试题 1 论一卡通系统中的智能卡的安全

2008 年德国研究员 Henry Plotz 成功破解了 NXP 的 Mifare 经典芯片（非接触智能卡，即平常所说的 M1 卡）的安全算法。为此，工信部发布了《关于做好应对部分 IC 卡出现严重安全漏洞工作的通知》，要求各地各机关和部门开展对 IC 卡使用情况的调查和应对工作。在我国，公交等众多部门一卡通系统采用的卡片都是 M1 卡。因此，如何应对是今后网络规划师和系统分析人员工作的重点。

请围绕“一卡通系统中的智能卡的安全”论题，依次从依下三个方面进行论述。

1、 要叙述你参与分析和设计的一卡通系统以及你所担任的主要工作。

2、 深入讨论针对智能卡的缺陷可能带来的安全问题。

3、 详细论述你采用的应对方案或者解决办法，并且分析和评价你的解决方案。

试题 1 解答要点

（1）首先用 400-500 字的篇幅简要叙述作者参与分析和设计的一卡通系统的概要介绍和所担任的工作。

（2）具体叙述你在系统设计中应对措施。

可以参考的措施有以下几点：

1. 升级为 GPU 卡，但是成本过高，一张 GPU 卡比 M1 卡贵 6~8 块。
2. 对小额面值的卡进行破解，成本过高，对破解人员要求比较高。
3. 加强管理机制，对一些系统尤其是校园一卡通系统进行小额消费限制，使得破解者无法快速获利。
4. 按照国际惯例，一旦卡片被复制进行了消费，应当由发卡方提供赔偿。
5. 联动的门禁系统，采用别的技术进行复合认证例如指纹技术。
6. 关键数据加校验码。如果关键数据被修改，卡将被拒绝使用。
7. 通过日常消费发现异常卡。
8. 采用一卡一密

（3）文章应该结合所举的一卡通系统项目的实际情况，指明在该系统中要解决的安全问题，并详细地论述所采取措施的重要性、合理性，并综合评价之。

（4）应对所选的技术与措施的效果进行分析，并力求实事求是，毕竟每一种都会有一定的适用范围和局限性。