ZIZA KANGUE

Sarah Géniva

BTS 1 SIO

# TP-Chiffrement

## I) Etude et Recherche

### Le Code César

Le code césar ou chiffrement césar est une méthode de chiffrement très simple utilisé par jules césar dans ses correspondances secrètes.

Le texte chiffré s'obtient en remplaçant chaque lettre du texte claire original par une lettre à une distance fixe, toujours du même côté dans l'ordre de l'alphabet.

Exemple1 : clair : ABCDEFGHIJKLMNOPQRSTUVWXYZ

Chiffré : DEFGHIJKLMNOPQRSTUVWXYZABC

Exemple2 : clair : SAINT LUC

Chiffré : VDLQW OXF

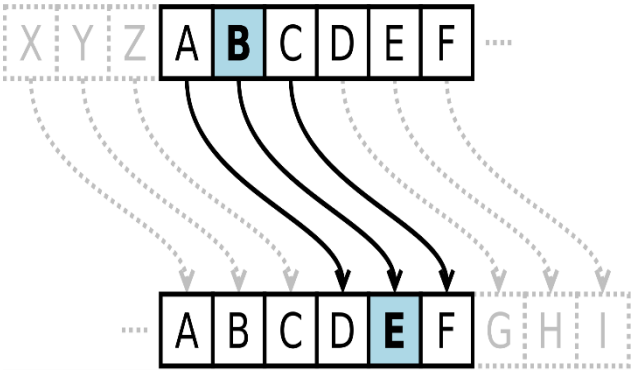
NB : longueur du décalage 3, constitue la *clé* du chiffrement

On peut coder un message à l'aide du code César avec n'importe quelle clé n, où n est un entier naturel.

Exemple3 : chiffrement avec une clé n=7

Clair : SAINT LUC

Chiffré : YGOTZ RAI




### Le Carré de Vigenère

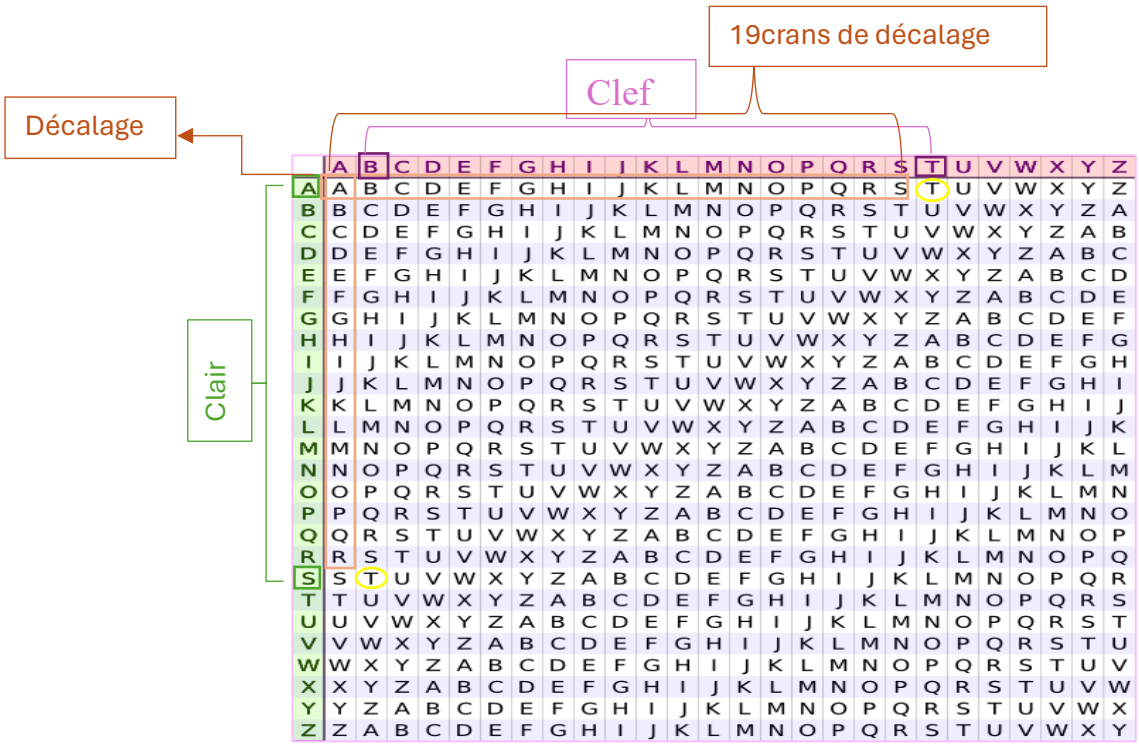
C'est un système de chiffrement par substitution poly alphabétique dans lequel une même lettre du message en clair peut, suivant sa position, être remplacée par des lettre différentes.

Sa force réside dans l'utilisation non pas d'un, mais de 26 alphabets décalés pour chiffrer un message.

Ce chiffrement utilise une **clef** qui définit le décalage pour chaque lettre du message (A : décalage de 0 cran, B: 1 cran, C: 2 crans, ..., Z: 25 crans).

