



[TP-B3]

[MOTY BERTRAND]

[ Bts sio 1ère année]

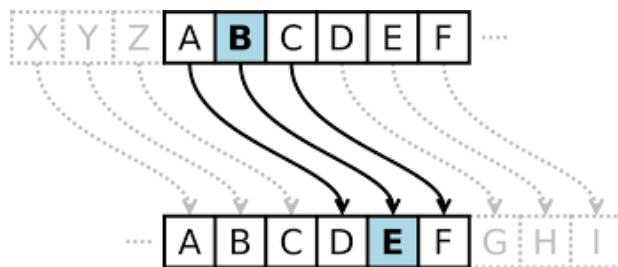
[M. FENETRE]

[27/03/2023]

## I) Etude et Recherche

### 1. Le Code César

C'est un alphabet qui décale les lettres. Par exemple, si le nombre d'espaces à décaler est de 3, alors la lettre A deviendra D, B deviendra E et ainsi de suite.



### 2. Le Carré de Vigenère

Il permet de remplacer une lettre par une autre qui n'est pas toujours la même. C'est un système de chiffrement poly alphabétique.

	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 »

La machine Enigma permet de brouiller les messages une lettre à la fois au moyen d'un réseau complexe de fils électriques. L'opérateur fait passer un courant électrique dans la machine en appuyant sur une touche.



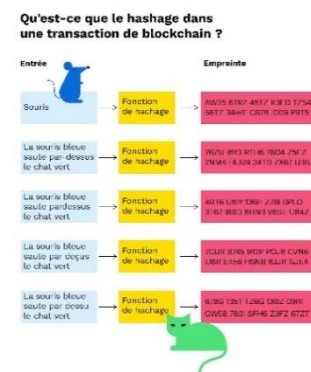
## 4. Le téléphone rouge

C'est un dispositif technique qui permet la communication directe, sans l'intermédiaire du corps diplomatique, entre les dirigeants des Etats-Unis et d l'URSS. Le téléphone rouge permettait de se parler rapidement dans les périodes de crise internationales.



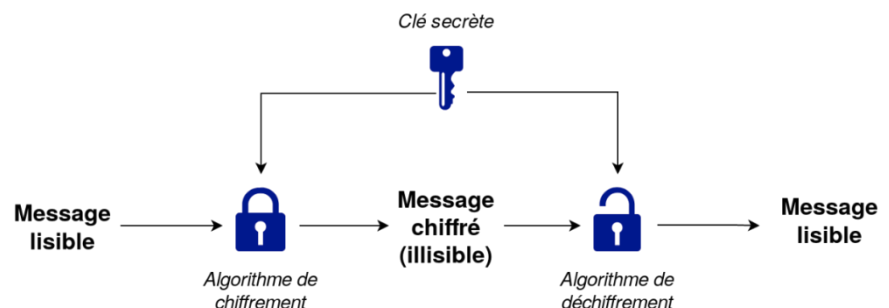
## 5. Le hachage

Le hachage est une méthode qui permet de ne pas stocker les mots de passe en clair dans la base mais uniquement de stocker une empreinte de ces derniers.



## 6. Le chiffrement à clé symétrique

Il y a une clé, qui est connue des deux parties, est utilisée pour transformer les données en texte illisible, ce qui en fait un moyen pratique de sécuriser les informations sensibles.

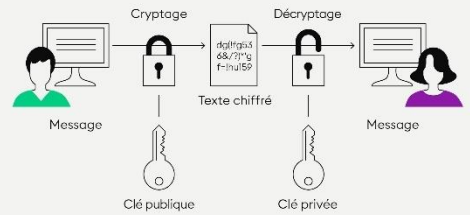


## 7. Le chiffrement à clé asymétrique

Le chiffrement à clé asymétrique on utilise la clé publique du destinataire pour chiffrer et la clé privée du destinataire pour déchiffrer un message. Par exemple si Alexis veut envoyer un message chiffré à ugo, il chiffre le message avec la clé publique de ugo puis envoie à ugo le texte chiffré.

