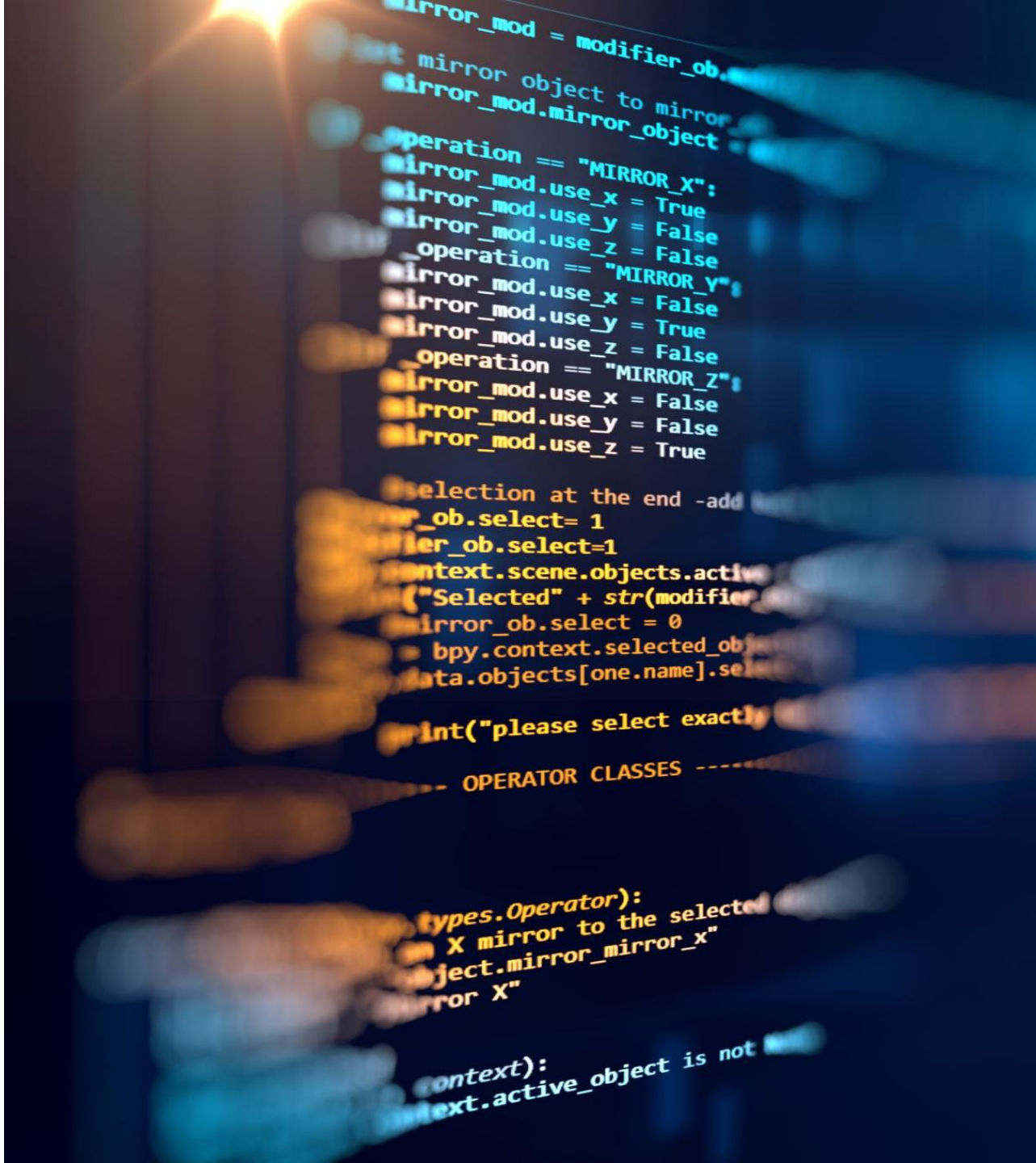
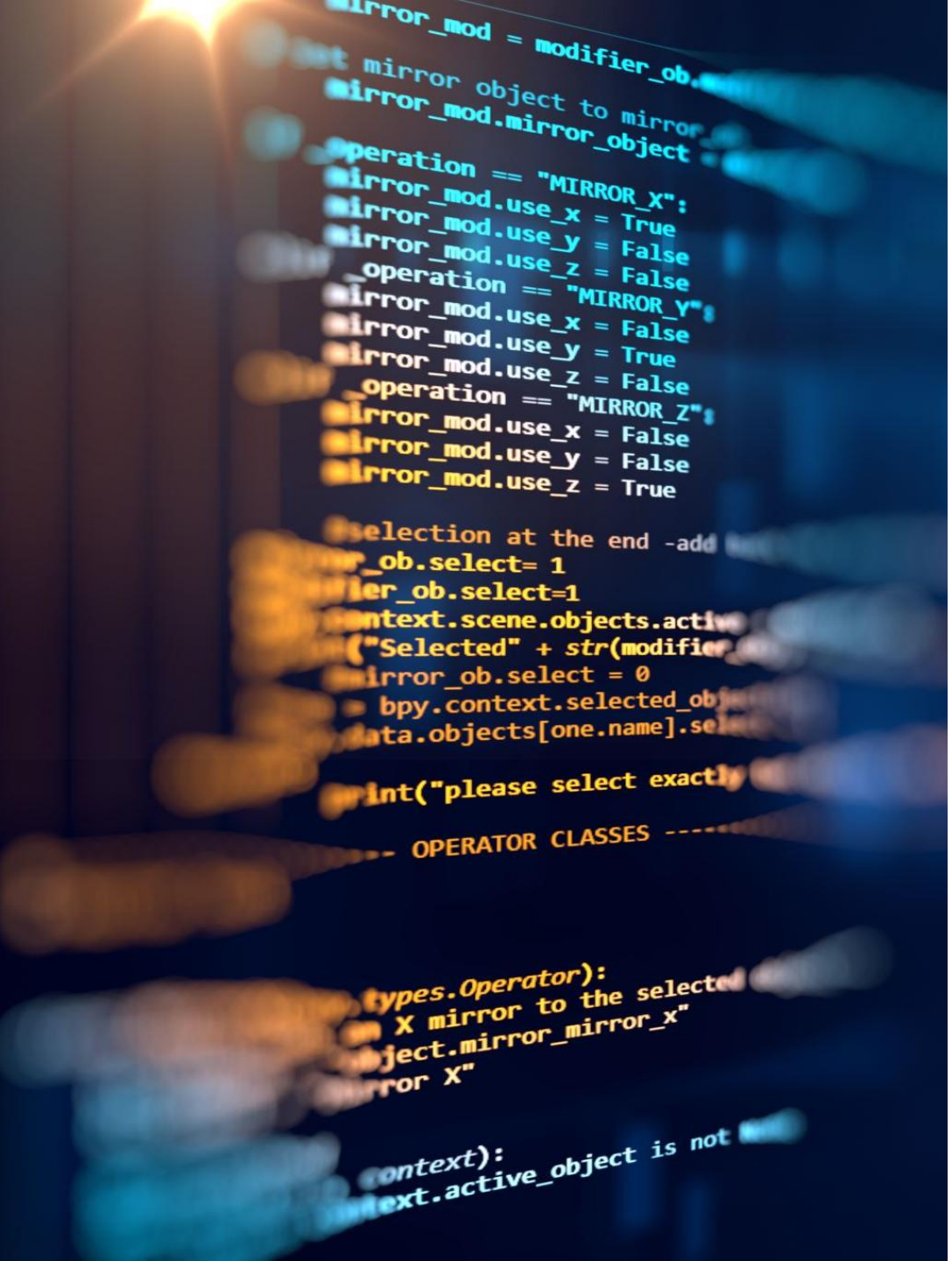
TP7 B3
Chiffrement

