\left((404 \cdot 181)^2\right)^2\right)^2\right)^2 181 \bmod 527 \\
&= \left(\left((398^2)^2\right)^2\right)^2 181 \\
&= \left((304^2)^2\right)^2 181 \bmod 527 \\
&= (191^2)^2 181 = 118^2 181 \bmod 527 \\
&= 222 \cdot 181 \bmod 527 = 130.
\end{aligned}
$$

Para el descifrado acelerado,

$$\begin{aligned} c^{d \bmod p-1} \bmod p &= 181^{113 \bmod 30} \bmod 31 = 26^{23} \bmod 31 \\ &= \left(\left((26^2)^2 26\right)^2 26\right)^2 26 \bmod 31 \\ &= \left((25^2 26)^2 26\right)^2 26 \bmod 31 \\ &= \left((5 \cdot 26)^2 26\right)^2 26 \bmod 31 \\ &= (6^2 26)^2 26 \bmod 31 = (5 \cdot 26)^2 26 \bmod 31 \\ &= 6^2 26 \bmod 315 \cdot 26 \bmod 31 = 6. \end{aligned}$$

y

$$c^{d \bmod q-1} \bmod q = 181^{113 \bmod 16} \bmod 17 = 11^1 \bmod 17 = 11,$$

por tanto

$$m = \chi^{-1}(6, 11) = 130.$$

3.3 Ataques

Ataque del módulo común. Supongamos que tenemos dos claves públicas con el mismo módulo, (n, e_1) y (n, e_2), tales que $(e_1, e_2) = 1$. Supongamos que $re_1 + se_2 = 1$ con $r < 0 < s$. Sea

$$c_i = m^{e_i} \bmod n$$

para $i = 1, 2$. Si $(c_1, n) \neq 1$, podemos factorizar n y romper la clave, por lo que podemos suponer que $c_1 \in \mathcal{U}(\mathbb{Z}_n)$. Calculamos c_1^{-1} con el algoritmo extendido de Euclides. Tenemos

$$(c_1^{-1})^{-r} c_2^s \equiv (m^{e_1})^r (m^{e_2})^s \equiv m^{e_1 r + e_2 s} = m \mod n,$$

por lo que averiguamos el mensaje.

Por otra parte, si las claves públicas con el mismo módulo se corresponden con dos usuarios distintos, cada uno de ellos puede calcular la clave privada del otro al conocer la factorización del módulo.

Ejemplo 3.7. $n = 1537$, $e_1 = 17$, $e_2 = 37$, $c_1 = 1298$, $c_2 = 614$. Calculamos r, s,

$$1 = re_1 + se_2 = (-13)17 + 6 \cdot 37.$$

Así,

$$\begin{aligned}(c_1^{-1})^{-r} c_2^s &= (1298^{-1})^{13} (614)^6 \equiv 1164^{13} 614^6 \mod 1537 \\ &\equiv 341 \cdot 661 \mod 1537 \equiv 999 \mod 1537\end{aligned}$$

Ataque del exponente de cifrado bajo. Enviamos el mismo mensaje m a varios receptores, con claves públicas (n_i, e), con $1 \leq i \leq r$. Supondremos que $(n_i, n_j) = 1$ si $i \neq j$, pues en otro caso podríamos factorizar el módulo correspondiente mediante el cálculo del máximo común divisor. Llamamos $c_i = m^e \bmod n_i$ para cada $1 \leq i \leq r$. Supongamos que $e \leq r$. Seleccionamos $\{i_1, \ldots, i_e\} \subseteq \{1, \ldots, r\}$

Empleando el inverso del isomorfismo de anillos

$$\chi : \mathbb{Z}_{n_{i_1} \cdots n_{i_e}} \to \mathbb{Z}_{n_{i_1}} \times \cdots \times \mathbb{Z}_{n_{i_e}}$$

dado por el Teorema Chino del Resto, podemos calcular

$$\chi^{-1}(c_{i_1}, \ldots, c_{i_e}) = m^e \bmod n_{i_1} \cdots n_{i_e},$$

Dado que $m^e < n_{i_1} \cdots n_{i_e}$, podemos calcular m calculando la raíz e–ésima en $\mathbb{Z} \subseteq \mathbb{R}$, que se puede hacer eficientemente mediante métodos numéricos, siempre que e sea pequeño.

