## ssh-keygen -t rsa -b 4096 -C "邮箱"：这条命令的目的是为了让本地机器ssh登录远程机器上的GitHub账户无需输入密码。将这条命令分解：

### 1、ssh-keygen：

SSH 为 Secure Shell 的缩写，SSH 为建立在应用层基础上的安全协议。SSH 是目前较可靠，专为远程登录会话和其他网络服务提供安全性的协议。利用 SSH 协议可以有效防止远程管理过程中的信息泄露问题。

从客户端来看，SSH提供两种级别的安全验证：

        第一种级别（基于口令的安全验证）：只要你知道自己帐号和口令，就可以登录到远程主机。所有传输的数据都会被加密，但是不能保证你正在连接的服务器就是你想连接的服务器。可能会有别的服务器在冒充真正的服务器，也就是受到“中间人”这种方式的攻击。

        第二种级别（基于密匙的安全验证）ssh-keygen：需要依靠密匙，你必须为自己创建一对密匙，并把公用密匙放在需要访问的服务器上。如果你要连接到SSH服务器上，客户端软件就会向服务器发出请求，请求用你的密匙进行安全验证。服务器收到请求之后，先在该服务器上你的主目录下寻找你的公用密匙，然后把它和你发送过来的公用密匙进行比较。如果两个密匙一致，服务器就用公用密匙加密“质询”（challenge）并把它发送给客户端软件。客户端软件收到“质询”之后就可以用你的私人密匙解密再把它发送给服务器。用这种方式，你必须知道自己密匙的口令。但是，与第一种级别相比，第二种级别不需要在网络上传送口令。第二种级别不仅加密所有传送的数据，而且“中间人”这种攻击方式也是不可能的（因为他没有你的私人密匙）。但是整个登录的过程可能需要10秒 。

        ssh-keygen有很多的参数，比如这里的-t -b -C都是他的一些参数。

### 2、-t rsa：t是type的缩写

-t即指定密钥的类型，密钥的类型有两种，一种是RSA，一种是DSA：

        RSA：RSA加密算法是一种非对称加密算法，是由三个麻省理工的牛人弄出来的，RSA是他们三个人姓的开头首字母组合。

        DSA：Digital Signature Algorithm (DSA)是Schnorr和ElGamal签名算法的变种。

为了让两个linux机器之间使用ssh不需要用户名和密码。所以采用了数字签名RSA或者DSA来完成这个操作。ssh-keygen默认使用rsa密钥，所以不加-t rsa也行，如果你想生成dsa密钥，就需要加参数-t dsa。

### 3、-b 4096：b是bit的缩写

-b 指定密钥长度。对于RSA密钥，最小要求768位，默认是2048位。命令中的4096指的是RSA密钥长度为4096位。

DSA密钥必须恰好是1024位(FIPS 186-2 标准的要求)。

### 4、-C "邮箱"：C是comment的缩写

-C表示要提供一个新注释，用于识别这个密钥，所以“”里面不一定非要填邮箱，可以是任何内容，邮箱仅仅是识别用的key

总结：当你创建ssh的时候：-t 表示密钥的类型 ，-b表示密钥的长度，-C 用于识别这个密钥的注释 ，这个注释你可以输入任何内容，很多网站和软件用这个注释作为密钥的名字