Romain Lheureux

TP-CHIFFREMENT

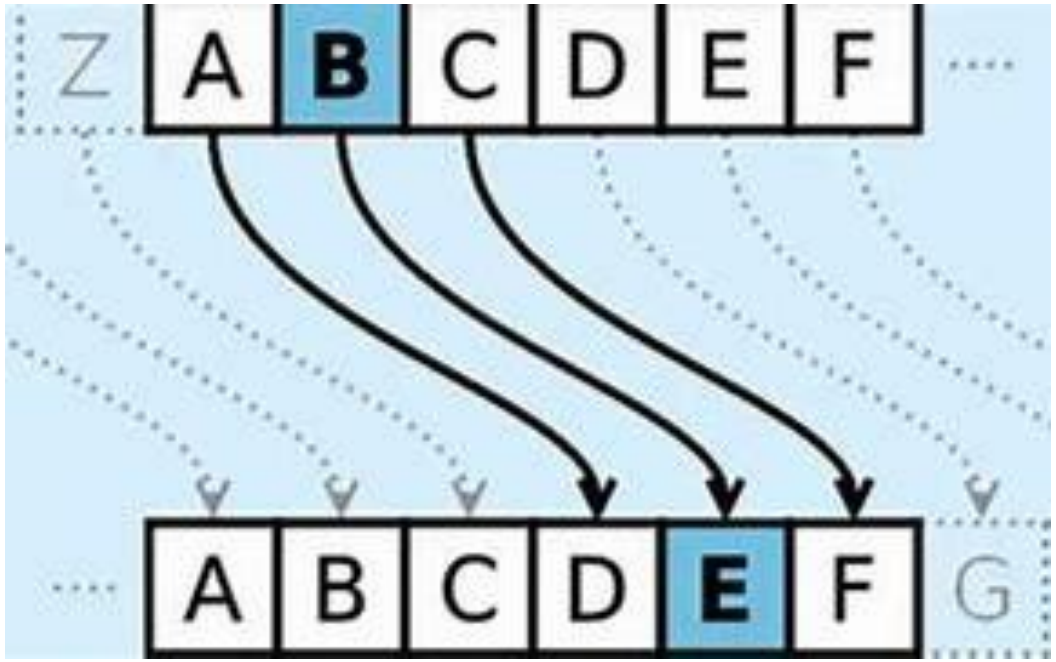
I) ETUDE ET RECHERCHE

- **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 vigeneère, mais où la clé est de la taille du message à envoyer, et où les lettres de cette clé sont choisis totalement aléatoirement. Si la clé ne sert qu'une fois (chiffre à usage unique), ce système est absolument sûr



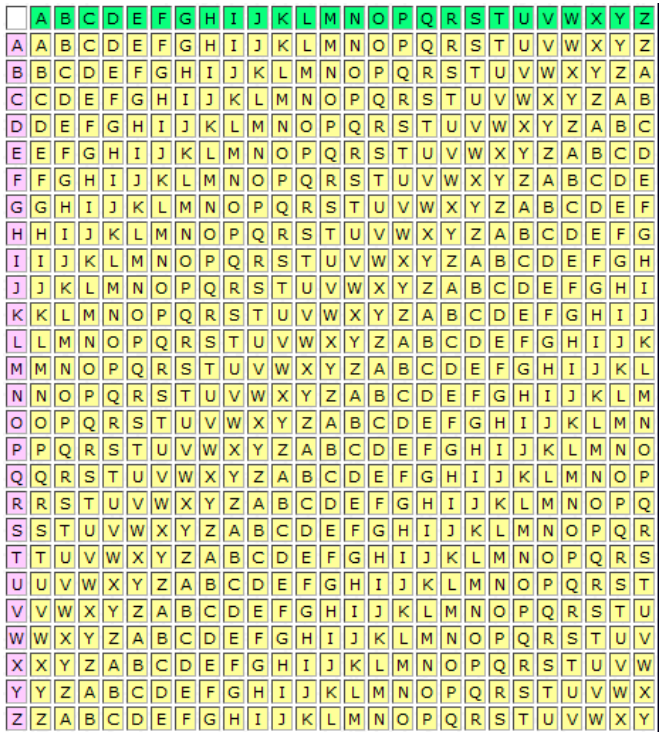
- **Le Carré de Vigenère:**

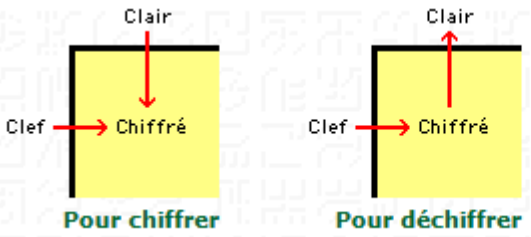
pour cette méthode nous allons utiliser le tableau ci-dessous. Dans cette table, l'alphabet est répété sur 26 lignes, avec un décalage à gauche de une lettre pour chaque nouvelle rangée.

