

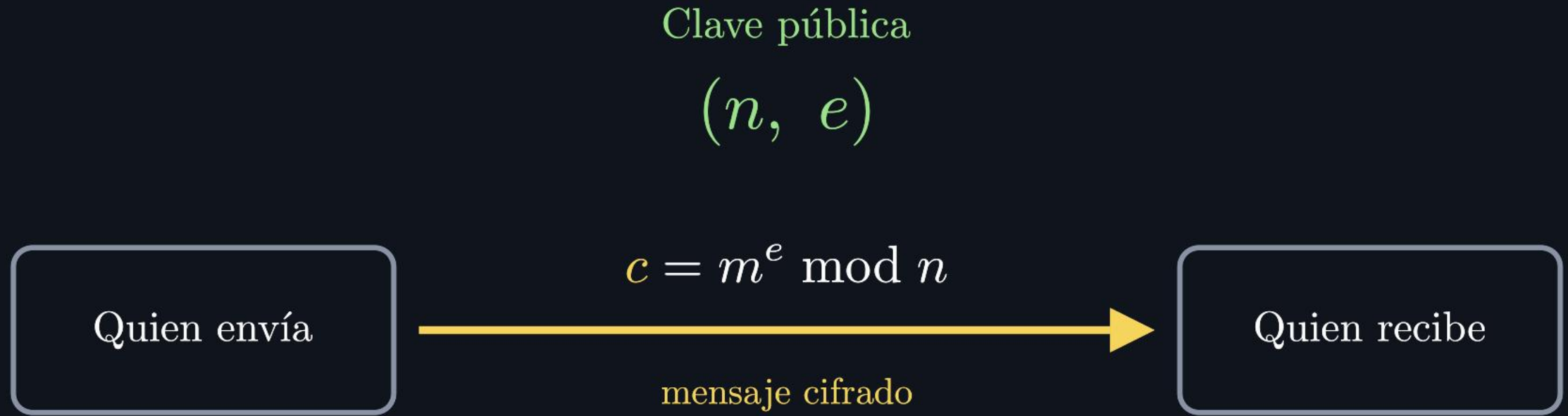
RSA

Primera parte: cifrar un mensaje

Daniel Felipe Triviño

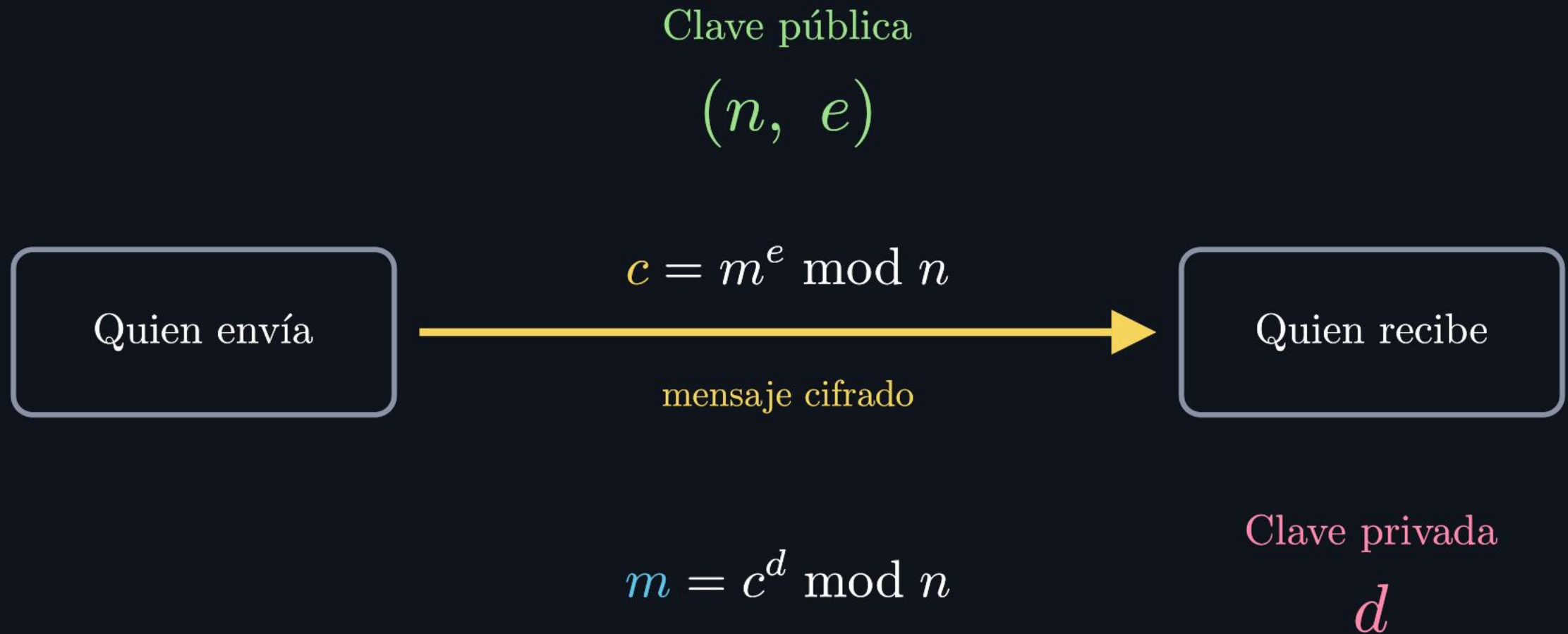
Asistente graduado · Fundamentos Matemáticos para la Computación · Universidad de los Andes