Florentin Bracq- -Flabat, BTS SIO 1

Le code César

- Le code César est un chiffrement par décalage, il peut être utilisé par exemple pour le chiffrement d'un texte
- Exemple :
- clair : ABCDEFGHIJKLMNOPQRSTUVWXYZ
- chiffré : DEFGHIJKLMNOPQRSTUVWXYZABC





Le Carré de Vigenère

- C’est un système de chiffrement par substitution polyalphabétique, qui peut être utilisé pour chiffrer un texte

La machine « Enigma »

- C’est une machine électromécanique portative qui a servi au chiffrement et déchiffrement d’informations, elle a été inventée par Arthur Scherbius,
- Cette machine a été utilisée pendant la 2ème guerre mondiale

Le téléphone rouge

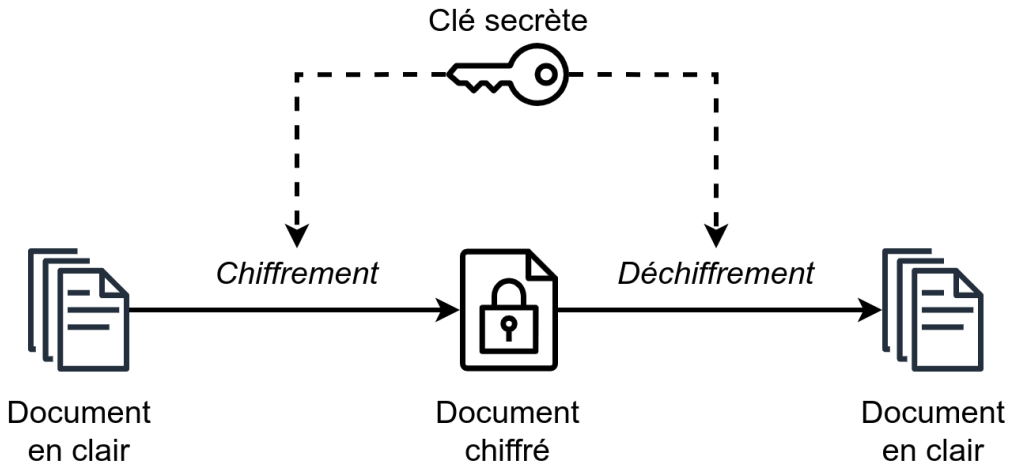
- Le téléphone rouge est une ligne de communication directe entre les États-Unis et l’Union soviétique

