TP - Chiffrement

MATHIUS Baptiste

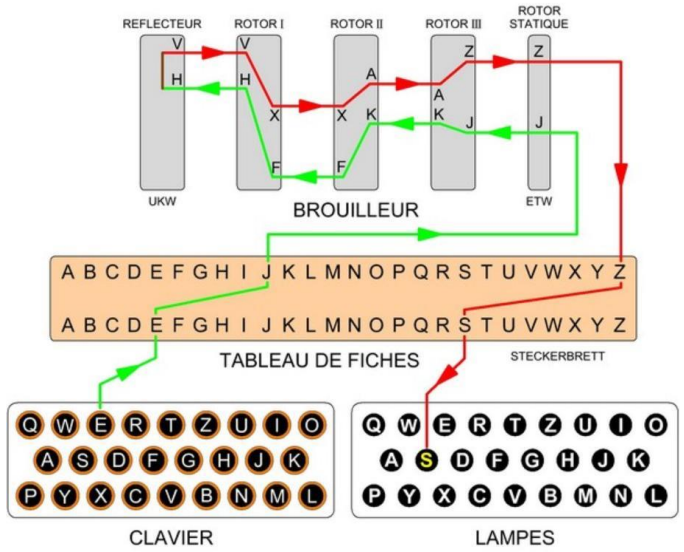
Étude et recherche

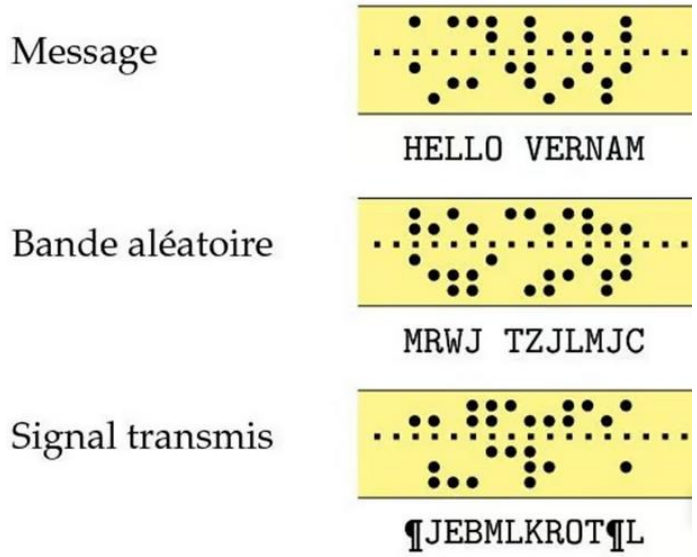
- Le code césar :
  - Aussi nommé chiffrement par décalage, cela fonctionne par le décalage des lettres de l'alphabet d'une distance de 3 lettres par exemple B devient E.
- Le carre de Vigenère :
  - L'idée est d'utiliser le cryptage césar avec un décalage de lettres en lettres, sous forme de tableau, en vert les lettres du mot en clair et en rouge, les lettres de notre clé.

	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

Étude et recherche

- La machine Enigma :
  - Lorsqu'on appuie sur la touche E du clavier, un courant électrique est envoyé dans le rotor et cela suit le câblage vert et cela ressort pour allumer la lettre S.
- Le téléphone rouge :
  - Cela se présente sous forme de bande perforée, avec 1 bande contenant le message, une bande aléatoire et la bande du signal transmis





Étude et recherche

- Le hachage
  - Généralement un algorithme de chiffrement qui va décomposer, résoudre et transformer les données de longueurs différentes en chaînes de longueurs égales.
- Le chiffrement à clé symétrique
  - Algorithme cryptographique qui va utiliser la même clé secrete pour le chiffrement et le déchiffrement d'un message, c'est une clé partagée.
- Le chiffrement à clé asymétrique
  - Les données chiffrées par la clé publique peuvent uniquement être déchiffrée par la clé privée, la clé publique ne peut que chiffrer les données.

