2.1.2 Homofónicos

- Cada carácter del alfabeto *A* en que se escribe el texto en claro es sustituido por un carácter cualquiera de entre un conjunto contenido en el alfabeto *B* en el que se escriben los criptogramas. En este caso entre *A* y *B* se establece una correspondencia que no es aplicación.

- A los elementos del conjunto *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

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.

P R O T E C C I O N D E L A I N F O R M A C I O N
D O C T O R A D O P R O T E C C I O N D E L A I N
S G Q N S T C L D C U S E E K O N D E O E N I W Z

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 $m=m_1m_2\ldots$ es el texto en claro y $k=k_1k_2\ldots$ es la clave, el criptograma $c=E_k(m)=c_1c_2\ldots$ se obtiene haciendo

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

- El algoritmo de descifrado D_k se obtiene de forma análoga

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

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

$$M=m_1 m_2 \ldots m_n m_{n+1} m_{n+2} \ldots m_{2n} \ldots$$

se transforma en el criptograma

$$C=c_1 c_2 \ldots c_n c_{n+1} c_{n+2} \ldots c_{2n} \ldots$$

donde

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

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.

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 σ:A⟶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

2.2 Criptosistemas basados en transposiciones

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,

σ⁻¹=(3 1 4 6 2 5).

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

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

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

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

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