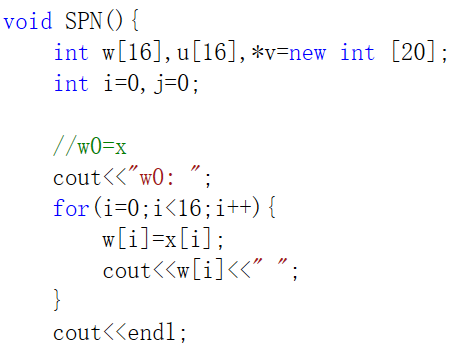
密码学基础实验报告实验一

王天行 2011428

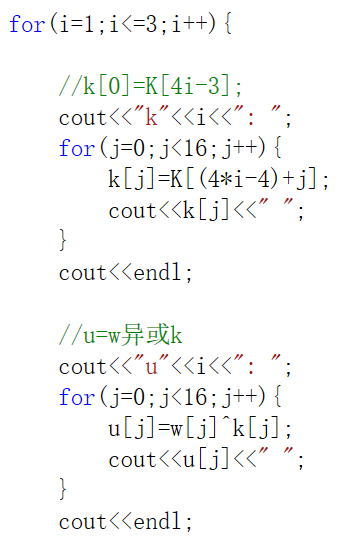
1. 实现SPN加解密算法
   1. 题目要求

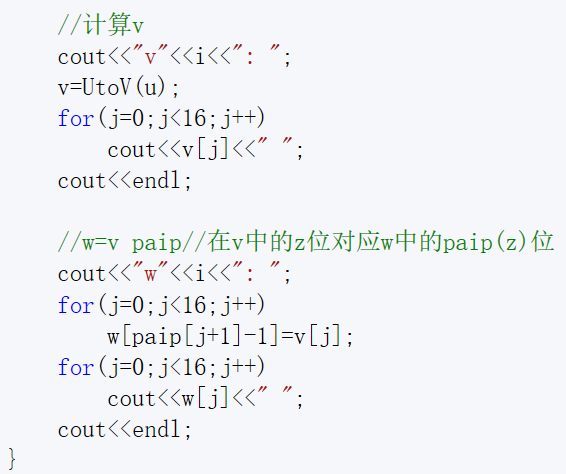
根据书上伪代码，复现SPN加密算法

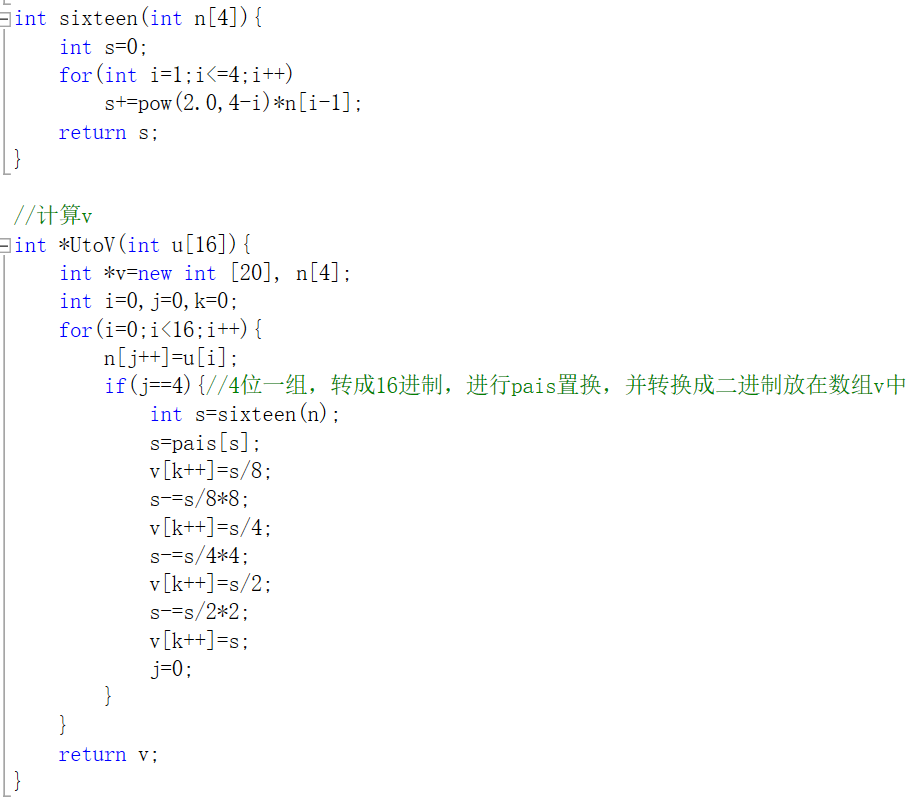
* 1. 主要代码（加密）
     1. 求w0



