



Al Imam Mohammad Ibn Saud Islamic University
College of Computer and Information Sciences
Computer Science Department

Course Title: Information Security

Course Code: CS 334

Instructor: Dr. Feras Abdulaziz Aljumah

Semester: Second Semester 2024

Student Name:	Abdulkarim Hassan Alharthi	Student ID:	441017066
----------------------	----------------------------	--------------------	-----------

Contents

Introduction	3
Tasks Overview	3
Task 2: Encryption using Different Ciphers and Modes	3
Encryption And Decryption using CBC Mode:	4
Encryption And Decryption using CFB Mode:	4
Encryption And Decryption using ECB Mode:	5
Task 3: Encryption Mode – ECB vs. CBC.....	6
Encryption using ECB Mode:	6
Encryption using CBC Mode:	7
Task 7: Programming using the Crypto Library (Java):	8
Lab Observations:.....	9
Encryption with Different Ciphers:	9
ECB vs. CBC Encryption Modes:.....	9
Java Crypto Library Programming:	9
Challenges	9
Conclusion.....	10
References:.....	10

Introduction

In this lab, we explored various aspects of secret-key encryption, delving into encryption algorithms, encryption modes, paddings, and initial vectors (IV). The primary focus was on gaining hands-on experience with encryption techniques and understanding common mistakes in their implementation.

The lab tasks covered key topics such as substitution ciphers, frequency analysis, encryption modes (specifically ECB vs. CBC), and programming using the crypto library. The tasks were designed to deepen our understanding of secret-key encryption and its practical applications.

Tasks Overview

Task 2: Encryption using Different Ciphers and Modes

In this task, we experimented with different encryption algorithms and modes. We used tools like OpenSSL to encrypt messages with AES, DES, and other ciphers. The objective was to understand how different algorithms and modes affect the security and confidentiality of the encrypted data.

Encryption And Decryption using CBC Mode:

The screenshot displays a Linux desktop environment within an Oracle VM VirtualBox window titled 'seedlabs [Running] - Oracle VM VirtualBox'. The desktop background is 'untu Desktop'. The top panel shows system icons and the time '11:50 PM'. The user is 'Abdulkarim Hassan Al-Harthi' with ID '441017066'. A terminal window is open, showing the following commands and output:

```
[01/20/24]seed@VM:~$ openssl enc -aes-128-cbc -e -in /home/seed/Desktop/text -out /home/seed/Desktop/encryption-cbc -k "00112233445566778889aabbccddeeff" -iv "0102030405060708"
[01/20/24]seed@VM:~$ openssl enc -aes-128-cbc -d -in /home/seed/Desktop/encryption-cbc -out /home/seed/Desktop/decryption-cbc -k "00112233445566778889aabbccddeeff" -iv "0102030405060708"
[01/20/24]seed@VM:~$
```

Three gedit windows are open, showing the content of the files:

- text (~/.Desktop) - gedit**: Contains the plain text: "this message from king,kill the queen."
- encryption-cbc (~/.Desktop) - gedit**: Contains the encrypted output, which is a base64-encoded string: "Salted_ÓÁvZ|/Y5@>#gÁtPaGeËötÜ*'P0aüidv;è) né1,"
- decryption-cbc (~/.Desktop) - gedit**: Contains the decrypted output, which matches the original text: "this message from king,kill the queen."

The bottom status bar shows 'Plain Text', 'Tab Width: 8', 'Ln 14, Col 62', and 'INS'.

