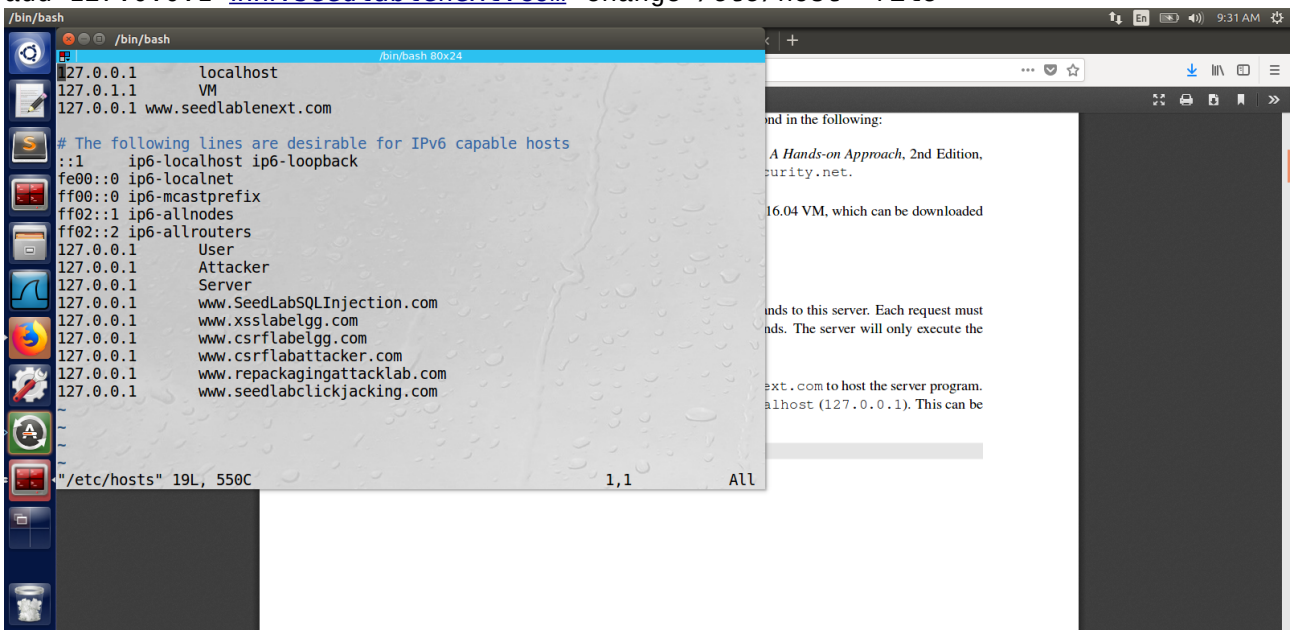
PES1201800410 sem V A R PRASHANTH

LAB 5

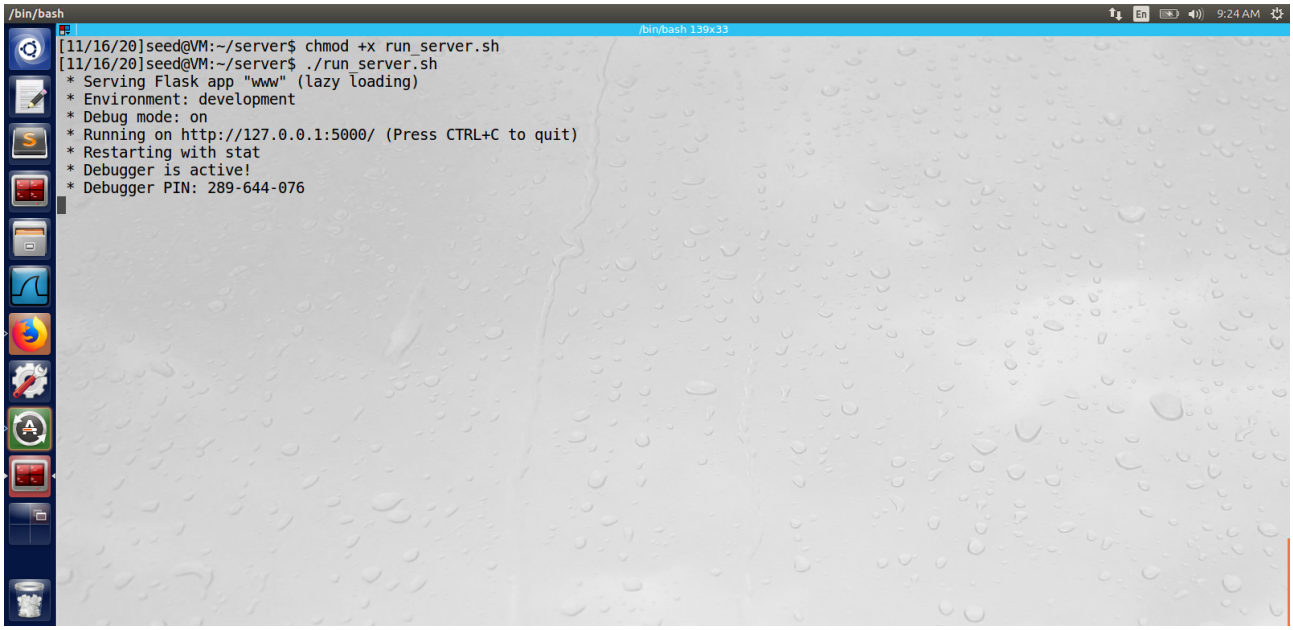
Hash Length Extension Attack Lab

Task 1

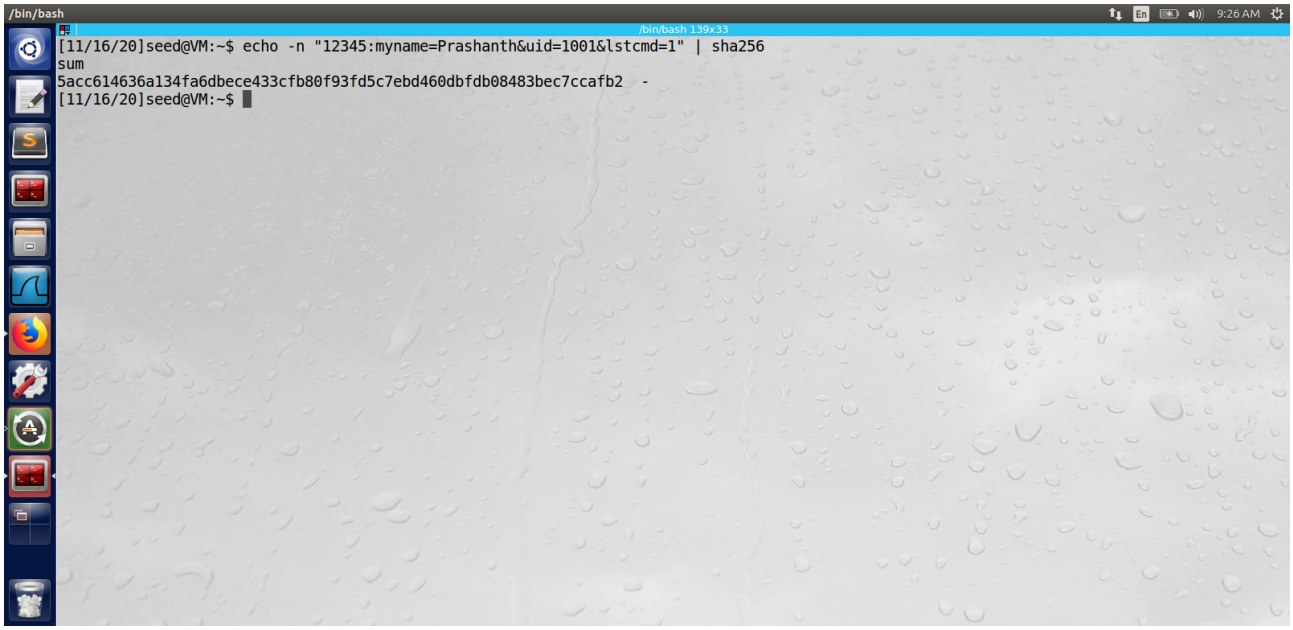
add 127.0.0.1 www.seedlablenext.com change */etc/*host file



