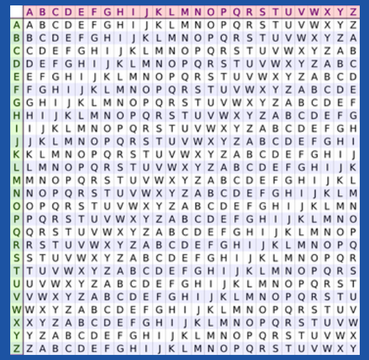
TP- CHIFFREMENT

Ladriere Valentine

Etude et Recherche

1. Le Code César
Un chiffrement par substitution monoalphabétique dans lequel chaque lettre du message est remplacée par une autre lettre située un certain nombre de positions plus loin dans l'alphabet.
Exemple : avec un décalage de 3, A devient D, B devient E, etc.

2. Le Carré de Vigenère
Un chiffrement par substitution polyalphabétique utilisant une clé (un mot) pour décaler les lettres du message selon plusieurs alphabets (un par lettre de la clé). Il utilise un tableau appelé carré de Vigenère pour appliquer le décalage.

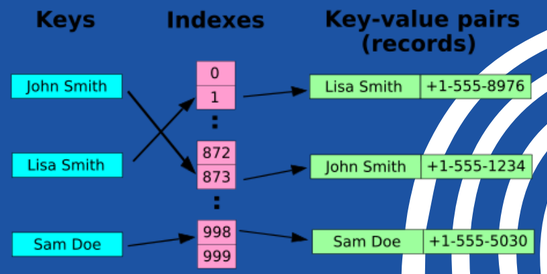


3. La machine « Enigma »
Une machine de chiffrement électromécanique utilisée par l'Allemagne nazie pendant la Seconde Guerre mondiale. Elle utilisait des rotors pour produire un chiffrement complexe, difficile à casser sans connaître la configuration exacte.

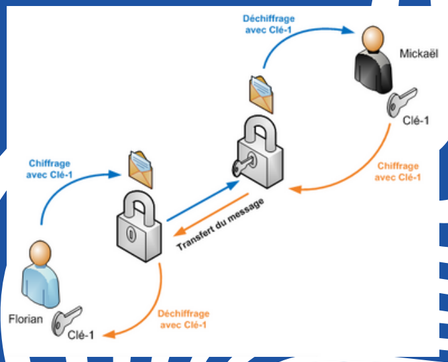
Etude et Recherche

4. Le téléphone rouge
Nom symbolique donné à la ligne de communication directe sécurisée entre les dirigeants des États-Unis et de l'Union soviétique (mise en place après la crise de Cuba en 1962). Il ne s'agissait pas réellement d'un téléphone rouge, mais plutôt d'un système de télétype chiffré.

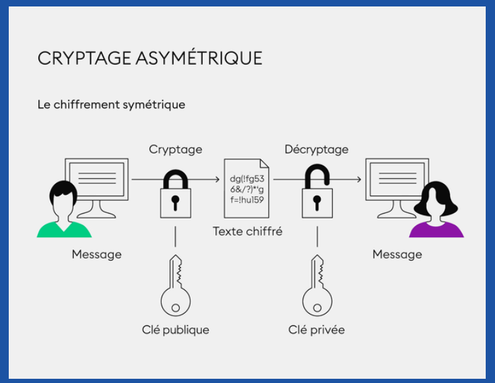
5. Le hachage
Un algorithme qui transforme une donnée (ex : mot de passe, fichier) en une empreinte unique de taille fixe, appelée hash. Il est non réversible, utilisé pour vérifier l'intégrité ou stocker des mots de passe.



6. Le chiffrement à clé symétrique
Un système de chiffrement où la même clé est utilisée pour chiffrer et déchiffrer les données. Exemple : AES, DES. Rapide mais nécessite un échange sécurisé de la clé.

