Métodos de sustitución poligráfica.

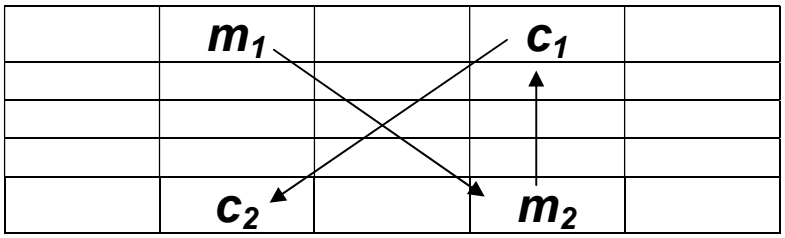
Denominamos así a todos aquellos sistemas de sustitución en los que se utiliza más de un grupo de caracteres en claro para la sustitución, que es a su vez sustituido por otro grupo de caracteres cifrados, no necesariamente de la misma longitud. Es decir, aquí no sustituiremos carácter a carácter, sino en grupos. La diferencia con un código es que aquí el grupo cifrado no es siempre el mismo ya que depende de la clave. Hablaremos de métodos de sustitución digráfica cuando se sustituyAn pares de caracteres. El método más conocido de este tipo es el cifrado de Playfair que explicamos a continuación.

Método de Playfair.

Este método de cifrado, aunque popularizado por el barón de Saint Andrews, Lyon Playfair, fue desarrollado por su amigo Sir Charles Wheatstone alrededor del año 1854. Playfair presentó el método al ministerio de asuntos exteriores británico que estaba buscando un método de cifrado para utilizarlo en la guerra contra los Boers. Al principio de la guerra el ejército británico utilizaba libros de códigos, pero al ser destruidos o capturados gran parte de ellos, los oficiales empezaron a enviarse los mensajes en latín. Este método, ya utilizado por Julio César en la guerra de las Galias, aunque sustituyendo el latín por el griego, tenía la desventaja de que no todos los oficiales británicos sabían latín y muy probablemente había entre las filas de los boers gente letrada que se manejase bien en esta lengua.

Este método, con algunas variaciones, fue utilizado hasta la segunda guerra mundial debido principalmente a su sencillez y a su fácil adaptación a cualquier entorno. Se trata de un cifrado digráfico formado por una matriz cuadrada de 5x5 elementos en los que se introducen las letras del alfabeto, utilizándose la misma celda para la I y la J al no disponer de celdas para ubicarlas separadamente. En español nos encontraríamos también con el problema de la Ñ. El método de cifrado es muy sencillo. En primer lugar se colocan las letras sin repeticiones de la palabra que se va a utilizar como clave, y posteriormente se añaden el resto de letras del alfabeto hasta rellenar la tabla. Una vez confeccionada ésta, se divide el texto a cifrar en grupos de dos letras consecutivas comprobando que no exista ningún par de letras iguales. En el caso de que esto ocurra, se inserta un nulo, es decir, una letra al azar que no dé lugar a confusión en el contenido del mensaje. Una vez hecho esto las reglas a seguir para cifrar son:

1. Si las dos letras a cifrar están en diagonal, el par cifrado será el formado por las letras que forman la diagonal de los otros dos vértices del rectángulo. Si el par del mensaje es m_1, m_2 y el del cifrado correspondiente es c_1, c_2 el proceso de cifrado se vería de la siguiente manera.



2. Si las dos letras a cifrar están en la misma línea horizontal, el par cifrado estará formado por las letras a la derecha de ambas, siendo la primera columna la que sigue a la última y la última la que antecede a la primera. Matemáticamente podemos decir que en el caso de que la letra cifrada corresponde a la letra en claro que está en la columna de la primera más o menos uno módulo 5.
3. Si las dos letras a cifrar están en la misma línea vertical, el par cifrado está formado por las letras debajo de ambas, siendo la primera fila la que sigue a la última y la última la que antecede a la primera. Matemáticamente podemos decir que en el caso de que la letra cifrada corresponde a la letra en claro que está en la fila de la primera más o menos uno módulo 5.

El proceso de descifrado es simplemente la realización de los pasos anteriores en sentido inverso. Por ejemplo, para cifrar la palabra CIEN, lo haríamos en dos pasos. Primero cifraremos el par CI y después el par EN con lo que obtendríamos:

Variantes del método de Playfair.

Cifrado con dos tablas.

Pueden utilizarse varias tablas para cifrar y descifrar en lugar de una sola. En este caso se escogería una letra en cada tabla. Se pueden utilizar dos, lo más habitual, o cuatro tablas como propuso Delastelle. El más común es el doble Playfair, que fue utilizado en la Segunda Guerra mundial por los alemanes con el nombre de *Doppelkastenschlussel.* Los criptoanalistas americanos lo conocían simplemente como NI. Básicamente consiste en poner dos tablas juntas tipo playfair con alfabetos distintos y hacer el cruce sobre las dos, es decir, de los dos caracteres a cifrar solo uno debía aparecer en cada tabla. Los alemanes realizaban esa operación dos veces, con lo que estamos hablando de un doble cifrado, el primero con el par de letras del mensaje en claro y el segundo con el par resultado de este cifrado. Los alemanes, muy precavidos, cambiaban las tablas cada tres horas, con lo que el criptoanálisis era extremadamente difícil.

Cifrado con tres tablas.

