# CHIFFREMENT

Thomas GRZESINSKI

# C’est quoi ce chiffrement ?

Le chiffrement est  un procédé de cryptographie grâce auquel on souhaite rendre la compréhension d’un document impossible à toute personne qui n’a pas la clé de chiffrement.

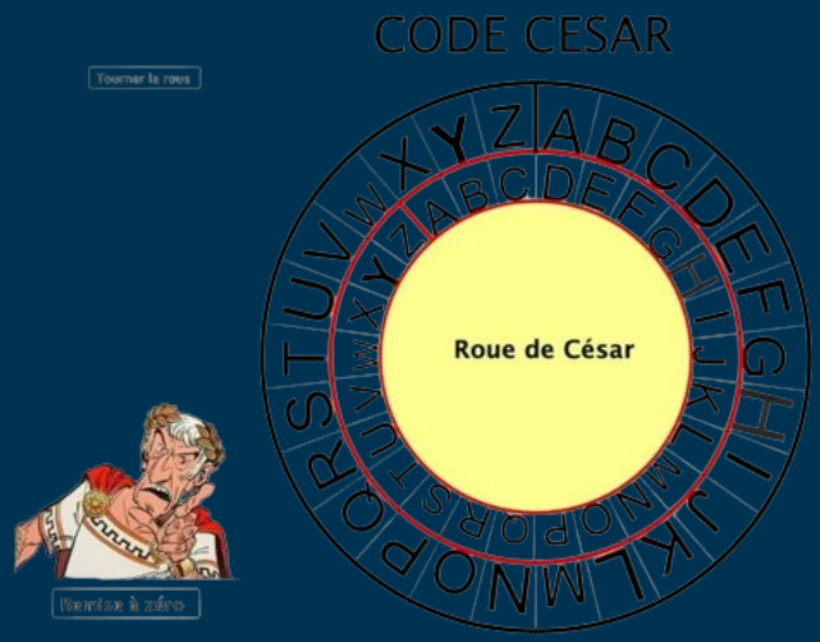
# LE CODE CESAR

Histoire: Le code César est un chiffrement par décalage qui a été utilisé par Jules César durant ses correspondances secrètes .

Fonctionnement: Le texte chiffré s’obtient en remplaçant chaque lettre du texte clair original par une lettre à distance fixe toujours du même côté/

Exemple en décalage de 3:

Texte clair: Bonjour
Chiffrement: Erqmrxu



# LE CARRE DE VIGENERE

Histoire: Système de chiffrement inventé par « Blaise Vigenère qui mit en échec les cryptanalystes durant trois siècles.

Fonctionnement: Il faut une clé de déchiffrement , cette clé est sous la forme d'un mot, d'un code ou même d'une phrase connue par l'émeteur du message et qui n'a aucun sens
Ensuite pour chiffré le message on regarde la lettre dans le sens horizontale et ensuite verticale.
Pour déchiffrer le message vous partez de la clé répeté jusqeu x lettre du message chiffré

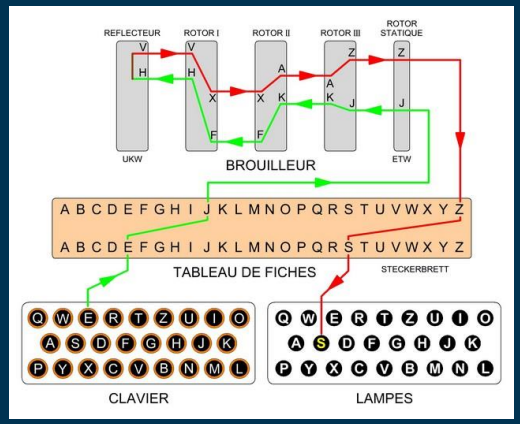
Exemple:
Clé: Pain
Message: Je suis en BTS SIO
Clé répétée: Pa inpa in pai npa
Message chiffré: YEAHX SMAQT AFXO

| | 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 |

# LA MACHINE « Enigma »

Histoire: Inventé en 1918 elle a principalement été utilisée par l'Allemagne Nazie et ses alliés pendant la seconde guerre mondiale car elle a était désigné « d'inviolable » par ses concepteurs.

