KeePassXC sous Windows

Avec Firefox

Introduction

KeePassXC et KeePass

KeePassXC est une version parallèle de **KeePass**, un gestionnaire de mots de passe **libre**. Il permet de regrouper tous ses identifiants en un seul fichier (à l'endroit que vous souhaitez), sécurisé par **chiffrement**. Pour se connecter à n'importe quel service, il ne suffit plus que d'une seule phrase de passe pour déchiffrer sa base de données (le fichier), et récupérer ses informations de connexion.

KeePass, la version originale, est recommandée par l'ANSSI (Agence Nationale de Sécurité de Système d'Information, https://www.ssi.gouv.fr/entreprise/certification_cspn/keepass-version-2-10-portable/), et mise en avant par la CNIL (Commission Nationale de l'Informatique et des Libertés, https://www.cnil.fr/fr/atom/14984), gage de sa fiabilité.

Penser phrase de passe

Pour qui voudrait cracker – c'est-à-dire briser – vos mots de passe, il y a deux principales possibilités :

- La **force brute** consiste à lancer un programme qui essayera successivement tous les mots de passe possibles, caractère par caractère. Il commencera par « a », puis « aa », « ab » et ainsi de suite. Un mot de passe court peut être trouvé en quelques jours seulement, tandis qu'un suffisamment long sera impossible à percer dans des délais viables ;
- L'**attaque par dictionnaire** est similaire à la force brute, mais au lieu d'essayer caractère par caractère, les tentatives sont faites mot par mot. Si l'assaillant arrive à se procurer des informations vous concernant (nom, prénom, ville, date de naissance, livre préféré…), via les réseaux sociaux par exemple, il peut les ajouter à la liste de mots à essayer. Avec, l'attaque sera beaucoup plus rapide, car la majorité des mots de passe contiennent des données personnelles.

On en retient donc qu'un mot de passe court, ou contenant des informations personnelles sera facile à déceler. On pourrait se dire que prendre une longue suite de caractères arbitraire serait une bonne solution, mais cela risque d'être difficile à retenir.

Il faut cesser de penser « mot de passe », et passer à la **phrase de passe**. Il s'agit simplement d'une **suite de mots** – au moins cinq –, **aléatoire** et **totalement impersonnelle** (pas de date de naissance, nom d'un animal de compagnie…). Par exemple, une bonne phrase de passe pourrait être « veste bondi mitre lavait jolis ».

Le fait d’utiliser des mots complets rend la phrase facile à mémoriser. Après l’avoir saisi quelques fois, elle sera retenue.

Pour la renforcer, ou satisfaire les demandes d’un service, on peut ajouter des chiffres et caractères spéciaux. Par exemple en remplaçant certaines lettres, ce qui pourrait donner « VesteB0nd!M!treLava!tJ0l!$ ».

Une phrase de passe est donc plus pratique et sûre qu’un mot de passe traditionnel ; elle est longue et impersonnelle, tout en restant facile à retenir.

Pour ceux en manque d’inspiration, curieux ou très soucieux de leur sécurité, la méthode **Diceware** est une bonne solution pour en créer une (http://weber.fi.eu.org/software/diceware/francais.pdf).

Le chiffrement

Le chiffrement (l’anglicisme « cryptage » est souvent utilisé à tort) consiste à « brouiller » des données avec un algorithme – une suite d’instructions –, en fonction d’une **clé**. Pour **déchiffrer** les données, c’est-à-dire pouvoir de nouveau les lire, on les fait passer par un autre algorithme en donnant la clé. Quand des données ne sont pas chiffrées, elles sont dites **en clair**.

La clé est souvent une phrase de passe, mais peut parfois être un fichier. Si on n’a pas la clé, impossible de lire les données. Il ne faut donc pas la perdre ! Ni d’ailleurs la donner au premier venu…

Le **chiffre de César** est un exemple de chiffrement basique. Cette méthode était utilisée par Jules César pour transmettre des messages militaires, sans qu’ils soient lisibles s’ils étaient interceptés.

