2023-2024

BTS SIO1

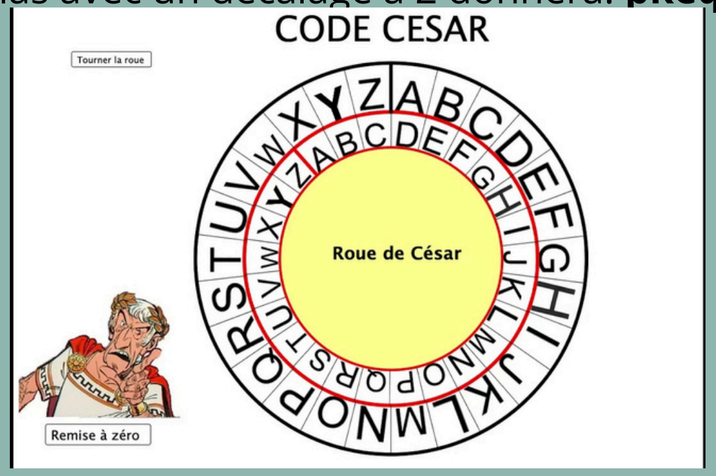
TP-CHIFFREMENT

Nicolas Debut

Études et Recherches

Le code César

Le code César est une méthode de chiffrement par décalage à facteur plus ou moins élevé c’est à dire que pour toutes les lettres de notre mot de pas nous allons les décalées d’un nombre de lettres définies. Par exemple le mot de passe nicolas avec un décalage à 2 donnera: **pkeqncu**



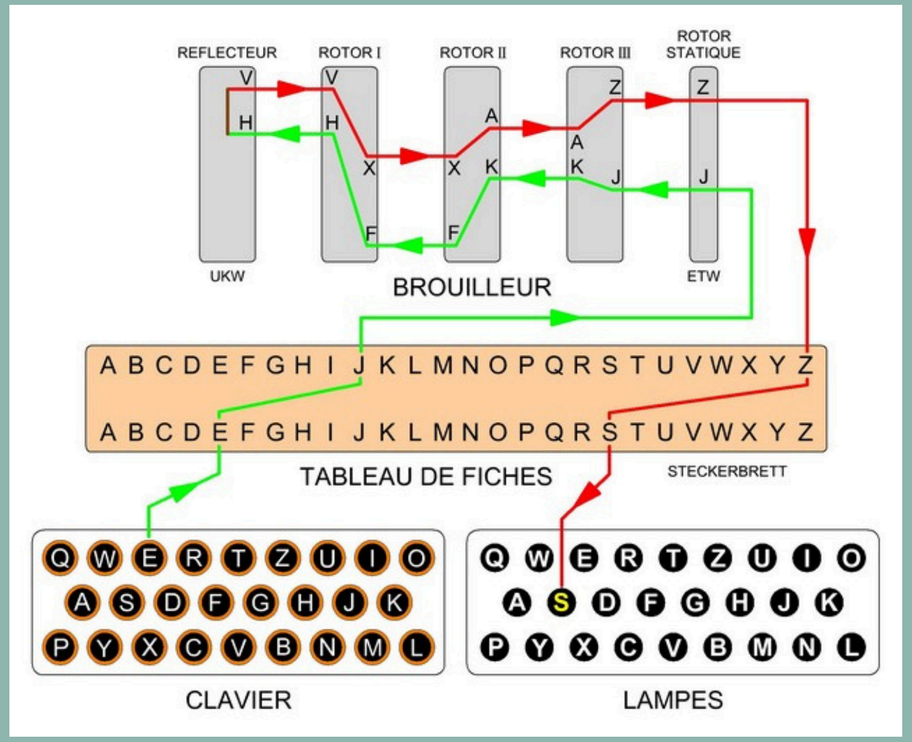
Le carré de Vigenère

L'idée du carré Vigenère est d'utiliser un chiffre de César, mais où le décalage utilisé change de lettre en lettre. Pour cela, on utilise une table composée de 26 alphabets, écrits dans l'ordre, mais décalés de ligne en ligne d'un caractère. On écrit encore en haut un alphabet complet, pour la clé, et à gauche, verticalement, un dernier alphabet, pour le texte à coder :

	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

Pour faire simple on va décider d’un mot de passe tout en choisissant une clé de même taille.
On va ensuite pour chiffrer sélectionner le croisement entre la ligne de la lettre du mot de passe et la colonne de la lettre de la clé de même position.
Par exemple le mot de passe nicolas avec la clé abricot ça donnera le mot de passe chiffré: njtwnol

La machine Enigma



La machine énigma est un chiffrement impossible à résoudre à la main lorsque l'utilisateur entre une lettre celle-ci sera modifiée en une autre via un tableau définit puis cette modification sera passée dans un rotor qui la modifiera et changera de position elle sera envoyée dans un deuxième rotor qui la modifiera à nouveau (ce deuxième rotor changera de position au bout de 26 tour du précédent) ce processus sera répéter autant de fois qu'il y a de rotor.

