***Objectif :***

Comprendre le fonctionnement des clés asymétriques.

Savoir comment utiliser le protocole et la connexion SSH de manière plus sécurisée en utilisant les méthodes de cryptages.

***Matériel nécessaire :***

Une machine Linux et une machine cliente Windows (ça peut être votre machine physique).

Avant de commencer ce TP, vérifier que vos 2 machines peuvent communiquer entre elles et que la machine linux a accès à internet.

# Installation du serveur SSH

Se connecter en SSH sur une machine est une utilisation très courante.

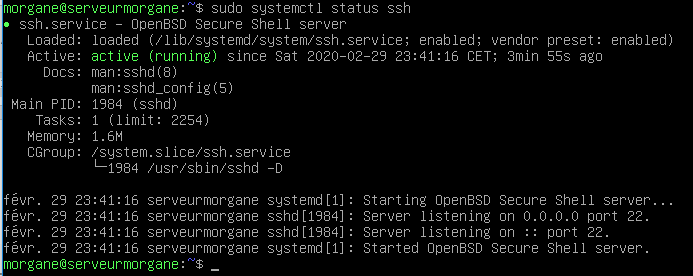
Sur votre machine Debian, Installez le service ssh sur votre machine :

sudo apt install openssh-server

Une fois le service installé, vérifiez bien son fonctionnement en consultant son status :

sudo systemctl status ssh

Vous devez obtenir cela :



Vous constatez que le service est actif, et sur le serveur est en écoute sur toutes les adresses IP sur le port 22.

# Connexion avec un client SSH sur Windows

Un client SSH est souvent bien plus pratique à utiliser que l’invite de commande.

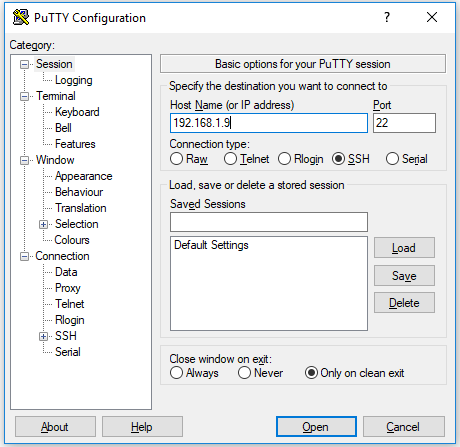
Nous allons apprendre à utiliser Putty.

Téléchargez le logiciel sur le site : <https://www.chiark.greenend.org.uk/~sgtatham/putty/latest.html>

Choisissez la version 64 bits.

Une fois installé, lancez le logiciel.

Sur la ligne « Hostname or IP address » saisissez l’adresse IP de votre machine Debian et le port du service SSH, par défaut celui-ci est 22.



Lancez la connexion en appuyant sur Open.

Vous allez avoir un message d’alerte. Répondez oui, le logiciel vous demande alors votre login (nom d’utilisateur Debian).

Saisissez-le. Puis saisissez votre mot de passe. Et vous voilà connecté avec Putty !

# Rappel : Faites Attention !

Ne confondez pas SSH, ssh et sshd !

SSH est le protocole de communication.

ssh est le programme client permettant de se connecter au serveur

sshd est le daemon ssh du serveur ssh qui communique par défaut sur le port 22.

Pourquoi faire la distinction entre tout ça ?

Principalement pour les fichiers de configuration.

Le fichier /etc/ssh/ssh\_config est le fichier de configuration du client ssh. On a rarement besoin d’y toucher.

Tandis que le fichier /etc/ssh/sshd\_config est le fichier de configuration du serveur ssh. Et vous allez le modifier dès à présent.

# Changement du numéro de port du serveur ssh

Manipulations sur la machine Linux, le serveur SSH.

sudo nano /etc/ssh/sshd\_config.

La ligne ‘Port 22’, signifie que votre serveur SSH écoute sur le port 22. Il s’agit du port par défaut. Décommentez la ligne en enlevant le # devant pour la rendre active. Puis changez le port, mettez un port personnalisé, par exemple le port 22320.

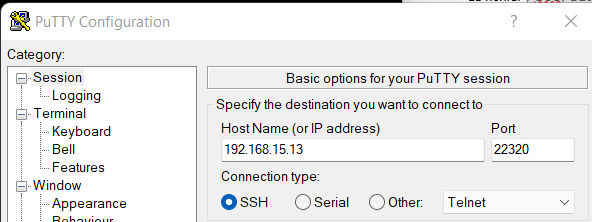
Vous avez changé le fichier de configuration, vous devez le relancer le service ssh pour que les modifications soient prises en compte.

systemctl restart sshd

De manière simple, tenter de vous connecter d’une machine cliente (Windows ou Linux) sur la machine Linux principale, en ssh. Pour que la machine cliente sache sur quel port elle doit communiquer avec le serveur, il faut lui préciser :

ssh [login]@[ip] -p 22320

Si vous le faites avec Putty, il y a juste à rentrer le bon port :



Vous voilà donc connecté à présent, avec une connexion ssh simple, ou autrement dit une connexion ssh avec des clés symétriques.