Ejemplo 3.8. Supongamos que tenemos las claves públicas $(n_1, e) = (731, 3)$, $(n_2, e) = (943, 3)$ y $(n_3, e) = (611, 3)$. Ciframos un mismo mensaje y obtenemos los criptogramas $c_1 = 505$, $c_2 = 876$ y $c_3 = 372$. La solución del sistema de congruencias

$$\begin{aligned} x &\equiv 505 \mod 731 \\ x &\equiv 876 \mod 943 \\ x &\equiv 372 \mod 611 \end{aligned}$$

es $x = 124251499$, cuya raíz cúbica es $m = 499$.

Ataque del criptograma elegido. Supongamos que Bob tiene como clave pública la pareja (n, e). Se cifra un mensaje m como $c = \mathrm{RSA}_{n,e}(m) = m^e \bmod n$. La atacante Eve[1] elige aleatoriamente $r \in \mathcal{U}(\mathbb{Z}_n)$ y solicita el descifrado del mensaje

$$\mathrm{RSA}_{n,e}^{-1}(r^e c \bmod n) = rm \bmod n.$$

El aspecto de $r^e c \bmod n$ es aleatorio y no parece tener que ver con c. Finalmente,

$$m \equiv r^{-1}(rm) \mod n,$$

[1] Suele emplearse este nombre por la similitud con *eavesdrop*, palabra inglesa cuyo significado es escuchar a escondidas.

por lo que se recupera el mensaje.

Ejemplo 3.9. Ciframos un mensaje con la clave pública $(n, e) = (989, 17)$, obteniendo el criptograma $c = 256$. Aleatoriamente $r = 357$, con lo que $r^e c \bmod n = 855$. El descifrado que pedimos es

$$\mathrm{RSA}^{-1}_{989,17}(855) = 315.$$

Finalmente, $m = 315 \cdot 357^{-1} \bmod 989 = 699$.

Ataque con primos muy próximos (Factorización de Fermat). Si $n = pq$ con $p > q$, entonces

$$n = \left(\tfrac{p+q}{2}\right)^2 - \left(\tfrac{p-q}{2}\right)^2.$$

Si p y q son cercanos, $s = \frac{p-q}{2}$ es pequeño y $t = \frac{p+q}{2}$ es un entero ligeramente mayor que $\sqrt{n}$ tal que $t^2 - n$ es un cuadrado perfecto. Probando sucesivamente con valores mayores que $\sqrt{n}$ hasta encontrar una descomposición $n = t^2 - s^2$, tenemos que $p = t + s$ y $q = t - s$.

Ejemplo 3.10. Calculamos la descomposición como producto de primos de 1591. Como $\sqrt{1591} \approx 39{,}89$ empezamos con $t = 40$.

t	$t^2 - n$
40	$9 = 3^2$

Por tanto $p = 40 + 3 = 43$ y $q = 40 - 3 = 37$

Congruencia de Legendre. La factorización de Fermat puede verse como un caso particular de una familia de algoritmos de factorización basados en una congruencia estudiada por Legendre.

Proposición 3.11. *Sea n un entero impar. Para cada y primo con n, la congruencia*

$$x^2 \equiv y^2 \mod n \tag{3.2}$$

tiene más de dos soluciones si y sólo si n es compuesto.

Demostración. Observemos que siempre hay al menos dos soluciones,

$$x \equiv \pm y \mod n.$$

Si n es primo, éstas son las únicas, pues un polinomio de grado dos tiene a lo sumo dos raíces. Supongamos que n es compuesto, por lo que podemos asumir $n = n_1 n_2$ con $(n_1, n_2) = 1$ y ambos no unidades. Tenemos cuatro sistemas de ecuaciones

$$\begin{cases} x \equiv \pm y \mod n_1 \\ x \equiv \pm y \mod n_2 \end{cases}$$

que, por el Teorema Chino del Resto, dan lugar a soluciones de (3.2). Sea z una solución del sistema

$$\begin{cases} x \equiv y \mod n_1 \\ x \equiv -y \mod n_2 \end{cases}$$

Si $z = y$, entonces

$$2y \equiv 0 \mod n_2.$$

Como n es impar, y por tanto n_2, necesariamente

$$y \equiv 0 \mod n_2,$$

lo que implica que n_2 es un factor común a n e y, en contradicción con la hipótesis de que y es primo con n. Por tanto $z \neq y$, y análogamente se comprueba que $z \neq -y$. Luego hemos encontrado una nueva solución a (3.2). □

