SCRAMDISK V2.02H MANUEL DE L'UTILISATEUR

(TRADUCTION: news:fr.misc.cryptologie, 1999)

LOGICIEL GRATUIT DE CRYPTAGE DU DISQUE DUR POUR WINDOWS 95 & 98

http://www.scramdisk.clara.net/
scramdisk@hotmail.com

Document rédigé par S. Simpson &Aman, 1er Avril 1999

Table des matières

Avertissement

> "*Nul ne sera soumis à des investigations arbitraires dans son intimité, sa famille, sa maison ou sa correspondance, ni attaqué dans son honneur et sa réputation. Chacun a droit à la protection de la loi contre de telles investigations ou attaques.*"
> -- Article 12 de la Déclaration Universelle des Droits de l'Homme

Ce programme fait appel à des méthodes de brouillage de disque dur pour empêcher tout accès non autorisé aux données stockées, ce qui peut être interprété par certains comme étant du "cryptage", et par conséquent son utilisation pourrait être réglementée ou interdite dans certains pays.

Il n'est pas destiné au stockage de données illégales dans votre pays, et un tel usage n'est pas le but recherché par l'auteur dans la diffusion de cet utilitaire.

L'auteur du programme (qui souhaite demeurer anonyme) ne peut pas être tenu pour responsable d'éventuelles pertes de données résultant d'incompatibilités du programme avec des configurations matérielles ou logicielles particulières.

Par l'utilisation du programme, la personne l'ayant installé reconnaît qu'il relève de sa ***propre*** responsabilité de sauvegarder ses données importantes, et est ici invitée à le faire avant d'installer le logiciel.

C'est une condition d'utilisation que toute perte de données résultant de tout bogue, erreur ou défaut n'engage pas la responsabilité des auteurs du programme. En cas de doute, sauvegardez vos données avant d'installer ce logiciel et, si possible, faites-le tourner sur un ordinateur qui ne contient pas de données vitales.

Les auteurs ne peuvent être tenus pour responsables, ou de prêter assistance, en cas de perte des mots de passe requis pour accéder aux données cryptées.

Introduction

> "*Pourquoi vous inquiéter si vous n'avez rien à cacher?*"
> -- J. Edgar Hoover

ScramDisk est un programme qui permet de gérer un disque virtuel crypté sous Windows 95 & 98. En gros, un conteneur est créé sur le disque dur et est ensuite ouvert par le logiciel ScramDisk. Celui-ci crée une nouvelle lettre de lecteur logique à travers laquelle on accède au disque. Le point important est que toute donnée écrite sur le nouveau lecteur est cryptée avec l'algorithme de votre choix.

Ce document ne comporte pas d'initiation au fonctionnement du cryptage.

Il existe des programmes offrant des fonctionnalités similaires sous Windows 95 & NT, mais ScramDisk est actuellement unique pour un certain nombre de raisons:

1. C'est un système pleinement opérationnel de cryptage de disque virtuel qui tourne aussi bien sous Windows 95 que Windows 98.

2. Il est entièrement libre de droits d'utilisation.

3. Le code source est disponible pour examen attentif et développement ultérieur sous un minimum de conditions (Voir le chapitre License Details).

4. Il a été développé en GB et, à ce jour, peut en être exporté sous forme électronique. Même si la loi devait changer à l'avenir, on espère que ScramDisk serait alors déjà largement diffusé.

5. Il est impossible de prouver qu'un fichier est un conteneur de disque virtuel ScramDisk sans connaître la phrase secrète. Les fichiers conteneurs ScramDisk n'ont pas d'extension ou d'en-tête spécifiques qui révéleraient qu'ils seraient autre chose que des données aléatoires. Utilisez le programme DieHard pour tester 'l'aléa' d'un disque virtuel ScramDisk.

6. Il peut être considéré comme un travail en devenir. On espère que des gens compétents prendront la suite et l'amélioreront en y ajoutant aussi bien de nouvelles fonctionnalités que de nouveaux algorithmes de cryptage. Le programme est conçu de manière à ce que de nouveaux algorithmes puissent être ajoutés sans trop de difficultés.

7. Les fichiers du programme sont très petits et peuvent être transportés sur une disquette 3,5".

8. Le programme vous permet de cacher un ensemble de fichiers dans un fichier WAV. Ce procédé est connu sous le nom de stéganographie.

9. Il est de loin plus difficile d'organiser une attaque par dictionnaire ou par force brute contre ScramDisk que contre l'un quelconque de ses concurrents.

10. L'"Ecran Rouge" de saisie des phrases secrètes qui les empêche de se faire intercepter par un programme tel que Skin98 ou Back Orifice.

Configuration requise

ScramDisk est peu exigeant en ressources:

- Un PC capable de faire fonctionner Windows 95 ou 98
- Au moins 1 Mo d'espace disque libre pour l'installation de ScramDisk.
- Suffisamment d'espace libre pour créer les fichiers volumes ScramDisk. Cet espace peut se trouver aussi bien sur un disque en FAT16 ou FAT32, une partition vierge, ou un grand fichier WAV au cas où l'on utiliserait la stéganographie.

Installer ScramDisk

ScramDisk est distribué en un fichier ZIP appelé SDisk.zip, téléchargeable depuis la page web de ScramDisk (http://www.scramdisk.clara.net/). Après l'avoir téléchargé, vous devez l'extraire dans un répertoire adéquat (par exemple 'c:\scramdisk\').

Problème identifié: n'essayez pas d'installer ScramDisk dans le répertoire où vous l'avez extrait.

Exécutez le fichier 'sdinstal.exe' et suivez les instructions à l'écran. Quand l'installation sera terminée, l'ordinateur devra redémarrer. Après redémarrage, vous serez en mesure d'utiliser le programme ScramDisk pour créer puis accéder aux volumes cryptés.

Au cas très improbable où le système planterait pendant l'installation, procédez de la manière suivante:

1. Démarrez en mode MSDOS en activant la touche de fonction appropriée

2. Effacez le fichier "C:\Windows\SYSTEM\IOSUBSYS\SD.VXD"

3. Redémarrez Windows. Scramdisk ne fonctionnera pas puisque le pilote aura été effacé.

Le chemin ci-dessus présume que le votre répertoire Windows est "C:\Windows\", si ce n'est pas le cas, utilisez le bon répertoire Windows.

Désinstaller ScramDisk

Chargez ScramDisk et choisissez l'option du menu 'File | Uninstall ScramDisk…'. Il vous sera demandé si vous voulez vraiment désinstaller ScramDisk et le programme redémarrera alors l'ordinateur.

Utiliser ScramDisk

Cette partie de la documentation vous guide pas à pas pour utiliser les fonctionnalités essentielles de ScramDisk.

Là où il y a plusieurs façons de procéder, le manuel vous décrira chacune d'elles et la marche à suivre dans chaque cas.

Pour tirer le meilleur parti de ce manuel, prenez le temps nécessaire pour vous familiariser avec les conventions utilisées, expliquées au paragraphe suivant.

Conventions

Les termes en **gras** indiquent les objets à l'écran; il peut s'agir d'un titre de menu, d'une commande de menu ou simplement d'une option dans une boîte de dialogue. Lorsque vous rencontrez un terme en **gras**, regardez l'écran ScramDisk et vous y verrez l'objet.

Les termes entre [crochets] sont habituellement les titres des zones des boîtes de dialogue, ils seront aussi en **gras** parce qu'il s'agit d'éléments présents à l'écran.

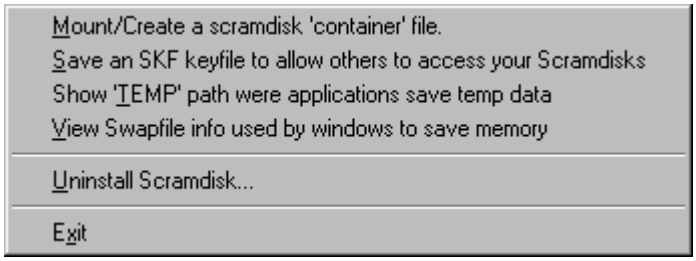
Les termes en `caractères à espacement fixe` sont des entrées de ligne de commande, il s'agit de texte tapé directement dans une fenêtre DOS.

Les procédures alternatives sont mentionnées à la suite de la procédure principale. C'est pourquoi les différentes façons de mener une action seront séparées par un –OU–. Cela assure que les autres procédures suivent la procédure principale. Les niveaux de retrait du texte peuvent servir de guide.

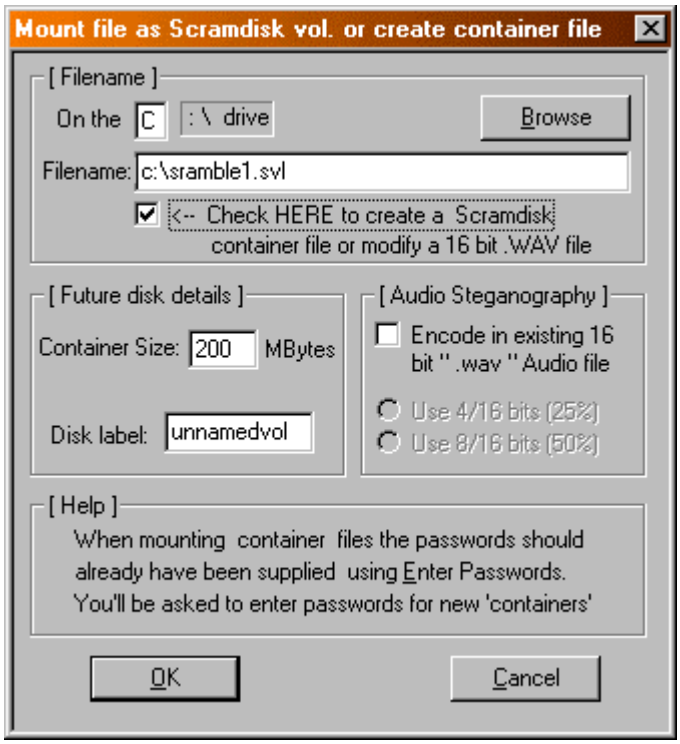
Créer un Volume crypté

A partir de l'écran principal:

Depuis le menu **File**, choisissez **Mount/Create a ScramDisk 'container' file**.



Remplissez les cases de la boîte de dialogue qui s'affiche en suivant ces instructions:



Dans la zone **[Filename]**:

Cochez "**Click HERE to create a ScramDisk container file or modify a 16bit .WAV file**".

Entrez le chemin d'accès au volume crypté, lecteur et nom de fichier (Filename peut aussi inclure le chemin du répertoire).

-OU-

Si vous voulez utiliser Audio Steganography, entrez le chemin d'accès à un fichier WAV adéquat ou cliquez sur **Browse** pour le localiser.

Dans la zone **[Future disk details]**:

Entrez la taille du nouveau volume (en Mo).

Donnez un nom au volume, comme vous le feriez pour un disque ordinaire.

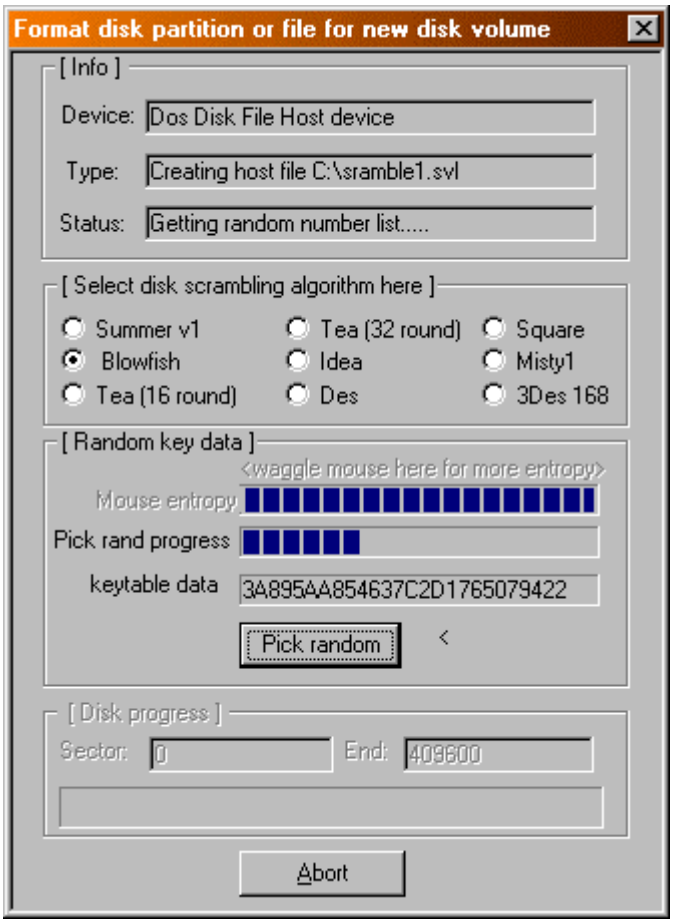
-OU-

Dans la zone **[Audio Steganography]**:

Cochez **Encode in existing 16bit**

Choisissez si vous utiliserez les 4 ou 8 bits du fichier pour le volume crypté. Cela vous donnera un Volume Crypté de taille égale à 25% ou 50% de celui du fichier Wave, respectivement.

Cliquez sur "**OK**" pour aller à l'écran Format.



Dans la zone **[Select disk scrambling algorithm here]**:

Choisissez l'algorithme que vous voulez utiliser pour crypter le volume.

Dans la zone **[Random Key data]**:

Déplacez la souris jusqu'à ce qu'une bonne partie, ou mieux la totalité, de la jauge **Mouse entropy** soit remplie.

Cliquez sur **Pick random** jusqu'à ce que la jauge **Pick rand progress** soit pleine.

-OU-

Cliquez sur **Pick random** une seule fois, pour l'activer, puis appuyez sur la BARRE D'ESPACE jusqu'à ce que la jauge **Pick rand progress** soit pleine.

Dans l’écran Password:

Saisissez la phrase secrète utilisée par l’algorithme.

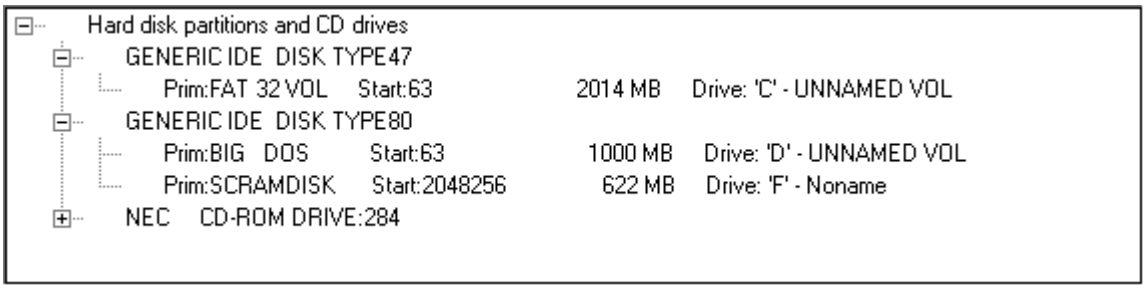
Il vous sera demandé de la saisir encore une fois pour la confirmer.

N.B. Cette phrase sera exigée pour accéder au volume crypté à l’avenir, aussi soyez sûr de vous en souvenir ainsi que de l’endroit où vous l’avez saisie!

Le volume sera alors créé par ScramDisk. Cela peut prendre du temps, en fonction de la taille du volume.

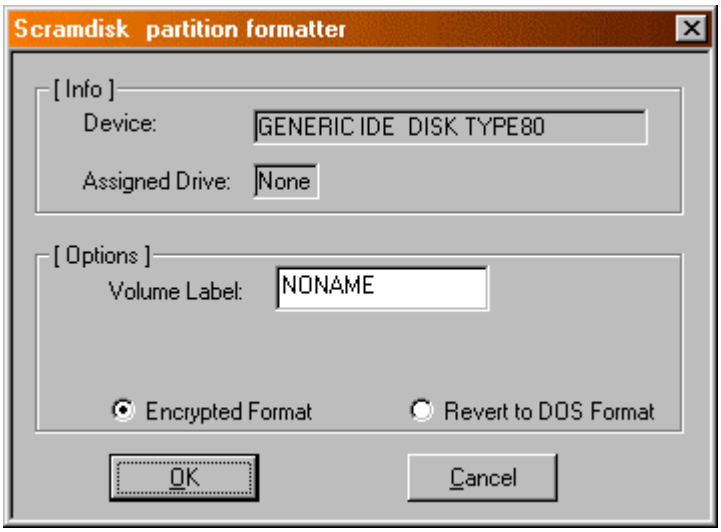
Créer une Partition Cryptée

Au milieu de la zone centrale de l'écran principal (voir description de l'écran plus loin dans ce manuel) est affichée une liste des disques équipant l'ordinateur.

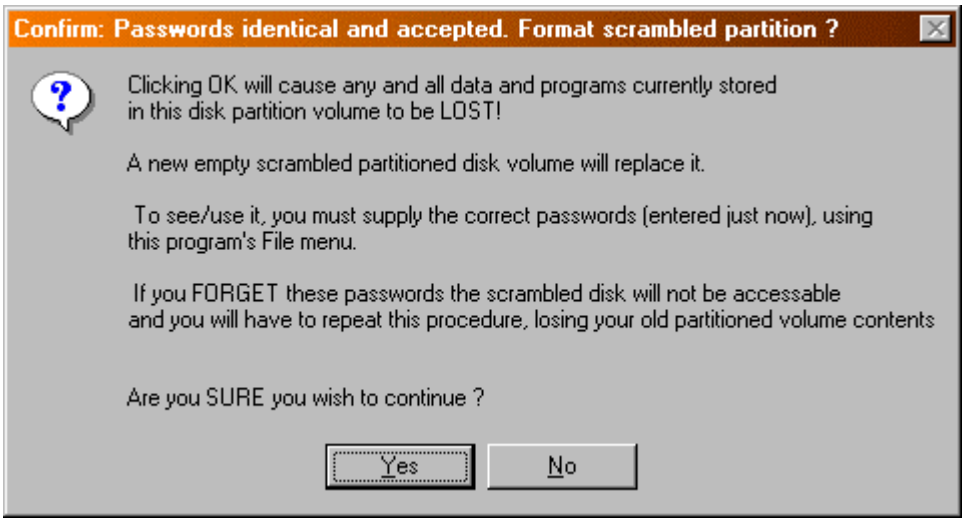


Double-cliquez sur la partition que vous voulez formater avec ScramDisk et une boîte de dialogue apparaîtra.

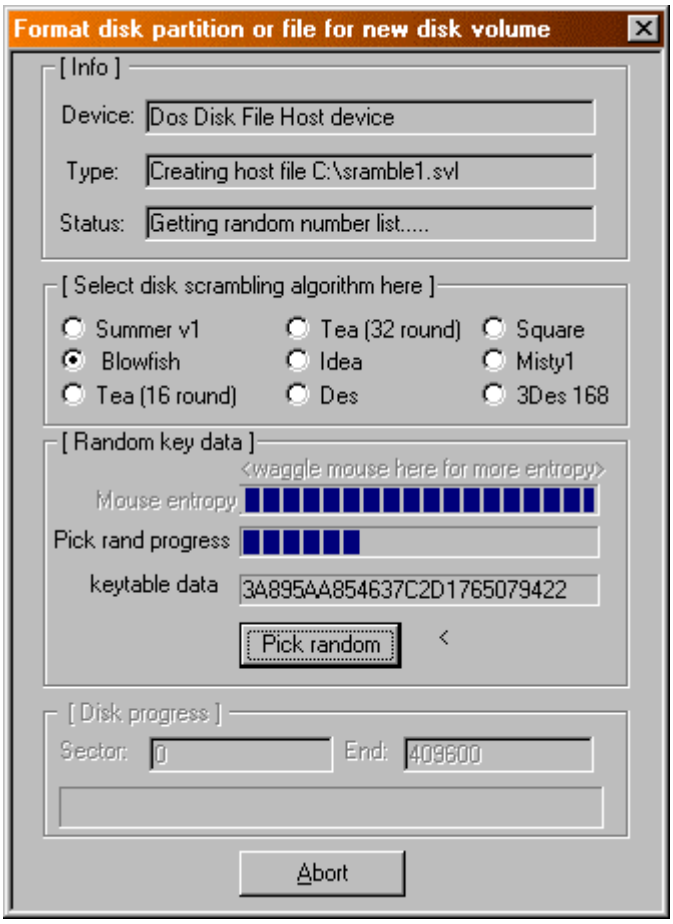
NOTE: Vous **ne devez pas** sélectionner une partition de taille supérieure à 2Gb ou bien le système **deviendra** instable.



