

**课 程 设 计 报 告**

**题目： 密码学课程设计**

**课程名称： 密码学课程设计**

**专业班级： 网安2002班**

**学 号： U202012043**

**姓 名： 范启航**

**指导教师：**

**报告日期：**

**教师评语：**

**分数：**

**网络空间安全学院**

目录

[一、设计过程 1](#_Toc27998)

[1.1 SPN实现（每一个题目不要超过一面） 1](#_Toc18507)

[1.2线性分析 2](#_Toc13401)

[1.3差分分析 3](#_Toc26212)

[1.4 SPN加强 4](#_Toc26513)

[二、实验心得 5](#_Toc28748)

[三、对课程设计内容和过程的建议 5](#_Toc31425)

## 一、设计过程

### 1.1 SPN实现（每一个题目不要超过一面）

（1）设计内容

SPN(代换-置换网络)是一个典型的迭代密码，这种密码明确定义了一个轮函数和一个秘钥编排方案，一个明文的加密将经过Nr轮相似的过程。

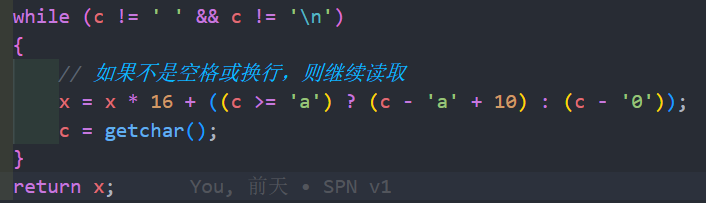
本题中将使用32位秘钥与16位明文，经过SPN加密得到16 位密文，并对密文做修改后，经过SPN解密得到16位明文。

本题中的秘钥为32位，轮秘钥为16位，共有5个，由秘钥生成，S盒为4位，P盒为16位。加密过程中，明文先通过3轮白化-S盒代换-P盒置换。最后一轮先白化后进行S盒代换，将结果与最后一个轮秘钥异或后得到结果。

（2）设计过程

SPN加解密的具体实现包括以下几个部分：1. 数据的读入输出2. 轮秘钥的生成 3. 白化 4. S盒代换 5. P盒置换 6. SPN主程序

1. 数据的读入输出：由于scanf,printf效率较低，故对循环getchar()进行封装实现对十六进制数字的快速读入



1. 轮秘钥生成采用移位与异或的方法，第一轮秘钥为0-16位，第二轮秘钥为4-20位，以此类推，第五轮秘钥为16-32位。
2. 白化采用异或操作，并对其进行封装。
3. S盒置换使用循环的方法，将明文或密文分为4组，分别对每一组进行代换后再将其使用或运算结合。
4. P盒置换使用循环的方法，i从1到16，先将第i位移动到最后一位再将其移动到P盒中指定的位置。速度较慢，优化方法：因数据量较小，采用打表输出。



1. SPN主程序，按照SPN流程，接收参数秘钥，明文或密文，加密或解密标志，依次调用以上函数实现SPN加解密。

（3）小结

运行结果，速度较快，最后一题为600ms左右，不足之处在于为保证速度，代码中存在冗余且不宜理解的地方。

### 1.2线性分析

1. 设计内容

线性密码分析的思想，原则上该思想可以被应用于任何迭代密码。假使能够在一个明文比特子集与最后一轮即将进行代换的输入状态比特子集之间找到一个线性关系，即存在一个比特子集使得其中元素的异或表现出非随机的分布（比如，该异或值以偏离1/2的概率取0）。

1. 设计过程

线性分析的具体实现包括以下几个部分：1. 对S盒分析，手动寻找两条线性逼近链。 2.读入大量明密文对。3. 分别对两条链进行线性分析，得到两个子秘钥。4. 穷举前16位秘钥与子秘钥组合进行测试，得出最终秘钥。