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)

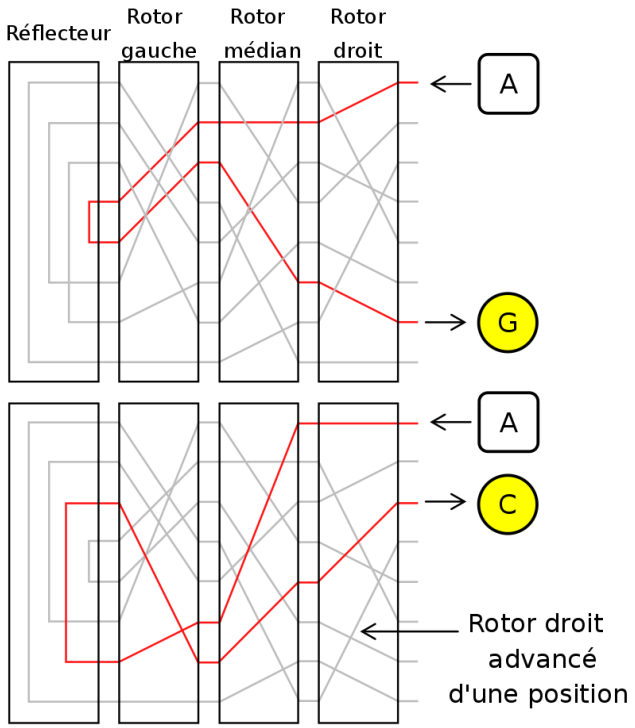




clair	MONMESSAGE
clef	MACLEFMACL
chiffré	YOPXIXEAIP

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

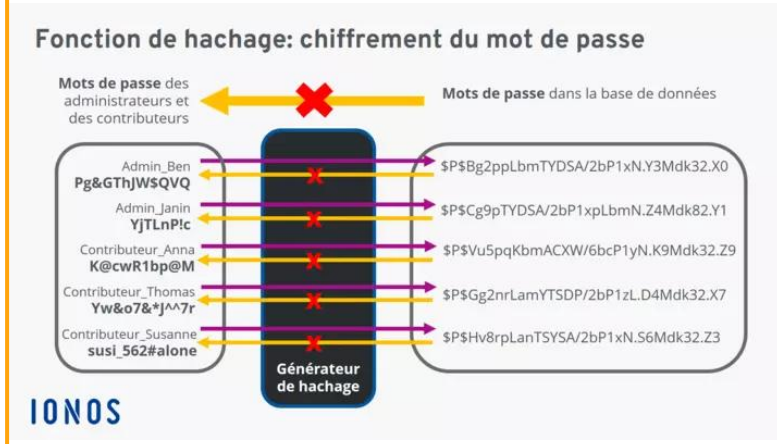


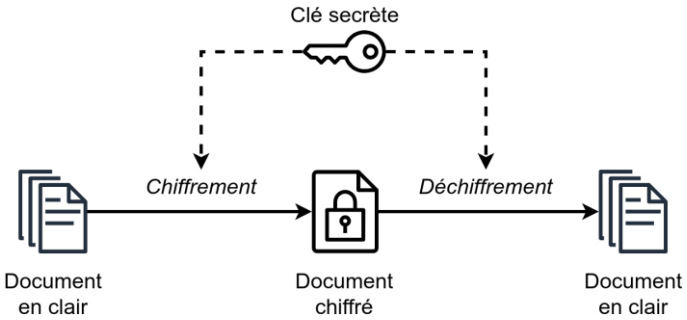
- **Hachage:**

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 a partir de celui ci

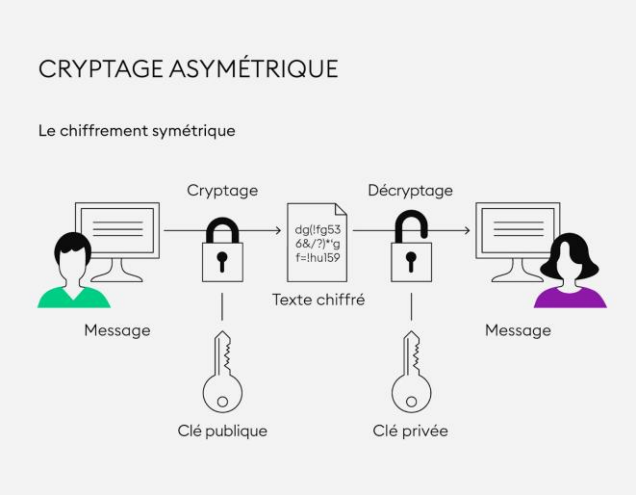
- **le chiffrement a clé symétrique:**

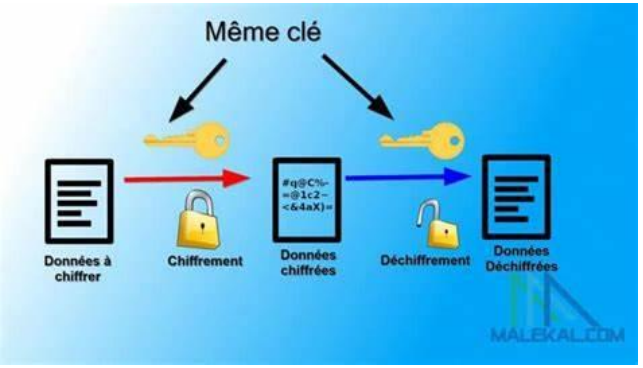
cette méthode de chiffrement utilise la même clé pour chiffrer les données mais aussi déchiffrer les données.





- **le chiffrement à clé asymétrique:** contrairement au chiffrement a 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 résident dans le déchiffrement en effet le chiffrement bijectif peut déchiffrer les données chiffrées pour retrouver les données originales contrairement au hachage

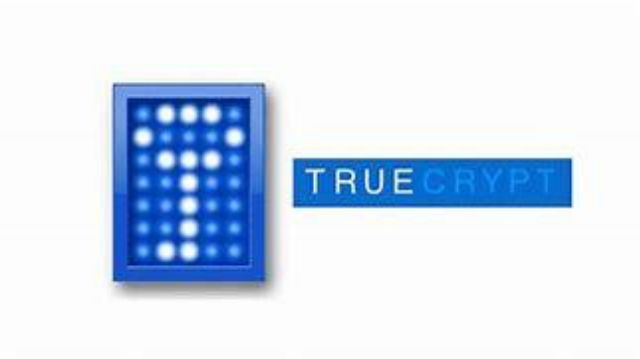
Les limites du hachage des mots de passe: il présente des limites car les attaques par brute force et par dictionnaire peuvent potentiellement retrouver les mots de passe a partir de leurs valeurs de hachage

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.

