2.- Criptografía clásica

2.1 - Criptosistemas basados en sustituciones
2.1 - Criptosistemas basados en transposiciones

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

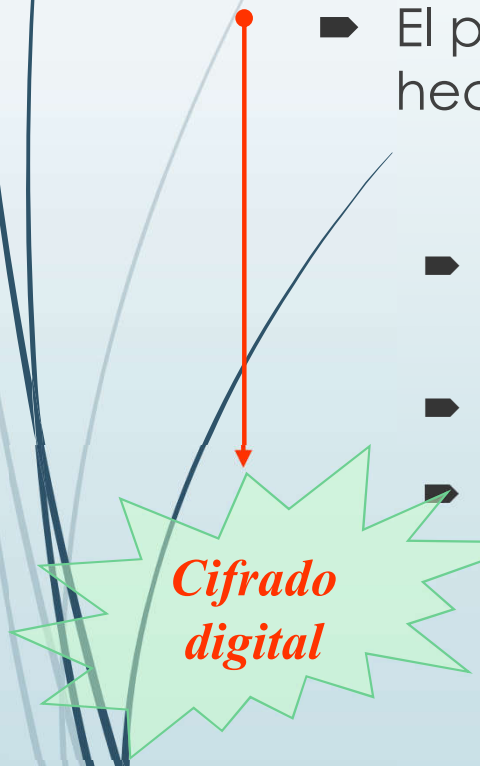
Cifrado con clave pública

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.



