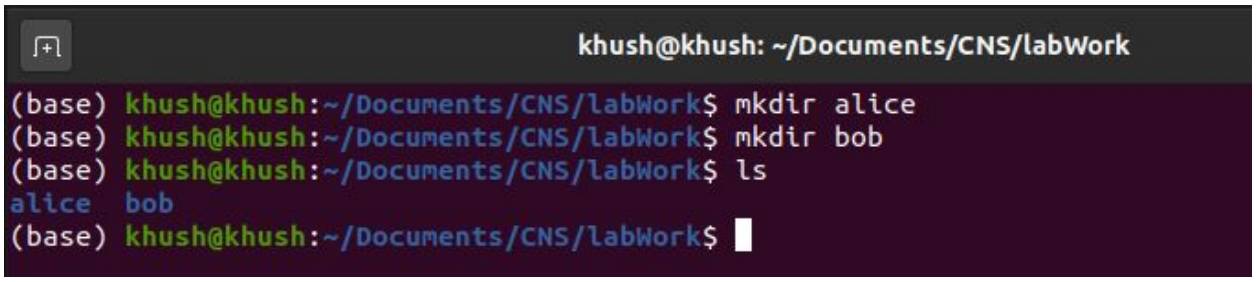
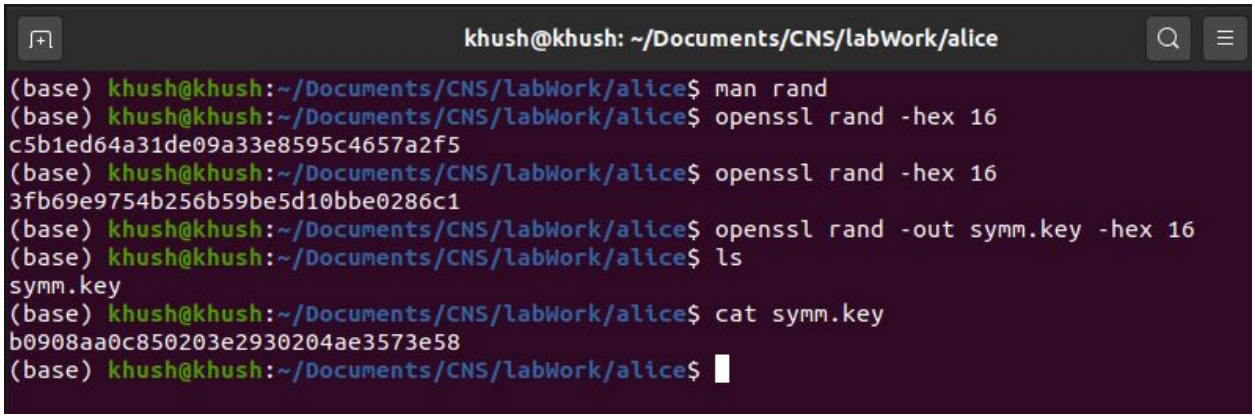
openSSL Assignment
1851: Khushboo Shetkar

