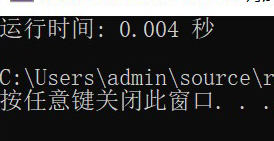
Python实现SM3算法

运行结果：

project4结果

C++实现对SM3的优化（借助openssl）

运行结果：



使用OpenSSL优化SM3算法，考虑以下几个方面：

1. 使用AES-NI指令集：AES-NI是现代处理器提供的硬件级别的加密指令集，可以加速SM3算法中的某些操作。您可以启用编译选项 `-maes` 来利用这些指令。

2. 并行计算：利用OpenSSL提供的多线程功能，使用多个线程同时计算多个数据块的哈希值，从而加快计算速度。您可以使用 `omp\_set\_num\_threads()` 设置线程数，然后使用 `#pragma omp parallel for` 来并行计算。

3. 使用优化的代码路径：OpenSSL库中提供了针对不同处理器架构的优化代码路径。您可以使用 `-march=native` 编译选项来让编译器自动选择适合您的处理器的优化代码路径。

4. 数据对齐：确保待处理的数据是按照字节对齐的，这可以减少内存访问的开销。