

# Chiffrement d'un disque avec TrueCrypt



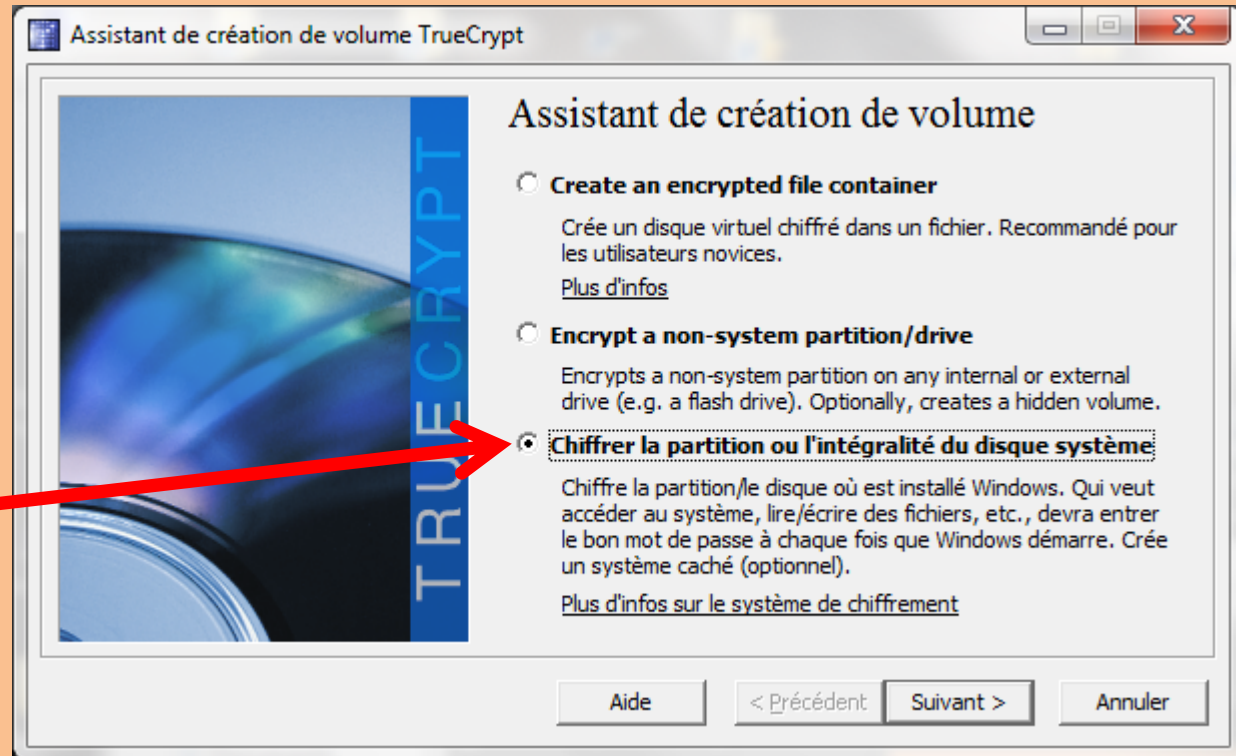
FDE (Full Disk Encryption)

Mai 2011

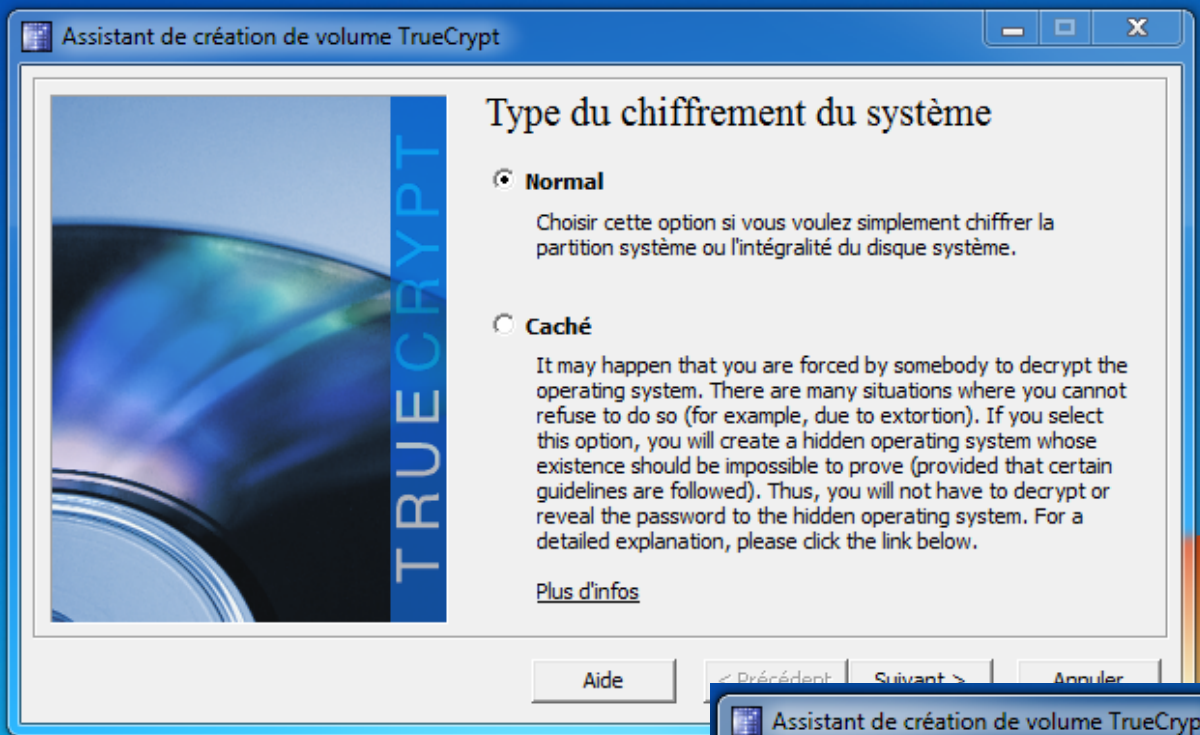
# Avant de commencer

- S'assurer que les données utilisateurs sont sauvegardées de façon régulière dans un endroit sécurisé.
- Installer truecrypt sur le poste

Lancer le script chiffreDisque.bat  
ou exécuter la commande suivante depuis le répertoire truecrypt  
"TrueCrypt Format.exe" /noisocheck



Chiffrer la disque



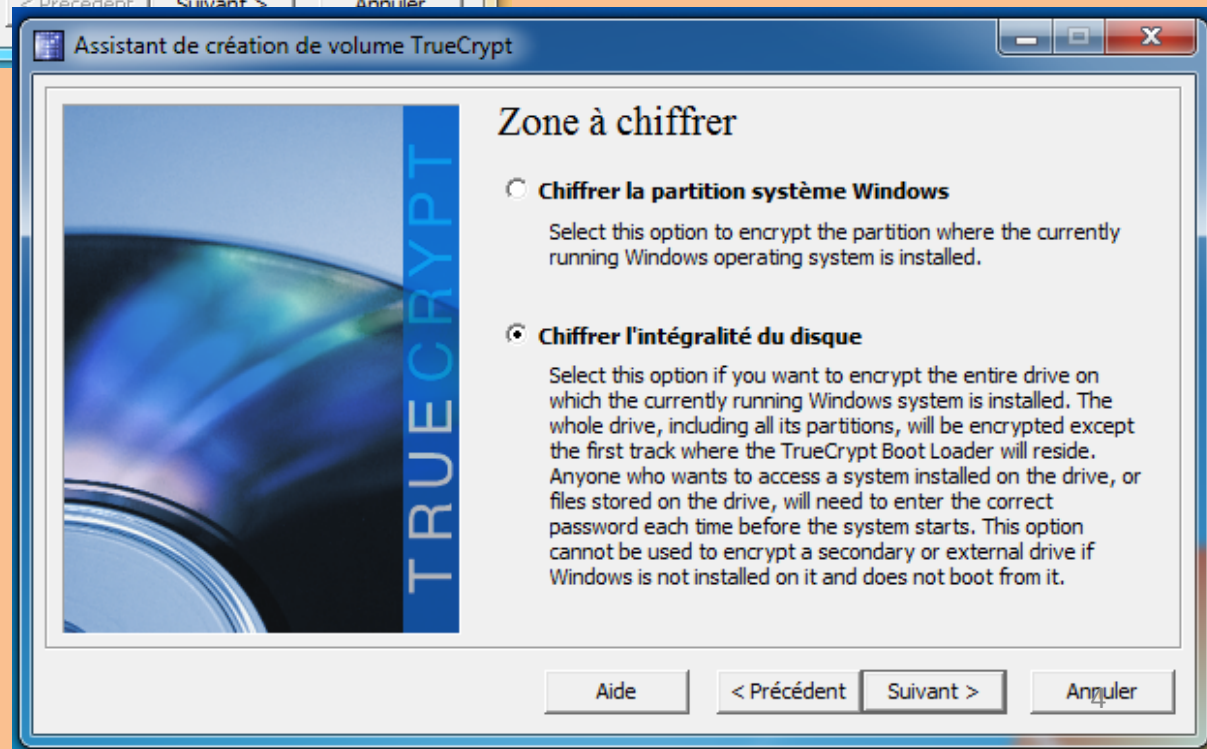
2 Modes :

