

Cryptage 1.0

Programme de cryptage pour Win95/98.

Deux algorithmes de codage sont disponibles :

- codage classique de vigenere
- codage xor et rotation de bits

Le codage de vigénère employé dans ce programme est une variante utilisant une grille de codage élargie. Il est proposé ici à titre anecdotique.

Il est prévu pour crypter uniquement des fichiers texte ascii simple, de toute taille, de type : ***.TXT**

Il est **lent** et à déconseiller pour de gros fichiers.

La clé de codage est une chaîne alphanumérique limitée à 255 caractères.

Le codage xor+rotation de bits utilise des clés numériques de 32 bits.
Il permet le cryptage de tous types de fichiers.
Une fois crypté le fichier est **compressé** avec un algorithme de compression non standard.
Il est assez rapide pour le codage.
La clé de codage est une chaîne alphanumérique limitée à 255 caractères.

Les majuscules, minuscules, symboles et ponctuation sont acceptées ainsi que les espaces.
Tous les caractères comptent.

Exemples de clés pour Vigenere ou Xor (maxi 255 caractères) :

les gaulois sont dans la plaine
ceci EST une CLE
cle de code 123456
666 666 666 666 666 cle de code
la cle : /*-+

Pour Codage Pro (maxi :8 caractères) :

essai
EsSai
cle12345
Clé_1234
...clé..

Cryptage

pour Win9x

Cryptage est un programme qui permet de :

1/ **Crypter** (coder) des fichiers selon plusieurs algorithmes en utilisant une clé de codage.

2/ **Compresser** des fichiers avec des algorithmes personnels. La décompression ne peut se faire qu'avec le programme Cryptage.

3/ **Effacement sécurisé** de fichiers (les outils de recherche direct sur le disque dur sont inopérants).

4/ Génération de Numéros de série

5/ Génération d'executables compressés auto extractibles.

Pour le Cryptage :

Deux algorithmes simples de codage sont disponibles :

- codage classique de vigenere
- codage xor et rotation de bits + **compression**

Voir Utilisation pour plus d'explications.

Le Codage Pro, propose des algorithmes de cryptages plus sophistiqués et utilise des clés standardisées de 128 et 256 bits.

Ce cryptage est accessible via l'onglet Codage Pro.

En cas d'oubli de la clé de codage, il est probable que les données cryptées seront irrémédiablement perdues.

Pour la compression :

Il s'agit d'un mode de protection sans mot de passe pour des informations peu sensibles.

On dispose de 2 algorithmes de compression non standard :

- 1/ DC : type Data Compression : fichiers textes ou image bmp
- 2/ LZ : type Lempel Ziv : tous types de fichiers.

Attention : les fichiers peuvent être décompressés par toute personne possédant le programme Cryptage.

Les fichiers compressés gardent leurs noms d'origine.

L'utilisateur doit se rappeler de la compression employée pour retrouver le fichier original.

*Les fichiers cryptés par XOR sont **déjà** compressés.*

L'onglet **EXE** permet de compresser les executables.

Une fois compressé l'exécutable s'exécute normalement (la décompression est automatique et instantanée).

Le programme utilise le moteur UPX pour la compression.

Le programme est **[FREEWARE](#)**.

L'auteur décline toute responsabilité concernant la perte de fichiers consécutive à l'oubli d'un mot de passe ou à un dysfonctionnement du programme.

L'auteur ne garantit pas l'inviolabilité des algorithmes de cryptages utilisés.

Mail : drremblain@voila.fr

Download : <http://move.to/landzone>

Program by **Roger REMBLAIN** - ©2001 - ***Code Forge®***

Le programme n'installe pas de DLL ni de fichiers .ini et ne touche pas à la base de registre.
Pour désinstaller il suffit d'effacer le programme.

Utilisation

Cryptage : Utilisation

Le fonctionnement du programme est très simple.
Poser la souris sur une icône affiche sa fonction.

Le programme accepte le **glisser/déposer** : il suffit de sélectionner un fichier dans l'explorateur et de le déposer n'importe où ou dans la fenêtre du programme.

Cliquer sur la barre de status (ou le nom du fichier déposé s'affiche) permet d'effacer le fichier sélectionné et d'avoir de nouveau accès au sélecteur de fichier standard.

Le programme accepte la **transmission de paramètres** (passage du nom d'un fichier).
Exemple : c:\temp\cryptage.exe essai.txt --> Lance cryptage avec essai.txt prêts à être utilisés.