Exemple

| Clair | S | A | I | N | T | L | U | C |
|---|---|---|---|---|---|---|---|---|
| Clef | B | T | S | S | I | O | B | T |
| Décalage | 1 | 19 | 18 | 18 | 9 | 14 | 1 | 19 |
| Chiffré | T | T | A | F | B | Z | V | V |



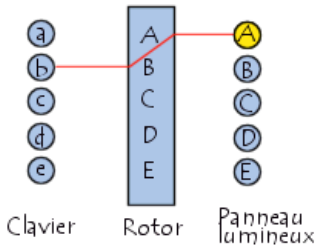

## La machine « Enigma »

**Enigma** est une machine électromécanique portative servant au chiffrement et au déchiffrement de l'information.

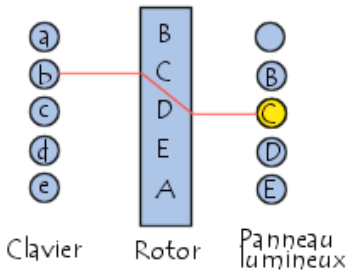
Elle chiffre les informations en faisant passer un courant électrique à travers une série de composants. Ce courant est transmis en pressant une lettre sur le clavier ; il traverse un réseau complexe de fils puis allume une lampe qui indique la lettre chiffrée.

A chaque pression d'une touche du clavier, une lettre du panneau lumineux s'illuminait. Il y avait ainsi 3 roues de codage, appelées « Brouilleur Rotor », qui reliaient le clavier au panneau lumineux.

Par exemple, avec un seul rotor, lorsque l'on appuie sur *B* le courant passe par le rotor et allume *A* sur le panneau lumineux :




Pour complexifier la machine, à chaque pression sur une touche, le rotor tourne d'un cran. Après la première pression on obtient donc :




**Le téléphone rouge**

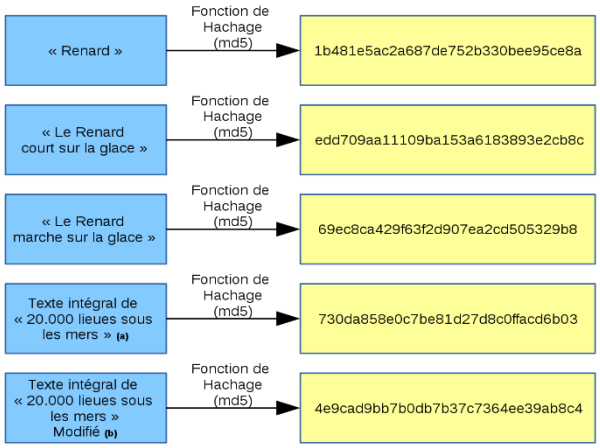
Le **téléphone rouge s**ymbole emblématique de la guerre froide est une ligne de communication directe établie le 30 août 1963 entre les États-Unis et l'Union soviétique à la suite d'un accord signé entre les deux pays et entré en vigueur le 20 juin 1963.

Cette dénomination de « téléphone rouge » est en réalité un raccourci lexical repris et popularisé par les médias occidentaux, la ligne étant au départ une ligne de téléscripteur, sa supposée couleur rouge symbolisant simplement le fait qu'il s'agissait d'une ligne d'urgence.

## Le hachage

Le hachage est une fonction ou un algorithme mathématique qui produit un résultat unique appelé empreinte ou signature (un hash). Le hachage est un outil indispensable dans tous les procédés cryptographiques. Il est apparu en informatique au cours des années 1950/1960 dans le but de réduire la taille des fichiers et désormais fortement utilisé dans la blockchain

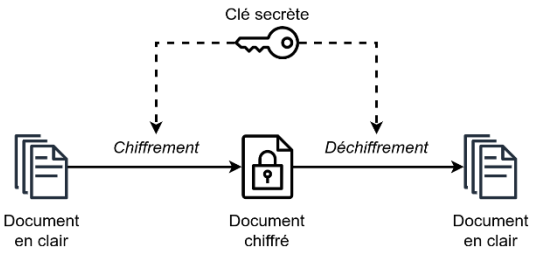
Son objectif principal est de permettre de ne pas stocker les mots de passe en clair dans la base mais uniquement de stocker une empreinte de ces derniers




## Le chiffrement à clé symétrique

La cryptographie symétrique, également dite à clé secrète (par opposition à la cryptographie asymétrique), est la plus ancienne forme de chiffrement. Elle permet à la fois de chiffrer et de déchiffrer des messages à l'aide d'un même mot clé.

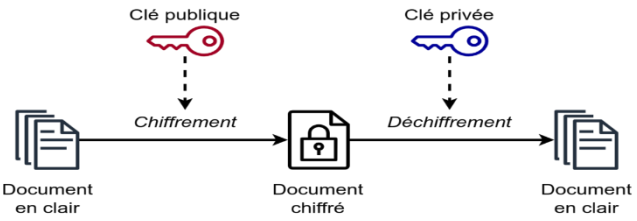
Ce terme est utilisé pour décrire les algorithmes de chiffrement qui utilisent une même clé pour le chiffrage et le déchiffrage.




