AxCrypt : Logiciel de chiffrement pour Windows

Guide d'installation rapide

Version 1.6.3

Mars 2007

Ce document décrit l'installation et la prise en main d'AxCrypt pour crypter, décrypter, éditer, enregistrer et envoyer des documents de façon confidentielle et sécurisée.

Table des matières:

1. Informations complémentaires

Ce guide d'utilisation contient seulement les informations de base nécessaires à l'installation et la prise en main du logiciel AxCrypt.

Consultez les ressources suivantes pour de plus amples informations:

Où	Quoi
http://axcrypt.sf.net	• Documentation complète • Respect de la vie privée • Foire aux questions (FAQ) • Utilisation en ligne de commande
http://www.axantum.com	• Introduction au chiffrement • Livre blanc 'About d'AES' • Livre blanc 'Public Key Based Licensing' • Informations concernant d'autres produits de chiffrement • A propos du concepteur d'Axcrypt
http://sf.net/projects/axcrypt	• Code source • versions Beta • Forums • Liste de diffusion

2. Environnement requis - limitations du produit

AxCrypt consomme peu de ressources et est compatible avec toutes les versions actuelles de Windows.

Ressource	Commentaire
Mémoire vive (RAM)	Environ 5 MO en exécution
Espace disque	2 méga-octets
Espace disque temporaire	Jusqu'à 1,5 fois la taille du fichier à chiffrer
Processeur	Pentium
Systèmes d'exploitation	Windows 98, ME, NT 4 sp 4, 2000, XP Home, XP Professional, 2003
Permissions de l'utilisateur	Tout utilisateur Windows peut utiliser AxCrypt
Permissions nécessaires pour l'installation	Permissions d'administrateur pour Windows NT, 2000, XP et 2003
Taille maximale de fichier	Environ 500 à 700 MO sous Windows 90 et ME. Limitation liée à l'espace disque disponible sous NTFS.
Nombre maximum de fichiers cryptés	Seulement limité par l'espace disque disponible
Environnement de développement	Pour recompiler AxCrypt à partir du code source téléchargeable, vous devez disposer de Visual Studio 2002 ou supérieur.

3. Procédure d'installation

Cette section explique comment installer AxCrypt, pas à pas.

> *Important : Vous devez être connecté sous un compte disposant de privilèges « Administrateur » pour installer AxCrypt sous Windows NT, 2000, XP ou 2003*

Procurez-vous la dernière version disponible d'AxCrypt

☞ Pour installer AxCrypt vous devez disposer du programme d'installation, téléchargez la dernière version disponible sur http://axcypt.sf.net avant de poursuivre.

Après téléchargement, vous pourrez choisir d'enregistrer le programme d'installation sur votre ordinateur et l'exécuter plus tard, ou l'exécuter directement depuis le site de téléchargement. Si vous l'exécutez directement, passer à la section 'Vérifier la signature numérique' ci-après.

Démarrez le programme d'installation

Le programme d'installation se nomme généralement AxCrypt-Setup.exe, mais il peut être suffixé du numéro de version, par exemple AxCrypt-1.6.exe.

Double-cliquez sur programme d'installation pour l'exécuter

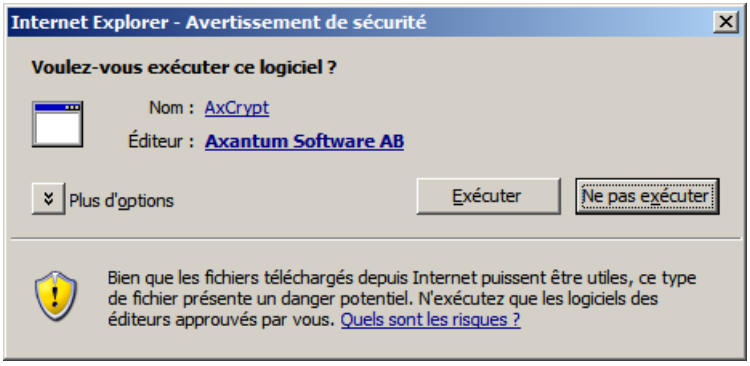
Vérifiez la signature numérique (Windows XP Service Pack 2 or supérieur)

Windows XP Service Pack 2 ou supérieur supporte la vérification automatique de signature numérique des programmes exécutables téléchargés depuis l'Internet, tel que le programme d'installation d'AxCrypt.

