

Secret-Key Encryption 2

Candidate Name: Alizeh Jafri

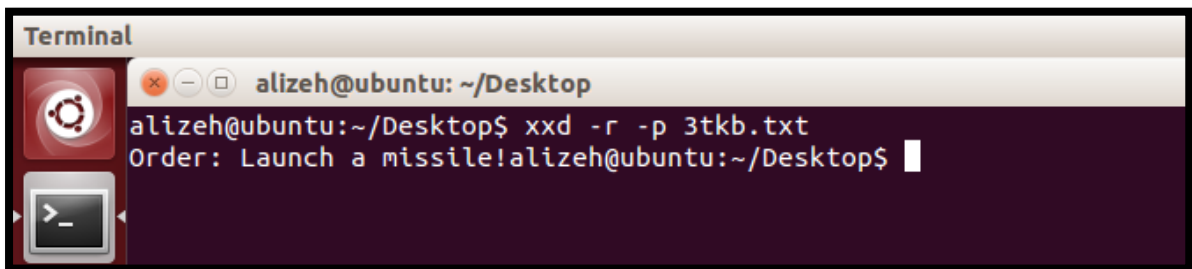
Introduction

The purpose of this lab to get familiar with the concepts of the secret-key encryption. After finishing the lab, we should be able to gain a first-hand experience on encryption algorithms, encryption modes, paddings, and initial vector (IV).

Task 1

Steps that were followed to perform this task:

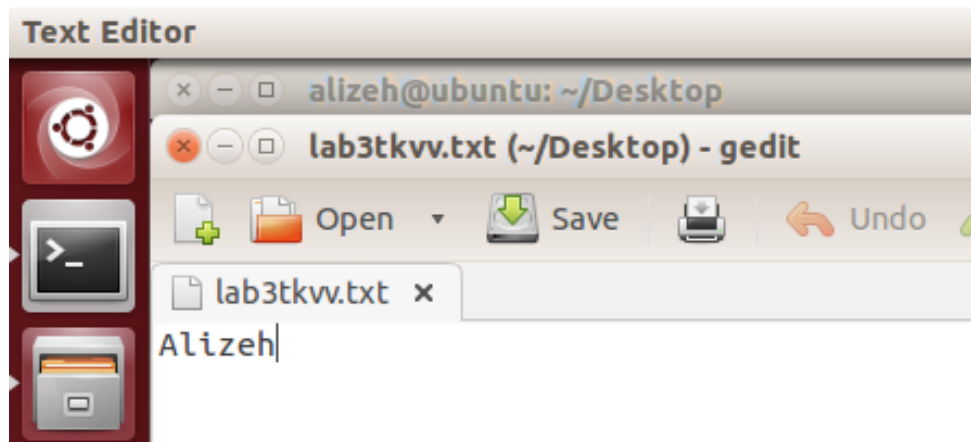
- 1) A file named '3tk3.txt' was created and the message in P1 was converted from plain text to hex.
- 2) After converting P1 to Hex, XOR was performed with C1 which gave is the IV
- 3) Next, that IV was XORed against C2 to obtain P2:
4F726465723A204C61756E63682061206D697373696C6521
- 4) Another text file '3tkb.txt' was created and P2 was copied
- 5) Finally, P2 in the file name '3tkb.txt' was converted from **hex to text** using the hex to text command '**xxd -r -p 3tkb.txt**'
- 6) The screen shot of the content of P2 is shown below:



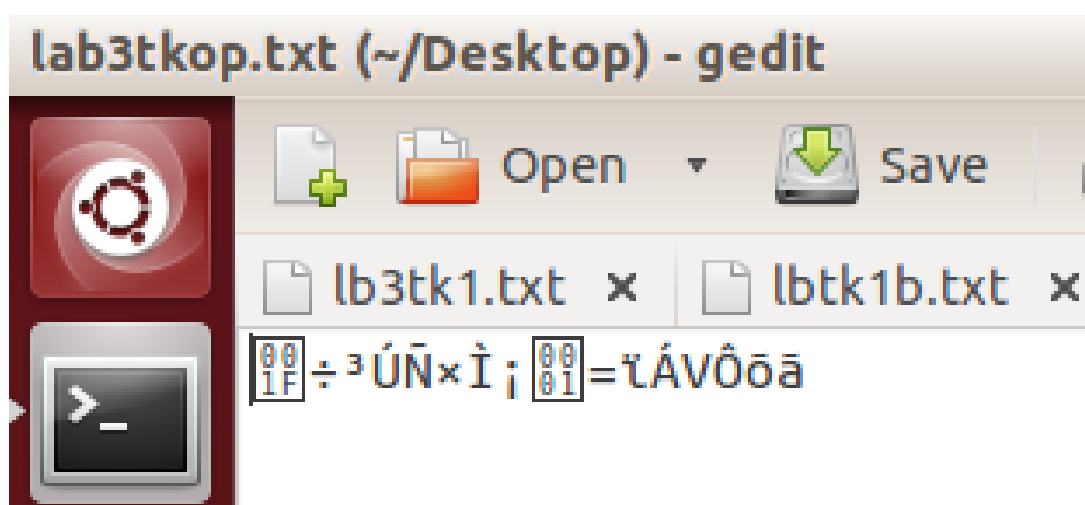
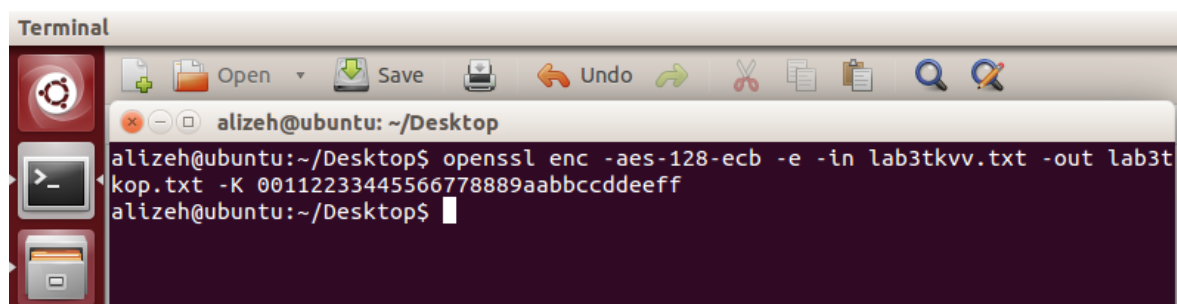
```
Terminal
alizerh@ubuntu: ~/Desktop
alizerh@ubuntu:~/Desktop$ xxd -r -p 3tkb.txt
Order: Launch a missile!alizerh@ubuntu:~/Desktop$
```

