

# TP– CHIFFREMENT

ZIZA KANGUE SARAH GÉNIVA

# 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 clair 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

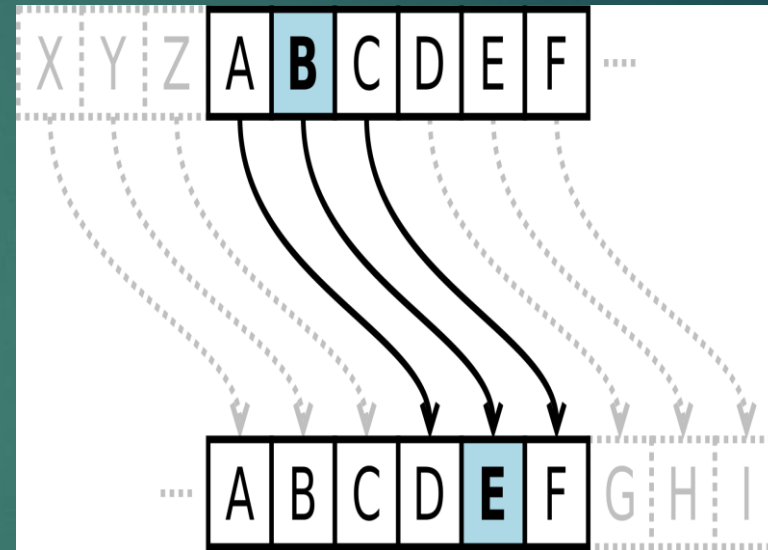
NB: longueur du décalage 3, constitue la *clé* du chiffrement

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

Décalage

	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

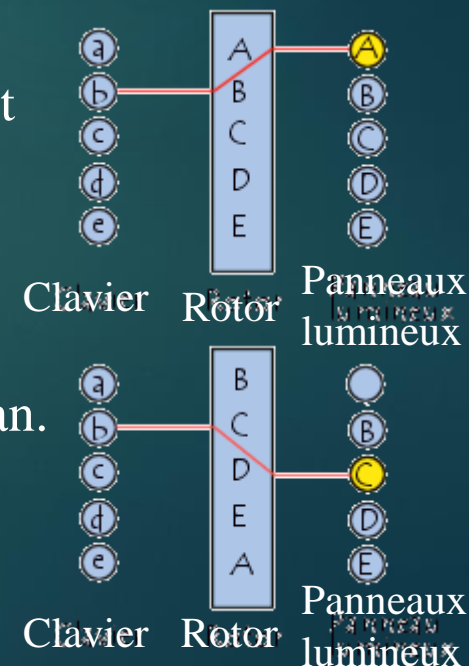
# La machine « Enigma »

**Enigma** est une machine électromécanique portable 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** symbole 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.

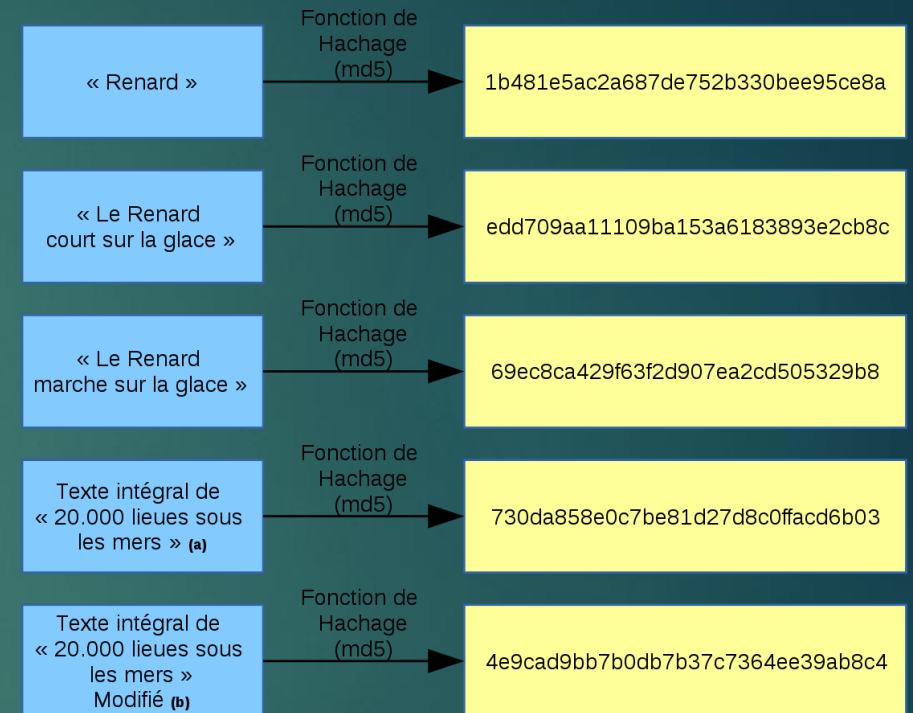
Cette dénomination de « téléphone rouge » est en réalité un raccourci lexical repris et popularisé par les médias occidentaux, la ligne étant au départ une ligne de téléscripteur, sa supposée couleur rouge symbolisant simplement le fait qu'il s'agissait d'une ligne d'urgence.