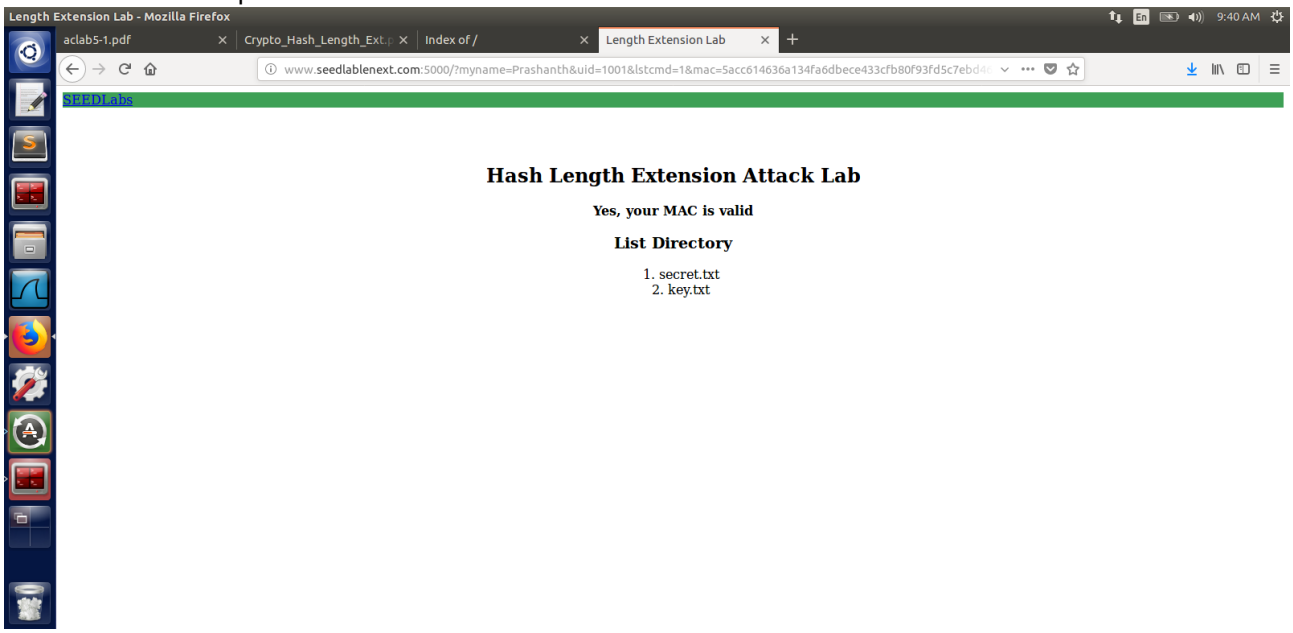
run the server



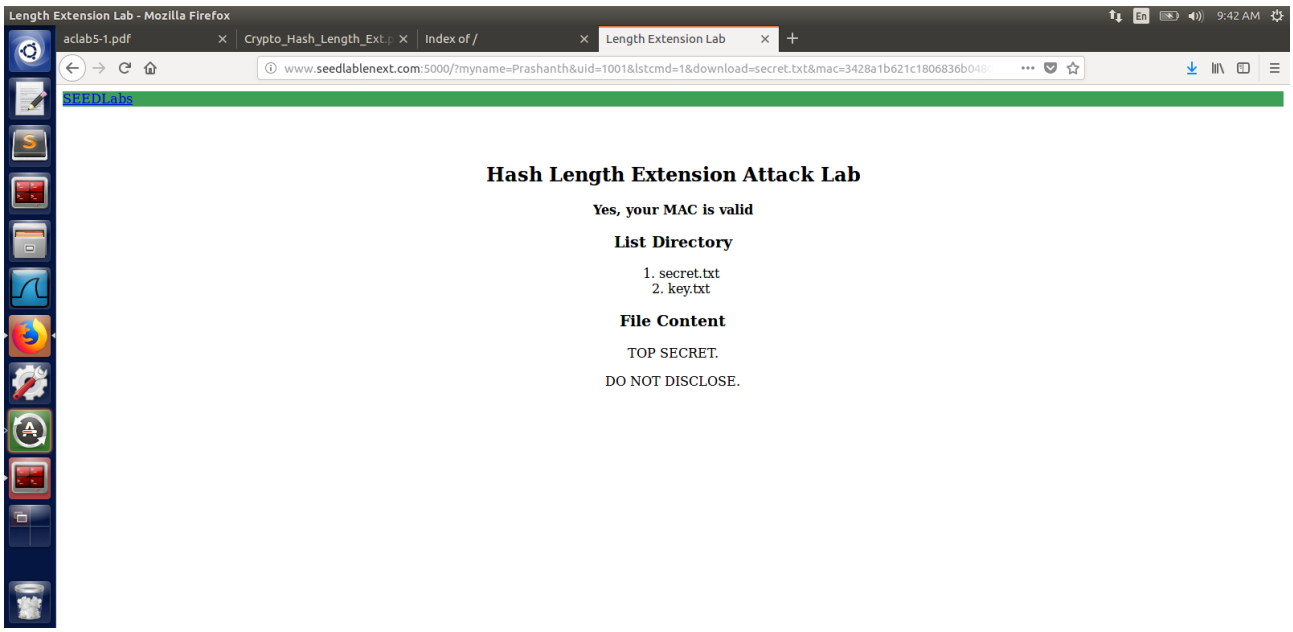
create mac



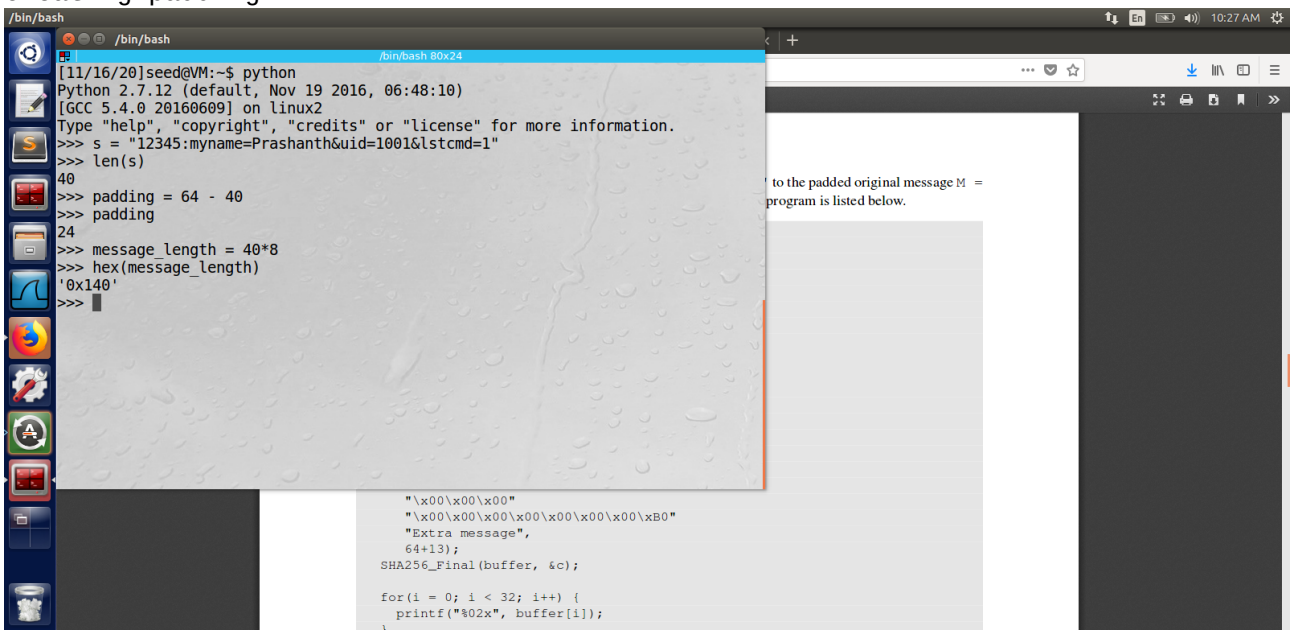
web browser request



mac for download=secret.txt

