

# RSA

Segunda parte: descifrar el mensaje

Daniel Felipe Triviño

Asistente graduado · Fundamentos Matemáticos para la Computación · Universidad de los Andes



1. Lo que tenemos

$$(n, e) = (91, 11)$$

|     |    |   |    |   |    |    |   |    |    |    |    |    |   |    |    |
|-----|----|---|----|---|----|----|---|----|----|----|----|----|---|----|----|
| $c$ | 38 | 0 | 86 | 0 | 58 | 58 | 0 | 61 | 23 | 58 | 61 | 23 | 1 | 23 | 75 |
|-----|----|---|----|---|----|----|---|----|----|----|----|----|---|----|----|

$$p = 7, \quad q = 13, \quad \varphi(n) = (7 - 1)(13 - 1) = 72$$

Quien recibe conoce  $p$ ,  $q$  y  $\varphi(n)$ .

2. La clave privada  $d$

$$(n, e) = (91, 11)$$

$c$             38    0    86    0    58    58    0    61    23    58    61    23    1    23    75

$$d = e^{-1} \bmod \varphi(n) = 11^{-1} \bmod 72$$

$$11 \cdot d \equiv 1 \pmod{72}$$

$d$  es el inverso de  $e$  módulo  $\varphi(n)$ .

2. La clave privada  $d$

$$(n, e) = (91, 11)$$

$c$       38    0    86    0    58    58    0    61    23    58    61    23    1    23    75

$$d = 11^{-1} \bmod 72 = ?$$

$$72 = 11 \times 6 + 6$$

$$11 = 6 \times 1 + 5$$

$$6 = 5 \times 1 + 1$$

$$5 = 1 \times 5 + 0$$

Algoritmo extendido de Euclides con 72 y 11.

2. La clave privada  $d$

$$(n, e) = (91, 11)$$

$c$             38    0    86    0    58    58    0    61    23    58    61    23    1    23    75

$$d = 11^{-1} \bmod 72 = ?$$

$$72 = 11 \times 6 + 6$$

$$11 = 6 \times 1 + 5$$

$$6 = 5 \times 1 + 1$$

$$5 = 1 \times 5 + 0$$

| $i$ | $r_i$ | $q_i$ | $s_i$ | $t_i$ |
|-----|-------|-------|-------|-------|
| 1   | 72    | —     | 1     | 0     |
| 2   | 11    | 6     | 0     | 1     |
| 3   | 6     | 1     |       |       |
| 4   | 5     | 1     |       |       |
| 5   | 1     | 5     |       |       |

Algoritmo extendido de Euclides con 72 y 11.

2. La clave privada  $d$

$$(n, e) = (91, 11)$$

$c$             38    0    86    0    58    58    0    61    23    58    61    23    1    23    75

$$d = 11^{-1} \bmod 72 = ?$$

$$72 = 11 \times 6 + 6$$

$$11 = 6 \times 1 + 5$$

$$6 = 5 \times 1 + 1$$

$$5 = 1 \times 5 + 0$$

| $i$ | $r_i$ | $q_i$ | $s_i$ | $t_i$ |
|-----|-------|-------|-------|-------|
| 1   | 72    | —     | 1     | 0     |
| 2   | 11    | 6     | 0     | 1     |
| 3   | 6     | 1     | 1     | -6    |
| 4   | 5     | 1     |       |       |
| 5   | 1     | 5     |       |       |

Dos filas arriba, menos el cociente por la fila anterior.

2. La clave privada  $d$

$$(n, e) = (91, 11)$$

$c$             38    0    86    0    58    58    0    61    23    58    61    23    1    23    75

$$d = 11^{-1} \bmod 72 = ?$$

$$72 = 11 \times 6 + 6$$

$$11 = 6 \times 1 + 5$$

$$6 = 5 \times 1 + 1$$

$$5 = 1 \times 5 + 0$$

| $i$ | $r_i$ | $q_i$ | $s_i$ | $t_i$ |
|-----|-------|-------|-------|-------|
| 1   | 72    | —     | 1     | 0     |
| 2   | 11    | 6     | 0     | 1     |
| 3   | 6     | 1     | 1     | −6    |
| 4   | 5     | 1     | −1    | 7     |
| 5   | 1     | 5     | 2     | −13   |

Dos filas arriba, menos el cociente por la fila anterior.