Le téléphone rouge

Le téléphone rouge fonctionne avec la technique du masque jetable c’est à dire que pour un appel des États-Unis vers Moscou, Moscou va fournir une clé unique à l’ambassade des États-Unis en Russie qui la fournira au gouvernement américain via une voie sécurisée afin d’accéder à la communication.

Le hachage

Le hachage est une méthode de chiffrement qui transforme les enregistrements et les caractères de toute longueur en hachages fixes et compacts. Le hachage offre plus de sécurité que le chiffrement, car les valeurs de hachage ne peuvent pas être reconverties en valeurs d’origine sans clé.
Le mot de passe qu’il aura choisi passera dans un algorithme de hachage qu’il pourra également choisir(il en existe plusieurs) et voilà.

Le chiffrement à clé symétriques

C’est une méthode de chiffrement qui permet de chiffrer et de déchiffrer des données avec une même clé de chiffrement/déchiffrement.

Le chiffrement à clé asymétrique

Cette méthode de chiffrement utilise une clé publique pour chiffrer les données et une clé privée pour les déchiffrer.

Le chiffrement AES

Le chiffrement AES est une méthode de chiffrement par bloc utilisant le système de chiffrement symétrique.

La différence entre le chiffrement bijectif et le hachage:

Le chiffrement bijectif **permet de s'assurer que lors du chiffrement tous les éléments aient une image différente**. Ainsi lors du déchiffrement, il n'y aura pas d'incohérence.
Un algorithme de hachage est une fonction mathématique qui brouille les données pour les rendre illisibles. De plus le hachage permettra de compresser les données.
Comme ces algorithmes sont des programmes à sens unique, personne d’autre ne peut décoder le texte.

Une fonction bijective associe chaque élément d'un ensemble à un seul et unique élément d'un autre ensemble, tandis qu'une fonction de hachage convertit une donnée en une valeur de taille fixe, sans garantir une correspondance un à un entre les entrées et les sorties.

Les limites du hachage des mots de passe.

Comme un mot de passe aura toujours le même hachage il reste sensible aux attaques par bruteforce.

Le salage des mots de passe.

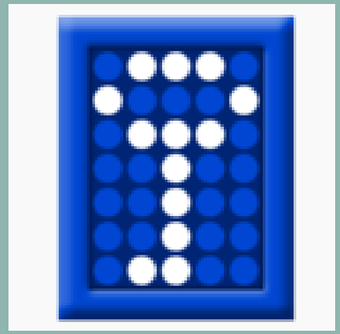
Le salage de mot de passe est un moyen de rendre le hachage des mots de passe plus sûr en ajoutant une chaîne aléatoire de caractères aux mots de passe avant que leur hachage ne soit calculé, ce qui les rend plus difficiles à annuler.

La stéganographie

La stéganographie cherche à dissimuler de l’information dans un autre contenu et non à la chiffrer.

L’outils Truecrypt

Truecrypt est un outil permettant de chiffrer un disque, une partition ou encore un périphérique ce chiffrement prendra effet sur tout l’appareil et les informations qu’il contient par exemple il pourra chiffrer des dossiers, des noms de fichiers…



Tout ce qui sera stocké dans un volume TrueCrypt sera entièrement chiffré, y compris noms de fichiers et répertoires. Les volumes TrueCrypt se comportent, une fois montés, comme des disques durs physiques. Il est ainsi possible par exemple de défragmenter les volumes créés par TrueCrypt.
C’est un outil open source (rare sous Windows) de plus le fait de créer un disque virtuel pour stocker les données permet un accès aux données beaucoup plus facile.

Tout ce qui sera stocké dans un volume TrueCrypt sera entièrement chiffré, y compris noms de fichiers et répertoires. Les volumes TrueCrypt se comportent, une fois montés, comme des disques durs physiques. Il est ainsi possible, par exemple, d'en réparer le système de fichiers avec Check Disk, ou de défragmenter les volumes créés par TrueCrypt. Cela permet pour une entreprise de gérer ses données beaucoup plus simplement et rapidement et comme il est possible de réparer le disque cela permet de réduire les couts pour l’entreprise de manière très importante.

