TP Hygiène Numérique HackademINT

Protégez vos données personnelles

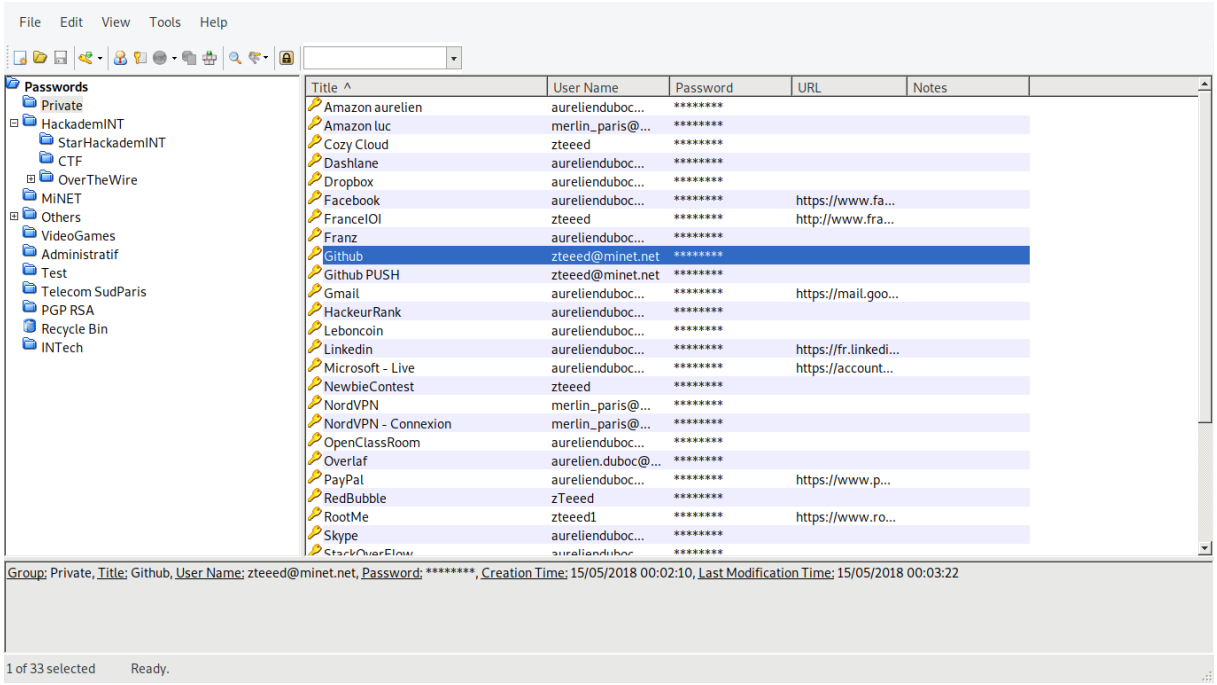
zTeeed

Table des matières

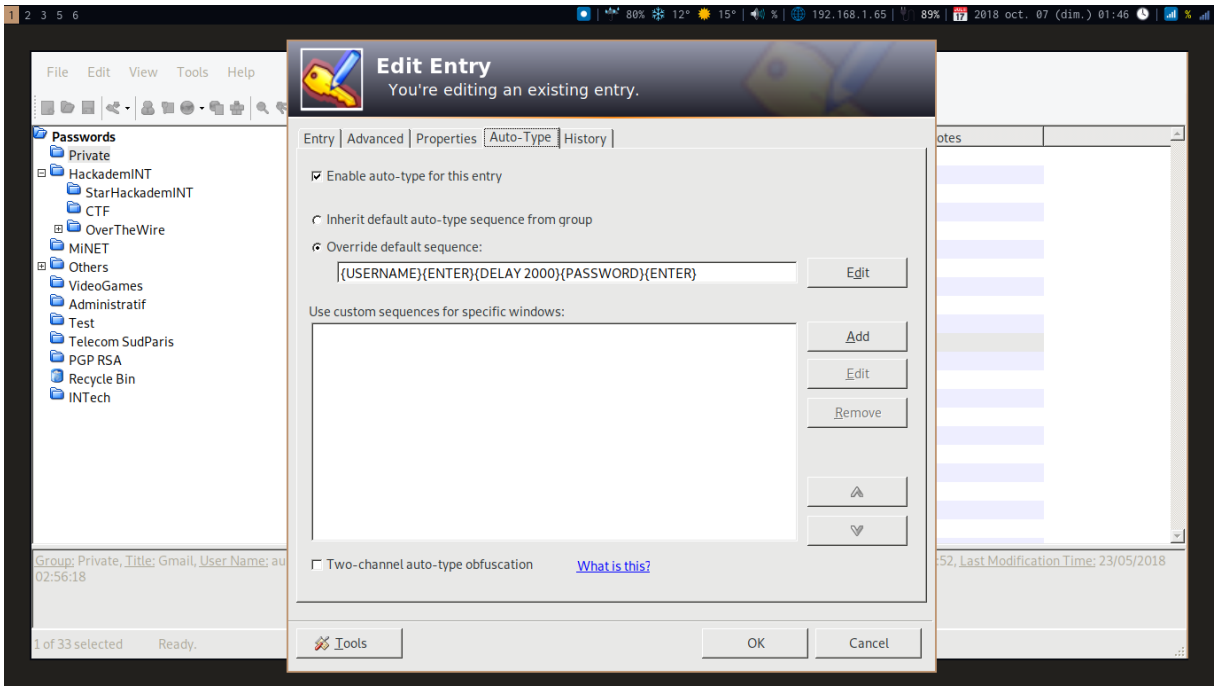
Gestionnaire de Mot de Passe

Keepass2

> KeePass est un gestionnaire de mots de passe qui sauvegarde les mots de passe dans un fichier chiffré appelé « base de données ». Cette base est accessible avec le mot de passe principal.



Configuration de l'AutoType



Chiffrement de données

cryptsetup

Munissez vous de votre clef USB. Nous allons effacer toutes les données dessus et rendre la clé chiffrée. Vous pouvez ainsi conserver vos données le splus précieuses sur vous tout le temps sans craindre que l'on vous vole le contenu si vous perdez cette clé. Vous pouvez de la même manière chiffrer un disque dur :

Documentation complète en ligne :
https://help.ubuntu.com/community/EncryptedFilesystemsOnRemovableStorage

Exemple avec une nouvelle clé USB (/dev/sdc) :
Attention : vérifiez bien que le device correspondant à votre clef USB !!

```
[zteeed@spider HackademINT]$ lsblk