La signature numérique vous garantit, si elle est correctement vérifiée, que le logiciel n'a pas été altéré par un virus et qu'il ne contient pas de code malveillant.

AxCrypt est signé numériquement par Axantum Software AB, ce qui vous garantit son authenticité.

Vous devriez voir une boîte de dialogue comme celle-ci :



☞ Suivant votre système d'exploitation, il se peut qu'aucune boîte de dialogue n'apparaisse. Cependant si une boîte comme ci-dessus apparaît, mais indiquant que la signature ne peut être vérifiée ou comportant des indications suspectes, vous devez être prudent et vérifier l'origine de votre téléchargement.

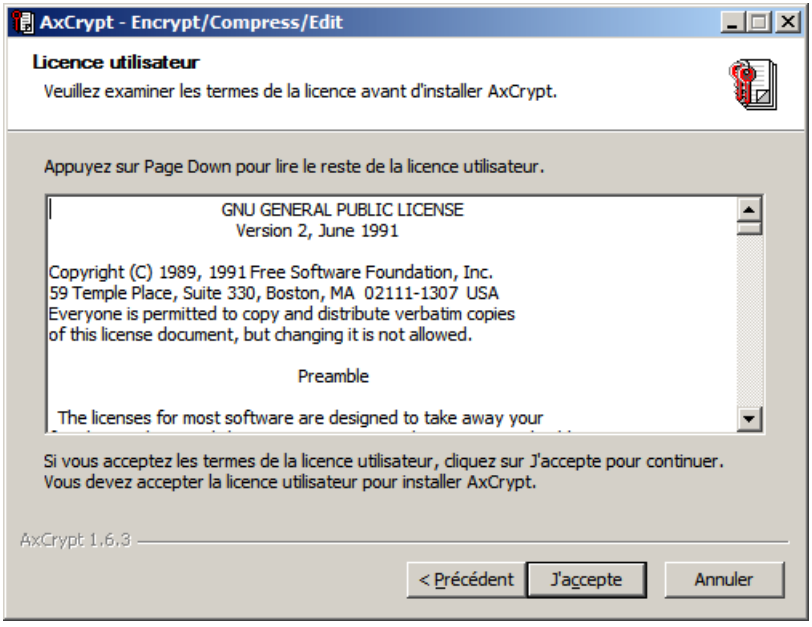
Choisissez la langue

AxCrypt supporte plusieurs langues pour son interface et ses commandes.

Sélectionnez la langue de votre choix, et cliquez sur le bouton OK.
La langue choisie sera utilisée pour la suite de l'installation, et dans les boîtes de dialogue et les menus de l'application AxCrypt.

Acceptation des conditions de la licence d'utilisation.

AxCrypt est distribué sous la licence GNU (General Public License). Il s'agit d'une licence "open-source" qui vous donne le droit d'utiliser librement le logiciel AxCrypt et de le distribuer à condition de ne pas le facturer et que toute modification du code source soit publiée.



