# Chiffrer fichiers et dossiers avec TrueCrypt

Emanuele Prestifilippo

Le chiffrement, aussi appelé cryptage, est l'opération qui consiste à transformer un message pour rendre sa compréhension impossible à toute personne qui n'a pas la clé pour le déchiffrer. Avec cette technique, non seulement votre transmission d'informations est sûre mais vos documents sont aussi protégés contre les accès de personnes non autorisées.

Le chiffrement s'appuie sur deux éléments :

- Une clé de chiffrement qui peut être symétrique (cryptographie symétrique) ou asymétrique (cryptographie asymétrique).
- L'algorithme qui combiner la clé de chiffrement et le message à chiffrer pour rendre le contenu illisible.

Pendant l'installation d'Ubuntu, il est possible de créer une partition chiffrée, mais il existe aussi de nombreux programmes qui permettent de chiffrer les fichiers, les dossiers et les partitions ; voyons comment utiliser TrueCrypt.

## Présentation de TrueCrypt

TrueCrypt est un logiciel de chiffrement gratuit et multi-plate-forme. L'interface graphique de la version pour Linux est disponible uniquement en anglais, mais il est assez simple à utiliser. Il permet d'utiliser plusieurs algorithmes de chiffrement et de créer des volumes, le chiffrement est automatique et transparent ; pour protéger vos fichiers et dossiers, placez-les dans un volume chiffré, c'est-à-dire un disque virtuel chiffré à l'intérieur d'un fichier qui peut être monté comme un disque réel. Avec TrueCrypt, vous chiffrez aussi une partition entière d'un disque dur ou un périphérique (clé USB, carte mémoire, etc.).

## Installer TrueCrypt

TrueCrypt n'est pas disponible dans les dépôts d'Ubuntu (les serveurs centralisés contenant des programmes). Pour l'installer, visitez le site officiel du projet à l'adresse *http://www.truecrypt.org/*, rendez-vous dans la section *Downloads,* sélectionnez grâce à la liste déroulante le paquet *Standard - 32-bit* ou *Standard - 64-bit* et cliquez sur le bouton *Download*.

**Note :** pour déterminer rapidement si votre système utilise une installation d'Ubuntu à 32 ou 64 bits et ainsi choisir le paquet de TrueCrypt adapté à votre configuration, ouvrez un terminal et tapez la commande `getconf LONG_BIT` Vous recevrez comme résultat 32 ou 64, c'est-à-dire le nombre de bits de la configuration de votre noyau (*kernel* en anglais).

Ouvrez le dossier où vous avez enregistré l'archive tar.gz, extrayez-le d'un clic droit de souris sur l'icône du fichier truecrypt (par exemple truecrypt-7.1-linux-x86.tar.gz) et dans le menu qui s'affiche, sélectionnez *Extraire ici*. Un nouveau fichier est créé dans le même dossier, double-cliquez dessus pour lancer l'installation du programme et dans la fenêtre qui apparaît, cliquez sur le bou-