Le chiffrement à clé asymétrique

La cryptographie asymétrique, ou cryptographie à clé publique est un domaine relativement récent de la cryptographie.

Le chiffrement 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.



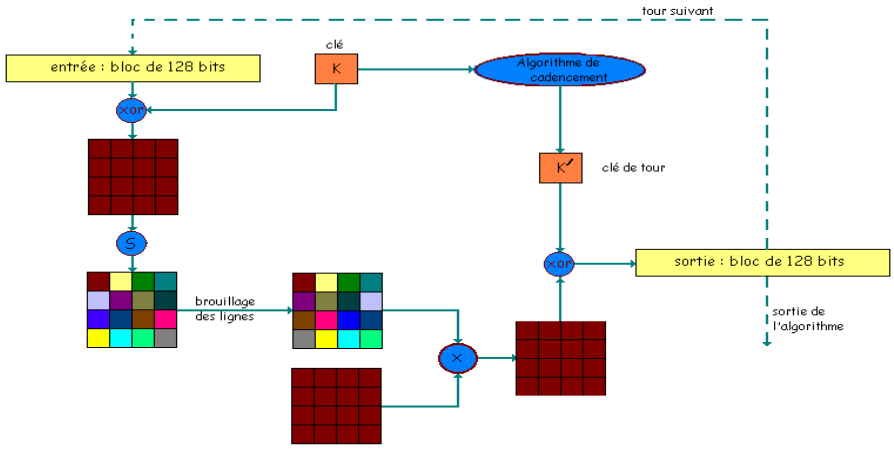

## Le chiffrement AES

Le chiffrement AES est un algorithme de chiffrement symétrique.

C'est un chiffrement par bloc symétrique utilisé pour chiffrer les données sensibles.

Il existe trois principaux types de cryptage AES :

| Version | Taille clé | Taille bloc | Nombre de tours | Combinaisons potentielles différentes |
|---|---|---|---|---|
| AES-128 | 128-bits | 128 | 10 | 3,4 x 1038 |
| AES-192 | 192-bits | 128 | 12 | 6,2 x 1057 |
| AES-256 | 256-bits | 128 | 14 | 1,1 x 1077 |




## La différence entre chiffrement bijectif et hachage

Le chiffrement bijectif est une fonction bidirectionnelle, comprenant le chiffrement et le déchiffrement tandis que le hachage est une fonction qui convertit le texte brut en un résumé unique et irréversible.

**Les limites du hachage des mots de passe**

Irréversibilité : Le hachage est irréversible Il s'agit d'une fonction à sens unique et garantit que même si quelqu'un accède aux mots de passe hachés, il ne sera pas en mesure de les déchiffrer pour retrouver les mots de passe originaux.

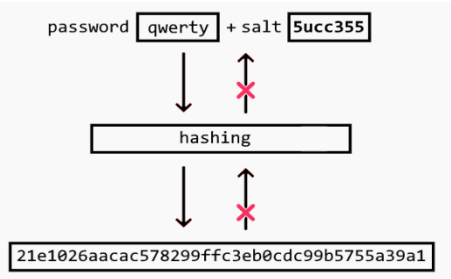
Consommation de la mémoire : le hachage des mots de passe est un processus qui nécessite beaucoup de mémoire.

**Le salage des mots de passe**

Le salage consiste à concaténer le mot de passe avec une chaîne de caractères quelconques, le plus souvent aléatoire. Le salage peut être statique : chaque mot de passe est salé avec la même chaîne de caractères (mais ce type de salage est considéré comme dépassé), ou dynamique : chaque mot de passe est salé aléatoirement (cela empêchera deux utilisateurs d'avoir la même empreinte s'ils ont le même mot de passe).

Dans le cas où le salage est dynamique, chaque enregistrement de la table de mots de passe du système d'authentification contient les informations suivantes :

Identifiant | hachage (mot de passe + salage) | salage




## La stéganographie

La **stéganographie** est un domaine où l'on cherche à dissimuler discrètement de l'information dans un media de couverture (typiquement un signal de type texte, son, image, vidéo, etc.).

L'intérêt de la stéganographie réside précisément dans la possibilité de communiquer en échangeant des contenus d'apparence anodines de façon à ne pas éveiller de soupçons.

**II) L'outil Truecrypt**

▶ Expliquer à quoi sert l'outil truecrypt.

Il est possible de créer un disque virtuel chiffré contenu dans un fichier grâce au logiciel Truecrypt, puis de le monter comme un disque réel. En outre, cet instrument a la capacité de crypter une partition complète ou un dispositif tels qu'une clé USB ou un disque. On procède à ce chiffrement de façon automatique, en temps réel et transparente.

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

La particularité de TrueCrypt par rapport à d'autres outils de chiffrement traditionnels réside dans sa capacité à générer des volumes chiffrés de manière progressive à mesure que vous ajoutez des fichiers.