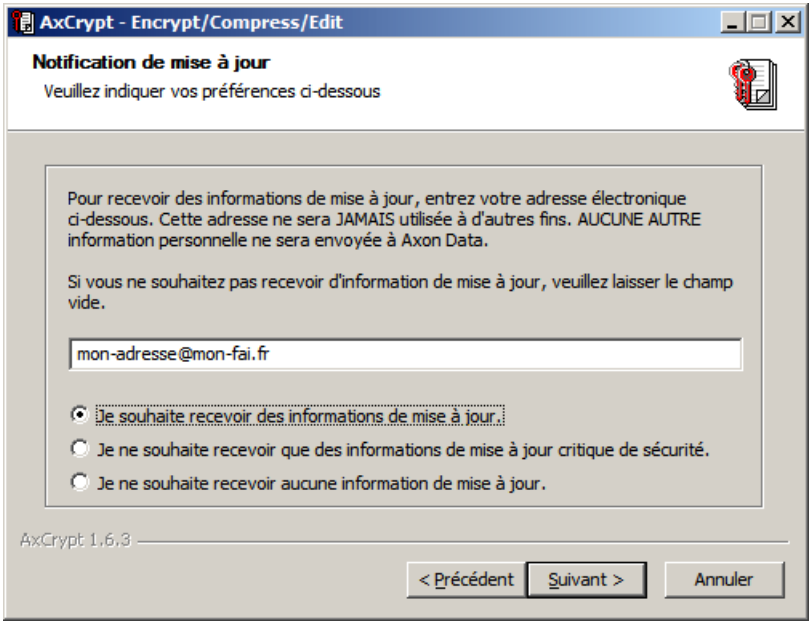
Prenez connaissance des termes de la licence et cliquez sur « J'accepte » si vous les approuvez.

Notifications de mise à jour

Tout utilisateur d'AxCrypt peut bénéficier d'informations gratuites de mise à jour. Plusieurs niveaux de notification sont disponibles :

- Pour toute mise à jour du logiciel
- Uniquement pour les mises à jour critiques de sécurité
- Aucune notification (non recommandé)

Merci de ne pas mentionner une adresse invalide ! Laissez le champ vide si vous ne souhaitez pas être notifié

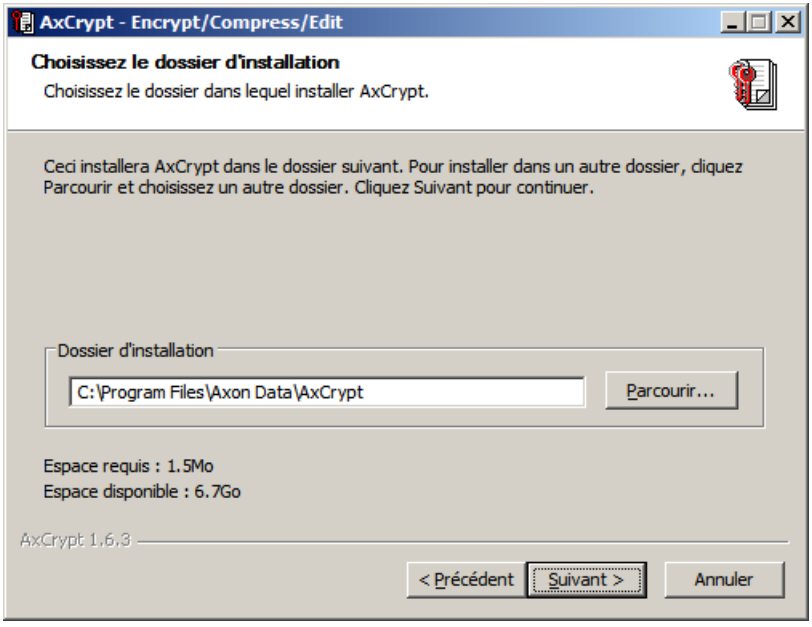


☞ Saisissez et vérifier votre adresse de messagerie ou laissez le champ vide.

Sélectionnez le niveau de notification souhaité puis cliquez sur le bouton Suivant

Sélection du répertoire d'installation (utilisateurs avancés seulement)

