Clasificación de los criptosistemas

- Los criptosistemas pueden clasificarse por:

  a) Su relación con la Historia en:

  - *Sistemas clásicos y sistemas modernos*

No es la mejor clasificación, pero nos permitirá comprobar el desarrollo de estas técnicas de cifrado.

b) El tratamiento de la información a cifrar en:
- *Sistemas de cifrado en bloque* y *en flujo*

c) El tipo de clave utilizada:
- *Sistemas de clave secreta (simétricos)* y c*lave pública (asimétricos)*

Cifrado en flujo

Cifrado en bloque

Cifrado con clave secreta

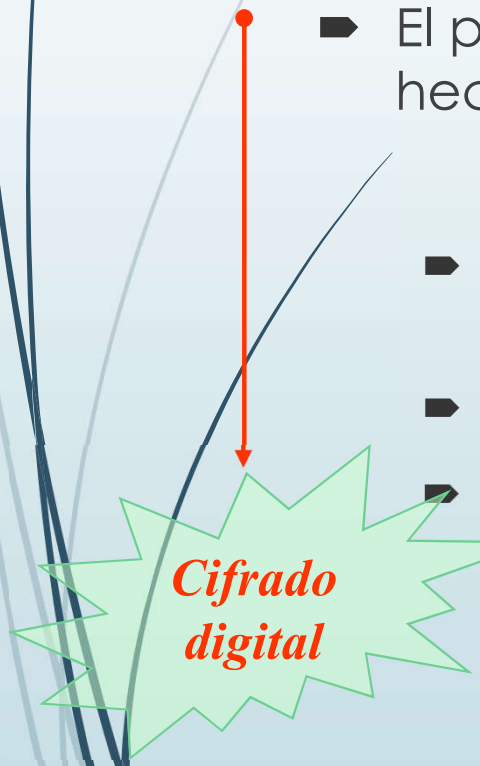
Cifrado con clave pública

Criptografía clásica

- La criptografía clásica abarca desde tiempos inmemoriales hasta la mitad del siglo XX.

- El punto de inflexión en esta clasificación la marcan tres hechos relevantes:

  - En el año 1948 se publica el estudio de C. Shannon sobre la Teoría de la Información.
  - En 1974 aparece el estándar de cifrado DES.
  - En el año 1976 se publica el estudio realizado por W. Diffie y M. Hellman sobre la aplicación de funciones matemáticas de un solo sentido a un modelo de cifra, denominado cifrado con clave pública.