Creating the directories

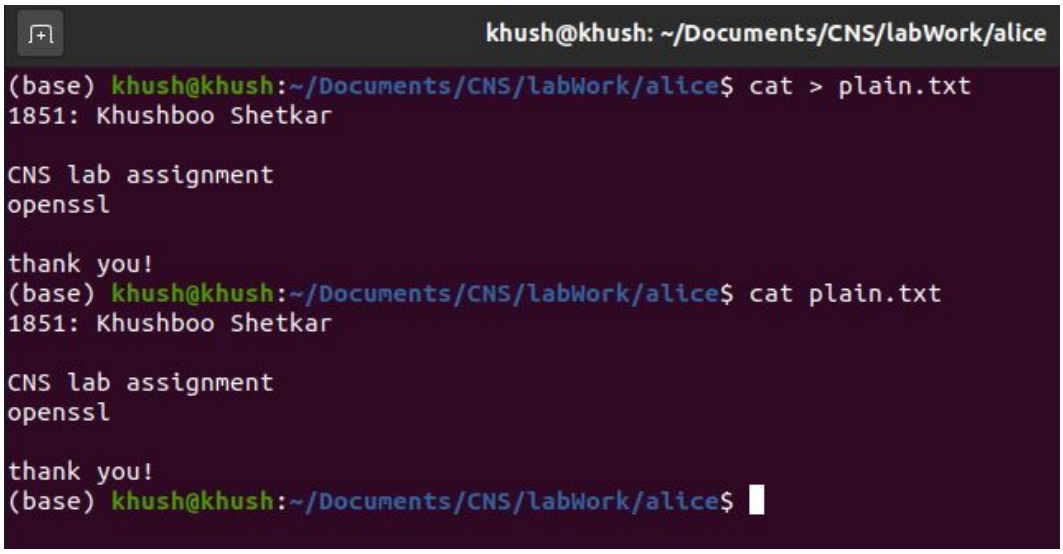


Confidentiality

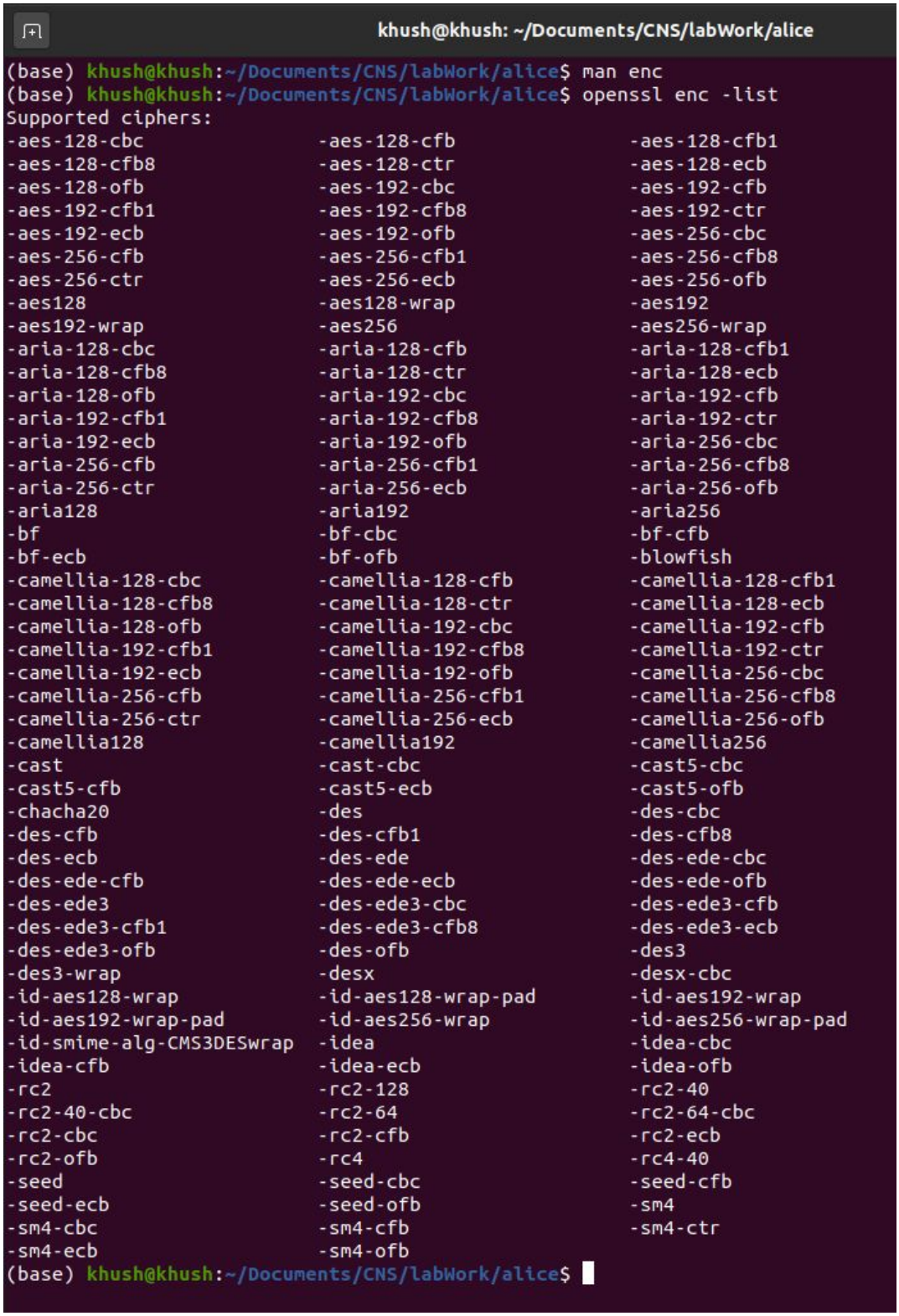
1. Creating a random key of size 128 bits (stored in symm.key)