NAME              MAJ:MIN RM   SIZE RO TYPE  MOUNTPOINT
...
sdc                 8:32   1  14,9G  0 disk
  sdc1              8:33   1  14,9G  0 part
```

Setup (après avoir créer une partition avec fdisk ou gparted) :

```
sudo apt install cryptsetup
sudo cryptsetup --verify-passphrase luksFormat /dev/sdc1 -c aes -s 256
    -h sha256
sudo cryptsetup luksOpen /dev/sdc1 key_dcrypt
sudo mkfs.ext4 /dev/mapper/key_dcrypt

[zteeed@spider HackademINT]$ lsblk
...
sdc                 8:32   1  14,9G  0 disk
  sdc1              8:33   1  14,9G  0 part
    key_dcrypt    254:4    0  14,9G  0 crypt

mount /dev/mapper/key_dcrypt /mnt
```

encfs

Dans le cas ou votre disque ne serait pas chiffré mais vous voudriez quand même chiffrer les données dans un dossier, voici la marche à suivre :

Installation :

```
sudo apt-get -y install encfs
mkdir -p ~/encrypted
mkdir -p ~/decrypted
encfs ~/encrypted ~/decrypted
Enter "p"
```

Déchiffrez le dossier et insérez y vos données

```
encfs ~/encrypted ~/decrypted
cd ~/decrypted
echo "confidential data" > mydata
```

