

# Método de encriptación RSA con Mathematica

Mariano González Ulloa  
mgonzal@pucp.edu.pe  
Pontificia Universidad Católica del Perú  
Departamento de Ciencias

19 de agosto de 2009

## Resumen

El sistema RSA es, hasta ahora, uno de los métodos de encriptación de información de llave pública más seguros. Aquí se hace una breve exposición de la base matemática de este sistema y al mismo tiempo se presenta una implementación del algoritmo con el software Mathematica.

## 1. Nociones preliminares

En esta sección se presenta los resultados fundamentales sobre anillos, especialmente el anillo de los números enteros módulo  $n$ , para plantear el algoritmo de encriptación de llave pública RSA.

### 1.1. Anillos

**Definición 1.1** Sea  $A$  un conjunto no vacío. En él se definen dos operaciones binarias denotadas con  $\oplus$  y  $\odot$

$$\begin{aligned} \oplus : A \times A &\longrightarrow A & \odot : A \times A &\longrightarrow A \\ (a, b) &\rightsquigarrow a \oplus b & (a, b) &\rightsquigarrow a \odot b \end{aligned}$$

La terna  $(A, \oplus, \odot)$  es un anillo si las operaciones  $\oplus$  y  $\odot$  satisfacen las siguientes condiciones:

1.  $a \oplus b = b \oplus a; \forall a, b \in A$  (propiedad conmutativa de la operación  $\oplus$ )
2.  $a \oplus (b \oplus c) = (a \oplus b) \oplus c$  (propiedad asociativa de la operación  $\oplus$ )
3. Existe un único elemento  $e \in A$  tal que  $\forall a \in A, a \oplus e = e \oplus a = a$  (existencia del elemento neutro o elemento identidad para la operación  $\oplus$ )
4. Para cada elemento  $a \in A$  existe  $b \in A$  tal que  $a \oplus b = b \oplus a = e$  (existencia del elemento inverso aditivo)
5.  $a \odot (b \odot c) = (a \odot b) \odot c$  (propiedad asociativa de la operación  $\odot$ )
6.  $a \odot (b \oplus c) = (a \odot b) \oplus (a \odot c)$  (propiedad distributiva de la operación  $\odot$  respecto a la operación  $\oplus$ )

El conjunto de números enteros,  $(\mathbb{Z}, +, \cdot)$ , con la adición,  $(+)$ , y la multiplicación,  $(\cdot)$ , habituales, es un anillo. Donde  $e = 0$  y el inverso aditivo de  $n \in \mathbb{Z}$  es  $-n$ . También el conjunto de números racionales,  $(\mathbb{Q}, +, \cdot)$ , y el conjunto de números reales,  $(\mathbb{R}, +, \cdot)$ , con las operaciones de adición y multiplicación habituales son anillos.

**Definición 1.2** Sea  $(A, \oplus, \odot)$  un anillo con elemento identidad aditivo  $e$ .

1. Si  $\forall a, b \in A, a \odot b = b \odot a$ ,  $(A, \oplus, \odot)$  se denomina anillo **conmutativo**.
2. Si para elementos cualesquiera  $a, b \in A, a \odot b = e$  implica que  $a=e$  ó  $b=e$  se dice que  $A$  no tiene divisores propios de la identidad.
3. Si existe un elemento  $u \in A$  tal que  $\forall a \in A, a \odot u = u \odot a = a$ ,  $u$  se denomina **identidad multiplicativa** o **elemento unitario** de  $A$  y en tal caso  $(A, \oplus, \odot)$  se denomina anillo con elemento unitario.

El anillo  $(\mathbb{R}, +, \cdot)$  es conmutativo con elemento unitario  $u = 1$  que no tiene divisores propios de cero.

También, si  $X = \{0, 1\}$  y  $A = \wp(X) = \{\emptyset, \{0\}, \{1\}, \{0, 1\}\}$  y definimos en  $A$  las operaciones  $\oplus$  y  $\odot$  mediante

$$R \oplus S = R \Delta S \quad \text{y} \quad R \odot S = R \cap S,$$

respectivamente, entonces  $(A, \oplus, \odot)$  es un anillo conmutativo con elemento unitario  $u = \{0, 1\}$  que tiene divisores propios de la identidad. Identifique el elemento identidad,  $e$ , y pruebe que tiene divisores propios.

**Teorema 1.1** Sea  $(A, \oplus, \odot)$  un anillo con elemento identidad  $e$ . Para cualquier  $a \in A$  se cumple que

$$a \odot e = e \odot a = e$$

**Prueba.-** Si  $e$  es el elemento identidad de  $A$  entonces  $e \oplus e = e$  y para cualquier elemento  $a \in A$

$$a \odot e = a \odot (e \oplus e) = (a \odot e) \oplus (a \odot e)$$

Pero  $(a \odot e) \oplus e = a \odot e$ , entonces

$$(a \odot e) \oplus e = (a \odot e) \oplus (a \odot e)$$

luego, “sumando” el inverso aditivo de  $a \odot e$  se tiene que  $a \odot e = e$ .