Étude et recherche

- Le chiffrement AES
  - Est un chiffrement symétrique, donc la même clé permet de chiffrer et déchiffrer le message.
- Différence entre chiffrement bijectif et hachage
  - Txt
- Les limites du hachage des mots de passe
  - Le hachage des mots de passe est une fonction à sens unique car il est impossible de faire l'inverse et de retrouver le mot de passe original à partir de sa forme hachée.

Étude et recherche

- Salage des mots de passe
  - Cela correspond à un fragment de données aléatoires ajouté au mot de passe avant qu'il passe dans l'algorithme de hachage et donc ne pas avoir 2 fois le même mot de passe haché.
- Stéganographie
  - Il s'agit de dissimulé des informations dans un autre message ou objet pour cacher tout type de contenu numérique (images, texte, vidéos, contenu audio...), le contenu dissimulé peut être chiffré avant d'être introduit dans le message.

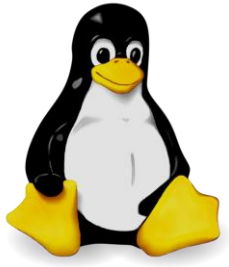
L'outil Truecrypt

- Truecrypt est un logiciel permettant de chiffrer à la volée nos données.
- Le principe de fonctionnement de Truecrypt est simple, il suffit d'installer l'outil et nous pouvons chiffrer une partition complète ou un périphérique USB.
- Le chiffrement est fait en temps réel pour une sécurité accrue.
- L'intérêt pour une entreprise d'utiliser Truecrypt est que c'est une solution gratuite et open source contrairement à d'autres

L'outil Truecrypt

- Disponible sur :