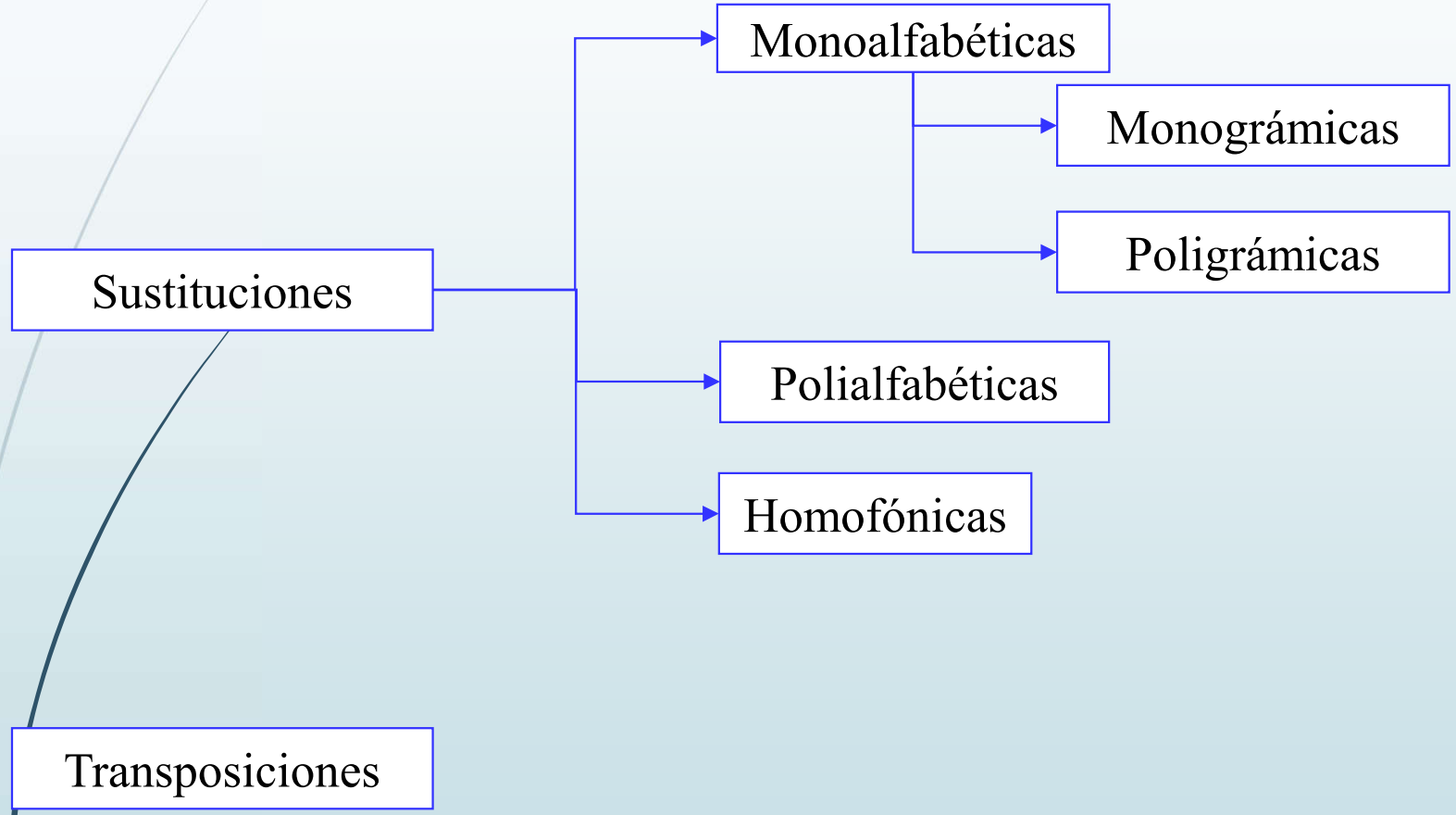
Alfabetos de cifrado

- 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.

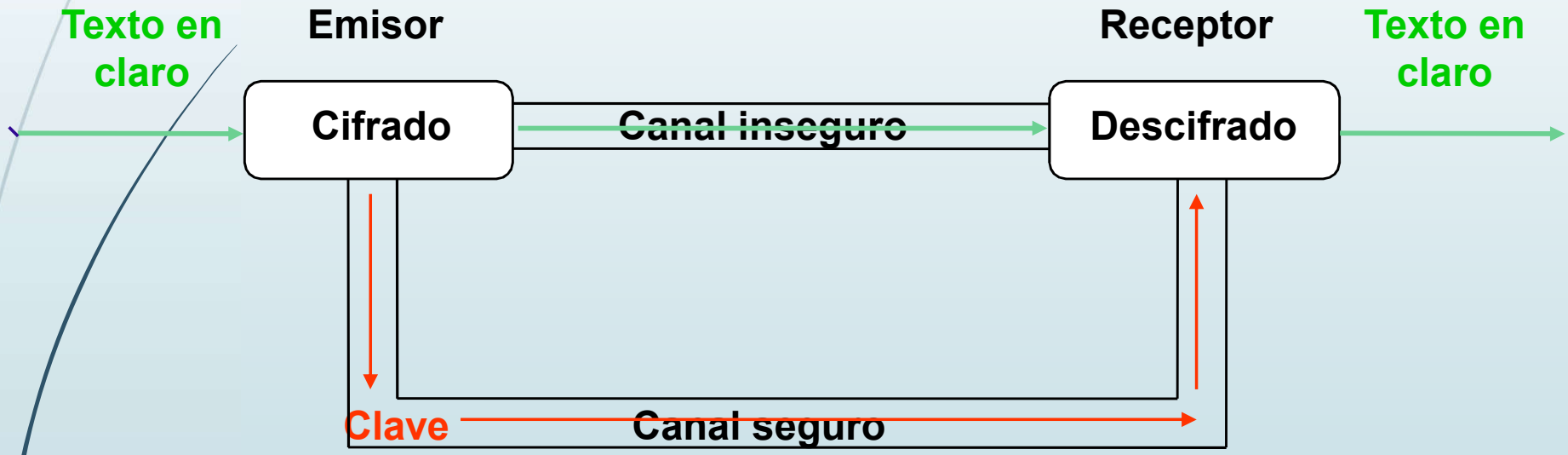
- Un criptosistema con clave secreta es aquel en el que el emisor y el receptor comparten una clave única k. Es condición indispensable, por tanto, la existencia de un canal libre de espionaje por el que se pueda hacer llegar la clave al legítimo receptor.

- 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

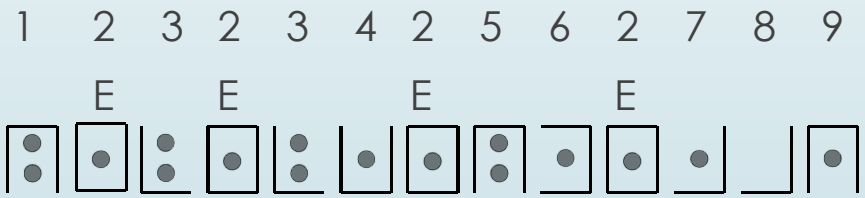
El alfabeto de texto en claro y el de cifrado no coinciden.