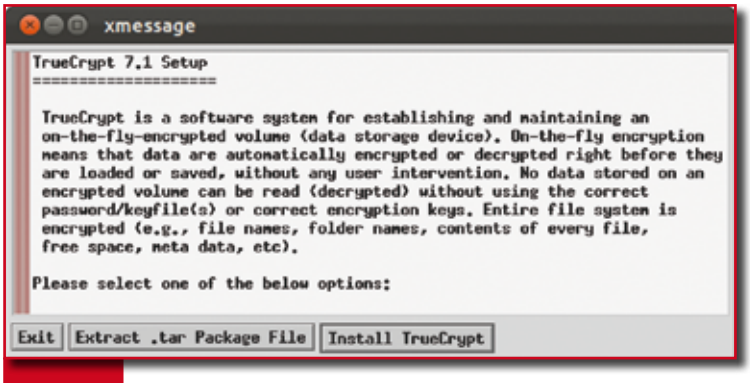


**Figure 1.** *La fenêtre d'installation de TrueCrypt*

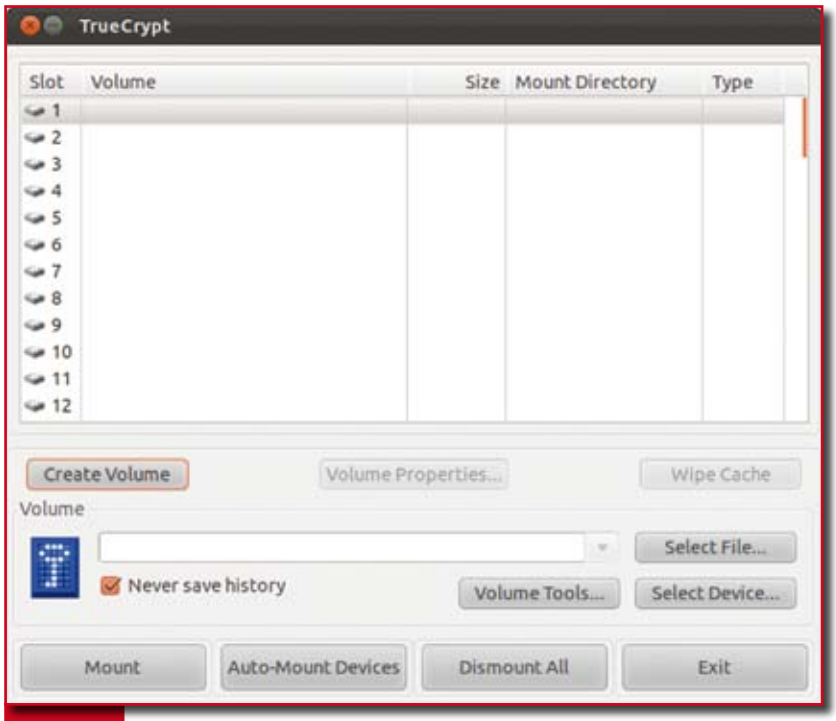


**Figure 2.** *La fenêtre principale de TrueCrypt*

ton *Lancer dans un terminal*. Dans la nouvelle fenêtre qui s'ouvre, cliquez sur le bouton *Install TrueCrypt*, lisez et acceptez les termes de la licence en cliquant sur le bouton *I accept* puis sur le bouton *Ok*. À l'invitation, insérez le mot de passe du super-utilisateur root et cliquez sur *S'authentifier*. Pour finir, appuyez la touche [*Entrée*] du clavier.

L'installation terminée, lancez le programme en cliquant sur l'icône d'Ubuntu dans la barre des lanceurs, tapez *truecrypt* dans la case de recherche et cliquez sur l'icône de TrueCrypt dans les résultats.

## Utiliser TrueCrypt

À l'ouverture du programme, la fenêtre principale apparaît. La partie haute contient la liste des slots libres et des volumes montés, le bas de la fenêtre contient les boutons pour la création et la gestion des volumes.

### Créer un volume

La première étape consiste à créer un nouveau volume ; pour ce faire, cliquez sur le bouton *Create Volume* pour ouvrir la fenêtre de l'assistant à la création d'un volume. Vous devez choisir où créer le nouveau volume, sélectionnez la première option


**Figure 3.** *La fenêtre de l'assistant à la création du volume*

pour créer un disque virtuel chiffré dans un fichier ou la seconde option pour chiffrer une partition entière d'un disque dur ou un périphérique.

Dans notre exemple, nous choisissons la première option : sélectionnez *Create an encrypted file container* et cliquez sur le bouton *Next* pour continuer. La nouvelle page qui s'affiche vous demande de choisir si vous souhaitez un volume TrueCrypt standard ou caché, choisissez la première option *Standard TrueCrypt volume* et cliquez sur *Next*. Dans la page qui suit, cliquer sur le bouton *Select File* ouvre la fenêtre d'exploration de votre système de fichiers, choisissez l'emplacement et le nom du fichier volume, cliquez sur *Enregistrer* pour fermer la fenêtre et sur *Next* pour avancer.