La ecuación (3.2) se emplea para dar algoritmos de factorización buscando soluciones no triviales. De hecho, si z es una solución no trivial tenemos que

$$(z+y)(z-y) = z^2 + y^2 \equiv 0 \mod n,$$

de donde

$$(z+y, n), (z-y, n)$$

van a proporcionar factores no triviales. Otro algoritmo clásico que utiliza esta idea es la criba cuadrática. Para ello necesitamos introducir algunos conceptos y algoritmos.

Raíces cuadradas. Dado un primo p, queremos dar un algoritmo que decida si $\left(\frac{\beta}{p}\right) = 1$ y, en dicho caso, calcular las dos raíces cuadradas de β módulo p.

Lema 3.12 (Criterio de Euler). *$\beta \in \mathbb{F}_p^*$ es residuo cuadrático si y solo si $\beta^{\frac{p-1}{2}} \equiv 1 \mod p$.*

Demostración. Si $\beta = \gamma^2$, entonces $\beta^{(p-1)/2} = \gamma^{p-1} \equiv 1 \mod p$ por el Teorema pequeño de Fermat.

Recíprocamente, supongamos que $\beta^{(p-1)/2} \equiv 1 \mod p$. Sea $g \in \mathbb{F}_p$ un elemento primitivo tal que $\beta = g^j$. Si j es impar tenemos que

$d = (j(p-1)/2, p-1)$ es un divisor propio de $p-1$, y como

$$1 \equiv (g^j)^{(p-1)/2} = g^{j(p-1)/2} \mod p,$$

tenemos que $g^d \equiv 1 \mod p$, por lo que g no puede ser primitivo. Por tanto j es par y β es un residuo cuadrático. □

Una vez que tenemos un procedimiento rápido para saber si un elemento dado tiene raíz cuadrada podemos calcular dicha raíz mediante el Algoritmo 1.

Veamos el porqué de su correcto funcionamiento. Si $\beta \in \mathbb{F}_p$ es un residuo cuadrático y $p \equiv 3 \mod 4$, entonces $\left(\beta^{\frac{p+1}{4}}\right)^2 = \beta^{\frac{p+1}{2}} = \beta\beta^{\frac{p+1}{2}-1} = \beta\beta^{\frac{p-1}{2}} \equiv \beta \mod p$, por lo que $\pm\beta^{(p+1)/4} \bmod p$ son sus dos raíces cuadradas.

Nos queda el caso $p \equiv 1 \mod 4$, en el que $\frac{p-1}{2}$ es par. Sea $\gamma \in \mathbb{F}_p$ un elemento no residuo cuadrático, es decir, satisface $\gamma^{(p-1)/2} \equiv -1 \bmod p$, que puede ser encontrado por una búsqueda aleatoria. Sean r impar y $l \geq 1$ tales que $\frac{p-1}{2} = 2^l r$. Sea, además, $s_0 = 0$. Tenemos que

$$\beta^{2^{l-1}r}\gamma^{s_0} = \beta^{(p-1)/2}\gamma^0 \equiv 1 \mod p.$$

Supongamos que hemos calculado s_{i-1} tal que $2^{l-i+2} \mid s_{i-1}$ y

$$\beta^{2^{l-i+1}r}\gamma^{s_{i-1}} \equiv 1 \mod p.$$

Sea $y_i = \beta^{2^{l-i}r}\gamma^{s_{i-1}/2} \bmod p$. Por nuestra hipótesis $y_i^2 \equiv 1 \mod p$, por lo que $y_i \equiv \pm 1 \mod p$. Si $y_i \equiv 1 \mod p$, llamamos $s_i = \frac{s_{i-1}}{2}$, por lo que $2^{l-i+1} \mid s_i$ y

$$\beta^{2^{l-i}r}\gamma^{s_i} = \beta^{2^{l-i}r}\gamma^{s_{i-1}/2} \equiv y_i \equiv 1 \bmod p.$$

