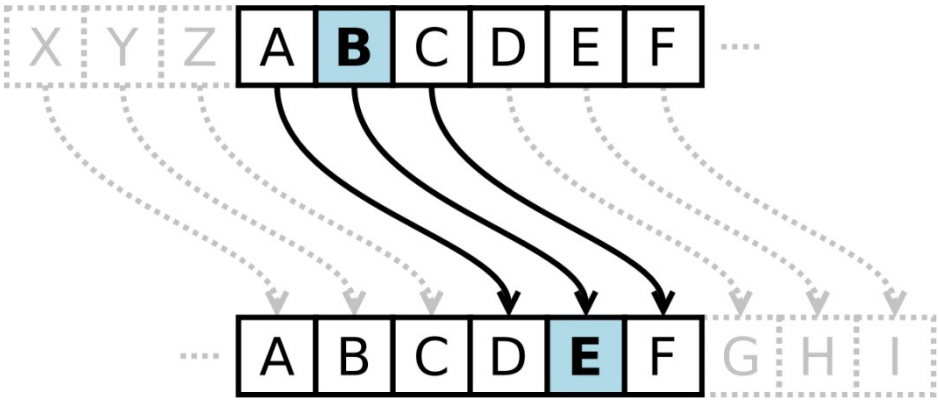
TP Chiffrement

I) Etude et Recherche.

1) Le Code César : Chiffrement par décalage de 3 rangs vers la droite dans l'alphabet.



2) Le Carré de Vigenère

Le chiffre de Vigenère est un système de chiffrement par substitution polyalphabétique dans lequel une même lettre du message clair peut, suivant sa position dans celui-ci, être remplacée par des lettres différentes

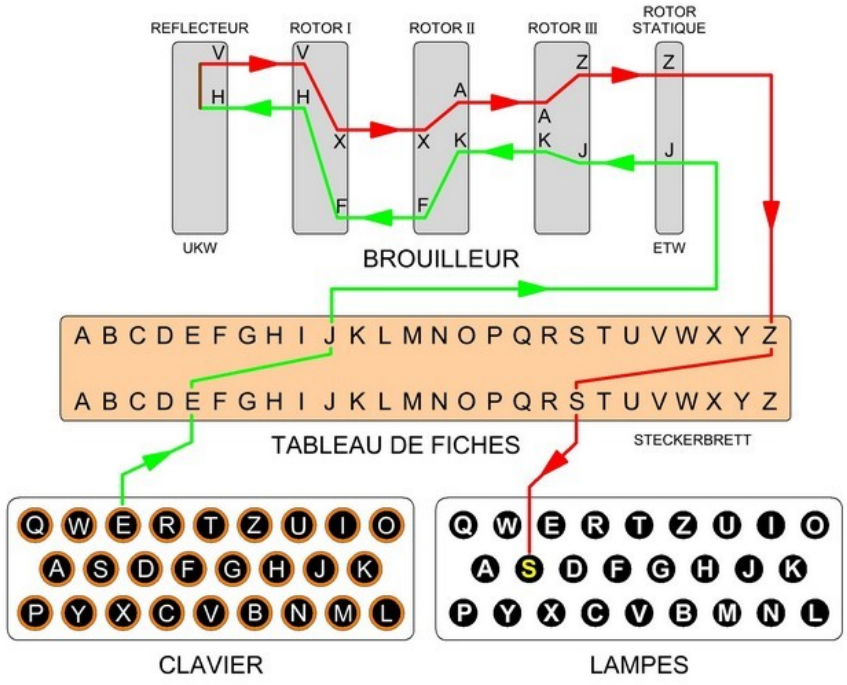
Exemple :

clair MONMESSAGE
clef MACLEFMACL
chiffré YOPXIXEAIP

	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

3) La machine « Enigma »

le chiffrement par substitution. chaque fois qu'une lettre est tapée au clavier, le rotor tourne d'un cran



4) Le téléphone rouge

Supposons que la clé aléatoire retenue, ou « masque », soit :

```
WMCKL
```

Cette clé est choisie à l'avance entre les deux personnes souhaitant communiquer. Elle n'est connue que d'elles.

```
   7 (H)   4 (E)  11 (L)  11 (L)  14 (O) message
+ 22 (W)  12 (M)   2 (C)  10 (K)  11 (L) masque
= 29      16      13      21      25     masque + message
=  3 (D)  16 (Q)  13 (N)  21 (V)  25 (Z) masque + message  modulo 26
```