Choisir **Encrypted Format** et cliquer sur OK fera apparaître un écran de confirmation.



Cliquer sur **Yes** ouvrira une boîte de dialogue commune à toutes les méthodes de création de volumes cryptés.



Dans la zone **[Select disk scrambling algorithm here]**:

Choisissez l'algorithme que vous voulez utiliser pour crypter la partition.

Dans la zone **[Random Key data]**:

Déplacez la souris jusqu'à ce qu'une bonne partie, ou mieux la totalité, de la jauge **Mouse entropy** soit remplie.

Cliquez sur **Pick random** jusqu'à ce que la jauge **Pick rand progress** soit pleine.

-OU-

Cliquez sur **Pick random** une seule fois, pour l'activer, puis appuyez sur la BARRE D'ESPACE jusqu'à ce que la jauge **Pick rand progress** soit pleine.

Dans l'écran Password:

Saisissez la phrase secrète utilisée par l'algorithme.

Il vous sera demandé de la saisir encore une fois pour la confirmer.

N.B. Cette phrase sera exigée pour accéder à la partition cryptée à l'avenir, aussi soyez sûr de vous en souvenir ainsi que de l'endroit où vous l'avez saisie!

La partition sera alors formatée par ScramDisk. Cela peut prendre du temps, en fonction de la taille de la partition et de l’algorithme choisi.

Ouvrir un Volume Crypté

A partir de l'écran principal:

Depuis le menu **Passwords**, choisissez **Enter ciphered disk volume passwords**

Saisissez la phrase secrète choisie quand vous avez créé le volume crypté, sur la même ligne où vous l'aviez saisie la première fois.

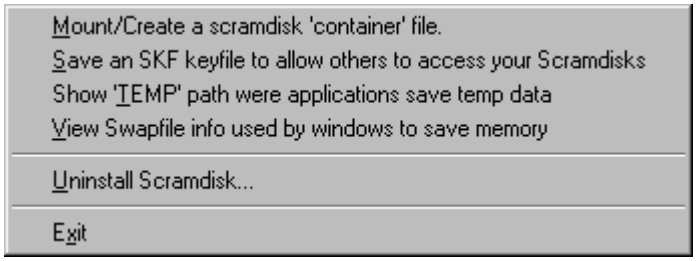
Si vous avez associé l'extension .SVL avec ScramDisk (voir Associer Conteneurs et Fichiers Clés avec ScramDisk), double-cliquez dessus dans une fenêtre de l'Explorateur.

-OU-

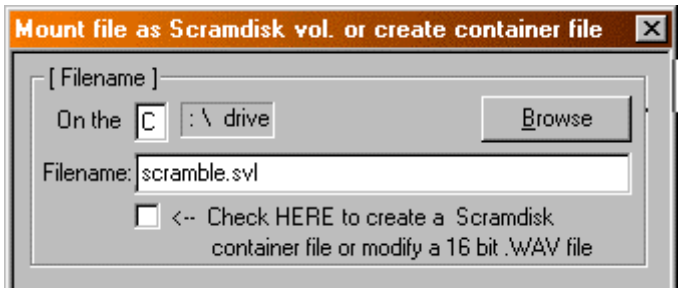
Draguez le fichier de Volume Crypté depuis une fenêtre de l'Explorateur et relâchez-le sur un slot vide.

-OU-

Depuis le menu **File**, choisissez **Mount/Create a ScramDisk 'container' file**



Remplissez les cases de la boîte de dialogue qui s'affiche en suivant ces instructions:



Dans la zone **[Filename]**:

Entrez le chemin d'accès au volume crypté, lecteur et nom de fichier (Filename peut aussi inclure le chemin du répertoire, mais pas la lettre de lecteur).

-OU-

Cliquez sur **Browse** pour le localiser.

Assurez-vous que "**Click HERE to create a ScramDisk container file or modify a 16bit .WAV file**" n'est pas coché, puis cliquez sur **OK** pour finir d'ouvrir le volume.

Le volume ouvert apparaîtra dans le premier slot libre dans l'Ecran Principal.

N.B. Voir les instructions de réglage des préférences pour modifier la façon dont le volume est affiché.

Ouvrir une Partition Cryptée

Saisissez la phrase secrète pour la partition en choisissant "**Enter ciphered disk volume passwords** " depuis le menu **Passwords**.

Si vous n'avez pas coché "**Don t scan HD partitions after entering passwords**" dans la boîte de dialogue **Timeout and Other Settings**, alors ScramDisk ouvrira automatiquement toute partition pour laquelle les mots de passe ont été saisis.

Si ce n'est pas le cas, vous devez choisir **Remount/Refresh** depuis le menu **SDPartitions** pour que ScramDisk ouvre la partition.

Accéder à un Volume Crypté

Exécutez ScramDisk et suivez les instructions pour ouvrir un volume.

On peut accéder au volume de plusieurs façons:

> Depuis l'Ecran Principal par l'icône du volume ouvert (voir Description de l'Ecran Principal pour plus de détails).
>
> -OU-
>
> Depuis l'Explorateur de la même manière que pour n'importe quel lecteur.
>
> -OU-
>
> Depuis n'importe quelle boîte de dialogue de fichiers, c-à-d le menu **Démarrer** la commande **Exécuter**, la boîte de dialogue **Fichier Ouvrir** dans toute application Microsoft Office etc.
>
> -OU-
>
> Depuis une fenêtre MS-DOS, utilisez la lettre de lecteur du volume exactement comme vous le feriez pour un disque dur.

L'utilisation du volume crypté est transparente à l'utilisateur et aux applications, si ce n'est une légère baisse de performance, dont l'ampleur dépend de l'algorithme utilisé et de la puissance du PC.

Les Volumes Cryptés restent accessibles jusqu'à la sortie de Windows. Puisque le pilote VxD est toujours chargé, vous n'avez pas besoin de laisser l'utilitaire ScramDisk actif une fois que les Volumes Cryptés ont été ouverts.

Fermer des Volumes Cryptés

A partir de l'écran principal:

Depuis le menu **Dismount**,

Choisissez **Dismount All**, pour fermer tous les Volumes actuellement ouverts.

-OU-

Choisissez **Dismount Brutal**, pour fermer brutalement tous les volumes ouverts. Cela fermera tous les volumes même si des fichiers ou fenêtres sont ouverts. ScramDisk attendra que 2 secondes se soient écoulées depuis la dernière opération d'E/S sur le Volume, pour permettre que des écritures en cours etc.

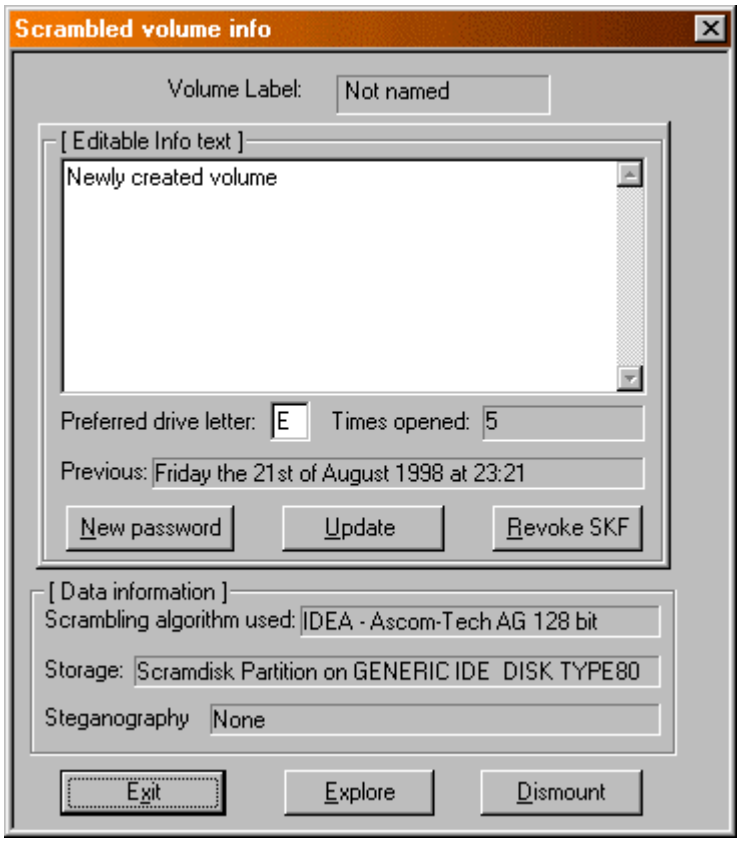
-OU-

Si vous voulez fermer un volume particulier en laissant les autres ouverts, faites un clic du bouton droit sur l'icône du Volume dans l'écran principal et cliquez sur **Dismount** dans la boîte de dialogue **Volume info**.

Régler les Préférences pour un Volume Crypté

A partir de l'écran principal:

Cliquez du bouton droit sur le slot contenant le volume ouvert dont vous voulez régler les préférences pour afficher la boîte de dialogue "**Scrambled Volume info**".



Dans la zone **[Editable Info Text]**:

Ajoutez des commentaires décrivant le volume (optionnel).

Saisissez une lettre de lecteur sous laquelle vous préférez ouvrir le volume. Si aucune n'est mentionnée, alors le volume se voit attribuer la première lettre disponible au moment où il est ouvert.

Cliquez sur **New Password** pour changer la phrase secrète du Volume.

Cliquez sur **Revoke SKF** pour révoquer les droits d'accès au Volume antérieurement accordés aux fichiers SKF.

Cliquez sur **Update** pour sauvegarder vos préférences pour le volume.

N.B. Si vous exécutez une application installée dans le volume, à laquelle se réfèrent des entrées de la base de registres, vous devriez alors être sûr que la même lettre est toujours assignée et disponible. Une bonne manière d'y arriver est de choisir une lettre éloignée de l'alphabet pour le lecteur (c-à-d X:) pour prévenir un incident avec votre CD-ROM ou d'autres volumes.

Cette zone donne aussi des informations concernant la date de la dernière ouverture du volume et le nombre de fois où il a été ouvert.

La zone **[Data information]** donne un résumé des informations relatives à l'Algorithme de Cryptage, l'unité de Volume Crypté et l'emploi de la Stéganographie (s'il y a lieu).

Vous pouvez aussi explorer ou fermer le volume depuis cet écran en cliquant sur **Explore** ou **Dismount**.

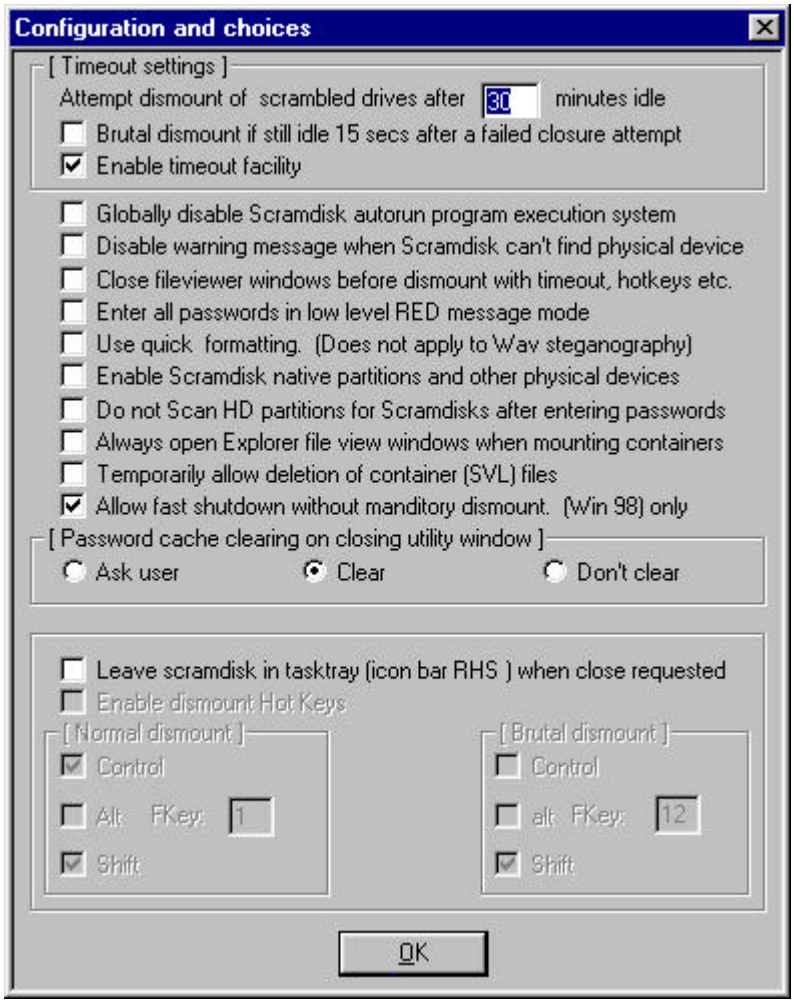
N.B. Si vous avez changé la lettre de lecteur préférée du volume, vous devez le fermer et le rouvrir pour que les modifications prennent effet.

Utiliser la Fonction de Délai d'Attente

A partir de l'écran principal:

Depuis le menu **Configure**, choisissez **Configure Scramdisk**

Dans la boîte de dialogue qui s'affiche,



Cochez "**Enable timeout facility**" pour activer cette fonction.

Dans la zone **[Timeout settings]**:

Entrez la durée de la période d'inactivité (en minutes) après laquelle ScramDisk fermera tous les volumes ouverts. Malgré ce réglage, ils ne seront cependant pas fermés si à ce moment-là des fichiers ou des fenêtres dépendants de(s) volume(s) crypté(s) sont ouverts.

Cochez "**Brutal dismount if still idle 15 secs after a failed closure attempt**" pour que ScramDisk force quand même la fermeture des volumes. Cela sera fait 15 secondes après la première tentative manquée pour les motifs indiqués ci-dessus.

Les autres réglages concernant la fonctionnalité de Délai d'Attente sont:

"**Close fileviewer windows before dismount with timeout, hotkeys etc.**".

> Cochez cette case pour que ScramDisk ferme toute fenêtre de type Explorateur qui serait ouverte à partir de volumes cryptés lorsqu'il essaye de les fermer.
> Le choix de cette option garantira une fermeture efficace et en douceur des Volumes.

"**Enable dismount Hot Keys**"

> Cochez cette case pour permettre à ScramDisk de fermer tous les Volumes Cryptés par un simple appel de touches.
>
> Pour que cela marche, vous devez aussi cocher la case "**Leave ScramDisk in tasktray…**".
>
> Une fois que "**Enable dismount Hot keys**" a été sélectionné, vous pouvez configurer les options adéquates dans les zones "**Normal dismount**" et "**Brutal dismount**" afin de choisir les combinaisons de touches des Raccourcis Clavier.

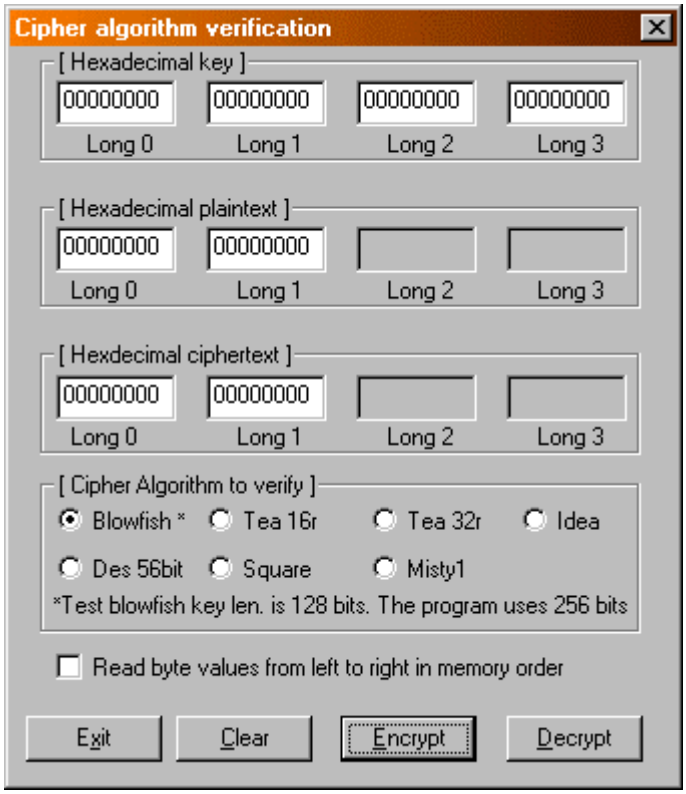
Les autres réglages figurant dans cette boîte de dialogue sont expliqués ailleurs dans ce manuel.

Vérifier les Algorithmes Utilisés

Procurez-vous un jeu fiable de textes clairs, clés et textes cryptés pour l'algorithme que vous voulez vérifier.

A partir de l'écran principal:

Depuis le menu **About**, choisissez **Cipher verifier**. Cela affichera l'utilitaire de vérification.



Dans la zone **[Hexadecimal key]**:

Entrez votre clé 'reconnue'.

Dans la zone **[Hexadecimal plaintext]**:

Entrez votre texte clair 'reconnu'.

Dans la zone **[Cipher Algorithm to verify]**:

Choisissez l'algorithme à tester en cochant le bon bouton.

Appuyez sur **Encrypt**.

Contrôlez les valeurs obtenues dans la zone **[Hexadecimal ciphertext]** par rapport à votre texte crypté 'reconnu'.

N.B. L'opération inverse peut aussi être testée en entrant le texte crypté "reconnu" et en actionnant **Decrypt** pour générer le texte clair aux fins de comparaison.

Voir le chapitre "Appendice A – Vecteurs de Test des Algorithmes" en page 79 pour les détails relatifs aux vecteurs de test publiés.

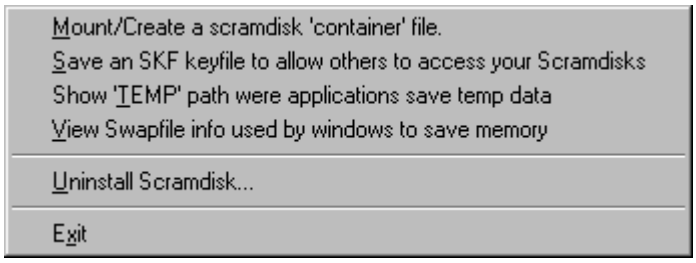
Accès d'un 2ème Utilisateur – Sauvegarder un Fichier Clé

Ouvrez tous les Volumes Cryptés auxquels vous voulez autoriser l'accès à un second utilisateur. Les instructions pour le faire figurent sous "**Ouvir un Volume Crypté**".

Saisissez la phrase secrète pour le fichier clé. Ce sera la seule phrase secrète dont le 2ème utilisateur aura besoin et aussi la seule qu'il aura à connaître.

A partir de l'écran principal:

Depuis le menu **File**, choisissez **Save an SKF keyfile to allow others to access your Scramdisks**.



Donnez un nom au Fichier Clé et sauvegardez-le où vous voudrez.

Le Fichier Clé est portable, mais n'est utilisable qu'avec l'ordinateur à partir duquel il a été généré et uniquement pour les volumes qui étaient ouverts quand il a été créé.

Un Fichier Clé sert à permettre à d'autres personnes d'accéder à un Volume Crypté sans avoir à leur révéler la phrase secrète pour le volume lui-même.

N.B. L'accès à un volume par Fichier Clé peut être révoqué pour l'avenir à partir de la boîte de dialogue "Scrambled Volume info".

L'accès via un Fichier Clé ne permet pas à cet utilisateur d'accéder à la boîte de dialogue des propriétés du volume, les volumes devant être ouverts avec leurs propres phrases secrètes pour qu'elle soit accessible. Font exception à cette règle les volumes cryptés avec Summer: ils en permettent l'accès même via les Fichiers Clés.

