Enigma M3 Crack (Version 1.0)

EnigmaM3Crack est un programme gratuit destiné à déchiffrer les messages codés par la légendaire machine Enigma utilisée par les armées allemandes durant la seconde guerre mondiale.

Le cryptage était basé sur un double système :

- Trois rotors mobiles choisis parmi un jeu de cinq rotors disponibles
- Un tableau de connexion (Stecker) pouvant permuter jusqu'à dix couples de lettres

Chaque rotor comportant les 26 lettres de l'alphabet, le jeu de trois rotors permettait donc 26x26x26 = 17576 combinaisons différentes.
Comme ces trois rotors étaient choisis au sein d'un groupe de cinq, il y avait 60 choix différents possibles (Nombre d'arrangements de 3 parmi 5).
Le Stecker est le dispositif qui offrait, et de loin, le nombre de possibilités de brouillage le plus grand : Dans le cas où on utilisait les dix câbles fournis, le calcul montre que le nombre de combinaisons possibles est de 1,5 x dix puissance 14.
En contrepartie, ce Stecker ne fournit qu'un chiffrement par substitution mono-alphabétique, vulnérable aux attaques par analyse de fréquences.
La puissance de cryptage d'Enigma provient donc surtout de la substitution poly-alphabétique fournie par les trois rotors à avance automatique, le Stecker étant surtout là pour augmenter considérablement le nombre de clés possibles, ce qui rend impossible le décryptage dit par « brute force » (test successif de toutes les clés possibles)
Le nombre total de clés possibles pour la machine Enigma M3 est de 17576 x 60 x de 1,5 x dix puissance 14 = 1,5 x dix puissance 20 : Même avec la puissance des ordinateurs modernes, il faudrait encore un paquet de millions d'années pour essayer successivement chacune de ces clés.

EnigmaM3Crack vous propose donc un outil fonctionnel destiné à réduire considérablement ce temps de décryptage.
Pour ce faire, il utilise le concept **d'indice de coïncidence (IOC)**, qui fut inventé en 1920 par William Friedman : Sur un très long texte, les IOC sont les suivants : Texte aléatoire (par exemple un texte crypté) = 0,0385, texte en français = 0,0778, texte en allemand = 0,0762, texte en anglais = 0,0667

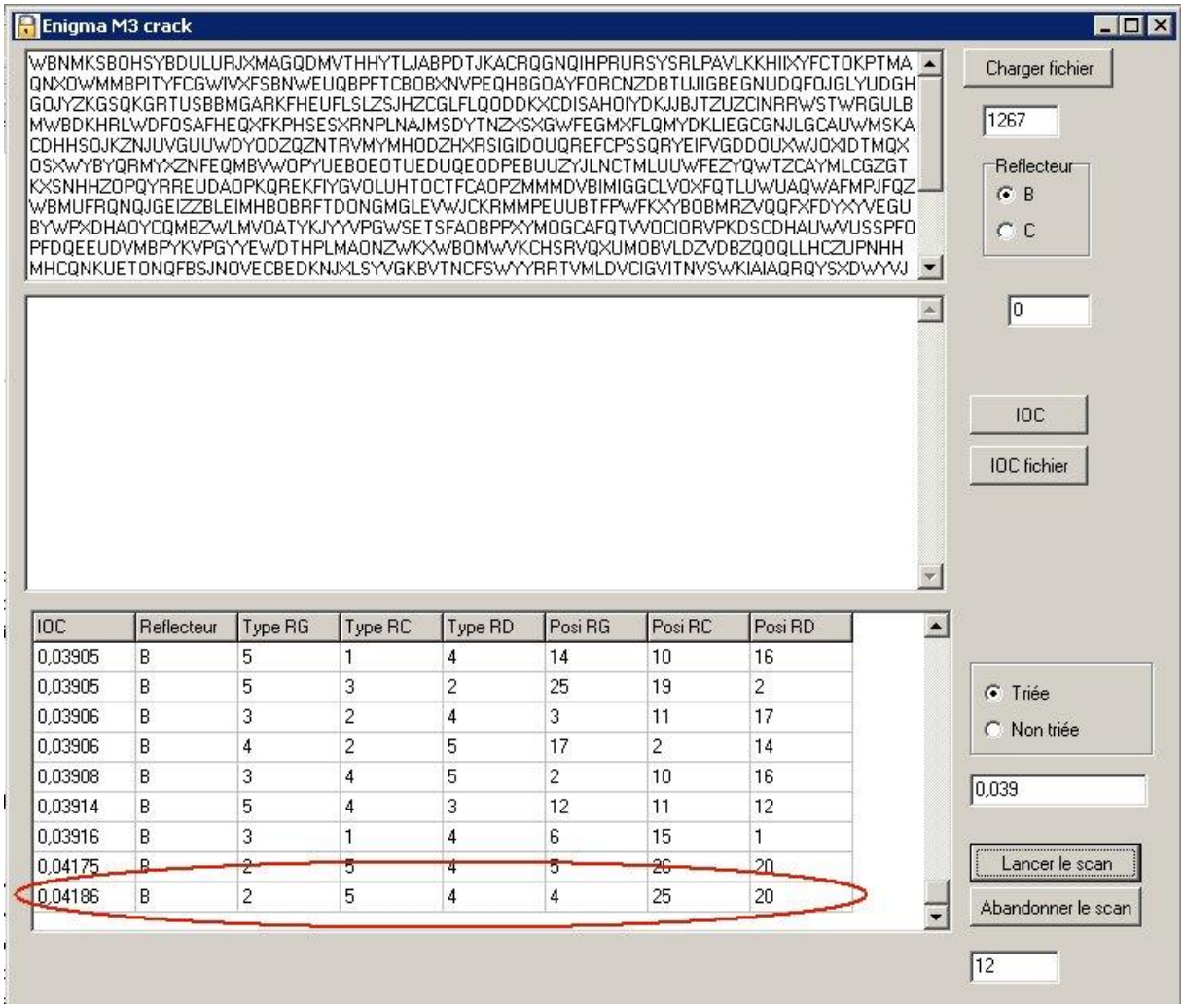
L'opération se déroule en deux temps :