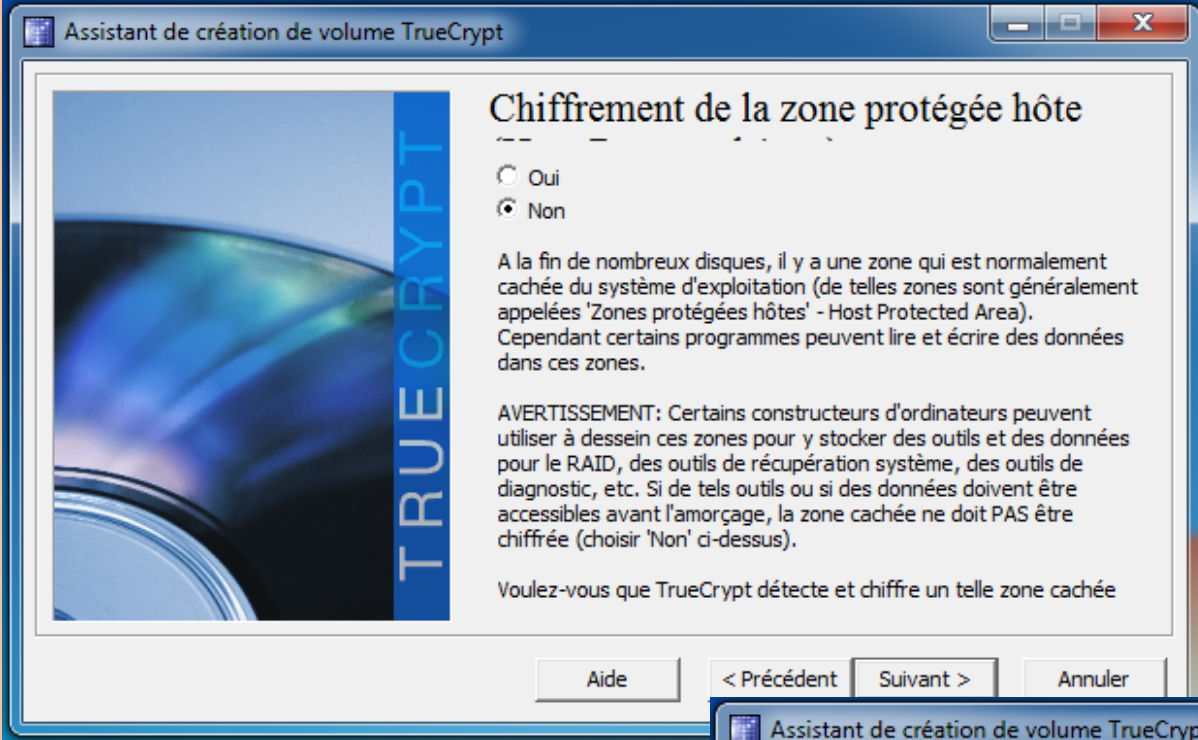
Normal

Caché

**choisir Normal**

Choix de la zone à chiffrer:  
Partition Système  
Intégralité du disque



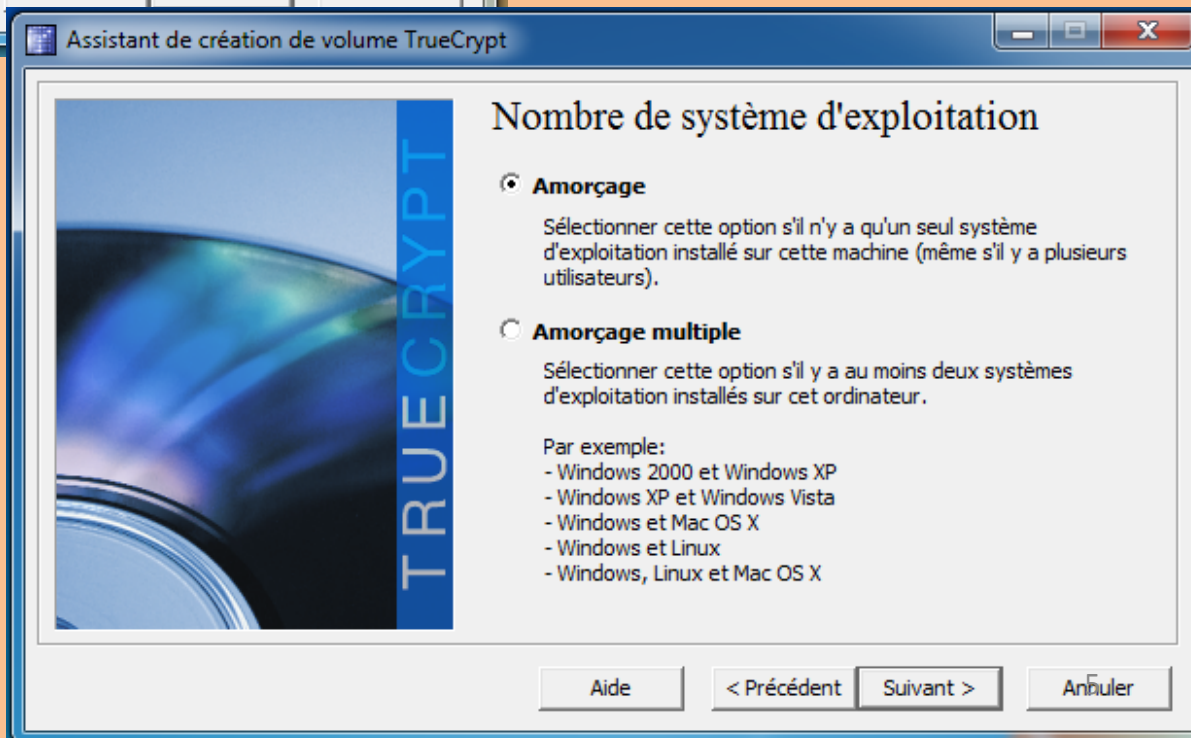


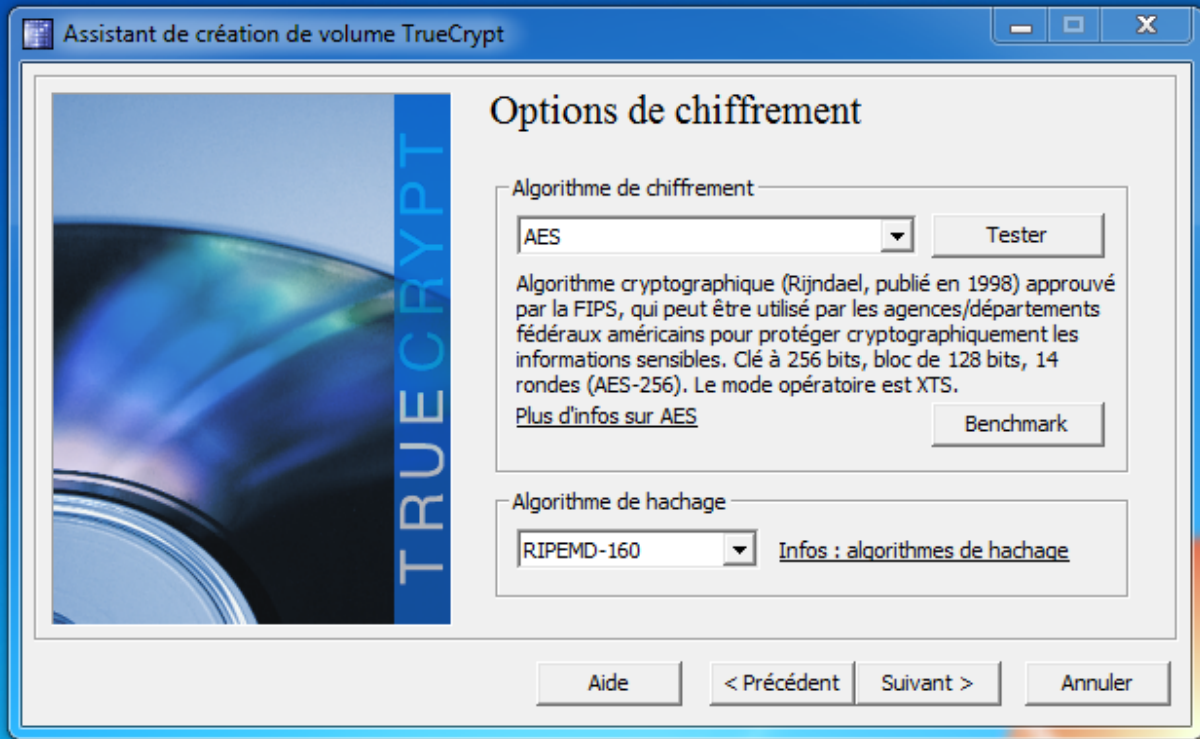
Chiffrement de la zone protégée (Oui/Non)