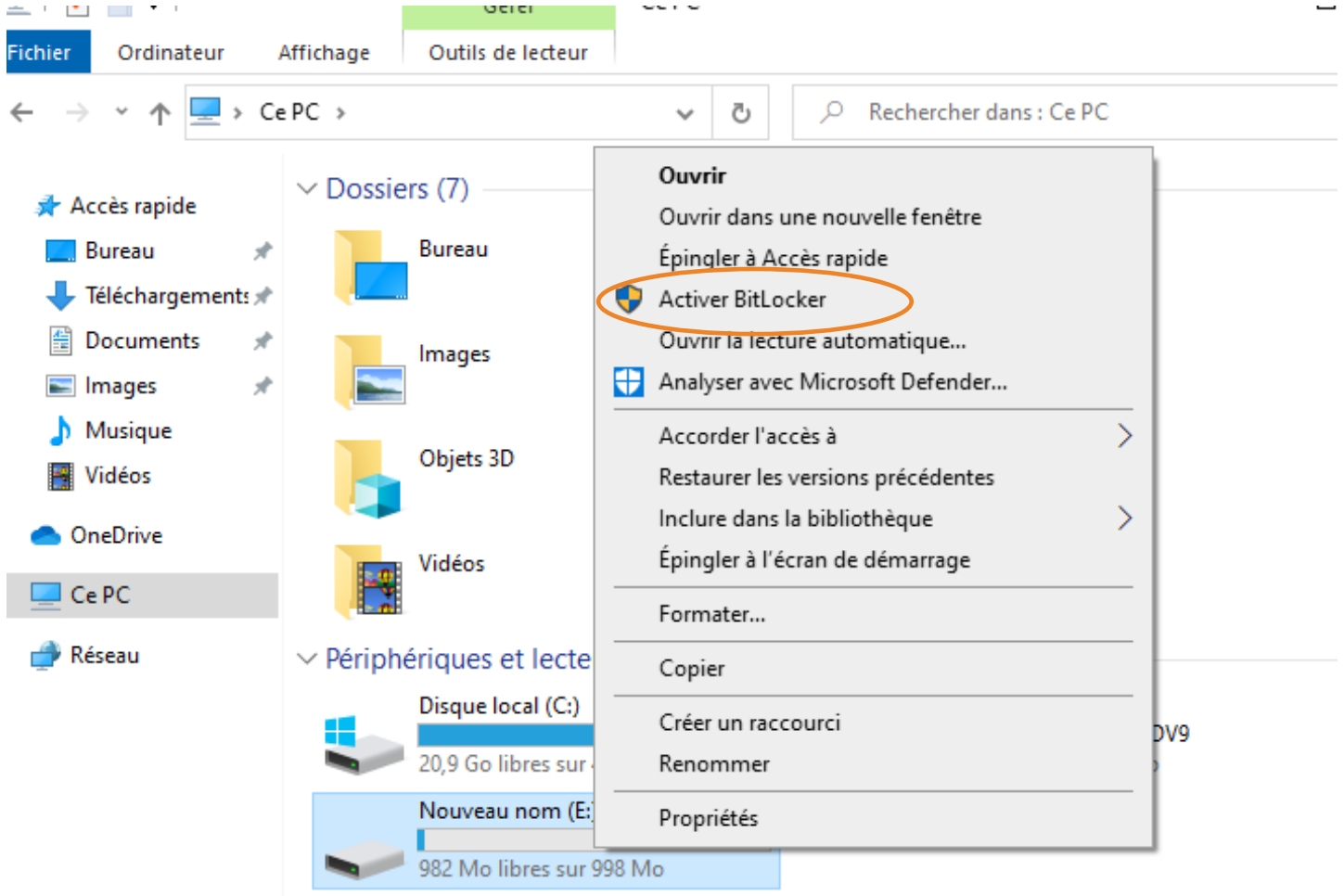
II) L’OUTIL TRUECRYT

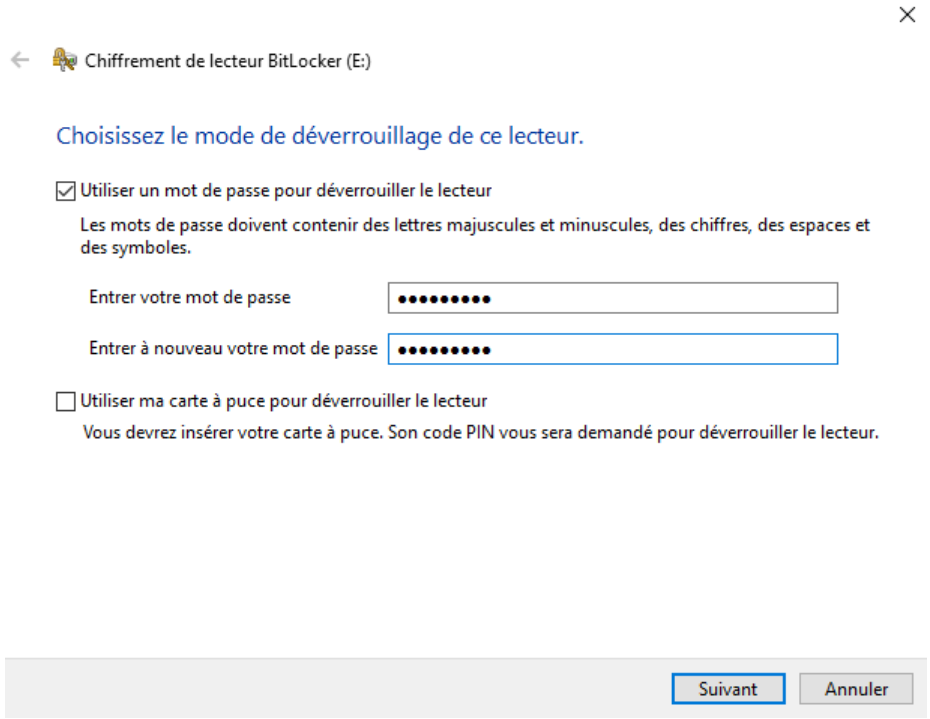
- c’est un outil de chiffrement open source qui permet de protéger nos données. c’est un logiciel qui se démarque des autres applications “classiques”, en effet il possède une variété de chiffrement (AES, Serpent, et Twofish). Il est capable de cacher un volume chiffré dans un autre volume chiffré, L'idée 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

