

TP-CHIFFREMENT



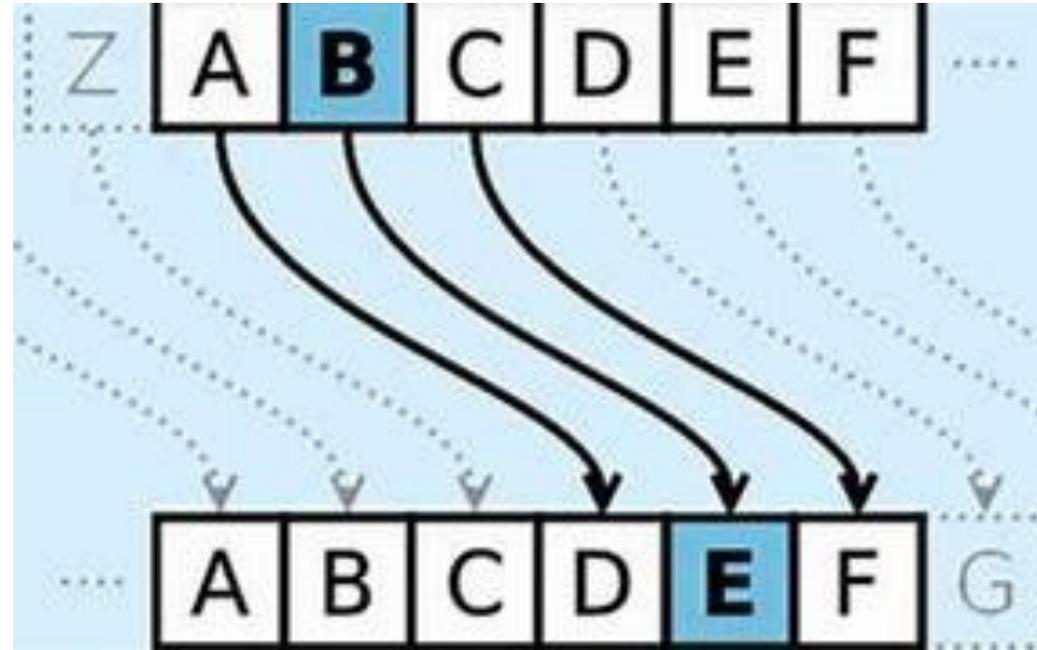
I) ETUDE ET RECHERCHE

- **Le Code César:**

il utilise le chiffrement avec l'alphabet pour se faire par exemple Par exemple avec un décalage de 3 vers la droite A est remplacé par D, B devient E et C devient F

- **Téléphone rouge :**

Le chiffrement a été mis en place par Gilbert Vernam en 1917, et est simplement un chiffre de Vigenère, mais où la clé est de la taille du message à envoyer, et où les lettres de cette clé sont choisies totalement aléatoirement. Si la clé ne sert qu'une fois (chiffre à usage unique), ce système est absolument sûr



■ Le Carré de Vigenère:

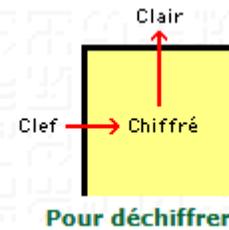
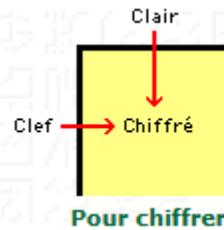
pour cette méthode nous allons utiliser le tableau ci-dessous. Dans cette table, l'alphabet est répété sur 26 lignes, avec un décalage à gauche de une lettre pour chaque nouvelle rangée.

Vigenère (chiffré = clair + clef)

pour se faire il nous faut (clair, chiffré) de même caractère .

