Tablero de Polibio

Introducción

El tablero de Polibio es una cifra de sustitución simple con la característica de que cada letra del texto plano queda cifrado con dos caracteres.

El algoritmo ofrece muy poca seguridad en la comunicación y puede ser “roto” fácilmente incluso a mano.

Ejemplo

Un rápido ejemplo de cifrado y descifrado a través del tablero de Polibio es este:

La clave consiste en una tabla de cinco filas por cinco columnas, lo que hace un total de 25 posibles caracteres así que las letras “i” y “j” y las letras “u” y “v” se usan indistintamente entre ellas (hay que tener en cuenta que estamos hablando del alfabeto latino).

Para hacer más segura la cifra el orden de las letras puede ser aleatorio. Un método que también se usa para ordenar las letras es la de elegir una palabra “clave” de la longitud que queramos pero con la particularidad de que no debe repetirse ninguna letra en ella, completando la tabla con el resto de letras, ya sea de forma ordenada o desordenada:

	A	B	C	D	E
A	p	h	q	g	m
B	e	a	y	l	n
C	o	f	d	x	k
D	r	c	v	s	z
E	w	b	u	t	i

	A	B	C	D	E
A	c	e	b	r	a
B	d	f	g	h	i
C	k	l	m	n	o
D	p	q	r	s	t
E	v	w	x	y	z

Un ejemplo de cifrado usando la clave de más arriba:

texto en claro: d e f e n d t h e e a s t w a l l o f t h e c a s t l e
texto cifrado: CCBACBBABECC EDABBA BABBDDED EABBBDBD CACB EDABBA DBBBDDEDBDBA

Es fácil ver cómo cada carácter del texto claro se reemplaza por dos caracteres del alfabeto de cifra: las coordenadas podríamos decir. El descifrado es igual de fácil.

Existe una variación mucho más moderna llamada cifrado ADFGVX en la que se emplean estas letras como fila cero y columna cero del cuadrado, lo que hace un total de 36 caracteres disponibles. Este número de caracteres nos permite tener las 26 letras del abecedario más los números de cero al nueve. ¿Y por qué estas 6 letras? Por la facilidad y claridad con que se transmiten y se comprenden cuando el texto cifrado se codifica en Morse para enviarlo vía radio.

Criptoanálisis

Es también un método muy fácil de descifrar al tratarse de una cifra de sustitución. Únicamente ha de tenerse en cuenta que el análisis debe hacerse sobre pares de caracteres en lugar de sobre caracteres individuales.