底层原理

SSH 之所以能够保证安全，原因在于它采用了公钥加密。

整个过程是这样的：

1. 远程主机收到用户的登录请求，把自己的公钥发给用户；
2. 用户使用这个公钥，将登录密码加密后，发送回来；
3. 远程主机用自己的私钥，解密登录密码，如果密码正确，就同意用户登录。