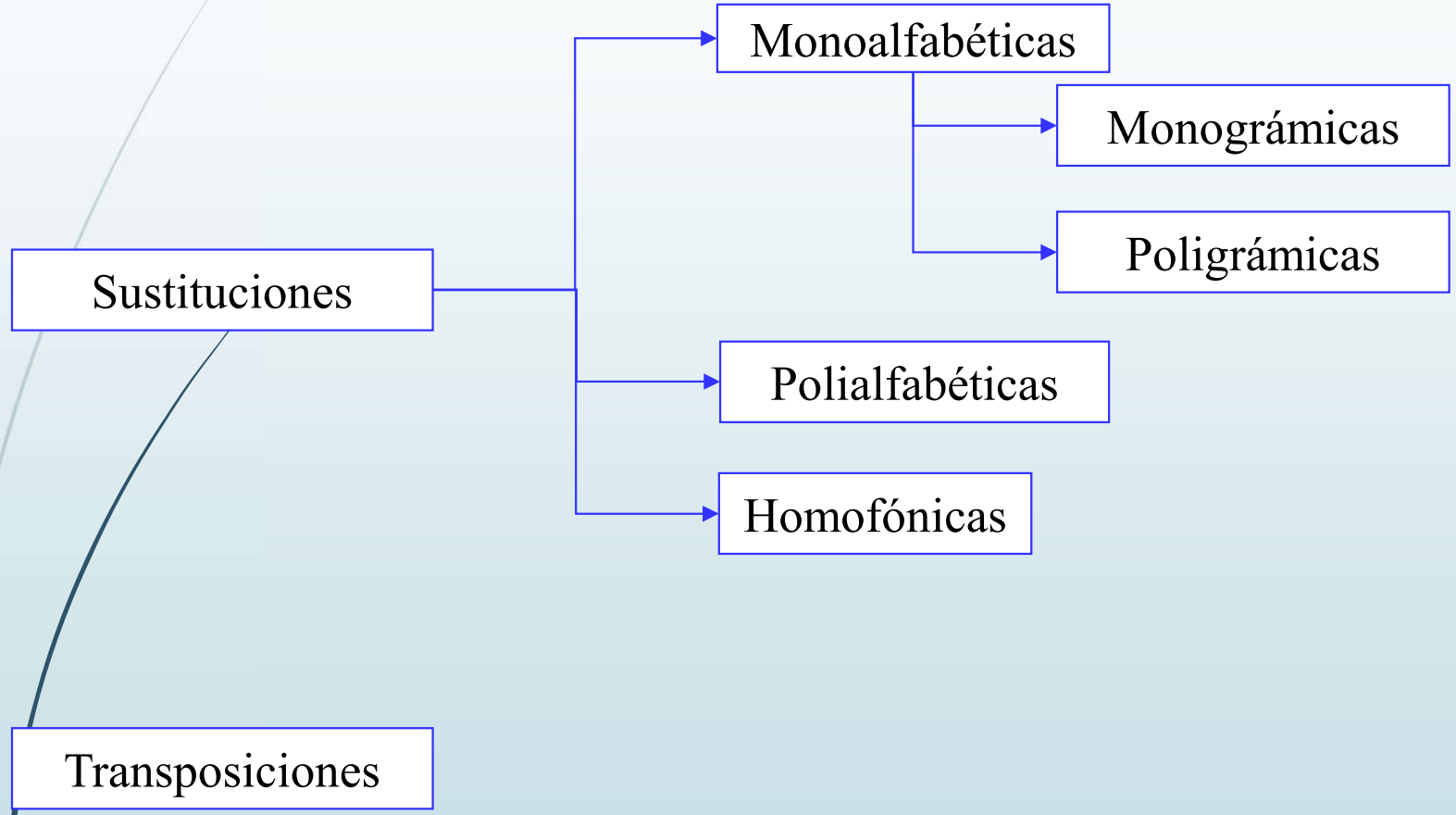
Alfabetos de cifrado

- En la mayoría de los cifradores clásicos se utiliza como alfabeto el mismo alfabeto del texto en claro.
- Para poder aplicar las operaciones de transformación se asocia a cada letra del alfabeto un número.
- Por ejemplo:

A	*B*	*C*	*D*	*E*	*F*	*G*	*H*	*I*	*J*	*K*	*L*	*M*	*N*
0	1	2	3	4	5	6	7	8	9	10	11	12	13

Ñ	*O*	*P*	*Q*	*R*	*S*	*T*	*U*	*V*	*W*	*X*	*Y*	*Z*
14	15	16	17	18	19	20	21	22	23	24	25	26

Clasificación de los criptosistemas clásicos



Criptosistemas con clave secreta

- Las técnicas utilizadas por los criptosistemas clásicos están orientadas al uso de clave secreta.

