Le principe du décryptement

Par Daniel TANT

Depuis que l'écriture existe, les rois, les princes et les riches ont utilisé la cryptographie pour transmettre des messages incompréhensibles à celui qui n'en détient pas la clé.

Depuis que la cryptographie existe, les mêmes rois, princes ou riches ont financé des « cabinets noirs » pour essayer de savoir ce que contenaient les messages saisis sur les coursiers ennemis.

Face à un amalgame incompréhensible, certains cryptoanalystes de ces cabinets noirs ont remarqué la fréquence des lettres d'une langue.

Dans le cas du français, dans l'ordre décroissant, les lettres le plus fréquemment utilisées sont :
ESARINTULO.

Ce n'est pas une science exacte, car il faut agir avec tâtonnements.

De plus, dans ce genre de messages, les espaces entre les mots n'existent pas.

Un cabinet noir reçoit à décrypter le message : XUUBRLRMANFLRJSRWXFBU.

Comptons d'abord les lettres : nous avons 2X, 3U, 2B, 4R, 2L, 1M, 1A, 1N, 2F, 1J, 1S, 1W.

Remplaçons les lettres les plus nombreuses du message chiffré (R) par le E qui est la lettre la plus fréquente de la langue française. Nous avons désormais (les lettres remplaçantes sont écrites gras et en majuscule) :
x u u b **E** l **E** m n a f l **E** j s **E** w x f b u.

Prenons ensuite la deuxième lettre la plus fréquente du message chiffré (U) que nous remplaçons par la 2° lettre de la fréquence littérale (S) nous obtenons :
x **S S** b **E** l **E** m n a f l **E** j s **E** w x f b **S**

Puis, dans l'ordre des fréquences du message crypté, nous avons le choix entre X, B, L ou F. Il faut essayer les 4 en les remplaçant par la lettre A.

X : **A S S** b **E** l **E** m n a f l **E** j s **E** w **A** f b **S**

B : **B S S** b **E** l **E** m n a f l **E** j s **E** w **B** f b **S**

L : **L S S** b **E** l **E** m n a f l **E** j s **E** w **L** f b **S**

F : **F S S** b **E** l **E** m n a f l **E** j s **E** w **F** f b **S**

De ces 4 solutions, la 1ère est la plus probable car de nombreux mots commencent pas ASS comme assigner, assister, assommer, assassiner, etc…

Vient donc le tour des lettres BLF du message chiffré pour être remplacées par la lettre R :

B : **A S S R E** l **E** m n a f l **E** j s **E** w **A** f **R** S

L : **A S S** b **R E** m n a f **R E** j s **E** w **A** f b **S**

F : **A S S** b **E** l **E** m n a **R** l **E** j s **E** w **A R** b **S**

Aucune de ces solutions n'est satisfaisante. Toujours par tâtonnements essayons si ces 3 lettres correspondent à la lettre suivante de la fréquence littérale : le I.

B : **A S S I E** l **E** m n a f l **E** j s **E** w **A f I S**

L : **A S S** b **E I E** m n a f **I E** j s **E** w **A** f b **S**

F : **A S S** b **E** l **E** m n a **I** l **E** j s **E** w **A I** b **S**

La première solution (celle du B) est la plus probable. Si nous revenons ensuite sur le R comme lettre possible dans l'ordre, pour remplacer le L et le F, nous obtenons :

L : **A S S I E R E** m n a f **R E** j s **E** w **A** f **I S**

F : **A S S I E** l **E** m n a **R** l **E** j s **E** w **A R I S**

Le remplacement par le F semble la meilleure solution.

Et ainsi de suite…

En quelques heures et par tâtonnements sort le message :

« assiegez d'urgence Paris ».

Le général L. Sacco, ancien chef du bureau du Chiffre de l'armée italienne a écrit l'ouvrage : « Manuel de cryptographie » paru aux éditions Payot en 1951. Dans les tables en fin d'ouvrage, pages 378 et suivantes, il donne les fréquences des lettres par langue française, italienne, espagnole, allemande, anglaise, serbo-croate et russe.