

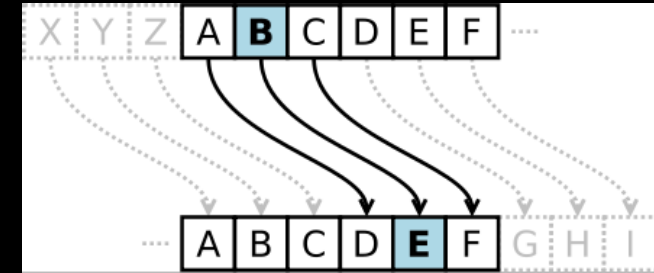
CHIFFREMENT



Raphaël ZAKRZEWSKI

Étude et Recherche

- **Code César** : Chiffrement par décalage, exemple de décalage par 3 :



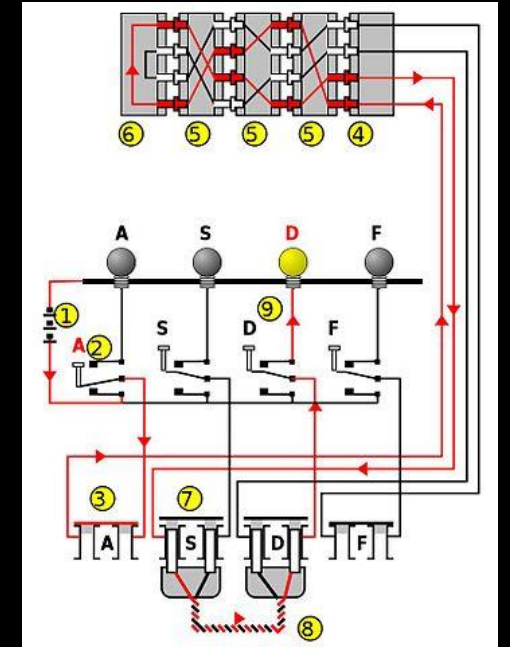
- **Carré de Vigenère** : On choisit une clé (ici « musique »), puis on cherche le croisement entre les colonnes (lettres du texte non chiffré) et les lignes (lettres de la clé) dans ce tableau :

Clé : musique	
Texte : J'adore écouter la radio toute la journée	
Texte en clair :	j'adore ecoutar la radio toute la journee
Clé répétée :	M USIQU EMUSIQU EM USIQU EMUSI QU EMUSIQU
	^ ^^^
	Colonne O, ligne I : on obtient la lettre W.
	Colonne D, ligne S : on obtient la lettre V.
	Colonne A, ligne U : on obtient la lettre U.
	Colonne J, ligne M : on obtient la lettre V.
Le texte chiffré est alors :	
V'UVWHY IOIMBUL PM LSLYI XAOLM BU NAOJVUY.	

	Lettre en clair																									
	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
Lettre de la clé	Lettres chiffrées (au croisement de la colonne Lettre en clair et de la ligne Lettre de la clé)																									
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

Étude et Recherche

- **Machine Enigma** : Ça substitue chaque lettre d'un message par une autre via un circuit électrique à travers des rotors. La configuration des rotors, qui peut être changée pour chaque message est la clé du chiffrement.
- **Téléphone rouge** : Ça utilise le principe du masque jetable, à l'aide de machines de chiffrement appeler « Electronic Teleprinter Cryptographic Regenerative Repeater Mixer (ETCRRM) », donc à chaque message envoyé une clé est générée et est à usage unique, la clé doit être une suite de caractères au moins aussi longue que le message à chiffrer, ces caractères sont choisis aléatoirement.