Son algorithme est le suivant :

```
Pour chaque lettre du message ;
     Ajouter à sa position dans l’alphabet la valeur de la clé ;
     Remplacer la lettre par celle à la position trouvée par l’addition.
```

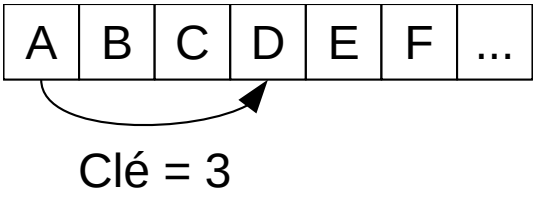

Figure 1: Décalage avec une clé égale à trois.

C’est en fait un simple décalage (Figure 1). Donc, avec le chiffre de César et une clé égale à trois, « A » devient « D ». Pour déchiffrer, on inverse l’algorithme (on soustrait la clé à la position de la lettre dans l’alphabet). Si on a la mauvaise clé, par exemple deux, « D » passe à « B », et non le « A » d’origine (Figure 2).

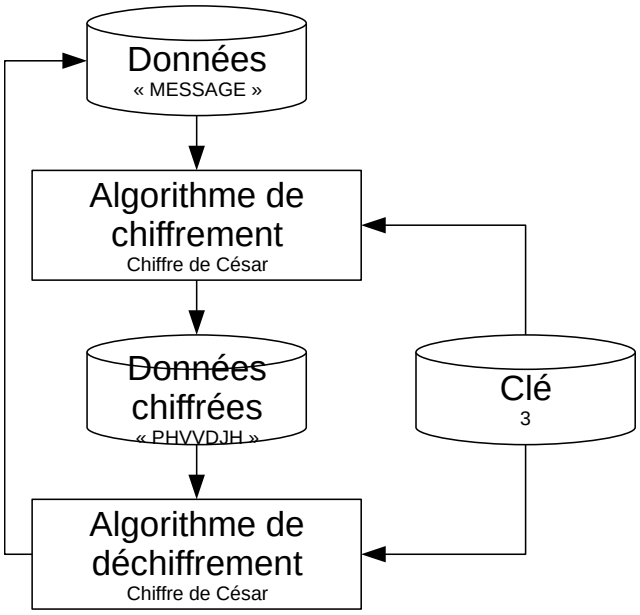

Figure 2: Chiffrement avec le chiffre de César.

Le chiffre de César est une technique de chiffrement primitive. Les algorithmes modernes sont extrêmement complexes, les opérations sont donc réalisées par ordinateur.

Libre ?

Un logiciel dit libre, offre les libertés suivantes :

- Le droit d'**utiliser** le logiciel comme on le souhaite, sans conditions ;
- Le droit de le **modifier** et de l'adapter à ses besoins ;
- Le droit de **distribuer** des copies ;
- Le droit de **publier les modifications** apportées au logiciel.

De par cette nature, les logiciels libres doivent offrir leur **code source** au public. C'est une forme de « recette ». Une fois « cuisinée », celle-ci nous donne notre « gâteau ». On remplace le « gâteau » par le logiciel et la préparation par un processus appelé compilation. Le « cuisinier » qui met au point la « recette » est le **développeur**.

Ces logiciels sont en opposition à ceux **privateurs** (aussi appelés « propriétaires » ou « privatifs »), souvent protégés par des licences restrictives. Leurs codes source ne sont que très rarement, voir jamais accessibles. Il est donc difficile de connaître leur fonctionnement interne ; on a notre « gâteau », mais impossible d'en connaître la « recette ». On peut prendre comme exemples Microsoft Windows, Adobe Photoshop et Google Chrome.

Les logiciels libres sont souvent développés collaborativement, par les membres d'une communauté. Dans le cadre de la sécurité recherchée ici, ils offrent un énorme avantage ; plusieurs personnes

indépendantes lisent et développent activement le code source, donc difficile d'y glisser discrètement des fonctions malveillantes. Aussi, le code étant en accès libre, il peut être audité sans l'autorisation des développeurs, contrairement à ceux privateurs.