$\mathcal{A}$={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: criptoanálisis

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

TZTLJPTCDTRHTHCBKIJTVCKCKÑHTPTPTMJVUKRHTÑJTCZEEUKZYTVMEPKZXJC
ECMJTVKZÑTVKCKTZYTCKZKILJKRHTVTZHUDEZHJMJPEYECDTCTVHCEPJLJZE

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

2.1.2 Homofónicos

- Cada carácter del alfabeto $\mathcal{A}$ en que se escribe el texto en claro es sustituido por un carácter cualquiera de entre un conjunto contenido en el alfabeto $\mathcal{B}$ en el que se escriben los criptogramas. En este caso entre $\mathcal{A}$ y $\mathcal{B}$ se establece una correspondencia que no es aplicación.
- A los elementos del conjunto $\mathcal{B}$ se les llama homofónos.
- Con la utilización de este sistema se evita el ataque estadístico de frecuencias ya que se puede conseguir que las frecuencias en los criptogramas sean distintas a las del texto en claro.

2.1.2 Homofónicos

Ejemplo

Supongamos que A={a,b,c,d,e} y que las frecuencias de aparición de estos caracteres en textos en claro es

Carácter	a	b	c	d	e
Frecuencia	40%	20%	20%	10%	10%

Sea B={0,1,2,3,4,5,6,7,8,9} el alfabeto en el que escribiremos los textos cifrados. Mediante la asignación

Texto en claro	a	b	c	d	e
Criptograma	0 1 2 3	4 5	6 7	8	9

se consigue que la frecuencia de todos los elementos de B sea del 10%.

2.1.3 Polialfabéticos monográmicos

- Una forma alternativa para evitar el ataque estadístico de frecuencias es utilizar varios alfabetos para cifrar el texto en claro.
- Si, por ejemplo, utilizamos dos alfabetos para cifrar generados a partir de las palabras clave "LOCOMOTORA" "MURCIELAGO"

1	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
2	L	O	C	M	T	R	A	B	D	E	F	G	H	I	J	K	N	Ñ	P	Q	S	U	V	W	X	Y	Z
3	Z	Y	X	W	V	T	S	Q	P	Ñ	N	K	J	H	F	D	B	O	G	A	L	E	I	C	R	U	M

el texto en claro

m=MAYO FLORIDO

se puede cifrar utilizando el segundo alfabeto para las letras que ocupen posición impar y el tercero para las que ocupen posición par, obteniendo

c=HZYD RKKPPMD

La frecuencia de aparición de la letra O en m es 3 veces mientras que ninguna letra aparece tres veces en c, en cambio en c hay tres letras que se repiten dos veces y en m ninguna.

2.1.3 Polialfabéticos monográmicos

- La mayoría de los sistemas de sustitución poligráfica están basados en la sustitución de los caracteres del texto en claro de una forma **periódica**:

  dados d alfabetos $\mathcal{B}_1, \mathcal{B}_2, \ldots, \mathcal{B}_d$, se establecen correspondencias $f_i: \mathcal{A} \longrightarrow \mathcal{B}_i$ entre el alfabeto del texto en claro y los alfabetos del criptograma; así, si $m = m_1 m_2 \ldots m_d m_{d+1} m_{d+2} \ldots m_{2d} \ldots$

  $$c = E_k(m) = f_1(m_1) f_2(m_2) \ldots f_d(m_d) f_1(m_{d+1}) f_2(m_{d+2}) \ldots f_d(m_{2d}) \ldots$$

2.1.3 Polialfabéticos monográmicos: método Vigenère

- Uno de los métodos más simples de sustitución polialfabética es el desarrollado por el francés Blaise Vigenère (1523-1596). En este método la clave es utilizada para indicar el alfabeto en el que se sustituirá cada carácter del texto en claro.

- Sea $k=k_1k_2...k_d$ la clave, en la que los elementos k_i representan caracteres del alfabeto A de los mensajes en claro y los números de las posiciones que ocupan en A.