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

TrueCrypt est bénéfique pour les entreprises qui souhaitent protéger leurs données sensibles, puisque l'outil permet de créer des volumes chiffrés, Volumes cachés et vérification en deux étapes pour améliorer Sécurité. Par conséquent, l'utilisation de TrueCrypt permet de garantir la confidentialité donnée et protéger contre les menaces de sécurité potentielles. Mais il faut noter que TrueCrypt n'est plus considéré Des alternatives sûres et plus modernes sont recommandées Protégez les données de l'entreprise de manière plus sécurisée

▶ Rechercher des solutions alternatives à Truecrypt.

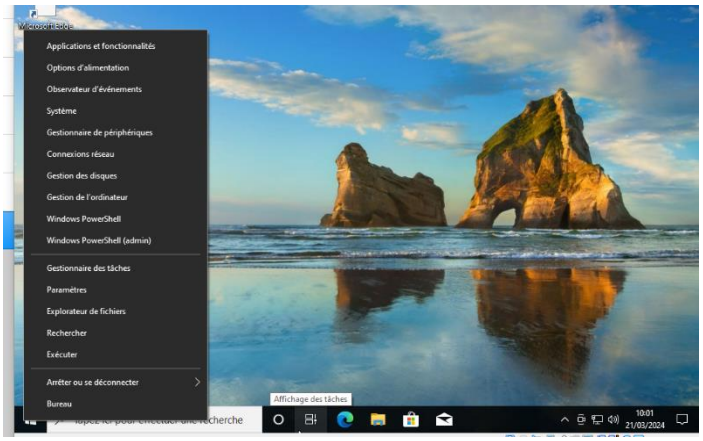
VeraCrypt; Bitlocker ; DiskCryptor ;Ciphershed ;FileVault 2 ;LUKS ;AxCrypt.

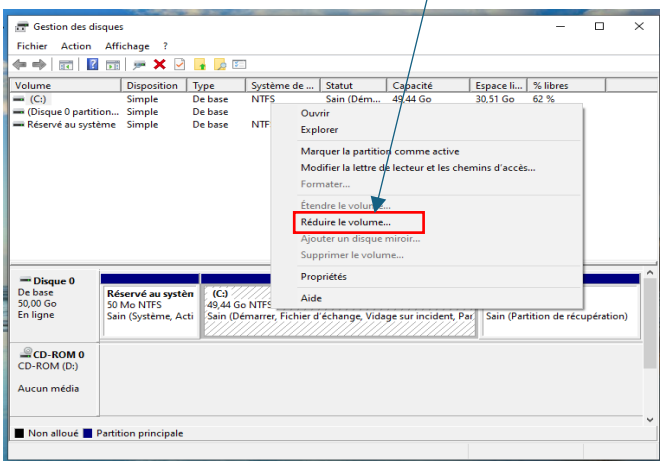
III) Mise en œuvre d'une solution de chiffrement

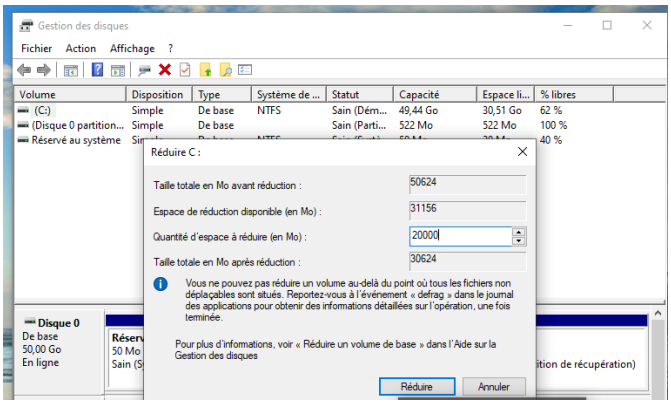
**SUR WINDOWS**

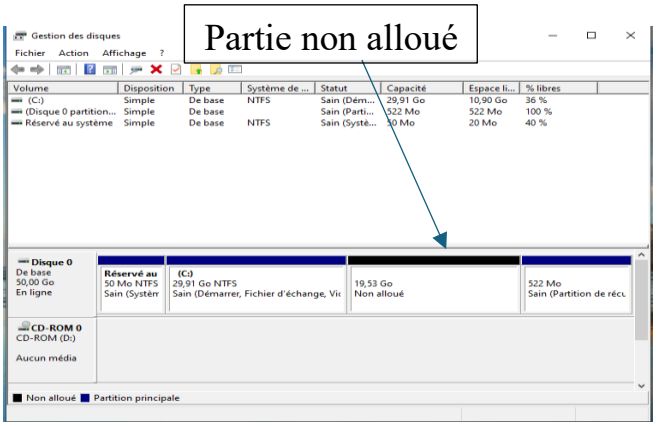
**Création de la partition que l'on va chiffrer**

