1901210488——时绍森

实验结果：



其中：

第一个输入的为密钥，为了获得它填充后的hash值和长度

第二个输入的为append值（具体是什么见作业中设计思路文档），为了进行第二轮加密，后续构成相同的hash值

密钥值和我们输入的与密钥值长度一样的字符串进行长度拓展攻击，两个hash值一样，就可以通过密钥验证，所以表示我们的长度拓展攻击成功。