

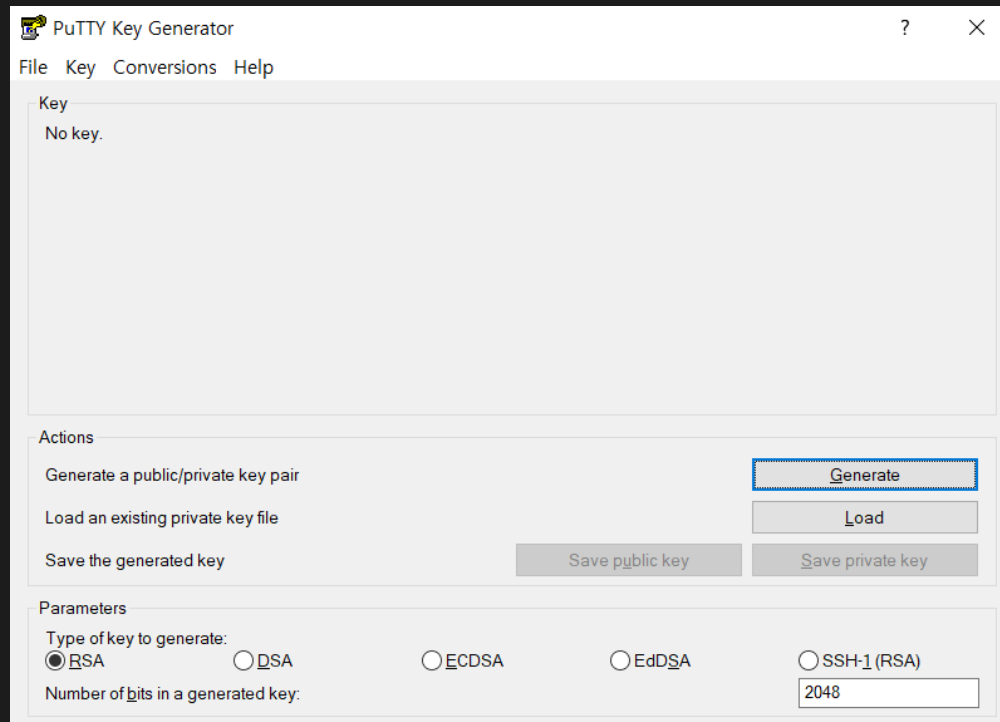
SSH

- Secure shell
 - 원격지 웹에 접속하기 위한 클라이언트. 축약해서 ssh라고 한다.
 - 두 단말기간의 네트워크를 하기 위한 프로그램이라고 생각해도 좋음.
- 윈도우에서 제공하는 openssh과 git과 같은 시스템을 설치할 때 사용되는 putty가 있다.
 - git을 사용하는 기반, 예를 들어 토토이즈깃이나 소스트리의 경우 putty를 이용한다.
 - openssh는 특정 윈도우10 버전 이상이면 내장으로 설치된다.
- 버전관리 시스템을 사용할 때, 원격 저장소에 접근을 해야 한다. 이때, 접근에 대한 권한 획득을 ssh를 통한 인증을 이용하는 경우가 많음.
 - 키 인증을 이용한 방법
 - 단순 로그인 방식
 - Id, password

