# TP3 : Authentification SSH par Login/Mot de Passe

Table des matières

[TP3 : Authentification SSH par Login/Mot de Passe 1](#_Toc43566676)

[1. Objectif 1 : Authentification par mot de passe : 1](#_Toc43566677)

[2. Objectif 2 : authentification par Certificat 3](#_Toc43566678)

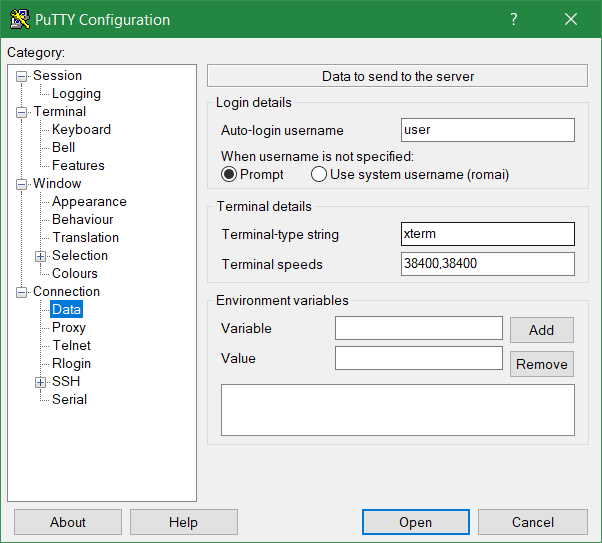
[A. Création de la clé 3](#_Toc43566679)

[B. Mise en place de la clé sur PuTTY 3](#_Toc43566680)

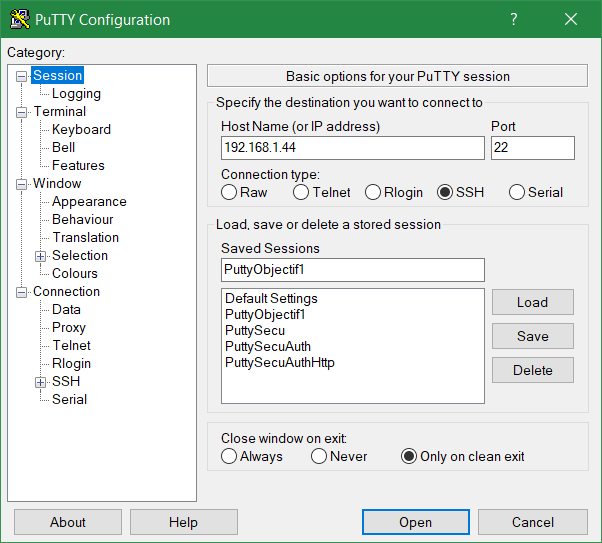
[C. Pratique 4](#_Toc43566681)

## Objectif 1 : Authentification par mot de passe :

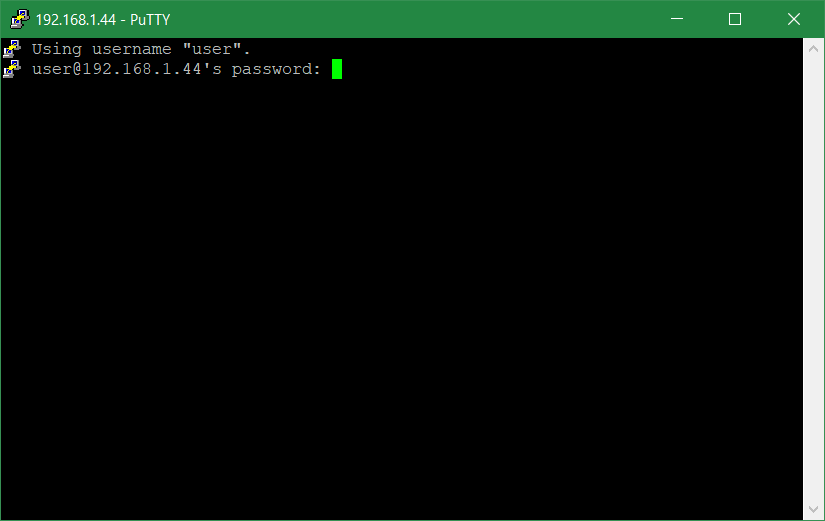
Pour avoir a éviter de rentrer a chaque fois son login, il est possible de l’enregistrer dans Putty :



