Lección 2. CONGRUENCIAS. ARITMÉTICA MODULAR

1. CONGRUENCIAS

DEFINICIÓN:

Sea n un entero mayor que 1. Dados a y b $\in \mathbb{Z}$, diremos que

a es congruente con b módulo n

y escribiremos

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

si

$$a-b=k\cdot n \text{ con } k \in \mathbb{Z}.$$

EJEMPLO:

$17 \equiv 2 \pmod{5}$ ya que $17-2=15=3\cdot 5$

$-7 \equiv -49 \pmod{6}$ ya que $-7-(-49)=42=7\cdot 6$

1. CONGRUENCIAS

TEOREMA

La relación de congruencia módulo n ($n > 1$) es una relación de equivalencia.

TEOREMA

Si $(x_n x_{n-1} \ldots X_1 x_0)_{10}$ es la representación en base 10 de un entero positivo x, entonces

$$x \equiv (x_0 + x_1 + \ldots + x_{n-1} + x_n) \pmod 9.$$

1. CONGRUENCIAS

APLICACIÓN: Estudiemos si la multiplicación

$$54321 \cdot 98765 = 5363013565,$$

está incorrectamente efectuada.

$$\left.\begin{array}{l} 54321 \equiv 15 \pmod 9 \equiv 6 \pmod 9 \\ 98765 \equiv 35 \pmod 9 \equiv 8 \pmod 9 \\ 5363013565 \equiv 37 \pmod 9 \equiv 10 \pmod 9 \equiv 1 \pmod 9 \end{array}\right\} \begin{array}{l} 54321 \equiv 6 \pmod 9 \\ 98765 \equiv 8 \pmod 9 \\ 5363013565 \equiv 1 \pmod 9 \end{array}$$

Por la compatibilidad de la relación de cong. con el producto:

$$54321 \cdot 98765 \equiv 6 \cdot 8 \pmod 9$$

$$54321 \cdot 98765 \equiv 48 \pmod 9 \equiv 12 \pmod 9 \equiv 3 \pmod 9$$

Por la transitividad

$$54321 \cdot 98765 \equiv 3 \pmod 9$$

Si la operación estuviera bien efectuada, entonces:

$$5363013565 = 54321 \cdot 98765 \equiv 3 \pmod 9$$

Luego la operación es incorrecta.

1. CONGRUENCIAS

APLICACIÓN: Estudiemos si la multiplicación

$$54321 \cdot 98765 = 5363013565,$$

está incorrectamente efectuada.

$$\underbrace{\underbrace{\underbrace{\underbrace{\underbrace{54321}_{15}}_{6} \cdot \underbrace{\underbrace{98765}_{35}}_{8}}_{6\cdot 8=48}}_{12}}_{3} = \underbrace{\underbrace{\underbrace{5363013565}_{37}}_{10}}_{1}$$

Como $3 \neq 1$, entonces la operación es incorrecta.

1. CONGRUENCIAS

¡CUIDADO!: Si una operación supera la prueba de los nueves, ello no implica que la operación sea correcta.

Estudiemos si

$$15\cdot 36=450,$$

está incorrectamente efectuada.

$$\underbrace{\underbrace{\underbrace{15}_{6}\cdot\underbrace{36}_{9}}_{6\cdot 9=54}}_{9} = \underbrace{450}_{9}$$

No podemos concluir nada sobre la falsedad o veracidad de la igualdad. Y, sin embargo, sabemos que la igualdad es falsa, ya que el producto 15·36 da como resultado 540 y no 450.

2. LOS ENTEROS MÓDULO n. ARITMÉTICA EN Z_n

$$Z_n = \{ [0], [1], \dots , [n - 1] \}$$

donde:

$$[0] = \{ 0 + kn \ / \ k \in Z \}$$
$$[1] = \{ 1 + kn \ / \ k \in Z \}$$
$$\dots$$
$$[n\text{-}1] = \{ (n - 1) + kn \ / \ k \in Z \}$$

Ya que, para todo $a \in Z$, $\exists!\ q, r \in Z$ tal que

$$a = q \cdot n + r, \ \ 0 \le r < |n|,$$

de modo que $a \equiv r \pmod n$ y por tanto

$$[a] = [r], \ \ 0 \le r < n - 1.$$

2. LOS ENTEROS MÓDULO n. ARITMÉTICA EN $\mathbb{Z}_n$

Dada una clase de equivalencia [a] de $\mathbb{Z}_n$, obtener un representante de clase entre 0 y n − 1:

El representante buscado es el resto de la división euclídea de a entre n.

