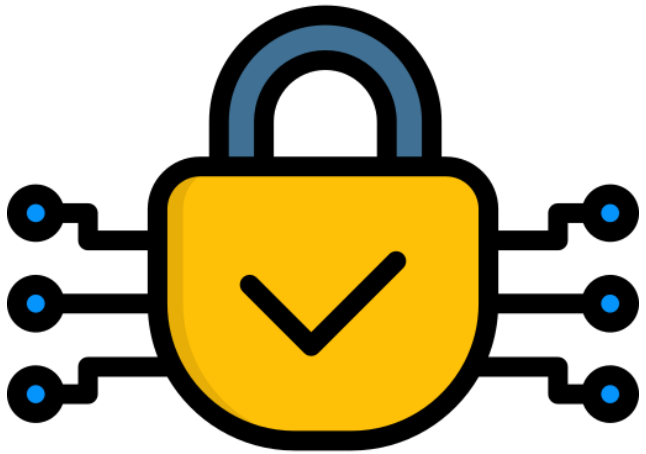


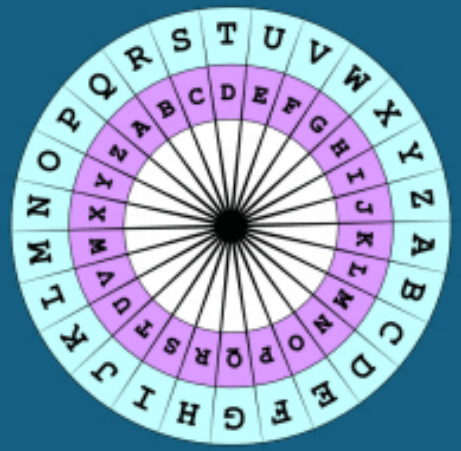
TP – Chiffrement

Sommaire

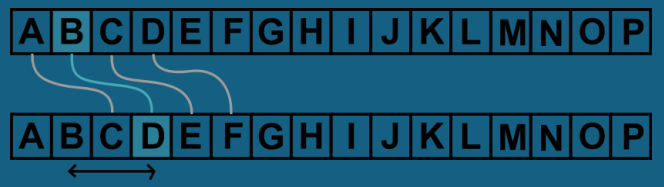
Étude et Recherche

Définition

Code césar



Le code césar consiste à chiffrer un message en remplaçant chaque lettre d'un message par une autre.



Le carré de Vigenère

	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z
A	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z
B	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A
C	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B
D	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C
E	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D
F	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E
G	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F
H	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G
I	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H
J	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I
K	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J
L	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K
M	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L
N	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M
O	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N
P	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O
Q	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P
R	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q
S	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R
T	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S
U	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T
V	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U
W	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V
X	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W
Y	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X
Z	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y

Méthode de chiffrement polyalphabétique qui utilise une clé et un tableau carré pour le chiffrement et déchiffrement.

Chaque lettre du message peut se voir chiffrée par n'importe quel alphabet de César.

Seul un mot ou bien une phrase clé permet de connaître l'alphabet utilisé pour le chiffrer.

Machine « Enigma »

L'Enigma est une machine électromécanique de chiffrement utilisée par l'Allemagne pendant la seconde Guerre mondiale.

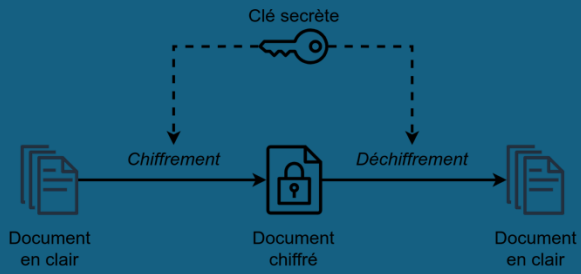
Celui-ci repose sur un principe d'un système de rotors qui modifient le signal électrique d'une touche en une lettre chiffrée avec un câblage interne qui change à chaque frappe.

Définition

Le hachage

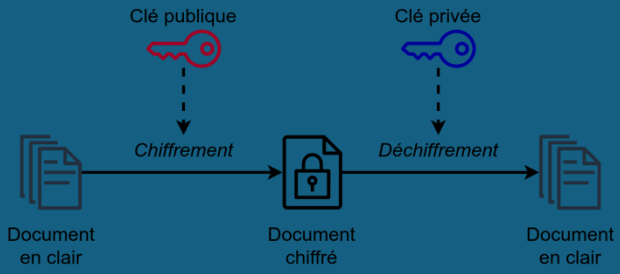
Le hachage est une fonction unidirectionnelle générant une empreinte (ex: SHA-256). Utilisé pour vérifier l'intégrité ou stocker des mots de passe (irréversible mais vulnérable aux attaques sans salage).

Chiffrement clé symétrique



Méthode où une seule clé secrète est utilisée pour chiffrer et déchiffrer les données. Il est rapide, adapté aux gros volumes de données mais nécessite un échange sécurisé de la clé.

Chiffrement clé asymétrique



Méthode qui utilise une paire de clés : une clé publique (partagée) pour chiffrer et une clé privée (secrète) pour déchiffrer. Il est plus lent que le chiffrement symétrique.

Définition

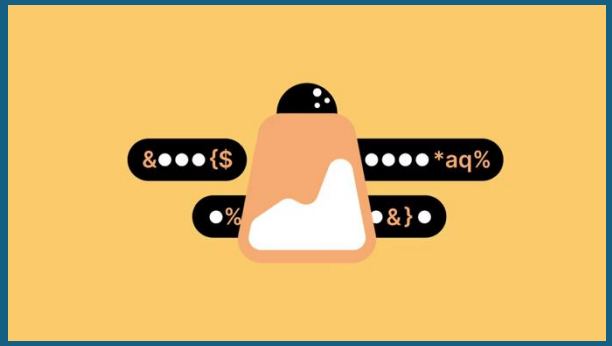
Chiffrement AES

AES est un algorithme de chiffrement symétrique par blocs qui a été standardisé en 2001 pour remplacer le DES. C'est aujourd'hui le chiffrement le plus utilisé mondialement (dans les banques, VPN, chiffrement de fichiers...).

Le téléphone rouge

Le téléphone rouge initialement prend son sens pendant la guerre froide (1963).
De nos jours, le téléphone rouge n'est plus un appareil mais un écosystème cryptographique conçu pour des échanges rapides, inviolables et vitaux.

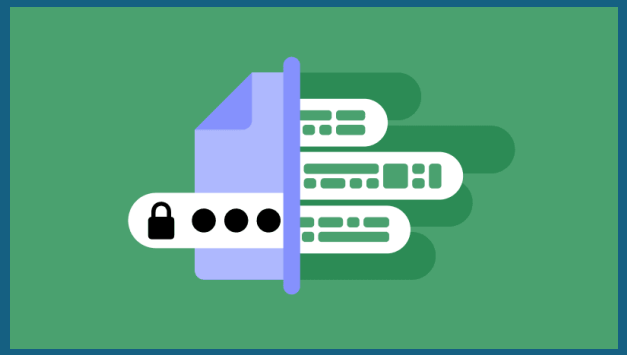
Salage des mots de passe



Le salage des mots de passe est une technique consistant à ajouter une chaîne aléatoire à un mot de passe avant de le hacher. Ainsi, cela évite les attaques par tables précalculées et de rendre unique deux hashs identiques pour des mots de passe similaires.

Définition

Limites du hachage des mots de passe



- **Attaque bruteforce et dictionnaire** : possibilité de tester des millions de combinaisons de mots de passe courants
- **Attaques par tables arc-en-ciel** : attaques utilisant des hashs précalculés pour retrouver les mots de passe courants
- **Collisions** : certains algorithmes produisent le même hash pour des entrées différentes
- **Absence/mauvais usage du salage** : sans salage deux mots de passe identiques ont le même hash facilitant les attaques.

Stéganographie

La stéganographie est une technique de dissimulation d'informations secrètes au sein d'un support innocent (image, vidéo, texte, vidéo) sans éveiller les soupçons contrairement au chiffrement qui rend les données illisibles.

Différence entre chiffrement bijectif et hachage

Chiffrement bijectif :

- Réversible : retrouver les données originales avec la clé
- Objectif : Confidentialité
- AES, RSA

Hachage :

- Irréversible : aucune clé ne permet de retrouver l'entrée originale
- Objectif : intégrité ou stockage sécurisé
- SHA-256, bcrypt

L’outil TrueCrypt

À quoi sert TrueCrypt ?

TrueCrypt est un outil qui permet de **créer un disque virtuel chiffré** contenu dans un fichier et de le **monter comme un disque physique réel**.

L'intérêt est de protéger la confidentialité des données ainsi que de réduire l'impact de leur perte en cas de vol ou de compromission par un cyberattaquant.