Il suffit ensuite d’enregistrer l’IP de la machine et de cliquer sur Open :



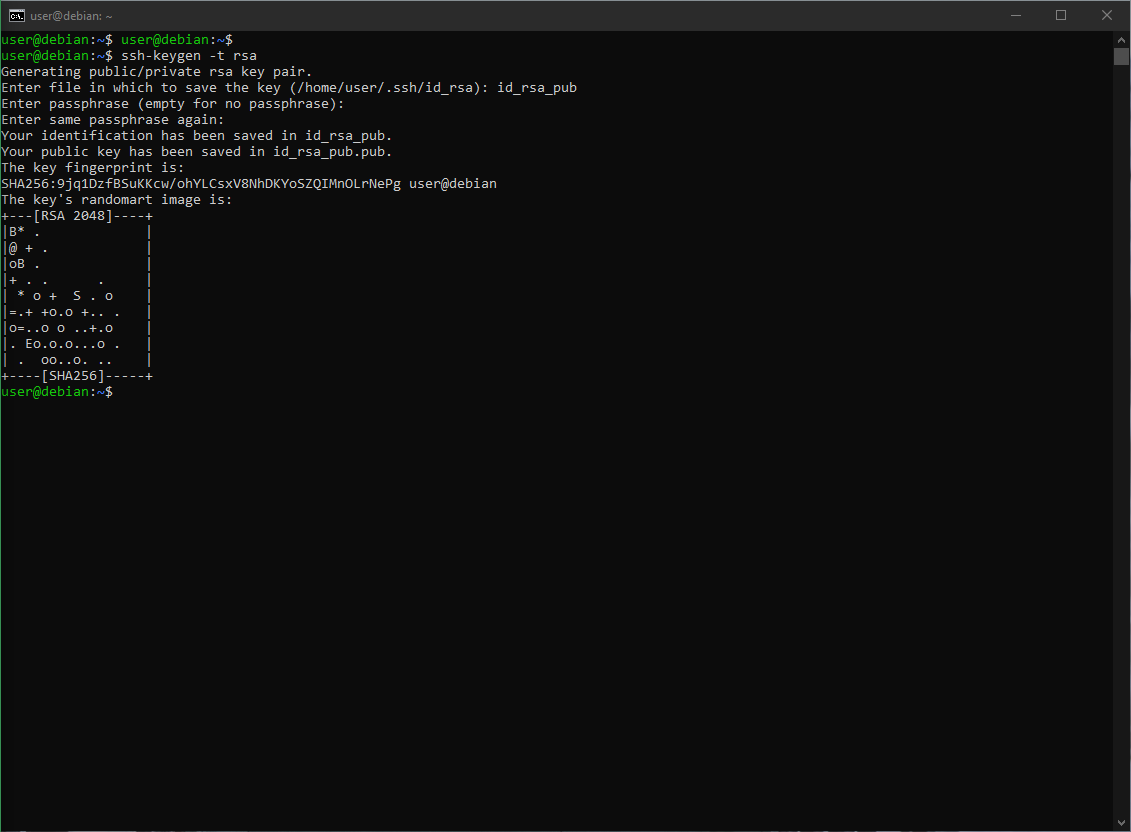
Nous pouvons maintenant nous connecter juste en tapant le mot de passe dans la console Putty