EJEMPLO: Sea $[149] \in \mathbb{Z}_{23}$. Calculemos un representante de clase entre 0 y 22:

$$149 = 6 \cdot 23 + 11$$

$$[149] = [11] \text{ en } \mathbb{Z}_{23}$$

Por otro lado, como

$$\begin{aligned} -149 &= (-6)\cdot 23 - 11 \\ &= (-6)\cdot 23 - 11 + 23 - 23 \\ &= (-7)\cdot 23 + 12, \end{aligned}$$

entonces $[-149] = [12]$ en $\mathbb{Z}_{23}$

2. LOS ENTEROS MÓDULO n. ARITMÉTICA EN Z_n

OPERACIONES INDUCIDAS EN Z_n

A partir de la suma y el producto de enteros podemos inducir dos nuevas operaciones en Z_n:

- La suma en Z_n: $[x] +_n [y] = [x+y]$
- El producto en Z_n: $[x] \cdot_n [y] = [x \cdot y]$

EJEMPLO: En Z_2 las tablas de las operaciones inducidas son:

$+_2$	$[0]$	$[1]$
$[0]$	$[0]$	$[1]$
$[1]$	$[1]$	$[0]$

$\cdot_2$	$[0]$	$[1]$
$[0]$	$[0]$	$[0]$
$[1]$	$[0]$	$[1]$

OPERACIONES INDUCIDAS EN $\mathbb{Z}_n$

EJEMPLO:

$$[128] +_{347} [306] \;=\; [128+306] = [434] = [87] \quad \leftarrow 434 = 1\cdot 347 + 87.$$

$$[-27] \cdot_{347} [370] \;=\; [(-27)\cdot 370] = [-9990] \underset{\uparrow}{=} [73]$$

$$-9990 = (-28)\cdot 347 - 274 = (-28)\cdot 347 - 274 + 347 - 347 = (-29)\cdot 347 + 73$$

Podríamos haber reducido previamente [-27] y [370]:

$$[-27] \cdot_{347} [370] \underset{\uparrow}{=} [320] \cdot_{347} [23] = [7360] = [73] \leftarrow 7360 = 21\cdot 347 + 73$$

$$[-27] \;=\; [320] \leftarrow -27 = (-27+347) - 347 = (-1)\cdot 347 + 320.$$

$$[370] \;=\; [23] \leftarrow 370 = 1\cdot 347 + 23$$

2. LOS ENTEROS MÓDULO n. ARITMÉTICA EN Z_n

Estas nuevas operaciones en Z_n heredan las propiedades de la suma y el producto en Z:

- $+_n$ y $\cdot_n$ son asociativas y conmutativas
- poseen elemento neutro ([0] y [1], respectivamente)
- todo elemento posee simétrico para $+_n$ ([a]+[-a]=[0])
- $\cdot_n$ es distributivo respecto de $+_n$

TEOREMA

Z_n es un anillo conmutativo con unidad con las operaciones inducidas:

3. ELEMENTOS INVERSIBLES EN $\mathbb{Z}_n$. FUNCION DE EULER

TEOREMA

Sea $\mathbb{Z}_n^*$ el conjunto de los elementos inversibles de $\mathbb{Z}_n$, para el producto. Son equivalentes:

1. $[a] \in \mathbb{Z}_n^*$

2. $\exists\ [b] \in \mathbb{Z}_n$ tal que $[a][b] = [1]$

3. $\exists\ b,k \in \mathbb{Z}$ tal que $ab - kn = 1$

4. $\mathrm{mcd}(a,n)=1$

EJEMPLO: Los enteros positivos menores que 8 y primos con 8 son: 1, 3, 5 y 7.

De modo que $\mathbb{Z}_8^* =\{[1],[3],[5],[7]\}$.