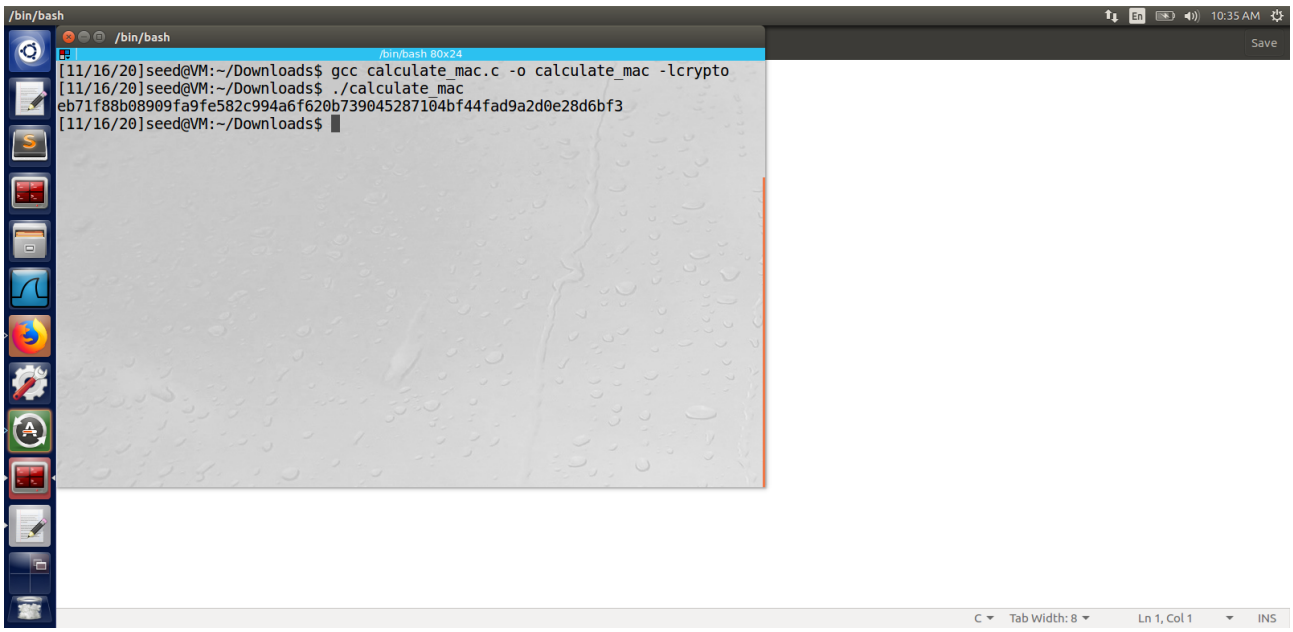


creating padding

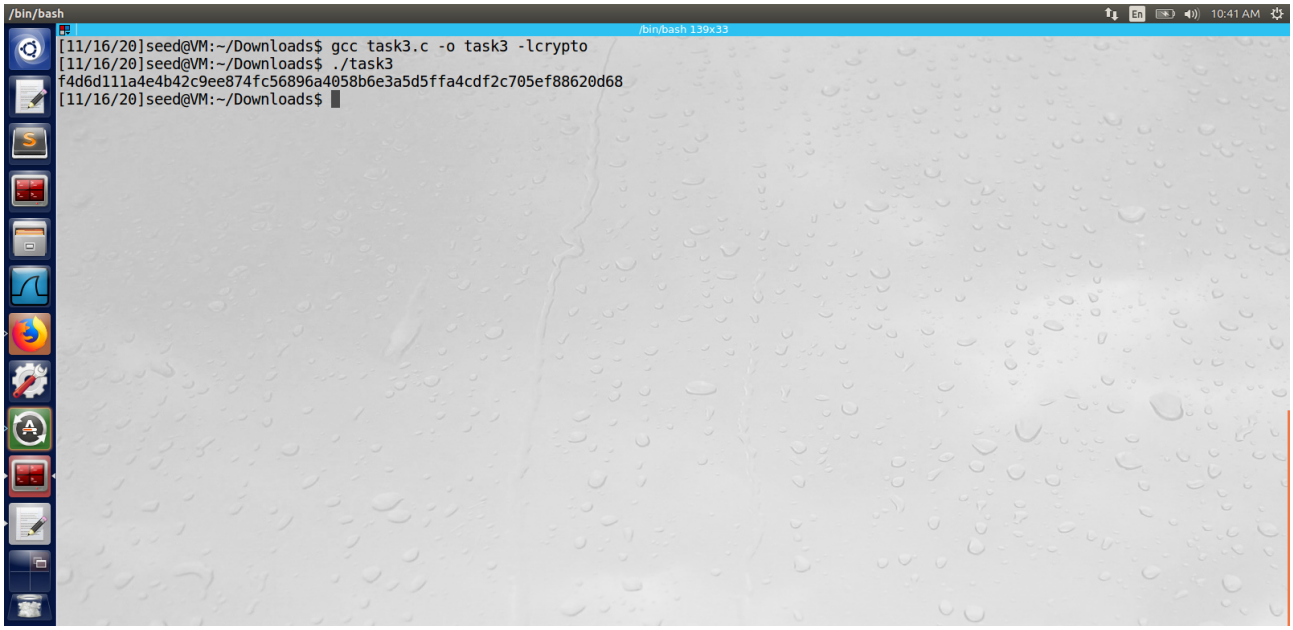


we can see we need 0x140 is the message lenght and
24 size of padding is required.