- il existe plusieurs méthode de chiffrement différente comme par exemple (Beaufort, Variante à l'allemande du chiffre de Beaufort, ect)

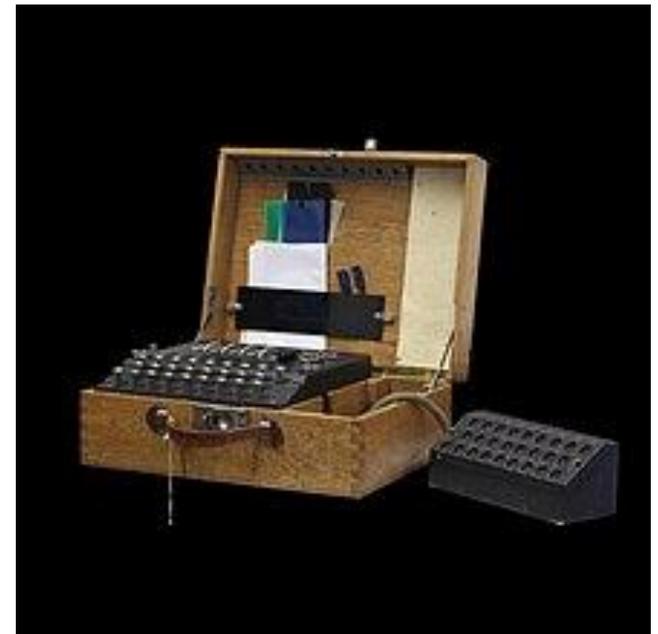
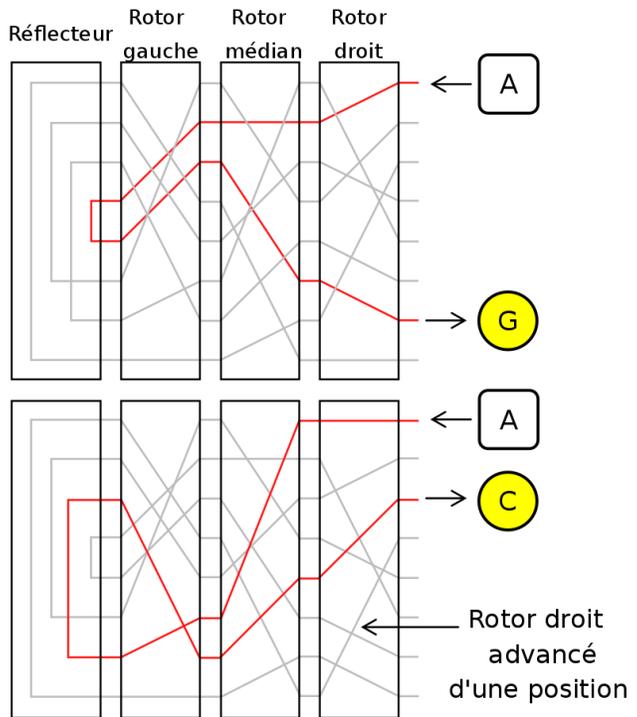
	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z
A	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z
B	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A
C	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B
D	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C
E	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T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



clair MONMESSAGE
 clef MACLEFMACL
 chiffré YOPXIXEAIIP

Exemple

- La machine « Enigma »:le chiffrement et effectuer avec le courant qui passe à travers un assemblage de rotors, puis par réflecteur et enfin à nouveau par les rotors dans le schéma la lettre A est chiffrée de manière différente lorsqu'on appuie deux fois consécutivement sur la même touche



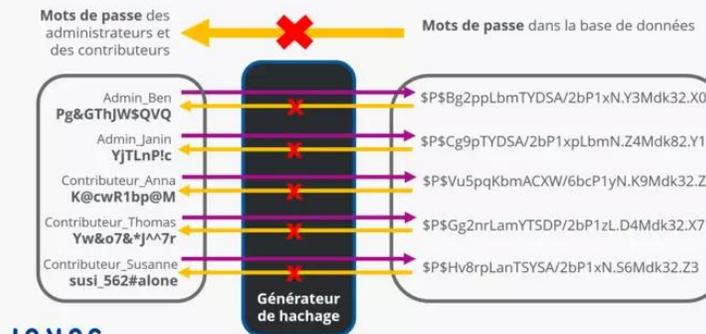
■ Hachage:

une fonction de hachage prend des données (comme un mot de passe) et les transforme en une valeur de hachage qui est irréversible en effet on ne peut retrouver les données d'origine à partir de celui ci

