Tp\_04 Utilisation d’un gestionnaire de mots de passe - Keepass

MERZOUGUI Shayma et VIALETTE CANDICE

B3-Sécurité au niveau des utilisateurs

2024-2025

Table des matières

[Introduction : 2](#_Toc182613639)

[1. Définition d’une nouvelle base et d’un mot de passe maître. 2](#_Toc182613640)

[a. Création de la nouvelle table 2](#_Toc182613641)

[b. Paramétrage de sécurité : 4](#_Toc182613642)

[2. Les deux algorithmes de chiffrement possibles et leur longueur de clé. 5](#_Toc182613643)

[3. Les groupes proposés par défaut par KeePass. 6](#_Toc182613644)

[4. Dans quel groupe existant mettre l’entrée pour l’utilisation d’Outlook d’Office 365 ? 6](#_Toc182613645)

[5. Création, détaille et illustration de l’utilisation d’Outlook. 7](#_Toc182613646)

[6. Présentation et Création du Groupe « BTS SIO » 8](#_Toc182613647)

[7. Présentation et création d’une entrée JobReady 10](#_Toc182613648)

[8. Automatiser les entrées 13](#_Toc182613649)

[9. Mode d’emploi des entrées créées dans KeePass. 14](#_Toc182613650)

[10. Avantage et inconvénients de KeePass 17](#_Toc182613651)

[a. Avantages : 17](#_Toc182613652)

[b. Inconvénients : 17](#_Toc182613653)

[Conclusion 18](#_Toc182613654)

[Source 19](#_Toc182613655)

# Introduction :

Pour la sécurité de nos comptes en ligne, le changement de mot de passe fréquent et des mots de passes longs et compliqués sont recommandés. Pour pallier cette difficulté, nous pouvons utiliser un gestionnaire de mots de passe. Un logiciel qui permet à un utilisateur de gérer ses mots de passe, en centralisant l'ensemble de ses identifiants et ses mots de passe dans base de données. Il est protégé par un mot de passe unique, le seul que l'utilisateur doit de retenir. Nous allons nous servir du logiciel KeyPass, un gestionnaire gratuit, portable (installé sur des périphériques de stockage) et sécurisé (chiffrement AES-256).

# Définition d’une nouvelle base et d’un mot de passe maître.

## Création de la nouvelle table

|  |  |
| --- | --- |
| Une image contenant texte, capture d’écran, Police  Description générée automatiquement | Nos données seront enregistrées dans un fichier spécifique au format KeePass.  On doit choisir l’endroit où ce fichier de base de données sera sauvegardé.  Une copie de ce fichier de base de données sur un autre support de stockage est vivement conseillée pour sa sauvegarde.  Le message d’avertissement qu’on voit quand on crée une nouvelle base veut dire qu’il ne faut surtout pas oublier le mot de passe maître. Si on le perd, on ne pourra plus accéder à la base parce que tout est sécurisé avec un chiffrement. C’est pour ça qu’il faut choisir un mot de passe fort, mais qu’on peut retenir facilement. |

|  |  |
| --- | --- |
| Une image contenant texte, capture d’écran, Police, nombre  Description générée automatiquement | Choix de l’emplacement et du nom du fichier. |
| Une image contenant texte, capture d’écran, Police, ligne  Description générée automatiquement | Création du seul mot de passe qu’on devra se souvenir |
| Une image contenant texte, Police, ligne, capture d’écran  Description générée automatiquement | Appellation de la base de données et une description si besoin |
| Une image contenant texte, capture d’écran, Police  Description générée automatiquement | Une feuille de secours est créée en cas d’oubli du mot de passe. |

## Paramétrage de sécurité :

|  |  |
| --- | --- |
|  | Ferme l’accès aux mots de passe lorsque l'application est réduite pour que les mots de passe restent invisibles. |
|  | Ressemblant à celle du haut mais pour la zone de notification. |
|  | Verrouillage de KeyPass en même temps que l’ordinateur pour que personne n’accède aux mots de passe. |
|  | Verrouillage de KeyPass en même temps que la mise en veille de l’ordinateur. |
|  | Verrouillage de KeyPass si un tiers prendre le contrôle de l’ordinateur à distance. |
|  | Fermeture complète de KeyPass après x temps d’inactivité. |
|  | KeyPass se ferme au lieu de simplement se verrouiller. |

Le 3, 4, 5 et 6 sont des cases à cocher pour nous car on rendra nos mots de passe invisible sur notre PC et l’accès à nos comptes impossibles si on s’absente trop longtemps. Nous avons aussi mis un délai pour verrouiller l’espace de travail après une période d’inactivité de l’utilisateur globale ( nous avons mis 600 seconde)

Une image contenant texte, Appareils électroniques, capture d’écran, logiciel

Description générée automatiquement

Une image contenant texte, Appareils électroniques, capture d’écran, logiciel

Description générée automatiquement

# Les deux algorithmes de chiffrement possibles et leur longueur de clé.

KeePass utilise deux algorithmes de cryptographie :

* **AES** : Clé de 256 bits.
* **Twofish** : Blocs de 128 bits, clé de 256 bits.

