

# A Top-down SSH Config Guidance

---

Boxuan Hu. Feb 23

# 目录

自顶向下的SSH配置指南

- 最基础的登陆方式
- SSH 免密登陆
- SSH on VSCode
- SSH 原理



# 最基础的登陆方式

# 基础说明

1. 我们创建了ics server, 为每个同学分配了账号和初始密码
2. 你需要通过账号+初始密码的方式进行首次登陆
3. 首次登陆需要修改密码(强制)

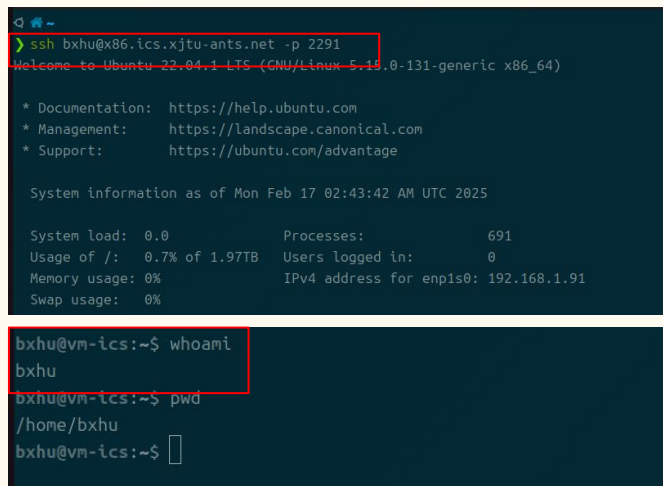
学生账号:你的学号 + ics

初始密码:你的学号

# 如何登陆

1. 确保你在校园网环境下
2. 打开终端(terminal)
3. 在终端中输入以下指令:

**ssh 学生账号@x86.ics.xjtu-ants.net -p 2291**



```
~  
> ssh bxhu@x86.ics.xjtu-ants.net -p 2291  
Welcome to Ubuntu 22.04.1 LTS (GNU/Linux 5.15.0-131-generic x86_64)  
  
* Documentation:  https://help.ubuntu.com  
* Management:    https://landscape.canonical.com  
* Support:        https://ubuntu.com/advantage  
  
System information as of Mon Feb 17 02:43:42 AM UTC 2025  
  
System load:  0.0          Processes:            691  
Usage of /:   0.7% of 1.97TB Users logged in:      0  
Memory usage: 0%          IPv4 address for enp1s0: 192.168.1.91  
Swap usage:   0%  
  
bxhu@vm-ics:~$ whoami  
bxhu  
bxhu@vm-ics:~$ pwd  
/home/bxhu  
bxhu@vm-ics:~$
```

至此，你已完成最基础的登陆配置：)

—

# SSH免密登陆

# 我们的假设是

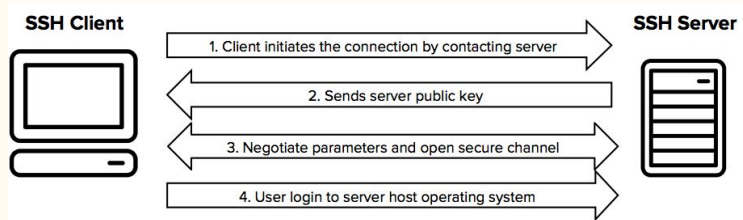
这是一门面向几乎零基础学生的计算机系统课程

我们默认你本身并没有提前准备好SSH相关的配置文件

- ~/.ssh 下的config文件
- id\_rsa (你的私钥)
- id\_rsa.pub (你的公钥)
- known\_hosts 文件

这里我们会一步步教你如何做 :))

- 如果有同学已经提前准备好了, 那么你可以浅浅摸鱼一会
- 配置教程适用于任何远程服务器的SSH连接, 具有普适性



# Step 1: 生成本机密钥

指令:

`ssh-keygen -t rsa`

中间出现的所有选项, 不用管, 回车即可

```
~/.ssh
> ssh-keygen -t rsa
Generating public/private rsa key pair. Private Key 和 Public Key 成对出现
Enter file in which to save the key (/home/bxhu/.ssh/id_rsa):
Enter passphrase (empty for no passphrase):
Enter same passphrase again:
Your identification has been saved in /home/bxhu/.ssh/id_rsa 密钥文件的位置
Your public key has been saved in /home/bxhu/.ssh/id_rsa.pub 公钥文件的位置
The key fingerprint is:
SHA256:zYpiA0CZm7z/M/FDV+OhM/L0TVJja85JzZjL01ShzEk bxhu@bxhu-ThinkBook-16-G4-IAP
The key's randomart image is:
+---[RSA 3072]-----+
| .o                |
|.o                  E . |
|o o                + o .|
| =                o + O .|
| o                S * = B .|
| . . . + B o B + |
| . + = * + X = |
| o = o . . O . |
| ..o . . . |
+----[SHA256]-----+

~/.ssh
> 
```