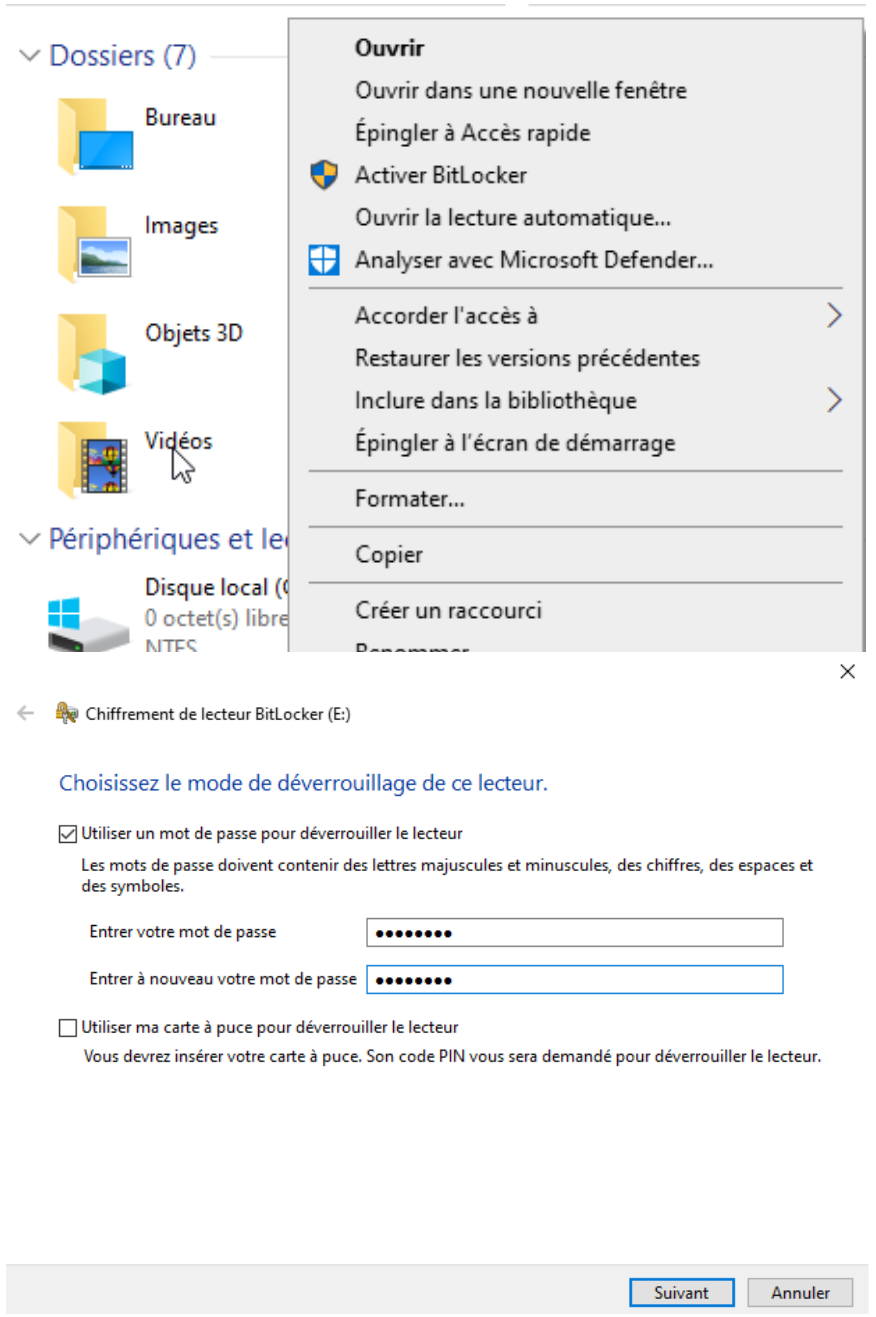


- Bien que cet outil soit plus qu'intéressant, il n'est plus maintenu depuis mai 2014.

- Alternatives à Truecrypt : Veracrypt, Bitlocker, FileVault 2,

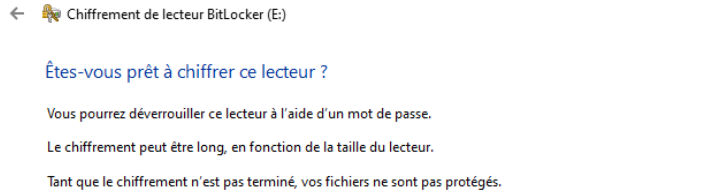
BitLocker

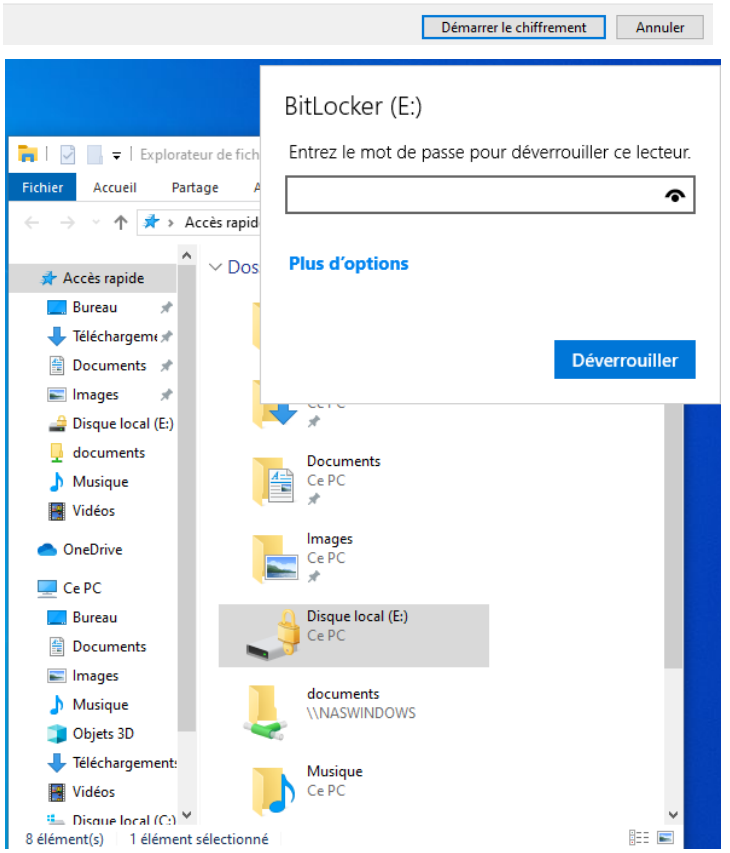
- Sur Windows, nous allons donc chiffrer une partition de disque avec BitLocker.
- On fait un clic droit sur la partition que l'on souhaite chiffrer et on clique sur **activer BitLocker.**
- On choisit l'option du mot de passe pour déverrouiller le lecteur.