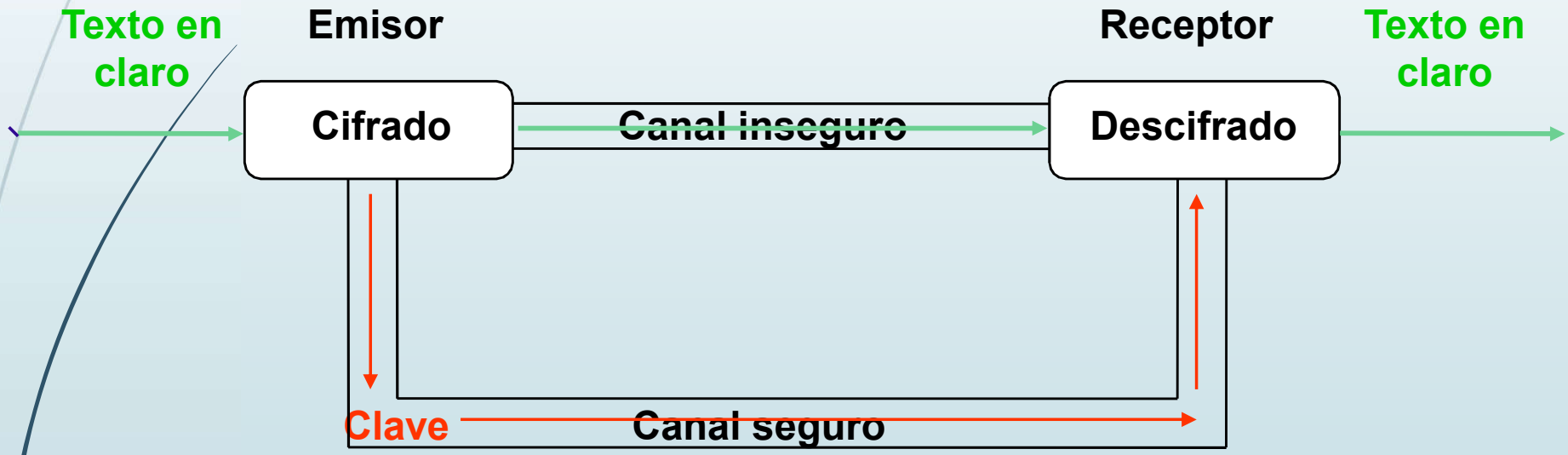
- Un criptosistema con clave secreta es aquel en el que el emisor y el receptor comparten una clave única k. Es condición indispensable, por tanto, la existencia de un canal libre de espionaje por el que se pueda hacer llegar la clave al legítimo receptor.

- El criptosistema está constituido por un **conjunto K de claves**, un **conjunto M de mensajes** en claro, un **conjunto C de mensajes cifrados** y para cada $k \in K$ un par de funciones $E_k: M \longrightarrow C$ y $D_k: C \longrightarrow M$ tales que

$$D_k[E_k(m)]=m \qquad \forall m \in M$$

Debe ser fácil obtener, para cada $k \in K$, los algoritmos necesarios para calcular E_k y D_k.

Esquema de criptosistemas con clave secreta



2.1 Criptosistemas basados en sustituciones

- Para cifrar un texto en claro se **sustituyen uno o varios caracteres** del mismo por **uno o más símbolos**.
  - Se establece por tanto **una o varias aplicaciones** entre el **alfabeto** en el que se escribe el **texto en claro y el alfabeto** o los alfabetos en los que se **escribe el criptograma**.

2.1.1 Sustitución simple

- El caso más sencillo es el de sustitución simple en el que cada carácter del texto en claro (escrito con un alfabeto A cuyos elementos están ordenados) es sustituido por su correspondiente carácter en un alfabeto ordenado B.
  - Si consideramos que $A=\{a_1,a_2,...,a_n\}$ entonces $B=\{f(a_1),f(a_2),...,f(a_n)\}$, donde $f:A\longrightarrow B$ es una **aplicación biyectiva**.
  - En este apartado podemos encuadrar el método de cifrado de **Julio César** o **el atbash hebreo** estudiados en el tema anterior.
- Un mensaje $m=m_1m_2.....$ se cifrará como

