# project-2

implement the Rho method of reduced SM3

# 实验步骤

1.首先用c++实现了reduced sm3算法

2.再通过rho攻击方法，通过不同迭代速度方式形成环，找到碰撞

# 实现方式

因为sm3与MD5和SHA-1类似，属于迭代压缩函数类型的哈希函数，所以可以使用rho碰撞攻击，选择两个不同的随机输入，并用哈希函数进行迭代压缩。第一个输入每次迭代一次，第二个每次迭代两次，然后比较每次的hash输出，找到碰撞，这种方法减少了存储空间。

# 实验环境

Windows10

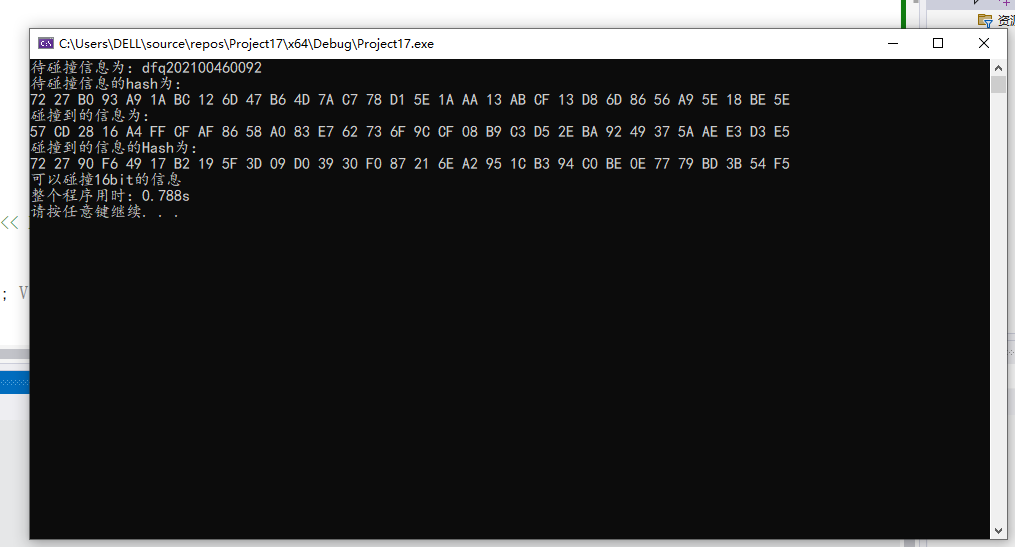
visual studio 2022

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

# 实现效果

运行速度0.788s

结果如图：



# 小组分工：

戴方奇202100460092个人完成project2