Choix Non

(partition cachée qui est utilisée pour stocker des softs constructeurs de gestion RAID ou dépannages)

Choix du type d'amorçage :  
Pas d'amorçage multiple  
dans notre cas





Choix du type de chiffrement

Laisser AES

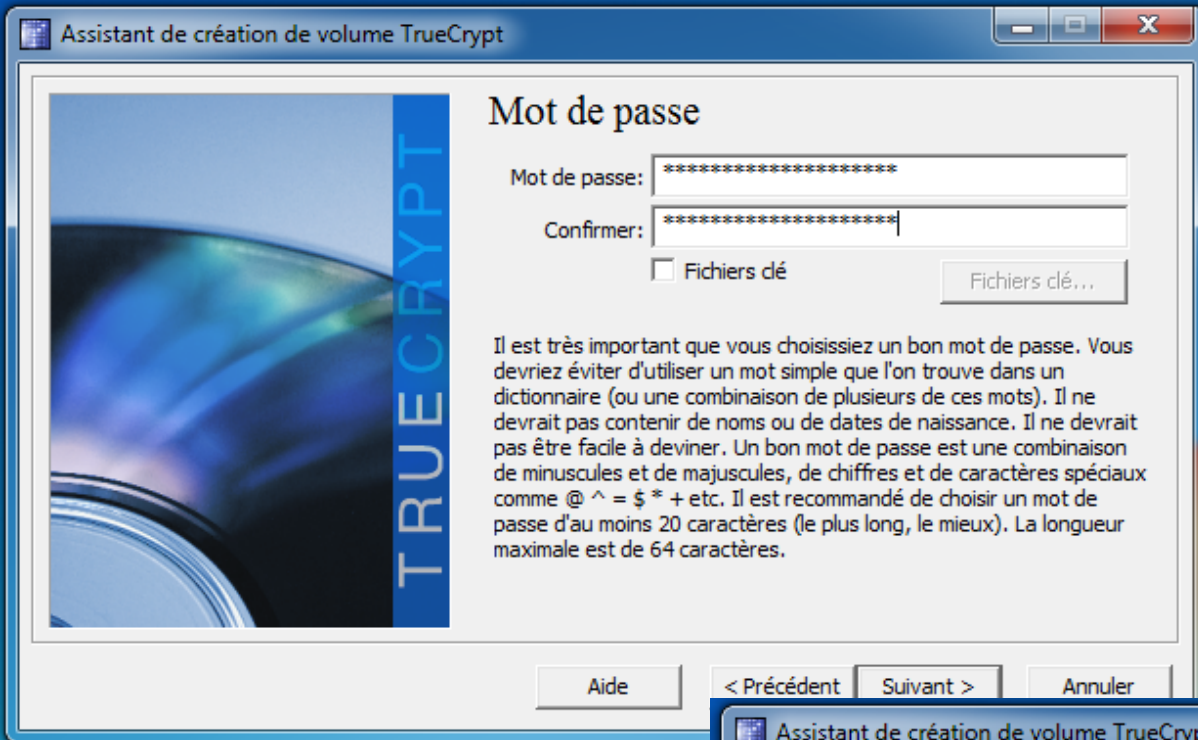
Plus le chiffrement est fort,  
plus le système sera sollicité.

TrueCrypt - Banc de test de l'algorithme de chiffrement

Tampon: 5 Mo Méthode de tri: Vitesse moyenne (décroissante)

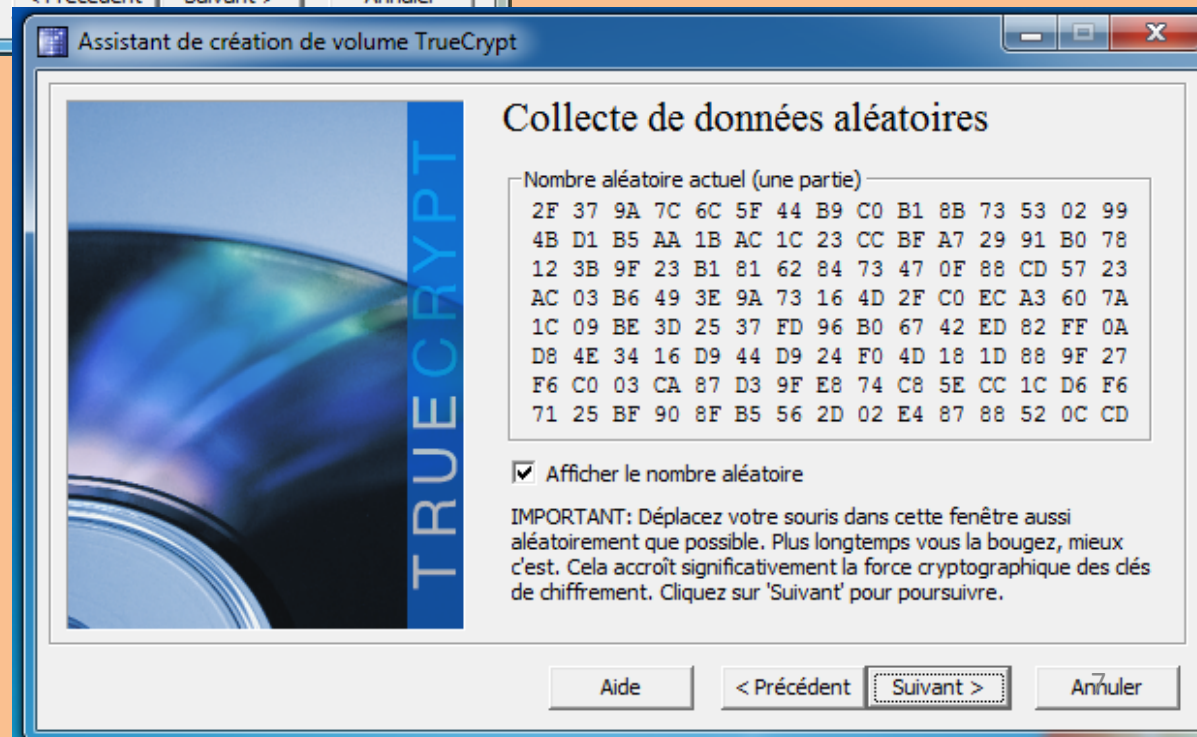
Algorithme	Chiffrement	Déchiffrement	Moyenne	
AES	236 Mo/s	241 Mo/s	238 Mo/s	<p>Test</p> <p>Fermer</p> <p>La vitesse est affectée par la charge du CPU ainsi que par les caractéristiques du périphérique de stockage.</p> <p>Ces tests ont lieu en RAM.<sup>6</sup></p>
Twofish	220 Mo/s	220 Mo/s	220 Mo/s	
AES-Twofish	115 Mo/s	141 Mo/s	128 Mo/s	
Serpent	109 Mo/s	119 Mo/s	114 Mo/s	
Twofish-Serpent	98.2 Mo/s	98.4 Mo/s	98.3 Mo/s	
Serpent-AES	92.2 Mo/s	97.5 Mo/s	94.8 Mo/s	
AES-Twofish-Serpent	72.3 Mo/s	72.9 Mo/s	72.6 Mo/s	
Serpent-Twofish-AES	69.9 Mo/s	71.8 Mo/s	70.8 Mo/s	