Le hachage

- Le hachage est une méthode de chiffrement qui permet de transformer des suites de caractères en hachages fixes et compacts
- Le hachage permet d’avoir une meilleure sécurité que le chiffrement, parce que les valeurs du hachage ne peuvent pas être reconverties à leur valeur d’origine sans clé

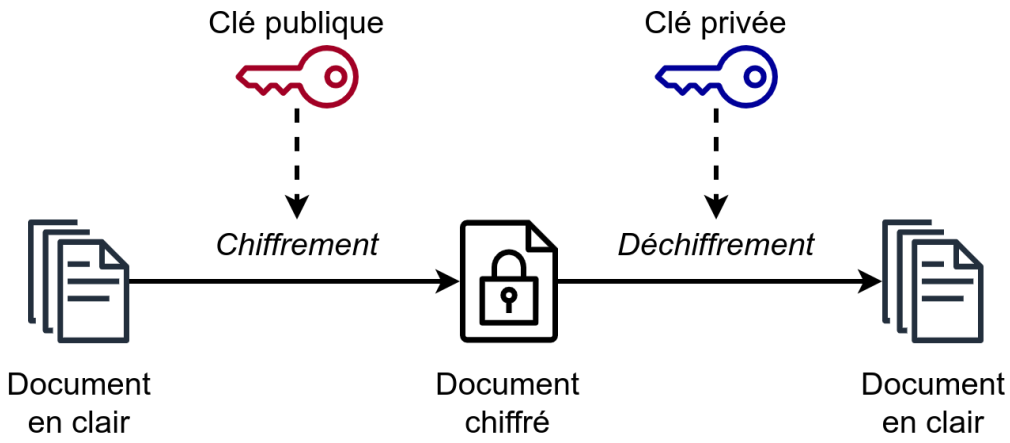
Le chiffrement à clé symétrique

Le chiffrement à clé symétrique, utilise la même clé pour le chiffrement et le déchiffrement, elle doit donc être partagée entre l'émetteur et le destinataire



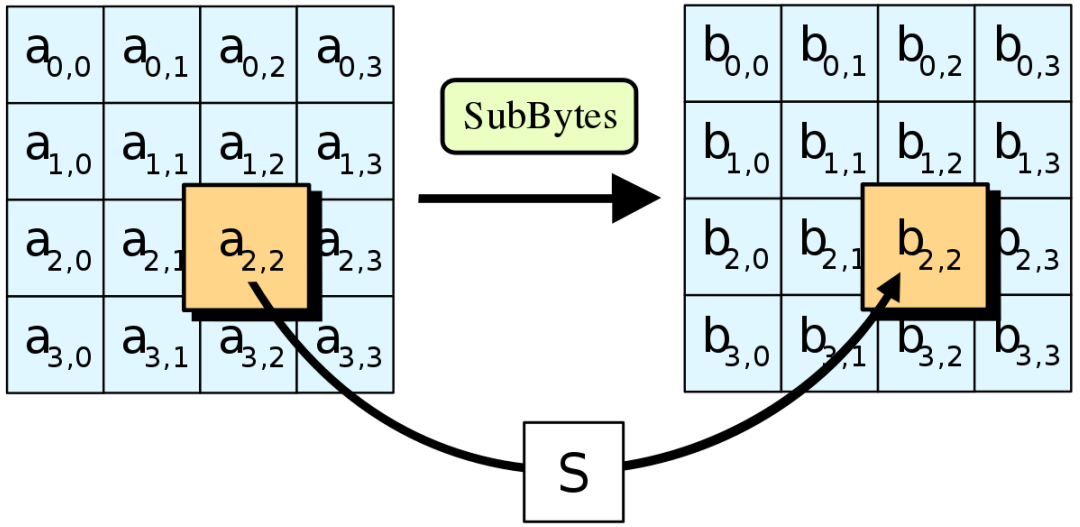
Le chiffrement à clé asymétrique

- Le chiffrement à clé asymétrique utilise deux clés, une clé publique et une clé privée
- La clé publique permet de chiffrer
- La clé privée permet de déchiffrer



Le chiffrement AES

- Le chiffrement AES, est un algorithme de chiffrement symétique, depuis octobre 2000, il est devenu la norme de chiffrement pour les organisations gouvernementales aux États-Unis



La différence entre chiffrement bijectif et hachage

- Le chiffrement bijectif permet de chiffrer et déchiffrer des données de manière réversible, et le hachage produit une empreinte numérique fixe des données d'entrée, mais est non réversible.