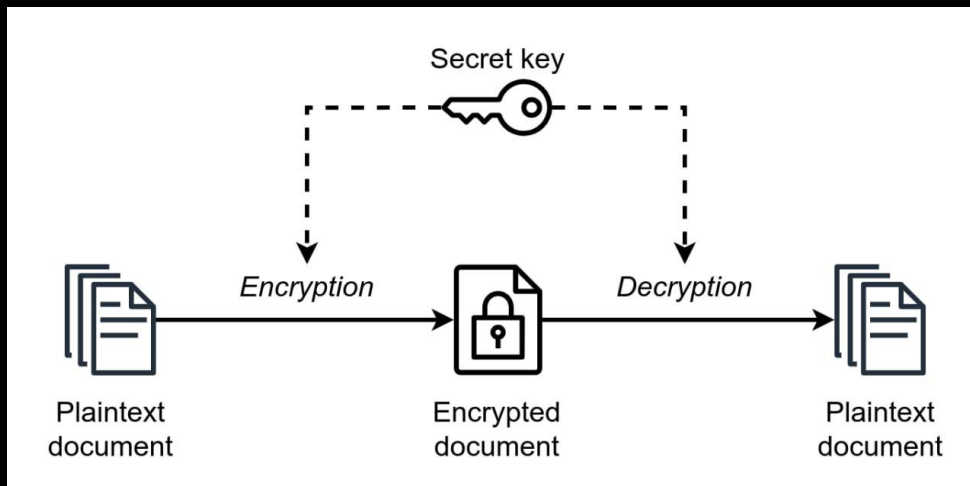


Étude et Recherche

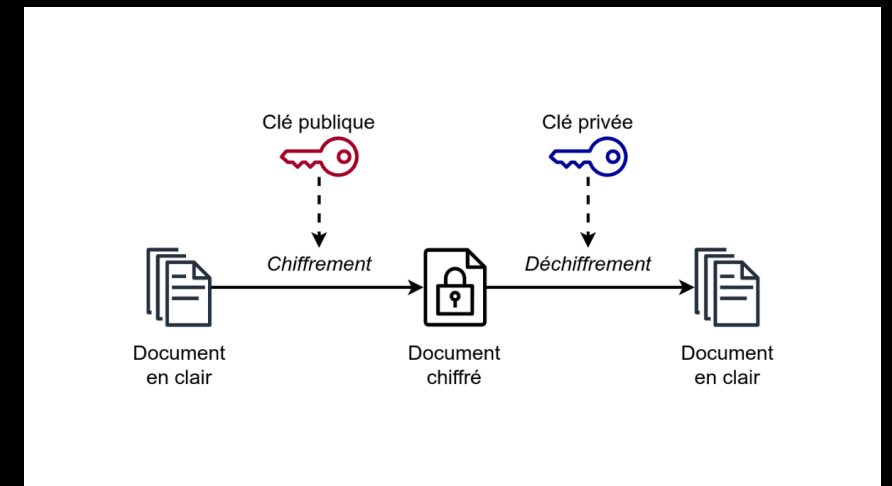
- **Hachage** : Ça permet un chiffrement avec une longueur fixe via des fonctions ici la fonction md5 :

« Renard »	md5	1b481e5ac2a687de752b330bee95ce8a
« Le Renard court sur la glace »	md5	edd709aa11109ba153a6183893e2cb8c
« Le Renard marche sur la glace »	md5	69ec8ca429f63f2d907ea2cd505329b8
Texte intégral de « 20.000 lieues sous les mers » (a)	md5	730da858e0c7be81d27d8c0ffacd6b03
Texte intégral de « 20.000 lieues sous les mers » Modifié (b)	md5	4e9cad9bb7b0db7b37c7364ee39ab8c4

Chiffrement à clé symétrique :



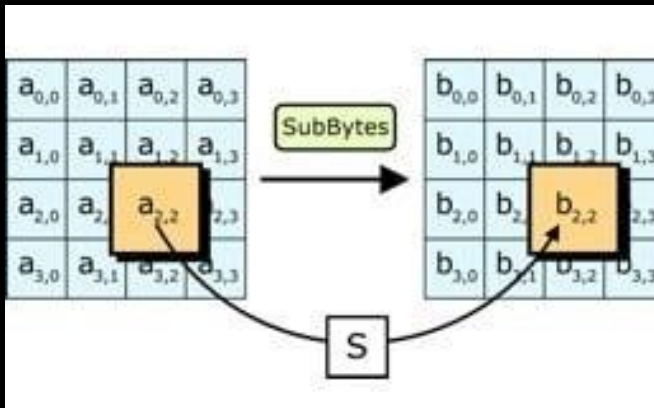
Chiffrement à clé asymétrique :