L’outil n’étant plus gérer depuis 2014 voici quelques alternatives gratuites ou non:
VeraCrypt est un logiciel open source basé sur TrueCrypt (un fork, un nouveau logiciel créé à partir du code source d’un logiciel existant) qui fonctionne sur Mac et PC et qui permet la création de disques virtuels chiffrés, son code a été audité.
Bitlocker est intégré à Windows, il n’est pas open source, il chiffre uniquement les disques complets, et ne dispose d’aucun mécanisme de déni plausible.
DiskCryptor est un outil fonctionnant uniquement sous Windows, il est open source mais non audité. Il permet au bootloader d’être installé sur une clé USB ou un CD, et est plus rapide que les autres.
Ciphershed est un fork de TrueCrypt, il est compatible avec les anciens disques chiffrés avec TrueCrypt, les mises à jour sont lentes, mais il fonctionne sur Mac, PC et Linux.
FileVault 2 est intégré à Mac OS X Lion et aux versions suivantes, il permet uniquement le chiffrement complet du disque, et n’est pas open source.
LUKS est un logiciel open source qui fonctionne sous Linux, il supporte plusieurs algorithmes, mais n’est pas compatible avec beaucoup d’autres systèmes en dehors de Linux.

Mise en œuvre du chiffrement.

Instalation et utilisation de veracrypt:

Installation:

```
root@debian11:~# apt install dirmngr software-properties-common apt-transport-https
 curl lsb-release ca-certificates -y
```

Nous allons installer l’outil depuis le site internet pour éviter les erreurs nous vous conseillons de copier le lien d’installation directement sur le site.

```
root@debian11:~# wget https://launchpad.net/veracrypt/trunk/1.26.7/+download/ver
acrypt-1.26.7-setup.tar.bz2
```

Nous allons ensuite le décompresser.

```
root@debian11:~# tar -jxvf veracrypt-1.26.7-setup.tar.bz2
```

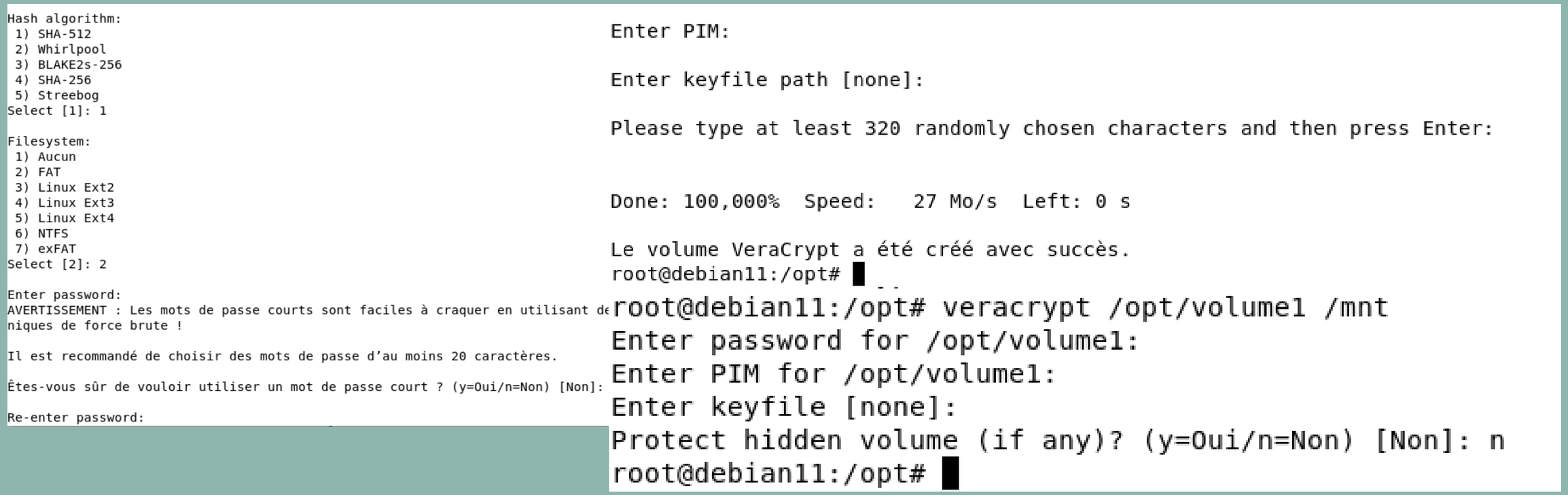
Pour ensuite lancer l’installation effectuez cette commande:./veracrypt-1.26.7-setup-gui-x64.