En forma similar se prueba que  $e \odot a = e$ .

**Definición 1.3** Sea  $(A, \oplus, \odot)$  un anillo con elemento identidad  $e$  y elemento unitario  $u$ . Si para cada  $a \in A, a \neq e$ , existe  $b \in A$  tal que  $a \odot b = b \odot a = u$ , el elemento  $b$  se denomina **inverso multiplicativo** de  $a$  y se denota con  $a^{-1}$ , es decir  $b = a^{-1}$ .

**Definición 1.4** Sea  $A$  un anillo conmutativo con elemento unitario  $u$ .

- a) Si  $A$  no tiene divisores propios de la identidad,  $A$  se denomina **dominio entero**.
- b) Si todo elemento de  $A$  distinto del elemento identidad tiene inverso multiplicativo,  $A$  se denomina campo

**Ejemplo 1.1** El anillo  $(\mathbb{Z}, +, \cdot)$  es un dominio entero pero no es un campo, ningún elemento de  $\mathbb{Z}$  tiene inverso multiplicativo. En cambio  $(\mathbb{Q}, +, \cdot)$  y  $(\mathbb{R}, +, \cdot)$  son dominios enteros y campos.

**Teorema 1.2** Sea  $(A, \oplus, \odot)$  un anillo conmutativo con elemento unitario  $u$ .  $A$  es un dominio entero si y sólo si para elementos cualesquiera  $a, b, c \in A$  tales que  $a \neq e$ ,  $a \odot b = a \odot c$  implica que  $b = c$ .

**Prueba.-**

$\Rightarrow$ ) Si  $A$  es un dominio entero, entonces para  $x, y \in A$ ,  $x \odot y = e$  implica que  $x = e$  ó  $y = e$ . Para  $a, b, c \in A$  tales que  $a \neq e$  y  $a \odot b = a \odot c$ . Sea  $d$  el inverso aditivo de  $c$ , entonces  $(a \odot b) \oplus (a \odot d) = (a \odot c) \oplus (a \odot d) = a \odot (c \oplus d) = a \odot e = e$ ; de donde se tiene que  $a \odot (b \oplus d) = e$ , pero  $a \neq e$  entonces  $b \oplus d = e$  luego  $(b \oplus d) \oplus c = e \oplus c = c$ . Por otro lado  $b \oplus (d \oplus c) = b \oplus e = b$ . De aquí resulta que  $b = c$ .

$\Leftarrow$ ) Recíprocamente, si  $A$  es un anillo conmutativo con elemento unitario  $u$  y para cualesquiera  $a, b, c \in A$ ,  $a \neq e$ , entonces  $a \odot b = a \odot c$  implica que  $b = c$

Sean  $x, y \in A$  con  $x \odot y = e$

Si  $x = e$ , no hay nada que probar.

Si  $x \neq e$ , como  $x \odot e = e$ , se puede escribir

$$x \odot y = e = x \odot e$$

de donde se tiene que  $y = e$ .

De esta manera se observa que no existen divisores propios de la identidad y en consecuencia  $A$  es un dominio entero.

**Teorema 1.3** Si  $(A, \oplus, \odot)$  es un campo, entonces  $(A, \oplus, \odot)$  es un dominio entero.

**Prueba.-** Sean  $e$  el elemento identidad,  $u$  el elemento unitario,  $x, y \in A$  tales que  $x \odot y = e$ . Si  $x = e$ , no hay nada para probar.

Si  $x \neq e$ , entonces existe el inverso multiplicativo de  $x$ ,  $x^{-1}$  y  $x^{-1} \odot (x \odot y) = x^{-1} \odot e = e$ .

Por otro lado

$(x^{-1} \odot x) \odot y = e$  de donde se tiene que  $u \odot y = e$  y en consecuencia  $y = e$ .

Así,  $(A, \oplus, \odot)$  no tiene divisores propios de la identidad, es decir que es un dominio entero.

**Teorema 1.4** Si  $(A, \oplus, \odot)$  es un dominio entero finito, entonces  $(A, \oplus, \odot)$  es un campo.

**Prueba.-** Si  $A$  es finito, entonces podemos suponer que tiene  $n$  elementos,

$$A = \{a_1, a_2, \dots, a_n\}.$$

Sea  $b \in A$ ,  $b \neq e$  y

$$b \odot A = \{b \odot a_1, b \odot a_2, \dots, b \odot a_n\}$$

entonces  $b \odot A \subset A$  ya que  $A$  es cerrado respecto a  $\odot$ .

**Afirmación.-** El número de elementos de  $b \odot A$  es  $n$ ,  $\eta(b \odot A) = n$ .

Supongamos que  $\eta(b \odot A) < n$ , entonces  $b \odot a_i = b \odot a_j$  para algunos  $i, j$ ,

$1 \leq i < j \leq n$ . Como  $b \neq e$  y  $A$  es un dominio entero entonces  $a_i = a_j$  lo que es una contradicción, en consecuencia  $\eta(b \odot A) = n$  de donde se tiene que  $b \odot A = A$ . Luego  $b \odot a_i = u$  el elemento unitario, para algún  $i$ ,  $1 \leq i \leq n$  entonces  $b$  es el inverso de  $a_i$ . Como  $b$  es arbitrario se sigue que  $(A, \oplus, \odot)$  es un campo.

