length_extension_attack_for_sm3项目说明

本项目是SM3的长度扩展攻击

代码说明

本项目主要用到了上个项目所实现的SM3的函数接口，并实现了SM3长度扩展攻击的函数接口，其函数原型如下

```
void sm3_len_attk(unsigned char*iv,unsigned char *input,unsigned long long mlen,unsigned long long olen)
```

从左到右的含义依次为需要设置成上一轮结果的数据iv，需要新加密的数据input，新加密数据的长度mlen，原来已经加密过的数据olen。

攻击方法为利用已经知道的哈希值，设置成iv，并根据已知长度设置padding，从而在不知道M1的情况下计算出SM3(M1|padding|M2)。

运行指导

直接运行即可，无需输入，输出为M1的散列值，构造出的M1|padding|M2的散列值，和计算出的M1|padding|M2的散列值。

运行全过程截图

直接运行：

```
SM3(M1)=0xfb6e2ceb514ae8e6a3d4cfc451e89ac91789c7d6c5a8b6fb4a1d643fdaaaffe4
SM3(M1|padding|M2)=0xe7ef6ec1800312cfd9767772fa4c7c108fb0886e26c2a86bad17c9a89cac9b05
利用SM3(M1)和M2计算得0xe7ef6ec1800312cfd9767772fa4c7c108fb0886e26c2a86bad17c9a89cac9b05
```

发现确实可以进行长度扩展攻击。

贡献说明

本组只有一个人