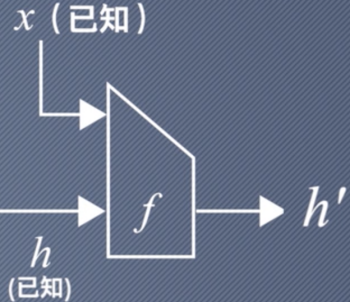
**\*Project3: implement length extension attack for SM3, etc.**

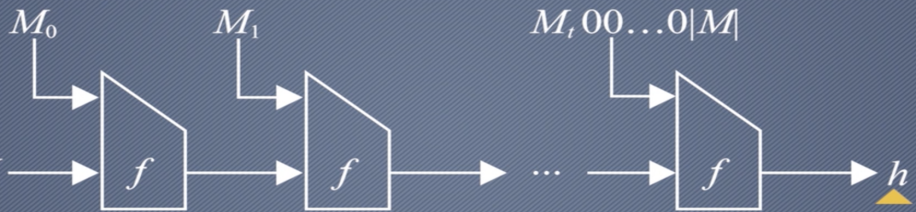
代码说明：

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：

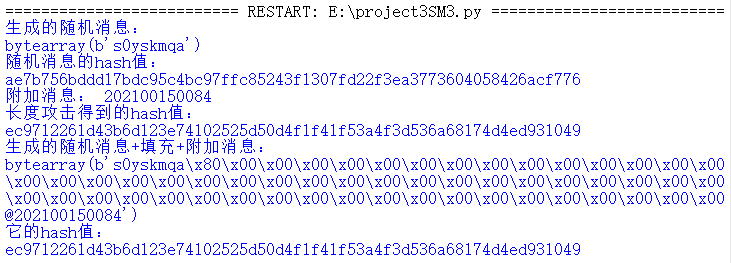
1. 定义len\_attack函数，接受参数m和length，m为原始消息（a）的hash值，length为原始消息的长度。在进行长度扩展攻击时，我们不知道原始消息具体是什么，只知道原始消息的长度，因此我们随意构造相同长度的消息（在这里我们每长度都用‘1’来构造）。
2. 对SM3函数进行改造：增加了两个参数：一个为IV，一个为flag。当flag为0时，按正常SM3计算消息m的hash值；当flag为1时，实际上是实现了从m中截取附加消息x，并利用h，x计算h’。
3. 我们将构造的相同长度的消息进行填充（fill）后，将附加消息'202100150084'拼接到其后面，然后将其传给稍微改造后的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



分工：自己独立完成