第2章 作业

- 作业
  1. 一个密码系统包括哪些要素？
  2. RSA算法的理论基础是什么？简述RSA算法的流程。
  3. 数字签名和消息鉴别的主要区别是什么？
  4. 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的。

- 实践（自己研究，不考核）
  - 熟悉Windows的Crypto API系统架构，阅读例子程序

    https://docs.microsoft.com/en-us/windows/win32/seccertenroll/understanding-cryptographic-providers
  - 试用Python语言实现AES对二进制文件的加/解密。