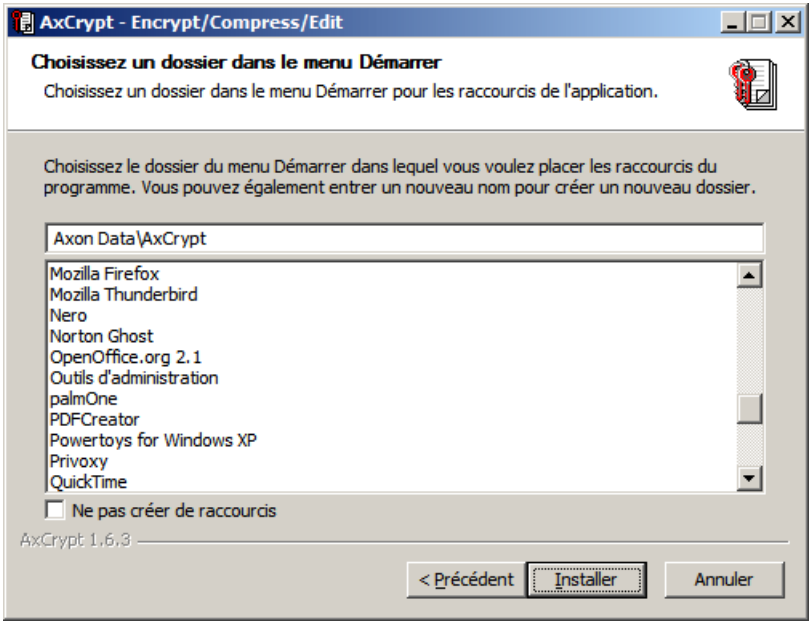
Vous pouvez spécifier le dossier dans lequel l'application sera installée sur votre ordinateur. En principe il n'y a pas lieu de changer le point d'installation proposé par défaut. Modifiez-le uniquement si vous avez une raison de le faire.



Cliquez sur le bouton Suivant

Sélection du dossier du menu « Démarrer » (utilisateurs avancés seulement)

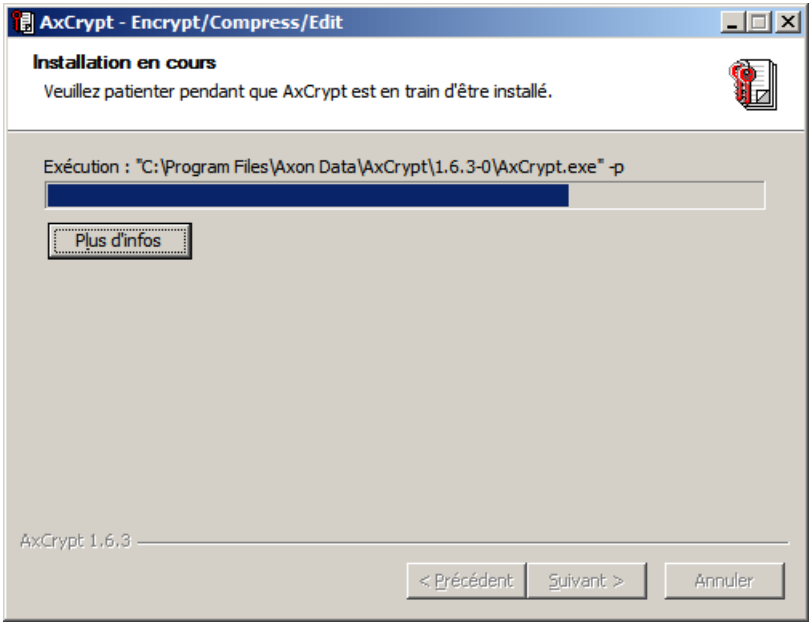
Vous pouvez spécifier le dossier du menu Démarrer dans lequel les raccourcis de l'application seront créés. En principe il n'y a pas lieu de changer le dossier proposé par défaut. Modifiez-le uniquement si vous avez une raison de le faire.



Cliquez sur le bouton Installer

Le programme s'installe

Vous pouvez suivre l'avancement de l'installation dans la barre de progression. La durée de l'installation varie de 5 à 20 secondes.