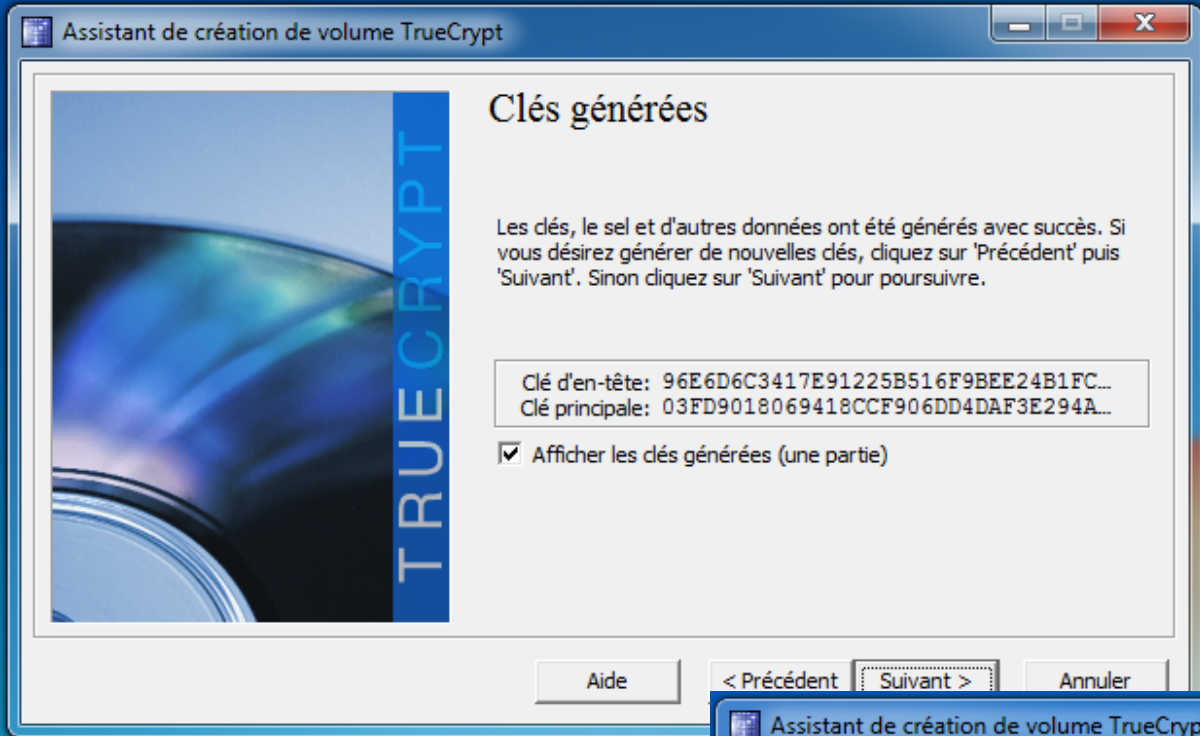




Saisie du mot de passe

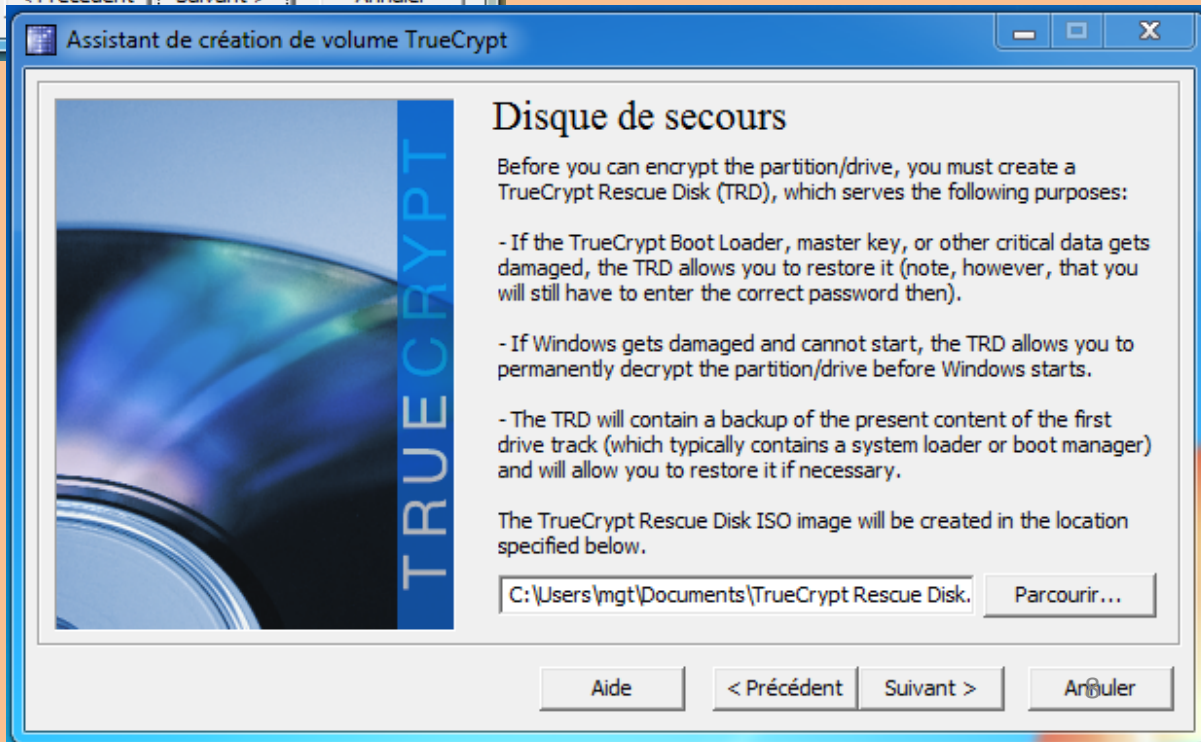
Randomisation de la clé par le déplacement de la souris