Fonctionnement: En tapant sur une lettre, un courant électrique passait par des composants appelés rotor. Après une série de transfert complexes, la machine indiquait à quelle lettre correspond la lettre donnée initialement. Cependant, à la rotation d'un de ces rotors, le passage du courant électrique changeait totalement, résultant en une toute nouvelle combinaison de lettres. Les rotors étant déplacés quotidiennement, casser le code était presque impossible
Seul Alan Turning a réussi à casser le déchiffrement de la machine due à la récurrence « Heil Hitler » qui était évoqué dans chaque télégramme.



# LE TELEPHONE ROUGE

Histoire: Ligne de télécommunication directe établie le 30 août 1963 entre les Etats-Unis et l'Union Soviétique à la suite d'un accord signé entre les deux pays et entré en vigueur le 20 juin 1963

Fonctionnement: Ligne de télécommunication sécurisé grâce au principe du masque jetable à l'aide de machines de chiffrement dites Electronic Teleprinter Cryptographic Regenerative Repeater Mixer (ETCRRM)

Les Soviétiques fournissent leurs clés de chiffrement à l'ambassade des États-Unis à Moscou et les Américains à l'ambassade de l'URSS à Washington5. Les clés sont changées à chaque communication et détruites lorsque celle-ci est terminée.Le message est envoyé dans la langue initiale du payspuis il est traduit au niveau du pays récepteur qui y joint le message initial

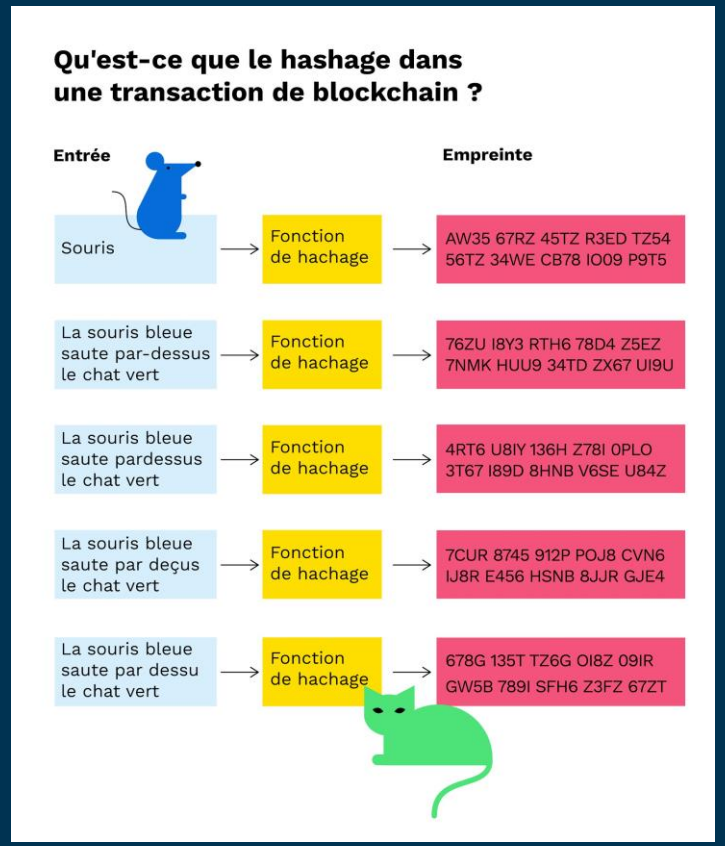
En 1971, le système filaire est doublé par les liaisons satellitaires via les satellites américains Intelsat et soviétiques Molnyia II9. En 1984, le système utilise les satellites géostationnaires soviétiques Gorizont et se sert du fax à haute vitesse et de ce fait la vitesse d'échange est accélérée à 4,8 kbit/s.

En 2008, la liaison utilise la fibre optique ce qui permet l'échange vocal et l'envoi de courriel. Les messages sont cryptés, les pays échangeant leurs clé de chiffrement qui changent à chaque communication.

# LE HACHAGE

Histoire: Le hachage permet de ne pas stocker les mots de passe en clair dans la base, mais uniquement de stocker une empreinte de ces derniers. Il est important d'utiliser un algorithme public réputé fort afin de calculer les dites empreintes.