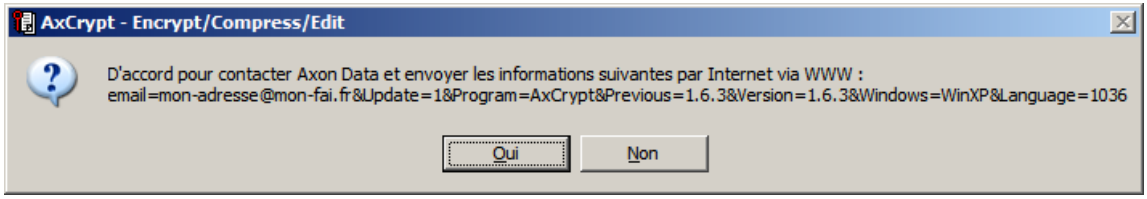


Accepter la connexion à Internet

Si vous avez choisi d'être informé des mises à jour, AxCrypt va maintenant se connecter au serveur d'Axantum pour lui communiquer les informations nécessaires.

Cependant, même si vous avez choisi de ne pas être averti des mises à jour, nous souhaiterions recevoir quelques informations de bases relatives à l'installation, mais aussi tout simplement savoir que le logiciel est utilisé. C'est souvent le seul retour que nous ayons et nous vous remercions d'accepter.

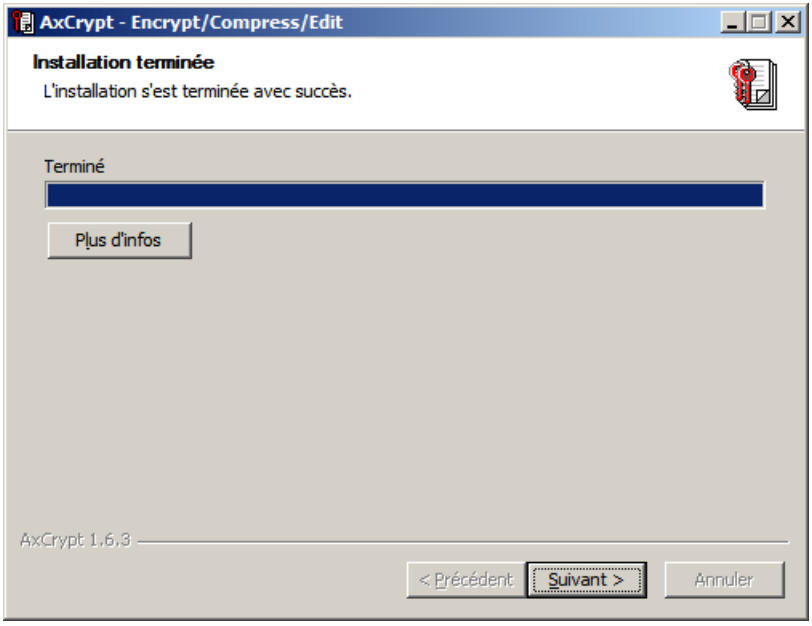
Aucune information personnelle ne sera transmise Vous pouvez consulter notre politique de confidentialité à l'adresse **http://axcrypt.sf.net** ainsi que le détail des informations transmises. La chaîne transmise apparaît également dans la boîte de dialogue :



Cliquez sur Oui ou Non selon votre choix.

Installation terminée

L'installation est maintenant terminée. Lisez le chapitre suivant pour apprendre à utiliser AxCrypt.



Cliquez sur le bouton Suivant, puis Fermer.