**AES** (Advanced Encryption Standard) est un algorithme qu’on utilise beaucoup pour sécuriser les données. Il est rapide, fiable et utilise une clé de 256 bits, ce qui le rend hyper difficile à pirater.

**Twofish**, c’est un autre algorithme de chiffrement. Il est un peu moins connu qu’AES, mais il est tout aussi sécurisé. Il fonctionne avec des blocs de 128 bits et une clé de 256 bits, mais il peut être un peu plus lent qu’AES.

# Les groupes proposés par défaut par KeePass.

Les groupes proposés par défaut sont :

* Général pour tous les mots de passe.
* Windows pour les mots de passe qui sont en liens à Windows.
* Réseau pour les différents mots de passe des réseaux.
* Internet pour les mots de passe liées à internet.
* Courriel pour les comptes de messagerie électronique.
* Banque à domicile pour les mots de passe en liens avec la finance.

Une image contenant texte, Police, logiciel, Icône d’ordinateur

Description générée automatiquement

# Dans quel groupe existant mettre l’entrée pour l’utilisation d’Outlook d’Office 365 ?

L’entrée pour l’utilisation d’Outlook d’Office 365 sera mis dans le groupe Courriel, car il est spécifiquement dédié aux services de messagerie électronique.

# Création, détaille et illustration de l’utilisation d’Outlook.

|  |  |
| --- | --- |
|  | Nous nous mettons dans le groupe Courriel car Outlook est un service de messagerie électronique. |
| Une image contenant texte, Appareils électroniques, capture d’écran, logiciel  Description générée automatiquement | En premier, le Titre :  Ici le champ Titre contient « Outlook Office 365 ». C’est le nom que l’on donne à l’entrée pour identifier facilement à quoi elle correspond.  En deuxième, le Nom d’utilisateur :  Ici, il contient mon address e-mail du BTS SIO. C’est l’identifiant nécessaire pour me connecter a mon compte Outlook 365.  En troisième, le Mot de passe :  Soit le gestionnaire de mots de passe en génère un automatiquement, soit on rentre notre mot de passe à nous.  On voit ici que la qualité est de 136 bits donc dans le vert, ce qui est largement suffisant pour sécuriser le compte. Il y a aussi une confirmation, ou l’on doit répéter notre mot de passe pour vérifier qu’il soit correct.  En quatrième, l’Adresse (URL) :  Le champ Adresse (URL) contient le lien direct pour accéder à la page de connexion d’Outlook (Office 365).  Ici, l’URL est : <https://login.live.com/>....  C’est pratique, car on peut cliquer directement sur ce lien depuis KeePass pour ouvrir la page de connexion.  En cinquième, Date d’expiration :  Ici la date d’expiration est configurée automatiquement au 15/11/2024 à minuit (car il n’a pas été changé)  Ca permet de nous rappeler qu’il faudra surement changer son mot de passe à cette date pour renforcer la sécurité. |
| Une image contenant texte, capture d’écran, logiciel, Police  Description générée automatiquement | Et pour finir nous pouvons voir notre entrée, avec notre mot de passe (flouté), notre nom d’utilisateur, le Titre et enfin l’adresse URL cliquable. |

