Lliçó 2. CONGRUÈNCIES. ARITMÈTICA MODULAR

1. Congruències.
2. Els enters mòdul *n*. Aritmètica en $\mathbb{Z}_n$.
3. Elements invertibles en $\mathbb{Z}_n$. Funció d'Euler.
4. Aplicació a la criptografia.

1. CONGRUÈNCIES

DEFINICIÓ:

Siga n un enter major que 1. Donats a i b $\in$ Z, direm que

a es congruent amb b mòdul n

i escriurem

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

si

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

EXEMPLE:

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

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

1. CONGRUÈNCIES

TEOREMA

La relació de congruència mòdul n (n > 1) és una relació d'equivalència.

TEOREMA

Si $(x_n x_{n-1} \ldots x_1 x_0)_{10}$ és la representació en base 10 d'un enter positiu x, aleshores

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

1. CONGRUÈNCIES

APLICACIÓ: Estudiem si la multiplicació

$$54321 \cdot 98765 = 5363013565,$$

està incorrectament efectuada.

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

Per la compatibilitat de la relació de cong. amb el producte:

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

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

Per la transitivitat

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

Si l'operació estiguera ben efectuada:

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

Per tant l'operació és incorrecta.

1. CONGRUÈNCIES

APLICACIÓ: Estudiem si la multiplicació

$$54321 \cdot 98765 = 5363013565,$$

està incorrectament efectuada.

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

$$\underbrace{\underbrace{6\cdot 8=48}_{12}}_{3}$$

Com $3 \neq 1$, aleshores l'operació es incorrecta.

1. CONGRUÈNCIES

ATENCIÓ!: Si una operació supera la prova dels nous, això no implica que l'operació siga correcta.

Estudiem si

$$15 \cdot 36 = 450,$$

està incorrectament efectuada.

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

No podem concloure res sobre la falsedat o veracitat de la igualtat. I, no obstant això, sabem que la igualtat és falsa, ja que el producte 15·36 dóna com resultat 540 i no 450.

2. ELS ENTERS MÒDUL n. ARITMÈTICA EN $\mathbb{Z}_n$

$$\mathbb{Z}_n = \{ [0], [1], \dots , [n-1] \}$$

on:

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

Ja que, per a tot $a \in \mathbb{Z}$, $\exists!\ q, r \in \mathbb{Z}$ tal que

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

de manera que $a \equiv r \pmod n$ i per tant

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

2. ELS ENTERS MÒDUL n. ARITMÈTICA EN $\mathbb{Z}_n$

Donada una classe d'equivalència [a] de $\mathbb{Z}_n$, obtindre un representant de classe entre 0 i n – 1:

El representant buscat és la resta de la divisió euclídea de a entre n.

EXEMPLE: Siga $[149] \in \mathbb{Z}_{23}$. Calculem un representant de classe entre 0 i 22:

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

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

D'altra banda, com

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

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

2. ELS ENTERS MÒDUL n. ARITMÈTICA EN $\mathbb{Z}_n$

OPERACIONS INDUÏDES EN $\mathbb{Z}_n$

A partir de la suma i el producte d'enters podem induir dos noves operacions en $\mathbb{Z}_n$:

- La suma en $\mathbb{Z}_n$: $[x] +_n [y] = [x + y]$
- El producte en $\mathbb{Z}_n$: $[x] \cdot_n [y] = [x \cdot y]$

EXEMPLE: En $\mathbb{Z}_2$ les taules de les operacions induïdes són:

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

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

OPERACIONS INDUÏDES EN $\mathbb{Z}_n$

EXEMPLE:

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

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

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

Podríem haver reduït prèviament [-27] y [370]:

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

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

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

2. ELS ENTERS MÒDUL n. ARITMÈTICA EN $\mathbb{Z}_n$

Aquestes noves operacions en $\mathbb{Z}_n$ hereten les propietats de la suma i el producte en $\mathbb{Z}$:

- $+_n$ i $\cdot_n$ són associatives i commutatives
- posseeixen element neutre ([0] y [1], respectivament)
- tot element posseeix simètric per a $+_n$ ([a]+[−a]=[0])
- $\cdot_n$ és distributiu respecte de $+_n$

TEOREMA

$\mathbb{Z}_n$ és un anell commutatiu amb unitat amb les operacions induïdes:

3. ELEMENTS INVERTIBLES EN $\mathbb{Z}_n$. FUNCIÓ D'EULER

TEOREMA

Siga Z_n^* el conjunt dels elements invertibles de Z_n, per al producte. Són equivalents:

1. $[a] \in Z_n^*$

2. $\exists\ [b] \in Z_n$ tal que $[a][b] = [1]$

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

4. $mcd(a,n)=1$

EXEMPLE: Els enters positius menors que 8 i primers amb 8 són: 1, 3, 5 y 7.

De manera que $Z_8^* = \{[1],[3],[5],[7]\}$.

3. ELEMENTS INVERTIBLES EN $\mathbb{Z}_n$. FUNCIÓ D'EULER

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

L'algoritme d'Euclides dóna lloc a:

$$72 = 2(25)+22,\ 0 < 22 < 25$$
$$25 = 1(22)+3,\ \ 0 < 3 < 22$$
$$22 = 7(3)+1,\ \ \ 0 < 1 < 3$$
$$3 = 3(1)+0.$$

Per tant, mcd(25,72) = 1. A més:

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

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

3. ELEMENTS INVERTIBLES EN $\mathbb{Z}_n$. FUNCIÓ D'EULER

DEFINICIÓ:

Siga n ≥ 1. Anomenem **funció d'Euler** sobre n i la denotem per φ(n) al cardinal de $\mathbb{Z}_n^*$.

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

Clarament si p és primer, φ(p) = p − 1.

EXEMPLE:

Com $\mathbb{Z}_8^*$ ={[1],[3],[5],[7]}, tenim que φ(8)=4.

EXEMPLE:

Com 17 és un nombre primer, φ(17)=17−1=16.

3. ELEMENTS INVERTIBLES EN $\mathbb{Z}_n$. FUNCIÓ D'EULER

TEOREMA (Teorema d'Euler)
Si $[y] \in Z_n^*$ aleshores, $[y]^{\varphi(n)} = [1]$

TEOREMA (Teorema d'Euler)
Siguen $y,n \in Z^+$ / mcd(y,n)=1, aleshores $y^{\varphi(n)} \equiv 1 \pmod{n}$

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

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

3. ELEMENTS INVERTIBLES EN $\mathbb{Z}_n$. FUNCIÓ D'EULER

TEOREMA (Teorema d'Euler)

Si $[y] \in \mathbb{Z}_n^*$ aleshores, $[y]^{\varphi(n)} = [1]$

EXEMPLE:

Aquest teorema ens pot ajudar a calcular potències grans de nombres enters.

Intentem calcular $[7]^{495}$ en $\mathbb{Z}_8$.

1. $\varphi(8)=4$ i com $[7] \in \mathbb{Z}_8^*$, pel teorema d'Euler:

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

2. A més, com $495=123\cdot 4+3$, podem escriure:

$$[7]^{495}=[7]^{123\cdot 4+3}=([7]^4)^{123}\cdot[7]^3=[1]\cdot[343]=[42\cdot 8+7]=[7]$$

3. ELEMENTS INVERTIBLES EN $\mathbb{Z}_n$. FUNCIÓ D'EULER

TEOREMA (Teorema d'Euler)

Siguen $y,n \in \mathbb{Z}^+$ / $\text{mcd}(y,n)=1$, aleshores $y^{\varphi(n)} \equiv 1 \pmod{n}$

COROL·LARI (Teorema de Fermat)

Siga $y \in \mathbb{Z}^+$ i p primer. Si p no divideix a y, aleshores

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

EXEMPLE:

Siga y=348 i el enter primer p=11.