# 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

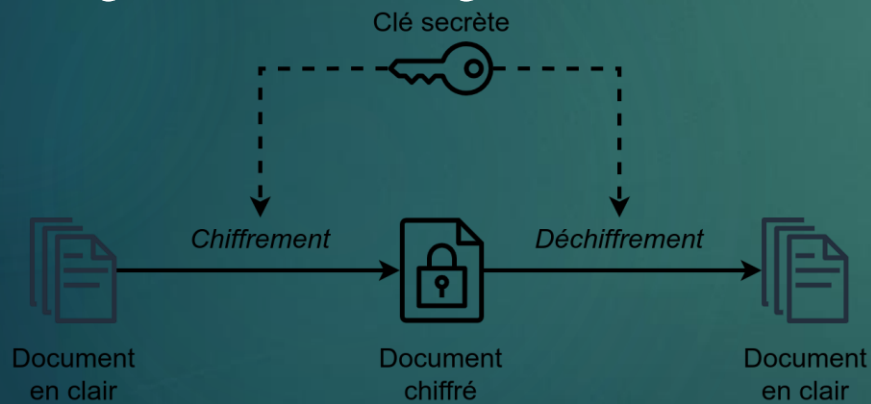
Son objectif principal est de permettre de ne pas stocker les mots de passe en clair dans la base mais uniquement de stocker une empreinte de ces derniers



# 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.

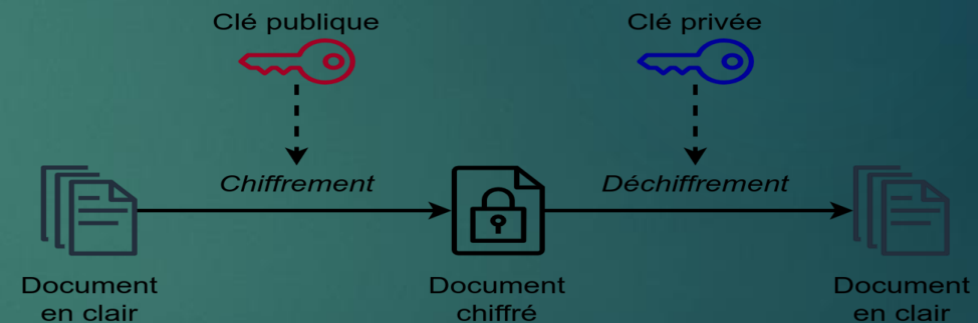
Ce terme est utilisé pour décrire les algorithmes de chiffrement qui utilisent une même clé pour le chiffage et le déchiffrement.



# 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 chiffement et une clé privée pour le déchiffrement, que seule une partie connaît.