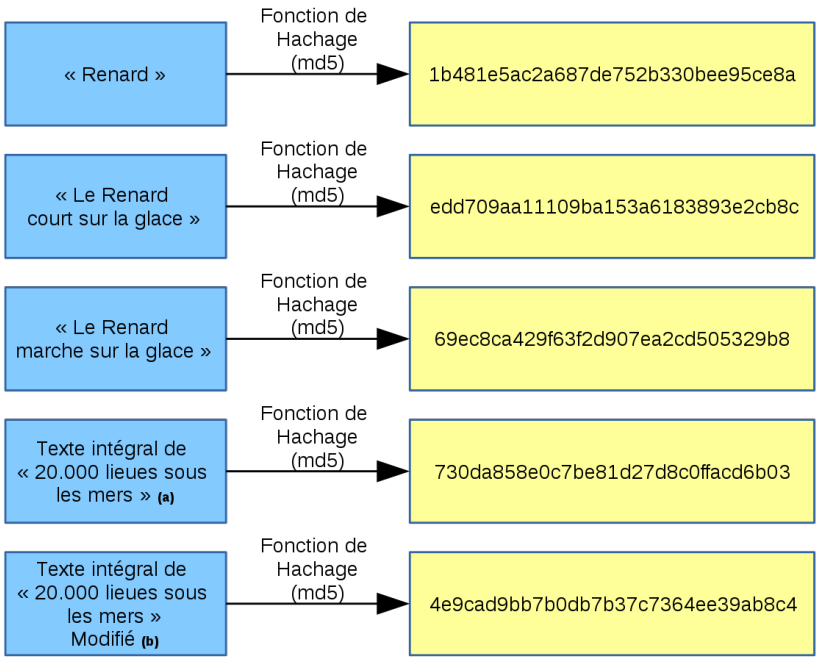
Le texte reçu par le destinataire est « DQNVZ ».

Le déchiffrement s'effectue de manière similaire, sauf que l'on soustrait le masque au texte chiffré au lieu de l'additionner. Ici encore on ajoute éventuellement 26 au résultat pour obtenir des nombres compris entre 0 et 25 :

```
    3 (D)  16 (Q)  13 (N)  21 (V)  25 (Z) message chiffré
-  22 (W)  12 (M)   2 (C)  10 (K)  11 (L) masque
= -19       4      11      11      14     message chiffré - masque
=   7 (H)   4 (E)  11 (L)  11 (L)  14 (O) message chiffré - masque modulo 26
```

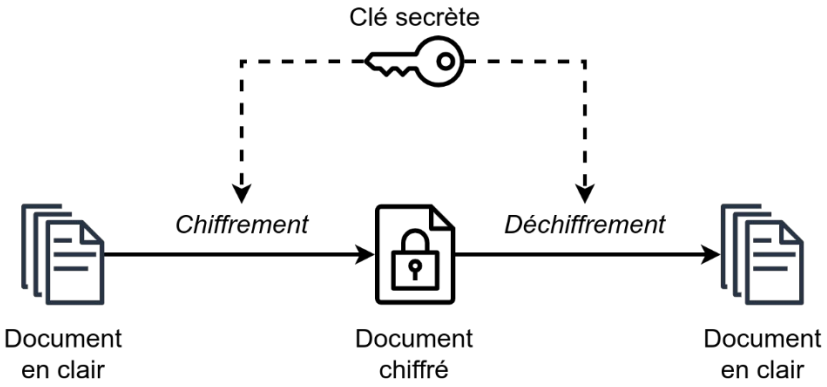
5) Le hachage

Le hachage est la transformation d'une chaîne de caractères en valeur ou en clé de longueur fixe, généralement plus courte, représentant la chaîne d'origine.



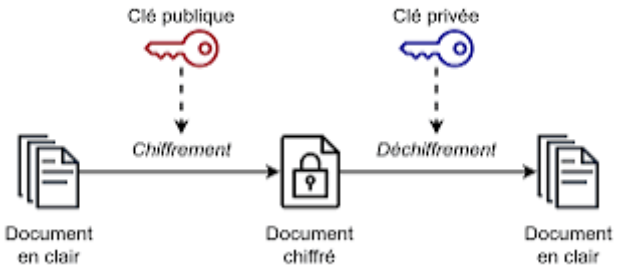
6) Le chiffrement à clé symétrique

un terme utilisé pour décrire les algorithmes de chiffrement qui utilisent une même clé pour le chiffrage et le déchiffrage.



