

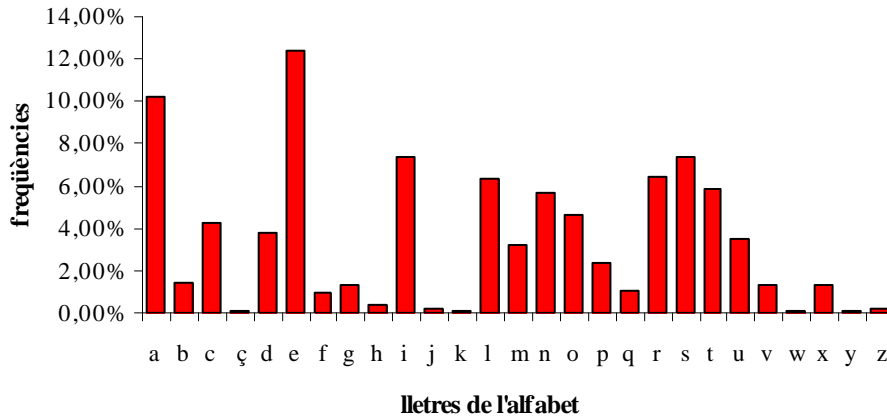


# Si ho amague, ho trobes? Aritmètica del rellotge

M<sup>a</sup> Joaquina Berral Yerón, Inmaculada Serrano Gómez



- Cal establir la freqüència de cada lletra de l'alfabet. La figura mostra els valors, en tant per cent, estudiats en arxius de 50.000 caràcters en català.



- Després s'examina el text xifrat i es determina la freqüència de cada lletra. Completa la taula següent

Caràcter	↙	⇒	⇒	▽	↙	◀	△	↘	←	⇒	▶	↔
Freqüència												

- Es lògic suposar que la lletra que més es repeteix en el text xifrat procedeix de la més repetida en el nostre alfabet.

També cal tenir en compte el sentit comú per poder donar sentit al missatge.

Has desxifrat ja el missatge? Doncs et proposem d'altre:



De ben segur que ara t'ha costat més. Hi ha una raó: és molt probable que els textos llargs vagen amb les freqüències habituals però els curts es desvien de les freqüències normals. Però cal anar amb compte ja que açò no és sempre així. Per exemple, l'autor francès George Perec es va dedicar a experimentar amb el llenguatge i té alguns palíndroms (frases que es llegeixen igual d'esquerra a dreta que de dreta a esquerra) increïbles:

A casa, cal refer la casaca.

# Si ho amague, ho trobes? Aritmètica del rellotge

M<sup>a</sup> Joaquina Berral Yerón, Inmaculada Serrano Gómez



El bé fa mal a la mà feble

Tramaran anar a Mart.

Aquest autor també va escriure *El secuestro* en 1969, i en tot el llibre no apareix ni una sola vegada la lletra “e” (té més de 200 pàgines). El novel·lista anglès Gilbert Adair va aconseguir traduir l’obra al seu idioma i també aconseguix que no aparega la lletra *e*. Els traductors al castellà, aconseguixen que al llibre no existesca la lletra *a*. Al català no està traduïda. Menuda forma de fer malbé l’anàlisi de freqüències!

En els dos exemples anteriors has comprovat que els xifrats per desplaçament són molt fàcils de trencar (hi ha prou amb fer servir un anàlisi de freqüències o un atac per força bruta). Per aquesta raó s’han sofisticat les tècniques de xifrat. Si t’ha agradat el tema pots investigar un poc en l’apartat Per a saber més