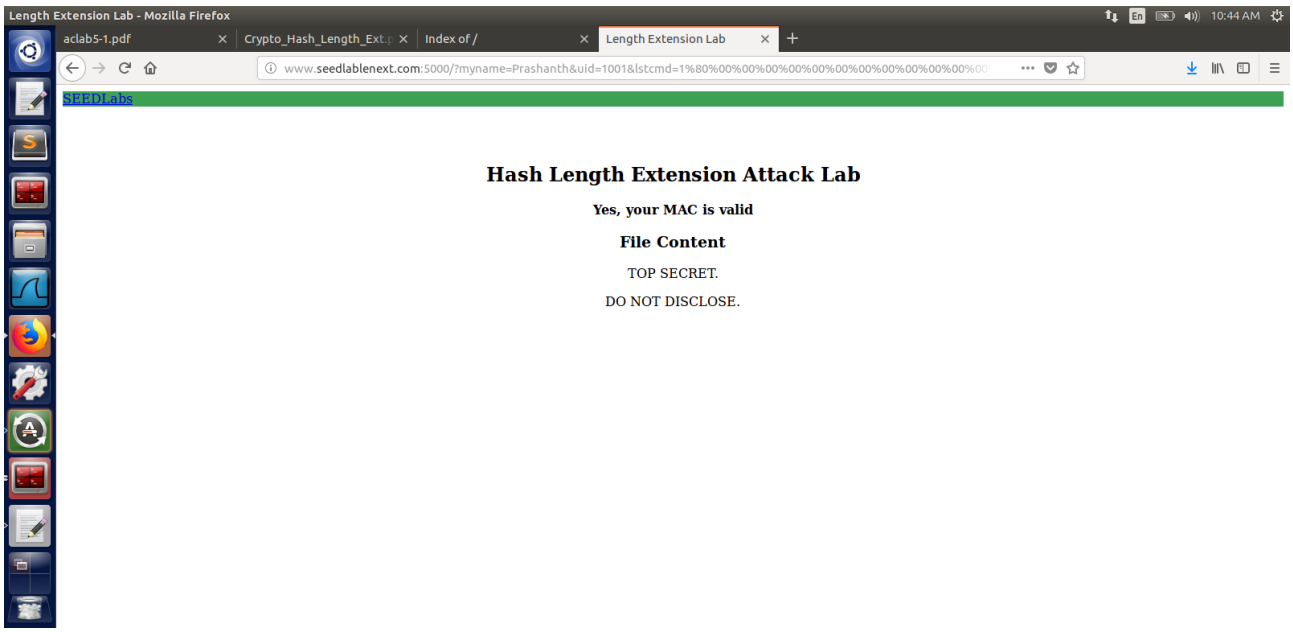
run calculate_mac



modify the file to create our mac
we get



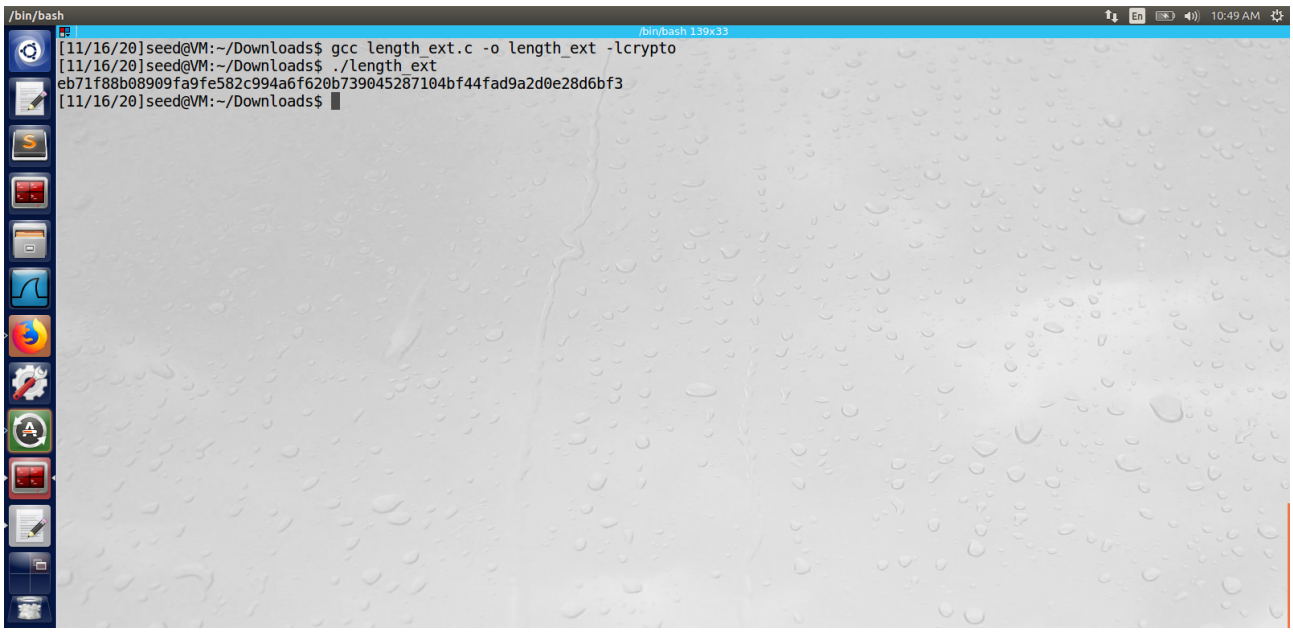
in browser



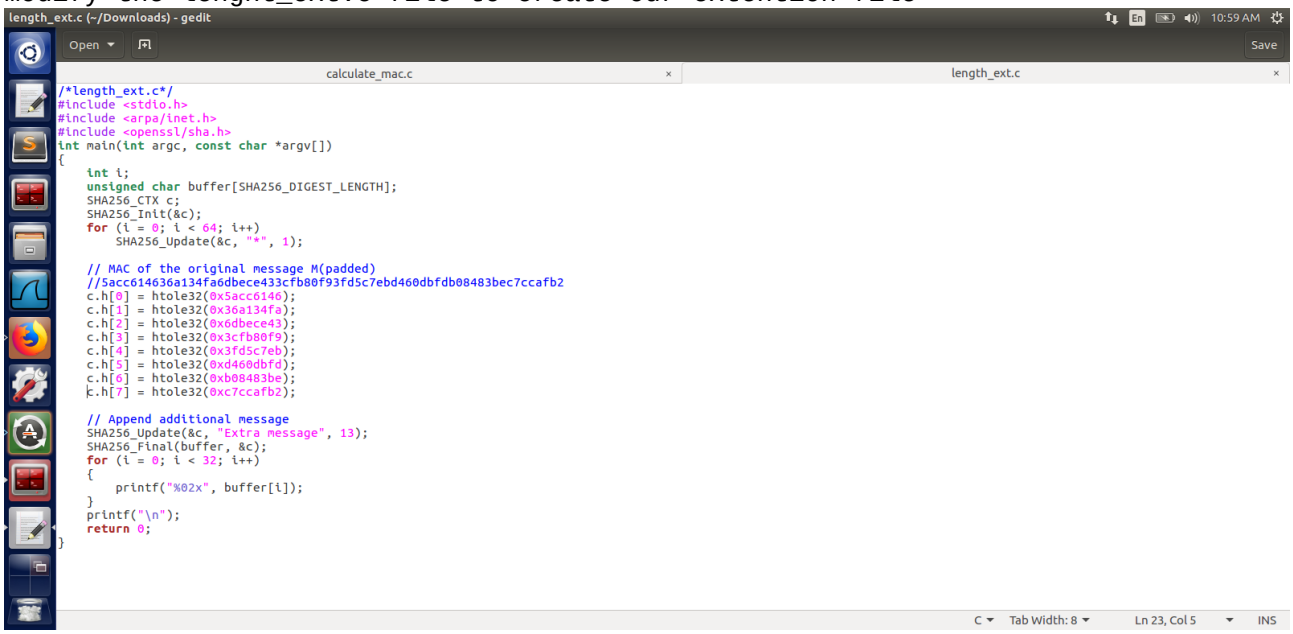