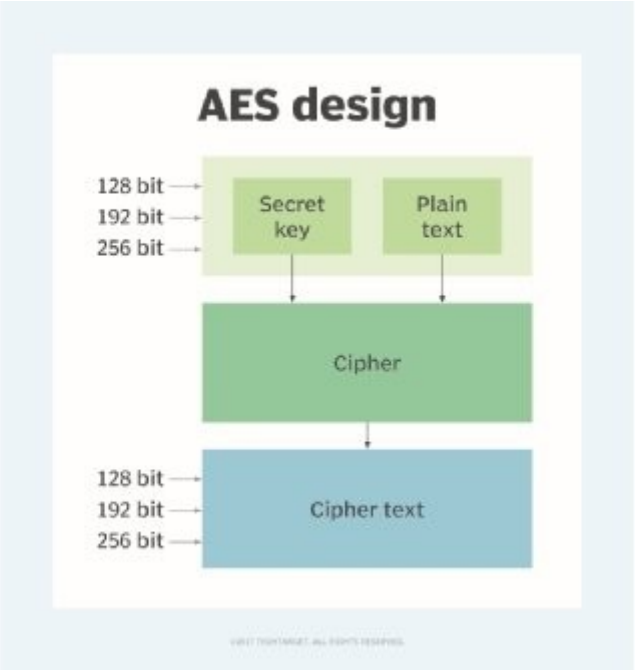
7) Le chiffrement à clé asymétrique

utilise un ensemble de deux clés : une clé publique pour le chiffrement et une clé privée pour le déchiffrement, que seule une partie connaît



8) Le chiffrement AES

AES est un réseau de substitution-permutation qui utilise un processus d'expansion de clé où la clé initiale est utilisée pour générer de nouvelles clés appelées clés de tour. Les clés de tour sont générées sur plusieurs tours de modification. Chaque tour rend le chiffrement plus difficile à casser.



9)La différence entre chiffrement bijectif et hachage

le chiffrement bijectif utilise une clé pour chiffrer et déchiffrer les données /mot de passe tandis que hachage ne permet pas le déchiffrement il chiffre le mot de passe mais ne permet pas de faire la manipulation inverse c'est donc une empreinte unique

10)Les limites du hachage des mots de passe

même si il y a une utilisation du hachage si le mot de passe est faible il pourra facilement être déchiffré

11)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.

12) La stéganographie

permet de dissimuler un mot de passe dans un texte , une vidéo , un audio ou encore un réseau.

II) L'outil Truecrypt

1) Expliquer à quoi sert l'outil truecrypt.

C'est un logiciel de chiffrement de données qui permet donc de créer des volumes chiffrés

2) Expliquer le principe de fonctionnement de TrueCrypt, et en particulier en quoi il est différent des autres outils « classiques » de chiffrement.

C'est un outil de chiffrement à la volée c'est a dire que dès que le conteneur (volume) est déchiffré l'utilisateur à accès a tout les fichier de ce volume mais dès qu'il n'en a plus besoin celui-ci est donc de nouveau chiffré. Truecrypt permet aussi de créer des volumes chiffrés de manière transparente c'est a dire sans faire de modification majeur sur les volumes de fichier c'est pour cela qu'il est facilement utilisable sur plusieurs systèmes d'exploitation

3) Concluez sur l'intérêt d'utiliser Truecrypt au sein d'une société.

Il peut permettre de sécuriser des données sensible, peut être utilisé sur plusieurs système d'exploitation (Windows, MacOS, Linux) .

4) Rechercher des solutions alternatives à Truecrypt.