Étude et Recherche

Chiffrement AES : L'algorithme prend en entrée un bloc de 128 bits (16 octets), la clé fait 128, 192 ou 256 bits. Les 16 octets en entrée sont permutés selon une table définie au préalable. Ces octets sont ensuite placés dans une matrice de 4x4 éléments et ses lignes subissent une rotation vers la droite. L'incrément pour la rotation varie selon le numéro de la ligne. Une transformation linéaire est ensuite appliquée sur la matrice, elle consiste en la multiplication binaire de chaque élément de la matrix avec des polynômes issus d'une matrice auxiliaire, cette multiplication est soumise à des règles spéciales selon GF(28) (groupe de Galois ou corps fini). La transformation linéaire garantit une meilleure diffusion (propagation des bits dans la structure) sur plusieurs tours.

Finalement, un OU exclusif XOR entre la matrice et une autre matrice permet d'obtenir une matrice intermédiaire. Ces différentes opérations sont répétées plusieurs fois et définissent un « tour ». Pour une clé de 128, 192 ou 256, AES nécessite respectivement 10, 12 ou 14 tours.



Étude et Recherche

La principale différence entre le hachage et le chiffrement bijectif est qu'on peut déchiffrer un message chiffré avec le chiffrement bijectif mais pas si il est haché car le hachage est unidirectionnel il ne permet pas grâce à la clé de retrouver le message initial.

Les limites du hachage sont :

- Les mots de passes faibles
- Les attaques brute force et par bibliothèques
- Avec le temps certains hachages deviennent obsolètes

Truecrypt

TrueCrypt est un logiciel de chiffrement de données utilisé pour créer des volumes cryptés sur des disques durs, des clés USB ou d'autres supports de stockage. Il permettait aux utilisateurs de protéger leurs fichiers en les rendant illisibles sans le mot de passe correct.

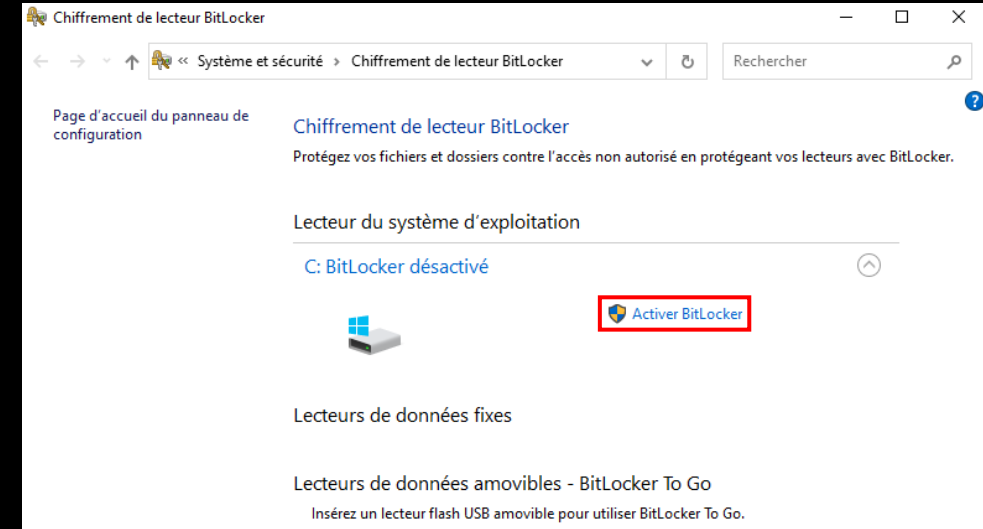
TrueCrypt était un logiciel sécurisé permettant de créer des espaces de stockage cryptés appelés "conteneurs". Ces conteneurs agissaient comme des coffres-forts numériques, protégeant les fichiers avec un mot de passe. En étant open source, TrueCrypt offrait simplicité et transparence, ce qui en faisait un choix populaire pour sécuriser les données confidentielles.