- Recherche des rotors (types et positions initiales) utilisés pour le cryptage
- Recherche des câbles (nombre et positions) utilisés pour le tableau de connexion (Stecker)

La première recherche se fait avec le programme **EnigmaM3Crack.exe**, la seconde se fait avec le programme **Enigma_M3_sim.exe**
Le texte ci-dessous indique pas à pas comment il faut procéder pour décrypter un message-exemple fourni.

Recherche des rotors

Lancez **EnigmaM3Crack.exe** et chargez le fichier **Message-exemple.txt**.
Avec le réflecteur B, choisi par défaut, appuyez sur le bouton '*Lancer le scan*'
Le scan va décoder le texte fourni avec chacune des 17576 x 60 configurations de rotors possibles, et calculer l'IOC sur le texte ainsi obtenu.
Quand le scan est terminé, vous obtenez une liste de des IOC obtenus, classée par ordre croissant, avec indication de la configuration de rotors correspondante.
Vous pouvez faire varier le nombre de lignes retenues en faisant varier le seuil minimum des IOC : Dans l'exemple, seuls les IOC d'au moins 0,03900 sont retenus.
La configuration utilisée pour le cryptage est soit la dernière de la liste, soit une des dernières, tout au moins quand il s'agit d'un texte relativement long (1267 caractères dans l'exemple fourni)



