Report2：

本次实验完成的是对于reduced-SM3用rho-method进行碰撞攻击，和之前的相同，使用的SM3实现方式是Python语言和基于GmSSL国密库的实现。因为要使用SM3进行不停的哈希，所以在这个实验中具体流程应该是：初始一个消息，然后对这个消息hash一下，算出具体的hash值后，因为使用reduced-SM3，所以应选取前n位（这个n应该根据每次测试改变）。然后对这个结果再次hash，再次选取前n位，直到我们找到一个环为止。

我使用的判断环的方法如下：规定两个变量msg1和msg2。msg1每次做一次hash截取，msg2做两次哈希两次截取，用index记录当前走过的步数。直到msg1和msg2相等时，说明出现了一个环，且index是环长的k倍，k为整数。

然后要找到环口，也就是环开始的地方。此时保持msg2不变，规定msg3从开头开始走，msg1从当前位置开始走，直到他们两个相遇，此时的值即为环口的值。

最后还要找环长，对于环长，只需要从上述环口位置，直到第一次走回环口，所经过的步数就是环长的值。

以下展示了通过rho-method，我所找到的不同位数的hash碰撞（其中只放了64、72、80、88位的hash碰撞，对于小的位数效果相同），可以看到，在不同位数的条件下，对于每次随机生成的一个消息，都找到了碰撞，并且求出了环口，环长。可以发现，这个方法的效率比起naive的birthday-attack来说要高上一些。（如果下图没有显示出来的话，可以到pics文件夹查看）(如果您想测试代码的正确性的话，直接运行可能较慢，您可以将[0:11]替换成[0:1]、[0:2]、[0:3]或[0:4]，这样可以较为快速的得出碰撞8bit、16bit、32bit和64bit的结果)

```
C:\Users\86180>set PYTHONIOENCODING=utf8 & C:\Users\86180\AppData\Local\Programs\Python\Python39\python.exe -u "c:\Users\86180\Desktop\sm3-rho.p
完成啦!
初始的消息为（hex类型）： f5b8905ecc381ef8c954e9ad97773028a89cded866d7e0511aea696f884fd3cf
找到的两个碰撞(16进制)为 6324ac13
一共走了  86178  步
找到碰撞花费时间为： 70.37435698509216
环口是（hex类型）： d85a9015  是第 58738 个
环长为： 28726
```

以上是找到的64位碰撞

```
C:\Users\86180>set PYTHONIOENCODING=utf8 & C:\Users\86180\AppData\Local\Programs\Python\Python39\python.exe -u "c:\Users\86180\Desktop\sm3-rho.py"
完成啦!
初始的消息为（hex类型）： bc5300a591146decee9be98f32cea00b83f5f7e53a74936e3d65cfcdd1c04cf5
找到的两个碰撞(16进制)为 4882a3632
一共走了  290184  步
找到碰撞花费时间为： 240.5075821876526
环口是（hex类型）： 89c3724f3  是第 161665 个
环长为： 290184
```

以上是找到的72位碰撞

```
C:\Users\86180>set PYTHONIOENCODING=utf8 & C:\Users\86180\AppData\Local\Programs\Python\Python39\python.exe -u "c:\Users\86180\Desktop\sm3-rho.p
完成啦!
初始的消息为（hex类型）： a4baf8cc9d80d2e89a45f5f9d2b63b55d0c51605ab306401348ae3ce43835565
找到的两个碰撞(16进制)为 b2ab2898f1
一共走了  1298086  步
找到碰撞花费时间为： 1042.038551568985
环口是（hex类型）： 9d6eef600d  是第 1022270 个
环长为： 1298086
```

以上是找到的80位碰撞

```
C:\Users\86180>set PYTHONIOENCODING=utf8 & C:\Users\86180\AppData\Local\Programs\Python\Pyth
完成啦!
初始的消息为（hex类型）： 749ceefe52a75e7d3c409660c374ab52f44b13af84e9cbd35ca0e7424b3c8e6b
找到的两个碰撞(16进制)为 e3534c6bc8f
一共走了  4225427  步
找到碰撞花费时间为： 3482.157767534256
环口是（hex类型）： 048c5d9245a  是第 1561378 个
环长为： 4225427
```

以上是找到的88位碰撞