**密码学实验三实验报告**

姓名：孟衍璋 学号：16337183

1. **实验目的**

对AES进行仿真实现。

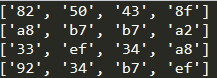
1. **实验内容**

使用AES的加密规则，对字符串“School of data science and computer, Sun Yat-sen University.”进行加密。并且选用CBC模式，密钥为sysu，密钥偏移量IV为123（10进制），补码填充方式为PKCS5Padding。

1. **实验及算法原理**

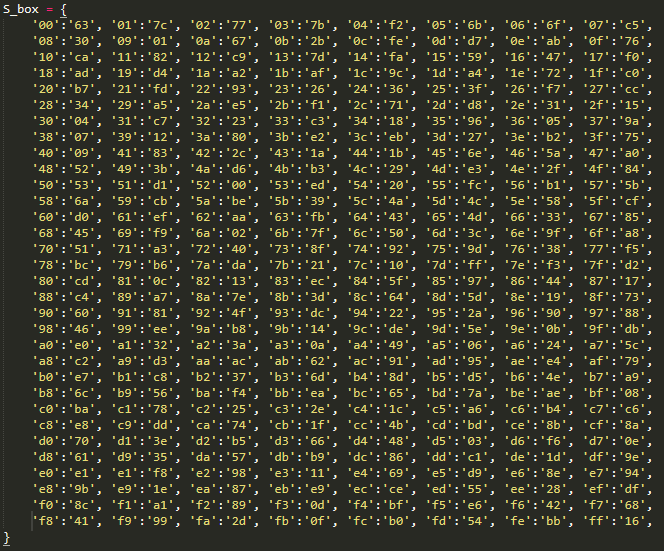
本次实验中，需要完整实现AES的加密过程。加密过程中有几个步骤比较重要。在编写代码时，用几个独立的函数来分别实现。

首先，每轮加密都是对state分组进行操作，每个分组128bits，所以在实现过程中，下列函数的输入输出的结构均如下图所示：

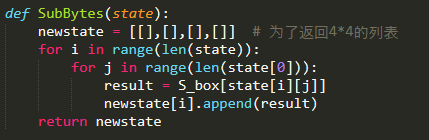


将128bits分为16组，每组8bits，用两个十六进制数来表示。

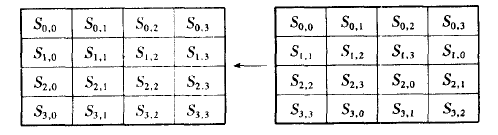
第一个要实现的函数是**SubBytes**，它使用一个S盒πS对state的每一个字节都进行独立的代换，其中πS是{0，1}8的一个置换。我采用字典的结构来完成这个置换的实现。其中AES的S盒如下：



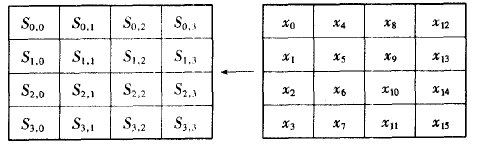
代码部分如下：



第二个要实现的函数是**ShiftRows**，是对state进行了行变换，变换操作如下：

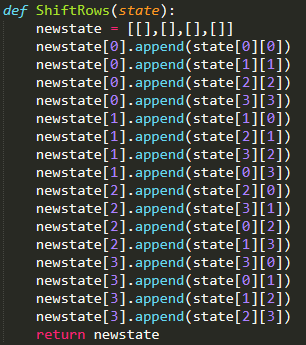


在实现这个函数的过程中，最开始对一个地方理解错误，所以进行了错误的变换，后来检查到了这个错误之处。出错的原因在于刚开始忽略了state是如何编排成4×4字节的矩阵的：



