*GLO - 3100 : Cryptographie et Sécurité informatique*

*Session A-2020*

TP1

**Par :**

Guillaume Doucet 111 123 716

Date de remise : 14 octobre 2020



**Faculté des sciences et de génie**

**Exercice 1 :**

Texte encrypté :

JEXCGQDUILIXXDIMXVNGXIBVPGLSMIUVVLZHPCQINXTOGFPWXMIFTXDVRWMCEKMIIAWZGBDWIYIJMSRVWMJJRFRPZVIZRAJVSZRUMCXEJIMQPKMIIGPCPYYTARMHOIMKMHOSJEMHOIACMADFAVXYSXRRPFZHRZTBZVIVBNYIRICJOMDEMMOLTIIPZVHVMHJXWVVQJVSJQIQMCXJLJQIYIOIMCKIFGMVZFFZGXGLYMXTOXVVGZKSJGEXEXYSXPTMJCIGZWUKEXISZVPVFVCOLBJXBVXRIIUOIIYIYIGGPTNDSCRRXOLTIIPZVHZRAYIRICJOMDEXBZHTKECGISFTYMEIZSHJJPTMJCIGZWWJRIISFGISSSNCFNKLYVPVFVCOLBRRXDRTRGBDRHKEHXIQPEEZCIYMMDWPJIWMIIZHYVPAPOHJACFRFTXDKLYXSBDYHDGPEXMPWJRPFTEHYSLOWIIMHBSUTLUMERKILNAWZGBDWCVIXZHIFHYXVNGXNCIRZTBZVIVBNVGGPTNJWNJXYHMHKLYJVSVVYYPXJXIAIAVQYIXHFJZDRXKIJJWHZFFZTARMHOIMKWZDRXKIJJWHZFFZGNGLYMXTOXMAMCZXYKSHJMVGIZVCMVRSKLYZRRICJOMDEEHYHTTVSKXXFRUGKDIMNCQHNLCXLRFVLZWEFRXOSTRGBFINBISNEGVMGKSGKEHOEHTMJCIGJACOLDLXPVVXRFFZOTPWWVRQVXLDZXRPFTFGFOYIAXKLIIPNKLYFRDNPYYKTFJNCIRZTBZVJJIXVRSRVYOLTIIZJVTLWYGIHJSLZZTEGIPRIVVJMSSLGNDZTWSLHSHKTOMTDJIMCMHKSLDGPCPSXMEYILNATIIIAXTEYMZHSZVYXXAPJIMICTVSKXXFRIMHTTVSKXXFRQDXWFYNVHSZXCJRPCTLJGTUYLZWHLGBVWPLXBZRIZGUOMDESLDRIVKLDXNTLYXOH

1. Test de Freidman

* Prend le result du test de Freidman 1, estime la key
* Part de cette valeur jusqu’au man de 9 pour chaque valeur fait le test de Freidman pour loccurence des sous chaine de longueur n jusqua temps que tu soit proche de 0.065. quand tu l’as, ta lalongueur de la clef
* kasiski

Il faut utiliser le test de Freidman pour estimer la longueur de la clef d’un texte encrypté avec le chiffrement de Vigenère. Pour ce faire, il faut calculer l’indice de coïncidence. Cet indice est donné par :

|  |  |  |
| --- | --- | --- |
|  |  | (1) |

Ainsi, il faut d’abord prendre le texte chiffré et calculer la fréquence d’occurrence de chaque lettre dans celui-ci () ainsi que la même valeur décrémentée de 1 (). Les résultats sont présentés au Tableau 1.

Tableau 1 : Analyse de Freidman.

|  |  |  |  |
| --- | --- | --- | --- |
|  | ni | ni-1 | ni(ni-1) |
| A | 19 | 18 | 342 |
| B | 19 | 18 | 342 |
| C | 34 | 33 | 1122 |
| D | 29 | 28 | 812 |
| E | 27 | 26 | 702 |
| F | 36 | 35 | 1260 |
| G | 40 | 39 | 1560 |
| H | 40 | 39 | 1560 |
| I | 89 | 88 | 7832 |
| J | 47 | 46 | 2162 |
| K | 29 | 28 | 812 |
| L | 39 | 38 | 1482 |
| M | 54 | 53 | 2862 |
| N | 24 | 23 | 552 |
| O | 27 | 26 | 702 |
| P | 35 | 34 | 1190 |
| Q | 12 | 11 | 132 |
| R | 49 | 48 | 2352 |
| S | 39 | 38 | 1482 |
| T | 42 | 41 | 1722 |
| U | 10 | 9 | 90 |
| V | 59 | 58 | 3422 |
| W | 27 | 26 | 702 |
| X | 64 | 63 | 4032 |
| Y | 40 | 39 | 1560 |
| Z | 49 | 48 | 2352 |
| total | 979 |  | 43140 |

En appliquant l’équation (1), on obtient :

|  |  |  |
| --- | --- | --- |
|  |  |  |

Ce qui donne un indice de coïncidence de 0.04505662. Sachant que le test claire est en anglais (indice de coïncidence de la langue anglaise = 0.065) et que l’indice du texte chiffré est plus grand que 0.0385, on peut assumer que la substitution poly alphabétique a été utilisé pour le chiffrement.

**Exercice 3 :**

adsdasd