CHIERENT



Raphaël ZAKRZEWSKI

• Code César : Chiffrement par décalage, exemple de décalage par 3 :

 Carré de Vigenère : On choisit une clé (ici « musique »), puis on cherche le croisement entre les colonnes (lettres du texte non chiffré) et les lignes (lettres de la clé) dans ce tableau :

Clé : musique Texte : J'adore éc	oute	er la radio toute la journée
Texte en clair Clé répétée	:	j'adore ecouter la radio toute la journee M USIQU EMUSIQU EM USIQU EMUSI QU EMUSIQU
		<pre> Colonne O, ligne I : on obtient la lettre W. Colonne D, ligne S : on obtient la lettre V. Colonne A, ligne U : on obtient la lettre U. Colonne J, ligne M : on obtient la lettre V.</pre>
Le texte chiffré est al	ors	:
V'UVWHY IOIMBU	IL PI	M LSLYI XAOLM BU NAOJVUY.



											L	.ett	re (en (clai	r										
	Α	в	С	D	Е	F	G	н	Т	J	ĸ	L	М	Ν	0	Ρ	Q	R	s	т	U	۷	w	х	Y	z
Lettre de la clé	Let	tres	s ch	iffré	es	(au	cro	iser	nen	t de	la (colo	onne	e Le	ettre	en	cla	ir e	t de	la I	igne	e Le	ettre	e de	la d	clé)
Α	Α	в	С	D	Е	F	G	Н	Т	J	ĸ	L	М	Ν	0	Ρ	Q	R	s	Т	U	۷	W	х	Y	Ζ
в	в	С	D	Е	F	G	н	Т	J	к	L	М	Ν	0	Ρ	Q	R	s	Т	U	v	w	х	Y	Ζ	Α
С	С	D	Е	F	G	Н	Т	J	к	L	М	Ν	0	Ρ	Q	R	s	Т	U	v	w	х	Y	Ζ	Α	в
D	D	Е	F	G	н	Т	J	к	L	М	Ν	0	Ρ	Q	R	s	т	U	V	W	х	Y	Ζ	Α	В	С
E	Е	F	G	Н	Т	J	к	L	М	Ν	0	Ρ	Ø	R	s	т	U	۷	w	х	Y	Z	Α	в	С	D
F	F	G	н	Т	J	ĸ	L	М	Ν	0	Ρ	Q	R	s	Т	U	۷	w	х	Y	Z	Α	в	С	D	Е
G	G	н	Т	J	к	L	М	Ν	0	Ρ	Q	R	S	т	U	۷	W	х	Y	Ζ	Α	В	С	D	Е	F
н	Н	Т	J	K	L	М	Ν	0	Ρ	Q	R	s	т	U	۷	W	х	Y	Ζ	Α	в	С	D	Е	F	G
I	Т	J	к	L	М	Ν	0	Ρ	Q	R	S	Т	U	v	w	х	Y	Z	Α	в	С	D	Е	F	G	н
J	J	к	L	М	Ν	0	Ρ	Q	R	s	Т	U	۷	w	х	Y	Ζ	Α	в	С	D	Е	F	G	Н	Т
к	к	L	М	N	0	Ρ	Q	R	s	т	U	v	w	х	Y	Ζ	А	в	С	D	Е	F	G	н	Т	J
L	L	М	Ν	0	Ρ	Ø	R	s	т	U	۷	w	Х	Y	Ζ	Α	В	С	D	Е	F	G	н	Т	J	к
м	М	Ν	0	P	Q	R	s	Т	U	۷	w	х	Y	Ζ	Α	В	С	D	Е	F	G	н	Т	J	K	L
N	Ν	0	Ρ	Q	R	s	т	U	v	w	х	Y	Ζ	Α	в	С	D	Е	F	G	н	Т	J	к	L	М
0	0	Ρ	Q	R	s	Т	U	۷	w	х	Y	Z	Α	в	С	D	Е	F	G	н	Т	J	к	L	М	Ν
P	Ρ	Q	R	S	Т	U	v	w	х	Y	Ζ	А	В	С	D	Е	F	G	н	Т	J	к	L	М	N	0
Q	Q	R	s	Т	U	۷	w	х	Y	Ζ	Α	в	С	D	Е	F	G	н	Т	J	к	L	М	Ν	0	Ρ
R	R	s	Т	U	۷	W	х	Y	Ζ	Α	В	С	D	Е	F	G	н	Т	J	к	L	М	Ν	0	Ρ	Q
S	S	т	U	۷	w	х	Y	Ζ	А	в	С	D	Е	F	G	н	Т	J	к	L	М	Ν	0	Ρ	Q	R
т	Т	U	V	w	х	Y	Ζ	Α	в	С	D	Е	F	G	н	Т	J	к	L	М	Ν	0	Ρ	Q	R	s
U	U	v	w	х	Y	Ζ	Α	в	С	D	Е	F	G	Н	Т	J	к	L	М	Ν	0	Ρ	Q	R	s	Т
v	۷	w	х	Y	Ζ	Α	В	С	D	Е	F	G	н	Т	J	к	L	М	Ν	0	Ρ	Q	R	s	Т	U
w	W	х	Y	Ζ	Α	в	С	D	Е	F	G	Н	Т	J	к	L	М	Ν	0	Ρ	Q	R	s	Т	U	۷
x	х	Y	Ζ	Α	в	С	D	Е	F	G	Н	T	J	к	L	М	Ν	0	Ρ	Q	R	S	Т	U	۷	W
Y	Υ	Ζ	Α	В	С	D	Е	F	G	н	Т	J	к	L	М	Ν	0	Ρ	Q	R	s	Т	U	v	W	х
Z	Ζ	Α	в	С	D	Е	F	G	н	Т	J	к	L	М	Ν	0	Ρ	Q	R	s	Т	U	v	w	Х	Y