## 1.2. Enteros módulo $n$

**Definición 1.5** Sea  $n \in \mathbb{Z}$ ,  $n > 1$ . Para  $a, b \in \mathbb{Z}$  se dice que  $a$  es congruente con  $b$  módulo  $n$  si  $n|(a - b)$  o equivalentemente si  $a = kn + b$  para algún  $k \in \mathbb{Z}$ .

Si  $a$  es congruente con  $b$  módulo  $n$  se escribe

$$a \equiv b \pmod{n}$$

### Ejemplos 1.1

- a)  $13 \equiv 8 \pmod{5}$  ; pues  $5|(13 - 8)$  ó  $13 = 1 \times 5 + 8$
- b)  $10 \equiv 4 \pmod{3}$  ; pues  $3|(10 - 4)$  ó  $10 = 2 \times 3 + 4$
- c)  $17 \equiv 3 \pmod{7}$  ; pues  $7|(17 - 3)$  ó  $17 = 2 \times 7 + 3$

**Teorema 1.5** Sea  $n \in \mathbb{Z}$ ,  $n > 1$

- 1)  $a \equiv a \pmod{n}$  ;  $\forall a \in \mathbb{Z}$
- 2) Si  $a \equiv b \pmod{n}$ , entonces  $b \equiv a \pmod{n}$  ;  $a, b \in \mathbb{Z}$
- 3) Si  $a \equiv b \pmod{n}$  y  $b \equiv c \pmod{n}$ , entonces  $a \equiv c \pmod{n}$

**Prueba.-** La prueba del teorema se deja como ejercicio para el lector.

Sea  $n \in \mathbb{Z}$ ,  $n > 1$  y  $a \in \mathbb{Z}$ , denotemos con

$$[a] = \{b \in \mathbb{Z}; b \equiv a \pmod{n}\} = \{a + kn; \text{ para algún } k \in \mathbb{Z}\} \\ = \{\dots, a - 3n, a - 2n, a - n, a, a + n, a + 2n, a + 3n, \dots\}$$

El conjunto  $\{[0], [1], [2], \dots, [n - 1]\}$  constituye una partición de  $\mathbb{Z}$  y cada elemento  $[k]$ ,  $k = 0, 1, 2, \dots, n - 1$  se denomina *clase de equivalencia*.

Denotemos con  $\mathbb{Z}_n = \{[0], [1], [2], \dots, [n - 1]\}$  y definamos en este conjunto dos operaciones  $+$  y  $\cdot$  de la siguiente manera:

$$+ : \mathbb{Z}_n \times \mathbb{Z}_n \longrightarrow \mathbb{Z}_n \qquad \cdot : \mathbb{Z}_n \times \mathbb{Z}_n \longrightarrow \mathbb{Z}_n \\ ([a], [b]) \rightsquigarrow [a + b] \qquad ([a], [b]) \rightsquigarrow [a \cdot b]$$

### Observaciones 1.1

- 1. Las operaciones  $a + b$  y  $a \cdot b$  son la adición y la multiplicación ordinarias en  $\mathbb{Z}$ .
- 2. Las operaciones en  $\mathbb{Z}_n$  están bien definidas, es decir que no dependen del elemento que se elija como representante de cada clase de equivalencia.

*En efecto*

Sean  $[a], [b], [c]$  y  $[d] \in \mathbb{Z}_n$  con  $a \neq c$  y  $b \neq d$  tales que  $[a] = [c]$  y  $[b] = [d]$  entonces  $a = k_1n + c$  y  $b = k_2n + d$

Luego

$$a + b = (k_1n + c) + (k_2n + d) = (k_1 + k_2)n + (c + d)$$

esto significa que  $[a + b] = [c + d]$ , en consecuencia  $[a] + [b] = [c] + [d]$

También

$$a \cdot b = (k_1n + c) \cdot (k_2n + d) = (k_1k_2n + k_1d + k_2c)n + c \cdot d$$

es decir  $[a \cdot b] = [c \cdot d]$ , en consecuencia  $[a] \cdot [b] = [c] \cdot [d]$

**Teorema 1.6** Para  $n \in \mathbb{Z}$ ,  $n > 1$ ,  $(\mathbb{Z}_n, +, \cdot)$  es un anillo conmutativo con elemento unitario  $[1]$ .

