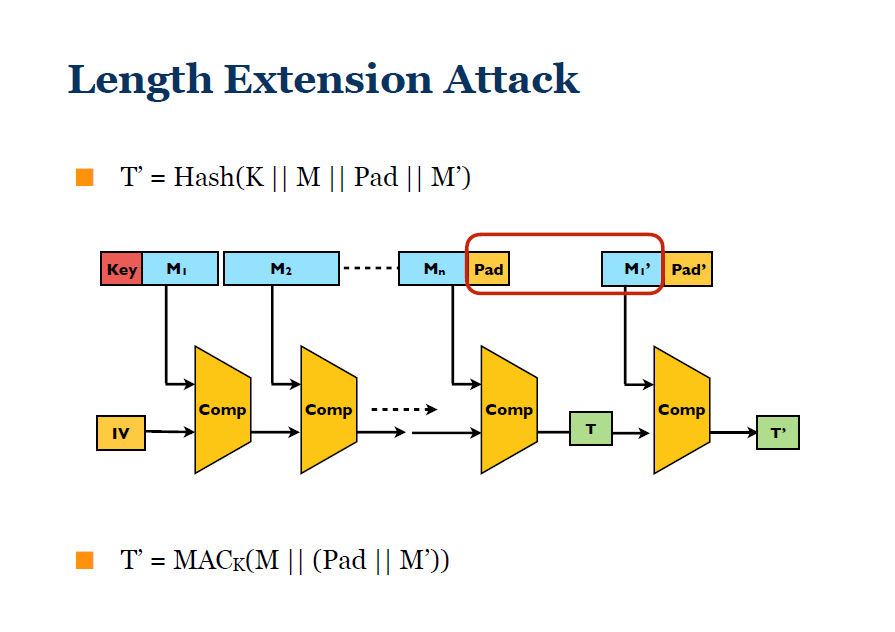
# 一、设计思路



就像上课老师ppt上所讲的一样，首先我们知道的是明文M1，M2……Mn的值，以及生成的哈希值T，在这个过程中间我们不需要知道key的值，就能通过这个来构造出另外的M-T’的对应。

我们在拿到了生成的T以及整个明文串M，我们需要知道明文的长度。

首先我们需要在Mn后面手动的填充pad，用0补全填充到后面，再用64bit长度来表示原明文M的长度进行手动补全，接下来我们利用sm（）函数来进行调用，sm（M，length，T）求得T’，此时我们就得到了T’= Hash(K||M||Pad||M’)。

在提交的文件中，sm3.c和sm3.h文件是sm3算法的库文件，sm3Attack是模拟sm3消息加长攻击的代码。

在程序中，设置的原明文为“aaa”，加长的消息为“bbbb”\*16个，最终得到的两次哈希值如图所示。

主要代码说明：

sm3(input, ilen, output);//第一次调用sm3进行hash

sm3\_starts( &ctx );//初始化

sm3\_finish( &ctx, output );//得到结果

# 二、实验结果

运行sm3Attack文件得到如下结果：

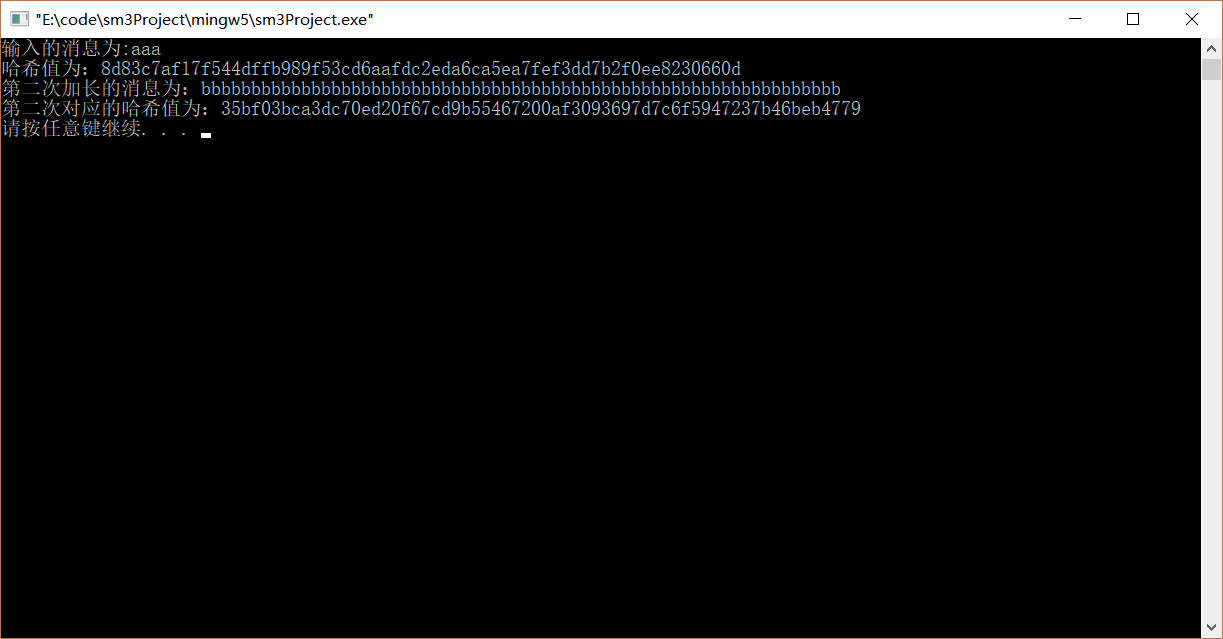


图2-1 运行结果截图

结论：结果正确