TP -Chiffrement



MATHIUS Baptiste

- 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.

	Α	В	С	D	Е	F	G	Н	Т	J	Κ	L	М	Ν	0	Ρ	Q	R	S	Т	U	۷	W	Х	Y	Ζ
Α	A	В	С	D	Е	F	G	н	Т	J	К	L	М	Ν	0	Ρ	Q	R	S	Т	υ	V	W	Х	Υ	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	Υ	Ζ	А
С	С	D	Е	F	G	Н	Т	J	Κ	L	М	Ν	0	Ρ	Q	R	S	Т	U	٧	W	Х	Υ	Ζ	А	В
D	D	Е	F	G	Н	T	J	Κ	L	М	Ν	0	Ρ	Q	R	S	Т	U	۷	W	Х	Υ	Ζ	А	В	С
Е	E	F	G	н	Т	J	К	L	М	Ν	0	Ρ	Q	R	S	Т	U	V	W	Х	Υ	Ζ	А	В	С	D
F	F	G	н	Т	J	Κ	L	М	Ν	0	Ρ	Q	R	S	Т	U	٧	W	Х	Υ	Ζ	А	В	С	D	Е
G	G	Н	Т	J	Κ	L	М	Ν	0	Ρ	Q	R	S	Т	U	۷	W	Х	Υ	Ζ	А	В	С	D	Е	F
н	н	Т	J	Κ	L	М	Ν	0	Ρ	Q	R	S	Т	U	۷	W	Х	Υ	Ζ	А	В	С	D	Е	F	G
1		J	к	L	М	Ν	0	Ρ	Q	R	S	т	U	V	W	Х	Υ	Ζ	А	в	С	D	Е	F	G	Н
J	J	К	L	М	Ν	0	Ρ	Q	R	S	Т	U	۷	W	Х	Υ	Ζ	А	В	С	D	Е	F	G	н	Т
к	K	L	М	Ν	0	Ρ	Q	R	S	т	U	V	W	Х	Υ	Ζ	А	В	С	D	Е	F	G	Н	Т	J
L	L	М	Ν	0	Ρ	Q	R	S	Т	U	V	W	Х	Υ	Ζ	А	В	С	D	Е	F	G	Н	Т	J	К
М	м	Ν	0	Ρ	Q	R	s	т	U	V	W	Х	Y	Ζ	А	В	С	D	Е	F	G	н	Т	J	к	L
Ν	N	0	Ρ	Q	R	S	Т	U	۷	W	Х	Υ	Ζ	А	В	С	D	Е	F	G	Н	Т	J	Κ	L	М
0	0	Ρ	Q	R	S	т	υ	V	W	Х	Υ	Ζ	А	в	С	D	Е	F	G	н	Т	J	к	L	М	Ν
Ρ	Р	Q	R	S	т	U	V	W	Х	Υ	Ζ	А	В	С	D	Е	F	G	Н	Т	J	к	L	М	Ν	0
Q	Q	R	S	Т	U	٧	W	Х	Υ	Ζ	А	В	С	D	Е	F	G	Н	Ι	J	Κ	L	М	Ν	0	Ρ
R	R	S	Т	U	V	W	Х	Υ	Ζ	А	В	С	D	Е	F	G	н	Т	J	К	L	М	Ν	0	Ρ	Q
S	S	Т	U	٧	W	Х	Υ	Ζ	А	В	С	D	Е	F	G	Н	Т	J	Κ	L	М	Ν	0	Ρ	Q	R
Т	Т.	U	V	W	Х	Υ	Ζ	А	В	С	D	Е	F	G	н	Т	J	к	L	М	Ν	0	Ρ	Q	R	S
U	υ	٧	W	Х	Υ	Ζ	А	В	С	D	Е	F	G	н	Т	J	Κ	L	М	Ν	0	Ρ	Q	R	S	Т
V	V	W	Х	Y	Ζ	А	В	С	D	Е	F	G	Н	Т	J	Κ	L	М	Ν	0	Ρ	Q	R	S	Т	U
W	W	Х	Y	Ζ	А	В	С	D	Е	F	G	Н	T	J	Κ	L	М	Ν	0	Ρ	Q	R	S	Т	U	V
Х	X	Y	Ζ	А	В	С	D	Е	F	G	Н	Т	J	Κ	L	М	Ν	0	Ρ	Q	R	S	Т	U	٧	W
Y	Y	Ζ	А	В	С	D	Е	F	G	Н	Т	J	Κ	L	М	Ν	0	Ρ	Q	R	S	Т	U	٧	W	Х
Ζ	Z	А	В	С	D	Е	F	G	Н	Т	J	К	L	М	Ν	0	Ρ	Q	R	S	Т	U	V	W	Х	Υ

- 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



- 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.

- 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.

- 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.