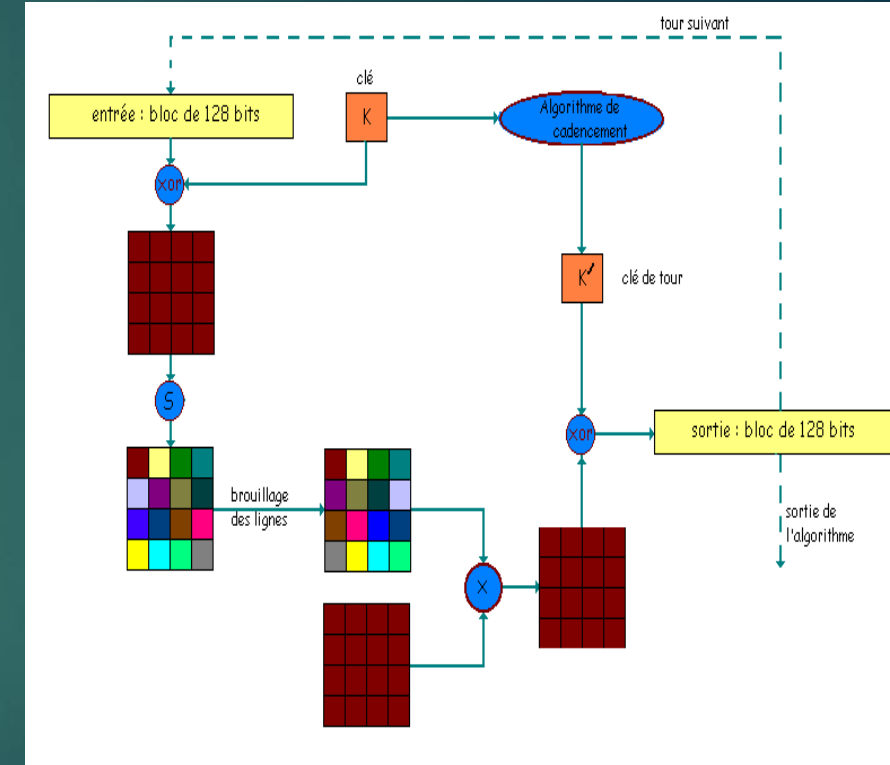
# Le chiffrement AES

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	$3,4 \times 10^{38}$
AES-192	192-bits	128	12	$6,2 \times 10^{57}$
AES-256	256-bits	128	14	$1,1 \times 10^{77}$





# 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.

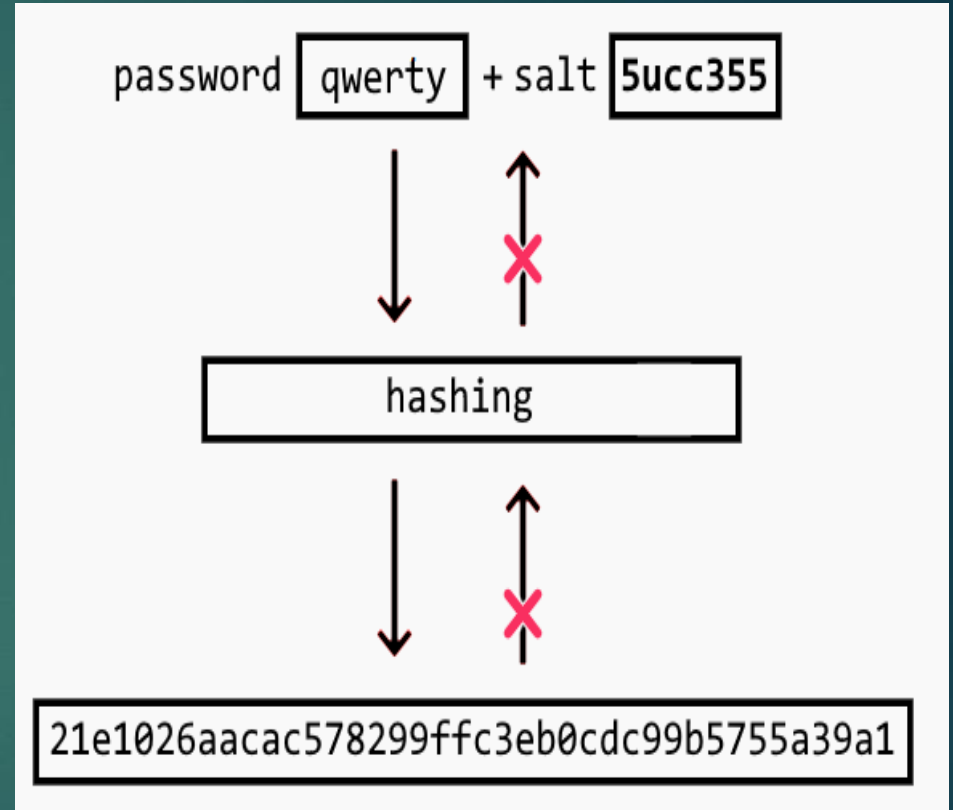
Consommation de la mémoire: le hachage des mots de passe est un processus qui nécessite beaucoup de mémoire.

