Cryptage version 1.3

D'après un algorithme de Alexandre Pukall

PRINCIPE

Le codage utilisé par ce programme est basé sur l'**algorithme PC1** (Pukall Cipher 1). C'est un algorithme de chiffrement en continu (chaque octet est chiffré séparément) en mode PFB (Plaintext Feedback : chaque octet clair modifie le codage des suivants). Il a été créé en 1991 par **Alexandre Pukall**.

L'algorithme est sous copyright mais les droits d'exploitation pour ce programme ont été délivrés par son auteur.

INTERFACE

Au premier démarrage, le programme détecte automatiquement le language utilisé par l'ordinateur et choisi lui-même le language de l'interface parmi les deux langues disponibles : française et américaine (anglaise). Pour changer de language par la suite, il suffit de cliquer sur un des deux drapeaux.

UTILISATION

L'utilisation est très simple : il suffit de saisir un mot de passe (code), de saisir ou de copier un texte en clair, et d'utiliser le bouton *Crypter* pour obtenir le cryptage du texte.

De même, un texte crypté sera très simplement déchiffré par le bouton "Décrypter", pour peu que le code utilisé soit le même !

MOT DE PASSE

Le **code** (mot de passe) peut être composé comme bon vous semble jusqu'à concurrence de **10 caractères**. Cependant, plus le code possède de caractères, plus le cryptage est efficace.

En effet, un code de **10 caractères** donne une clé de **80 bits**. Hors, essayer de casser (essayer de pirater) une clé de 80 bits en effectuant tous les essais possibles, avec 1 million d'essais par seconde, demanderait 38 milliards d'années !

Explications :

2 puissance 80 = nombre d'essais à effectuer pour trouver la bonne clé.
Soit, 2 puissance 80 = 1,208925819615 E 24 (24 zéros) essais.

Nombre d'essais / 1.000.000 (1 million) d'essais par seconde = 1,208925819615 E 18 secondes.
Soit, 1,208925819615 E 18 / 60 (minute) / 60 (heure) / 24 (jour) / 365 (année) = 38334786263,78
Soit, 38 milliards d'années.

Pour choisir son code, il est recommandé d'utiliser une **clé hachée** dont le principe consiste à choisir une phrase facile à retenir (si possible de 10 mots) et à prendre la **première lettre** de chaque mot.

Voici un exemple :

Phrase : **M**on **o**rdinateur **e**t **m**oi-**m**ême **s**ommes **t**rès **b**ons **a**mis **!**
Code : **Moemmstba!**

Cet exemple nous donne un mot de passe de 10 caractères (80 bits).

// Notez que les majuscules et les minuscules ne sont pas équivalentes, et que les signes de ponctuations peuvent très bien être utilisés.

TEXTE NORMAL

Le **texte normal** est le texte destiné à être crypté. Vous pouvez utiliser les signes de ponctuation ou des retours à la ligne (même des lignes blanches) : l'ensemble sera alors crypté comme il se doit.

- Le bouton représentant une *poubelle fermée* vous permet de supprimer le texte.
- Le bouton représentant une *poubelle pleine* vous permet de récupérer ce texte.

Il s'agit d'une corbeille interne attribuée au **texte normal** (suppression et restauration). Elle n'afflige en aucune manière le contenu du Presse-papiers, ni les opérations "Copier/Coller" classiques. Un texte supprimé remplace le précédent et reste disponible à tout moment dans la seconde corbeille.

Notez qu'il n'est pas utile de supprimer le texte en utilisant le premier bouton, ni même d'effacer le texte avant une importation classique (bouton "Coller") puisque cette dernière opération efface et supprime d'office le texte éventuellement affiché.

- Le bouton *A* (*Police)* vous permet de choisir une police proportionnelle ou non.
- Le bouton *Copier* vous permet de copier le texte dans le Presse-papiers.
- Le bouton *Coller* vous permet de coller un texte depuis le Presse-papiers.
- Le bouton *Crypter* crypte le texte normal et l'envoie dans la zone "Texte crypté".

L'option *Formater le texte crypté à x caractères* permet de formater le texte crypté selon vos désirs. Elle sera notamment utile avec certaines messageries dont les lignes de texte ne doivent pas dépasser une certaine longueur. Le nombre de caractères peut être modifié de 1 à 255 !

L'option *Groupes*, disponible seulement si l'option précédente est sélectionnée, permet de découper le texte en groupes de x caractères. Elle sera notamment utile avec certains serveurs de messageries de type Unix afin d'éviter que le texte crypté soit considéré comme un fichier binaire (et non plus texte comme il se devrait). Les groupes créés sont en principe constitués de 5 caractères, mais ils peuvent variés en bout de lignes selon le nombre de caractères choisis avec l'option précédente. Cela n'a aucune incidence pour le but recherché.

// Astuce : un formatage de 60 caractères par ligne (valeur par défaut) donne des groupes de 5 caractères pleins (60 / 5 = 12 groupes).

// Note : le texte complet ne doit pas excéder 16 Ko !

TEXTE CRYPTE

Le **texte crypté** est le texte destiné à être décrypté. Il s'agira en principe d'un texte reçu d'un correspondant : il suffira de le saisir avec attention ! Si le texte provient d'un support informatique (disquette, messagerie, etc.), la chose sera aisée : un simple "Coller" suffira.

