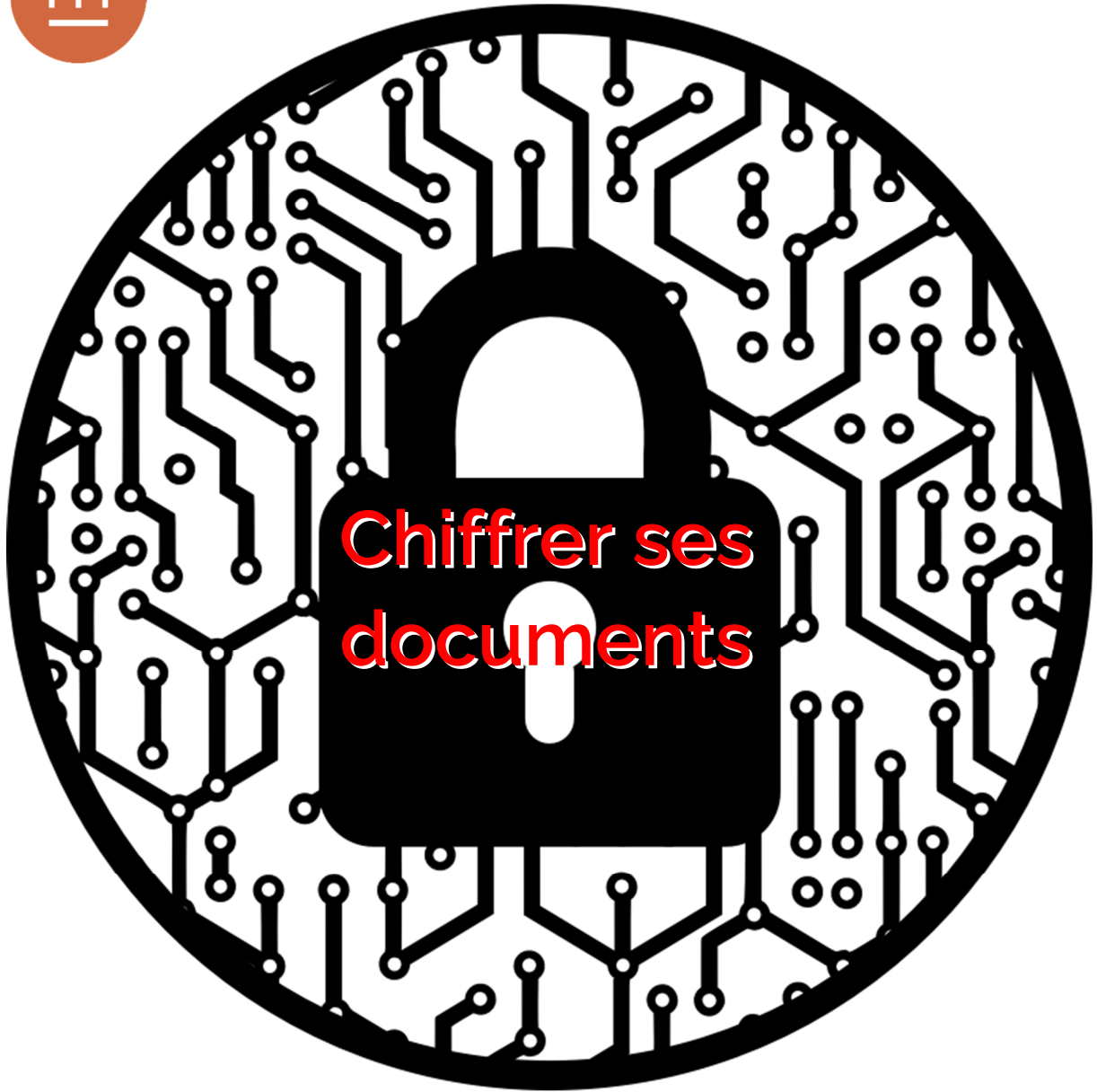


13

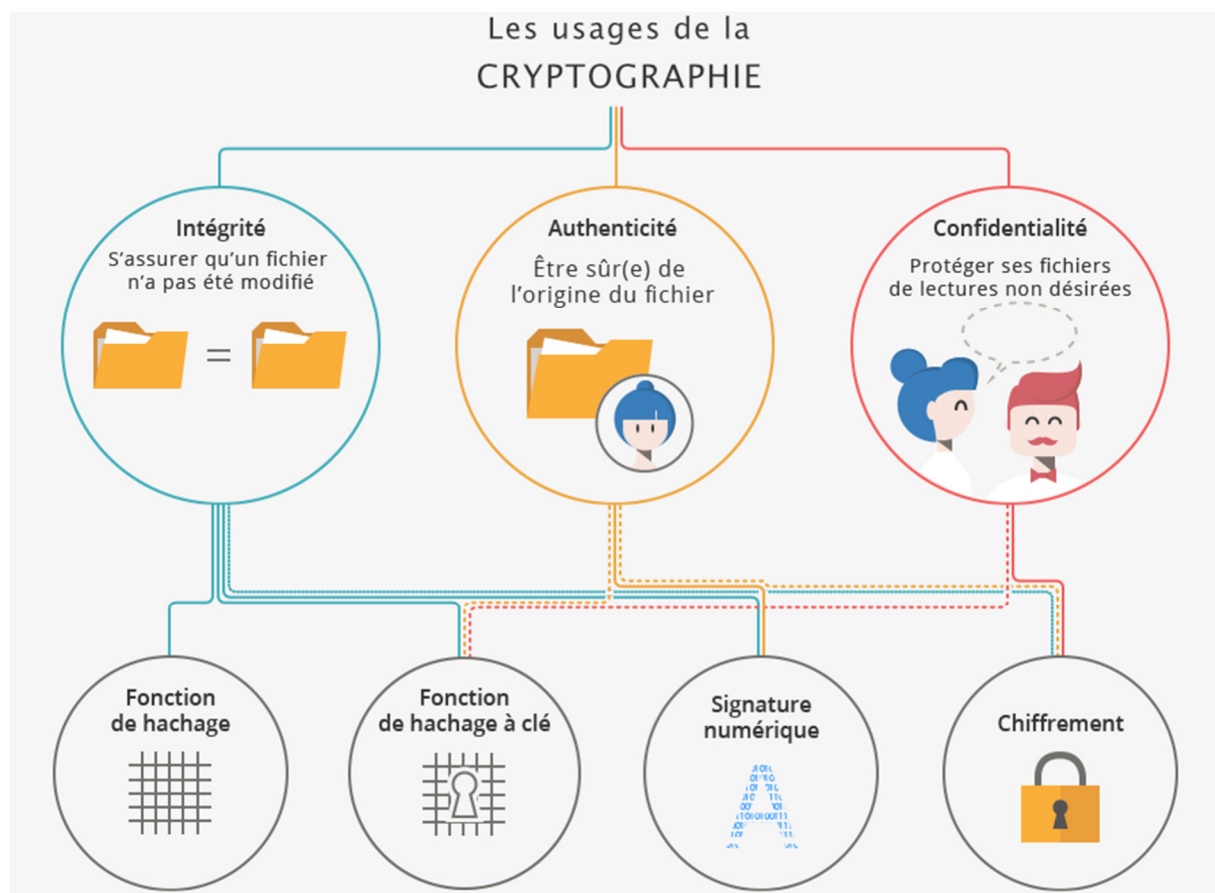


Introduction

Le chiffrement est une méthode qui consiste à protéger ses documents en les rendant illisibles par toute personne n'ayant pas accès à une clé dite de déchiffrement.