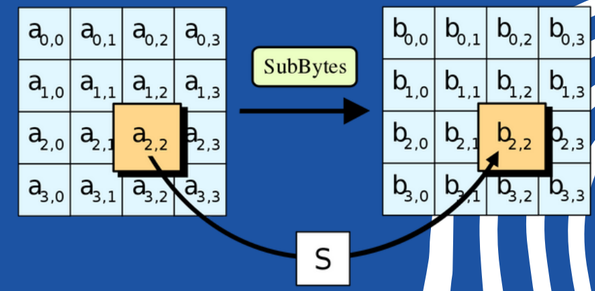


Etude et Recherche



7. Le chiffrement à clé asymétrique
Utilise une paire de clés : une clé publique pour chiffrer, et une clé privée pour déchiffrer. Exemple : RSA. Permet des échanges sécurisés sans partager la clé privée.

8. Le chiffrement AES
Advanced Encryption Standard, un algorithme de chiffrement symétrique très utilisé aujourd'hui. Il fonctionne par blocs de 128 bits, avec des clés de 128, 192 ou 256 bits. Il est considéré comme très sécurisé.

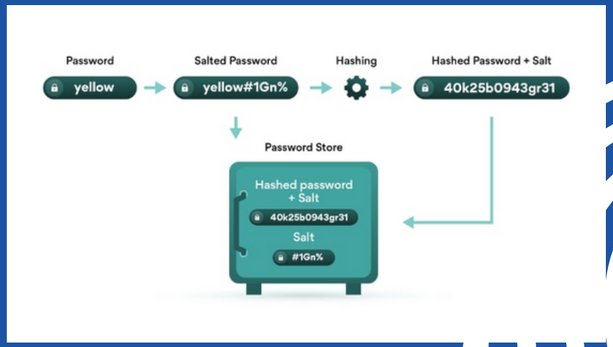


9. Différence entre chiffrement bijectif et hachage

- Le chiffrement bijectif est réversible (on peut retrouver les données originales avec la clé).
- Le hachage est non réversible : on ne peut pas retrouver le message initial à partir du hash.

Etude et Recherche

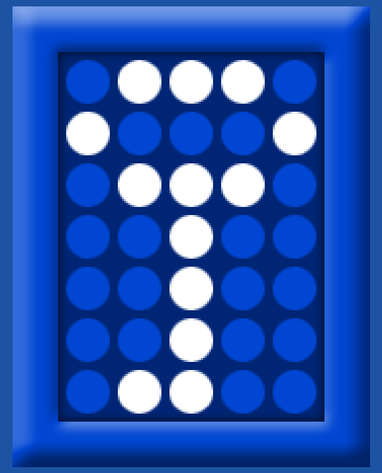
10. Limites du hachage des mots de passe
    - Si deux utilisateurs ont le même mot de passe, leur hash sera le même → attaque par dictionnaire.
    - Des tables de correspondance (rainbow tables) peuvent être utilisées pour retrouver des mots de passe faibles.



11. Le salage des mots de passe
Ajout d'une valeur aléatoire (sel) au mot de passe avant de le hacher, pour éviter que deux mots de passe identiques aient le même hash. Cela renforce la sécurité contre les attaques par dictionnaire ou rainbow table.

12. La stéganographie
Technique de cacher un message dans un autre contenu (image, son, texte…) de façon invisible. Contrairement au chiffrement, le message caché n'attire pas l'attention.

Le logiciel de chiffrement Truecrypt



Le logiciel permet de créer des volumes chiffrés sur un disque dur ou une clé USB :
Ces volumes se présentent comme des fichiers normaux mais sont en fait des conteneurs chiffrés.
Une fois monté avec le mot de passe correct, le volume se comporte comme un disque dur virtuel, dans lequel tu peux stocker des fichiers normalement.

Fonctionnement général :

1) Création d'un volume chiffré :

- Il peut s'agir d'un fichier conteneur (coffre virtuel), d'une partition ou même du disque système entier.
- L'utilisateur choisit un mot de passe et un algorithme de chiffrement (AES, Serpent, etc.).

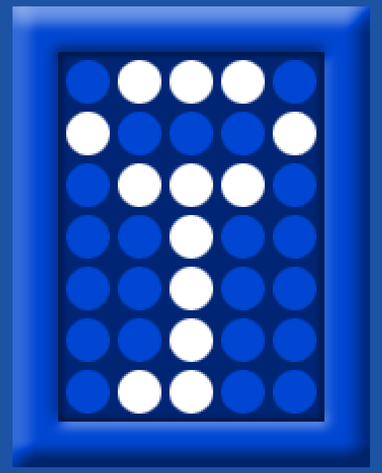
2) Montage du volume chiffré :

- Une fois ouvert avec le bon mot de passe, le volume apparaît comme un nouveau disque (ex : E:).
- L'utilisateur peut y copier, modifier ou supprimer des fichiers normalement.