Task4: The lenght extenstion Attack

check sha256sum for “This is a test message”

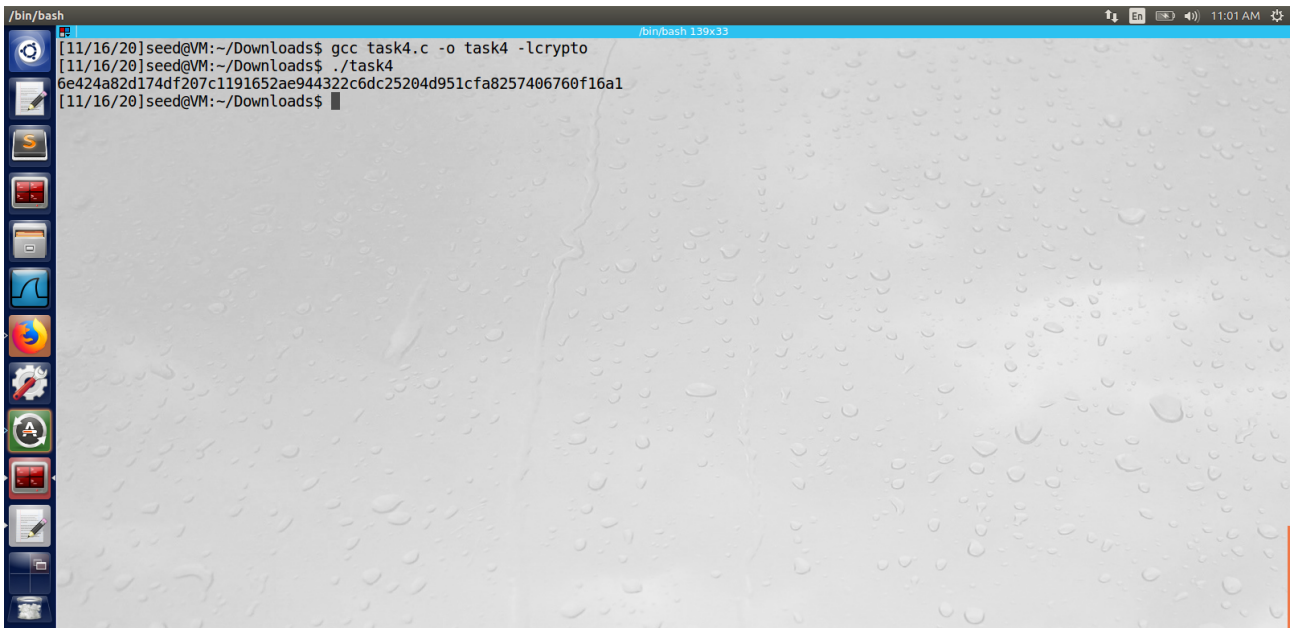
complie and execute the lenght_ext.c file