Les solutions alternatives possible sont : Veracrypt, Bitlocker,Ciphershed

III) Mise en œuvre d'une solution de chiffrement

1. Installer une solution de chiffrement sur une machine virtuelle :

bitlocker : Windows

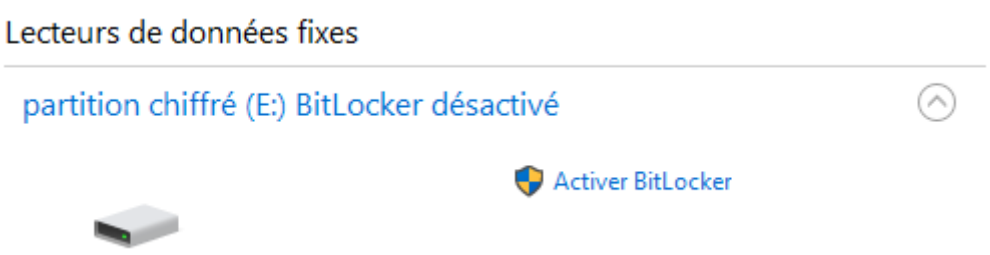
veracrypt: Linux

2. Vous pratiquerez un chiffrement d'une partition de votre machine virtuelle.

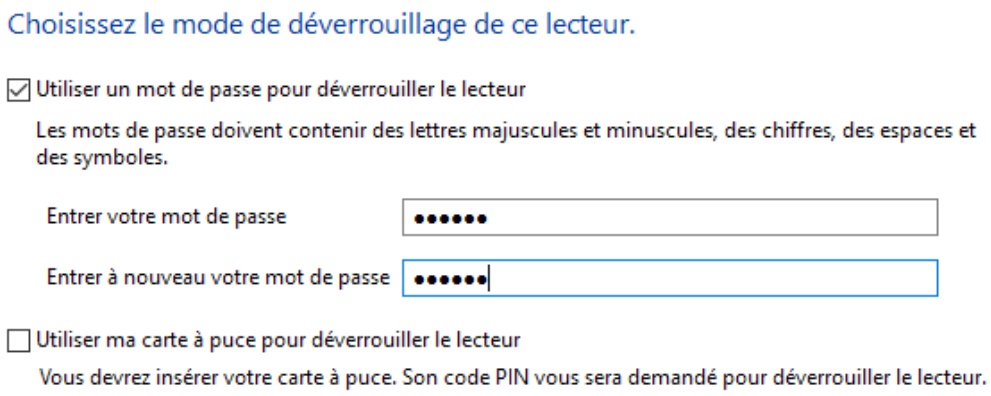
3. Vous rédigerez une notice technique d'utilisation de chiffrement et de déchiffrement

Chiffrement sur Bitlocker :

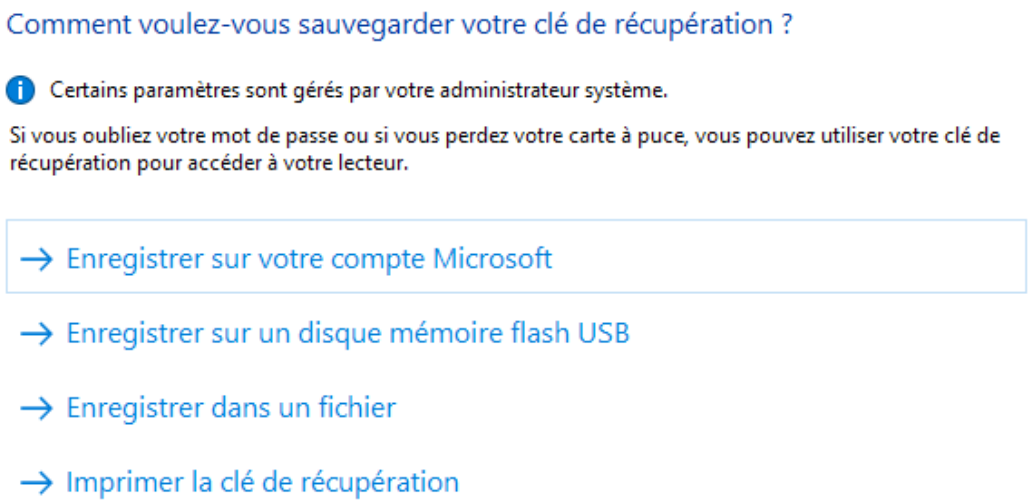
Dans la barre de recherche taper « **Gérer BitLocker** » puis y accéder . Sélectionner le disque dur puis cliquer ensuite sur « **Activer BitLocke**r »