La mise en page du texte crypté n'a pas d'importance, car le programme la gère lui-même. C'est ainsi que les retours à la ligne, les espaces et les tabulations sont traités comme il se doit. Autrement dit, vous n'avez pas à vous en soucier et les options *Groupes* et *Formater le texte à x caractères* n'auront aucune incidence sur le décryptage.

Cette **version 1.2** interprète également les éventuelles lettres majuscules (voire tout le texte) pouvant se trouver dans le texte crypté. Ceci est notamment utile après passage par certaines messageries de type Unix (qui transforment tout en majuscules) afin de restaurer le cryptage initial (constitué de minuscules).

// Note: l'opération se déroule en interne au moment du décryptage.

- Le bouton représentant une *poubelle fermée* vous permet de supprimer le texte.
- Le bouton représentant une *poubelle pleine* vous permet de récupérer ce texte.

Il s'agit d'une corbeille interne attribuée au **texte crypté** (suppression et restauration). Elle n'afflige en aucune manière le contenu du Presse-papiers, ni les opérations "Copier/Coller" classiques. Un texte supprimé remplace le précédent et reste disponible à tout moment dans la seconde corbeille.

Notez qu'il n'est pas utile de supprimer le texte en utilisant le premier bouton, ni même d'effacer le texte avant une importation classique (bouton "Coller") puisque cette dernière opération efface et supprime d'office le texte éventuellement affiché.

- Le bouton *A* (*Police)* vous permet de choisir une police proportionnelle ou non.
- Le bouton *Copier* vous permet de copier le texte dans le Presse-papiers.
- Le bouton *Coller* vous permet de coller un texte depuis le Presse-papiers.

- Le bouton *Décrypter* décrypte le texte et l'envoie dans la zone "Texte normal".

Le décryptage suppose bien entendu que le code adéquat soit saisi.

// Note : le texte complet ne doit pas excéder 32 Ko !

EXPERIENCE 1

- Indiquez un **code** de votre choix.
- Saisissez une ligne de **texte normal** (ou copier une partie de ce texte)
- Appuyez sur le bouton **Crypter**.

Le texte crypté apparaît dans la zone "Texte crypté"

Pour vérifier qu'il sera bien décrypté, appuyez sur le bouton "Décrypter" :
- Votre texte initial (texte normal) doit rester strictement inchangé.

Vous pouvez modifier une lettre de votre mot de passe ou une lettre du texte crypté pour vous rendre compte de l'efficacité du cryptage.

EXPERIENCE 2

- Indiquez un **code** de votre choix.
- Saisissez une ligne de **texte normal**.
- Effectuez un passage à la ligne (**Return**).
- **Recopiez** plusieurs fois cette même ligne (Ctrl C - Ctrl V).
- Appuyez sur le bouton **Crypter**.

Le texte crypté apparaît dans la zone "Texte crypté".
Observez que la même ligne n'est pas cryptée de la même manière !

// Note : Le programme ne gère pas le texte ligne par ligne en reprenant le processus depuis le début (le cryptage serait le même pour une même ligne), mais il considère le texte complet comme une seule et unique ligne, procurant ainsi un cryptage beaucoup plus efficace.

INFORMATIONS

Cette version ne permet plus le redimensionnement de l'application ainsi que tous ces constituants. De même, le placement de la fenêtre n'est plus mémorisé et celle-ci apparaîtra toujours au centre. Ce changement rend possible l'utilisation de ce programme sous diverses configurations (notamment avec des configurations n'utilisant pas de polices standards).

Ce programme a été développé sous **Windows 95** et il fonctionne également sous **Windows 98**. Il s'agit toutefois d'un programme **16 bits** qui

fonctionne sans inconvénient sous **Windows 3.x**

L'auteur se dégage de toutes responsabilités concernant l'usage et l'emploi de ce programme qui a été développé dans le seul but de mettre en pratique le principe de l'algorithme PC1 [1]. Il ne pourra en aucun cas être tenu responsable des utilisations que vous voudrez bien en faire.

L'auteur, **Pierre TORRIS**

---

[1] ***Algorithme PC1*** *(Pukall Cipher 1)*

- Créé en Assembleur 6809 Motorola en 1991 par ***Alexandre Pukall***
- Traduit en Turbo C en 1991 par ***Alexandre Pukall***
- Traduit en Turbo Pascal (Delphi) en 1998 par ***Pierre Torris***

L'algorithme PC1 a été conçu à l'origine pour ne traiter que des fichiers, c'est à dire tous les caractères du jeu ASCII (caractères de contrôle, etc.) - Il a donc été légèrement modifié par son auteur afin de convenir au fonctionnement de ce programme. C'est pourquoi le texte crypté fera toujours ici le double de celui d'origine (chaque octet codé normalement par l'algorithme étant recodé par deux lettres). A son avantage, le texte crypté ne sera toujours composé que des lettres "a à p" et il ne causera aucun souci avec les traitements de textes et les messageries qui ne pourraient pas accepter tous les caractères mis en oeuvre.

Pour information :

Les éventuelles mises à jour de ce programme seront disponibles en téléchargement sur le sibe Web de l'auteur. De même, d'autres programmes de cryptographie sont disponibles en téléchargement sur ce même site.

E-mail : **Pierre.Torris@wanadoo.fr** Web : **http://www.mygale.org/11/ptorris**