Reduction du volume du disque © pour obtenir une partie allouée du disque

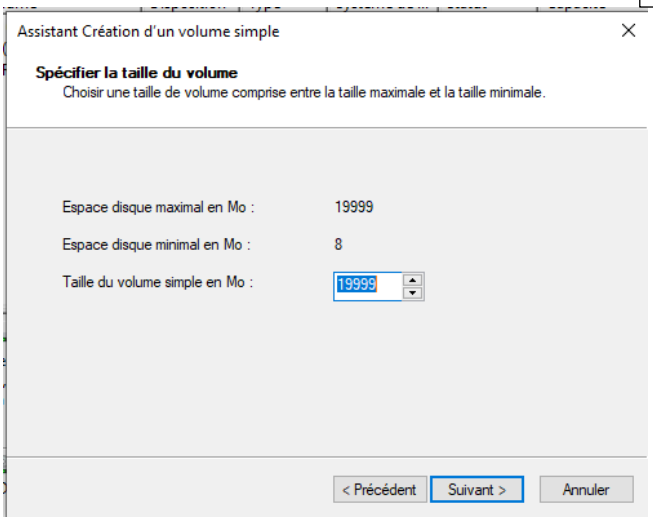


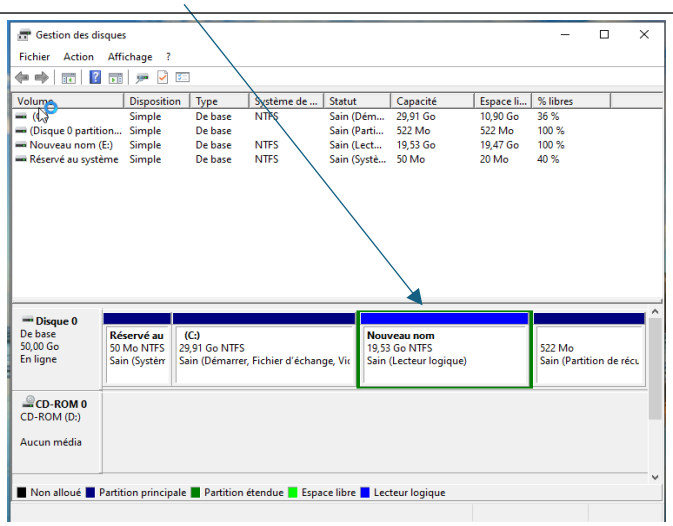





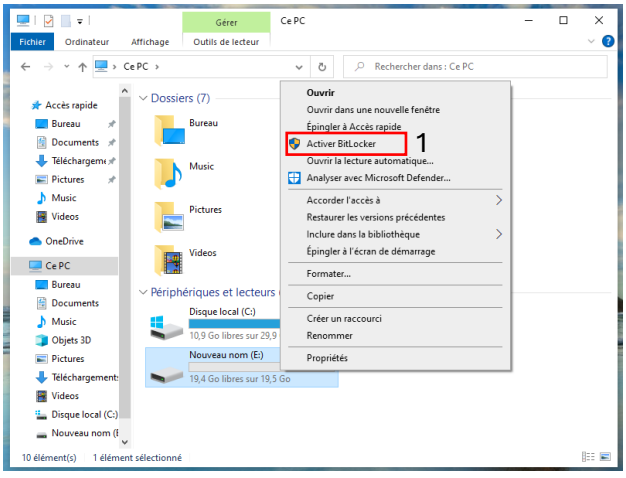

Le nouveau disque nommé (E) a bien été créé

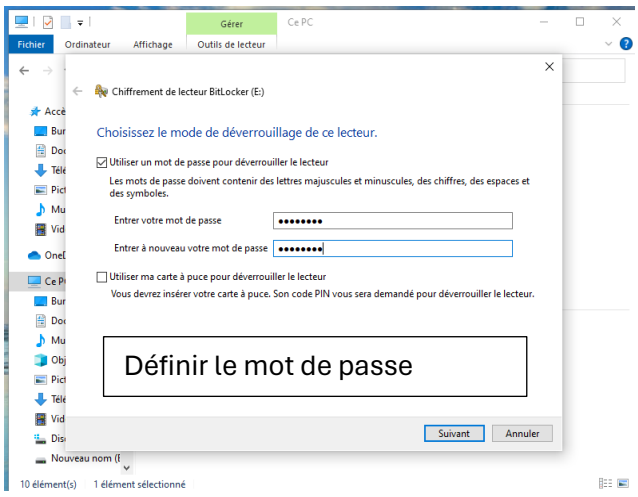


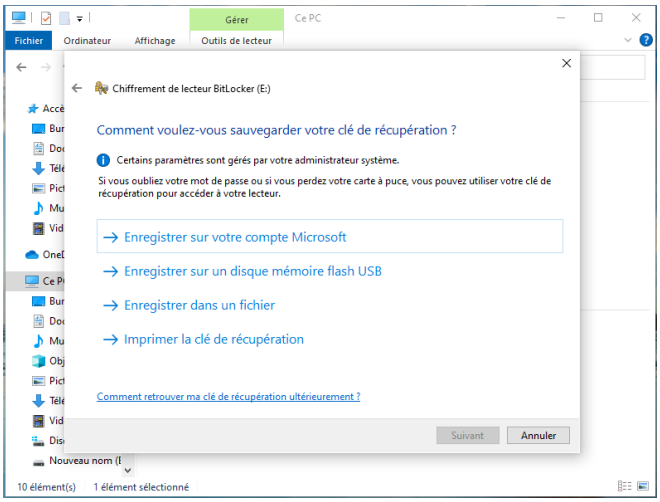

NB : Pour plus de détaille dans la création d'une nouvelle partition confère TP B3 : Gestion des accès.