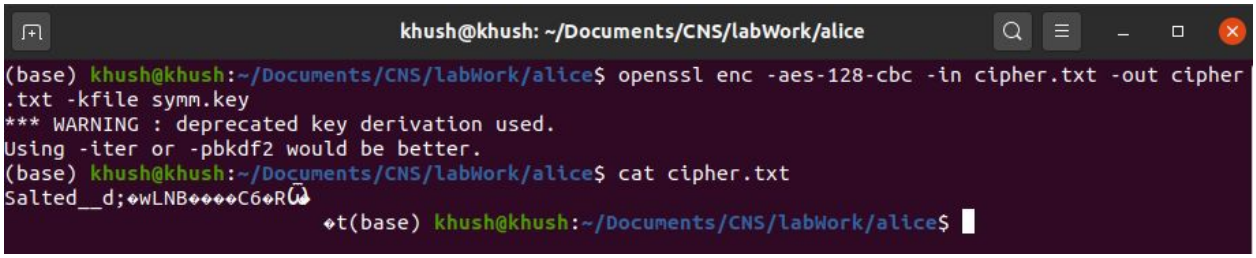


2. Creating a file with dummy data (plain.txt)

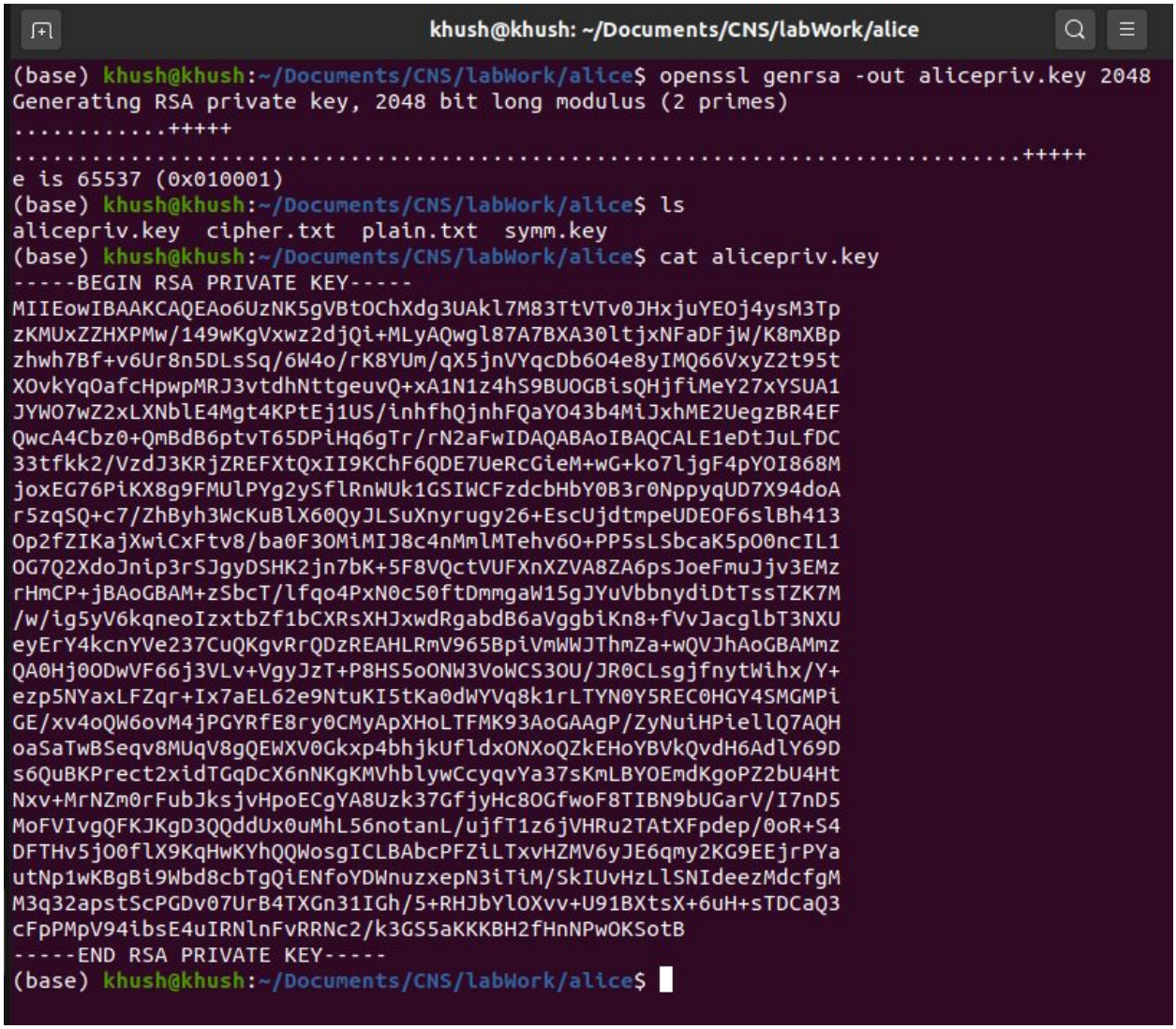


3. Encrypting the contents of plain.txt to cipher.txt using