Celui-ci peut être utile si vous souhaitez conserver des documents confidentiels sur un support qui pourrait être volé (clé USB, ordinateur portable, etc.) ou sur un ordinateur que vous partagez avec des personnes qui ne doivent pas pouvoir y accéder. Enfin, le plus souvent, lorsque vous stockez des documents dans le *cloud*, la confidentialité de ces fichiers n'est pas garantie, il est donc intéressant de les chiffrer.

Le chiffrement n'est qu'une des applications de la **cryptographie** puisqu'en plus de protéger la **confidentialité** de vos documents ou communications, elle permet d'assurer également leur **authenticité** (qui a créé le document ?) et son **intégrité** (le document a-t-il été modifié ?).



Concrètement, sans la cryptographie, il serait impossible de lire des courriels, de faire des transactions bancaires, ou même d'utiliser un téléphone portable...

Pour en savoir plus, vous pouvez consulter la page de la CNIL sur le sujet à cette adresse :

<https://www.cnil.fr/fr/comment-chiffrer-ses-documents-et-ses-repertoires>

Un peu de vocabulaire...

Le **chiffrement** est la transformation d'une information en clair en une information chiffrée, incompréhensible, mais que l'on peut déchiffrer avec une clé pour obtenir l'information d'origine.

La **clé de chiffrement** est l'information qui permet de transformer un texte en clair en texte chiffré en utilisant un algorithme de chiffrement. De même, la **clé de déchiffrement** est l'information qui permet de transformer un texte chiffré en son texte clair d'origine.

Si la clé de chiffrement et la clé de déchiffrement sont identiques, on parle de **clé secrète** et de **chiffrement symétrique**.

Avec le **chiffrement asymétrique**, les clés de chiffrement et de déchiffrement sont différentes et on parle de clés publique et privée.

Le **hachage** en cryptographie est une fonction permettant de générer une « empreinte ADN » unique à un document donné. Cette fonction est particulièrement utile dans les domaines de l'authentification et des signatures numériques.

Les termes **crypter** ou **encrypter** sont des anglicismes et n'existent pas dans la langue française.

Décrypter un document signifie « retrouver un texte en clair sans connaître la clé »

Déchiffrer qui signifie « retrouver un texte en clair avec la clé de déchiffrement ».

Un peu d'histoire...



Le premier document chiffré connu remonte à l'Antiquité. Il s'agit d'une tablette d'argile, gravée par un potier qui y avait consigné sa recette secrète en supprimant des consonnes et en modifiant l'orthographe des mots.



La **scytale** est considérée comme le plus ancien dispositif de chiffrement militaire connu. Après avoir enroulé une lanière de cuir autour du bâton, on y inscrivait le message en plaçant une lettre par tour. Pour déchiffrer le message, le destinataire devait posséder un bâton au diamètre identique. Le philosophe Plutarque raconte son utilisation en 404 avant JC.



Le **chiffre de César** : il s'agit simplement d'un chiffrement par décalage alphabétique. Par exemple, avec un décalage de 1, **A** devient **B**, **B** devient **C** et ainsi de suite. Historiquement, Jules César utilisait un décalage de 3 lettres avec un alphabet grec, mais d'autres chiffrements par décalage ont été utilisés avant lui. D'une manière générale, c'est un chiffrement assez facile à casser puisqu'il n'y a que 25 décalages à tester.

Leon Battista Alberti publie en 1467 le premier chiffrement polyalphabétique. Bien plus efficace que le chiffre de César, ce chiffrement ne fut cassé que 400 ans plus tard.



La **machine Enigma** fut notamment utilisée pendant la seconde guerre mondiale par l'Allemagne nazie. Il s'agit d'un système électromécanique faisant passer un courant électrique à travers une série de fils et de composants et actionnant des rotors à chaque fois qu'une lettre est tapée. Les services de renseignements alliés parvinrent à casser le chiffrement ce qui a contribué à changer profondément le cours de la guerre.