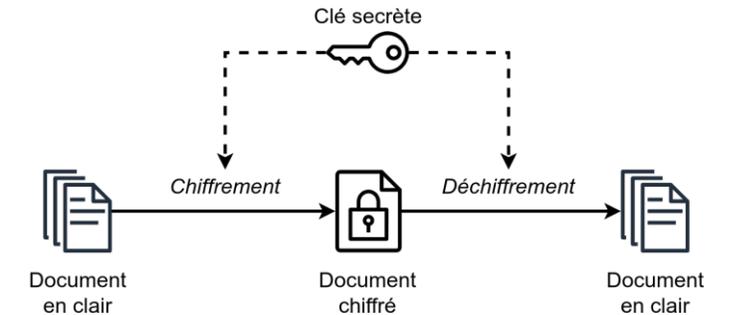
■ le chiffrement a clé symétrique:

cette méthode de chiffrement utilise la même clé pour chiffrer les données mais aussi déchiffrer les données.

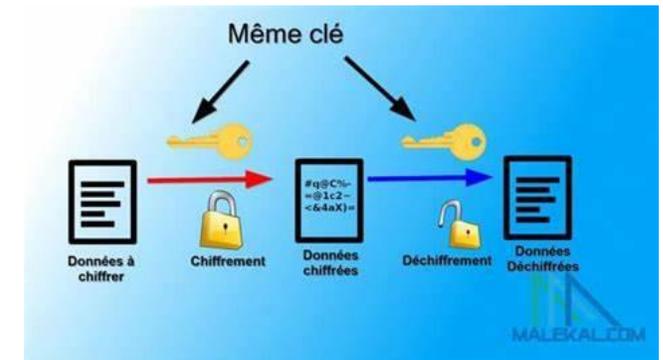
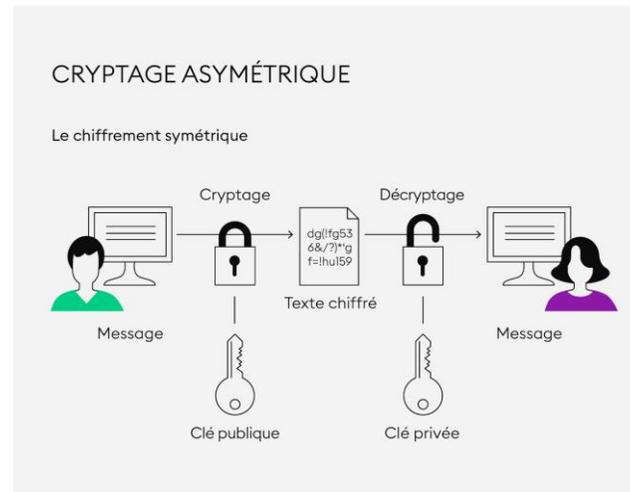
Fonction de hachage: chiffrement du mot de passe



IONOS



- **le chiffrement à clé asymétrique:** contrairement au chiffrement à clé symétrique, celui-ci utilise plusieurs clés, en effet il utilise une clé publique qui aura le rôle de chiffrer les données et une clé privée qui aura pour rôle de déchiffrer les données
- le chiffrement AES: L'algorithme AES prend des données et une clé secrète, puis les mélange de manière complexe pour les rendre illisibles. Cette manipulation est répétée plusieurs fois pour augmenter la sécurité. Pour déchiffrer les données, on utilise la même clé pour inverser le processus et retrouver les données d'origine. la sécurité des données dépend de la longueur de la clé qui peut varier entre 128 à 256 bits.