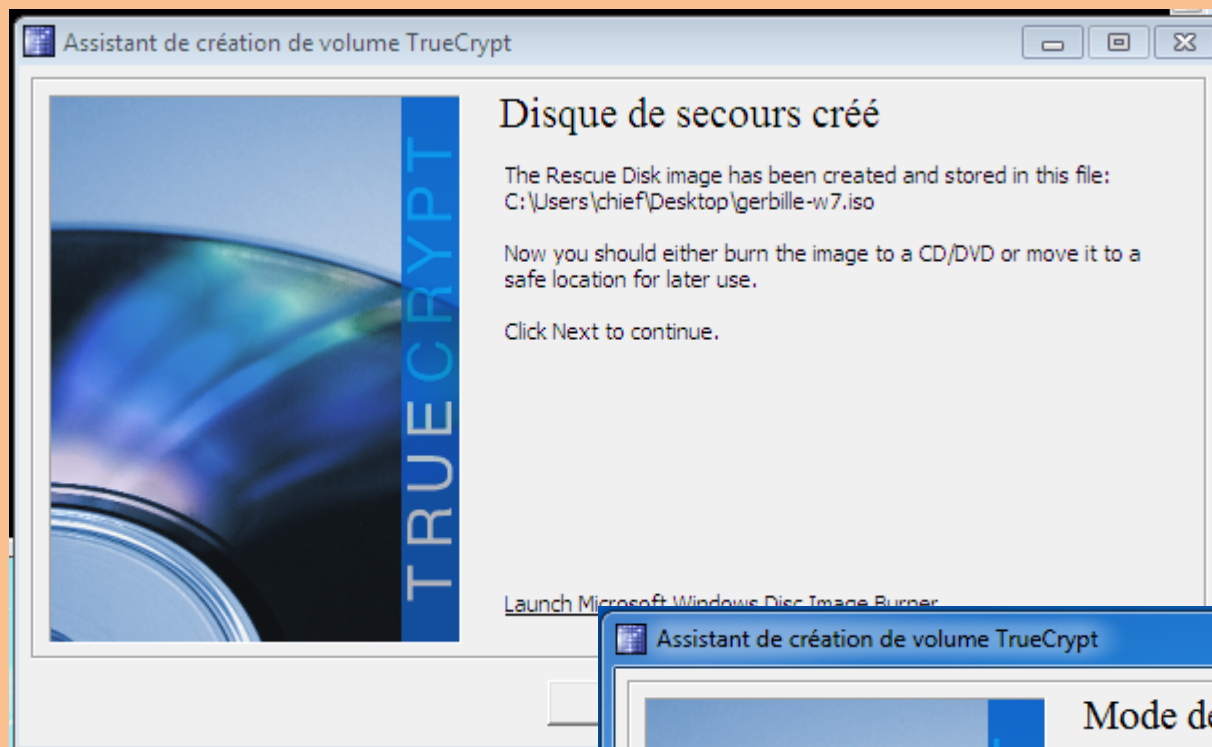
Affichage de la clé

Création du disque de secours  
image iso



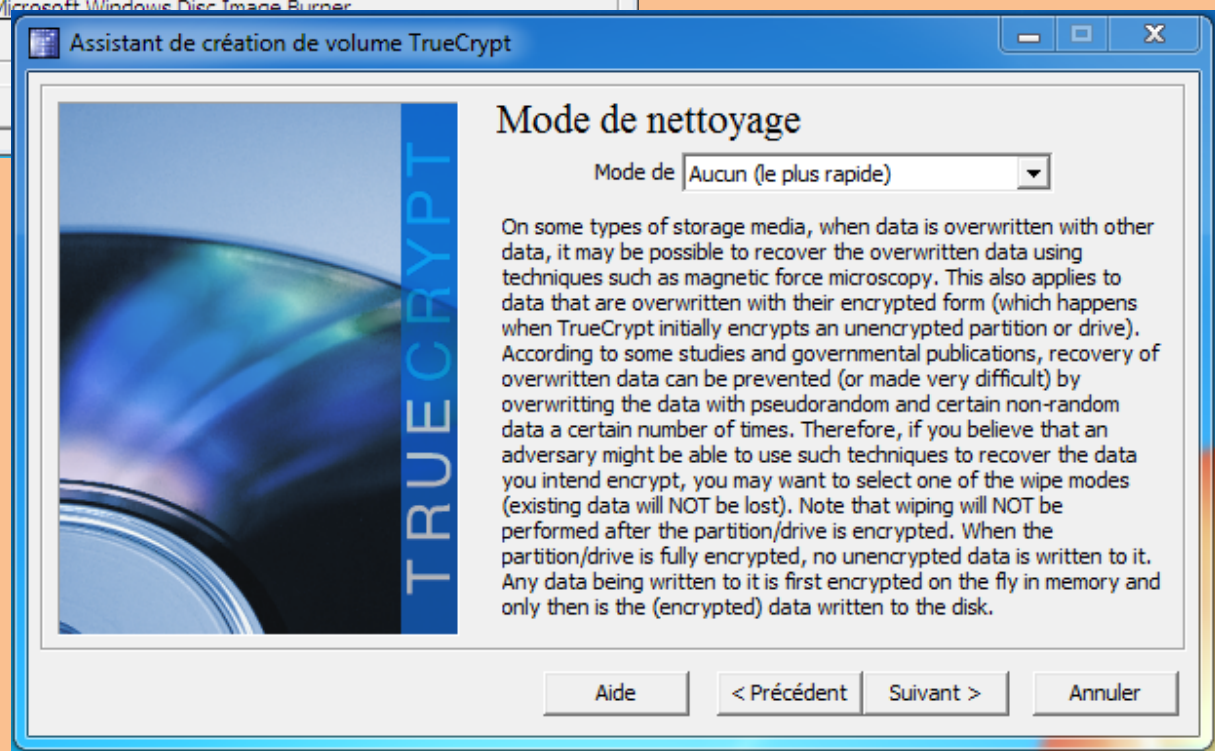


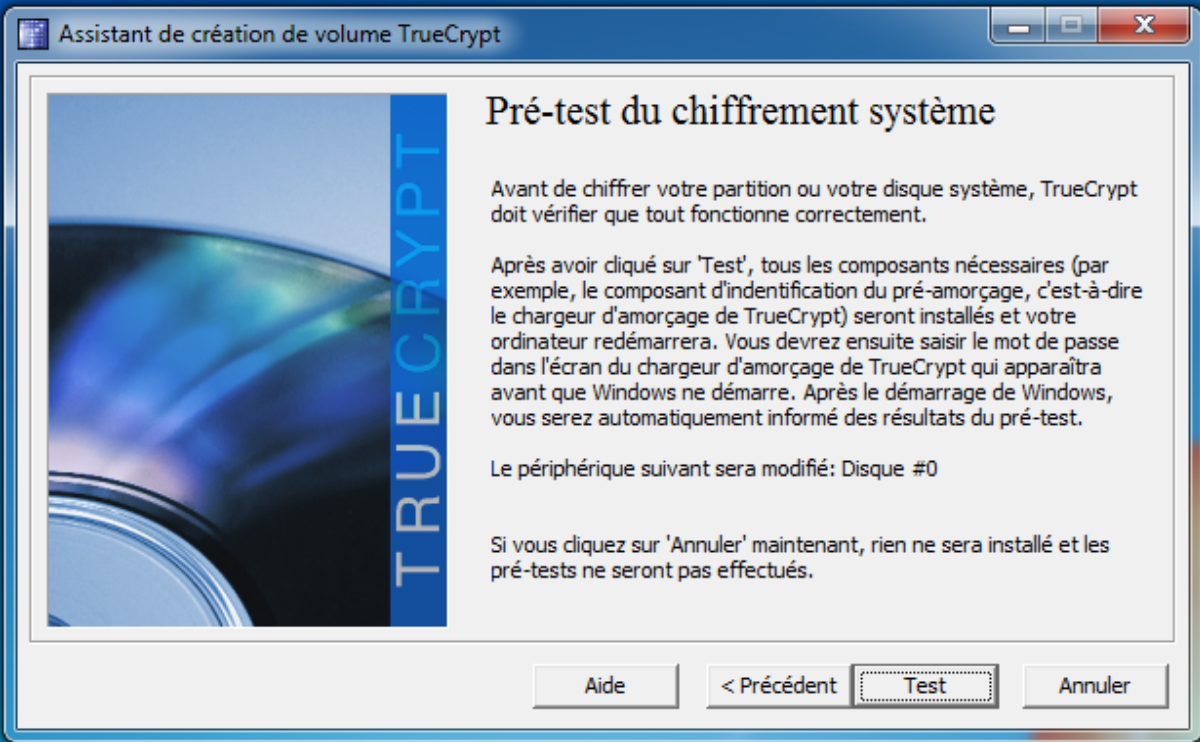
Vérification que le disque de secours a bien été gravé.



Mode de nettoyage  
Choisir aucun

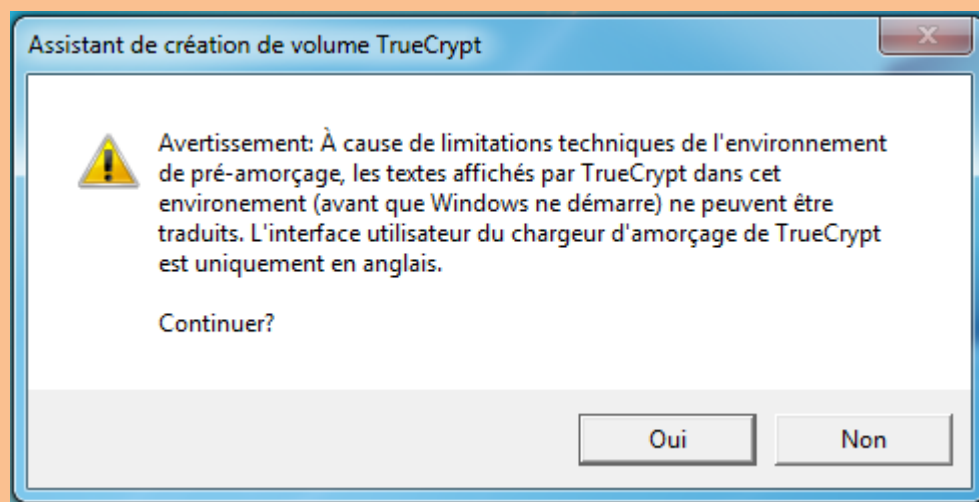
(comment réécrire de manière  
chiffrée par dessus les données  
existantes afin d'éviter que les  
anciennes ne soient  
récupérables.)

