

Vigenere Soluce

V2.0 Avril 2018

Description

Le cryptage de textes utilisant la substitution poly-alphabétique de Blaise de Vigenère est encore fréquemment utilisé de nos jours, en particulier dans les applications ludiques, par exemple pour le geocaching.

La clef de décodage n'est pas toujours simple à trouver, en particulier quand on est sur le terrain dans une zone où la réception Internet est médiocre, ce qui interdit de se connecter à des sites distants.

Vigenere_Soluce permet, sur un P.C. portable local, de rechercher cette clef.

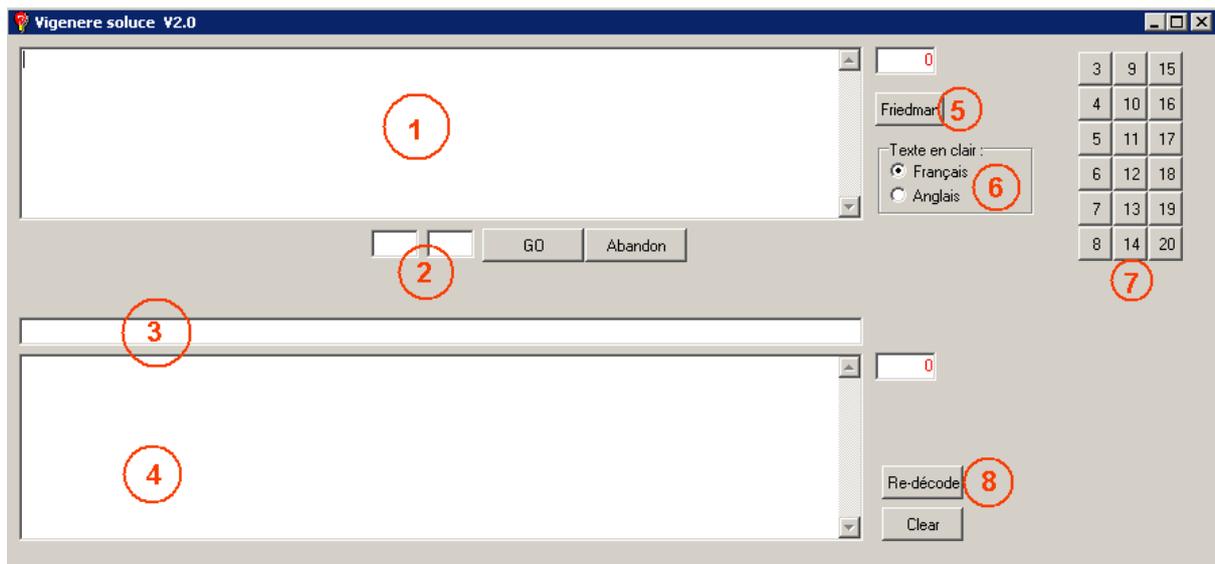
Installation

Vigenere_soluce est une application portable : Décompressez simplement le fichier Vigenere_Soluce.zip dans un répertoire vide..

Utilisation

Double-cliquez sur 'Vigenere_soluce.exe'

Collez (ctrl + V) votre texte crypté dans la zone marquée 1.



- Si vous connaissez la longueur de la clef, appuyez directement sur un des boutons de la zone 7 (Clefs longues de 3 à 20 caractères)

- Si vous ne connaissez pas la longueur de la clef, appuyez sur le bouton marqué 5 : Vous obtiendrez une liste de 28 valeurs, calculées à partir de l'indice de coïncidence de Friedman. Cette liste vous permet dans beaucoup de cas (en particulier sur les textes cryptés longs), de déterminer la ou les longueurs possibles de la clef.

- Si l'utilisation de cet indice de coïncidence de Friedman ne permet pas de se faire une bonne idée de la longueur de la clef, entrez les mini-maxi à tester dans la zone 2 (valeurs de 3 à 30) et appuyez sur 'GO' : Ces différentes longueurs de clefs seront testées successivement.

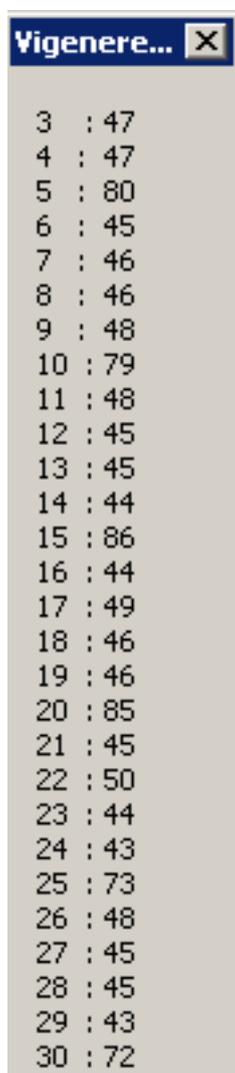
Le résultat du décryptage s'affichera en zone 4, et la clef utilisée en zone 3.

Dans certains cas, Vigenere_soluce n'arrive pas à déterminer un des caractères de la clef : Ce caractère est alors indiqué par un '?' dans la zone 3. Si le texte obtenu dans la zone 4 est partiellement compréhensible, vous pouvez remplacer de '?' par un caractère alphabétique (A à Z) et appuyer sur le bouton 8.

