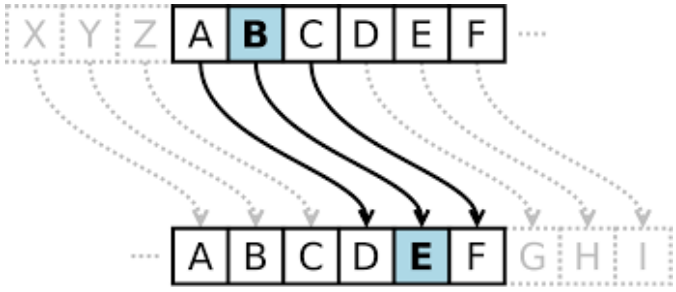
TP– CHIFFREMENT

AXEL HESPEL

I) Etude et Recherche:

1. **Le Code César**

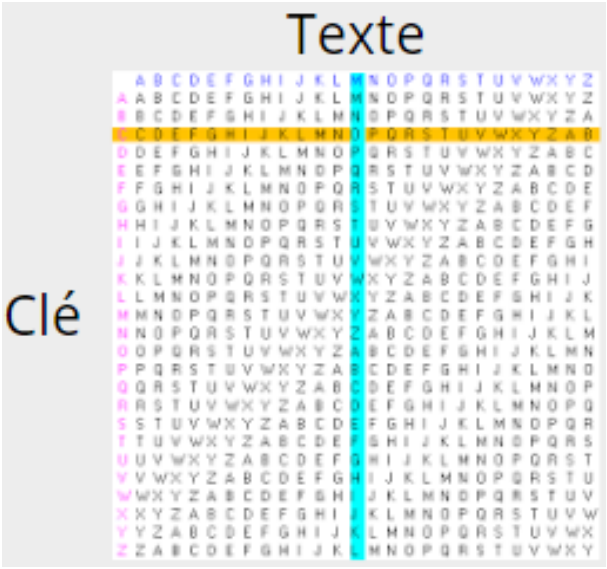


On décale le mot que l'on veut coder par un nombre défini dans l'alphabet.

Code par un décalage de 1, devient :

Dpef

2. **Le Carré de Vigenère**



Chiffrement = Clé + texte

Exemple

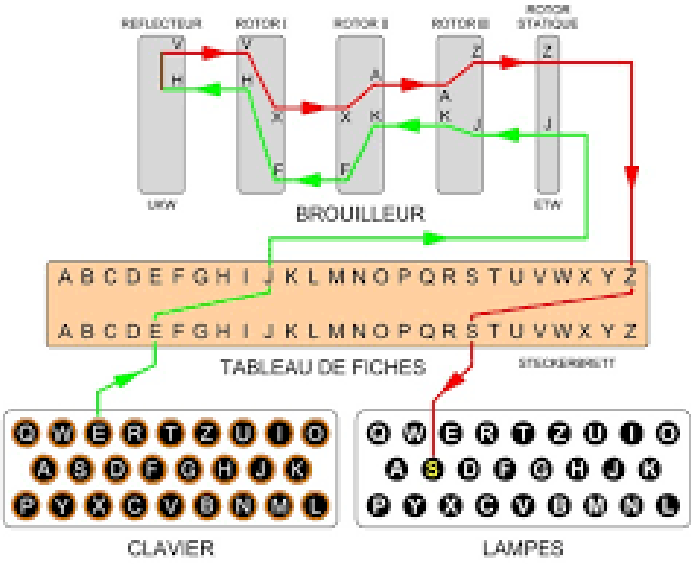
Clé=code

Texte=texte

Chiffrement= vjaxg

Le chiffrement associe chaque lettre du texte clair à une lettre du texte codé, en utilisant une correspondance entre la lettre du texte clair et celle du code, qui est déterminée par la position de la lettre dans la clé (une fois arrivé à la fin de la clé, on la répète).

3. **La machine « Enigma »**



Il s'agit d'une machine qui chiffre un message de façon mécanique. On positionne des rotors représentant chaque lettre de l'alphabet (généralement 3 ou 4 rotors), qui tournent à chaque lettre entrée. La clé consiste en la position initiale des rotors, suivie des connexions au brouilleur. Ensuite, on entre le texte et une lettre en ressort

4. **Le téléphone rouge**

Échange entre deux pays (par texte) chiffré par un masque jetable. On choisit un code aléatoire plus long que le texte à chiffrer. Ensuite, on

additionne les valeurs numériques de chaque paire de lettres (a=1), puis on prend le reste de la division par 26.

