Tony Chang 的文档库

发布 *0.0.1*

Tony Chang

2022 年 03 月 31 日

GitHub

轩辕黄帝四千七百十九年。岁在壬寅之春。

欲整理档案。成此文档库。

一字一符。希冀略有裨益。

若无所得。亦毋悲已。

心平气清。恒念辞句。

秦穆饮盗马。楚客报绝缨。

CHAPTER 1

GitHub

文章 *SSH 密钥创建大法 | SSH*

词汇表 *词汇表*

1.1 SSH 密钥创建大法

无论是实现 SSH 免密登录，还是想要 SCP 免密发送文件，还是 Git 免密提交代码，都需要用到 SSH 密钥。本文简单介绍 SSH 密钥的生成方法。

1.1.1 科普几个基本概念

密钥 在密码学中，**密钥**[1] *Key* 是指某个用来完成加密、解密、完整性验证等密码学应用的秘密信息。在 **对称密钥算法** *Symmetric-key algorithm* 中，加密和解密用的是同一个钥匙，因此钥匙需要保密。而在 **公开密钥密码学** *Public-key cryptography* 中，加密和解密用的钥匙不同，一个是公开密钥，称为 **公钥** *Public key* ，另一个是私有密钥，称为 **私钥** *Private key* 。

对称密钥算法 **对称密钥算法** *Symmetric-key algorithm* 又称为对称加密、私钥加密、共享密钥加密，是密码学中的一类加密算法。这类算法在加密和解密时使用相同的密钥，或是使用两个可以简单地相互推算的密钥。

[1] 「密钥」中的「钥」为多音字。其在文言文中有文白异读的现象。1985 年 12 月，中华人民共和国国家语委、国家教委和广播电视部联合发布的《普通话异读词审音表》将其标注为 yào（语）和 yuè（文）两种读音。《现代汉语词典（第 7 版）》中将其注明为「【密钥】mìyuè（口语中多读 mìyào）」。

公开密钥密码学 **公开密钥密码学** *Public-key cryptography*，也称 **非对称式密码学** *Asymmetric cryptography*，是密码学的一种算法，它需要两个密钥，一个是公开密钥，称为 **公钥** *Public key*，另一个是私有密钥，称为 **私钥** *Private key*。公钥用作加密，私钥则用作解密。使用公钥把明文加密后所得的密文，只能用相对应的私钥才能解密并得到原本的明文，最初用来加密的公钥不能用作解密。由于加密和解密需要两个不同的密钥，故被称为非对称加密；不同于加密和解密都使用同一个密钥的对称加密。公钥可以公开，可任意向外发布；私钥不可以公开，必须由用户自行严格秘密保管，绝不透过任何途径向任何人提供，也不会透露给被信任的要通信的另一方。

公钥 **公钥** *Public key* 和 **私钥** *Private key* 是通过 **公开密钥密码学** *Public-key cryptography* 的某种算法得到的、相互对应形成一对密钥对。其中可以向外界公开的，称为公钥；另个自己妥善保管，万万不可随意共享、传输给他人，称为私钥。通过这种算法得到的密钥对能保证在世界范围内是唯一的。使用这对密钥对的时候，使用公钥来对数据进行加密，使用私钥来对数据进行解密。

私钥 **私钥** *Private key* 详见上述 **公钥** *Public key* 的描述。

> **警告:** 同学们一定要保护好自己的密钥文件，尤其是私钥文件，不要轻易分享给他人！

当本文使用「密钥」这个词时，指的是一对公钥和私钥相互对应形成的「密钥对」，如果使用「公钥」、「私钥」这样的词，则特指「公钥」、「私钥」。

1.1.2 ssh-keygen 简介

`ssh-keygen` 命令用于生成、管理和转换 SSH 所支持的认证密钥，它支持 `RSA` 和 `DSA` 两种认证密钥。

语法格式

```
$ ssh-keygen [参数]
```

常用参数

参数	含义
-b	指定密钥长度
-e	读取 openssh 的私钥或者公钥文件
-f	指定用来保存密钥的文件名
-t	指定要创建的密钥类型
-C	添加注释

1.1.3 生成 SSH 密钥

打开 **终端** *Terminal* ，首先确认当前用户的 *home* 目录下有没有一个叫 *.ssh* 的目录，不存在的话请先创建，并赋予 `700` 的权限。

```
$ cd ~
$ mkdir -p ~/.ssh
$ chmod 700 ~/.ssh
```