# 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 média 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.

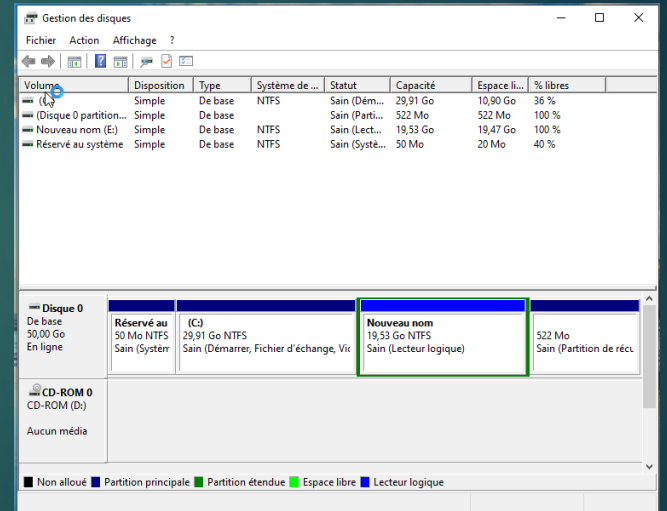
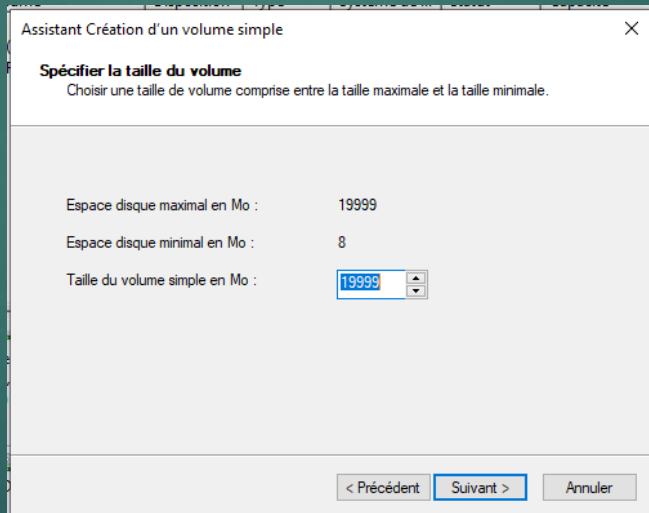
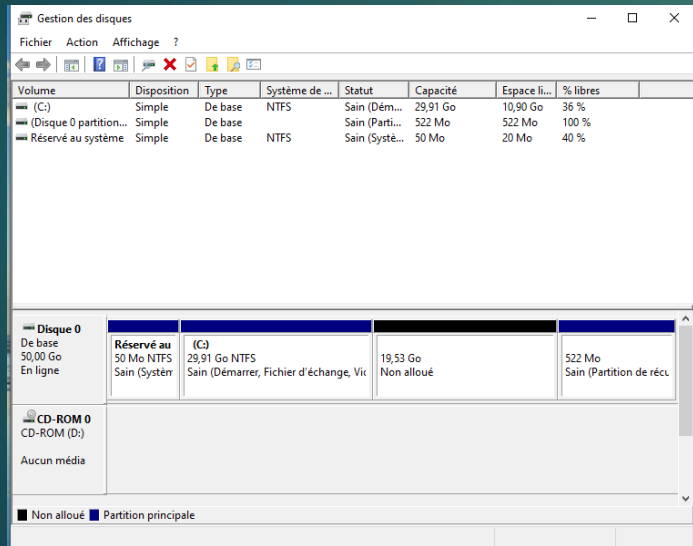
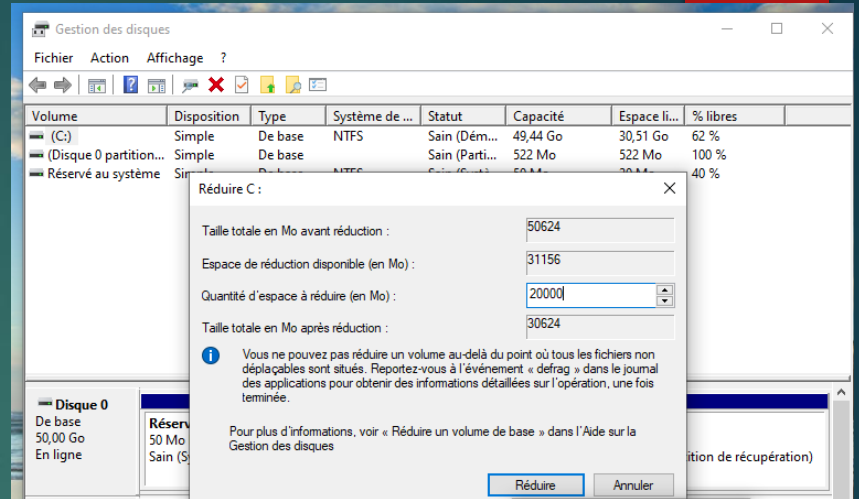
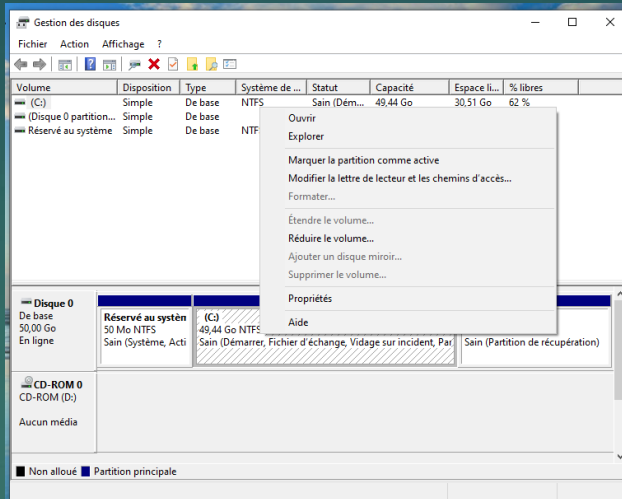
Il est possible de créer un disque virtuel chiffré contenu dans un fichier grâce au logiciel Truecrypt, puis de le monter comme un disque réel. En outre, cet instrument a la capacité de crypter une partition complète ou un dispositif tels qu'une clé USB ou un disque. On procède à ce chiffrement de façon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