EJEMPLO: Hállese $[25]^{-1}$ en $\mathbb{Z}_{72}$.

El algoritmo de Euclides da lugar a:

$$\begin{aligned} 72 &= 2(25)+22, \quad 0 < 22 < 25 \\ 25 &= 1(22)+3, \quad 0 < 3 < 22 \\ 22 &= 7(3)+1, \quad 0 < 1 < 3 \\ 3 &= 3(1)+0. \end{aligned}$$

Por tanto, mcd(25,72) = 1. Además:

$$\begin{aligned} 1 &= 22 - 7(3) = 22 - 7(25 - 22) \\ &= (-7)(25) + (8)(22) \\ &= (-7)(25) + 8(72 - 2(25)) \\ &= 8(72) - 23(25). \end{aligned}$$

Luego $[25]^{-1} = [-23] = [-23 + 72 - 72] = [49 - 72] = [49]$.

3. ELEMENTOS INVERSIBLES EN Z_n. FUNCION DE EULER

DEFINICIÓN:

Sea n ≥ 1. Llamamos **función de Euler** sobre n y la denotamos por φ(n) al cardinal de $\mathrm{Z}_n{}^*$.

$$\varphi(n) = card\{x \in \mathbb{Z}^+ \ / \ x \leq n \text{ y } mcd(x,n) = 1\}.$$

Claramente si p es primo, ϕ(p) = p − 1.

EJEMPLO:

Como $\mathrm{Z}_8{}^*$ ={[1],[3],[5],[7]}, tenemos que φ(8)=4.

EJEMPLO:

Como 17 es un número primo, φ(17)=17−1=16.

3. ELEMENTOS INVERSIBLES EN $\mathbb{Z}_n$. FUNCION DE EULER

TEOREMA (Teorema de Euler)

Si $[y] \in Z_n^*$ entonces, $[y]^{\varphi(n)} = [1]$

TEOREMA (Teorema de Euler)

Sean $y,n \in Z^+$ / mcd(y,n)=1, entonces $y^{\varphi(n)} \equiv 1 \pmod{n}$

EJEMPLO:

Como $\varphi(8)=4$ y $Z_8^*=\{[1],[3],[5],[7]\}$, tenemos que:

$3^4 \equiv 1 \pmod{8}$, $5^4 \equiv 1 \pmod{8}$, $7^4 \equiv 1 \pmod{8}$

3. ELEMENTOS INVERSIBLES EN $\mathbb{Z}$n. FUNCION DE EULER

TEOREMA (Teorema de Euler)

Si $[y] \in Z_n^*$ entonces, $[y]^{\varphi(n)} = [1]$

EJEMPLO:

Este teorema nos puede ayudar a calcular potencias grandes de números enteros.

Intentemos calcular $[7]^{495}$ en Z_8.

1. $\varphi(8)=4$ y como $[7] \in Z_8^*$, por el teorema de Euler:

$$[7]^4=1.$$

2. Además, como $495=123\cdot4+3$, podemos escribir:

$$[7]^{495}=[7]^{123\cdot4+3}=([7]^4)^{123}\cdot[7]^3=[1]\cdot[343]=[42\cdot8+7]=[7]$$

3. ELEMENTOS INVERSIBLES EN $\mathbb{Z}_n$. FUNCION DE EULER

COROLARIO (Teorema de Fermat)

Sea $y \in \mathbb{Z}^+$ y p primo. Si p no divide a y, entonces

$$y^{p-1} \equiv 1 \pmod p$$

EJEMPLO:

Sea y=348 y el entero primo p=11.