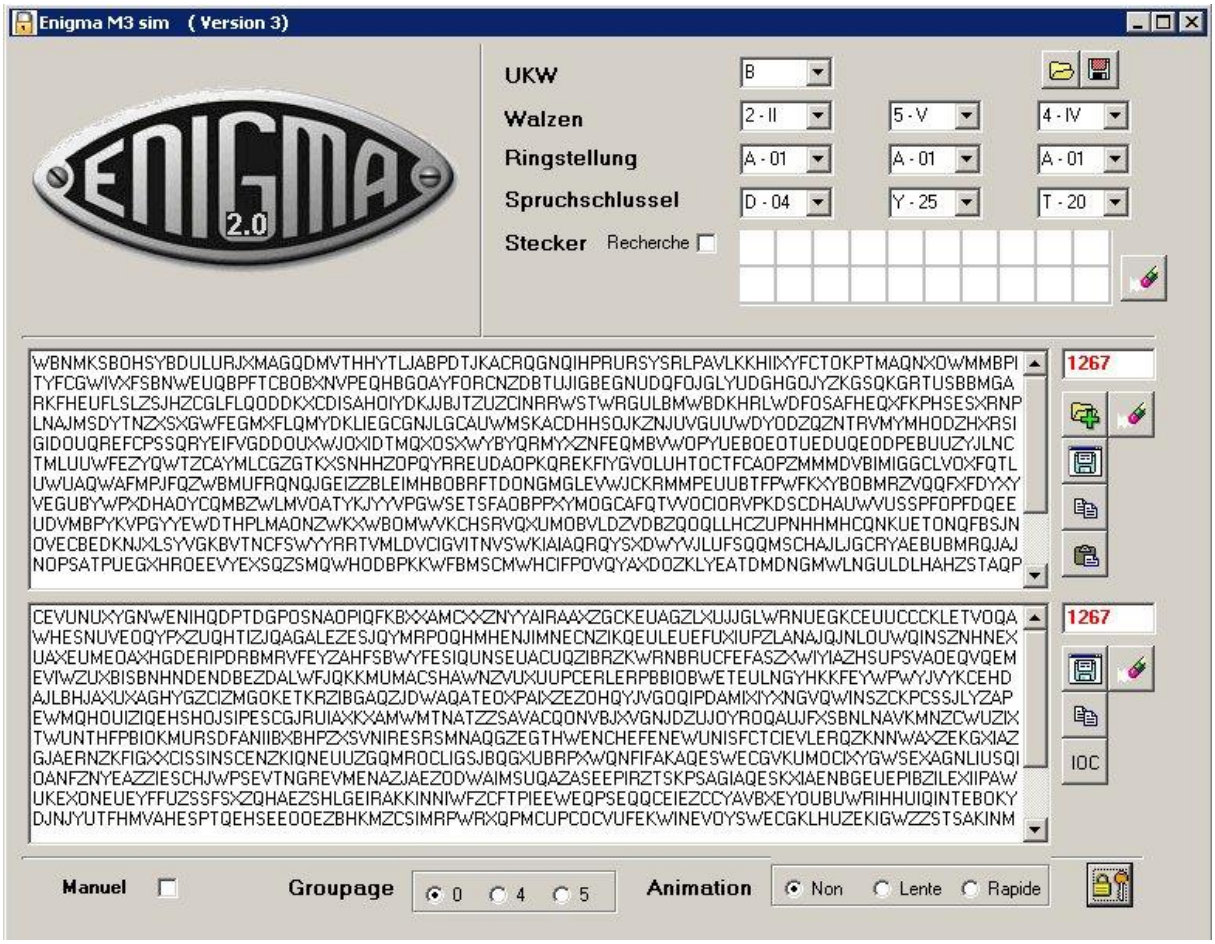
IOC	Reflecteur	Type RG	Type RC	Type RD	Posi RG	Posi RC	Posi RD
0,03905	B	5	1	4	14	10	16
0,03905	B	5	3	2	25	19	2
0,03906	B	3	2	4	3	11	17
0,03906	B	4	2	5	17	2	14
0,03908	B	3	4	5	2	10	16
0,03914	B	5	4	3	12	11	12
0,03916	B	3	1	4	6	15	1
0,04175	B	2	5	4	5	26	20
0,04186	B	2	5	4	4	25	20

Si vous renouvelez l'opération en utilisant le réflecteur C au lieu du réflecteur B, vous constaterez que les IOC obtenus sont au plus de 0.03933 au lieu de 0,04186 : Il est donc probable que le réflecteur utilisé pour le cryptage était le B.

A présent, muni de la configuration probable des rotors, vous pouvez vous attaquer au tableau de connexions.

Recherche des câbles du Stecker

Lancez **Enigma_M3_sim.exe** version 3 ou plus récente, affichez la configuration des rotors obtenue ci-dessus, et chargez le fichier **Message-exemple.txt**.
Appuyez sur le bouton de décryptage, en bas à droite : Vous constatez que le texte obtenu est incompréhensible, ce qui signifie qu'un ou plusieurs câbles du Stecker ont été utilisés au moment du cryptage.



Cocher la case '*Stecker, recherche*' et appuyez sur le bouton de décryptage, en bas à droite : Pour chacun des couples de lettres possibles (AB, AC,….., XZ, YZ), le programme va calculer l'IOC du texte obtenu, et vous présenter le résultat dans un tableau à double entrée 25 x 25.