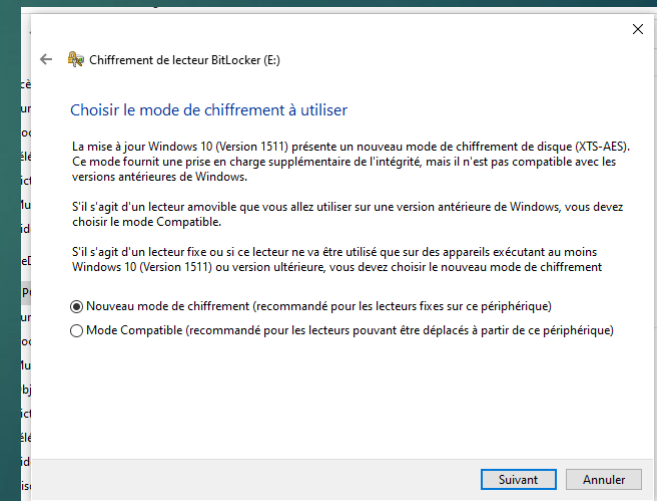
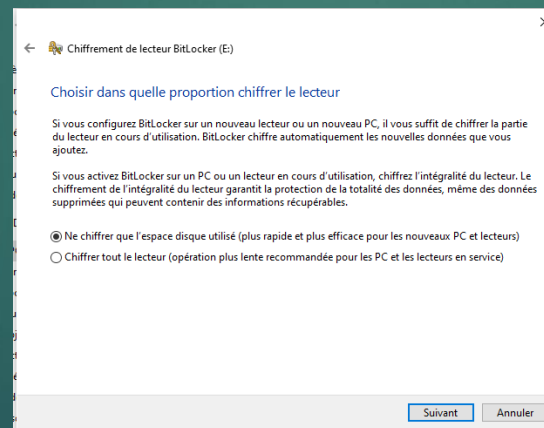
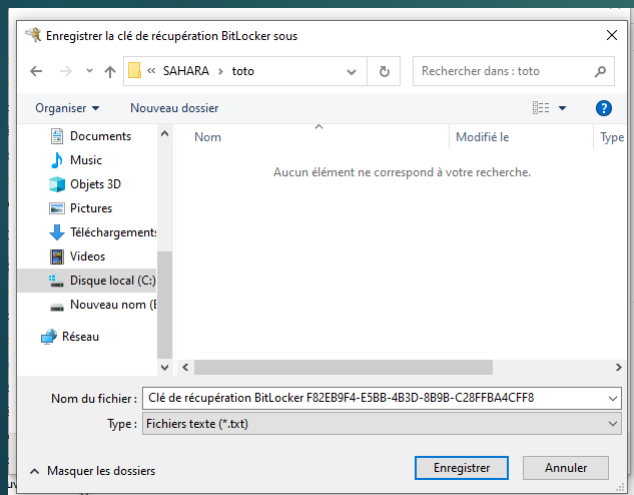
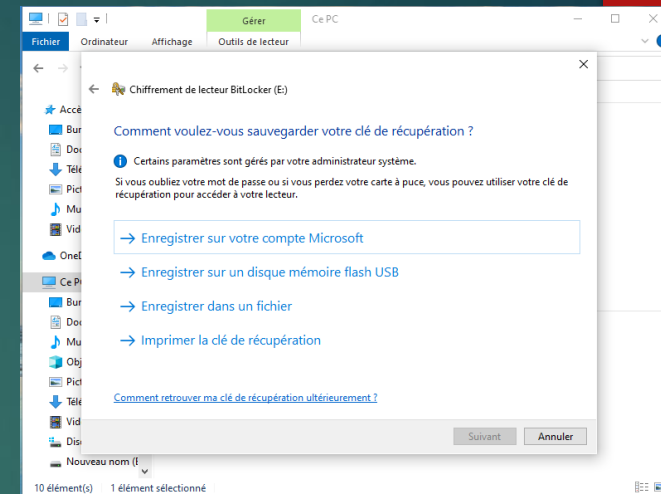
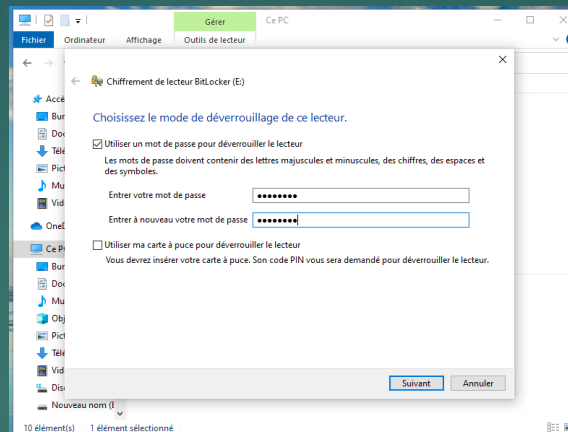
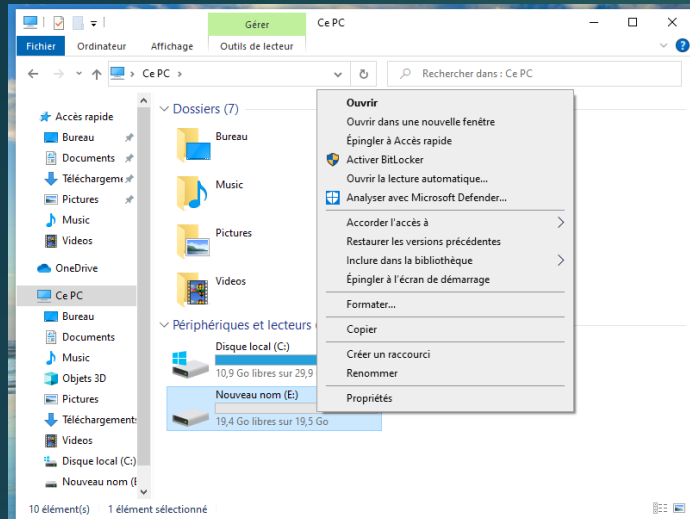
- Expliquer le principe de fonctionnement de TrueCrypt, et en particulier en quoi il est différent des autres outils « classiques » de chiffrement.

