Git Security SSH

- Thông thường kết nối tới repo thì sử dụng HTTPS
- Nên sử dụng SSH nếu làm việc với các mạng không bảo mật
- Đôi khi, 1 dự án sẽ yêu cầu sử dụng SSH

SSH là gì

- SSH là giao thức mạng shell an toàn được sử dụng để quản lý mạng, truyền tệp từ xa và truy cập hệ thống từ xa.
- SSH sử dụng một cặp khóa SSH để thiết lập giao thức mạng bảo mật được xác thực và mã hóa. Nó cho phép liên lạc từ xa an toàn trên các mạng mở không bảo mật.
- Khóa SSH được sử dụng để bắt đầu "bắt tay" an toàn. Khi tạo một bộ khóa, bạn sẽ tạo khóa "công khai" và "riêng tư".
- Khóa "công khai" là khóa bạn chia sẻ với bên ở xa. Hãy nghĩ về điều này nhiều hơn như ổ khóa.
- Khóa "riêng tư" là khóa bạn giữ cho riêng mình ở một nơi an toàn. Hãy coi đây là chìa khóa của ổ khóa.
- Khóa SSH được tạo thông qua thuật toán bảo mật. Tất cả đều rất phức tạp, nhưng nó sử dụng các số nguyên tố và số ngẫu nhiên lớn để làm khóa chung và khóa riêng.
- Nó được tạo để khóa chung có thể được lấy từ khóa riêng, nhưng không phải ngược lại.

Tạo cặp khoá SSH

- Sử dụng email làm nhãn:

```
ssh-keygen -t rsa -b 4096 -C “email
```

- Tiếp đến, thêm cặp khoá SSH vào SSH-Agent (Vị trí tệp đc miêu tả khi tạo) Enter file in which to save the key (/c/Users/user/.ssh/id_rsa)

```
ssh-add /Users/user/.ssh/id_rsa
```

Sử dụng key SSH trên repo

- Sao chép khoá công khai

```
clip < /Users/user/.ssh/id_rsa.pub
```

- Truy cập vào repo (github, gitlab), vào setting, vào SSH and GPG keys
- Thêm khoá vào rồi save

Kiểm tra kết nối SSH với Github

ssh -T git@github.com