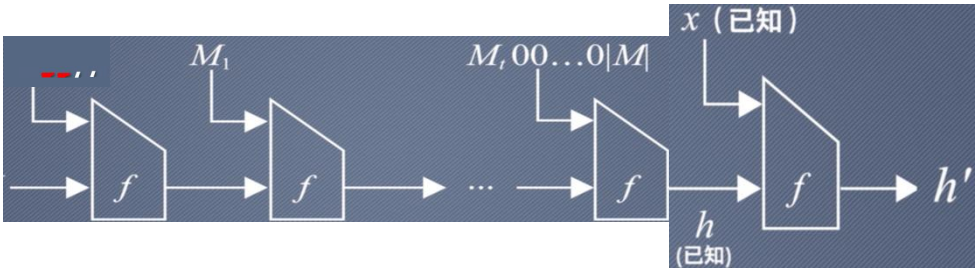
*Project3: implement length extension attack for SM3, etc.

代码说明：

此项目是实现长度扩展攻击，在此实现了对 SM3 的长度扩展攻击。

SM3 长度拓展攻击是一种利用哈希函数的长度扩展性质的攻击方式。SM3 算法在哈希计算中采用了 MD 结构，这种结构使得：可以通过已知原始消息 M 的长度及其 hash 值 h，令 z= 0^d|| |M| ||x，x 为任意长度的附加消息，则根据 h 可计算 h',满足 H(M||z)=h'。(M||z, h')即是一个利用长度扩展攻击得到的伪造。

这是因为 MD 结构在处理消息块时，不对整个消息进行完整的处理，而是对每个消息块进行局部处理，因此可以对部分原始消息进行长度拓展。



步骤：

（1）定义 len_attack 函数，接受参数 m 和 length，m 为原始消息（a）的 hash 值，length 为原始消息的长度。在进行长度扩展攻击时，我们不知道原始消息具体是什么，只知道原始消息的长度，因此我们随意构造相同长度的消息（在这里我们每长度都用‘1’来构造）。

（2）对 SM3 函数进行改造：增加了两个参数：一个为 IV，一个为 flag。当 flag 为 0 时，按正常 SM3 计算消息 m 的 hash 值；当 flag 为 1 时，实际上是实现了从 m 中截取附加消息 x，并利用 h，x 计算 h'。

（3）我们将构造的相同长度的消息进行填充（fill）后，将附加消息'202100150084'拼接到其后面，然后将其传给稍微改造后的 SM3 函数的 m，把原始消息的 hash 值 m 传给 SM3 函数的 IV，SM3 函数的 flag 取 1。计算得到长度扩展后的结果 c（即 h'）。

（4）再构造出 a|| 0^d|| |a| ||x，进行 SM3 计算出 H(a|| 0^d|| |a| ||x)，与 h'比较，若相等，则长度扩展攻击成功。

Ps：可任意更改生成的随机消息的长度，也可任意更改附加消息。

实现方式：python

效果：在自己电脑上 CPU：11 代 i7

```
========================== RESTART: E:\project3SM3.py ==========================
生成的随机消息：
bytearray(b's0yskmqa')
随机消息的hash值：
ae7b756bddd17bdc95c4bc97ffc85243f1307fd22f3ea3773604058426acf776
附加消息： 202100150084
长度攻击得到的hash值：
ec9712261d43b6d123e74102525d50d4f1f41f53a4f3d536a68174d4ed931049
生成的随机消息+填充+附加消息：
bytearray(b's0yskmqa\x80\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00
\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00
\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00
@202100150084')
它的hash值：
ec9712261d43b6d123e74102525d50d4f1f41f53a4f3d536a68174d4ed931049
```

分工：自己独立完成