3)Chiffrement transparent :

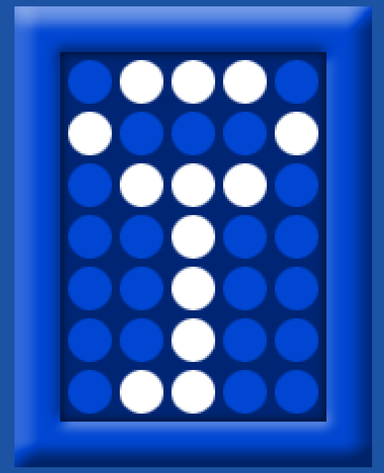
- Les données sont chiffrées/déchiffrées en temps réel, dans la mémoire vive (RAM), sans stocker les données en clair sur le disque.

Le logiciel de chiffrement Truecrypt



Aspect	TrueCrypt	Outils classiques
Chiffrement à la volée	Oui, automatique et transparent	Non, il faut souvent chiffrer/déchiffrer manuellement chac
Volume virtuel	Crée un fichier-contener agissant comme un disque dur	Chiffre des fichiers individuellement
Plausible deniability	Oui : possibilité de cacher un volume dans un autre	Non, les fichiers chiffrés sont clairement visibles
Chiffrement système	Possible (disque système ou partitions)	Rare ou limité
Multi-algorithmes combinés	Possibilité de combiner AES, Serpent, Twofish	Souvent limité à un seul algorithme (ex : AES seulement)

Le logiciel de chiffrement Truecrypt



Intérêt d’utiliser Truecrypt au sein d’une société.

TrueCrypt permet de protéger efficacement les fichiers sensibles (documents RH, données clients, projets internes, etc.) contre :

- Les accès non autorisés,
- Le vol de matériel (PC, disques durs, clés USB),
- Les fuites de données en cas de perte d’un support.

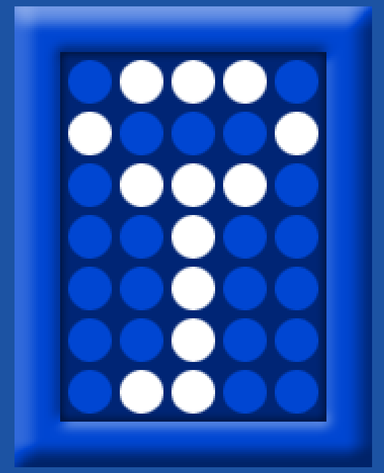
Grâce au chiffrement à la volée, les utilisateurs peuvent travailler normalement sur leurs fichiers une fois le volume monté, sans devoir chiffrer/déchiffrer manuellement. Cela offre un bon compromis entre sécurité et simplicité d’usage.

Avec sa fonction de volume caché, TrueCrypt permet de masquer l’existence même de certaines données sensibles, ce qui peut être utile en cas de tentative d’extorsion, d’espionnage industriel ou de situation critique.

TrueCrypt n’est plus maintenu depuis 2014, ce qui peut représenter un risque de sécurité. Une entreprise souhaitant utiliser un outil similaire doit plutôt opter pour VeraCrypt, qui est basé sur TrueCrypt mais mis à jour régulièrement.

Utiliser un outil comme TrueCrypt permet à une société de renforcer la confidentialité, la conformité et la résilience de ses systèmes d’information, à condition de choisir une version sécurisée et maintenue comme VeraCrypt.

Le logiciel de chiffrement Truecrypt



Solutions alternatives à Truecrypt

VeraCrypt

- Successeur officiel de TrueCrypt, développé à partir de son code source.
- Corrige les failles de sécurité connues de TrueCrypt.
- Fonctionnalités :
- Chiffrement à la volée,
- Chiffrement de partitions/disques entiers,
- Volumes cachés,
- Gratuit et open source, multiplateforme (Windows, Linux, macOS).