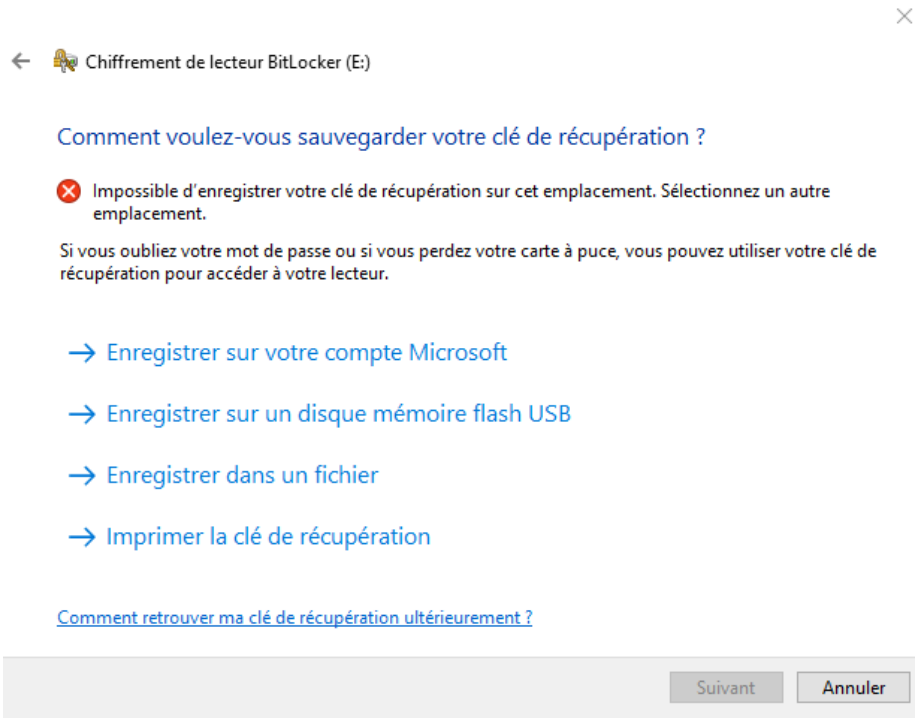


BITLOCKER

- 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 surla partition, et nous allons aller sur activer bitlocker