TrueCrypt est désormais un logiciel abandonné par ses auteurs originaux et ce depuis le 7 février 2012 (date de la dernière mise à jour).

Il est actuellement remplacé par l'outil **VeraCrypt** (développé par la société française **IDRIX**).

Différence entre TrueCrypt et VeraCrypt

	TrueCrypt	VeraCrypt
Sécurité	Vulnérabilités connues	Correctifs des failles de TrueCrypt
Algorithmes	AES, Serpent, Twofish	Ajout de Camellia, Kuznyechik et modes de hachage plus fort (SHA-256, SHA-3, Streebog)
Protection contre le bruteforce	Faible	Renforcée
Chiffrement système	Obsolète (non sécurisé sur Windows 10+)	Support moderne (UEFI, Secure Boot)
Mode « hidden volume »	Oui	Amélioré
OS supportés	Windows, macOS, Linux	Meilleure compatibilité
Mises à jour	Abandonné en 2014	Actif et régulièrement mis à jour

Principe de fonctionnement de TrueCrypt

TrueCrypt est un outil de chiffrement à la volée (on-the-fly encryption) qui se distingue des solutions classiques par son approche unique de la protection des données.

Les données sont chiffrées/déchiffrées automatiquement en mémoire vive. De plus, l'utilisateur n'a pas besoin de déchiffrer manuellement les fichiers.

Depuis son arrêt, des alternatives comme DiskCryptor pour Windows et FileVault pour MacOs offrent des fonctionnalités similaires mais sans support pour les volumes cachés. LUKS, sur Linux, supporte plusieurs algorithmes de chiffrement.

Ces alternatives offrent des améliorations par rapport à TrueCrypt.

L’intérêt d’utiliser TrueCrypt au sein d’une société

L’utilisation de TrueCrypt au sein d’une société présente plusieurs avantages en matière de sécurité des données.

Il permet d’avoir une confidentialité renforcée sur le chiffrement intégral des disques ainsi que des volumes cachés pour protéger des données critiques en cas de cyberattaque.

Il offre du contrôle puisque c’est une solution open-source, il est multiplateforme (Windows, macOS, Linux).

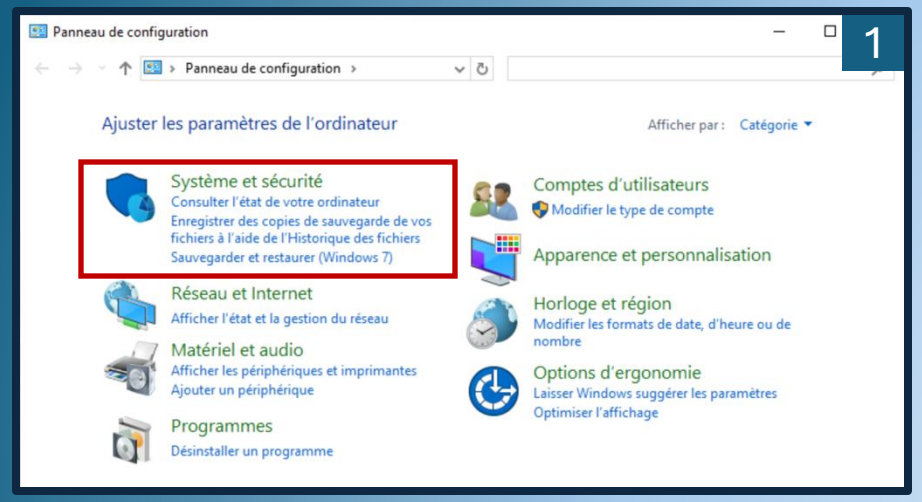
Il protège contre les menaces internes et externes en empêchant l’accès à certaines données et ne laisse pas de traces.

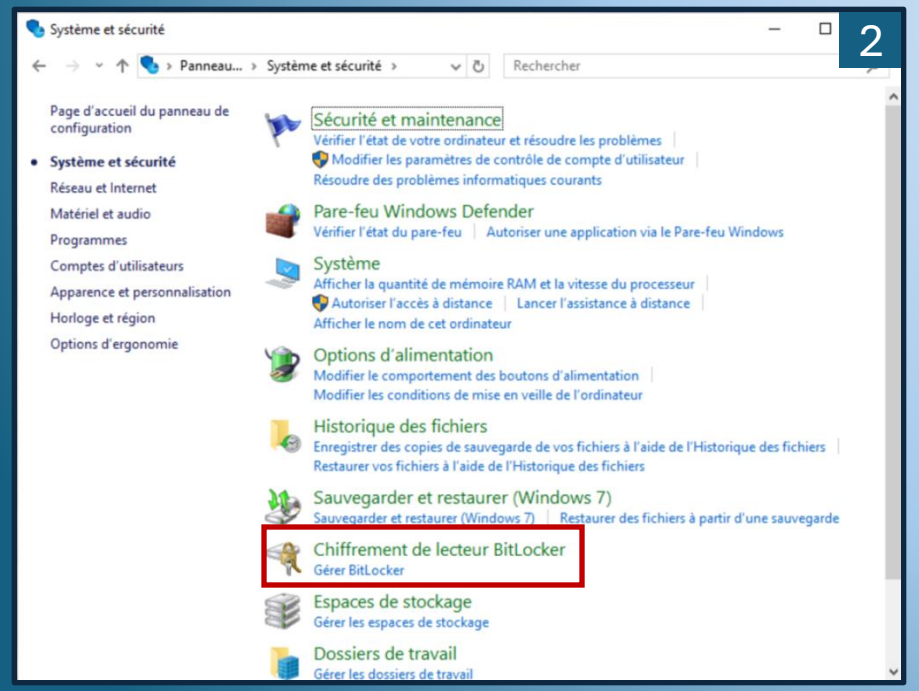
De plus, celui-ci permet de répondre aux exigences du RGPD dans la sécurité des données personnelles.

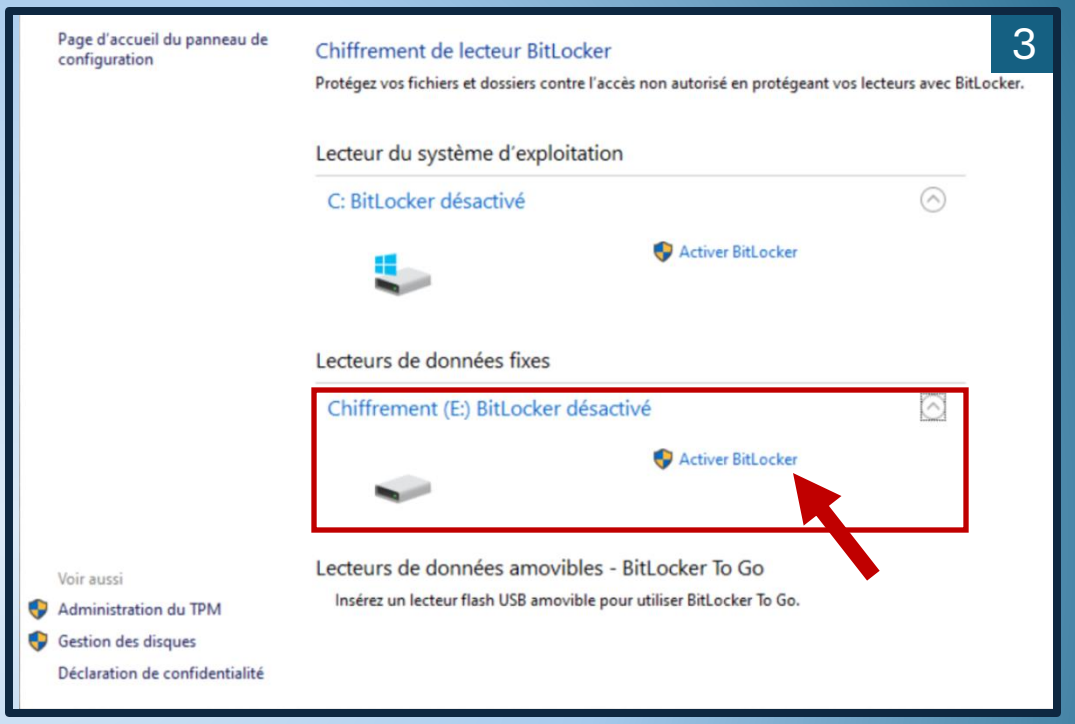
En outre, TrueCrypt (particulièrement son successeur VeraCrypt) est pertinent pour sécuriser ses bases de données, fichiers, les sauvegardes, etc.