Fonctionnement: un algorithme de chiffrement qui décompose, résout et transforme complètement des données de longueurs différentes en chaînes de longueurs égales.



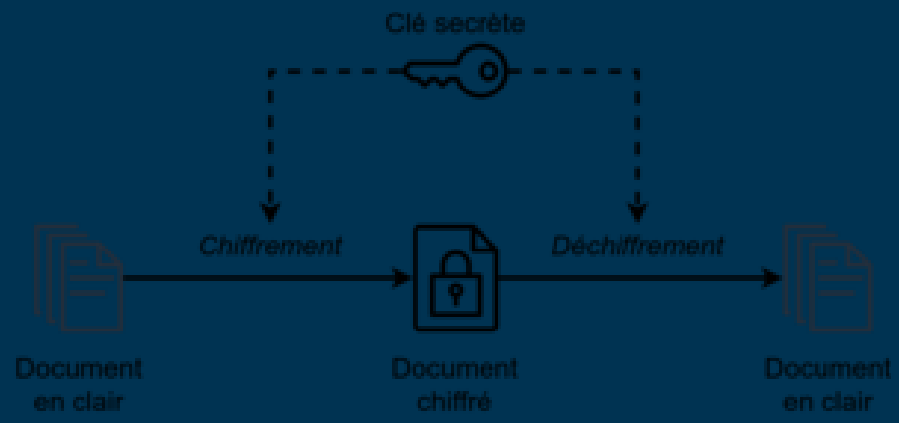
# LE CHIFFREMENT A CLE SYMETRIQUE

Histoire: Le chiffrement par clé symétrique est un terme utilisé pour décrire les algorithmes de chiffrement qui utilisent une même clé pour le chiffrage et le déchiffrage. La clé est généralement appelée « clé secrète ».

Fonctionnement:
-1ère étape
-Génération de la clé secrète par Maxime
-Envoi de cette clé secrète à Arnaud, de manière sécurisée

-2e étape
-Chiffrement du message par Maxime, avec la clé secrète
-Envoi de ce message chiffré à Arnaud

-3e étape
-Réception du message chiffrée par Maxime
-Déchiffrement du message avec la clé secrète reçue auparavant



# LE CHIFFREMENT A CLE ASYMETRIQUE

Histoire: Protocole de cryptographie qui utilise deux clés de chiffrement : une clé publique et une clé privée. La clé publique permet de crypter ou de chiffrer les données. La clé privée sert à déchiffrer ou décrypter des données reçues par le destinataire.

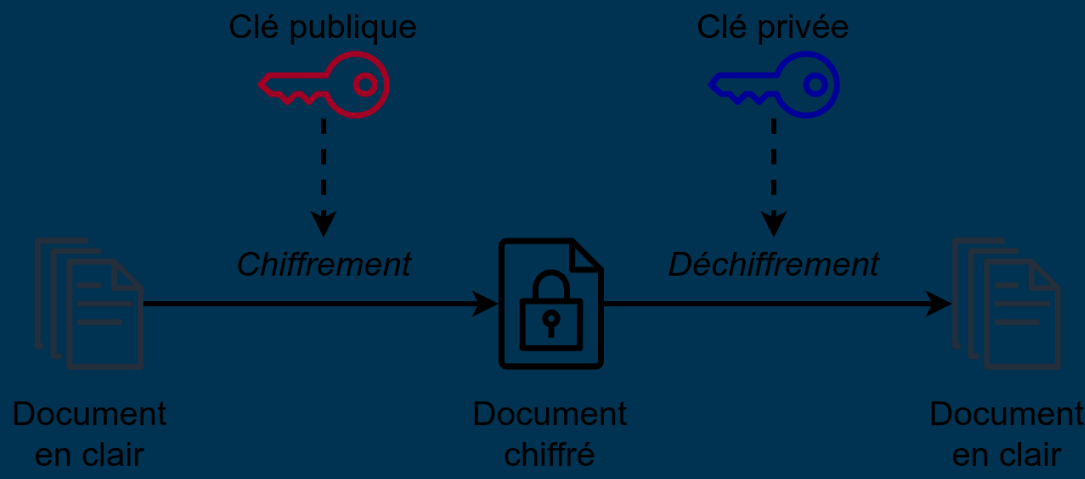
Fonctionnement:

-Le destinataire d'un message ou d'un fichier crée une paire de clés, une publique et une privée. Il conserve la clé privée pour le déchiffrement du message qu'il reçoit

-Le destinataire transmet la clé publique à l'expéditeur via les services d'un fournisseur de clés ou d'une autorité de certification

-La clé publique est utilisée par l'expéditeur pour crypter ou chiffrer le message qu'il envoie

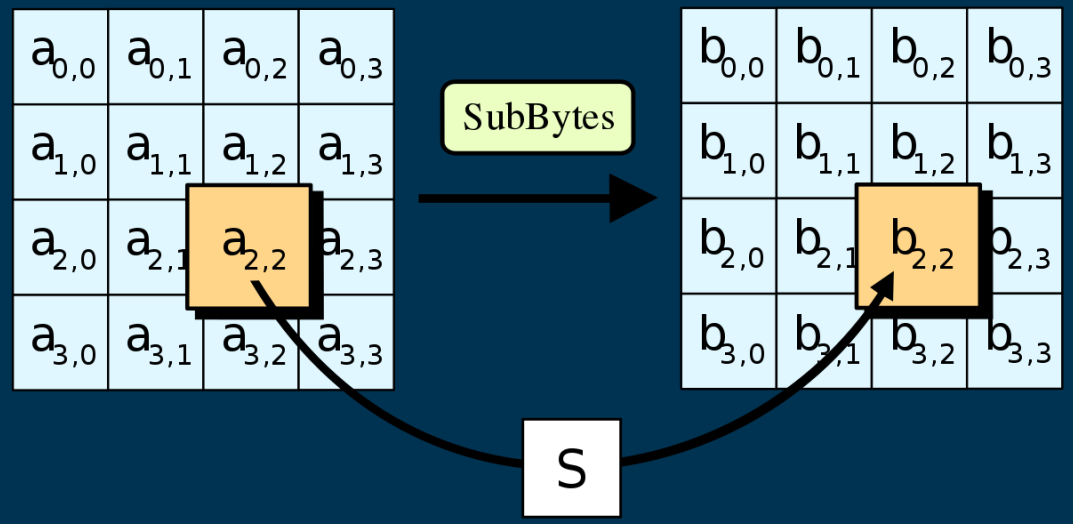
-Le destinataire se sert de sa clé privée pour déchiffrer le message reçu



# LE CHIFFREMENT AES

Histoire: Advanced Encryption Standard ou AES st un algorithme de chiffrement symétrique. La même clé est utilisée pour chiffrer et déchiffrer un texte.
Il repose entièrement sur des notions mathématiques liées aux ensembles (les corps notamment) et a l'arithmétique modulaire.

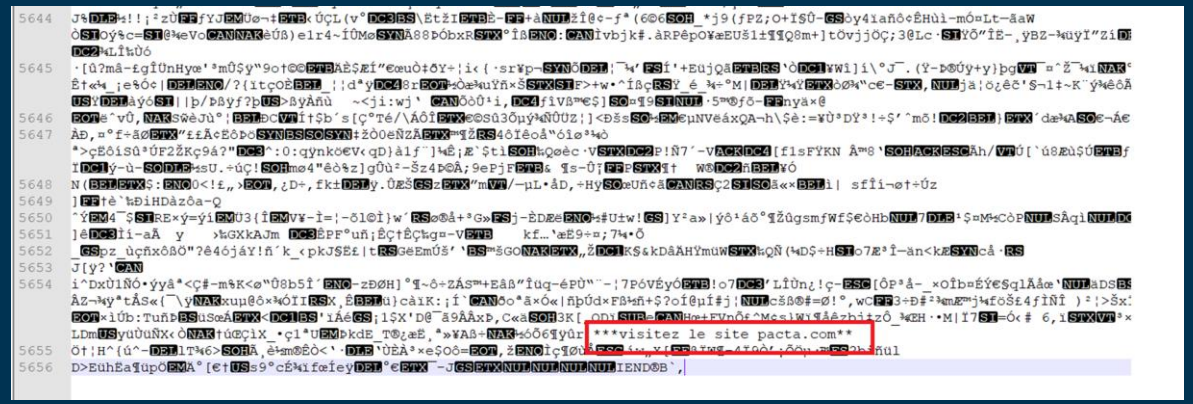
Fonctionnement: AES utilise une seule clé pour le chiffrement et le déchiffrement. AES divise le texte en blocs de 16 octets et effectue plusieurs tours de chiffrement ou de déchiffrement, avec le nombre de tours dépendant de la longueur de la clé (10 tours pour AES-128, 12 pour AES-192 et 14 pour AES-256).



