哈尔滨工业大学（深圳）

《密码学基础》实验报告

Hash 长度扩展攻击实验

学　院: 计算机科学与技术

姓　名: 宗晴

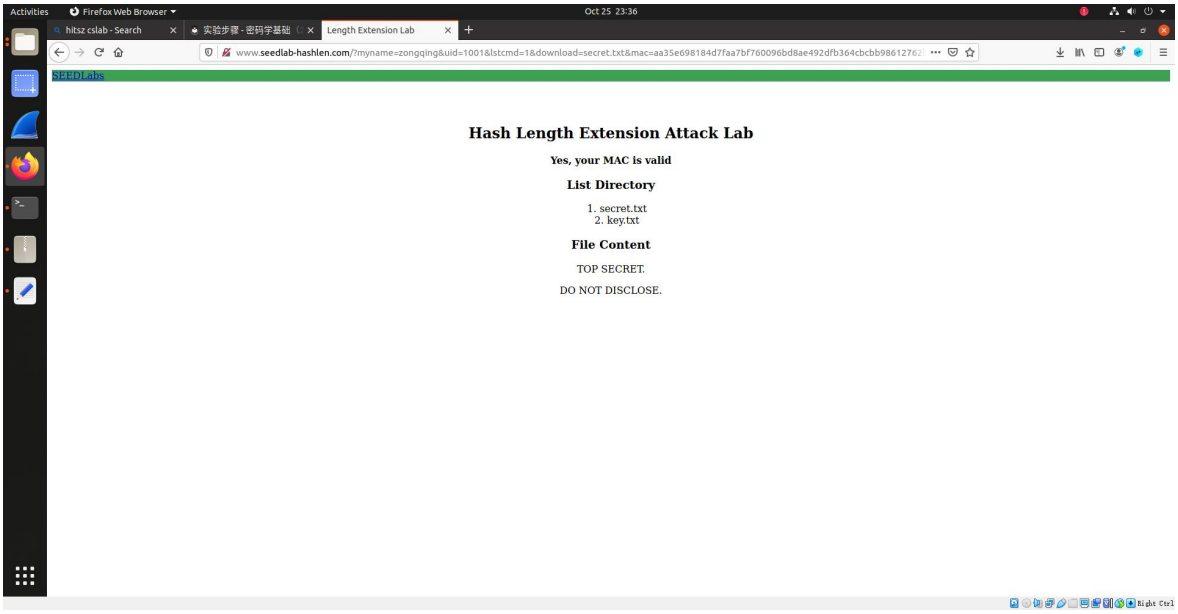
学　号: 200110513

专　业: 计算机科学与技术

日　期: 2022-10-26

1、 请发送一个`download`命令到服务区，myname 的信息修改为你自己的姓名拼音，并且记录你得到的响应内容（截图显示）。

http://www.seedlab-hashlen.com/?myname=zongqing&uid=1001&lstcmd=1&download=secret.txt&mac=aa35e698184d7faa7bf760096bd8ae492dfb364cbcbb98612762ba02cd39e9d6



2、 为消息<key>:myname=<name>&uid=<uid>&lstcmd=1 创建对应 padding，其中`<key>`和`<uid>`的实际内容应该从`LabHome/key.txt`文件中得到，myname 依然用你自己的姓名。

结果类似这样，红色部分可以参考代码换成 AAAAAA，不影响填充的内容：

```
123456:myname=SEEDManual&uid=1001&lstcmd=1
%80%00%00%00%00%00%00%00%00%00%00%00%00%00%00%00%00%00%00%00%01%50
```

padding 的结果如下：

123456:myname=zongiqing&uid=1001&lstcmd=1%80%00%00%00%00%00%00%00%00%00%00%00%00%00%00%00%00%00%00%00%01%48

3、 为下面的请求生成一个有效的 MAC，其中`<key>`和`<uid>`的实际内容应该从`LabHome/key.txt`文件中得到，name 就是自己的姓名拼音。