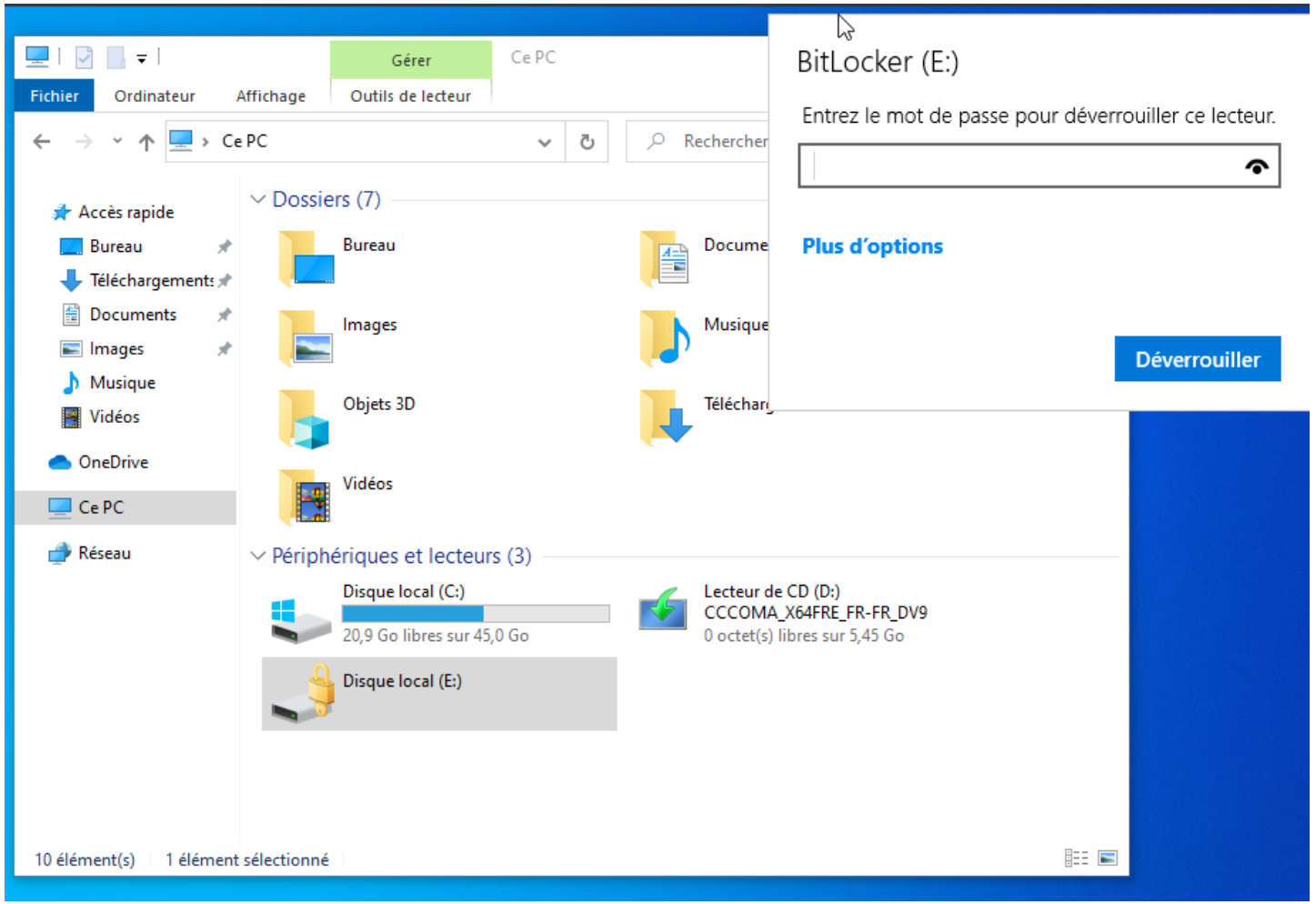






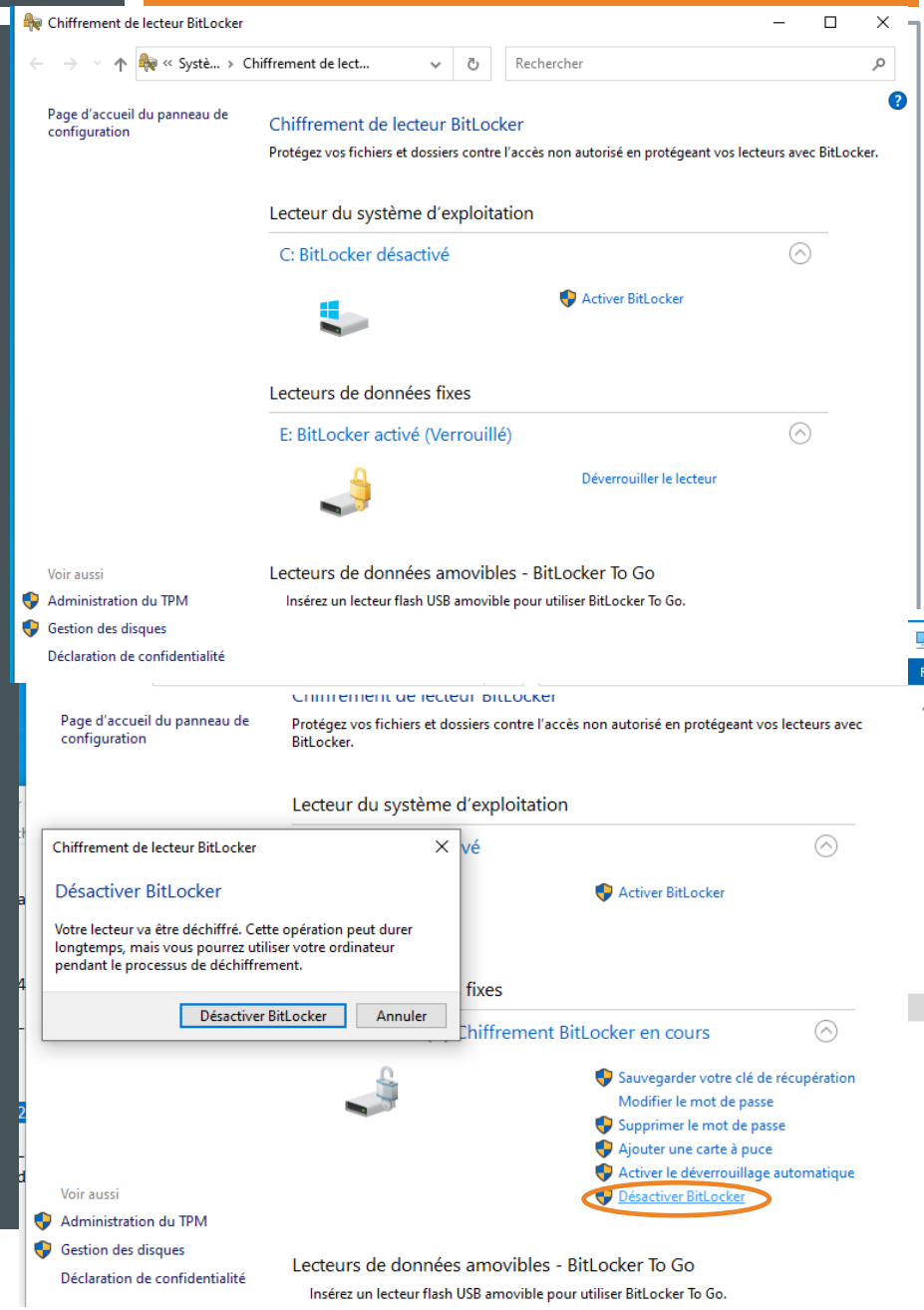
- Ensuite, nous allons définir un mot de passe qui doit comporter des majuscules, minuscules, des chiffres ect
- Ensuite nous allons sauvegarder la cle dans un fichier

