Les éditions
Le Perif'
Maths en Scène

Correction : cryptologie 1

Livre *Les petits Champollions de Paris*

1. Naissance : Rome, 100 av. J.-C. ; mort : Rome, 44 av. J.-C. (assassiné).

2. « On a beau tout rêver, tu dépasses le rêve » : Victor Hugo, « L'Amour », *La Légende des siècles*, 1883. Texte chiffré :

« AZ M NQMG FAGF DQHQD, FG PQBMEEQE XQ DQHQ. »

3. La lettre la plus fréquente est W (soit 22), qui correspond sans doute à E (soit 4), donc le décalage est probablement 18.

4. Avec un décalage de 18, on obtient :

« Et ma vie pour tes yeux lentement s'empoisonne »

(Guillaume Apollinaire, *Les Colchiques*, 1901).

5. « Vos yeux beaux d'amour me font, belle Marquise, mourir » : Molière, *Le Bourgeois gentilhomme*, 1670. Texte chiffré :

« PZD GAYX CAOYX S'OQZYK QA LZIF, CAEEA QOKNYUDA, QZYKUK. »

6. Al-Kindi (801-873), mathématicien et philosophe, a vécu en Perse (qui correspond à peu près aux actuels Irak et Iran,). Il a décrit la méthode dite *d'analyse de fréquence*, qui permet de déchiffrer le code de substitution mono-alphabétique.

7. Les lettres les plus fréquentes en français sont, dans l'ordre : E, A, S, I, N, T, R, L… Dans le message, le S est le plus fréquent (13 occurrences), suivi de J (8 occurrences), K, R, U, Y (7 occurrences chacun), puis E et W (5 occurrences), etc.

Le S représente donc certainement un E. Le J apparaît souvent à la fin des mots, c'est probablement un S. Le R apparaît deux fois doublé et est une lettre fréquente : c'est donc vraisemblablement un L, un N, un R, voire un T. Essayons L, doublon le plus fréquent en français après EE et SS.
Le X apparaît deux fois avant une apostrophe, ce peut être un L ou un D, ou, moins fréquent, un N ou un M. Ce ne peut être N car le mot XSJ est traduit par « *es ». Puisque L est déjà pris, on penche pour un D, plus fréquent avant une apostrophe que M.
On a donc pour l'instant, où les lettres décodées sont marquées en minuscules :

UYTN NeK d'KG ZEYBWBeGU NTKY des BEllETGs d'WsUYes,
El leKY ZWllWEU Ues MeKO eU leKYs seAYeUs CeBeWKO

Le premier mot de la seconde ligne est sûrement « il », donc E désigne I. Le U se retrouve dans les mots « Ues » et « eU », c'est probablement T. Il reste K et Y comme lettres fréquentes ; le K se retrouve dans « d'KG », c'est probablement U dans le mot « d'un » ; et ainsi G code N. Le Y se trouve devant un e dans « WsUYes », ce n'est donc pas A : ce peut être R (lettre fréquente). Enfin, le W (autre lettre fréquente) peut être A qui n'est pas encore utilisé. On a pour l'instant :

trTN Neu d'un ZirBaBent NTur des BilliTns d'astres,
il leur Zallait tes MeuO et leurs seArets CeBeauO

On devine alors que Z vaut F (dans « fallait »), que B et T valent M et O (dans « millions »), que N vaut P, que A vaut C, M et O valent Y et X (dans « yeux »), et enfin que C vaut G. D'où le texte clair :

« Trop peu d'un firmament pour des millions d'astres,
Il leur fallait tes yeux et leurs secrets gémeaux »

(Louis Aragon, *Les Yeux d'Elsa*, 1942).

8. « Le monde a soif d'amour : tu viendras l'apaiser » : Arthur Rimbaud, *Soleil et Chair*, 1870. Texte chiffré :

« HM KQNJM A CQYP J'AKQIZ : FI LYMNJZAC H'ATAYCMZ. »

9. Modulo 26, l'inverse de 3 est 9 : il suffit donc de multiplier le numéro de chaque lettre par 9 pour retrouver le texte clair.

« Aimer à loisir, / Aimer et mourir / Au pays qui te ressemble ! »

(Charles Baudelaire, « L'Invitation au voyage », *Les Fleurs du mal*, 1857).

10. La cryptologie est la science des codes secrets, dans son ensemble. Elle se divise en deux sous-domaines : la cryptographie d'une part, dont la tâche est de concevoir les méthodes de chiffrement, et la cryptanalyse d'autre part, dont l'objectif est de déchiffrer les codes conçus par les cryptographes.