文件总结

- .certSigningRequest文件
  - Mac公钥
- .cer文件
  - 利用Apple私钥（CA），对Mac公钥生成了数字签名
- .mobileprovision
  - 利用Apple私钥，对【.cer证书+devices+AppID+entitlements】进行数字签名

知识点总结

加密解密算法

- 对称密码
  - 加密解密用的是同一个密钥
  - 加密解密速度快
  - 无法解决密钥配送问题
- 公钥密码
  - 加密解密用是不同的密钥
  - 公钥加密，私钥解密
  - 私钥加密，公钥解密
  - 加密解密速度慢
  - 解决密钥配送问题

单向散列函数

- 根据消息生成对应的固定长度的散列值
- 防止数据被篡改

数字签名

- 用私钥加密消息的散列值，生成的密文

证书

- 用CA的私钥，对其他人的公钥生成数字签名