Cela permet de sécuriser les fichiers de l'entreprise ce qui peut contrer plusieurs types d'attaque comme le phishing les ransomware et plein d'autre.

D'autres logiciels peuvent être utilisés comme Bitlocker pour Windows et VeraCrypt pour Linux

Mise en œuvre Windows

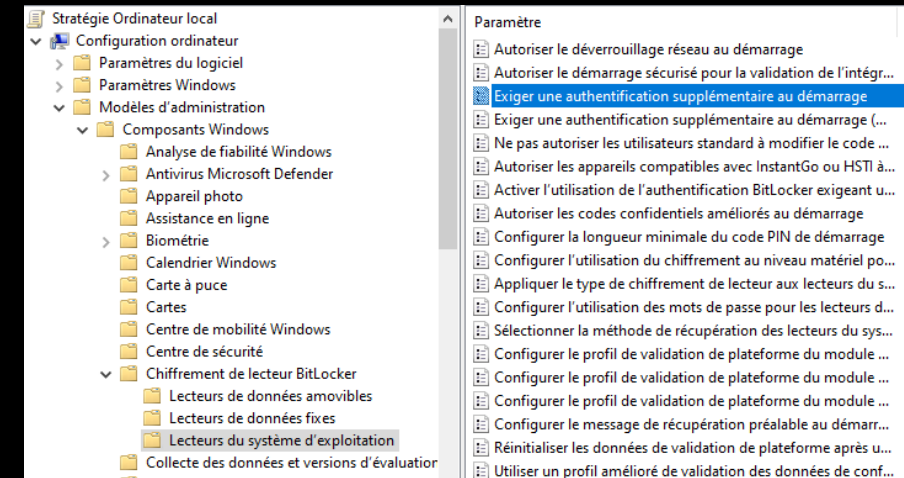
- Chercher dans la barre de recherche Windows « Gérer BitLocker » puis l'activer :
- Si ce message s'affiche c'est que l'ordinateur n'a pas de puce TPM ce qui signifie que si on active BitLocker Windows ne pourras pas déverrouiller l'accès au disque seul car la clé secrète qui sert à le déverrouiller est normalement stockée dans la puce TPM, ce qui implique quelque étape supplémentaire.



