

# 8.11

## Método RSA paso a paso

The logo for Cartagena99 features the text 'Cartagena99' in a stylized, dark green font. The '99' is significantly larger and more prominent than the 'Cartagena' part. The text is set against a light blue, cloud-like background that tapers to the right. Below the text, there is a horizontal orange and yellow gradient bar.

CLASES PARTICULARES, TUTORÍAS TÉCNICAS ONLINE  
LLAMA O ENVÍA WHATSAPP: 689 45 44 70

---

ONLINE PRIVATE LESSONS FOR SCIENCE STUDENTS  
CALL OR WHATSAPP:689 45 44 70

# 1) Paso previo

- Elegimos 2 primos  $p$  y  $q$  que mantenemos en secreto (los que yo quiera)
  - Ej.
    - $p = 7$
    - $q = 11$
- Calculamos el valor de su producto al que denominamos  $n = p \cdot q$ 
  - Ej.
    - $n = p \cdot q = 7 \cdot 11 = 77$

**Cartagena99**

CLASES PARTICULARES, TUTORÍAS TÉCNICAS ONLINE  
LLAMA O ENVÍA WHATSAPP: 689 45 44 70

---

ONLINE PRIVATE LESSONS FOR SCIENCE STUDENTS  
CALL OR WHATSAPP:689 45 44 70

# Paréntesis: Cálculo del máximo común divisor (Método 1)

Método 1:

- Escribimos todos los divisores de cada número, y de éstos señalamos los divisores comunes.
- El divisor mayor será el MCD de esos números.
- Ej.  $mcd(15, 20)$
- **Divisores de 15:**
  - $15 / 1 = 15$ , y resto 0 por lo que **1 y 15 son divisores de 15.**
  - $15 / 2 = 7$ , el resto es 1, por lo que **2 no es divisor de 15.**
  - $15 / 3 = 5$ , y resto 0 por lo que **3 es divisor de 15.**
  - $15 / 4 = 3$ , el resto es 3, por lo que **4 no es divisor de 15.**
  - $15 / 5 = 3$ , y resto 0 por lo que **5 es divisor de 15.**

Por tanto, los divisores de 15 son: **1, 3, 5 y 15.**

- **Divisores de 20:**
  - $20 / 1 = 20$ , y resto 0 por lo que **1 y 20 son divisores de 20.**
  - $20 / 2 = 10$ , y resto 0 por lo que **2 y 10 son divisores de 20.**
  - $20 / 3 = 6$ , el resto es 2, por lo que **3 no es un divisor de 20.**
  - $20 / 4 = 5$ , y resto 0 por lo que **4 y 5 son divisores de 20.**

The logo for Cartagena99 features the text 'Cartagena99' in a stylized, bold font. The 'C' is large and blue, while the rest of the text is in a dark green color. The logo is set against a light blue and white background with a subtle wave pattern.

CLASES PARTICULARES, TUTORÍAS TÉCNICAS ONLINE  
LLAMA O ENVÍA WHATSAPP: 689 45 44 70

---

ONLINE PRIVATE LESSONS FOR SCIENCE STUDENTS  
CALL OR WHATSAPP:689 45 44 70

# Paréntesis: Cálculo del máximo común divisor

- **Divisor común:** número que es divisor a la vez de dos o más números, es decir, es un divisor común a esos números.
  - En el ejemplo,
    - Divisores de 15: **1, 3, 5 y 15.**
    - Divisores de 20: **1, 2, 4, 5, 10 y 20.**

Los **divisores comunes que tienen 15 y 20 son el 1 y el 5.**

- Máximo común divisor es el número mayor entre los divisores comunes,
  - En el ejemplo
    - Divisores comunes de 15 y 20: **1 y 5**