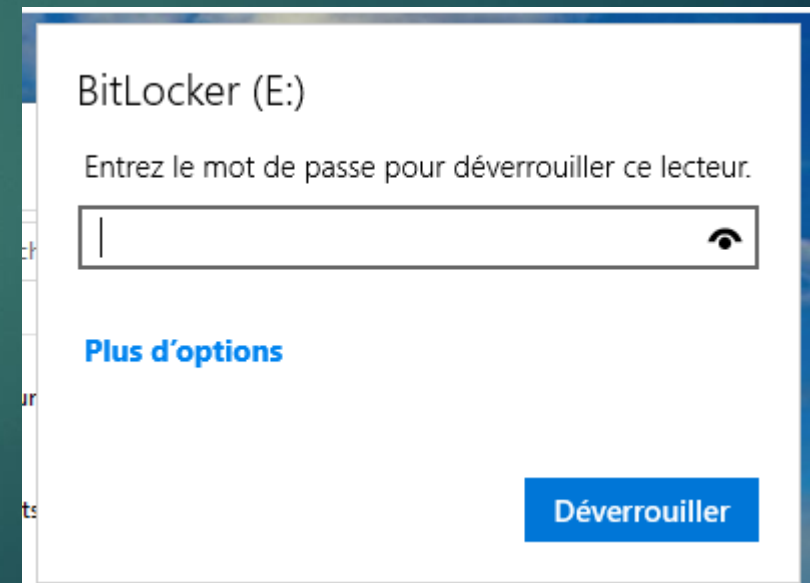
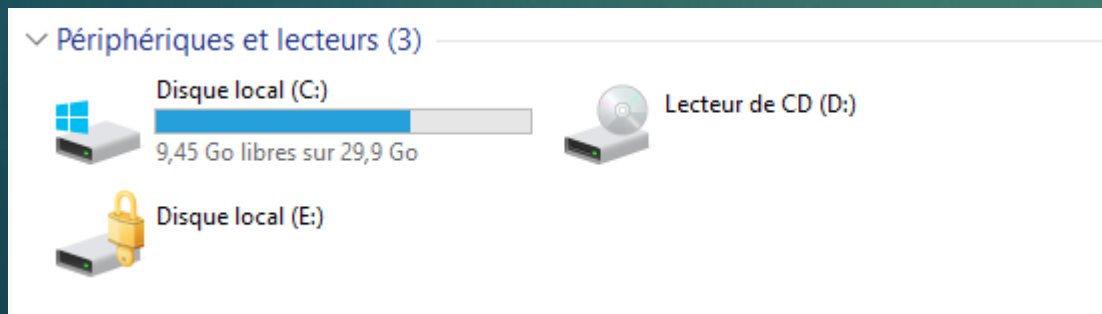
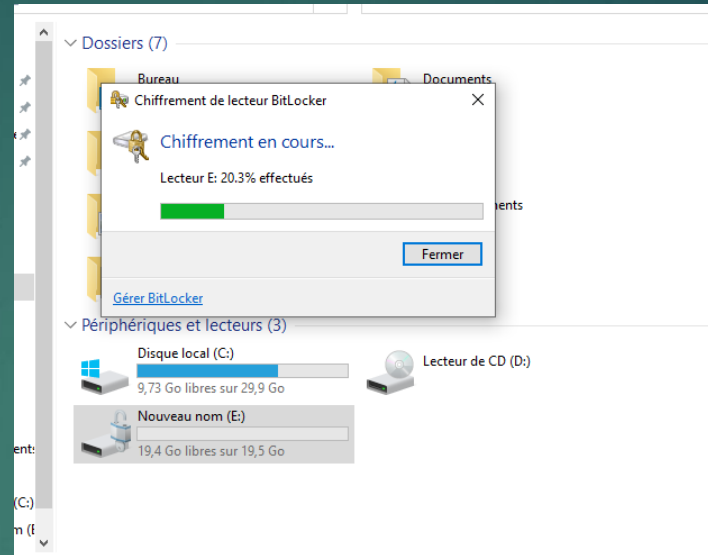
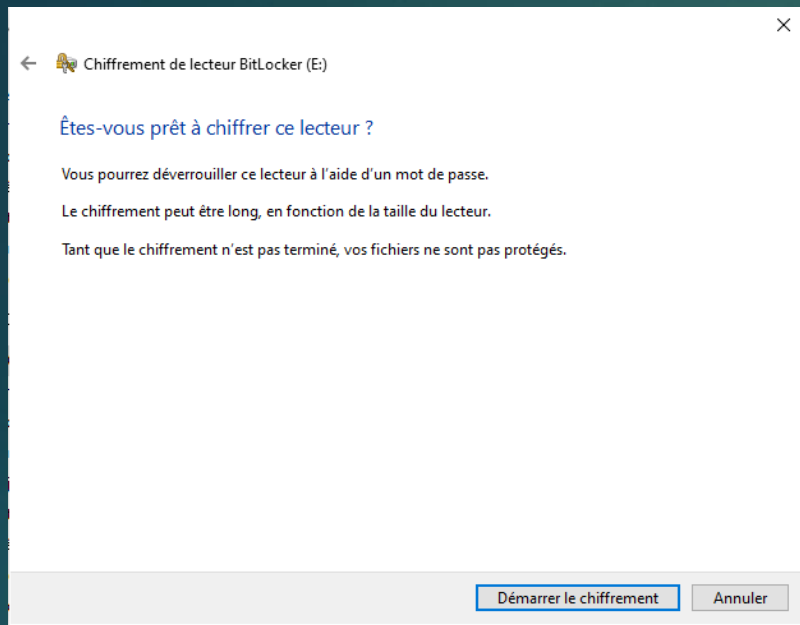
La particularité de TrueCrypt par rapport à d'autres outils de chiffrement traditionnels réside dans sa capacité à générer des volumes chiffrés de manière progressive à mesure que vous ajoutez des fichiers.