1. La idea



Clave pública: la conocen todos y sirve para cifrar.

1. La idea



Clave privada: solo la tiene quien recibe, y sirve para descifrar.

2. Armar la clave pública

$$p = 7, \quad q = 13$$

p y q : dos primos secretos.

2. Armar la clave pública

$$p = 7, \quad q = 13$$

$$n = p \times q = 7 \times 13 = 91$$

p y q : dos primos secretos.

2. Armar la clave pública

$$p = 7, \quad q = 13$$

$$n = p \times q = 7 \times 13 = 91$$

$$\varphi(n) = (p - 1)(q - 1) = 6 \times 12 = 72$$

$\varphi(n) = (p - 1)(q - 1)$ también se guarda en secreto.

2. Armar la clave pública

$$p = 7, \quad q = 13$$

$$n = p \times q = 7 \times 13 = 91$$

$$\varphi(n) = (p - 1)(q - 1) = 6 \times 12 = 72$$

$$e = 11 \quad \text{mcd}(e, \varphi(n)) = 1$$

e y $\varphi(n)$ deben ser primos relativos.

2. Armar la clave pública

$$p = 7, \quad q = 13$$

Euclides

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

$$n = p \times q = 7 \times 13 = 91$$

$$\varphi(n) = (p - 1)(q - 1) = 6 \times 12 = 72$$

$$e = 11 \quad \text{mcd}(e, \varphi(n)) = 1$$

e y $\varphi(n)$ deben ser primos relativos.

2. Armar la clave pública

$$p = 7, \quad q = 13$$

$$n = p \times q = 7 \times 13 = 91$$

$$\varphi(n) = (p - 1)(q - 1) = 6 \times 12 = 72$$

$$e = 11 \quad \text{mcd}(e, \varphi(n)) = 1$$

Euclides

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

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

$$6 = 5 \times 1 + \boxed{1}$$

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

$$\text{mcd}(72, 11) = 1 \checkmark$$

e y $\varphi(n)$ deben ser primos relativos.

2. Armar la clave pública

$$p = 7, \quad q = 13$$

$$n = p \times q = 7 \times 13 = 91$$

$$\varphi(n) = (p-1)(q-1) = 6 \times 12 = 72$$

$$e = 11 \quad \text{mcd}(e, \varphi(n)) = 1$$

Euclides

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

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

$$6 = 5 \times 1 + \boxed{1}$$

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

$$\text{mcd}(72, 11) = 1 \checkmark$$

Clave pública: $(n, e) = (91, 11)$

Se publica (n, e) ; lo demás queda en secreto.