Solution 1

Activer BitLocker



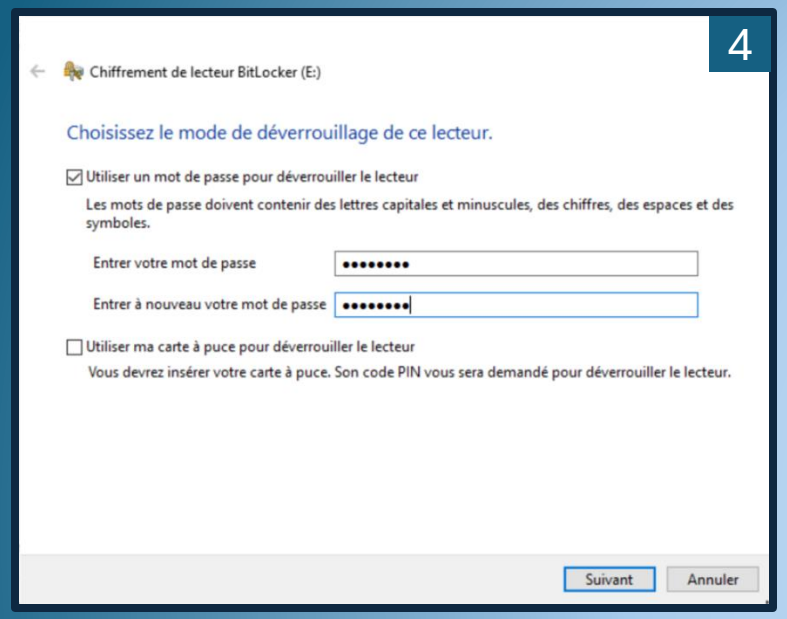


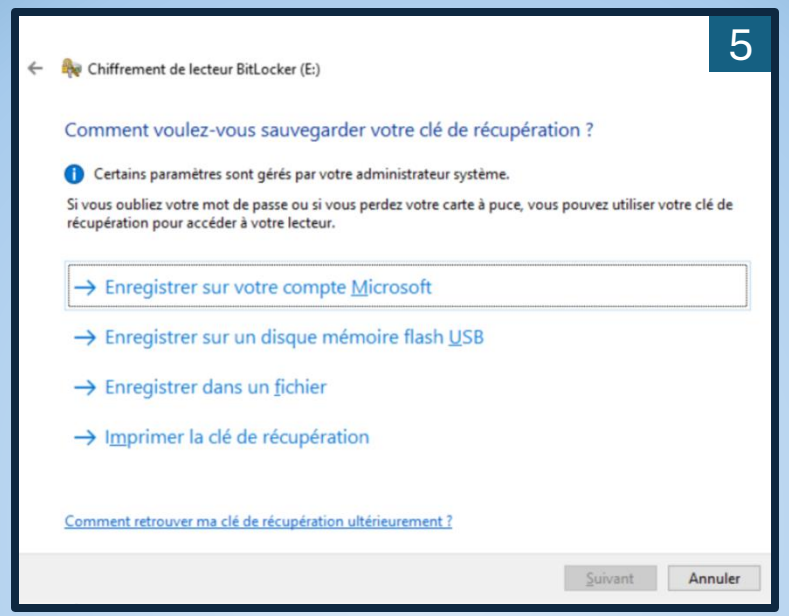


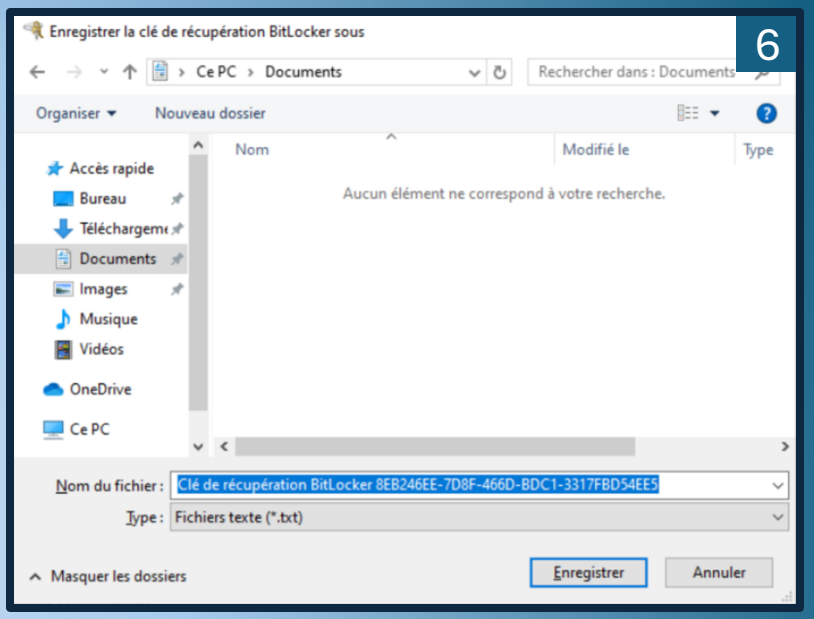
Afin d'activer Bitlocker, nous devrons nous rendre dans le **panneau de configuration**, « **Système et sécurité** », « **Chiffrement de lecteur BitLocker** » puis cliquez sur le lecteur que vous souhaitez chiffrer.

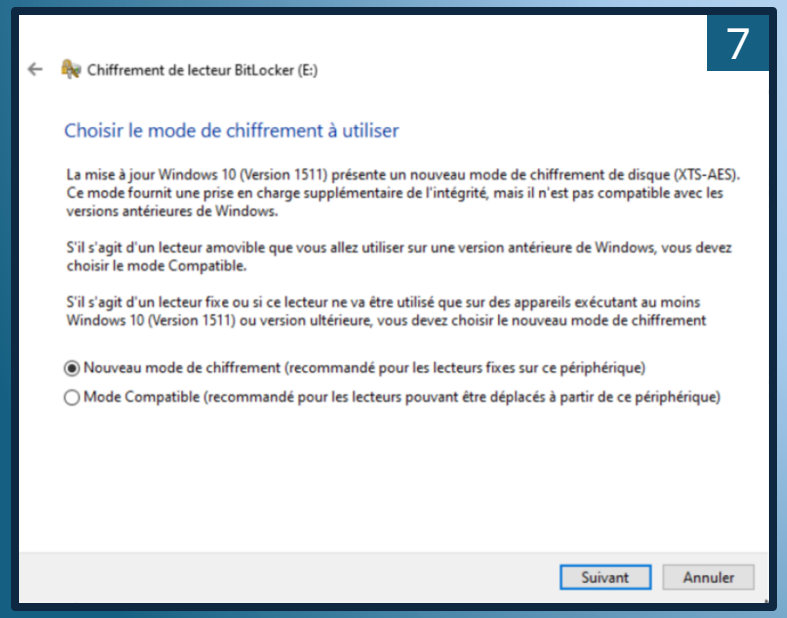
Dans ce cas précis, j'ai créé un lecteur **E:** spécialement pour chiffrer ce disque en particulier.