BitLocker

- Après avoir cliqué sur suivant, nous arrivons la dessus, on clique sur **Démarrer le chiffrement.**
- Ensuite, on redémarre notre machine Windows.
- Et lorsqu'on veut accéder au disque, on nous demande notre mot de passe créer précédemment.

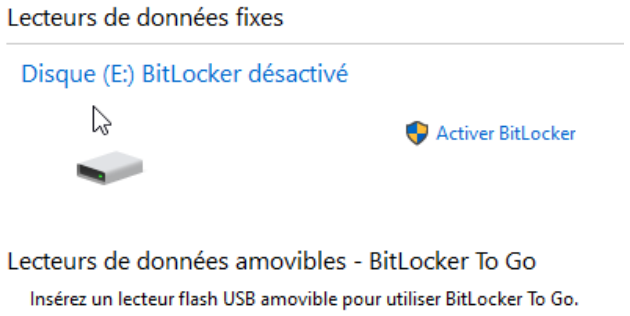


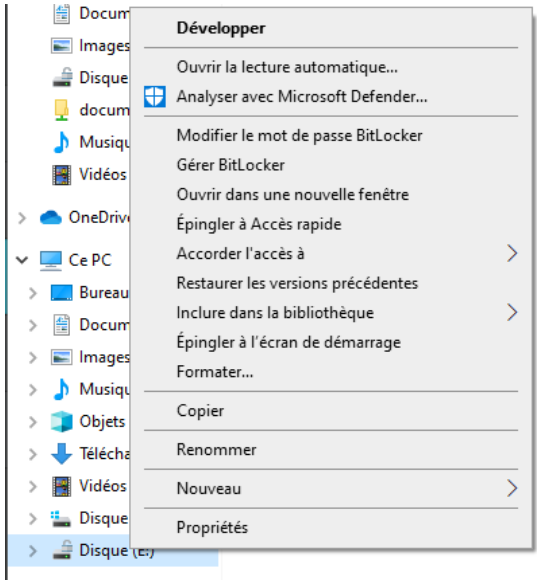


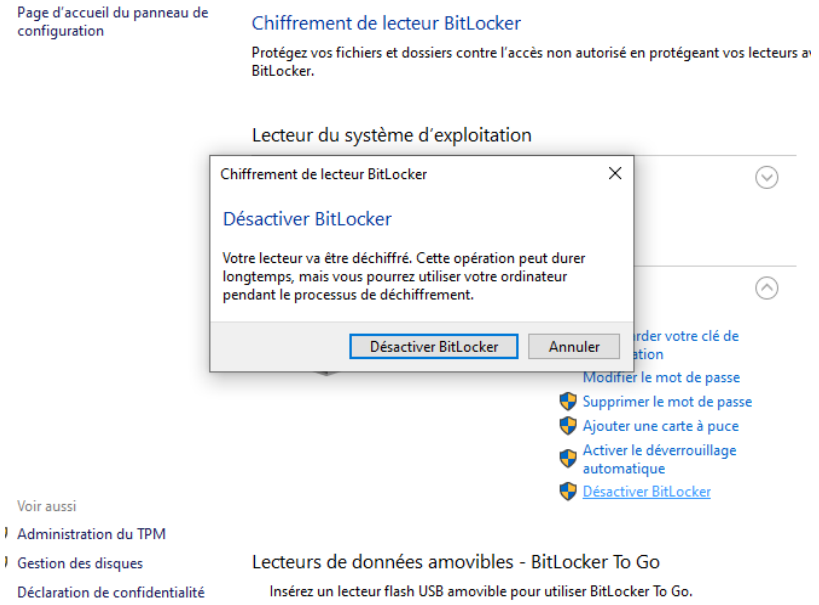
BitLocker

- Pour déchiffrer notre disque, nous pouvons accéder au disque et entrer le mot de passe ou bien désactiver le chiffrement par BitLocker.