BitLocker

- Solution de chiffrement intégrée à Windows.
- Permet le chiffrement complet du disque, y compris la partition système.
- Intégration native avec l’Active Directory et les politiques de groupe.

FileVault

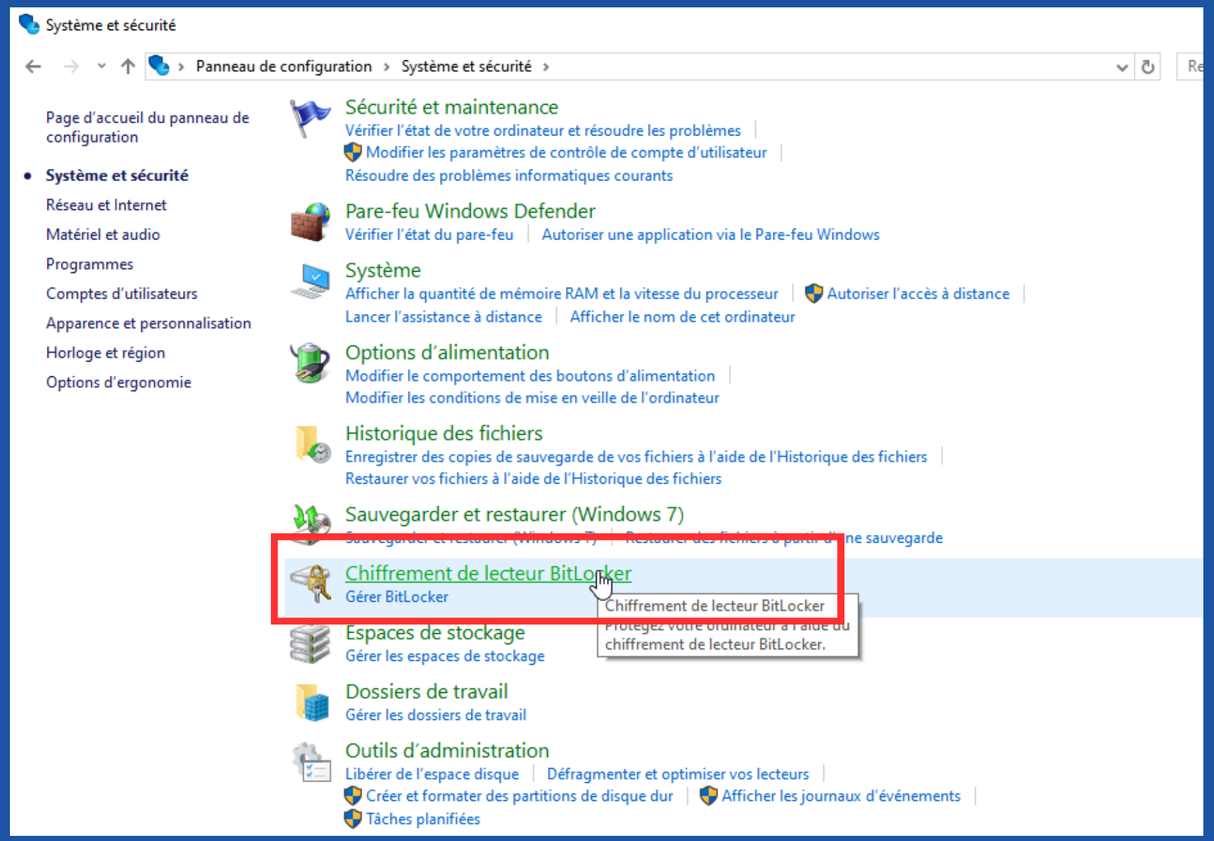
- Outil de chiffrement intégré aux Mac.
- Permet le chiffrement du disque système avec une intégration fluide à macOS.
- Utilise le chiffrement XTS-AES-128 avec une clé de 256 bits.

Mise en œuvre d’une solution de chiffrement sur Windows

Le logiciel de chiffrement Truecrypt

Étape 1 : Activer BitLocker

Clique droit sur le menu démarrer → Panneau de configuration > Système et sécurité > BitLocker Drive Encryption.