4. Mode d'emploi

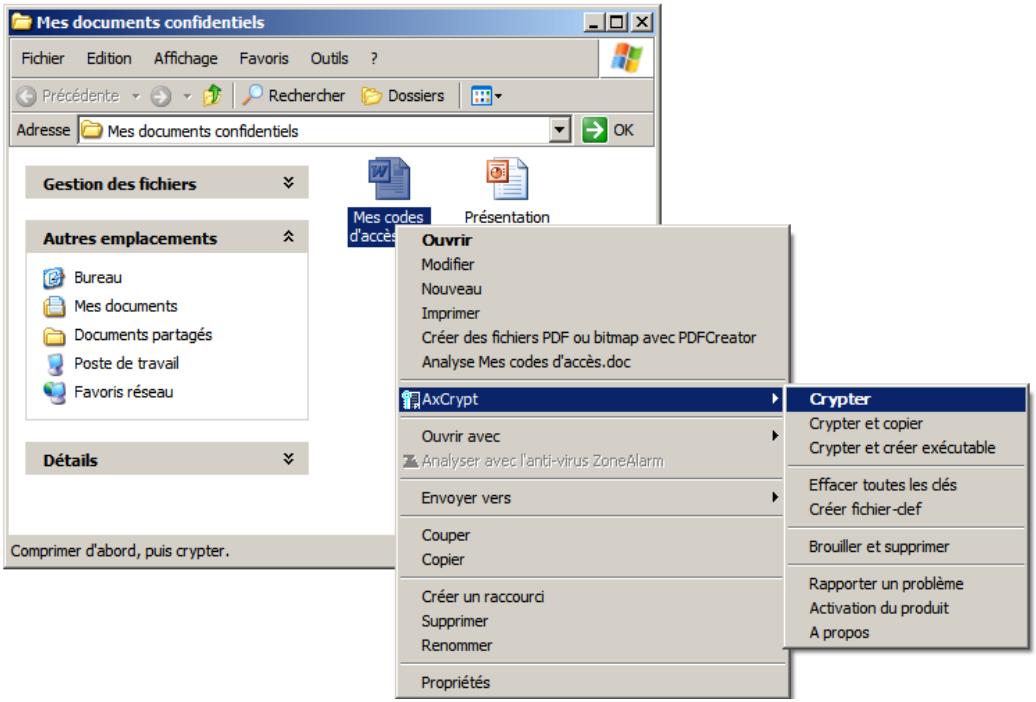
AxCrypt peut être utilisé en ligne de commande, appelé depuis d'autres programmes ou depuis le menu contextuel de l'explorateur Windows. Le mode intégré dans l'explorateur Windows sera abordé dans ce guide. Consultez la page d'accueil du produit sur Internet pour les autres possibilités.

L'explorateur Windows gère l'affichage de votre bureau. C'est un composant de Windows communément utilisé pour l'affichage et le parcours de vos dossiers et documents, lorsque vous double-cliquez pour ouvrir par exemple.

Menu contextuel

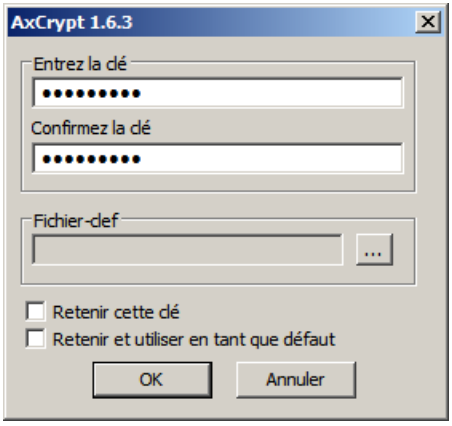
Si l'on peut ouvrir un document par double-clic avec l'explorateur Windows, il est également possible de faire un clic droit pour afficher un menu de choix spécifique à un document.

Ce menu de choix est appelé *menu contextuel*, vous y retrouverez la plupart des fonctionnalités d'AxCrypt.



Crypter

Pour crypter, faire un clic droit sur le fichier, puis dans le sous-menu contextuel AxCrypt, sélectionnez Crypter. Vous devrez choisir un mot de passe (ou phrase secrète), et optionnellement un fichier-clé.



L'utilisation d'un fichier-clé permet de mettre en œuvre pleinement la robustesse du chiffrement d'AxCrypt, mais cette fonctionnalité dépasse l'objet de ce guide de prise en main.
Saisissez un mot de passe ou mieux, une phrase secrète (plusieurs mots). Ce secret protègera vos documents des regards indiscrets et des attaques de personnes malveillantes.

☞ **Notez que le chiffrement ne protège pas contre la perte de données. Une copie de sauvegarde régulière est la seule prévention efficace de ce risque**.