Algorithm 1 Raíces cuadradas módulo p

Input: p primo impar y β

Output: Las dos raíces cuadradas de β módulo p, si existen.

if $\beta^{\frac{p-1}{2}} \equiv 1 \mod p$ **then**
  if $p \equiv 3 \mod 4$ **then**
    return $\pm\beta^{\frac{p+1}{4}} \mod p$
  else
    $\{p \equiv 1 \mod 4\}$
    Sea γ tal que $\gamma^{\frac{p-1}{2}} \equiv -1 \mod p$ {búsqueda aleatoria}
    Descomponemos $\frac{p-1}{2} = 2^l r$ con r impar.
    Sea $s_0 = 0$.
    for $1 \leq i \leq l$ **do**
      $y_i = \beta^{2^{l-i}} \gamma^{\frac{s_{i-1}}{2}} \mod p$
      if $y_i \equiv 1 \mod p$ **then**
        $s_i = \frac{s_{i-1}}{2}$
      else
        $s_i = \frac{s_{i-1}}{2} + \frac{p-1}{2}$
    return $\pm\beta^{\frac{r+1}{2}} \gamma^{\frac{s_l}{2}} \mod p$
else
  return β no es un residuo cuadrático.

Si $y_i \equiv -1 \mod p$, llamamos $s_i = \frac{s_{i-1}}{2} + \frac{p-1}{2}$. Dado que $2^l \mid \frac{p-1}{2}$ tenemos que $2^{l-i+1} \mid s_i$. Además

$$\begin{aligned}\beta^{2^{l-i}r}\gamma^{s_i} &= \beta^{2^{l-i}r}\gamma^{s_{i-1}/2}\gamma^{(p-1)/2} \\ &\equiv y_i\gamma^{(p-1)/2} \equiv (-1)(-1) = 1 \mod p.\end{aligned}$$

En ambos casos, hemos encontrado s_i tal que $2^{l-i+1} \mid s_i$ y

$$\beta^{2^{l-i}r}\gamma^{s_i} \equiv 1 \mod p.$$

Después de l pasos, llegamos a $s = s_l$ tal que $2 = 2^{l-l+1} \mid s_l$ y

$$\beta^r\gamma^s = \beta^{2^{l-l}r}\gamma^{s_l} \equiv 1 \mod p.$$

Por tanto,

$$\left(\beta^{\frac{r+1}{2}}\gamma^{\frac{s}{2}}\right)^2 = \beta^{r+1}\gamma^s \equiv \beta \mod p,$$

lo que nos da una raíz cuadrada de β.

Criba cuadrática. La idea de la criba cuadrática consiste en encontrar suficientes parejas (x_i, y_i) tales que $x_i^2 \equiv y_i \mod n$ y $\prod_i y_i = z^2$ es un cuadrado perfecto. De esta forma,

$$x^2 = \prod_i x_i^2 \equiv \prod_i y_i = z^2 \mod n,$$

lo que daría una solución no trivial de (3.2). El primer problema consiste en determinar que $\prod_i y_i$ es un cuadrado perfecto y calcular su raíz cuadrada. Esta tarea es más sencilla si dichos números satisfacen la siguiente definición.

Definición 3.13. sea $B \in \mathbb{Z}^+$ un entero positivo. Se dice que $m \in \mathbb{Z}$ es B-suave si $p \mid m$ con p primo implica $p \leq B$.

Un entero B-suave, puede escribirse como

$$p_1^{e_1} p_2^{e_2} \cdots p_{\pi(B)}^{e_{\pi(B)}},$$

donde $p_{\pi(B)}$ es el mayor primo por debajo de B, y es un cuadrado perfecto si y sólo si $e_1, \ldots, e_{\pi(B)}$ son pares, lo que permite calcular con facilidad su raíz cuadrada.

El siguiente Lema permite garantizar cómo calcular dichos elementos.