Astuce :

- > Créer un raccourci de cryptage et le copier dans le dossier Windows/SendTo
- > Ouvrir l'explorateur de fichiers, sélectionner un fichier et cliquer sur le bouton droit de la souris
- > Sélectionner dans le menu Envoyer vers puis Cryptage
- > Cryptage se lance avec le fichier prêt à être traité (crypté ou décrypté)

L'onglet **Codage Simple** permet l'accès au codage Vigenere et Xor.
L'onglet **Codage Pro** permet de coder en Blowfish, Gost, Rijndael, Twofish.
L'onglet **Compression** permet d'effectuer une simple compression.

Avant de lancer le codage ou le décodage, il faut saisir la clé et l'algorithme de codage souhaité.

L'icône clé permet de générer un mot de passe aléatoire.

Pour décoder, il faut donc **impérativement** se rappeler :

- 1/ la clé (exacte)
- 2/ le mode de codage
- 3/ la taille de la clé en bits (pour Blowfish)

Le fichier crypté par *Vigenere* ou *Xor* change de nom :

avant : essai.txt
après : essai_cod.txt

Pour le décryptage de même :

avant : essai_cod.txt
après : essai_decod.txt

Ces algorithmes simples ne vérifient pas la validité de la clé.

En cas de mauvaise clé, le décryptage se fait quand même mais le fichier obtenu **est toujours codé**. On ne peut retrouver le fichier original qu'avec une bonne clé.

Pour le Codage Pro :

Les fichiers cryptés gardent leur nom d'origine.

Pour decoder un fichier codé, il faut saisir le mot de passe exact et le nombre de bits de la clé (utilisée pour le codage).

Le codage Pro vérifie la validité de la clé et ne lance pas le décryptage si la clé n'est pas bonne.

Si l'algorithme de cryptage choisi n'est pas celui qui a servi au codage, le décryptage ne se fait pas.

L'icone, Voir un fichier crypté, permet une visualisation des fichiers textes cryptés. Il faut **impérativement** saisir le mot de passe et choisir l'algorithme de codage employé pour coder le fichier. Le fichier est ensuite affiché dans une fenêtre tout en restant crypté sur le disque.

Intro

Pour le Codage Pro, l'utilisateur utilise une clé alpha numérique de 8 caractères au maximum. Tous les caractères peuvent être utilisés.

4 algorithmes sont disponibles (vitesse de codage indiquée) :

- Blowfish 2.46 mb/sec
- Gost 1.63 mb/sec
- Rijndael 2.12 mb/sec
- Twofish 1.52 mb/sec

Dans cette version, seules les clés de **128** et **256** bits sont fonctionnelles.

Le programme utilise un algorithme **Hash** pour la protection de la clé.

Le données sont cryptées au format **CBC** (Cipher Block Chaining) pour brouiller la structure du fichier.

Les fichiers de tous types peuvent être cryptés (texte, binaire, exe).

Le fichier original est effacé en utilisant l'effacement sécurisé :

- effacement dans la FAT.
- effacement physique sur le disque octet par octet.

Numéros de série

Le champ **FORMAT** détermine le type de numéro de série généré :

- > le type de caractères générés de façon aléatoire
- > la positions qu'il doivent occuper

Caractères réservé (7)

H or h : Génère un caractère hexadécimal (0 à 9, A, B, C, D, E, F)

Exemple :
HHHHHHHH-HHHH-HHHH-HHHH-HHHHHHHHHHHHH
produit :
2F68143A-A5B0-4FF0-BB94-67C4D6139CAE

Tout caractère non réservé peut être inclu dans le format.

Exemple :
SNHHH-HHH-HHH
produit :
SN796-8DD-1AC ou
SNBF0-0FA-056

A : Génère une lettre majucule.

Exemple:
AAAA-HHHH
produit :
RNBB-97F9 ou
KPMH-473E

a : Génère une lettre minuscule.

Exemple:
aaaa-hhhh
produit :
rnbb-97F9 ou
kpmh-473E

9 : Génère un chiffre.

Exemple:
999-hHhH
poduit :
8049-97F9 ou
kpmh-473E

@ : Génère une lettre (majuscule ou minuscule).

Exemple:
@@@@-AAAA
produit :
jPvE-DSCX ou
Vyfp-OMOT

! : Génère un caractère alphanumérique (majucule ou minuscule).

Exemple:

!!!!-!!!!

produit :

65L6-yH0x ou

Fo8a-Km7g

Pour inclure dans le format un caractère réservé, il faut utiliser :_/

Exemple :

SN9999/@AAAAA-DI/A

produit :

SN2053@JESAV-DIA

SN7581@ASNWB-DIA

SN3271@PTDGC-DIA

Résumé :

/a = Insère le symbole a

/A = Insère le symbole A /h = Insère le symbole h /H = Insère le symbole H

/9 = Insère le symbole 9 /@ = Insère le symbole @

!/ = Insère le symbole !

// = Insère le symbole /

Intro