AES-128 algorithm in CBC mode, using symm.key

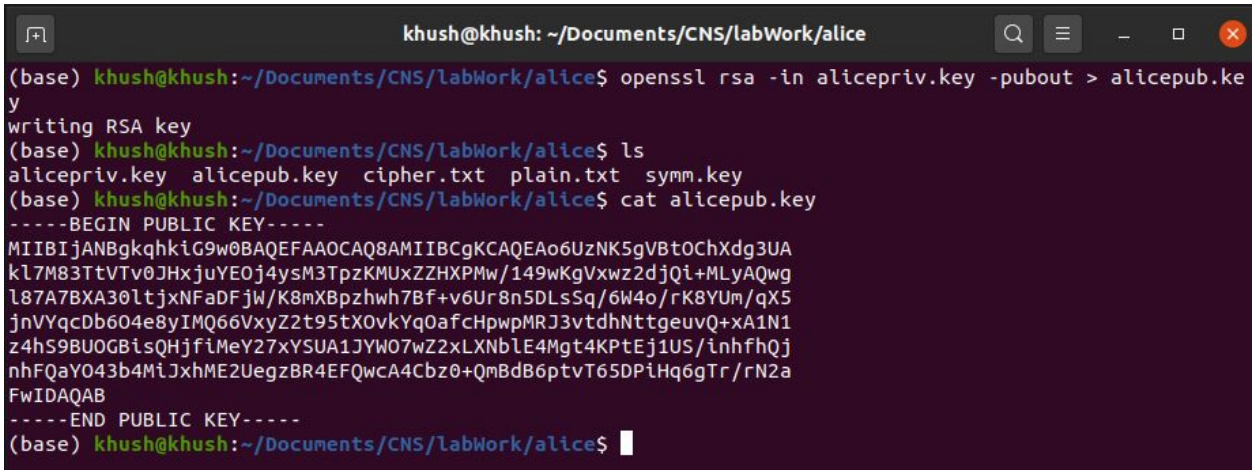




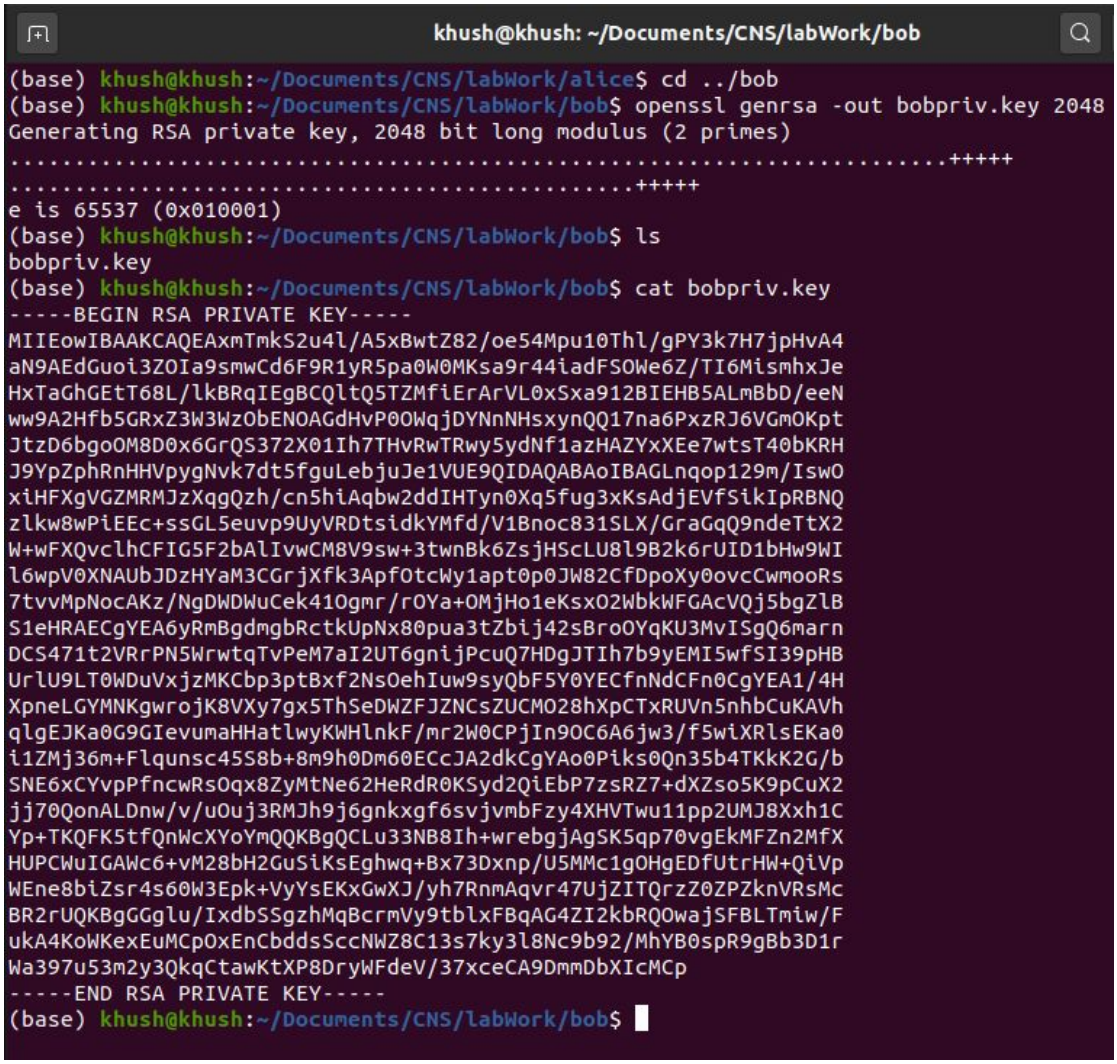
4. Creating a 2048 bit RSA private key (stored in alicepriv.key)