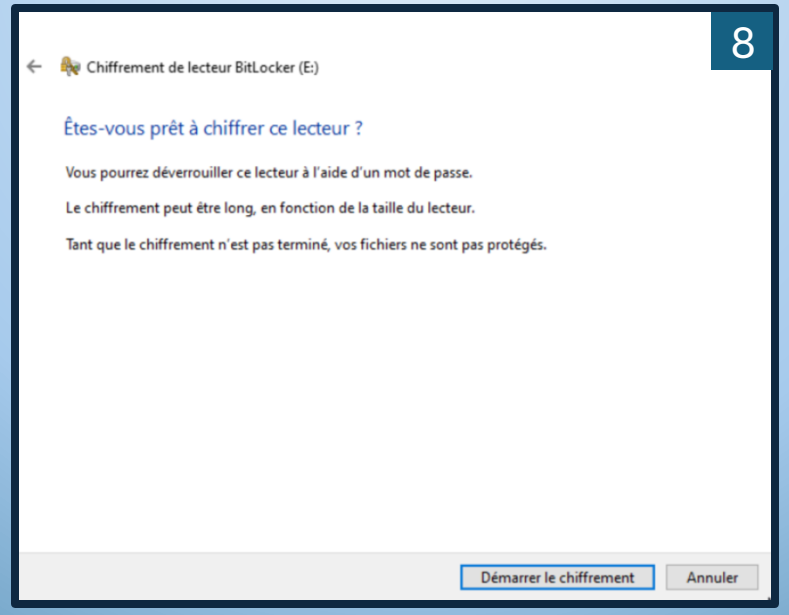
Créer une partition chiffrée









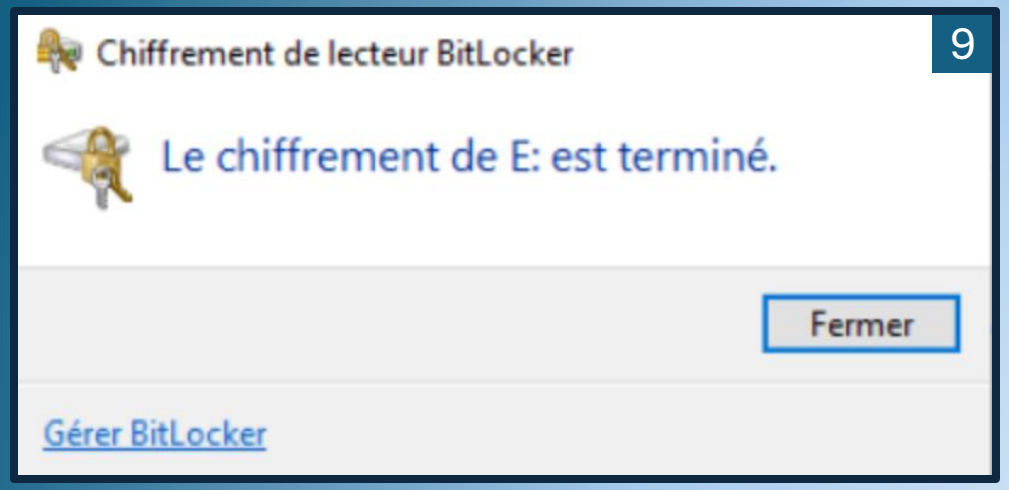


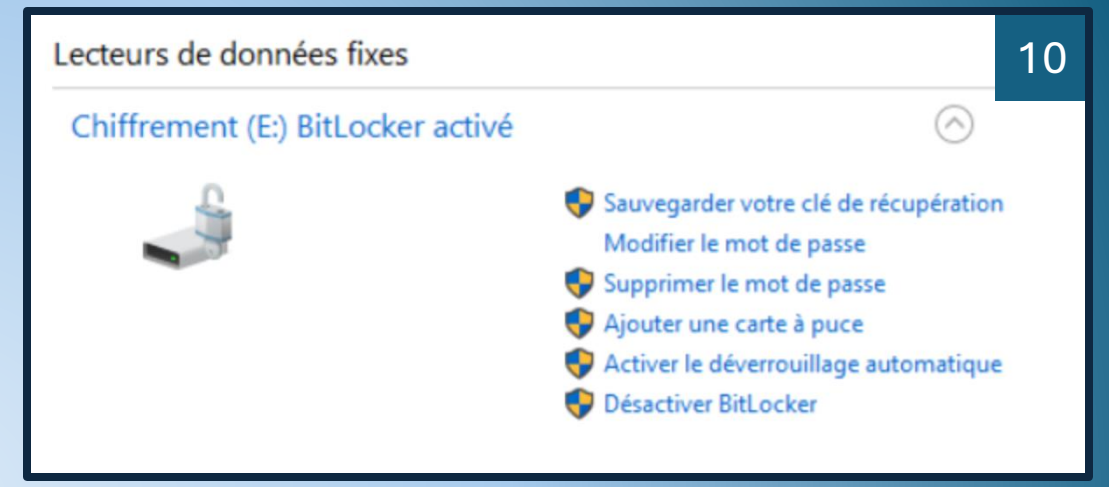
Une fenêtre va s'ouvrir, nous demandant si nous souhaitons affecter un mot de passe (**recommandé**).

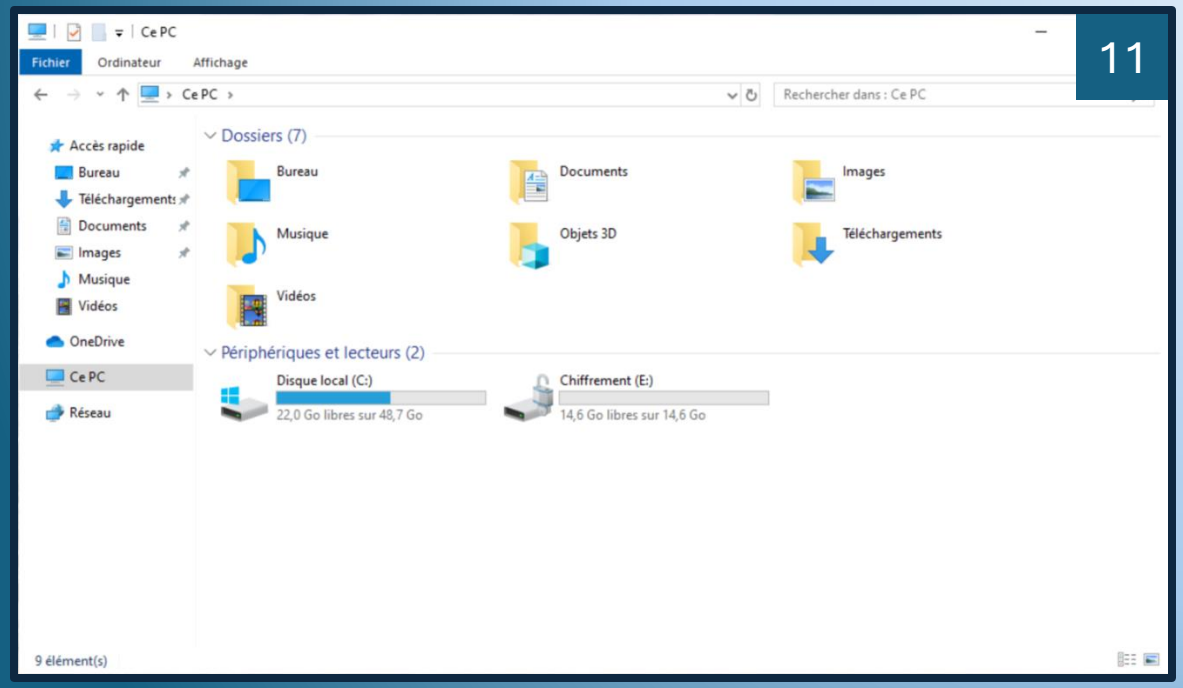
Ensuite, d'enregistrer la clé de récupération soit en l'enregistrant dans un fichier (ce que j'ai fais), en l'enregistrant sur un compte Microsoft, etc.

Enfin, sélectionnez le mode de chiffrement à utiliser (ici c'est un lecteur fixe donc nous resterons sur la case par défaut). Autrement, si vous chiffrez une clé USB, un disque dur externe, il est préférable d'opter pour le mode compatible puis démarrons le chiffrement.

Créer une partition chiffrée







Patientez quelques instants le temps que la partition se chiffre puis en retournant sur l'onglet **BitLocker** du panneau de configuration, nous remarquons que le chiffrement sur le lecteur **E:** est bien chiffrée.

Et, lorsque l'on va dans « **Ce PC** », nous pouvons remarquer que l'icône du Lecteur **E:** est bien chiffrée avec le cadenas.

Ainsi, nous avons pu mettre en place le chiffrement d'une partition sur Windows à l'aide de **BitLocker**.