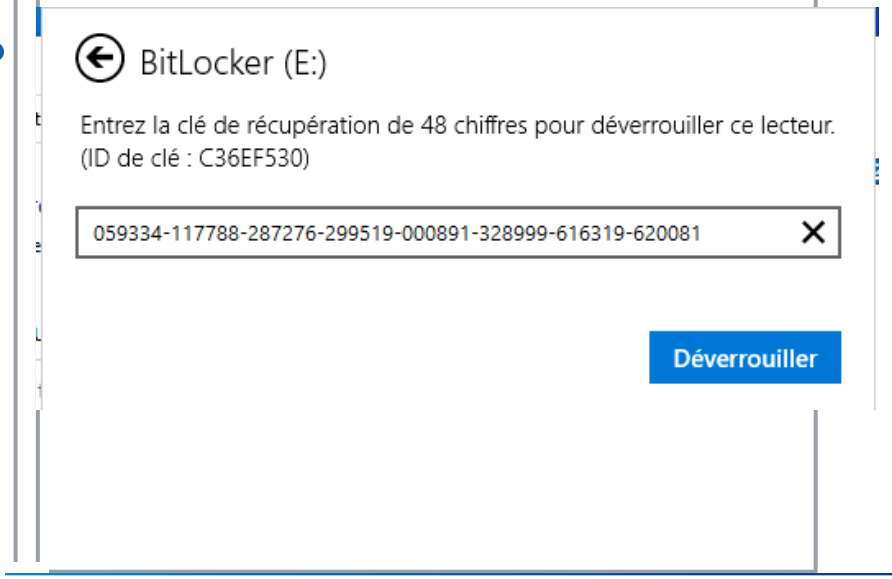
- Comme nous pouvons le voir la partition est chiffré