Como 11 no divide a 348, el teorema de Fermat nos garantiza que

$$348^{10} \equiv 1 \pmod{11}.$$

CÁLCULO DE LA FUNCIÓN DE EULER

PROPOSICIÓN

Si p $\in \mathbb{Z}^+$ es un número primo y u $\in \mathbb{Z}^+$, entonces

$$\varphi(p^u) = p^{u-1}(p-1).$$

TEOREMA

1. Sean $n_1, n_2, \ldots, n_k$ enteros positivos primos entre sí dos a dos. Si $n = n_1 n_2 \cdots n_k$, entonces

$$\varphi(n) = \varphi(n_1)\varphi(n_2)\cdots\varphi(n_k).$$

2. Si $n = p_1^{r_1} p_2^{r_2} \cdots p_k^{r_k}$ es la descomposición en factores primos de un entero positivo n,

$$\begin{aligned}\varphi(n) &= \\ &= p_1^{r_1-1}(p_1-1)p_2^{r_2-1}(p_2-1)\cdots p_k^{r_k-1}(p_k-1) \\ &= n\left(1-\frac{1}{p_1}\right)\left(1-\frac{1}{p_2}\right)\cdots\left(1-\frac{1}{p_k}\right).\end{aligned}$$

3. ELEMENTOS INVERSIBLES EN $\mathbb{Z}_n$. FUNCION DE EULER

EJEMPLO:

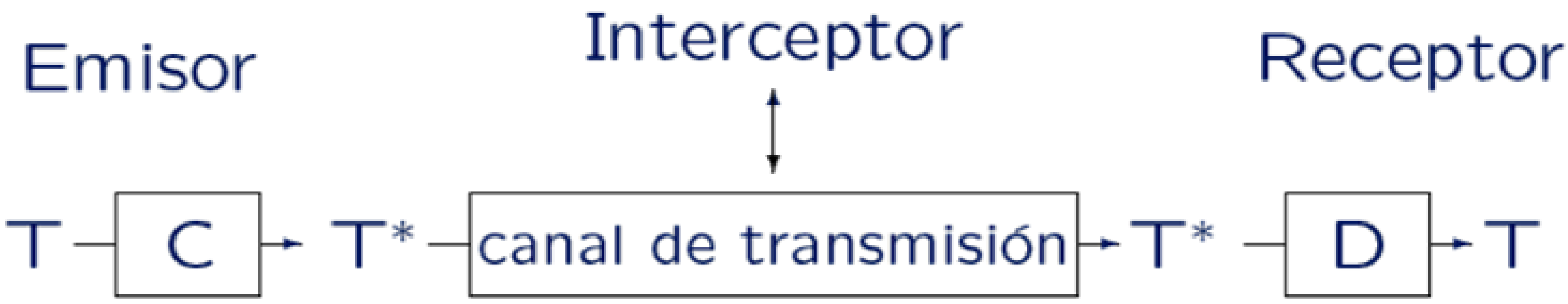
Consideremos el entero n=167544. Como su descomposición en factores primos es

$$167544=2^3\cdot 3^2\cdot 13\cdot 179,$$

se tiene que el valor de la función de Euler calculada sobre dicho entero es:

$$\varphi(167544) = 167544\left(1-\frac{1}{2}\right)\left(1-\frac{1}{3}\right)\left(1-\frac{1}{13}\right)\left(1-\frac{1}{179}\right) = 51264.$$

4. APLICACIÓN A LA CRIPTOGRAFÍA



T: Texto llano (en lenguaje natural o bien reducido a una sucesión de dígitos de transcripción inmediata).

T*: Criptograma, o texto cifrado (ilegible para quien no conozca D).

C: Función de cifrado o de codificación, conocida por el emisor.

D: Función de descifrado o de decodificación, conocida por el receptor. C y D son funciones inversas una de otra.

4. APLICACIÓN A LA CRIPTOGRAFÍA

DEFINICIÓN:

Un sistema criptográfico o criptosistema consiste en cinco componentes: M, M^*, K, C y D.