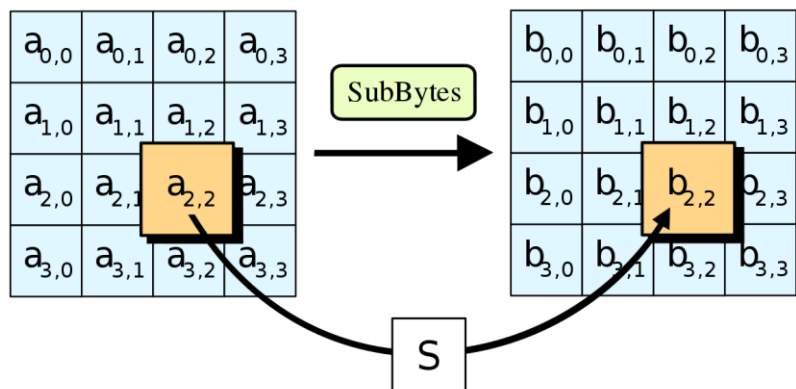
## CRYPTAGE ASYMÉTRIQUE

Le chiffrement symétrique



### 8. Le chiffrement AES

AES est un algorithme de chiffrement par blocs, les données sont traitées par blocs de 128 bits pour le texte clair et le chiffré. La clef secrète a une longueur de 128 bits



### 9. La différence entre chiffrement bijectif et hachage

Le chiffrement bijectif est une forme de cryptographie qui permet de cryptographier et de dé cryptographier des données en utilisant des clés spécifiques. Il permet de transformer les données de manière que seules les personnes possédant la clé peuvent les décrypter. Le hachage ne peut pas être inversé et ne peut donc pas être utilisé pour décrypter des données. Il est principalement utilisé pour vérifier l'intégrité des données et pour empêcher les modifications non autorisées.

### 10. Les limites du hachage des mots de passe

La principale limite du hachage des mots de passe est qu'il ne fonctionne que dans un sens. Une fois qu'un mot de passe a été haché, il est impossible de le déchager pour retrouver le mot de passe original.

Une autre limite du hachage des mots de passe est que les mêmes mots de passe hachés peuvent produire des résultats identiques. Par exemple, le mot de passe « motdepasse123 » et « MotDePasse123 » produiront le même hachage. Cela signifie qu'un pirate peut essayer des mots de passe similaires et obtenir le même résultat.

## 11. Le salage des mots de passe

Le salage des mots de passe est quand le mot passe est un texte aléatoire qui est généré. Ducoup il est difficile de retrouver car si on le force brut il n'est pas dans un dictionnaire.

## 12. La stéganographie

La stéganographie est une technique utilisée pour cacher des messages, des informations ou des données dans des fichiers ou des images. Ces informations sont cachées de manière invisible et ne peuvent être décodées que par le destinataire. La stéganographie est parfois utilisée dans des situations où une communication confidentielle est nécessaire, mais elle est également utilisée pour partager des informations secrètes et des informations illégales

## II) L'outil Truecrypt

### 1. Expliquer à quoi sert l'outil truecrypt.

TrueCrypt est un logiciel de chiffrement open source qui permet aux utilisateurs de crypter leurs données et de les protéger contre les accès non autorisés.

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

Voici comment fonctionne TrueCrypt :

Premièrement TrueCrypt chiffre toutes les données stockées sur le disque dur, Il utilise une combinaison de chiffrement symétrique et asymétrique pour garantir la sécurité des données. Ensuite TrueCrypt crée des volumes chiffrés qui agissent comme des disques durs virtuels. Les utilisateurs peuvent créer ces volumes dans des fichiers, des partitions ou des disques entiers. Puis TrueCrypt utilise des méthodes d'authentification avancées, telles que les mots de passe, les fichiers-clés. Cela garantit que seuls les utilisateurs autorisés peuvent accéder aux données chiffrées.

Il peut aussi configurer pour monter automatiquement les volumes chiffrés au démarrage du système ou lorsqu'un utilisateur se connecte. Cela facilite l'accès aux données chiffrées.

Pour ce qui concerne les différences avec les autres outils classiques de chiffrement, TrueCrypt a été conçu pour être plus sûr. Contrairement à d'autres outils de chiffrement, TrueCrypt ne stocke jamais les mots de passe en clair, ce qui réduit les risques de vol de mots de passe. Enfin TrueCrypt prend en charge la dissimulation de volumes, ce qui signifie que même si un attaquant parvient à accéder au système, il ne pourra pas savoir que des volumes chiffrés sont présents.