La clé de chiffrement et celle de déchiffrent sont identique. Elles sont symétriques.

Cette connexion est initialisée par le client qui demande une connexion ssh au serveur, le serveur envoi l’empreinte de sa clé ssh symétrique et demande au client d’accepter l’utilisation de cette clé. Lorsque c’est fait, le client s’authentifie par mdp. La clé publique est donc stockée, sur la machine cliente qui a demandé la connexion dans le dossier personnel de l’utilisateur qui s’est connecté .ssh/know\_hosts

Le client l’utilise pour chiffrer ses communications, et le serveur utilise la clé de son côté pour déchiffrer les communications.

# Authentification par clés avec Putty (Linux / Windows)

À présent, apprenons à sécuriser un peu plus cette connexion ssh, en utilisant les clés asymétriques.

Manipulation sont à fait sur la machine cliente Windows et sur la machine serveur Linux.

Au lieu de s’authentifier par mot de passe, c’est-à-dire de manière « classique », les utilisateurs peuvent s’authentifier grâce à la cryptographie asymétrique et son couple de clefs privées/publiques.

Pour paramétrer cette authentification par clé asymétrique, c’est la machine dite ‘cliente’ qui va générer les clés, et qui ensuite enverra la clé publique au serveur.

## Générer les clés

Il est possible de se connecter avec Putty, et le système de clés.

Cela se fait grâce à l’utilitaire ‘Puttygen’ que vous avez installé à même temps que Putty. Lancez-le.

Cliquer sur le bouton ‘Generate’.

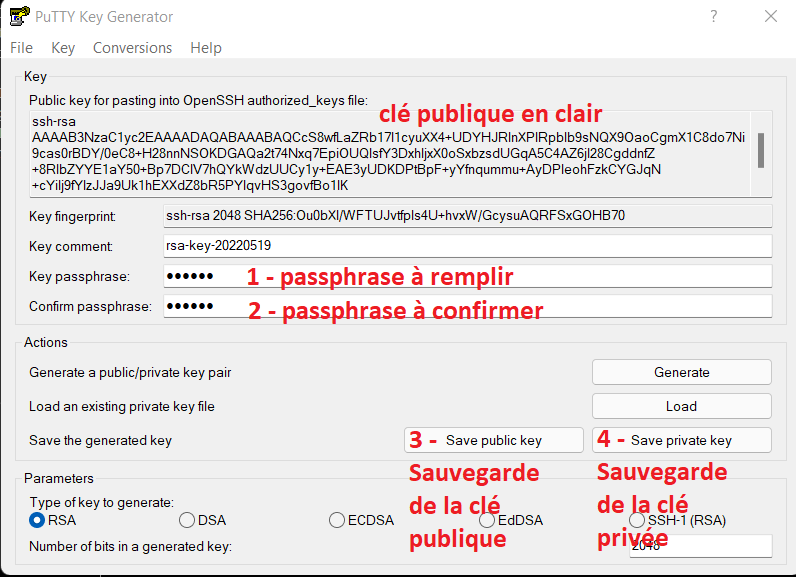
Le programme va générer la clé privée et la clé publique. Mais il a besoin de votre aide pour cela. Il faut le ‘réveiller’, pour cela, bougez votre souris rapidement dans la fenêtre de Putty pour faire avancer la barre de ‘chargement’.

Une fois cela fait, vous voyez votre clé publique apparaitre, elle est en clair.

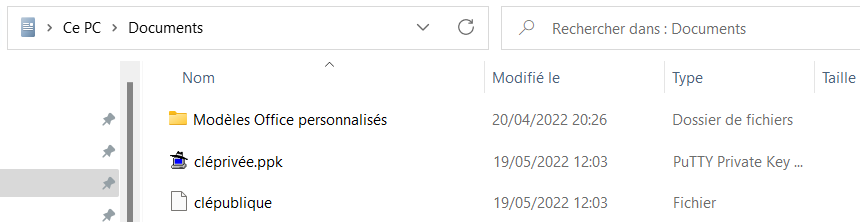
Pour plus de sécurité, il est recommandé de saisir une ‘passphrase’ qui sera le ‘mot de passe’ pour créer et **chiffrer** votre clé publique. Donc elle ne sera plus ‘en clair’.

Saisissez une phrase que vous retiendrez. Attention, vous aurez besoin de vous rappeler de cette passphrase, car elle sera demandée à chaque connexion.

Ensuite, enregistrez en cliquant sur ‘Save **public** key’.   
Enregistrez là ou bon vous semble, sous le nom que vous souhaitez. Choisissez quand même un nom parlant !   
Ensuite, enregistrez la clé privée ‘Save **private** key’. Nommez là comme bon vous semble, mais donnez-lui l’extension .ppk .