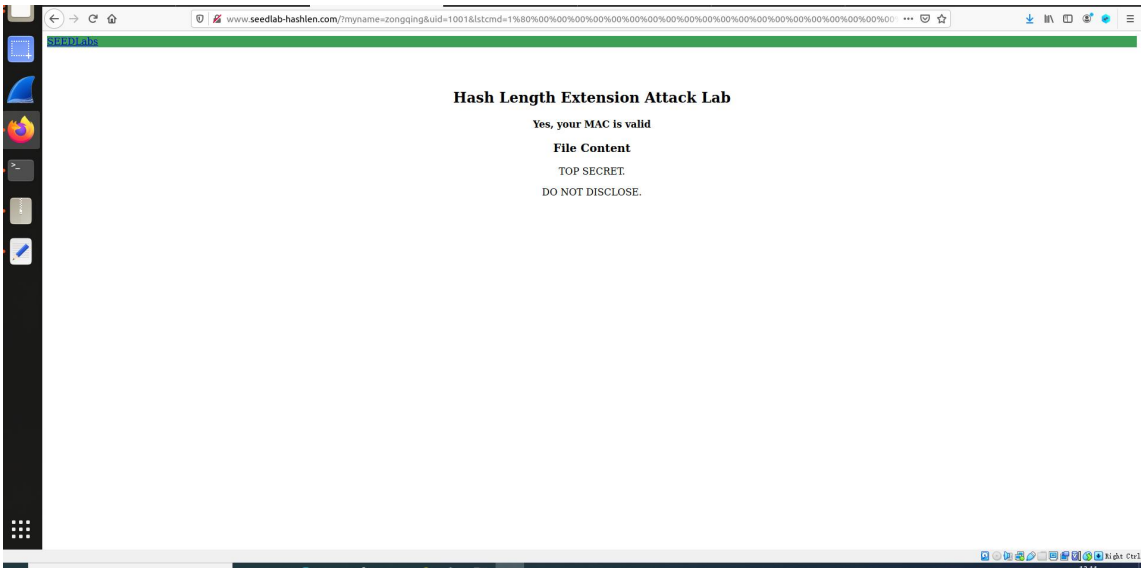
http://www.seedlab-hashlen.com/?myname=<name>&uid=<uid>&lstcmd=1&mac=<mac>

http://www.seedlab-hashlen.com/?myname=zongqing&uid=1001&lstcmd=1&mac=d2d18aeff4e163c3b6d676d0690eeeda042902c951be494072fc03d4a3292b05

4、 发送构造好的新请求到服务器，padding 是上面获取到的信息，记录收到的服务器响应并截图。

http://www.seedlab-hashlen.com/?myname=<name>&uid=<uid>&lstcmd=1<padding>&download=secret.txt&mac=<new-mac>

http://www.seedlab-hashlen.com/?myname=zongqing&uid=1001&lstcmd=1%80%00%00%00%00%00%00%00%00%00%00%00%00%00%00%00%00%00%00%00%00%00%00%00%01%40&download=secret.txt&mac=cfcc71ea457d00a0b9c603ac61688b7a8dfa543e78d0ec7031620228def2754c