Saisissez votre phrase secrète une seconde fois pour vérification. Il est absolument essentiel de contrôler votre saisie et de vous souvenir de cette phrase secrète.

Cliquez sur OK

☞ **Il n'y a pas de fonction masquée de recouvrement dans AxCrypt. Si vous oubliez la phrase secrète, vos documents seront définitivement irrécupérables. Pour prévenir ce genre d'accidents, vous devez préalablement les imprimer ou les sauvegarder et les conserver en lieu sur.**

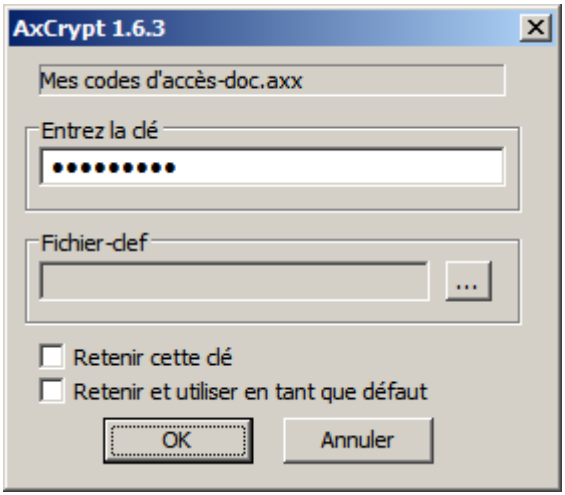
Ouvrir un document crypté.

Un document crypté est suffixé par l'extension .axx et apparaît avec l'icône d'AxCrypt.

Pour décrypter un document temporairement (pour le consulter ou le modifier), double-cliquez sur le document, il sera ouvert avec l'application d'origine. Lorsque vous fermerez l'application, il sera automatiquement recrypté s'il a été modifié.

Décrypter un document crypté.

Pour décrypter un document de façon permanente, faites un clic droit et sélectionnez « Décrypter » dans le sous-menu contextuel d'AxCrypt, puis saisissez la phrase secrète :



Cliquez sur OK

Le fichier sera décrypté et restauré dans son état original (nom et extension).

Mémorisation temporaire de la phrase secrète

AxCrypt a la capacité de mémoriser plusieurs phrases secrètes pour les opérations de déchiffrement, et une phrase secrète par défaut pour les futurs chiffrements.

Cette mémorisation ne dure que le temps de votre session Windows.

☞ Si vous utilisez la mémorisation de phrase secrète, vous devez protéger votre écran de veille par un mot de passe et ne pas laisser votre ordinateur sans surveillance.

Pour utiliser cette fonctionnalité, cochez la cas « Retenir cette clé » dans la boîte de dialogue (voir partie inférieure de l'écran ci-dessus)

Toutes les options d'AxCrypt sont « rémanentes », ce qui signifie que votre dernier choix pour une option sera automatiquement proposé par défaut.

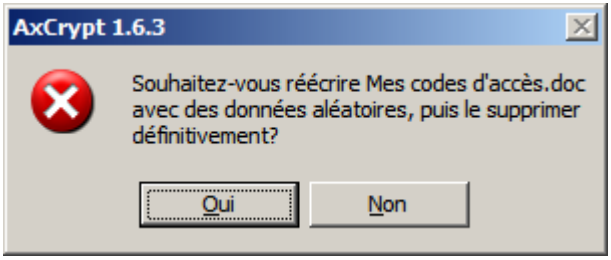
Effacement sécurisé de fichiers (brouillage)

Lorsque vous supprimez des fichiers, ceux-ci peuvent être facilement récupérés grâce à de nombreux outils tiers disponibles sur Internet. Un outil de ce type est même intégré aux versions les plus récentes de Windows (La restauration depuis la corbeille)

Avec AxCrypt, vous pouvez choisir de supprimer des fichiers et documents (et leur contenu) de façon définitive.

