*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

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 commencer par poser une longueur de clé *m* = 1 et calculer l’indice de coïncidence de tout le message chiffré. Il faut ensuite répéter l’opération pour différentes valeurs de *m* en divisant le message chiffré en *m* bloques sachant que le maximum que *m* peut prendre (selon l’énoncé) est 9. La sous-chaîne d’un bloc est donnée par la concaténation des charactères de séparés par un distance *m* dans le texte chiffré. La longueur sera trouvée quand l’indice de coïncidence de chaque bloque sera le plus prêt de celui de la langue d’origine (anglais), soit 0.065. Chaque itération est détaillée ci-dessous.

Tableau 1 : Freidman, m =1.

|  |  |  |  |
| --- | --- | --- | --- |
|  | 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 un indice de coïncidence de 0.04505662. Les tableaux sont omis pour les itérations subséquentes. Voici tous les résultats intermédiaires pour les indices de coïncidence avec différentes longueurs de *m*:

Tableau 2 : Test de Freidman pour toutes les longueurs de m avec m >= 1 et m <= 9.

|  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| m |  |  |  |  |  |  |  |  |  |
| 1 | 0.0450566 |  |  |  |  |  |  |  |  |
| 2 | 0.0490464 | 0.0463475 |  |  |  |  |  |  |  |
| 3 | 0.0478978 | 0.0581973 | 0.0658801 |  |  |  |  |  |  |
| 4 | 0.0466377 | 0.0462362 | 0.0492807 | 0.0461445 |  |  |  |  |  |
| 5 | 0.0420199 | 0.0474621 | 0.0424908 | 0.0429095 | 0.0458366 |  |  |  |  |
| 6 | 0.0632201 | 0.0682421 | 0.0653639 | 0.064758 | 0.068848 | 0.0649852 |  |  |  |
| 7 | 0.049332 | 0.0414183 | 0.0475848 | 0.0446043 | 0.048407 | 0.0435766 | 0.0426441 |  |  |
| 8 | 0.0463814 | 0.0477142 | 0.0481141 | 0.0432191 | 0.0485029 | 0.0452513 | 0.0483674 | 0.047419 |  |
| 9 | 0.0487598 | 0.0572545 | 0.0749235 | 0.0494393 | 0.0511383 | 0.0591233 | 0.0468909 | 0.0595362 | 0.0595362 |

Selon ces résultats, la longueur *m* qui donne des indices de coïncidence les plus proches de 0.065 est *m=6*. La longueur de la clef est donc estimée à 6.

1. Trouver le message clair

À partir de l’information obtenue que la longueur de la clef est 6, il faut maintenant trouver le texte de la clef. Pour ce faire, il faut d’abord séparer le texte encrypter en 6 bloques : avec . On obtient les chaînes de charactères suivantes :

Y0 :

JDXNPUPTXDEWIRRISXPPAMJAARRIRDTHWSCICVXTZXPGXVBRIGCTHRDTSIPGISNVBTHQIPIACDBPJHIURWCINRIGNHSXAHXHAMXHNTCHZSRDTXDHRETNGGHGDXTQXGXNDTRJSTTHTISTHDHPETTSACXTXWSPTHPIDINH

Y1 :

EUDGGVCOMVKZYVFZZEKCRKECVRZVIEIVVJXYKZGOKETZIFJIYPRIZIEKFZTZISKFRRKPYJZPFKDERYITKZVFGZVPJKVJVFKZRKKZGOZJVKIETFINFFRBVKTJLRPVRFKKNFZJRILJEVLWKJKCYIEZPTFTFFZCULLZEVT

Y2 :

XIIXLVQGIRMGIWRRRJMPMMMMXPTBCMIMVQJIIFLXSXMWSVXIITRIRCXETSMWSSLVRGEEMIHORLYXPSMLIGIHXTBTXLVXQJIFMWIFLXXMCLCEVRMLVRGIMEMAXFWXPOLLPJTIVIWSGVGSTISPIIYVJVRVRYXTYGXGSKL

Y3 :

CLMISLIFFWIBJMPAUIIYHHHAYFBNJMPHQILOFFYVJYJUZCBUYNXPAJBCYHJWFNYCXBHEMWYHFYHMFLHULBXYNBNNYYYIYZJFHZJFYMYVMYJHSUNCLXBSGHJCPFWLFYIYYNBXYZYLIJNLOMLSLIMYISISQNCLLBBULLY

Y4 :

GIXBMZNPTMIDMJZJMMIYOOODSZZYOOZJJQJIGZMVGSCKVOVOIDOZYOZGMJCJGCVODDXZDMVJTXDPTOBMNDZXCZVJHJYAIDJZODJZMAKGVZOYKGCXZOFNKOCOVZVDTIIFYCZVOJGZPMDHMCDXNAZXMKMKDVJJZVZODDX