Encryption And Decryption using CFB Mode:

The screenshot displays a Linux desktop environment within an Oracle VM VirtualBox window titled 'seedlabs [Running] - Oracle VM VirtualBox'. The desktop background is 'untu Desktop'. The top panel shows system icons and the time '11:58 PM'. The user is 'Abdulkarim Hassan Al-Harthi' with ID '441017066'. A terminal window is open, showing the following commands and output:

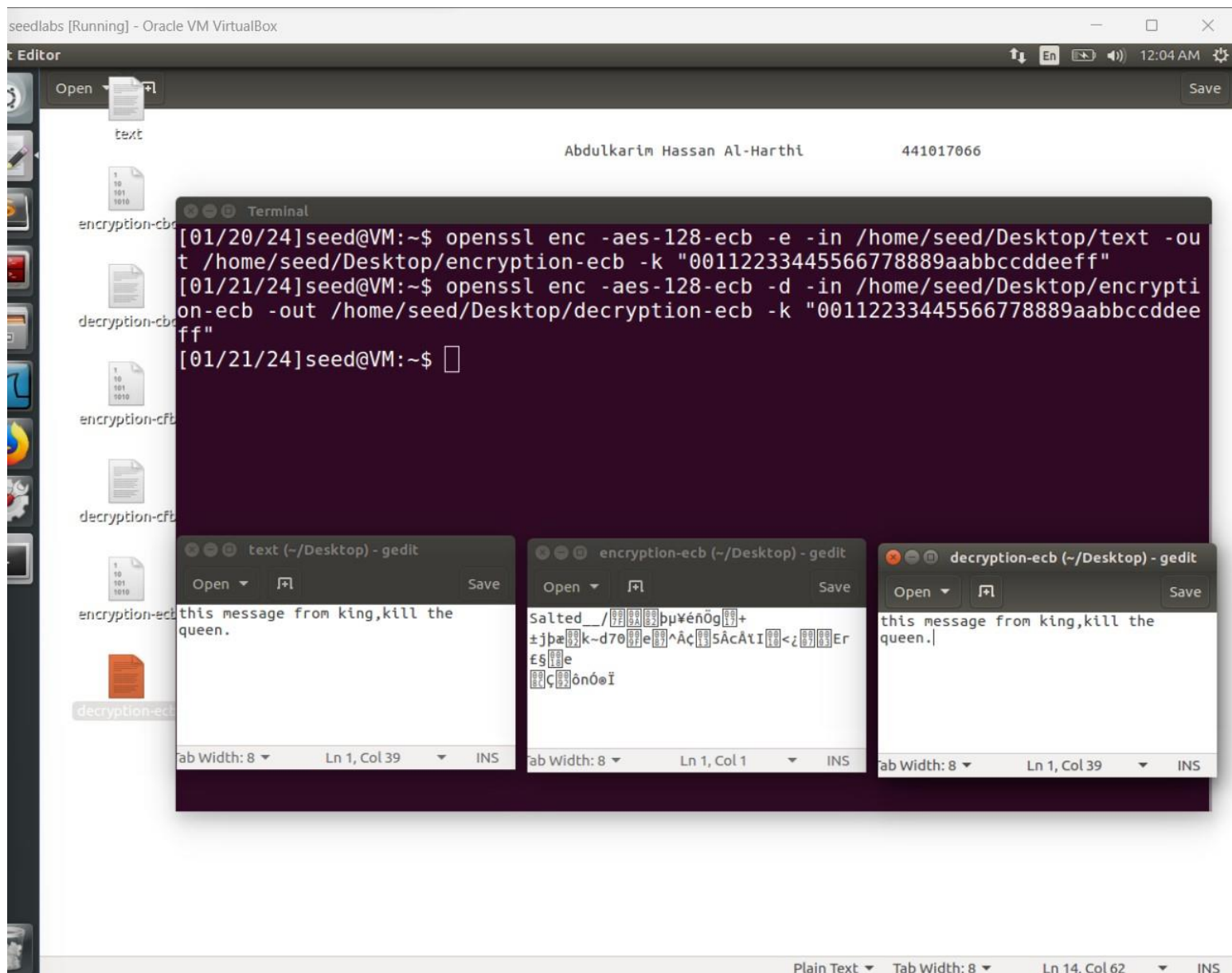
```
[01/20/24]seed@VM:~$ openssl enc -aes-128-cfb -e -in /home/seed/Desktop/text -out /home/seed/Desktop/encryption-cfb -k "00112233445566778889aabbccddeeff" -iv "0102030405060708"
[01/20/24]seed@VM:~$ openssl enc -aes-128-cfb -d -in /home/seed/Desktop/encryption-cfb -out /home/seed/Desktop/decryption-cfb -k "00112233445566778889aabbccddeeff" -iv "0102030405060708"
[01/20/24]seed@VM:~$
```