2. La clave privada  $d$

$$(n, e) = (91, 11)$$

$c$             38    0    86    0    58    58    0    61    23    58    61    23    1    23    75

$$d = 11^{-1} \bmod 72 = ?$$

$$72 \times 2 + 11 \times (-13) = 1$$

| $i$ | $r_i$ | $q_i$ | $s_i$ | $t_i$ |
|-----|-------|-------|-------|-------|
| 1   | 72    | —     | 1     | 0     |
| 2   | 11    | 6     | 0     | 1     |
| 3   | 6     | 1     | 1     | -6    |
| 4   | 5     | 1     | -1    | 7     |
| 5   | 1     | 5     | 2     | -13   |

Dos filas arriba, menos el cociente por la fila anterior.

2. La clave privada  $d$

$$(n, e) = (91, 11)$$

$c$             38    0    86    0    58    58    0    61    23    58    61    23    1    23    75

$$d = 11^{-1} \bmod 72 = ?$$

$$72 \times 2 + 11 \times (-13) = 1$$

Sustitución hacia atrás

$$6 = 72 - 11 \times 6$$

$$5 = 11 - 6 \times 1$$

$$1 = 6 - 5 \times 1$$

$$1 = 6 \times 2 - 11 \times 1$$

$$1 = 72 \times 2 - 11 \times 13$$

También sale por sustitución hacia atrás.

2. La clave privada  $d$

$$(n, e) = (91, 11)$$

$c$             38    0    86    0    58    58    0    61    23    58    61    23    1    23    75

$$d = 11^{-1} \bmod 72 = ?$$

$$\cancel{72} \times 2 + 11 \times (-13) = 1$$

$$11 \times (-13) \equiv 1 \pmod{72}$$

Módulo 72, todo múltiplo de 72 vale 0.

2. La clave privada  $d$

$$(n, e) = (91, 11)$$

$c$             38    0    86    0    58    58    0    61    23    58    61    23    1    23    75

$$d = 11^{-1} \bmod 72 = ?$$

$$\cancel{72} \times 2 + 11 \times (-13) = 1$$

$$11 \times (-13) \equiv 1 \pmod{72}$$

$$d = -13 \bmod 72 = 59$$

El inverso de  $e$  es el coeficiente que lo acompaña:  $t$ .

2. La clave privada  $d$

$$(n, e) = (91, 11)$$

$c$             38    0    86    0    58    58    0    61    23    58    61    23    1    23    75

$$d = 11^{-1} \bmod 72 = ?$$

$$\cancel{72} \times 2 + 11 \times (-13) = 1$$

$$11 \times (-13) \equiv 1 \pmod{72}$$

$$11 \times 59 = 649 = 72 \times 9 + 1 \quad \checkmark$$

$$d = -13 \bmod 72 = 59$$

11 · 59 deja residuo 1 al dividir entre 72.

3. Descifrar:  $m = c^d$  módulo  $n$

$$(n, e) = (91, 11)$$

$$d = 59$$

$c$             38    0    86    0    58    58    0    61    23    58    61    23    1    23    75

$m$

$$m = c^d \bmod n$$

$$m = c^{59} \bmod 91$$

Descifrar es la misma operación, con el exponente  $d$ .

3. Descifrar:  $m = c^d$  módulo  $n$

$(n, e) = (91, 11)$   
 $d = 59$

$c$   
 $m$

38086058580612358612312375

$59 = 32 + 16 + 8 + 2 + 1 = (111011)_2$

543210

| $i$ | $b_i$ | Square | Multiply |
|-----|-------|--------|----------|
|-----|-------|--------|----------|

---

Square: siempre. Multiply: solo si el bit es 1.

3. Descifrar:  $m = c^d$  módulo  $n$

$$(n, e) = (91, 11) \quad d = 59$$

|     |    |   |    |   |    |    |   |    |    |    |    |    |   |    |    |
|-----|----|---|----|---|----|----|---|----|----|----|----|----|---|----|----|
| $c$ | 38 | 0 | 86 | 0 | 58 | 58 | 0 | 61 | 23 | 58 | 61 | 23 | 1 | 23 | 75 |
| $m$ |    |   |    |   |    |    |   |    |    |    |    |    |   |    |    |

$$m = 38^{59} \bmod 91$$

$$59 = 32 + 16 + 8 + 2 + 1 = \begin{pmatrix} 1 & 1 & 1 & 0 & 1 & 1 \end{pmatrix}_2$$

5   4   3   2   1   0

|     |       |        |          |
|-----|-------|--------|----------|
| $i$ | $b_i$ | Square | Multiply |
|-----|-------|--------|----------|

---

Square: siempre. Multiply: solo si el bit es 1.