Más allá del deber

Uno de los lemas de la Universidad de los Andes

Se publica (n, e) ; lo demás queda en secreto.

3. El mensaje, en números

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

MASALLADELDEBER

A B C D E F G H I J K L M N O P Q R S T U V W X Y Z

~~á é í ó ú ñ~~

A propósito: sin tildes y sin ñ.

3. El mensaje, en números

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

MASALLADELDEBER

A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z
0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25

$$A = 0, B = 1, \dots, Z = 25.$$

3. El mensaje, en números

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

letra	M	A	S	A	L	L	A	D	E	L	D	E	B	E	R
<i>m</i>	12	0	18	0	11	11	0	3	4	11	3	4	1	4	17

A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z
0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25

$$A = 0, B = 1, \dots, Z = 25.$$

4. Cifrar: $c = m^e$ módulo n

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

letra	M	A	S	A	L	L	A	D	E	L	D	E	B	E	R
m	12	0	18	0	11	11	0	3	4	11	3	4	1	4	17
c															

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

$$c = m^{11} \bmod 91$$

Cada letra se cifra por separado con la clave pública.

4. Cifrar: $c = m^e$ módulo n

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

letra	M	A	S	A	L	L	A	D	E	L	D	E	B	E	R
m	12	0	18	0	11	11	0	3	4	11	3	4	1	4	17
c															

$11 = 8 + 2 + 1 = \begin{pmatrix} 1 & 0 & 1 & 1 \\ 3 & 2 & 1 & 0 \end{pmatrix}_2$

i	b_i	Square	Multiply
-----	-------	--------	----------

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

4. Cifrar: $c = m^e$ módulo n

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

letra	M	A	S	A	L	L	A	D	E	L	D	E	B	E	R
m	12	0	18	0	11	11	0	3	4	11	3	4	1	4	17
c															

$$c = 12^{11} \bmod 91$$

$$11 = 8 + 2 + 1 = \begin{pmatrix} \textcolor{brown}{1} & 0 & \textcolor{brown}{1} & \textcolor{brown}{1} \end{pmatrix}_2$$

3 2 1 0

i	b_i	Square	Multiply
-----	-------	--------	----------

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

4. Cifrar: $c = m^e$ módulo n

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

letra	M	A	S	A	L	L	A	D	E	L	D	E	B	E	R
m	12	0	18	0	11	11	0	3	4	11	3	4	1	4	17
c															

$c = 12^{11} \bmod 91$

$11 = 8 + 2 + 1 =$

1

0

1

1

_{3 2 1 0}

i	b_i	Square	Multiply
3	1	$w = 1^2 = 1$	$w = 1 \times 12 = 12$

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

4. Cifrar: $c = m^e$ módulo n

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

letra	M	A	S	A	L	L	A	D	E	L	D	E	B	E	R
m	12	0	18	0	11	11	0	3	4	11	3	4	1	4	17
c															

$c = 12^{11} \bmod 91$

$11 = 8 + 2 + 1 = \begin{pmatrix} 1 & 0 & 1 & 1 \\ 3 & 2 & 1 & 0 \end{pmatrix}_2$

i	b_i	Square	Multiply
3	1	$w = 1^2 = 1$	$w = 1 \times 12 = 12$
2	0	$w = 12^2 = 144 \equiv 53$	

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

4. Cifrar: $c = m^e$ módulo n

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

letra	M	A	S	A	L	L	A	D	E	L	D	E	B	E	R
m	12	0	18	0	11	11	0	3	4	11	3	4	1	4	17
c															

$c = 12^{11} \bmod 91$
 $11 = 8 + 2 + 1 = \begin{pmatrix} 1 & 0 & 1 & 1 \\ 3 & 2 & 1 & 0 \end{pmatrix}_2$

i	b_i	Square	Multiply
3	1	$w = 1^2 = 1$	$w = 1 \times 12 = 12$
2	0	$w = 12^2 = 144 \equiv 53$	—
1	1	$w = 53^2 = 2809 \equiv 79$	$w = 79 \times 12 = 948 \equiv 38$

