作业与实践

- **作业**

1. 在腾讯会议系统中，对称密码技术和公钥密码技术适合应用在哪几个阶段？说明理由。
2. 假设计算能力遵循摩尔定律，分析三重DES目前在计算上是否安全。
3. 简述散列函数MD5的碰撞问题。既然MD5存在碰撞问题，为何http://mirrors.ustc.edu.cn/ubuntu-releases/16.04/仍然给出MD5值作为完整性验证的依据。
4. 简述用RSA公钥算法实现数字签名的过程。

- 实践(不考核，自己练习)

1. 熟悉OpenSSL命令行程序的使用。
2. 用Python语言实现AES对二进制文件的加/解密。
3. 修改例程cryptoDemo.cpp为encfile.cpp：从命令行接受3个字符串类型的参数：参数1，参数2，参数3。参数1=enc表示加密，参数1=dec表示解密；参数2为待加密、解密的文件名；参数3为密码。
4. 熟悉Gpg4win的使用。