Git Kullanım Rehberi

DOWNLOAD AND INSTALL THE LATEST VERSION OF GIT

On your computer, open the Terminal application.

```
sudo apt-get install git-core
```

Setup Git Config

```
sudo nano ~/.gitconfig
```

Or you can use the follow commands to add in the required information.

```
git config --global user.name ''NewUser''
git config --global user.email newuser@example.com
git config --list
```

Authenticating with Github from Git

If you clone with SSH, you must generate SSH keys on each computer you use to push or pull from GitHub.

GENERATING SSH KEYS

First, we need to check for existing SSH keys on your computer. Open Terminal and enter:

```
ls -al ~/.ssh
# Lists the files in your .ssh directory, if they exist
```

GENERATE A NEW SSH KEY

With Terminal still open, copy and paste the text below. Make sure you substitute in your GitHub email address.

```
ssh-keygen -t rsa -b 4096 -C ''your_email@example.com''
# Creates a new ssh key, using the provided email as a label
# Generating public/private rsa key pair.
```

ADD YOUR KEY TO THE SSH-AGENT

To configure the ssh-agent program to use your SSH key
Ensure ssh-agent is enabled:

```
# start the ssh-agent in the background
eval ''$(ssh-agent -s)''
```

Add your SSH key to the ssh-agent:

```
ssh-add ~/.ssh/id_rsa
```

ADD YOUR SSH KEY TO YOUR ACCOUNT

To configure your GitHub account to use your SSH key:

```
xclip -sel clip < ~/.ssh/id_rsa.pub
# Copies the contents of the id_rsa.pub file to your clipboard
```

Add the copied key to GitHub

TEST THE CONNECTION

To make sure everything is working, you'll now try to SSH into GitHub. When you do this, you will be asked to authenticate this action using your password, which is the SSH key passphrase you created earlier.

```
ssh -T git@github.com
# Attempts to ssh to GitHub
```