本来应该是以列为单位，分组中的比特依次从左到右摆放，而我错误地理解成了一行一行依次摆放，所以刚开始写的变换是有问题的。

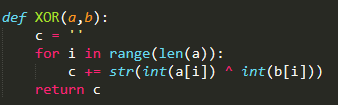
更改之后的代码如下：

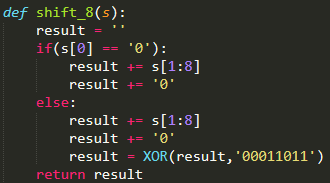


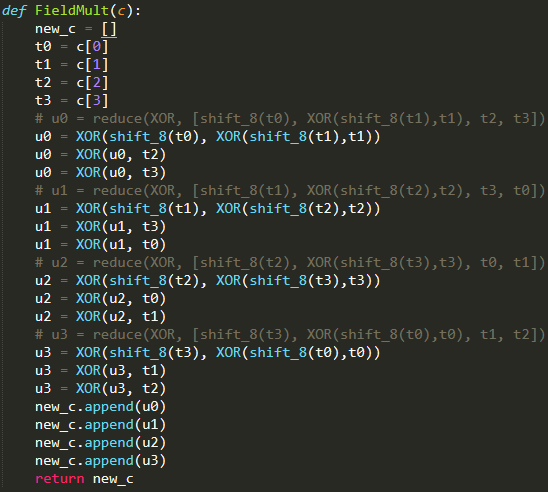
第三个要实现的函数是**MixColumns**，即对state的每一列都进行操作，替换为新的列，这个新列由原列乘上域中的元素组成的矩阵而来。

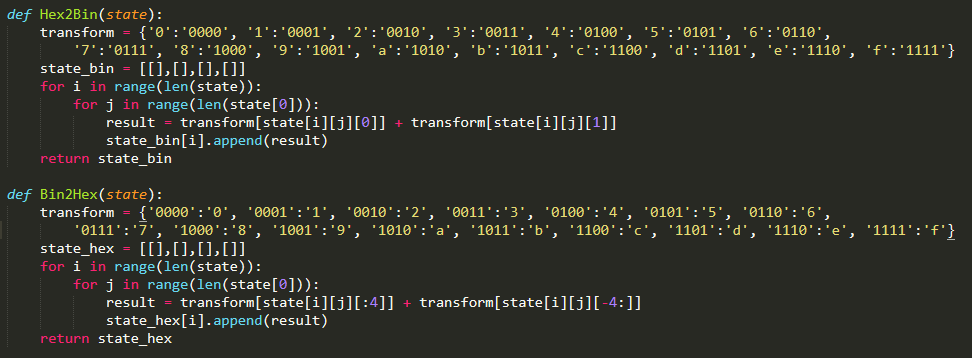
因为对于AES来说，域乘法只需要算与x和x+1的乘积，乘以x相当于左移一位，乘以x+1相当于左移一位之后与自身相异或。但是由于是在域中，还要考虑模一个多项式之后的结果，所以还要考虑到这点，不能简单地移位。刚开始也是忽略了这一点，所以出了些错误。

为了完成MixColumns还需要完成下列函数：

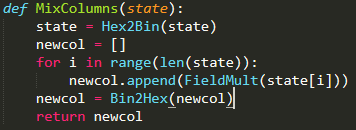






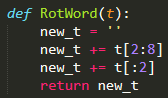


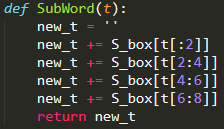
MixColumns的代码如下：



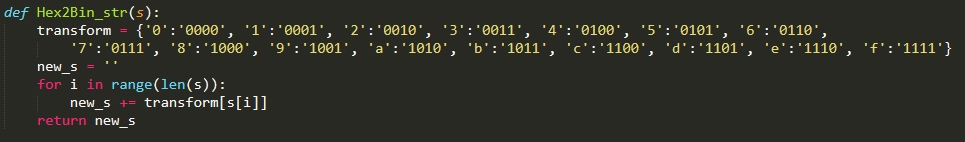
第四个要实现的函数是**keyExpansion**，即AES的密钥编排方案。要将128bits的种子密钥扩展为11个轮密钥，每个轮密钥由16个字节组成。最后返回的扩展密钥由44个字组成，表示为w[0],…,w[43]，其中每个w[i]都是一个字。

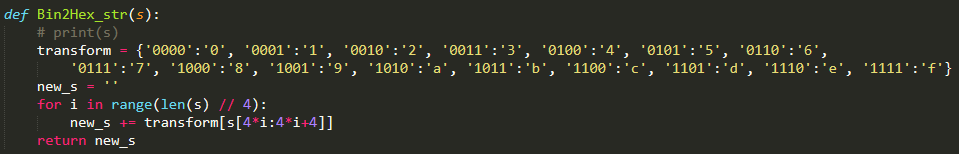
为了实现keyExpansion操作，还需要完成两个操作：RotWord和SubWord。RotWord对4个字节进行循环移位，SubWord对4个字节使用AES的S盒，实现分别如下：