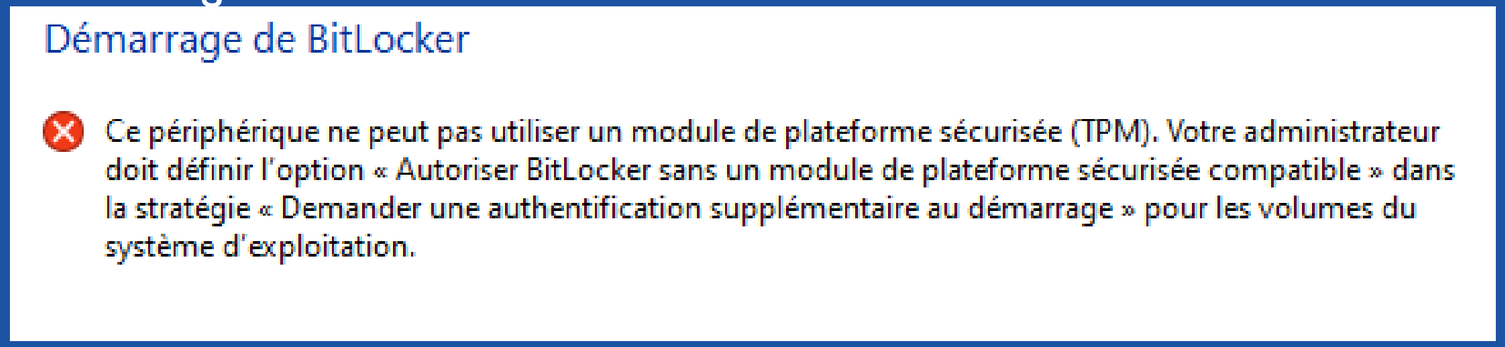


Le logiciel de chiffrement Truecrypt

Étape 1 : Activer BitLocker

Sélectionne le disque secondaire , puis clique sur Activer BitLocker.

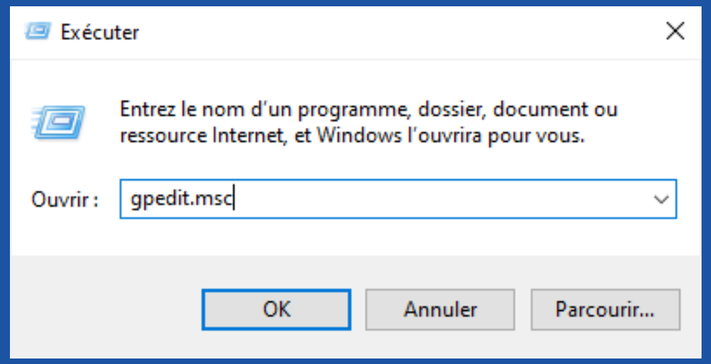
Ce message s'affiche:

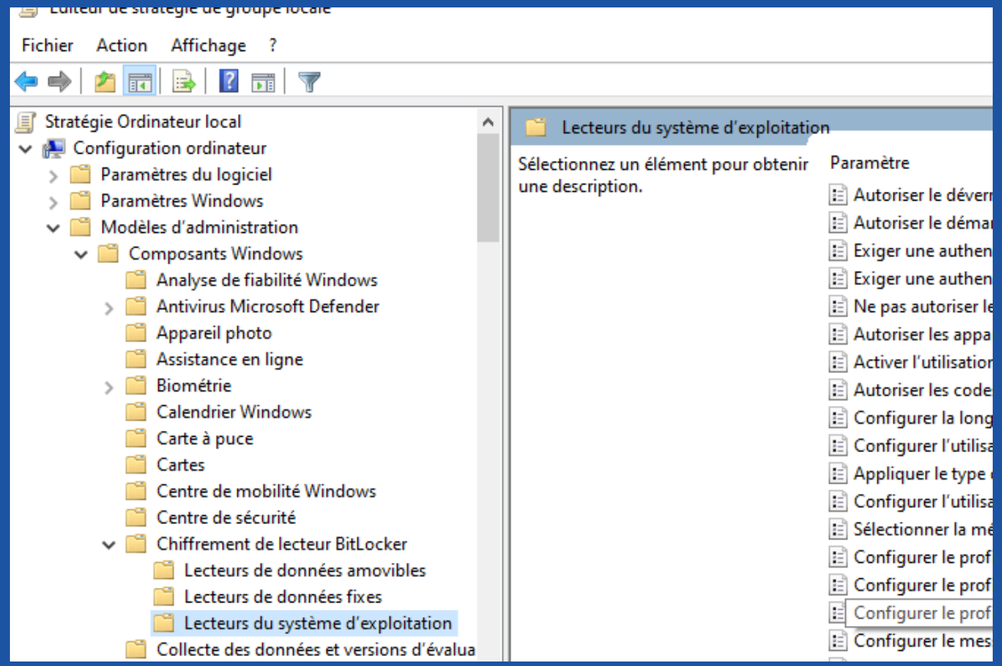


Le logiciel de chiffrement Truecrypt

Étape 1 : Activer BitLocker

Voici comment remédier au problème: Windows + R et saisir gpedit.msc



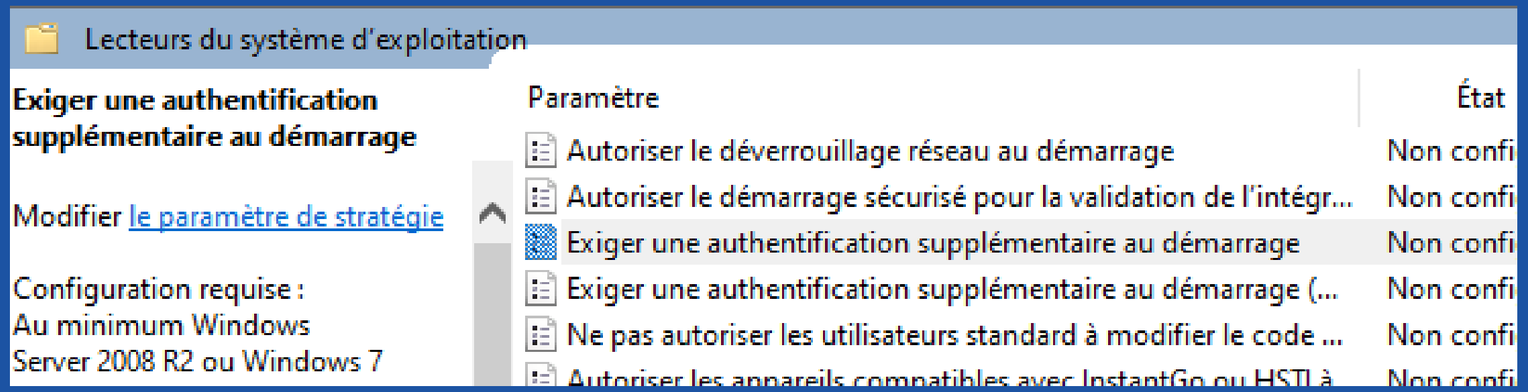


Aller dans:
Configuration ordinateur >
Modèles d'administration >
Composants Windows >
Chiffrement de lecteur BitLocker >
Lecteurs du système d'exploitation