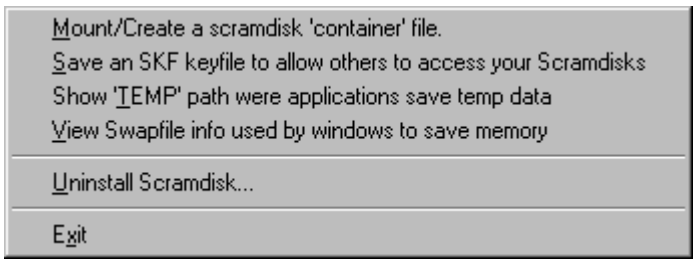
Accès d'un 2ème Utilisateur - Ouvrir des Volumes Cryptés

A partir de l'écran principal:

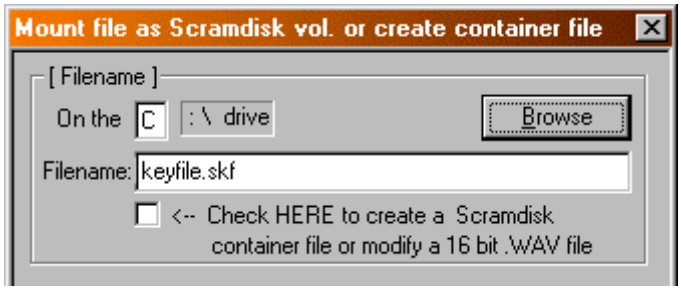
Depuis le menu **Passwords**, choisissez **Enter Keyfile password [SKF access files]**, cela fera apparaître l'écran Password.

Saisissez la phrase secrète choisie lors de la création du Fichier Clé, sur les mêmes lignes où vous l'aviez saisie à l'origine.

Depuis le menu **File**, choisissez **Mount/Create a ScramDisk 'container' file.**



Remplissez la boîte de dialogue qui s'ouvre conformément aux instructions suivantes:



Dans la zone **[Filename]**:

Entrez le chemin d'accès au Fichier Clé, lecteur et nom de fichier (Filename peut aussi inclure le chemin du répertoire, mais pas la lettre de lecteur).

-OU-

Cliquez sur **Browse** pour le localiser.

Assurez-vous que " **Click HERE to create a ScramDisk container file or modify a 16bit .WAV file** " n'est pas coché, puis cliquez sur **OK**.

Le(s) volume(s) ouvert(s) apparaîtront dans le(s) slot(s) dans l'Ecran Principal.

N.B. Les Fichiers Clés créés avec une version antérieure de Scramdisk ne fonctionneront pas avec la V2.02. Vous devrez d'abord les révoquer (Voir Régler les préférences pour un volume crypté) puis les recréer avec la V2.02.

Associer Conteneurs et Fichiers Clés avec ScramDisk

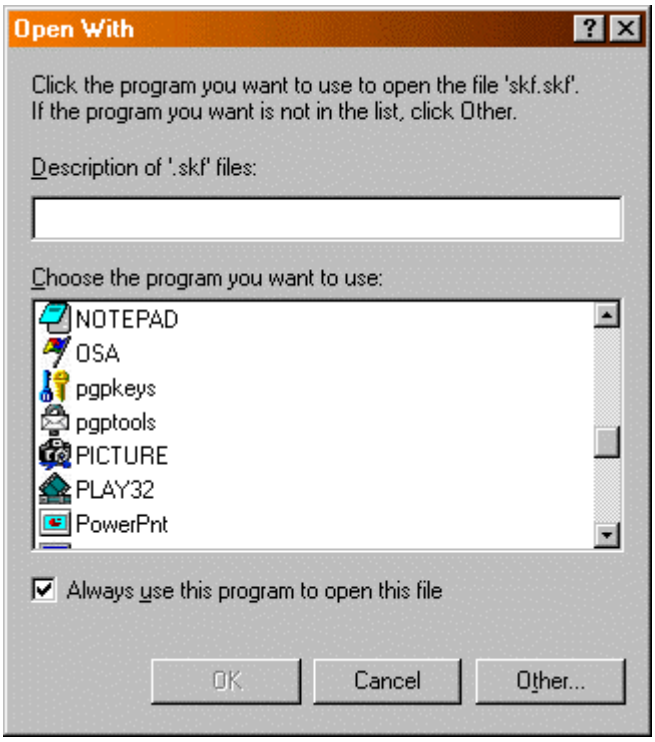
Par l'**Explorateur** ou le **Poste de Travail**, localisez un Fichier Clé (.skf) ou un fichier conteneur (.svl).

Cliquez sur le fichier pour le sélectionner (le nom sera mis en surbrillance).

Gardez la touche MAJ appuyée et cliquez du bouton droit sur l'icône du fichier.

Choisissez **Ouvrir Avec** depuis le menu contextuel qui apparaît.

Une boîte de dialogue s'ouvrira:



Cliquez sur **Autre** et allez là où se trouve le fichier ScramDisk.exe (Si vous ne savez pas où il est, utilisez **Rechercher** du menu **Démarrer** pour le retrouver).

Sélectionnez le fichier ScramDisk.exe puis **OK**.

Assurez-vous que **Toujours utiliser ce programme pour ouvrir ce fichier** est coché et que ScramDisk est sélectionné dans la zone **Choisissez le programme à utiliser**.

Confirmez les choix par **OK**.

La prochaine fois que vous cliquerez sur un Fichier Clé ou un fichier conteneur, ScramDisk l'ouvrira et demandera une phrase secrète (si elle n'est pas déjà en cache).

Ouvrir un ou des volume(s) ou partition(s) crypté(s) au démarrage

Il existe deux méthodes pour ouvrir des volumes au démarrage, entre lesquelles vous choisirez en fonction du nombre et du genre de volumes que vous voulez ouvrir.

Quelle que soit la méthode retenue, vous devrez avoir préalablement associé le type de fichier avec ScramDisk.exe. Pour savoir comment faire, lisez le chapitre "Associer Conteneurs et Fichiers Clés avec ScramDisk".

Utilisez le tableau ci-dessous pour décider de la méthode qui vous convient.

Volume(s) Crypté(s)	Méthode
Un seul fichier conteneur (.svl)	1 – Raccourci vers le nom de fichier
Plusieurs fichiers conteneur (.svl)	2 - Raccourci vers le fichier SKF
Volume(s) Stéganographique(s) (.wav)	2 - Raccourci vers le fichier SKF
Partition(s) Cryptée(s)	2 - Raccourci vers le fichier SKF

METHODE 1 RACCOURCI VERS LE NOM DE FICHIER:

Ouvrez le **Menu Démarrer** en cliquant du bouton droit sur **Démarrer**.

Allez dans le dossier **Démarrage** (il se trouve dans le dossier **Programmes**).

Cliquez du bouton droit dans un endroit libre dans le dossier.

Choisissez **Nouveau** puis **Raccourci** depuis le menu qui apparaît.

Entrez le chemin d'accès à votre fichier conteneur (.svl) dans la fenêtre **Ligne de commande** puis faites **OK**.

Donnez un nom au raccourci puis faites **OK**.

La prochaine fois que vous démarrerez Windows, ScramDisk ouvrira votre fichier conteneur et demandera la phrase secrète.

Après l'avoir saisie, votre Volume Crypté sera accessible.

METHODE 2 RACCOURCI VERS LE FICHIER SKF:

Ouvrez d'abord tous les fichiers conteneurs et les partitions à ouvrir au démarrage.

Sauvegardez un fichier SKF comme indiqué au chapitre "Accès d'un 2ème Utilisateur - Sauvegarder un Fichier Clé".

Suivez la **Méthode 1** en indiquant cette fois le chemin d'accès à votre Fichier Clé.

La prochaine fois que vous démarrerez Windows, ScramDisk ouvrira le(s) volume(s) accessibles par Fichier Clé et demandera la phrase secrète.

Après l'avoir saisie, le(s) Volume(s) Crypté(s) seront accessibles.

Fonction Lancement Automatique

ScramDisk v2.02h dispose dorénavant d'une fonctionnalité qui permet à un programme ou à un document associé d'être lancé automatiquement chaque fois que des conteneurs spécifiques sont ouverts.

Créez dans la racine d'un volume ScramDisk ('f:\' par exemple) un raccourci vers quelque chose que vous voulez lancer ou démarrer (comme si vous double-cliquiez sur le raccourci) chaque fois qu'un conteneur particulier est ouvert.

Rennommez le raccourci en 'ScramDisk'

C'est tout! Chaque fois que le conteneur ScramDisk est ouvert, l'application ou le fichier de données pointé par le raccourci est exécuté.

Cette fonctionnalité est intégrée en réponse à ceux qui se plaignaient que des applications ne pouvaient pas être lancées via le dossier "Démarrage", si elles se trouvaient dans un volume ScramDisk. Désormais elles le peuvent, si ScramDisk est lancé, et les conteneurs ouverts, via le dossier "Démarrage". ScramDisk lancera les applications comme elles auront été réglées.

Il est possible de désactiver cette fonctionnalité depuis la boîte de dialogue Configure.

Accès via la Ligne de Commande

ScramDisk permet les actions suivantes via la ligne de commande au moyen de paramètres:

Action	Paramètre	Exemple
Ouvrir[1]	Chemin au volume	`SCRAMDISK.EXE C:\monvolume.svl`
Ouvrir[1a]	Chemin au fichier	`SCRAMDISK.EXE C:\monfichierclé.skf`
Fermeture Normale	/DN	`SCRAMDISK.EXE /DN`
Fermeture Brutale[2]	/DB	`SCRAMDISK.EXE /DB`

[1] ScramDisk essayera d'ouvrir le volume spécifié avec les mots de passe actuellement en cache. Si le(s) mot(s) de passe sont incorrects ou ne sont pas en cache, l'écran Password s'affichera.

[1a] ScramDisk ouvrira tous les volumes pour lesquels le Fichier Clé a été généré. Vous ne pourrez essayer de saisir le mot de passe qu'une seule fois, si vous vous trompez, vous devrez relancer la commande une nouvelle fois.

[2] Fermeture Brutale ne fermera pas le(s) volume(s) avant que 2 secondes ne se soient écoulées depuis la dernière opération d'E/S.

N.B. Les paramètres peuvent être utilisés avec un raccourci vers l'exécutable ScramDisk (ScramDisk.EXE), mais vous devrez mettre le chemin d'accès à un volume entre guillemets s'il comporte des espaces.

Description des Ecrans et des Menus

Cette partie de la documentation décrit les écrans les plus utilisés et tous les menus de l'Ecran Principal.

Les écrans les plus utilisés sont illustrés par des copies d'écran et les légendes en expliquent les éléments.

Tous les menus de l'Ecran Principal sont figurés par une copie d'écran et une description des fonctions de chacun de ses éléments.

Conventions (description des Menus)

Les éléments en **gras** se réfèrent aux options des menus eux-mêmes.

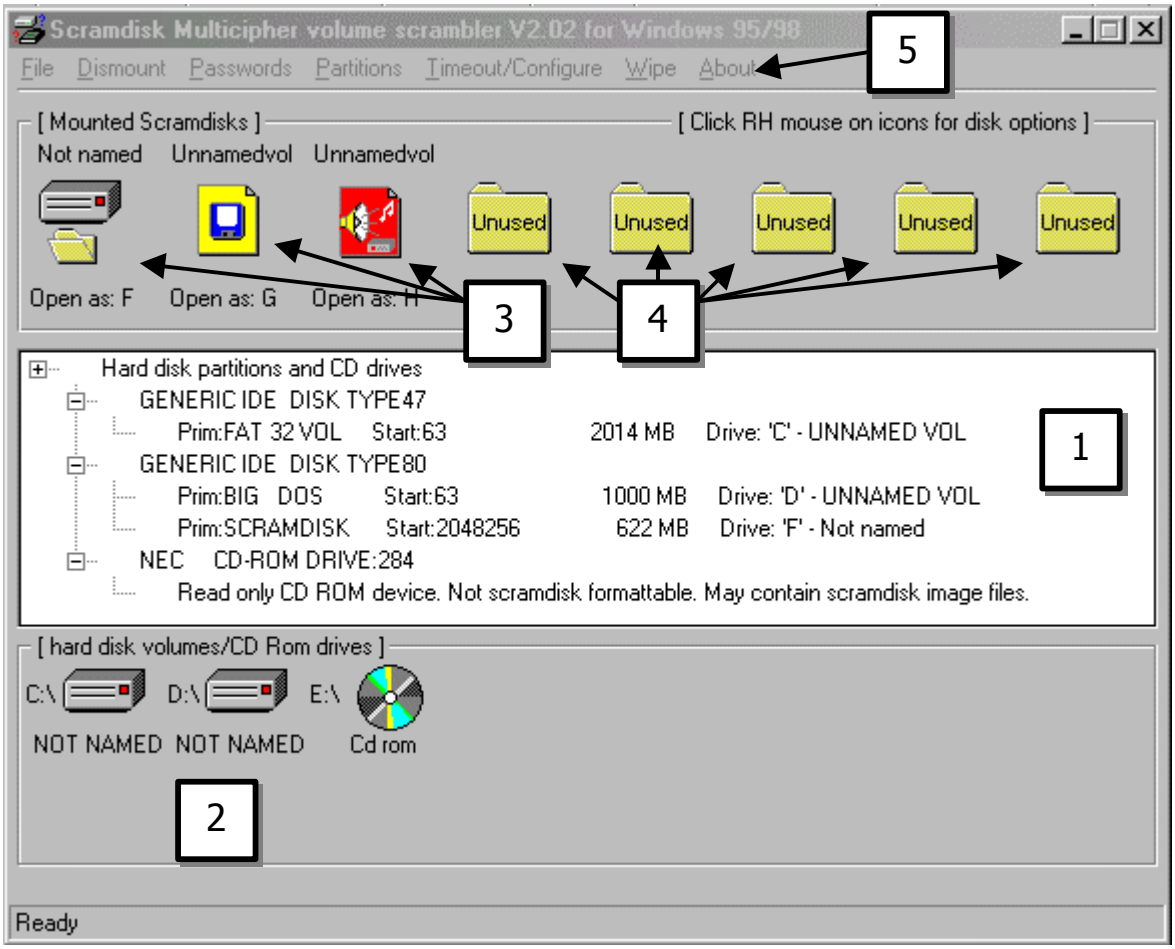
Le texte relatif à chaque élément figure en paragraphe indenté.

Donc la forme générale est:

ELEMENT DE MENU (gras, PETITES CAPITALES)

Description de l'élément. (indenté)

L'Ecran Principal



Légende:

1 Cette zone affiche les périphériques attachés au système. Pour formater une partition comme partition ScramDisk, double-cliquez simplement dessus. Attention! Cela détruira toutes les données se trouvant dans cette partition! Depuis la v2.02g, cette zone est, par défaut, cachée. Affichez cette zone en sélectionnant l'option correspondante dans la boîte de dialogue Configure.

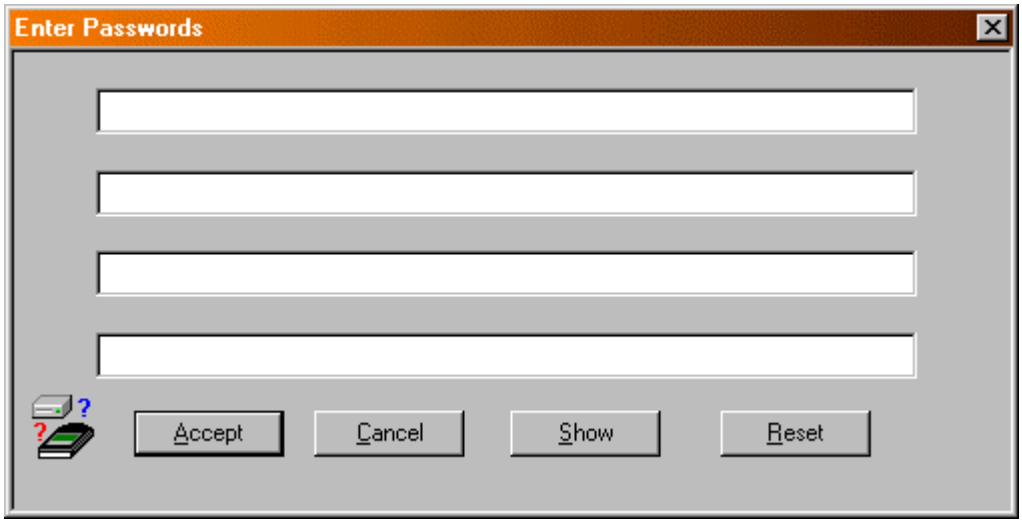
2 Cette zone affiche les 16 premiers Disques Durs et CD ROMs attachés au système.
Cliquer sur une icône ouvre ce volume.
Cliquer du bouton droit sur une icône ouvre ce volume dans une fenêtre d'Explorateur.

3 Cette zone montre les volumes ouverts et les slots disponibles.

4 L'exemple [3] montre 3 volumes ouverts (une partition, un fichier conteneur et un conteneur stéganographique wave, respectivement). L'exemple [4] montre 5 slots vides.
Cliquer sur un slot vide affiche l'écran de saisie des mots de passe, préparant le slot à accueillir le volume à ouvrir.
Cliquer sur un slot occupé ouvre le volume.
Cliquer du bouton droit sur un slot occupé affiche la fenêtre volume info.

5 Menus.
Voir les pages suivantes pour les descriptions individuelles.

Ecrans Password et Confirm Password



[Mots de passe des volumes]:

Cette partie comporte 4 zones de saisie de texte, pour saisir votre phrase secrète; vous pouvez utiliser autant de lignes qu'il vous faut, dans la limite de 4.

Utilisez le(s) touche(s) **Tab** et **Maj+Tab** pour vous déplacer entre les 4 zones de saisie de texte.

Boutons:

Accept	Sauvegarde les mots de passe saisis et ferme cette boîte de dialogue.
Cancel	Ferme cette boîte de dialogue sans rien faire.
Show	Bascule entre l'affichage des mots de passe sous forme d'astérisques ou de texte visible.
Hide	
Reset	Efface toutes les zones de texte.

N.B. A l'exception du titre de la fenêtre dans la barre de titre, les écrans Confirm Passwords et keyfile Password sont identiques à l'écran Password.

L'Ecran Rouge de Bas Niveau des Messages

Cette fonctionnalité est conçue pour faire échec à tout programme ou processus de copie ou d'enregistrement subreptice des frappes clavier sous Windows.

Si elle est activée dans "**Configure**", cette fonctionnalité prévaut sur les écrans Windows normaux de saisie des mots de passe.

A la place sera affiché un écran rouge, dans le vieux style graphique CGA.

Cet écran a exactement la même fonction que les écrans de saisie des mots de passe, à ceci près que des touches remplacent les boutons suivant le tableau de correspondance suivant:

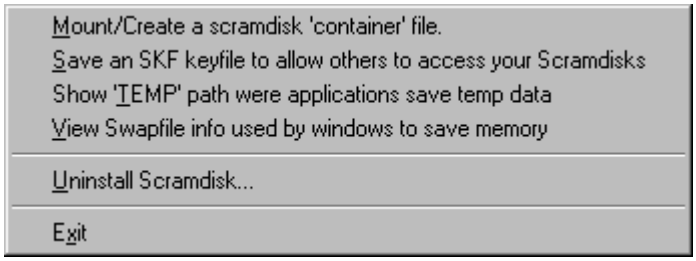
Touche	Bouton
Entrée	Accept
PgDn	Show
PgUp	Hide
Esc	Cancel
Origine	Reset

En plus des touches ci-dessus, F1 entre un | (barre verticale) et F2 entre un # (dièse).

Cette fonctionnalité ne devrait pas être utilisée lorsque le clavier utilisé n est pas un clavier QWERTY standard (par ex. un clavier français).