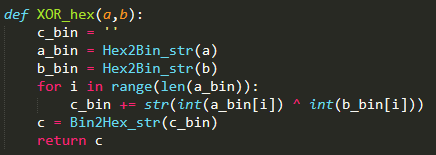




为了完成keyExpansion操作，还需要增加如下函数：







用来完成相应操作与结构的统一。

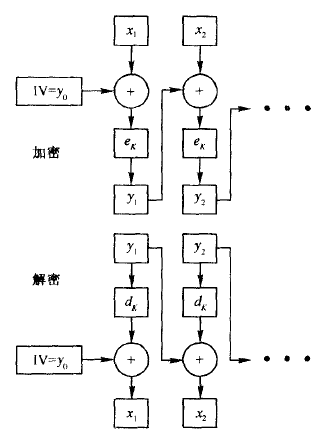
最后keyExpansion的代码如下：



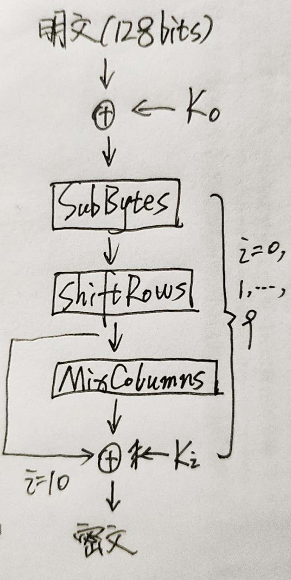
分别实现了上述函数之后，就要考虑执行AES加密的工作。首先要理解padding的部分，密钥和密钥偏移量转换为二进制之后，只需要在后面补0补至128位。明文转换为二进制后，需要分为128bits一组的多个分组，剩下的一组如果不足128bits，并且还差x比特到128比特，就在后面补t=（x/32）个‘0x0t’。

然后就要理解CBC模式的含义，每一个密文分组在用密钥K加密之前，都要先跟下一个明文分组相异或。比如开头密钥偏移量IV与第一个明文分组异或之后再用密钥K进行加密。

CBC模式示意图如下：



加密过程的示意图如下：



最后，经过10轮迭代，得到的state即为最终的密文。

1. **实验代码**

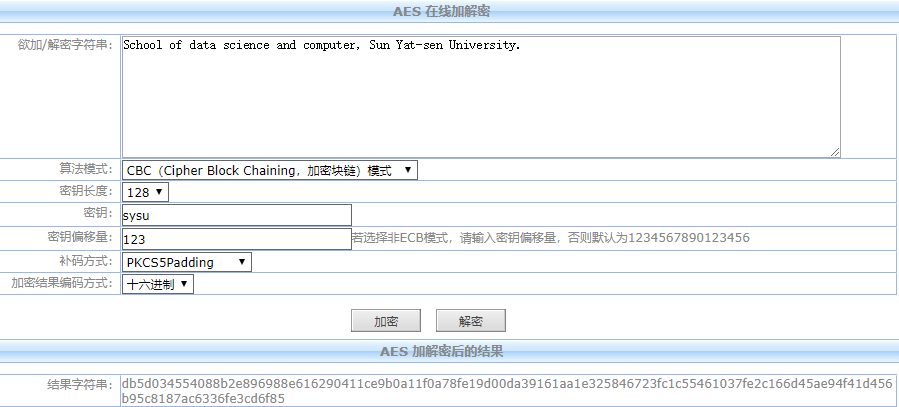


1. **运行截图**



1. **结果分析**

在AES在线解密的网站上运行如下：



与我的实验结果相符。

1. **总结**

这次实现AES的实验，过程看似复杂，但其实如果将过程一步步列举出来，先实现几个重要的函数，再按照加密的流程一步步走，最后总能完整地再现AES的过程。

在完成作业的过程中，开始对AES不太熟悉，后来将书上有关AES的内容读了几遍，才完全清楚流程。这次实验最大的难点应该在于AES的过程过于繁琐，所以在实现过程中哪怕出了一点小小的差错也会失之毫厘、差之千里，只有对照着过程一步一步核对，但想要找出错误十分困难。

刚开始的时候理解错了一些地方，比如对PKCS5Padding的理解不够透彻，后来发现形成明文分组的时候出了问题。还有对state结构的错误理解导致ShiftRows的操作错误。

总而言之， 在这次AES的实现过程中，对这种加密算法有了很透彻的理解，了解了其复杂的结构，也明白了为何对现在的所有已知攻击而言，AES是安全的。感觉这次的实验让我收获颇丰。