## Step 2: 将本机公钥添加到服务器上

指令:

```
cat ~/.ssh/id_rsa.pub | ssh bxhu@x86.ics.xjtu-ants.net -p 2291 "mkdir -p ~/.ssh && tee  
-a ~/.ssh/authorized_keys"
```

- cat ~/.ssh/id\_rsa.pub: 输出公钥的内容, 以便后续**通过管道**传递给 SSH 命令
- ssh bxhu@igw.dfshan.net -p 2291: 连接远程服务器
- mkdir -p ~/.ssh: **新建** ~/.ssh 文件夹
- tee -a ~/.ssh/authorized\_keys: 在不覆盖现有内容的情况下将**新内容添加**到文件末尾
  - 没有文件就新建
  - 有文件就尾加

再次输入登陆指令，你就可以惊奇地发现可以“免密登陆”了

```
bxhu@igw.dfshan.net ~$ ssh bxhu@igw.dfshan.net -p 2291
Welcome to Ubuntu 22.04.1 LTS (GNU/Linux 5.15.0-131-generic x86_64)

 * Documentation:  https://help.ubuntu.com
 * Management:    https://landscape.canonical.com
 * Support:       https://ubuntu.com/advantage

System information as of Sat Feb 15 04:37:56 PM UTC 2025

System load:  0.0          Processes:           687
Usage of /:   0.7% of 1.97TB Users logged in:      0
Memory usage: 0%          IPv4 address for enp1s0: 192.168.1.91
Swap usage:   0%

 * Strictly confined Kubernetes makes edge and IoT secure. Learn how MicroK8s
   just raised the bar for easy, resilient and secure K8s cluster deployment.

https://ubuntu.com/engage/secure-kubernetes-at-the-edge

111 updates can be applied immediately.
To see these additional updates run: apt list --upgradable

New release '24.04.1 LTS' available.
Run 'do-release-upgrade' to upgrade to it.

Last login: Sat Feb 15 16:27:34 2025 from 192.168.1.1
To run a command as administrator (user "root"), use "sudo <command>".
See "man sudo_root" for details.

bxhu@vm-ics:~$
```

与我们在上面讲解的一致

```
bxhu@vm-ics:~$ cd ~/.ssh
bxhu@vm-ics:~/.ssh$ ls
authorized_keys
bxhu@vm-ics:~/.ssh$ cat authorized_keys
ssh-rsa AAAAB3NzaC1yc2EAAAADAQABAAQgQC7tn0XBrv+Aik8ljPjCps9MqVcThEBgj4JMnyR259qRPwqiuLw8xpdaQi9huyQMfVd7YL+g5JsXIOvXxarfHLSM8D6RzWJNcaHB4L4s5FP6WHESTPtHudXpTxxMn8PgDwABX7tV2xuPunnAX72nmKfSNUYo46Rg7Y9jj4aWmeeFkeIQy9sJpRe6ukAbpM034990QFrZ767wRBEqtT7
8xUDUdWd7UwFzrQcEnrkjJ2zZPpT2n0pAf/qWUtuWMTmutQkKkARH/1MPufB0M2Utwb9jmuXwC6zkbUfkbR2VRmb1VPpdj1bNxFS9M0uFLRRLHf6FHk2JA2bQZCnz3pZwTQHsx5jNhFea1eaIZUH23VwnNbadIINF5FrLLsnckA7eE7cPFDFuz5kBgRcnzNCJY/23IWBBL/OfCu3qe28cWaIwnEFc8FSPntnf8mviwhn4topRIgPJkm
sX/JFrD7JB5A3nUsw/DymEL2DbAOWNLKfMIq9CM3x1WmrMYDWowlsHB= huluobo@huluobodeMacBook-Pro.local
ssh-rsa AAAAB3NzaC1yc2EAAAADAQABAAQgODGh1p/fHCQnUA5T+kkYsFLRrmIFFmDqK5tgnJ3xhxcB7RW1L8vOhlQs0H4IeKXy6dD039S6SndEcURXTLzbPxGgdJSRQdGXydl/rjSqp1Bc9WzrzNq5jlnIeRYhCpz92fRNWDoGJHgqwKCZDbcyUh2FKbwQvUWwVwxE5bUdNF92D5G8BoIsD/g8f7pHxt65TtE/t9hLZR6w2RwIkaEDW
Z/mHBvPwAAUByjaQBoUkDK+kl/BFFOWXdu7GZWL9TV73HoLUdb7kPlA06GDbDb0uS58CDQ0c1gGzqqm91zhJDE2ae/MAK6A+5cYtSEfpx47lQTl5jof4aNpdheWHNRKSTJqFAePVNVt0kUnlzVxd7wi1PefmEjodnDt3xgmQbWfVTV2TzqNEndMH8ZJCQPzMEDdwVUCmmpFB43JUNBWSanJFZZAY96YqllgeIIwlpznhdhfgC69C5J
sLhHpF3MVB/00yGMZ8DHpc1j7FfI/nvTy88L6vIcnW+H0HqSLmLxCp0= bxhu@bxhu-ThinkBook-16-G4-IAP
bxhu@vm-ics:~/.ssh$
```