- Si $a \in A$

$$f_i(a)=(a+k_i) \bmod n$$

donde n es el número de elementos de A.

2.1.3 Polialfabéticos monográmicos: método Vigenère

- La tabla facilita la labor de cifrado y descifrado, para ello hay que repetir la clave tantas veces como sea preciso hasta cubrir el texto en claro

M

R

D

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

2.1.3 Poli. monog.: ejemplo Vigenère

Supongamos que queremos cifrar el mensaje

m=MAYO LLOVIDO Y FLORIDO

utilizando la clave

k=ROSA

M	**A**	**Y**	**O**	**L**	**L**	**O**	**V**	**I**	**D**	**O**	**Y**	**F**	**L**	**O**	**R**	**I**	**D**	**O**
R	O	S	A	R	O	S	A	R	O	S	A	R	O	S	A	R	O	S
D	**O**	**Q**	**O**	**C**	**Z**	**H**	**V**	**Z**	**R**	**H**	**Y**	**W**	**Z**	**H**	**R**	**Z**	**R**	**H**

Observemos que

3=12+18 mod 27 (D=M+R mod 27)

15=0+15 mod 27 (O=A+O mod 27)

⋮

7=15+19 mod 27 (G=O+S mod 27)

además las secuencias ZH Y ZRH se repiten en el criptograma, esto es debido a que en el texto en claro se repiten el digrama LO y el trigrama IDO que corresponde cifrarlos con el digrama OS y el trigrama ROS de la clave, respectivamente.

2.1.3 Poli. monog.: cifrador autoclave

- Es una variante del algoritmo de Vigenère, conocida también como segundo cifrado de Vigenère, cuya característica radica en que se cifra el mensaje con una clave que consiste en el mismo mensaje al que se añade al comienzo una clave denominada primaria.
  - La secuencia de clave es, por tanto, tan larga como el propio mensaje.

PROTECCION DE LA INFORMACION
DOCTORADOP RO TE CCIONDELA IN
SGQNSTCLDC US EE KONDEOENIWZ

http://www.criptored.upm.es/thoth/#

(Píldora 19: ¿Qué es la cifra de Vigenère?)

(Píldora 20: ¿Cómo se ataca por Kasiski la cifra de Vigenère?)

2.1.3 Poli. monog.: cifrador Vernam

- El ingeniero estadounidense Gilbert Vernam en 1918 diseñó un sistema de cifrado que inicialmente fue utilizado en la comunicación a través del telégrafo.
  - Está basado en los códigos Baudot de los teletipos desarrollados por su compañía.
- Como clave se toma una secuencia aleatoria infinita binaria que se suma módulo 2 al texto en claro (en binario) para obtener el mensaje cifrado.
- Mediante esta técnica las características de frecuencia y periodicidad de los caracteres no pueden ser utilizadas por los criptoanalistas ya que son totalmente aleatorias.
- Si $m=m_1m_2...$ es el texto en claro y $k=k_1k_2...$ es la clave, el criptograma $c=E_k(m)=c_1c_2...$ se obtiene haciendo

$$c_i=(m_i+k_i) \bmod 2 \quad i=1,2,...$$

- El algoritmo de descifrado D_k se obtiene de forma análoga

$$m_i=(c_i+k_i) \bmod 2 \quad i=1,2,...$$

2.1.3 Poli. monog.: ejemplo de cifrador Vernam

ASCII

Texto en claro	1	1	0	0	1	0	0	1
Clave	0	0	1	1	1	1	0	0
Criptograma	1	1	1	1	0	1	0	1

Utilizando el código ASCII binario vamos a cifrar el mensaje m=SAL utilizando la clave k=YES.

LETRA	*ASCII*	*BINARIO*
S	83	01010011
A	65	01000001
L	76	01001100
Y	89	01011001
E	69	01000101

SAL	83 65 76	01010011	01000001	01001100
YES	89 69 83	01011001	01000101	01010011
LF EOT US	10 04 31	00001010	00000100	00011111

2.1.3 Poli. monog.: cifrador Vernam

- En este criptosistema cada clave es utilizada una sola vez (**one-time pad**) lo que le resta eficiencia ya que el esfuerzo necesario para hacer llegar la clave con seguridad al receptor es el mismo que para que le llegue el mensaje en claro. Si la clave es utilizada varias veces el sistema puede ser roto mediante estudio estadístico de frecuencias.

