Etude de différents outils de chiffrement

BREANT Kévin
BRUN Gaëtan

Sécurité, Dossiers et Fichiers

1. Donner la procédure permettant de chiffrer un dossier ou un fichier dans Windows.
2. Documenter l'usage de la fonction Bitlocker.
3. Tester et documenter (une page par produit) les outils logiciels suivants :

   Si l'un d'entre eux n'existe plus, en proposer un autre.

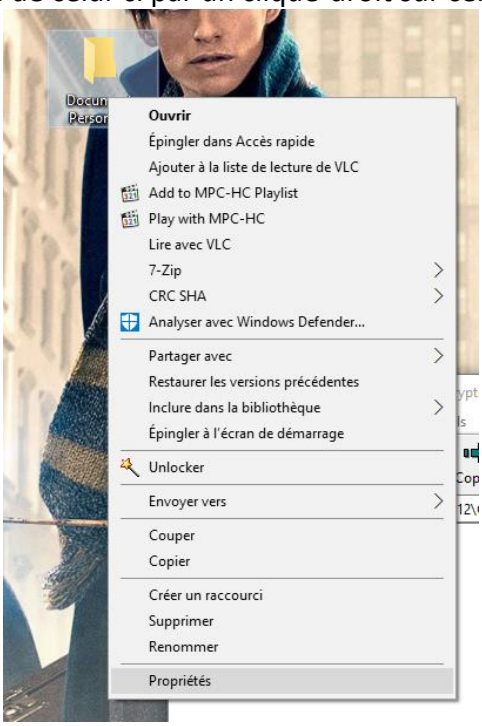
   - Axcrypt
   - Truecrypt
   - Encrypt on click
   - Lock Folder
   - GPG

Table des matières

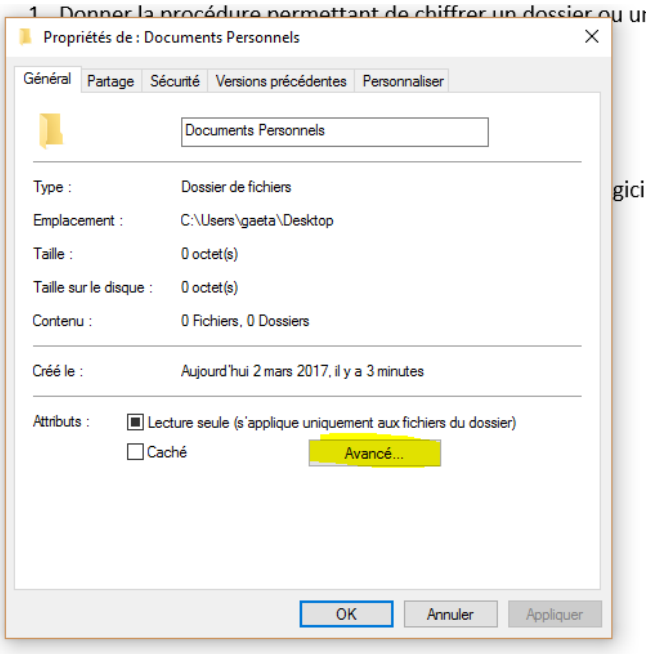
Procédure de chiffrement d'un dossier ou d'un fichier dans Windows

Nous allons donc aborder la technique de chiffrement que propose Windows pour les fichiers ou dossiers.