**Cartagena99**

CLASES PARTICULARES, TUTORÍAS TÉCNICAS ONLINE  
LLAMA O ENVÍA WHATSAPP: 689 45 44 70

---

ONLINE PRIVATE LESSONS FOR SCIENCE STUDENTS  
CALL OR WHATSAPP:689 45 44 70

# Paréntesis: Cálculo del máximo común divisor (Método 2)

- Descomposición de factores o descomposición en números primos.
  - Descomponemos cada número en factores primos.
  - Después, señalamos los factores comunes.
  - A continuación, en cada uno de los comunes, escogemos el factor con menor exponente.
  - Y por ultimo, multiplicamos los factores elegidos.
- Ejemplo:

$$mcd(8, 12) = 4$$

8		2	12		2
4		2	6		2
2		2	3		3

Cartagena99

CLASES PARTICULARES, TUTORÍAS TÉCNICAS ONLINE  
LLAMA O ENVÍA WHATSAPP: 689 45 44 70

ONLINE PRIVATE LESSONS FOR SCIENCE STUDENTS  
CALL OR WHATSAPP:689 45 44 70

0 = 2      12 = 2 \* 3

# 1) Paso previo

- Escogemos un número  $e$  que sea primo relativo de  $(p - 1)(q - 1)$ , es decir,

$$\text{mcd}(e, (p - 1)(q - 1)) = 1$$

- Ej.

- $\text{mcd}(e, (p - 1)(q - 1)) = 1 \Rightarrow$   
 $\Rightarrow \text{mcd}(e, (7 - 1)(11 - 1)) =$   
 $\text{mcd}(e, (6)(10)) =$   
 $\text{mcd}(e, (2 \cdot 3)(2 \cdot 5)) = 1$

Luego debo escoger  $e$  no puede ser divisible por 2, 3 y 5 por ejemplo  $e = 13$

**Cartagena99**

CLASES PARTICULARES, TUTORIAS TECNICAS ONLINE  
LLAMA O ENVIA WHATSAPP: 689 45 44 70

---

ONLINE PRIVATE LESSONS FOR SCIENCE STUDENTS  
CALL OR WHATSAPP:689 45 44 70

# 1) Paso previo

- Hallamos el inverso multiplicativo de  $e \pmod{(p-1)(q-1)}$ , es decir,  $e^{-1} \pmod{(p-1)(q-1)}$  al que denominaremos  $d$

$$d = e^{-1} \pmod{(p-1)(q-1)}$$

Ej.

$$\begin{aligned} d &= e^{-1} \pmod{(p-1)(q-1)} \\ &= e^{-1} \pmod{(7-1)(11-1)} \end{aligned}$$

**Cartagena99**

CLASES PARTICULARES, TUTORIAS TECNICAS ONLINE  
LLAMA O ENVIA WHATSAPP: 689 45 44 70

---

ONLINE PRIVATE LESSONS FOR SCIENCE STUDENTS  
CALL OR WHATSAPP:689 45 44 70

# 1) Paso previo: Cálculo de $e^{-1}$

- Inverso multiplicativo de  $e$ :  $e \cdot e^{-1} \equiv 1 \pmod{((p-1)(q-1))}$
- Métodos:
  - 1) Fermat:
    - ¿  $(p-1)(q-1)$  primo?,
    - ¿  $e \neq$  múltiplo de  $(p-1)(q-1)$ ?
    - Si se cumple,  $e^{-1} = e^{((p-1)(q-1))-2}$

En el ejemplo,

- ¿  $(p-1)(q-1)$  primo?,  $(7-1)(11-1) = 60 \neq$  primo



Cartagena99

CLASES PARTICULARES, TUTORÍAS TÉCNICAS ONLINE  
LLAMA O ENVÍA WHATSAPP: 689 45 44 70

---

ONLINE PRIVATE LESSONS FOR SCIENCE STUDENTS  
CALL OR WHATSAPP: 689 45 44 70



# 1) Paso previo: Cálculo de $e^{-1}$

- Inverso multiplicativo de  $e$ :  $e \cdot e^{-1} \equiv 1 \pmod{((p-1)(q-1))}$
- Métodos:
  - 2) Euler:
    - ¿  $\text{mcd}(e, (p-1)(q-1)) = 1$ ?, es decir, ¿  $e$  y  $(p-1)(q-1)$  son primos relativos ?

