SSH (GIT) Secure Shell

SSH (Secure Shell) verification is a method used to securely authenticate and establish a connection between your local Git environment and a remote repository (e.g., GitHub, GitLab). Instead of using your username and password for every push or pull operation, SSH uses a pair of cryptographic keys:

Private Key: Stored on your local machine, this remains secret.

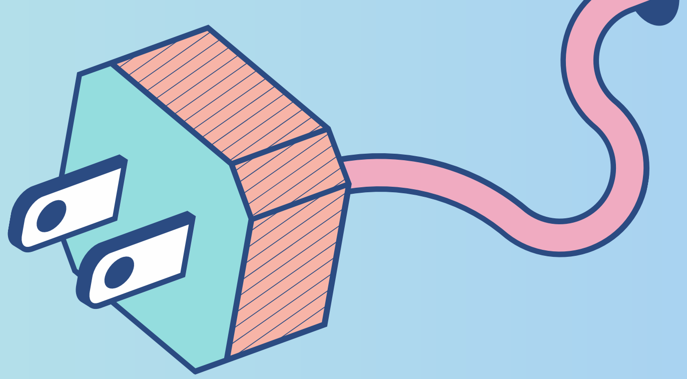
Public Key: Shared with the remote repository, this is used to verify your identity.

-Rabindra Mishra

Why we need SSH?

- **Enhanced Security:** SSH is encrypted and uses a private-public key pair, making it more secure than using plain HTTPS with username and password.
- **Passwordless Authentication:** Once set up, SSH doesn’t require you to enter your credentials every time.
- **Better Automation:** SSH keys are ideal for automated tasks like CI/CD pipelines because they don’t require manual intervention for authentication.

Advantages of SSH



High Security:

- No plain-text credentials are transmitted.
- Keys are difficult to intercept or crack due to encryption.

Ease of Use After Setup:

- No need to enter your credentials for each Git operation.

Best for Automation:

- Ideal for integrating Git into scripts or CI/CD systems.