2.1.4 Poligrámicos monoalfabéticos

- Los métodos de sustitución anteriormente estudiados sustituyen uno a uno los caracteres del texto en claro por otro carácter del alfabeto o alfabetos de cifrado,
  - en cambio los métodos de cifrado poligrámico sustituyen bloques de caracteres del mensaje a cifrar, consecutivos o no, por otros bloques de símbolos del alfabeto de criptogramas;
  - de esta forma se destruye la significancia de las frecuencias de aparición de monogramas.
- El sistema más simple es aquel que permite sustituir digramas del texto plano por parejas de símbolos del alfabeto de cifrado.

2.1.4 … Criptosistemas matriciales. Método Hill

- En 1929 Hill propuso que los criptosistemas se formulasen con un modelo simple de transformaciones sobre M.
  - Asignando a cada carácter del texto en claro un entero positivo, un mensaje a cifrar puede ser identificado con una **n-tupla** de **enteros positivos** y las operaciones de cifrado y descifrado con una pareja de transformaciones lineales inversas.
- El modelo más sencillo de cifrado consiste en **multiplicar** por una **matriz cuadrada e invertible** el texto en claro, utilizando el **producto por su inversa para descifrar** los textos cifrados.

2.1.4 … Criptosistemas matriciales. Método Hill

- Si el alfabeto utilizado para escribir los mensajes en claro tiene m elementos y la matriz de cifrado (clave) es

$$K = \begin{bmatrix} k_{11} & k_{12} & \cdots & k_{1n} \\ k_{21} & k_{22} & \cdots & k_{2n} \\ \vdots & \vdots & \ddots & \vdots \\ k_{n1} & k_{n2} & \cdots & k_{nn} \end{bmatrix}$$

un texto en claro

$$M=m_1m_2\ldots m_nm_{n+1}m_{n+2}\ldots m_{2n}\ldots$$

se transforma en el criptograma

$$C=c_1c_2\ldots c_nc_{n+1}c_{n+2}\ldots c_{2n}\ldots$$

donde

$$c_{rn+i} = \sum_{j=1}^{n} k_{ij} m_{rn+i} \mod n \quad \forall i=1,\ldots,n \quad \forall r=0,\ldots$$

2.1.4 … Criptosistemas matriciales. Método Hill

- Expresando M en forma matricial,

$$\mathrm{M} = \begin{bmatrix} m_1 & m_{n+1} & \cdots \\ m_2 & m_{n+2} & \cdots \\ \vdots & \vdots & \\ m_n & m_{2n} & \cdots \end{bmatrix}$$

el cifrado se expresa

$$C=E_k(M)=K\ M \mod n$$

- El descifrado se obtiene utilizando K^{-1}

$$D_k(C)=K^{-1}\ C \mod n=K^{-1}K\ M \mod n=M$$

2.1.4 … Criptosistemas matriciales. Método Hill

- *Notemos que este método sustituye* ***n-gramas del texto en claro*** *por* ***n-gramas del mensaje cifrado***.

- La **matriz K debe ser siempre cuadrada** y sus elementos serán la clave secreta además debe ser no singular; esto es

$$\det(K) \neq 0$$

- Este criptosistema, bajo ciertas condiciones, presenta alta seguridad y puede implementarse fácilmente en los ordenadores.

2.2 Criptosistemas basados en transposiciones

- En este tipo de criptosistemas el cifrado se realiza **reordenando** los caracteres del texto en claro.
  - El resultado de esta acción es la **difuminación** de la información del texto en claro y provocar, por tanto, la ***difusión*** propuesta por Shannon para la protección de la misma.

2.2 Criptosistemas basados en transposiciones

- La reordenación se suele realizar de acuerdo con un **esquema preestablecido**, por lo general coincidente con algún tipo de figura (la más común es una tabla bidimensional).
- Se escriben los caracteres en un determinado orden (por ejemplo por filas) para leerlos a continuación en otro distinto (por ejemplo por columnas), el resultado de esta lectura es el mensaje cifrado.
- El descifrado se obtiene escribiendo el criptograma en el segundo orden (columnas) para leerlo de la misma manera que se escribió originalmente (por filas).
- Un ejemplo de este tipo de cifrado lo constituye la **scitala** espartana estudiada en una sección anterior.