Exemples d'utilisation

Interprétation de l'indice de Friedman :

1 - Ouvrez le fichier 'Texte crypté Exemple 1.txt' et collez son contenu en zone 1.
Appuyez sur le bouton 5. Vous obtenez la liste suivante :



Longueur de la clef	Valeur de l'indice
3	47
4	47
5	80
6	45
7	46
8	46
9	48
10	79
11	48
12	45
13	45
14	44
15	86
16	44
17	49
18	46
19	46
20	85
21	45
22	50
23	44
24	43
25	73
26	48
27	45
28	45
29	43
30	72

Vous pouvez voir que la valeur de l'indice va en croissant pour les clefs de longueur 3, 4 et 5, puis décroît brusquement pour la longueur 6 : Ceci indique que la clef recherchée pourrait bien être de longueur 5.
Appuyez sur le bouton 5 (zone 7) et vous obtiendrez le texte décrypté, ainsi que la valeur exacte de la clef.

A noter que la valeur de l'indice se comporte de cette même façon pour les multiples de la longueur de clef (10, 15, 20, 25 et 30)

2 - Procédez de même avec le fichier 'Texte crypté Exemple 2.txt'

Bien que ce texte soit beaucoup plus court, la longueur de la clef se laisse facilement deviner grâce à l'indice : A vous de jouer.

3 - Procédez de même avec le fichier 'Texte crypté Exemple 3.txt'

Ici aussi, grâce à l'indice, la longueur de la clef se laisse facilement deviner.

4 - Procédez de même avec le fichier 'Texte crypté Exemple 4.txt'

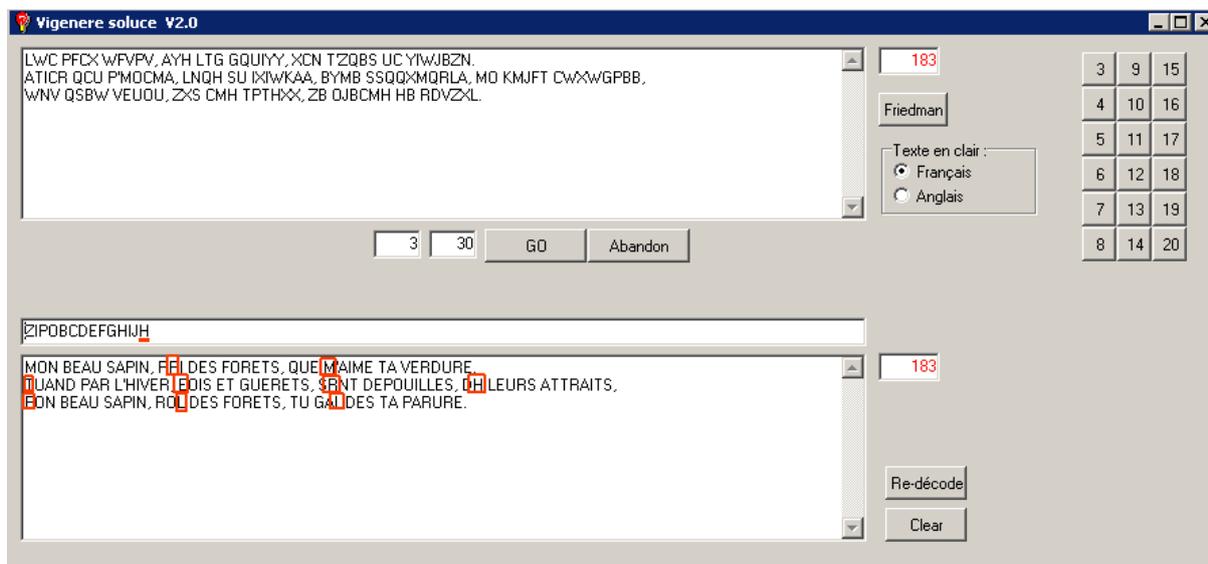
Selon l'indice, la longueur de la clef pourrait être 8 (ou un de ses multiples : 16, 24). Appuyez sur le bouton 8 : Le résultat obtenu n'est pas satisfaisant.

Essayez avec 16. Vous obtiendrez un texte en clair en langue anglaise.

5 - Procédez de même avec le fichier 'Texte crypté Exemple 5.txt'

L'indice de Friedman ne donne pas d'indications bien flagrantes : Il faut donc essayer en fixant un mini-maxi de longueur de clef (3 à 15 par exemple) et appuyer sur le bouton 'GO'.

On peut constater que le texte en clair obtenu est compréhensible, mais tous les 14 caractères la lettre obtenue est erronée :



Cela indique que le 14^e caractère de la clef utilisée n'est pas le bon : Remplacez 'H' par 'K' en zone 3, et appuyez sur le bouton 'Re-décoder'.

6 - Procédez de même avec le fichier 'Texte crypté Exemple 6.txt'

Selon l'indice, la longueur de la clef pourrait être 15, 17 ou 21.

15 et 17 ne donnent pas de résultat satisfaisant.

Vous pourrez essayer la dernière valeur en mettant mini = 21 et maxi = 21, et en appuyant sur 'GO'

7 - Procédez de même avec le fichier 'Texte crypté Exemple 7.txt'

L'indice de Friedman ne permet pas de trouver quelle est la longueur probable de la clef.

Il faut donc essayer de décrypter entre un mini-maxi de longueurs (par exemple 10 à 20).

Si vous avez considéré que le texte en clair est un texte en langue française, aucune solution n'est trouvée.

Par contre, si vous indiquez en zone 6 que le texte en clair est un texte en langue anglaise, vous verrez apparaître la solution.

Conditions d'utilisation

VigenereSolveur est fourni à titre gratuit, et ne bénéficie d'aucune garantie. Son utilisation se fait aux seuls risques et périls de la personne qui choisit de l'utiliser. En aucun cas, l'auteur de ce programme ne peut être tenu pour responsable de quelque dommage que ce soit survenant suite à l'utilisation de ce programme.

Version : 2.0

Mis à jour : 15 avril 2018

Forum d'aide : <http://alainlecomte.free.fr/phpBB2/index.php>

Mises à jour : <http://alainlecomte.free.fr/Download2.htm>