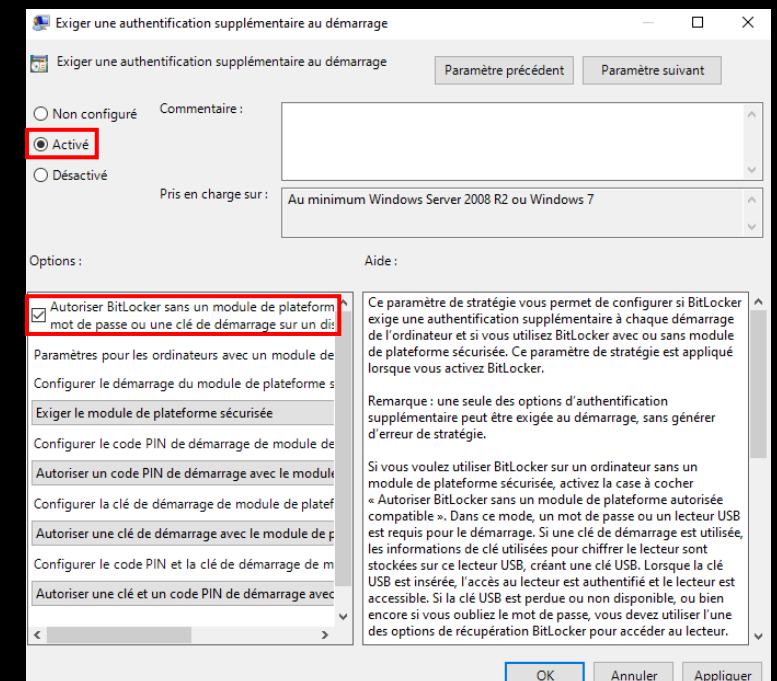
Mise en œuvre Windows

Sans puce TPM

- Faire « Win + R » puis « gpedit.msc » et aller dans « Exiger une authentification supplémentaire au démarrage » :

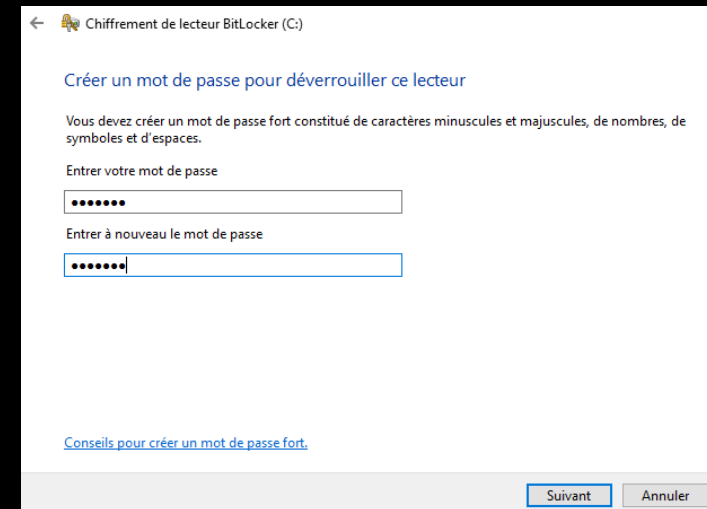
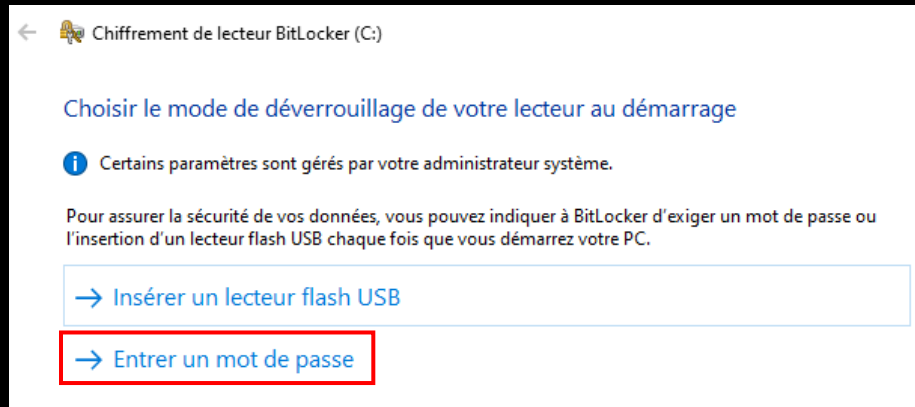


- Sélectionner « Activé » et cocher « Autoriser BitLocker ... » :