- Puis on clique sur **Désactiver BitLocker**

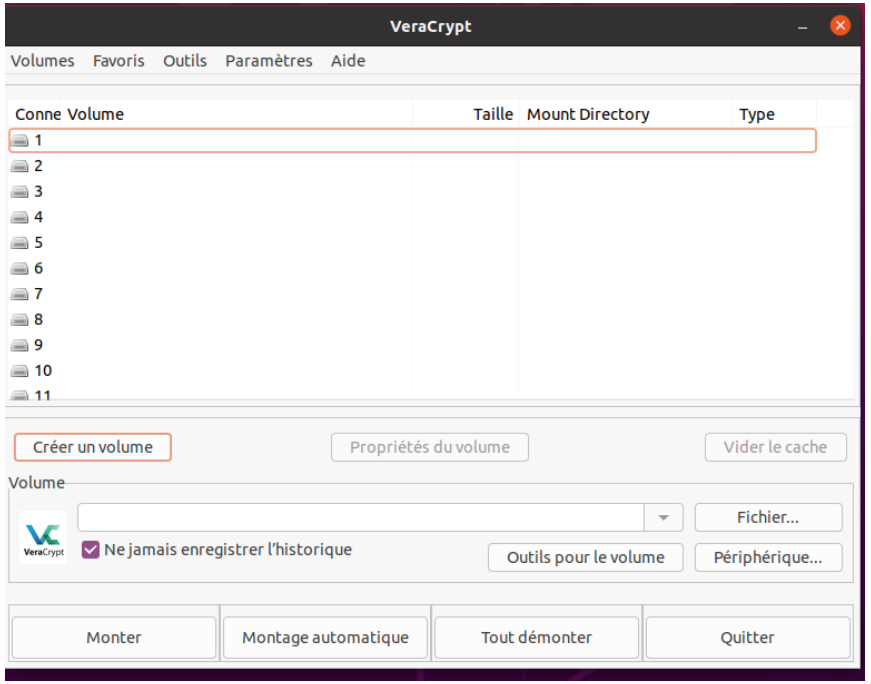


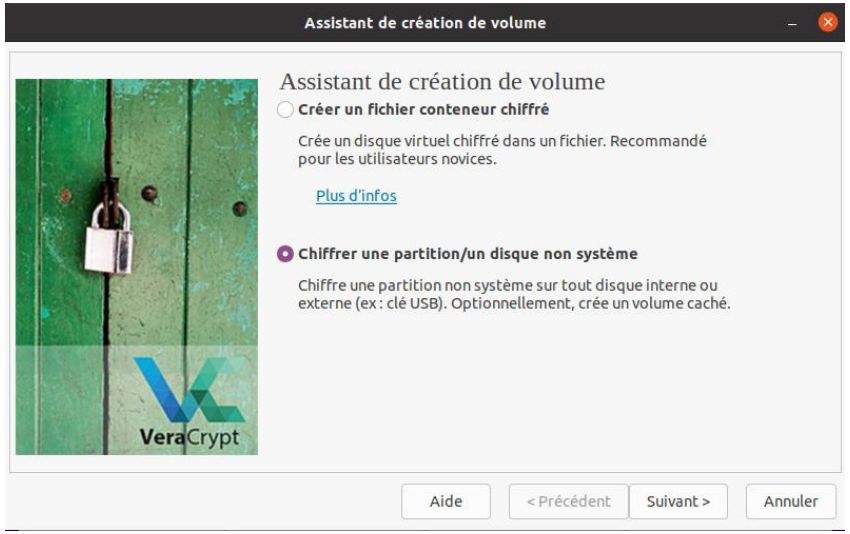




VeraCrypt

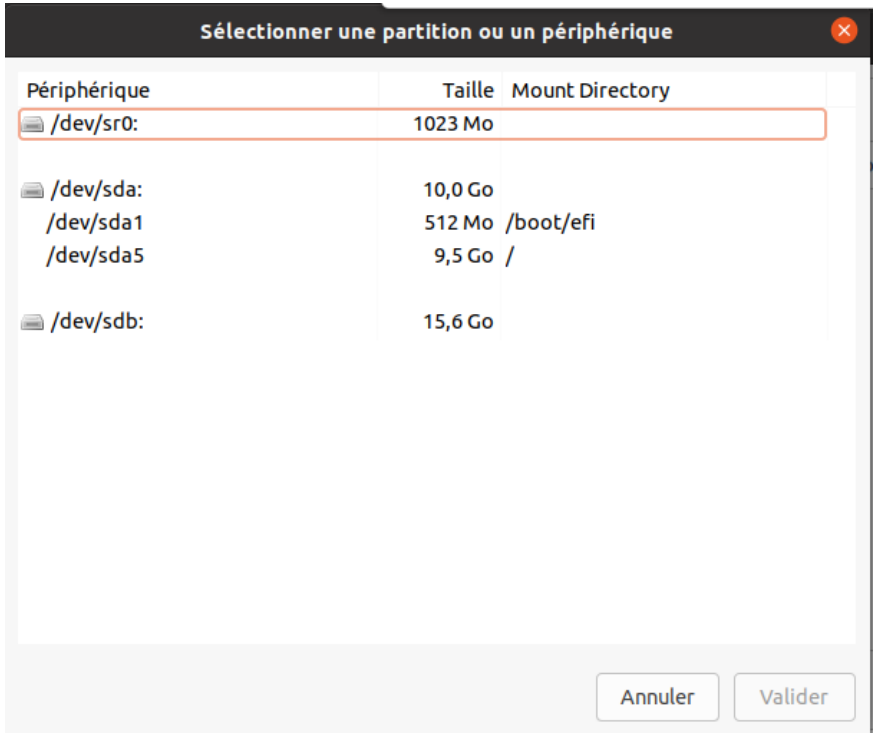
- Pour installer VeraCrypt, il faut être dans le terminal et taper **sudo apt install veracrypt**
- Ensuite on le décompresse et une fois dans le bureau on peut voir le logo de VeraCrypt.
- On lance VeraCrypt et on fait **créer un volume**
- On sélectionne la 2e option.