Le **chiffrement RSA** nommé par les initiales de ses inventeurs (Rivest, Shamir et Adleman) fut décrit pour la première fois en 1977. C'est un chiffrement **asymétrique** : la **clé publique** qui sert à chiffrer des données n'est pas la même que la **clé privée** qui sert à déchiffrer. Ce chiffrement est notamment utilisé pour les connexions sécurisées sur Internet (le fameux https) et pour les signatures électroniques.



L'algorithme **Rijndael** a été choisi en 2000 comme standard de chiffrement pour les agences gouvernementales américaines et est depuis désigné sous le nom **AES** (Advanced Encryption Standard). Ce standard est largement implémenté en informatique, que ce soit pour protéger des documents ou les communications.

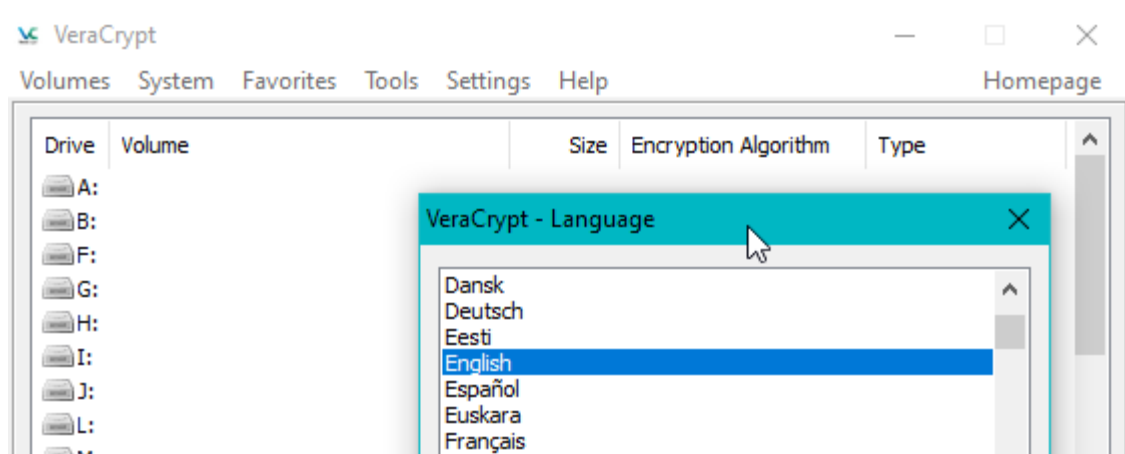
Présentation de VeraCrypt

VeraCrypt est un logiciel libre et gratuit édité par la société française IDRIX permettant de créer des conteneurs chiffrés, des sortes de « clés USB virtuelles » sécurisées, voir même de chiffrer intégralement le disque dur principal.

Vous pouvez télécharger le logiciel à l'adresse suivante :

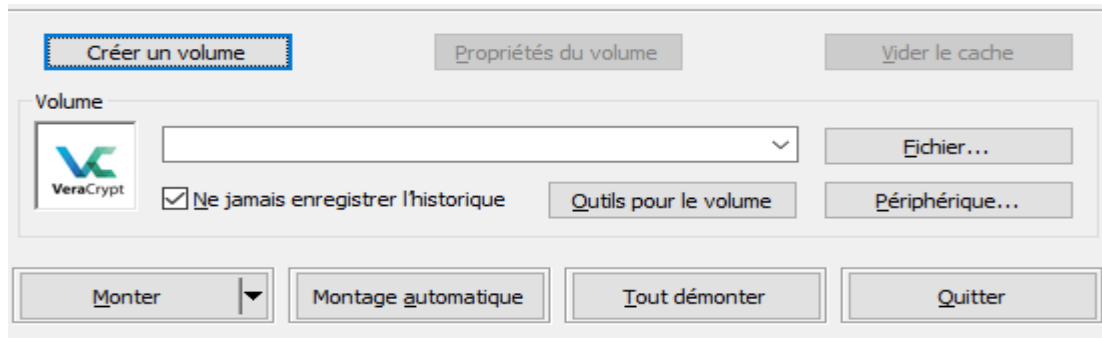
<https://veracrypt.fr/en/Downloads.html>

Au premier lancement, VeraCrypt sera en anglais, pour le passer en français, cliquez dans le menu **Settings** puis dans **Language** et choisissez **Français** dans la liste.