Sélectionnez ensuite les options que vous souhaitez.

```
VeraCrypt 1.26.7 Setup
_____________________


Installation options:

 1) Install veracrypt_1.26.7_amd64.tar.gz
 2) Extract package file veracrypt_1.26.7_amd64.tar.gz and place it to /tmp

To select, enter 1 or 2: 1

Before you can use, extract, or install VeraCrypt, you must accept the
terms of the VeraCrypt License.

Press Enter to display the license terms...
```

Une fois installer vous pourrez créer votre volume chiffré avec les commandes suivantes.
lors de cette création vous devrez choisir votre algorithme de chiffrement, et de hachage pour finir avec votre système de fichiers.

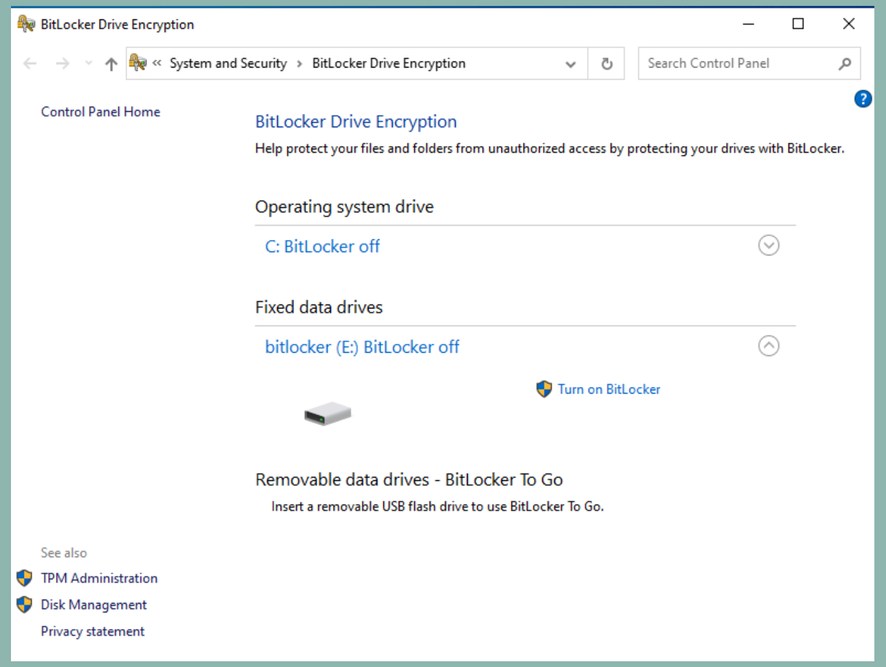
```
root@debian11:/opt# veracrypt -t -c
Volume type:
 1) Normal
 2) Hidden
Select [1]: 1

Enter volume path: /opt/volume1

Enter volume size (sizeK/size[M]/sizeG.sizeT/max): 200M

Algorithme de chiffrement:
 1) AES
 2) Serpent
 3) Twofish
 4) Camellia
 5) Kuznyechik
 6) AES(Twofish)
 7) AES(Twofish(Serpent))
 8) Camellia(Kuznyechik)
 9) Camellia(Serpent)
 10) Kuznyechik(AES)
 11) Kuznyechik(Serpent(Camellia))
 12) Kuznyechik(Twofish)
 13) Serpent(AES)
 14) Serpent(Twofish(AES))
 15) Twofish(Serpent)
Select [1]: 1
```