Description des menus

File



MOUNT/CREATE A SCRAMDISK 'CONTAINER' FILE:

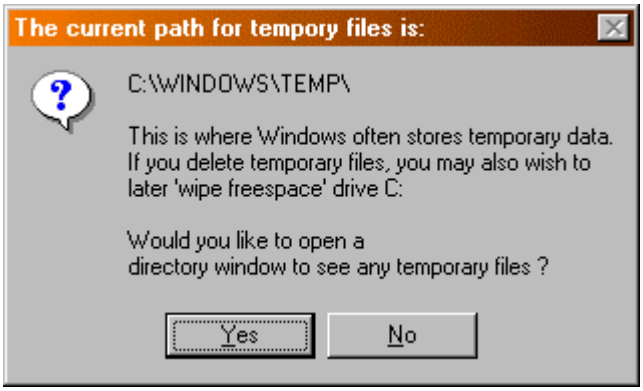
Utilisé pour créer un nouveau volume crypté ou pour ouvrir ceux déjà créés. Voir 'Ouvrir un Volume crypté' pour les détails.

SAVE AN SKF KEYFILE TO ALLOW OTHERS TO ACCESS YOUR SCRAMDISKS:

Voir les chapitres " Accès d'un 2ème Utilisateur".

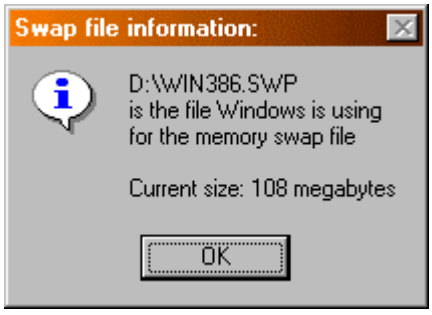
SHOW 'TEMP' PATH WHERE APPLICATIONS SAVE TEMP DATA:

Affiche le chemin d'accès au répertoire dans lequel les applications écrivent les données temporaires (défini par la variable d'environnement TEMP), et vous permet de l'examiner.



Les données écrites là ne sont pas cryptées, ce qui les expose donc au risque d'une possible capture.

VIEW SWAPFILE INFO USED BY WINDOWS TO SAVE MEMORY:



Windows 'pagine' sur le disque les données en mémoire non immédiatement utilisées, le disque étant utilisé comme une zone mémoire supplémentaire dite 'Mémoire Virtuelle'.

Les données écrites dans le fichier d'échange de 'mémoire virtuelle' ne sont pas cryptées, ce qui les expose donc au risque d'une possible capture.

Voir aussi le menu **Wipe** pour l'aide sur la destruction des résidus du fichier d'échange.

UNINSTALL SCRAMDISK:

Efface complètement le programme et le pilote ScramDisk de l'ordinateur.

EXIT:

Quitte ScramDisk, en vous offrant de vider le cache des mots de passe s'il y a lieu.

N.B. Vos volumes cryptés demeurent accessibles jusqu'à ce que vous redémarriez Windows ou utilisiez ScramDisk pour les fermer.

Dismount

DISMOUNT ALL:

Ferme tous les volumes ouverts.

DISMOUNT BRUTAL:

Ferme brutalement tous les volumes ouverts.

Voir “Fermer des Volumes Cryptés” pour plus d’informations.

Passwords

ENTER CIPHERED DISK VOLUME PASSWORDS:

Affiche la boîte de dialogue pour saisir votre phrase secrète pour ouvrir ou créer un Volume Crypté.

ENTER KEYFILE PASSWORD (SKF ACCESS FILES):

Affiche l'écran Password pour saisir la phrase secrète que vous utiliserez pour limiter l'accès via un Fichier Clé.

Voir les chapitres "**Accès d un 2ème Utilisateur**", pour les instructions d'utilisation.

CLEAR ALL PASSWORDS CACHED IN DRIVER ETC:

Efface toute phrase secrète conservée en mémoire par le composant VxD et l'interface ScramDisk.

N.B. Si "**Enter all passwords in low level RED message mode**" est activé, les deux premiers éléments de ce menu l'utiliseront plutôt que les fenêtres normales des écrans Password.

Partitions

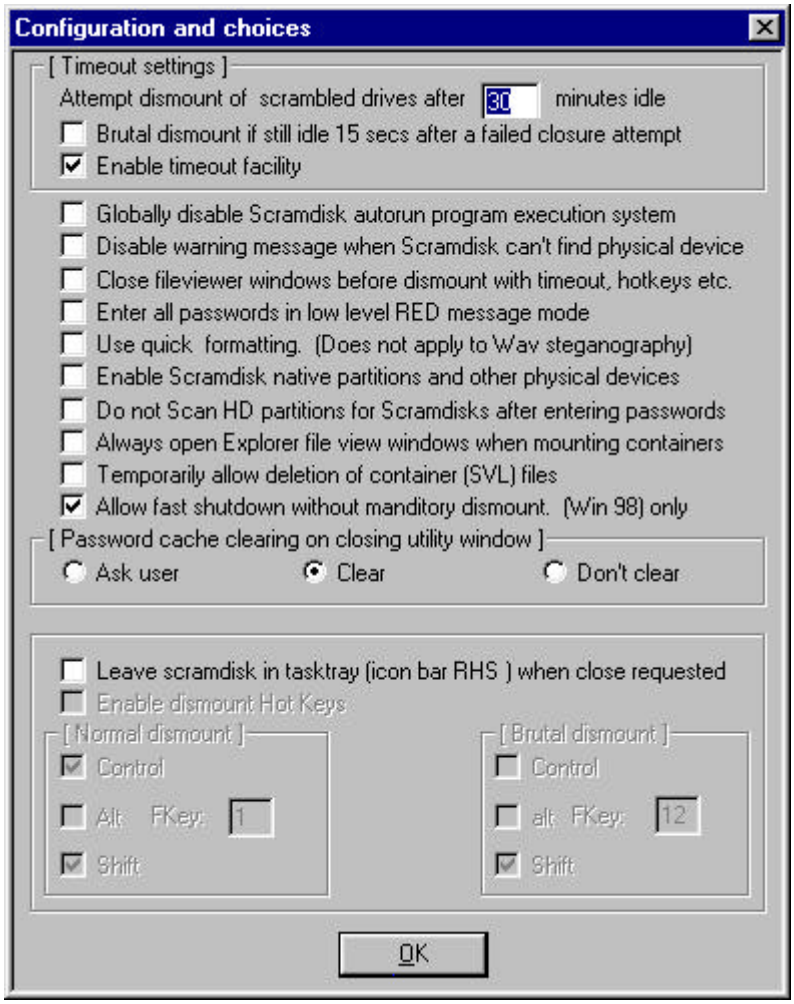
REMOUNT/REFRESH:

Met à jour la fenêtre Device / Partition et indique à ScramDisk d'essayer d'ouvrir toute(s) Partition(s) Cryptée(s) dont la phrase secrète est en cache.

Configure

CONFIGURE SCRAMDISK:

Appelle la boîte de dialogue de configuration du délai d'attente et d'autres réglages.



Voir les chapitres correspondants:

"**Utiliser la Fonction de Délai d Attente**" pour une description de la plupart de ces réglages.

"**Créer un volume crypté**" pour l'utilisation de "**Use quick formatting (Does not apply to Wav steganography)**".

Voir "**Description des Ecrans et des Menus**" à propos de "**L Ecran Rouge de Bas Niveau des Messages**" pour explications sur les effets de la fonction "**Enter all passwords in low level RED message mode**".

Globally disable ScramDisk autorun program execution system

Désactive la fonction de lancement automatique présente dans la v2.02h.

DISABLE WARNINGS WHEN SCRAMDISK CAN T FIND PHYSICAL DRIVE:

Habituellement ScramDisk vous avertit que la présence du périphérique physique ne peut pas être vérifiée, ce qui n'est pas un problème si le disque se trouve sur un disque dur local. Si le volume ScramDisk se trouve sur un lecteur réseau ou un support amovible, ScramDisk affiche un avertissement. Cette option désactive l'avertissement et a été ajoutée à la demande de plusieurs utilisateurs.

CLOSE FILEVIEWER WINDOWS BEFORE DISMOUNT WITH TIMEOUT, HOTKEYS ETC:

Cochez cette option pour fermer automatiquement toutes les fenêtres affichant le contenu des volumes cryptés lorsque les conteneurs sont fermés après expiration d'un délai ou par raccourcis clavier.

Use quick formatting:

Cochez cette option si vous ne voulez pas que ScramDisk nettoie le disque avant que vous l'utilisiez. Cela accélère le formatage, mais peut ne pas être sûr car les fichiers existants pourraient être retrouvés.

ENABLE SCRAMDISK NATIVE PARTITIONS AND OTHER PHYSICAL DEVICES:

Désactivé par défaut. Activez cette option pour visualiser les partitions physiques connectées à l'ordinateur.

DO NOT SCAN HD PARTITIONS FOR SCRAMDISKS AFTER ENTERING PASSWORDS:

Dit à ScramDisk de ne pas effectuer une recherche de toutes les partitions existantes quand vous saisissez une nouvelle phrase secrète.

ALWAYS OPEN EXPLORER FILE VIEW WINDOWS WHEN MOUNTING CONTAINERS:

Quelquefois, Windows 95 ou 98 ouvre une fenêtre d'Explorateur (quand on double-clique sur un conteneur depuis une fenêtre ouverte, par exemple). Cette fonctionnalité vous permet de contraindre ScramDisk à se comporter de manière consistante au regard du mécanisme utilisé pour ouvrir le conteneur.

TEMPORARILY ALLOW DELETION OF CONTAINER (SVL) FILES:

Depuis la v2.02g, ScramDisk dispose d'une fonctionnalité empêchant l'effacement accidentel des fichiers SVL. Si vous avez vraiment besoin d'effacer un fichier conteneur, cochez cette case, effacez le fichier, et ensuite décochez cette case.

ALLOW FAST SHUTDOWN WITHOUT MANDITORY DISMOUNT (WIN 98) ONLY:

Cette fonctionnalité vous permet d'éteindre votre ordinateur sous Windows 98 sans avoir à fermer préalablement tous les volumes ScramDisk. Elle est sans effet sous Windows 95, sous lequel vous ne pouvez pas éteindre sans risque si des volumes sont ouverts.

[PASSWORD CACHE CLEARING ON CLOSING UTILITY WINDOW]:

Vous permet de spécifier la manière dont ScramDisk efface les phrases secrètes de son cache lorsque l'utilitaire est fermé.

LEAVE SCRAMDISK IN TASKTRAY (ICON BAR RHS) WHEN CLOSE/EXIT REQUESTED:

ScramDisk affiche son icône dans la barre des tâches après avoir été fermé. Cette option doit être cochée pour permettre la fermeture par raccourci clavier.

Wipe

FREE SPACE:

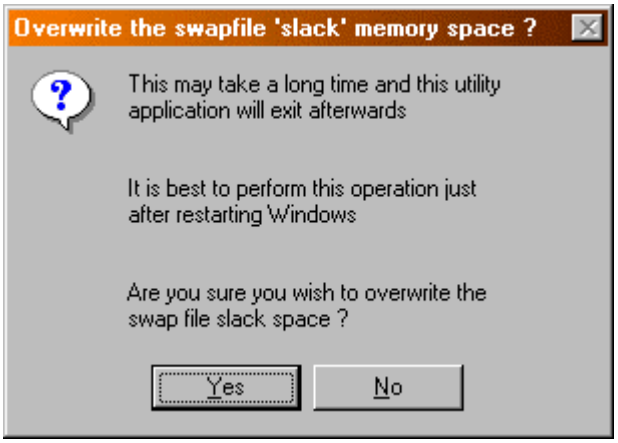
ScramDisk écrit des données aléatoires sur tout l'espace libre du disque. Cele empêche la restauration des données à partir des résidus des fichiers effacés.

Vous pouvez spécifier le lecteur sur lequel ScramDisk procédera au nettoyage (wipe) et le nombre de fois qu'il répétera l'opération (c-à-d les passes).

Habituellement, les données des fichiers effacés restent toujours physiquement présentes sur le disque, dans l'espace considéré comme libre après leur effacement.

Le nettoyage (wipe) de l'espace libre garantit que les fichiers préalablement effacés ne pourront pas être récupérés par Undelete ou par un éditeur de secteurs de disque.

OVERWRITE SWAPFILE SLACK:



Tout résidu résultant d'une réduction de la taille du fichier d'échange peut contenir des données, l'écriture par dessus ces résidus les efface de manière irréversible.

About

ABOUT:

Attributions et informations de Version.

REVIEW LICENCE:

Une occasion de lire et de confirmer à nouveau ou de refuser la licence d'utilisation que vous aviez agréée en utilisant ce logiciel.

CIPHER VERIFIER:

Appelle un utilitaire vous permettant de vérifier que les algorithmes utilisés par ScramDisk produisent le même texte crypté que les réalisations 'reconnues' publiées par ailleurs.

Voir à ce propos le chapitre 'Vérifier les Algorithmes Utilisés'.

Attaques Théoriques contre ScramDisk

Introduction

Il existe deux types d'attaques qui peuvent être employées contre la plupart des cryptosystèmes modernes:

i) Une Attaque par Dictionnaire. Elle consiste à essayer toutes les expressions d'un dictionnaire contre le conteneur. Si le mot de passe se trouve dans le dictionnaire, l'attaquant "décroche le jackpot ".

ii) Une Attaque par Force Brute. Elle consiste à essayer tous les mots de passe possibles contre un conteneur ScramDisk. C'est une tentative **très** longue, comme nous le verrons plus loin.

Cette partie de la documentation discute la faisabilité d'une telle attaque contre ScramDisk.

Q: Est-il plus faible que PGPDisk / BestCrypt etc?

R: Non. En fait, ceci confirme ce que nous supposions: SD est *plus résistant* contre une attaque par force brute que ces programmes. Chaque essai de mot de passe dans ScramDisk demande approximativement 0,5 seconde (sur un P166) – c'est très long pour une attaque par Force Brute.

Q: Pourquoi estimez-vous que ces attaques sont "difficiles" contre SD?

R: Les conteneurs ScramDisk ne contiennent aucune information sur l'algorithme de cryptage utilisé pour les crypter. Chaque fois que vous essayez d'ouvrir un conteneur, voici ce qui se passe (au minimum):

a) 1x SHA-1 de la phrase secrète
b) Et pour chacun des algorithmes (il y en a 9 actuellement):
    i) 1x initialisation de l'algorithme par blocs
    ii) 2x décryptage par l'algorithme par blocs

Pour certains algorithmes par blocs (e.g. BlowFish) le coût [temps de mise en place] de la phase d'initialisation est très important.

Dans la plupart des programmes de cryptage de disque, le volume crypté contient une indication sur l'algorithme utilisé – ce qui facilite les attaques par force brute.

Q: A quel point ces attaques sont-elles (im)praticables?

R: Cela dépend de votre imagination dans le choix de vos phrases secrètes ☺ Si vous avez utilisé une phrase secrète de qualité raisonnable (voir la question suivante!) alors cette attaque n'a absolument aucune chance d'aboutir. Voici quelques exemples d'attaques[1]:

Attaque par Dictionnaire:

100,000 mots contre une phrase secrète d'une ligne = 1 seconde
100,000 mots contre une phrase secrète de 2 lignes = 1 jour
100,000 mots contre une phrase secrète de 3 lignes = 300 ans
100,000 mots contre une phrase secrète de 4 lignes = 3 Millions d'années

Attaque par Force Brute (contre une seule ligne):

7 caractères (la taille minimum d'une phrase secrète) alphabétiques minuscules = 22 heures
7 caractères (la taille minimum d'une phrase secrète) alphabétiques = 7 ans

[1] L'exemple proposé suppose 10.000x PII 450Mhz en parallèle et chacun d'eux effectuant 100 essais par seconde (ce qui est très optimiste – un P166 ne peut en faire que 2 par seconde!).

11 caractères alphabétiques = 3 Millions d'années

Il est donc évident que, même avec un matériel de rêve, une attaque contre une phrase secrète bien choisie est impraticable.

Q: Quelle sorte de phrase secrète pourra être trouvée avec ces attaques?

R: Des phrases secrètes courtes, contenant seulement des mots figurant dans le dictionnaire & celles construites à partir d'un alphabet réduit. Voir "Q: Qu'est-ce qui fait qu'une phrase secrète est bonne?" dans la FAQ pour des détails sur la manière de choisir une "bonne" phrase secrète.

Q: Un système peut-il être conçu de manière à pouvoir résister à coup sûr à une attaque par Force Brute ou par Dictionnaire?

R: On peut classer les informations relatives à la sécurité en deux groupes:

i) Sécurité offerte par des procédés cryptographiques.
ii) Sécurité offerte par le secret.

Un procédé courant pour combattre une attaque par Dictionnaire ou par Force Brute consiste à insérer une boucle retardatrice dans le code qui teste un mot de passe / phrase secrète. Le remplacement de cette partie du code par une autre tourne aisément cette "sécurité" – par conséquent, aucune sécurité réelle n'est donnée par l'inclusion de cette boucle.

Une réelle sécurité, telle qu'elle est offerte dans SD, ne peut pas être circonvenue par ce biais: SD n'emporte aucune information sur l'algorithme utilisé pour crypter le disque (comme le fait BestCrypt, un "concurrent" de SD). Ainsi, fondamentalement, pour chaque phrase secrète que vous voulez essayer, vous devez procéder à plusieurs opérations: 1x SHA-1, 1x initialisation & 2x décryptage POUR CHAQUE ALGORITHME (il y a 9 algorithmes).

Par conséquent, les attaques précédemment mentionnées sont DE LOIN plus difficiles contre SD que contre PGPDisk, BestCrypt et autres. Nous estimons que SD est plus de 10 fois plus difficile à attaquer par force brute que ses concurrents.

Survol Technique

Le Processus de Cryptage

Le processus de création d'un disque crypté est indépendant de l'algorithme choisi. Tous les conteneurs sont créés de la manière suivante. A l'ouverture d'un disque (on suppose, pour simplifier, qu'un seul algorithme est disponible) voici ce qui se passe:

1. Les premiers 2048 octets du conteneur sont lus dans un tampon.

2. Le mot de passe (jusqu'à 160 octets de texte et en supposant qu'il est correct) est haché par SHA-1, qui en donne une empreinte.

3. L'algorithme de cryptage choisi est initialisé avec la clé constituée par l'empreinte obtenue avec SHA-1 en (2).

4. Les 2048 octets lus dans le tampon en (1) sont alors déchiffrés avec l'algorithme choisi initialisé avec l'empreinte.

5. La CLE PRINCIPALE (jusqu'à 256 bits) stockée dans le tampon + 1024 est récupérée. Cette valeur a été déchiffrée à l'étape (4) avec le reste.

6. L'algorithme choisi est réinitialisé avec [la clé constituée par] le sous-ensemble adéquat de bits récupérés en (5) (256 pour Blowfish etc.). C'est cette clé-là qui est maintenant utilisée pour décrypter le disque entier.

7. Deux secteurs qui avaient été remplis avec des données aléatoires identiques (cryptés avec la CLE PRINCIPALE au moment du formatage, comme l'ont été toutes les zones de données) sont lus et décryptés avec la clé principale et les vecteurs d'initialisation (IV) etc.

8. Si ces deux secteurs donnent alors des données identiques, on peut en conclure que le couple CLE/IV est le bon, et Windows est appelé pour initialiser le disque. Si ce n'est pas le cas, le pilote s'en retourne sans rien faire.

9. Si tout se passe bien, Windows voit un nouveau disque, auquel les accès passeront par le pilote virtuel sd.VxD via les DCB pour le nouveau périphérique. Les "appels" dans les DCB recourront au code correct pour décrypter tous les secteurs concernés etc.

Ainsi, pour résumer: Votre phrase secrète hachée avec SHA-1 ouvre 2 zones du disque. Une zone contenant les valeurs aléatoires qui seront utilisées pour les IV et le "pré-blanchiment"[2]. Une autre zone totalement distincte qui contient la clé servant au cryptage ou au décryptage des secteurs du disque. Cette clé est alors utilisée comme clé de l'algorithme de cryptage conventionnel. La même clé est utilisée pour tous les secteurs du disque, ce qui n'a pas d'importance dès lors qu'un IV différent est utilisé pour chaque secteur.

Les deux zones de données aléatoires n'ont absolument aucun lien entre elles.

