

SSH Keys

Computing

Generating, adding and using a key pair instead of a password.

Modern practice: ed25519 rather than RSA.

1

Generate

```
ssh-keygen -t ed25519 -C "you@example.com"
```

2

Use a passphrase

It encrypts the key on disk. The agent means you type it once per session.

3

Add to the agent

```
ssh-add ~/.ssh/id_ed25519
```

4

Copy the PUBLIC key

The .pub file. `ssh-copy-id`, or paste it into the service.

5

Test

```
ssh -T git@github.com
```

FILES

`id_ed25519` — private, never share

`id_ed25519.pub` — public, safe to paste

`~/.ssh/config` — per-host settings

Private keys need mode 600 and the `.ssh` directory 700. SSH refuses to use a key anyone else can read.