**Tìm hiểu SSH bằng key pair**

1. Khái niệm

SSH Key là một phương thức chứng thực người dùng truy cập bằng cách đối chiếu giữa một key cá nhân (Private Key) và key công khai(Public Key).

1. Thành phần chính của một SSH Key

Khi tạo ra một SSH Key,  có 3 thành phần quan trọng như sau:

**Public Key (dạng file và string)** – copy ký tự key này sẽ bỏ vào file ~/.ssh/authorized\_keys trên server của bạn.

**Private Key (dạng file và string)** – lưu file này vào máy tính, sau đó sẽ thiết lập cho PuTTY, WinSCP, MobaXterm,..để có thể login.

**Keypharse (dạng string, cần ghi nhớ)** – Mật khẩu để mở private key, khi đăng nhập vào server nó sẽ hỏi cái này.

1. Cách tạo SSH key
2. Tạo bằng Windows

* Tạo SSH Key bằng phần mềm putty gen

**Graphical user interface, application

Description automatically generated**

Rê con chuột xung quanh để tạo  

**Graphical user interface, text, application, email

Description automatically generated**

Nhập passphrase và save private key

1. Tạo bằng Linux

Bước 1: Mở Terminal và gõ lệnh ssh-keygen -t rsa

**Text

Description automatically generated**

Kết quả sẽ ra như hình

Bước 2: Mở file id\_rsa bằng lệnh cat id\_rsa

**Text

Description automatically generated**

Copy file này và lưu lại

Bước 3:  Truy cập vào sshd\_config bằng lệnh sudo nano /etc/ssh/sshd\_config để sửa lại **#PubkeyAuthentication yes** thành **PubkeyAuthentication yes** 

**Text

Description automatically generated**

Bước 4: Bây giờ dùng MobaXterm truy cập SSH

**Graphical user interface

Description automatically generated**

Ở phần Use private key tick vào đó và chọn file key pair đã lưu sau đó bấm OK

Bước 5: Nhập private key



Bước 6: Tiếp theo, điền login và pass



Bước 7: Đăng nhập thành công

**Text

Description automatically generated**