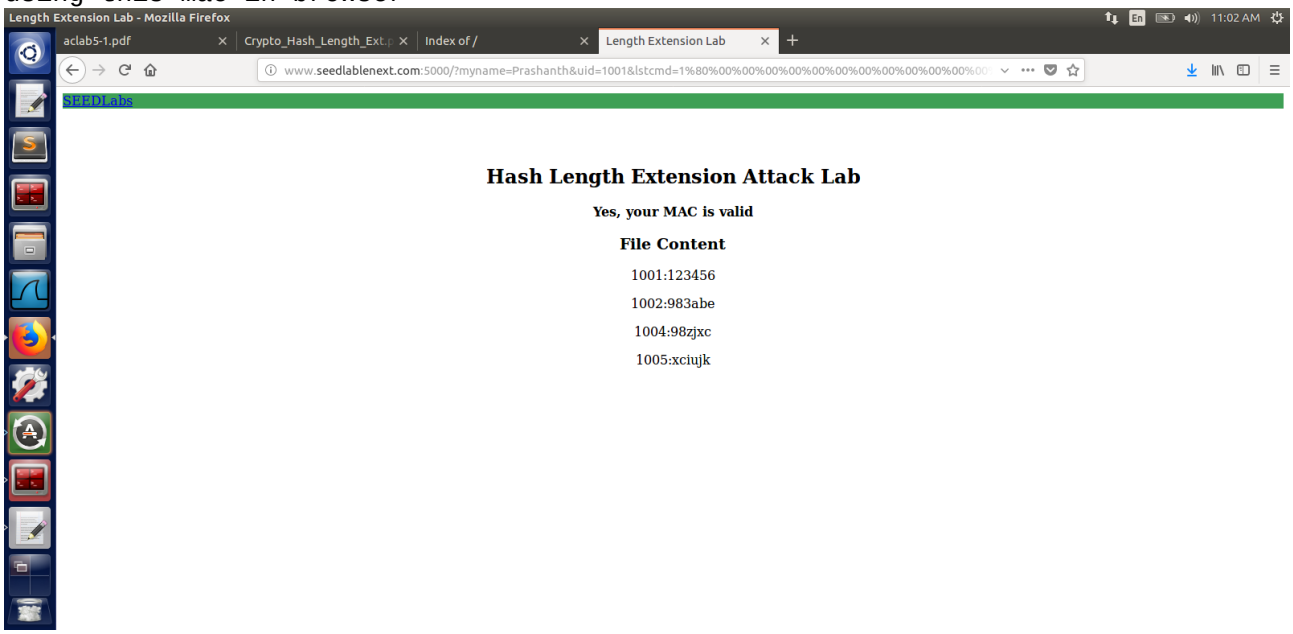
modify the lenght_ext.c file to create our extention file



