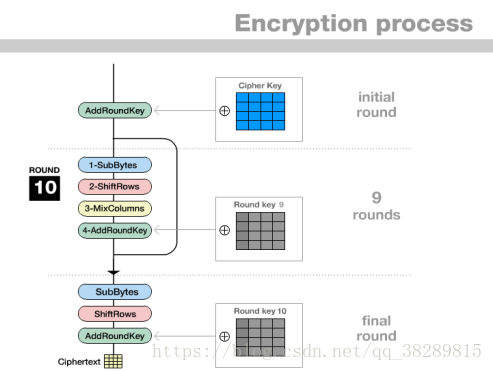
# Project9 AES/SM4softwareimplementation

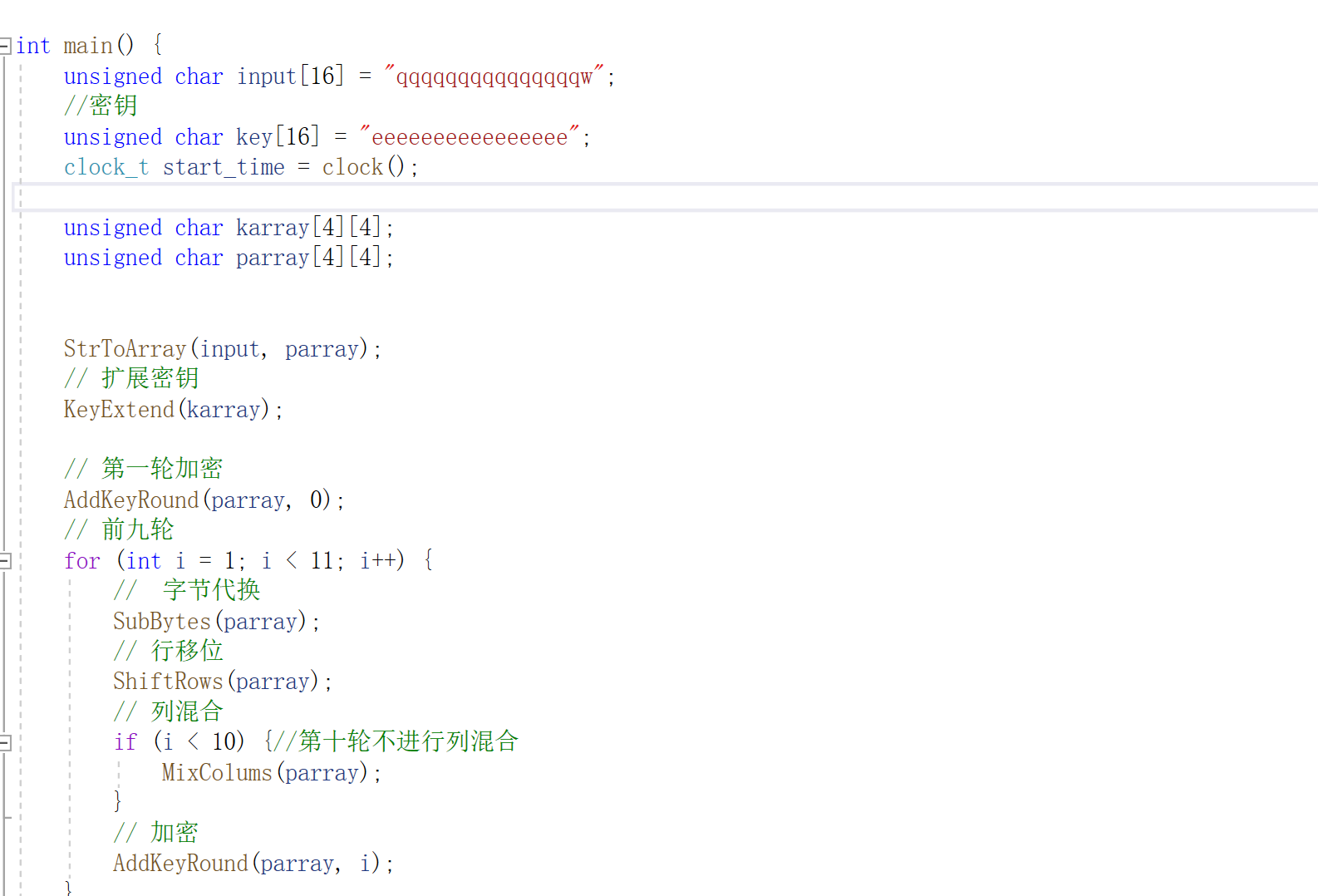
实现方式：

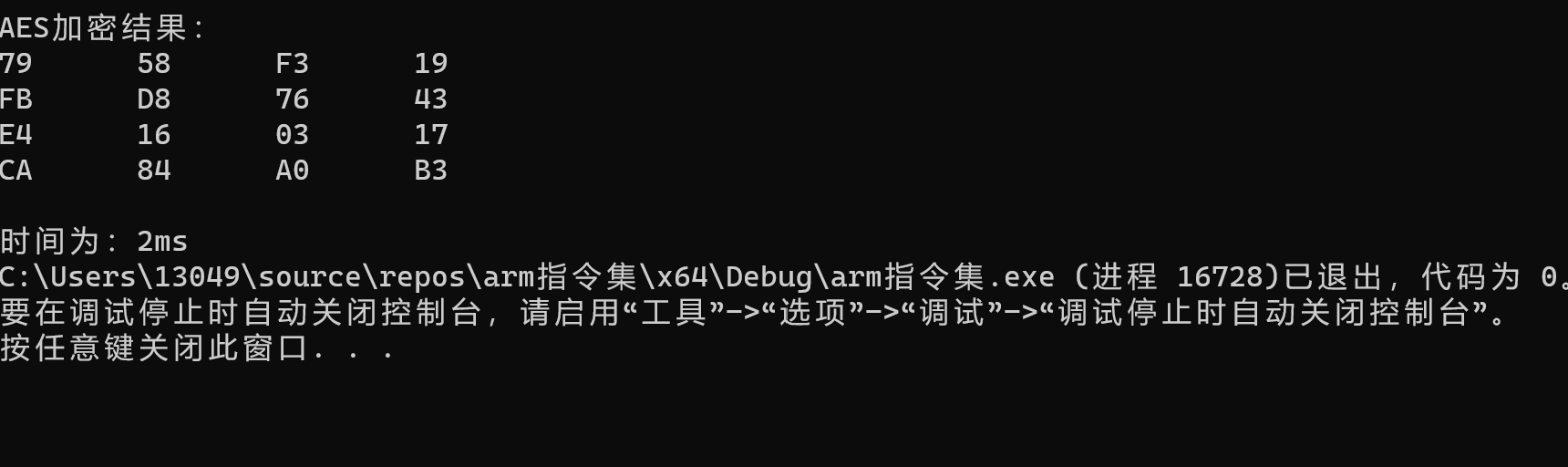
1.字节替换：字节代替的主要功能是通过S盒完成一个字节到另外一个字节的映射。

2.行移位：行移位的功能是实现一个4x4矩阵内部字节之间的置换。

3.列混淆

4.轮密钥加：加密过程中，每轮的输入与轮密钥异或一次（当前分组和扩展密钥的一部分进行按位异或）；因为二进制数连续异或一个数结果是不变的，所以在解密时再异或上该轮的密钥即可恢复输入。首尾使用轮密钥加的理由：若将其他不需要密钥的阶段放在首尾，在不用密钥的情况下就能完成逆过程，这就降低了算法的安全性。