**Prueba.-** La prueba del teorema se deja como ejercicio para el lector.

**Notación.-** En lo que sigue la clase de equivalencia  $[a]$  la denotaremos simplemente con  $a$ .

### Ejemplos 1.2

a) Consideremos  $\mathbb{Z}_4$  y denotando con  $a$  la clase de equivalencia  $[a] \in \mathbb{Z}_4$  se tiene

$+$	$0$	$1$	$2$	$3$
$0$	$0$	$1$	$2$	$3$
$1$	$1$	$2$	$3$	$0$
$2$	$2$	$3$	$0$	$1$
$3$	$3$	$0$	$1$	$2$

$\cdot$	$0$	$1$	$2$	$3$
$0$	$0$	$0$	$0$	$0$
$1$	$0$	$1$	$2$	$3$
$2$	$0$	$2$	$0$	$2$
$3$	$0$	$3$	$2$	$1$

Observar que  $\mathbb{Z}_4$  tiene divisores propios de la identidad ( $2 \cdot 2 = 0$ ), en consecuencia  $\mathbb{Z}_4$  no es un dominio entero y por tanto no es un campo.

b) Consideremos ahora  $\mathbb{Z}_5$

$+$	$0$	$1$	$2$	$3$	$4$
$0$	$0$	$1$	$2$	$3$	$4$
$1$	$1$	$2$	$3$	$4$	$0$
$2$	$2$	$3$	$4$	$0$	$1$
$3$	$3$	$4$	$0$	$1$	$2$
$4$	$4$	$0$	$1$	$2$	$3$

$\cdot$	$0$	$1$	$2$	$3$	$4$
$0$	$0$	$0$	$0$	$0$	$0$
$1$	$0$	$1$	$2$	$3$	$4$
$2$	$0$	$2$	$4$	$1$	$3$
$3$	$0$	$3$	$1$	$4$	$2$
$4$	$0$	$4$	$3$	$2$	$1$

En  $\mathbb{Z}_5$  todos los elementos distintos de cero tienen inverso multiplicativo, en consecuencia  $\mathbb{Z}_5$  es un campo.

**Teorema 1.7**  $\mathbb{Z}_n$  es un campo si y sólo si  $n$  es primo.

**Prueba.-**

$\Rightarrow$ ) Si  $\mathbb{Z}_n$  es un campo, entonces  $n$  es primo, o equivalentemente, si  $n$  no es primo entonces  $\mathbb{Z}_n$  no es un campo.

Si  $n$  no es primo entonces es compuesto, es decir existen  $n_1, n_2 \in \mathbb{Z}^+$ ,

$1 < n_1, n_2 < n$  tales que  $n = n_1 \cdot n_2$  lo que quiere decir que  $[n_1] \neq [0]$  y  $[n_2] \neq [0]$ . Pero  $[n_1] \cdot [n_2] = [n_1 \cdot n_2] = [n] = [0]$  esto implica que  $\mathbb{Z}_n$  ni siquiera es un dominio entero, por tanto no puede ser un campo.

$\Leftarrow$ ) Si  $n$  es primo, entonces  $\mathbb{Z}_n$  es un campo.

Basta probar que cualquier elemento no nulo de  $\mathbb{Z}_n$  tiene inverso multiplicativo.

Sea  $[a] \neq [0]$  un elemento cualquiera de  $\mathbb{Z}_n$ , entonces  $0 < a < n$  y  $MCD(a, n) = 1$ , pues

$n$  es primo, lo que implica que existen  $s, t \in \mathbb{Z}$  tales que  $1 = tn + sa$ ,  $s \neq 0$ . Así que  $sa \equiv 1 \pmod{n}$  lo que implica que  $[s \cdot a] = [1]$  ó  $[s] \cdot [a] = [1]$ , es decir que  $[a]^{-1} = [s]$  esto significa que  $\mathbb{Z}_n$  es un campo.

**Teorema 1.8** Sea  $[a] \in \mathbb{Z}_n$ ,  $[a]$  tiene inverso multiplicativo si y sólo si  $MCD(a, n) = 1$ .

**Prueba.-**

Sea  $[a] \in \mathbb{Z}_n$ .

$\Rightarrow$ ) Si  $[a]$  tiene inverso multiplicativo, entonces  $MCD(a, n) = 1$ .

Si  $[a]$  tiene inverso multiplicativo, entonces existe  $s \in \mathbb{Z}$ ,  $0 < s < n$ , tal que  $[a]^{-1} = [s]$ .

Pero  $[a \cdot s] = [a] \cdot [s] = [1]$  o que es lo mismo  $as \equiv 1 \pmod{n}$  ó  $as = 1 + tn$ , para algún  $t \in \mathbb{Z}$  de donde  $1 = sa + (-t)n$ .

Por otro lado, si  $MCD(a, n) \neq 1$ , entonces existe un entero  $p$ ,  $1 < p < n$  tal que  $p|a$  y  $p|n$ , en consecuencia  $p|1$  que es una contradicción.

Por tanto  $MCD(a, n) = 1$ .

$\Leftarrow$ ) Si  $MCD(a, n) = 1$ , entonces  $[a]$  tiene inverso multiplicativo.

Si  $MCD(a, n) = 1$ , entonces existen enteros no nulos  $s, t \in \mathbb{Z}$  tales que

$1 = sn + ta$  ó  $ta \equiv 1 \pmod{n}$  de donde  $[t \cdot a] = [1]$  ó  $[t] \cdot [a] = [1]$  lo que significa que  $[a]^{-1} = [t]$ .