Lema 3.14. *Sean $y_1, \ldots, y_{\pi(B)+1}$ enteros B-suaves. Existe un subconjunto $\{y_{i_1}, \ldots, y_{i_k}\}$ de ellos tal que $\prod_{j=1}^{k} y_{i_j}$ es un cuadrado perfecto.*

Demostración. Este esquema de la demostración indica además cómo calcular los elementos $\{y_{i_1}, \ldots, y_{i_k}\}$. Observemos que la multiplicación se convierte en suma de los exponentes. Trabajando con los exponentes módulo 2, tenemos que encontrar una combinación lineal de los vectores asociados a los exponentes que nos de el vector cero, lo que equivale a exponentes pares. Dado que tenemos más vectores que dimensión, dicha combinación lineal siempre existe. □

Para proseguir con la búsqueda, observemos que encontrar $x^2 \bmod n$ es equivalente a encontrarlo en el rango $\sqrt{n} < x < \sqrt{2n}$. Observemos, además, que $p \mid x^2 - n$ si y sólo si n es un residuo cuadrático módulo p. Por tanto, para buscar elementos tales que $x^2 - n$ es B-suave basta con seleccionar de aquellos primos menores o iguales que B aquellos para los que n es un residuo cuadrático. Dado que no perdemos generalidad con suponer que $p \nmid n$, pues en ese caso habríamos

encontrado un factor, tenemos que las raíces cuadradas de n módulo p no son cero.

Dado un intervalo $[a, b]$, el primer entero contenido en el mismo congruente con 0 módulo p es $\left\lceil \frac{a}{p} \right\rceil p$. Sean $\pm s$ las dos raíces cuadradas de n módulo p, que pueden ser calculadas mediante el Algoritmo 1. Todos los elementos x tales que $x^2 - n$ son divisibles por p están, por tanto, en el conjunto

$$C_{a,b,p} = \left\{ \left\lceil \frac{a}{p} \right\rceil p - s, \left\lceil \frac{a}{p} \right\rceil p + s, \left\lceil \frac{a}{p} \right\rceil p - s + p, \left\lceil \frac{a}{p} \right\rceil p + s + p, \right.$$
$$\left\lceil \frac{a}{p} \right\rceil p - s + 2p, \left\lceil \frac{a}{p} \right\rceil p + s + 2p,$$
$$\left. \left\lceil \frac{a}{p} \right\rceil p - s + 3p, \left\lceil \frac{a}{p} \right\rceil p + s + 3p, \ldots \right\} \subseteq [a, b].$$

Estas ideas se resumen en el Algoritmo 2.

Ejemplo 3.15. Vamos a utilizar la criba cuadrática para descomponer $n = 105481$. Partimos de un valor $B = 15$, lo que nos da como posibles primos $\{2, 3, 5, 7, 11, 13\}$. Estudiamos para cuáles de ellos n es residuo cuadrático. Aplicamos el Algoritmo 1, aunque los casos $2, 3, 5$ son triviales dado que

$$n \equiv 1 \mod 2, 3, 5$$

por lo que es obviamente residuo cuadrático con raíz cuadrada 1. Como

$$n^3 \equiv 6 \mod 7$$

y

$$n^5 \equiv 10 \mod 11$$

Algorithm 2 Criba cuadrática

(1) Fijamos un entero B. Para cada primo $p \leq B$ comprobamos si $\left(\frac{n}{p}\right) = 1$, en cuyo caso calculamos s tal que $s^2 \equiv n \mod p$. Guardamos la lista $\{(2,1),(p_2,s_2),\dots(p_m,s_m)\}$ obtenida.

(2) Calculamos $C = \bigcup_{j=1}^{m} C_{\sqrt{n},\sqrt{2n},p_j}$.

(3) Tomamos $x_1,\dots,x_{m+1} \in C$ tales que $y_i = x_i^2 - n$ es B-suave. Calculamos $e_{i1},\dots,e_{im}$ tales que $y_i = \prod_{j=1}^{m} p_j^{e_{ij}}$.

(4) Mediante el Lema 3.14, calculamos $\{y_{i_1},\dots,y_{i_k}\}$ tales que $\prod_{j=1}^{k} y_{i_j}$ es un cuadrado perfecto, y calculamos su raíz y.