• Machine Enigma : Ça substitue chaque lettre d'un message par une autre via un circuit électrique à travers des rotors. La configuration des rotors, qui peut être changée pour chaque message est la clé du chiffrement.

Téléphone rouge : Ça utilise le principe du masque jetable, à l'aide de machines de chiffrement appeler « Electronic Teleprinter Cryptographic Regenerative Repeater Mixer (ETCRRM) », donc à chaque message envoyé une clé est générée et est à usage unique, la clé doit être une suite de caractères au moins aussi longue que le message à chiffrer, ces caractères sont choisis aléatoirement.





• **Hachage :** Ça permet un chiffrement avec une longueur fixe via des fonctions ici la fonction md5 :

Chiffrement à clé symétrique :





Chiffrement à clé asymétrique :



Chiffrement AES: L'algorithme prend en entrée un bloc de 128 bits (16 octets), la clé fait 128, 192 ou 256 bits. Les 16 octets en entrée sont permutés selon une table définie au préalable. Ces octets sont ensuite placés dans une matrice de 4x4 éléments et ses lignes subissent une rotation vers la droite. L'incrément pour la rotation varie selon le numéro de la ligne. Une transformation linéaire est ensuite appliquée sur la matrice, elle consiste en la multiplication binaire de chaque élément de la matrice avec des polynômes issus d'une matrice auxiliaire, cette multiplication est soumise à des règles spéciales selon GF(28) (groupe de Galois ou corps fini). La transformation linéaire garantit une meilleure diffusion (propagation des bits dans la structure) sur plusieurs tours.

Finalement, un OU exclusif XOR entre la matrice et une autre matrice permet d'obtenir une matrice intermédiaire. Ces différentes opérations sont répétées plusieurs fois et définissent un « tour ». Pour une clé de 128, 192 ou 256, AES nécessite respectivement 10, 12 ou 14 tours.



La principale différence entre le hachage et le chiffrement bijectif est qu'on peut déchiffrer un message chiffrer avec le chiffrement bijectif mais pas si il est hacher car le hachage est unidirectionnel il ne permet pas grâce à la clé de retrouver le message initial.

Les limites du hachage sont :

- Les mots de passes faible
- Les attaques brute force et par bibliothèques
- Avec le temp certain hachage devienne obsolète

Truecrypt

TrueCrypt est un logiciel de chiffrement de données utilisé pour créer des volumes cryptés sur des disques durs, des clés USB ou d'autres supports de stockage. Il permettait aux utilisateurs de protéger leurs fichiers en les rendant illisibles sans le mot de passe correct.

TrueCrypt était un logiciel sécurisé permettant de créer des espaces de stockage cryptés appelés "conteneurs". Ces conteneurs agissaient comme des coffres-forts numériques, protégeant les fichiers avec un mot de passe. En étant open source, TrueCrypt offrait simplicité et transparence, ce qui en faisait un choix populaire pour sécuriser les données confidentielles.