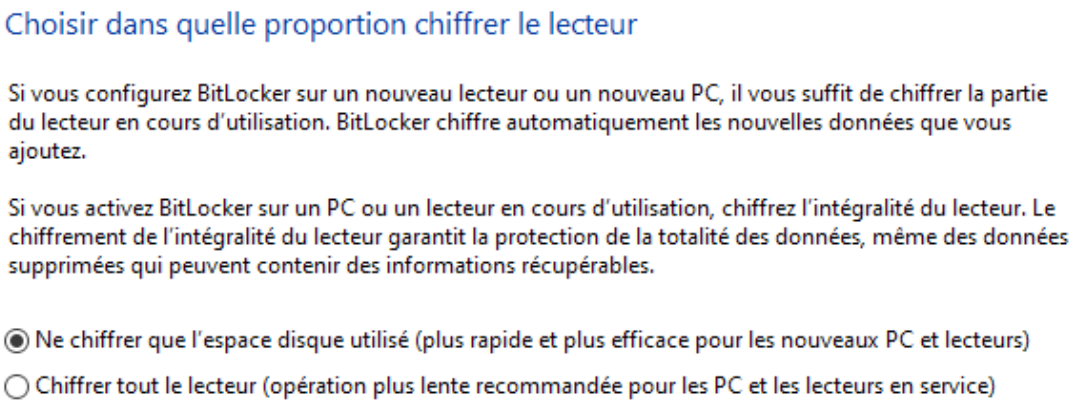
Choisir son modèle de verrouillage :



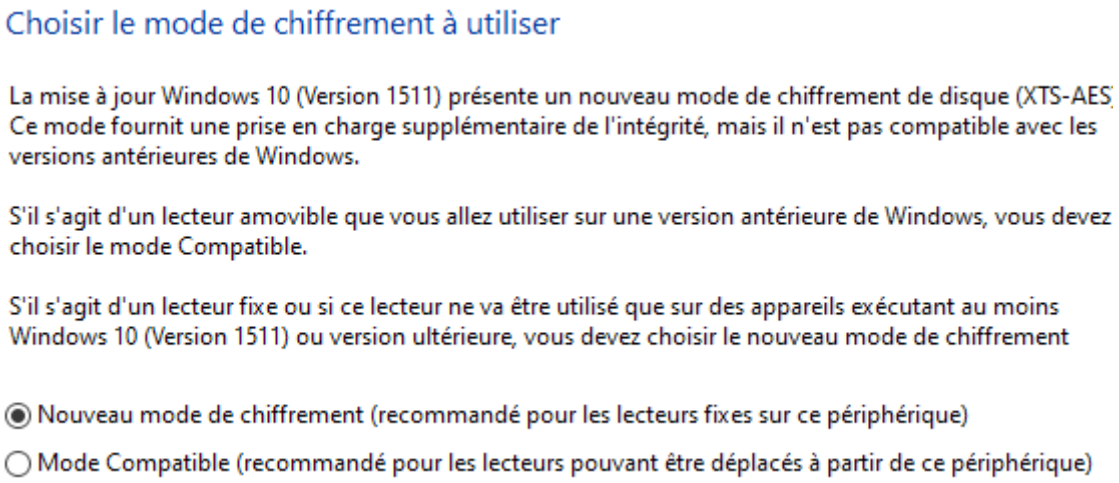
Choisir ou sauvegarder notre clé de récupération :



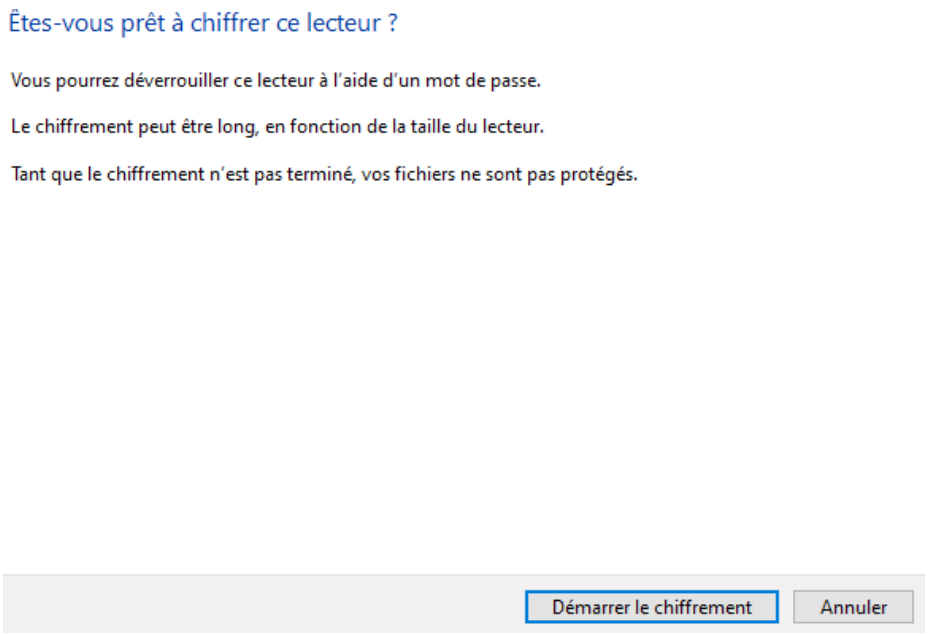
Choisir comment chiffrer son disque :