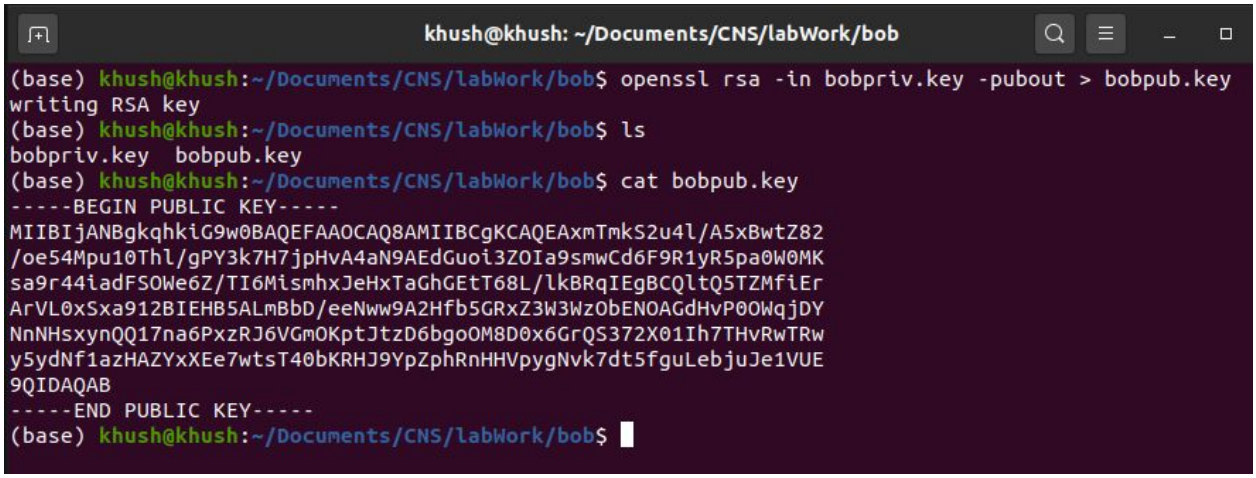


5. Extracting the public key from alicepriv.key and storing in file alicepub.key

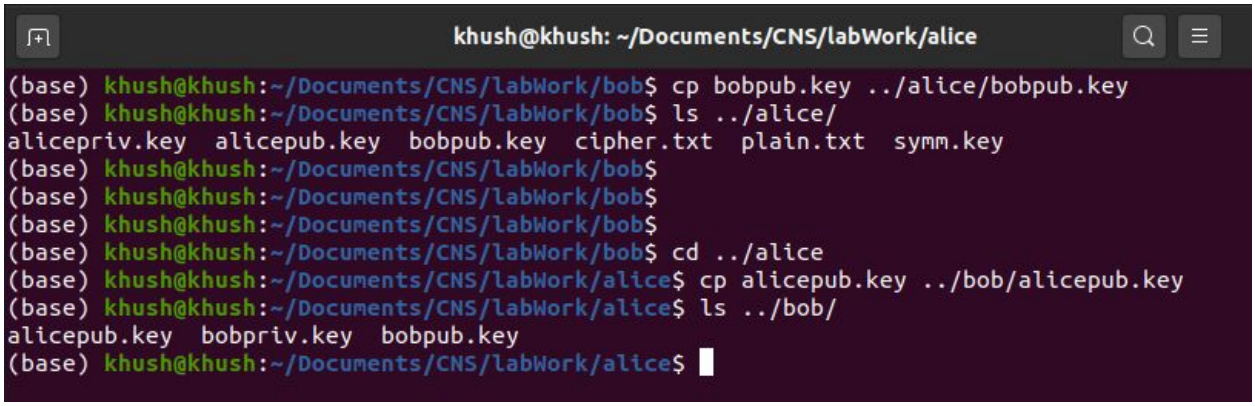


6. Repeating steps 4 and 5 for Bob (bobpriv.key and bobpub.key)

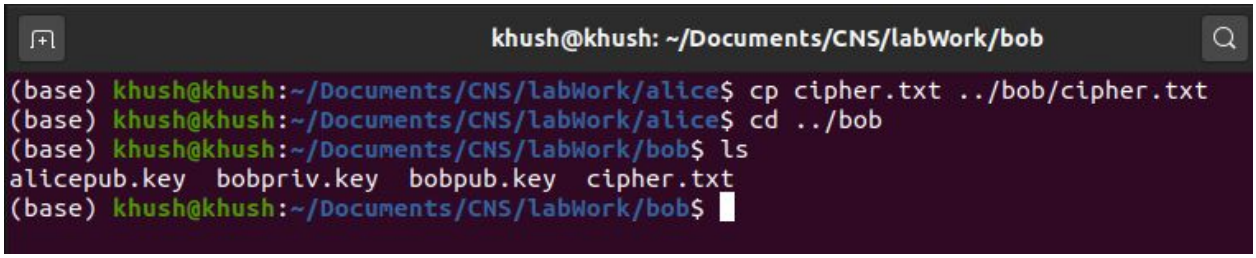




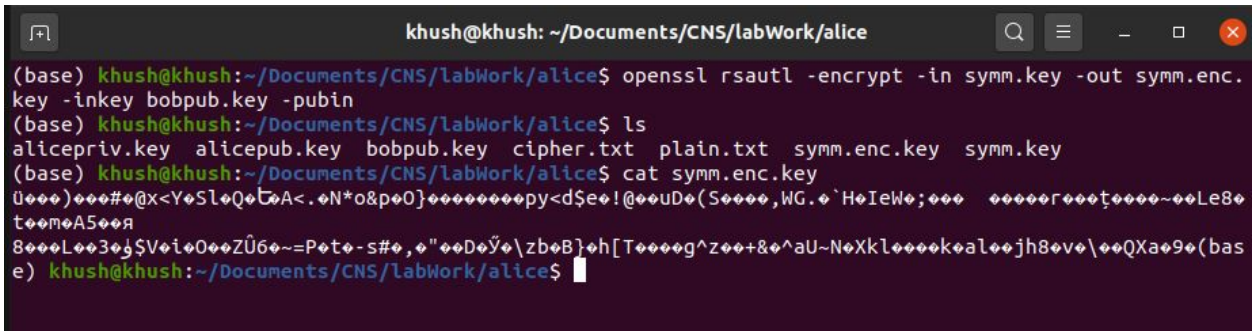
Alice and Bob exchange their public keys



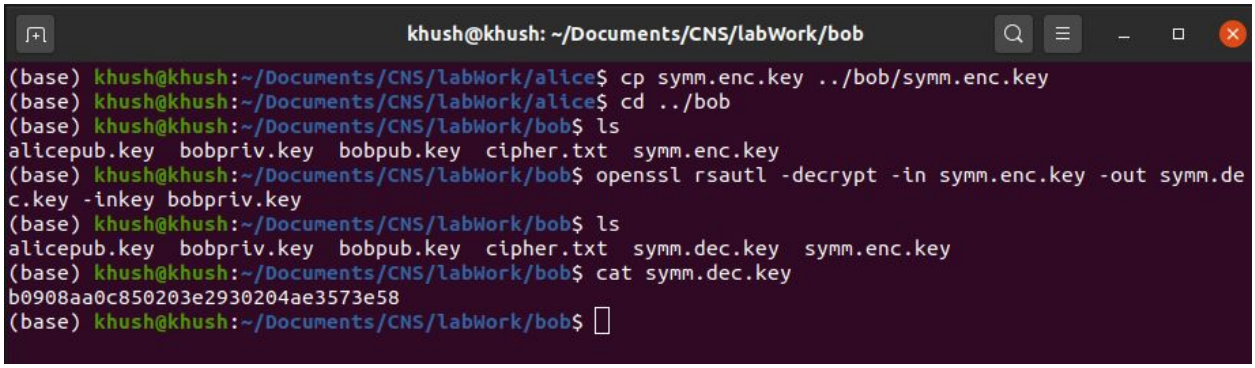
7. Alice sends cipher.txt to Bob



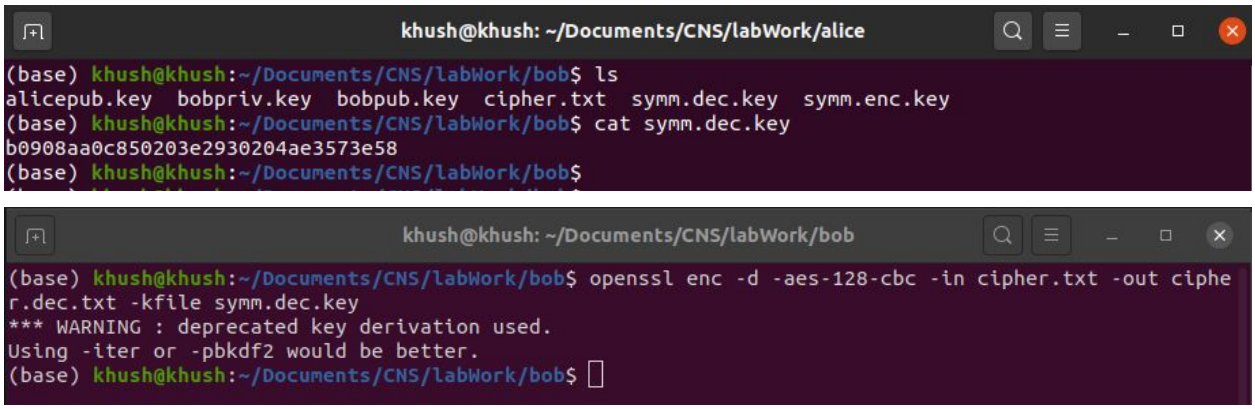
8. Alice encrypts symm.key using the public key of Bob (stored in symm.enc.key)

