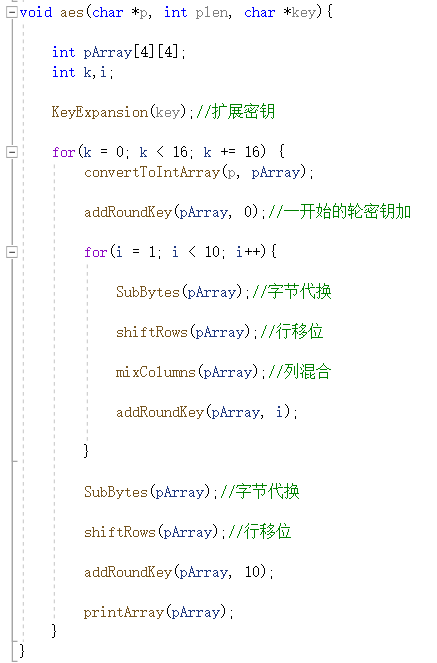
密码学基础实验报告实验二

姓名：王天行 学号：2011428

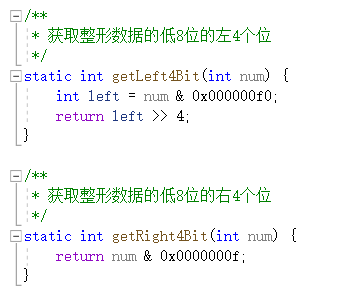
1. AES-128的一个分组的加密算法
2. 题目要求

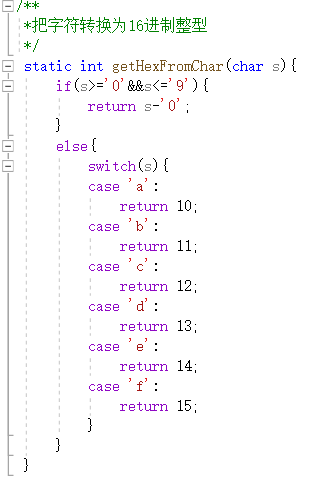
给定十六进制的明文和密钥，求出密文

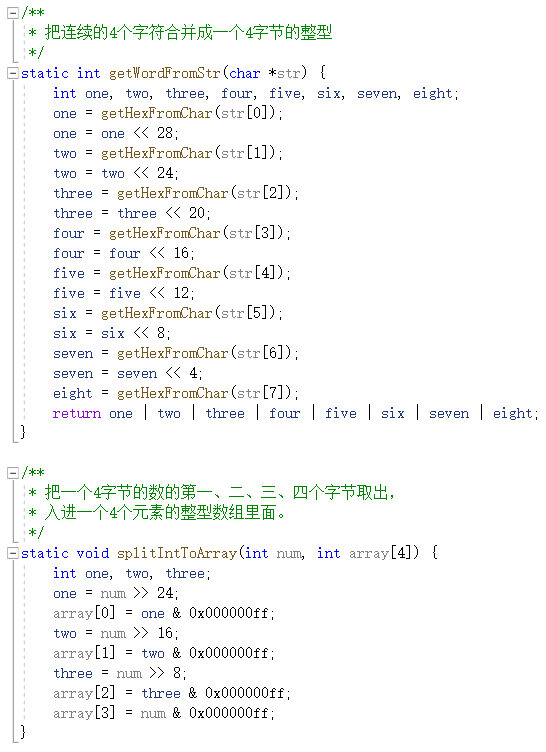
1. 主要代码
   1. AES主体



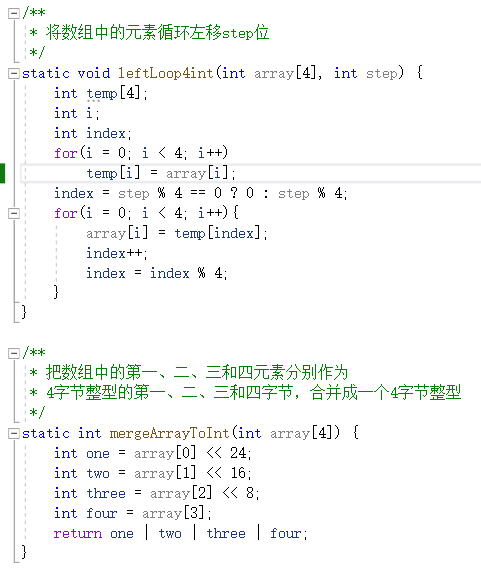
* 1. 用到的一些函数定义







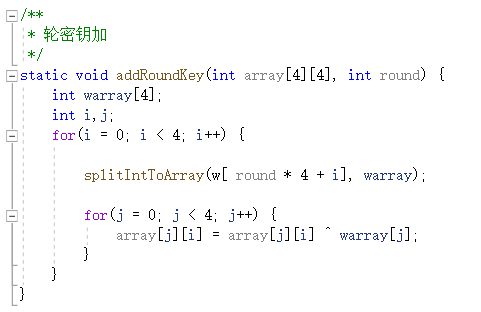




* 1. 密钥拓展 KeyExpansion



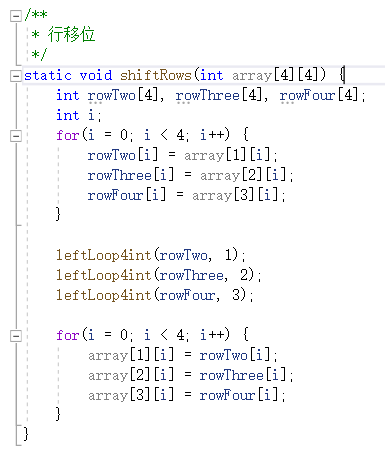
* 1. addRoundKey



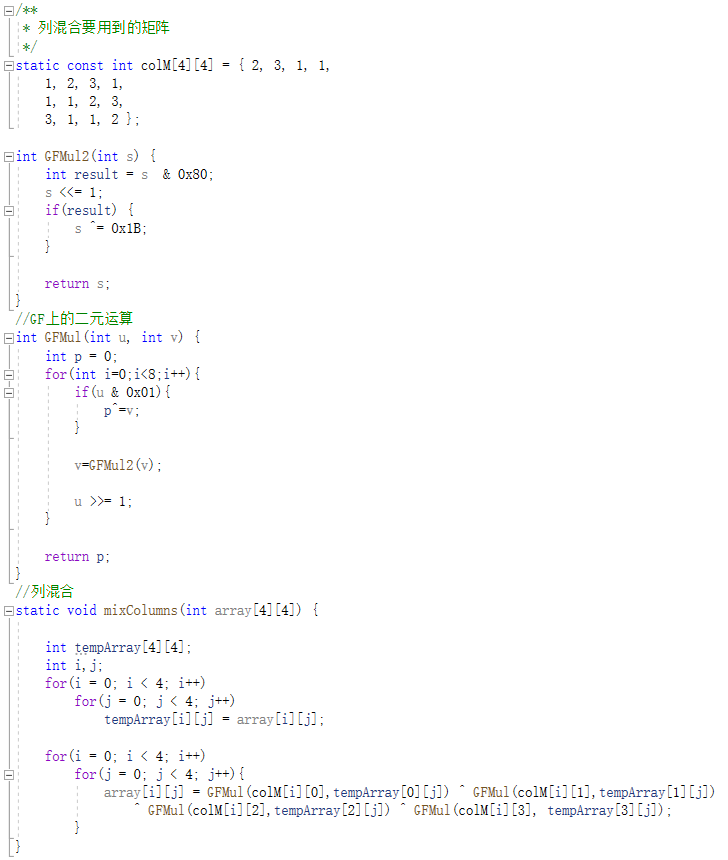
* 1. 字节代换



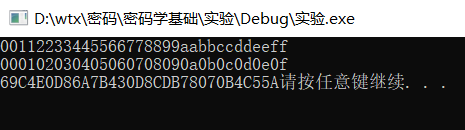
* 1. 行移位 shiftRows



