# Solution Proposée pour le décryptage des fichiers

## Décryptage du rébus



Je viens d'a  
ppliquer un al  
gorithme de c  
ryptage xo  
r (sur) tous vos fich  
iers. Je vous laisse   
une semaine   
pour trouver la c  
lé de SIX carac  
tère alPHA minus  
cules,   
maxi.Le texte,   
écarter lettre   
par lettre  
,avec la clé, car  
actère par cara  
ctère.

## Décryptage brutal des fichiers

La stratégie adoptée pour le décryptage des fichiers se base sur la méthode brutale :

* Récupérer les 50 premiers caractères du premier fichier (pour plus de vitesse d’exécution)
* Utiliser une clé pour crypter ces caractères
* Vérifier la phrase décryptée à l’aide d’un dictionnaire de français
* Déposer les solutions probables dans un fichier pour qu’un humain les vérifie.

### Génération des clés

Nous savons grâce au rébus que la clé est composée de six lettres minuscules. La totalité des solutions possibles s’élève donc à 26^6 soit 308 millions de clé différentes. Après avoir tenté de toutes les générer pour ensuite les utiliser individuellement pour décrypter les fichiers, nous nous sommes rendus comptes que la mémoire vive utilisée était trop grande : plusieurs giga octets de mémoire vive étaient monopolisés pour la seule liste contenant les clés.

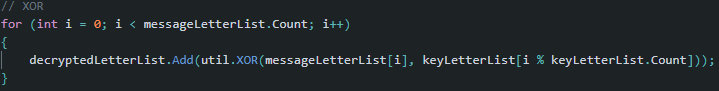
La décision a donc été prise de générer les clés à la volée à chaque tentative de décryptage. Notre programme utilise un générateur de clé qui, à chaque fois qu’il sert une clé au décrypteur, modifie la combinaison de 6 lettres qui servira à générer la prochaine clé. Le système garantit que toutes les possibilités de clés sont testées par ordre croissant, et sans doublons.

### Cryptage XOR

La clé unique est envoyée avec la phrase de 50 caractères dans le décryptage XOR, où chaque caractère de la phrase et comparé à chaque lettre de la clé un à un, dans la forme binaire de leur code ASCII.

|  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| 102 = 'f' | 0 | 0 | 1 | 1 | 0 | 0 | 1 | 1 | 0 |
| 55 = '7' | 0 | 0 | 0 | 1 | 1 | 0 | 1 | 1 | 1 |
| xor = 'Q' | 0 | 0 | 1 | 0 | 1 | 0 | 0 | 0 | 1 |

Tous les 6 caractères comparés, on recommence à la première lettre de la clé à l’aide d’un modulo sur l’index, jusqu’à ce que la totalité des 50 caractères du fichier soient décryptés.



### Vérification des solutions

Le candidat décrypté passe ensuite dans un vérificateur dont le rôle est de s’assurer qu’il contient des mots intelligibles et une structure de phrase rudimentaire. Nous disposons pour cela d’un dictionnaire de 22740 mots français. Cependant, la taille de ce dictionnaire décourage fortement de vérifier toutes les tentatives : 308 millions de candidats, dans lesquels tester chaque mot présent sur une liste de 22740 mots ? Nous avons essayé, et malgré l’efficacité garantie de la méthode, le temps d’exécution du brute force dépassait la centaine d’heures. Nous avons donc opté pour une méthode moins infaillible, mais beaucoup plus rapide.

Plutôt que de vérifier la présence de mots français dans chaque candidat, nous commençons par le comptage des espaces et des ensembles de lettres dans le candidat décrypté. S’il y en a au moins quatre, alors on vérifie qu’au moins 3 de ceux-ci sont présent dans le dictionnaire français. Si c’est le cas, la clé est écrite dans un fichier ainsi que le candidat décrypté, pour que l’un de nous puisse vérifier les candidats et identifier la bonne clé.

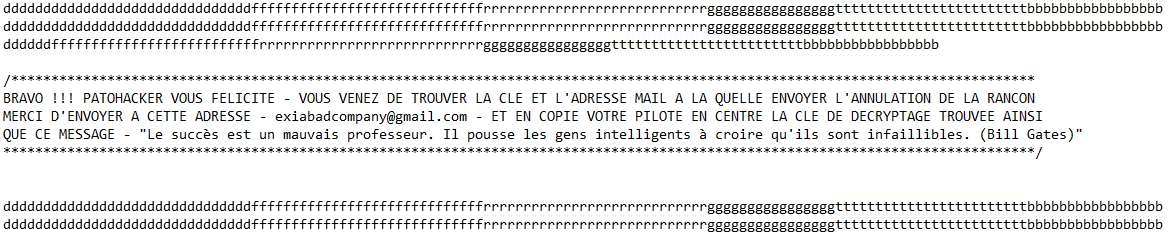
La vitesse d’exécution du programme est passée à environ 3h, et ce pour tester toutes les clés possibles. La clé à été trouvée en 50 min. La phrase était la seule à vérifier les conditions du vérificateur du programme.

La clé de décryptage est la suivante : vrhpaf

## Décryptage des fichiers

Une fois la clé obtenue, il suffit de lancer le décryptage sur l’intégralité des fichiers. Cette étape prend moins d’une seconde et les fichiers redeviennent compréhensibles.

On découvre dans le fichier PC.txt un message caché qui contient des instructions, que nous avons suivies :



Patohacker est vaincu et la paix est de retour dans la galaxie.