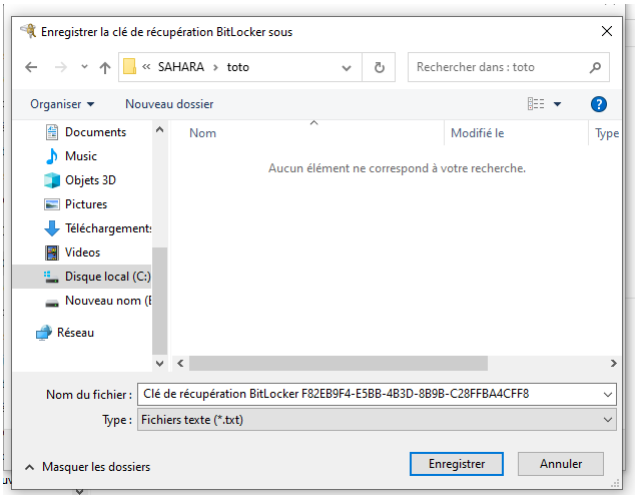
**Chiffrement de la partition avec BitLocker qui est au préalable installer sur Windows par défaut.**



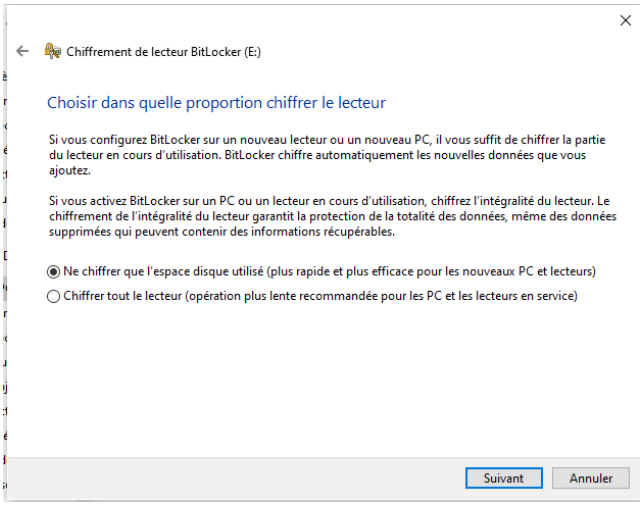



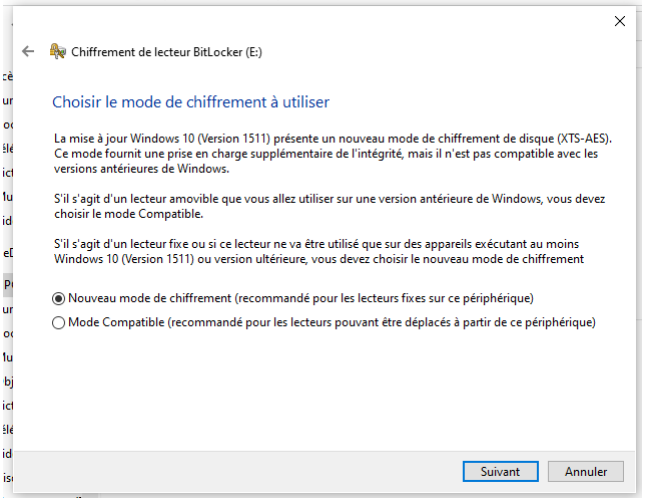
Pour récupérer le mot de passe en cas d'oubli vous pouvez enregistrer votre clé selon les options. Attention : Enregistrer la clé de chiffrement dans un fichier n'est pas la meilleure solution en termes de sécurité. Je vous conseille de l'enregistrer sur une clés USB chiffrer qui vous placerez en sécurité sellons l'importance des données chiffrées.