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

L'utilisation de TrueCrypt peut être bénéfique pour une entreprise pour plusieurs raisons, notamment :

Protection des données sensibles : Les entreprises traitent souvent des données sensibles telles que des informations financières, des données clients et des secrets commerciaux. Le chiffrement avec TrueCrypt peut aider à protéger ces données contre les accès non autorisés.

Protection contre le vol : Les ordinateurs portables et les périphériques de stockage peuvent être volés ou perdus, ce qui peut entraîner une violation de la sécurité des données. Grâce au chiffrement les données pourront être récupérés.

Flexibilité : TrueCrypt peut être utilisé pour chiffrer des disques durs entiers, des partitions, des fichiers ou même des clés USB.

#### 4. Rechercher des solutions alternatives à Truecrypt

Comme solution alternatives il y a :


- VeraCrypt
- CipherShed
- AES Crypt
- BitLocker
- DiskCryptor
- BoxCryptor
- FileVault
- LUKS
- Symantec Drive Encryption

## II) Mise en œuvre d'une solution de chiffrement



VeraCrypt est un logiciel libre qui permet de chiffrer un répertoire sous Windows, Mac et GNU/Linux.

### 1. Créer un volume chiffré VeraCrypt




# VeraCrypt Files

Open source disk encryption with strong security for the Paranoid  
Brought to you by: [idrassi](#)

[Summary](#) [Files](#) [Reviews](#) [Support](#) [Source Code](#) [Forums](#) [Tickets](#) [Documentation](#) [FAQ](#) [Donate](#) [...](#)

[Download Latest Version](#)  
VeraCrypt Setup 1.25.9.exe (22.2 MB)

[Get Updates](#)



Home

Name	Modified	Size	Downloads / Week
VeraCrypt 1.25.9	2022-05-18		1,485
VeraCrypt Nightly Builds	2022-03-21		95
VeraCrypt 1.25.7	2022-01-08		21
VeraCrypt 1.25.4	2021-12-05		14
VeraCrypt 1.25	2021-11-29		19
VeraCrypt 1.24-Update7	2021-11-04		52
VeraCrypt 1.24-Update8	2020-12-12		5
VeraCrypt 1.24-Update4	2020-05-08		1
VeraCrypt 1.24-Update6	2020-03-11		11
VeraCrypt 1.24-Update5	2020-03-10		1
VeraCrypt 1.24-Update3	2019-12-24		0

Prenez la dernière version, celle qui est tout en haut pour l'installation puis prenez le lien et dans votre terminale mettez :

```
localhost:~# wget http://sourceforge.net/projects/veracrypt/files/Veracrypt201.0f-2/veracrypt-1.0f-2-setup.tar.bz2
```

Vous aurez donc ceci : (Screen fait à l'école ce qui explique le changement de couleur)

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

Installation options:

  1) Install veracrypt_1.0f-2_console_i386.tar.gz
  2) Extract package file veracrypt_1.0f-2_console_i386.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... _
```

Pour l'installer il faudra cliquer sur 1 puis vous aurez une licence à lire et à accepter.

Pour créer un volume chiffre vous devez taper cette commande :

```
localhost:~# veracrypt -t -c
```

Cette commande va nous lancer une suite d'option qu'on devra configurer.

```
localhost:~# veracrypt -t -c
Volume type:
1) normal
2) Hidden

Enter volume path: /opt/volume1

Enter volum size (sizeK/size[M]/sizeG): 200M

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)
Select [1] : 1
```



Dans un premier temps il nous demande si le Volume sera un volume caché ou un volume normal. Un volume caché est un volume chiffré caché dans un autre. Nous allons pour l'instant faire simple et saisir "1". On pourra ensuite saisir le chemin vers le volume à créer et aussi son nom.

Ensuite Il demande l'algorithmme de chiffrement que nous souhaitons utiliser. Pour rester simple nous allons garder la proposition par défaut qui est "AES" en saisissant "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
```

Ensuite, il nous sera demandé l'algorithmme de hashage à utiliser, ici aussi, nous allons garder l'algorithmme proposé qui est "SHA-512" et également le système de fichier. Si votre volume chiffré n'est destiné qu'à être utilisé sous Linux, vous pouvez sélectionner Ext3 ou Ext4. Si votre volume chiffré pourra être utilisé sous des machines Windows choisissez plutôt FAT ou NTFS.

