

Bing

Le fichier **id_ed25519.pub** dans le répertoire **.ssh** correspond à la **clé publique** utilisée pour l'authentification par échange de clés SSH. Voici quelques explications pour mieux comprendre :

1. Authentification par échange de clés SSH :

- L'authentification par échange de clés SSH est un moyen sécurisé de se connecter à un ordinateur distant.
- Elle fonctionne en utilisant une **paire de clés** : une **clé publique** (fichier **id_ed25519.pub**) et une **clé privée** (généralement nommée **id_ed25519**).
- Ces deux clés sont liées l'une à l'autre. Pour se connecter, vous présentez la **clé privée** au serveur distant via la **clé publique**.

2. Fichiers associés aux clés SSH :

- Sur votre ordinateur :
 - **id_ed25519** : votre **clé privée**.
 - **id_ed25519.pub** : votre **clé publique**.
- Sur le serveur distant :
 - **authorized_keys** (dans le répertoire **~/.ssh**) : liste des **clés publiques** autorisées pour se connecter à l'utilisateur (c'est ici que vous devez placer votre **clé publique**).

3. Algorithme Ed25519 :

- L'algorithme **Ed25519** est considéré comme le plus sûr pour générer des clés SSH aujourd'hui.
- Il est recommandé d'utiliser ce type de clé pour renforcer la sécurité de vos connexions SSH.

Si vous souhaitez configurer l'authentification par clés SSH, vous pouvez suivre les étapes décrites dans cet [article](#) (en français). N'hésitez pas à générer votre paire de clés et à sécuriser vos connexions ! 🚀

cet article (en français).

<https://lecrabeinfo.net/se-connecter-en-ssh-par-echange-de-cles-ssh.html>