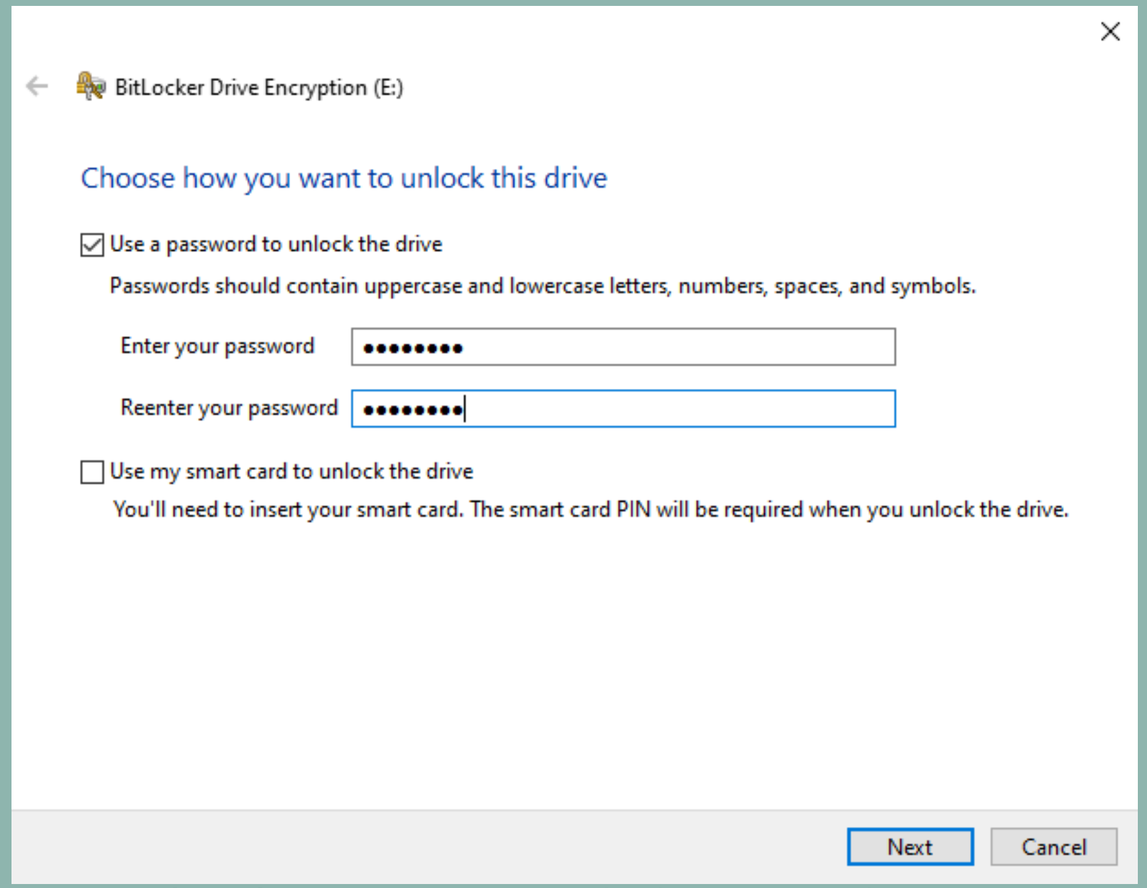
Voici votre volume chiffré.

Si vous voulez le déchiffrer vous pourrez utiliser la commande:
veracrypt -d volume1

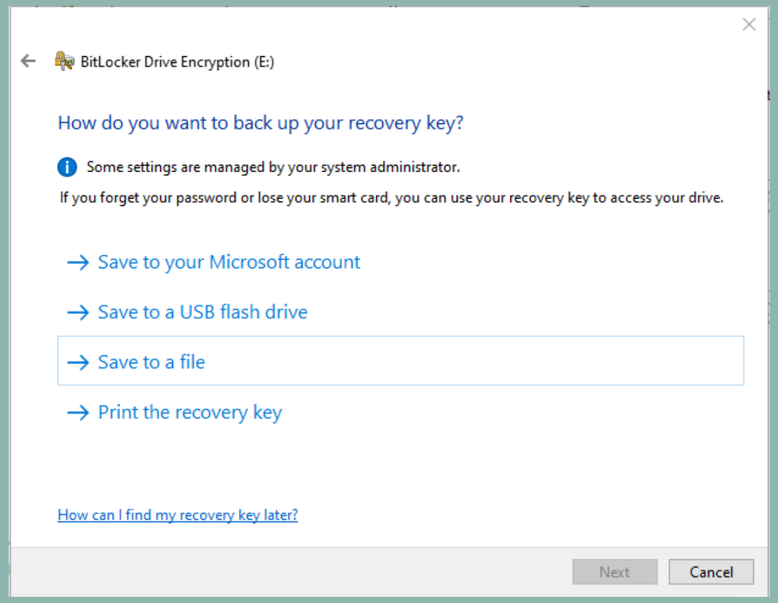
Passons maintenant sous Windows avec Bitlocker.
Remarque: Si vous possedez la version home de windows vous ne pourrez pas utiliser Bitlocker.
Pour y accéder tapez dans la barre de recherche en bas de votre écran manage Bitlocker.
Vous arriverez sur cette interface.