Three gedit windows are open, showing the content of the files:

- text (~/.Desktop) - gedit**: Contains the plain text: "this message from king,kill the queen."
- encryption-cfb (~/.Desktop) - gedit**: Contains the encrypted output, which is a base64-encoded string: "Salted_šJ»:L#â!0}~,~e9neôSÉi'úa'dAç«pi"
- decryption-cfb (~/.Desktop) - gedit**: Contains the decrypted output, which matches the original text: "this message from king,kill the queen."

The bottom status bar shows 'Plain Text', 'Tab Width: 8', 'Ln 14, Col 62', and 'INS'.

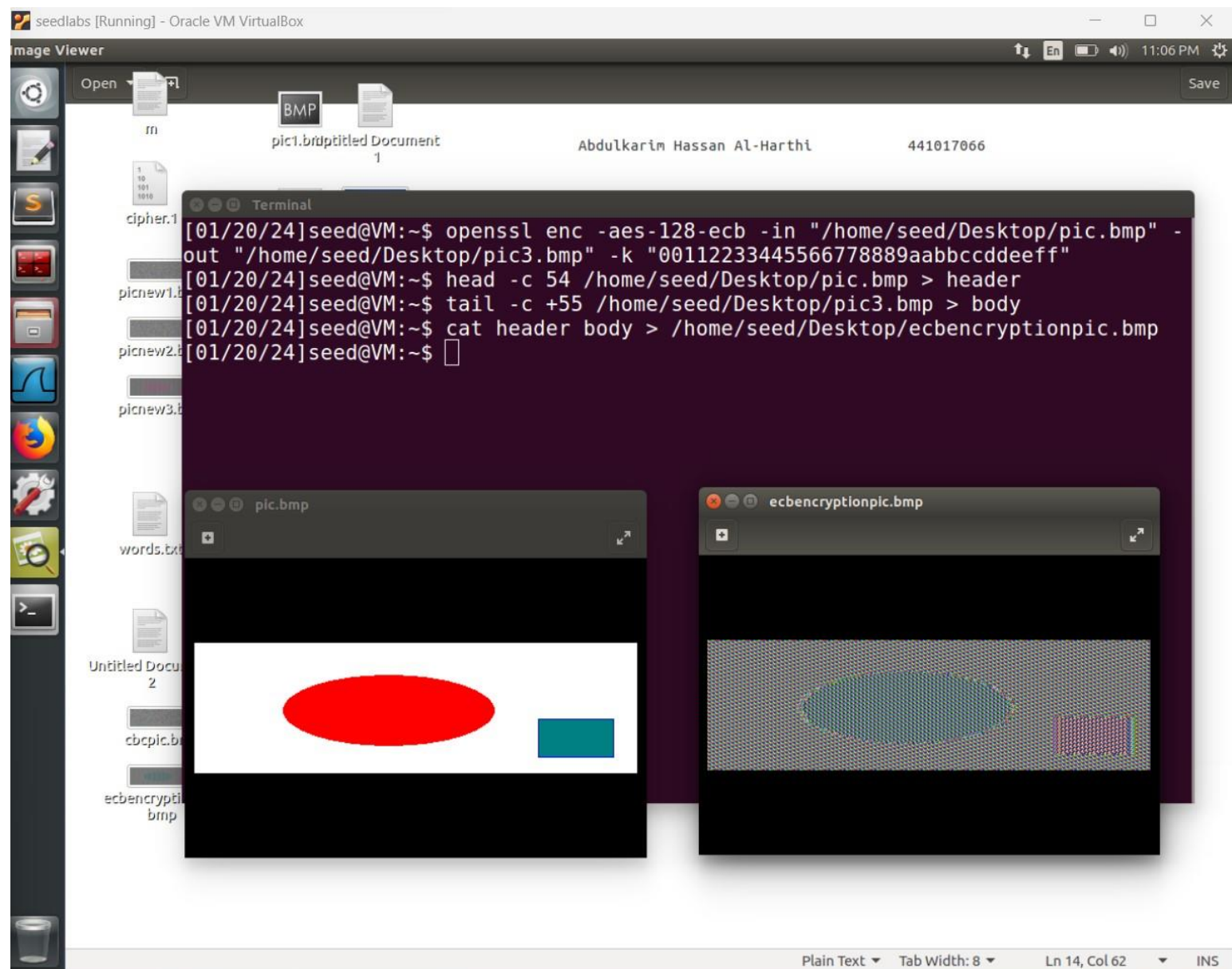
Encryption And Decryption using ECB Mode:



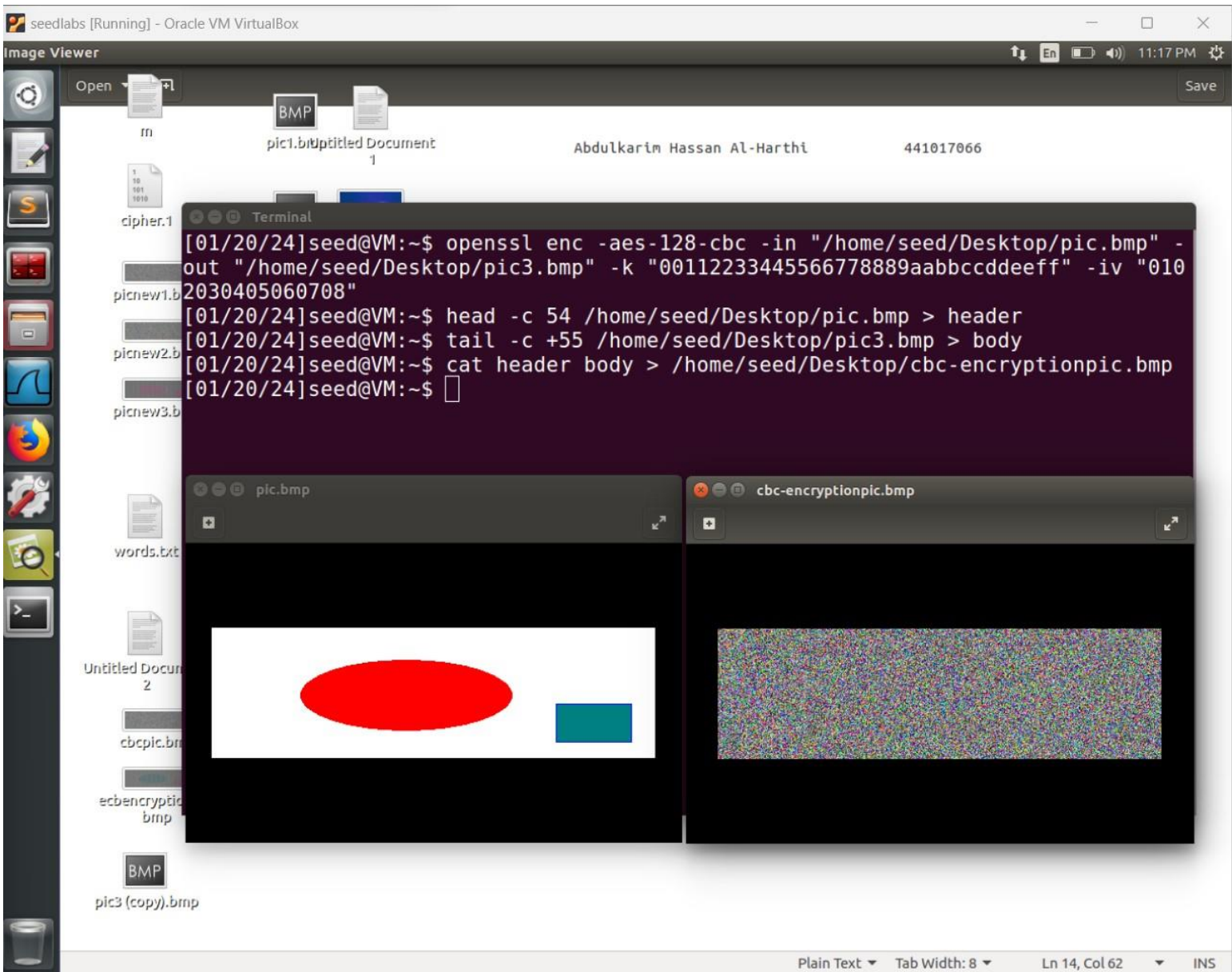
Task 3: Encryption Mode – ECB vs. CBC

Task 3 focused on comparing two encryption modes: Electronic Code Book (ECB) and Cipher Block Chaining (CBC). We encrypted a picture using both modes and observed the differences. This task provided insights into the importance of choosing the right encryption mode for different scenarios.

Encryption using ECB Mode:

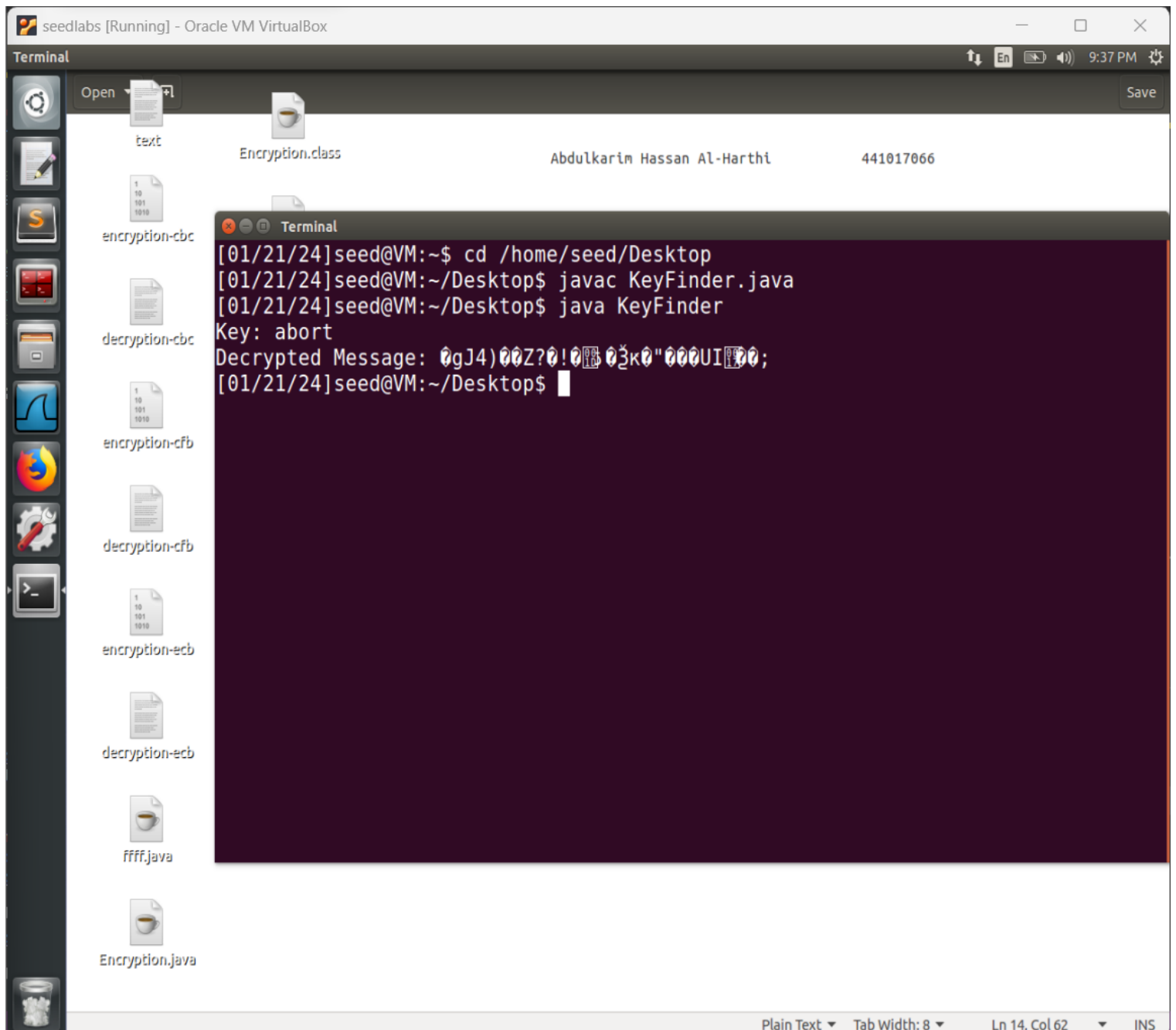


Encryption using CBC Mode:



Task 7: Programming using the Crypto Library (Java):

- Developed a Java program named KeyFinder to decrypt a given ciphertext using a wordlist-based key search.
- Utilized the Java Crypto library to implement AES decryption in CBC mode with PKCS5Padding.
- Integrated error handling for potential key mismatches and implemented key generation logic.
- Tested the program on the provided Ubuntu VM, ensuring compatibility with the specified environment.



```
seedlabs [Running] - Oracle VM VirtualBox
Terminal
Open [Save]
text
Encryption.class
Abdulkarim Hassan Al-Harthi 441017066
encryption-cbc
decryption-cbc
decryption-cfb
encryption-cfb
decryption-ecb
encryption-ecb
decryption-ecb
ffff.java
Encryption.java

Terminal
[01/21/24]seed@VM:~$ cd /home/seed/Desktop
[01/21/24]seed@VM:~/Desktop$ javac KeyFinder.java
[01/21/24]seed@VM:~/Desktop$ java KeyFinder
Key: abort
Decrypted Message: 0gJ4)00Z?0!000 03k0"000UI00;
[01/21/24]seed@VM:~/Desktop$
```


Lab Observations:

Encryption with Different Ciphers:

- Noticed variations in encryption speed and complexity across DES, AES, and Blowfish.
- Explored the impact of key size on security and performance.

ECB vs. CBC Encryption Modes:

- Identified patterns in ciphertext generated using ECB and CBC modes.
- Noted that ECB does not provide as much diffusion as CBC, leading to potential vulnerabilities.
- Discussed the importance of initialization vectors (IVs) in CBC mode.