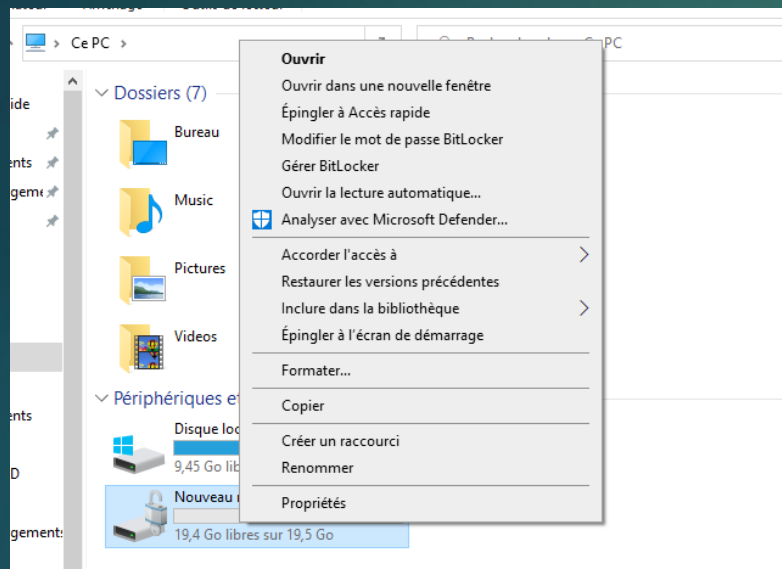
- 
- ▶ Concluez sur l'intérêt d'utiliser Truecrypt au sein d'une société.
  - ▶ Rechercher des solutions alternatives à Truecrypt.
    - VeraCrypt
    - Bitlocker
    - DiskCryptor
    - Ciphershed
    - FileVault 2
    - LUKS
    - AxCrypt











