

LABORATOIRE 7

Buts: Utiliser un programme principal avec paramètres, lire et écrire dans des fichiers,

Écrire un programme en ligne de commande permettant de lire un fichier et d'écrire son contenu crypté dans un autre fichier, ou vice-versa.

Pour crypter, on lancera la commande :

```
crypt.exe -c fichier_source fichier_crypte
```

Le même programme pourra être utilisé pour décrypter un fichier:

```
crypt.exe -d fichier_crypte fichier_decrypte
```

Le programme demande un mot de passe et fait le travail de cryptage ou de décryptage.

On prendra soin de « blinder » le code en fermant tout fichier qui aurait été ouvert ou en libérant tout tableau qui aurait été réservé dynamiquement avant la terminaison du programme

De plus, il faut envoyer un message d'erreur explicite avant de terminer le programme si :

- L'utilisateur ne donne pas les bons paramètres

- Le fichier source n'existe pas ou ne peut être ouvert
- On ne peut ouvrir ou écrire dans le fichier de destination
- Il y a une erreur, par exemple lors de la lecture ou lors de l'écriture

Il faut également envoyer un message d'avertissement si un fichier est sur le point d'être écrasé
Finalement, si tout s'est bien passé, on indiquera le nombre d'octets écrits dans le fichier de destination

Découper de manière logique ce programme en fonctions et fichiers séparés.

Technique de cryptage à utiliser

Utiliser la clé fournie par l'utilisateur pour initialiser les germes d'un générateur pseudo-aléatoire (voir exercice IV.2)

Chaque caractère du fichier à crypter est remplacé par son code augmenté d'un nombre généré aléatoirement

Pour le fichier à décrypter, il suffit d'initialiser le générateur avec le même germe et de diminuer le code lu par le prochain nombre aléatoire

Durée : 2 séances; le laboratoire sera évalué