Ex

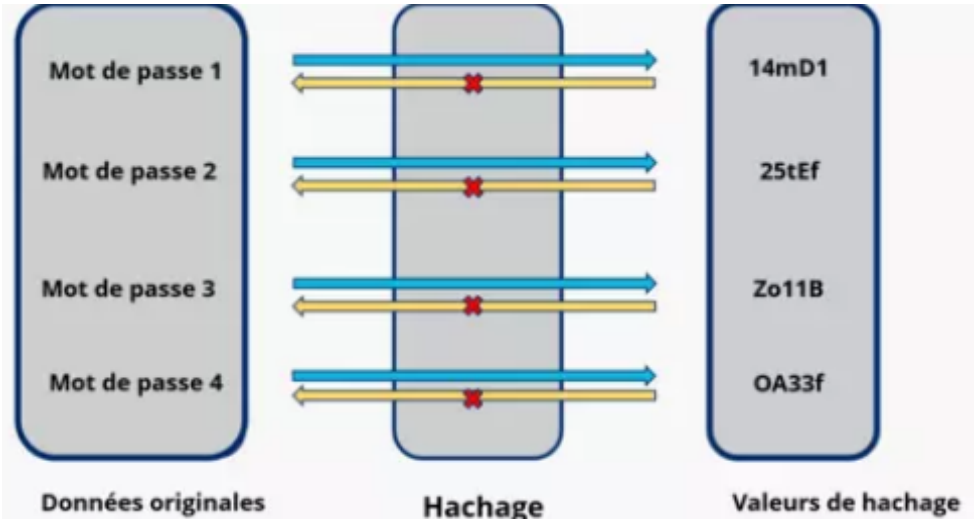
7 (H) 4 (E) 11 (L) 11 (L) 14 (O) message

+ 22 (W) 12 (M) 2 (C) 10 (K) 11 (L) masque

= 29 16 13 21 25 (masque + message)

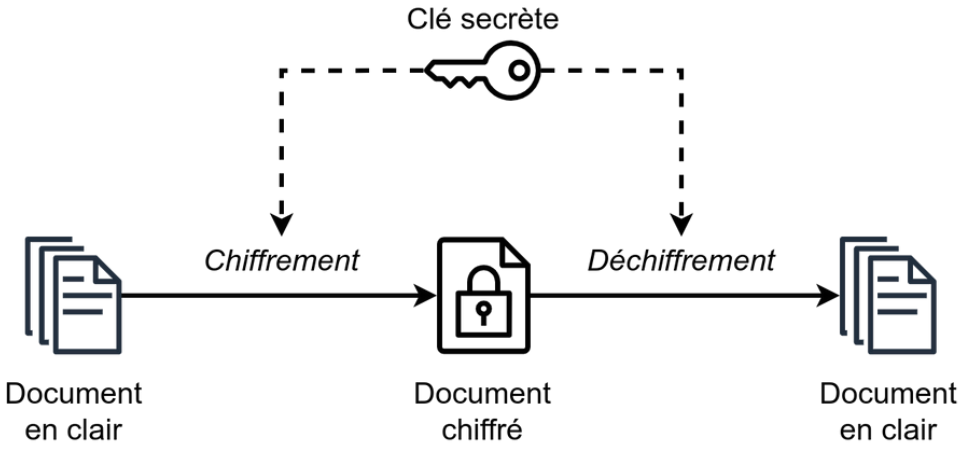
= 3 (D) 16 (Q) 13 (N) 21 (V) 25 (Z) masque + message / division par 26