1. S盒分析，可采用手动或编程方法测试，选取一条链关联两个子秘钥，另一条链关联3个或4个子秘钥。

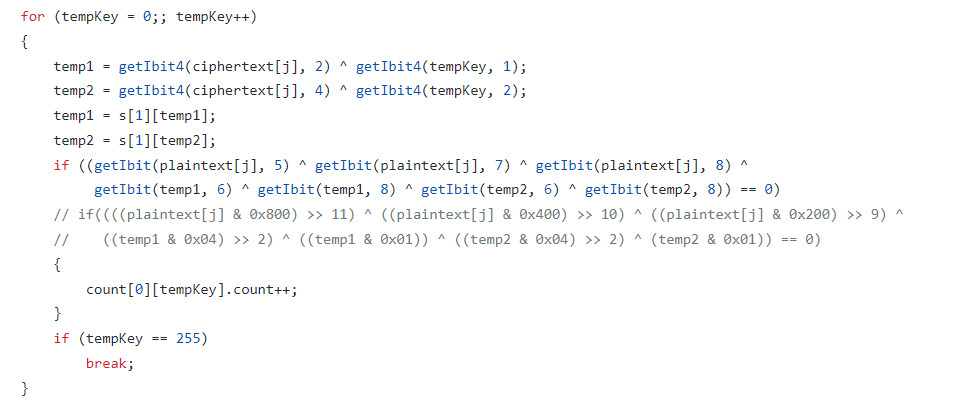


第一条链

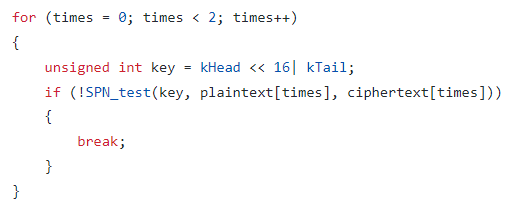


第二条链

1. 使用实验一中的快速读入大量明密文对。
2. 对链1进行线性分析，统计子秘钥对应的偏差并排序。对链2进行线性分析，统计子秘钥对应的偏差并排序。



1. 穷举前16位秘钥，依次取偏差率较大的子秘钥，组合成完整的秘钥，从明密文对中选取若干明密文进行测试，若均正确则选出正确的秘钥。



1. 小结

因本次实验数据量较大，需要反复对候选秘钥进行测试，因此效率较低，经过对输入输出、循环、编译等优化后可达到900ms通过。此外本题效率依赖线性链的选择，链1的偏差较小，误差较大。

### 1.3差分分析

1. 设计内容

差分密码分析与线性密码分析较为相似，主要差别在于差分密码分析包含了将两个输入的异或与其对应的两个输出的异或相比较。通过对S盒的输入异或，输出异或进行分析，发现对于特定的S盒，若输入值的异或一定，则输出值的异或分布偏向某一特定值，称为异或扩散率。对任何一轮的差分进行分析，得到一个差分链。通过对最后一轮的差分进行分析，即可找出最后一轮的秘钥。

1. 设计过程

差分分析的具体实现包括以下几个部分：1. 对S盒分析，手动寻找两条差分链。 2.读入大量明密文对。3. 分别对两条链进行差分分析，得到两个子秘钥。4. 穷举前16位秘钥与子秘钥组合进行测试，得出最终秘钥。

1. S盒分析，可采用手动或编程方法测试，选取两条链均关联两个子秘钥。



第一条链



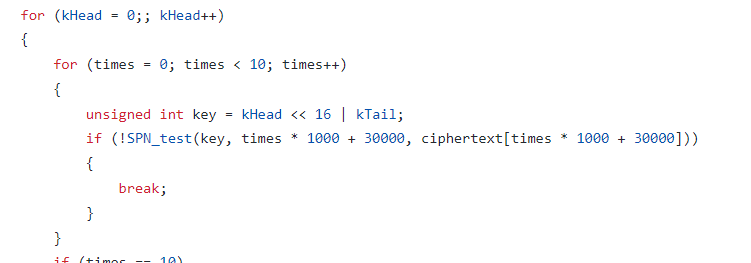
第二条链

1. 使用实验一中的快速读入大量明密文对。
2. 对链1进行线性分析，统计子秘钥对应的差分并排序。对链2进行线性分析，统计子秘钥对应的差分并排序。因差分攻击的效率较高，可知选取50-100个明密文对的值，此外可以丢弃不满足对应比特不相同的明密文组，过滤随机噪声，提高差分攻击效率。