3. Descifrar:  $m = c^d \text{ módulo } n$ 

$(n, e) = (91, 11)$ 
 $d = 59$

$c$

$m$

38

0
86
0
58
58
0
61
23
58
61
23
1
23
75

$m = 38^{59} \text{ mod } 91$ 

$59 = 32 + 16 + 8 + 2 + 1 =$ 

1

1

1

0

1

1

5

4

3

2

1

0

| $i$ | $b_i$ | Square        | Multiply               |
|-----|-------|---------------|------------------------|
| 5   | 1     | $w = 1^2 = 1$ | $w = 1 \times 38 = 38$ |

Square: siempre. Multiply: solo si el bit es 1.

3. Descifrar:  $m = c^d \text{ módulo } n$

$(n, e) = (91, 11)$

$d = 59$

$c$

38

0

86

0

58

58

0

61

23

58

61

23

1

23

75

$m$

$m = 38^{59} \text{ mod } 91$

59 = 32 + 16 + 8 + 2 + 1 =

1

1

1

0

1

1

5

4

3

2

1

0

| $i$ | $b_i$ | Square                      | Multiply                            |
|-----|-------|-----------------------------|-------------------------------------|
| 5   | 1     | $w = 1^2 = 1$               | $w = 1 \times 38 = 38$              |
| 4   | 1     | $w = 38^2 = 1444 \equiv 79$ | $w = 79 \times 38 = 3002 \equiv 90$ |

Square: siempre. Multiply: solo si el bit es 1.

3. Descifrar:  $m = c^d \text{ módulo } n$

$(n, e) = (91, 11)$

$d = 59$

$c$

38

0

86

0

58

58

0

61

23

58

61

23

1

23

75

$m$

$m = 38^{59} \text{ mod } 91$

$59 = 32 + 16 + 8 + 2 + 1 =$ 

1

1

1

0

1

1

5

4

3

2

1

0

| $i$ | $b_i$ | Square                      | Multiply                            |
|-----|-------|-----------------------------|-------------------------------------|
| 5   | 1     | $w = 1^2 = 1$               | $w = 1 \times 38 = 38$              |
| 4   | 1     | $w = 38^2 = 1444 \equiv 79$ | $w = 79 \times 38 = 3002 \equiv 90$ |
| 3   | 1     | $w = 90^2 = 8100 \equiv 1$  | $w = 1 \times 38 = 38$              |

Square: siempre. Multiply: solo si el bit es 1.

3. Descifrar:  $m = c^d$  módulo  $n$

$(n, e) = (91, 11)$   
 $d = 59$

$c$   
 $m$

38

0

86

0

58

58

0

61

23

58

61

23

1

23

75

$m = 38^{59} \bmod 91$

$59 = 32 + 16 + 8 + 2 + 1 = \begin{pmatrix} 1 & 1 & 1 & 0 & 1 & 1 \\ 5 & 4 & 3 & 2 & 1 & 0 \end{pmatrix}_2$

| $i$ | $b_i$ | Square                      | Multiply                            |
|-----|-------|-----------------------------|-------------------------------------|
| 5   | 1     | $w = 1^2 = 1$               | $w = 1 \times 38 = 38$              |
| 4   | 1     | $w = 38^2 = 1444 \equiv 79$ | $w = 79 \times 38 = 3002 \equiv 90$ |
| 3   | 1     | $w = 90^2 = 8100 \equiv 1$  | $w = 1 \times 38 = 38$              |
| 2   | 0     | $w = 38^2 = 1444 \equiv 79$ |                                     |

Square: siempre. Multiply: solo si el bit es 1.