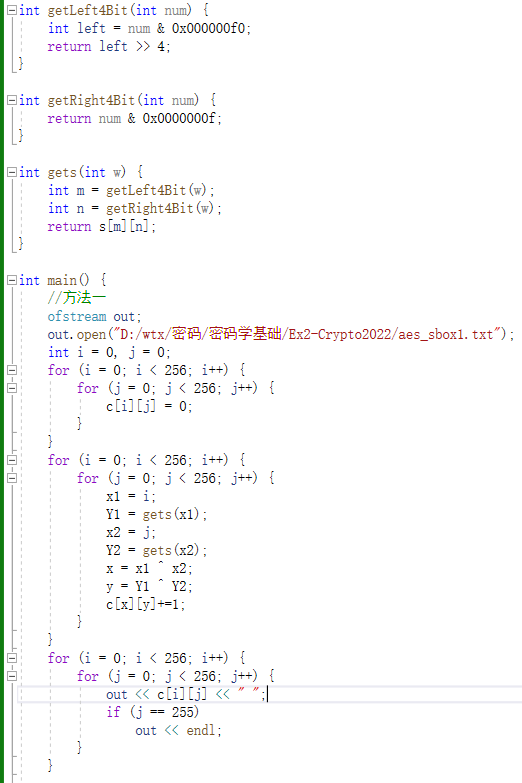
* 1. 列混合



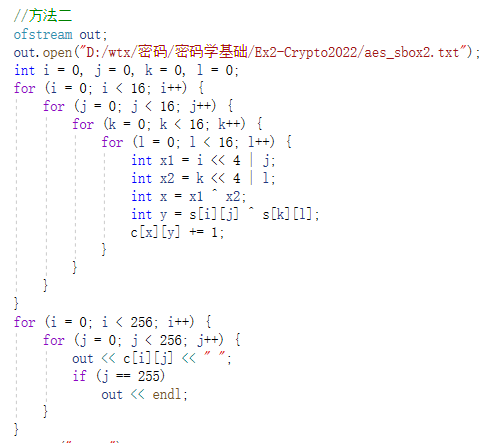
1. 输出结果



1. 实验思考
   1. 学会使用位移、与、异或运算符：位移运算符可以代替2的次方的乘法，运算速度较快，且可以获得任意bit的字符；与运算就是在二进制下的乘法运算，也可以用来得到指定位或bit的字符
   2. 从整型二进制形式进行思考，在字节上进行计算考虑
   3. 以char型数组读入的16进制的数字表示，考虑到位的不同，两位一组以对应10进制存储到int型数据中
   4. 以16进制大写形式输出并且设定两位输出且空格改为0输出
2. 计算AES SBox的差分分布表
3. 题目要求
4. 主要代码
   1. 方法一：考虑x1,x2，用过得到x1与x2的低八位的左四位和低八位的有四位计算出对应s盒的横纵坐标，然后求出y1,y2。



* 1. 方法二：从s盒横纵坐标出发考虑，从横纵坐标进行枚举，然后合并得到x1和x2的值，顺便也就得到了y1和y2的值。



1. 输出结果



1. 实验思考
   1. 从思路和代码上来说，整体还是比较简单的
   2. 从生成的差分分布表来看，以0、2为主，分布有少量的4和一个256，整体比较平均。尤其是和SPN比较，AES显然更不容易被差分攻击攻击成功。