Cela permet de sécuriser les fichiers de l'entreprise ce qui peut contrer plusieurs types d'attaque comme le phishing les ransomware et plein d'autre.

D'autre logiciels peuvent être utiliser comme Bitlocker pour Windows et Veracrypt pour Linux

 Chercher dans la barre de recherche Windows « Gérer BitLocker » puis l'activer :

 Si ce message s'affiche c'est que l'ordinateur n'a pas de puce TPM ce qui signifie que si on active BitLocker Windows ne pourras pas déverrouiller l'accès au disque seul car la clé secrète qui sert à le déverrouiller est normalement stockée dans la puce TPM, ce qui implique quelque étape supplémentaire.

Chiffrement de lecteur BitLock	er				-		×
$ ightarrow ~ \uparrow i i i i i i i i i i i i i i i i i i$	et sécurité > Chiffrement de lecteur BitLocker	~	Ū	Rechercher			Q
Page d'accueil du panneau de configuration	Chiffrement de lecteur BitLocker Protégez vos fichiers et dossiers contre l'accès	non autori	sé en pr	otégeant vos lecte	urs avec	BitLocl	? ker.
	Lecteur du système d'exploitation						
	C: BitLocker désactivé				\bigcirc		
	5	🗣 Activ	ver BitLo	cker			
	Lecteurs de données fixes						
	Lecteurs de données amovibles - Bi Insérez un lecteur flash USB amovible pour	tLocker utiliser BitL	TO GO ocker To	o Go.			

🔶 🛛 🏘 Chiffrement de lecteur BitLocker (C:)

Démarrage de BitLocker

Ce périphérique ne peut pas utiliser un module de plateforme sécurisée (TPM). Votre administrateur doit définir l'option « Autoriser BitLocker sans un module de plateforme sécurisée compatible » dans la stratégie « Demander une authentification supplémentaire au démarrage » pour les volumes du système d'exploitation.

Sans puce TPM

 Faire « Win + R » puis « gpedit.msc » et aller dans « Exiger une authentification supplémentaire au démarrage » :

Sélectionner « Activé » et cocher « Autoriser BitLocker … »