Voilà ce que donne la sauvegarde de mes clés sur la machine cliente Windows, sur laquelle j’ai créé les clés.



## Envoi de la clé publique au serveur Linux

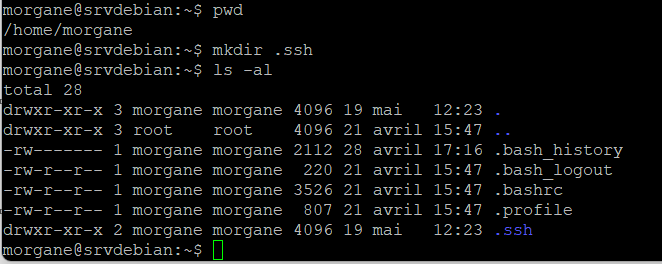
À présent, envoyons la clé publique au serveur Linux sur lequel on voudrait se connecter.

Ouvrez Putty, attention, sans fermer Puttygen. Connectez-vous au serveur Linux en connexion ssh simple ou classique, c’est-à-dire avec le mot de passe, comme vous le faites d’habitude.

Déplacez-vous dans le dossier personnel de votre utilisateur ~ : pour moi = /home/morgane

Créez dedans un dossier caché nommé .ssh

/!\ ne créez pas le dossier en mettant sudo, sinon vous ne serez pas le propriétaire du dossier.



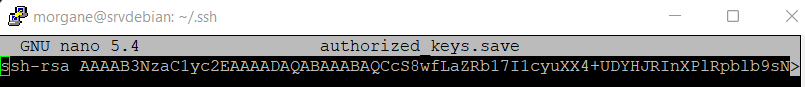
Vu que vous êtes connecté en ssh, vous allez pouvoir faire des copier / coller !

Déplacez-vous dans le dossier .ssh que vous venez de créer. Vous allez créer le fichier nommé authorized\_keys



Retournez sur la fenêtre de votre PuttyGen, et sélectionnez en entier la clé publique écrite, elle doit commencer par « ssh-rsa » et terminer par « rsa-key-date », copiez cette clé.

Allez sur votre fenêtre de putty qui est connectée à votre machine, avec le fichier authorized\_keys ouvert. Faites un clic droit sur votre souris pour coller votre clé dans le fichier.



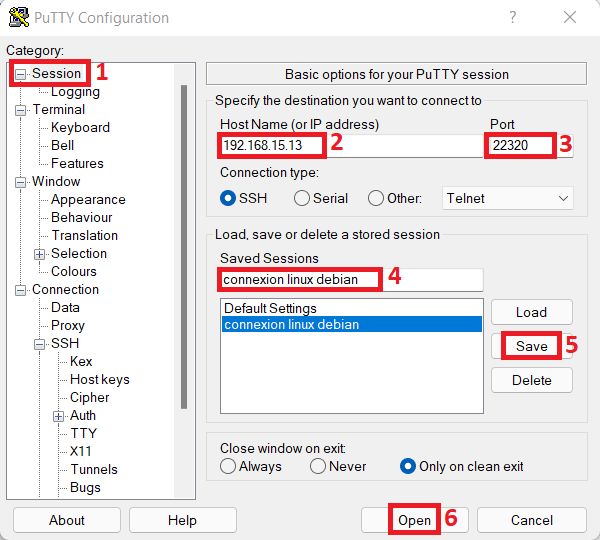
Toute la clé s’écrit sur une seule ligne. Enregistrez le fichier.

Vous voilà donc sur votre serveur Linux, avec dans votre dossier personnel un dossier caché nommé .ssh, et dedans un fichier nommé « authorized\_keys » qui contient la clé publique que vous aviez préalablement générée sur votre machine cliente.

Vous pouvez fermer les fenêtres de putty et putty Gen, car nous allons lancer une nouvelle connexion ssh en utilisant les clés asymétriques.

## Connexion avec les clés

Ouvrez une nouvelle fois Putty. À gauche dans les catégories, cliquez sur ‘Connection’, puis sur ‘SSH’, et sur ‘Auth’. Grâce au bouton ‘Browse’, recherchez sur votre machine le fichier contenant votre clé privée, celui que vous avez nommé terminant par .ppk.

À gauche, retournez sur la catégorie ‘Session’. Entrez l’adresse IP de votre serveur, ainsi que le port ssh. Avant de faire ‘Open’, donnez un nom à votre connexion dans le champ ‘Save‘, et cliquez sur ‘Save’. Cela enregistrera tous les paramètres que vous venez de saisir pour cette connexion. À présent, vous pouvez cliquer sur ‘Open’.

Comme d’habitude, on vous demande le nom de votre utilisateur, et ensuite la passphrase que vous avez paramétrée à partir de Putty.



Vous voilà connectés de manière sécurisée grâce aux clés et à la passphrase !!

Voici un schéma récapitulatif de la connexion ssh avec les clés asymétriques.

