Exercices et problèmes de cryptographie

Damien Vergnaud

Exercice complémentaire n° 1.1 (bis)

Exercice 1.1 (bis) CHIFFREMENT DE CÉSAR

Décrypter le texte suivant qui a été obtenu en appliquant le chiffrement de César sur un texte en langue française dans lequel les espaces ont été supprimées :

```
lgmlwdsysmdwwklvanakwwwfljgakhsjlawkvgfldmfwwklzstalww
hsjdwktwdywkdsmljwhsjdwksimalsafkdsljgakawewhsjuwmpima
  vsfkdwmjdsfymwkwfgeewfluwdlwkwlvsfkdsfgljwysmdgak
```

Solution : Le chiffrement de César est un mode de chiffrement par substitution, il ne modifie donc pas la fréquence d'apparition des lettres. La lettre la plus fréquente dans un texte français étant le « e », le décalage entre la lettre la plus fréquente dans ce texte chiffré et la lettre « e » doit donc nous révéler la clé utilisée pour le chiffrement. La lettre qui apparaît le plus souvent dans le texte chiffré est le « w » avec 27 occurrences (puis vient la lettre « s » avec seulement 16 occurrences). Le décalage utilisé est donc vraisemblablement de 18 lettres vers la gauche et l'on obtient le message clair suivant :

```
toutelagauleestdiviseeentroispartiesdontluneesthabitee
parlesbelgeslautreparlesaquitainslatroisiemeparceuxqui
   dansleurlanguesenommentceltesetdanslanotregaulois
```

En ajoutant les espaces et la ponctuation, nous retrouvons la première phrase du Livre I de *Guerre des Gaules (Bellum Gallicum)* écrit par J. César vers 52-51 av. J.-C. (dans la traduction de de la Collection Nisard) :

Toute la Gaule est divisée en trois parties, dont l'une est habitée par les Belges, l'autre par les Aquitains, la troisième par ceux qui, dans leur langue, se nomment Celtes, et dans la nôtre, Gaulois. □