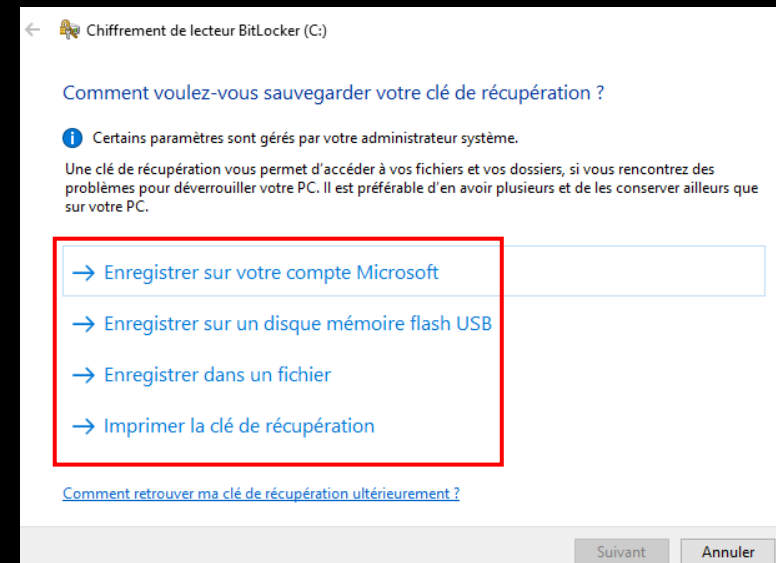


Mise en œuvre Windows

Choisir « Entrer un mot de passe » et en saisir un :

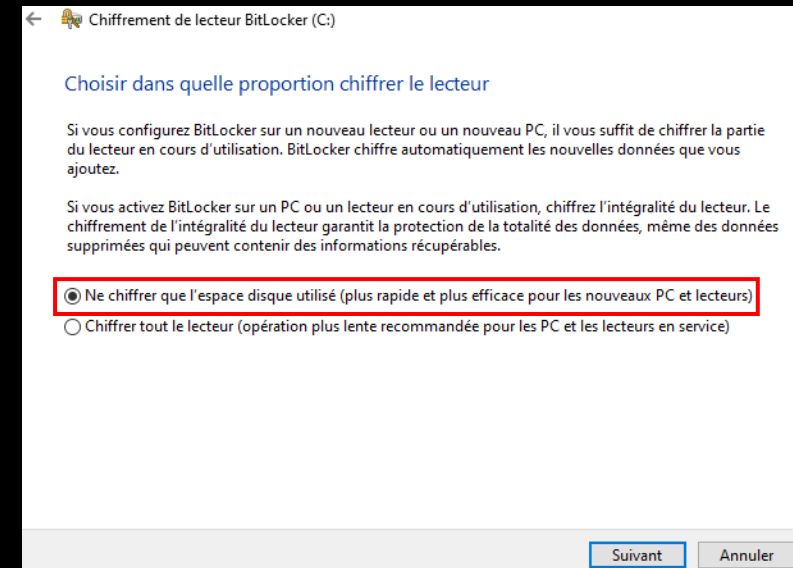


Choisir le mode de conservation de la clé de chiffrement :

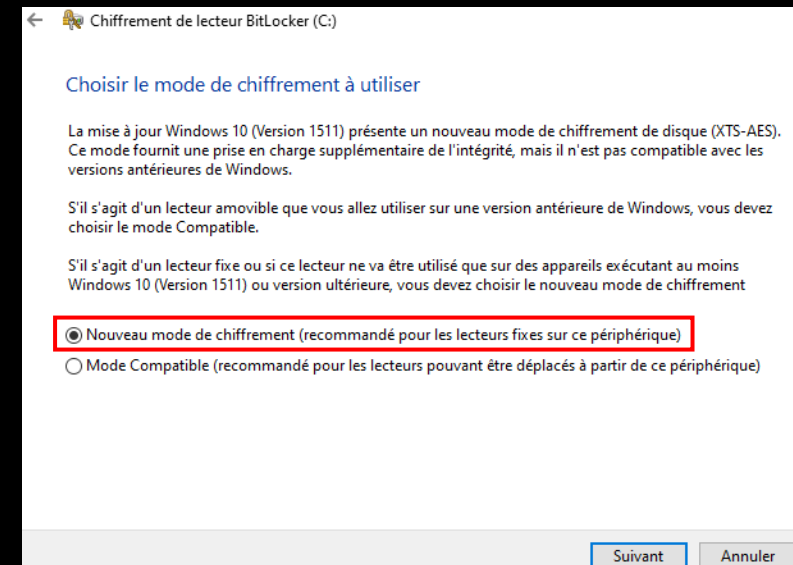


Mise en œuvre Windows

- Ici on veut chiffré uniquement une partition :