De plus, le caractère libre du logiciel assure sa pérennité. Si celui-ci cesse d'être mis à jour, une autre équipe peut immédiatement reprendre le projet.

Avantages et risques

Un gestionnaire de mots de passe offre un grand confort en plus d'une sécurisation solide. Vous pouvez, pour chaque service, utiliser un mot de passe différent sans avoir à tous les retenir.

A savoir qu'il faut **toujours** utiliser un mot de passe **unique** par service. Si vous utilisez les mêmes identifiants partout, et qu'un site que vous utilisez se fait cracker, tous vos comptes seront compromis.

Si quelqu'un utilise votre ordinateur sans autorisation, ou que vous le perdez dans le cas d'un portable, il sera impossible de déchiffrer vos mots de passe sans votre clé. Par contre, il faudra en choisir une robuste. Une clé faible (par exemple un seul mot), sera très facile à cracker.

Aussi, si votre ordinateur est compromis par un **malware** (appelé virus à tort), et que vous tapez votre clé dans KeePassXC, celle-ci pourra être volée. L'attaquant aura donc la possibilité d'utiliser vos identifiants.

En informatique, il n'existe aucune solution magique ; tout a ses avantages et ses failles.

Pourquoi pas KeePass ?

KeePassXC a été choisi pour sa simplicité d'utilisation. Son interface est un peu plus épurée que KeePass. Surtout, il est facile à intégrer à Firefox (ou la plupart des navigateurs populaires), ce qui permet de saisir automatiquement ses mots de passe.

La majeure partie de ce tutoriel reste utilisable avec KeePass.

Utilisation de KeePassXC

Installation

Allez sur la page de téléchargement de KeePassXC (https://keepassxc.org/download/) et cliquez sur le lien « **MSI Installer** » en dessous de la version qui vous convient. Celle **64-bit** répondra à la majorité des cas, si vous avez un ordinateur ancien, la 32-bit sera peut-être nécessaire.

Pour connaître la compatibilité de votre système, ouvrez l'explorateur de fichier, faites un clic droit sur « Ce PC » et choisissez « Propriétés ». « Type de système » indique s'il est 32 ou 64 bits.

Une fois téléchargé, lancez l'installateur. Cliquez sur « **Next** » à chaque étape pour continuer. Cochez la case d'acceptation lors de l'affichage de la licence (GNU GPL, licence libre). Quand vous cliquerez sur « **Install** », les droits d'administrateur vous seront demandés, validez.

KeePassXC est maintenant installé !

Premier lancement

Lancez KeePassXC par une recherche dans le menu Démarrer.

Lors du premier lancement, il vous sera demandé si vous souhaitez que les mises à jour soient vérifiées au lancement du programme (Figure 3). Il est recommandé d'accepter, cliquez sur « **Yes** ».

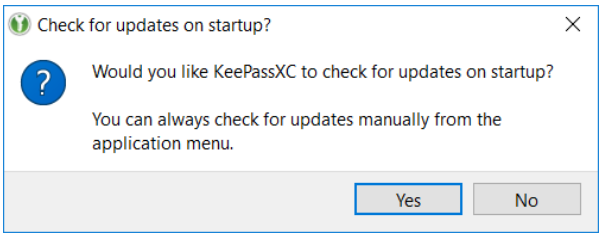

Figure 3: Demande pour la vérification des mises à jours au lancement.

Changer la langue

Par défaut KeePassXC est en anglais. Pour passer en français, suivez ces étapes :

1) Dans le menu, cliquez sur « **Tools »**, puis « **Settings »** ;
2) Tout en bas de la catégorie « **General** », dans le menu déroulant légendé « **Language** », choisissez « **French** » ;
3) Cliquez sur « **OK** » en bas à droite ;
4) **Fermez** KeePassXC et relancez-le.