1. M es el conjunto de todos los mensajes a transmitir;

2. M^* el de todos los mensajes cifrados;

3. K el conjunto de claves a utilizar, es decir los parámetros que controlan los procesos de cifrado y descifrado;

4. C el conjunto de todos los métodos de cifrado:

$$C = \{C_k : M \longrightarrow M^*,\ k \in K\};$$

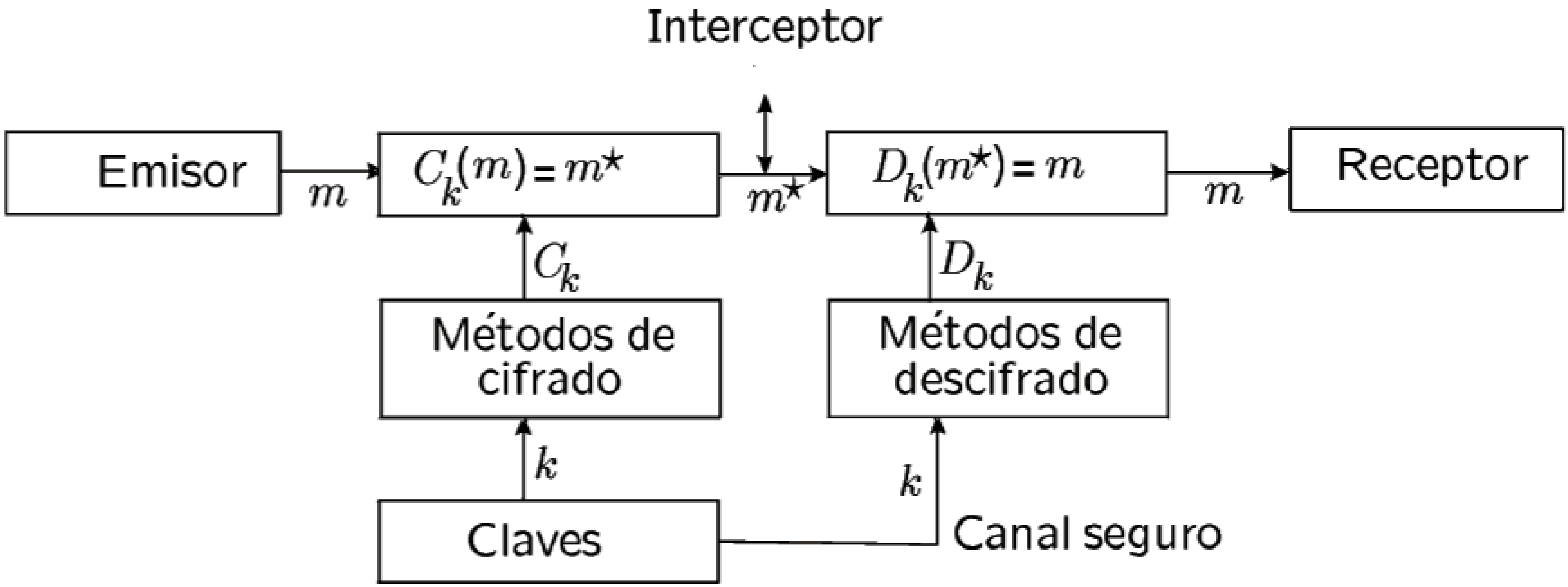
5. D el de todos los métodos de descifrado:

$$D = \{D_k : M^* \longrightarrow M,\ k \in K\}.$$

Para una clave dada k, la transformación D_k es la inversa de C_k, es decir,

$$D_k\left(C_k(m)\right) = m, \quad \forall m \in M.$$

4. APLICACIÓN A LA CRIPTOGRAFÍA



4. APLICACIÓN A LA CRIPTOGRAFÍA

CRIPTOSISTEMAS DE CLAVE PRIVADA

Un criptosistema de clave privada basa su técnica en un valor secreto llamado clave.

El emisor y el receptor establecen de mutuo acuerdo el sistema criptográfico, y la clave concreta que utilizarán en sus comunicaciones.

Este tipo de criptosistemas permite, conociendo la función de cifrado, obtener la de descifrado, y viceversa.

4. APLICACIÓN A LA CRIPTOGRAFÍA

EJEMPLO:

Identificando las letras del alfabeto con los enteros módulo 27:

A	B	C	D	E	F	G	H	I	J	K	L	M	N	Ñ	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	26

es decir, $M=M^*=Z_{27}$

La función de cifrado $C_{r,s} : M \longrightarrow M^*$, $r, s \in \mathbb{Z}$, viene definida por

$$C_{r,s}([m]) = [r][m] + [s], \quad \text{con} \quad \text{mcd}(r, 27) = 1.$$

La función de descifrado será

$$D_{r,s} : M^* \longrightarrow M \;/\; D_{r,s}([m^*]) = [r]^{-1}([m^*] - [s]).$$

