

Criptoanálisis

1. Deducir por criptoanálisis el alfabeto utilizado para cifrar el siguiente texto. Se tiene como dato que el texto está en español (sin letra ñ) y que el cifrado es monoalfabético. Se recomienda utilizar análisis de la frecuencia y, naturalmente, sentido común.

phtsilbjgbilcvpbegybvvpbgqycvysesptbislhtsybosjci vlthacxsvcs
 xsvcihbvltcehipcxstsbbycnhbspsxslsipcvbxbtesibilbebilbsysvjce
 xybmsvybabvhigfbtvsvybvjpspsxsvcnhbxbivspcabvlhpgspcxstsublcp
 cxhpgbtsjcbzgvlgtbixsoavhxtbesstecigsjhsipcvbpgcgigjgcsyqtsi
 mhqbchigfbtvsvysesptbislhtsybosvcycpgvxcigspbhivjhsilcvslce
 cvpbkgptcqbicxbtcvhgi jtbgywbgcsqgisjgciavhxcpbjtbslgfcjcebi
 ostciscwtstegysqtcvbmhilstciycvslcecvpbkgptcqbicxstsksjbtbv
 ltbyysvuhbpswsiwtgyycajcyctsyhigfbtvcbivhgiltgctvbnhbtciinct
 esipcsllcecvpbcltceslbtgsybvkybgcjstwcicczgqbicesvlstpbkgbtt
 cvgygjgcsyhegigcalpcycpbesvyhbqcsyqhisvpbbvlsvbvlbtbyysvbzxy
 clstciapbvxpGBTcisYbvxsjgcegybvpbegyycibvpblcibyspsvpbeslbt
 gsysktsjciesvbybebilcvysesptbislhtsybosbi jciltcbyqtsimhbqce
 hjkcesvpgfbtlgpcpbjggpcmhilstpgegihlsvjsilgpspbvpbeslbtgsyjs
 ipbilbaxcibtysvbictwglspbbvsvbvlbtbyysvuhbaskswgskbjkcjcebios
 tcisbzgvlgtycvxysiblsvuhbehapbsxcuhglcvbnhbtci bintgsipc

2. Deducir longitud de clave y clave del siguiente texto, cifrado con Vigenère. Usar Kasiski y/o Índice de Coincidencia, luego análisis de la frecuencia.

bzfdtvdurmmcvltpxfsqrcmvmxreaffectpvmmdvdrmxreqcbsibztjgubpu
 fgeiqinajpofmaibysbdzoarddvdqeumupcljlrqai fxtpxfspvmrnsqebpv
 mpvtuvsffeqqppfbxifpveaimmgvqiumufqeudremlcutbprfzjvxreaepdk
 fevfztpzksmsbrlfdkfyvofvtqcmubpvcuupmlorvsaqbfrrgvrgvfzvtqd
 pyvofffekbnrtgwsuvopf

Tabla 1: Frecuencias características del idioma español

L	%	L	%	L	%	L	%	L	%	L	%	L	%	L	%
A	12.53	B	1.42	C	4.68	D	5.86	E	13.68	F	0.69	G	1.01	H	0.7
I	6.25	J	0.44	K	0.00	L	4.97	M	3.15	N	6.71	O	8.68	P	2.51
Q	0.88	R	6.87	S	7.98	T	4.63	U	3.93	V	0.90	W	0.02	X	0.22
Y	0.90	Z	0.52	Ñ	0.03										

Índice de coincidencia para el idioma Español: 1.94