*Project1: implement the naïve birthday attack of reduced SM3

代码说明：

此项目是实现 SM3 生日攻击。

生日攻击是利用概率论中的生日问题,找到冲突的 Hash 值,伪造报文,使身份验证算法失效。生日攻击的基本思想是寻找两个不同的输入消息，它们经过 SM3 算法后产生相同的 hash 值。根据生日悖论，n 位的哈希值经过 2^(n/2)次尝试预计可以约 1/2 的概率产生一次碰撞。

本项目我先用 python 实现了 FF、GG、p0、p1、消息填充、消息扩展、压缩、迭代等函数，进而实现了 SM3 算法，再进行生日攻击，实现 SM3 生日攻击的前 n 位比特的碰撞的步骤如下：

（1）定义 v 函数，接受参数 n，生成一个随机 8 位（可改为自己想要的位数）字符串 s，并将其转换为字节数组 a。然后，对 a 进行 SM3 哈希，并截取前 n 位比特得到 j。最后，将 a 和 j 作为一对返回。

（2）定义 birthday_attack 函数，接受参数 n，将 n 转换为前 n 位比特数，并调用 v 函数生成两个不同的 pair（a1, j1）和（a2, j2）。然后，在 for 循环中比较 a1、a2，j1、j2。如果找到两个不同的字符串（即 a1≠a2），且它们的前 n 位哈希值相同（即 j1=j2），则认为攻击成功。如果不满足，则继续生成新的随机字符串对，并进行下一轮循环。

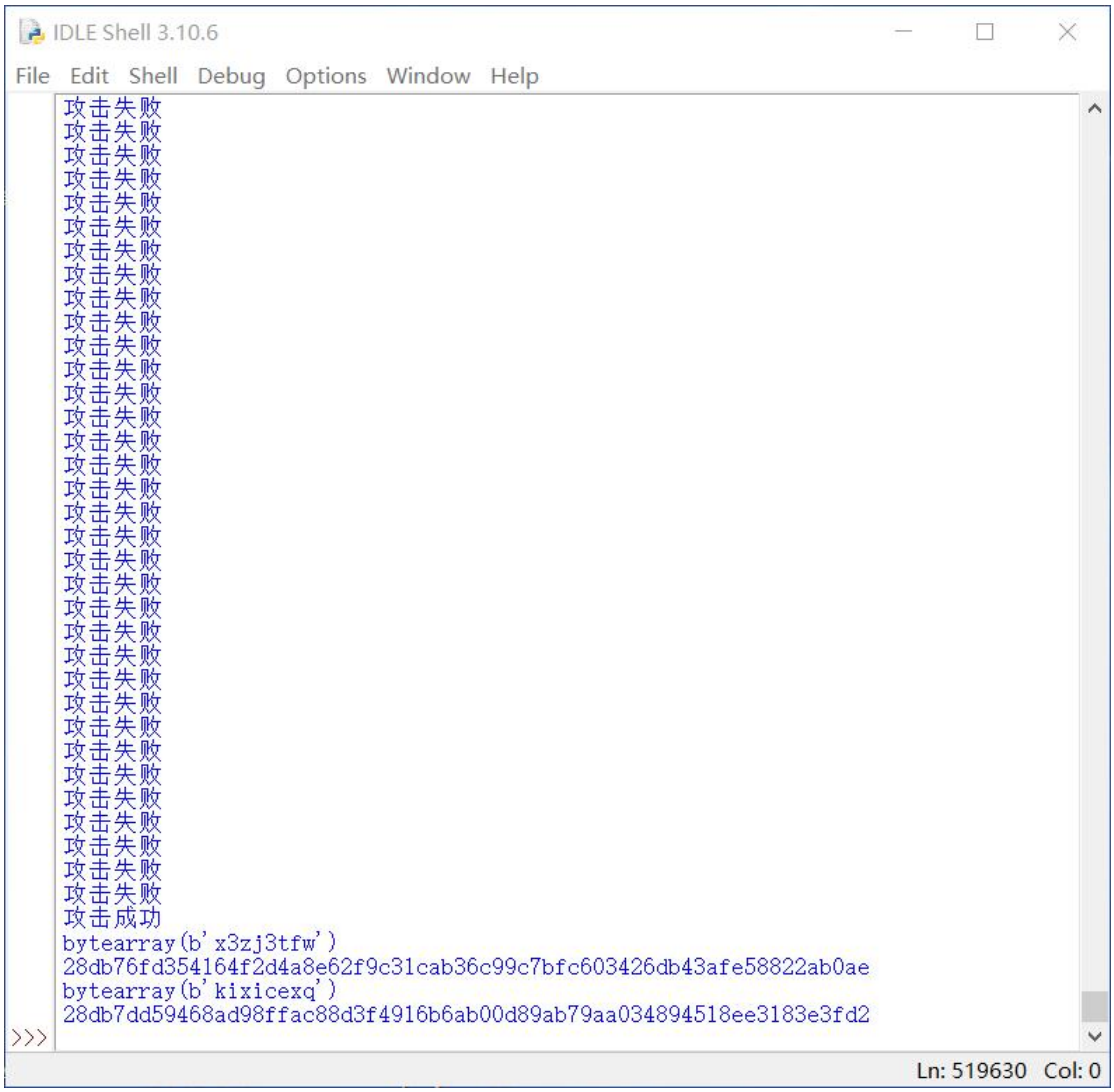
Ps：birthday_attack(n)函数中的 n=int(n / 4)是因为产生的随机消息一位单位为一个字节，除 4 后单位为 1bit。

birthday_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 birthday_attack(20)为例，展示其结果：


IDLE Shell 3.10.6
File Edit Shell Debug Options Window Help
攻击失败
攻击失败
攻击失败
攻击失败
攻击失败
攻击失败
攻击失败
攻击失败
攻击失败
攻击失败
攻击失败
攻击失败
攻击失败
攻击失败
攻击失败
攻击失败
攻击失败
攻击失败
攻击失败
攻击失败
攻击失败
攻击失败
攻击失败
攻击失败
攻击失败
攻击失败
攻击失败
攻击失败
攻击失败
攻击失败
攻击成功
bytearray(b'x3zj3tfw')
28db76fd354164f2d4a8e62f9c31cab36c99c7bfc603426db43afe58822ab0ae
bytearray(b'kixicexq')
28db7dd59468ad98ffac88d3f4916b6ab00d89ab79aa034894518ee3183e3fd2
>>>
Ln: 519630 Col: 0

分工：自己独立完成