过滤噪声

1. 穷举前16位秘钥，依次取偏差率较大的子秘钥，组合成完整的秘钥，从明密文对中随机选取若干明密文进行测试，若均正确则选出正确的秘钥。



结果验证

（3）小结

本次实验中，因差分攻击效率较高，因此采取了一些措施，如过滤噪声，减少取样数，增加检验数的方法来提高速率，实现了对秘钥的快速破解。此外，可以相对线性分析，差分分析可以选取两个独立的子秘钥链进行分析，效率相对更高。

### 1.4 SPN增强

（1）设计内容

对实验一中的SPN加解密进行优化，1.对秘钥长度，分组长度，S盒、P盒和轮数进行优化。2、 对轮秘钥生成算法进行优化。3、 使用分组密码加密模式对大量明文进行加密。

1. 提高效率。 5、 输出达到随机数检测标准。

本实验中 128 为秘钥， 64位为一个分组，明密文长度均为64位，使用16位S盒和64位P盒。轮数为4轮。为提高密文的随机性，采用了CBC模式，设定一个较大的初始向量，向量与明文进行异或后进行加密，加密结果作为下一个分组的向量。轮秘钥采用多次移位的方式产生。

（2）设计过程

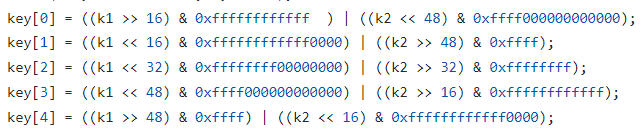
SPN增强加解密的具体实现包括以下几个部分：1. 数据的读入输出2. 轮秘钥的生成3. 分组密码模式 4. 白化 5. S盒代换 6. P盒置换 7. SPN主程序

1. 数据的读入输出：因为明密文的长度较长，使用scanf, printf的时间损耗较大，故使用fread、fwrtie来实现大量数据的读入，秘钥长度为128位，而C中unsigned long long最长为64位，使用两个unsigned long long 类型来存储初始秘钥。

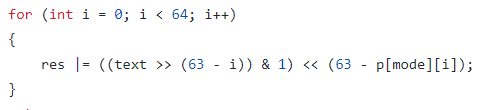




1. 轮秘钥的生成：使用多次移位来生成5个轮秘钥，如下图：



1. 分组密码模式：使用密码分组链接模式(CBC)，将每个明文组与前一个密文异或后再进行加密，初始向量为6420946196872948572。
2. 白化：同原SPN，将其扩展到64位。
3. S盒代换：同原SPN，将其扩展到64位。
4. P盒代换：同原SPN，将其扩展到64位。



1. SPN主程序：同原SPN，将调用函数改为对应64位操作。
2. 小结

本实验中为了能达到随机数检测标准作了一下优化，将秘钥长度增大到128位，同时轮秘钥的生成方式更加复杂，提高混乱性。采用CBC模式，将明文与上一轮加密的密文进行异或后加密，同时使用一个随机生成的大数作为初始向量，提高混乱性。

（1）设计内容

（2）设计过程

（3）小结

（1）设计内容

（2）设计过程

（3）小结

（1）设计内容

（2）设计过程

（3）小结

（1）设计内容

（2）设计过程

（3）小结

（1）设计内容

（2）设计过程

（3）小结

（1）设计内容

（2）设计过程

（3）小结

（1）设计内容

（2）设计过程

（3）小结

## 二、实验心得

## 三、对课程设计内容和过程的建议