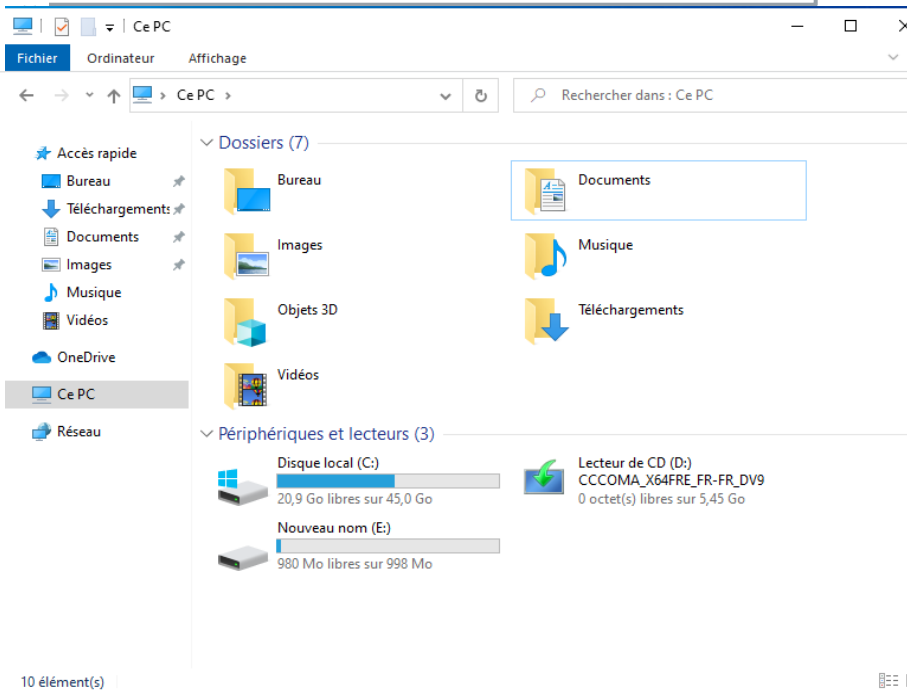


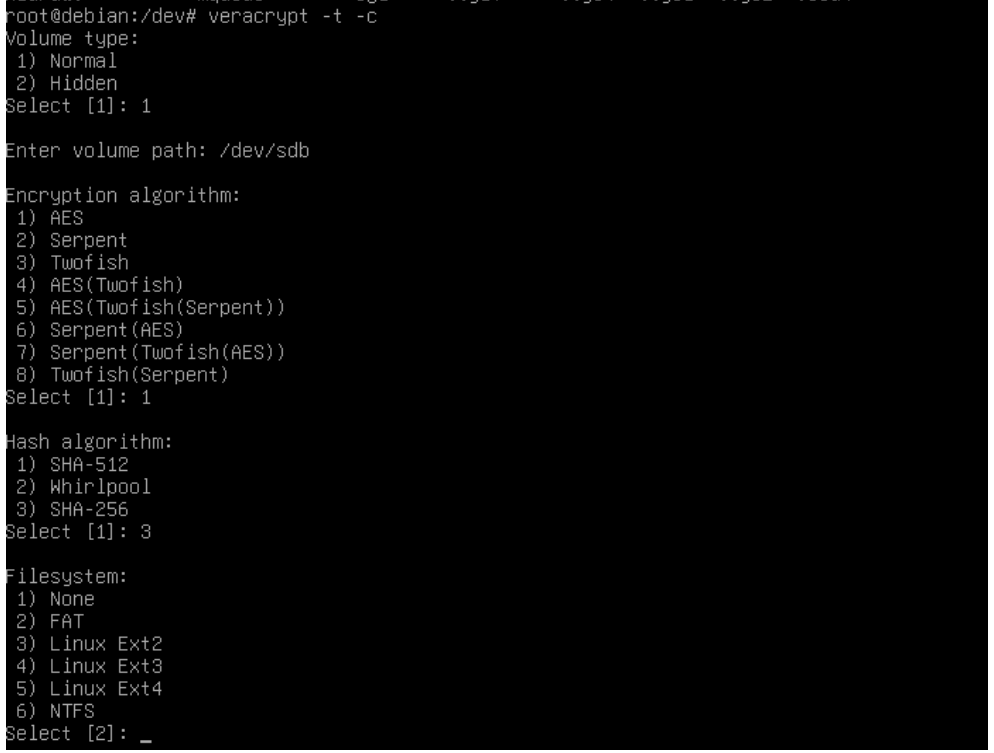
DÉCHIFFREMENT

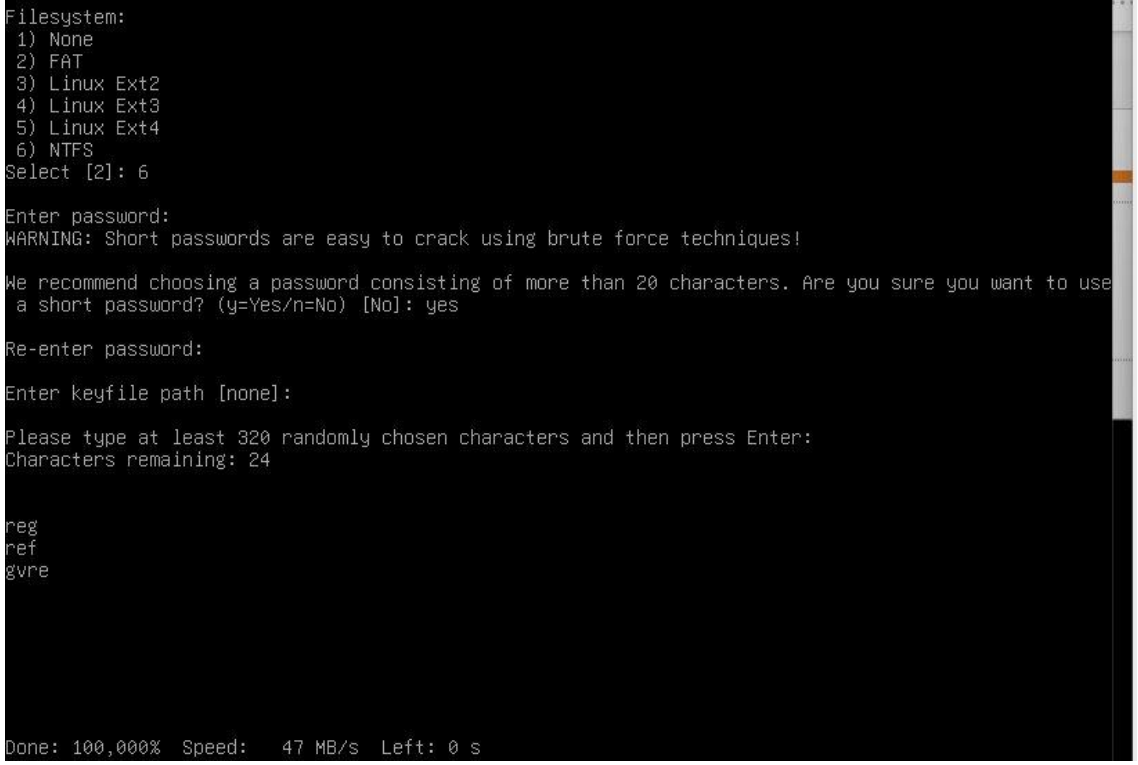
POUR SE FAIRE NOUS ALLONS NOUS RENDRE DANS GÉRÉ BITLOCKER, AFIN DE LE DÉSACTIVER.











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 definir un mot de passe
- Avec la commande veracrypt –d /chemin d'accès nous allons démonter le volume chiffré VeraCrypt