Les limites du hachage des mots de passe

- Les limites du hachage des mots de passe sont les attaques par force brute, les dictionnaires, ainsi que les vulnérabilités algorithmiques.

Le salage des mots de passe

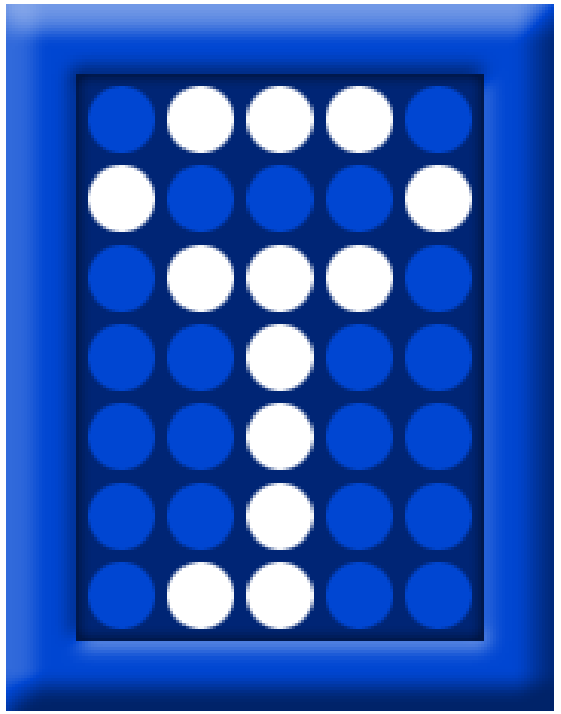
- Le salage des mots de passe est appelé password salt en anglais, consiste à ajouter une partie aléatoire dans le mot de passe avant de le donner à un algorithme de hachage,

La stéganographie

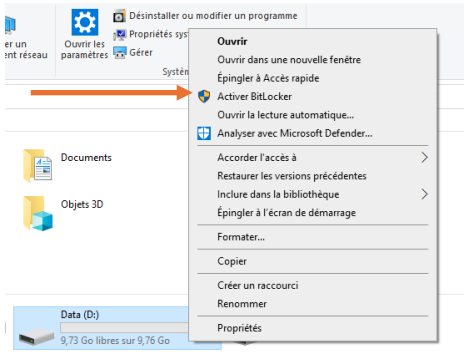
- C’est un domaine où on cherche à dissimuler discrètement de l’information, par exemple dans des images ou par exemple des fichiers audios
- La stéganographie est utilisée pour des raisons de confidentialité, de sécurité ou même à des fins malveillantes

Truecrypt

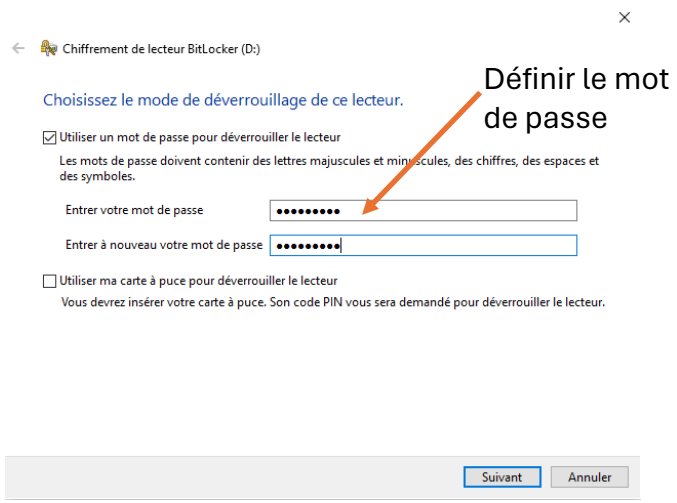
- TrueCrypt était un logiciel de chiffrement de disque utilisé pour sécuriser les données sensibles, il n’est plus développé ni maintenu depuis 2014
- TrueCrypt offre un chiffrement transparent et une portabilité des volumes sécurisés
- L’intérêt d’utiliser Truecrypt est d’offrir une flexibilité et une portabilité, et de contrôler l’accès aux données
- Alternatives : VeraCrypt, BitLocker, FileVault



