

# Mise en place d'une connexion ssh par échange de clef

---

Pour administrer des serveur linux je connecte régulièrement via le protocole ssh, la plus par du temp c'est via un mot de passe.

Mais cette méthode de connexion est loin d'être idéal elle a plusieurs défaut :


- Redondante de saisir du mot de passe
- Vulnérable à plusieurs type d'attaque par ForceBrute par exemple
- Et toutes personnes qui connaissent le mot de passe ou qui l'aurait obtenue de façon illégitime peuvent se connecter sur le serveur (Du moins si l'on n'a pas de filtrage d'adresse ip)

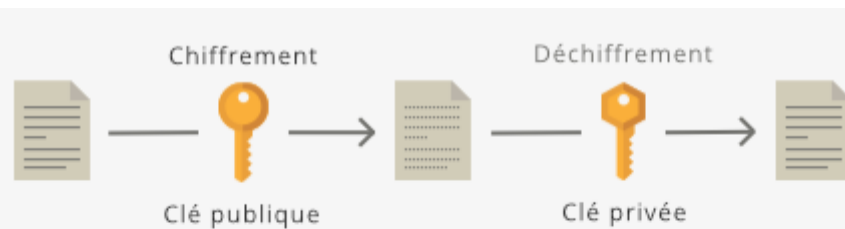
Le mieux serait de se connecter avec un échange de clefs de chiffrement

cette méthode présente 3 avantages majeurs

- Plus besoin de taper le mot de passe ssh
- Une meilleure protection contre les attaques "classiques"
- Limiter les connexions au possesseur de clef de chiffrement uniquement.

Et bien pour faire ça il va falloir mettre en place un chiffrement Asymétrique par échange de clef pour le protocole ssh

 Pour comprendre le fonctionnement de cet échange de clef la CNIL a mis à disposition des informations bien utiles, comme cette image ;)



## CHIFFREMENT ASYMÉTRIQUE

Le chiffrement asymétrique repose sur l'utilisation d'une paire de clés : une publique et une privée.

La clé publique, accessible à tous, est utilisée pour chiffrer les fichiers. Seule la clé privée permet de déchiffrer ces fichiers, celle-ci étant connue que d'un seul individu.

## MISE EN PRATIQUE

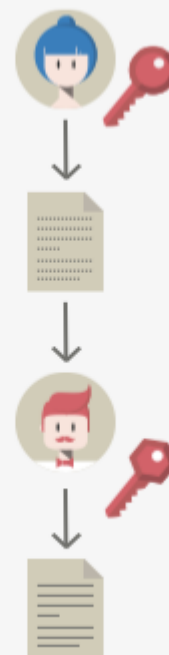
Alice, hackeuse, vient de découvrir des informations d'intérêt public. Elle veut les transmettre à Bob, journaliste, pour qu'il enquête.

1. Alice vient de récupérer la clé publique de Bob. Elle l'utilise pour chiffrer son document.

2. Elle l'envoie à Bob.

3. Bob reçoit le document et le déchiffre à l'aide de sa clé privée.

4. Une fois le document déchiffré, il rédige un article puis le publie dans son journal.



## Création du trousseau de clefs ssh

Dans un premier temps j'ai du gérer la pair de clef privée & publique.

- Clef privée devras rester Privé donc connue uniquement de moi
- Clef publique sera déposer sur le serveur dans le fichier `~/.ssh/authorized_keys`

```
cd ~/.ssh # Aller dans le dossier .ssh
ssh-keygen -t ed25519 # Génère la paires de clefs
```

La rien de très complexe il ma suffis de suivre les instructions de création, une fois terminé, je vérifie que la paire de clefs à bien était crée en listant les fichiers présent dans le répertoire `~/.ssh`

```
ls -l ~/.ssh
```

Maintenant que le trousseau de clef est créé il va me falloir envoyer la clef publique sur le serveur ou je veux me connecter.

```
apt-get install openssh-client && ssh-copy-id username@hostname
```

Bien évidemment username@hostname c'est un exemple il faut remplacer par le nom d'utilisateur et l'adresse IP du serveur.

Bon après ça, la connexion ssh via clef devrait être fonctionnelle. Il suffit de tester la connexion ssh.

```
ssh username@hostname
```

Après une connexion réussie via l'échange de clef 🐼

Je désactive la connexion par mot de passe qui n'est plus d'aucune utilité et représente un risque de sécurité

1. Éditez le fichier `etc/ssh/sshd_config`
2. Remplacez la valeur de PasswordAuthentication par no. (Bien évidemment la ligne doit être décommentée donc on retire le # si il en a un)

## Sources

---

📄 [Cnil la cryptologie](#)

📄 [lecrabeinfo.net SSH par échange de clefs](#)