Créer un conteneur chiffré

La première étape consistera donc à créer une de ces « clés USB virtuelles ». Pour ce faire, cliquez sur **Créer un volume**

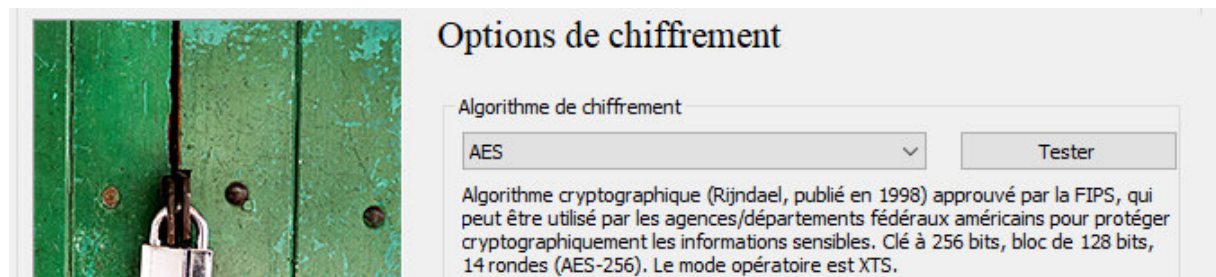


Un assistant de création de volume s'affichera alors qui vous guidera pas à pas :

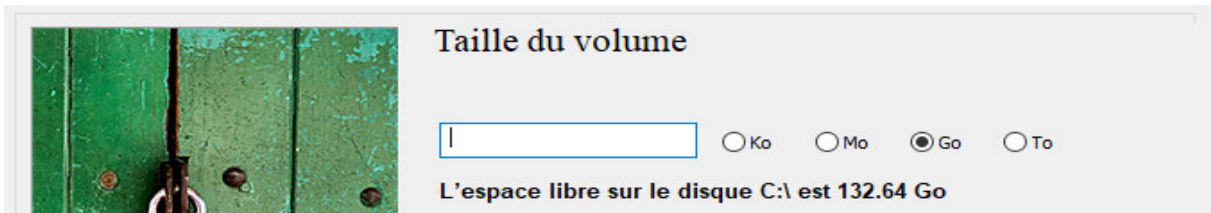
Dans notre exemple, nous présenterons la création d'un volume simple donc nous choisirons successivement **Créer un fichier conteneur chiffré** puis **Volume VeraCrypt standard** et enfin nous cliquerons sur le bouton **Fichier** afin de choisir l'emplacement où sera sauvegardé le conteneur.



Vous êtes ensuite invité à choisir l'algorithme de chiffrement, l'option par défaut AES convient parfaitement, cliquez donc sur le bouton **Suivant**.