5. **Le hachage**



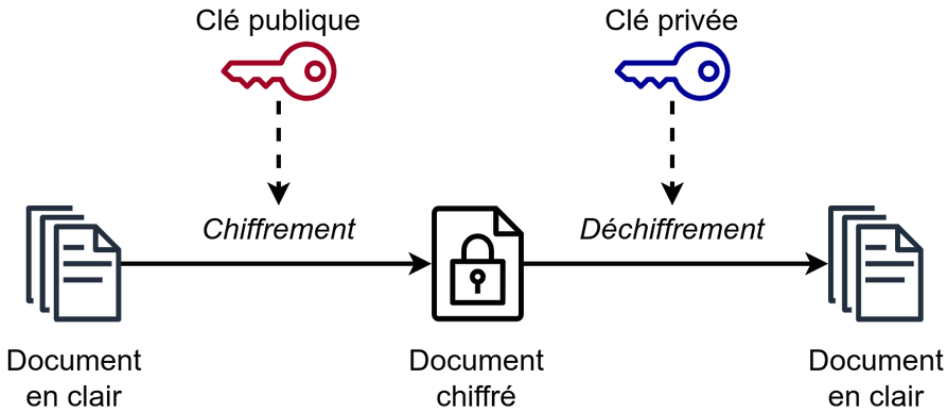
Le hachage est un algorithme qui transforme un texte donné en une suite de caractères fixes. Par exemple, le SHA-256 transforme tout texte en une suite de 256 caractères. La sécurité dépend donc de la fonction de hachage elle-même et de sa résistance à la rétro-ingénierie (’déhashage’), car un texte haché donnera toujours le même résultat avec le même algorithme de hachage.

6. **Le chiffrement à clé symétrique**



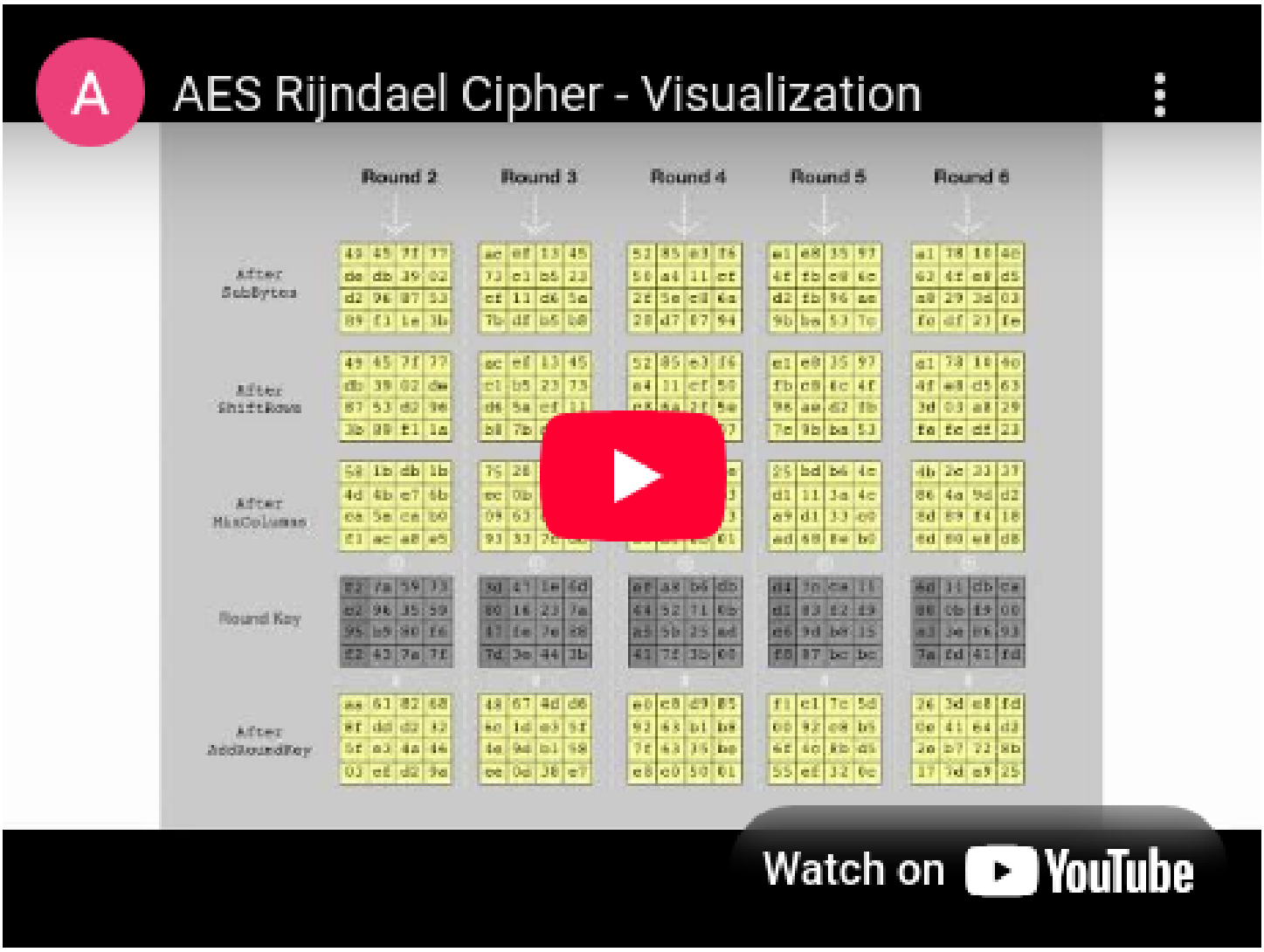
Il s'agit d'un système de chiffrement qui dépend d'une clé unique pour le chiffrement et le déchiffrement. Il est donc faible en termes de taille et de complexité, et si la clé est révélée, tous les messages peuvent être déchiffrés.