(5) Si $x = x_{i_1}\cdots x_{i_k}$, devolvemos $(x-y,n)$.

para ninguno de ellos es residuo cuadrático. Finalmente

$$n^6 \equiv 1 \mod 13$$

n sí es un residuo cuadrático módulo 13, además, dado que $13 \equiv 1 \mod 4$ tenemos que aplicar la segunda parte del algoritmo de cálculo de raíces cuadradas. Seleccionamos $\gamma = 11$, y calculamos $l = 1, r = 3$. Tenemos que

$$y_1 = n^3 \equiv 12 \mod 13,$$

por lo que $s_1 = 6$. Una raíz cuadrada de n es, por tanto

$$n^2\gamma^3 \mod 13,$$

es decir,

$$105481^2 11^3 \equiv 5 \mod 13.$$

Tras esta parte, tenemos

$$S = \{(2,1),(3,1),(5,1),(13,5)\}.$$

Tras el cribado, el conjunto C calculado tiene 128 elementos, entre los que buscamos las parejas x_i, y_i. Dichas parejas son

x_i	y_i
325	$2^4 \times 3^2$
333	$2^5 \times 13^2$
334	$3^5 \times 5^2$
341	$2^4 \times 3^3 \times 5^2$
343	$2^3 \times 3^2 \times 13^2$
359	$2^3 \times 3^2 \times 5^2 \times 13$
395	$2^4 \times 3^5 \times 13$

La aplicación del Lema 3.14 nos lleva a buscar combinaciones lineales de las filas de la matriz

$$\begin{pmatrix} 0 & 0 & 0 & 0 \\ 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 1 & 0 & 0 & 0 \\ 1 & 0 & 0 & 1 \\ 0 & 1 & 0 & 1 \end{pmatrix}$$

que den cero. La primera fila ya es de dicho tipo, lo que nos da $x = 325$, $y = 2^2 \times 3$. De hecho

$$\left(n, 325 - 2^2 3\right) = 313.$$

Otra posible opción sería tomar $x_{i_1} = 333$, $y_{i_1} = 2^5 \times 13^2$ y $x_{i_2} = 343$, $y_{i_2} = 2^3 \times 3^2 12^2$, lo que nos da $x = 333 \times 343$ e $y = 2^4 \times 3 \times 13^2$, obteniendo

$$(n, x - y) = 313.$$

Método de factorización $P-1$ de Pollard. Este último método utiliza un concepto más restrictivo de primo suave, que pasamos a describir.

Definición 3.16. Se dice que m es b-potencia suave si $p^r \mid m$ con p primo implica que $p^r \leq b$.

Lema 3.17. *Si $m \in \mathbb{Z}$ es b-potencia suave entonces $m \mid b!$.*

Demostración. Supongamos que $m = \pm p_1^{r_1} \cdots p_s^{r_s}$ es su descomposición en producto de potencias de primos distintos. Si m es b-potencia

suave, tenemos que $p_i^{r_i} \leq b$ para cada $1 \leq i \leq s$, por tanto $m = \pm p_1^{r_1} \cdots p_s^{r_s} \mid b!$. □

Sea $n = pq$. Supongamos que existe b tal que $p - 1$ es b-potencia suave. Por el Lema 3.17, $p-1 \mid b!$. Supongamos, además que $q-1 \nmid b!$, y en particular $q-1$ no es b-potencia suave. Supongamos que podemos calcular

$$a = 2^{b!} \bmod n.$$

Podemos cambiar 2 por cualquier otro número primo con n en esta fórmula. Como $p - 1 \mid b!$, tenemos que $a \equiv 1 \mod p$. Por otra parte, dado que $q - 1 \nmid b!$, $a \not\equiv 1 \mod q$. Por tanto $p \mid a - 1$ pero $q \nmid a - 1$. Podemos encontrar $p = (n, a - 1)$.

Se puede demostrar que este método tiene complejidad

$$\mathcal{O}\left(b \max\{(\log b)(\log n)^2, (\log n)^3\}\right).$$

Ejemplo 3.18. Sea $n = 1457$. Como no conocemos b, vamos a probar con varios. Empezamos con $b = 3$. Tenemos que

$$2^{3!} = 64 \bmod 1457, (64 - 1, 1457) = 1.$$

Para $b = 4$,

$$2^{4!} = 64^4 \equiv 1318 \mod 1457, (1318 - 1, 1457) = 1.$$

Para $b = 5$,

$$2^{5!} = 1318^5 \equiv 32 \mod 1457, (32 - 1, 1457) = 31.$$

Este método de factorización sugiere que los primos p_A y q_A deben ser elegidos de forma que $p_A - 1$ y $q_A - 1$ no sean b-potencia suave para valores pequeños de b. Una forma de garantizar esto es emplear primos p tales que $p - 1$ no solo tiene divisores pequeños. Un ejemplo de éstos son los que se conoce como primos fuertes. Otros algoritmos de factorización, como la criba en cuerpos de números algebraicos, funcionan para cualesquiera primos, por lo que la necesidad de emplear primos fuertes se ha reducido.