# LA STEGANOGRAPHIE

La stéganographie est une technique consistant à dissimuler un message ou des données à l'intérieur d'un autre fichier (texte, image, audio, vidéo...). Elle diffère en cela de la cryptologie, où le message n'est pas caché mais rendu inintelligible sans un code de décryptage.

L’intérêt est précisément de communiquer en échangeant des contenus d’apparence anodines de façon à ne pas éveiller de soupçon



# LE SALAGE DES MOTS DE PASSE

En général les mots de passe ne sont pas stockés en clair, lorsque on se connecte a un compte, le mot de passe par un algorithme de hachage unidirectionnel. Il est ainsi transformé en une chaîne de caractères indéchiffrable et totalement distincte, le problème est que si deux mots passe sont identiques leur hachage sera donc identique ce qui permet aux hackeurs de vite trouver les mots de passe.

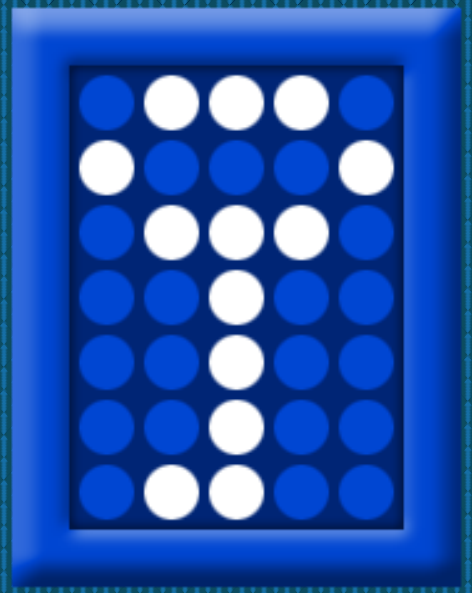
Le salage permet donc d'ajouter une portion de données au mot de passe avant de le soumettre  a l'algorithme de hachage.

Exemple si deux utilisateurs utilise le mot de passe « azerty » chacun des deux ajoutes des caractères aléatoires exemple « azertyHD464$# » « azerty cduco£#45 » ils auront tout les deux des hachages différents

# INFO

La différence entre chiffrement bijectif et le hachage : Le chiffrement bijectif permet de transformer des données de manière réversible, tandis que le hachage est un processus unidirectionnel qui produit une empreinte (valeur de hachage) des données, mais ne permet pas de les retrouver à partir de cette empreinte.

Les limites du hachage des mots de passe: Etant donné que le mot de passe entier est utilisé pour générer le hachage, il n'existe aucune limite de longueur de mot de passe lorsque des algorithmes de hachage de mot de passe sont utilisés pour chiffrer le mot de passe



# TRUECRYPT

# TRUECRYPT

Truecrypt est un logiciel de chiffrement à la  volée (consiste à rattacher un volume chiffré à l'arborescence du système de fichiers comme s'il était un périphérique amovible. Cela rend son contenu accessible de la même manière que le contenu des volumes non chiffrés) , il permet  de créer des disques virtuels chiffrés dans des fichiers, ainsi que de chiffrer des partitions ou des périphériques comme des clés USB. Le chiffrement est automatique, en temps réel et transparent, il se distingue donc des autres logiciels.