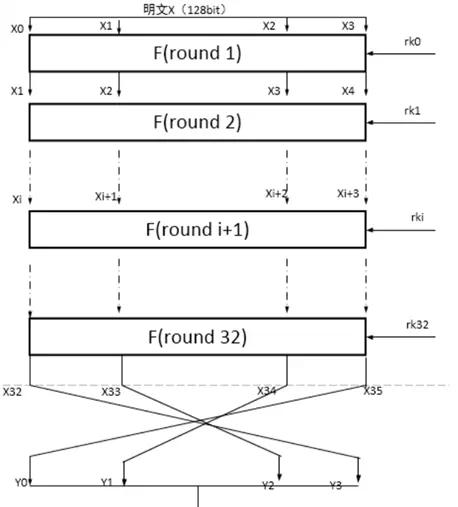
# SM4

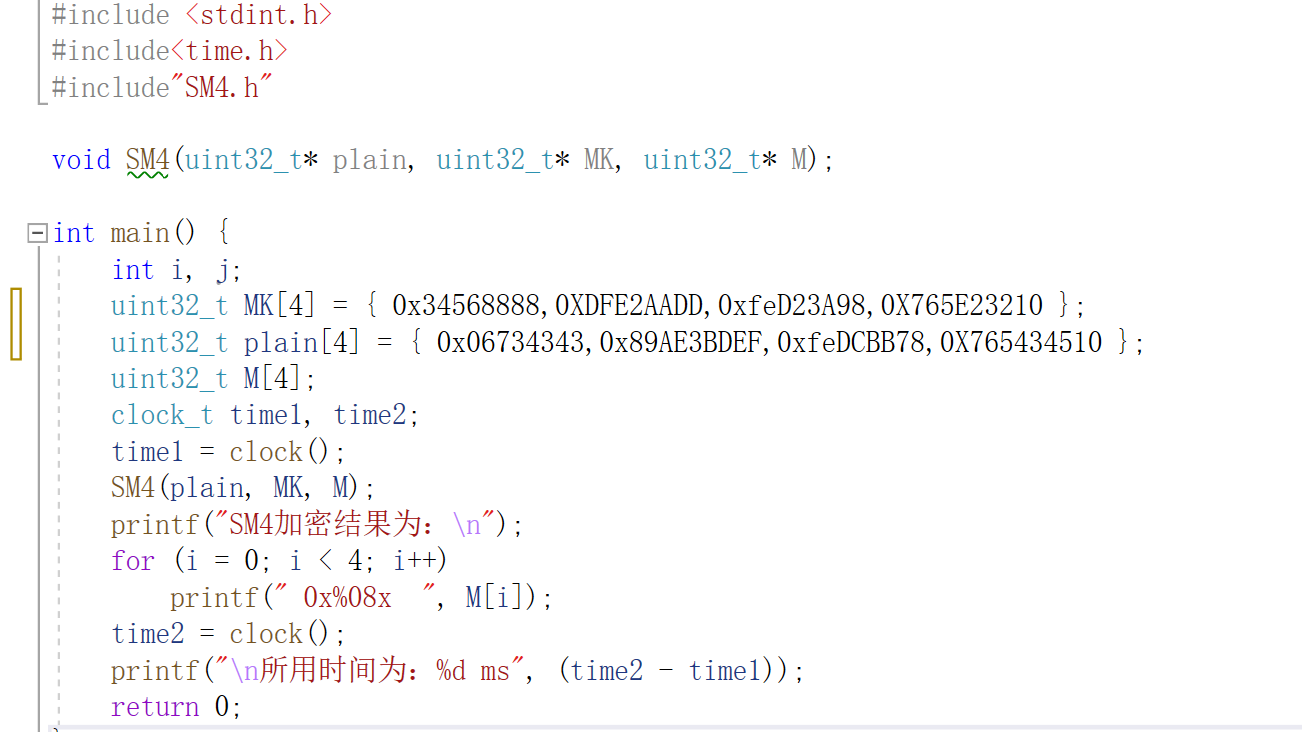
· 与DES和AES算法类似，SM4算法是一种分组密码算法。

· 其分组长度为128bit，密钥长度也为128bit。

· 加密算法与密钥扩展算法均采用32轮非线性迭代结构，以字（32位）为单位进行加密运算，每一次迭代运算均为一轮变换函数F。

· SM4算法加/解密算法的结构相同，只是使用轮密钥相反，其中解密轮密钥是加密轮密钥的逆序。





# 实现结果