# Présentation et Création du Groupe « BTS SIO »

|  |  |  |
| --- | --- | --- |
|  | | On ajoute un groupe sous le Nom BTS SIO on peut aussi choisir l’Icône, ici nous avons choisis l’icône d’un dossier. |
|  | En premier, le Titre :  Ici le champ Titre contient « Réseau SIO».  En deuxième, le Nom d’utilisateur :  Ici, il contient mon nom d’utilisateur Réseau du BTS SIO « UTI022 ».  En troisième, le Mot de passe :  On voit ici que la qualité est de 96 bits donc dans le vert, ce qui est suffisant pour sécuriser le compte (améliorable).  En quatrième, l’Adresse (URL) :  Ici nous n’avons pas besoin d’adresse (URL), car il n’y en a tout simplement pas.  En cinquième, Date d’expiration :  Ici la date d’expiration est configurée automatiquement au 14/11/2024 à minuit (car il n’a pas été changé) | |
|  | En premier, le Titre :  Ici le champ Titre contient « Netacad (Académie Cisco)».  En deuxième, le Nom d’utilisateur :  Ici, il contient mon nom d’utilisateur de mon compte Netacad « Merzouguishayma24@gmail.com».  En troisième, le Mot de passe :  On voit ici que la qualité est de 47 bits donc dans le jaune, ce qui est insuffisant pour sécuriser le compte, donc il faut le changer.  En quatrième, l’Adresse (URL) :  Le champ Adresse (URL) contient le lien direct pour accéder à la page d’accueil de Netacad, car le lien direct pour la page de connexion ne fonctionne pas.  Ici, l’URL est : <https://www.netacad.com/>  En cinquième, Date d’expiration :  Ici la date d’expiration est configurée automatiquement au 14/11/2024 à minuit (car il n’a pas été changé) | |
| Une image contenant texte, capture d’écran, Police, ligne  Description générée automatiquement | Et pour finir nous pouvons voir nos entrées, avec nos mots de passe (flouté), nos noms d’utilisateur, les Titre et enfin l’adresse URL cliquable.  Tout ça dans le groupe BTS SIO | |

# Présentation et création d’une entrée JobReady

|  |  |
| --- | --- |
| Une image contenant texte, Appareils électroniques, capture d’écran, logiciel  Description générée automatiquement | En premier, le Titre :  Ici le champ Titre contient « JobReady INGE+».  En deuxième, le Nom d’utilisateur :  Ici, il contient mon nom d’utilisateur de mon compte JobReady « Merzouguishayma24@gmail.com».  En troisième, le Mot de passe :  On voit ici que KeePass m’a généré un mot de passe fort ou la qualité est de 113 bits donc dans le vert, ce qui est suffisant pour sécuriser le compte, mais ça ne me suffisait pas. |
| Une image contenant texte, Police, ligne, diagramme  Description générée automatiquement | Pour cela on clique sur Générer un mot de passe tout a droite du champ « Confirmation » |
| Une image contenant texte, capture d’écran, Police, logiciel  Description générée automatiquement | Puis on clique sur « Ouvrir le générateur de mot de passe » |
| Une image contenant texte, Appareils électroniques, capture d’écran, logiciel  Description générée automatiquement | On n’arrive donc sur cette page, qui sert à paramétré les options de génération de mots de passe selon nos choix. Ici j’ai ajouté 2 cases :   * Trait de soulignement souligné (\_) * Spéciaux ( !, $, %, & …)   Ce qui permet de le modifier autant que vous le voulez, si vous voulez aussi qu’il soit plus compliqué ou plus simplifié. |
| Une image contenant texte, Appareils électroniques, capture d’écran, logiciel  Description générée automatiquement | Donc ici on peut voir que le mot de passe a changé, et la qualité aussi il est passé a 130 bits avec des caractères spéciaux en plus.  En quatrième, l’Adresse (URL) :  Le champ Adresse (URL) contient le lien direct pour accéder à la page de connexion de JobReady.  En cinquième, Date d’expiration :  Ici la date d’expiration est configurée automatiquement au 14/11/2024 à minuit (car il n’a pas été changé) |
| Une image contenant texte, capture d’écran, Police, logiciel  Description générée automatiquement | Et pour finir nous pouvons voir notre entrée, avec notre mot de passe (flouté), notre nom d’utilisateur, le Titre et enfin l’adresse URL cliquable. |

# Automatiser les entrées

|  |  |
| --- | --- |
| Une image contenant texte, Appareils électroniques, capture d’écran, affichage  Description générée automatiquement | Dans l’entrée choisi faire clic droit, puis Editer l’entrée. |
| Une image contenant texte, capture d’écran, Police, logiciel  Description générée automatiquement | Une fois fait cliquer sur Saisie automatique. |
| Une image contenant texte, Appareils électroniques, capture d’écran, logiciel  Description générée automatiquement | Il faut s’assurer que « Activer la saisie automatique pour cette entrée » soit coché. |
| Une image contenant texte, Appareils électroniques, capture d’écran, affichage  Description générée automatiquement | Une fois tout ça de fait, revenir a la page ou les entrées sont, et refaire clic droit sur l’entrée. Une fois l’URL ouvert il n’y a plus que le raccourci CTRL + V à faire et les données se remplirons automatiquement. |

