Les éditions
Le Perif'
Maths en Scène

La fiche : cryptologie 1

Livre *Les petits Champollions de Paris*

Alphonse veut envoyer un message à son amie Bertha. Pour le chiffrer, il souhaite décaler chaque lettre du message d'un même nombre de rangs : par exemple, dans le cas d'un décalage de trois rangs, A devient D, B devient E, etc., puis W devient Z, X devient A, et Y devient B. Ce code s'appelle « code de César » car Jules César, dit-on, en aurait fait usage.

1. Quand Jules César a-t-il vécu ? . . . . . .

2. Pour son premier essai, Alphonse utilise un décalage égal à 12. Qu'obtient-il après codage du message : « On a beau tout rêver, tu dépasses le rêve » ?

. . . . . .

. . . . . .

3. Alphonse est mécontent de son essai. Pour sa lettre définitive, il change de texte et de décalage. Bertha reçoit le message codé :

« WL ES NAW HGMJ LWK QWMP DWFLWEWFL K'WEHGAKGFFW ».

Elle ne connaît pas le décalage utilisé par Alphonse. Grâce à l'analyse de fréquence, aide Bertha à retrouver le décalage utilisé par Alphonse.

. . . . . .

4. Aide-la à déchiffrer le message.

. . . . . .

. . . . . .

C'est maintenant Conan qui écrit à Dora. Mais il est plus prudent et utilise une *substitution monoalphabétique*[1], où l'alphabet est permuté complètement : on substitue donc à chaque caractère du texte clair la lettre correspondante dans l'alphabet permuté. Par exemple, si l'alphabet permuté est :

OCHSALWMUTREQIZBNKDFYPVXGJ,

alors A sera remplacé par O, B par C, C par H, etc., et enfin Z par J.

5. Chiffre de cette façon le premier essai de Conan : « Vos yeux beaux d'amour me font, belle Marquise, mourir. »

. . . . . .

. . . . . .

6. Qui est Al-Kindi ? Qu'a-t-il apporté à la substitution monoalphabétique ? Où a-t-il vécu : comment s'appelait son pays à l'époque, et maintenant ?

. . . . . .

. . . . . .

7. Pour sa lettre définitive, Conan change de texte et d'alphabet chiffré. Euphroisie intercepte la lettre destinée à Dora. Jalouse, elle veut la déchiffrer, mais elle ne connaît pas l'alphabet permuté. Le message est le suivant :

« UYTN NSK X'KG ZEYBWBSGU NTKY XSJ BERRETGJ X'WJUYSJ,
ER RSKY ZWRRWEU USJ MSKO SU RSKYJ JSAYSUJ CSBSWKO »

Aide-la à le déchiffrer grâce à l'analyse de fréquence.

. . . . . .

. . . . . .

. . . . . .

8. Fridolin écrit à sa dulcinée, Gertrude, et code son message en multipliant par 3 le numéro de chaque lettre (modulo 26). Il s'entraîne sur le texte suivant :

« Le monde a soif d'amour : tu viendras l'apaiser. »

Dis-lui quel est le résultat du codage.

. . . . . .

. . . . . .

1. Dans le livre, cette méthode est seulement mentionnée dans l'historique.

9. Après cet essai, Fridolin change de texte, mais pas de méthode. Henriette intercepte la lettre de Fridolin. Elle lit :

« AYKMZ A HQYCYZ, AYKMZ MF KQIZYZ AI TAUC WIY FM ZMCCMKDHM ! »

mais n'y comprend rien. Furieuse, elle veut la décoder. Aide-la.

. . . . . .

. . . . . .

10. Quelles sont les différences entre *cryptologie*, *cryptographie* et *cryptanalyse* ?

. . . . . .

. . . . . .

11. Retrouve d'où sont issues toutes les citations utilisées.