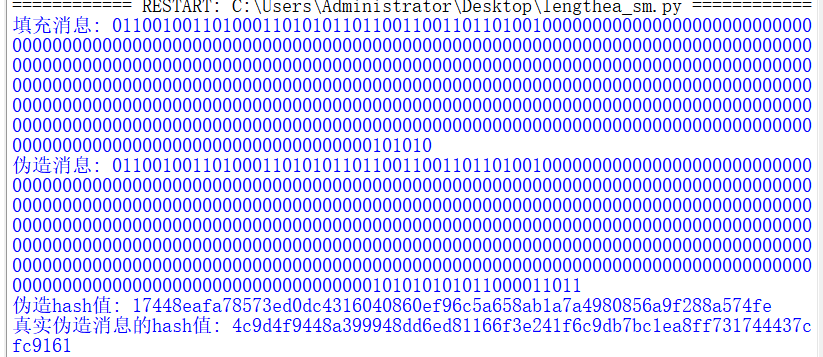
运行结果：



根据结果可以看出伪造的hash值和伪造消息的直接hash值不同，可知长度扩展攻击并不适用于SM3算法，原因在于长度扩展攻击是指对哈希函数的一种攻击方式，利用哈希函数的特性，通过已知消息的哈希值和长度，构造出一个新的消息和对应的哈希值，而无需知道原始消息的内容。

对于SM3哈希函数来说，由于其使用了消息填充和压缩函数，使得长度扩展攻击不适用。在SM3中，消息填充会将消息的长度信息添加到消息的末尾，同时还会添加一些特定的填充字节，以保证消息长度对压缩函数的影响。

具体来说，SM3的消息填充方式是将一个0x80字节添加到消息的末尾，然后添加一个64位的消息长度，表示原始消息的比特数。这样，在构造长度扩展的攻击时，攻击者无法知道填充的内容和长度信息，从而无法正确计算出新的哈希值。

因此，对于SM3哈希函数来说，长度扩展攻击是不可行的。这也是SM3相对于一些其他哈希函数的优势之一，可以提供更好的安全性。