Task 2

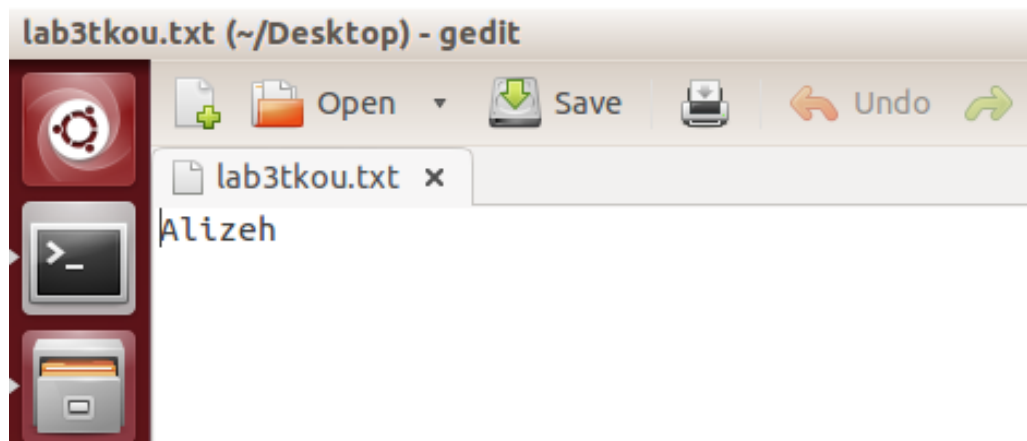
In this task, the focus is on the padding schemes. Firstly a file name 'lab3tkvv.txt' was created which is 7 bytes as shown below:



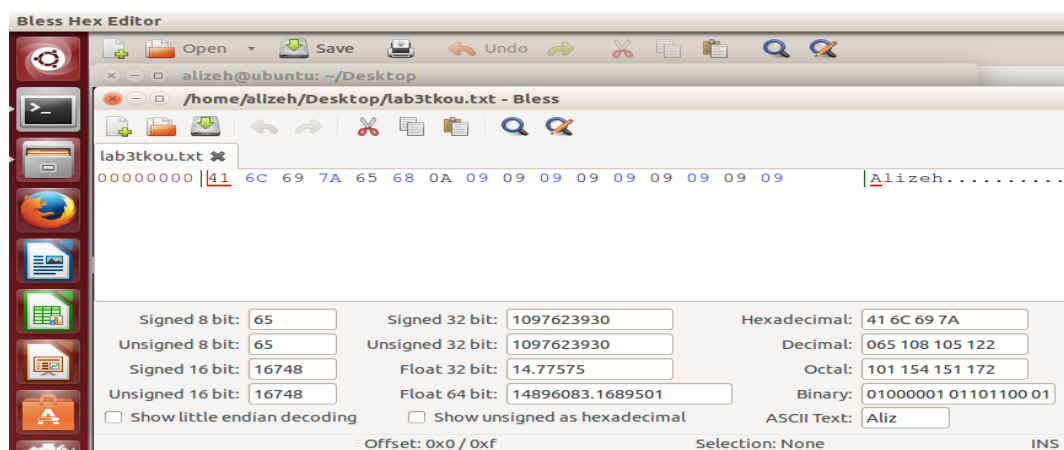
Next, the file 'lab3tkvv.txt' was encrypted using ECB mode to give the file 'lab3tkop' as an output as shown in the screen shot below:



Then the file 'lab3tkop' was decrypted:



The command 'no pad' was used and the Bless Hex editor was used to see the appending as shown below:



This experiment shows that openssl are using PKCS5 for padding. Since in ECB mode the input is in integral no. of blocks, padding should be done to confirm that. PKCS5 is for padding as it adds a minimum of 1 byte. Therefore OpenSSL will append the minimum number of bytes which are required to reach the next multiple of the size of a block. So, if blocks have the size of 'n' then padding will also be between 1 and 'n' extra bytes (to make it 16 bytes) as in AES us 16-byte blocks are used.