4. APLICACIÓN A LA CRIPTOGRAFÍA

EJEMPLO:

A	B	C	D	E	F	G	H	I	J	K	L	M	N	Ñ	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	26

Tomando como caso particular r = 2 y s = 3:

$$C_{2,3}([m]) = [2][m] + [3], \text{ con mcd}(2,17)=1.$$

$$D_{23}([m^*]) = [2]^{-1}([m^*] - [3]).$$

C I F R A D O

Símbólico	Numérico	Cifrado: $C_{2,3}$	Símbólico
R	[18]	[12]	M
O	[15]	[6]	G
M	[12]	[0]	A
A	[0]	[3]	D

$C_{2,3}([18])=[2][18]+[3]=[39]=[1\cdot 27+12]=[12]$

$C_{2,3}([15])=[2][15]+[3]=[33]=[1\cdot 27+6]=[6]$

$C_{2,3}([12])=[2][12]+[3]=[27]=[0]$

$C_{2,3}([0]) \ =[2][0]+[3]=[3]$

4. APLICACIÓN A LA CRIPTOGRAFÍA

DESCIFRADO

EJEMPLO:

A	B	C	D	E	F	G	H	I	J	K	L	M	N	Ñ	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	26

Tomando como caso particular r = 2 y s = 3:

$$C_{2,3}([m]) = [2][m] + [3], \text{ con mcd}(2,17)=1.$$

$$D_{23}([m^*]) = [2]^{-1}([m^*] - [3]).$$

Símbólico	Numérico	Descifrado: $D_{2,3}$	Símbólico
M	[12]	[18]	R
G	[6]	[6]	O
A	[0]	[0]	M
D	[3]	[3]	A

$D_{2,3}([12])=[2]^{-1}([12] - [3])=[14]([12]-[3])=[126]=[4\cdot 27+18]=[18]$

$D_{2,3}([6])=[2]^{-1}([6]-[3])=[14]([6]-[3])=[42]=[1\cdot 27+15]$

$D_{2,3}([0])=[2]^{-1}([0]-[3])=[14]([0]-[3])=[-42]=[(-2)\cdot 27+12]=[12]$

$D_{2,3}([3]) =[2]^{-1}([3]-[3])=[0]$

4. APLICACIÓN A LA CRIPTOGRAFÍA

CRIPTOSISTEMAS DE CLAVE PUBLICA

Basan su técnica en que la clave para cifrar es pública, mientras que la de descifrar sólo es conocida por el usuario correspondiente, y además, es computacionalmente difícil encontrar la clave de descifrado a partir del conocimiento de la de cifrado.

Dan respuesta a la necesidad de dotar de clave secreta a cada par de miembros potencialmente comunicantes de una comunidad de individuos.

Cada usuario $\boldsymbol{U}$ tiene asignadas un par de semiclaves:

- La primera semiclave determina la función de cifrado $\boldsymbol{C_U}$ que debe aplicar cualquiera que desee enviarle un mensaje al usuario $\boldsymbol{U}$; $\boldsymbol{C_U}$ debe ser del dominio público.
- La segunda semiclave debe reservarse en secreto por parte de $\boldsymbol{U}$; la función de descifrado $\boldsymbol{D_U}$ que determina, será aplicada por él para interpretar los mensajes que reciba.

Es condición imprescindible que la semiclave secreta sea prácticamente imposible de deducir de la semiclave pública.

4. APLICACIÓN A LA CRIPTOGRAFÍA

CRIPTOSISTEMAS DE CLAVE PUBLICA

EJEMPLO: Sistema Rivest-Shamir-Adleman (Sistema RSA).

Sean p y q dos números primos, y $n = p \cdot q$.

Consideremos $M = M^* = Z_n^*$ y t un entero tal que

$$\text{mcd}(t, \varphi(n)) = 1.$$

En estas condiciones existe un entero s tal que

$$t \cdot s \equiv 1 \ (\text{mod } \varphi(n)),$$

esto es, $t \cdot s = k \cdot \varphi(n) + 1$ para algún $k \in Z$.

