《密码学》课程习题

执笔 张焕国

第九章习题

1、 阐述密钥管理的原则，并说明为什么需要这些原则？

2、 阐述传统密码体制的密钥组织的合理性，能否在这一组织结构中加入或删掉一个层次的密钥？

3、 阐述密钥产生的主要方法。

4、 请举出3种电子真随机源的实例。

5、 软件实现基于AES的ANSI X9.17算法。

6、 对于图9-6的初级密钥的网络分配方案中，如果敌手能够截获RN和发送RN，对该方案会构成威胁吗？为什么？

7、 软件实现图9-6初级密钥的网络分配方案。

8、 对Diffie-Hellman密钥分配方案实施中间人攻击，并说明应如何阻止这种攻击。

9、 证明，高级密钥只能以明文形式存储。

10、 阐述密钥更新的原则。

11、 编写一个能够安全删除磁盘数据的程序。

12、 在图9-8（a）中增加一个新的安全类SC_7，使SC_7是SC_2的直接后继。**KMC**要作哪些工作？

13、 从图9-9（a）中删除安全类SC_2。**KMC**需要作哪些工作？

14、 公钥密码体制的公开密钥存在哪些安全威胁？如何对付这些安全威

胁？

15、 什么是 PKI？它对公钥密码体制的密钥管理有何作用？

16、 讲述一个自己实际应用 PKI 的实例。

17、 分析 PKI 的优缺点。

18、 阐述 CPK 的原理，并分析 CPK 的优缺点。