**\*Project2: implement the Rho method of reduced SM3**

代码说明：

此项目是实现SM3的Rho攻击。

Rho攻击是一种基于碰撞概率的攻击方法，适用于部分哈希函数。这种攻击方法利用了哈希函数的迭代结构和碰撞概率，通过找到两个具有相同哈希值的输入来构造攻击。

基本原理是通过选择不同的初始输入值，并跟踪哈希函数迭代过程中产生的中间值，以期望找到具有相同中间值的两个输入，进而产生哈希碰撞。

实现SM3的前n位Rho攻击：

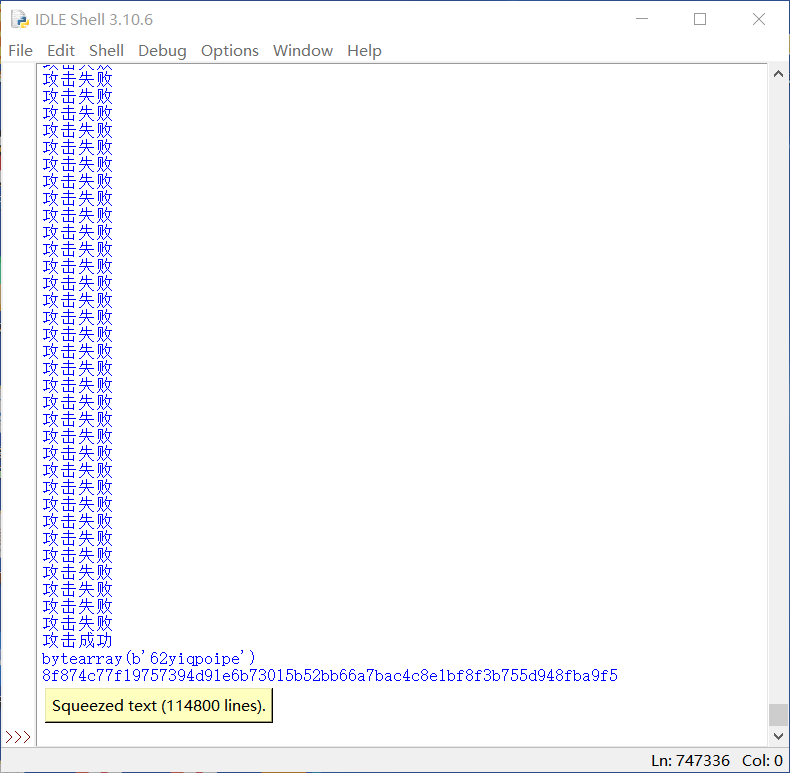
定义generate\_random\_string函数，接受一个参数length，生成一个长度为length的随机字符串。定义rho\_attack函数，接受一个参数n，将n转换为前n位比特数。然后，通过for循环迭代生成大量随机字符串b，并计算其SM3哈希值的前n位比特c。检查c是否在列表a中，如果在，则认为攻击成功，并打印出成功信息以及找到的两个不同字符串和哈希值。如果不在，将c添加到列表a中，并继续生成新的随机字符串b。

注：rho\_attack(n) 中可根据需要将函数变量n改为任意整数。

实现方式：python

效果：在自己电脑上CPU：11代i7

这里以rho\_attack(40)为例，展示其结果：



Squeezed text(114800 lines)中的内容：



分工：自己独立完成