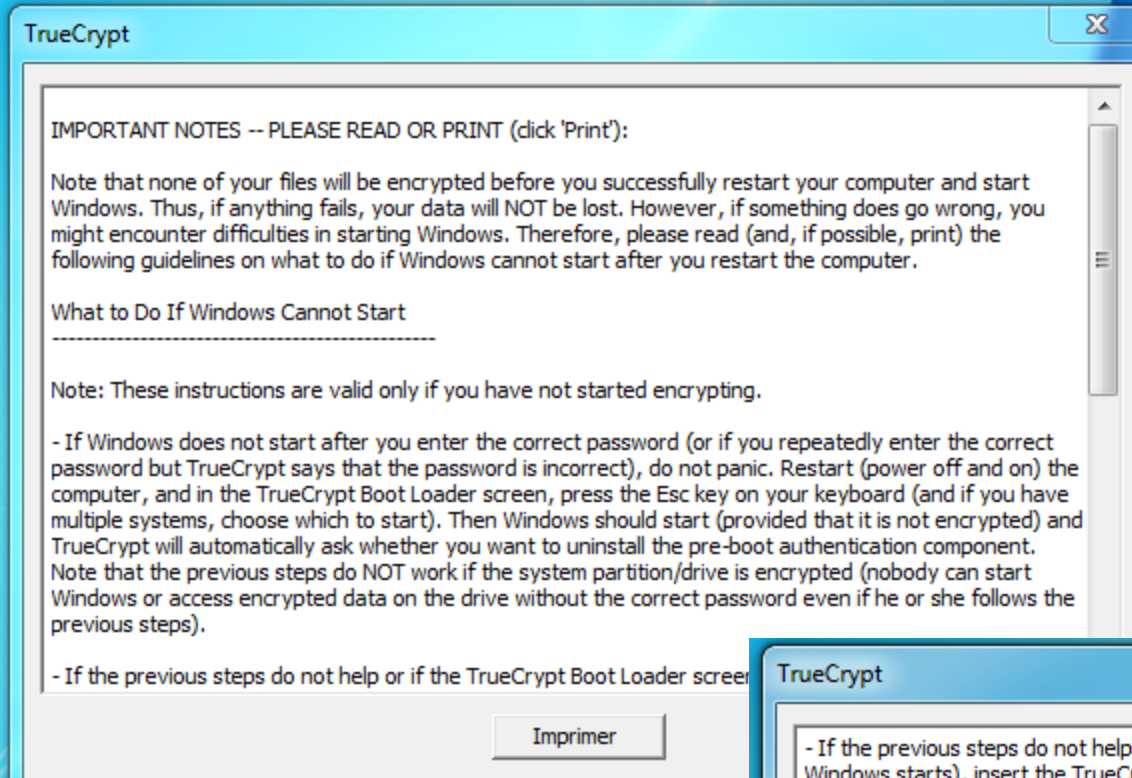




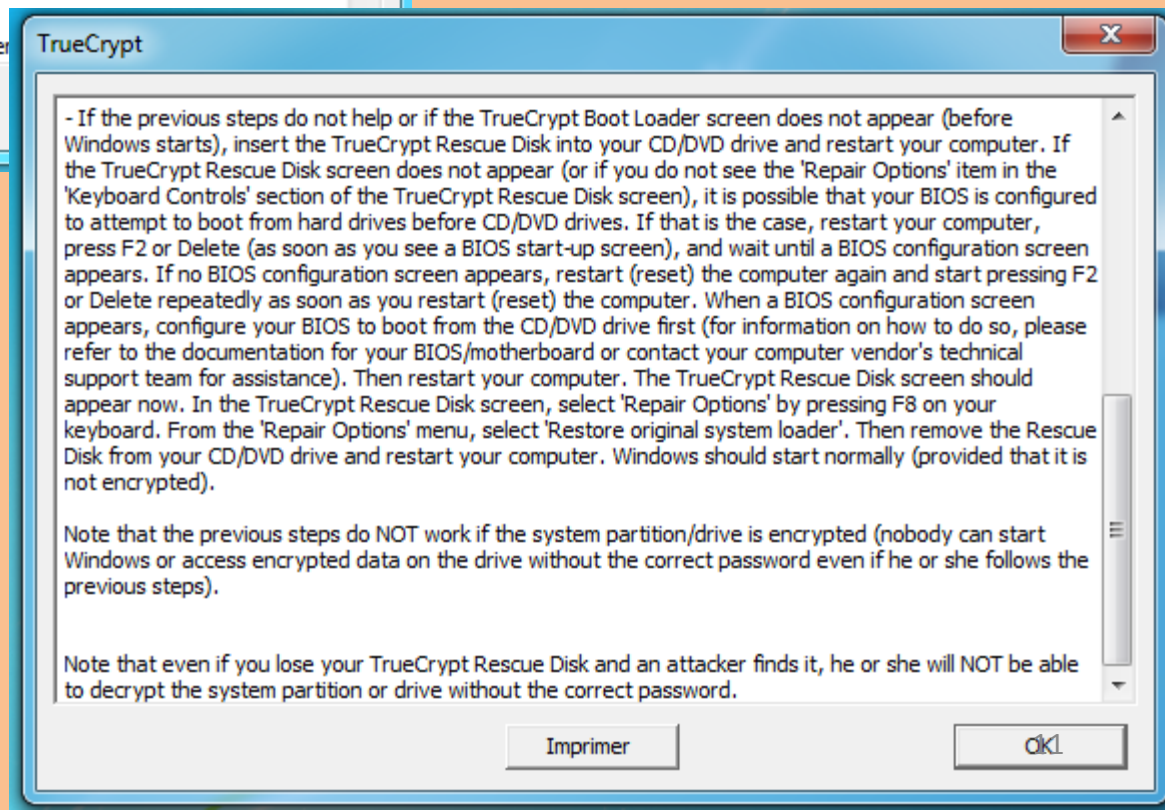
Pré-test, installation du  
bootloader sur le disque de  
démarrage

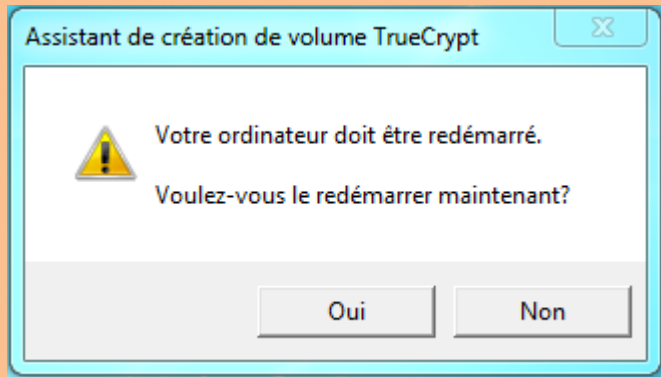
English only, pour l'interface  
utilisateur en mode DOS.





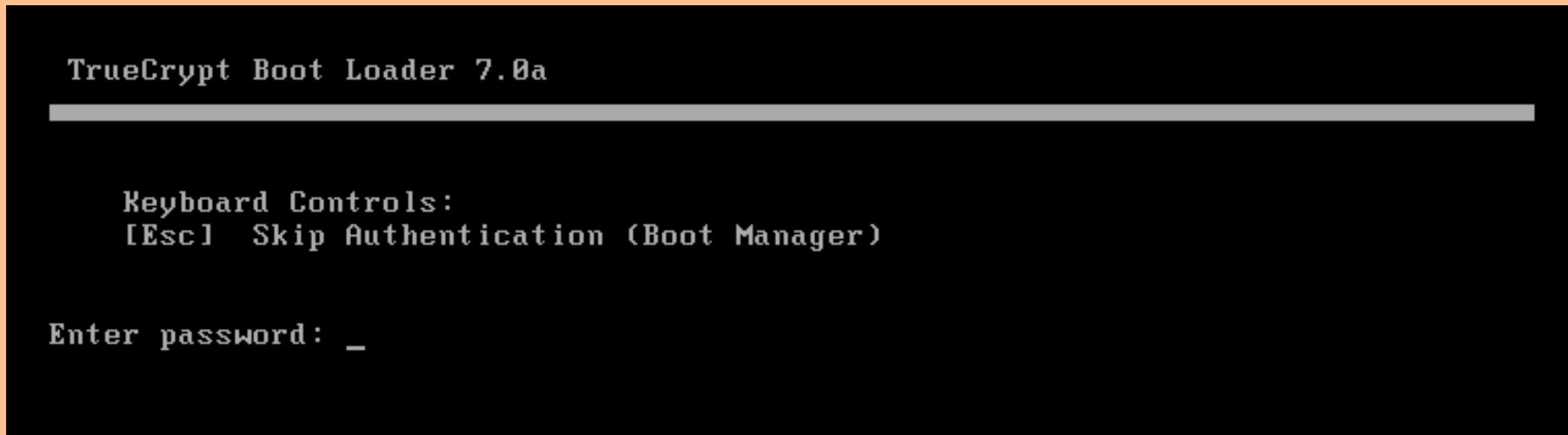
Procédure si jamais le pré-test  
n'est pas concluant.