Exiger une authentification supplémentaire au démarrage Paramètre précédent Paramètre suivant Non configure Commentaire : Autorise Activé Pris en charge sur : Au minimum Windows Server 2008 R2 ou Windows 7 Image: Commentaire au démarrage Options : Autoriser BitLocker sans un module de plateform mot de passe ou une clé de démarrage sur un dit de l'ordinateur et si vous utiliser BitLocker co us ans module de plateforme sécurisée. Ce paramètre de stratégie vous permet de configurer si BitLocker exige un authentification supplémentaire à chaque démarrage de l'ordinateur et si vous utiliser BitLocker co us ans module de plateforme sécurisée. Ce paramètre de stratégie est appliqué lorsque vous activez BitLocker. Paramètres pour les ordinateurs avec un module de plateforme sécurisée. Ce paramètre de stratégie est appliqué lorsque vous activez BitLocker. Remarque : une seule des options d'authentification supplémentaire peut être exigée au démarrage, sans générer d'erreur de stratégie. Si vous voulez utiliser BitLocker sur un ordinateur sans un module de plateforme sécurisée. Configurer la cté de démarrage de module de plateforme sécurisée. Si une clé de démarrage seu tuilisée, l'accèx au lecture est autonisée compatible.». Dans ce mode, un mot de passe ou une lecteur USB. Lorsque la cté de démarrage est utilisée, l'arcèx au lecteur est autonisée fil cocker sur ou non disponible, ou bien encore si vous oubliez le mot de passe, vous devez utilisée au chisée pour chiftée le lecteur est activisée i laccèx au lecteur est autorisée run accèder au lecteur. Configurer le côde PIN de démarrage avec Si la cé USB est perdue ou non dispo	Exiger une authentification supplémer	taire au déma	arrage					×
○ Non configure Commentaire :	Exiger une authentification supplémer	taire au déma	rrage	Paramètre	précédent	Paramètre	e suivant	
Obésactivé Pris en charge sur : Autoriser BitLocker sans un module de plateform mot de passe ou une clé de démarrage sur un dia de plateforme sécurisée. Configurer la clé de démarrage de module de plateforme sécurisée. Configurer la clé de démarrage avec le module de plateforme souriser BitLocker sur un ordinateur sans un module de plateforme sécurisée. Configurer la clé de démarrage de module de plateforme securisée. Configurer la clé de démarrage de module de plateforme securisée. Configurer la clé de démarrage de module de plateforme securisée. Si vous vultiser BitLocker sur un ordinateur sans un module de plateforme sécurisé. Ce paramètre de stratégie. Si vous voulez utiliser BitLocker sur un ordinateur sans un module de plateforme sécurisé. Activez la case à cocher « Autoriser une clé de démarrage de module de plateforme sécurisé. Sui vous vultez utiliser BitLocker sur un ordinateur sans un module de plateforme sécurisé. Sui vous voulez utiliser BitLocker sur un ordinateur sans un module de plateforme sécurisé. Sui vous voulez utiliser BitLocker sur un ordinateur sans un module de plateforme sécurisé. Sui cocher « Autoriser BitLocker sur un un del de plateforme autorisée Configurer la clé de démarrage de module de plateforme sécurisée. Sui une clé USB. Lorsque la clé utilisée, la case au cocher « Autoriser BitLocker sur un colé plater exispe la cléteur utilisée le lecteur est authentifie et lecteur est authentifie et lecteur est accessible. Si la clé USB est insée, accivez au lecteur est authentifie et lecteur est accessible. Sui la clé USB est perdue ou non disponible, ou bien encore si vous oubliez le mot de passe, vous devez utiliser l'une des options de récupération BitLocker au acceder au lecteur.	○ Non configuré Commentaire : ● Activé							^