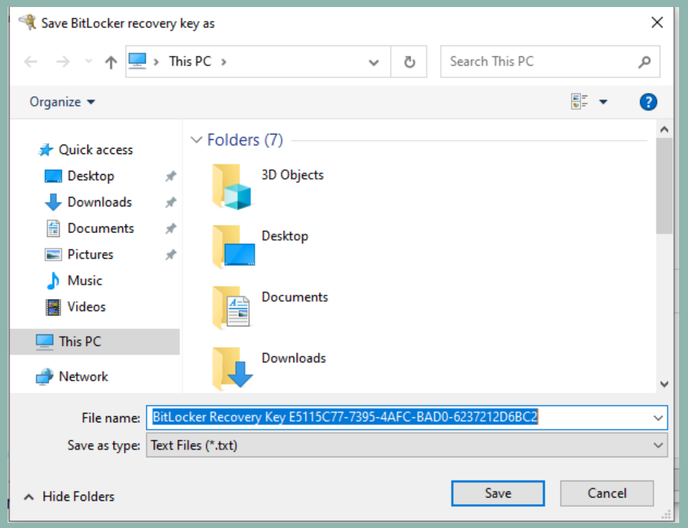
Pour activer Bitlocker vous devrez cliquer sur Turn on Bitlocker puis vous devrez sélectionner comment vous voulez déverrouiller votre disque.



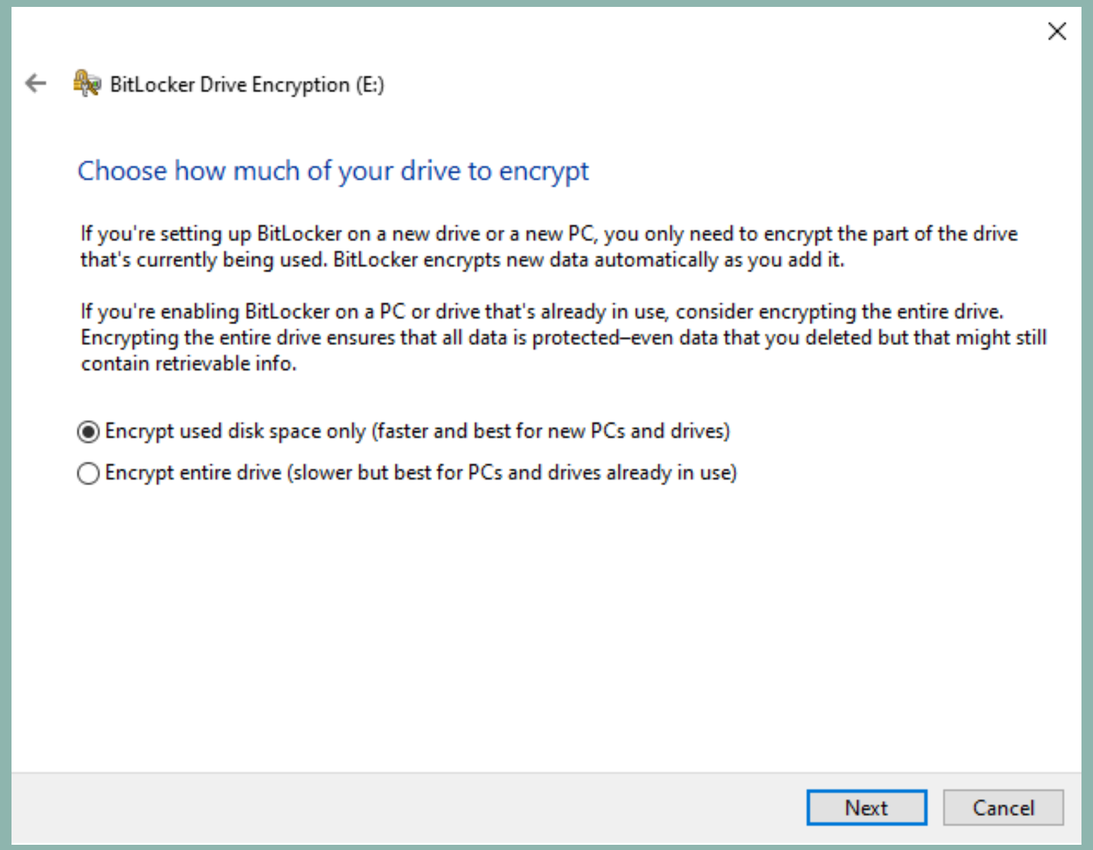
Ici vous devrez sélectionner comment récupérer votre sauvegarde de Recovery key nous avons opté pour enregistrer un fichier.