**Definición 1.6** Sea  $n \in \mathbb{Z}$ ;  $n > 1$  y

$$S_n = \{a \in \{1, 2, 3, 4, \dots, n\}; MCD(a, n) = 1\}.$$

La función

$$\varphi : \mathbb{Z}^+ \longrightarrow \mathbb{Z}^+$$

$$n \rightsquigarrow \varphi(n) = \eta(S_n),$$

donde  $\varphi(n) = \eta(S_n)$  = número de enteros entre  $1, 2, 3, 4, \dots, n$  que son coprimos con  $n$ , se denomina **función de Euler**.

Algunos valores de esta función son:

$S_2 = \{1\}$  en consecuencia  $\varphi(2) = 1$

$S_3 = \{1, 2\}$  en consecuencia  $\varphi(3) = 2$

$S_4 = \{1, 3\}$  en consecuencia  $\varphi(4) = 2$

$S_5 = \{1, 2, 3, 4\}$  en consecuencia  $\varphi(5) = 4$

$S_6 = \{1, 5\}$  en consecuencia  $\varphi(6) = 2$

$S_7 = \{1, 2, 3, 4, 5, 6\}$  en consecuencia  $\varphi(7) = 6$

**Teorema 1.9** Si  $p \in \mathbb{Z}^+$  es primo, entonces  $\varphi(p) = p - 1$ .

**Prueba.-** Si  $p$  es un número primo, entonces  $S_p = \{1, 2, 3, \dots, p - 1\}$ , en consecuencia  $\varphi(p) = p - 1$

**Teorema 1.10** Si  $p, q \in \mathbb{Z}^+$  son números primos distintos, entonces

$$\varphi(pq) = (p - 1)(q - 1).$$

**Prueba.-** Si  $p, q \in \mathbb{Z}^+$ , se tiene los números  $1, 2, 3, \dots, pq$ . De esta lista eliminamos los múltiplos de  $p$  y los múltiplos de  $q$  que son divisores de  $pq$ . Como se puede ver claramente hay  $p$  múltiplos de  $q$  y  $q$  múltiplos de  $p$ . Además el único múltiplo común de  $p$  y  $q$  es  $pq$ . Luego

$$\varphi(pq) = pq - p - q + 1 = (p-1)(q-1)$$

**Teorema 1.11** Sean  $a, n \in \mathbb{Z}^+$ . Si  $MCD(a, n) = 1$ , entonces

$$a^{\varphi(n)} \equiv 1 \pmod{n}$$

**Prueba.-** Sea

$$S_n = \{r_1, r_2, r_3, \dots, r_{\varphi(n)}\}$$

el conjunto de los enteros entre  $1, 2, 3, \dots, n$  que son coprimos con  $n$ .

Afirmación 1:

Si  $MCD(a, n) = 1$ , entonces los enteros

$$ar_1, ar_2, ar_3, \dots, ar_{\varphi(n)}$$

también son coprimos con  $n$

En efecto

Si algún  $ar_i$ ;  $1 \leq i \leq \varphi(n)$  no fuera coprimo con  $n$ , entonces existiría un entero  $k > 1$  tal que  $k|ar_i$  y  $k|n$  lo cual implica que  $(k|a$  ó  $k|r_i)$  y  $k|n$  o que es lo mismo  $(k|a$  y  $k|n)$  ó  $(k|r_i$  y  $k|n)$ , cualquier caso contradice al hecho que  $MCD(a, n) = 1$  ó al hecho que  $MCD(r_i, n) = 1$

Afirmación 2:

Los enteros  $ar_1, ar_2, ar_3, \dots, ar_{\varphi(n)}$  no son congruentes dos a dos módulo  $n$ .

En efecto

Supongamos lo contrario, es decir que para algunos  $i, j$  con  $1 \leq i < j \leq \varphi(n)$

$$ar_i \equiv ar_j \pmod{n}$$

Como  $MCD(a, n) = 1$ , por el teorema 1.8, existe  $d \in \mathbb{Z}_n$  tal que

$$da \equiv 1 \pmod{n}$$

en consecuencia

$$\begin{aligned} r_i &\equiv 1 \cdot r_i \pmod{n} \\ &\equiv (da) r_i \pmod{n} \\ &\equiv d(ar_i) \pmod{n} \\ &\equiv d(ar_j) \pmod{n} \\ &\equiv (da) r_j \pmod{n} \\ &\equiv r_j \pmod{n} \end{aligned}$$

que es una contradicción.

La afirmación 2 nos permite concluir que cada uno de los números

$ar_1, ar_2, ar_3, \dots, ar_{\varphi(n)}$  es congruente  $\pmod{n}$  con solamente uno de los enteros

$r_1, r_2, r_3, \dots, r_{\varphi(n)}$ .