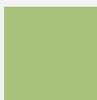
La différence entre chiffrement bijectif et hachage: la différence réside dans le déchiffrement en effet le chiffrement bijectif peut déchiffrer les données chiffrées pour retrouver les données originales contrairement au hachage



Les limites du hachage des mots de passe: il présente des limites car les attaques par brute force et par dictionnaire peuvent potentiellement retrouver les mots de passe à partir de leurs valeurs de hachage



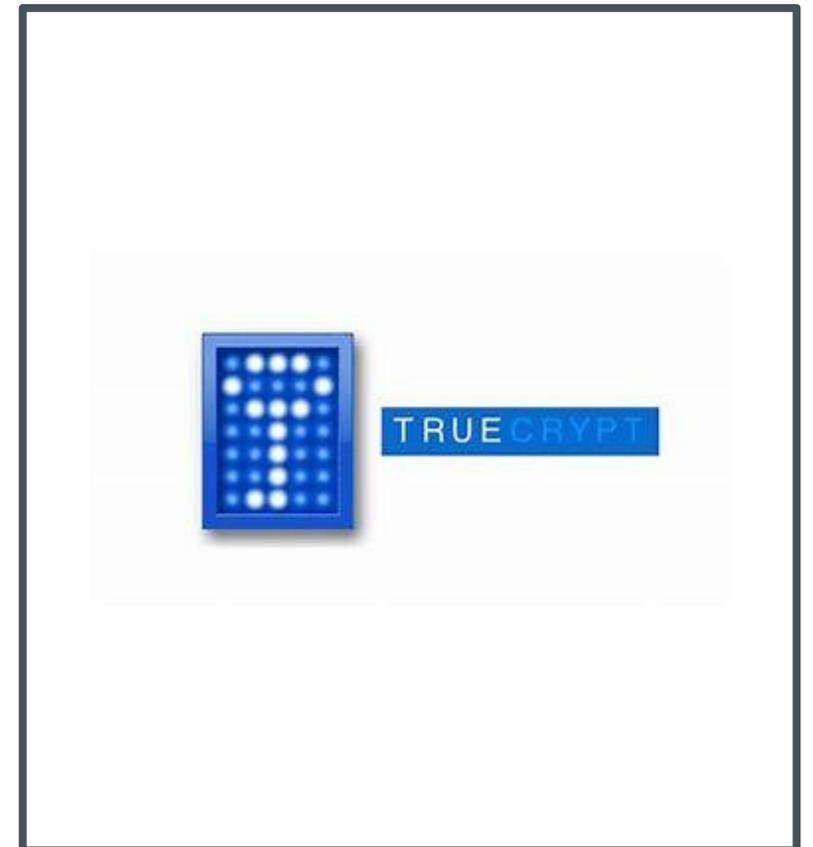
Le salage des mots de passe: le salage consiste à ajouter un fragment de données aléatoires au mot de passe avant de le soumettre à l'algorithme de hachage (par exemple le mot de passe d'origine est romain et avec le sel cela peut nous donner romain2@4Sep#)



La stéganographie: cela consiste à cacher des données au sein d'un support existant (image, vidéo, fichiers audio ect) de manière à ce qu'elles ne soient pas visibles. par exemple il est possible de dissimuler des données afin de cacher un outil malveillant ou encore envoyer des instructions à des serveurs de commande pour les contrôler.

