

Le but de cette activité est de décoder le message crypté par un *chiffre décalé de César*. C'est un chiffre de substitution mono alphabétique, c'est-à-dire que chaque lettre de l'alphabet est remplacée par une autre.

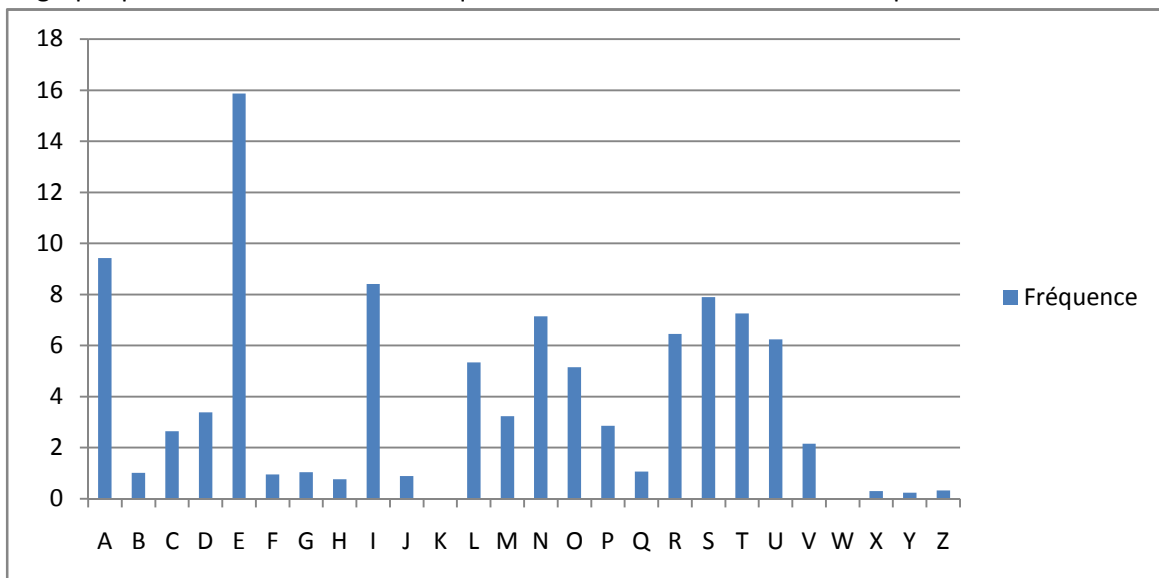
Les cryptanalystes utilisent pour casser ces types de chiffres l'analyse de fréquence : ils calculent les pourcentages de présence de chacune des lettres de l'alphabet dans le texte crypté, et les comparent aux pourcentages que l'on obtient avec un texte écrit 'en clair' afin d'essayer de retrouver les correspondances.

1. À partir du texte chiffré, établir le tableau des fréquences pour chacune des lettres de l'alphabet.

lettre	A	B	C	D	E	F	G	H	I	J	K	L	M	N
nombre d'occurrence														
fréquence (à 1 % près)														

lettre	O	P	Q	R	S	T	U	V	W	X	Y	Z	total
nombre d'occurrence													
fréquence (à 1% près)													100 %

2. Tracer le graphique en barres des fréquences des lettres du texte chiffré.
(prendre modèle sur le graphique ci-dessous)
3. Le graphique ci-dessous donne les fréquences 'normales' des lettres de l'alphabet dans un texte en français.



On peut supposer que les trois lettres qui apparaissent le plus dans le texte crypté correspondent aux mêmes trois lettres apparaissant le plus en temps normal.

Décrypter alors le texte, en s'aidant des fréquences, mais aussi de logique et d'astuce (penser aux terminaisons, conjugaisons, à des mots possibles, des associations de lettres ...)

Message chiffré :

BGIMCFEDALRQGPCAPEECABBGQMNOCQLHQJJBQNC
IGKQGFHQNABCVCAPJMGNEGEAXRQAPCFNOAGFKQA
BFGNGPMHQVCPGFLHMGKQGFKQCPMAGDGDCANHFFH
NCAPBGJBCANCFPGMLGPCAPQFEGLGNGNJMAPNEMH
APNKQACJJMGFFGFPEAUUALABGDGFPKQAFGEGVAF
GFPMAGFNGQBGDGFPKQCFEABNCVCAPQFGLRHNGAB
BCNCVCAPCUHFEGPJHQMPHQTHQMNUHMPLHDDGPCA
BBGCLHQJNEGRCLRGABMGIFCAPGFDCAPMGJGFECF
PBGNMGLMGCPAHFNBGIMCFEDALRQNGJBCANCAPCQ
LHBBGIGLGKQAFGPCAPJCNBGDHAFAEMGEGFHNGPHF
FGDGFPNABFYGJMHQVCAPKQQFNQJJBALGEHFPABF
HNCAPJCMBGMBUCADBIMCFEDALRQCVCAPPHQTH
QMNUCAD

Message chiffré :

BG IMCFE DALRQ GPCAP , E' CABBGQMN , OGCQLHQJ
JBQN CIG KQG FHQN . AB CVCAP JMGN EG EAX-
RQAP CFN , OAGF KQ'AB FG NG PMHQVCP GFLHMG
KQ'GF KQCPMAGDG . DCAN HF F'HNCAP BG
JBCANCFPGM . L'GPCAP QF EG LGN GNJMAPN
EMHAPN , KQA CJJMGFFGFP EAUUALABGDGFP , KQA
FG EGVAFGFP MAGF ; NGQBGDGF , KQCFE AB
NCVCAP QFG LRHNG , AB BC NCVCAP C UHFE GP
JHQM PHQTHQMN . UHMP , LHDDG PCABBG C LHQJN
EG RCLRG , AB MGIFCAP GF DCAPMG JGFECFP BGN
MGLMGCPAHFN . BG IMCFE DALRQ NG JBCANCAP CQ
LHBBGIG , LG KQA F'GPCAP JCN BG DHAFEMG EG
FHN GPHFFGDGFN . AB F'Y GJMHQVCAP KQ'QF
NQJJBALG EHFP AB F'HNCAP JCMBGM : BC UCAD .
BG IMCFE DALRQ CVCAP PHQTHQMN UCAD .