Ejercicios de RSA

Ejercicio 3.1. Si la clave pública de un criptosistema RSA es $(2291, 17)$,

1. calcula $2291 = pq$ sabiendo que $\varphi(n) = 2184$,
2. calcula $d = e^{-1} \bmod 2184$,
3. calcula $2291 = pq$ sabiendo que $d = 257$,
4. calcula $\mathrm{RSA}_{2291,17}(1116)$,
5. descifra el mensaje anterior empleando el Teorema Chino del Resto,
6. descifra el mensaje anterior sin emplear el Teorema Chino del Resto.

Ejercicio 3.2. Comprueba que existe una biyección entre divisores de n mayores que $\sqrt{n}$ y descomposiciones de n como diferencia de dos cuadrados.

Ejercicio 3.3. Intenta romper el criptosistema RSA con clave pública $(n, e) = (536813567, 3602561)$.

Ejercicio 3.4. Factoriza 23360947609 mediante la factorización de Fermat. ¿Funciona en este caso la criba cuadrática?

Ejercicio 3.5. Factoriza 332483, 279533 mediante el algoritmo $P - 1$ de Pollard.

Ejercicios de evaluación del Criptosistema RSA

Ejercicio. Este ejercicio es individualizado. Cada uno parte del número de su DNI, supongamos por ejemplo 12340987. Dividimos dicho número en dos bloques, 1234 y 0987. Si alguno de ellos es menor que 1000, rotamos las cifras a la izquierda hasta obtener un número mayor o igual que 1000, en nuestro caso 9870 (si alguien tuviese como un bloque el 0000, que coja un número mayor que 1000 cualquiera a su elección. Sean p y q los primeros primos mayores o iguales que los bloques anteriores. Concretamente, en el ejemplo $p = 1237$ y $q = 9871$. Sea $n = pq$ y e el menor primo mayor o igual que 11 que es primo relativo con $\varphi(n)$. Sea $d = e^{-1} \bmod \varphi(n)$.

1. Cifra el mensaje $m = 0xCAFE$ (recordad que $0x$ indica que el número está escrito en hexadecimal).
2. Descifra el criptograma anterior.
3. Intenta factorizar n mediante el método $P - 1$ de Pollard. Para ello llega, como máximo a $b = 8$.
4. Intenta factorizar n a partir de $\varphi(n)$.
5. Intenta factorizar n a partir de e y d.

Bibliografía

[1] Gregory V. Bard. *Algebraic Cryptanalysis*. Springer Science and Business Media, 2009.

[2] Hans Delfs and Helmut Knebl. *Introduction to Cryptography*. Information Security and Cryptography. Springer-Verlag Berlin Heidelberg, 2015.

[3] Andreas Enge. *Elliptic curves and their applications to cryptography. An Introduction.* Kluwer Academic Publishers, 1999.

[4] G. H. Hardy and E. M. Wright. *An Introduction to the Theory of Numbers*. Oxford University Press, fourth edition, 1960.

[5] Nathan Jacobson. *Basic Algebra: I*. W.H. Freeman & Company, second edition, 1985.

[6] Neal Koblitz. *A Course in Number Theory and Cryptography*, volume 114 of *Graduate Texts in Mathematics*. Springer-Verlag New York, 2 edition, 1994.

[7] National Institute of Standards and Technology (NIST). *Digital Signature Standard (DSS)*, July 2013.

[8] Harald Niederreiter and Arne Winterhof. *Applied Number Theory*. Springer International Publishing, 2015.

[9] Nigel P. Smart. *Cryptography Made Simple*. Information Security and Cryptography. Springer International Publishing, 2016.

[10] Joachim von zur Gathen. *CryptoSchool*. Springer-Verlag Berlin Heidelberg, 2015.