## Step 3: 在本机添加配置文件

先前指令格式

`ssh bxhu@igw.dfshan.net -p 2291`

```
1 Host ics-ta  简写名称(自定义)
2   HostName igw.dfshan.net  远程服务器名称
3   Port 2291  远程连接端口
4   User bxhu  用户名(学生学号)
5   IdentityFile ~/.ssh/id_rsa
6   
```

使用这个密钥进行“免密登陆”

```
~/.ssh
> vim config

~/.ssh
> ls
authorized_keys  config  id_rsa  id_rsa.pub  known_hosts

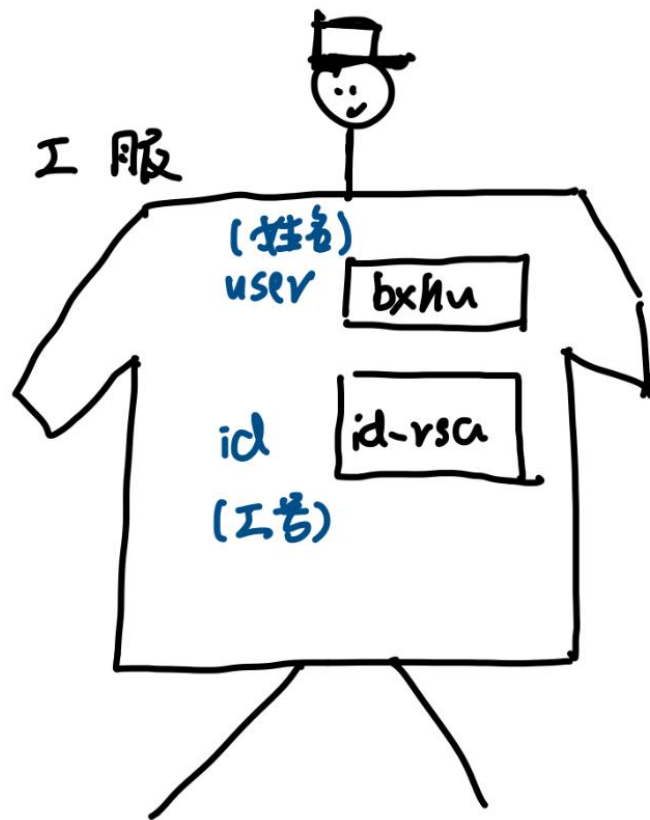
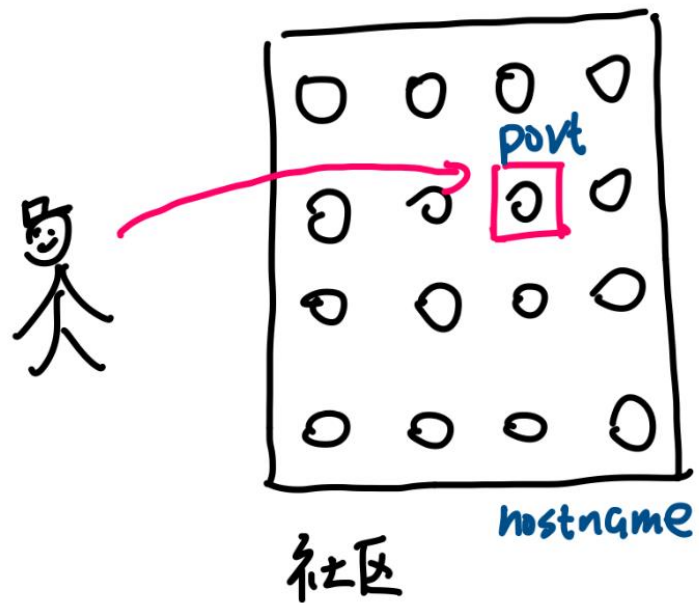
~/.ssh
> chmod +600 config

~/.ssh
> chmod +600 ~/.ssh/id_rsa

~/.ssh
> 
```

