Sistemas de sustitución monoalfabéticos multiliterales.

Denominamos así a todos aquellos sistemas en los que se sustituye un símbolo o letra por más de un símbolo (multiliteral), pero siempre el mismo, es decir, utilizando un solo alfabeto de sustitución (monoalfabético). Básicamente, al igual que en los monoliterales tenemos dos alfabetos que utilizaremos para cifrar o descifrar. La diferencia básica está en que en este tipo de cifrados lo que se suele utilizar para cifrar y descifrar suele ser una tabla. El método más conocido de este estilo es el denominado cifrado de Polibio, aunque el más sencillo es simplemente hacer una cifra de sustitución simple como las que hemos visto anteriormente, pero cambiando las letras por un número de x dígitos. En el ejemplo siguiente lo cambiamos por su posición relativa en el alfabeto.

Claro	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
Cifrado	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

En este caso la palabra CIEN se transmitiría como: 03090514

Cifrado de Polibio.

Se trata del primer caso conocido de sustitución monoalfabética multilateral. El historiador griego Polibio (203-120 a.c.), creó un sistema de enviar mensajes por medio de antorchas encendidas. Como vemos, en un principio no tenía una función criptográfica, pero sí es la base de muchos de los cifrados que le siguieron. El método consistía básicamente en la creación de una matriz cuadrada de 5 x 5 tal como la siguiente.

	1	*2*	*3*	*4*	*5*
1	A	B	C	D	E
2	F	G	H	IJ	K
3	L	M	N	O	P
4	Q	R	S	T	U
5	V	W	X	Y	Z

El mensaje cifrado venía dado por los números que estaban en la columna y la fina donde estaba la letra. Normalmente, se suele cifrar poniendo como primer número la fila y como segundo la columna. Sin embargo, tal como lo definió Polibio, el primer número es el que define la columna y el segundo la fila. Por ejemplo si queremos cifrar la palabra CIEN, el resultado sería:

Claro	**C**	**I**	**E**	**N**
Cifrado	31	42	51	33

Tal como se utiliza actualmente, el resultado sería el mismo pero con los números intercambiado, es decir:

Claro	**C**	**I**	**E**	**N**
Cifrado	13	24	15	33

Como vemos, uno de los problemas de este tipo de cifrado, en realidad de todos los multilaterales, es que aumenta la longitud del texto, con lo que se tarda más en enviar el mensaje. En la historia ha habido muchas variaciones sobre este tipo de cifrado. Una de ellas es la utilizada en Japón en el siglo XVI por el general Uesugi Kenshin, por los revolucionarios rusos y por Canaris y sus camaradas encarcelados. Básicamente utilizaban una tabla de Polibio, transmitiendo la información mediante ruidos, generalmente hechos golpeando con algo. Según David e. Newton, una variante del cifrado de Polibio, utilizado por los comunistas en la guerra civil española consistía en generar una tabla con tres filas de diez columnas. La fuente es David Kahn que señala que lo utilizaba el sueco Per Meurling, acompañante de Álvarez del Vayo para enseñarle criptografía a su novia. La clave que utilizaba era MDELVAYO, señalando que M era la abreviatura del agente. Probablemente M sería simplemente la abreviatura de Monsieur y tan solo fuese un pasatiempo. Las cifras del Ministerio de Estado que dirigía Del Vayo eran códigos supercifrados. Volviendo a este sistema, la primera fila no tenía numeración y la segunda y tercera se numeraban respectivamente con dos de los números no utilizados en las columnas de la primera fila. Las columnas se numeraban con una permutación de los dígitos del cero al nueve.

El proceso de cifrado consistía en poner una palabra de ocho o menos letras diferentes en la primera fila. En esta palabra se eliminaban las letras repetidas y el resto, hasta completar el alfabeto, se disponían en las dos filas siguientes. El cifrado es similar al de Polibio, pero en este caso las letras pueden codificarse como uno o dos números lo que reduce el tamaño del mensaje y, lo hace un poco más difícil de descifrar, aunque no mucho.

Por ejemplo si queremos cifrar el mensaje CIEN con la clave COMUNIST y utilizando el alfabeto en el orden habitual tendríamos la siguiente tabla:

	8	**3**	**0**	**2**	**4**	**6**	**1**	**7**	**5**	**9**
	C	O	M	U	N	I	S	T		
5	A	B	D	E	F	G	H	J	K	L
9	Ñ	P	Q	R	V	W	X	Y	Z	

El mensaje cifrado sería 86524. El descifrado es sencillo, ya que si el dígito inicial es un cinco o un nueve sabemos que es el carácter viene representado por dos dígitos, en caso contrario, por uno solo.