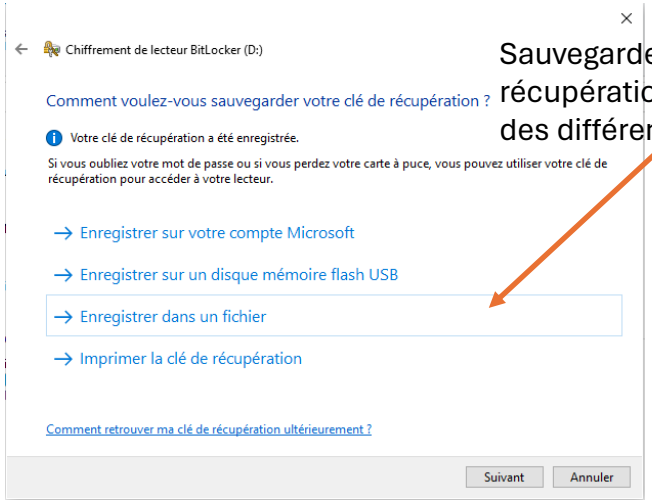
Mise en place de Bitlocker



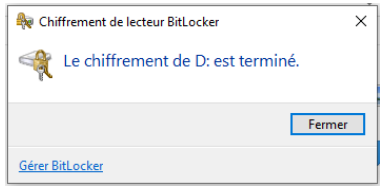
Cliquer sur le lecteur, puis cliquer sur Activer Bitlocker