**Note :** le fichier contenant le volume chiffré est un fichier comme tous les autres, il peut être déplacé, renommé et effacé comme tout fichier normal.

L'étape suivante permet de sélectionner l'algorithme de chiffrement et l'algorithme de hachage pour le volume. Si vous ne savez pas lesquels choisir, laissez les options prédéfinies ; votre choix fait, cliquez sur *Next*. Comme tous les disques ou partitions, même le volume virtuel que nous créons doit avoir une dimension pré-établie, insérez maintenant sa dimension en Ko, Mo ou Go, choisissez bien parce que vous ne pourrez plus la modifier par la suite ; cliquez sur *Next* pour continuer.

Dans la page suivante, l'assistant vous invite à insérer et confirmer un mot de passe pour accéder au volume. En complément du mot de passe, vous pouvez choisir un fichier appelé keyfile, c'est-à-dire un fichier dont le contenu est combiné avec un mot de passe ; jusqu'à ce que le fichier keyfile correct soit fourni, aucun volume qui l'utilise ne peut être monté. Votre mot de passe confirmé, cliquez sur le bouton *Next*.

**Note :** il est très important de choisir bon un mot de passe pour garantir la sécurité de vos données. Pour avoir un mot de pas-

se sûr, TrueCrypt conseille d'utiliser 20 caractères au minimum, des numéros, des caractères spéciaux, des lettres majuscules et minuscules. Évitez d'utiliser les suites de numéros et les mots communs.

La nouvelle page vous invite à choisir le système de fichiers du volume grâce à la liste déroulante *Filesystem type*, cliquez sur *Next* et déplacez le pointeur de la souris durant environ 30 secondes à l'intérieur de la fenêtre de l'assistant, cela vous permet de générer une clé de chiffrement du volume de façon aléatoire en fonction de la position du curseur dans la fenêtre. Plus vous bougez la souris, plus le niveau de sécurité de la clé de chiffrement augmente. Quand vous êtes prêt, cliquez sur *Format* pour lancer la création du volume, un message vous informe de la fin de l'opération, cliquez sur *Valider* et dans la page qui suit, cliquez sur *Next* pour ajouter un autre volume ou sur *Exit* pour fermer l'assistant.

### Monter le volume

Il ne vous reste qu'à monter le volume créé, cliquez sur le bouton *Select File ;* dans la fenêtre qui s'ouvre, choisissez le fichier du volume à monter et cliquez sur le bouton *Ouvrir.* Dans le bas de la fenêtre de TrueCrypt, le parcours du fichier apparaît, sélectionnez une ligne dans la liste des volumes et cliquez sur le bouton *Mount* pour le monter. Entrez le mot de passe du volume et cliquez sur *Valider*. À l'invitation, insérez le mot de passe de l'administrateur root et cliquez sur le bouton *Valider.* Une fois monté, le volume est considéré comme un support externe, vous pouvez l'ouvrir avec Nautilus (le gestionnaire de fichiers par défaut d'Ubuntu) et ainsi, commencer à archiver les fichiers et les dossiers que vous désirez protéger.

Pour monter un volume, vous pouvez aussi cliquer avec la touche droite de la souris sur un slot libre dans la liste en haut de la fenêtre et dans le menu qui s'affiche, sélectionnez la voix *Select File and Mount*.

Pour démonter le volume, sélectionnez-le dans la liste des volumes et cliquez sur le bouton *Dismount*. Cliquer sur le bouton *Dismount All* démonte tous les volumes montés.

### Changer le mot de passe du volume

Pour changer le mot de passe d'un volume, sélectionnez-le dans la liste s'il est monté ou sélectionnez le fichier à l'aide du bouton *Select File* ; allez dans le menu *Volume –> Change Volume Password* ou cliquez sur le bouton *Volume Tools* et dans le menu qui s'affiche, choisissez *Change Volume Password*. La fenêtre qui s'ouvre contient les champs pour modifier le mot de passe et d'utilisation éventuelle d'un keyfile.