Créer sa base de données

La base de données contiendra vos identifiants chiffrés. Il faut la créer préalablement.

1) Cliquez sur « **Créer une nouvelle base de données** » ;
2) Choisissez-lui un nom et une optionnellement une description ;
3) Cliquez sur « **Continuer** » jusqu'à ce que la saisie de la clé vous soit demandée, vous pouvez ignorer les autres options proposées ;

4) La clé vous permettra de déchiffrer la base de données, il faut qu'elle soit sûre. Il est préconisé d'utiliser une **phrase de passe**, comme expliqué dans le chapitre Penser phrase de passe. Une fois choisie, saisissez-la dans les deux champs de texte ;

5) Cliquez sur « **Terminer** » ;

6) Dans la boîte de dialogue d'enregistrement, choisissez où placer la base de données (dans votre dossier d'utilisateur ou « Documents » par exemple) et cliquez sur « **Enregistrer** ».

Si la phrase de passe que vous avez choisi ne vous convient finalement pas, allez dans le menu « **Base de données** », puis « **Changer la clé maîtresse...** ». Cliquez enfin sur « **Modifier Mot de passe** ».

Dès que vous lancerez KeePassXC, votre phrase de passe vous sera demandée, pour déchiffrer la base de donnée. Si vous perdez cette clé, vous ne pourrez plus accéder aux identifiants enregistrés, donc retenez la bien ! Bien que compliquée à retenir, ne notez **absolument jamais** cette phrase dans un fichier. Après l'avoir tapé plusieurs fois, votre mémoire fera le travail.

La fenêtre principale

Maintenant que KeePassXC est configuré, vous pouvez commencer à entrer vos identifiants. La fenêtre principale (Figure 4) est coupée en deux, de manière semblable à l'explorateur de fichier :

- A droite les **groupes**, nous permettant d'organiser nos identifiants par thème (administratif, loisirs, boutiques, banques…) ;
- A gauche la liste des **entrées** – éléments stockées dans la base de données – placées dans le groupe actuellement sélectionné. Elles stockent les identifiants.

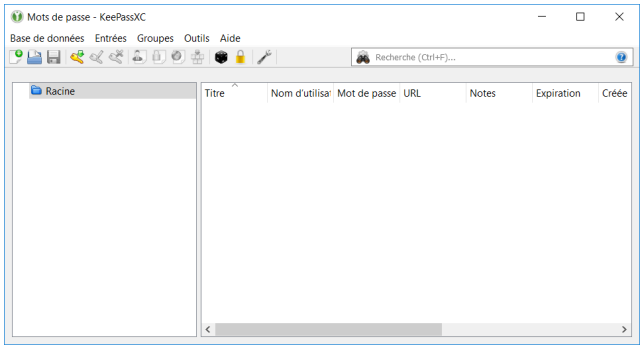

Figure 4: La fenêtre principale.

Gérer les groupes

Vous pouvez faire un clic droit dans l'encadré des groupes pour choisir entre trois options explicites ; « **Créer un groupe** », « **Modifier le groupe** » et « **Supprimer le groupe** ».

Un groupe créé le sera dans celui qui est sélectionné, permettant de les hiérarchiser. Le groupe « Racine » est la base de cette arborescence.

Enregistrer ses identifiants

Nous pouvons maintenant enregistrer nos identifiants. Il faut créer une entrée dans la base de données :

1) Faites un clic droit dans l'encadré de gauche et choisissez « **Nouvelle entrée** », la fenêtre vous demande maintenant de saisir les informations (Figure 5) ;

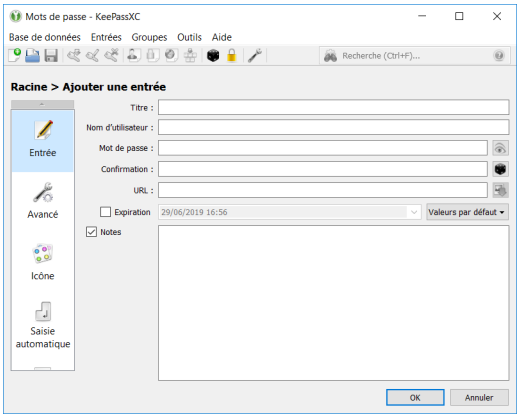

Figure 5: Ajouter une entrée.