Ensuite après avoir appuyez sur entrer vous devriez choisir un mot de passe qui pour un taux de sécurité élevé je vous conseille de suivre les conditions de la CNIL sur les mots de passe.

## 2. Monter un volume chiffré VeraCrypt

Maintenant que notre volume chiffré est généré, nous allons vouloir l'utiliser. Pour cela, il faut exactement le monter sur un dossier vide existant Nous allons ensuite monter notre volume chiffré dans ce répertoire /mnt avec la commande suivante :

```
localhost:~# veracrypt /opt/volume1 /mnt
```

Cette commande va préciser en premier notre volume chiffré puis notre dossier de destination sur lequel monter notre volume.

## 3. Démonter un volume chiffré VeraCrypt

Une fois que nous avons fini de travailler sur notre volume chiffré, nous pouvons le démonter du système de fichier actuel avec cette commande :

```
localhost:~# veracrypt -d volume 1
```

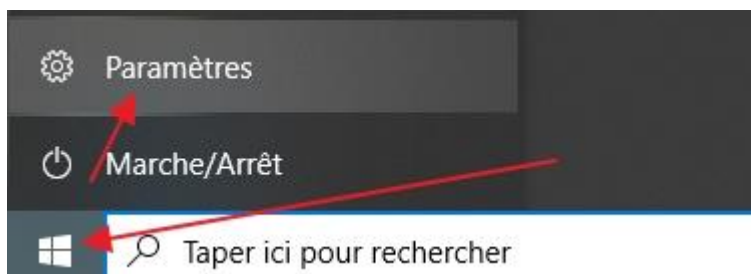
J'ai démonté le volume ducoup il devient impossible de savoir ce qu'il y a à l'intérieur.



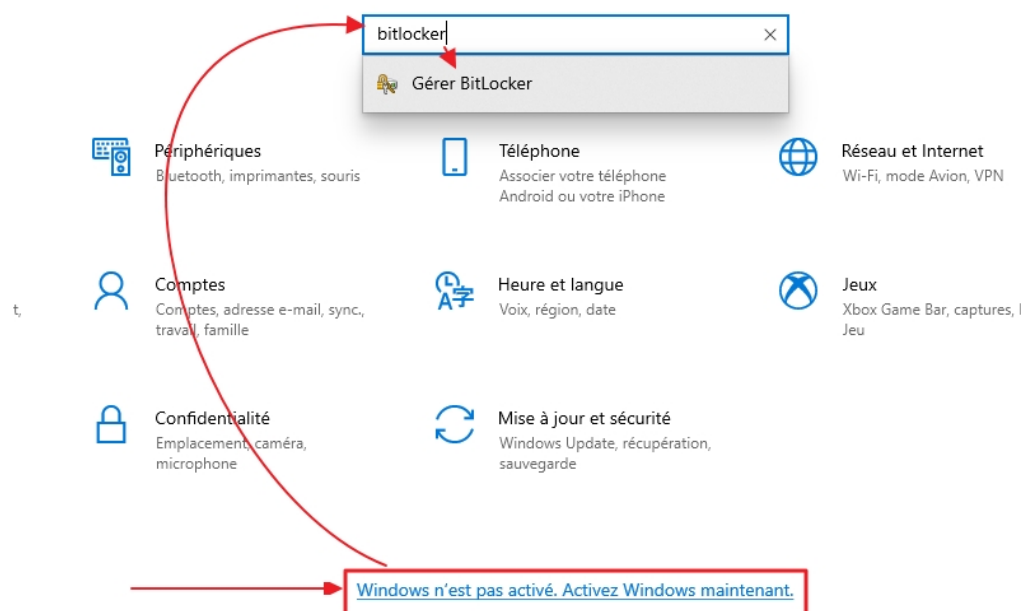
BitLocker peut être utilisé pour chiffrer l'intégralité du contenu d'un lecteur de données.