V Dossiers (7)		Ouvrir	
Bureau	(Ouvrir dans une nouvelle fenëtre	
		Epingler à Accès rapide	
V	- 💎 /	Activer BitLocker	
Images	(Ouvrir la lecture automatique	
	t	Analyser avec Microsoft Defender	
Objets 3D	,	Accorder l'accès à	>
	F	Restaurer les versions précédentes	
	1	nclure dans la bibliothèque	>
Vidéos		Épingler à l'écran de démarrage	
	- 1	Formater	
✓ Périphériques et le	(Copier	
Disque local (0	(Créer un raccourci	
NITES		Denommer	~
← 🏘 Chiffrement de lecteur BitLo	ocker (E:)		
Choisissez le mode de d	léverrou	uillage de ce lecteur.	
Utiliser un mot de passe pou Les mots de passe doivent co des symboles.	ir déverrou ontenir de	uiller le lecteur Is lettres majuscules et minuscules, des chiffres, des espaces et	
Entrer votre mot de passe		•••••	
Entrer à nouveau votre mot	t de passe	•••••	
Utiliser ma carte à puce pour Vous devrez insérer votre car	r déverrou rte à puce.	iller le lecteur . Son code PIN vous sera demandé pour déverrouiller le lecteu	r.

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.

← 🏘 Chiffrement de lecteur BitLocker (E:)

Êtes-vous prêt à chiffrer ce lecteur ?

Vous pourrez déverrouiller ce lecteur à l'aide d'un mot de passe.

- Le chiffrement peut être long, en fonction de la taille du lecteur.
- Tant que le chiffrement n'est pas terminé, vos fichiers ne sont pas protégés.



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



Docum Développer	
Images	
Disque	
docum 🗖 Analyser avec Microsoft Defender	
Musiqu Modifier le mot de passe BitLocker	
Gérer BitLocker	
Ouvrir dans une nouvelle fenêtre	
> OneDriv(Épingler à Accès rapide	
✓ Ce PC Accorder l'accès à >	
Restaurer les versions précédentes	
> 🛱 Docum	
Épingler à l'écran de démarrage	
Formater	
> Dojets	
> 🕹 Télécha Renommer	
> 🛃 Vidéos 🛛 Nouveau >	
> 🏪 Disque Propriétés	
> 🚔 Disque (c:)	
age d'accueil du panneau de onfiguration Protégez vos fichiers et dossiers contre l'accès non autorisé en protég BitLocker.	geant v
Lecteur du système d'exploitation	
Chiffrement de lecteur BitLocker X	
Désactiver Bitl ocker	
Votre lecteur va être déchiffré. Cette opération peut durer longtemps, mais vous pourrez utiliser votre ordinateur pendant le processus de déchiffrement.	
Désactiver BitLocker Annuler ation	re clé d
Modifier le mot d	de pass

Lecteurs de données amovibles - BitLocker To Go

Insérez un lecteur flash USB amovible pour utiliser BitLocker To Go.

vos lecteurs av

🍚 Ajouter une carte à puce

ésactiver BitLocker

Activer le déverrouillage automatique

MATHIUS Baptiste

Voir aussi Administration du TPM

Gestion des disques
Déclaration de confidentialité

- 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.





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

Sélectionner u	ne partition ou	ı un périphérique	×
Périphérique	Taille	Mount Directory	
📄 /dev/sr0:	1023 Mo		
📄 /dev/sda:	10,0 Go		
/dev/sda1	512 Mo	/boot/efi	
/dev/sda5	9,5 Go	/	
🚔 /dev/sdb:	15,6 Go		
		Annuler Valid	ler

	Assistant d	e création de v	ol	ume			-	×
	Mot de pase : Mot de passe : Confirmer : Il est très import Vous devriez évil un dictionnaire (ne devrait pas être combinaison de caractères spéci choisir un mot de	sse du volu 	t d ich ich isc isc isc isc isc isc	e passe iers clés sissiez un bon mo ot simple que l'or on de plusieurs d u de dates de nai: n bon mot de pas najuscules, de ch \$ * + etc. Il est rec 20 caractères (li	ot de pass n trouve de e ces mot ssance. Il n sse est une iffres et d command e plus long	Fich e. ans s). Il e é de g, le	iers clés	
rendery pr		Aide		< Précédent	Suivant	>	Annule	er -

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

	Assist	tant de cr	éation de v	volume		- 🔇
VeraCrypt	Forma Options Système Options Forma In order to volume, it filesystem If your volu can use 'Qu volume.	tage du NTFS atage rapi o enable yc has to be type. ume is goi uick forma	de de ng to be hos t' to skip er	g system to mount vith a filesystem. P ited on a device or ccryption of free sp	your new lease select a partition, you pace of the	
			Aide	< Précédent	Suivant >	Annuler

- 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**

	Vera	Crypt			- (
Volumes Favoris Outils	Paramètres Aide				
Conne Volume		Taille	Mount Directory	Туре	
🚍 1 🛛 /dev/sdb		15,6 Go	/media/veracrypt	1 Normal	
i 2					
3					
4					
5					
6					
7					
8					
i 9 □ 10					
■ 10					
Créer un volume	Propriété	s du volume		Vi	ler le cache
	rioprice	3 du votanie			der te coerie
Volume					
				- I	ichier
veraCrypt 🛛 Ne jamais enreg	istrer l'historique	C	Outils pour le volun	ne Péri	phérique