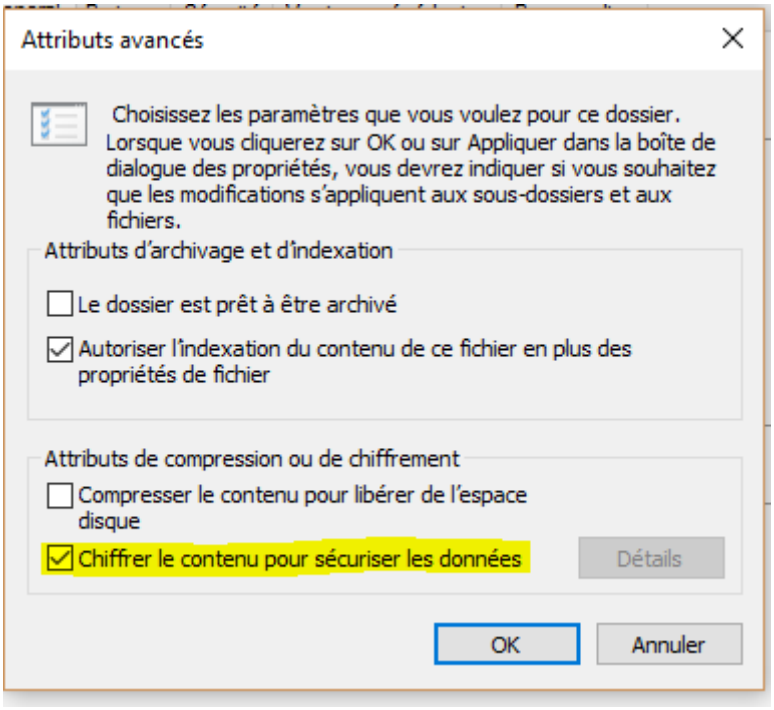
Il faut donc sélectionner un dossier ou un fichier que l'on souhaite chiffrer, dans ce cas j'ai choisis un dossier nommé « Documents Personnels ».
Il faut accéder à la propriété de celui-ci par un clique-droit sur celui-ci.



On se rend ensuite dans l'onglet « Général » puis « Avancé » de la fenêtre qui s'est ouverte.



Il faut ensuite cocher la case « Chiffrer le contenu pour sécuriser les données » et de validé ce choix en cliquant sur **OK**.



Il faut ensuite **appliquer** les paramètres et de cliquer à nouveau sur **OK** pour terminer.

Usage de la fonction Bitlocker

Présentation de Bitlocker :

Bitlocker est une technique de chiffrement de lecteur qui permet de sécuriser vos données par mot de passe. Celles-ci sont cryptées même si le système d'exploitation n'est pas démarré.

Prérequis à l'utilisation de Bitlocker :

Pour utiliser Bitlocker, il est nécessaire de posséder une version de Windows authentique parmi les versions suivantes :

- Windows Vista Intégrale, Ultimate, Business, Entreprise et Professionnelle,
- Windows 7 Intégrale et Entreprise,
- Windows Serveur 2008 et Serveur 2008 R2 ou supérieur,
- Windows 10 Professionnelle.

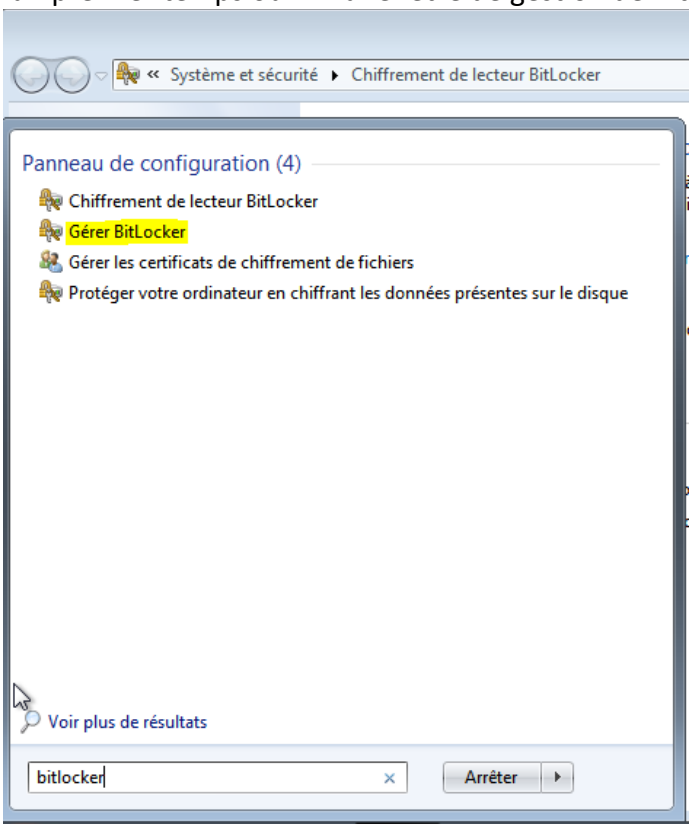
Différents modes de chiffrage mise en place par Bitlocker :