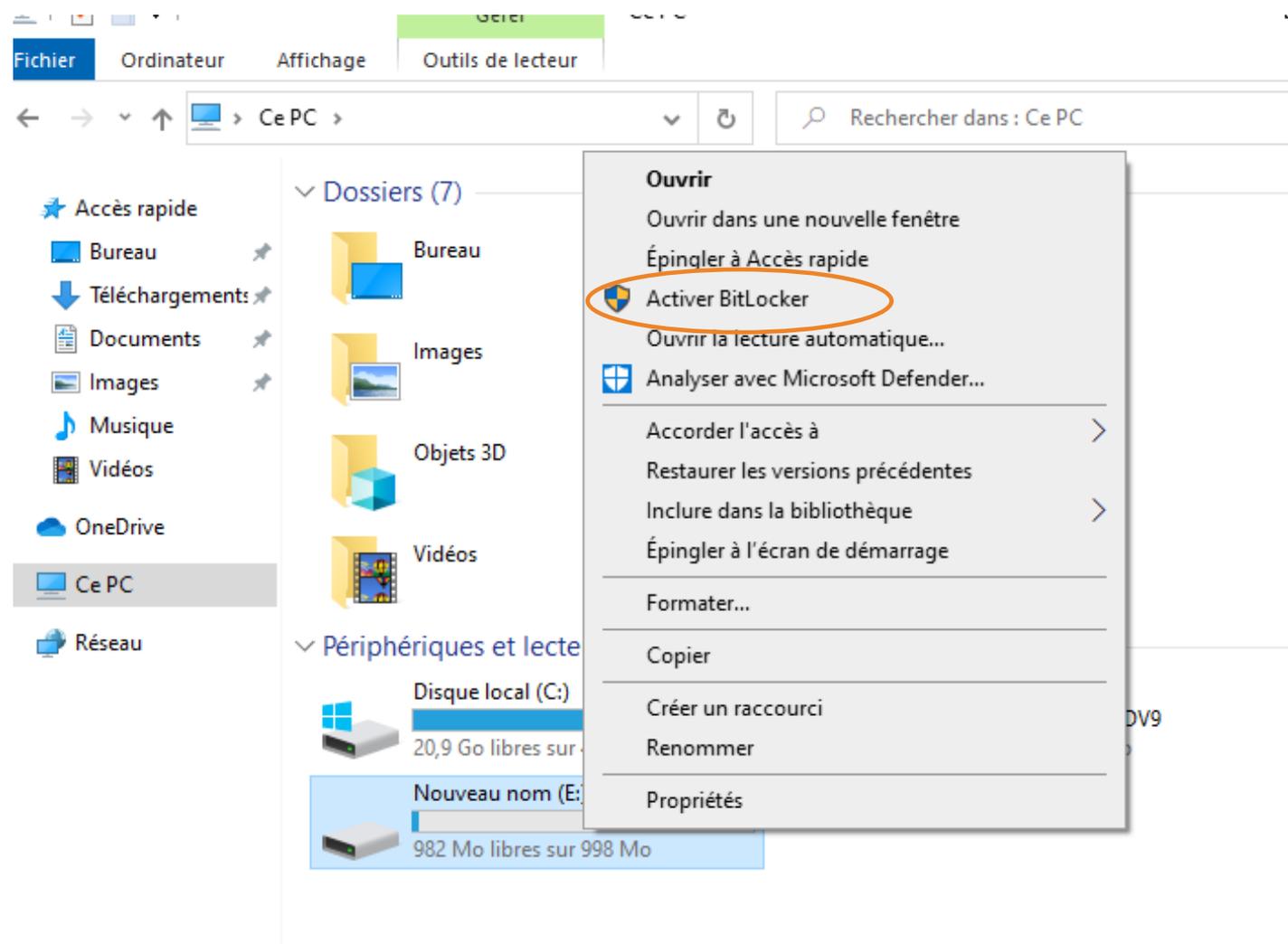
II) L'OUTIL TRUECRYPT

- c'est un outil de chiffrement open source qui permet de protéger nos données. c'est un logiciel qui se démarque des autres applications "classiques", en effet il possède une variété de chiffrement (AES, Serpent, et Twofish). Il est capable de cacher un volume chiffré dans un autre volume chiffré, L'idée est que si quelqu'un découvre le premier volume chiffré, il ne pourra pas prouver qu'il existe un deuxième volume caché à l'intérieur sans le mot de passe approprié.
- comme solutions alternative nous pouvons utiliser bitlocker, qui est aussi un crypteur de disque complète sous windows ou on a aussi North Locker, qui est développé par l'équipe derrière NordVPN



BITLOCKER

- nous allons effectuer le chiffrement sur une nouvelle partition.
- Pour commencer nous allons nous diriger dans l'explorateur de fichiers afin de nous rendre sur la partition, ensuite nous effectuerons un clique droit sur la partition, et nous allons aller sur activer bitlocker



← Chiffrement de lecteur BitLocker (E:) ×

Choisissez le mode de déverrouillage de ce lecteur.