Choisir son mode de chiffrement :

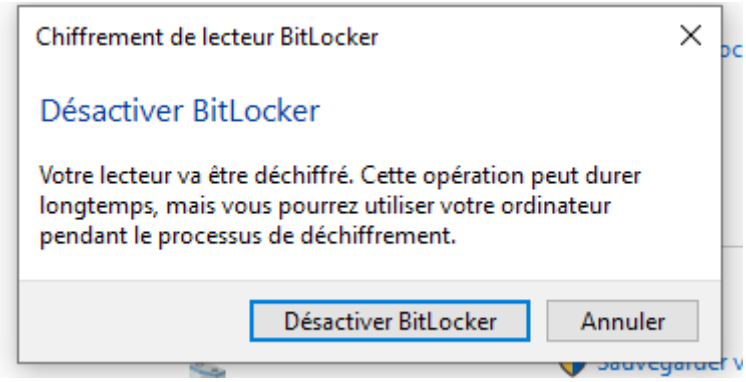


Démarrer le chiffrement



Déchiffrement sur Bitlocker :

Aller dans « G**érer Bitlocker** » puis cliquer sur « **Désactiver BitLocker** » sur la partition souhaité.



Installation de VeraCrypt :

Telecharger veracrypt avec la ligne suivante **wget http://sourceforge.net/projects/veracrypt/files/VeraCrypt%201.0f-2/veracrypt-1.0f-2-setup.tar.bz2**

décompresser l'archive avec la commande **tar xvjf veracrypt-1.0f-2-setup.tar.bz2**

taper la commande **uname -r** pour vérifier quelle version installer :

```
root@deb11rwz:/home/non-root# uname -r
5.10.0-26-amd64
```

dans notre cas taper la commande **./veracrypt-1.0f-2-setup-console-x64**

```
Installation options:

 1) Install veracrypt_1.0f-2_console_amd64.tar.gz
 2) Extract package file veracrypt_1.0f-2_console_amd64.tar.gz and place it to /
tmp

To select, enter 1 or 2: 1
```

taper 1 puis confirmer les termes de la licence

Chiffrement sur VeraCrypt :

taper **veracrypt -t -c pour créer un volume chiffré.** Sélectionner les option souhaité

Q

```
root@deb11rwz:/home/non-root# veracrypt -t -c
Volume type:
 1) Normal
Enter password:
Re-enter password:

Enter keyfile path [none]:

Please type at least 320 randomly chosen characters and then press Enter:
Characters remaining: 315
Characters remaining: 20
Characters remaining: 5


Done: 100,000%  Speed:   22 MB/s  Left: 0 s
The VeraCrypt volume has been successfully created.
 6) Serpent(AES)
 7) Serpent(Twofish(AES))
 8) Twofish(Serpent)
Select [1]: 1

Hash algorithm:
 1) SHA-512
 2) Whirlpool
 3) SHA-256
Select [1]: 1

Filesystem:
 1) None
 2) FAT
 3) Linux Ext2
 4) Linux Ext3
 5) Linux Ext4
 6) NTFS
Select [2]: 2

Enter password:
Re-enter password:
```

pour monter un volume chiffré taper la commande **veracrypt *home*/non-root/volumechiffré /dossierchiffré**

Déchiffrement sur VeraCrypt :

Pour démonter un volume chiffré taper la commande **veracrypt -d volumeademonter** pour tout démonter tout les volumes veracrypt -d