Afin d'éclaircir le résultat affiché, le chiffre présenté est l'IOC multiplié par 100000

De plus, vous pouvez filtrer le résultat en masquant tous les nombres inférieurs à un seuil fourni (4300 dans l'exemple ci-dessous, c'est à dire un IOC de 0,04300)

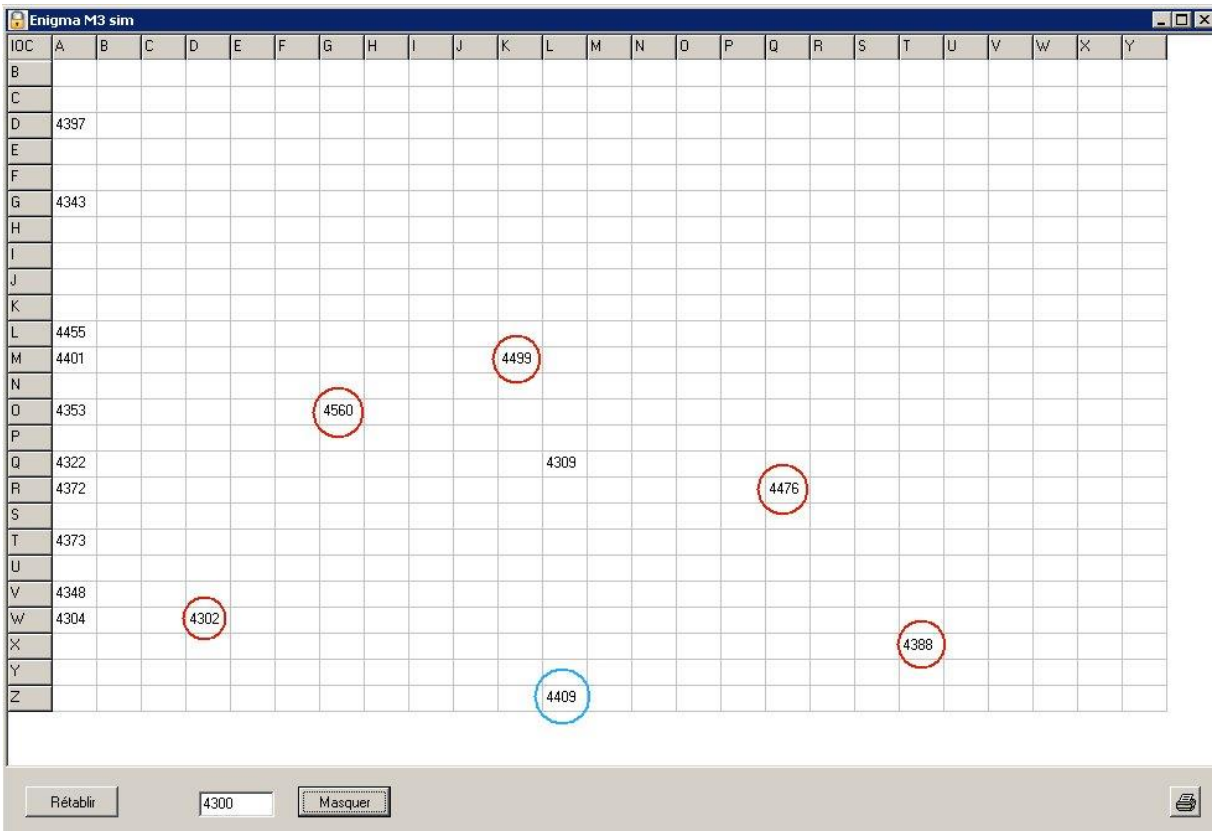
Vous pouvez aussi placer des marqueurs rouges en faisant un clic droit sur une cellule de la grille, ou les supprimer en y faisant un clic gauche.

Dans l'image ci-dessous, vous pouvez constater les associations probables des lettres suivantes :