# Mode d’emploi des entrées créées dans KeePass.

Etapes pour utiliser une entrée dans KeePass :

1. Ouvrir KeePass :
   * Lancez l’application et entrez le mot de passe principal pour accéder à notre base.

Une image contenant texte, capture d’écran, logiciel, Icône d’ordinateur

Description générée automatiquement

1. Rechercher ou créer une entrée :
   * Utilisez la barre de recherche en haut pour trouver rapidement une entrée grâce à son titre.
   * Créer une entrée dans le dossier spécifique en appuyant sur ajouter une entrée.

Une image contenant texte, Police, capture d’écran, logiciel

Description générée automatiquement

Ou :

Une image contenant texte, capture d’écran, Police, ligne

Description générée automatiquement

1. Afficher les détails :
   * Si la table est déjà créée, faire double-clic sur l’entrée ou clic droit, choisir Edit l’entrée pour voir toutes les informations( Nom d’utilisateur, Mot de passe, URL).
   * Si la table n’et pas encore crée, cliquer sur Ajouter une entrée et remplir toutes les informations nécessaires.

Une image contenant texte, Appareils électroniques, capture d’écran, logiciel

Description générée automatiquement

Ou :

Une image contenant texte, capture d’écran, logiciel, affichage

Description générée automatiquement

Un mot de passe fort est déjà généré automatiquement.

1. Utiliser la saisie automatique :
   * Appuyer sur CTRL + V pour que KeePass entre automatiquement vos Identifiants. (Configuré avec la séquence {USERNAME}{TAB}{PASSWORD}{ENTER}, elle peut être modifié selon nos envie et besoin).

Une image contenant texte, Appareils électroniques, capture d’écran, affichage

Description générée automatiquement

1. Sauvegarder les modifications :
   * Après avoir utilisé ou modifié une entrée, cliquez sur Fichier 🡪 Enregistrer pour ne pas perdre nos données.

# Avantage et inconvénients de KeePass

### Avantages :

1. **Sécurité renforcée** :  
   Les mots de passe sont cryptés avec des algorithmes puissants comme AES-256, ce qui les protège bien contre les attaques.
2. **Gestion centralisée** :  
   Tous les mots de passe sont stockés dans un seul endroit, ce qui permet de les retrouver facilement.
3. **Génération de mots de passe forts** :  
   KeePass permet de créer des mots de passe complexes et uniques pour chaque compte, ce qui est très pratique pour la sécurité.
4. **Saisie automatique** :  
   Cela permet de gagner du temps en remplissant automatiquement les champs de connexion sur les sites.
5. **Portabilité** :  
   KeePass fonctionne sur plusieurs plateformes (Windows, MacOs, Linux, Android, etc.), donc il est très flexible.

### Inconvénients :

1. **Dépendance au mot de passe principal** :  
   Si on perd le mot de passe principal, on risque de ne plus avoir accès à tous les autres mots de passe enregistrés.
2. **Complexité initiale** :  
   L'installation et l'utilisation de certaines fonctions, comme la saisie automatique, peuvent être compliquées pour quelqu'un qui débute.
3. **Risque de corruption des fichiers** :  
   Si le fichier de la base de données est corrompu ou supprimé sans avoir fait de sauvegarde, toutes les données seront perdues.
4. **Vulnérabilité en cas de vol de fichier** :  
   Si le fichier KeePass est volé, un attaquant pourrait tenter de le déchiffrer, même si c'est assez difficile.

# Conclusion

KeePass est un gestionnaire de mots de passe très pratique pour sécuriser et organiser ses identifiants. Il permet d’éviter les oublis et d’améliorer la sécurité grâce à des mots de passe forts et uniques. Sa fonction de saisie automatique simplifie la connexion, mais il nécessite un apprentissage pour configurer correctement les entrées. On pourrait se pencher sur un gestionnaire plus simple d’utilisation comme Bitwarden par exemple, qui est un gagne temps avec son gestionnaire de mot de passe développé et simple d’utilisation.

# Source

<https://keepass.cool/1.x/1.41/Lasaisieautomatique.html#:~:text=La%20m%C3%A9thode%20est%20simple%20%3A%20clic,%2BV%20pour%20cette%20commande>).

<https://www.jobready.fr/>

<https://www.tutos.eu/9919>

<https://fr.wikipedia.org/wiki/KeePass>