[2] Comme expliqué dans Applied Cryptography 2nd Ed, p. 366 [ouvrage traduit en français (2ème édition) aux Editions O'Reilly, 1997]

Algorithmes de Cryptage Intégrés

> "*The irony of the Information Age is that it has given new respectability to uninformed opinion.*"
> --John Lawton

ScramDisk intègre un certain nombre d'algorithmes dans cette version. Tous les Algorithmes sont utilisés en mode CBC utilisant une valeur aléatoire comme IV. De plus, une autre valeur aléatoire est utilisée pour brouiller le lien entre le texte clair et le texte crypté (ce processus est appelé 'pré-blanchiment'). Les algorithmes sont les suivants:

- **3DES**. Il est bien meilleur que DES; il applique 3 fois l'algorithme DES en mode EDE (Encipher-Decipher-Encipher) avec des clés totalement indépendantes. Outer-CBC est utilisé. Cet algorithme est considéré comme très sûr (de grandes banques l'utilisent pour protéger de très importantes transactions) mais il est aussi très, très lent.

- **Blowfish**. C'est un algorithme de cryptage de haute sécurité conçu par Bruce Schneier, auteur de Applied Cryptography et dirigeant de la société Counterpane. Cet algorithme est très rapide, est considéré comme sûr et est résistant à la cryptanalyse linéaire et différentielle. Personnellement, c'est mon préféré. NOTE: ScramDisk utilise le code Blowfish exempt de bogue.

- **DES**. C'est l'algorithme Data Encryption Standard conçu au début des années 1970 par IBM (avec implication de la NSA). Il est OK, mais une clé peut être cassée en 3 jours par une organisation sans grands moyens (l'EFF!) ☹. Cet algorithme est offert dans le souci d'être complet, mais il est assez lent et considéré comme faible en raison de la taille de la clé.

- **IDEA**. C'est un algorithme réalisé par Xuejia Lai & James Massey. Il est assez rapide et considéré comme sûr. Il est aussi résistant à la cryptanalyse linéaire et différentielle. Tout usage autre que strictement personnel impose de payer des royalties à Ascom. Voir les détails de licence à ce sujet plus loin dans ce document.

- **MISTY1**. C'est un algorithme conçu par M. Matsui de Mitsubishi. Il est raisonnablement rapide et est résistant à la cryptanalyse linéaire et différentielle. Il est cependant assez récent, aussi utilisez-le avec précaution.

- **Square**. Square est un algorithme de cryptage par blocs très rapide et raisonnablement sûr réalisé par John Daemen et Vincent Rijmen. Il n'a pas fait l'objet d'un examen aussi étendu que Blowfish, 3DES, IDEA etc. et peut être l'objet d'attaques.

- **Summer**. C'est un algorithme propriétaire de cryptage par flux réalisé par l'auteur. Il est conçu pour la seule rapidité. Il est fourni avec le programme pour des raisons de compatibilité avec la version 1 de ScramDisk et n'est pas recommandé pour créer de nouveaux disques. Utilisez plutôt TEA ou Blowfish, qui sont raisonnablement rapides.

- **TEA**. Tiny Encryption Algorithm est un algorithme très rapide et modérément sûr réalisé par David Wheeler et Roger Needham du Cambridge Computer Laboratory. Il existe une faiblesse identifiée dans la mise en place de la clé aussi n'est-il pas recommandé si la sécurité est la considération principale. TEA est fourni en deux versions, 16 & 32 rondes. 32 rondes sont évidemment plus sûres que 16, mais ce sera aussi plus lent.

Sommaire des Algorithmes

Le tableau suivant détaille les performances des différents algorithmes:

Algorithme	Auteur	Réalisation	Taille Blocs (bits)	Taille Clé (bits)	Vitesse (ms)
3DES (3-clés, EDE)	Diffie & Hellman	Assembleur	64	168	4:05
Blowfish	B.Schneier	C	64	256	0:55
DES	IBM & NSA	Assembleur	64	56	1:42
IDEA	Xuejia Lai & J.Massey	Assembleur	64	128	1:07
MISTY1	M.Matsui	C	64	128	2:50
Square	J.Daemon & V.Rijmen	C Optimisé & ASM	128	128	0:39
Summer (Flux)	Aman	Assembleur	N/A	128	0:31
TEA (16 Rondes)	D.Wheeler & R.Needham	Assembleur	64	128	0:46
TEA (32 Rondes)	D.Wheeler & R.Needham	Assembleur	64	128	1:03

La colonne 'Vitesse' illustre les performances pour tous les algorithmes. Les temps ont été mesurés en copiant un fichier de 50 Mo d'un disque normal sur un disque ScramDisk sur un Pentium 166 Mhz. La copie du même fichier d'un disque normal sur un autre disque normal (c-à-d un volume non crypté) a pris 28 secondes.

Foire Aux Questions (FAQ)

Q: Que puis-je stocker sur mon ordinateur avec ScramDisk?
R: Tout ce que vous pouvez conserver sur n'importe quel autre disque sous Windows, à l'exception des fichiers images ScramDisk. Ils ne peuvent pas être eux-mêmes stockés de manière récursive sur d'autres disques ScramDisk. Autrement programmes, données, n'importe quoi.

Q: Qu'est-ce que la licence d'utilisation signifie en bon français?
R: Plusieurs questions ont été soulevées au sujet de la signification précise de la licence d'utilisation. Ce qui suit devrait aider à clarifier la question. Les personnes physiques et les sociétés peuvent utiliser ScramDisk pour protéger leurs données dans les conditions suivantes:

i) Le logiciel n'est pas proposé à titre onéreux par quiconque et/ou pour quiconque.
ii) Le logiciel n'est pas employé pour crypter des données, quelles qu'elles soient, proposées à la vente.
iii) Nous n'assumons aucune responsabilité pour toute perte, de données ou autres, qui pourrait survenir.
iv) IDEA nécessite une licence pour l'utilisation commerciale.

Fondamentalement, nous ne voulons pas que quiconque fasse de l'argent avec le fruit de notre propre labeur, ou celui des développeurs ou des intégrateurs des algorithmes.

Q: Comment quelqu'un peut-il savoir si ScramDisk est installé?
R: Les modifications (indispensables) suivantes sont apportées au système:

- Le fichier "C:\windows\system\ioSubSys\sd.vxd" est ajouté. C'est le pilote logiciel.
- Le fichier "C:\windows\scramdisk.ini" est ajouté. Il contient les paramètres de configuration.
- Le fichier "*chemind'installation*\scramdisk.exe" est ajouté. C'est l'exécutable.

Q: Quel est le meilleur algorithme de cryptage?
R: Je ne sais pas! En fait, personne ne sait. Certains algorithmes sont certainement reconnus comme étant "faibles" (e.g. ils succombent à des attaques publiées). Le fait qu'un algorithme ne succombe devant aucune attaque connue ne signifie pas pour autant que sa force est "prouvée" – mais simplement qu'elle l'est par rapport aux algorithmes "faibles". On considère d'ailleurs qu'il est improbable que la force d'un algorithme de cryptage puisse être prouvée prochainement[3].

Disant cela, je crois utile de donner quelques indications aux utilisateurs:

- 3DES est considéré comme extrêmement fort, mais peut-être trop lent pour être utilisé pour tous les disques cryptés.
- IDEA et Blowfish sont de bons choix – ils sont tous deux considérés comme sûrs contre toutes les attaques connues.
- Personnellement j'aime Blowfish à cause de sa grande taille de clé, sa vitesse très acceptable, l'absence de problèmes de droits d'utilisation et sa robustesse face aux attaques.
- IDEA nécessite une licence pour l'utilisation commerciale. Voir le chapitre "IDEA Conditions d'utilisation et avis imposé" en page 63 pour les détails.
- Summer est faible.
- TEA, Square & MISTY1 sont OK mais ils sont relativement récents.
- DES est certainement faible contre un adversaire déterminé (en raison de sa petite taille de clé).

[3] Extrait de la documentation de TwoFish: "toute preuve raisonnable de la sécurité d'un algorithme de cryptage par blocs prouverait aussi P ≠ NP"

Q: Qu'est-ce que c'est que cet horrible "écran rouge" dans lequel je dois taper les mots de passe?

R: Cet écran est un mécanisme de ***très*** bas niveau fourni dans Windows 95 qui est habituellement utilisé pour afficher des messages d'erreurs critiques. En entrant un mot de passe dans cet écran, plutôt que dans celui de la fenêtre normale des mots de passe, vous empêchez certains programmes "sniffeurs", comme Skin98, de lire les frappes clavier lors de la saisie de votre phrase secrète.

Q: Quelle sorte de "disque" Windows voit-il sur un disque ScramDisk?

R: Windows "voit" un disque FAT16 normal dans tous les cas. Les données peuvent être en réalité stockées sur une partition, ou dans un fichier [formaté] en FAT32 ou FAT16, dans un fichier CD en CDFS, même à l'autre bout d'un réseau.

Q: Si je crée un disque virtuel avec ScramDisk, puis-je le défragmenter et le réparer comme d'autres disques FAT?

R: Defrag peut être exécuté sur un disque "Scramdisk" exactement de la même façon que sur n'importe quel disque normal. Scandisk peut être exécuté pour réparer toute structure de fichiers DOS éventuellement endommagée, exactement comme un disque normal. Le système ne sait vraiment pas qu'il ne s'agit pas d'un disque normal!

Q: Qu'en est-il de la gestion de la FAT32?

R: La gestion de la FAT32 par ScramDisk est limitée: il est possible de créer un fichier volume ScramDisk sur un disque formaté en FAT32, mais il n'est pas possible d'y créer un volume FAT32. Pour l'instant, tous les conteneurs ScramDisk doivent être formatés en FAT16 – ce qui limite la taille maximum des volumes ScramDisk à 2 Go.

Q: Où les mots de passe sont-ils conservés sur le disque?

R: Ils n'y sont pas. Le disque est ouvert de façon statistique, et non pas en comparant des mots de passe. Il y a deux secteurs sur le disque contenant les mêmes données (générées aléatoirement) cryptés avec des clés différentes. Les données de ces secteurs lues avec un mauvais mot de passe apparaissent différentes. Seul le bon mot de passe donne la paire de clés (une pour chaque secteur) qui permettent de lire les mêmes données dans les deux secteurs, et d'authentifier le mot de passe.

Q: N'importe qui peut-il voir les noms des fichiers que j'ai mis sur le disque, lorsqu'il est inaccessible?

R: Non. Le secteur de boot, les répertoires, la Table d'Allocation des Fichiers, et les données sont tous cryptés avec l'algorithme de votre choix.

Q: Comment puis-je sauvegarder mes fichiers, stockés sur des disques ScramDisk?

R: Comme vous le faites habituellement. Cependant, s'ils doivent demeurer en sécurité, vous devrez les sauvegarder sur un second disque ScramDisk. Ouvrez simplement les deux disques, et déplacez les fichiers de l'un à l'autre dans Windows. Une autre façon de procéder est de sauvegarder le volume crypté en entier.

Q: Pourquoi ScramDisk ne fonctionne-t-il pas avec le programme X?

R: ScramDisk *devrait* fonctionner avec tous les programmes, mais il existe des problèmes particuliers avec certains programmes, par exemple avec JBN. 9 fois sur 10, les utilisateurs qui se plaignent de rencontrer des problèmes avec ScramDisk font en réalité des manipulations erronées, par exemple:

1. En essayant de créer trop de fichiers dans le répertoire racine d'un disque.

2. En essayant de faire quelque chose avec un fichier en lecture seule.

Evidemment, ces mêmes erreurs se produiraient avec n'importe quel type de disque. SVP, veuillez informer l'auteur de tout problème particulier avec certains programmes.

Q: ScramDisk fonctionne-t-il avec DOS?
R: ScramDisk est un pilote VxD Windows, avec un utilitaire Win32. Il fonctionnera parfaitement bien à partir de la ligne de commande DOS sous Windows, et permet d'utiliser des programmes DOS pour accéder à ses disques de la manière habituelle mais, naturellement, il ne fonctionnera que si Windows 95 est le système d'exploitation sous-jacent [et donc pas en mode MSDOS].
Il existe une version DOS de ScramDisk, mais elle ne permet de lire que des partitions ScramDisk et non des fichiers hôtes.

Q: Dois-je laisser tourner l'utilitaire "Scramdisk.exe" sur le Bureau quand j'utilise mes disques ScramDisk?
R: Non. Le pilote VxD "SD.vxd" installé dans le répertoire "..\system\iosubsys" fait tout le travail. A moins que vous souhaitiez fermer des disques ou en ouvrir de nouveaux, vous pouvez fermer l'utilitaire lorsque vous en avez fini avec lui.

Q: Pourquoi ne fonctionne-t-il pas sous Windows NT?
R: Windows NT utilise un modèle de pilotes complètement différent, appelé Kernel Mode Driver (KMD) qui requiert une base de connaissances différentes pour programmer. Windows 95/98 utilise "VxDs" et "IOS" pour les pilotes de disques. Ils sont complètement différents et incompatibles. Espérons qu'une bonne âme s'intéressera au sujet et aidera à réaliser une version NT. Le nouveau Windows Driver Model qui s'annonce avec NT v5 & Windows 98 ne sera d'aucun secours, puisqu'il ne concerne que les pilotes d'affichage & multimedia.

Q: Que faire si j'oublie ma phrase secrète?
R: Considérez que vous avez perdu vos données! Ce ne serait pas un système très sûr si je pouvais vous dire comment les retrouver[sans elle], non?

Q: Qu'est-ce qui fait qu'une phrase secrète est bonne?
R: Plusieurs conseils peuvent être donnés aux utilisateurs qui ont à choisir une phrase secrète:

1. Faites-en une aussi longue que possible. Elle peut avoir jusqu'à 39 caractères par ligne et il y a 4 lignes – par conséquent, elle peut faire jusqu'à 156 caractères.

2. Essayez d'utiliser aussi bien des lettres majuscules que minuscules.

3. Incluez-y aussi bien des chiffres que des caractères de ponctuation, tels que ; : , . ! " £ etc.

4. Essayez d'éviter de choisir un simple mot ou une expression célèbre – cela rendrait possible une attaque par dictionnaire.

Avec ScramDisk, entreprendre une attaque par dictionnaire est une tâche ardue et demande des délais considérables – pour chaque mauvais mot de passe essayé, les opérations suivantes doivent être effectuées: 1x SHA-1 suivie de 1x initialisation et de 2x décryptages de bloc **pour chaque algorithme** – et cela parce que l'algorithme utilisé pour crypter chaque disque n'y est pas stocké.

Q: Au secours! Des parties de ma phrase secrète apparaissent dans le volume crypté!?
R: Statistiquement, c'était prévisible. Par exemple, si vous créez un volume crypté de 100 Mo, il faut s'attendre à ce que chaque combinaison de 3 caractères (par ex. AAA, AAB, AAC, etc.) se rencontre approximativement 16 fois: $(100*1024*1024)/256^3$. Donc, la phrase secrète des utilisateurs a de fortes chances d'apparaître dans des blocs de 3 lettres dans le volume crypté.

Cela arrive parce que les données cryptées ressemblent à des nombres aléatoires – il serait possible pour ScramDisk de vérifier et de s'assurer que des parties de la phrase secrète n'y figurent pas – mais cela faciliterait une cryptanalyse. Puisque $(16*1024*1024)/256^3=1$, vous pouvez vous attendre, en moyenne, à trouver toutes les combinaisons possibles de 3 caractères dans un fichier de 16 Mo.

Vous seriez en droit vous alarmer si des groupes de 5 caractères de votre phrase secrète étaient trouvés dans le volume – mais la probabilité pour que cela se produise est extrêmement faible.

Q: Comment se fait-il que chaque disque que je crée apparaisse différent des autres, même avec le même mot de passe, le même algorithme et les mêmes données?

R: Vous ne créerez jamais la même table de clé principale. La probabilité pour que cela se produise est infime. C'est cette table de clé principale qui est cryptée avec votre mot de passe et la table décryptée qui (dé)crypte les données sur votre disque. Il n'y a pas deux tables de clé principale identiques –sauf si vous copiez un fichier hôte ScramDisk ailleurs.

Q: Y a-t-il quelque chose que je ne devrais pas faire?

R: Ne copiez pas des fichiers hôtes ScramDisk (ceux qui "contiennent" un disque ScramDisk) pour les utiliser parallèlement. Pour chaque nouveau disque que vous voulez créer, vous devriez plutôt passer par les voies normales de création de volumes ou de partitions fournies par l'utilitaire. Cela assure une plus grande sécurité. Si vous copiiez un fichier hôte et contiuiiez à l'utiliser, alors les deux disques opéreraient avec les mêmes valeurs d'IV et de pré-blanchiment (parce qu'ils ont les mêmes données aléatoires au début du disque), ce qui pourrait faciliter une cryptanalyse.

Q: Pourquoi le programme a-t-il été réalisé?

R: Pourquoi PGP a-t-il été réalisé? Pourquoi pas? Si nous avions réellement pensé que la cryptographie forte était de nature à mettre des vies en danger ou à menacer la sécurité nationale, nous nous serions sentis moralement obligés de renoncer à ce projet. Mais la vérité est qu'il n'y a pas d'argument convaincant, parmi ceux avancés par des dirigeants politiques, pour lequel la cryptographie forte ne devrait pas être produite, utilisée, diffusée et vendue.

Personnellement, j'aime assez l'analogie des 'clés'. Nous n'avons pas à donner au Gouvernement les copies des clés de notre domicile ou de notre bureau, alors pourquoi devrions-nous lui confier celles de nos données? Je ne vois pas d'inconvénient à ce que la police accède à mes données si elle agit sur réquisition judiciaire, de la même façon qu'elle peut pénétrer chez moi dans les mêmes conditions.

J'aime aussi l'argument de la 'carte postale' de Phil Zimmermann. Quand les gens envoient des lettres, ils utilisent des enveloppes pour s'assurer un minimum de protection; ils n'envoient pas de lettres sans enveloppe parce qu'ils n'ont pas à le faire. Envoyer des lettres sous enveloppe est universellement admis parce que tout le monde le fait. Tout le monde devrait avoir le droit d'utiliser la crypto forte.

La vraie raison pour laquelle les gouvernements américain (et anglais?) sont opposés à la crypto forte est qu'ils recueillent bien trop de renseignements par voie d'interception de communications pour permettre le développement de la crypto forte, qui rendrait leur besogne forcément plus difficile. Lisez Puzzle Palace et For the President's Eyes Only si vous ne nous croyez pas!

Moi-même et l'auteur du programme sommes des professionnels des Technologies de l'Information sans antécédents judiciaires (pas même une contravention pour infraction au Code de la route!). Nous ne sommes ni des "rebelles à la loi" ni des "anarchistes" – nous pensons simplement que le respect de la vie privée devrait être un droit et que la cryptographie forte devrait être accessible à tous ceux qui le veulent.

Nous n'approuvons en aucune façon l'utilisation de ScramDisk à des fins illicites.

Q: Quels autres logiciels similaires existent?

R: Bestcrypt de Jetico, et PGPDisk de Network Associates. Ils sont naturellement incompatibles entre eux, et utilisent des algorithmes de cryptage différents. BestCrypt utilise Blowfish / GOST/ DES, PGPDisk utilise CAST. ScramDisk (étant gratuit) est le moins cher. Jetico ne produit pas le code source de BestCrypt.

Q: Existe-t-il des problèmes "internationaux"?
R: Juste un seul: l'utilisation de l'Ecran Rouge de bas niveau devrait être évité si vous n'utilisez pas exclusivement un clavier QWERTY.

Le manuel de l'utilisateur est en cours de traduction en Français & en Russe.

Q: Pourquoi une fenêtre de type explorateur apparaît-elle lorsque j'ouvre un volume ScramDisk? Est-il possible de désactiver cette fonctionnalité?
R: Cette "fonctionnalité" a été intégrée pour 2 raisons:

1. Sans appel d'une fenêtre de type Explorateur affichant le nouveau disque, les programmes et les autres fenêtres du même type ne seront pas mis à jour pour refléter l'existence du nouveau disque – ce qui est source de confusion pour beaucoup d'utilisateurs.

2. Windows 95/98 est inconsistant – même sans appel volontaire d'une fenêtre Explorateur, elle est *quelquefois* automatiquement ouverte par le système d'exploitation. L'auteur a décidé qu'il valait mieux rendre l'opération consistante.

