

Método Atbash

Introducción

Método de cifrado por sustitución monoalfabética simple basado en un alfabeto reversible, empleado por los antiguos hebreos entre los años 600 y 500 a.C. La última columna de la imagen muestra el alfabeto utilizado para escribir parte de los *rollos del Mar Muerto*.

El nombre deriva del sistema que designa, pues se refiere a las letras primera, segunda, penúltima y última del alfabeto hebreo.

En este sistema cada letra del texto plano se sustituye por la equivalente del alfabeto invertido, tal que en nuestro alfabeto la “a” se sustituye por la “z”, la “b” por la “y” y así sucesivamente.

Para descifrar el receptor tiene que realizar operaciones inversas a las que realiza el que cifra.

	Atbash	Atbash	Atbash	Cryptic Script B
Aleph 1	א	ז	ח	א
Beth 2	ב	ז	ט	ב
Ghimel 3	ג	ח	י	ג
Daleth 4	ד	ט	כ	ד
Hé 5	ה	י	ל	ה
Vau 6	ו	כ	מ	ו
Zain 7	ז	ל	נ	ז
Heth 8	ח	מ	ס	ח
Teth 9	ט	נ	פ	ט
Yod 10	י	ס	צ	י
Kaph 20	כ	פ	ק	כ
Lamed 30	ל	צ	ר	ל
Mem 40	מ	ק	ש	מ
Nun 50	נ	ר	ת	נ
Samekh 60	ס	ש	י	ס
Ayin 70	ע	ת	פ	ע
Phe 80	פ	י	צ	פ
Tzaddi 90	צ	פ	ק	צ
Guoph 100	ק	ק	ל	ק
Resh 200	ר	ר	מ	ר
Shin 300	ש	ש	נ	ש
Tau 400	ת	ת	ז	ת

Ejemplo

texto claro: metodoatbash

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

texto cifrado: nvglwlgzyzhs

Criptoanálisis

Se sigue el mismo procedimiento que con cualquier cifrado de sustitución: análisis de frecuencias.