2) Saisissez le **titre**, qui décrit l'entrée, le **nom d'utilisateur** (ou identifiant, souvent l'adresse e-mail) et votre **mot de passe** pour le service voulu. Le mot de passe doit être écrit deux fois, la seconde dans le champ « **Confirmation** » ;

3) Pour remplir le champ « **URL** », allez sur la page Web de connexion du site avec votre navigateur, par exemple celle de la Médiathèque Numérique du Puy-de-Dôme (https://cas.mediadome.syrtis.fr/cas/login?service=https%3A//mediatheque-numerique.puy-de-dome.fr/casservice), puis copiez-collez l'adresse. Assurez-vous que celle-ci commence par **HTTPS** ;

4) Saisissez des notes si vous le souhaitez ;

5) Cliquez sur « **OK** » pour finaliser.

L'entrée avec vos identifiants s'affiche maintenant (Figure 6).

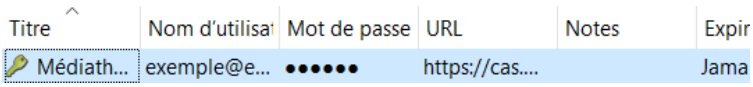

Figure 6: L'entrée affichée.

Un clic droit sur l'entrée permet, comme pour les groupes, de la modifier ou de la supprimer. « **Ouvrir l'URL** » vous enverra directement sur la page de connexion.

Saisir ses identifiants

On peut utiliser KeePassXC sans intégration dans le navigateur Web. Faire un clic droit sur l'entrée concernée propose plusieurs options :

- « **Copier le nom d'utilisateur** » et « **Copier le mot de passe** » mettront les informations respectives dans le presse-papier. Elles peuvent ensuite être collées dans le formulaire de connexion ;
- « **Effectuer un remplissage automatique** » saisira automatiquement l'identifiant et le mot de passe. Cliquez d'abord sur le champ de texte d'identifiant sur la page Web du service, puis sélectionnez cette option dans KeePassXC.

Sauvegarder sa base de donnée

Il est grandement recommandé de sauvegarder régulièrement sa base de données (celle que nous avons créée au chapitre Créer sa base de données). Copiez la sur une clé USB, disque dur externe ou CD, et gardez le support en lieu sûr. Si votre ordinateur plante ou que vous le perdez (dans le cas d'un portable), vous pourrez retrouver tous vos mots de passe, sains et saufs !

KeePassXC « Portable »

La page de téléchargement de KeePassXC, comme vu dans le chapitre Installation, propose une version dite « portable ». Ces logiciels ne nécessitent aucune installation. A noter qu'ils ne sont pas compatibles avec tous les systèmes d'exploitation.

Pour pouvoir retrouver vos mots de passe où que vous soyez, copiez la version portable sur une clé USB, ainsi que votre base de données. Il faudra par contre recopier cette dernière régulièrement, pour tenir compte des modifications apportées.

Mais attention, déchiffrer vos identifiants sur un ordinateur infecté par un malware les compromettra.

Intégration à Firefox

Configurer KeePassXC

Pour autoriser la transmission des mots de passe à Firefox, suivez ces étapes dans KeePassXC :

1) Allez dans le menu « **Outils** », puis « **Paramètres** » ;
2) Cliquez sur la catégorie « **Intégration aux navigateurs** » ;
3) Cochez la case « **Activer l'intégration de KeePassXC aux navigateurs** » ;
4) Cochez enfin « **Firefox and Tor Browser** ».

Installer le module

L'intégration à Firefox se fait par l'installation d'un module complémentaire. Allez sur la page d'installation du module (https://addons.mozilla.org/fr/firefox/addon/keepassxc-browser/) avec Firefox. Cliquez sur « **Ajouter à Firefox** », puis sur « **Ajouter** » dans la bulle qui s'affiche.