Pour l'instant, il n'est pas possible de désactiver cette fonctionnalité.

Q: Pourquoi ScramDisk inclut-il autant d'algorithmes de cryptage?
R: Quand on a annoncé la sortie du programme, plusieurs utilisateurs l'ont critiqué parce qu'il contenait beaucoup trop d'algorithmes et avancaient trois principaux arguments:

1. La possibilité de choisir entre un grand nombre d'algorithmes peut troubler les utilisateurs.

2. Mieux vaudrait disposer d'un programme qui intègre moins d'algorithmes et fonctionne [bien avec eux] plutôt que de se disperser entre une telle quantité d'algorithmes.

3. Proposer plus d'un algorithme n'ajoute aucune sécurité.

Aussi bien l'auteur que moi-même pensons qu'il existe de bons arguments en faveur d'une abondance d'algorithmes:

1. L'algorithme offert par défaut est Blowfish, qui est un algorithme de cryptage par blocs rapide et sûr sans meilleure attaque connue que la force brute [recherche de toutes les clés] en dépit de la cryptanalyse étendue à laquelle il a été soumis. Si les utilisateurs ne connaissent rien aux différents algorithmes proposés, alors celui-ci est un choix par défaut acceptable.

2. Le code source, très bien connu, de tous les algorithmes intégrés, provient du Web, plutôt que d'avoir été réécrit. Il est hautement improbable que leur code soit défectueux, puisque tous les algorithmes ont été vérifiés avec les Vecteurs de Test librement disponibles sur le Web. Les utilisateurs peuvent les vérifier par eux-mêmes grâce à l'utilitaire adéquat intégré au programme.

3. Même si un algorithme défectueux avait été ajouté au programme, il ne causerait de problèmes que lorsque cet algorithme là serait choisi. La sécurité du système lui-même ne serait pas compromise, seuls le seraient les disques créés avec cet algorithme.

4. Nous pensons que la sécurité est certainement renforcée par l'intégration de plusieurs algorithmes. Le disque virtuel ne contient nulle part d'indication au sujet de l'algorithme employé pour le crypter. Par conséquent, quelqu'un qui voudrait 'craquer' un disque crypté devrait d'abord identifier l'algorithme employé. Et comme, en général, des données cryptées ressemblent toutes à des nombres aléatoires, ce ne sera pas facile!

5. En réponse au point 3 ci-dessus; si le programme avait été fourni avec un seul algorithme intégré et qu'il était ultérieurement découvert qu'il était faible, alors tous les utilisateurs auraient des disques cryptés faibles aussi. Cela voudrait dire que le programme serait inutilisable jusqu'à ce que quelqu'un ajoute un nouvel algorithme! Les utilisateurs de ScramDisk peuvent choisir l'algorithme qui leur inspire confiance. L'auteur a pensé qu'il était injustifié d'imposer à tous les utilisateurs l'algorithme qu'ils devaient utiliser. Maintenant, au moins, ils ont une possibilité de choix raisonnable. A la vérité, le fait de pouvoir choisir l'algorithme peut être vu comme une partie de la clé.

6. Aucun algorithme n'est parfaitement adapté à toutes les situations; quelques données ne requièrent qu'un cryptage 'basse sécurité' affectant peu la vitesse, alors que d'autres situations exigent un très haut niveau de sécurité. 3DES peut être regardé comme l'algorithme le plus sûr, mais il est très lent, alors que c'est l'inverse pour TEA; il est extrêmement rapide, mais pourait se révéler peu sûr face à un adversaire bien équipé.

7. Si des utilisateurs ont lu ce qui précède et pensent toujours qu'il vaut mieux n'utiliser ScramDisk qu'avec un seul algorithme, rien ne les empêche d'enlever tous les autres algorithmes et de recompiler le programme.

Q: Quelles sont les portes cachées dans ScramDisk?

R: A notre connaissance, aucune. Nous n'avons aucune raison d'en mettre, aussi, tirez-en vos propres conclusions. Oh, et d'ailleurs, vérifiez donc le code source si le cœur vous en dit!

ScramDisk n'est pas absolument sûr (de même que n'importe quel autre programme de ce genre!). Il existe nombre de méthodes pour un attaquant pour essayer de pénétrer votre système:

1. Regarder les programmes qui laissent traîner des données derrière elles. Un très célèbre traitement de texte est affigé d'un bogue intéressant qui laisse sur le disque des parties des éléments d'origine lorsqu'il est sauvegardé comme document incluant des liens OLE.

2. Regarder les données qui ne sont pas réellement effacées. Ok, tout le monde sait qu'on peut aisément recupérer un fichier effacé. Mais saviez-vous qu'il est possible de le faire aussi avec un fichier 'nettoyé' en examinant la surface du disque? Les fichiers effacés devraient être nettoyés à l'aide d'un utilitaire approprié (PGP v6 en intègre un bon – les utilisateurs de PGP v5.x doivent savoir que celui qui y est intégré est probablement inefficace).

3. Regarder les données traînant d'une autre façon. On songe aux fichiers temporaires et au fichier d'échange. Ceux-ci aussi ont besoin d'être nettoyés.

4. Recourir à une attaque du genre "Tempest". En gros, les émissions électromagnétiques de l'écran, du disque dur et même du clavier peuvent être repérées et enregistrées à distance. Cela peut permettre à un indiscret de voir ce qui s'affiche sur votre écran ou de capturer votre phrase secrète pendant que vous la tapez.

5. La Force Brute. Cela peut se faire de plusieurs façons: ils peuvent l'essayer sur votre phrase secrète ou sur l'algorithme. Pour contrecarrer la première attaque, il est important d'utiliser une phrase secrète longue et difficile à deviner, contenant des caractères en minuscule et en majuscule, et des chiffres. C'est difficile (et demande environ 2^{127} essais avec la plupart des algorithmes intégrés à ScramDisk – sauf pour DES & Summer).

6. Quelques algorithmes intégrés sont peut-être susceptibles d'attaques inconnues de la recherche publique. La NSA/GCHQ ***peut*** disposer d'un moyen plus rapide que la force brute pour attaquer les algorithmes. Nous n'avons inclus aucun algorithme faible dans la distribution originale (sauf Summer, pour des raisons de compatibilité), mais qui peut dire ce que les Services de Renseignement peuvent faire avec Blowfish, IDEA, 3DES et autres?

7. Installer une version modifiée de ScramDisk qui conserve secrètement votre phrase secrète de sorte qu'un agent de la CIA pourra la lire. (Ou utilise un programme comme SKIN98 pour

le faire!) On cherche trop loin? Possible, mais vous devez savoir que ce genre d'attaque existe. Il n'y a pas de bon moyen de s'en défendre. Vérifiez les signatures PGP sur les fichiers exécutables ScramDisk dans votre ordinateur, mais peut-être votre copie de PGP a-t-elle aussi été modifiée?

8. Vous frapper jusqu'à ce que vous lâchiez votre phrase secrète. Les sérums de vérité marchent aussi, apparemment.

L'auteur a fait autant qu'il a pu; vous donnant un programme qui utilise des algorithmes réputés sûrs, ne contenant aucun mécanisme de recouvrement des clés, distribué avec son code source de sorte que vous pouvez vérifier par vous-même ce que fait le programme, et fournit des fichiers de signature PGP permettant de vérifier l'authenticité et l'intégrité de l'ensemble. Pour le reste, à vous de jouer!

Q: Comment puis-je me débarrasser d'un conteneur ScramDisk dont je n'ai plus besoin?

R: La nouvelle version de ScramDisk comporte une protection des conteneurs – elle peut vous protéger d'un simple effacement d'un fichier conteneur. Au lieu de cela, vous pouvez ne pas charger le pilote VxD (en l'effaçant, par exemple) et vous pouvez alors effacer le fichier physique.

Q: Quelle version de Blowfish est intégrée?

R: La version sans bogue!

Q: Pourquoi ne puis-je pas définir des raccourcis clavier?

R: Assurez-vous que la case "Leave ScramDisk in the systray" est cochée avant de définir un Raccourci Clavier.

Q: Pourquoi n'intégrez-vous pas la fonctionnalité x?

R: Comme déjà expliqué, ScramDisk est un travail en progression. On nous demande constamment "Pourquoi n'intégrez-vous pas la fonctionnalité x". Le temps! Un seule personne se charge réellement de développer, aussi nous ne pouvons ajouter toutes les fonctionnalités souhaitées par les utilisateurs. Voir ci-dessous la liste des fonctionnalités que nous n'intégrerons certainement pas:

Fonctionnalité demandée	Raison pour ne pas l intégrer
Compression de disque	C'est un sacré boulot! Que ce soit pour ajouter cette fonctionnalité ou pour travailler sur une version NT… Et puis – les disques durs sont bon marché!
Ajustement automatique de la taille du disque	Là aussi, ce serait un sacré boulot. Si vous avez vraiment besoin de cette fonctionnalité, codez-la vous même ☺
Ajout de l'algorithme x	Nous avons dit que nous aimerions ajouter de bons algorithmes à ScramDisk. Cependant, nous ne voulons pas y voir ajoutés d' algorithmes "faibles". La communauté cryptographique décide ce qui est "fort" et ce qui est "faible". Par exemple, nous n'ajouterons pas ROT-13 de sitôt! Nous ne souhaitons pas non plus ajouter des algorithmes encombrés de brevets – nous croyons qu'il existe suffisamment d'algorithmes robustes et libres de droits disponibles.
Réencryptage du disque	Problèmes potentiels en cas de panne de courant etc.

Présentation du Programme

Ce chapitre vise à préciser pourquoi ScramDisk fonctionne comme il le fait.

Q: Pourquoi saisissez-vous les mots de passe en premier?

R: Comme ça, ils peuvent être utilisés ultérieurement et toute partition qui les utilise sera ouverte. Dès qu'un mot de passe est saisi, il peut être utilisé pour tous les disques formatés avec lui, jusqu'à ce que vous vidiez le cache (dans le programme) ou en saisissiez plus de 8. Dans ce dernier cas, il quitte la liste des mots de passe actifs.

Q: Pourquoi ne pouvez-vous pas double-cliquer sur un fichier hôte ScramDisk pour ouvrir le disque?

R: N'importe quel type de fichier peut être utilisé comme fichier hôte. C'est délibéré; il rend les volumes ScramDisk plus difficiles à repérer.

On peut remarquer qu'on fait un usage aussi limité que possible de la base de registres et des types de fichiers. C'est délibéré. Il n'est pas nécessaire que le logiciel soit enregistré par le système, aussi peut-il en être retiré presque sans laisser de trace si nécessaire. L'application Win32 Scramdisk.exe peut même tenir sur une disquette si besoin est. Le pilote "sd.vxd" doit se trouver dans le répertoire system\iosubsys; il n'y a pas d'alternative. Mais il peut être simplement effacé.

Il faudra renoncer à certaines possibilités, si l'usage du registre système doit être évité. L'une d'elles est de pouvoir lancer l'application en cliquant sur un conteneur. Des versions ultérieures vous permettront de régler vous-même les extensions de fichiers et les associations. Pour l'instant, vous devrez vous contenter de "Parcourir" et "Glisser-Déposer" depuis l'application Scramdisk.exe.

Q: Pourquoi n'obtenez-vous pas de message d'erreur, quand vos mots de passe sont incorrects?

R: En donner révèlerait que le fichier était réellement un fichier crypté (plutôt qu'un fichier plein de merde, et dans le cas d'un WAV, un quelconque fichier musical). Le fait que les fichiers ne soient pas typés, et que tous les algorithmes possibles doivent être "essayés" contre eux, signifie que les erreurs ne signifient rien. ScramDisk ne sait pas qu'un fichier donné n'est pas un fichier valide. Il sait seulement quand il a de bons mots de passe, et d'autres données, pour convertir des octets en leur valeur correcte, ce qui nous donne alors un disque Win95!

Q: Pourquoi ne pouvez-vous pas changer vos mots de passe?

R: Depuis la v2.02 il **est** possible de changer le mot de passe associé à un volume. Malheureusement, cela ne réencrypte toujours pas complètement le disque – mais seulement la zone contenant la clé au début du disque. Le réencryptage complet du disque peut être problématique en cas de coupures d'alimentation.

Q: Pourquoi un fichier clé n'ouvre-t-il pas les nouveaux disques que je formate avec le même mot de passe?

R: Les fichiers clés sont conçus pour permettre l'accès à ***certains*** disques, tout en gardant secrets vos mots de passe. Les données d'un fichier clé ne contiennent les informations que pour décrypter uniquement ceux des disques qui étaient ouverts par ScramDisk quand le fichier clé a été créé. Les données d'un fichier clé sont cryptées "comme si" le fichier clé avait été utilisé comme mot de passe quand le disque a été formaté. Votre propre mot de passe n'est jamais concerné quand un disque ScramDisk est ouvert avec un fichier clé.

Développements Futurs

> "*Ceux qui oublient le passé sont condamnés à le revivre.*"
> -- George Santayana

ScramDisk est un travail en progression. La version 2 est la première version à être placée dans le domaine public. On souhaite que, partout dans le monde, des gens aideront à développer ScramDisk. L'auteur et moi-même avons ouvert un certain nombre de pistes en vue des développements futurs. Elles sont listées par ordre d'importance décroissant:

1) Rendre l'interface utilisateur plus facile d'emploi. Eventuellement fournir des outils utilisables via la ligne de commande pour ouvrir / fermer des lecteurs etc, permettre l'association du programme avec une extension de fichier (.SVL?) si l'utilisateur le souhaite.

2) Développer une version de ScramDisk pour Windows NT et Linux.

3) Changer l'architecture pour la rendre plus normalisée et modulaire. Le programme ignore certaines conventions du C, ce qui peut être aisément corrigé. Il doit aussi être modifié pour faciliter l'ajout de nouveaux algorithmes de cryptage ou de hachage.

4) Ajouter d'autres algorithmes[4]. Ce programme dispose déjà d'un bon nombre d'algorithmes bien estimés, mais nous voudrions lui en voir ajoutés davantage. Pourquoi? Voir le chapitre FAQ pour les détails… Nous sommes particulièrement enthousiastes à l'idée d'y voir ajoutés d'autres candidats, de belle apparence, à l'AES, à savoir Serpent, TwoFish & Rijndael. ScramDisk fonctionne mieux avec des algorithmes présentant les caractéristiques suivantes:

   i) Initalisation de la clé lente, mais cryptage rapide (de préférence à une initialisation rapide et un cryptage lent).

   ii) Une faible quantité de données dépendant de la clé. Ces données doivent être mises en mémoire du noyau non mappable, aussi le plus petit serait le mieux.

5) Ajouter d'autres algorithmes de hachage. Actuellement, n'est géré que SHA-1 qui est OK, mais si une faiblesse majeure était découverte, le programme entier serait inutilisable et tous les disques créés avec ScramDisk seraient compromis. Et RIPEMD-160 ou Tiger sont probablement aussi de bons choix.

6) Changer le langage du C à l'assembleur pour intégrer Blowfish, Misty1 & Square, ou au moins utiliser une version C optimisé.

7) Ajouter une version améliorée de TEA (appelée TEAX) qui résoud le problème de la mise en place de la clé. Cela imposera probablement de l'ajouter en plus de l'intégration existante pour assurer la compatibilité.

Si vous êtes intéressés par les futurs développements du programme, que ce soit dans l'une des voies indiquées ou dans d'autres directions, contactez-nous, SVP. Nous sommes très intéressés par une coordination de l'effort de développement pour assurer que chaque réalisation est dépourvue de bogues et, autant que possible, est compatible avec d'autres versions. Nous aimerions aussi conserver une version définitive du programme sur le site Web (en plus de toute autre réalisation).

[4] Nous ne voulons pas voir d'algorithmes brevetés ajoutés à ScramDisk. Nous croyons qu'il existe assez d'algorithmes robustes et libres de droits disponibles pour qu'il n'y ait pas besoin de se soucier des algorithmes brevetés. Nous ne pouvons pas assurer le suivi d'algorithmes additionnels tels que ceux des candidats IBM ou Rivest à l'AES s'il existe des problèmes de propriété intellectuelle.

Peut-être le développement de ScramDisk constituera-t-il un jour un exercice pour étudiants en fin d'études?

Révisions du Programme

Ce chapitre vise deux objectifs: il met en évidence les diverses versions de ScramDisk en circulation et recense quelques problèmes identifiés qui doivent être / ont été résolus.

Versions du Programme

Version	Date Réalisation	Details de la Réalisation
V2.02h	1er Avril 99	Option pour ne plus demander si les phrases secrètes doivent être purgées. Ajouté dispositif de lancement automatique. Autorise l'extinction automatique sous 98. Plusieurs bogues intermittents réparés.
V2.02g	17 Nov 98	Répare plusieurs bogues: Fermeturs des conteneurs inaccessibles, problèmes d'extinction, surcharge 100% CPU. Nouvelle fonctionnalité: Protection des fichiers SVL contre l'effacement.
V2.02e	10 Nov 98	Répare plusieurs bogues: FindFast, pas de disques libres, DieHard, 98 plante en condition de surcharge, Agent & JBN. ScramDisk ne change plus désormais la date Last Modified sur les fichiers WAV. Nouvelles fonctionnalités: Affichage de la liste des périphériques physiques et option pour ne pas afficher de fenêtre Explorateur.
V2.02c	20 Sept 98	Corrige plusieurs bogues: Formatage Rapide sous 98, problème de la réapparition de la fenêtre Password, problème du "blocage" dans l'Explorateur. La documentation a été corrigée à plusieurs endroits et est maintenant également disponible au format Adobe Acrobat.
V2.02	24 Août 98	Résoud les bogues suivants: BestCrypt, Polices des Fenêtres, bogue de la Déconnexion / Connexion, bogue SKF, bogue du blocage intermittent (causé par une affectation de tampon incorrecte). Améliorations incluant: • Peut maintenant ouvrir 8 volumes au lieu de 4. • Ecran (Rouge) de très bas niveau de saisie du mot de passe qui empêche SKIN98 etc. d'enregistrer les frappes clavier. • 16 périphériques (NORMAUX) peuvent être affichés au lieu de 8. • Affiche l'heure et le jour de la dernière ouverture d'un volume crypté. • Changements mineurs de la Vérification d'Algorithme. • Permet maintenant la fermeture forcée de lecteurs. • Option pour minimiser dans la barre des tâches. • Raccourcis clavier pour fermeture et fermeture brutale. • Quelques options de la ligne de commande ont été ajoutées. (Pour ouvrir conteneur / fermeture / fermeture brutale). • Peut maintenant changer la phrase secrète utilisée pour accéder à un disque (bien que cela ne réencrypte pas le disque). • La révocation d'un accès SKF est maintenant possible. • Manuel de l'Utilisateur entièrement réécrit. • Maintenant fourni avec une petite application exemple qui montre comment ouvrir des disques de manière programmée. • Option pour désactiver le message d'avertissement "No physical". (Pour "mémoire").
V2.01	21 Juillet 98	Une réalisation intérimaire de ScramDisk qui corrigeait le bogue BestCrypt. Non largement distribuée.

V2.00	14 Juillet 98	La première réalisation placée dans le domaine public. Contient les algorithmes suivants: 3DES, Blowfish, DES, IDEA, Misty1, Square, Summer, TEA (16 & 32). SHA-1 est l'unique algorithme de hachage et le programme gère la stéganographie 8 & 4 bit WAV. Cette verson fonctionne sous Win98.
V1.00	20 Nov 97	Première réalisation. Contient seulement l'algorithme propriétaire 'Summer'. Elle n'a pas été placée dans le domaine public.

Bogues

Les 'bogues' suivants ont été identifiés et seront corrigés comme il se doit. Pour signaler de nouveaux bogues, envoyez un e-mail à Sam Simpson à l'adresse indiquée au chapitre 'Contacter l'auteur'.