Solution 2

debian

Mise en place de VeraCrypt

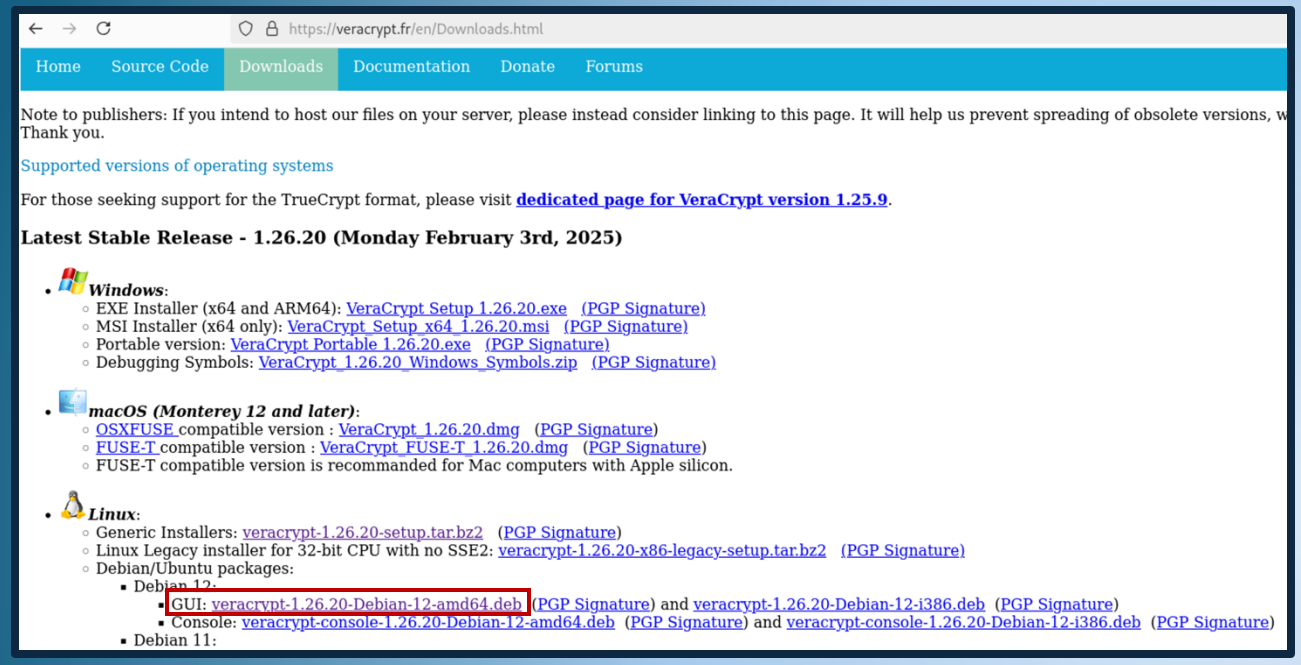
VeraCrypt

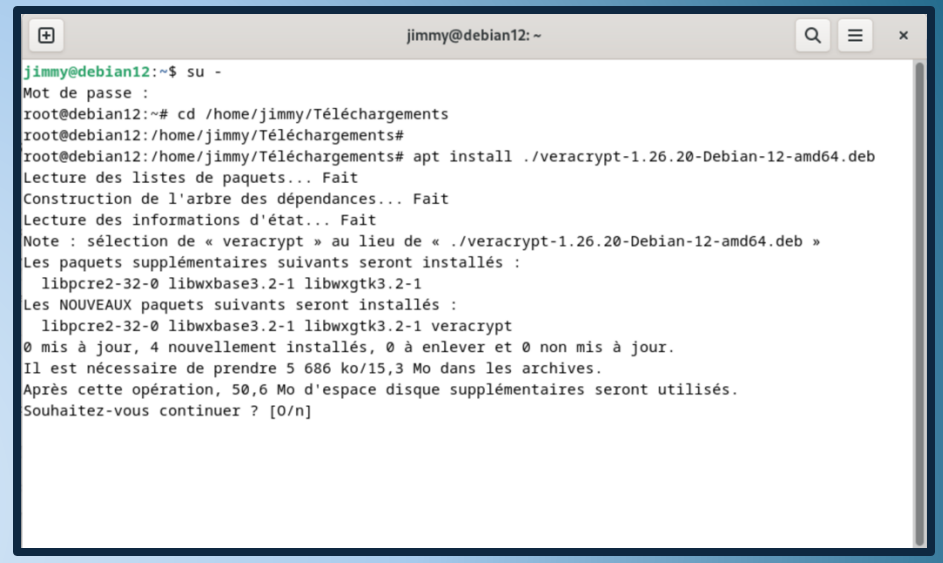
Mise en garde

Avant toute chose, il est impératif de savoir que le chiffrement sur une partition, à l'aide de VeraCrypt, va supprimer l'intégralité de vos données stockées sur la partition choisie.

Veillez donc à effectuer une sauvegarde au préalable sur un support de stockage si vous stockez des données.

Installation de VeraCrypt sur Debian 12






```
root@debian12:~# usermod -aG sudo jimmy
```

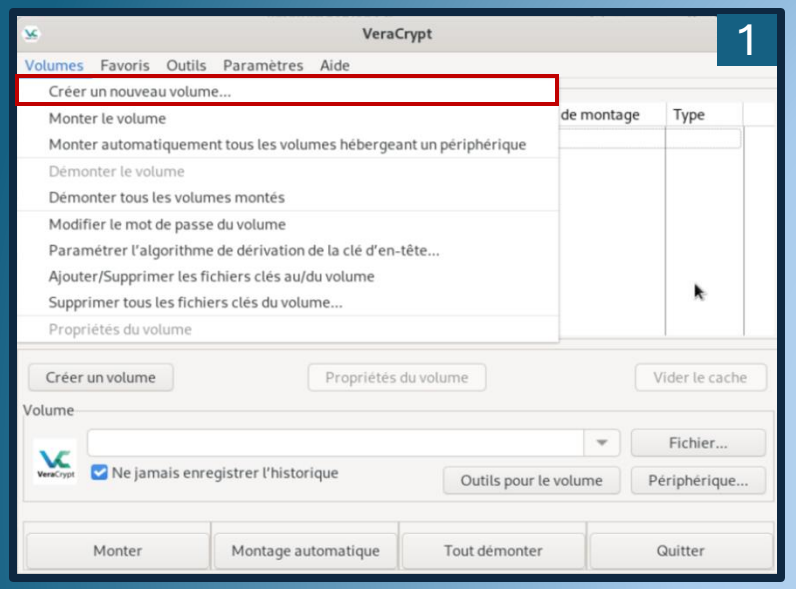
Dans un premier temps, téléchargez **VeraCrypt** sur le site officiel : https://www.veracrypt.fr/en/Downloads.html

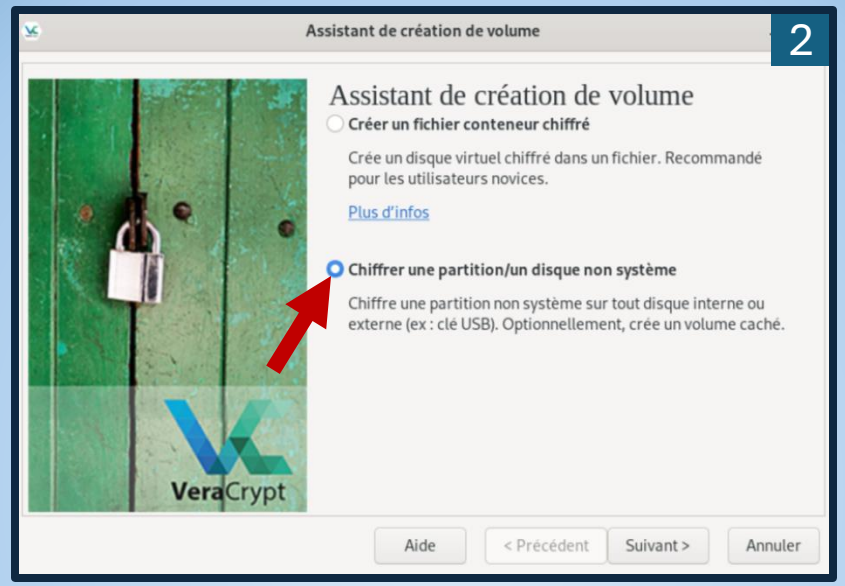
Ensuite, lancez le terminal, mettez-vous en tant qu'utilisateur **root** puis avec la commande « **cd** » rejoignez le répertoire où le fichier **.deb** a été téléchargé.

Une fois dans le répertoire, faites simplement « **apt install ./[nom_du_fichier]** » et confirmez l'installation.

De plus, il est nécessaire d'ajouter au groupe « sudo » un utilisateur. Sinon, vous ne pourrez pas chiffrer une partition.