complie and exceute

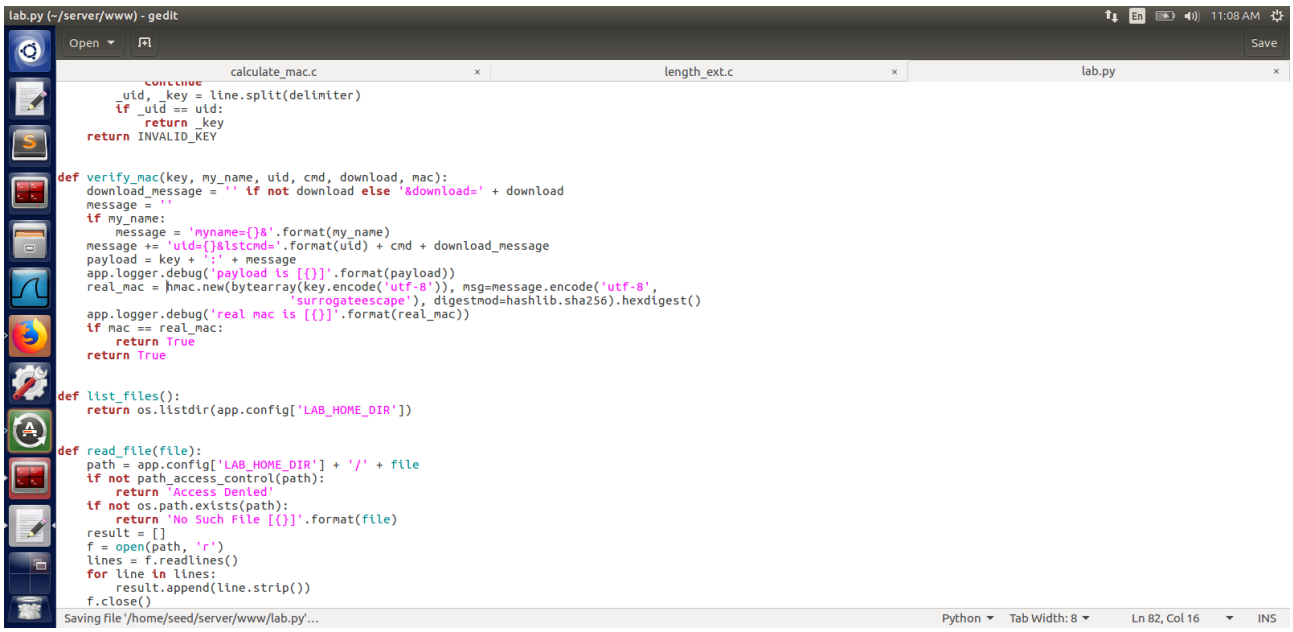


using this mac in browser

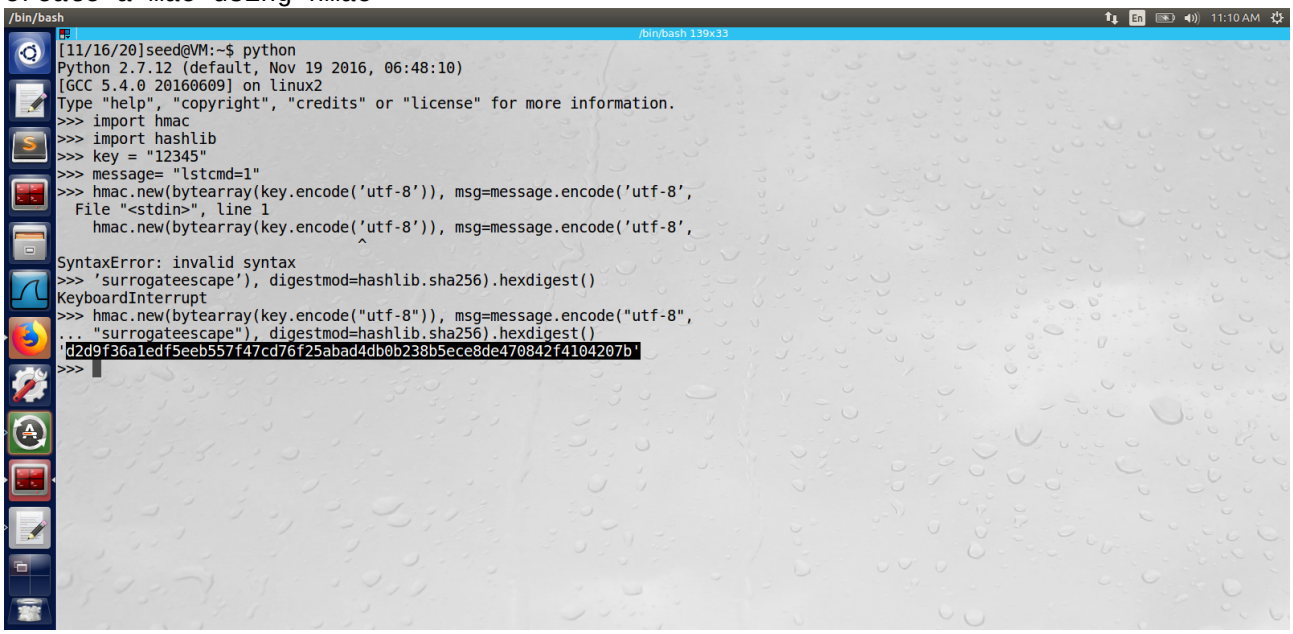


Task5 Attack Mitigation using HMAC

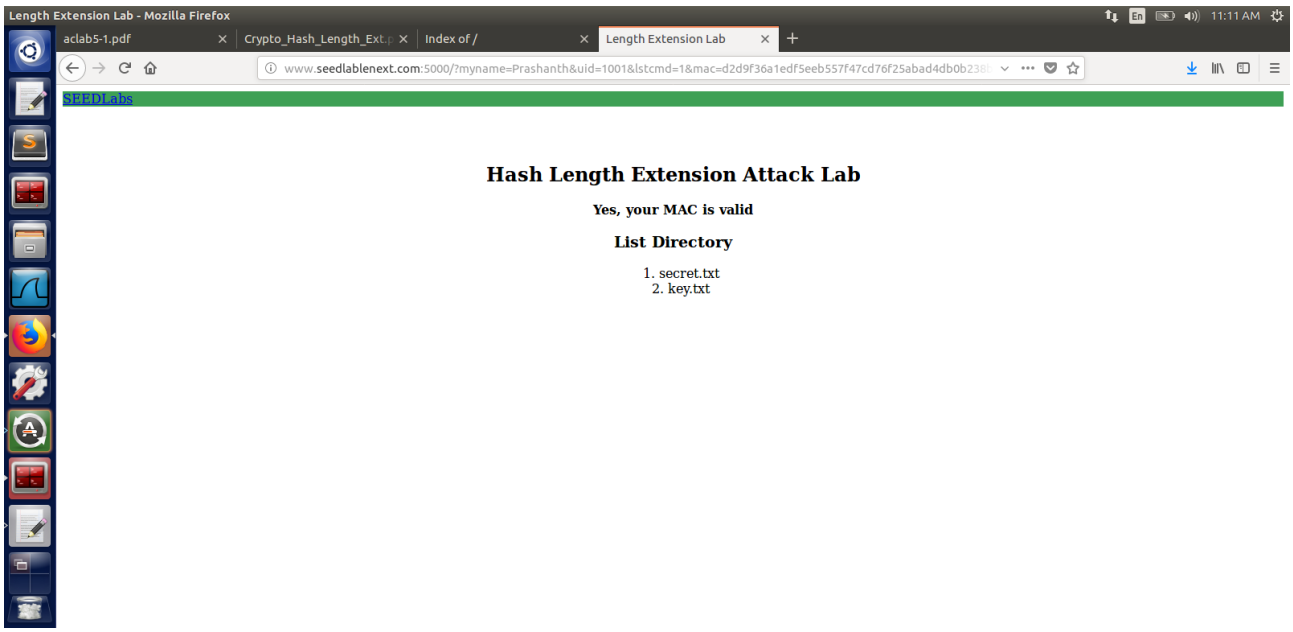
changing sha256 to hmac ... in source file



create a mac using hmac



using the mac in browser


Length Extension Lab - Mozilla Firefox
11:11 AM
aclab5-1.pdf
Crypto_Hash_Length_Ext
Index of /
Length Extension Lab
www.seedlablenext.com:5000/?myname=Prashanth&uid=1001&lstcmd=1&mac=d2d9f36a1edf5eeb557f47cd76f25abad4db0b238
SEEDLabs
Hash Length Extension Attack Lab
Yes, your MAC is valid
List Directory
1. secret.txt
2. key.txt