Vous devriez voir l'icône du module dans la barre d'outils en haut à droite. Cliquer dessus affichera une bulle (Figure 7).

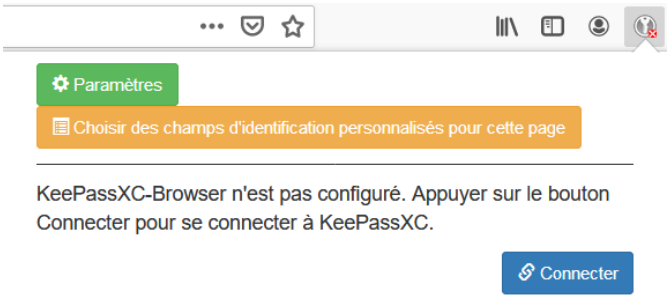

Figure 7: Bulle du module non configuré.

Il se peut que vous ne voyiez pas la même bulle, et qu'il vous est juste dit que la connexion a échoué. Assurez-vous bien que KeePassXC soit lancé, et que vous avez saisi votre clé de chiffrement. Cliquez ensuite sur « **Réessayer** » dans la bulle.

Il est maintenant dit que le module « n'est pas configuré » ; il faut associer Firefox au logiciel.

Cliquez sur le bouton « **Connecter** ». Dans la boîte de dialogue (Figure 8), tapez un nom pour l'autorisation (par exemple « Firefox ») et validez en cliquant sur « **Enregistrer et autoriser l'accès** ».

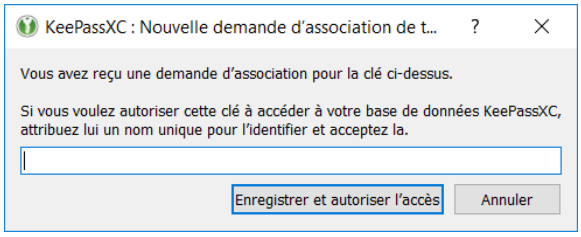

Figure 8: Demande de nouvelle association.

Utilisation

Pour utiliser le module, KeePassXC doit être lancé et la base de données déchiffrée.

Quand vous allez sur la page de connexion d'un service que vous avez enregistré, il vous sera demandé d'autoriser l'utilisation de vos identifiants. Prenons par exemple celle de la Médiathèque Numérique du Puy-de-Dôme (Figure 9).

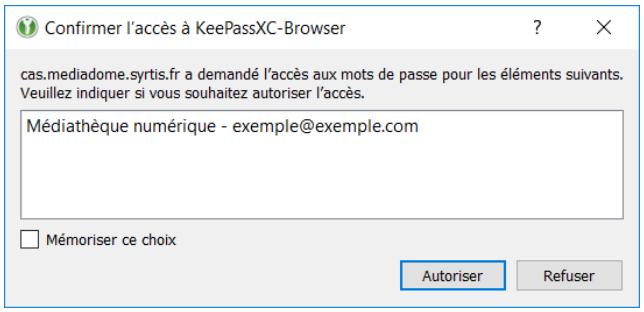

Figure 9: Fenêtre de confirmation d'accès.

Une fois la demande d'accès validée. La bulle du module vous proposera les identifiants que vous avez enregistrés pour ce site (Figure 10). Cliquer sur ceux-ci remplira automatiquement le formulaire de connexion.

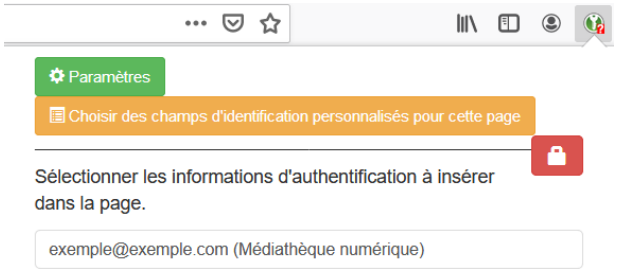

Figure 10: Bulle listant les identifiants.