Dans un premier temps si vous avez un message d'erreur comme moi quand vous lancez BitLocker suivez ces étapes :

Aller dans les paramètres de Windows, en bas à gauche



Il se peut que votre Windows ne soit pas activé pour cela il faudra cliquer sur ceci :



## Chiffrement de lecteur BitLocker

← → ↕ ↗ > Panneau de configuration > Système et sécurité > Chiffrement de lecteur BitLocker

Page d'accueil du panneau de configuration

### Chiffrement de lecteur BitLocker

Protégez vos fichiers et dossiers contre l'accès non autorisé en protégeant vos lecteurs avec BitLocker.

#### Lecteur du système d'exploitation

C: BitLocker désactivé



Activer BitLocker



## Chiffrement de lecteur BitLocker (C:)

### Démarrage de BitLocker

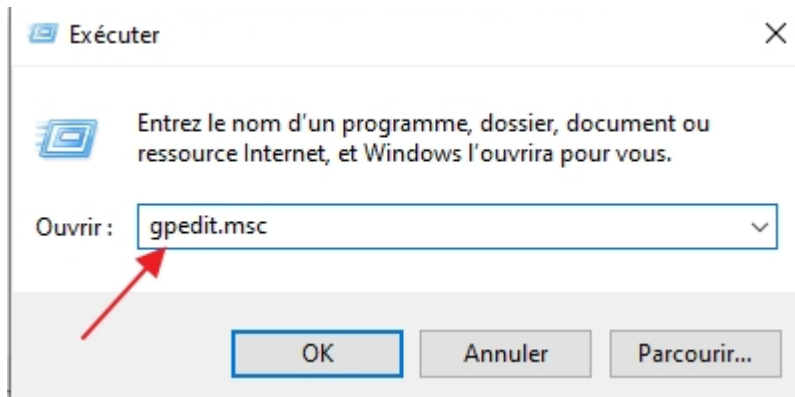


Ce périphérique ne peut pas utiliser un module de plateforme sécurisée (TPM). Votre administrateur doit définir l'option « Autoriser BitLocker sans un module de plateforme sécurisée compatible » dans la stratégie « Demander une authentification supplémentaire au démarrage » pour les volumes du système d'exploitation.

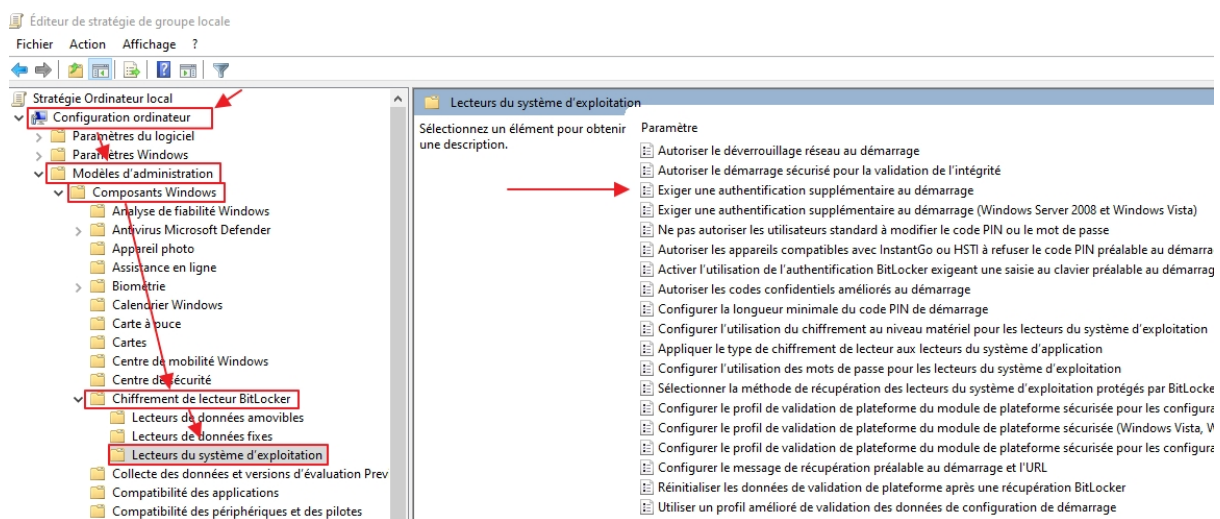
[Quelle est la configuration requise pour BitLocker ?](#)