直接使用 `ssh-keygen` 命令，不带任何参数，生成一对默认的公钥和私钥。

```
$ ssh-keygen
```

由于我们没有使用 `-f` 参数指定路径和文件名，程序会有如下提示。

> Generating public/private rsa key pair.
>
> Enter file in which to save the key (/Users/tony/.ssh/id_rsa):

直接敲回车，使用默认路径和文件名。程序又会有如下提示，询问是否为密钥文件设置密码。

> Enter passphrase (empty for no passphrase):
>
> Enter same passphrase again:

我们为了免密使用密钥，对于这两条提示都直接敲空格。如果有特殊的用途需要设置密码，那么请一定要将密码妥善保管。

> **警告:** 若没有为密钥设置密码（密码为空，直接两次敲了空格），请一定要保护好自己的私钥文件，不要轻易分享给他人！

小技巧: 若要为密钥设置密码，强烈建议使用密码生成器自动生成强密码，并使用密码管理工具，例如 Apple 平台的「钥匙串」。

设置密码后，程序会提示如下，表明公钥和私钥文件已经创建完成。

> Your identification has been saved in /Users/tony/.ssh/id_rsa.
>
> Your public key has been saved in /Users/tony/.ssh/id_rsa.pub.
>
> The key fingerprint is:
>
> ...(此处省略内容视实际情况)

`id_rsa` 文件即是密钥文件，`id_rsa.pub` 即是公钥文件。

从这个示例来看，不带任何参数的情况下，`ssh-keygen` 会默认生成一对 `RSA` 类型的公钥和私钥。

当然，你还可以使用 `-t` 参数手动指定生成 RSA 类型的公钥和私钥。

```
$ ssh-keygen -t rsa
```

1.1.4 其他示例

使用 -t 参数手动指定生成 RSA 类型的公钥和私钥，并使用 -C 参数添加注释，例如邮箱地址：

```
$ ssh-keygen -t rsa -C "your_email_address@example.com"
```

使用 -e 参数读取 openssh 的私钥或者公钥文件：

```
$ ssh-keygen -e
```

1.2 SSH

SSH 为 Secure Shell 的缩写，由 IETF 的网络小组（Network Working Group）所制定；SSH 为建立在应用层基础上的安全协议。SSH 是较可靠，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。SSH 最初是 UNIX 系统上的一个程序，后来又迅速扩展到其他操作平台。SSH 在正确使用时可弥补网络中的漏洞。SSH 客户端适用于多种平台。几乎所有 UNIX 平台（包括 HP-UX、Linux、AIX、Solaris、Digital UNIX、Irix）以及其他平台，都可运行 SSH。

1.2.1 功能

传统的网络服务程序，如：FTP、POP 和 Telnet 在本质上都是不安全的，因为它们在网络上用明文传送口令和数据，别有用心的人非常容易就可以截获这些口令和数据。而且，这些服务程序的安全验证方式也是有其弱点的，就是很容易受到「中间人」（man-in-the-middle）这种方式的攻击。

所谓「中间人」的攻击方式，就是「中间人」冒充真正的服务器接收你传给服务器的数据，然后再冒充你把数据传给真正的服务器。服务器和你之间的数据传送被「中间人」一转手做了手脚之后，就会出现很严重的问题。通过使用 SSH ，你可以把所有传输的数据进行加密，这样「中间人」这种攻击方式就不可能实现了，而且也能够防止 DNS 欺骗和 IP 欺骗。

使用 SSH ，还有一个额外的好处就是传输的数据是经过压缩的，所以可以加快传输的速度。SSH 有很多功能，它既可以代替 Telnet，又可以为 FTP、PoP、甚至为 PPP 提供一个安全的「通道」。