Configurer une sauvegarde chiffrée

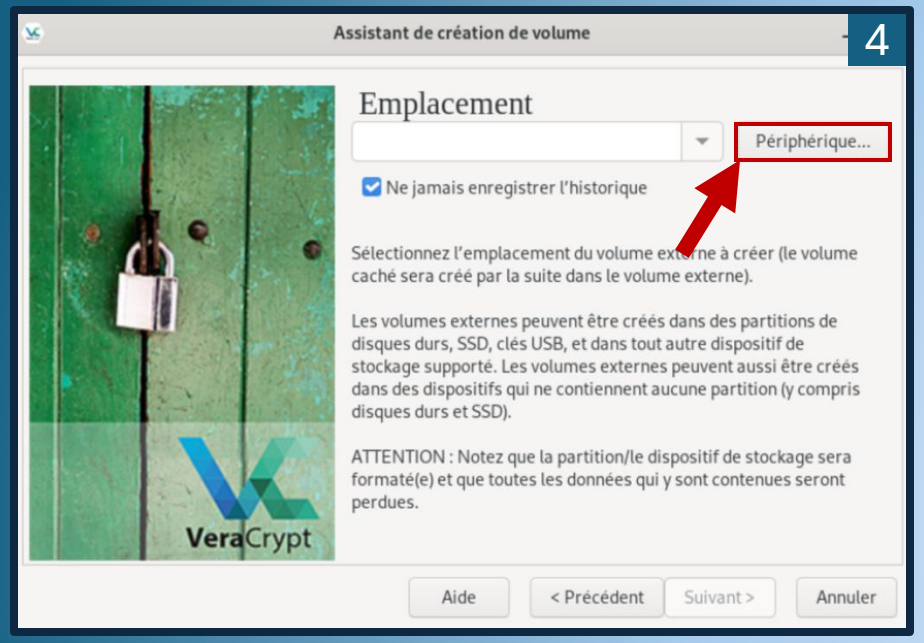


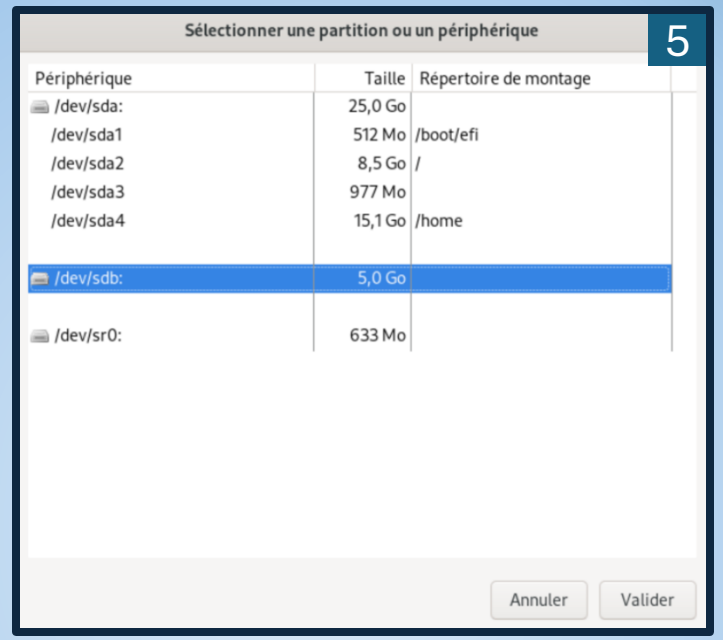


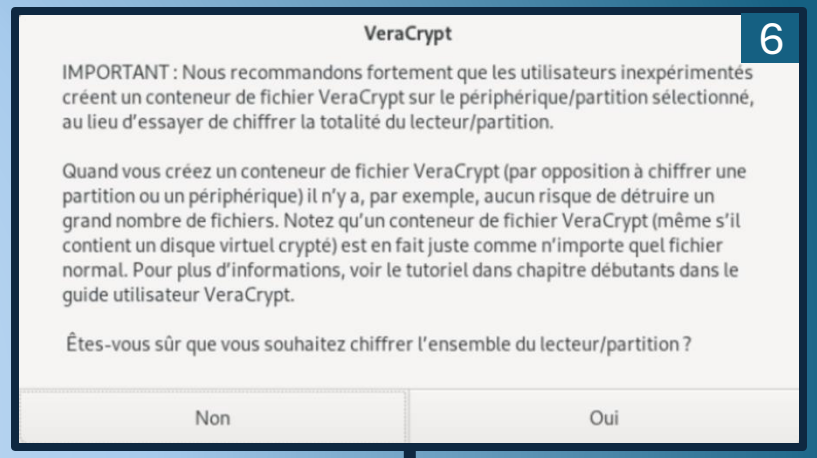
Lançons VeraCrypt où nous irons dans « **Volumes** » puis « **Créer un nouveau volume...** ».

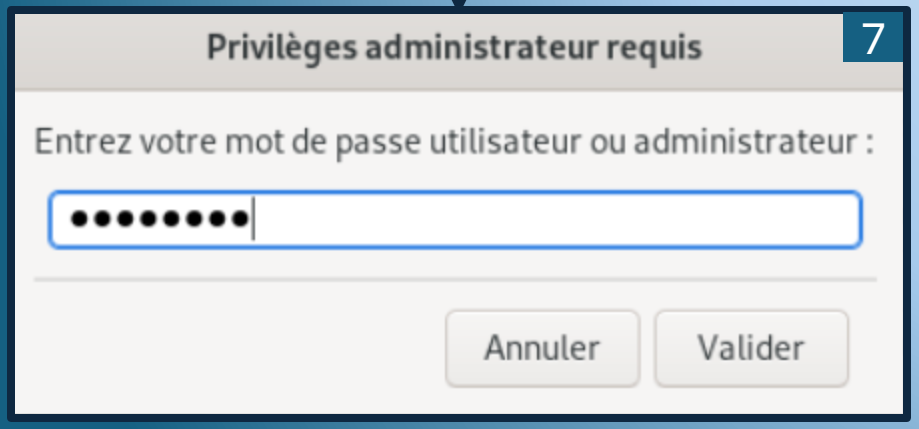
Une fenêtre d'assistant va s'ouvrir, nous cocherons la case « **Chiffrer une partition/un disque non système** » et « **Volume VeraCrypt caché** » sur la page suivante.

Configurer une sauvegarde chiffrée









Ensuite, on vous demandera de sélectionner l'emplacement de votre support. Dans ce cas précis, j'ai créé un lecteur virtuel mais cela peut également fonctionner avec des supports amovibles.

Un message d'avertissement prévient des risques de chiffrer la totalité du lecteur, nous cliquerons sur « **Oui** » et rentrez le mot de passe **root** afin de valider.

Configurer une sauvegarde chiffrée

Dans l'onglet suivant, c'est ici que l'on sélectionne l'algorithme de chiffrement. Il est recommandé de prendre le chiffrement en **AES** qui est performant et sécurisé et le **SHA-254** qui est un hachage robuste et un standard de confiance.

De plus, il est obligatoire de fournir un mot de passe en suivant les recommandations préconisées par la CNIL (12 caractères minimum, chiffres, symboles, utiliser des phrases de passe, etc.)

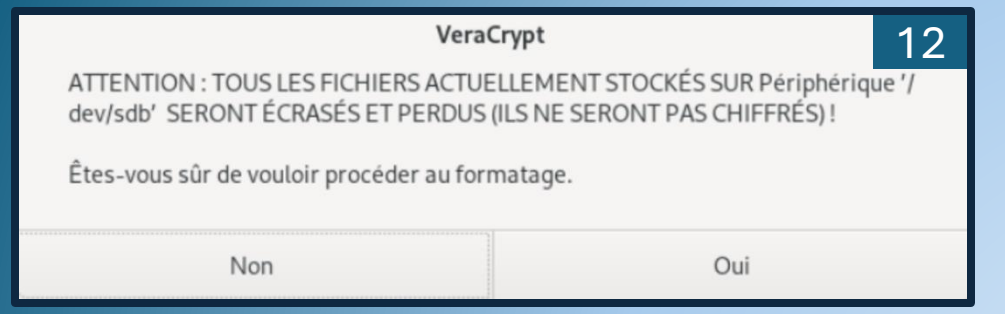
Configurer une sauvegarde chiffrée

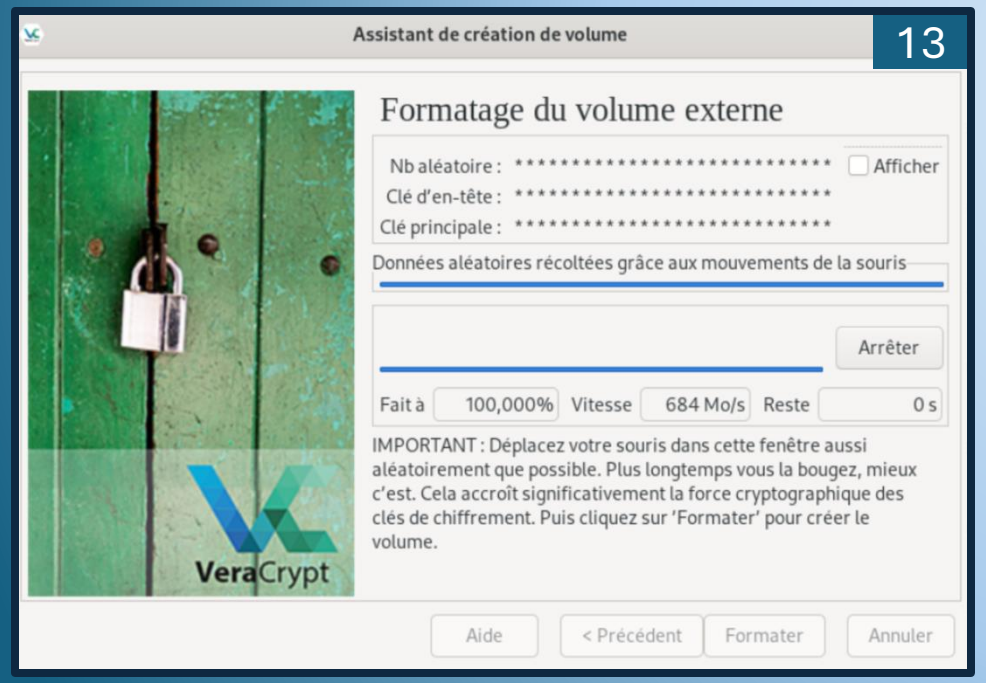
Après validation du mot de passe, sélectionnez la case en fonction des fichiers que vous chiffrerez.