Annuler

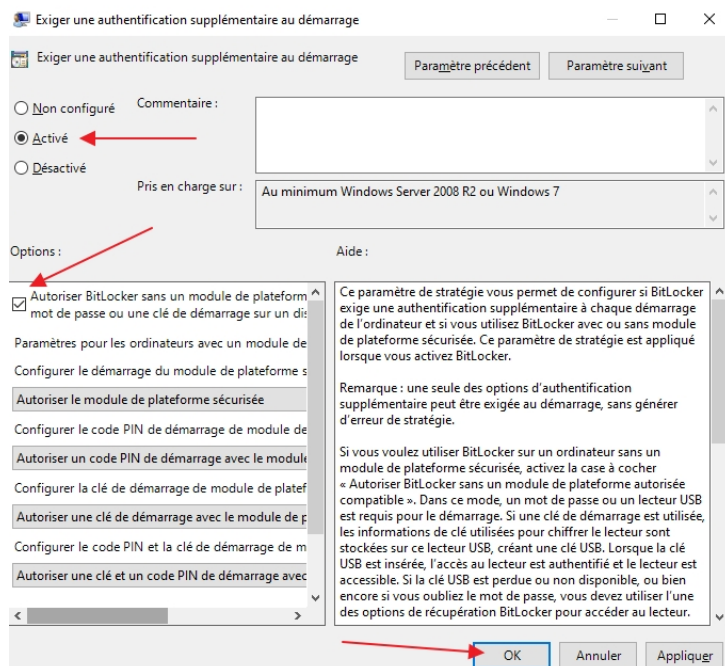
Si vous avez ce message d'erreur vous pouvez le modifier en quelques étapes, il faudra d'abord lancer une commande en cliquant en même temps sur Windows+r




Puis aller dans Configuration ordinateur > Modèles d'administration > Composants Windows > Chiffrement de lecteur BitLocker > Lecteurs du système d'exploitation



Puis il faudra cliquer sur activer la stratégie et autoriser Bitlocker sans un module de plateforme sécurisée compatible



Une fois fait BitLocker sera utilisable et vous pourrez faire l'installation du chiffrement

←  Chiffrement de lecteur BitLocker (C:)

### Installation du chiffrement de lecteur BitLocker


Lorsque vous activez BitLocker, votre ordinateur exécute les étapes suivantes :

Préparation de votre lecteur pour BitLocker  
Chiffrement du lecteur

[Quelle est la configuration requise pour BitLocker ?](#)

 **Suivant**

Annuler

←  Chiffrement de lecteur BitLocker (C:)

### Préparation de votre lecteur pour BitLocker

Un lecteur existant ou de l'espace libre non alloué sur le disque dur sera utilisé pour activer BitLocker.

⌵ Détails

Attention :

⚠ Il est conseillé de sauvegarder les fichiers et les données critiques avant de continuer.  
[Utiliser l'historique des fichiers pour effectuer une sauvegarde](#)

⚠ Ce processus peut être long, selon la taille et le contenu du lecteur.

**Suivant**

Annuler

## Installation du chiffrement de lecteur BitLocker

✗ Vous ne pourrez plus utiliser l'Environnement de récupération Windows (WinRE) à moins qu'il ne soit activé manuellement et déplacé vers le lecteur système.

Lorsque vous activez BitLocker, votre ordinateur exécute les étapes suivantes :

- ✓ Préparation de votre lecteur pour BitLocker
- Chiffrement du lecteur

[Quelle est la configuration requise pour BitLocker ?](#)

Suivant

Annuler

Cliquer sur « Suivant »

Ensuite il faudra choisir le mode de déverrouillage du lecteur

## Choisir le mode de déverrouillage de votre lecteur au démarrage

i Certains paramètres sont gérés par votre administrateur système.

Pour assurer la sécurité de vos données, vous pouvez indiquer à BitLocker d'exiger un mot de passe ou l'insertion d'un lecteur flash USB chaque fois que vous démarrez votre PC.