Com 11 no divideix a 348, el teorema de Fermat ens garanteix que

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

3. ELEMENTS INVERTIBLES EN $\mathbb{Z}_n$. FUNCIÓ D'EULER

CÁLCULO DE LA FUNCIÓ D'EULER

PROPOSICIÓ

Si $p \in \mathbb{Z}^+$ és un nombre primer i $u \in \mathbb{Z}^+$, aleshores

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

TEOREMA

1. Siguen $n_1, n_2, \ldots, n_k$ enters positius primers entre si dos a dos. Si $n = n_1 n_2 \cdots n_k$, aleshores

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

2. Si $n = p_1^{r_1} p_2^{r_2} \cdots p_k^{r_k}$ és la descomposició en factors primers d'un enter positiu 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. ELEMENTS INVERTIBLES EN $\mathbb{Z}_n$. FUNCIÓ D'EULER

EXEMPLE:

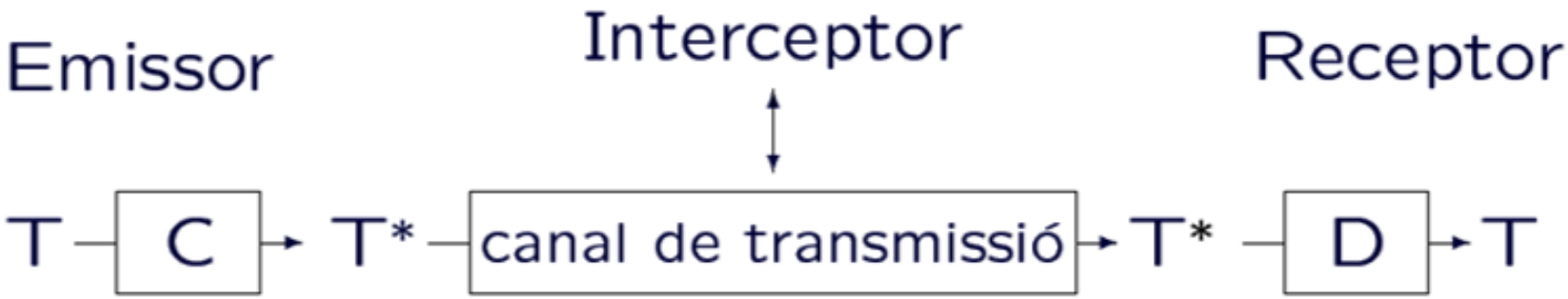
Considerem el enter n=167544. Com la seua descomposició en factors primers és

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

es té que el valor de la funció d'Euler calculada sobre aquest enter és:

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

4. APLICACIÓ A LA CRIPTOGRAFIA



T: Text pla (en llenguatge natural o bé reduït a una successió de dígits de transcripció immediata).

T*: Criptograma, o text xifrat (il·legible per a qui no conega D).

C: Funció de xifrat o de codificació, coneguda per l'emissor.

D: Funció de desxifrat o de descodificació, coneguda pel receptor. C i D són funcions inverses una d'una altra.

4. APLICACIÓ A LA CRIPTOGRAFIA

DEFINICIÓ:

Un sistema criptogràfic o criptosistema consisteix en cinc components: *M*, *M**, *K*, *C* i *D*.