Bitlocker permet plusieurs types de chiffrage. Le premier de ceux-ci s'effectue via une puce TPM *(« Trusted Platform Module » C'est une puce dite de confiance qui peut crypter des données)*, avec un module TPM, la sécurité ne repose plus uniquement sur le support logiciel mais également sur un cryptage matériel liés au logiciel.
En second mode de chiffrage, l'utilisateur doit s'authentifier
Pour le démarrage de la machine soit par un code PIN ou bien par l'utilisation d'une clé USB contenant une clé valide.

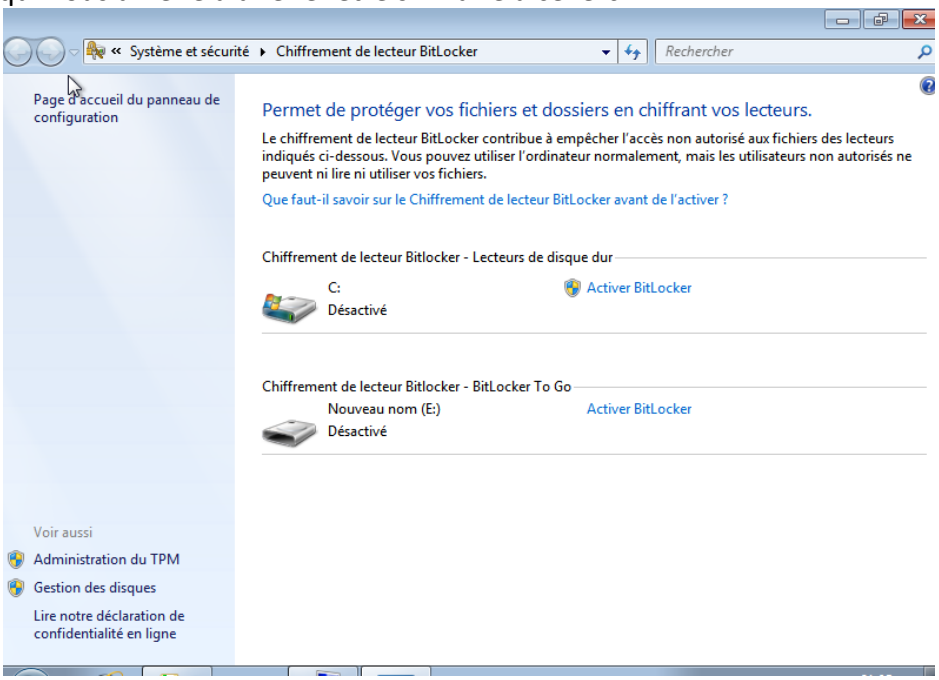
Mise en place de Bitlocker

Nous allons donc voir la mise en place de Bitlocker, ici sur un système Windows 7 Ultimate.