## Lecteurs de données fixes

Nouveau nom (E:) Chiffrement BitLocker en cours



- Sauvegarder votre clé de récupération
- Modifier le mot de passe
- Supprimer le mot de passe
- Ajouter une carte à puce
- Activer le déverrouillage automatique
- Désactiver BitLocker

## Chiffrement de lecteur BitLocker

Protégez vos fichiers et dossiers contre l'accès non autorisé en protégeant vos lecteurs avec BitLocker

### Lecteur du système d'exploitation

C: BitLocker désactivé

### Lecteurs de données fixes

Nouveau nom (E:) BitLocker désactivé



Activer BitLocker

### Chiffrement de lecteur BitLocker

#### Désactiver BitLocker

Votre lecteur va être déchiffré. Cette opération peut durer longtemps, mais vous pourrez utiliser votre ordinateur pendant le processus de déchiffrement.

Désactiver BitLocker

Annuler



- **Linux:**

- Generic Installers: [veracrypt-1.26.7-setup.tar.bz2](#) (PGP Signature)
- Linux Legacy installer for 32-bit CPU with no SSE2: [veracrypt-1.26.7-x86-legacy-setup.tar.bz2](#) (PGP Signature)
- Debian/Ubuntu packages:
  - Debian 12:
    - GUI: [veracrypt-1.26.7-Debian-12-amd64.deb](#) (PGP Signature) and [veracrypt-1.26.7-Debian-12-i386.deb](#) (PGP Signature)
    - Console: [veracrypt-console-1.26.7-Debian-12-amd64.deb](#) (PGP Signature) and [veracrypt-console-1.26.7-Debian-12-i386.deb](#) (PGP Signature)
  - Debian 11:
    - GUI: [veracrypt-1.26.7-Debian-11-amd64.deb](#) (PGP Signature)
    - Console: [veracrypt-console-1.26.7-Debian-11-amd64.deb](#) (PGP Signature)