## Objectif 2 : authentification par Certificat

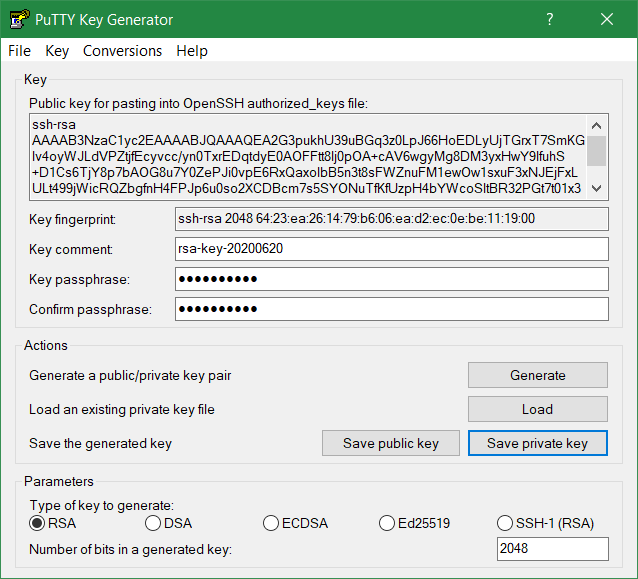
### Création de la clé

Grace a la commande **ssh-keygen -t rsa** nous pouvons créerun certificat pour pouvoir, au final, se connecter sans donner de mdp. Il suffit de trouver une paraphrase pour générer une clé en SHA256. Pour ma part la paraphrase est rattrapage.



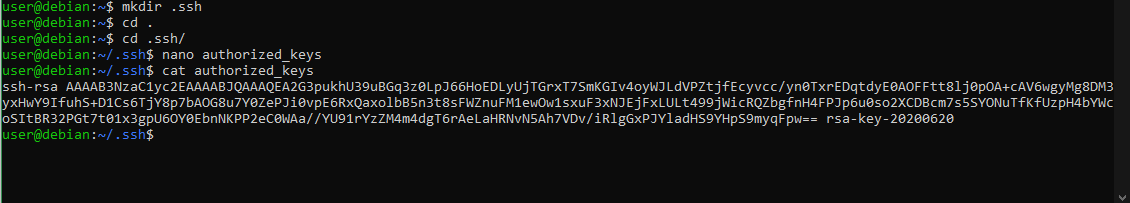
### Mise en place de la clé sur PuTTY

Nous devons maintenant générer la clé sur putty. Pour ça, nous allons utiliser PuTTYGen pour pouvoir générer des clés. Je vais utiliser la même paraphrase que sur mon client : rattrapage



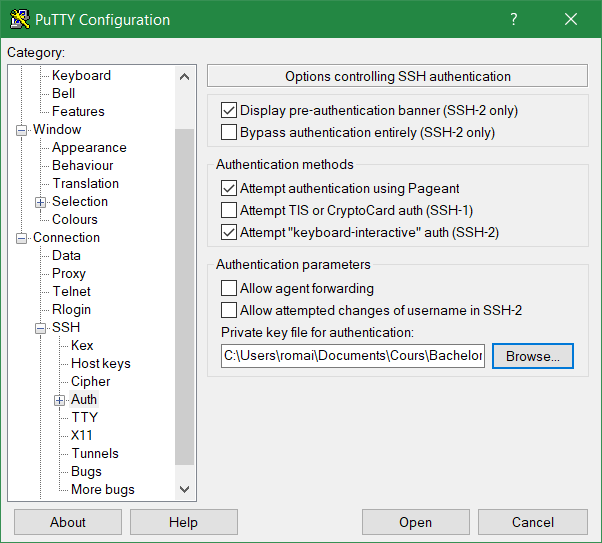
J’ai maintenant enregistré les 2 clé (private et public) dans un dossier.

Il faut aussi enregistrer la clé dans le linux dans un dossier que nous devons créé : .ssh/authorized\_keys



### Pratique

Maintenant que toute la mise en place a été faite, il faut maintenant activer la configuration. Pour cela il faut aller dans PuTTY puis dans Auth et indiquer le chemin du fichier ou nous avons enregistrer les clé de PuTTYGen :



On peut voir que cela a fonctionner puisqu’il nous demande la phrase de sécurité, ici rattrapage.