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

4. Cifrar: $c = m^e \text{ módulo } n$ $(n, e) = (91, 11)$

letra	M	A	S	A	L	L	A	D	E	L	D	E	B	E	R
m	12	0	18	0	11	11	0	3	4	11	3	4	1	4	17
c															

$c = 12^{11} \text{ mod } 91$

$11 = 8 + 2 + 1 = \begin{pmatrix} 1 & 0 & 1 \\ 3 & 2 & 1 \end{pmatrix} \begin{pmatrix} 1 \\ 0 \end{pmatrix}_2$

i	b_i	Square	Multiply
3	1	$w = 1^2 = 1$	$w = 1 \times 12 = 12$
2	0	$w = 12^2 = 144 \equiv 53$	—
1	1	$w = 53^2 = 2809 \equiv 79$	$w = 79 \times 12 = 948 \equiv 38$
0	1	$w = 38^2 = 1444 \equiv 79$	$w = 79 \times 12 = 948 \equiv 38$

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

4. Cifrar: $c = m^e \text{ módulo } n$

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

letra	M	A	S	A	L	L	A	D	E	L	D	E	B	E	R
m	12	0	18	0	11	11	0	3	4	11	3	4	1	4	17
c	38														

$c = 12^{11} \text{ mod } 91 = 38$
 $11 = 8 + 2 + 1 = \begin{pmatrix} 1 & 0 & 1 & 1 \\ 3 & 2 & 1 & 0 \end{pmatrix}_2$

i	b_i	Square	Multiply
3	1	$w = 1^2 = 1$	$w = 1 \times 12 = 12$
2	0	$w = 12^2 = 144 \equiv 53$	—
1	1	$w = 53^2 = 2809 \equiv 79$	$w = 79 \times 12 = 948 \equiv 38$
0	1	$w = 38^2 = 1444 \equiv 79$	$w = 79 \times 12 = 948 \equiv 38$

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

4. Cifrar: $c = m^e$ módulo n

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

letra	M	A	S	A	L	L	A	D	E	L	D	E	B	E	R
m	12	0	18	0	11	11	0	3	4	11	3	4	1	4	17
c	38														

$$c = 0^{11} \bmod 91$$

$$11 = 8 + 2 + 1 = \begin{pmatrix} \mathbf{1} & 0 & \mathbf{1} & \mathbf{1} \end{pmatrix}_2$$

3
2
1
0

i	b_i	Square	Multiply
-----	-------	--------	----------

Square: siempre. Multiply: solo si el bit es $\mathbf{1}$.

4. Cifrar: $c = m^e$ módulo n $(n, e) = (91, 11)$

letra	M	A	S	A	L	L	A	D	E	L	D	E	B	E	R
m	12	0	18	0	11	11	0	3	4	11	3	4	1	4	17
c	38	0													

$c = 0^{11} \bmod 91 = 0$

$11 = 8 + 2 + 1 = \begin{pmatrix} \textcolor{brown}{1} & 0 & \textcolor{brown}{1} & \textcolor{brown}{1} \end{pmatrix}_2$

3

2

1

0

i	b_i	Square	Multiply
3	$\textcolor{brown}{1}$	$w = 1^2 = 1$	$w = 1 \times 0 = 0$
2	0	$w = 0^2 = 0$	—
1	$\textcolor{brown}{1}$	$w = 0^2 = 0$	$w = 0 \times 0 = 0$
0	$\textcolor{brown}{1}$	$w = 0^2 = 0$	$w = 0 \times 0 = 0$

Square: siempre. Multiply: solo si el bit es $\textcolor{brown}{1}$.

4. Cifrar: $c = m^e$ módulo n

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

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

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

4. Cifrar: $c = m^e$ módulo n

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

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

Mensaje cifrado

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

Solo viajan los números c .

4. Cifrar: $c = m^e$ módulo n

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

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

Mensaje cifrado

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

Ejemplo de juguete: un RSA real cifra bloques grandes, no letras.

4. Cifrar: $c = m^e$ módulo n

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

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

Mensaje cifrado

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

Siguiente video: la clave privada y el descifrado.