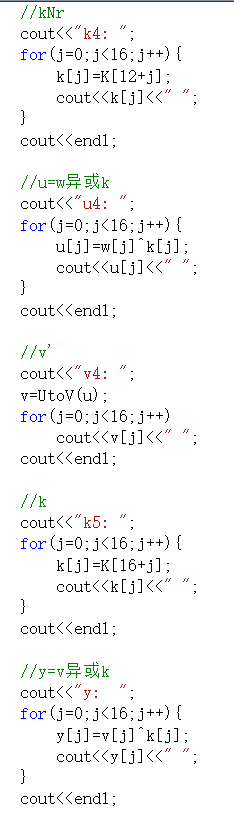
* + 1. 循环



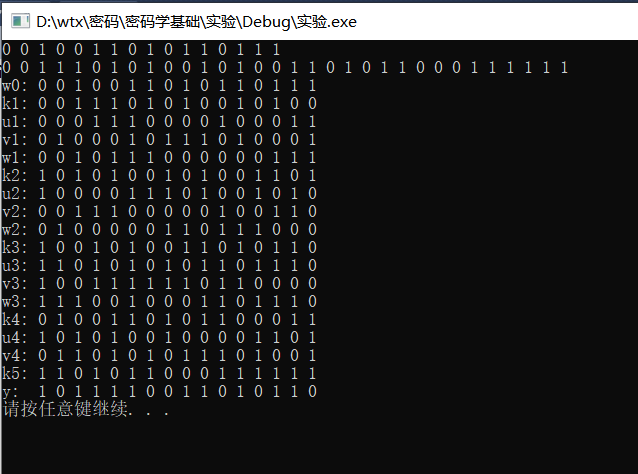


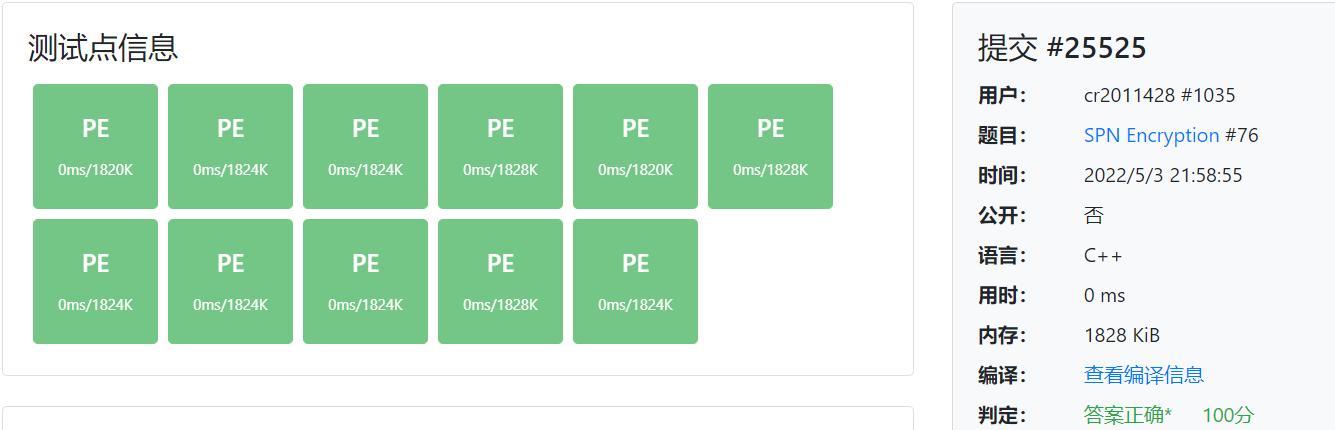


* + 1. 输出y



* 1. 输出结果



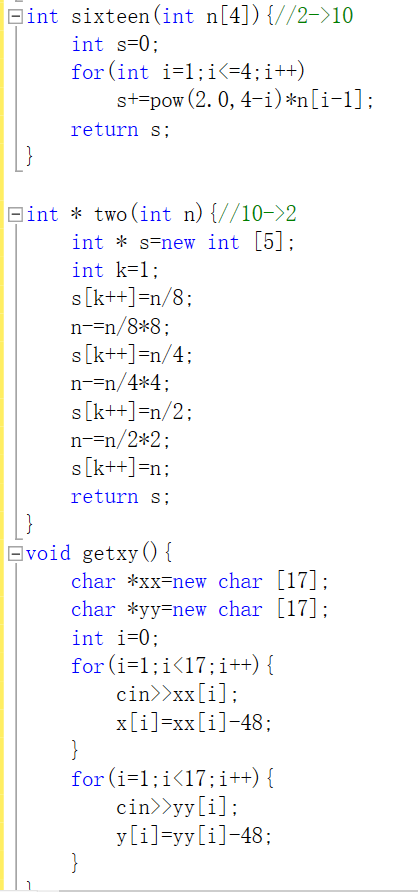
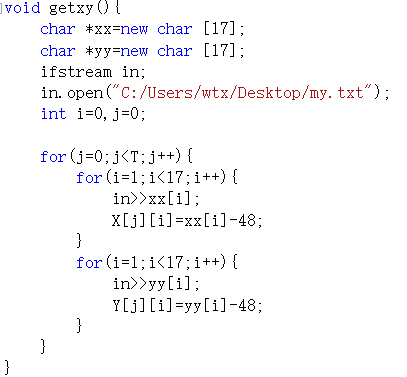