Definimos la función de cifrado por

$$C: M \rightarrow M^* \ / \ C([m]_n) = [m]_n^t.$$

Y la función de descifrado por

$$D: M^* \rightarrow M \ / \ D([m^*]_n) = [m^*]_n^s.$$

La semiclave que pública es el par (n,t).

La semiclave secreta es el par (n,s).

Deben mantenerse en secreto p, q, $\varphi(n)$ y s.

4. APLICACIÓN A LA CRIPTOGRAFÍA

EJEMPLO:

Supongamos el caso concreto donde $p = 13$ y $q = 17$. Entonces,

$$n = 13 \cdot 17 = 221 \text{ y}$$

$$\varphi(n) = (p-1)\cdot(q-1) = 12 \cdot 16 = 192.$$

Por tanto $M = M^* = Z_{221}{}^*$.

Entonces, escogiendo

$$t=11 \quad (\text{ya que, } mcd(11,192)=1)$$

calculamos el valor de s tal que

$$t \cdot s \equiv 1 \pmod{192}$$

y encontramos $s=35$.

Por tanto:

$$C([m]_{221})=[m]_{221}{}^{11}$$

$$D([m^*]_{221})=[m^*]_{221}{}^{35}$$

4. APLICACIÓN A LA CRIPTOGRAFÍA

EJEMPLO:

A	B	C	D	E	F	G	H	I	J	K	L	M	N	Ñ	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	26

$$C([m]_{221})=[m]_{221}{}^{11}$$
$$D([m^*]_{221})=[m^*]_{221}{}^{35}$$

CIFRADO

Símbólico	Numérico	m^{11}	m^{11} (mod 221)
R	018	64268410079232	086
O	015	8649755859375	111
M	012	743008370688	142
A	000	0	000

4. APLICACIÓN A LA CRIPTOGRAFÍA

EJEMPLO:

A	B	C	D	E	F	G	H	I	J	K	L	M	N	Ñ	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	26

DESCIFRADO

$$C([m]_{221})=[m]_{221}{}^{11}$$

$$D([m^*]_{221})=[m^*]_{221}{}^{35}$$

Texto cifrado	m^{35}	m^{35} (mod 221)	Simbólico
086	Necesitaríamos algún algoritmo de exponenciación modular	018	R
111		015	O
142		012	M
000		000	A

4. APLICACIÓN A LA CRIPTOGRAFÍA

EJEMPLO: Supongamos que queremos calcular

$$C([m]_{221})=[111]_{221}{}^{35}$$

Podemos ir calculando potencias de 2, e ir reduciendo a módulo 221:

$[111]^2 = [12321] = [55\cdot 221 + 166] = [166]$

$[111]^4 = ([111]^2)^2 = [166]^2 = [27556] = [124\cdot 221 + 1] = [152]$

$[111]^8 = ([111]^4)^2 = [152]^2 = [23104] = [104\cdot 221 + 120] = [120]$

$[111]^{16} = ([111]^8)^2 = [120]^2 = [14400] = [65\cdot 221 + 35] = [35]$

$[111]^{32} = ([111]^{16})^2 = [35]^2 = [1225] = [5\cdot 221 + 120] = [120]$

$[111]^{35} = [111]^{32}\cdot[111]^3 = [120]\cdot[1367631]$

$= [120]\cdot[6188\cdot 221 + 83] = [120]\cdot[83]$

$= [9960] = [45\cdot 221 + 15] = [15]$

4. APLICACIÓN A LA CRIPTOGRAFÍA

EJEMPLO: Supongamos que queremos calcular

$$C([m]_{221})=[86]_{221}{}^{35}$$

Podemos ir calculando potencias de 2, e ir reduciendo a módulo 221:

$[86]^2 = [7396] = [33\cdot 221 + 103] = [103]$

$[86]^4 = ([86]^2)^2 = [103]^2 = [10609] = [48\cdot 221 + 1] = [1]$

$[86]^{32} = ([86]^4)^8 = [1]$

$[86]^{35} = [86]^{32}\cdot[86]^3 = [1]\cdot[636056] = [2878\cdot 221 + 18] = [18]$