En este caso hablamos de una versión del cifrado de Polibio. Para hacerlo se utilizan tres tablas dispuestas de la siguiente manera:

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

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

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

La forma de cifrar es muy sencilla, para hacerlo cogemos la tabla de la izquierda como tabla de la primera letra y la superior como la de la segunda. La letra cifrada aparece en la tabla inferior izquierda como la intersección de las otras dos letras. Por ejemplo, si queremos cifrar la palabra CIEN, obtendremos el criptograma FN Tal como muestran las imágenes siguientes.

2

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

1

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

3

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

2

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

1

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

3

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

Sin embargo, no será eso lo que enviaremos, dado que al descifrar no sabríamos qué letra de la fila de la izquierda o qué letra de la columna de la fila

superior correspondería con la letra original. Para ello se escogen dos letras cualesquiera de la columna donde se encuentra la letra de la izquierda, la que hemos señalado con un uno encima de la tabla y otras dos de la fila donde se encuentra la segunda letra del par, en la tabla que hemos marcado como dos. Eso nos permitirá determinar claramente el par de letras en claro. Normalmente la letra cifrada se pone en medio. En nuestro caso el criptograma final correspondiente a la palabra CIEN podría ser KEO BNH.

Cifrado de Hill.

Es el método más matemático, y no es de extrañar ya que su inventor, Lester Hill (1891-1961), era un profesor de matemáticas. En 1929 publicó un artículo en *The American Mathematical Monthly* con el título "*Cryptography in an algebraic alphabet*" en el que exponía su método de cifrado. En este artículo Hill proponía por primera vez la utilización de ecuaciones en aritmética modular para cifrado de información. En 1931 en otro artículo proponía la utilización de matrices para el cifrado de información. Este método de sustitución poligráfica parte de la utilización de una matriz cuadrada invertible *K* que se utiliza como clave. El proceso de cifrado y descifrado es como sigue:

CIFRADO

1) Codificar el mensaje en claro en forma numérica.
2) Dividir el mensaje en trozos de longitud *r*, siendo *r* el rango de la matriz *K*.
3) Realizar con los trozos del mensaje la operación $C = M.K$, siendo *C* el vector que contiene el texto cifrado y *M* el mensaje en claro.

DESCIFRADO

1) Dividir el mensaje cifrado en trozos de longitud *r*.
2) Calcular K^{-1}.
3) Hacer la operación $K^{-1}.C = K^{-1}.K.M=I.M=M,$ siendo *I* la matriz identidad.

Lo cierto es que el método de Hill no es muy práctico, ya que las operaciones con matrices son lentas y además obligan, en el caso de no utilizar dispositivos electrónicos, a guardar la clave *K* en un medio físico. Sin embargo, es la primera aproximación seria de las matemáticas a la criptografía y quizás la primera vez que se utilizaba un problema matemático, fuera de los clásicos de la permutación de elementos, como medio para cifrar información.

Vamos a ver un ejemplo, aunque, tendremos que explicar algunos conceptos de matrices y determinantes. En primer lugar tenemos que ver si la matriz es invertible, para ello calculamos su determinante. Si el determinante es diferente de cero la matriz es invertible, en caso contrario no lo es. Para calcular la inversa de una matriz, hay que calcular primero la matriz adjunta, después aplicarle una trasposición para encontrar la matriz traspuesta y finalmente dividirla por el valor de su determinante. Es decir, si *K* es la matriz clave, los pasos a aplicar serían:

1. Calcular el determinante de *K*, llamémosle *k*.
2. Calcular la matriz adjunta de *K*, que llamaremos *A*.

3. Calcular la matriz traspuesta de *A*, que llamaremos *T*.
4. Dividiremos *T* por *k* y obtenemos K^{-1}

Veámoslo con un ejemplo. Sea *K* la matriz $\begin{pmatrix}3 & 2\\ 3 & 5\end{pmatrix}$, su determinante *k* sería 3x5-2x3=9.

Calculamos la matriz adjunta *A* = $\begin{pmatrix}5 & -3\\ -2 & 3\end{pmatrix}$

Calculamos la traspuesta *T* =$\begin{pmatrix}5 & -2\\ -3 & 3\end{pmatrix}$

Calculamos la inversa K^{-1}=$\begin{pmatrix}5/9 & -2/9\\ -3/9 & 3/9\end{pmatrix}$

Utilizando la siguiente tabla:

Letra	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
Número	01	02	03	04	05	06	07	08	09	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26	27

El mensaje CIEN se codificaría como 3 9 5 14, con lo que para cifrar hacemos las siguientes operaciones: $\begin{pmatrix}27\\ 54\end{pmatrix} = \begin{pmatrix}3 & 2\\ 3 & 5\end{pmatrix}\begin{pmatrix}3\\ 9\end{pmatrix}$ y $\begin{pmatrix}43\\ 85\end{pmatrix} = \begin{pmatrix}3 & 2\\ 3 & 5\end{pmatrix}\begin{pmatrix}5\\ 14\end{pmatrix}$.

Enviaríamos pues el mensaje 25 47 43 85. El receptor simplemente calcularía el inverso de la siguiente manera:

$$\begin{pmatrix}3\\ 9\end{pmatrix} = \begin{pmatrix}5/9 & -2/9\\ -3/9 & 3/9\end{pmatrix}\begin{pmatrix}27\\ 54\end{pmatrix} \text{ y } \begin{pmatrix}5\\ 14\end{pmatrix} = \begin{pmatrix}5/9 & -2/9\\ -3/9 & 3/9\end{pmatrix}\begin{pmatrix}43\\ 85\end{pmatrix}$$

Luego iríamos a la tabla de conversión y obtendríamos el resultado: CIEN.