Options : Aide : Autoriser BitLocker sans un module de plateform mot de passe ou une clé de démarrage sur un dia de l'ordinateur et si vous utilisez BitLocker exige une authentification supplémentaire à chaque démarrage de l'ordinateur et si vous utilisez BitLocker exo us ans module de plateforme sécurisée. Ce paramètre de stratégie est appliqué lorsque vous activez BitLocker exige au démarrage, sans généer d'erreur de stratégie. Remarque : une seule des options d'authentification supplémentaire puet être exigée au démarrage, sans généer d'erreur de stratégie. Si vous voulez utiliser BitLocker sur un ordinateur sans un module de plateforme sécurisée. Configurer la clé de démarrage de module de plateforme sécurisée. Configurer la clé de démarrage de module de plateforme sécurisée. Configurer la clé de démarrage avec le module de plateforme sécurisée. Si une clé de démarrage est utilisée, les informations de clé utilisées pour chifter le lecteur sot tockées sur ce lecteur USB. Lorsque la clé USB est perdue ou non disponible. ou bien encore si vous oubliez le mot de passe, vous acezed auties rune de soptions de récupération BitLocker pour accéder au lecteur.	O Désactivé Pris en charge sur :	Au minimur	m Windows S	ierver 2008 R2	2 ou Window	s 7		~ ~
Autoriser BitLocker sans un module de plateform mot de passe ou une clé de démarrage sur un dis Paramètres pour les ordinateurs avec un module de Configurer le démarrage du module de plateforme sécurisée. Ce paramètre de stratégie est appliqué lorsque vous activez BitLocker avec ou sans module de l'ardinateur et si vous utilisez BitLocker ec us ans module de l'ardinateur et si vous utilisez BitLocker avec ou sans module de l'ardinateur et si vous utilisez BitLocker avec ou sans module de l'ardinateur et si vous utilisez BitLocker sur un ordinateur sans un module de plateforme sécurisée. Configurer la clé de démarrage de module de Autoriser un clé de démarrage de module de plateforme Autoriser un clé de démarrage avec le module de futoriser un clé de démarrage avec le module de Autoriser un clé de démarrage avec le module de Autoriser un clé de démarrage avec le module de Autoriser un clé de démarrage avec le module de futoriser un clé de démarrage avec le module de Autoriser un clé USB est necét, l'accès au lecteur est authentifie de lecteur est accessible. Si la clé USB est perdue ou non disponible, ou bien encore si vous oubliez le mot de passe, vous devez ultiser l'une des options de récupération BitLocker pour accèder au lecteur. Dis a de los passe, vous devez ultiser l'une des options de récupération BitLocker pour accèder au lecteur. V	Options :		Aide :					
	Autoriser BitLocker sans un module de mot de passe ou une clé de démarrage Paramètres pour les ordinateurs avec un r Configurer le démarrage du module de pli Exiger le module de plateforme sécurisée Configurer le code PIN de démarrage de r Autoriser un code PIN de démarrage avec Configurer la clé de démarrage de module Autoriser une clé de démarrage avec le m Configurer le code PIN et la clé de démar Autoriser une clé et un code PIN de démar	plateform sur un die nodule de teforme s nodule de le module de platef padule de p arge de m rrage avec v >	Ce paramè exige une a de l'ordinal de platefor lorsque voi Remarque supplémen d'erreur de Si vous vou module de « Autoriser est requis p les informa stockées su USB est ins accessible. encore si v des option:	tre de stratég iuthentificati- tieur et si vours me sécurisée us activez Bitl : une seule di- taire peut êtr stratégie. lez utiliser Bi plateforme s BitLocker sa s. Dans cen so iutions de clé ti ro ce lecteur l' érée, l'accès i Si la clé USB ous oubliez le s	je vous perm on suppléme so suppléme su tilisez BitL. C Ce paramèt Locker. es options d'are ex exigée au d ttocker sur u scécurisée, acti ns un modur rage. Si une scéurisée, acti ns un mod rage. Si une scéurisée, acti ns un mod rage. Si une su lecteur est est perdue ou e mot de pass tion BitLocke	et de configu maire à chaq ocker avec ou re de stratégie uuthentificatio émarrage, sa n ordinateur r vez la case à i de plateforn de passe ou de plateforn chiffrer le lec a cuthentific e u non disponi «, vous devez r pour accédi	irrer si BitLocue démarrai se démarrai sens modu e est applique on ns générer sans un cocher ne autorisée un lecteur (rage est utili teur sont orsque la clé t le lecteur of ble, ou bier z utiliser l'un er au lecteu	:ker ∧ ge ile ué JSB isée, fé est n ne rr. ∨