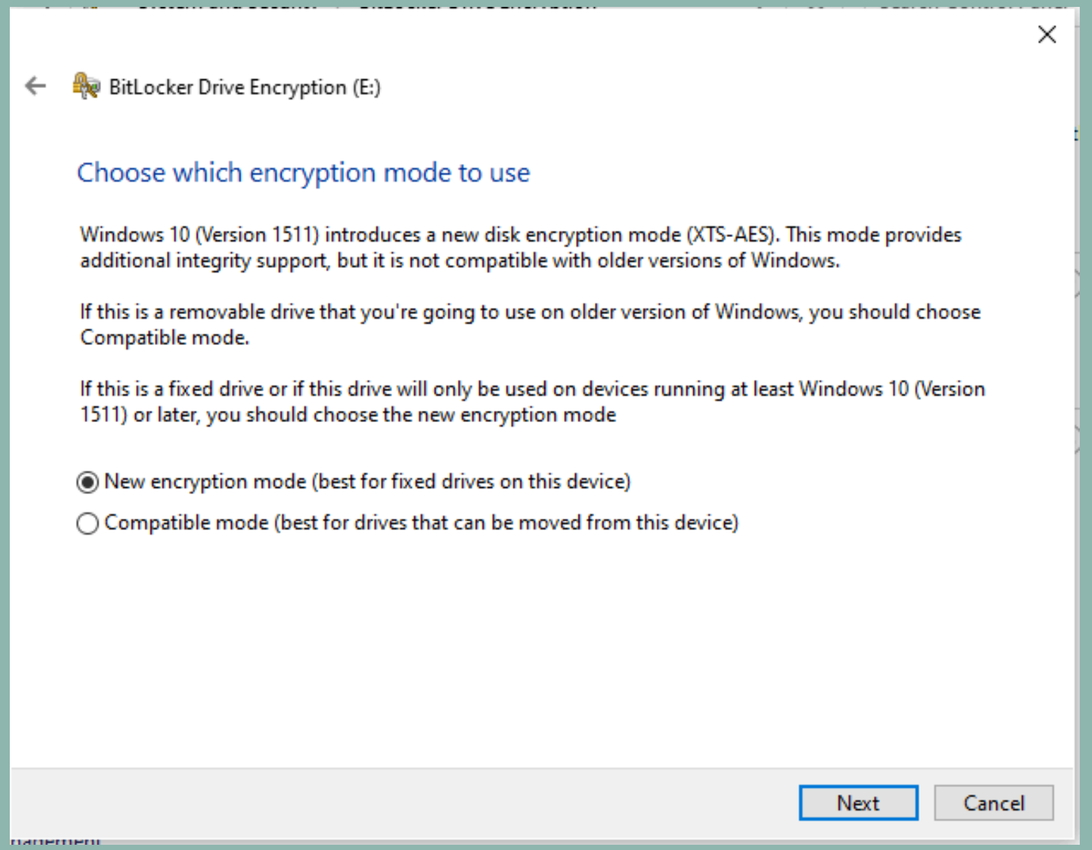


Sélectionnez ensuite l'endroit où mettre le fichier.