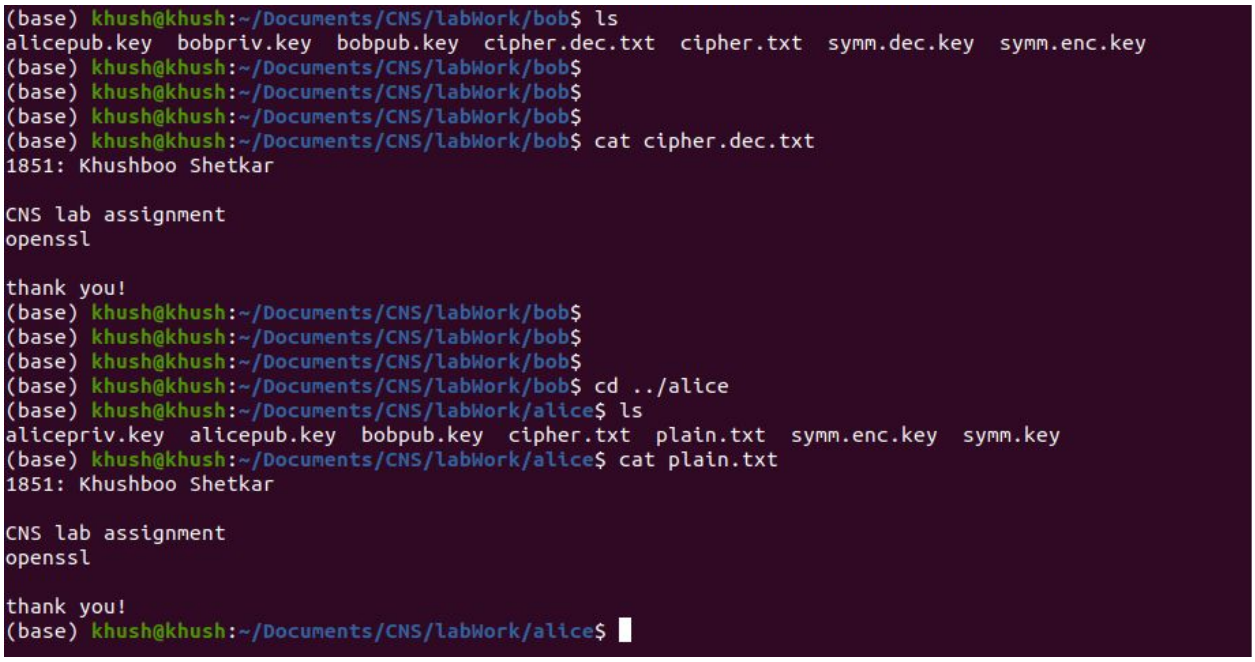


9. Bob decrypts symm.enc.key using his private key and stores the output in symm.dec.key



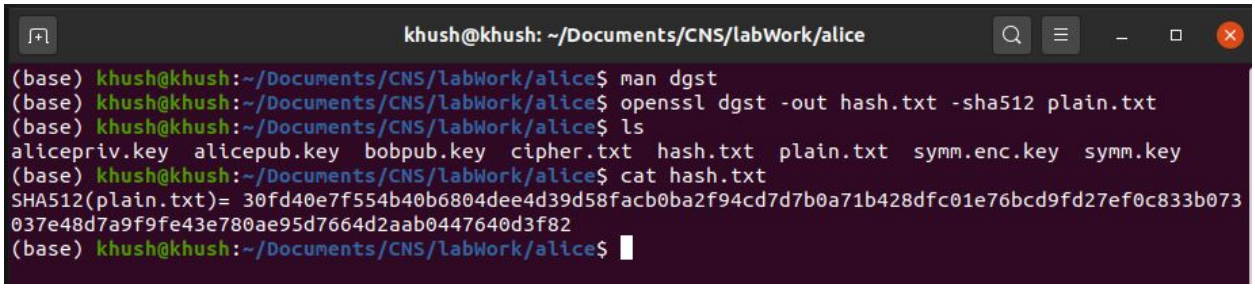
10. Bob decrypts cipher.txt using symm.dec.key and stores the output in cipher.dec.txt. The cipher.dec.txt and plain.txt has same contents.



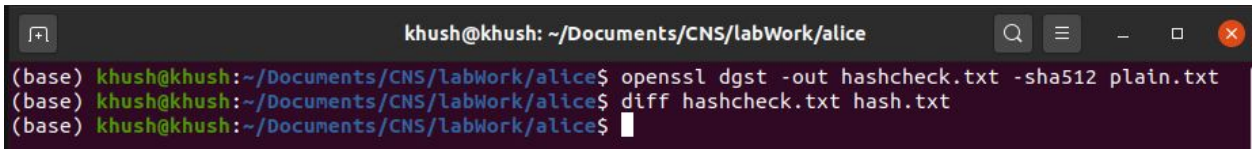


Integrity Check

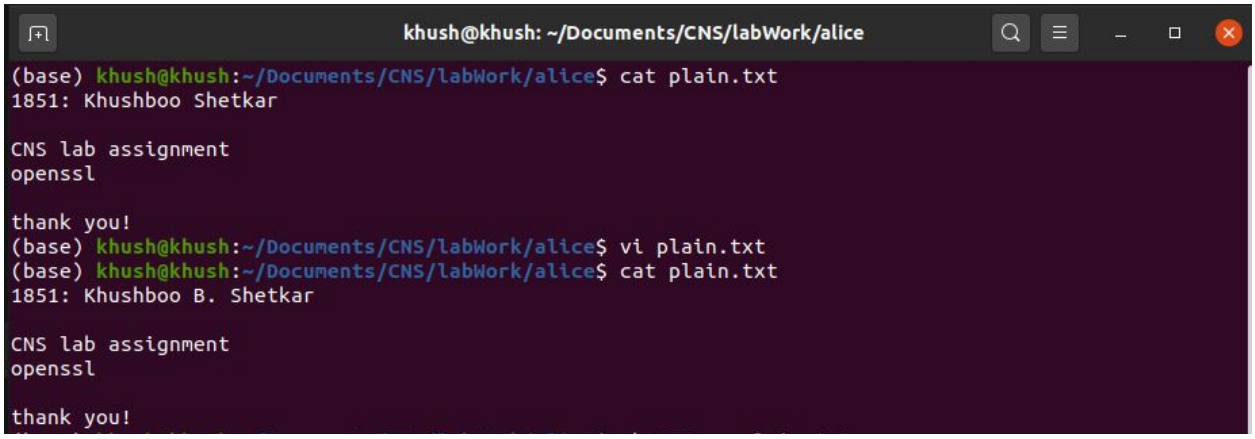
11. Compute sha-512 hash on plain.txt and store in hash.txt.