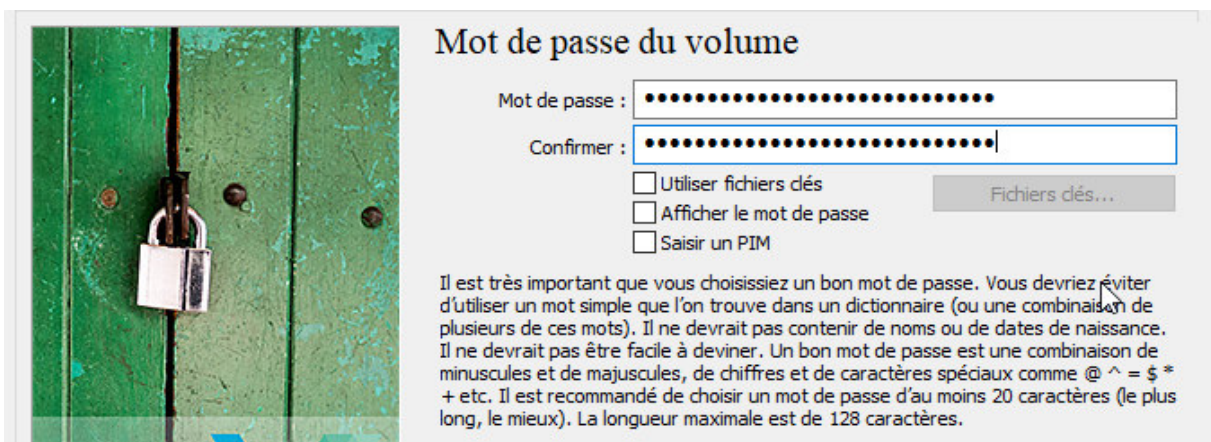


Indiquez ensuite la taille de votre conteneur. Prévoyez un espace suffisant pour le cas où vous auriez ensuite d'autres documents à protéger. Cliquez sur le bouton **Suivant** pour continuer.

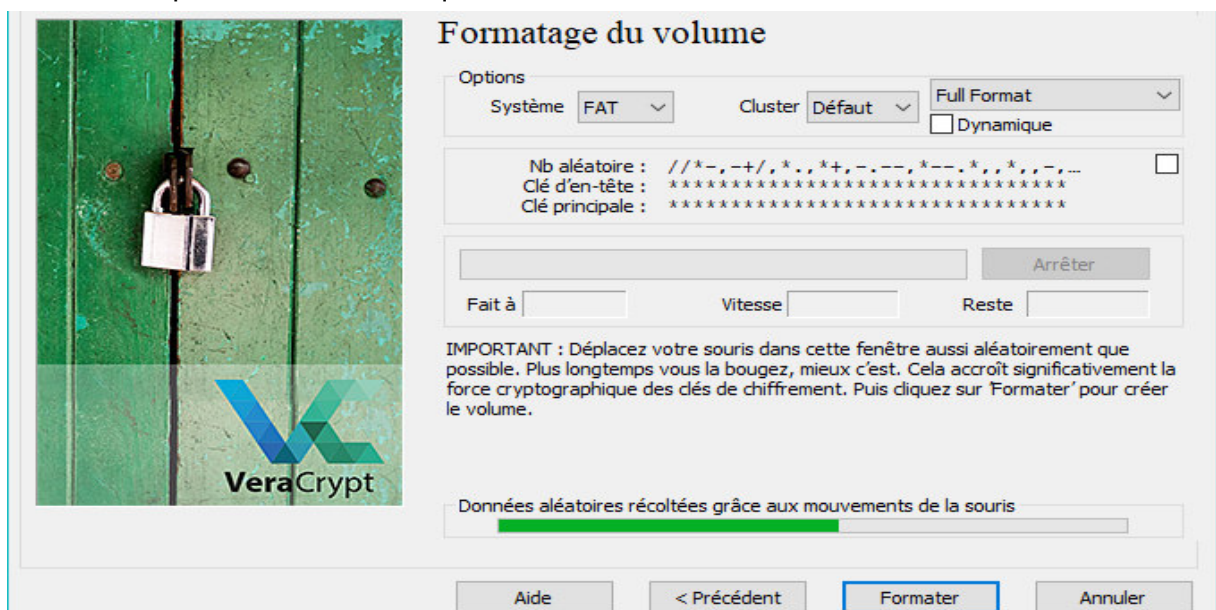


C'est le moment où vous définissez le mot de passe de protection.

Une bonne méthode pour générer de tels mots de passe est de passer par des phrases de passe. Vous pouvez vous aider du site <https://diceware.fr> pour générer ce genre de phrases si vous êtes à court d'inspiration.