Y5 :

QXVVIHXWXCAWSJVVCQGTISIFXHVIMLVXVMQMMGXGEXIEPLXIGSLVIMHIEJIRIFPLRRICWIPAXSGWEWSEAWHVIVGWMVPIXRWTIRWGXMSIRRMHXKQLWSIESEILVORZFAPRKIVRLVIZRSZSTMGMAXHXIXHXXHRGWWRMRXO

Ensuite, pour chacun de ces bloques, il faut trouver le décalage en comparant la lettre la plus fréquente de la langue anglaise (e) avec la lettre la plus fréquente de *Yi*. Le décalage nous permet de trouver *Ki*, une des lettres de la clef. Pour les fréquences des lettres dans la langue anglaise, les fréquences suivantes sont utilisées[[1]](#footnote-1) :

Tableau 3 : Fréquence des lettres dans la langue anglaise.

|  |  |
| --- | --- |
| A | 0.082 |
| B | 0.015 |
| C | 0.028 |
| D | 0.043 |
| E | 0.13 |
| F | 0.022 |
| G | 0.02 |
| H | 0.061 |
| I | 0.07 |
| J | 0.0015 |
| K | 0.0077 |
| L | 0.04 |
| M | 0.024 |
| N | 0.067 |
| O | 0.075 |
| P | 0.019 |
| Q | 0.00095 |
| R | 0.06 |
| S | 0.063 |
| T | 0.091 |
| U | 0.028 |
| V | 0.0098 |
| W | 0.024 |
| X | 0.0015 |
| Y | 0.02 |
| Z | 0.00074 |

Donc, dans la langue anglaise, la lettre *e* possède une fréquence d’occurrence de 13%. Les résultats suivants sont obtenus pour l’analyse des blocs *Yi* :

Tableau 4 : Résultat de l’analyse des Yi en comparaison à la fréquence de la lettre « e » dans la langue anglaise.

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
|  | Lettre | Fréquence | Décalage |  | Lettre de |
| 0 | X | 0.1898734 | 15 | 15 | P |
| 1 | K | 0.122699 | 6 | 6 | G |
| 2 | I | 0.128834 | 4 | 4 | E |
| 3 | Y | 0.147239 | 20 | 20 | U |
| 4 | Z | 0.128834 | 21 | 21 | V |
| 5 | I | 0.128834 | 4 | 4 | E |

Ainsi, selon cette analyse, la clef devrait être PGEUVE. Cependant, le programme de décryptage fournit (*Vigenere.jar*) ne donne pas un texte lisible avec cette clef. Il semble logique que le résultat doit être PREUVE pour que la clef soit un mot lisible, donc il faut s’attarder à . La deuxième lettre la plus fréquente dans est Z, ce qui se traduit par un décalage de 21 et devient V pour obtenir la clef PVEUVE. Encore une fois, le message n’est pas décrypté avec cette clef. Pour obtenir la lettre R pour , il faut un décalage de 17, ce qui correspond à la lettre chiffrée V. Cette lettre a une fréquence assez importante dans , soit 0.0981595 (16 occurrences, 3ième plus fréquente lettre). Il faut cependant comprendre pourquoi la lettre R n’a pas été obtenue pour . La raison pour laquelle la lettre chiffrée V n’est pas la plus fréquente dans ce cas est probablement les limites que présentent les analyses de fréquences. En effet, l’échantillon est petit et peut ne pas être représentatif par rapport à la langue anglaise.

En utilisant la clef PREUVE, le message clair suivant est obtenue :

*Until modern times cryptography referred almost exclusively to encryption which is the process of converting ordinary information called plain text into unintelligible text called cipher text decryption is the reverse in other words moving from the unintelligible cipher text back to plain text a cipher is a pair of algorithms that create the encryption and the reversing decryption the detailed operation of a cipher is controlled both by the algorithm and in each instance by a key this is a secret ideally known only to the communicants usually a short string of characters which is needed to decrypt the cipher text a crypto system is the ordered list of elements of finite possible plain texts finite possible cypher texts finite possible keys and the encryption and decryption algorithms which correspond to each key keys are important as ciphers without variable keys can be trivially broken with only the knowledge of the cipher used and are therefore useless or even counter productive for most purposes historically ciphers were often used directly for encryption or decryption without additional procedures such as authentication or integrity checks*

**Exercice 3 :**

adsdasd

1. https://en.wikipedia.org/wiki/Letter\_frequency [↑](#footnote-ref-1)