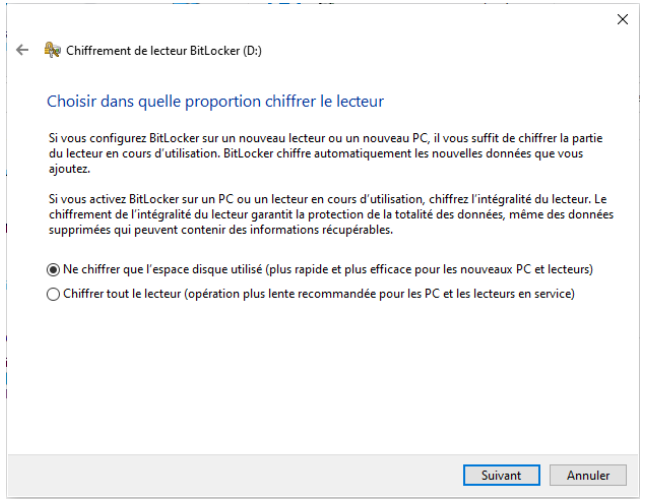


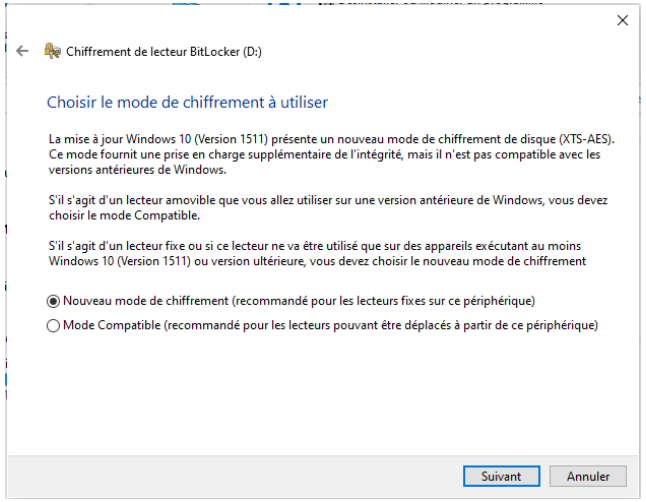
Définir le mot de passe

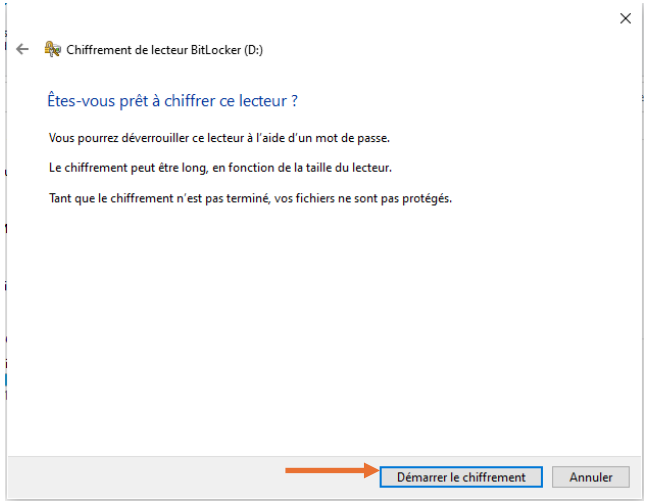


Sauvegarder la clé de récupération à l'aide des différentes options









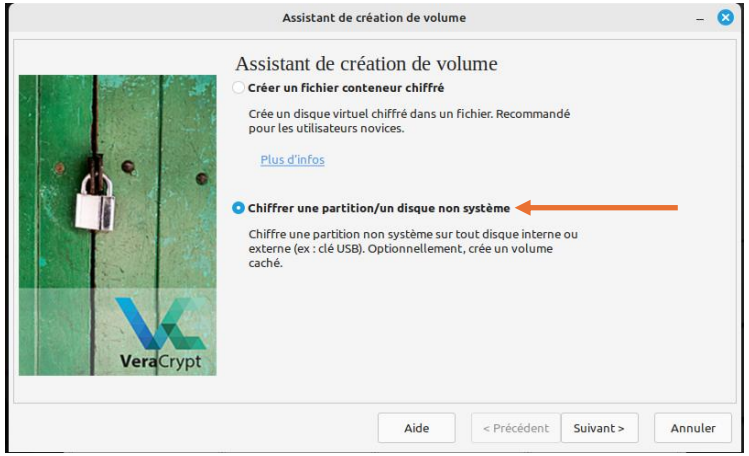
Installation de VeraCrypt

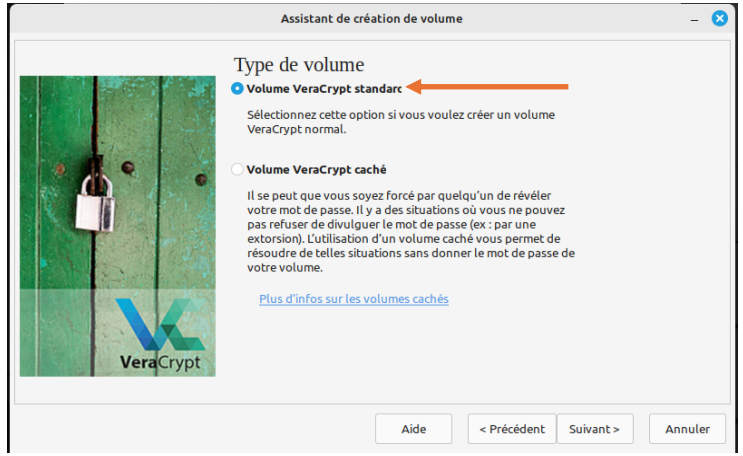
```
florentin@florentin-VirtualBox:~$ sudo add-apt-repository ppa:unit193/encryption
[sudo] Mot de passe de florentin :
Vous êtes sur le point d'ajouter le PPA suivant :
 https://www.veracrypt.fr/
VeraCrypt - Open source disk encryption with strong security for the Paranoid, based on TrueCrypt.

Debian and Rasbian builds: https://build.opensuse.org/project/show/home:unit193:veracrypt
 Plus de renseignements : https://launchpad.net/~unit193/+archive/ubuntu/encryption
Appuyez sur Entrée pour continuer ou Ctrl+C pour annuler

gpg: répertoire « /root/.gnupg » créé
gpg: le trousseau local « /root/.gnupg/pubring.kbx » a été créé
gpg: /root/.gnupg/trustdb.gpg : base de confiance créée
gpg: le trousseau local « /etc/apt/keyrings/3BFB8E06536B8753AC58A4A303647209B58A653A.keyring » a été créé
gpg: clef 03647209B58A653A : clef publique « Launchpad PPA for Unit 193 » importée
gpg: Quantité totale traitée : 1
gpg:               importées : 1
```