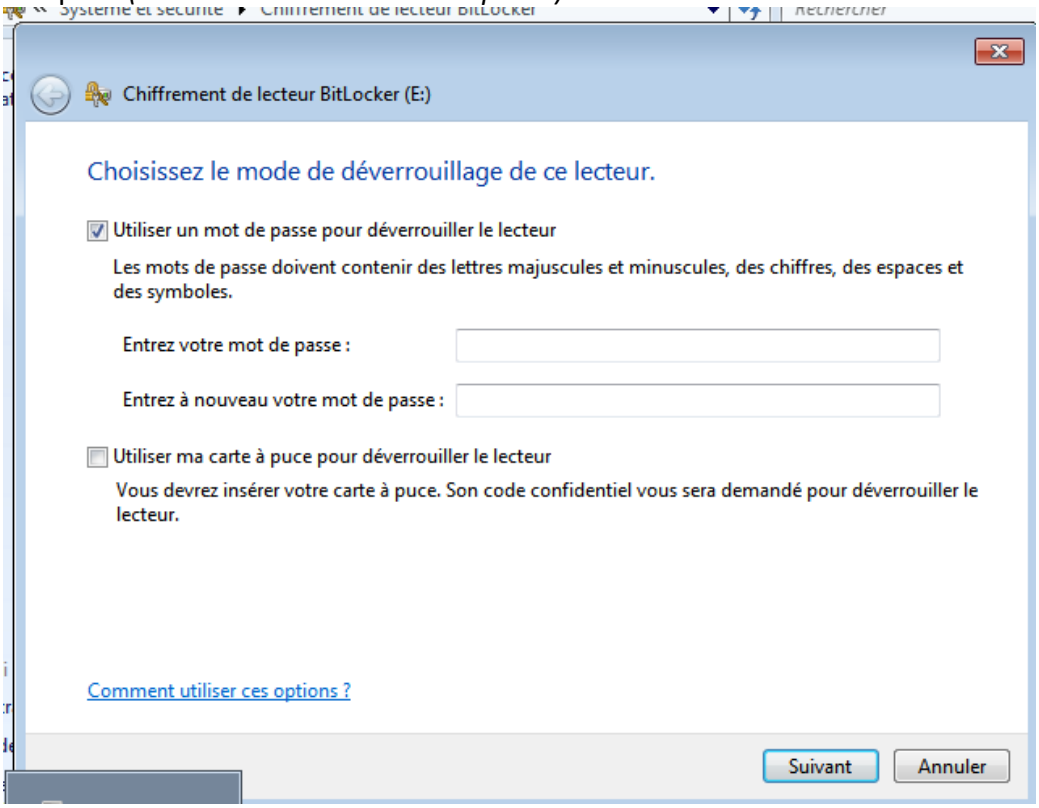
Il faut donc dans un premier temps ouvrir la fenêtre de gestion de Bitlocker



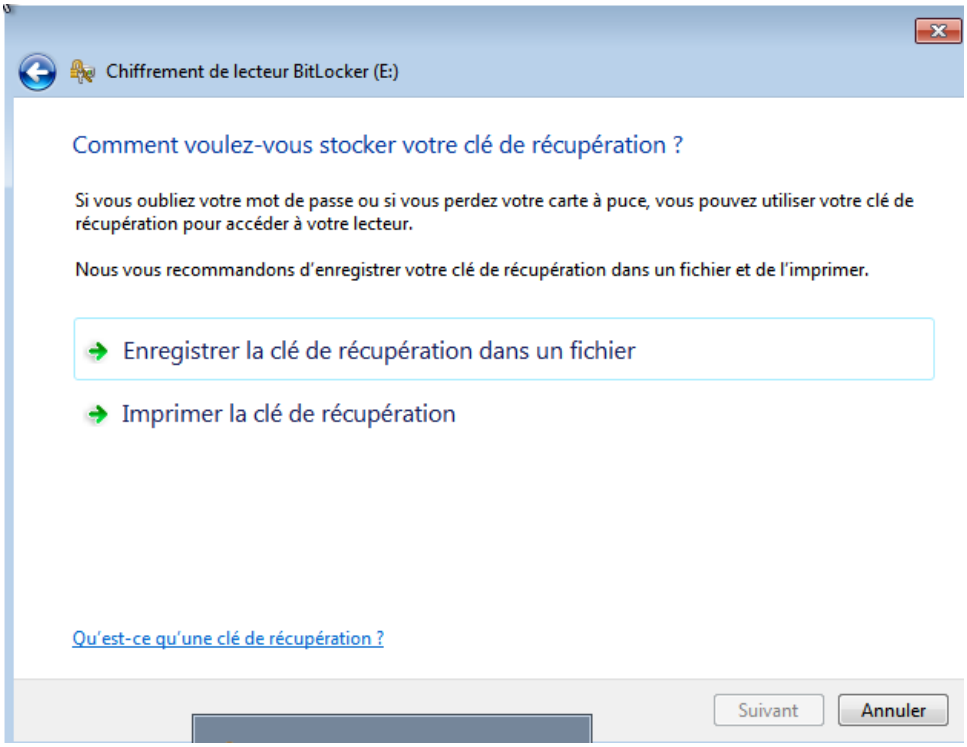
Ce qui nous amène à une fenêtre similaire à celle-ci :