1.2.2 如何使用

待更新内容。

1.3 词汇表

密钥 在密码学中，密钥（key，又常称：金钥）是指某个用来完成加密、解密、完整性验证等密码学应用的秘密信息。在对称密码学（或称：密钥密码学）中，加密和解密用的是同一个钥匙，因此钥匙需要保密。而在非对称密码学（或称：公钥密码学）中，加密和解密用的钥匙不同：通常一个是公开的，称为公钥；另一个保密，称为私钥。其书面语读音为 mìyuè ，口语读音为 mìyào 。[1]

[1] 「密钥」中的「钥」为多音字。其在文言文中有文白异读的现象。1985 年 12 月，中华人民共和国国家语委、国家教委和广播电视部联合发布的《普通话异读词审音表》将其标注为 yào（语）和 yuè（文）两种读音。《现代汉语词典（第 7 版）》中将其注明为「【密钥】mìyuè（口语中多读 mìyào）」。

CHAPTER 2

macOS

文章 免费的 *macOS* 菜单栏工具，轻松隐藏图标：*Hidden Bar*

词汇表 词汇表

2.1 免费的 macOS 菜单栏工具，轻松隐藏图标：Hidden Bar

> Hidden Bar lets you hide menu bar items to give your Mac a cleaner look.
>
> Hidden Bar 帮您隐藏菜单栏图标，让您的 Mac 更清爽哟！*Tony Chang* 倾情翻译

每天使用 Mac 的你，一定安装了不少 App，随着 App 数量的增加，macOS 系统的菜单栏想必也被各种图标占领，你可能也想过，有没有一种小工具，把不常用的图标隐藏起来，看起来清清爽爽。

看看 Julien Grand-Poisson(@bfishadow) 怎么说：

> 一直不喜欢乱七八糟的 Menu 图标，之前都在用 Bartender 来管理。但升级 macOS Catalina 之后，它找我索取「全屏录制」权限，于是删了……
>
> 今天，发现了一个超级好用的替代品 Hidden Bar
>
> --- Julien Grand-Poisson(@bfishadow)

Hidden Bar 非常轻量，简洁的界面和方便的操作实现了隐藏菜单栏图标的需求。

运行 Hidden Bar，菜单栏上会出现一条分割线 | 和一个尖括号 > 。分割线 | 左侧是被隐藏的图标，简称为「隐藏区」，分割线 | 右侧则是长期显示的图标，简称为「显示区」。点按尖括号 > 用来控制「隐藏区」展开与否。

现在，就可以按住键盘上的 *command* 键，按自己的喜好拖拽图标了，要隐藏的图就把它拖到分割线 | 左侧哦！

要提醒各位，这个小工具有一项「自动隐藏图标」的功能，默认是开启状态，默认时间是 10 秒。所以，为了方便操作，可以先右键单击分割线 | > 偏好设置，进入设置窗口，把这项功能关闭先。图标都拖动完毕了，再开启。

全局快捷键请自行设置。这里给出我的快捷键仅供参考：⌃ *command* + ⌃ *option* + *L* 。

那么，这么好用的 App 要怎么安装呢?

1. Mac App Store
2. 下载 `.dmg` 包手动安装：dwarvesf/hidden Releases
3. `brew` 安装方式：

```
$ brew cask install hiddenbar
```

2.2 词汇表

Mac Mac 通常指 Macintosh /'mækintɒʃ/，麦金塔电脑，是自 1984 年 1 月起由苹果公司设计、开发和销售的个人电脑系列产品。

CHAPTER 3

古文精选

文章 明成祖

3.1 明成祖

文皇少長習兵。據幽燕形勝之地。乘建文孱弱。長驅🄵向。奄有四海。即位以後。躬行節儉。水旱朝告夕振。無有壅蔽。知人善任。表裏洞達。雄武之略。同符高祖。六師屢出。漠北塵清。至其季年。威德遐被。四方賓服。明命而入貢者。殆三十國。幅隕之廣。遠迈漢唐。成功駿烈。卓乎盛矣。然而革除之際。倒行逆施。慚德亦曷可掩哉。

皓月摘自明史成祖本紀

夏🄵辛丑年丙申月乙巳日

西🄵二千二十一年八月廿五日

索引