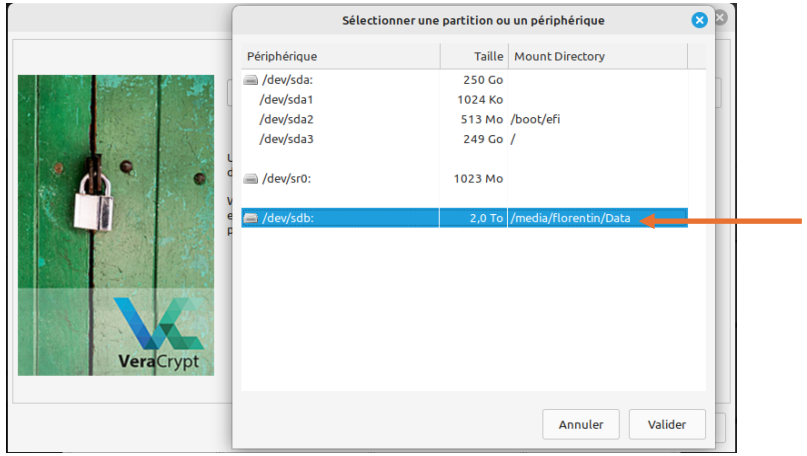
```
florentin@florentin-VirtualBox:~$ sudo apt-get update
Réception de :1 https://ppa.launchpadcontent.net/unit193/encryption/ubuntu jammy InRelease [23,8 kB]
Atteint :2 http://archive.ubuntu.com/ubuntu jammy InRelease
Réception de :3 http://archive.ubuntu.com/ubuntu jammy-updates InRelease [119 kB]
Réception de :4 https://ppa.launchpadcontent.net/unit193/encryption/ubuntu jammy/main amd64 Packages [620 B]
Atteint :5 http://archive.ubuntu.com/ubuntu jammy-backports InRelease
Réception de :6 https://ppa.launchpadcontent.net/unit193/encryption/ubuntu jammy/main Translation-en [480 B]
Réception de :7 http://security.ubuntu.com/ubuntu jammy-security InRelease [110 kB]
Ign :8 http://packages.linuxmint.com virginia InRelease
Réception de :9 http://archive.ubuntu.com/ubuntu jammy-updates/main i386 Packages [592 kB]
Atteint :10 http://packages.linuxmint.com virginia Release
Réception de :11 http://archive.ubuntu.com/ubuntu jammy-updates/main amd64 Packages [1 490 kB]
Réception de :12 http://archive.ubuntu.com/ubuntu jammy-updates/main Translation-en [288 kB]
Réception de :13 http://archive.ubuntu.com/ubuntu jammy-updates/restricted amd64 Packages [1 605 kB]
Réception de :14 http://archive.ubuntu.com/ubuntu jammy-updates/restricted Translation-en [268 kB]
Réception de :16 http://security.ubuntu.com/ubuntu jammy-security/main i386 Packages [421 kB]
Réception de :17 http://security.ubuntu.com/ubuntu jammy-security/main amd64 Packages [1 246 kB]
Réception de :18 http://security.ubuntu.com/ubuntu jammy-security/main Translation-en [225 kB]
Réception de :19 http://security.ubuntu.com/ubuntu jammy-security/universe amd64 Packages [851 kB]
Réception de :20 http://security.ubuntu.com/ubuntu jammy-security/universe i386 Packages [599 kB]
Réception de :21 http://security.ubuntu.com/ubuntu jammy-security/universe Translation-en [162 kB]
8 000 ko réceptionnés en 2s (4 402 ko/s)
Lecture des listes de paquets... Fait
```

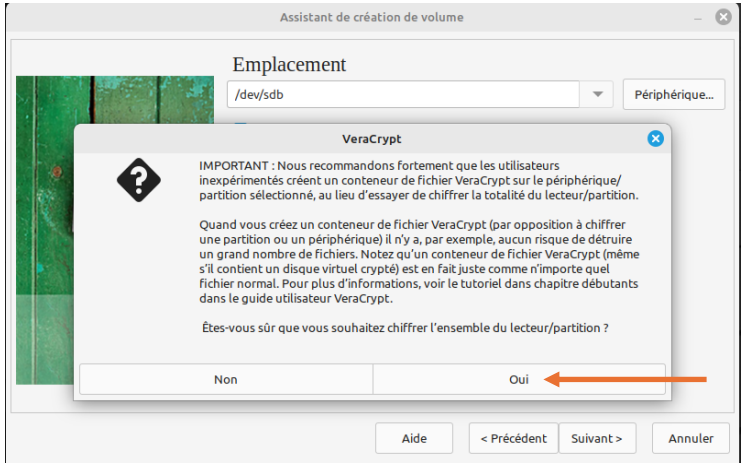
```
florentin@florentin-VirtualBox:~$ sudo apt-get install veracrypt
Lecture des listes de paquets... Fait
Construction de l'arbre des dépendances... Fait
Lecture des informations d'état... Fait
Les paquets supplémentaires suivants seront installés :
  libwxbase3.0-0v5 libwxgtk3.0-gtk3-0v5
Les NOUVEAUX paquets suivants seront installés :
  libwxbase3.0-0v5 libwxgtk3.0-gtk3-0v5 veracrypt
0 mis à jour, 3 nouvellement installés, 0 à enlever et 1 non mis à jour.
Il est nécessaire de prendre 11,9 Mo dans les archives.
Après cette opération, 44,9 Mo d'espace disque supplémentaires seront utilisés.
Souhaitez-vous continuer ? [O/n] o
Réception de :1 http://archive.ubuntu.com/ubuntu jammy/universe amd64 libwxbase3.0-0v5 amd64 3.0.5.1+dfsg-4 [881 kB]
Réception de :2 https://ppa.launchpadcontent.net/unit193/encryption/ubuntu jammy/main amd64 veracrypt amd64 1.26.7-0vanir1~bpo22.04 [6 612 kB]
Réception de :3 http://archive.ubuntu.com/ubuntu jammy/universe amd64 libwxgtk3.0-gtk3-0v5 amd64 3.0.5.1+dfsg-4 [4 368 kB]
11,9 Mo réceptionnés en 3s (3 999 ko/s)
Sélection du paquet libwxbase3.0-0v5:amd64 précédemment désélectionné.
(Lecture de la base de données... 567430 fichiers et répertoires déjà installés.)
Préparation du dépaquetage de .../libwxbase3.0-0v5_3.0.5.1+dfsg-4_amd64.deb ...
Dépaquetage de libwxbase3.0-0v5:amd64 (3.0.5.1+dfsg-4) ...
Sélection du paquet libwxgtk3.0-gtk3-0v5:amd64 précédemment désélectionné.
Préparation du dépaquetage de .../libwxgtk3.0-gtk3-0v5_3.0.5.1+dfsg-4_amd64.deb ...
Dépaquetage de libwxgtk3.0-gtk3-0v5:amd64 (3.0.5.1+dfsg-4) ...
Sélection du paquet veracrypt précédemment désélectionné.
Préparation du dépaquetage de .../veracrypt_1.26.7-0vanir1~bpo22.04_amd64.deb ...
Dépaquetage de veracrypt (1.26.7-0vanir1~bpo22.04) ...
Paramétrage de libwxbase3.0-0v5:amd64 (3.0.5.1+dfsg-4) ...
Paramétrage de libwxgtk3.0-gtk3-0v5:amd64 (3.0.5.1+dfsg-4) ...
Paramétrage de veracrypt (1.26.7-0vanir1~bpo22.04) ...
update-rc.d: warning: start and stop actions are no longer supported; falling back to defaults
Traitement des actions différées (« triggers ») pour mailcap (3.70+nmu1ubuntu1) ...
Traitement des actions différées (« triggers ») pour desktop-file-utils (0.26+mint3+victoria) ...
Traitement des actions différées (« triggers ») pour doc-base (0.11.1) ...
Traitement de 1 fichier de documentation ajouté…
Traitement des actions différées (« triggers ») pour gnome-menus (3.36.0-1ubuntu3) ...
Traitement des actions différées (« triggers ») pour libc-bin (2.35-0ubuntu3.6) ...
Traitement des actions différées (« triggers ») pour man-db (2.10.2-1) ...
Traitement des actions différées (« triggers ») pour shared-mime-info (2.1-2) ...
florentin@florentin-VirtualBox:~$
```