`cd ~/.ssh`  
`vim config`  
`..... (config file)`  
`chmod +600 config`  
`chmod +600 ~/.ssh/id_rsa`

你是邮差



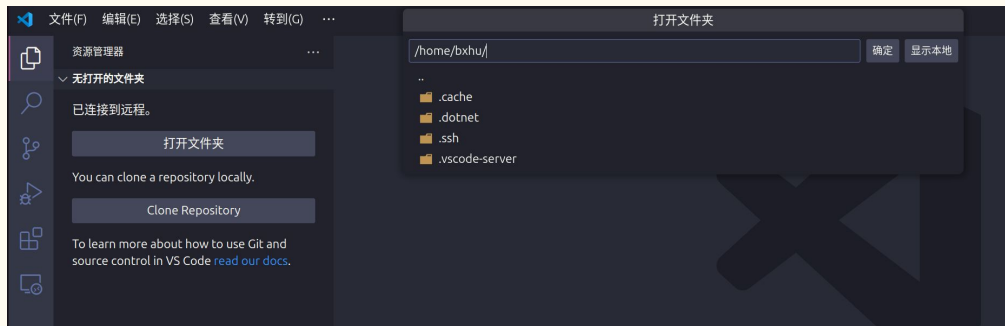
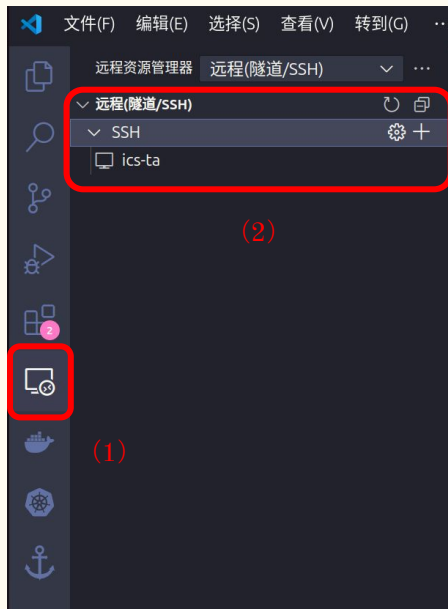
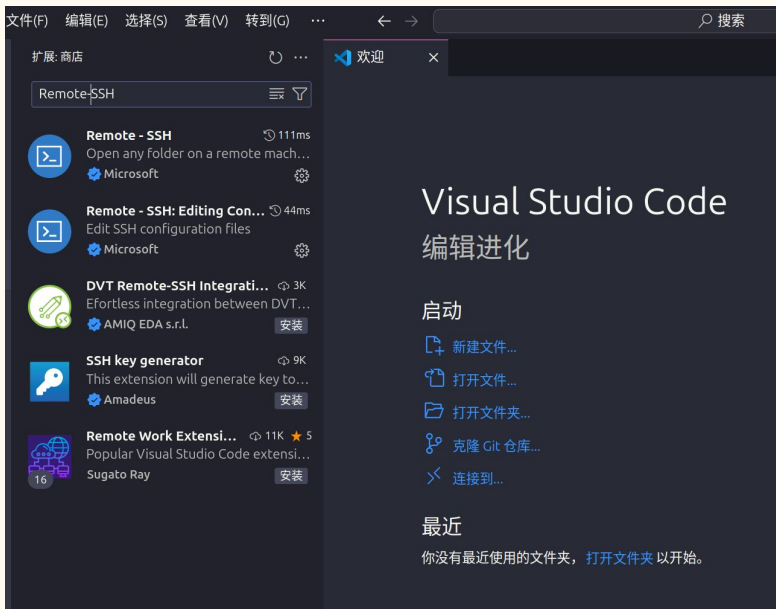
至此，你已完成了CLI中的SSH配置