OBSERVACIÓN: El requisito para que exista inverso multiplicativo es el mismo que para poder aplicar el método de Euler

En el ejemplo,

- ¿  $\text{mcd}(e, (p-1)(q-1)) = 1$ ?, ¿  $\text{mcd}(13, 60) = 1$ ?,

Luego podemos calcular el inverso multiplicativo por Euler:



1. Calcular la función indicatriz:

$$\phi((p-1)(q-1)) = (p-1)(q-1) \prod_{s \in \text{primo}}^j \left(1 - \frac{1}{s_j}\right)$$

2. Inverso multiplicativo:

**Cartagena99**

CLASES PARTICULARES, TUTORÍAS TÉCNICAS ONLINE  
LLAMA O ENVÍA WHATSAPP: 689 45 44 70

---

ONLINE PRIVATE LESSONS FOR SCIENCE STUDENTS  
CALL OR WHATSAPP: 689 45 44 70

# 1) Paso previo: Cálculo de $e^{-1}$

- Inverso multiplicativo de  $e$ :  $e \cdot e^{-1} \equiv 1 \pmod{((p-1)(q-1))}$

Luego podemos calcular el inverso multiplicativo por Euler:

1. Calcular la función indicatriz:

$$\phi((p-1)(q-1)) = (p-1)(q-1) \prod_{s \in \text{primo}}^j \left(1 - \frac{1}{s_j}\right)$$

En el ejemplo,

$$(7-1)(11-1) = (6)(10) = 60$$

$$60 \mid 2$$

$$30 \mid 2$$

$$60 = 2^2 \cdot 3 \cdot 5$$

Factores primos de 60

**Cartagena99**

CLASES PARTICULARES, TUTORÍAS TÉCNICAS ONLINE  
LLAMA O ENVÍA WHATSAPP: 689 45 44 70

---

ONLINE PRIVATE LESSONS FOR SCIENCE STUDENTS  
CALL OR WHATSAPP: 689 45 44 70

# 1) Paso previo: Cálculo de $e^{-1}$

- Inverso multiplicativo de  $e$ :  $e \cdot e^{-1} \equiv 1 \pmod{((p-1)(q-1))}$

1. (Continuación) Calcular la función indicatriz del ejemplo:

$$\phi((p-1)(q-1)) = (p-1)(q-1) \prod_{s \in \text{primo}}^j \left(1 - \frac{1}{s_j}\right)$$

$$(7-1)(11-1) = (6)(10) = 60$$

Factores primos de  $60 = 2^2 \cdot 3 \cdot 5$

$$\begin{aligned} \phi(60) &= 60 \left[1 - \frac{1}{2}\right] \left[1 - \frac{1}{3}\right] \left[1 - \frac{1}{5}\right] \\ &= 60 \left[\frac{1}{2}\right] \left[\frac{2}{3}\right] \left[\frac{4}{5}\right] = 16 \end{aligned}$$

2. Inverso multiplicativo:

The logo for Cartagena99, featuring the text "Cartagena99" in a stylized font with a blue and orange gradient background.