3. Descifrar:  $m = c^d \text{ módulo } n$

$(n, e) = (91, 11)$  $d = 59$

$c$  $m$

38

086058580612358612312375

$m = 38^{59} \text{ mod } 91$

$59 = 32 + 16 + 8 + 2 + 1 = \left( \begin{smallmatrix} 1 & 1 & 1 & 0 & 1 & 1 \\ 5 & 4 & 3 & 2 & 1 & 0 \end{smallmatrix} \right)_2$

| $i$ | $b_i$ | Square                      | Multiply                            |
|-----|-------|-----------------------------|-------------------------------------|
| 5   | 1     | $w = 1^2 = 1$               | $w = 1 \times 38 = 38$              |
| 4   | 1     | $w = 38^2 = 1444 \equiv 79$ | $w = 79 \times 38 = 3002 \equiv 90$ |
| 3   | 1     | $w = 90^2 = 8100 \equiv 1$  | $w = 1 \times 38 = 38$              |
| 2   | 0     | $w = 38^2 = 1444 \equiv 79$ | —                                   |
| 1   | 1     | $w = 79^2 = 6241 \equiv 53$ | $w = 53 \times 38 = 2014 \equiv 12$ |

Square: siempre. Multiply: solo si el bit es 1.

3. Descifrar:  $m = c^d$  módulo  $n$

$(n, e) = (91, 11)$

$d = 59$

$c$

38

0

86

0

58

58

0

61

23

58

61

23

1

23

75

$m$

$m = 38^{59} \bmod 91$

$59 = 32 + 16 + 8 + 2 + 1 =$ 

1

1

1

0

1

1

5

4

3

2

1

0

| $i$ | $b_i$ | Square                      | Multiply                            |
|-----|-------|-----------------------------|-------------------------------------|
| 5   | 1     | $w = 1^2 = 1$               | $w = 1 \times 38 = 38$              |
| 4   | 1     | $w = 38^2 = 1444 \equiv 79$ | $w = 79 \times 38 = 3002 \equiv 90$ |
| 3   | 1     | $w = 90^2 = 8100 \equiv 1$  | $w = 1 \times 38 = 38$              |
| 2   | 0     | $w = 38^2 = 1444 \equiv 79$ | —                                   |
| 1   | 1     | $w = 79^2 = 6241 \equiv 53$ | $w = 53 \times 38 = 2014 \equiv 12$ |
| 0   | 1     | $w = 12^2 = 144 \equiv 53$  | $w = 53 \times 38 = 2014 \equiv 12$ |

Square: siempre.

Multiply: solo si el bit es 1.

3. Descifrar:  $m = c^d$  módulo  $n$

$(n, e) = (91, 11)$   
 $d = 59$

|       |    |   |    |   |    |    |   |    |    |    |    |    |   |    |    |
|-------|----|---|----|---|----|----|---|----|----|----|----|----|---|----|----|
| $c$   | 38 | 0 | 86 | 0 | 58 | 58 | 0 | 61 | 23 | 58 | 61 | 23 | 1 | 23 | 75 |
| $m$   | 12 |   |    |   |    |    |   |    |    |    |    |    |   |    |    |
| letra | M  |   |    |   |    |    |   |    |    |    |    |    |   |    |    |

$m = 38^{59} \bmod 91 = 12$

$59 = 32 + 16 + 8 + 2 + 1 = \begin{pmatrix} 1 & 1 & 1 & 0 & 1 & 1 \end{pmatrix}_2$   

543210

| $i$ | $b_i$ | Square                      | Multiply                            |
|-----|-------|-----------------------------|-------------------------------------|
| 5   | 1     | $w = 1^2 = 1$               | $w = 1 \times 38 = 38$              |
| 4   | 1     | $w = 38^2 = 1444 \equiv 79$ | $w = 79 \times 38 = 3002 \equiv 90$ |
| 3   | 1     | $w = 90^2 = 8100 \equiv 1$  | $w = 1 \times 38 = 38$              |
| 2   | 0     | $w = 38^2 = 1444 \equiv 79$ | —                                   |
| 1   | 1     | $w = 79^2 = 6241 \equiv 53$ | $w = 53 \times 38 = 2014 \equiv 12$ |
| 0   | 1     | $w = 12^2 = 144 \equiv 53$  | $w = 53 \times 38 = 2014 \equiv 12$ |

Square: siempre. Multiply: solo si el bit es 1.

