Chaves SSH são a forma de autenticação do github para quando tentamos fazer commits a um repositório remoto. Nessa ocasião o git verifica se a chave SSH local de nossa máquina abre a chave pública que está no servidor, se isso acontecer então estamos liberados para fazer commits.

- Como gerar o par de chaves SSH:

Comando: ssh-keygen -C “e-mail do usuário usado no github”

Após executar o comando ira aparecer a mensagem abaixo indicando que a chave SSH pública e privada foi gerada:



Abaixo ira aparecer uma mensagem solicitando o nome do diretório aonde as chaves serão salvas, o padrão é o informado na mensagem (mudando apenas o usuário) e se não quiser alterar aperte enter:



Abaixo dela ira aparecer uma mensagem solicitando uma senha e a confirmação da mesma, caso não queira informar e só apertar “enter” nas duas:



- Aonde as chaves SSH são armazenadas no disco?:

As chaves ficam armazenadas no diretório “.ssh” do nosso usuário, com o comando ls podemos ver os a chave privada “id\_rsa” e a chave pública “id\_rsa.pub” no diretório conforme abaixo:



A chave que deve ser adicionada ao servidor é a que está no arquivo “id\_rsa.pub”, para mostra-la via git bash digite “cat id\_rsa.pub”. Após pegar a chave pública vá em seu Github e faça os seguintes passos:

1 – Settings(Configurações);

2 – SSH and GPG Keys (chaves SSH e GPG);

3 – new SSH key (nova chave SSH);

4 – Cole a chave no campo “key” e defina o título para identificação da chave, este título só é utilizado no Github para identificar melhor a chave.

5 – clique em “Add SSH key”(adicionar chave SSH);