CLASES PARTICULARES, TUTORÍAS TÉCNICAS ONLINE  
LLAMA O ENVÍA WHATSAPP: 689 45 44 70

---

ONLINE PRIVATE LESSONS FOR SCIENCE STUDENTS  
CALL OR WHATSAPP: 689 45 44 70

# 1) Paso previo: Cálculo de $e^{-1}$

- Inverso multiplicativo de  $e$ :  $e \cdot e^{-1} \equiv 1 \pmod{((p-1)(q-1))}$

2. Inverso multiplicativo:

$$e^{-1} = e^{\overset{d}{\phi((p-1)(q-1))^{-1}}} \pmod{((p-1)(q-1))}$$

En el ejemplo,

$$13^{-1} = 13^{\overset{d}{\phi(60)^{-1}}} \pmod{60}$$

$$13^{-1} = 13^{16^{-1}} \pmod{60}$$

$$13^{-1} = 13^{15} \pmod{60}$$

**Cartagena99**

CLASES PARTICULARES, TUTORÍAS TÉCNICAS ONLINE  
LLAMA O ENVÍA WHATSAPP: 689 45 44 70

---

ONLINE PRIVATE LESSONS FOR SCIENCE STUDENTS  
CALL OR WHATSAPP: 689 45 44 70

# 1) Paso previo: Cálculo de $e^{-1}$

- Inverso multiplicativo de  $e$ :  $e \cdot e^{-1} \equiv 1 \pmod{((p-1)(q-1))}$

2. Inverso multiplicativo:

Luego debemos calcular  $13^{15} \pmod{60}$  mediante el método de las potencias de 2.

Descomponemos el exponente, 15, en potencias de 2:

$$8 = 2^3$$

$$4 = 2^2$$

$$2 = 2^1$$

$$1 = 2^0$$

The logo for Cartagena99 features the text "Cartagena99" in a stylized, bold font. The "C" is large and blue, while "artagena99" is in a dark green color. The text is set against a light blue and orange gradient background.

CLASES PARTICULARES, TUTORÍAS TÉCNICAS ONLINE  
LLAMA O ENVÍA WHATSAPP: 689 45 44 70

---

ONLINE PRIVATE LESSONS FOR SCIENCE STUDENTS  
CALL OR WHATSAPP:689 45 44 70

# 1) Paso previo: Cálculo de $e^{-1}$

- Inverso multiplicativo de  $e$ :  $e \cdot e^{-1} \equiv 1 \pmod{(p-1)(q-1)}$

2. Inverso multiplicativo:

$$13^{15} = 13^8 \cdot 13^4 \cdot 13^2 \cdot 13^1$$

Operamos utilizando la aritmética modular,

$$13^2 = 169 \equiv 49 \pmod{60}$$

$$\begin{array}{r|l} 169 & 60 \\ \hline & 2 \\ \hline 49 & \end{array}$$

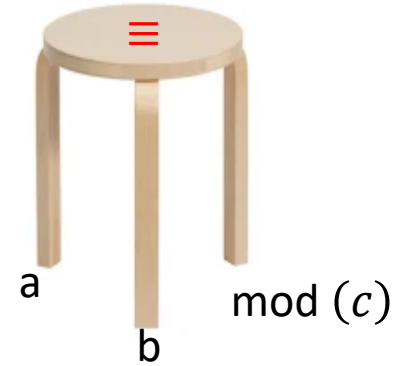
luego 49 es el resto  
(169 % 60)

$$13^4 = (13^2)^2 \equiv 49^2 = 2401 \equiv 1 \pmod{60} \quad (2401 \% 60 = 1)$$

$$13^8 = (13^4)^2 \equiv 1^2 = 1 \pmod{60}$$

$$13^{15} \equiv 1 \cdot 1 \cdot 49 \cdot 13 = 637 \equiv 37 \pmod{60} \quad (637 \% 60 = 37)$$

= operación "normal Ej.  $2 \cdot 2 = 4$   
 $a \equiv b \pmod{c} \Rightarrow$   
 $\Rightarrow$  cálculo de restos:  $res(a, c) = b$



**Cartagena99**

CLASES PARTICULARES, TUTORIAS TECNICAS ONLINE  
 LLAMA O ENVIA WHATSAPP: 689 45 44 70

ONLINE PRIVATE LESSONS FOR SCIENCE STUDENTS  
 CALL OR WHATSAPP: 689 45 44 70

# 1) Paso previo: Claves pública y privada

El final de este paso viene dado por la definición de las claves pública y privada con los elementos calculados anteriormente:

- CLAVE PÚBLICA:  $(e, n)$
  - CLAVE PRIVADA:  $(d, n)$
- Sistema de cifrado asimétrico

En el ejemplo,

- CLAVE PÚBLICA:  $(13, 77)$
- CLAVE PRIVADA:  $(37, 77)$

The logo for Cartagena99 features the text 'Cartagena99' in a stylized, green, serif font. The '99' is significantly larger and more prominent than the 'Cartagena' part. The text is set against a light blue and white background with a subtle wave-like pattern.

CLASES PARTICULARES, TUTORÍAS TÉCNICAS ONLINE  
LLAMA O ENVÍA WHATSAPP: 689 45 44 70

---

ONLINE PRIVATE LESSONS FOR SCIENCE STUDENTS  
CALL OR WHATSAPP: 689 45 44 70

## 2) Cifrado

- Para cifrar un mensaje  $m$ , lo elegimos tal que

$$\text{mcd}(m, n) = 1$$

Entonces,

$m$  y  $n$  son primos relativos

$$m' = \text{res}(m^e, n)$$

Ej. Para el ejemplo vamos a suponer que hemos capturado 4 mensajes cifrados por lo que no vamos a tener que descifrarlos (podría haberlos pedido el cifrado)

$$m'_1 = 37$$

$$m'_2 = 26$$

The logo for Cartagena99 features the text 'Cartagena99' in a stylized, bold font. The 'C' is large and blue, while the rest of the text is in a dark green color. The logo is set against a light blue and orange gradient background.

CLASES PARTICULARES, TUTORÍAS TÉCNICAS ONLINE  
LLAMA O ENVÍA WHATSAPP: 689 45 44 70

---

ONLINE PRIVATE LESSONS FOR SCIENCE STUDENTS  
CALL OR WHATSAPP:689 45 44 70



### 3) Descifrado

- Para descifrar el mensaje debemos aplicar

$$m = \text{res}(m'^d, n) = m_1'^d \pmod{n}$$

Para el ejemplo,

$$\begin{aligned} m_1 &= m_3 = 37^{37} \pmod{77} \\ m_2 &= m_4 = 26^{37} \pmod{77} \end{aligned}$$

Luego de nuevo debemos de aplicar la aritmética modular para

The logo for Cartagena99 features the text 'Cartagena99' in a stylized, bold font. The 'C' is large and blue, while the rest of the text is in a dark green color. The logo is set against a light blue and orange gradient background.

CLASES PARTICULARES, TUTORÍAS TÉCNICAS ONLINE  
LLAMA O ENVÍA WHATSAPP: 689 45 44 70

---

ONLINE PRIVATE LESSONS FOR SCIENCE STUDENTS  
CALL OR WHATSAPP:689 45 44 70

# 3) Descifrado (continuación ejemplo)

- $m_1 = m_3 = 37^{37} \pmod{77}$

- Descomponemos el exponente, 37, en potencias de 2:

$$\begin{aligned} 32 &= 2^5 \\ 4 &= 2^2 \\ 1 &= 2^0 \end{aligned}$$

luego

$$37^{37} = 37^{32} \cdot 37^4 \cdot 37^1$$

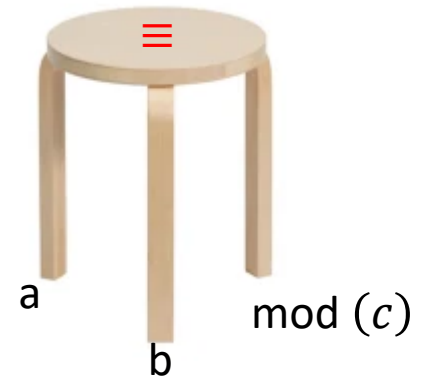
Operando con la aritmética modular,

$$\begin{aligned} 37^2 &= 1369 \equiv 60 \pmod{77} && (1369 \% 77 = 60) \\ 37^4 &= (37^2)^2 \equiv 60^2 = 3600 \equiv 58 \pmod{77} && (3600 \% 77 = 58) \\ 37^8 &= (37^4)^2 \equiv 58^2 = 3364 \equiv 53 \pmod{77} && (3364 \% 77 = 53) \\ 37^{16} &= (37^8)^2 \equiv 53^2 = 2809 \equiv 37 \pmod{77} && (2809 \% 77 = 37) \end{aligned}$$