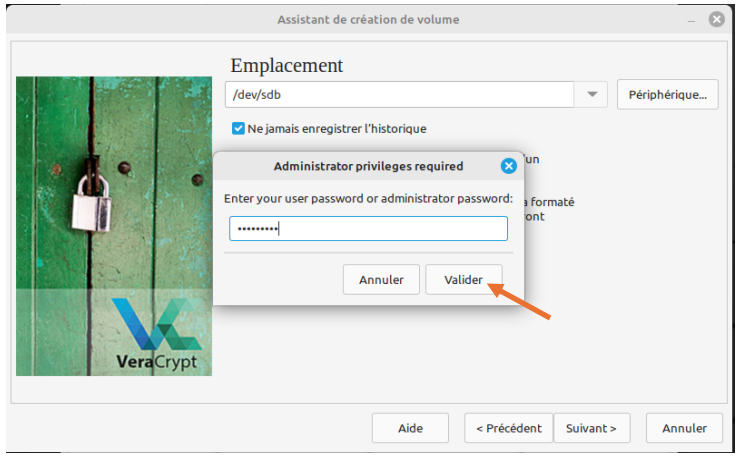
Mise en place de VeraCrypt

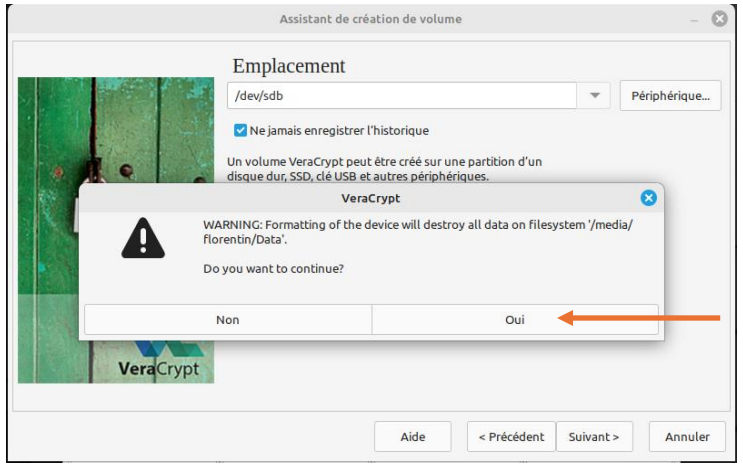












Suite mise en place de VeraCrypt