Utiliser un mot de passe pour déverrouiller le lecteur
Les mots de passe doivent contenir des lettres majuscules et minuscules, des chiffres, des espaces et des symboles.

Entrer votre mot de passe

Entrer à nouveau votre mot de passe

Utiliser ma carte à puce pour déverrouiller le lecteur
Vous devrez insérer votre carte à puce. Son code PIN vous sera demandé pour déverrouiller le lecteur.

Suivant Annuler

← Chiffrement de lecteur BitLocker (E:) ×

Comment voulez-vous sauvegarder votre clé de récupération ?

❌ Impossible d'enregistrer votre clé de récupération sur cet emplacement. Sélectionnez un autre emplacement.

Si vous oubliez votre mot de passe ou si vous perdez votre carte à puce, vous pouvez utiliser votre clé de récupération pour accéder à votre lecteur.

→ Enregistrer sur votre compte Microsoft

→ Enregistrer sur un disque mémoire flash USB

→ Enregistrer dans un fichier

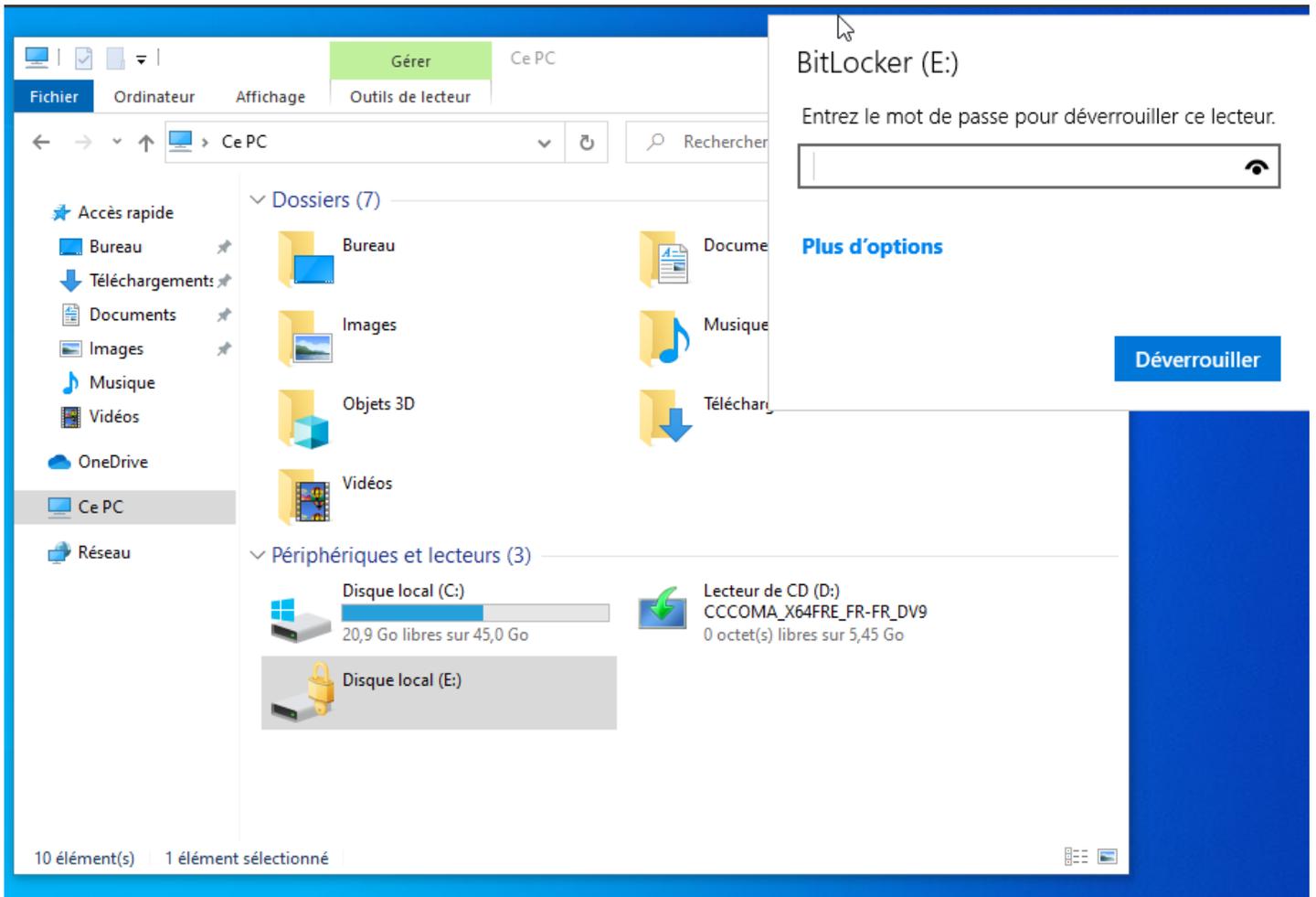
→ Imprimer la clé de récupération

[Comment retrouver ma clé de récupération ultérieurement ?](#)

Suivant Annuler

- Ensuite, nous allons définir un mot de passe qui doit comporter des majuscules, minuscules, des chiffres ect
- Ensuite nous allons sauvegarder la cle dans un fichier

- Comme nous pouvons le voir la partition est chiffré



DÉCHIFFREMENT

POUR SE FAIRE NOUS
ALLONS NOUS RENDRE
DANS GÉRÉ BITLOCKER,
AFIN DE LE DÉSACTIVER.

The screenshot shows the Windows BitLocker management console. The main window is titled "Chiffrement de lecteur BitLocker". It displays the status of the operating system drive (C:) as "désactivé" and the fixed data drive (E:) as "activé (Verrouillé)". A dialog box titled "Chiffrement de lecteur BitLocker" is open, showing the "Désactiver BitLocker" option. The dialog text reads: "Votre lecteur va être déchiffré. Cette opération peut durer longtemps, mais