Java Crypto Library Programming:

- Successfully implemented a Java program for AES decryption using a wordlist-based key search.
- Handled potential exceptions, including `BadPaddingException` for incorrect keys.
- Demonstrated the effectiveness of the program in finding the correct key from the provided wordlist.

Challenges

- Sharing Files Between Windows and Ubuntu in a Virtual Machine
- Uses Command-Line to run the code

Conclusion

In this lab, we explored various encryption tasks, including using different ciphers and modes, comparing ECB vs. CBC encryption, and programming in Java with the Crypto library. The hands-on experience provided valuable insights into the strengths and weaknesses of different encryption techniques. The Java program, KeyFinder, demonstrated practical implementation skills in cryptography, showcasing the importance of key management and encryption mode selection.

References:

1. Seed Labs. "Crypto Encryption Lab Guide." [Online]. Available: https://moodle2021.up.pt/pluginfile.php/204769/mod_resource/content/2/Crypto_Encryption-v2-LabGuide.pdf.
2. Li, Xin Yi. "Seed Lab - Secret-Key Encryption README." [Online]. Available: <https://github.com/li-xin-yi/seedlab/blob/master/Secret-Key-Encryption/README.MD>.
3. Security Platform. "Crypto Lab: Task 7 Programming using the Crypto Library." [Online Video]. Available: https://www.youtube.com/watch?v=6UzmB1k000s&ab_channel=SecurityPlatform.