Exercices et problèmes de cryptographie

Damien Vergnaud

Exercice complémentaire n° 1.2 (bis)

Exercice 1.2 (bis) CHIFFREMENT AFFINE

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

```
efklzxxdhmfycvfsfmffcslypffcifyfcslycahyfkfttfzyvd
yyhffcnhfelztffcnhztlztffcnhzyfxcvulnhfkdzxyzcdhcl
 klzcoltftfyzcdhclklzchyflhcsffctlztffctfvdtisfya
```

Solution : Le chiffrement affine ne modifie pas la fréquence d'apparition des lettres. La lettre la plus fréquente dans un texte français est le « e » et les lettres suivantes sont par ordre de fréquence le « a », le « i », le « n », le « s » et le « t » (avec des fréquences très variables d'un texte à l'autre). La lettre qui apparaît le plus souvent dans le texte chiffré est le « f » avec 31 occurrences puis vient la lettre « c » avec 18 occurrences.

En supposons que la lettre « f » correspond à la lettre « e » et que la lettre « c » correspond à l'une des lettres « a », « i », « n », « s » ou « t », nous devons résoudre pour chaque choix un système linéaire à deux équations et deux inconnues dans $(\mathbb{Z}/26\mathbb{Z})$ de la forme

$$\begin{cases} a \cdot 5 + b &= 4 \\ a \cdot 2 + b &= \ell \end{cases}$$

où ℓ est l'entier 0, 8, 13, 18 ou 19 selon que la lettre testée pour « c » est « a », « i », « n », « s » ou « t » (respectivement). Le couple (a, b) obtenu est testé en déchiffrant les premiers caractères du chiffré et nous obtenons les résultats suivants :

Lettre testée	« a »	« i »	« n »	« s »	« t »
ℓ	0	8	13	18	19
(a, b)	$(10, 6)$	$(16, 2)$	$(23, 19)$	$(4, 10)$	$(21, 3)$
Début du « clair » associé	`uecmwc`	`oegwmg`	`hepmwc`	`aeycgy`	`jefais`

La clé à utiliser pour le déchiffrement est donc vraisemblablement le couple $(21, 3)$ et nous obtenons le message clair suivant :

```
jefaissouventcereveetrangeetpenetrantdunefemmeinco
nnueetquejaimeetquimaimeetquinestchaquefoisnitouta
 faitlamemenitoutafaituneautreetmaimeetmecomprend
```

Il s'agit bien sûr du premier quatrain du sonnet *Mon rêve familier* écrit par P. Verlaine en 1866.

□