$$\mathbf{c=E_k(m)=f(m_1)f(m_2)...}$$

2.1.1 Sustitución simple: cifrado monoalfabético

Ejemplo

- Supongamos que queremos cifrar el mensaje

$$m=AGOSTO$$

el alfabeto en el que está escrito es

$\mathcal{A}=\{A,B,C,D,E,F,G,H,I,J,K,L,M,N,Ñ,O,P,Q,R,S,T,U,V,W,X,Y,Z\}$

y en el que debemos cifrar

$\mathcal{B}=\{Q,W,E,R,T,A,S,D,F,G,Z,X,C,V,B,P,O,I,U,Y,Ñ,L,K,J,H,M,N\}$

- Supongamos que $f:\mathcal{A}\longrightarrow\mathcal{B}$ asocia a cada elemento de $\mathcal{A}$ el correspondiente en $\mathcal{B}$ que ocupa su misma posición. Se tiene

$$c=E_k(m)=QSPYÑP$$

2.1.1 Sustitución simple: cifrado monoalfabético

Cifradores tipo César con alfabetos mixtos

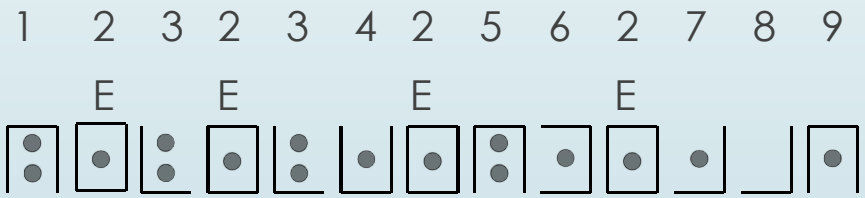
El alfabeto de texto en claro y el de cifrado no coinciden.

$\mathcal{A}$={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}

$\mathcal{B}$={! ,1, #, =, *,2, +, },",3,.....}

- Lápida del cementerio de Trinity

  Desde el punto de vista histórico, quizás, uno de los casos más interesantes se encuentra en la inscripción de una lápida del cementerio de Trinity (un distrito de Nueva York), realizada en 1794.



Este criptograma fue descifrado en 1896.

Criptoanálisis del cifrado del César

TexCif01.txt

QYIWXVSTVMPIVGVMTXSEQEOMWMW

CripClas

https://www.visca.com/regexdict/

https://regex101.com/

2.1.1 Sustitución simple: sustitución afín

- Los **cifradores monoalfabéticos genéricos**, también llamados de **transformaciones afines**, sustituyen los caracteres del texto en claro usando la transformación

$$c_i=E_k(m_i)=(r\,m_i+k) \bmod n \qquad k,r\in\{0,1,2,\ldots,n-1\}$$

  - En donde **r** se conoce como constante de **decimación** y **k** como constante de **desplazamiento**.
  - El par **(k,r)** constituye la clave

- La función de descifrado se obtiene haciendo uso de la aritmética modular, se tiene $c_i= (rm_i+k) \bmod n \rightarrow c_i-k = rm_i \bmod n \rightarrow m_i= [(c_i-k)r^{-1}] \bmod n$, luego

$$D_k(c_i) = m_i= [(c_i-k)r^{-1}] \bmod n$$

- Es necesario exigir que **mcd(n,r)=1** para que la ecuación **r x mod n=1** tenga solución, por lo que el número de claves distintas es **n ϕ(n)**, es decir, los **n posibles desplazamientos** por la **función** de **Euler de n**.

2.1.1 Sustitución simple: sustitución afín

Ejemplo

- Consideremos el alfabeto A={_ABCDEFGHIJKLMNÑOPQRSTUVWXYZ} y el texto en claro

m=TRANSFERENCIA_CONFORME

- A cada símbolo del alfabeto le asociamos un número

_	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	27

- Para cifrar m utilizamos la clave k=2 y r=3, obteniendo

$E_k(T)=E_k(21)= 3\cdot21+2 \bmod 28 = 9 = I$
$E_k(R)=E_k(19)= 3\cdot19+2 \bmod 28 = 3 = C$
$E_k(E)=E_k(5) = 3\cdot5+2 \bmod 28 = 17 = P$

o sea

c=ICEOFSPCPOKAEBKUOSUCMP

Ejemplo

- Para descifrar c utilizamos la clave k=2 y r^{-1}=19*, obteniéndose

$D_k(I) = D_k(9) = (9-2)\ 19 \bmod 28 = 21 = T$
$D_k(C) = D_k(3) = (3-2)\ 19 \bmod 28 = 19 = R$
$D_k(P) = D_k(17) = (17-2)19 \bmod 28 = 5 = E$

- Si generamos el alfabeto de cifrado, se simplificará el descifrado de posteriores criptogramas en los que se haya utilizado la misma clave.