L'intérêt serait donc d'utiliser ce logiciel au sein des entreprises serait:

-Possibilité d'utilisation sur tout type d'OS et basculer
-Stockages chiffré de données facile et pratique
-Création  de volumes chiffrés de différentes tailles et leur montage comme des disques virtuels
-Garantit une sécurité renforcée des données sensible en les chiffrant avant de les stocker
-Simplifie l'accès aux données tout en maintenant un haut niveau de sécurité
-Le chiffrement protège contre les logiciels malveillants et les cyberattaques
-Les administrateurs peuvent gérer les accès aux données chiffrées ce qui assure la sécurité des données sensible de l'entreprise

# TRUECRYPT

Le problème est que Truecrypt n’est plus maintenu depuis 2014 et donc les attaques et la technologie est avancé et il existe d’autre logiciel alternatives a Truecrypt :

Pour Windows:
-Veracrypt est un logiciel utilitaire sous licence libre utilisé pour le chiffrement à la volée

-DiskCryptor solution de chiffrement ouverte qui offre le chiffrement de toutes les partitions de disque, y compris la partition système.

-Bitlocker spécification de protection des données développée par Microsoft, et qui fournit le chiffrement de partition.

-Cryptomator logiciel libre à code source ouvert de chiffrement à la volée multi-plateformes

-File Lock PEA utilitaire de chiffrement qui vous permet de protéger vos fichiers et répertoires à l'aide d'un mot de passe.

-GNU Privacy Guard implémentation open source du célèbre Pretty Good Privacy (PGP). GnuPG est un outil de chiffrement de volume et de fichiers grâce à une douzaine de systèmes de cryptage différents. Grâce au chiffrement et aux serveurs de clés publiques, GnuPG est un formidable outil de communication chiffré

# SOLUTION DE CHIFFREMENT

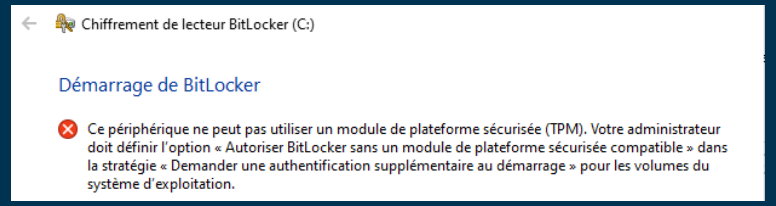
# Bitlocker

# Bitlocker

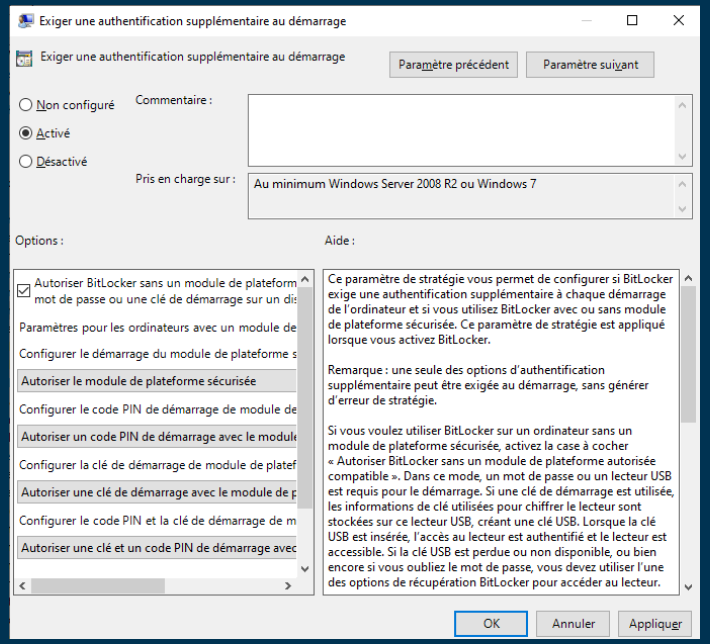
BitLocker est  un produit Microsoft de chiffrement conçu pour protéger les données utilisateur sur un ordinateur, le problème est que Bitlocker ne peut être disponible que sur la version  Windows professionnel .