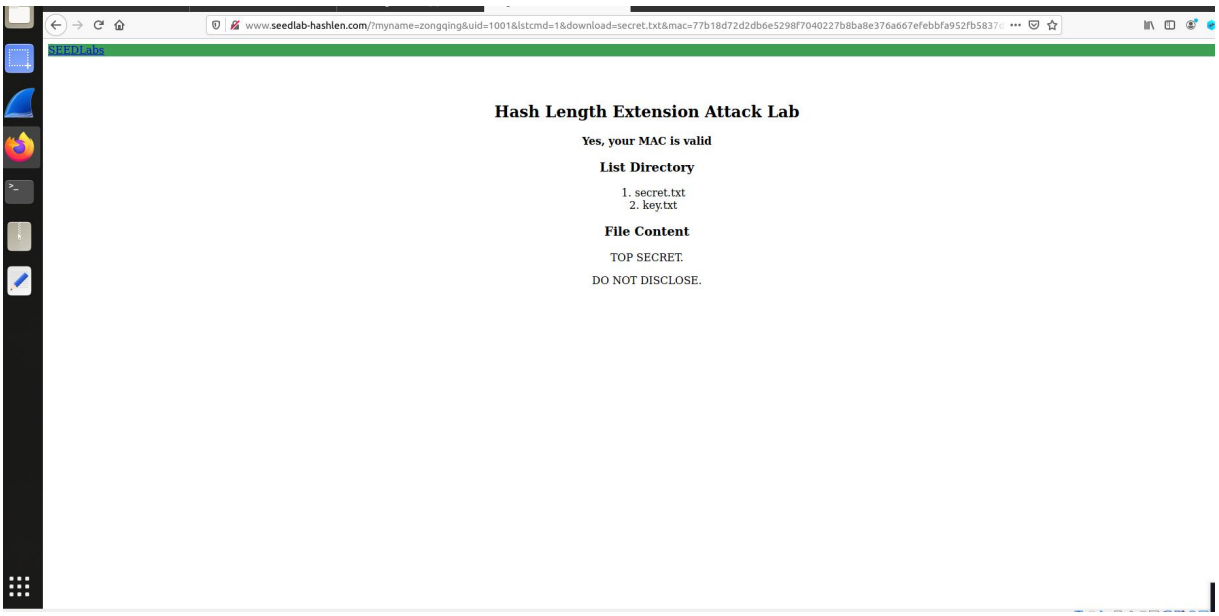


5、 用 HMAC 算法修改代码后，记录使用长度攻击的结果，根据收到的服务器响应进行截图。

替换为 HMAC 算法后，按照任务一的流程，求出 mac 及完整请求如下：

http://www.seedlab-hashlen.com/?myname=zongqing&uid=1001&lstcmd=1&download=secret.txt&mac=77b18d72d2db6e5298f7040227b8ba8e376a667efebbfa952fb5837d12c7319c

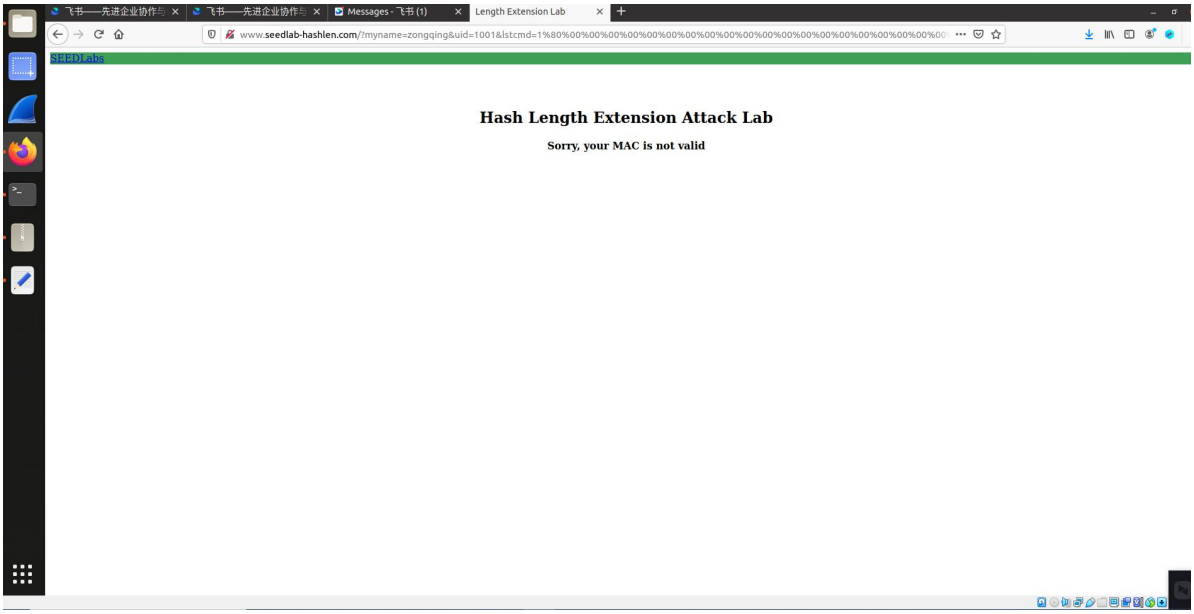
访问网页成功：



填充后的请求为：

http://www.seedlab-hashlen.com/?myname=zongqing&uid=1001&lstcmd=1%80%00%00%00%00%00%00%00%00%00%00%00%00%00%00%00%00%00%00%00%00%00%00%00%00%00%00%01%40&download=secret.txt&mac=7aa1d74ff387dcdf94c466cec9547a42097f4ae14f6412d62e3aafdf07b8fc24

访问网页失败：



分析：HMAC 使用两轮散列而 MAC 只使用了一轮散列，由于 HMAC 进行了双重摘要，因此密钥不再受长度扩展攻击的影响。