En consecuencia

$$\begin{aligned} r_1 r_2 r_3 \cdots r_{\varphi(n)} &\equiv (a r_1) (a r_2) (a r_3 \cdots (a r_{\varphi(n)})) \pmod{n} \\ &\equiv a^{\varphi(n)} r_1 r_2 r_3 \cdots r_{\varphi(n)} \pmod{n} \end{aligned}$$

Pero  $MCD(r_1 r_2 r_3 \cdots r_{\varphi(n)}, n) = 1$ , entonces por el teorema 1.8 existe un entero  $s \in \mathbb{Z}_n$  tal que

$$r_1 r_2 r_3 \cdots r_{\varphi(n)} s \equiv 1 \pmod{n}$$

Luego

$$\begin{aligned} 1 &\equiv r_1 r_2 r_3 \cdots r_{\varphi(n)} s \pmod{n} \\ &\equiv (a^{\varphi(n)} r_1 r_2 r_3 \cdots r_{\varphi(n)}) s \pmod{n} \\ &\equiv a^{\varphi(n)} (r_1 r_2 r_3 \cdots r_{\varphi(n)} s) \pmod{n} \\ &\equiv a^{\varphi(n)} \pmod{n} \end{aligned}$$

o equivalentemente

$$a^{\varphi(n)} \equiv 1 \pmod{n}$$

**Corolario 1.12** Sean  $a, n \in \mathbb{Z}^+$ . Si  $MCD(a, n) = 1$ , entonces el inverso multiplicativo de  $a$  en  $\mathbb{Z}_n$  es  $a^{\varphi(n)-1}$

**Prueba.-** Del teorema se tiene que

$$a^{\varphi(n)} \equiv 1 \pmod{n}$$

luego

$$a^{\varphi(n)-1} a \equiv 1 \pmod{n}$$

de donde se concluye la afirmación del corolario.

## 2. Sistema RSA

Uno de los métodos de encriptación de mensajes de llave pública es conocido como el método RSA debido a sus creadores Ron Rivest, Adi Shamir y Len Adleman. Resultado que fue publicado en *Scientific American* en agosto de 1977.

Este método de encriptación se apoya fundamentalmente en el teorema 1.11 y en el hecho de que se requiere de mucho tiempo para factorizar números enteros de más de 200 dígitos. La idea es bastante simple: Se considera dos números primos diferentes  $p$  y  $q$  suficientemente grandes, de alrededor de 100 dígitos cada uno. Los valores de  $p$  y  $q$  constituyen parte de la clave secreta mientras que el valor de  $n = pq$  es parte de la clave pública y se denomina el **módulo del código**.

De acuerdo al teorema 1.10 el valor de la función de Euler en  $n$  es

$$\varphi(n) = (p-1)(q-1)$$

valor que, también, debe ser guardado en secreto.

Antes de codificar un mensaje se identifican los caracteres a usar con números naturales menores que  $n$ , con lo cual se tiene el mensaje precodificado. Dicha identificación debe ser conocida tanto por el emisor como por el receptor del mensaje.

Supongamos ahora que se tiene un sistema con  $m$  usuarios. A cada usuario  $i$ ,  $1 \leq i \leq m$ , se le asigna una clave pública  $e_i$  y una clave privada  $d_i$ . Estas claves son números enteros tales que

$$MCD(e_i, \varphi(n)) = 1$$

y

$$e_i d_i \equiv 1 \pmod{\varphi(n)}$$

Supongamos que un usuario cualquiera del sistema desea enviar al usuario  $i$  un mensaje precodificado  $x$  ( $x \in \mathbb{Z}^+$ ,  $x < n$ )

El mensaje codificado,  $C(x, e_i) = c$ , se obtiene mediante

$$C(x, e_i) = c \equiv x^{e_i} \pmod{n}; \quad 0 < c < n$$

Cuando el usuario  $i$  recibe el mensaje codificado  $c$  puede obtener el mensaje decodificado,  $D(c, d_i) = y$ , usando la expresión

$$D(c, d_i) = y \equiv c^{d_i} \pmod{n}; \quad 0 < y < n$$

donde  $d_i$  es su clave personal secreta;  $y$  es el mensaje decodificado que podrá leer recurriendo a la identificación preestablecida entre los caracteres y los números naturales.

### Observaciones 2.1

1. La seguridad del método RSA se basa en el hecho de que para decodificar un mensaje se requiere conocer los enteros  $p$  y  $q$  es decir factorizar el número compuesto  $n = pq$  (número de más de 200 dígitos), proceso que requiere de mucho tiempo.
2. La razón de guardar en secreto el número de Euler  $\varphi(n)$ , calcular su valor es una tarea tan difícil como hallar  $p$  y  $q$ , es la siguiente: conociendo  $\varphi(n)$  y teniendo en cuenta que  $n$  es de conocimiento público se puede escribir

$$\varphi(n) = (p-1)(q-1) = pq - p - q + 1 = n - p - q + 1$$

de donde se tiene

$$p + q = n - \varphi(n) + 1 \tag{1}$$

Por otro lado

$$(p-q)^2 = p^2 - 2pq + q^2 = (p+q)^2 - 4pq = (n - \varphi(n) + 1)^2 - 4n \tag{2}$$

Si los valores de  $n$  y  $\varphi(n)$  son conocidos, fácilmente de (1) y (2) se puede conocer  $p+q$  y  $p-q$  y en consecuencia  $p$  y  $q$ .