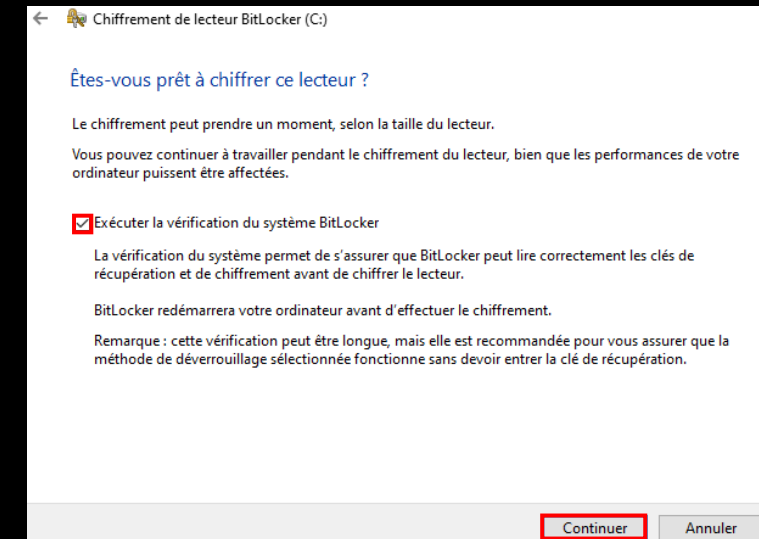


- Ici on utilise un lecteur fixe :



Mise en œuvre Windows

- Cocher « Exécuter la vérification du système BitLocker » et faire « Continuer » puis redémarrer la machine :

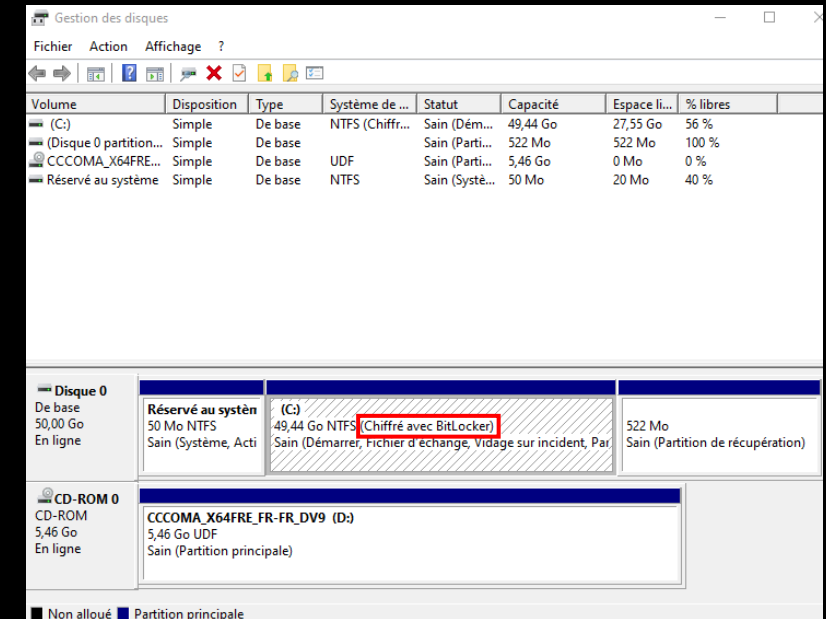


- Pendant le redémarrage de la machine il faudra entrer le mot de passe définie avant :