→ Insérer un lecteur flash USB

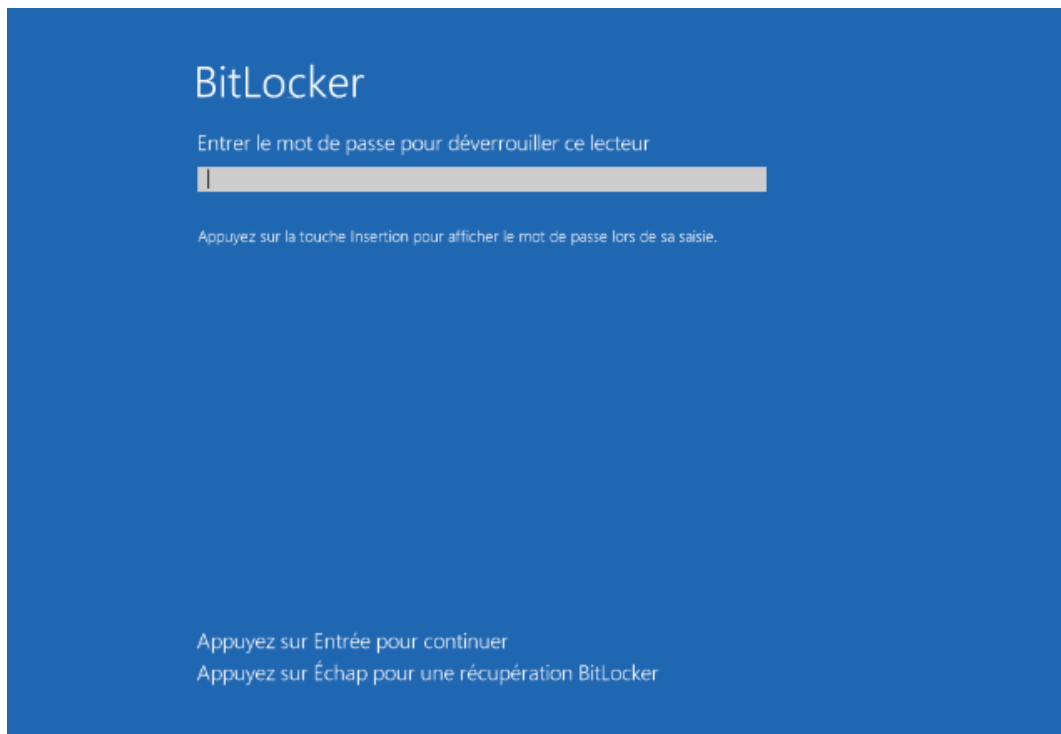
→ Entrer un mot de passe

Annuler

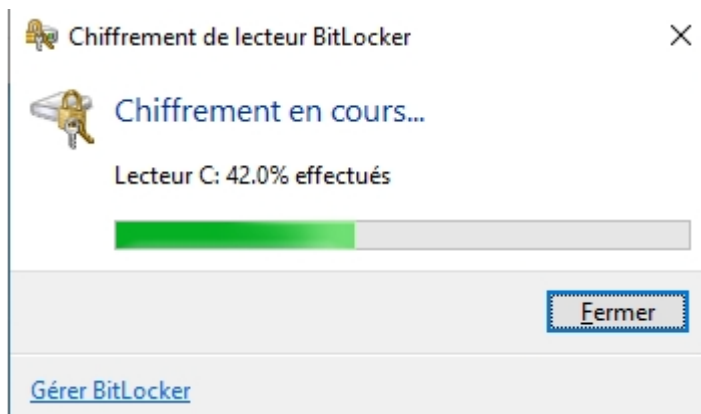
Je vous conseille de cliquer sur Entrer un mot de passe. C'est le mode de déverrouillage le plus simple et le plus sûr pour éviter les soucis liés au déverrouillage de votre disque dur.

Ensuite il faut choisir le mot de passe que vous devrez saisir à chaque démarrage de l'ordinateur pour déverrouiller votre disque dur. Comme ce mot de passe sera utilisé pour chiffrer tout le contenu de votre lecteur, choisissez un mot de passe qui respecte les conditions de la CNIL

Il faudra redémarrer votre ordinateur pour que cela s'affiche :



Le chiffrement du lecteur débutera ensuite automatiquement après le redémarrage de Windows.



Voilà maintenant vous savez maintenant utilisé BitLocker. Pour faire le déchiffrement de BitLocker c'est très simple vous devez :

- 1- Cliquer sur Windows et sélectionner « Paramètres de chiffrement d'appareil »
- 2- Cliquer sur « désactiver »