Ed25519 sample

We will show a sample SSH setting using Ed25519 key in this page.
The procedure itself is common among Windows PowerShell, Mac Terminal.app, and various Linux terminal emulators.
You need to type (or paste) red-colored texts. Blue-colored texts are mere comments or notes.
Some strings, such as "user" and "hostname", are system-dependent.

First, we generate a new key pair.

```
user@hostname ~ %ssh-keygen -t ed25519
Generating public/private ed25519 key pair.
Enter file in which to save the key (/Users/user/.ssh/id_ed25519): (press enter is default loc is OK)
Enter passphrase (empty for no passphrase): (input password for this key)
Enter same passphrase again: (input password for this key, again)
Your identification has been saved in /Users/user/.ssh/id_ed25519 (private key file)
Your public key has been saved in/Users/user/.ssh/id_ed25519.pub (public key file)
The key fingerprint is:
SHA256:********************************************** user@hostname.domain
The key's randomart image is:
+--[ED25519 256]--+
|             |
|             |
|             |
|             |
|  (skipped)  |
|             |
|             |
|             |
|             |
+----[SHA256]-----+
user@hostname ~ %
```

You need to upload contents of public key ~/.ssh/id_ed25519.pub (/Users/user/.ssh/id_ed25519.pub) to this website according to the guide in this page.
The location of key files can be found in the ssh-keygen log. The public key file (.pub) is a text file and it should contain single-line text.
You should upload that line. You MUST NOT upload private key file (~/.ssh/id_ed25519 here).

The key pair generated here can be used for other software such as WinSCP, cyberduck, and FileZilla.

Once you uploaded the public key, let's login to login server.

```
user@hostname ~ %ssh uid@ccfep.ims.ac.jp (uid is a three-letter ID provided by RCCS (e.g. xxx))
The authenticity of host 'ccfep.ims.ac.jp (133.48.230.13)' can't be established.
ED25519 key fingerprint is SHA256:0KL38Yn/kBee1pAuxyKwenEwXjtPxr9ZElolfVqXvbI. (some other string might be shown; see below)
This key is not known by any other names
Are you sure you want to continue connecting (yes/no/[fingerprint])?yes (required upon first login)
Warning: Permanently added 'ccfep.ims.ac.jp' (ED25519) to the list of known hosts.
Enter passphrase for key '/Users/user/.ssh/id_ed25519': (input password used at ssh-keygen step)
[uid@ccfep* ~]$ (you can login to one of login server if you input correct password.)
```

Most of the strings other than passphrase one are first-time only. You won't see those confirmation messages on second and subsequent login attempts.

Tips

Some tips about login.

Host fingerprint

After the "*** key fingerprint is" message, one of following fingerprints will be displayed.

- ad:de:79:30:81:b0:b1:6a:17:f5:6f:ea:f4:b4:3b:de (MD5)
- e3:a9:bb:6f:e4:a9:37:fd:98:14:54:16:3c:81:2d:aa (MD5)

- 07:7e:df:7b:16:47:a8:f5:7c:48:b0:a3:d3:86:71:6a (MD5)
- wnEM30z4AxyDJ9XI/DdGr2PlNeoivFRR8v5krXHEmdU (SHA256)
- 0KL38Yn/kBee1pAuxyKwenEwXjtPxr9ZEIolfVqXvbI (SHA256)
- Nhg+9Lgj3XeuW//A/j7jqgUJlIxWehryCtStIp1Dir (SHA256)

Configuration file (~/.ssh/config)

You can save settings in ~/.ssh/config file. You can omit domain name (.ims.ac.jp), username (e.g. xxx) by using following example.
Blue-colored "uid" must be replaced with your user ID (three-letter ID provided by RCCS).
If you have more than one keys, you may need to specify key file with "IdentityFile" keyword.

```
Host ccfep
  HostName ccfep.ims.ac.jp
  User uid
```