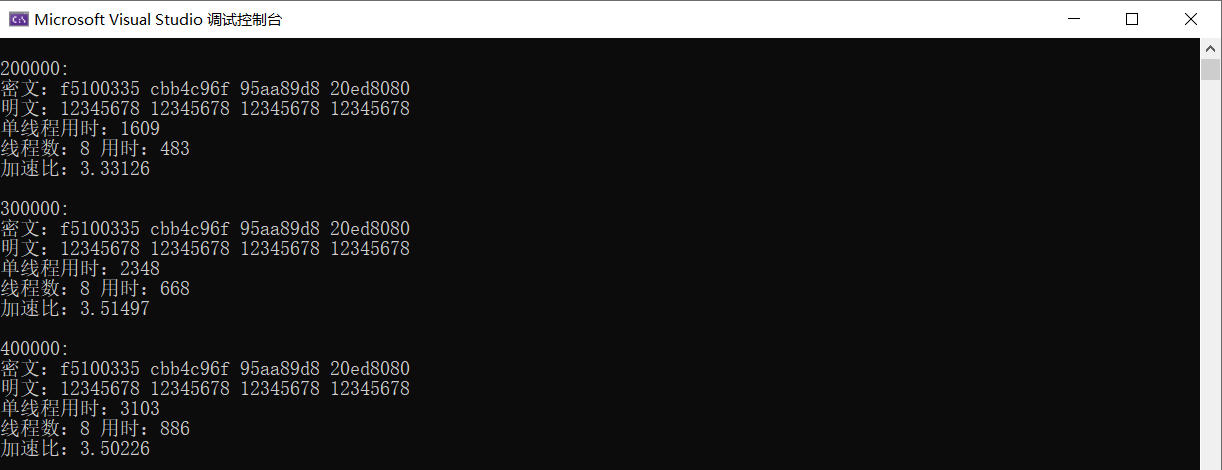
**项目名称：**SM4算法实现并优化

**项目完成人：**202000460080杜浩菘

**项目简介：**笔者先通过学习SM4算法的基本过程，实现了基本的SM4算法，然后又通过查阅资料，学习了一些加速算法的方法，最终通过使用SIMD和多线程，使得加速比达到3以上。

**项目代码具体说明：**相较之前的代码，这次代码中的ROL函数和T函数，都通过inline将其指定为内联函数，以省去函数调用的开销，提高运行效率。在密钥生成函数中，通过使用\_\_m128i数据类型，实现同时操作128比特，使用immintrin.h库中的一些函数，实现了异或、赋值等操作。笔者查询电脑配置得知CPU线程数为8，所以在使用多线程的函数中，线程数的实参为8，另外笔者又加写了几个实现多次重复加解密、生成密钥的函数（仅为了测试多线程的加速效率），在主函数中选取较大的数N来测试加速效率。

**代码运行结果：**



参考资料：

<http://t.csdn.cn/tscq9>

<http://t.csdn.cn/ZiefV>

<https://www.bilibili.com/video/BV1Ut411X7HE?spm_id_from=333.337.search-card.all.click&vd_source=19322a924880f3ef71159cb338b6161d>

<https://www.bilibili.com/video/BV1LS4y167r3?spm_id_from=333.337.search-card.all.click&vd_source=19322a924880f3ef71159cb338b6161d>