**SM3长度扩展攻击**

**作业说明**

**1.设计思路**

在密码学和计算机安全中，长度扩展攻击（Length extension attacks）是指针对某些允许包含额外信息的加密散列函数的攻击手段。该攻击适用于在消息与密钥的长度已知的情形下，所有采取了H(secret || data) 此类构造的散列函数。

即使我们不知道secret 的值，我们还是可以得出（secret || data || append\_data）的哈希值，以此来进行攻击。

只要取出H(secret || data)的值，在后面附加上消息，再进行一轮运算，便可以得出虚假消息的哈希值。

**2.程序结构**

本作业源码分为5个文件：SM3.c、SM3.h、SM3\_extension\_attack.c、SM3\_extension\_attack.h、main.c。

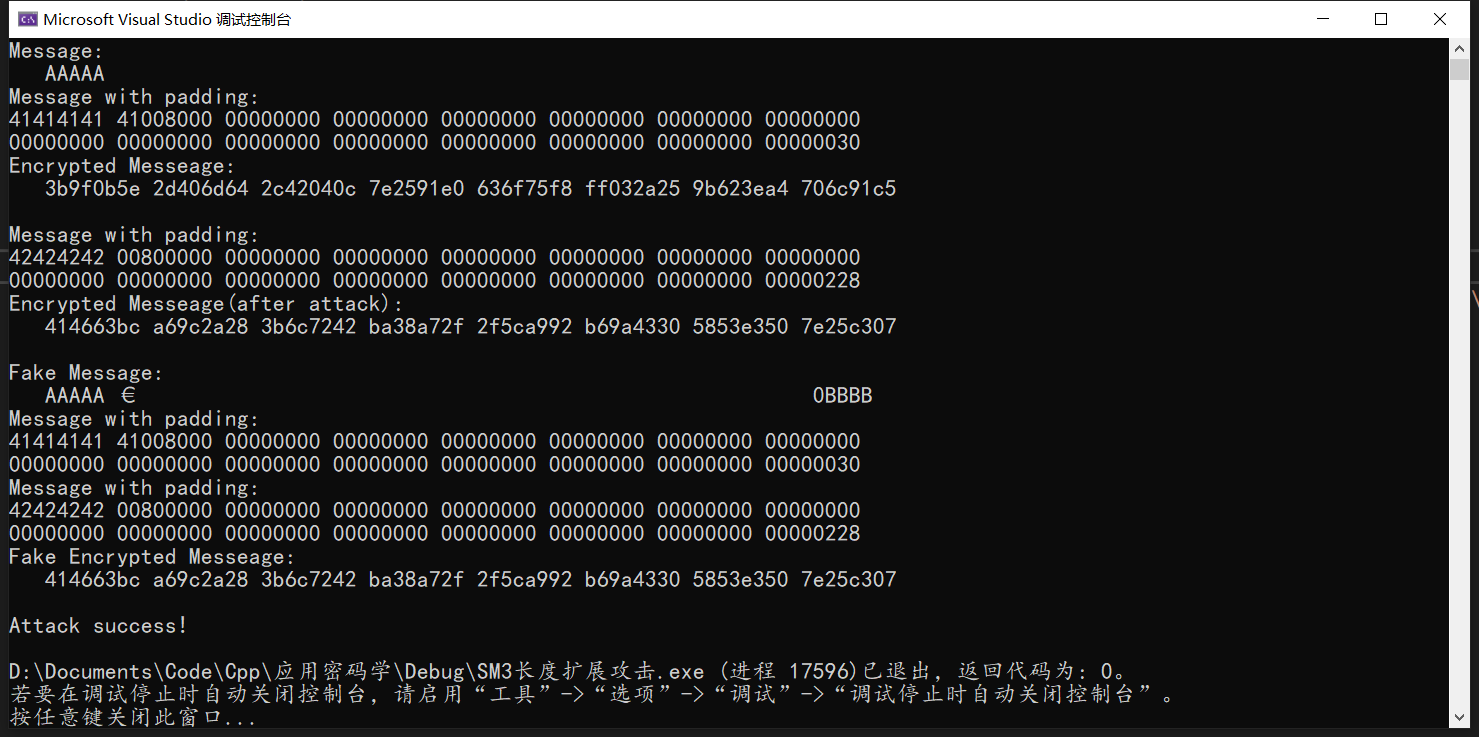
其中，SM3.c和SM3.h为SM3加密算法的源代码和头文件；

SM3\_extension\_attack.c、SM3\_extension\_attack.h为长度扩展攻击的源代码和头文件；

main.c为测试代码，其中主程序是长度扩展攻击的代码，test\_abc函数是用来测试SM3加密算法本事是否有问题的。

更详细的说明见源代码中的注释。

**3.运行结果**



如图所示，进行长度扩展攻击后发送的hash码值和接收者收到的虚假消息（Fake Message）hash码值相同，长度扩展攻击成功。

本来要发送的消息："AAAAA"

攻击者附加的消息："BBBB"

接收端误以为收到的消息："AAAAA"+pad+"BBBB"，