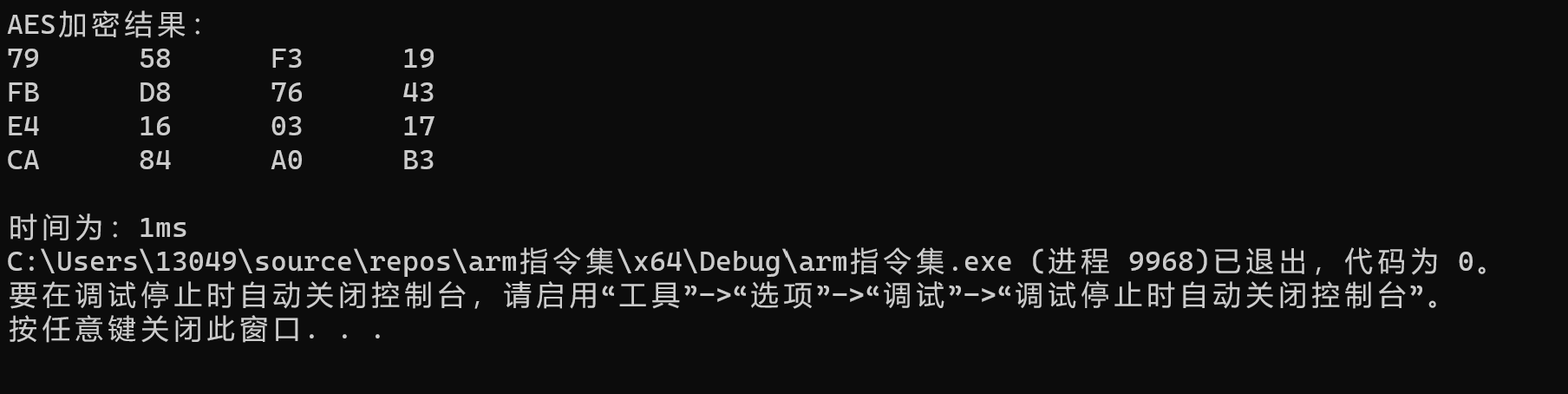
# \*Project9 AES/SM4softwareimplementation

# AES实现原理

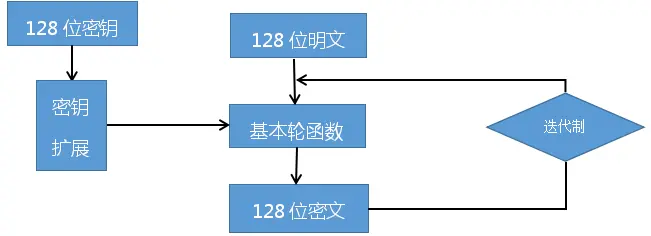
AES加密过程涉及到 4 种操作，分别是**字节替代、行移位、列混淆和轮密钥加**。解密过程分别为对应的逆操作。由于每一步操作都是可逆的，按照相反的顺序进行解密即可恢复明文。加解密中每轮的密钥分别由初始密钥扩展得到。算法中 16 个字节的明文、密文和轮密钥都以一个 4x4 的矩阵表示。



# 实现结果



# SM4算法



SM4算法的基本步骤如下：

密钥扩展：根据输入的密钥生成轮密钥，用于后续的加密和解密操作。

轮函数：SM4算法使用32位的字作为数据块，轮函数包括四个运算：非线性变换、线性变换、循环左移和异或运算。

a. 非线性变换：通过S盒代替输入的字节，S盒是固定的非线性变换表。

b. 线性变换：通过固定的置换操作，改变字的位置。

c. 循环左移：将字中的位进行循环左移操作。

d. 异或运算：将变换后的字与轮密钥进行按位异或运算。

加密/解密轮处理：SM4算法采用多轮迭代处理来加密和解密数据。每一轮的操作包括以下四个步骤：

a. 轮函数运算：使用轮函数对输入数据块进行变换操作。

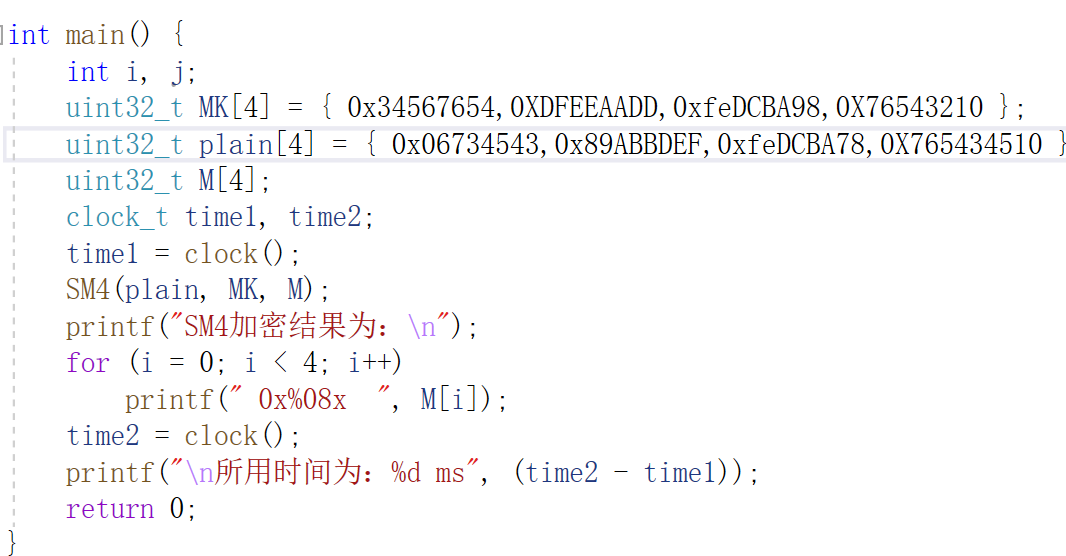
b. 轮密钥加：将当前轮的轮密钥与数据块进行按位异或运算。

c. 列混淆：对输入数据块的列进行线性变换。

d. 轮密钥更新：生成下一轮使用的轮密钥。

最后一轮处理：最后一轮处理与其他轮不同，它不包括列混淆。

密文输出（加密）/明文输出（解密）：经过多轮迭代后，最后一轮的输出即为加密后的密文或解密后的明文



**实现结果**