Fermez l'accès au dossier ~/decrypted :

```
fusermount -u ~/decrypted
```

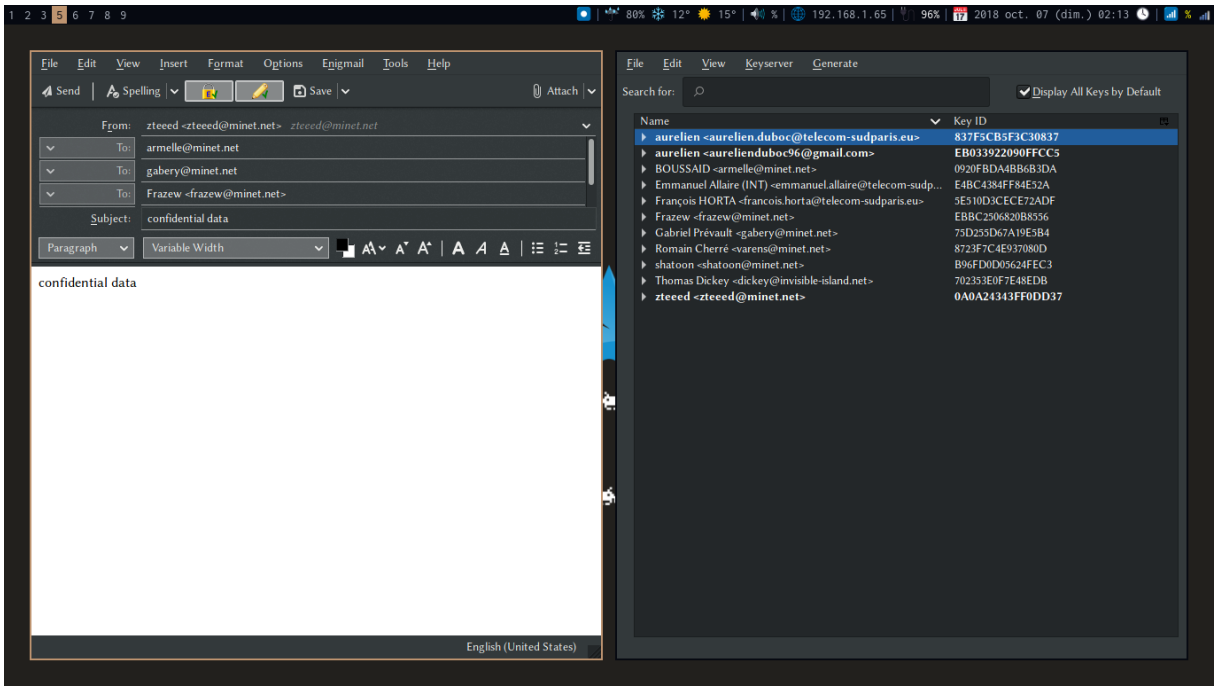
Chiffrement de mail

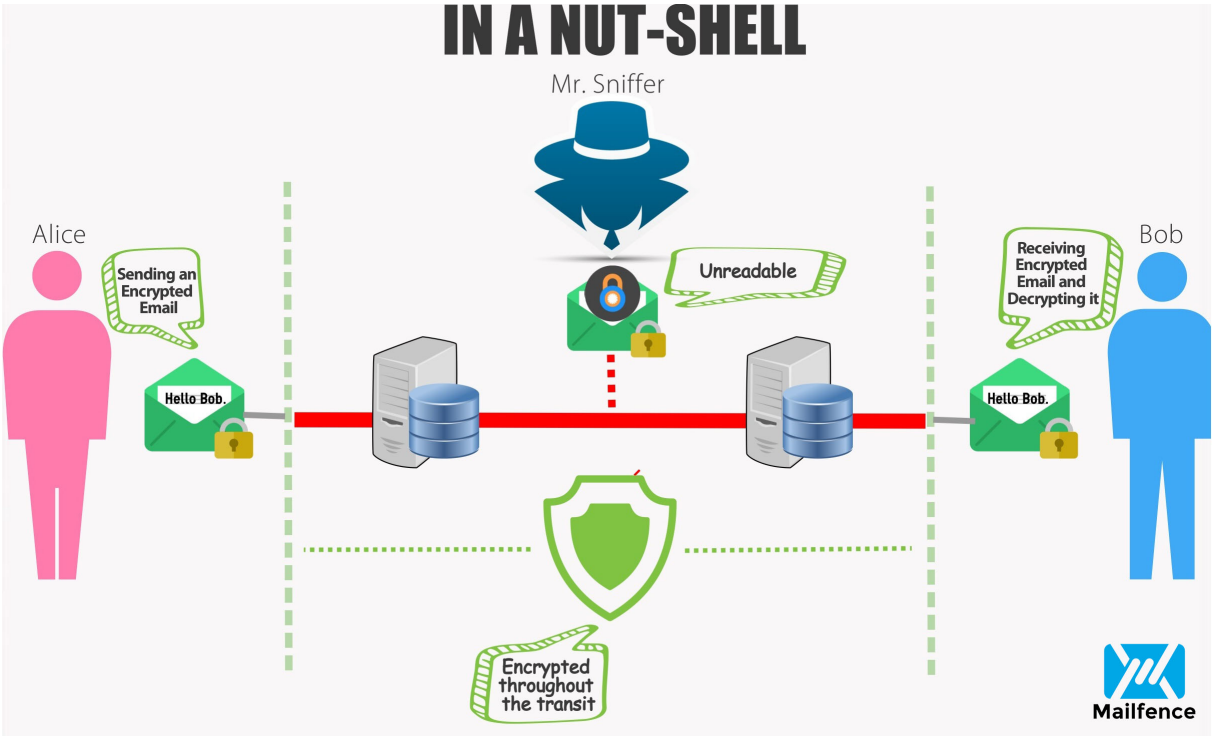
gpg

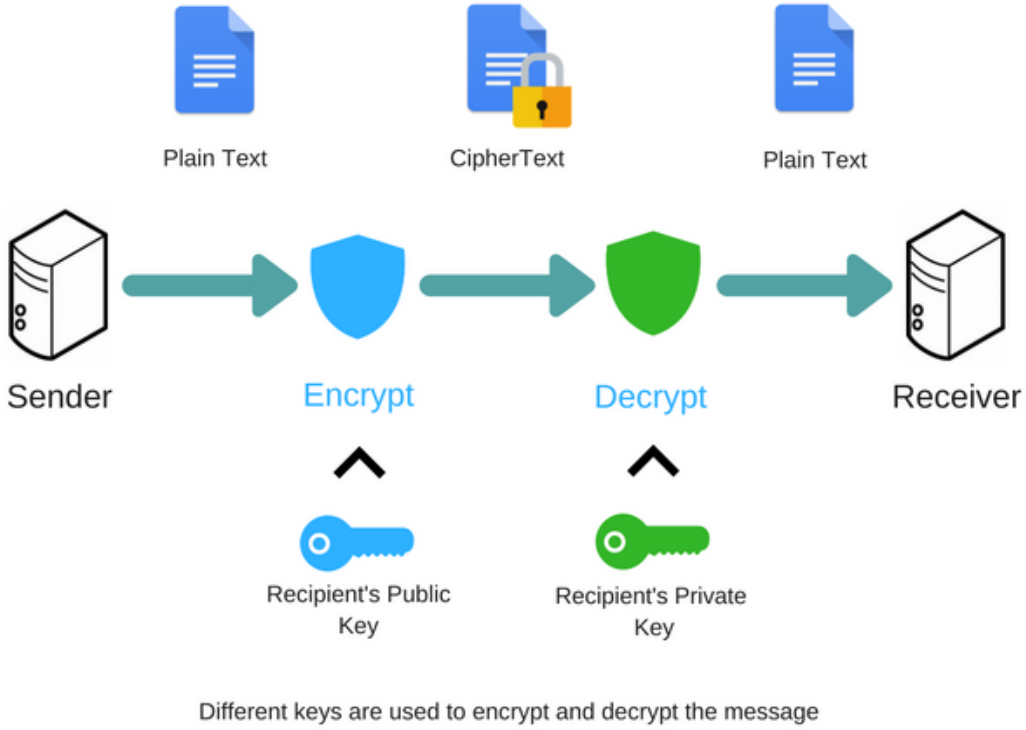
Pour les curieux, je vous invite à consulter cet article qui est plus que complet :
https://wiki.minet.net/wiki/guide_du_debutant/cle_openpgp

thunderbird

Je vous renvoie vers la documentation en ligne :
https://support.mozilla.org/fr/kb/signature-numerique-et-chiffrement-des-messages




IN A NUT-SHELL
Mr. Sniffer
Alice
Sending an Encrypted Email
Hello Bob.
Unreadable
Bob
Receiving Encrypted Email and Decrypting it
Hello Bob.
Encrypted throughout the transit
Mailfence


Plain Text
CipherText
Plain Text
Sender
Encrypt
Decrypt
Receiver
Recipient's Public Key
Recipient's Private Key
Different keys are used to encrypt and decrypt the message