1. *M* és el conjunt de tots els missatges a transmetre;
2. *M** és el conjunt de tots els missatges xifrats;
3. *K* és el conjunt de claus a utilitzar, és a dir, els paràmetres que controlen els processos de xifrat i desxifrat;
4. *C* és el conjunt de tots els mètodes de xifrat:

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

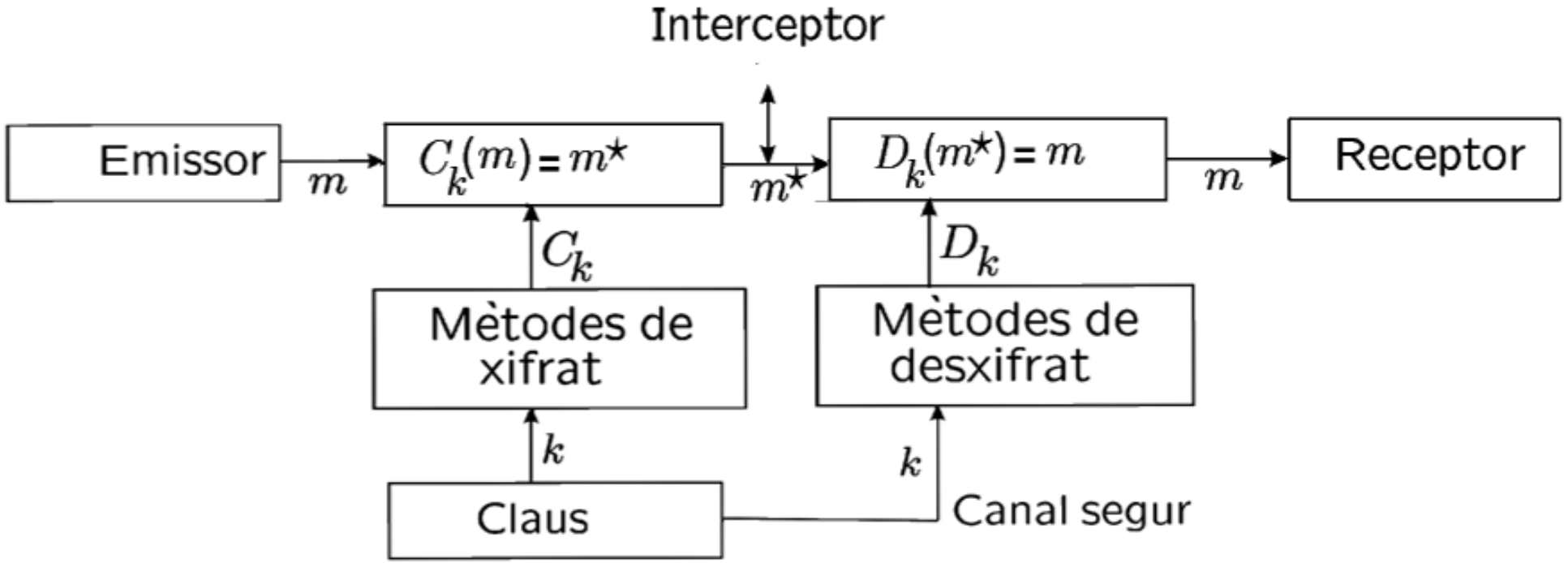
5. *D* és el conjunt de tots els mètodes de desxifrat:

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

Per a una clau donada *k*, la transformació D_k és la inversa de C_k, és a dir,

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

4. APLICACIÓ A LA CRIPTOGRAFIA



4. APLICACIÓ A LA CRIPTOGRAFIA

CRIPTOSISTEMES DE CLAU PRIVADA

Un criptosistema de clau privada basa la seua tècnica en un valor secret anomenat clau.

L'emissor i el receptor estableixen de mutu acord el sistema criptogràfic, i la clau concreta que utilitzaran en les seues comunicacions.

Aquest tipus de criptosistemes permet, coneixent la funció de xifrat, obtindre la de desxifrat, i viceversa.