3. Si se envía el mismo mensaje a diferentes usuarios estos recibirán diferentes mensajes codificados  $c$  debido a que cada usuario tiene una clave pública  $e_i$  diferente.

4. La condición  $e_i d_i \equiv 1 \pmod{\varphi(n)}$  asegura que el mensaje decodificado,  $y$ , sea el mensaje original enviado por el emisor ya que ésta condición garantiza la existencia de un entero  $k_i \in \mathbb{Z}$  tal que

$$e_i d_i = k_i \varphi(n) + 1$$

con lo cual se tiene

$$\begin{aligned} y &\equiv c^{d_i} \pmod{n} \\ &\equiv (x^{e_i})^{d_i} \pmod{n} \\ &\equiv x^{e_i d_i} \pmod{n} \\ &\equiv x^{k_i \varphi(n) + 1} \pmod{n} \\ &\equiv (x^{\varphi(n)})^{k_i} x \pmod{n} \\ &\equiv x \pmod{n} \end{aligned}$$

gracias al teorema 1.11.

En la siguiente tabla se muestra como se distribuye las claves del sistema RSA.

Conocimiento público	Secreto para el usuario $i$	Conocimiento solamente del responsable del sistema
$n; e_1, e_2, \dots, e_m$	$d_i$	$p, q; \varphi(n)$

Todo lo descrito antes se puede resumir en un algoritmo.

## 2.1. Algoritmo RSA

El algoritmo es el siguiente:

1. Generar dos números primos diferentes  $p, q$ .
2. Calcular  $n = pq$ ,  $\phi(n) = (p-1)(q-1)$ .
3. Elegir enteros (llaves públicas)  $e_1, e_2, \dots, e_m$  con  $1 < e_i < \phi(n)$  tales que  $MCD(e_i, \phi(n)) = 1$ ;  $i = 1, 2, \dots, m$
4. Calcular enteros (llaves privadas)  $d_i; i = 1, 2, \dots, m$  donde  $d_i e_i \equiv 1 \pmod{\phi(n)}$ .
5. El emisor calcula  $c \equiv x^{e_i} \pmod{n}$  con la llave pública  $(n, e_i)$  { \* mensaje codificado \* }
6. El receptor recupera el mensaje mediante  $x \equiv c^{d_i} \pmod{n}$ , con su llave privada  $d_i$  { \* mensaje decodificado \* }
7. Fin

Con la finalidad de mostrar un ejemplo del sistema **RSA**, identifiquemos a los caracteres alfanuméricos con números enteros como se muestra en la siguiente tabla (al código ASCII le sumamos 55):

A	B	C	D	E	F	G	H	I	J	K	L	M	N
120	121	122	123	124	125	126	127	128	129	130	131	132	133

  

O	P	Q	R	S	T	U	V	W	X	Y	Z	...
134	135	136	137	138	139	140	141	142	143	144	145	...

A continuación se presenta el algoritmo anterior implementado en Mathematica v 6.1.0.1

```
(* SISTEMA RSA EN MATHEMATICA*)

(* cambio de linea *)
nl := FromCharacterCode[13];
(* Funcion de Euler *)
FuncionEuler[n_] := Dimensions[
DeleteCases[Table[If[GCD[k, n] == 1, k, 0], {k, 1, n}], 0]][[1]];
i = 11; (* para usar el i-esimo numero primo como el valor de p *)
j = 7; (* para usar el j-esimo numero primo como el valor de q *)
p=Prime[i]; q = Prime[j]; n = p*q;

(* numero de usuarios del sistema *)
userNumber = 5;
(* lista de usuarios *)
usuarios := Table[k, {k,1, userNumber}];
(* Generacion de las posibles claves individuales publicas *)
ClavesPersonalesPublicas := DeleteCases[ Table[If[GCD[k,
FuncionEuler[n]] == 1, k, 0], {k, 1,FuncionEuler[n]}], 0];

(* Generacion de claves *)

(* generacion aleatoria de las claves personales publicas*)
Clavepub= RandomSample[ClavesPersonalesPublicas, userNumber];

(* claves personales privadas *)
Clavepri := Table[PowerMod[Clavepub[[k]],
FuncionEuler[FuncionEuler[n]] - 1,
FuncionEuler[n]], {k, 1, Dimensions[Clavepub] [[1]]}];

(* Impresión de las claves publicas y privadas *)

Print["Claves publicas ", nl, MatrixForm[usuarios],
MatrixForm[Clavepub], nl, "Claves privadas ", nl,
MatrixForm[usuarios], MatrixForm[Clavepri]]

(* Codificacion y decodificacion del mensaje *)

(* mensaje original *)
mensaje := "HOLA";
```

```
(* mensaje precodificado: al codigo ASCII de cada caracter se le
suma \ 55 *)

mensaje precod := ToCharacterCode[mensaje] + 55;

(* mensaje codificado *)
mcod := Table[ PowerMod[mensaje precod[[j]], Clavepub[[i]], n], {i,
1, Dimensions[Clavepub][[1]]}, {j, 1,
Dimensions[mensaje precod][[1]]}];

(* mensaje decodificado *)
mdecod := Table[PowerMod[mcod[[j]][[i]], Clavepri[[j]], n], {j, 1,
Dimensions[Clavepri][[1]]}, {i, 1, Dimensions[mensaje precod][[1]]}];

(* mensaje original recibido por el receptor *)

mensajeOut := FromCharacterCode[mdecod[[1]] - 55];

(* impresion de resultados *)

Print[nl, nl, "p= ", p, " ; ", "q= ", q, " ; ", "n= ", n, " ; ", "\
\[\Phi](n)= ", FuncionEuler[n], nl,
nl, "Mensaje original", nl, mensaje, nl, nl, "Mensaje precodificado \
", nl, mensaje precod, nl, nl,
"Claves publicas", nl, MatrixForm[usuarios],
MatrixForm[Clavepub], nl, nl, "Mensaje codificado ", nl,
MatrixForm[usuarios],
MatrixForm[mcod], nl, nl, "Claves privadas", nl,
MatrixForm[usuarios],
MatrixForm[Clavepri], nl, nl, "Mensaje decodificado", nl,
MatrixForm[usuarios],
MatrixForm[mdecod], nl, nl, "Mensaje final", nl, mensajeOut]
```