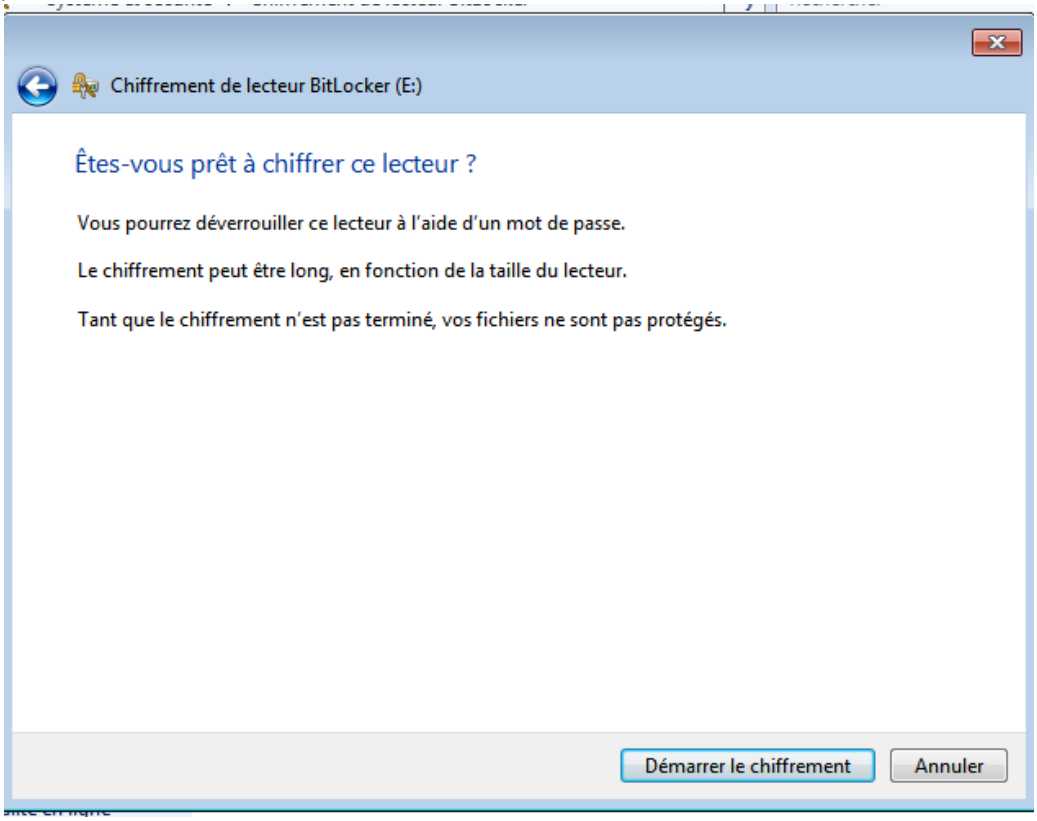
Nous allons ici choisir de chiffrer le lecteur via une clé USB *(Bitlocker To Go)* car je ne dispose pas de module TPM ce qui est nécessaire pour activé Bitlocker sur le lecteur principal.
Il nous est donc proposé de sécurisé le lecteur via un mot de passe ou bien via une carte à puce *(nous choisirons un mot de passe)*