Enfin, VeraCrypt va formater votre conteneur sécurisé, pour renforcer la force du chiffrement, vous êtes invité à déplacer votre souris dans la fenêtre jusqu'à ce que la barre en bas passe au vert et cliquez sur le bouton **Formater**

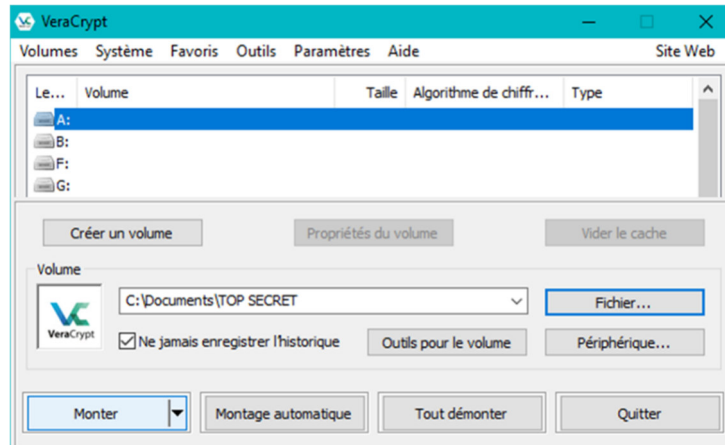


Accéder à un conteneur chiffré

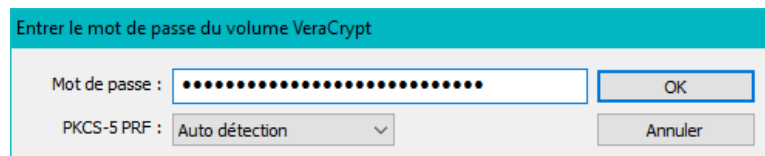
Votre « clé USB virtuelle » prête il ne vous reste plus qu'à y accéder.

Commencez par choisir un lecteur dans la liste puis cliquez sur le bouton **Fichier...** et naviguez jusqu'à l'emplacement où vous avez enregistré votre conteneur.

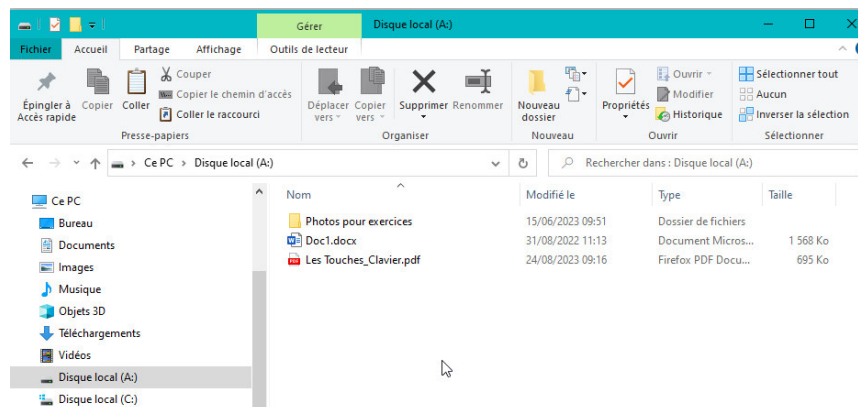
Enfin, cliquez sur le bouton **Monter**.



Vous êtes ensuite invité à rentrer votre mot de passe :



Dans l'explorateur de fichier, vous retrouverez votre conteneur sous forme de clé USB virtuelle à la lettre de lecteur que vous aurez choisi :



Il ne vous reste plus qu'à transférer les dossiers ou documents que vous souhaitez protéger sur cette clé USB. N'oubliez pas d'effacer les documents originaux cela fait.

Pour éjecter votre clé virtuelle, cliquez sur le bouton **Tout démonter** dans VeraCrypt.

Date de dernière mise à jour : mars 2024