* 1. 实验思考
     1. 按部就班编写的代码，没有使用进行简化，性能一般，占用空间没有进行优化
     2. 代码在提交到oj平台时进行了小的修改，包括用char型数组输入，转为int型；规范输出格式。
     3. 对于spn解密算法，将每轮顺序逆转，对于置换的解密算法可以写一个逆的对应的数组，替换加密算法中的代换数组，对于异或的解密算法即为再次与密钥异或。

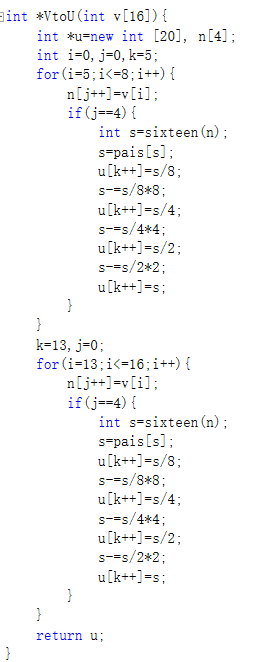
1. 线性攻击算法
   1. 题目要求

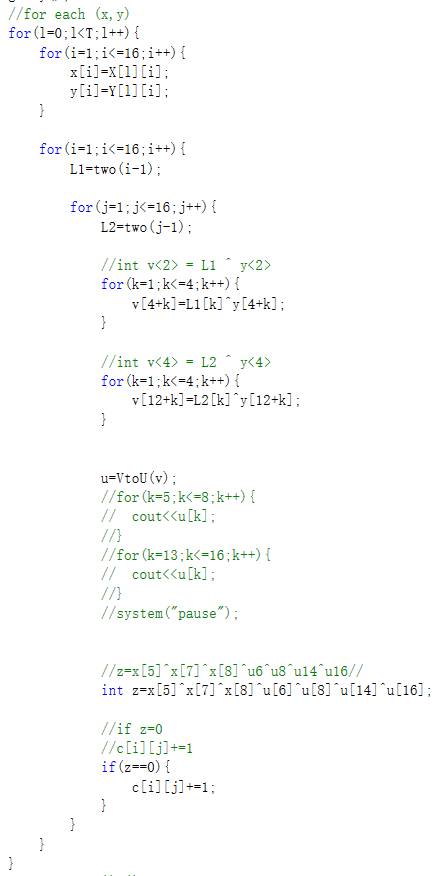
根据书上所给的伪代码，复现第五轮密钥

* 1. 主要代码：复现书上所给的伪代码，实现线性分析攻击K<2>和K<4>
     1. 通过加密算法获取10000个明密文对，保存在txt文档中
     2. 一些所用到的函数：二进制与十进制的转换；从txt文档中获取明密文对

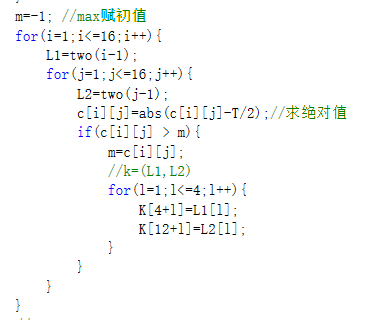


* + 1. 对于每一个明密文对进行分析

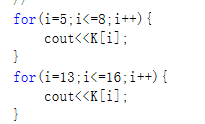




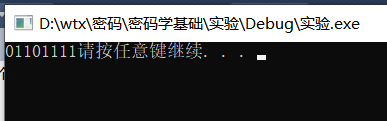
* + 1. 选取概率最大的一个密钥



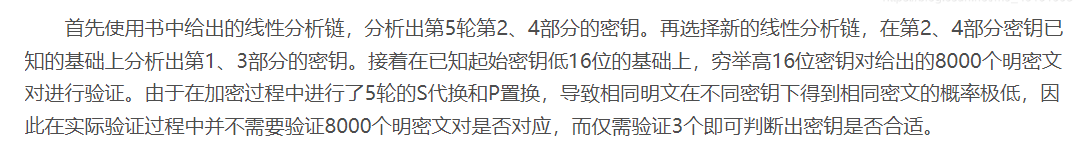
* + 1. 输出密钥



* 1. 输出结果



* 1. 实验思考
     1. 在书上代码复现后，上网查找别人的代码思路，在查阅时发现书上给的伪代码是攻击第五轮密钥的一部分，而要实现完整密钥，需要攻击出第五轮密钥的另一部分，即密钥的低16位，和密钥的高16位。由于时间原因，在此我没有进行第五轮第一部分和第三部分的攻击，个人想法是通过暴力搜索破解。



所以该攻击方法主要是通过分析，攻击出部分代码，然后缩小了穷尽的范围，减少了时间。

* + 1. 我的代码的破解速度在6秒左右，跟毫秒级别比还是有所差距的，而且我并没有攻击出全部的密钥。主要原因可能在于在求异或时，我是将L1和L2转换为二进制，与密文进行异或，应该是比将密钥转化为整型直接和i、j异或要慢。同时在攻击函数中引用更多的函数，多层函数嵌套，函数调用需要时间。