A savoir, vous pouvez aussi saisir vos identifiants en faisant un clic droit sur un des champs du formulaire, puis en allant dans la catégorie « **KeePassXC-Browser** » du menu contextuel.

Les formulaires spéciaux

Il arrive que certains formulaires de connexion ne soient pas détectés par le module. Pour y remédier, vous pouvez utiliser l'outil « **Choisir des champs d'identification personnalisés pour cette page** » dans la bulle. Suivez ensuite les instructions à l'écran.

Il faudra cliquer en premier sur le champ de nom d'utilisateur, puis sur celui de mot de passe. Vous pouvez ignorer un des champs (s'il n'est pas présent sur la page) en cliquant sur « **Ignorer** ».

Conclusion

Voilà, vous savez maintenant utiliser KeePassXC et son module pour Firefox ! Vous pouvez maintenant stocker tous vos identifiants en sécurité et délester votre mémoire des dizaines de mots de passe que vous utilisez couramment.

En dehors de l'utilisation de KeePassXC, retenez bien les informations suivantes :

- Que ce soit pour votre clé de chiffrement ou vos identifiants en ligne, il est recommandé d'utiliser une **phrase de passe impersonnelle** d'au moins **cinq mots** (pour rappel, le Diceware permet d'en créer facilement) ;
- Le **chiffrement** permet de protéger des données de manière sûre, mais seulement si l'on utilise une clé solide ;
- Chaque service utilisé doit avoir un mot de passe **unique** ;
- Les logiciels **libres** sont souvent plus fiables que ceux privateurs ;
- **Aucune solution est sans faille**, utiliser KeePassXC sur un ordinateur infecté par un malware peut être dangereux.

Aller plus loin

Si vous souhaitez aller plus loin, vous pouvez par exemple :

- Paramétrer le logiciel pour chiffrer automatiquement la base de données si elle reste inutilisée pendant un certain temps ;
- Explorer les diverses versions de KeePass sur d'autres plateformes, comme Android et iPhone (https://keepass.info/download.html);
- Stocker votre base de données sur un service d'hébergement en ligne (de confiance, bien sûr) pour « synchroniser » vos divers appareils.

Crédits

- Rédaction : DALECKI Léo ;
- Relecture : Médiathèque des Jardins de la Culture, Riom Limagne et Volcans.

Glossaire

Algorithme
Suite d’instructions, de commandes.

Attaque par dictionnaire
Deviner un mot de passe grâce à un logiciel qui testera toutes les combinaisons de mots possibles.

Attaque par force brute
Deviner un mot de passe grâce à un logiciel qui essaye tous ceux possible, caractère par caractère.

Base de données
Structure de stockage de données.

Chiffrement
« Brouiller » des données via en algorithme en fonction d’une clé.

Code source
Programme écrit en langage humainement lisible.

Compilation
Transformation du code source en programme exécutable par un ordinateur.

Cracker
Outrepasser, briser un système de sécurité informatique.

Déchiffrer
Rendre des données chiffrées lisibles en fournissant la clé à l’algorithme de déchiffrement.

Développeur
Personne ou organisation créant ou maintenant un code source.

Données en clair
Données non chiffrées.

Entrée
Élément d’une base de données.

Identifiants
Données permettant de prouver son identité, souvent un identifiant et un mot de passe.

Logiciel libre
Logiciel autorisant l’utilisation, modification, redistribution et publication des altérations, et ce sans conditions.

Logiciel portable
Logiciel ne nécessitant pas d’installation.

Logiciel privateur
Logiciel protégé par une licence restrictive.

Malware
Logiciel malveillant, installé à l’insu de l’utilisateur. Parfois appelé maliciel en français.

Phrase de passe
Suite de mots ayant la même fonctionnalité qu’un mot de passe.

Presse-papier
Mémoire conservant les données copiées ou coupées, pour être ultérieurement collées.