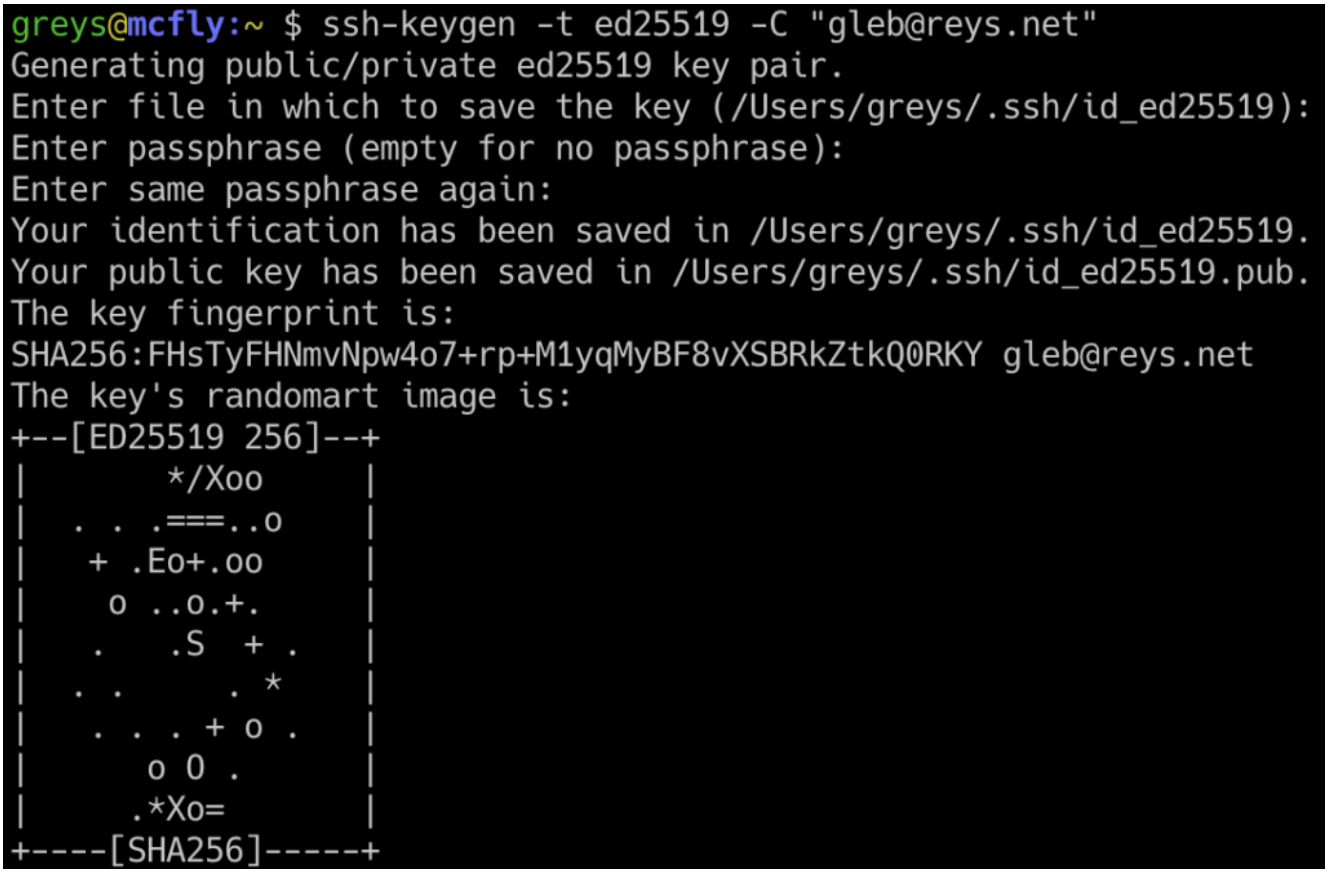
How To Generate ed25519 SSH Key



Generating ed25519 SSH Key

I'm hoping to reinstall my MacBook Pro 15″ 2017 with a fresh macOS Catalina sometime soon, and part of preparations is testing my install methods (hello, brew!) and configuration files migration. Today I decided to **setup a new SSH keypair**.

What is ed25519?

ed25519 is a relatively new cryptography solution implementing Edwards-curve Digital Signature Algorithm (EdDSA).

I say relatively, because ed25519 is supported by OpenSSH for about 5 years now – so it wouldn't be considered a cutting edge. Still, people are such creatures of habits that many IT professionals daily using SSH/SCP haven't even heard of this key type.

Similarly, not all the software solutions are supporting ed25519 right now – but SSH implementatinos in most modern Operating Systems certainly support it.

Why ed25519 Key is a Good Idea

Compared to the most common type of SSH key – RSA – ed25519 brings a number of cool improvements:

- it's faster: to generate and to verify
- it's more secure
- collision resilience – this means that it's more resilient against hash-function collision attacks (types of attacks where large numbers of keys are generated with the hope of getting two different keys have matching hashes)
- keys are smaller – this, for instance, means that it's easier to transfer and to copy/paste them

Generate ed25519 SSH Key

Here's the command to generate an ed25519 SSH key:

```
greys@mcfly:~ $ ssh-keygen -t ed25519 -C "gleb@reys.net"
Generating public/private ed25519 key pair.
Enter file in which to save the key (/Users/greys/.ssh/id_ed25519):
Enter passphrase (empty for no passphrase):
Enter same passphrase again:
Your identification has been saved in /Users/greys/.ssh/id_ed25519.
Your public key has been saved in /Users/greys/.ssh/id_ed25519.pub.
The key fingerprint is:
SHA256:FHsTyFHNmvNpw4o7+rp+M1yqMyBF8vXSBRkZtkQ0RKY gleb@reys.net
The key's randomart image is:
+--[ED25519 256]--+
|       */Xoo     |
|  . . .===..o    |
|   + .Eo+.oo     |
|    o ..o.+.     |
|   .   .S  + .   |
|  . .     . *    |
|   . . . + o .   |
|      o O .      |
|     .*Xo=       |
+----[SHA256]-----+
```

That’s it — this keypair is ready to be deployed to SSH servers, GitHub or any other service that can use them.

Check out how short the public key is:

```
ssh-ed25519 AAAAC3NzaC1lZDI1NTE5AAAAIK0wmN/Cr3JXqmLW7u+g9pTh+wyqDHpSQEIQczXkVx9q gleb@reys.net
```

See Also

- **SSH Reference**
- **Passwordless SSH**
- SSH Port Forwarding
- **SSH Port**
- Use multiple ports with SSH
- Check SSH key fingerprint
- ssh command