On choisit le **FAT** comme solution de formatage (recommandé car compatible avec différents systèmes d'exploitation).

Ensuite, sur la page suivante, vous devrez bouger votre souris dans la fenêtre afin de complexifier la génération des clés puis cliquez sur « **Formater** ».

Configurer une sauvegarde chiffrée





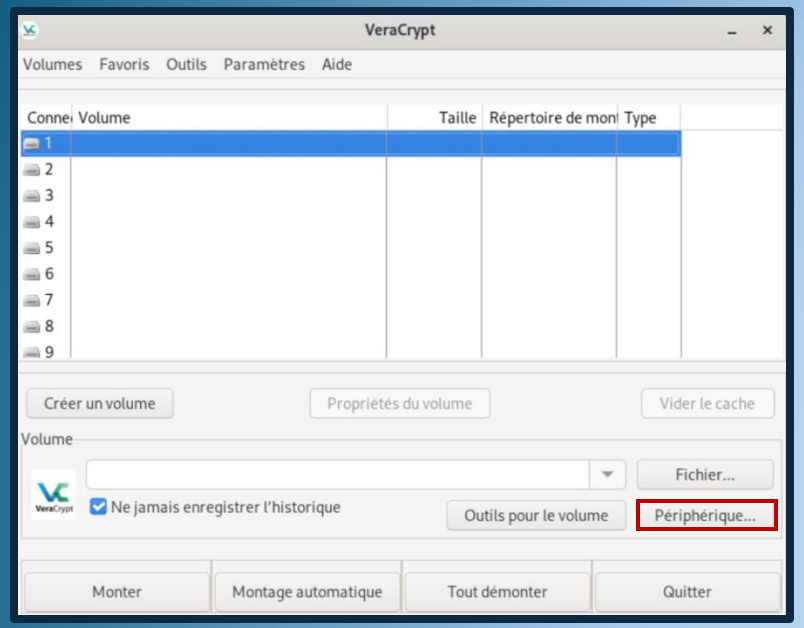
Comme précisez auparavant lorsque vous validerez, **VeraCrypt** procédera à un formatage donc attention si vous manipulez des données importantes.

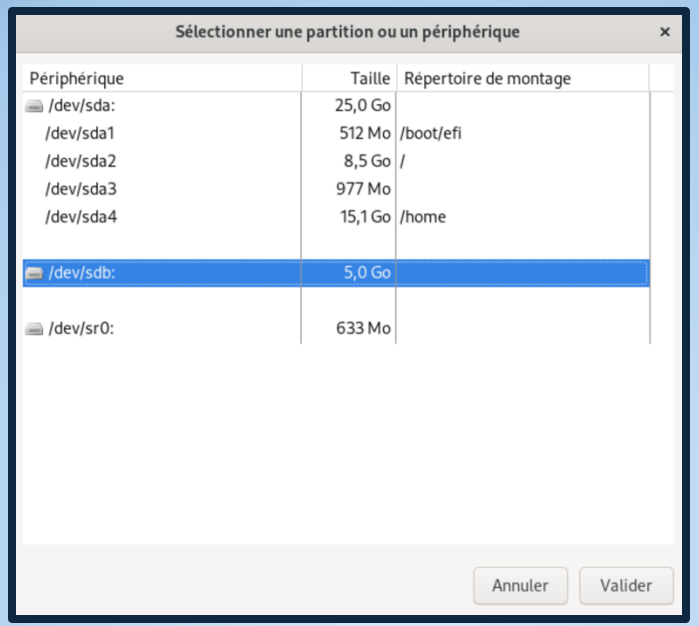
Puis faites suivant jusqu'à la dernière étape qui concerne le volume caché.

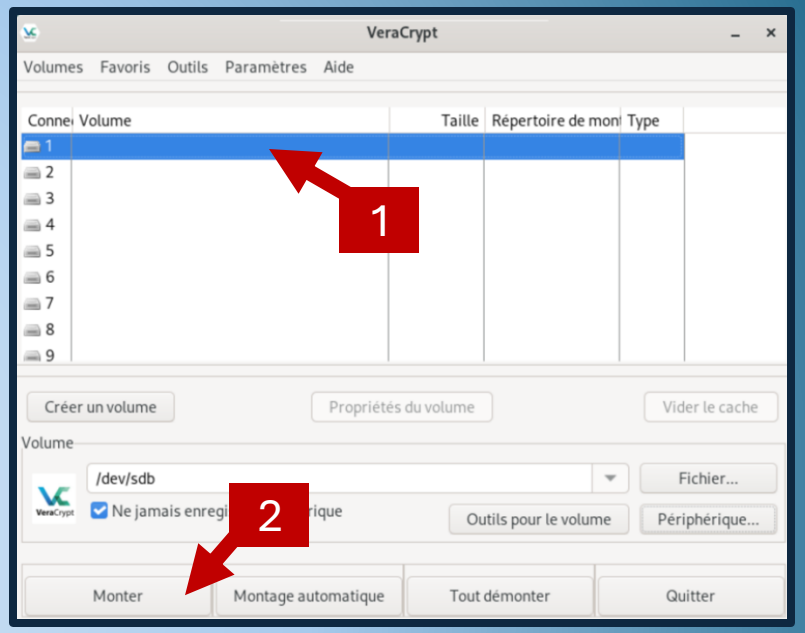
Création du volume caché

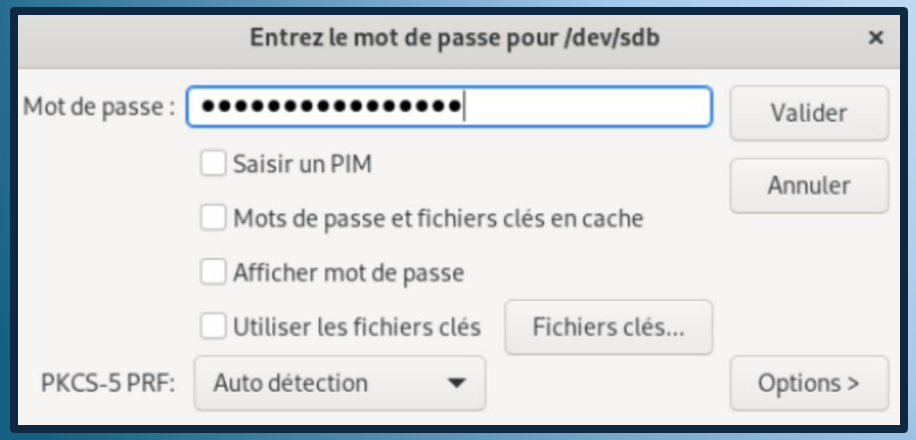
Pour le volume caché, se réitérez à la création d'un volume comme nous avons fait précédemment.