Para mostrar una corrida del algoritmo consideremos el siguiente ejemplo. Por razones obvias se considera los números primos  $p$  y  $q$  pequeños.

Consideremos los números primos  $p = 17$  y  $q = 31$  entonces  $n = 527$  y  $\varphi(527) = (17 - 1)(31 - 1) = 480$

Para elegir las claves tanto públicas como privadas se requiere hallar elementos de  $\mathbb{Z}_{480}$  que tienen inverso multiplicativo. Para ello bastará hallar, según el teorema 1.8, enteros,  $a$ , coprimos con 480.

Asumiremos que se tiene 5 usuarios y sus respectivas claves son

Usuario	Clave personal pública	Clave personal privada
1	$e_1 = 443$	$d_1 = 467$
2	$e_2 = 43$	$d_2 = 67$
3	$e_3 = 209$	$d_3 = 209$
4	$e_4 = 161$	$d_4 = 161$
5	$e_5 = 269$	$d_5 = 389$

Observar que para cada  $i$ ,  $1 \leq i \leq 5$ ,  $e_i d_i \equiv 1 \pmod{480}$

Ahora suponga que el responsable del sistema desea enviar a todos los usuarios el siguiente mensaje

*HOLA*

El mensaje precodificado, de acuerdo a las identificaciones previamente establecidas, será

127 134 131 120

El mensaje codificado que recibirá cada usuario se muestra en la siguiente tabla:

Usuario	127	134	131	120	Mensaje codificado
1	$127^{443} = 104$	$134^{443} = 417$	$131^{443} = 227$	$120^{443} = 494$	104 417 227 494
2	$127^{43} = 427$	$134^{43} = 9$	$131^{43} = 329$	$120^{43} = 494$	427 9 329 494
3	$127^{209} = 331$	$134^{209} = 338$	$131^{209} = 505$	$120^{209} = 426$	331 338 505 428
4	$127^{161} = 416$	$134^{161} = 236$	$131^{161} = 454$	$120^{161} = 120$	416 236 454 120
5	$127^{269} = 145$	$134^{269} = 121$	$131^{269} = 133$	$120^{269} = 426$	145 121 133 426

El mensaje decodificado por cada usuario,  $i$ , según su clave secreta,  $d_i$ , se muestra en la siguiente tabla:

Usuario					Mens. decodificado
1	$104^{467} = 127$	$417^{467} = 134$	$227^{467} = 131$	$494^{467} = 120$	127 134 131 120
2	$427^{67} = 127$	$9^{67} = 134$	$329^{67} = 131$	$494^{67} = 120$	127 134 131 120
3	$331^{209} = 127$	$338^{209} = 134$	$505^{209} = 131$	$426^{209} = 120$	127 134 131 120
4	$416^{161} = 127$	$236^{161} = 134$	$454^{161} = 131$	$120^{161} = 120$	127 134 131 120
5	$145^{389} = 127$	$121^{389} = 134$	$133^{389} = 131$	$426^{389} = 120$	127 134 131 120

la última columna de la tabla muestra los mismos valores para todas las filas, que al ser traducidos en caracteres, cada usuario recibe el mensaje original

*HOLA*

**Observación 2.1** *Notar que en ambas tablas las potencias se calculan módulo 527.*

## Referencias

- [1] Grassmann W. y Tremblay J. *Matemática Discreta y Lógica*, Prentice Hall, Madrid, (1996)
- [2] Grimaldi, Ralph , *Matemática Discreta y Combinatoria*. Una introducción con aplicaciones, Addison-Wesley Iberoamericana, (1997)
- [3] Koblitz, Neal, *A Course in Number Theory and Cryptography*, Graduate Texts in Mathematics/Editorial Board, (1987)
- [4] Liu, C. L., *Elementos de Matemáticas Discretas*, McGraw-Hill 2da Edición, (1995)
- [5] Wolfram, *Mathematica* v 6.1.0.1 (2007)