Choisir « Entrer un mot de passe » et en saisir un :

 Choisir le mode de déverrouillage de votre lecteur au démarrage i Certains paramètres sont gérés par votre administrateur système. Pour assurer la sécurité de vos données, vous pouvez indiquer à BitLocker d'exiger un mot de passe ou l'insertion d'un lecteur flash USB chaque fois que vous démarrez votre PC. → Insérer un lecteur flash USB → Entrer un mot de passe 	 Choisir le mode de déverrouillage de votre lecteur au démarrage I Certains paramètres sont gérés par votre administrateur système. Pour assurer la sécurité de vos données, vous pouvez indiquer à BitLocker d'exiger un mot de passe ou l'insertion d'un lecteur flash USB chaque fois que vous démarrez votre PC. → Insérer un lecteur flash USB → Entrer un mot de passe 	 Choisir le mode de déverrouillage de votre lecteur au démarrage i Certains paramètres sont gérés par votre administrateur système. Pour assurer la sécurité de vos données, vous pouvez indiquer à BitLocker d'exiger un mot de passe ou l'insertion d'un lecteur flash USB chaque fois que vous démarrez votre PC. → Insérer un lecteur flash USB → Entrer un mot de passe 	 Choisir le mode de déverrouillage de votre lecteur au démarrage I Certains paramètres sont gérés par votre administrateur système. Pour assurer la sécurité de vos données, vous pouvez indiquer à BitLocker d'exiger un mot de passe ou l'insertion d'un lecteur flash USB chaque fois que vous démarrez votre PC. → Insérer un lecteur flash USB → Entrer un mot de passe 	 Choisir le mode de déverrouillage de votre lecteur au démarrage I Certains paramètres sont gérés par votre administrateur système. Pour assurer la sécurité de vos données, vous pouvez indiquer à BitLocker d'exiger un mot de passe ou l'insertion d'un lecteur flash USB chaque fois que vous démarrez votre PC. → Insérer un lecteur flash USB → Entrer un mot de passe 	÷	Rev Chiffrement de lecteur BitLocker (C:)
 Certains paramètres sont gérés par votre administrateur système. Pour assurer la sécurité de vos données, vous pouvez indiquer à BitLocker d'exiger un mot de passe ou l'insertion d'un lecteur flash USB chaque fois que vous démarrez votre PC. → Insérer un lecteur flash USB → Entrer un mot de passe 	 Certains paramètres sont gérés par votre administrateur système. Pour assurer la sécurité de vos données, vous pouvez indiquer à BitLocker d'exiger un mot de passe ou l'insertion d'un lecteur flash USB chaque fois que vous démarrez votre PC. → Insérer un lecteur flash USB → Entrer un mot de passe 	 Certains paramètres sont gérés par votre administrateur système. Pour assurer la sécurité de vos données, vous pouvez indiquer à BitLocker d'exiger un mot de passe ou l'insertion d'un lecteur flash USB chaque fois que vous démarrez votre PC. → Insérer un lecteur flash USB → Entrer un mot de passe 	 Certains paramètres sont gérés par votre administrateur système. Pour assurer la sécurité de vos données, vous pouvez indiquer à BitLocker d'exiger un mot de passe ou l'insertion d'un lecteur flash USB chaque fois que vous démarrez votre PC. → Insérer un lecteur flash USB → Entrer un mot de passe 	 Certains paramètres sont gérés par votre administrateur système. Pour assurer la sécurité de vos données, vous pouvez indiquer à BitLocker d'exiger un mot de passe ou l'insertion d'un lecteur flash USB chaque fois que vous démarrez votre PC. → Insérer un lecteur flash USB → Entrer un mot de passe 		Choisir le mode de déverrouillage de votre lecteur au démarrage
Pour assurer la sécurité de vos données, vous pouvez indiquer à BitLocker d'exiger un mot de passe ou l'insertion d'un lecteur flash USB chaque fois que vous démarrez votre PC. → Insérer un lecteur flash USB → Entrer un mot de passe	Pour assurer la sécurité de vos données, vous pouvez indiquer à BitLocker d'exiger un mot de passe ou l'insertion d'un lecteur flash USB chaque fois que vous démarrez votre PC. → Insérer un lecteur flash USB → Entrer un mot de passe	Pour assurer la sécurité de vos données, vous pouvez indiquer à BitLocker d'exiger un mot de passe ou l'insertion d'un lecteur flash USB chaque fois que vous démarrez votre PC. → Insérer un lecteur flash USB → Entrer un mot de passe	Pour assurer la sécurité de vos données, vous pouvez indiquer à BitLocker d'exiger un mot de passe ou l'insertion d'un lecteur flash USB chaque fois que vous démarrez votre PC. → Insérer un lecteur flash USB → Entrer un mot de passe	Pour assurer la sécurité de vos données, vous pouvez indiquer à BitLocker d'exiger un mot de passe ou l'insertion d'un lecteur flash USB chaque fois que vous démarrez votre PC. → Insérer un lecteur flash USB → Entrer un mot de passe		 Certains paramètres sont gérés par votre administrateur système.
→ Insérer un lecteur flash USB → Entrer un mot de passe	 → Insérer un lecteur flash USB → Entrer un mot de passe 	 → Insérer un lecteur flash USB → Entrer un mot de passe 	 → Insérer un lecteur flash USB → Entrer un mot de passe 	→ Insérer un lecteur flash USB → Entrer un mot de passe		Pour assurer la sécurité de vos données, vous pouvez indiquer à BitLocker d'exiger un mot de passe ou l'insertion d'un lecteur flash USB chaque fois que vous démarrez votre PC.
→ Entrer un mot de passe		→ Insérer un lecteur flash USB				
						\rightarrow Entrer un mot de passe

Choisir le mode de conservation de la clé de chiffrement :

←	🎭 Chiffrement de lecteur BitLocker (C:)	
	Créer un mot de passe pour déverrouiller ce lecteur	
	Vous devez créer un mot de passe fort constitué de caractères minuscules et majuscules, de nombres, de symboles et d'espaces.	
	Entrer votre mot de passe	
	•••••	
	Entrer à nouveau le mot de passe	
	•••••	
	Conseils pour créer un mot de passe fort.	
	Suivant Annuler	

- 🏘 Chiffrement de lecteur BitLocker (C:)

Comment voulez-vous sauvegarder votre clé de récupération ?

() Certains paramètres sont gérés par votre administrateur système.

Une clé de récupération vous permet d'accéder à vos fichiers et vos dossiers, si vous rencontrez des problèmes pour déverrouiller votre PC. Il est préférable d'en avoir plusieurs et de les conserver ailleurs que sur votre PC.

