双向签名签名原理&重签名

- 什么是数据签名(代码签名)
  - 1.计算出需要校验的数据HASH值
  - 2.将校验HASH值进行RSA加密
  - 3.这部分利用RSA加密过后的HASH值,我们称之为"数字签名"
  - 提示:被校验的数据如果是代码,我们就称为"代码签名"
- iOS 双向签名验证
  - 1.Mac电脑通过CSR文件(本地公钥)向App Store申请证书(证书包含在描述文件)
  - 2.Mac电脑拿到证书会将本地私钥(P12)进行绑定
  - 3.安装APP时,利用本地私钥(P12)对APP 进行签名.并且将描述文件\APP签名\证书一并打包APP
  - 4.iOS系统两次签名验证
    - 4.1 iOS系统利用内置公钥验证证书
    - 4.2 取出证书中的公钥 验证APP签名
  - 概念:
    - 证书:内容是公钥或者私钥.由机构对它进行签名组成的数据包!
    - P12:就是本地私钥.可以导入到其他电脑
    - Entitlements:包含了APP的权限列表
    - CSR:本地公钥
    - 描述文件:包含了证书\Entitlements等数据.有苹果后台私钥签名的数据包!
- 利用Xcode进行重签名
  - 1.需要查看APP可执行文件(MachO文件)的加密信息.
  - 2.删除插件,因为无法重签名
  - 3.利用Xcode新建同名工程
  - 4.修改Info.plist 文件.将BundleID改了
  - 5.利用codesign重签Frameworks
  - 6.给可执行文件上可执行权限
  - 7.将需要重签名的APP包替换新工程的APP包.运行!!