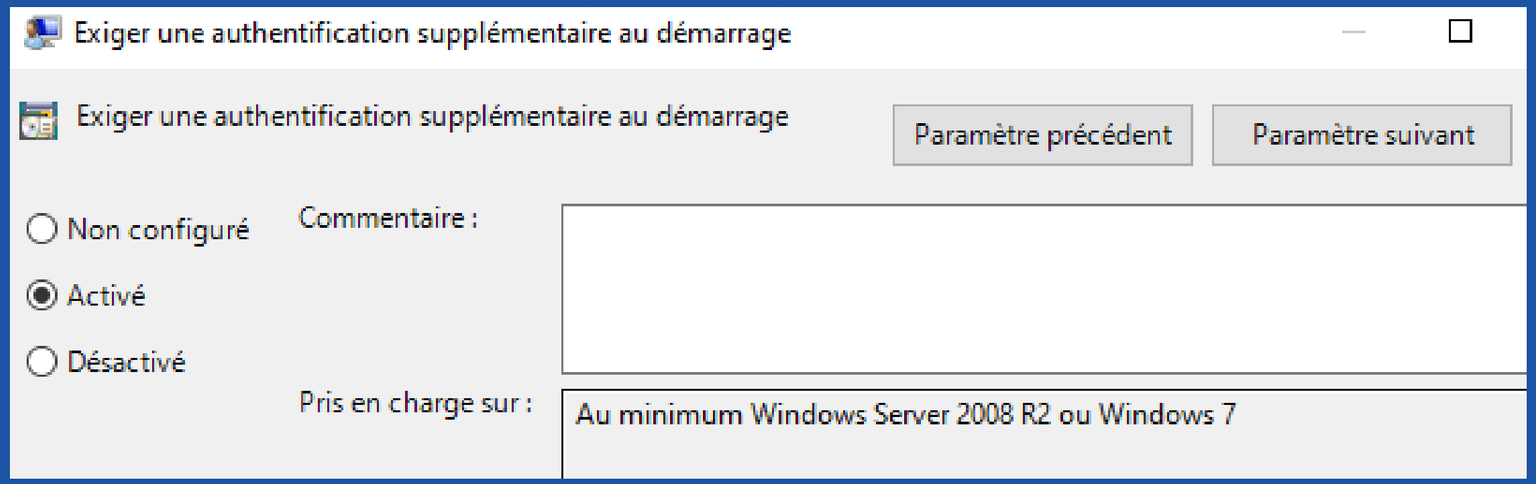
Le logiciel de chiffrement Truecrypt

Étape 1 : Activer BitLocker

Double-clique sur "Exiger une authentification supplémentaire au démarrage".



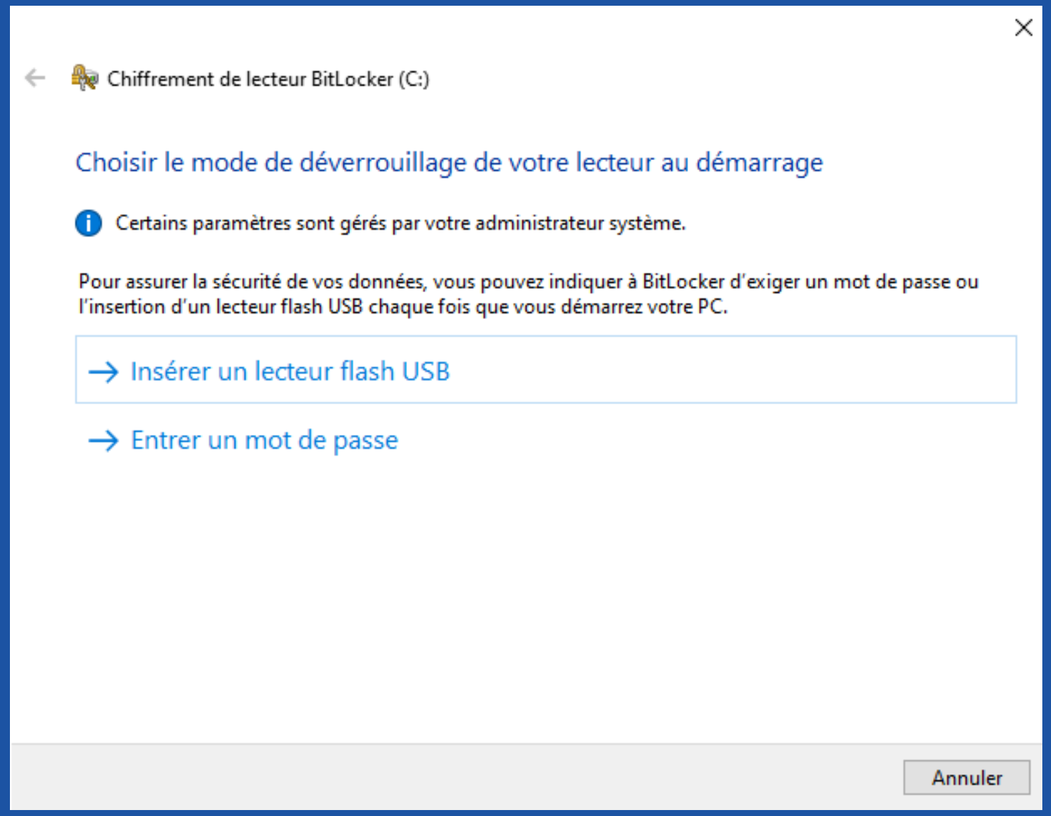
Coche "Activé". Clique sur Appliquer, puis OK.