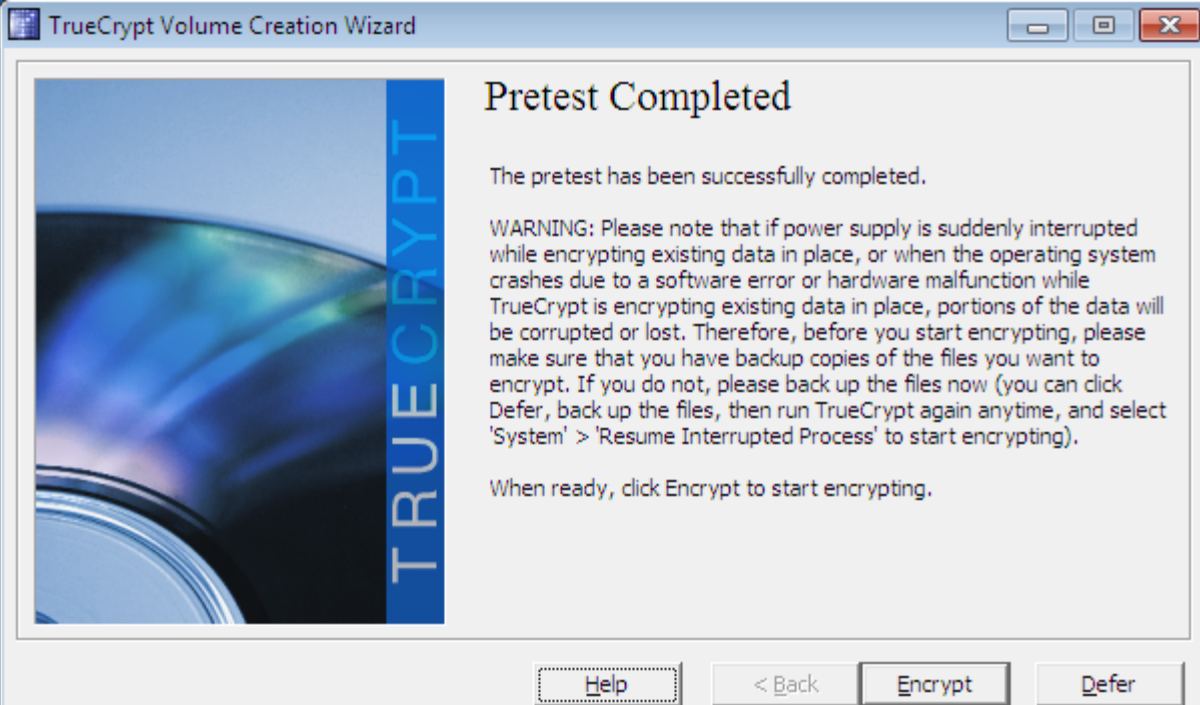




Reboot pour lancer le pré-test

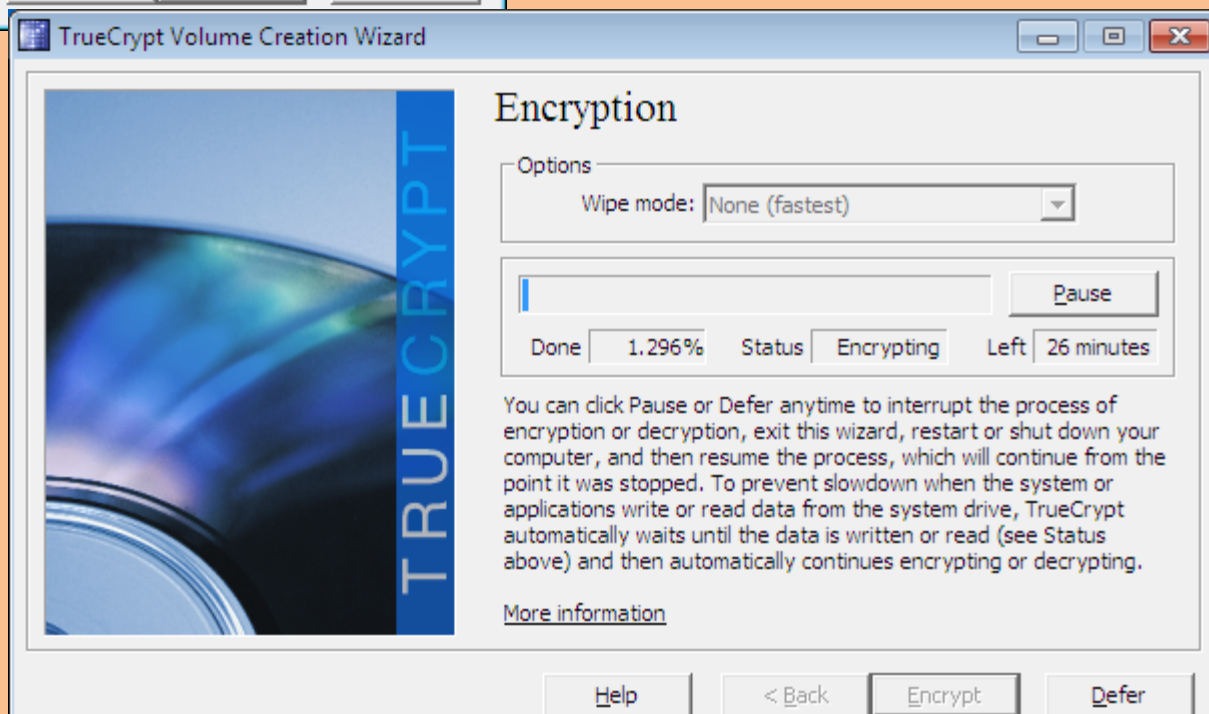
Saisie du mot de passe pour amorcer le système





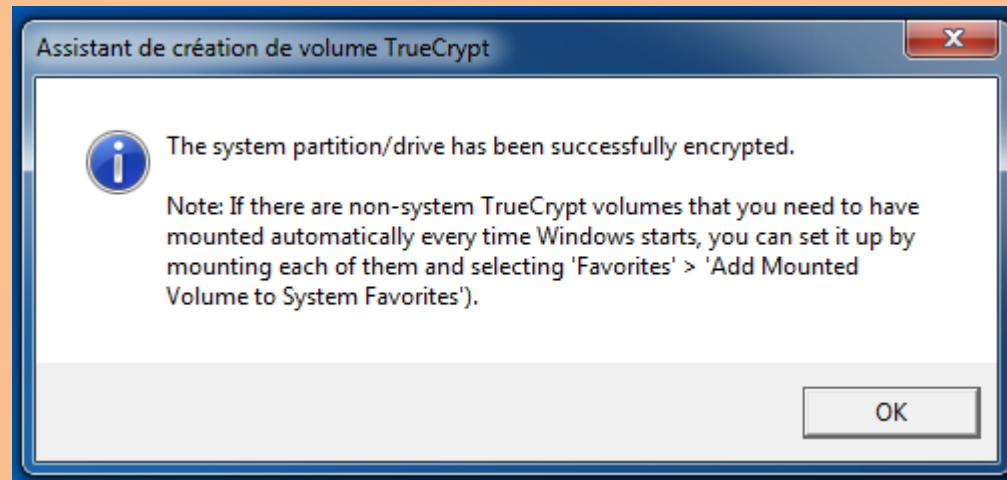
Pré-test concluant

Lancement du chiffrement du  
disque.  
5h/500Go  
Interruptible  
Ralentit par l'activité système