4. APLICACIÓ A LA CRIPTOGRAFIA

EXEMPLE (xifrat afí):

Identificant les lletres de l'alfabet amb els enters mòdul 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

és a dir, $M=M^*=\mathrm{Z}_{27}$

La funció de xifrat $C_{r,s} : M \longrightarrow M^*$, $r, s \in \mathbb{Z}$, ve definida per

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

La funció de desxifrat serà

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

4. APLICACIÓ A LA CRIPTOGRAFIA

EXEMPLE:

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

Prenent com a cas particular r = 2 i s = 3:

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

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

XIFRAT

Simbòlic	Numèric	Xifrat: $C_{2,3}$	Simbòlic
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. APLICACIÓ A LA CRIPTOGRAFIA

EXEMPLE:

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

DESXIFRAT

Prenent com a cas particular r = 2 i s = 3:

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

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

Simbòlic	Numèric	Desxifrat: $D_{2,3}$	Simbòlic
M	[12]	[18]	R
G	[6]	[15]	O
A	[0]	[12]	M
D	[3]	[0]	A

$D_{2,3}([12])=[2]^{-1}([12] - [3])=[14]([12]-[3])=[126]=[4\cdot27+18]=[18]$

$D_{2,3}([6])=[2]^{-1}([6]-[3])=[14]([6]-[3])=[42]=[1\cdot27+15]=[15]$

$D_{2,3}([0])=[2]^{-1}([0]-[3])=[14]([0]-[3])=[-42]=[(-2)\cdot27+12]=[12]$

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

4. APLICACIÓ A LA CRIPTOGRAFIA

CRIPTOSISTEMES DE CLAU PUBLICA

Basen la seua tècnica en què la clau per a xifrar és pública, mentres que la de desxifrar només és coneguda per l'usuari corresponent, i a més, és computacionalment difícil trobar la clau de desxifrat a partir del coneixement de la de xifrat.

Donen resposta a la necessitat de dotar de clau secreta a cada parell de membres potencialment comunicants d'una comunitat d'individus.

Cada usuari U té assignades un parell de semiclaus:

- La primera semiclau determina la funció de xifrat C_U que ha d'aplicar qualsevol que desitge enviar-li un missatge a l'usuari U; C_U ha de ser del domini públic.
- La segona semiclau ha de reservar-se en secret per part de U; la funció de desxifrat D_U que determina, serà aplicada per ell per a interpretar els missatges que reba.

És condició imprescindible que la semiclau secreta siga pràcticament impossible de deduir de la semiclau pública.

4. APLICACIÓ A LA CRIPTOGRAFIA

CRIPTOSISTEMES DE CLAU PUBLICA

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

Siguen p i q dos nombres primers, i n = p·q.
Considerem $M = M^* = Z_n^*$ i t un enter tal que

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

Amb aquestes condicions hi ha un enter s tal que

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

és a dir, $t \cdot s = k \cdot \varphi(n) + 1$ per a algun $k \in Z$.
Definim la funció de xifrat per

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

I la funció de desxifrat per

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

La semiclau que és pública és el parell (n,t).
La semiclau secreta és el parell (n,s).
Han de mantindre's en secret p, q, φ(n) i s.

Índex

4. APLICACIÓ A LA CRIPTOGRAFIA

EXEMPLE:

Suposem el cas concret on p = 13 i q = 17. Aleshores,

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

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

Per tant $M = M^* = Z_{221}^*$.

Aleshores, triant

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

calculem el valor de s tal que

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

i trobem s=35.

Per tant:

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

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

4. APLICACIÓ A LA CRIPTOGRAFIA

EXEMPLE:

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

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

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

XIFRAT

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

4. APLICACIÓ A LA CRIPTOGRAFIA

EXEMPLE:

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

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

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

DESXIFRAT

Text xifrat	m^{35}	m^{35} (mod 221)	Simbòlic
086	Necessitaríem	018	R
111	algun algoritme	015	O
142	d'exponenciació	012	M
000	modular	000	A

4. APLICACIÓ A LA CRIPTOGRAFIA

EXEMPLE: Suposem que volem calcular

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

Podem anar calculant potències de 2, i anar reduint a mòdul 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. APLICACIÓ A LA CRIPTOGRAFIA

EXEMPLE: Suposem que volem calcular

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

Podem anar calculant potències de 2, i anar reduint a mòdul 221:

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

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

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

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