OpenSSH를 이용한 키 생성

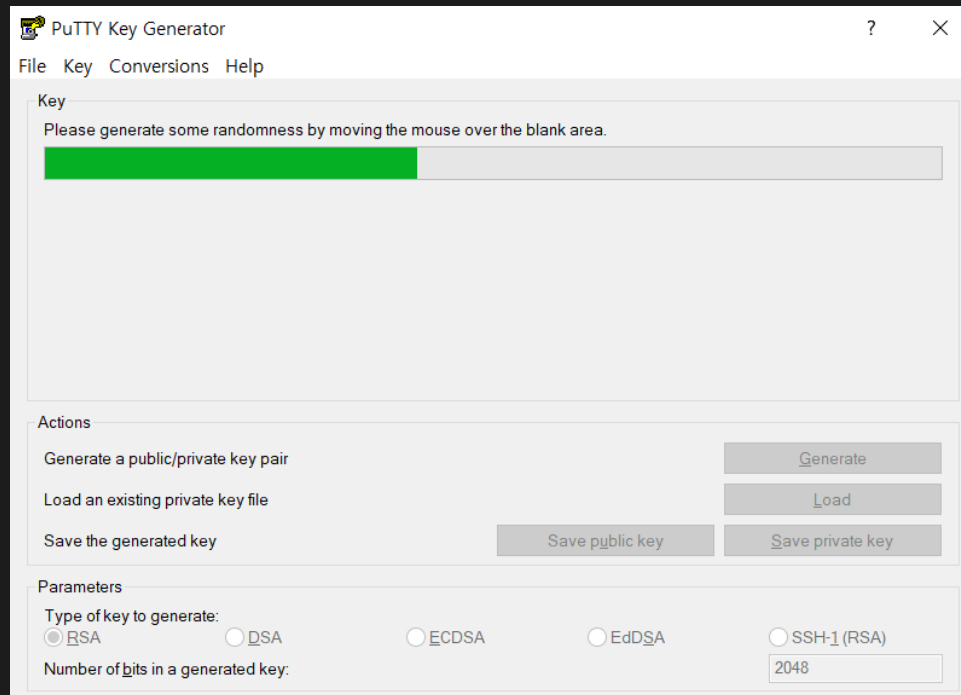
- `ssh-keygen -t rsa -b 4096 -C "your_email@example.com"`
 - `-t rsa` 알고리즘 사용
 - `-b 4096` 키 길이를 4096 비트로 설정
 - `-C` 키 식별을 위한 주석 (일종의 시그니처)
 - 로그인한 user 폴더 아래에 `.ssh` 폴더 기준으로 `id_rsa / id_rsa.pub` 파일 생성
 - 키 생성시 암호를 묻는 과정이 진행되는데, 필수는 아님. (권고)

Putty를 이용한 키 생성 - 1



- puttygen.exe
- 파라미터에서 키 생성 알고리즘을 선택.

Putty를 이용한 키 생성 - 2



- 키 생성 시작하면, 랜덤 요소를 적용하기 위해 마우스 이동을 진행.

Putty를 이용한 키 생성 - 3

The screenshot shows the PuTTY Key Generator window. The 'Key' section displays the public key for pasting into an OpenSSH authorized_keys file. The key is a long string of characters. Below the key, there are fields for the key fingerprint, key comment, key passphrase, and confirm passphrase. The 'Actions' section contains buttons for 'Generate', 'Load', 'Save public key', and 'Save private key'. The 'Parameters' section shows the type of key to generate (RSA is selected) and the number of bits in a generated key (2048).

Key

Public key for pasting into OpenSSH authorized_keys file:

```
ssh-rsa AAAAB3NzaC1yc2EAAAADAQABAAQDYNcZ8mQeSWMDwlsK4N2+idtGh23zdCh
+q2OCNnoUPVXFD2Felur2+1/FOCLyRvG3vYxG0wElqwNvAn8m1AkkM7clMvPKGOVpzQL4tWUcvxSgpm
+axC6ewqlqL9w+Hquvq6hhPz1sT9zIF7Vpv+m/V5qEuTXruuhH2dtEejxbKVv7eMcW7lkm1h
+5wfaIKMD4shZHPri0ztrDtS5YNuewLCtkthix
+0J8g7D010Pg5s4SJT/y/FPYz/FmojMm3f/GlmAa/z/dpn0dOMDPZHlxwryp7Kz1nlivczdtVJEsFPVJGqk2fPfwk3vkdttWY
```

Key fingerprint: ssh-rsa 2048 SHA256:X7XmFAQ/g7Dx1SFBGcMDQX7g9uFJVTI2gEoV4ibqUpU

Key comment: rsa-key-20241207

Key passphrase:

Confirm passphrase:

Actions

Generate a public/private key pair Generate

Load an existing private key file Load

Save the generated key Save public key Save private key

Parameters

Type of key to generate: ☒ RSA ☐ DSA ☐ ECDSA ☐ EdDSA ☐ SSH-1 (RSA)

Number of bits in a generated key: 2048

- 완료되면, public key 값이 생성되어 있음.
- public, private key를 각각 저장할 수 있음. 일반적으로 ssh키는 사용자계정/.ssh/ 밑으로 생성한다.