Sélectionnez les fichiers que vous souhaitez broyer et sélectionnez « *Brouillez et supprimer* » dans le menu contextuel d'AxCrypt

Une confirmation vous sera systématiquement demandée, car cette opération est irréversible.



Cliquez sur Oui ou Non selon votre choix

Si vous choisissez Oui, les fichiers sélectionnés seront réécrits avec des données aléatoires avant d'être supprimés définitivement.

Utilisation avancée

AxCrypt propose de nombreuses fonctionnalités pour une utilisation avancée. Celles-ci seront simplement listées dans ce guide :

- Possibilité de renommer des fichiers cryptés avec des noms « anonymes » (sans rapport avec le nom original). Le nom original sera toujours restauré lors du déchiffrement du fichier.
- Possibilité de créer des fichiers cryptés auto-extractibles pour les envoyer à des correspondants qui n'ont pas installé AxCrypt.
- Il existe un programme AxDecrypt qui comporte uniquement la fonction de déchiffrement de fichier pour les visualiser. Ce programme peut être utilisé sans qu'il soit nécessaire d'installer toute l'application.
- Vous pouvez créer et utiliser des fichier-clés. Il s'agit de fichiers contenant des clés de cryptage robustes générées aléatoirement. Cette méthode vous garantit que le cryptage de vos fichiers ne sera pas vulnérable suite au choix d'un mot de passe faible. Ces fichiers doivent impérativement être sauvegardés sur des supports amovibles tels que des lecteurs USB.

5. Informations relatives à la sécurité

Le chiffrement à lui-seul ne vous garantit pas une sécurité totale. C'est un outil indispensable, mais qui doit être utilisé avec discernement. Un outil unique répondra rarement à tous les besoins de sécurité.

Cette section aborde quelques points complémentaires relatifs à l'utilisation de produits de chiffrement tels qu'AxCrypt, notamment sous l'aspect de la confidentialité et de l'intégrité.

Le niveau de sécurité garanti par AxCrypt

Les caractéristiques suivantes s'appliquent à un fichier crypté avec AxCrypt :

- Si vous utilisez un fichier-clé, vos informations seront protégées par la robustesse du chiffrement AES-128 bits, considéré comme non-cassable à l'heure actuelle.
- Si vous utilisez seulement une phrase secrète, AxCrypt protègera vos informations dans la limite de la robustesse de cette phrase secrète. Si elle est trop courte, le niveau de protection s'en ressentira. Toute chaîne inférieure à 10 caractères est courte. Pour bénéficier pleinement de la robustesse du chiffrement 128 bits, il faut une chaîne non signifiante d'une longueur minimum de 22 caractères.

☞ Si vous souhaitez obtenir de plus amples informations sur la sécurité de l'algorithme de chiffrement AES-128 et d'AxCrypt, lisez le livre blanc « About AES » disponible sur le site web d'AxCrypt **http://www.axantum.com**

Contournement de la sécurité

L'algorithme AES-128, et par conséquent AxCrypt, est actuellement considéré comme non-cassable, dès lors que vous utilisez un fichier-clé. Pour autant, peut-on en déduire que vous êtes en sécurité ? Pas nécessairement. Comme toujours, la meilleure façon de franchir une barrière consiste à la contourner. Cette règle s'applique également au chiffrement.

Voici différents moyens de contournement de la sécurité d'AxCrypt :

- Lorsque vous éditez ou visualisez des documents sur un ordinateur, les applications ou le système peuvent conserver des copies partielles ou complètes dans des dossiers temporaires ou dans le fichier de mémoire virtuelle du système. Ceci est vrai pour Word et Excel par exemple.
- Il est possible qu'un enregistreur de clavier (matériel ou logiciel) soit installé à votre insu sur votre ordinateur. Ce dispositif peut permettre de capter votre phrase secrète.
- Vous pouvez être confronté à des contraintes légales, économiques ou physiques pour vous obliger à révéler la phrase secrète.

Il s'agit de quelques exemples de contournement d'AxCrypt. Les parades à ces situations variées diffèrent selon le cas de figure.