# Bitlocker

Avant de chiffrer vous risquez de rencontrer un problème comme celui-ci :




Pour résoudre ce problème vous devez activer l'authentification supplémentaire au démarrage
Et le problème sera régler




Pour faire ceci:
-Editeurs de stratégie de groupe locale -> Composants Windows -> Chiffrement de lecteur Bitlocker -> Lecteurs du système d'exploitation -> Exiger une authentification supplémentaire au démarrage

# Bitlocker

| Avantages | Inconvénients |
| --- | --- |
| Protection des données | Oubli du mot de passe |
| Intégration à Windows | Perte de la clé de récupération |
| Prise en charge des clés de récupération | Complexité |
| Conformité réglementaire | Failles potentielles de sécurité |
| | Disponible que sur Windows Pro |

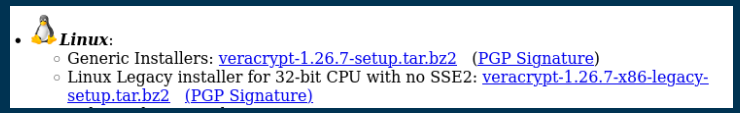
# VeraCrypt

# VeraCrypt

VeraCrypt est un logiciel utilitaire sous licence libre utilisé pour le chiffrement à la volée (OTFE). Il est développé par la société française IDRIX2 et permet de créer un disque virtuel chiffré dans un fichier ou une partition. L'ensemble du dispositif de stockage demande une authentification avant de monter le disque virtuel

Pour installer VeraCrypt, allez dans le terminale de commande et puis:

-Apt update (mettre à jour les paquets)
-Copier sur le site VeraCrypt le lien de téléchargement et faites un wget (https://launchpad.net/veracrypt/trunk/1.26.7/+download/veracrypt-1.26.7-setup.tar.bz2

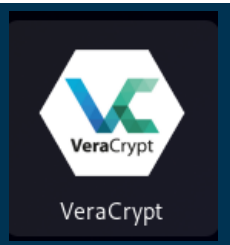



-Ensuite dézippé le fichier à l'aide la commande

```
root@linux:~# sudo tar -jxvf veracrypt-1.24-Update7-setup.tar.bz2
```

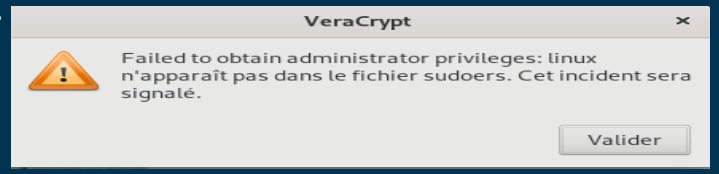
-Installer VeraCrypt

```
root@linux:~# sudo ./veracrypt-1.24-Update7-setup-gui-x64
```



# VeraCrypt

Il y a un problème que vous pouvez rencontrer comme moi lors du lancement de VeraCrypt, en effet votre utilisateur peut ne pas être pas reconnu pas reconnu en tant que superutilisateur et donc. Et donc vous ne pourrez pas utiliser le logiciel.



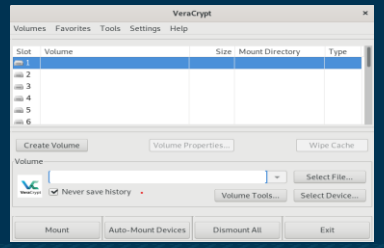

Pour régler ce souci, vous devez ajouté votre utilisateur a la liste des sudoers à l'aide de la *commande adduser linux sudo*

```
root@linux:~# adduser linux
adduser : L'utilisateur « linux » existe déjà.
root@linux:~# adduser linux sudo
Ajout de l'utilisateur « linux » au groupe « sudo »...
Adding user linux to group sudo
Fait.
```

A l'aide de la *commande Visudo*, donnez les droits à votre utilisateur en l'ajoutant

```
# User privilege specification
root    ALL=(ALL:ALL) ALL
linux   All=(ALL:ALL) ALL
```

Vous pouvez enfin accéder au logiciel



# VeraCrypt

| Avantages | Inconvénients |
| --- | --- |
| Gratuit pour tous les supports | Risque de problème de droits d’utilisateurs par moment |
| Simple d’utilisation | Devoir régler des problèmes de droit avant de pouvoir chiffrer un disque |
| Mode console et graphique disponible | |
| | |

# Notes techniques

Les notes techniques sont écrites dans un fichier PDF écrits en Markdown