7. **Le chiffrement à clé asymétrique**



Il s'agit d'un chiffrement très différent des autres, car vous devez utiliser une clé publique fournie par le destinataire pour chiffrer un message qui ne pourra être déchiffré que par la personne qui le reçoit via sa clé privée. On les appelle clé publique et clé privée car la clé publique peut être révélée ; elle ne sert qu'à chiffrer, tandis que la clé privée ne sert qu'à déchiffrer.

8. **Le chiffrement AES** [VIDEO]



L'AES est un système de chiffrement complexe standardisé qui utilise une clé de 128, 192 ou 256 bits pour chiffrer un message de taille fixe. On entre donc un texte et une clé, et il va réaliser différents calculs, tels que la multiplication des deux sous forme de matrice, les déplacements dans la matrice verticalement ou horizontalement, et utiliser la méthode des carrés de Vigenère pour rendre le texte très différent.

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

Une fonction bijective est une fonction qui assure qu'à chaque élément correspond une image unique, évitant ainsi les incohérences lors du décryptage.

Une fonction de hachage permet de crypter un message d'une longueur de X bits et de produire un code de longueur Y bits en sortie. Une fonction de hachage n'est pas forcément bijective.

La principale différence réside dans la réversibilité : avec une fonction bijective, il est possible de retrouver l'entrée à partir de la sortie, tandis qu'une fonction de hachage est pratiquement irréversible.

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

Le hachage a une limite fondamentale : il est possible de retrouver le texte original à partir du hachage par force brute si l'on connaît le type de hachage utilisé. De plus, le type de hachage utilisé est souvent facilement identifiable avec la clé elle-même.

11. **Le salage des mots de passe**

Le salage est une technique dérivée du hachage. On utilise une fonction de hachage sur un mot de passe auquel on ajoute une donnée supplémentaire, afin de rendre la technique de hachage moins susceptible d'être brute-forcée pour retrouver le mot de passe directement. En effet, pour effectuer cette attaque, il faudrait connaître la donnée ajoutée avant le hachage

12. **La stéganographie**

La stéganographie est une pratique qui vise à cacher des messages dans d'autres médias. L'exemple le plus connu est le livre-code, qui consiste à crypter un message en référençant les pages d'un livre où les mots se trouvent.

Attention.

Crypter signifie rendre des données illisibles en utilisant une clé, hacher signifie créer une empreinte unique des données, tandis que chiffrer implique de rendre des données sécurisées en utilisant un algorithme et une clé pour qu'elles puissent être déchiffrées plus tard.

Crypter: pas besoin de la clé pour decrypter

hacher: besoin de la fonction de déhachage

chiffrer: besoin de la clé

II) L'outil Truecrypt

1. **A quoi sert l'outil truecrypt.**

TrueCrypt est un outil permettant de chiffrer des données, qu'il s'agisse de partitions de disque, de périphériques ou de la création de disques virtuels chiffrés qui agissent comme des disques physiques. Il permet le chiffrement en temps réel, contrairement au chiffrement effectué a posteriori ou à intervalles réguliers.

2. **Expliquer le principe de fonctionnement de TrueCrypt**

TrueCrypt est un logiciel gratuit mais non libre. Il est qualifié de logiciel de chiffrement « à la volée », ce qui signifie qu'il permet de chiffrer des données stockées dans un conteneur. Pendant que le conteneur est ouvert, les données sont accessibles en clair. Plusieurs mesures de sécurité sont mises en place, parmi lesquelles les deux principales sont les suivantes : premièrement, la création de la partition TrueCrypt n'est pas identifiable, et même Windows peut la lire comme une partition corrompue en raison de la disposition aléatoire des données ; deuxièmement, il possède une fonction de cryptage imbriqué, permettant d'utiliser plusieurs algorithmes de chiffrement pour renforcer la sécurité. Les algorithmes mis en place sont AES, Serpent et Twofish (Cliquer pour en apprendre plus)

Cependant, il se distingue surtout par son système de chiffrement automatique en temps réel. Le seul problème majeur réside dans le stockage de la clé en mémoire lorsque la partition est montée, ce qui constitue une faille de sécurité significative.