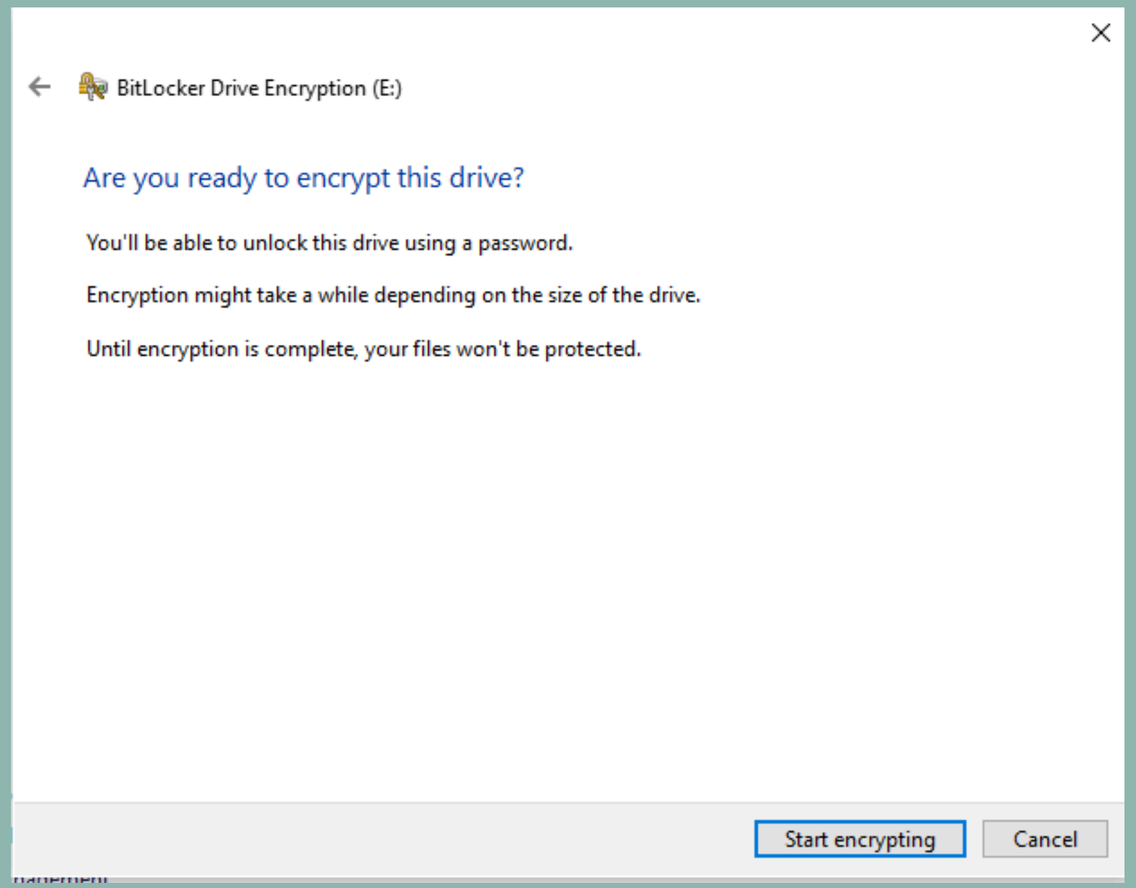


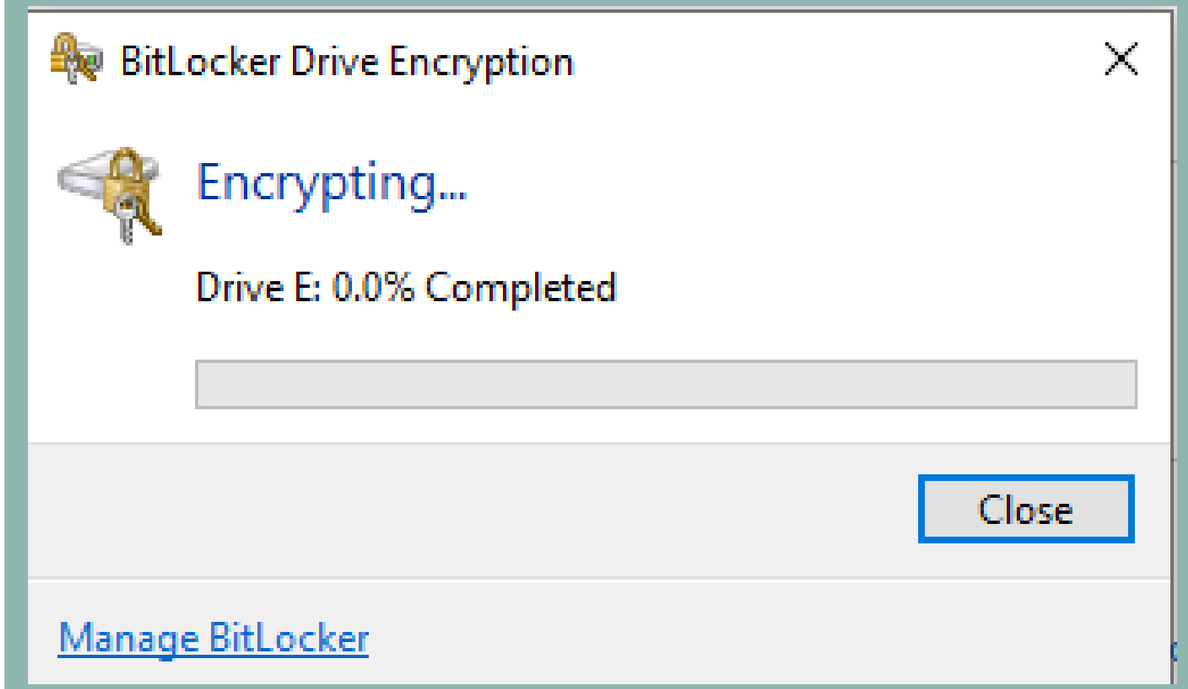
Ici choisissez si vous voulez chiffrer tout le disque ou seulement une partie.





Lancez ensuite le chiffrement.





Voici votre partition chiffrée, si vous voulez y accéder vous devrez donc entrer le mot de passe que vous aurez utilisé précédemment.

Et si vous voulez directement enlever le chiffrement alors retournez dans manage Bitlocker et cliquez sur TurnOff Bitlocker.