Exercices et problèmes de cryptographie

Damien Vergnaud

Exercice complémentaire n° 1.5 (bis)

Exercice 1.5 (bis) CHIFFREMENT DE VIGENÈRE - INDICE DE COÏNCIDENCE

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

```
uzssgbufmdymbfykciyfrockmbnsxovanzcgfvyigslgkofwpsmjqqbwdqbwedimdaiftwmlawlw
psfggwmpujdwfcgtmwjsdvukmfxkgffweayeawlweryepollmuhszwghdwgweqieysfsbzoksfuf
psjsdhcwpsmggjlsssmvqqylfsyhaeowaifweoolqilkfshsushlmrcjqzunqfclqgufeofdqfzs
ufymzhimddfmecoeawhkxchymzutmgnaxzysmamlqfxsyqbwldcwdfyjaiawxsnaffyeqgyvgwma
fxydqgyebcllmwwzqngguopwozuhqfgaegcgzryexswgzgyjhonwgfvaqbyffshvgxydqgxwhclsu
```

Utiliser l'indice de coïncidence pour déterminer la longueur de la clé utilisée et décrypter ce texte.

Solution : Dans une première étape de cryptanalyse, nous calculons l'indice de coïncidence moyen obtenu à partir des sous-chiffrés en fonction de la longueur de la clé.

Longueur	1	2	3	4	5	6	7	8
Indice	0.04687	0.05881	0.04733	0.07155	0.04734	0.0587	0.04708	0.07224

Nous en déduisons que la clé est probablement de longueur 4 ce qui donne les trois sous-chiffrés c_0, c_1, c_2 et c_3 formés des 96 caractères de rang congru à 0 modulo 4 et des 95 caractères de rang congru à 1, 2 et 3 modulo 4 (respectivement) :

c_0 = `ugmbcrmxnfgkpqdedtapgufmdmgeaepmzdeybspdpgsqfaaeqfumqqqequzdeaxmmxmqyldaxfqgfqbmquoqezxzhgqfgqhu`
c_1 = `zbdfiobozvsosqqdawwswjcwvffawrouwwqszfshsjsqseioissrzfgoffhdcwczgzafqdfisfgwxgcwnozfgrsgofbsxgc`
c_2 = `suyyycnvcylfmbbiimlfmdgjuxfylylhggifoujcmlmyyofolhhcucufzyifohhunymxbcyanyymyylwgpugcywynvyhyxl`
c_3 = `sfmkfksagigwjwwmflwgpwtskkwewelshweskfswgsvlhwwlksljnlfdsmmmekytaslswwjwaevadelzgwhagegjwafvdws`

La lettre la plus fréquente dans le chiffré c_0 (*resp.* c_1, *resp.* c_2, *resp.* c_3) est le `q` (*resp.* le `s`, *resp.* le `y`, *resp.* le `w`). En supposant que ces lettres représentent la lettre « e » dans le texte clair, nous en déduisons que la clé utilisée pour le premier chiffré (*resp.* le second chiffré, *resp.* le troisième chiffré, *resp.* le quatrième chiffré) est probablement le `m` (*resp.* le `o`, *resp.* le `o`, *resp.* le `s`). Nous obtenons ainsi le texte clair

```
ilyaunanapeupresquenfaisantalabibliothequeroyaledesrecherchespourmonhistoire
delouisxivjetombaiparhasardsurlesmemoiresdemdartagnanimprimescommelaplusgran
departiedesouvragesdecetteepoqueoulesauteurstenaientadirelaveritesansallerfa
ireuntourplusoumoinslongalabastilleaamsterdamchezpierrerougeletitremeseduisi
tjelesemportaichezmoiaveclapermissiondemleconservateurbienentendujelesdevorai
```

En ajoutant les espaces et la ponctuation, nous retrouvons le paragraphe

> Il y a un an à peu près, qu'en faisant à la Bibliothèque royale des recherches pour mon histoire de Louis XIV, je tombai par hasard sur les Mémoires de M. d'Artagnan, imprimés – comme la plus grande partie des ouvrages de cette époque, où les auteurs tenaient à dire la vérité sans aller faire un tour plus ou moins long à la Bastille – à Amsterdam, chez Pierre Rouge. Le titre me séduisit : je les emportai chez moi, avec la permission de M. le conservateur ; bien entendu, je les dévorai.

qui introduit le roman *Les Trois Mousquetaires* écrit par A. Dumas en 1844. □