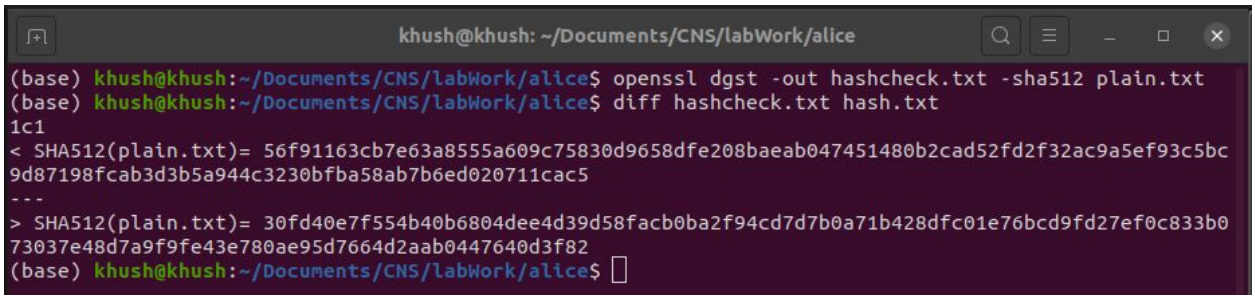


12. Verifying the hash



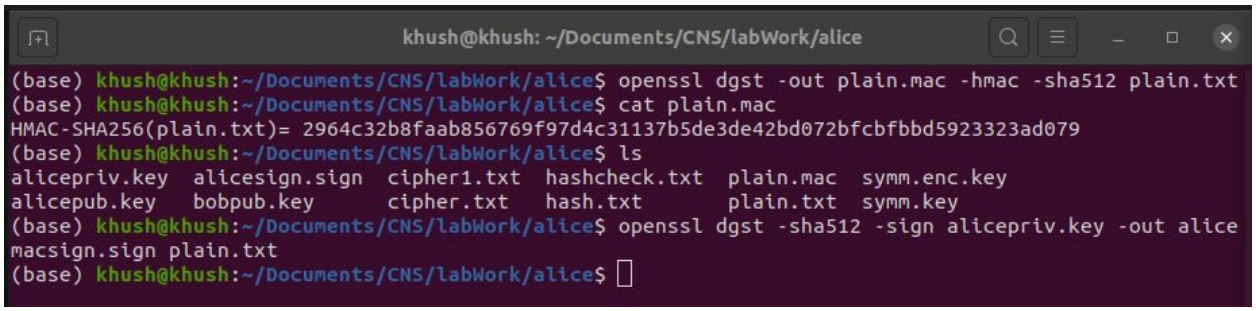
13. Making some change in plain.txt to see the verification fail



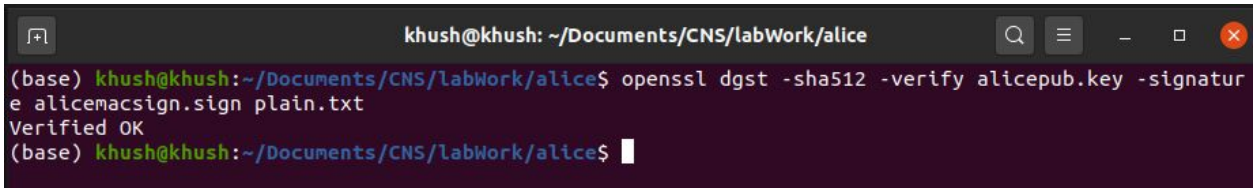


Authentication Check

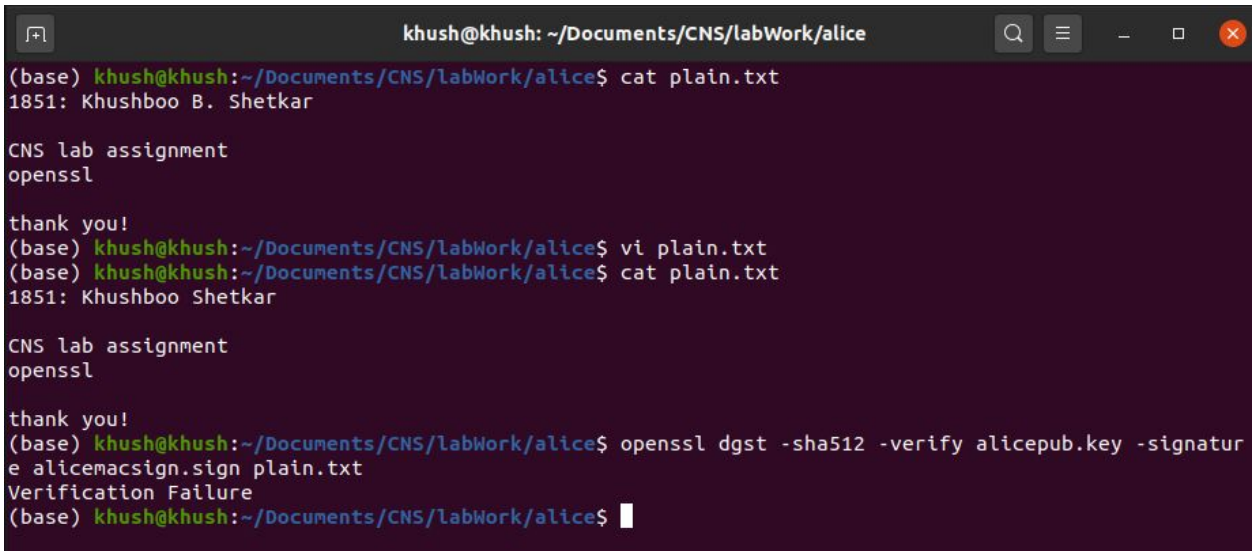
14. Computing MAC on plain.txt using sha-512 and store in plain.mac



