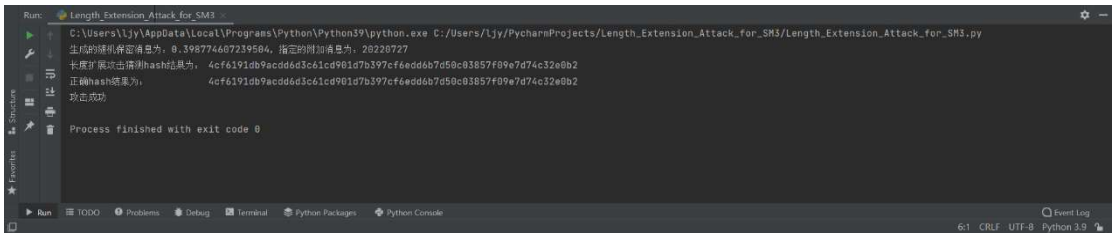
代码说明

首先随机生成一个随机浮点数作为保密信息(secret)，得到保密信息的长度。然后选定一个附加消息(extend_msg)，长度扩展攻击的目标即得到保密消息填充后级联上附加消息的 hash 值。本次实验采取的 hash 函数为 SM3，填充规则为首先填充一个 1，随后填充 0，直到消息长度为 56(或者再加整数倍的 64)字节，最后 8 字节用来填充消息的长度。在实现攻击时，用与 secret 等长的由字符'A'组成的字符串代替 secret 并完成填充，然后级联 extend_msg。这个时候用稍加修改的 extend_sm3_hash 函数完成加密。该函数相较于 sm3 函数的具体修改内容为将 secret 的 64-bit 的 hash 结果拆为 8 个 8-bit 数作为当前的 8 个向量值替代 IV。然后加密从 extend_msg 的第一位开始。最后将长度扩展攻击猜测 hash 结果与正确 hash 结果比较，如果攻击成功二者应该相同。

运行指导

下载项目解压后在 Pycharm 中打开该项目，安装国密库 gmssl，直接运行 Length_Extens ion_Attack_for_SM3.py 文件即可

运行过程截图



成员分工

该项目由廖健有独立完成

参考资料

https://blog.csdn.net/szuaurora/article/details/78125585