密码学课程设计任务书

题目:

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）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 等大数运算库的低层基本函数，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。
（5） 独立完成课程设计内容，现场演示并讲解。
（6） 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