Problème	Identifié le	Résolu dans la version
ScramDisk fait monter le CPU à 100% sur certaines machines.	10 Nov 98	2.02g
Utiliser ScanDisk ou Defrag sur un disque dans lequel se trouve un conteneur ScramDisk provoque l'apparition d'un Ecran Bleu de la Mort. Ces programmes essayent de fermer les fichiers RING0.	27 Oct 98	N/A
Plante quelquefois sous condition de surcharge (Windows 98 seul[t]).	19 Oct 98	V2.02e
Find Fast d'Office 95 & Office 97 bloque ScramDisk à l'ouverture d'un volume ScramDisk.	13 Oct 98	V2.02e
Les conteneurs ouverts deviennent inaccessibles lorsque les volumes se trouvent sur un disque hôte sur lequel sont lancés scandisk or defrag. On ne peut même plus fermer le conteneur.	Oct 98	2.02g
Windows 95 OSR2 – Windows échoue à envoyer un message de fermeture Kernel32, ce qui bloque ScramDisk quand on veut éteindre l'ordinateur. Il est recommandé de fermer tous les volumes ouverts avant d'éteindre.	9 Oct 98	2.02g
Problèmes quand JBN fonctionne dans un volume ScramDisk	21 Aug 98	V2.02e
Problèmes quand Agent fonctionne dans un volume ScramDisk	16 Sept 98	V2.02e
ScramDisk échoue aux tests DieHard parce qu'une zone inutilisée de 100 octets est pleine de zéros. Cela n'affecte pas la sécurité de ScramDisk.	1[er] Oct 98	V2.02e
Le Formatage Rapide peut mal fonctionner sous Windows 98.	13 Sept 98	V2.02c
Blocage intermittent quand on clique sur des fenêtres type Explorateur.	5 Sept 98	V2.02c
Fenêtre Password reste apparente, même si on choisit Cancel.	3 Sept 98	V2.02c
Quand les utilisateurs se déconnectent puis se reconnectent (c-à-d. sans arrêter l'ordinateur) ScramDisk peut refuser de se charger.	18 Août 98	V2.02
Icône document au lieu de dossier dans la fenêtre principale.	24 Juillet 98	V2.02
Le Délai d'Attente ne fonctionne pas en certaines circonstances quand l'exécutable ScramDisk n'est pas chargé.	19 Juillet 98	V2.02
Le programme bloque complètement l'ordinateur si on essaye d'ouvrir un disque ScramDisk quand il n'y a pas de lettres de lecteur disponibles. Cela peut provenir aussi bien de ce que toutes les lettres de lecteurs sont prises que d'un paramétrage incorrect de la valeur "lastdrive=***x***" dans config.sys	17 Juillet 98	N/A
IE4 (et donc Windows 98) a des problèmes quand il redessine les fenêtres d'arborescence.	11 Juillet 98	V2.02
BestCrypt et ScramDisk ne coexistent pas parfaitement. Cela tient à ce que BestCrypt crée des tas de ports que ScramDisk croit être de vrais disques durs.	21 Juin 98	V2.02
Bogue du blocage intermittent – causé par une affectation de tampon incorrecte.	20 Juin 98	V2.02

Les polices sous les lecteurs ne sont pas correctement affichées quand les Grandes polices sont utilisées.	20 Juin 98	V2.02
L'échec de l'ouverture ultérieure des fichiers WAV, dans une session [déjà commencée], signifie que vous ne pouvez pas allouer le tampon nécessaire. Aucune erreur n'est signalée, simplement vous ne pouvez pas accéder à votre disque WAV. Le tampon n'est alloué (de manière permanente) que lorsque un fichier WAV est utilisé depuis le début. Ouvrez le WAV dès le début de la session pour éviter ça. Des versions ultérieures généreront un message d'erreur et/ou disposeront d'une option qui reservera le tampon au démarrage. Les partitions et fichiers conteneurs ScramDisk normaux ne sont pas concernés.	20 Juin 98	V2.02

Détails de la Licence

> "*La légalité? Cette question n'entre pas en ligne de compte dans les discussions.*"
> -- Benson K Buffham, Deputy Director NSA

ScramDisk ne peut être utilisé que si vous agréez les termes et conditions suivants:

1. Vous acceptez que le créateur de ce logiciel ne puisse être tenu pour responsable pour ***toute*** perte de données qui pourrait survenir (même causée par une action erronée du logiciel en dépit de ses 'meilleurs efforts') et vous acceptez de sauvegarder tout fichier jugé important avant d'utiliser ce logiciel sur votre ordinateur.

2. Vous acceptez que le créateur de ce programme soit anonyme, mais souhaite cependant se réserver le copyright et les droits d'exploitation commerciale sur ce logiciel.

3. Vous acceptez de ne pas redistribuer ce logiciel sous toute autre forme que celle sous laquelle vous l'avez vous-même reçu, et si vous deviez le redistribuer, il incluerait tous les fichiers exactement dans l'état où ils ont été reçus.

4. Vous acceptez que dans l'éventualité d'une perte, ou d'un oubli des mots de passe, aucune assistance technique n'est due pour recouvrer ces mots de passe. L'oubli de tout mot de passe EQUIVAUT A perdre vos données si elles sont conservées sur toute partition, ou fichier disque créé ou ouvert en exécutant ce logiciel. Vous acceptez qu'il n'existe pas de portes cachées, pour accéder aux données cryptées.

5. Vous acceptez que certains des algorithmes utilisés appartiennent à d'autres et peuvent demander une licence pour usage commercial, comme l'utilisation sur des ordinateurs d'entreprise. Vous êtes informé que cela est particulièrement vrai dans le cas de l'algorithme IDEA et lirez les documents concernant les conditions posées par Ascom pour l'utilisation de IDEA, qui se trouvent au bas de cette page.

6. Vous acceptez que si vous vous procurez le code source publiquement disponible et le modifiez, vous devrez soumettre le programme modifié et le nouveau code source aux auteurs originels aux fins de publication, et comprenez que ces modifications de devront pas compromettre la compatibilité avec les versions plus anciennes du logiciel ou en aucune façon réduire les niveaux de sécurité.

IDEA Conditions d'utilisation et avis imposé:

This Software/Hardware product contains the algorithm IDEA as described and claimed in US Patent No. 5,214,703, EPO Patent No. 0482154 and filed Japanese Patent Application No. 508119/1991 "Device for the conversion of a digital block and use of same" (hereinafter referred to as "Algorithm").

Any use of the Algorithm for Commercial Purposes is thus subject to a license from Ascom Systec Ltd. of CH-5506 Mägenwil (Switzerland), being the patentee and sole owner of all rights, including the term IDEA.

Commercial Purposes shall mean any revenue generating purpose including but not limited to:

i) using the Algorithm for company internal purposes (subject to a Site License).

ii) incorporating an application software containing the Algorithm into any hardware and/or software and distributing such hardware and/or software and/or providing services related thereto to others subject to a Product License).

iii) using a product containing an application software that uses the Algorithm (subject to an End-User License), except in case where such End-User has acquired an implied license by purchasing the said product from an authorised licensee or where the End-User has already signed up for a Site License.

All such commercial license agreements are available exclusively from Ascom Systec Ltd. and may be requested via the Internet World Wide Web at http://www.ascom.ch/systec or by sending an electronic mail to IDEA@ascom.ch. Any misuse will be prosecuted.

Use other than for Commercial Purposes is strictly limited to data transfer between private individuals and not serving Commercial Purposes. The use by government agencies, non-profit organisations etc. is considered as use for Commercial Purposes but may be subject to special conditions. Requests for waivers for non-commercial use (e.g. by software developers) are welcome.

Sources

Voir la page Web de ScramDisk pour une collection de liens vers des sites intéressants traitant de cryptographie et de sécurité. De toutes façons, je recommande chaudement les livres suivants:

Cryptographie et sécurité

Applied Cryptography - 2nd Edition, B.Schneier, 1996.
ISBN: 0-471-11709-9
La bible de la cryptographie aussi bien pour les apprentis crypteurs que pour les professionnels. LE livre sur la question, que dire de plus?

Handbook of Applied Cryptography, Menzes et al, 1996.
ISBN: 0-8493-8523-7
Dense et exhaustif! Un "must".

Cryptography - Theory and Practice, Douglas R Stinson, 1995.
ISBN: 0-8493-8521-0
Autre grand livre.

A **Course in Number Theory**, Neal Koblitz, 1994.
ISBN: 0-387-94293-9
Aspects mathématiques de la crypto.

Decrypted Secrets, F.L.Bauer, 1997.
ISBN: 3-540-60418-9
Bonne discussion sur la cryptographie ancienne manière.

Computers and Intractability, Michael Garey & David Johnson, 1997.
ISBN: 0-7167-1045-5
Un guide de la théorie de NP-complet. Difficile mais gratifiante lecture!

Computational Complexity, Christos Papdimitriou, 1994.
ISBN: 0-201-53082-1
Un examen exhaustif de la complexité algorithmique.

Cryptography and Data Security, D.Denning, 1983.
ISBN: 0-201-10150-5
Une bonne introduction à la cryptographie.

Security in Computing - 2nd Edition, C.Pfleeger, 1997.
ISBN: 0-13-185794-0
Couvre la cryptographie et les problèmes plus généraux des systèmes d'information & informatiques.

Computer Security Handbook - 3rd Edition, Hutt, Bosworth & Hoyt, 1995.
ISBN: 0-471-11854-0
La bible du responsable sécurité. Un pavé très sérieux!

Cryptography and Secure Communication, M.Rhee, 1994.
ISBN: 0-07-112502-7
Les écueils de la cryptographie.

E-Mail Security with PGP and PEM, B.Schneier, 1995.
ISBN: 0-47-105318-x

Comme le titre l'indique.

Thèmes plus généraux

Privacy on the Line - The Politics of Wiretapping and Encryption, W.Diffie & S.Landau, 1998.
ISBN: 0-262-04167-7
Excellente discussion sur le renforcement de la sécurité nationale au détriment de la protection de la vie privée.

Building in Big Brother, L.Hoffman, 1995.
ISBN: 0-387-94441-9
Excellente compilation de documents sur la cryptographie – même si un peu daté.

The Code-Breakers, D.Kahn, 1996.
ISBN: 0-684-83130-9
"La grande histoire des communications secrètes depuis les temps anciens jusqu'à Internet". Tout simplement!

The Puzzle Palace, J.Bamford, 1983.
ISBN: 0-14-006748-5
Le service de renseignement le plus secret des Etats-Unis dévoilé. Fascinant! Qui sait seulement de combien ils ont progressé dans les 15 années qui ont suivi la publication?

For the President's Eyes Only, C.Andrew, 1996.
ISBN: 0-06-092178-1
Pas un livre sur Mlle Lewinsky mais "Le renseignement et la Présidence américaine de Washington à Bush". Un bon éclairage sur les différents services de renseignement des Etats-Unis.

Marching Orders - The Untold Story of World War II, B.Lee, 1995.
ISBN: 0-517-57576-0
Décrit l'utilisation de ULTRA & MAGIC par les alliés.

Inside CIA s private world, H.B.Westerfield, 1995.
ISBN: 0-300-07264-3
Articles récemment rendus publics du rapport de la CIA *Studies in intelligence*. Intéressant!

Betrayal The Story Of Aldrich Ames An American Spy, Weiner, Johnston & Lewis, 1995.
ISBN: 1-86066-046-0
Qui était le plus incompétent? Ames ou bien la CIA?

A Century Of Spies Intelligence in the Twentieth Century, J.T.Richelson, 1995.
ISBN: 0-19-511390-x
OK, bien qu'un peu léger.

The US Intelligence Community, J.T.Richelson, 1995.
ISBN: 0-8133-2376-2
"Le guide incontesté du gratin clandestin américain". Vraiment!

Persuasion and Privacy in Cyberspace, L.Gurak, 1997.
ISBN: 0-300-06963-4
Pas encore lu.

Technology and Privacy: The New Landscape, P.Agre & M.Rotenberg, 1997.
ISBN: 0-262-01162-x
Pas encore lu.

Shamans, Software and Spleens, J.Boyle, 1996.
ISBN: 0-674-80522-4
Pas encore lu.

The Art of Computer Programming Volume 2 Seminumerical Algorithms, D.Knuth, 1998.
ISBN: 0-201-89684-2
Des tonnes de détails sur la génération de nombres pseudo aléatoires, l'exponentiation etc.

The Right To Privacy, E.Alderman & C.Kennedy, 1995.
ISBN: 0-679-41986-1
Pas encore lu.

Grandes Citations Crypto & Sécurité

"Nul ne sera soumis à des investigations arbitraires dans son intimité, sa famille, sa maison ou sa correspondance, ni attaqué dans son honneur et sa réputation. Chacun a droit à la protection de la loi contre de telles investigations ou attaques."
-- Article 12 de la Déclaration Universelle des Droits de l'Homme

"The real aim of current policy is to ensure the continued effectiveness of US information warfare assets against individuals, businesses and governments in Europe and elsewhere"
-- Ross Anderson, posting to ukcrypto, 4th Dec 1998

"self-regulation is fine when the consumer's interests are at stake, but legislation is thought essential when the spooks consider their interests to be at stake."
-- Marc Rotenberg

"1984 - Orwell ne s'est trompé que d'une décade ou deux."
-- Anon

"I am smug enough to say that NSA can't break RSA or discrete logs."
-- Bob Silverman posting to sci.crypt, January 5, 1996.

"RSA seems to me to be elegant in its simplicity (even I cannot forget it, though I try every time I leave the country) and ease of demonstration."
-- William Hugh Murray to talk.politics.crypto 7 Dec 1998

"An NSA-employed acquaintance, when asked whether the government can crack DES traffic, quipped that real systems are so insecure that they never need to bother. Unfortunately, there are no easy recipes for making a system secure, no substitute for careful design and critical, ongoing scrutiny."
-- Matt Blaze in AC2

(BS) "You cannot trust an encryption algorithm designed by someone who had not 'earned their bones' by first spending a lot of time cracking codes."
(PRZ) "...Practically no one in the commercial world of cryptography qualified under this criterion!"
(BS) "Yes, and that makes our job at the NSA so much easier"
-- Coversation between Philip Zimmermann and Brian Snow, a senior cryptographer with the NSA.

"Even the Four Horsemen of Kidporn, Dope Dealers, Mafia and Terrorists don't worry me as much as totalitarian governments. It's been a long century, and we've had enough of them."
-- Bruce Sterling

"You want us to put an ax in your hand and you're promising to hit us with only the flat side of it. But the Chinese don't see it that way; they're already licensing fax machines and they're gonna need a lot of new hardware to gear up for Tiananmen II"
-- Bruce Sterling

"I'd rather have him inside the tent pissing out than outside the tent pissing in"
-- Lyndon B Johnson on why he retained J. Edgar Hoover at the FBI, _Guardian Weekly_ 12/18/71.

"England has never enjoyed a genuine social revolution. Maybe that's what's wrong with that dear, tepid, vapid, insipid, stuffy, little country."
-- Edward Abbey

"*Le droit de tout individu à la sûreté de ses biens, affaires et propriétés, contre toute enquête ou saisie injustifiées, devra être préservé....*"
-- Quatrième Amendement à la Constitution des Etats-Unis

"*Le Congrès ne fera aucune loi concernant l'institution d'une religion ou prohibant leur libre exercice; ou restreignant la liberté de parole, ou de la presse; ou le droit du peuple à se réunir paisiblement, et à*

demander au gouvernement la réparation des injustices."
– Premier Amendement à la Constitution des Etats-Unis

"No man's life, liberty, or property is safe while the legislature is in session."
-- Judge Gideon J. Tucker, 1866.

"*La liberté de parole et de la presse garanties par la Constitution comprennent au moins celle de discuter publiquement et sincèrement de tous les sujets d'intérêt public sans restriction ou crainte de poursuites.*"
-- Roth v. United States, 354 U.S. 476 (1957)

"*...domestic intelligence activities [that] threaten to undermine our democratic society and fundamentally alter its nature*"
-- Senate Church Committee report, 1976

"*the debate over national cryptography policy can be carried out in a reasonable manner on an unclassified basis*"
-- A Congress requested National Research Council report "Cryptography's role in securing the information society", 1996

"*au total, les avantages d'une diffusion de la cryptographie l'emportent sur les désavantages* "
-- ibid

"Escrowed encryption [encryption for which a third party holds a key] by design introduces a system weakness ... and so if the procedures that protect against improper use of that access somehow fail, information is left unprotected."
-- ibid

"I Really think we would do better to discuss this in executive session"
-- William E Colby, CIA Director, 1975

"La légalité? Cette question n'entre pas en ligne de compte dans les discussions."
-- Benson K Buffham, Deputy Director NSA when questioned by the Senate Church Committee about domestic monitoring

"*The FBI, on the other hand, stretched the truth and distorted the fact. It seems fair to conclude that the government has not made its case regarding encryption.*"
-- Diffie in "Privacy on the line", 1998 - explaining how intelligence agencies (mis)use wiretap statistics.

"*In total, therefore, the U.S. economy will lose between $35.16 and $95.92 billion over the next five years, as a consequence of current administration policy [on crypto].*"
-- Economic Strategy Institute report "Finding the Key", 1998

"*The right to be let alone is indeed the beginning of all freedom.*"
-- Supreme Court Justice William O. Douglas 1952, Public Utilities Commission vs. Pollak

"*The right to be left alone - the most comprehensive of rights, and the right most valued by civilized men.*"
-- Supreme Court Justice Louis Brandeis

"*There is no assurance, without scrutiny, that all keying material introduced during the chip programming is not already available to the NSA..... As long as the programming devices are controlled by the NSA, there is no way to prevent the NSA from routinely monitoring all SKIPJACK encrypted traffic. Moreover, compromise of the NSA keys, such as in the Walker case, could compromise the entire EES system.*"
-- NASA comments on EES, 1993. ok - branches of the government don't trust the NSA, but we should?

"In some countries, strong encryption has been banned or the keys have to be escrowed for government officials. With invisibility readily available to anyone with moderate programming skills, it is obvious that any such measures are ineffective. Restrictions on encryption cannot stop criminals from

using, but may hurt law-abiding businesses and individuals who could greatly benefit from mass application of cryptographic techniques."
-- Counterintelligence News and Developments, National Counterintelligence Center, Volume 2 - June 1998

"*Just because you're paranoid doesn't mean some one isn't out to get you...*"
-- Unknown

"Any time that you're developing a new product, you will be working closely with the NSA"
-- Ira Rubenstein, Microsoft attorney

"All data is illegal - all you need is the appropriate one time pad"
-- AMAN, 25 September 1998

"*Il en va du cryptage de disque comme de toute autre chose qui peut être utilisée pour faire le bien, ou le mal (je pourrais étrangler quelqu'un avec un stéthoscope par exemple...)*"
-- AMAN, 6 Juillet 1998

"*La loi ne m'autorise pas à témoigner sur aucun aspect de la National Security Agency, même devant la Commission du Sénat sur le renseignement.*"
-- Général Allen, Directeur de la NSA, 1975

"*Salauds!*"
-- guy@panix.com en réponse à la citation ci-dessus du Général Allen :-)

"You don't want to buy a set of car keys from a guy who specializes in stealing cars"
-- Marc Rotenberg commenting on Clipper

"*There can be no greater good than the quest for peace, and no finer purpose than the preservation of freedom.*"
-- U.S. President Ronald Reagan

"*La confiance, je crois savoir ce que c'est. J'en ai l'ancienne conception. Je l'ai méritée.*"
--Bill Clinton, in Federal News Service, 28 October 1992. Héhéhéhé.