15. Verifying the MAC

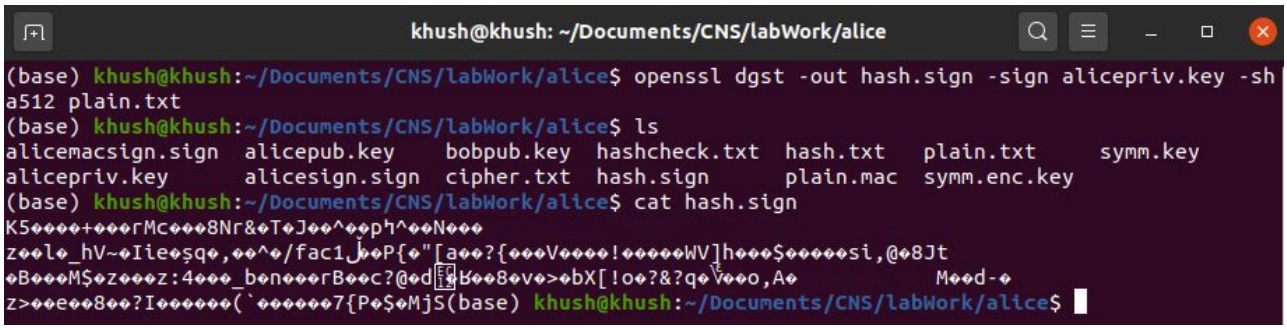


16. Making some change in plain.txt to see the verification fail

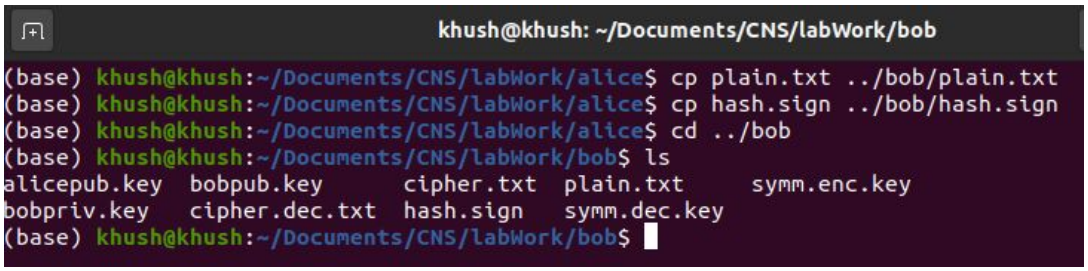


Digital Signature

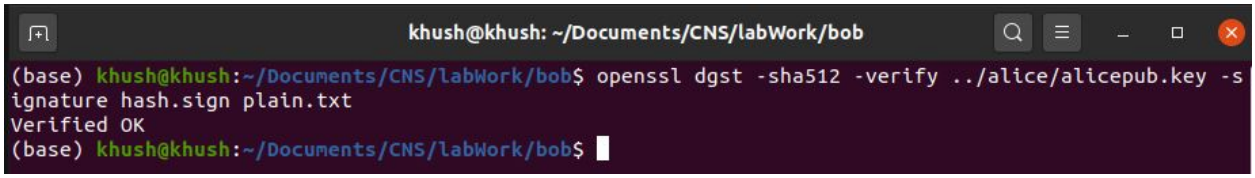
17. Alice creates sha-512 hash on plain.txt and signs it using her private key. Store signed hash in file hash.sign



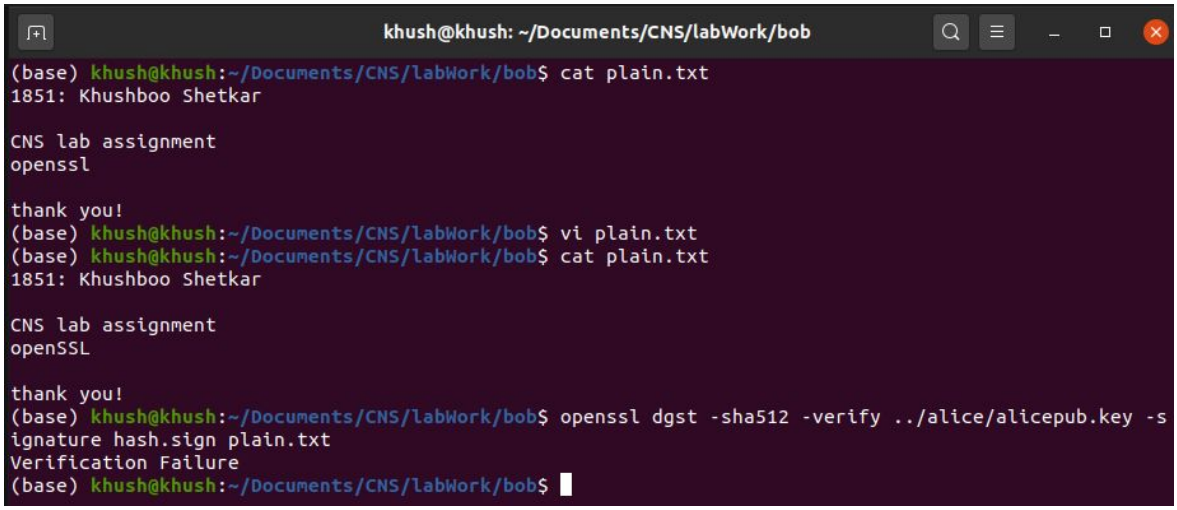
18. Alice sends plain.txt and hash.sign to Bob



19. Bob verifies the signature using the public key of Alice



20. Check that the verification fails if the file plain.txt is modified


khush@khush: ~/Documents/CNS/labWork/bob
(base) khush@khush:~/Documents/CNS/labWork/bob$ cat plain.txt
1851: Khushboo Shetkar
CNS lab assignment
openssl
thank you!
(base) khush@khush:~/Documents/CNS/labWork/bob$ vi plain.txt
(base) khush@khush:~/Documents/CNS/labWork/bob$ cat plain.txt
1851: Khushboo Shetkar
CNS lab assignment
openSSL
thank you!
(base) khush@khush:~/Documents/CNS/labWork/bob$ openssl dgst -sha512 -verify ../alice/alicepub.key -s
ignature hash.sign plain.txt
Verification Failure
(base) khush@khush:~/Documents/CNS/labWork/bob$