_	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	27
2	5	8	11	14	17	20	23	26	1	4	7	10	13	16	19	22	25	0	3	6	9	12	15	18	21	24	27
B	E	H	K	N	P	S	V	Y	A	D	G	J	M	O	R	U	X	_	C	F	I	L	Ñ	Q	T	W	Z

- Tenemos lo que se conoce como ***caja de sustitución***.

2.1.1 Sustitución simple: Inverso en Z_n

*Algoritmo extendido de Euclides

¿ **x** = 3^{-1} mod 28 ? → 1 = **x**·3 mod 28 (existe ya que mcd(28,3)=mcd(2^2·7,3)=1)

D = c · d + r

28 = 9·3+ **1** ⇒

1 = 28 - 9·3 mod 28 = (-9)·3 mod 28 = (28-9)·3 mod 28 =

= **19** ·3 mod 28

Luego **x** = 3^{-1} mod 28 = **19**

Ejemplo de Inverso en Z_n

Algoritmo extendido de Euclides

¿ **x** = 17^{-1} mod 29 ? → 1 = **x**·17 mod 29

(existe ya que mcd(29,17)=1)

D = c · d + r

29 = 1·17 + **12** ⇒ **12** = 29 - 1·17 mod 29 = **(-1)·17** mod 29

17 = 1·**12** + **5** ⇒ **5** = 17 - 1·**12** mod 29 = 17 – 1·**(-1) ·17** mod 29
= **2·17** mod 29

12 = 2·**5** + **2** ⇒ **2** = **12** - 2·**5** mod 29 = **(-1)·17** – 2·**2·17** mod 29
= (-5)·17 mod 29 = **(-5)·17** mod 29

5 = 2·**2** + **1** ⇒ **1** = **5** - 2·**2** mod 29 = **2·17**– 2·**(-5)·17** mod 29
= **12**·17 mod 29

- Luego **x** = 17^{-1} mod 29 = **12**

Ejemplo de Inverso en Z_n

Algoritmo extendido de Euclides

¿ **x** = 18^{-1} mod 29 ? → **1** = **x**·18 mod 29

(existe ya que mcd(29,18)=1)

D = c · d + r

29 = 1·18 + **11** ⇒ **11** = 29 - 1·18 mod 29 = **(-1)·18** mod 29

18 = 1·**11** + **7** ⇒ **7** = 18 - 1·**11** mod 29 = 18 – 1·**(-1)** ·**18** mod 29
= **2·18** mod 29

11 = 1·**7** + **4** ⇒ **4** = **11** - 1·**7** mod 29 = **(-1)·18** – 1·**2·18** mod 29
= **(-3)·18** mod 29

7 = 1·**4** + **3** ⇒ **3** = **7** - 1·**4** mod 29 = **2·18**– **(-3)** ·**18** mod 29 = **5·18** mod 29

4 = 1·**3** + **1** ⇒ **1** = **4** - 1·**3** mod 29 = **(-3)·18**– 1·**5·18** mod 29
= **(-8)** ·18 mod 29 = **21**·18 mod 29

- Luego **x** = 18^{-1} mod 29 = **21**

2.1.1 Sustitución simple: criptoanalisis

Cifrados monoalfabéticos por sustitución

- El número de claves, en general, es n!; que para un alfabeto de 26, 27 ó 28 caracteres es bastante grande.
- El elevado número de claves hace que el criptoanálisis mediante estudio exhaustivo de las claves requiera mucho tiempo.
- En un alfabeto con 27 letras si se utiliza un ordenador capaz de comprobar la validez de una clave en una millonésima de segundo, para estudiarlas todas necesitaríamos 10^{22} segundos, lo que equivale a

$$\frac{10^{22}}{3 \cdot 10^{7}} \cong 345.283.785.100.000$$

años.