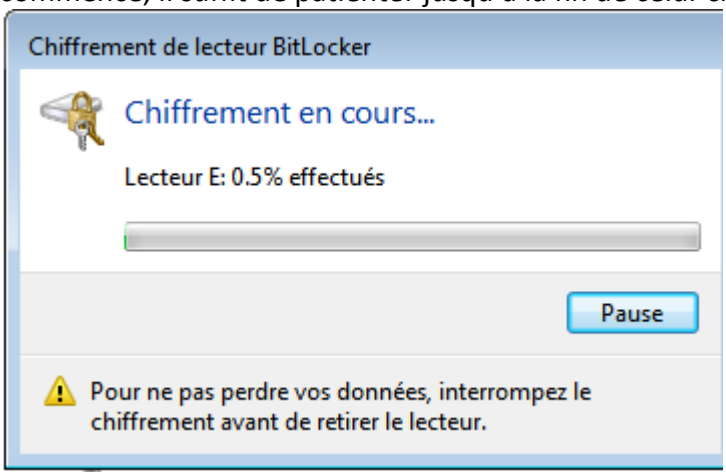
Il faut ensuite choisir le mode de stockage de la clé de récupération qui sera utile pour accéder au lecteur.



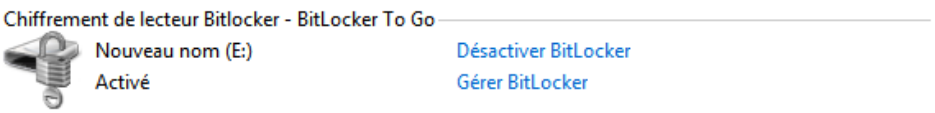
Nous choisirons de suivre les conseille de Windows et donc d'enregistrer la clé de récupération afin de l'imprimer. Une fois celle-ci enregistré dans un emplacement sûr, il faut démarrer le chiffrement du lecteur.



Le chiffrement commence, il suffit de patienter jusqu'à la fin de celui-ci.



Le lecteur est maintenant chiffré et les données qu'il contient sont sécurisé, il faut maintenant un mot de passe pour y accéder et le déverrouillé



Teste et documentation de différents outils logiciels

AxCrypt

Présentation

Il s'agit d'un outil disponible sur Windows qui permet de chiffrer document et fichier.

Fonctionnalités

Cet outil dispose d'une multitude de fonctionnalité détaillé ci-dessous :

- Cryptage fort grâce à une méthode de cryptage AES 128 ou 256-bit,
- Outil intuitif,
- Fonction de sécurisation automatique vers le cloud,
- Gestion des mots de passe,
- Vérification de l'intégrité des données,
- Résiste aux attaques « brute-force »
- Logiciel open sources sous License GNU.

Installation et utilisations

Pour l'installation de cet outil il faut au préalable se rendre sur le site de l'éditeur *(*axcrypt.net*)* afin de télécharger la version correspondante à votre installation Windows et de l'exécuter.

TrueCrypt

Présentation

Il s'agit d'un outil disponible sur Windows, Mac OS X et GNU/Linux qui permet de chiffrer document et fichier ainsi que chiffrer une partition entière ou un périphérique.