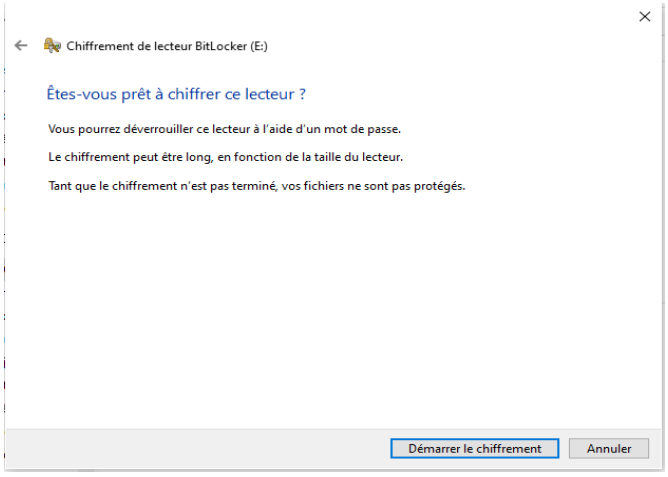


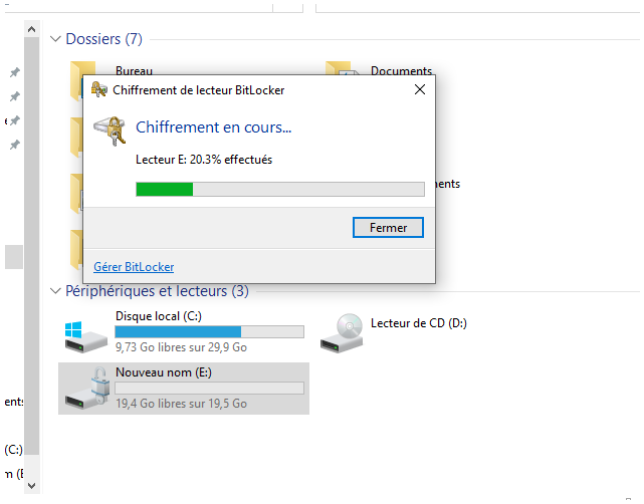




Dans mon cas j'ai choisi d'enregistrer la clé de chiffrement dans un fichier car la partition est vide

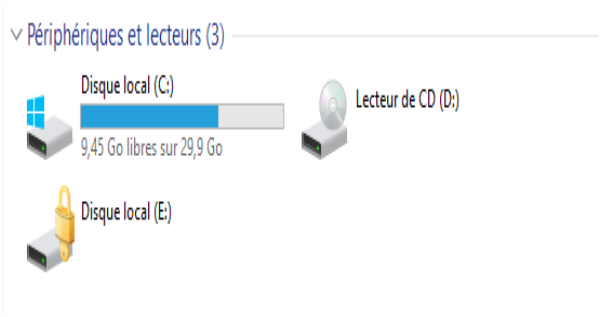


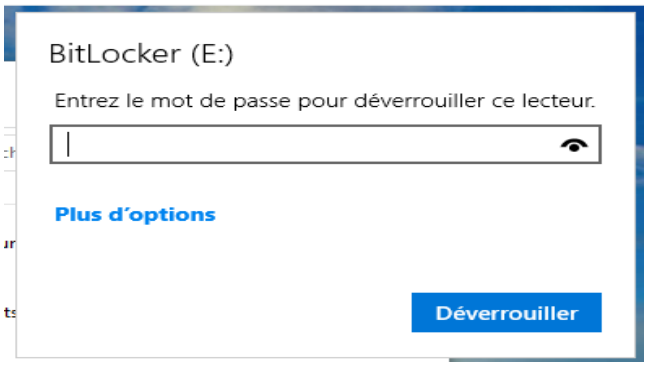



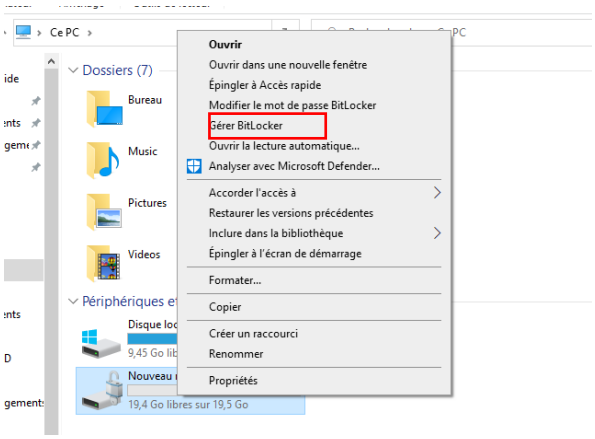



Mon disque (E :) à bien été chiffré

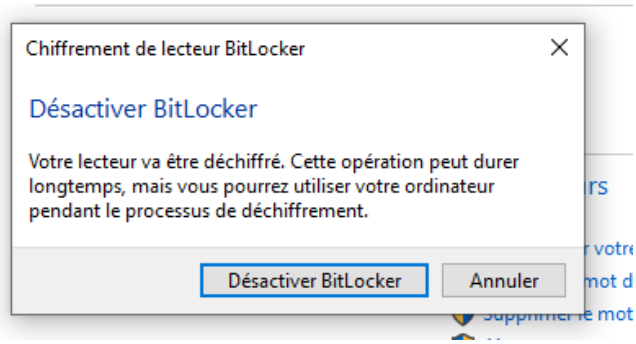


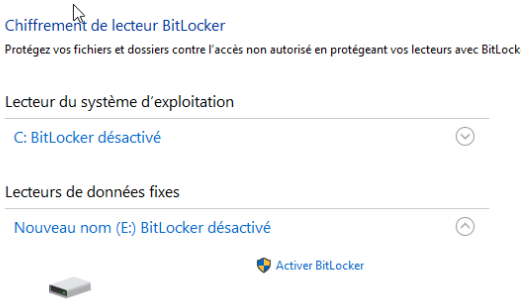

Pour Déchiffrer la partition nous aurons juste qu'a désactiver BitLocker après l'ouverture du disque.