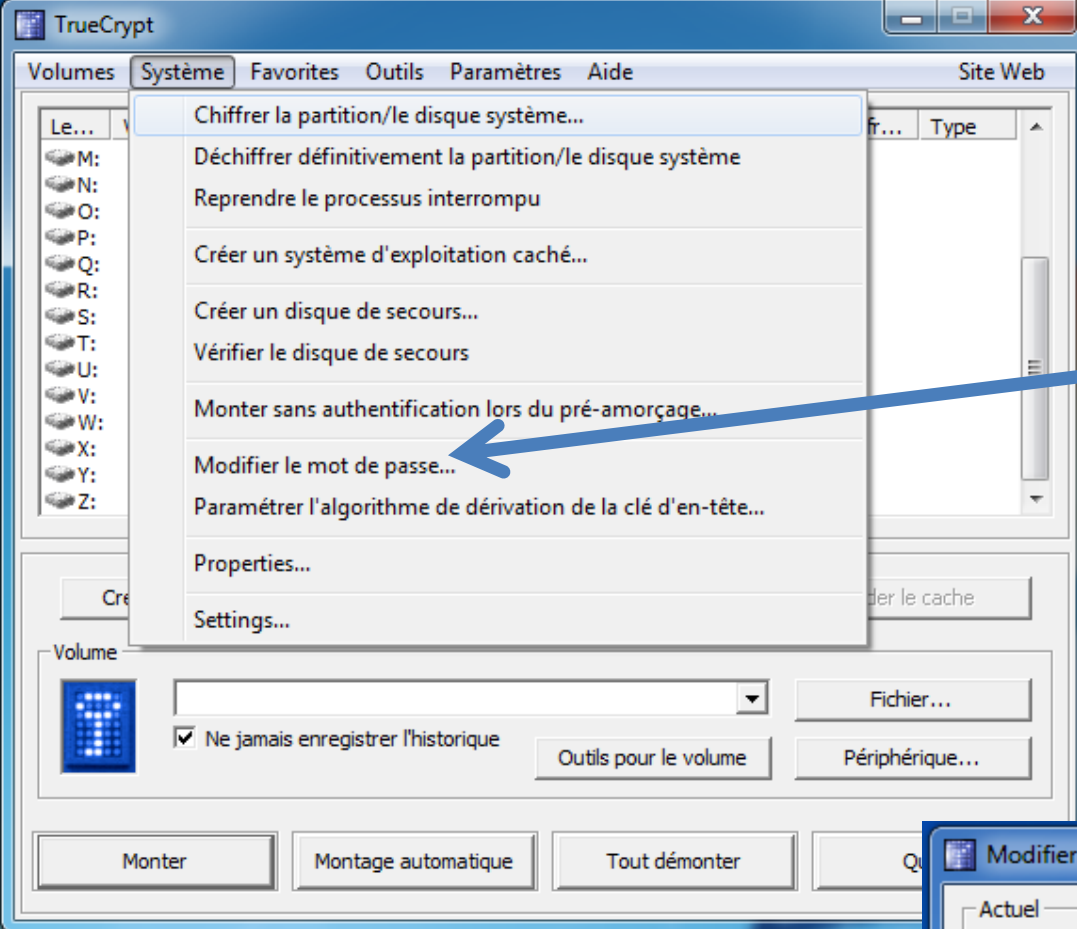




## Fin du chiffrement

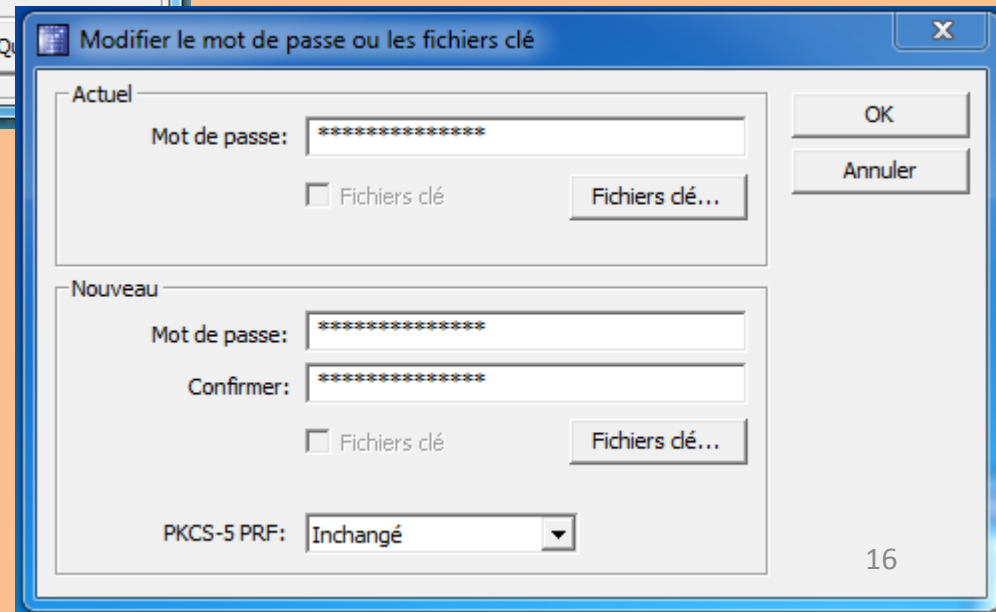


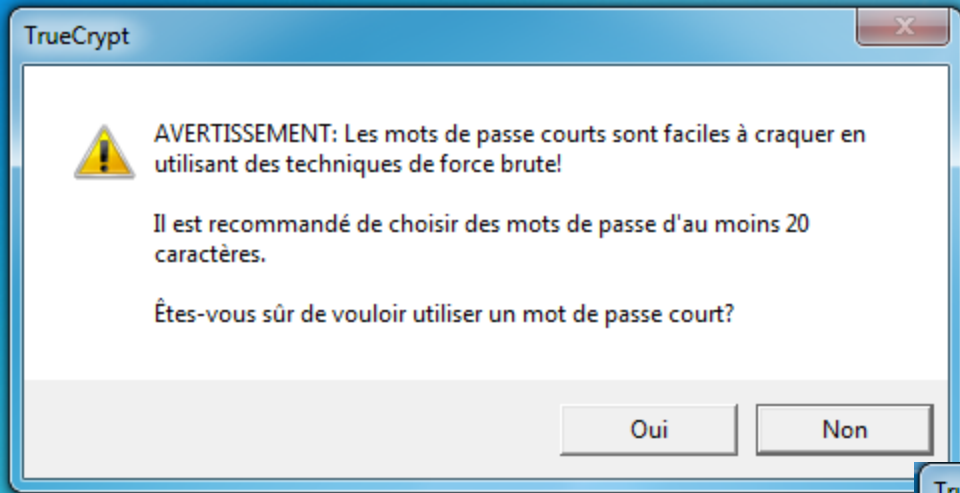
# Changement du mot de passe



Changement du mot de passe de boot

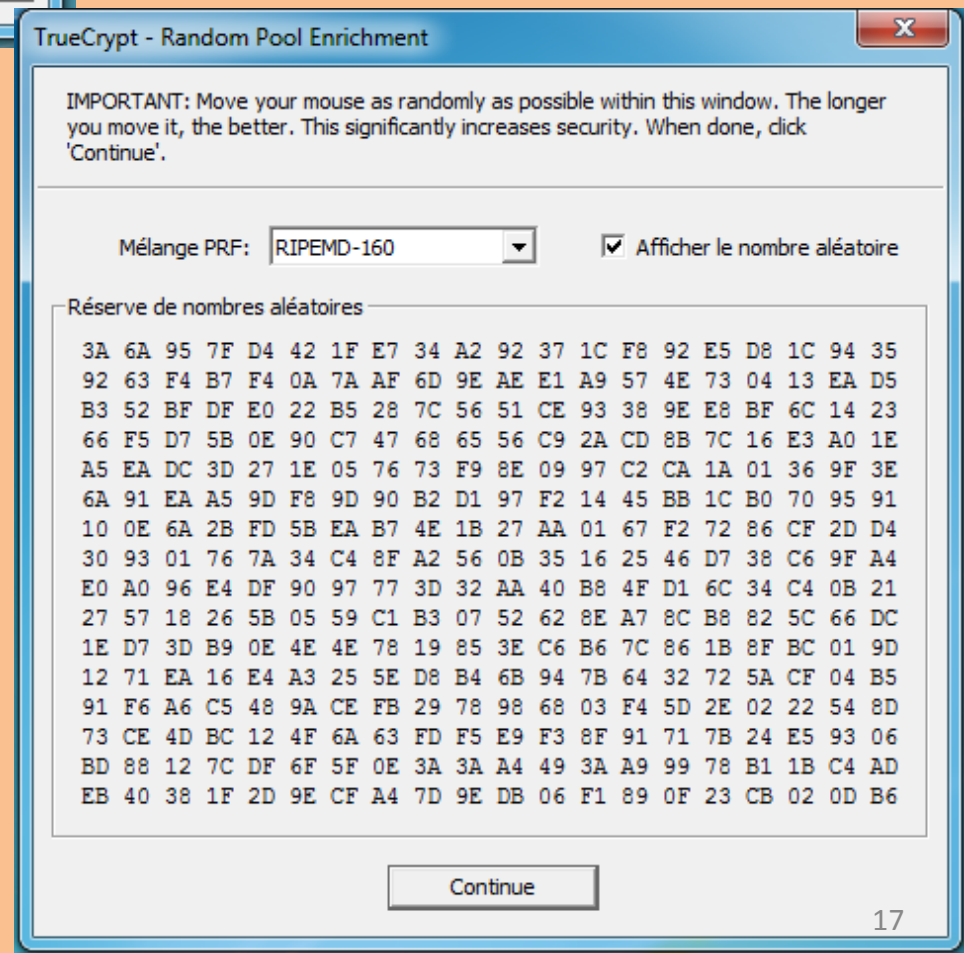
Saisie de l'ancien mot de passe et deux fois le nouveau

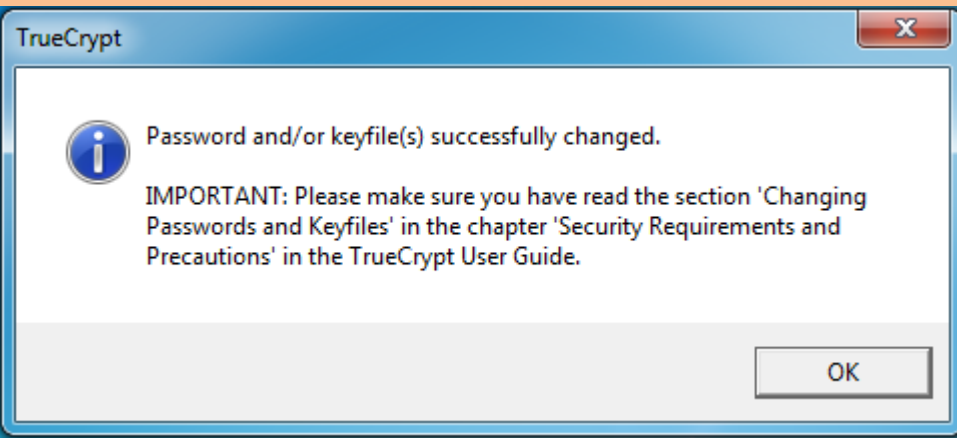




Saisie du mot de passe  
(>10 caractères)

Randomisation de la clé par le  
déplacement de la souris

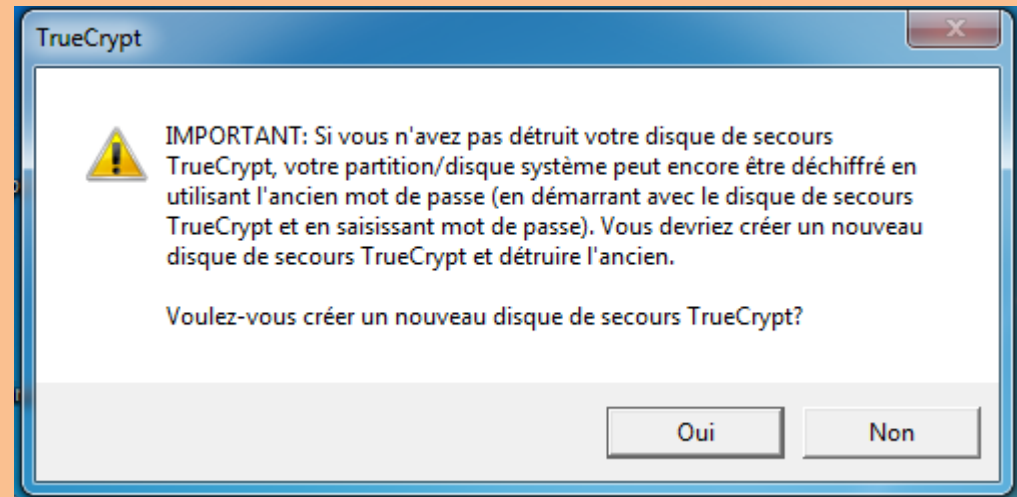




Mot de passe changé

Possibilité de créer un disque de secours avec le nouveau mot de passe

Répondre « non » dans notre cas





Dépannage oubli du mot de passe  
Restauration à partir du CD

- Graver le CD de restauration avec le mot de passe connu
- Booter sur le CD

```
TrueCrypt Rescue Disk 7.0a
-----

Keyboard Controls:
[Esc] Skip Authentication (Boot Manager)
[F8]  Repair Options

Enter password: _
```

- F8 Pour les Options de réparations

- Choisir l'option 3 pour restaurer le mot de passe d'origine

```
TrueCrypt Rescue Disk 7.0a
Available Repair Options:
[1]  Permanently decrypt system partition/drive
[2]  Restore TrueCrypt Boot Loader
[3]  Restore key data (volume header)
[4]  Restore original system loader
[Esc] Cancel
To select, press 1-9: _
```

- utiliser le mot de passe original