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

TrueCrypt pourrait être intéressant en entreprise pour permettre le cryptage des différents stockages de données, qu'il s'agisse de simples

fichiers sur un ordinateur ou sur des clés USB (pour éviter les fuites de données en cas de perte), mais également pour crypter les données présentes dans des partages de fichiers, qu'ils soient publics ou non

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

VeraCrypt est une version récente de TrueCrypt basée sur le même principe. Il est considéré comme la reléve de TrueCrypt et il est le leader des logiciels libre dans se domaine.

DiskCryptor est spécifique à Windows.

LUKS est un logiciel open source fonctionnant sous Linux, qui prend en charge plusieurs algorithmes de chiffrement, mais n'est pas compatible avec de nombreux autres systèmes en dehors de Linux.

GNU Privacy Guard: Logiciel multi platforme gratuit, il permet de chiffrer beaucoup de chose et également les supports connecté a un PC, peut etre utile pour un NAS par exemple.

AxCrypt: Il se situe plus dans le monde professionnelle avec une offre payante, mais sa simplicité peux etre un défaut pour une entreprise.

III) Installer une solution de chiffrement sur une machine virtuelle :

bitlocker : Windows

veracrypt: Linux

Veracrypt:

```
wget https://launchpad.net/veracrypt/trunk/1.26.7/+download/veracrypt-console-1.26.7-Debian-12-amd64.deb
```

```
sudo dpkg -i veracrypt-console-1.26.7-Debian-12-amd64.de
```

Si il vous manque des dépendance:

```
sudo apt --fix-broken install
```

Ensuite:

Créons le premier fichier crypter (il doit déja exister avant)

```
root@debian22:/home# veracrypt -t -c
Volume type:
 1) Normal
 2) Hidden
Select [1]: 1

Enter volume path: /home/Fichier1Crypter_
```

Ensuite choisir la taille est l'algorithme, dans notre cas pour des testes nous prendrons un facile (AES) vue précédemment.

Ensuite, vous entrez un mot de passe, VeraCrypt recommande un minimum de 20 caractères. Pour nos tests, nous pouvons utiliser un mot de passe faible, mais en production, il est important d'avoir un mot de passe robuste, sinon même les meilleurs systéme de cryptage du monde deviendront obsolètes.

Ensuite, vous devez choisir aléatoirement 320 caractères pour créer de l'entropie (aléatoire) dans votre fichier. Cette suite sera propre à chacun ; il vous suffit de taper frénétiquement sur votre clavier.

```
Enter PIM:

Enter keyfile path [none]:

Please type at least 320 randomly chosen characters and then press Enter:
Characters remaining: 317
Characters remaining: 282
Characters remaining: 162



Done:   8.111%  Speed: 143 MiB/s  Left: 77 s
```

Monter et démonter:

On peut maintenant monter le volume

veracrypt /home/Fichier1Crypter /mnt

On vous demanderas votre MDP ou/et un fichier avec une clée.

Et pour démonter notre volume:

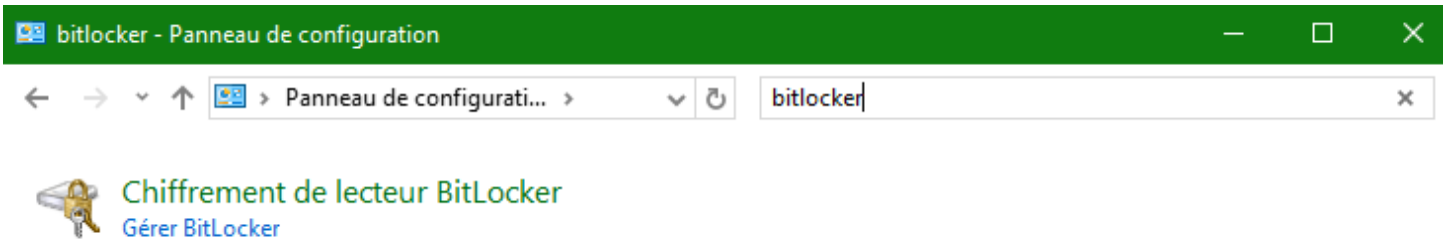
veracrypt -d

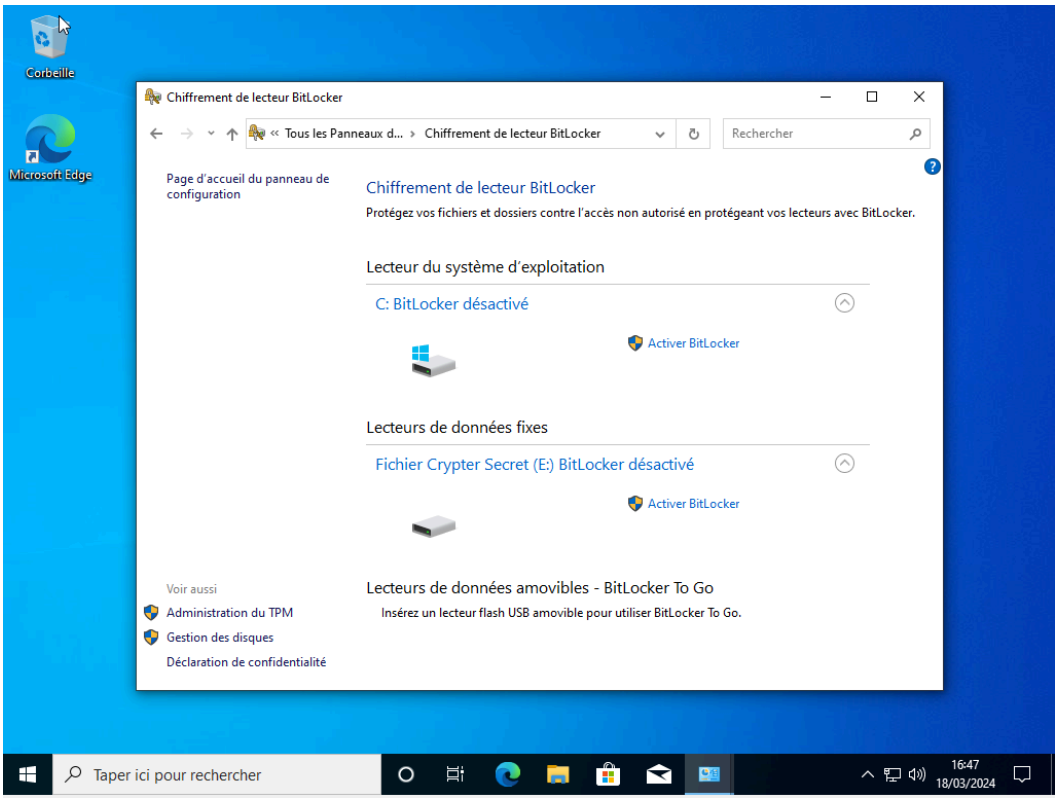
Bitlocker

Bitlocker est installé nativement sur windows.

Nous pouvons chiffrer directement une partition , pour l'exemple nous allons créer une partition comme dans ce tp (cliquable)puis la chiffrer

Panneau de configuration >Bitlocker > MONFICHIER





Ensuite, vous devez conserver votre clé de récupération et cliquer sur suivant. Il s'agit d'un fichier donc elle ne doit pas être accessible sur le bureau par exemple

Et voilà, vous disposez maintenant d'un fichier crypté automatiquement sur Windows. Cependant, il sera ouvert à chaque fois que l'ordinateur est lancé. Par conséquent, une fois que vous avez fini de l'utiliser, il est important de fermer la connexion avec la partition ou les fichiers seront visible.

Attention, cette protection ne protège pas vraiment les connexions physiques.

Le plus gros problème de ces deux logiciels est également leur avantage : une fois ouverts, vous pouvez accéder aux fichiers ou à la partition. Cependant, cela signifie que tout le monde y a accès. Par exemple, sur un serveur de production, utiliser une solution de ce type peut être dangereux car on accède aux données en permanence, ce qui signifie que les partitions sont toujours montées.

Il est encore plus dangereux de ne pas utiliser qu'une clé de récupération sous forme de fichier. Il serait recommandé de la hacher et de la garder hors site, et non sur la machine elle-même.