Déchiffrement Réussi BitLocker à bien été désactiver




**SUR LINUX**

Téléchargement d'une version de Veracrypte

```
sarah@debian12:~$ wget http://sourceforge.net/projects/veracrypt/files/VeraCrypt%201.0f
-2/veracrypt-1.0f-2-setup.tar.bz2

veracrypt-1.0f-2-setu 100%[=======================>]  15,12M   629KB/s    ds 34s

2024-03-22 12:46:10 (452 KB/s) – « veracrypt-1.0f-2-setup.tar.bz2 » sauvegardé [1585444
3/15854443]
```

Décompresser l'archive

Ici, on voit donc que l'on peut installer VeraCrypt en ligne de commande pour les processus 64 bits, 32 bits et la même chose en mode graphique

```
sarah@debian12:~$ tar xvjf veracrypt-1.0f-2-setup.tar.bz2
veracrypt-1.0f-2-setup-console-x64
veracrypt-1.0f-2-setup-console-x86
veracrypt-1.0f-2-setup-gui-x64
veracrypt-1.0f-2-setup-gui-x86
```

Vérification du type de processeur de notre

```
sarah@debian12:~$ uname -r
6.1.0-18-amd64
```

Installation

```
sarah@debian12:~$ ./veracrypt-1.0f-2-setup-console-x64
```

```
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: 1
```

```
Do you accept and agree to be bound by the license terms? (yes/no):
```

```
To uninstall VeraCrypt, please run 'veracrypt-uninstall.sh'.

Installing package...
usr/
usr/bin/
usr/bin/veracrypt-uninstall.sh
usr/bin/veracrypt
usr/share/
usr/share/applications/
usr/share/applications/veracrypt.desktop
usr/share/veracrypt/
usr/share/veracrypt/doc/
usr/share/veracrypt/doc/License.txt
usr/share/veracrypt/doc/VeraCrypt User Guide.pdf
usr/share/pixmaps/
usr/share/pixmaps/veracrypt.xpm

Press Enter to exit...
```

Créer un volume chiffré VeraCrypt

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

Enter volume path: /opt/volume1

Enter volume 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

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:
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
u want to use a short password? (y=Yes/n=No) [No]: y

Re-enter password:

Enter keyfile path [none]:

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

Il nous est dans un premier temps demandé 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*".

Ensuite saisir le chemin vers le volume à créer et par la même occasion son nom. Dans mon cas le nom de mon volume est : Volume1 et sa taille 200M

Il nous est demandé l'algorithme de chiffrement que nous souhaitons utiliser. Ici nous allons garder la proposition par défaut qui est *"AES"* en saisissant "1".

Ici nous allons garder l'algorithme proposé qui est *"SHA-512"* et également le système de fichier.

Ensuite la partie mot de passe, ici, il est important de saisir un mot de passe robuste. L'exemple présenté en dessous montre qu'en aillant saisi un mot de passe faible (en dessous de 20 caractères selon VeraCrypt), VeraCrypt me prévient et me conseille d'utiliser un mot de passe plus robuste.

Pour terminer, et initialiser le chiffrement du volume, il va falloir générer de l'entropie en saisissant au moins 320 caractères de façon aléatoire sur son clavier.

```
Done: 100,000%  Speed:    20 MB/s  Left: 0 s
```

Le volume chiffré a chiffré été créer

```
root@debian:/home/sarah# veracrypt /opt/volume1 /mnt
Enter password for /opt/volume1:
Enter keyfile [none]:
Protect hidden volume (if any)? (y=Yes/n=No) [No]: NO
```

Monter un volume chiffré VeraCrypt

```
root@debian:/home/sarah# mount
```

Vérifier que le volume est bien monté, vous pouvez utiliser la commande ″mount " résultat ci-dessous :

```
/dev/mapper/veracrypt1 on /mnt type vfat (rw,relatime,fmask=0077,dmask=0077,codepage=43
7,iocharset=ascii,shortname=mixed,utf8,errors=remount-ro)
```

```
root@debian:/home/sarah# cd /mnt
root@debian:/mnt#
```

Une fois le volume chiffré monté, on pourra librement y accéder en allant, dans le cas présent, dans le dossier /mnt.

Pour Déchiffrer la partition nous aurons juste qu'à démonter le volume1 monté.

Démonter un volume chiffré VeraCrypt

```
root@debian:/home/sarah# veracrypt -d
```

Désinstaller VeraCrypt

```
root@debian:/home/sarah# veracrypt-uninstall.sh
VeraCrypt uninstalled.
```