# SSH on VSCode

插件 > Remote-SSH 点击安装

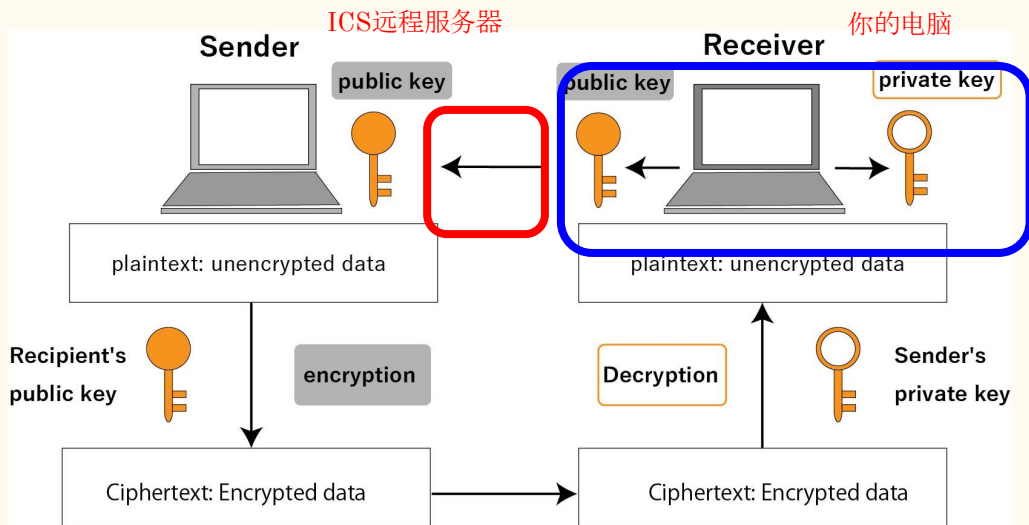
SSH扩展 > 点击ics服务器(ics-ta) > 成功登陆



# SSH 原理



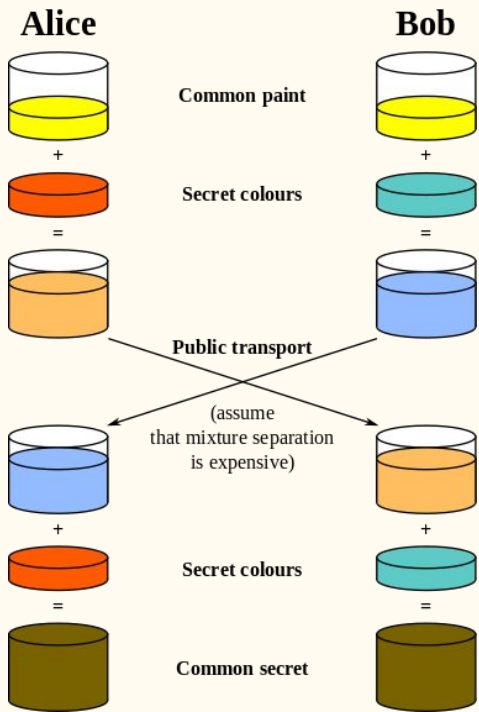
## 回忆: 我们做了哪些...



SSH服务是基于**非对称加密** (public-key cryptography, 也称**公钥加密**) 算法实现数据加密传输的。

非对称加密算法需要两个密 钥:**公钥与私钥, 它们是一对**。如果用公 钥对数据进行加密, 只有用 对应的私钥才能解密。

由于加密和解密使用的是两个不同的密 钥, 所以叫作**非 对称加密算法**。



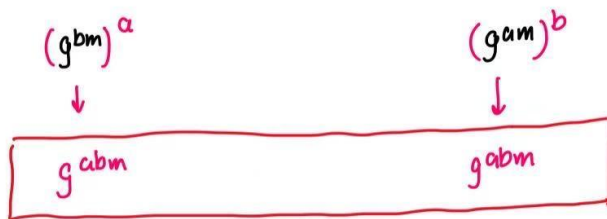
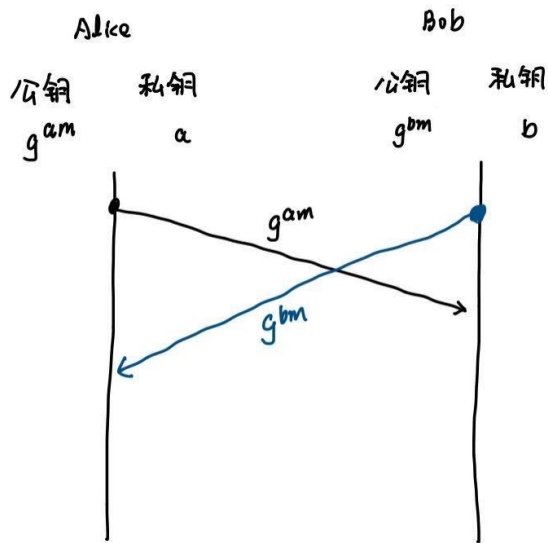
# 直观理解非对称加密的合理性

① key-gen:

② swap pubkey

③ “真”解密

钥匙相同.



# 致谢

SSH配置指南参考了以下来源:

1. [XJTU-ICS Textbook Chapter 4.5](#)
2. [ICS Spring 2024 SSH Tutorial](#)