Monter la partition chiffrée





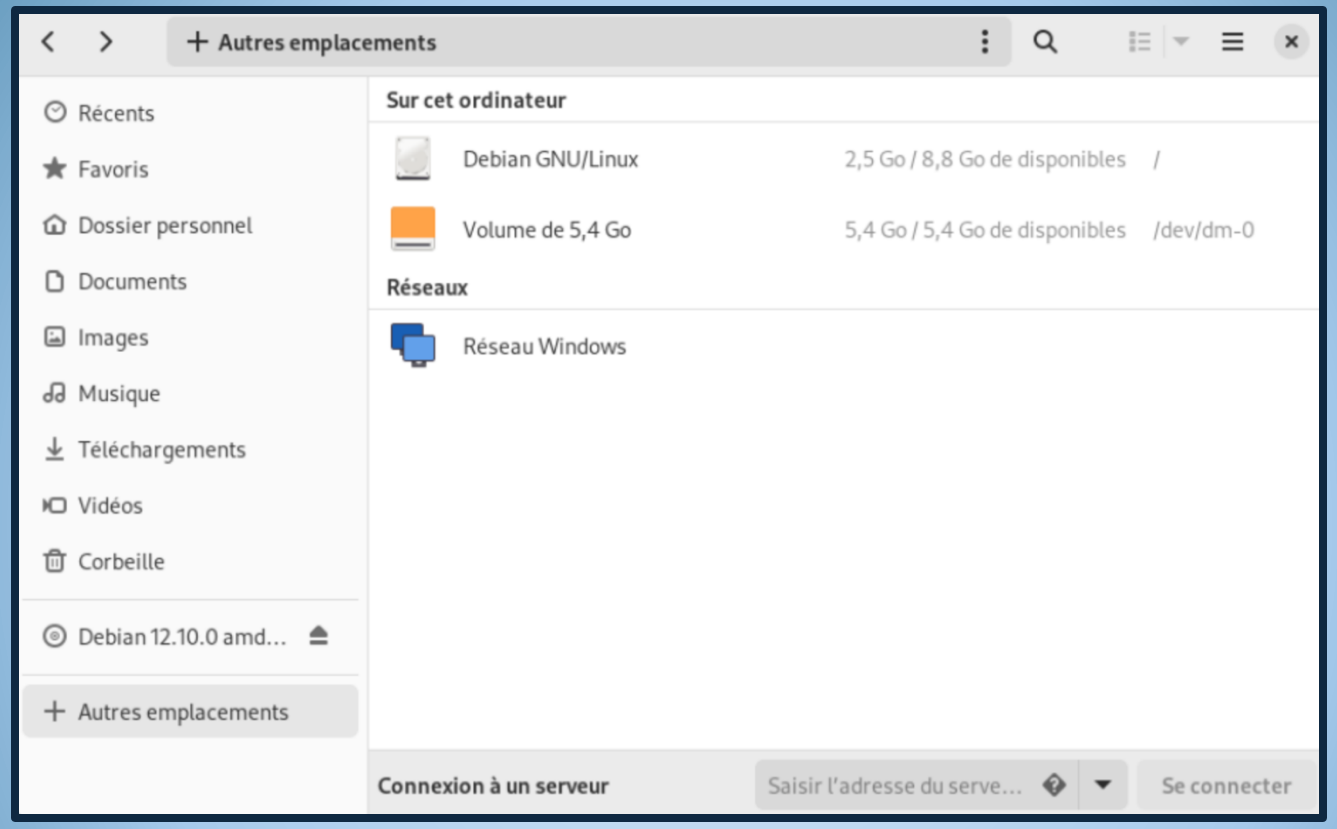




Pour monter une partition chiffrée, cliquez sur « **Périphérique…** », « **votre_partition_chiffrée** » et sélectionnez un n° de volume puis cliquez sur « **Monter** ».

Vous devrez rentrer votre mot de passe de volume afin de valider l'opération.

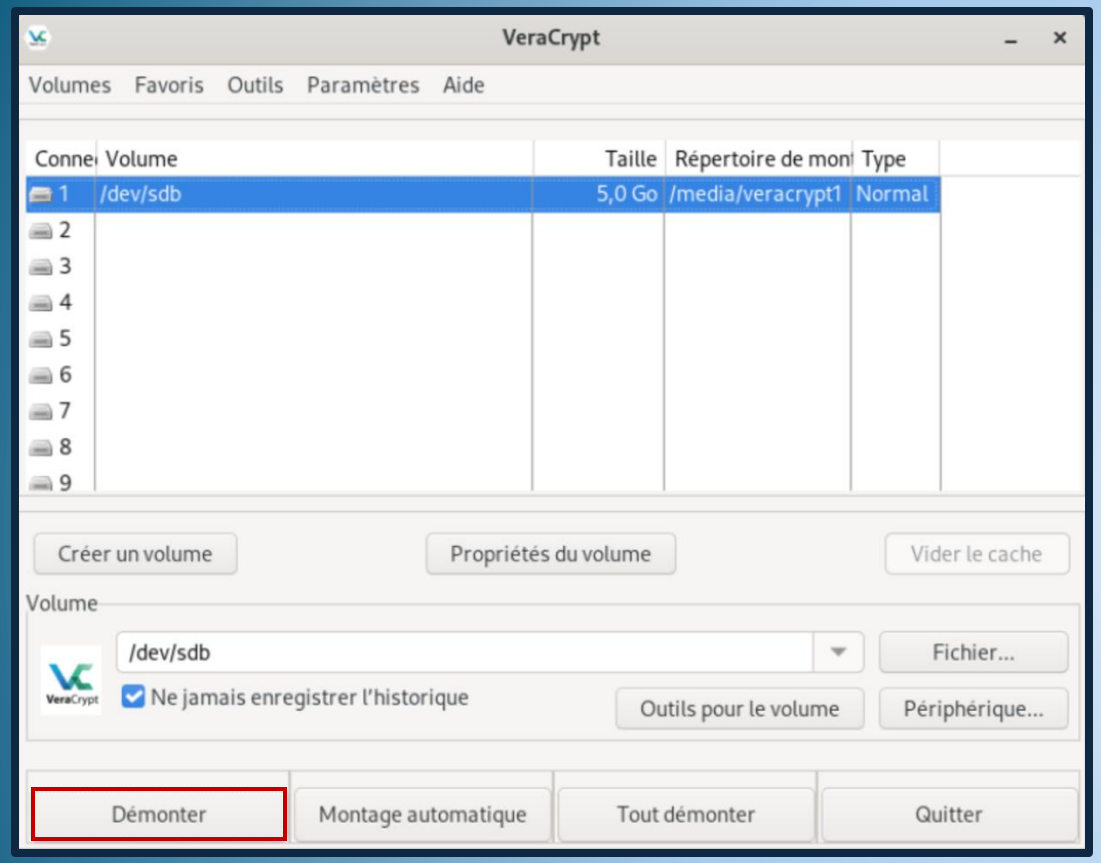
Vérifions si la partition a correctement été montée

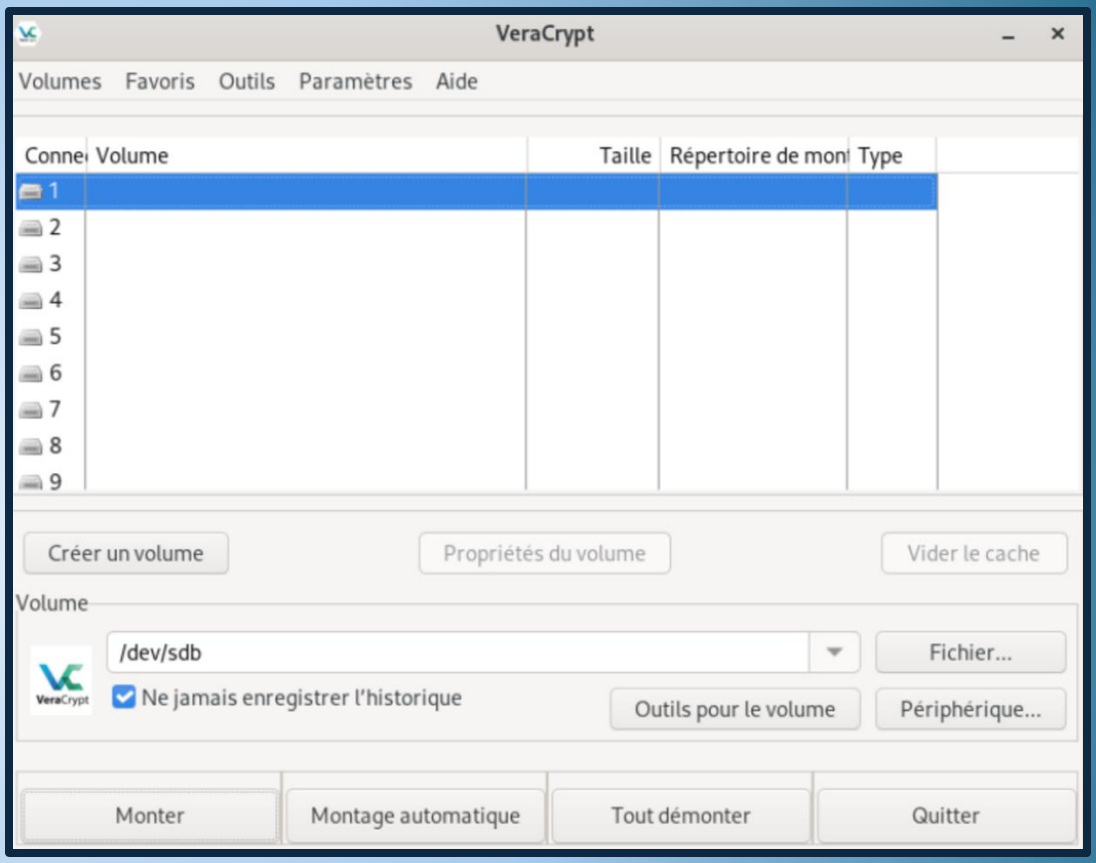


Lorsque l'on se rend dans l'explorateur de fichier, nous pouvons voir le volume chiffrée.

Ainsi, le chiffrement de la partition a été un succès et nous pouvons désormais y transférer des fichiers en toute sécurité.

Démonter le conteneur





Une fois les fichiers transférés, retournons sur VeraCrypt puis démontons le conteneur associé à la sauvegarde chiffrée.