= operación "normal Ej.  $2 \cdot 2 = 4$

$$a \equiv b \pmod{c} \Rightarrow$$

$\Rightarrow$  cálculo de restos:  $res(a, c) = b$



Cartagena99

CLASES PARTICULARES, TUTORIAS TECNICAS ONLINE  
LLAMA O ENVIA WHATSAPP: 689 45 44 70

ONLINE PRIVATE LESSONS FOR SCIENCE STUDENTS  
CALL OR WHATSAPP: 689 45 44 70

teniendo en cuenta el abecedario,  $m_1 = m_3 = 16 \Rightarrow P$

### 3) Descifrado (continuación ejemplo)

- $m_2 = m_4 = 26^{37} \pmod{77}$ 
  - Descomponemos el exponente, 37, en potencias de 2:

$$\begin{aligned}32 &= 2^5 \\4 &= 2^2 \\1 &= 2^0\end{aligned}$$

luego

$$26^{37} = 26^{32} \cdot 26^4 \cdot 26^1$$

Operando con la aritmética modular,

$$\begin{aligned}26^2 &= 676 \equiv 60 \pmod{77} \\26^4 &= (26^2)^2 \equiv 60^2 = 3600 \equiv 58 \pmod{77} \\26^8 &= (26^4)^2 \equiv 58^2 = 3364 \equiv 53 \pmod{77} \\26^{16} &= (26^8)^2 \equiv 53^2 = 2809 \equiv 37 \pmod{77}\end{aligned}$$



CLASES PARTICULARES, TUTORIAS TECNICAS ONLINE  
LLAMA O ENVIA WHATSAPP: 689 45 44 70

---

ONLINE PRIVATE LESSONS FOR SCIENCE STUDENTS  
CALL OR WHATSAPP:689 45 44 70

teniendo en cuenta el abecedario,  $m_1 = m_3 = J \rightarrow L$

ve el mensaje total es  $m_1 m_2 m_3 m_4 = PEPE$

# Resumen

## 1. Paso previo

1. Elegimos 2 primos  $p$  y  $q$  que mantenemos en secreto (los que yo quiera)
2. Escogemos un número  $e$  que sea primo relativo de  $(p - 1)(q - 1)$ , es decir,

$$\text{mcd}(e, (p - 1)(q - 1)) = 1$$

3. Hallamos el inverso multiplicativo de  $e \pmod{(p - 1)(q - 1)}$ , es decir,  $e^{-1} \pmod{(p - 1)(q - 1)}$  al que denominaremos  $d$

- CLAVE PÚBLICA:  $(e, n)$
- CLAVE PRIVADA:  $(d, n)$

## 2. Cifrado:

- Para cifrar un mensaje  $m$ , lo elegimos tal que

$$\text{mcd}(m, n) = 1$$

$$m' = \text{res}(m^e, n)$$

## 3. Descifrado:

The logo for Cartagena99 features the text 'Cartagena99' in a stylized, bold font. The 'C' is large and blue, while 'artagena99' is in a dark green color. The text is set against a light blue and orange gradient background.

CLASES PARTICULARES, TUTORÍAS TÉCNICAS ONLINE  
LLAMA O ENVÍA WHATSAPP: 689 45 44 70

---

ONLINE PRIVATE LESSONS FOR SCIENCE STUDENTS  
CALL OR WHATSAPP:689 45 44 70