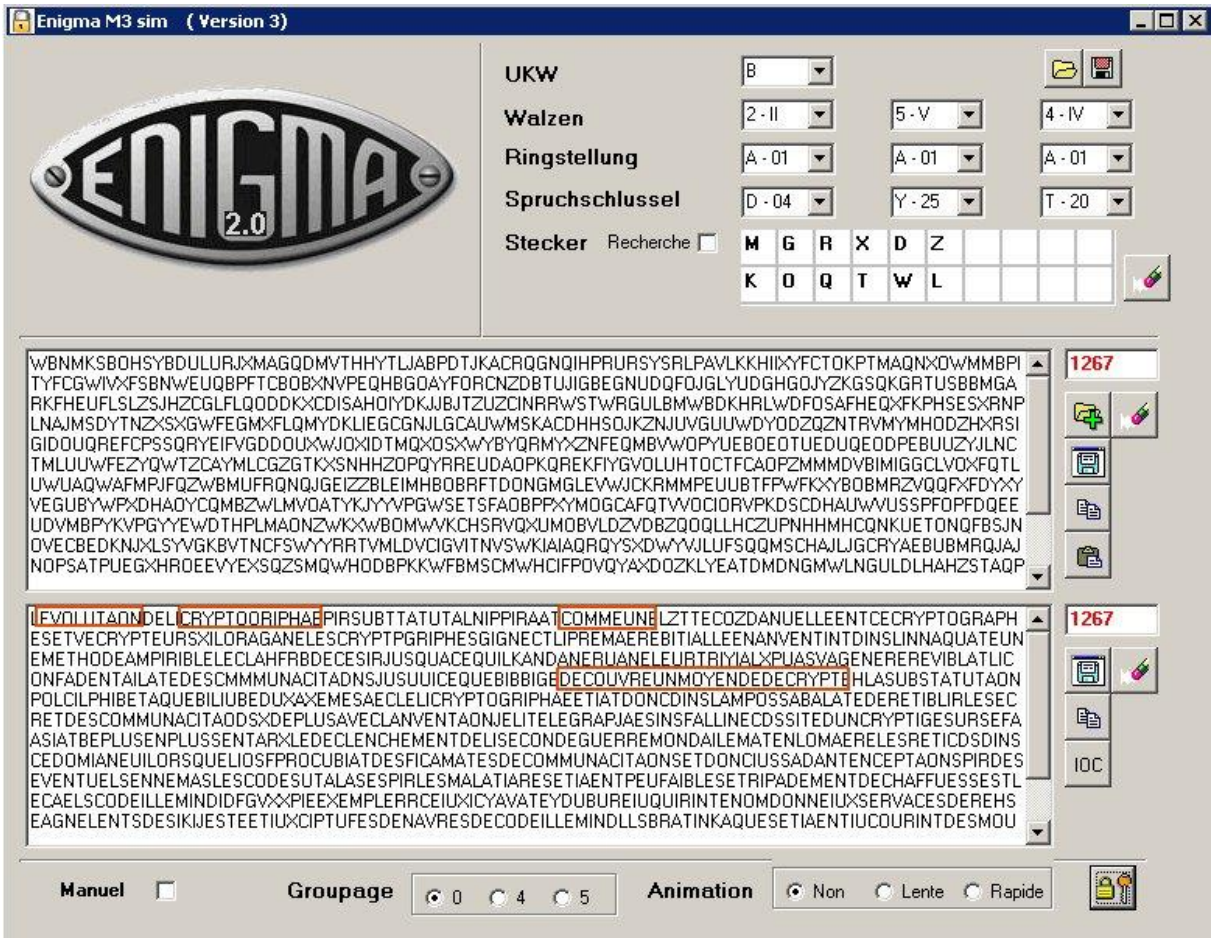
- D avec W
- G avec O
- K avec M
- Q avec R
- T avec X

Concernant la lettre L, deux associations fournissent un IOC élevé : Z et Q, la lettre Z semblant la plus probable.