"*La force de la Constitution réside entièrement dans la détermination de chaque citoyen à la défendre. Les droits constitutionnels ne seront préservés que si chaque citoyen, pour la part qui lui revient, se sent personnellement investi de la mission de les défendre.*"
-- Albert Einstein

"At the very least, an effort should be made to develop minimal due process guarantees for individuals who are threatened with a secrecy order. The burden of proof should be on the gov't to show why a citizen's constitutional rights must be abridged in the interests of 'national security'."
-- pp 33 & 34 Werner Baum 1978 July [chaired an NSF committee on cryptography]

"Nearly all men can stand adversity, but if you want to test a man's character, give him power."
-- Abraham Lincoln

"*Il est dangereux d'avoir raison quand le gouvernement a tort.*"
-- Voltaire

"*Pour ce qui nous concerne, il n'y a pas de différence entre un fichier crypté et une valise fermée à clé*"
-- Officier des douanes anglaises, Août 98. A part le fait que l'on peut forcer une valise :-)

"*Si tous les ordinateurs personnels du monde – ~ 260 millions – étaient affectés à décrypter le même message crypté par PGP, cela prendrait malgré tout environ 12 millions de fois l'âge de l'univers, en moyenne, pour en décrypter un seul.*"
-- William Crowell, Directeur en chef de la National Security Agency, Mars 1997

"*Sans contrôle, les choses peuvent devenir extrèmement confuses dans l'esprit du grand public.*"
-- Général William Westmoreland, USA

"*I would rather be exposed to the inconveniences attending too much liberty than those attending too small a degree of it.*"
-- Thomas Jefferson

"The spirit of resistance to government is so valuable on certain occasions that I wish it to be always kept alive"
-- Thomas Jefferson

"*Mon avis est que le FBI est incompétent, ment, ou bien les deux...*"
-- Bruce Schneier à propos de l'affirmation du FBI selon laquelle il n'aurait pas de machines spécialisées capables de décrypter DES

"It is insufficient to protect ourselves with laws; we need to protect ourselves with mathematics."
-- Bruce Schneier

"Cryptography products may be declared illegal, but the information will never be"
-- Bruce Schneier

"*But I'd also ask American business not to make a campaign out of just trying to bust through export controls as though somehow there was a God-given, inherent right to send the strongest encryption to anybody in the world, no matter who they are. I don't agree with that. I will never agree with that.*"
-- Deputy Secretary of Defense John J. Hamre, 21 July, 1998. *But who said there is a god given right that the DoD can read my messages?*

"*Vous pouvez me torturer autant que vous voulez, je ne sais rien*"
"*te torturer... voilà une bonne idée*"
-- Resevoir Dogs (Quentin Tarantino)

"*La réponse de la NSA fut, 'Bien, c'était intéressant, mais il n'y a pas d'algorithme comme ça.'*"
-- Gus Simmons - "The History of Subliminal Channels"

"*Un secret à deux est un secret de Dieu; un secret à trois est le secret de tout le monde.*"
– Proverbe Français (à propos du système clipper / key-escrow? :-))

"*Can you say 'cryptographic filesystem'? Can you say 'custom filesystem'?*"
-- James MacDonald posting to sci.crypt, August 14, 1998. Sarcastic comment - made unwittingly to the author of ScramDisk :-)

"*The obvious mathematical breakthrough would be development of an easy way to factor large prime numbers.*"
-- Bill Gates from The Road Ahead, p265

"*Cryptography is like literacy in the Dark Ages. Infinitely potent, for good and ill... yet basically an intellectual construct, an idea, which by its nature will resist efforts to restrict it to bureaucrats and others who deem only themselves worthy of such Privilege.*"
-- A Thinking Man's Creed for Crypto

"*There is a secret message embedded in the phosphor of this period.*"
-- David Honig [honig@sprynet.com] .sig

"*It's the dungheap of History. If you look really, really closely at the tippy top, you can see Louis Freeh holding a Clipper chip.*"
-- Xcott Craver posting to sci.crypt 20 August 1998. Describing the 'pyramid thing' on the cover of AC2 :-)

"*You shouldn't overestimate the I.Q. of crooks.*"
-- NYT: Stuart A. Baker, General Counsel for the NSA, explained why crooks and terrorists who are

smart enough to use data encryption would be stupid enough to choose the U.S. Government's compromised data encryption standard.

"*An essential element of freedom is the right to privacy, a right that cannot be expected to stand against an unremitting technological attack.*"
-- Whitfield Diffie, Distinguished Engineer at Sun Microsystems

"*It must always be remembered that crime statistics are highly inflammatory---an explosive fuel that powers the nation's debate over a large number of important social issues---and that FBI Director Louis Freeh today is the leading official shovelling the fuel into the blazing firebox.*"
-- David Burnham

"*Pourquoi vous inquiéter si vous n'avez rien à cacher?*"
-- J. Edgar Hoover

"*J'aime mon pays mais je crains mon gouvernement*"
-- Anonyme

"*...Finally, face it; PGP, albeit useful for some niche applications, is a little pissant pimple on the body of cryptographic usage.*"
-- David Sternlight posting to comp.security.pgp.discuss, June 25, 1997. Click here for more :-)

"The irony of the Information Age is that it has given new respectability to uninformed opinion."
--John Lawton, as previously quoted in D.Sternlights .sig But was it written about him? :-)

"*Where the hell is your great contribution to the field that I worked in?????*"
-- Robert Gifford posting to comp.security.pgp.discuss, Aug 25, 1998 to David Sternlight :-).

"*I have not got any father than just a few variables past one round. I tried to search for real info on the 3.5 rounds that some one reverseved engineered but could not find it.*"
-- The literate David A. Scott posting to sci.crypt , June 26, 1998. RE his analysis of IDEA :-)

"*I have developed an encryption software package that I can best describe as a ONE-TIME-PAD GENERATOR.*"
-- Anthony Stephen Szopa posting to sci.crypt, August 8, 1997

"*Is it time for another one of these already? Oh, bother.*"
-- Bruce Schneier posting to sci.crypt, August 8, 1997 - in response to the Szopa quote :-)

"*Quis Custodiet Ipsos Custodes.*" -> "*Qui surveillera les surveillants.*"
-- Juvenal, circa 128 AD

"*Anyone who considers arithmetical methods of producing random digits is, of course, in a state of sin.*"
-- John Von Neumann, 1951

"Deception is a state of mind - and the mind of the state"
-- James Angleton, the late CIA superspy, quoted in the book, DECEPTION by Edward Jay Jones (1989)

"The limits of tyrants are prescribed by the endurance of those whom they oppress."
-- Frederick Douglass

"I swear to tell the truth, the whole truth, just the way the President did."
-- Timothy C. May .sig

"*Random numbers should not be generated with a method chosen at random.*"
-- Donald Knuth, vol 2.

"*Key escrow to rule them all; key escrow to find them. Key escrow to bring them all and in the darkness bind them. In the land of surveillance where Big Brother lies.*"
-- Peter Gutmann

"*When cryptography is outlawed, bayl bhgynjf jvyy unir cevinpl.*"
-- Kevin McCurleys Thought for the day, June 24, 1997

"The greatest calamity which could befall us would be submission to a government of unlimited powers."
--Thomas Jefferson, 1825

"I regret to say that we of the FBI are powerless to act in cases of oral-genital intimacy, unless it has in some way obstructed interstate commerce."
-- J. Edgar Hoover

"50 million potential S/Mime users can't be wrong.... But they can all be stupid!"
-- Sam Simpson, 4th December 98

"1 million PGP users can't be wrong.... But they can all be stupid! (But at least they ain't spied upon by Echelon)"
-- Sam Simpson, 7 Dec 98 (In response to Sternlights complaint about the previous quote)

"*Mary had a little key (It's all she could export),*
and all the email that she sent was opened at the Fort."
-- Ron Rivest

"*Mary had a crypto key, she kept it in escrow,*
and everything that Mary said, the Feds were sure to know."
-- Sam Simpson, July 9, 1998

"Mary had a scrambler prog, equipped with key recovery,
the snoops, her data, they did log, much to her shock discovery!"
-- AMAN, 22 September, 1998

"*There is a group at Fort Meade*
who fear that which they cannot read
so they fight with their friends
(God knows to what ends!)
In attempts to get more than they need."
-- Jim Bidzos, CEO of RSA Data Security

"*Feistel and Coppersmith rule. Sixteen rounds and one hell of an avalanche.*"
-- Stephan Eisvogel in de.comp.security, Jan 1998

"*La NSA ment régulièrement aux gens qui lui demandent son avis au sujet des règles d'exportation. Ils n'ont aucune raison de ne pas le faire; atteignant leur objectif par tout moyen légal qui leur plaît. Mentir est légal pour un fonctionnaire d'Etat.*"
-- John Gilmore (gnu@toad.com)

"*En Dieu nous croyons. Pour tous les autres, nous vérifions avec PGP!*"
-- Tim Newsome

"*BTW, I learned a lovely new acronym today: "Law Enforcement Agency Key" - LEAK.*"
-- Charles H. Lindsey (chl@clw.cs.man.ac.uk)

"*They that give up essential liberty to obtain a little temporary safety deserve neither liberty nor safety.*"
-- Benjamin Franklin

"[U]ncontrolled search & seizure is one of the first & more effective weapons in the arsenal of every arbitrary government."
-- Robert Jackson 1949 Brinegar v US 338 US 160, 180-181

"Wherever a man may be, he is entitled to know that he will remain free from unreasonable searches & seizures."
-- Supremes 1967 in Katz v US 389 US 347, 359

"When the President does it, that means that it's not illegal."
-- Richard M. Nixon in an interview with David Frost, 19th May, 1977

"Asking the Government to protect your Privacy is like asking a Peeping Tom to install your window blinds"
-- Founder of the EFF

"Whoever would overthrow the liberty of a nation must begin by subduing the freeness of speech."
-- Benjamin Franklin

"We must ensure that new technology does not mean new and sophisticated criminal and terrorist activity which leaves law enforcement outmatched -- we can't allow that to happen"
-- Al Gore - Sept. 16, 1998

"Civilization is the progress toward a society of privacy.The savage's whole existence is public, ruled by the laws of his tribe. Civilization is the process of setting man free from men"
-- Ayn Rand, The Fountainhead (1943)

"Individual rights are not subject to a public vote; a majority has no right to vote away the rights of a minority; the political function of rights is precisely to protect minorities from oppression by majorities (and the smallest minority on earth is the individual)"
--Ayn Rand

"*Necessity is the plea for every infringement of human freedom. It is the argument of tyrants; it is the creed of slaves.*"
-- William Pitt, British Prime Minister, November 18, 1783

"*There's no way to rule innocent men. The only power any government has is the power to crack down on criminals. Well, when there aren't enough criminals, one makes them. One declares so many things to be a crime that it becomes impossible to live without breaking laws.*"
-- Ayn Rand, "Atlas Shrugged"

"I apprehend no danger to our country from a foreign foe ... Our destruction, should it come at all, will be from another quarter. From the inattention of the people to the concerns of their government, from their carelessness and negligence, I must confess that I do apprehend some danger."
-- Daniel Webster, June 1, 1837

"*This method, seemingly very clever, actually played into our hands! And so it often happens that an apparently ingenious idea is in fact a weakness which the scientific cryptographer seizes on for his solution.*"
-- Herbert Yardley, The American Black Chamber, p282, referring to a Japanese method of transposing the sections of a code message to hide the beginning and end.

"*I applied ROT13 to this, but that didn't make it any more intelligible!*"
-- Roger Schlafly posting to sci.crypt, 21st June 98 in response to a message posted in German :-)

"*The Internet treats censorship as a malfunction and routes around it.*"
-- John Perry Barlow

"*Liberté signifie responsabilité. C'est pourquoi la plupart des hommes la redoutent.*"
-- George Bernard Shaw

"The greatest trick the devil ever played was convincing everyone he didn't exist"
-- Verbal Kint. (Written about the NSA?)

"It is better to weep with wise men than to laugh with fools."

-- Spanish Proverb

"The best defense against logic is ignorance."
-- anon

"I think there's a world market for about five computers."
-- Watson, Thomas (Founder of IBM)

"Besides a mathematical inclination, an exceptionally good mastery of one's native tongue is the most vital asset of a competent programmer."
-- Edsger W.Dijkstra

"I know not with what weapons World War III will be fought, but World War IV will be fought with sticks and stones."
-- Albert Einstein

"Terrorism: deadly violence against humans and other living things, usually conducted by government against its own people."
-- Edward Abbey

"No poor bastard ever won a war by dying for his country. He won it by making other bastards die for their country."
-- George Smith Patton

"Si j'ai pu voir si loin, c'est parce que je suis monté sur les épaules de géants."
-- Sir Isaac Newton (1642-1727)

"Ceux qui oublient le passé sont condamnés à le revivre."
-- George Santayana (1863-1952)

"*Furem fur cognoscit et lupum lupus. " -> "Un voleur reconnaît un voleur et un loup un loup.*"
-- Anonyme

"In some ways, cryptography is like pharmaceuticals. Its integrity may be absolutely crucial. Bad penicillin looks the same as good penicillin. You can tell if you spread sheet is wrong, but how do you tell if your cryptography package is weak? The ciphertext produced by a weak encryption algorithm looks as good as ciphertext produced by a strong encryption algorithm. There's a lot of snake oil out there. A lot of quack cures. Unlike the patent medicine hucksters of old, these sofwtare implementors usually don't even know their stuff is snake oil. They may be good software engineers, but they usually haven't even read any of the academic literature in cryptography. But they think they can write good cryptographic software. And why not? After all, it seems intuitively easy to do so. And their software seems to work ok"
-- Philip Zimmermann

"Are there any users of cellular phones here? Because people are concerned (2-3 people finally clap) I knew it was a sophisticated group. Um, no. People are concerned about the privacy you know. Newt Gingrich, what happened to him. So a couple of months ago they set out to make these things a lot better so that you couldn't break in. Well. Put in a new code. Yesterday, a team of computer experts announced that they had already cracked the electronic code. And sadly, none of them knew how, still, to unhook a bra."
-- Politically Incorrect on ABC, 21 March 98

"First they came for the hackers.
But I never did anything illegal with my computer,
so I didn't speak up.
Then they came for the pornographers.
But I thought there was too much smut on the Internet anyway,
so I didn't speak up.
Then they came for the anonymous remailers.
But a lot of nasty stuff gets sent from anon.penet.fi,
so I didn't speak up.

Then they came for the encryption users.
But I could never figure out how to work PGP anyway,
so I didn't speak up.
Then they came for me.
And by that time there was no one left to speak up."
-- Unknown

"Buy four copies of the book, and mail one to each of the top four names on the list. Then add your name to the bottom of the list. In just a few short weeks you'll receive 2^56 copies of Applied Cryptography from all over the world...."
-- Bruce Schneier posting to sci.crypt, 19 October, 1998. Aren't pyramid schemes illegal? :-)

Contacter l'auteur

L'auteur du programme souhaite demeurer anonyme pour des raisons personnelles. Si vous voulez lui envoyer un message, envoyez-le à l'adresse ci-dessous, de préférence crypté PGP. Autrement, envoyez un message au compte scramdisk@hotmail.com, qui est lu par AMAN et moi-même.

L'auteur peut aussi être contacté en écrivant dans les forums sci.crypt ou alt.security.pgp avec le mot 'Scramdisk' dans l'en-tête du sujet. L'auteur utilise le pseudonyme AMAN.

Il existe maintenant quatre clés PGP – une pour le compte HotMail ScramDisk (qui est lu par AMAN et moi-même), deux pour S.Simpson & une pour A.Jeffries:

Adresses e-mail	Type de clé	Taille (bits)	Créée	Clé ID
Scramdisk@hotmail.com	Diffie-Hellman/DSS	3072/1024	02/11/98	0xC0E0C17A
ssimpson@hertreg.ac.uk	Diffie-Hellman/DSS	3072/1024	24/07/97	0x433FDB4F
ssimpson@hertreg.ac.uk	RSA	2048	22/08/97	0x560D21A9
ajeffries@kwikrite.clara.net	Diffie-Hellman/DSS	4096/1024	11/12/98	0xF4B8DEE4

Les mises à jour de ScramDisk et les informations sur le travail de développement peuvent être trouvées sur le site: http://www.scramdisk.clara.net/

Remerciements

> "*Is it time for another one of these already? Oh, bother.*"
> -- Bruce Schneier posting to sci.crypt, August 8, 1997

Tout d'abord: absolument aucun remerciement au Gouvernement du Royaume-Uni qui semble vouloir restreindre les droits à la cryptographie pour ses citoyens (ainsi que ceux à la confidentialité) avec deux nouveaux projets de loi. Les Conservateurs avaient-ils raison – "New Labour, new danger"? Le Parti Travailliste a manqué honteusement à ses promesses électorales au sujet de la crypto….

Juste au moment où le Canada dessère ses contrôles à l'exportation, nous commençons à les ressérer. Hhhmm.

Nous voudrions remercier des douzaines de personnes qui aident à la cause de la crypto, mais je n'ai pas eu le temps d'en dresser une liste exhaustive ☹ Les personnes notoires sont Phil Zimmermann, David Kahn, les Professeurs Bernstein & Junger, James Bamford, Charles (Softwar), Paul Leyland & Ross Anderson pour si bien exposer leurs opinions sur la cryptographie. Ensuite, il y a les rois de la crypto, qui développent, cryptanalysent et commentent intelligemment la cryptographie, les: Matt Blaze, Martin Hellman, Ross Anderson (ENCORE!),Bruce Schneier, John Savard, Don Coppersmith, Ron Rivest, Eli Biham, Ralph Merkle, David Wagner, Antoon Bosselaers, Bart Preneel, John Daemen, Vincent Rijmen, Sean Murphy, James Massey et beaucoup trop d'autres pour tous les mentionner.

Grand merci à Andy Jeffries (ajeffries@kwikrite.clara.net) de Kwik-Rite Development (www.kwikrite.clara.net) pour produire les composants Delphi TkrScramDisk et l'assistance avec le développement d'applications Delphi.

Merci au Dr Brian Gladman, Ross Anderson, Ian Sparkes, Bruce Schneier et les innombrables autres qui nous ont fourni une assistance technique et des avis qualifiés au cours du développement de ScramDisk.

Merci à Dan "the" Horne pour la lecture approfondie du manuel.

Grand merci à Michel Bouissou qui a patiemment répondu aux questions sur ScramDisk avec une compétence "quasi officielle" sur les Groupes de Discussion.

Merci à Emilio Oriente (oriente@citoyen.com) & Michael Ruder (ruder@gmx.de) pour avoir traduit le manuel en Français et en Allemand, respectivement.

Merci à Ed Mortensen pour avoir miroité le site de ScramDisk aux USA.

Merci à tous ceux qui nous ont écrit pour nous faire connaître leur avis – les Français & les Russes semblent particulièrement reconnaissants pour des programmes comme ScramDisk pour certaines raisons…

Oh, je devrais aussi mentionnerl'auteur du programme, pour avoir infatigablement produit et amélioré le programme! Je suis certain qu'il atteindra à juste tire à la dignité (anonyme) de saint de l'internet, qui qu'il soit!

N'hésitez pas à me faire connaître tous commentaires, erreurs et omissions.

Appendice A – Vecteurs de Test des Algorithmes

Algorithme	Source	Réordonner[5]	Clé	Texte clair	Texte crypté
Blowfish	Counterpane web site	Non	00000000 00000000	00000000 00000000	4EF99745 6198DD78
Blowfish	Counterpane web site	Non	FFFFFFFF FFFFFFFF	FFFFFFFF FFFFFFFF	51866FD5 B85ECB8A
Blowfish	Counterpane web site	Non	FFFFFFFF FFFFFFFF	00000000 00000000	F21E9A77 B71C49BC
DES	www.itl.nist.gov/div897/pubs/fip81.htm	Oui	01234567 89ABCDEF	4E6F7720 69732074	3FA40E8A 984D4815
DES	Applied Cryptography 2nd edition, p631	Oui	01234567 89ABCDEF	01234567 89ABCDEF	C9574425 6A5ED31D
IDEA	Cryptlib Source Code	Oui	00010002 00030004 00050006 00070008	00000001 00020003	11FBED2B 01986DE5
MISTY1	MISTY1 RFC	Non	00112233 44556677 8899AABB CCDDEEFF	01234567 89ABCDEF	8B1DA5F5 6AB3D07C
Square	www.esat.kuleuven.ac.be/~rijmen/downloadable/square/vdata	Oui	80000000 00000000 00000000 00000000	00000000 00000000 00000000 00000000	05F8AAFD EFB4F5F9 C751E5B3 6C8A37D8
TEA32	Sci.crypt	Non	00000000 00000000 00000000 00000000	00000000 00000000	41EA3A0A 94BAA940
TEA32	Sci.crypt	Non	4C617073 616E675F 536F7563 686F6E67	4561726C 47726579	4B20E121 C32E8546

[5] Cette colonne indique si vous devez cocher la case "Read byte values from left to right in memory order" pour vérifier convenablement les vecteurs de test.