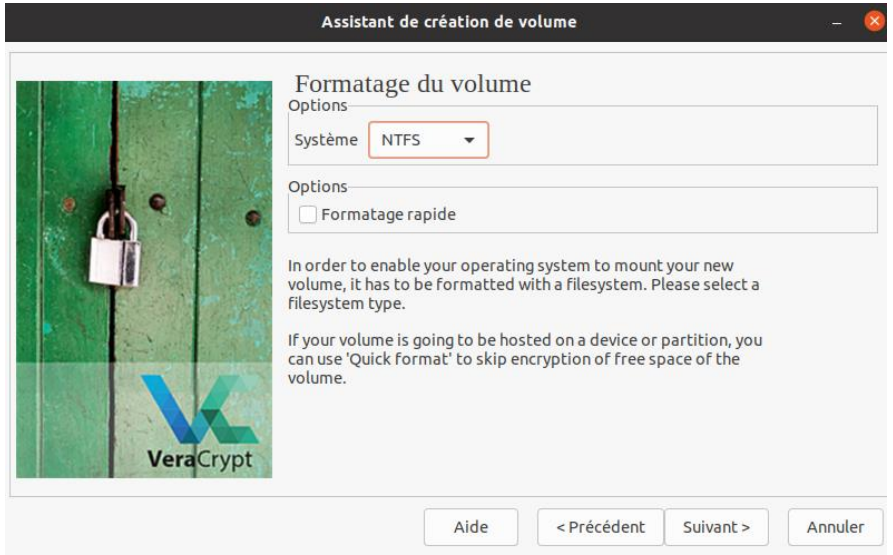
VeraCrypt

- On sélectionne notre disque que l'on veut chiffrer
- Puis on rentre le mot de passe



VeraCrypt

- Ensuite on choisit le formatage du volume que l'on souhaite



VeraCrypt

- Ensuite on sélectionne **monatge automatique,** on rentre notre mdp.
- Le volume créer précédemment est bien visible.
- Pour déchiffrer la partition, il suffit de sélectionner la partition et cliquer sur **Démonter**