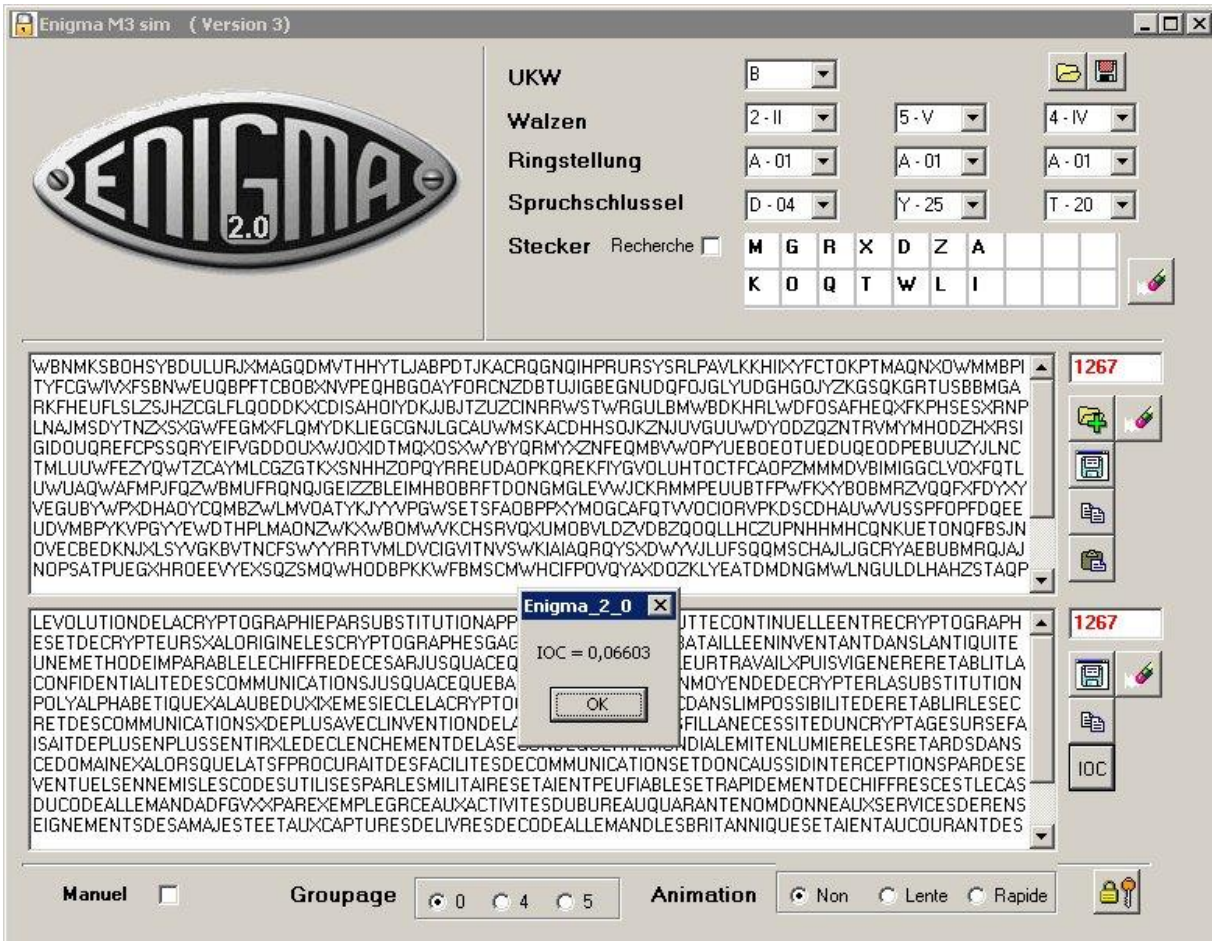
Concernant la lettre A, aucune conclusion n'est possible, car tous les IOC trouvés ont des valeurs proches.
Il faut donc essayer de décrypter avec les associations DW, GO, KM, QR, TX et LZ, et tenter de trouver la bonne lettre associée pour A, sachant que les binômes possibles sont seulement les lettres restantes : B, C, E, F, H, I, J, N, P, S, U, V et Y.



Décochez la case '*Stecker, recherche*', saisissez les lettres du Stecker supposées bonne (DW, GO, KM, QR, TX et LZ) et appuyez de nouveau sur le bouton de décryptage, en bas à droite :



Vous pouvez constater que le texte décrypté est devenu beaucoup moins hermétique : Des morceaux entiers de phrases sont devenus lisibles.
Il faut à présent déterminer quelle est la bonne lettre à associer à A, parmi les treize lettres possible (: B, C, E, F, H, I, J, N, P, S, U, V et Y)
Le plus simple est d'essayer successivement ces 13 binômes possibles, et vous constaterez rapidement que le seul couple donnant un texte complètement lisible est AI.
A noter que pour cette opération finale, le texte lisible n'est pas forcément celui donnant l'IOC le plus élevé, car le texte n'est pas assez long : 'AI' donne un IOC = 0,06603, alors qu'avec 'AV' on obtient un IOC = 0,06812
(Rappel : L'IOC sur un très long texte en langue Française est de 0.0778)



Remarque

Le double programme proposé ici ne vous fournira pas, la plupart du temps, une *solution 'clé en main*', surtout si le texte codé est court et si de nombreuses substitutions de lettres ont été opérées au niveau du Stecker.
Il s'agit avant tout d'un outil destiné à rendre possible, avec un peu de temps et de jugeote, un décryptage qui serait incassable par les méthode habituelles ('brute force', fréquence d'apparition des lettres, etc.)

Condition d'utilisation

Ce double programme est fourni gratuitement et en l'état, sans aucune garantie explicite ou implicite. Son utilisation se fait aux seuls risques de l'utilisateur qui choisi librement de l'utiliser. En aucun cas, l'auteur ne peut être tenu pour responsable de quelque dommage que ce soit lié à cette utilisation.

La version la plus récente peut être obtenu ici : http://www.allec.fr/Download2.htm

Une aide peut être obtenu sur ce forum de discussion : http://alainlecomte.free.fr/phpBB2/index.php