课程设计

调研题目

1. 2017年2月19日,google发布SHA-1的碰撞,调研SHA-1在目前计算机系统及网络的应用情况，面对这一威胁，各系统如何应对？
2. 剖析office，window等你所熟悉的应用系统中的加密方案，分析其安全性？

实践题目

3 调研该论文及相关资料，描述攻击原理、步骤，并尝试模拟该攻击。

Key Reinstallation Attacks

--Breaking WPA2 by forcing nonce reuse

Discovered by Nathy Vanhoef of inec-DistriNet, KU Leuven

课程设计

- 任选上述题目中一个，自由组队完成，第十四周末确定组队名单，请学委将名单发送给我。
- 考核方式：

1）每队准备PPT课堂展示（十五或十六周），并展示模拟结果；

2）每队撰写报告（含组员任务分工，调研分析等内容，实践题目还包含程序设计、测试报告，源程序），期末考试前一同提交。