3. Descifrar:  $m = c^d \text{ módulo } n$ 

$(n, e) = (91, 11)$ 
 $d = 59$

|       |    |   |    |   |    |    |   |    |    |    |    |    |   |    |    |
|-------|----|---|----|---|----|----|---|----|----|----|----|----|---|----|----|
| $c$   | 38 | 0 | 86 | 0 | 58 | 58 | 0 | 61 | 23 | 58 | 61 | 23 | 1 | 23 | 75 |
| $m$   | 12 |   |    |   |    |    |   |    |    |    |    |    |   |    |    |
| letra | M  |   |    |   |    |    |   |    |    |    |    |    |   |    |    |

$m = 0^{59} \text{ mod } 91$ 

$59 = 32 + 16 + 8 + 2 + 1 =$ 

1

1

1

0

1

1

5

4

3

2

1

0

|     |       |        |          |
|-----|-------|--------|----------|
| $i$ | $b_i$ | Square | Multiply |
|-----|-------|--------|----------|

---

Square: siempre.
Multiply: solo si el bit es 1.

3. Descifrar:  $m = c^d$  módulo  $n$ 

$(n, e) = (91, 11)$

$d = 59$

|       |    |   |    |   |    |    |   |    |    |    |    |    |   |    |    |
|-------|----|---|----|---|----|----|---|----|----|----|----|----|---|----|----|
| $c$   | 38 | 0 | 86 | 0 | 58 | 58 | 0 | 61 | 23 | 58 | 61 | 23 | 1 | 23 | 75 |
| $m$   | 12 | 0 |    |   |    |    |   |    |    |    |    |    |   |    |    |
| letra | M  | A |    |   |    |    |   |    |    |    |    |    |   |    |    |

$m = 0^{59} \bmod 91 = 0$ 

$59 = 32 + 16 + 8 + 2 + 1 =$ 

1

1

1

0

1

1

5

4

3

2

1

0

| $i$ | $b_i$ | Square        | Multiply             |
|-----|-------|---------------|----------------------|
| 5   | 1     | $w = 1^2 = 1$ | $w = 1 \times 0 = 0$ |
| 4   | 1     | $w = 0^2 = 0$ | $w = 0 \times 0 = 0$ |
| 3   | 1     | $w = 0^2 = 0$ | $w = 0 \times 0 = 0$ |
| 2   | 0     | $w = 0^2 = 0$ | —                    |
| 1   | 1     | $w = 0^2 = 0$ | $w = 0 \times 0 = 0$ |
| 0   | 1     | $w = 0^2 = 0$ | $w = 0 \times 0 = 0$ |

Square: siempre.
Multiply: solo si el bit es 1.

3. Descifrar:  $m = c^d$  módulo  $n$

$(n, e) = (91, 11)$

$d = 59$

|       |    |   |    |   |    |    |   |    |    |    |    |    |   |    |    |
|-------|----|---|----|---|----|----|---|----|----|----|----|----|---|----|----|
| $c$   | 38 | 0 | 86 | 0 | 58 | 58 | 0 | 61 | 23 | 58 | 61 | 23 | 1 | 23 | 75 |
| $m$   | 12 | 0 | 18 | 0 | 11 | 11 | 0 | 3  | 4  | 11 | 3  | 4  | 1 | 4  | 17 |
| letra | M  | A | S  | A | L  | L  | A | D  | E  | L  | D  | E  | B | E  | R  |

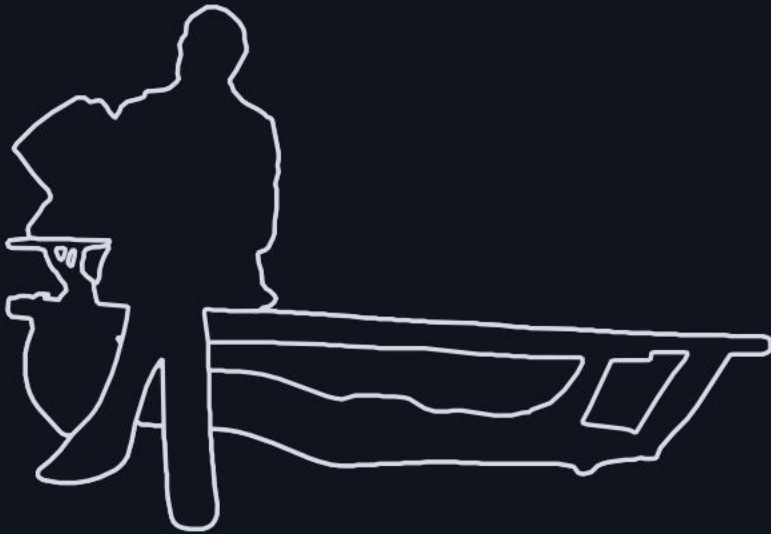
Square: siempre. Multiply: solo si el bit es 1.