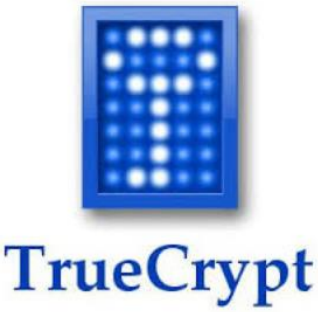
Fonctionnalités

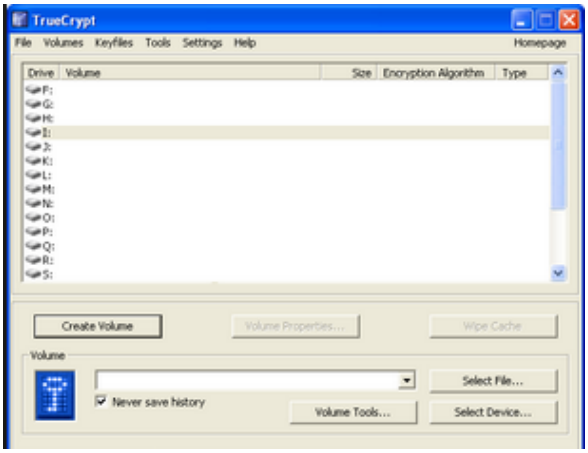
Cet outil dispose d'une multitude de fonctionnalité détaillé ci-dessous :

- Cryptage fort grâce à une méthode de cryptage AES-256-bit,
- Outil gratuit et code source disponible,
- Fonction de hachage cryptographique : RIPEMD-160
- Accélération matérielle au chiffrement/déchiffrement
- Gestion des mots de passe,

Installation et utilisations

Pour l'installation de cet outil il faut au préalable se rendre sur le site de l'éditeur [(http://truecrypt.sourceforge.net/)](http://truecrypt.sourceforge.net/) afin de télécharger la version correspondante à votre installation Windows/Mac OS X et GNU/Linux et de l'exécuter.





Encrypte on click

Présentation

Il s'agit d'un outil disponible sur Windows qui permet de compression et de chiffrement qui vous permet de sécuriser fichiers et dossier contenant des informations sensibles.

Fonctionnalités

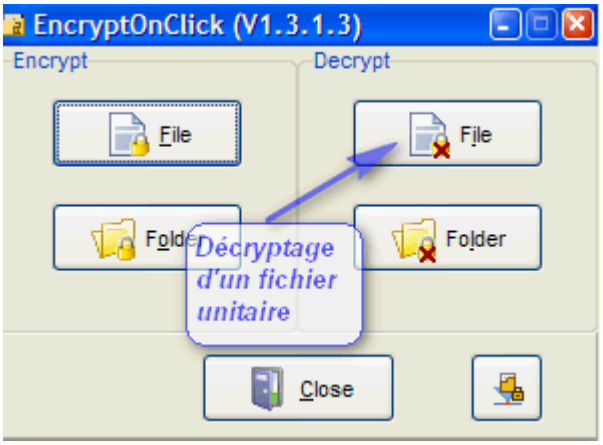
Cet outil dispose d'une multitude de fonctionnalité détaillé ci-dessous :

- Cryptage fort grâce à une méthode de cryptage AES-256-bit,
- Outil gratuit.
- EncryptOnClick logiciel fluide, rapide et facile d'utilisation.
- Gestion des mots de passe,

Installation et utilisations

Pour l'installation de cet outil il faut au préalable se rendre sur le site de l'éditeur (http://www.01net.com/telecharger/windows/Utilitaire/cryptage_et_securite/fiches/132286.html)

Afin de télécharger la version correspondante à votre installation Windows et de l'exécuter.



LockFolder

Présentation

Il s'agit d'un outil disponible sur Windows qui permet de chiffrer document et fichier.

Ce logiciel masquera vos fichiers sensibles afin qu'ils ne puissent pas être vus ou accessibles. Même les liens dans votre menu de documents récents ne seront pas en mesure de trouver vos fichiers cachés ! Pour plus de sécurité, utilisez un mot de passe pour empêcher quiconque d'accéder à vos fichiers. Vous pouvez exécuter ce logiciel en mode furtif afin que personne ne sait qu'il est là, et de masquer ou de montrer vos fichiers sensibles à l'aide de raccourcis clavier.