### Faire des copies de sauvegarde

Il est toujours recommandé de faire régulièrement des copies de sauvegarde de vos données pour éviter toute perte d'information en cas de problèmes. Pour faire la copie de sauvegarde d'un volume, préférez le clonage du volume à la simple copie du fichier du volume ; créez un nouveau volume avec les mêmes caractéristiques que celui à cloner et, après l'avoir monté, copiez manuellement les fichiers avec le gestionnaire de fichiers.

**Attention :** si vous dupliquez le fichier d'un volume et utilisez à la fois le volume et le clone de façon telle qu'ils contiennent des données différentes, vous diminuez la sécurité de vos données car les deux volumes partagent la même clé de chiffrement.

### Configurer TrueCrypt

La fenêtre des préférences de TrueCrypt est accessible par le menu *Settings –> Preferences*. Dans l'onglet *System Integration,* cochez la case *Open Explorer window for successfully mounted volume* pour parcourir le volume avec Nautilus quand il est monté avec succès. Utilisez l'onglet *Mount Options* pour modifier les options de montage des volumes et l'onglet *Keyfiles* pour ajouter et supprimer les fichiers keyfile.

## Conclusion

Chiffrer vos fichiers et dossiers n'a jamais été aussi simple. TrueCrypt est très pratique et facile à utiliser. La création des volumes est simplifiée grâce à l'assistant et leur gestion se fait de façon très intuitive.

Vous trouverez intéressante la liste des volumes favoris, surtout si vous décidez d'utiliser de nombreux volumes.

Voici deux programmes du même genre susceptibles de vous intéresser : Cryptkeeper et EasyCrypt. ■

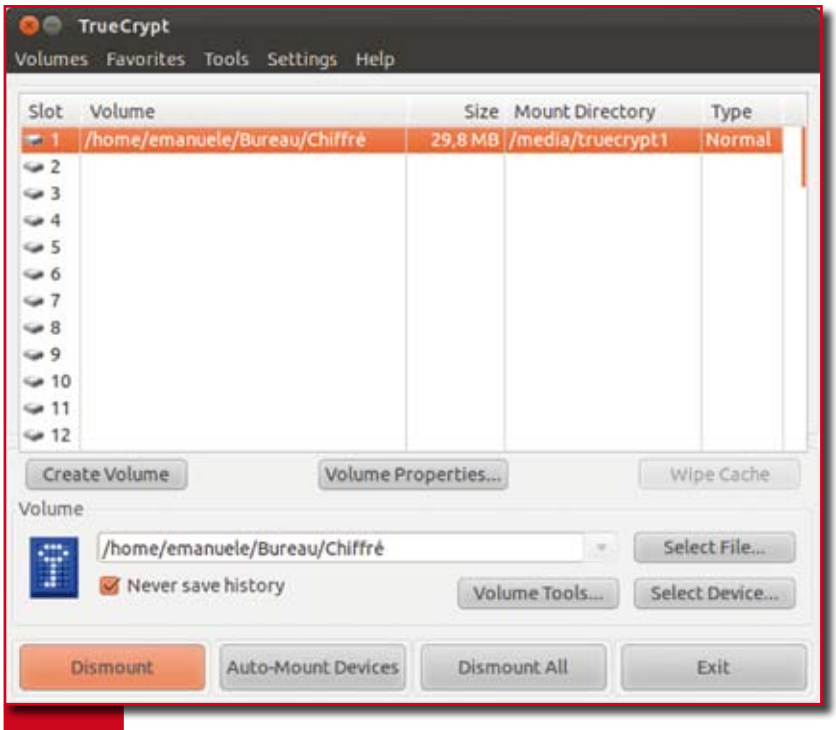


***Figure 4.*** *La fenêtre principale après avoir monté un volume*