3. Descifrar:  $m = c^d \text{ módulo } n$

$(n, e) = (91, 11)$

$d = 59$

|       |    |   |    |   |    |    |   |    |    |    |    |    |   |    |    |
|-------|----|---|----|---|----|----|---|----|----|----|----|----|---|----|----|
| $c$   | 38 | 0 | 86 | 0 | 58 | 58 | 0 | 61 | 23 | 58 | 61 | 23 | 1 | 23 | 75 |
| $m$   | 12 | 0 | 18 | 0 | 11 | 11 | 0 | 3  | 4  | 11 | 3  | 4  | 1 | 4  | 17 |
| letra | M  | A | S  | A | L  | L  | A | D  | E  | L  | D  | E  | B | E  | R  |



MAS ALLA DEL DEBER

Más allá del deber

Uno de los lemas de la Universidad de los Andes

Estatua de Mario Laserna, en el campus

Las tildes no viajaron: el alfabeto no las tiene.

4. ¿Por qué funciona?

$$c^d = (m^e)^d = m^{e \cdot d}$$

4. ¿Por qué funciona?

$$c^d = (m^e)^d = m^{e \cdot d} \equiv m \pmod{n}$$

$$e \cdot d \equiv 1 \pmod{\varphi(n)}$$

$$11 \times 59 = 649 = 72 \times 9 + 1$$

Teorema de Euler:  $m^{e \cdot d} \equiv m \pmod{n}$ .

4. ¿Por qué funciona?

$$c^d = (m^e)^d = m^{e \cdot d} \equiv m \pmod{n}$$

$$e \cdot d \equiv 1 \pmod{\varphi(n)}$$

$$11 \times 59 = 649 = 72 \times 9 + 1$$

$$91 = 7 \times 13$$

Si  $p$  y  $q$  no son primos no hay  $\varphi(n)$ , y sin  $\varphi(n)$  no hay  $d$ .

RSA, de principio a fin

## RSA, de principio a fin

1. Dos primos  $p$  y  $q$ :  $n = p \times q$ ,  $\varphi(n) = (p - 1)(q - 1)$ .

## RSA, de principio a fin

1. Dos primos  $p$  y  $q$ :  $n = p \times q$ ,  $\varphi(n) = (p - 1)(q - 1)$ .
2. Un exponente  $e$  con  $\text{mcd}(e, \varphi(n)) = 1$ . Clave pública:  $(n, e)$ .

## RSA, de principio a fin

1. Dos primos  $p$  y  $q$ :  $n = p \times q$ ,  $\varphi(n) = (p - 1)(q - 1)$ .
2. Un exponente  $e$  con  $\text{mcd}(e, \varphi(n)) = 1$ . Clave pública:  $(n, e)$ .
3. Cifrar:  $c = m^e$  módulo  $n$ , con square and multiply.

## RSA, de principio a fin

1. Dos primos  $p$  y  $q$ :  $n = p \times q$ ,  $\varphi(n) = (p - 1)(q - 1)$ .
2. Un exponente  $e$  con  $\text{mcd}(e, \varphi(n)) = 1$ . Clave pública:  $(n, e)$ .
3. Cifrar:  $c = m^e$  módulo  $n$ , con square and multiply.
4. Clave privada:  $d = e^{-1}$  módulo  $\varphi(n)$ , con Euclides extendido.

## RSA, de principio a fin

1. Dos primos  $p$  y  $q$ :  $n = p \times q$ ,  $\varphi(n) = (p - 1)(q - 1)$ .
2. Un exponente  $e$  con  $\text{mcd}(e, \varphi(n)) = 1$ . Clave pública:  $(n, e)$ .
3. Cifrar:  $c = m^e$  módulo  $n$ , con square and multiply.
4. Clave privada:  $d = e^{-1}$  módulo  $\varphi(n)$ , con Euclides extendido.
5. Descifrar:  $m = c^d$  módulo  $n$ .