综合实验

一、实验目的

针对一学期理论课和实验课所学知识，为了提高同学们综合运用密码算法的能力，熟悉常用密码算法在现实中的应用场景。

通过设计综合程序的结构，增强程序的实用性和可扩展性，提高编程能力。

二、实验内容

从下面一类题目中任选一题：

1. SM2 快速实现
2. SM4 分组密码算法的软件优化实现
3. ZUC 算法的快速优化实现
4. 基于 sm2/3/4 的安全文件共享系统
5. 个人数据加密
6. 物联网轻量级密码算法研究
7. 基于优化 ZUC 算法的加解密软件应用设计

或从下面题目中任选一题：

1. 公开信道安全通信的加密方案设计与安全性分析

要求：

初始会话时，需要进行密钥协商，生成会话密钥；

会话时，需要考虑通信时延，因此需要选择高效的加解密算法；

会话中断时，需要合理的中断流程；

再次会话时，考虑需要是否重新进行密钥协商；

会话密钥的使用时间周期需要考虑；

重新生成密钥的过程需要给出。

至于通信信道的选择：

通信的方式不考察，因此可以选择任意方式，比如 UDP、进程间通信等等。

安全性分析：

是否可以抵抗重放攻击；

是否可以抵抗中间人攻击；

是否还有其它安全性问题……

2. 软件版权许可证在线认证与离线认证方案设计与安全性分析

要求：

授权的序列号如何生成（永久性和非永久性）；

永久授权软件与非永久授权软件的认证过程（在线与离线）；

如何保证序列号只能被一个合法用户使用（在线与离线），比如在 PC 上可以通过一些特定的标识来表示，如 MAC 地址、CPU ID 等；

在线认证可以通过远程访问数据库的方式，或是用访问特定文件的方式模拟，获取认证状态。

离线认证需要通过序列号在本地实现认证。

安全性分析：

不考虑可以绕过认证机制（脱壳）时，给出在线认证和离线认证的安全性分析；

3. 一种简单的可搜索加密系统设计

要求：

对文件或文章进行加密，然后可以在密文上做搜索功能，可搜索加密的一般过程如下。

Step 1. 加密过程.用户使用密钥在本地对明文文件进行加密,并将其上传至服务器.

Step 2. 陷门生成过程.具备检索能力的用户,使用密钥生成待查询关键词的陷门,要求陷门不能泄露关键词的任何信息.

Step 3. 检索过程.服务器以关键词陷门为输入,执行检索算法,返回所有包含该陷门对应关键词的密文文件,要求服务器除了能知道密文文件是否包含某个特定关键词的陷门外,无法获得更多信息.

Step 4. 解密过程.用户使用密钥解密服务器返回的密文文件,获得查询结果.

用户的公私钥由用户本地生成，公钥发送给服务器；

服务器需判断当前申请查询的用户是否具有检索文件的权限，然后返回相应的查询结果；

用户端程序和服务器端程序间的通信可以使用任意方式，比如 TCP、UDP、进程间通信等等。

参考文献：

[1] 李经纬, 贾春福, 刘哲理, et al. 可搜索加密技术研究综述[J]. 软件学报, 2015, 26(1):109-128.

[2] 沈志荣, 薛巍, 舒继武. 可搜索加密机制研究与进展[J]. 软件学报, 2014, 25(4):880-895.

或自选题目（需满足实验目的）

或进一步优化实验六（软件快速实现）

三、实验要求

1. 每一个算法的实现独立为一个代码文件，同实验报告一起打包提交，压缩文件命名格式为： 学号_ 姓名_ 综合实验.rar，如：17061001_***_综合实验.rar。

2. 代码应有必要的注释。实验报告应至少含有算法原理、算法流程、测试样例及运行结果，以及心得体会或感想建议。

3. 请在 7 月 1 日中午 12 点前完成实验，将源码及实验报告打包发送到指定邮箱 buaa_2019@163.com。

4. 本学期所有未交和想要修改的实验报告和代码请务必确保在 7 月 1 日中午 12 点前提交，逾期不候！