目录

[一 https原理 1](#_Toc30861)

[1 非对称加密 1](#_Toc20095)

[2 对称加密 1](#_Toc7532)

[3 https原理图解 2](#_Toc8009)

[二 nginx配置https证书的准备 2](#_Toc27377)

[1 安装证书确认项目 2](#_Toc31916)

[2生成密钥和CA证书 3](#_Toc28694)

[2.1 生成key密钥 3](#_Toc18424)

[2.2 生成证书签名请求文件（csr文件），发送给ca进行签名 3](#_Toc26144)

[2.3 生成证书签名文件（ca文件）（自签名过程） 4](#_Toc9652)

[3 苹果要求的证书文件 4](#_Toc13956)

[三 nginx实际https证书配置项及优化 5](#_Toc31836)

[1 Nginx --https设置 5](#_Toc19754)

[2 https优化 5](#_Toc4656)

# 一 https原理

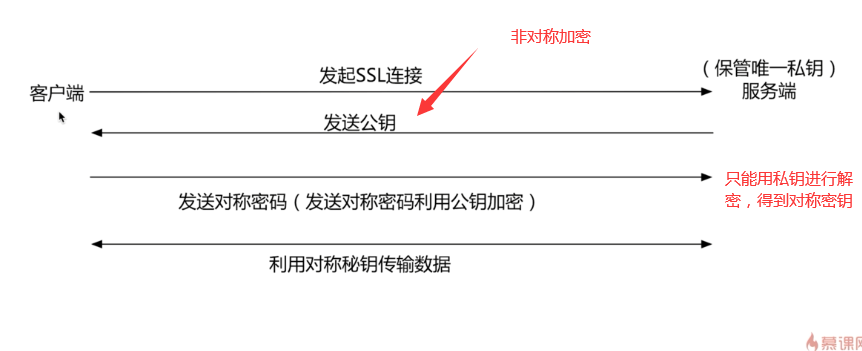
1 非对称加密

加密方和解密方的密钥不一致（公钥用于加密，私钥用于解密）

## 2 对称加密

加密方和解密方的密钥一致

## 3 https原理图解



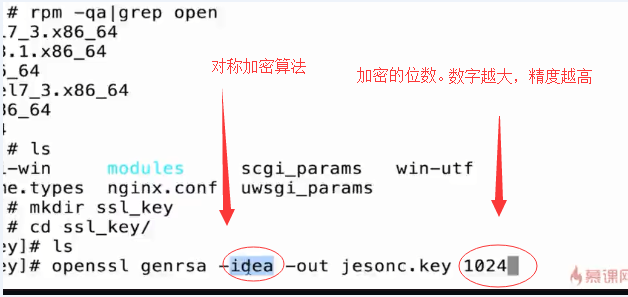
# 二 nginx配置https证书的准备

## 1 安装证书确认项目

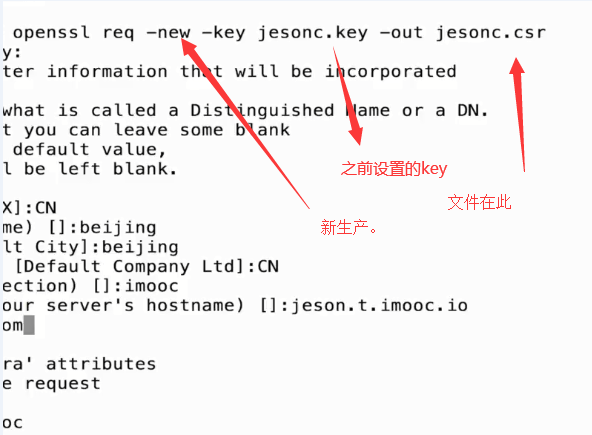


## 2生成密钥和CA证书

### 2.1 生成key密钥



### 2.2 生成证书签名请求文件（csr文件），发送给ca进行签名



### 2.3 生成证书签名文件（ca文件）（自签名过程）

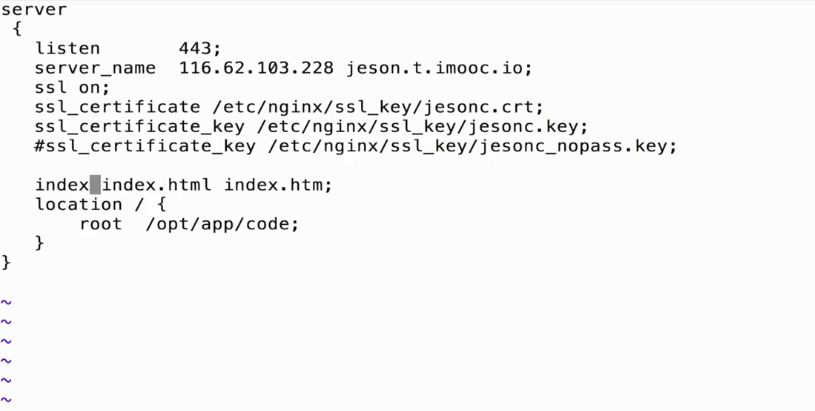


## 3 苹果要求的证书文件



# 三 nginx实际https证书配置项及优化

## 1 Nginx --https设置



## 2 https优化

