密码学课程设计任务书

|  |
| --- |
| 课题内容：  （1）原始SPN（教材上）算法的实现。  （2）对上述算法进行线性密码分析及差分密码分析（求出所有32比特密钥）。  （3）增强以上SPN的安全性（如增加分组的长度、密钥的长度、S盒、轮数等）。  （4）对原始及增强的SPN进行随机性检测，对检测结果进行说明。  （5）生成RSA算法的参数（如p、q、N、私钥、公钥等）。  （6）快速实现RSA（对比模重复平方、蒙哥马利算法和中国剩余定理）。  （7）利用椭圆曲线密码算法、HASH函数、压缩函数、对称加密算法实现一个类似PGP的文件加解密及完整性校验功能。  （8）利用USBKEY和数字证书实现简单的文件加密保护。  （9）构造彩虹表破解HASH函数。 |
| 课题任务要求：   1. 掌握线性、差分分析的基本原理与方法。 2. 体会位运算、预计算在算法快速实现中的作用。 3. 可借助OpenSSL、GMP、BIGINT、FLINT等大数运算库的低层基本函数（加、减、乘、除、模），实现过程中必须体现模重复平方、中国剩余定理和蒙哥马利算法的过程。内容(7)的算法可以直接调用OpenSSL或者其它密码库。 4. 了解和掌握彩虹表构造的基本原理和方法，能够设计和实现约化函数（Reduction Function），针对特定的HASH函数构造彩虹表，进行口令破解，了解彩虹表的弱点及防范方法。 5. 独立完成课程设计内容，现场演示并讲解。 6. 掌握USBKEY和证书的基本使用方法。 7. 课程设计完成后一周内，提交课程设计报告。 |
| 主要参考文献（由指导教师选定）   1. 密码学原理与实践（第三版）. DouglasR.Stinson著，冯登国译，电子工业出版社，2009 2. 应用密码学：协议算法与C源程序（第二版）. Bruce Schneier 著，吴世忠等译，机械工业出版社，2014 |
| 同组设计者 无 |