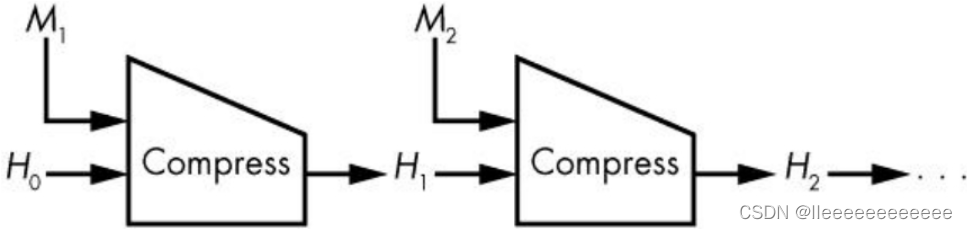
# project-3

# implement length extension attack for SM3, SHA256, etc.

长度扩展攻击是利用了SM3、SHA256、MD4、MD5、SHA-1、SHA-2这些hash算法的MD结构，在知晓信息的长度之下，可以在后续追加自定义信息来伪造有效hash值的一种攻击。

MD结构如图所示：



# 实现方式

在知晓待hash的信息长度前提之下，在信息之后填充一定数量的零，直达信息长度为分组长度的整数倍，然后再添加自定义的信息，根据MD结构，这样操作之后的信息的hash值可以由以原先信息的hash值作为IV，新自定义信息作为待hash信息得到。我们将这样操作之后得到的hash值与plaintext||000...000||data\_append的hash值做对比，若相同，则说明正确。

# 实验环境

Windows10

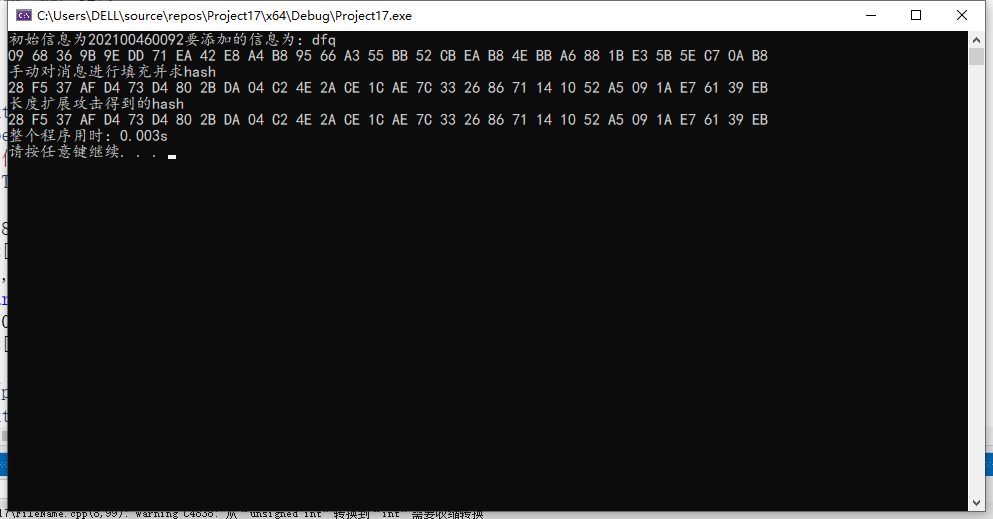
visual studio 2022

CPU：11th Gen Intel(R) Core(TM) i7-11800H @ 2.30GHz

# 实现效果

运行速度0.003s

结果如图：



# 小组分工：

戴方奇202100460092个人完成project3