AESCrypt

https://www.aescrypt.com/ -> Il n'est pas nécessaire d'être un expert pour utiliser AES Crypt, ni de comprendre la cryptographie. AES Crypt est conçu pour être aussi simple à utiliser que possible, tout en offrant la puissance de cryptage la plus élevée qui soit.

- Utilisation sur Linux

Utilisation sur Linux

Installation

Lien de téléchargement ici.

Installation en ligne de commande

Pour installer AESCrypt en ligne de commande seulement, vous pouvez télécharger AES Crypt source code (Linux) (Code source pour la construction du binaire en ligne de commande Linux).

Une fois l'archive du code source téléchargé vous allez devoir l'extraire :

```
tar -xzf aescrypt-3.16.tgz
```

Entrer dans le dossier de l'extraction et compiler le code source :

```
cd aescrypt-folder/

# Compilation du code source
make

# Test des commandes
make test

# Installation des commandes de manières permanantes
sudo make install
```

Installation de l'interface

Pour installer AESCrypt avec une interface, vous pouvez télécharger AES Crypt - GUI (Linux 64-bit) ou (Linux 32-bit) (Version 64 bits ou 32-bits fonctionnant dans l'interface graphique et la version en ligne de commande est incluse).

Une fois l'archive du code source téléchargé vous allez devoir l'extraire :

```
gzip -d aescrypt-GUI-3.11-Linux-x86_64-Install.gz
```

Pour continuer l'installation il faut donner le droit d'exécution du fichier extrait puis exécuter le fichier :

```
# On donne le droit d'exécution
sudo chmod +x aescrypt-GUI-3.11-Linux-x86_64-Install

# On exécute le fichier
./aescrypt-GUI-3.11-Linux-x86_64-Install
password:
```

Une fois le mot de passe administrateur saisie une fenêtre d'installation va apparaître puis terminer l'installation avec la pop-up.

pop-install.png

Utilisation

> **Chiffrer un dossier**
> L'inconvénient de AESCrypt c'est qu'il est possible de chiffrer uniquement des fichiers. Pour chiffrer un dossier il faut d'abord convertir le dossier en archive (`.gz` de préférence) puis d'exécuter la commande de chiffrement/déchiffrage sur l'archive.

Chiffrage d'un fichier

L'utilisation de la commande de chiffrement est compatible avec tous les fichiers, quelque soit sont extension.

Via l'invite de commande

Commande basique pour chiffrer un fichier en précisant le mot de passe :

```
# -e  encrypt un fichier
# -p  précise le mot de passe
aescrypt -e -p <password> <filename>

# Exemple
aescrypt -e -p motDePasse123 monfichier.pdf
```

L'équivalent sans préciser le mot de passe dans la commande :

```
aescrypt -e monfichier.pdf
Enter password:
Re-Enter password:
```

Via l'interface

Pour utiliser l'interface il faut faire clic-droit sur n'importe quel type de fichier puis "ouvrir avec" et sélectionner le logiciel "AESCrypt" comme le montre l'image ci-dessous :

ouvriravec.png

Une fois AESCrypt sélectionné, une petite fenêtre va s'ouvrir pour entrer un mot de passe qui chiffrera le fichier sélectionné.

Il faudra saisir le mot de passe 2 fois pour valider le chiffrement du fichier.

chiffre1.png

La commande garde le fichier d'origine et crée un nouveau fichier qui aura l'extension `.aes` qui correspond au fichier chiffré:

fileaes.png

Déchiffrage d'un fichier

Via l'invite de commande

Commande basique pour déchiffrer un fichier .aes en précisant le mot de passe :

```
# -d décrypt un fichier
# -p précise le mot de passe
aescrypt -d -p <password> <filename>.aes

# Exemple
aescrypt -d -p motDePasse123 monfichier.pdf.aes
```

L'équivalent sans préciser le mot de passe dans la commande :

```
aescrypt -d monfichier.pdf.aes
Enter password:
```

Via l'interface

Pour déchiffrer un fichier avec l'interface il faut faire exactement la même procédure que pour chiffrer sauf qu'il faut le faire sur un fichier qui a l'extension `.aes`

Clic-droit sur n'importe quel type de fichier qui a une extension `.aes` puis "ouvrir avec" et sélectionner le logiciel "AESCrypt" comme le montre l'image ci-dessous :

ouvriravec.png

Une fois AESCrypt sélectionné, une petite fenêtre va s'ouvrir pour entrer un mot de passe qui déchiffrera le fichier sélectionné.

chiffre1.png

Le déchiffrement garde une copie du fichier chiffré et créé un nouveau fichier déchiffré dans le même répertoire que le fichier en `.aes`.

aze.png

Désinstallation

Pour désinstaller AESCypt sur Linux, il suffit d'exécuter la commande suivante :

```
sudo /usr/share/aescrypt/uninstall
```