**设计思路：**

长度扩展攻击的过程：

设原信息为’test’， 记做变量secret，未知

已知hash(secret)=55e12e91650d2fec56ec74e1d3e4ddbfce2ef3a65890c2a19ecf88a307e76a23，len(secret)=4，

sm3为大端方式，修改第二轮IV为hash(secret),可用于求hash(secret||padding||length||x)

构造任意str使得len(str)==len(secret)，第一轮计算后截断，结果IV修改为hash(secret)的分组，再进行第二轮，即可求得可用于求hash(secret||padding||length||x)

‘test’位数不够扩展后数据为：

’test’+'\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\x00\x00\x00\x00\20’+‘attack’

构造攻击,random变量为’aaa’，扩展数据为：

’aaaa’+'\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\x00\x00\x00\x00\20’+‘attack’

运行结果