2.2 Criptosistemas basados en transposiciones

Ejemplo

Si deseamos cifrar el mensaje **m=UN_DIA_CUALQUIERA** escribiendo por filas en una tabla 4x5, tendremos

	1	2	3	4	5
1	U	N		D	I
2	A		C	U	A
3	L	Q	U	I	E
4	R	A			

Si leemos las columnas en el orden 1,3,5,2,4 el mensaje cifrado que se obtiene es

c=UALR_CU_IAE_N_QADUI_

La clave utilizada puede ser del tipo k=45c13524

Para descifrar c, utilizando la clave anterior k, debemos utilizar una tabla 4x5 (45), escribir los caracteres en columna (c) en el orden 1,3,5,2,4 y posteriormente leer por filas.

2.2 Criptosistemas basados en transposiciones

- En algunos métodos los caracteres del texto en claro son permutados con un periodo fijo d.

- Dado $A=\{1,2,...,d\}$ y $\sigma:A\longrightarrow A$ una permutación cualquiera de A, la clave del cifrado viene dada por el par

$$k=(d,\sigma)$$

- El texto en claro se divide en bloques de d caracteres que son permutados de acuerdo con σ.

- Así, el mensaje

$$\mathbf{m=m_1m_2...m_d \mid m_{d+1}m_{d+2}....m_{2d} \mid m_{2d+1}....}$$

es cifrado

$$\mathbf{c=E_k(m)=m_{\sigma(1)}m_{\sigma(2)}...m_{\sigma(d)} \mid m_{d+\sigma(1)}m_{d+\sigma(2)}...m_{d+\sigma(d)} \mid m_{2d+\sigma(1)}....}$$

- El descifrado se realiza usando la permutación inversa de σ.

Ejemplo

Supongamos que d=6 y σ=(2 5 1 3 6 4). El mensaje del ejemplo anterior

m=UN_DIA_CUALQUIERA

tiene el siguiente cifrado

c=NIU_ADCL_UQAIAUE_R

Para descifrar c utilizaremos la permutación inversa de σ,

$\sigma^{-1}=(3\ 1\ 4\ 6\ 2\ 5)$.

$$\sigma=\begin{pmatrix}1 & 2 & 3 & 4 & 5 & 6\\ 2 & 5 & 1 & 3 & 6 & 4\end{pmatrix}$$

$$1 \overset{\sigma}{\mapsto} 2$$
$$2 \overset{\sigma}{\mapsto} 5$$
$$3 \overset{\sigma}{\mapsto} 1$$
$$4 \overset{\sigma}{\mapsto} 3$$
$$5 \overset{\sigma}{\mapsto} 6$$
$$6 \overset{\sigma}{\mapsto} 4$$

$$\sigma^{-1}=\begin{pmatrix}1 & 2 & 3 & 4 & 5 & 6\\ 3 & 1 & 4 & 6 & 2 & 5\end{pmatrix}$$

$$1 \overset{\sigma^{-1}}{\leftarrow} 2$$
$$2 \overset{\sigma^{-1}}{\leftarrow} 5$$
$$3 \overset{\sigma^{-1}}{\leftarrow} 1$$
$$4 \overset{\sigma^{-1}}{\leftarrow} 3$$
$$5 \overset{\sigma^{-1}}{\leftarrow} 6$$
$$6 \overset{\sigma^{-1}}{\leftarrow} 4$$

2.2 Criptosistemas basados en transposiciones

Criptoanálisis

- En el criptoanálisis, un sistema de transposición de caracteres es fácilmente reconocible, ya que **las frecuencias de aparición de los mismos coinciden** con las del mensaje original.
- La técnica utilizada para romper el cifrado es el **uso de anagramas** que reordenan los caracteres del criptograma hasta situarlos en su posición inicial.
  - Esta tarea es facilitada por el uso de frecuencias de aparición en determinado lenguaje de digramas, trigramas, etc.

TPNOTOAOPODRYADOAUROSUNAS

TODOSPARAUNOYUNOPARATODOS

TexCif03.txt

CripClas