2.1.1 Sustitución simple: criptoanalisis

- Observemos que en el ejemplo la letra E aparece tres veces en el texto en claro, el mismo número de veces que aparece P en el texto cifrado. Lo mismo ocurre con las letras A y E, O y U, etc.

m=TRANSFERENCIA_CONFORME c=ICEOFSPCPOKAEBKUOSUCMP

- El sistema puede ser atacado mediante análisis estadístico de las frecuencias de aparición de los distintos caracteres en los criptogramas interceptados, comparándolas con las frecuencias de aparición de las distintas letras en un determinado idioma.

- Si alguna letra "x" del criptograma tiene frecuencia claramente similar a la frecuencia de alguna letra "y" del idioma, se descifra x como y. El estudio estadístico se completa con las frecuencias de aparición de digramas, trigramas, etc.

2.1.1 Sustitución simple: criptoanalisis, ejemplo

- Un equipo de delincuentes informáticos ha interceptado un mensaje cifrado que se transmite entre dos sucursales bancarias, tras meses de intento. El mensaje contiene la clave de acceso a las bases de datos para el día. Se sabe que el sistema criptológico que utilizan es de sustitución afín y que a las letras C e I del texto en claro le corresponden C y Z respectivamente en el criptograma. El alfabeto utilizado es

  A={ ABCDEFGHIJKLMNÑOPQRSTUVWXYZ}

  ¿Pueden obtener la clave utilizada con estos datos?

- Supongamos que se ha realizado la siguiente asignación numérica al alfabeto de 27 letras

A	*B*	*C*	*D*	*E*	*F*	*G*	*H*	*I*	*J*	*K*	*L*	*M*	*N*
0	1	2	3	4	5	6	7	8	9	10	11	12	13
Ñ	*O*	*P*	*Q*	*R*	*S*	*T*	*U*	*V*	*W*	*X*	*Y*	*Z*	
14	15	16	17	18	19	20	21	22	23	24	25	26	

2.1.1 Sustitución simple: criptoanalisis, ejemplo

La función de cifrado debe tener la forma

$$E_k(m_i) = (r\, m_i + k) \bmod 27$$

Sabemos que

$$E_k(2) = (2r + k) \bmod 27 = 2 \bmod 27$$

$$E_k(8) = (8r + k) \bmod 27 = 26 \bmod 27$$

Resolviendo el sistema

$$\left.\begin{aligned} 2r+k &= 2 \bmod 27 \\ 8r+k &= 26 \bmod 27 \end{aligned}\right\}$$

obtenemos

$$6\, r = 24 \bmod 27 \longrightarrow r = 4 \bmod 27$$

$$k = -6 \bmod 27 = 21 \bmod 27$$

Por tanto la función de cifrado es

$$E_k(m_i) = (4m_i + 21) \bmod 27$$

2.1.1 Sustitución simple: criptoanalisis, ejemplo

- Vamos a intentar descifrar este criptograma realizado por sustitución

TZTLJPTCDTRHTHCBKIJTVCKCKÑHTPTPTMJVUKRHTÑJTCZEEUKZYTVMEPKZ XJCECMJTVKZÑTVKCKTZYTCKZKILJKRHTVTZHUDEZHJMJPEYECDTCTVHCE PJLJZE

ES EVIDENTE QUE UN GOBIERNO NO PUEDE DECIR LO QUE PIENSA A LOS MERCADOS FINANCIEROS, PERO NO ES MENOS OBVIO QUE RESULTA SUICIDA MANTENER UNA DIVISA

TexCif02.txt

CripClas