- → Enregistrer sur votre compte Microsoft
- → Enregistrer sur un disque mémoire flash USB
- → Enregistrer dans un fichier
- → Imprimer la clé de récupération

Comment retrouver ma clé de récupération ultérieurement ?

• Ici on veut chiffré uniquement une partition :

• Ici on utilise un lecteur fixe :

A the second seco

Choisir dans quelle proportion chiffrer le lecteur

Si vous configurez BitLocker sur un nouveau lecteur ou un nouveau PC, il vous suffit de chiffrer la partie du lecteur en cours d'utilisation. BitLocker chiffre automatiquement les nouvelles données que vous ajoutez.

Si vous activez BitLocker sur un PC ou un lecteur en cours d'utilisation, chiffrez l'intégralité du lecteur. Le chiffrement de l'intégralité du lecteur garantit la protection de la totalité des données, même des données supprimées qui peuvent contenir des informations récupérables.

Ne chiffrer que l'espace disque utilisé (plus rapide et plus efficace pour les nouveaux PC et lecteurs)

Chiffrer tout le lecteur (opération plus lente recommandée pour les PC et les lecteurs en service)

Representation of the second se

Choisir le mode de chiffrement à utiliser

La mise à jour Windows 10 (Version 1511) présente un nouveau mode de chiffrement de disque (XTS-AES). Ce mode fournit une prise en charge supplémentaire de l'intégrité, mais il n'est pas compatible avec les versions antérieures de Windows.

S'il s'agit d'un lecteur amovible que vous allez utiliser sur une version antérieure de Windows, vous devez choisir le mode Compatible.

S'il s'agit d'un lecteur fixe ou si ce lecteur ne va être utilisé que sur des appareils exécutant au moins Windows 10 (Version 1511) ou version ultérieure, vous devez choisir le nouveau mode de chiffrement

Nouveau mode de chiffrement (recommandé pour les lecteurs fixes sur ce périphérique)

O Mode Compatible (recommandé pour les lecteurs pouvant être déplacés à partir de ce périphérique)

Suivant

Annuler

 Cocher « Exécuter la vérification du système BitLocker » et faire « Continuer » puis redémarrer la machine :

 Pendant le redémarrage de la machine il faudra entrer le mot de passe définie avant :

🗧 🏘 Chiffrement de lecteur BitLocker (C:)

Êtes-vous prêt à chiffrer ce lecteur ?

Le chiffrement peut prendre un moment, selon la taille du lecteur.

Vous pouvez continuer à travailler pendant le chiffrement du lecteur, bien que les performances de votre ordinateur puissent être affectées.

Exécuter la vérification du système BitLocker

La vérification du système permet de s'assurer que BitLocker peut lire correctement les clés de récupération et de chiffrement avant de chiffrer le lecteur.

BitLocker redémarrera votre ordinateur avant d'effectuer le chiffrement.

Remarque : cette vérification peut être longue, mais elle est recommandée pour vous assurer que la méthode de déverrouillage sélectionnée fonctionne sans devoir entrer la clé de récupération.

Continuer Annuler

BitLocker

Mot de passe incorrect. Entrez à nouveau le mot de passe

•••••

Appuyez sur la touche Insertion pour afficher le mot de passe lors de sa saisie.

Appuyez sur Entrée pour continuer Appuyez sur Échap pour une récupération BitLocker

 On peut vérifier que la partition à bien été chiffrer en allant dans le gestionnaire de disque :

• Pour déchiffrer la partition il suffit de désactiver BitLocker :

