DÉCHIFFRAGE FRÉQUENTIEL

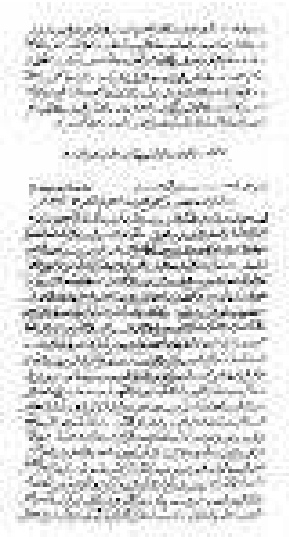
Niveau : seconde, en devoir en temps libre (DM).

Lien avec le programme : statistiques, fréquences.

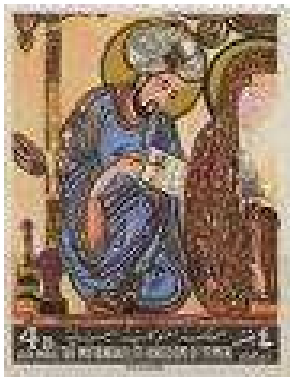
Lien avec *Les maths au quotidien* : **Cryptographie / Chiffre de César**.

La cryptanalyse est une méthode permettant de décrypter certains messages codés, en utilisant les statistiques. Dans ces messages, dits monoalaphabétiques, les lettres du texte à coder sont remplacées par d'autres lettres de la façon suivante :

- Deux lettres différentes sont codées de façons différentes.
- La même lettre est toujours codée de la même façon.



Le premier traité exposant une procédure pour décrypter un texte codé de cette façon a été écrit par le savant arabe Al-Kindi, au IX^{e} siècle après J.-C. Sa théorie repose sur le fait que dans un texte, les lettres ont des fréquences différentes. Par exemple, en français, la fréquence de la lettre E est, selon le texte, presque toujours supérieure aux fréquences des autres lettres. Selon sa théorie, il y a donc de fortes chances pour que, dans un texte codé, la lettre qui apparaît le plus fréquemment représente un E. Les lettres les moins fréquentes représentent probablement un W, un K ou un X...



Le tableau ci-dessous exprime, en pourcentages, les fréquences moyennes, arrondies au dixième, des lettres utilisées dans les textes écrits en français.

A	B	C	D	E	F	G	H	I	J	K	L	M
7,8%	1,1%	3,5%	3,9%	15%	1,2%	0,9%	0,7%	7,7%	0,5%	0,1%	5,7%	3,2%
N	O	P	Q	R	S	T	U	V	W	X	Y	Z
7,2%	5,6%	3%	1,5%	6,8%	8.1%	7,4%	6,5%	1,7%	0,1%	0,4%	0,3%	0,1%

En utilisant le tableau précédent, décoder le message suivant écrit en français :

OASDEDHCHDIRF, YIGF YARAQ TA TAEJDOOKAK EA NAFFCMA EITA AR GHDSDFCRH SAF FHCHDFHDBGAF YIHKA WKIOAFFAGK TA NCHJANCHDBGAF AFH ODAK TA YIGF. AR WCFFCRH, WIGYAQ-YIGF EDHAK GR MKCRT NCHJARCHDEDAR CKCZA TA S'AWIBGA T'CS-VDRTD, C S'IKDMDRA TAF NIHF CSMIKDHJNA AH CSMAZKA ?