vous pourrez utiliser votre ordinateur pendant le processus de déchiffrement." Below the dialog, there are several options: "Sauvegarder votre clé de récupération", "Modifier le mot de passe", "Supprimer le mot de passe", "Ajouter une carte à puce", "Activer le déverrouillage automatique", and "Désactiver BitLocker" (which is circled in red).

The screenshot shows a BitLocker recovery key prompt for drive E: (BitLocker (E:)). The prompt asks for the 48-digit recovery key to unlock the drive. The key ID is C36EF530. The recovery key is displayed in a text box: 059334-117788-287276-299519-000891-328999-616319-620081. A blue "Déverrouiller" button is visible at the bottom right.

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

Enter volume path: /dev/sdb

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

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

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

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

Enter password:
WARNING: Short passwords are easy to crack using brute force techniques!

We recommend choosing a password consisting of more than 20 characters. Are you sure you want to use
a short password? (y=Yes/n=No) [No]: yes

Re-enter password:

Enter keyfile path [none]:

Please type at least 320 randomly chosen characters and then press Enter:
Characters remaining: 24

reg
ref
gvre

Done: 100,000% Speed: 47 MB/s Left: 0 s
```

```
oot@debian:~# veracrypt -d /dev/sdb
```

VERACRYPT

- Après avoir installé veracrypt sous linux, nous allons créer un volume chiffrer avec la commande `veracrypt -t -c` ce qui va nous lancer une suite d'option qui vont nous permettre de le configurer
- Ensuite nous Allons définir un mot de passe
- Avec la commande `veracrypt -d /chemin d'accès` nous allons démonter le volume chiffré VeraCrypt