Le logiciel de chiffrement Truecrypt

Étape 1 : Activer BitLocker

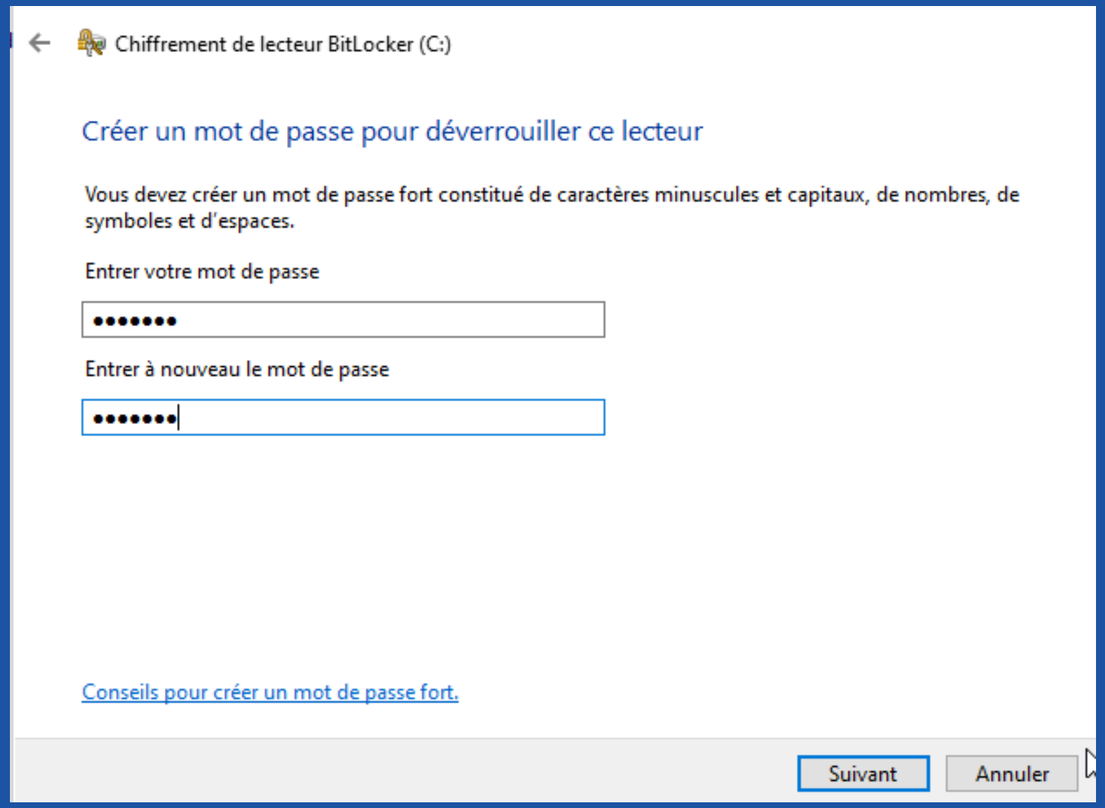
Activer BitLocker fonctionne. Cliquez sur



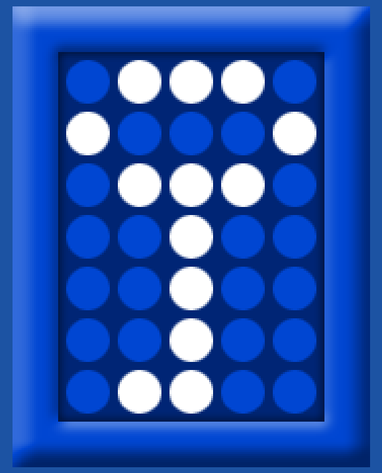
Le logiciel de chiffrement Truecrypt

Étape 1 : Activer BitLocker

Je configure un mot de passe pour déverrouiller le lecteur (btssio2025)
Enregistre la clé de récupération (dans un fichier ou imprimer)



Le logiciel de chiffrement Truecrypt



Étape 1 : Activer BitLocker

Choisis Chiffrer tout le disque, puis Mode compatible (recommandé pour disques amovibles).

Démarre le chiffrement.

Résultat :
Le disque devient chiffré.
Il est accessible seulement après authentification.