🖶 Gestion des dis	sques						- [- ×			
Fichier Action	Affichage ?										
🖛 🏟 📷 👔	🖬 🗩 🗙 🛃	2 🔒 🍃 🖾									
Volume	Disposition	Туре	Système de	Statut	Capacité	Espace li	% libres				
💻 (C:)	Simple	De base	NTFS (Chiffr	Sain (Dém	49,44 Go	27,55 Go	56 %				
- (Disque 0 partiti	on Simple	De base		Sain (Parti	522 Mo	522 Mo	100 %				
Réservé au systè	RE Simple	De base De base	NTES	Sain (Parti Sain (Systè	5,46 Go 50 Mo	0 Mo 20 Mo	0 % 40 %				
Disque 0 De base 50,00 Go	Réservé au syst 50 Mo NTFS	tèn (C:) 49,44 Go	NTFS <mark>(</mark> Chiffré av	vec BitLocker)		522 Mo					
En ligne	Sain (Système, A	cti Sain (Dér	narrer, Fichier d	échange, Vid	age sur incident, Pa	Sain (Part	tition de récupé	ration)			
CD-ROM 0 CD-ROM 5,46 Go En ligne	CCCOMA_X64FF 5,46 Go UDF Sain (Partition pr	RE_FR-FR_DV9	(D:)								
Non alloué 📕 🖡	Partition principale	e					_				
Real Chiffrement de l	lecteur BitLocker						- 🗆	\times			
$\leftarrow \rightarrow \cdot \cdot \uparrow$	🔖 « Système et sé	écurité > Chiff	rement de lecteu	r BitLocker	5 v	Rechercher		Q			
Page d'accueil d configuration	lu panneau de	Chiffrement de lecteur BitLocker Protégez vos fichiers et dossiers contre l'accès non autorisé en protégeant vos lecteurs avec BitLocker.									
		Lecteur du	système d'e	xploitation							
		C: BitLock	œr activé				\bigcirc				
		Ų			 Suspendre la p Sauvegarder v Modifier le mo Supprimer le r Désactiver Bitl 	rrotection otre clé de réc ot de passe not de passe Locker	cupération				
		Lecteurs de	e données fix	ies							
				Chiffr	ement de lecteur BitL	.ocker		×			
		Lecteurs de	e données an	novib Dés	activer BitLocker	ſ					
Voir aussi		Insérez un I	ecteur flash USB	amovik Iongt	lecteur va être déchif emps, mais vous pou	ífré. Cette opé urrez utiliser vo	ration peut dure otre ordinateur	r			
Administration of the second secon	du TPM			pend	ancie processus de di	econtrement.					
Gestion des disq Déclaration de c	ues onfidentialité				Dés	sactiver BitLoo	cker Annu	iler			
beclaration de c	structure.										

- Pour installer Veracrypt faire « wget <u>http://sourceforgenet/projects/veracrypt/files/Veracrypt%</u>201.0f-2/veracrypt-1,0f-2-setup.tar.bz2 »
- Ensuite on l'extrait « tar xvjf veracrypt-1.0f -2-setup.tar.bz2 »
- Puis on l'execute « ./veracrypt-1.0f -2-setup.console-x64» et faire 1 :

VeraCrypt 1.0f-2 Setup

Installation options:

```
    Install veracrypt_1.0f-2_console_amd64.tar.gz
    Extract package file veracrypt_1.0f-2_console_amd64.tar.gz and place it to /tmp
```

To select, enter 1 or 2:

• On choisit les paramètres de l'installation :

root@root:/home/root2023# veracrypt -t -c	Hash algorithm:	Re-enter password:
Volume type:	1) SHA-512	
1) Normal	2) Whirlpool	
2) Hidden	3) SHA-256	Enter keyfile path [none]:
Select [1]: 1	Select [1]: 1	
Enter volume path: /home/root2023/dossier_chiffrer		Please type at least 320 randomly chosen characters and then press Enter:
Enter volume size (sizeK/size[M]/sizeG): 400M	Filesystem: 1) None	
Encryption algorithm:	2) FAT	Done: 100.000% Speed: 8.2 MB/s Left: 0 s
1) AES	3) Linux Ext2	Dener 100,000% Speed: 7,7 MB/s Left: 0 s
2) Serpent	4) Linux Ext3	Done: 100,000% Speed: 7,7 MB/S Left: 0 S
3) Twofish	5) Linux Ext4	
AES(Twofish)	6) NTFS	
<pre>5) AES(Twofish(Serpent))</pre>	Select [2]: 6	
<pre>6) Serpent(AES)</pre>	561666 [2]: 0	
<pre>7) Serpent(Twofish(AES))</pre>	Entern meneric and a	The VeraCrypt volume has been successfully created.
<pre>8) Twofish(Serpent)</pre>	Enter password:	

• Ensuite on créer un dossier pour pouvoir monter le volume chiffrer créer au préalable :



 Apres toute ses étapes on reçoit une notification qui approuve la création d'un volume :

Volume de 419 Mo	
------------------	--

• Pour supprimer le volume il suffit de rentrer cette commande :

root@root:/home/root2023# veracrypt -d /home/root2023/volume_chiffre