**Lab2**

1. **Lab Requirements**

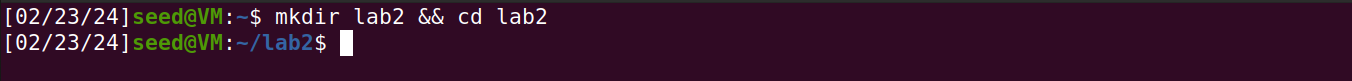


Figure 1: Create new directory and access to it

**Task 1: Monoalphabetic Substitution Cipher A screenshot of a computer error

Description automatically generated**

Figure 3: The content of challenge05.txt

A screenshot of a computer screen

Description automatically generated

**Figure 4: Analytics of the appearance per characters**

**Guesswork to find the key string and replace the keyA computer screen shot of random lines

Description automatically generated with medium confidence**

**A computer screen shot of text

Description automatically generated**

**Figure 5: The content of decrypted challenge05.txt message**

* **Key String: abcdefghijklmnopqrstuvwxyz**
* **Replace By: AOZYGQJBIHCUKDNFMRLTXWVSEP**

**Task 2: Encryption using Different Ciphers and Modes**

**A screenshot of a computer code

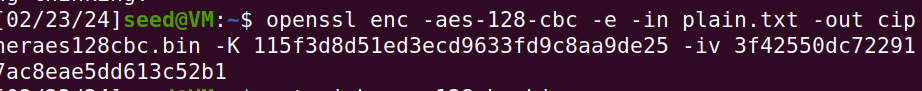
Description automatically generated**

**Figure 6: Creating the file .txt**

To use openssl enc, I need to generate a specific key hex string to use as the KEY, and another as the IV (initialization vector), both of which are 32-bit:

**key = '115f3d8d51ed3ecd9633fd9c8aa9de25'**

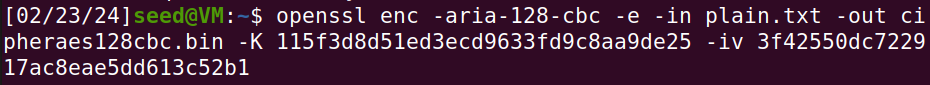
**iv = '3f42550dc722917ac8eae5dd613c52b1'**

****

**Figure 7: Creating encrypted file**

****

**Figure 8: The content of the binary encrypted file**

****

**Figure 9. Different methods for encrypting file**

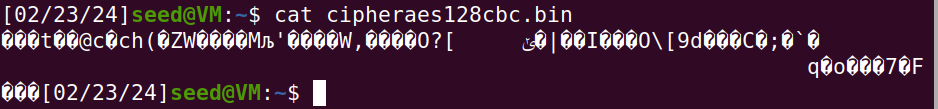
****

**Figure 10. The content of the binary encrypted file after differenting methods**

**A computer screen with white text

Description automatically generated**

**Figure 11. Final encryption mode for the file**

****

**Figure 12. The final preview of the binary file**

**Task 3: Encryption Mode – ECB vs. CBC**

**A screenshot of a computer

Description automatically generated**

**Figure 13. The original picture was given to encrypt**

****

**Figure 14. Encryption process for picture**

Since the format of a BMP file is broken during encryption, we will have to fix it with head, tail, and cat commands to rebuild the structure of that file to a new file; the following bash lines show how it has done.



**Figure 15. Rebuild the header structure file**

****

**Figure 16. . Commands to fix the header of the image file**

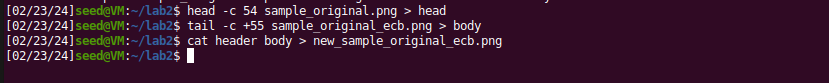
**A screenshot of a computer

Description automatically generated**

**Figure 17. The sample original picture was given to encrypt**

****

**Figure 18. Encryption process for sample original picture**

****

**Figure 19. Rebuild the header structure file**

**Task 4: Padding**

**A screenshot of a computer

Description automatically generated**

**Figure 20. Creating different file sizes**

**A screenshot of a computer code

Description automatically generated**

**A computer screen with white text

Description automatically generated**

**Figure 21. Encrypt with 5 bytes, 10 bytes, 16 bytes using AES**

use ls -l to see the sizes of encrypted cipher text

A screen shot of a computer screen

Description automatically generated

**Figure 21. The size of 3 files including 5 bytes, 10 bytes, 16 bytes using AES using different encryption mode**

A computer screen with white text

Description automatically generated

**Figure 22. Viewing binary of 5 bytes original file**

**A computer screen shot of a program

Description automatically generated**

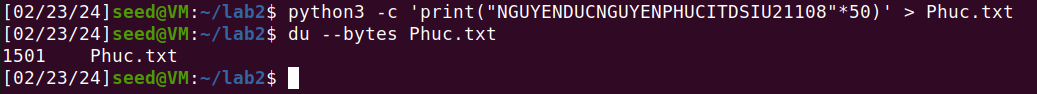
**Figure 23. Viewing binary of 5 bytes CBC decrypted file**

**A computer screen with white text

Description automatically generated**

**Figure 23. Viewing binary of 5 bytes CFB decrypted file**

**Task 5: Error Propagation – Corrupted Ciphertext**

****

**Figure 24. Creating and verifying 1501 bytes file python**

**A computer screen shot of a program

Description automatically generated**

**Figure 25. Encryption modes in action**

**A screenshot of a computer

Description automatically generated**

**A screenshot of a computer

Description automatically generated**

**Figure 26. Before/After modifying the ECB encryption mode**

**A computer screen shot of a computer code

Description automatically generated**

**Figure 26. Decrypt the the file ecb**

**A screenshot of a computer

Description automatically generated** **A screenshot of a computer

Description automatically generated Figure 26. Before/After modifying the OFB encryption mode**

**A computer screen shot of a computer screen

Description automatically generated**

**Figure 26. Decrypt the the file ofb**

**A screenshot of a computer screen

Description automatically generated**

**A computer screen with a number on it

Description automatically generated with medium confidence**

**Figure 27. Compilation of different modes for decryption printed out**