Fonctionnalités

Cet outil dispose d'une multitude de fonctionnalité détaillé ci-dessous :

- Cryptage fort grâce à une méthode de cryptage Blowfish 256-bit,
- Outil intuitif, complet et furtif
- Gestion des mots de passe,
- Vérification de l'intégrité des données,
- Résiste aux attaques « brute-force »
- Protection efficace face au virus et trojan.
- Logiciel Gratuit

Installation et utilisations

Pour l'installation de cet outil il faut au préalable se rendre sur le site de l'éditeur (https://www.lock-folder.com/) afin de télécharger la version correspondante à votre installation Windows et de l'exécuter.

GPG

Présentation

GnuPG (ou GPG, de l'anglais *GNU Privacy Guard*) est l'implémentation GNU du standard OpenPGP défini dans la RFC 4880[5], distribuée selon les termes de la licence publique générale GNU.

Ce logiciel permet la transmission de messages électroniques signés et chiffrés, garantissant ainsi leurs authenticité, intégrité et confidentialité.

GnuPG est un logiciel stable distribué dans tous les systèmes d'exploitation libres, notamment GNU/Linux.
Bien que le logiciel GnuPG soit doté d'une interface en ligne de commande, plusieurs applications ou extensions lui fournissent une interface graphique ; par exemple, il a été intégré entre autres à Mozilla Thunderbird et SeaMonkey via Enigmail, ou encore à KMail, le client de messagerie fourni avec KDE et enfin à Mail, le client de messagerie d'OS X, via GPGMail.

Fonctionnalités

Cet outil dispose d'une multitude de fonctionnalité détaillé ci-dessous :

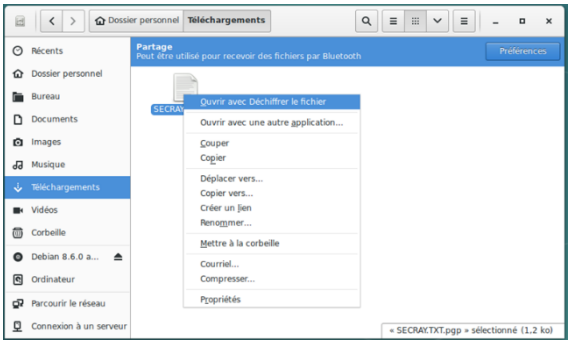
- Cryptage fort grâce à une méthode de cryptage AES 128 ou 256-bit,
- Utile pour les systèmes Linux
- Interface en ligne de commande
- Paramétrage Manuel
- Plusieurs applications ou extensions lui fournissent une interface graphique
- Disponible aussi sous Microsoft Windows et appareil Android
- Gestion des mots de passe,
- Logiciel open sources sous License GNU.

GnuPG est aujourd'hui communément utilisé, notamment depuis les révélations sur le programme de surveillance PRISM

Il figure parmi les outils généralement recommandés[11]. Sa robustesse face aux attaques de la NSA a été confirmée dans un article publié en décembre 2014 par *Der Spiegel*[12].

Installation et utilisations

Pour l'installation de cet outil il faut au préalable se rendre sur le site de l'éditeur https://www.gnupg.org/ afin de suivre le tutoriel et les consignes.


Dossier personnel
Téléchargements
Récents
Dossier personnel
Bureau
Documents
Images
Musique
Téléchargements
Vidéos
Corbeille
Debian 8.6.0 a...
Ordinateur
Parcourir le réseau
Connexion à un serveur
Partage
Peut être utilisé pour recevoir des fichiers par Bluetooth
Préférences
Ouvrir avec Déchiffrer le fichier
Ouvrir avec une autre application...
Couper
Copier
Déplacer vers...
Copier vers...
Créer un lien
Renommer...
Mettre à la corbeille
Courriel...
Compresser...
Propriétés
« SECRAY.TXT.pgp » sélectionné (1,2 ko)

Conclusion :

Le cryptage est très important dans le cadre de la sécurité informatique dans les entreprises. Il permet de sécurisée des données sensibles.

En effet chaque type de logiciels rencontrée on diffèrent avantage et inconvénient.