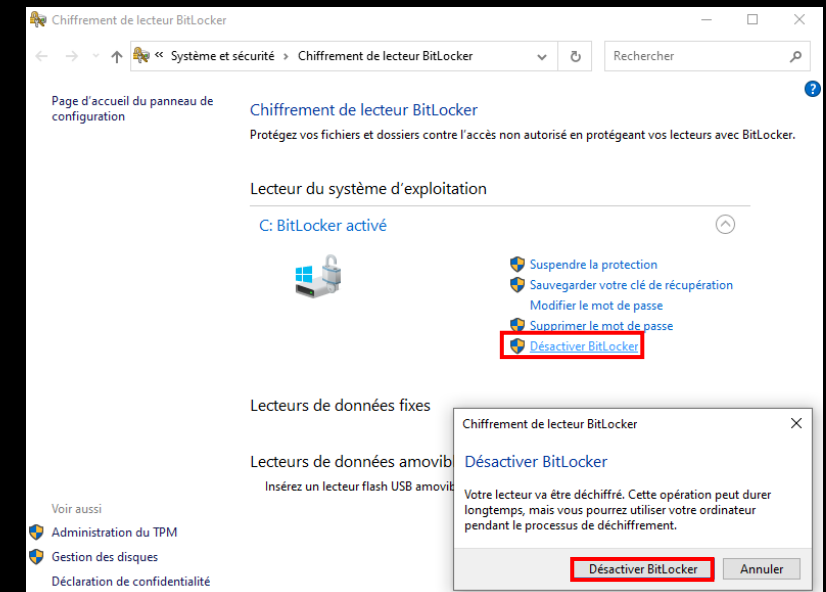


Mise en œuvre Windows

- On peut vérifier que la partition à bien été chiffrer en allant dans le gestionnaire de disque :



- Pour déchiffrer la partition il suffit de désactiver BitLocker :



Mise en œuvre Linux

- Pour installer Veracrypt faire « wget <http://sourcefor-genet/projects/veracrypt/files/Veracrypt%201.0f-2/veracrypt-1,0f-2-setup.tar.bz2> »
- Ensuite on l'extrait « tar xvjf veracrypt-1.0f -2-setup.tar.bz2 »
- Puis on l'exécute « ./veracrypt-1.0f -2-setup.console-x64 » et faire 1 :

```
VeraCrypt 1.0f-2 Setup
```

```
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:
```

Mise en œuvre Linux

- On choisit les paramètres de l'installation :

```
root@root:/home/root2023# veracrypt -t -c
Volume type:
 1) Normal
 2) Hidden
Select [1]: 1

Enter volume path: /home/root2023/dossier_chiffre

Enter volume size (sizeK/sizeM/sizeG): 400M

Encryption algorithm:
 1) AES
 2) Serpent
 3) Twofish
 4) AES(Twofish)
 5) AES(Twofish(Serpent))
 6) Serpent(AES)
 7) Serpent(Twofish(AES))
 8) Twofish(Serpent)
```

```
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]: 6

Enter password:
```

```
Re-enter password:

Enter keyfile path [none]:

Please type at least 320 randomly chosen characters and then press Enter:

Done: 100,000% Speed: 8,2 MB/s Left: 0 s
Done: 100,000% Speed: 7,7 MB/s Left: 0 s

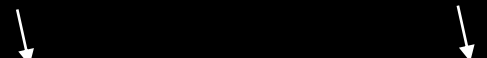
The VeraCrypt volume has been successfully created.
```

Mise en œuvre Linux

- Ensuite on créer un dossier pour pouvoir monter le volume chiffrer créer au préalable :

Volume chiffrer

Dossier où on va monter le volume



```
root@root:/home/root2023# veracrypt /home/root2023/dossier_chiffre /home/root2023/volum
e_chiffre
Enter password for /home/root2023/dossier_chiffre:
Enter keyfile [none]:
Protect hidden volume (if any)? (y=Yes/n=No) [No]: n
```

Mise en œuvre Linux

- Après toutes ses étapes on reçoit une notification qui approuve la création d'un volume :



Volume de 419 Mo

- Pour supprimer le volume il suffit de rentrer cette commande :

```
root@root:/home/root2023# veracrypt -d /home/root2023/volume_chiffre
```