CHAPTER 9

IMPLEMENTATION OF LAO-3D LIGHTWEIGHT BLOCK CIPHER

9.1 Introduction

This chapter presents the implementation of LAO-3D lightweight block cipher on software applications. Two types of software development were carried out on LAO-3D algorithm that includes desktop and mobile applications to observe the functionality of the lightweight block cipher.

9.2 Software Implementation of LAO-3D Lightweight Block Cipher

In order to demonstrate the applicability of LAO-3D lightweight block cipher, two software implementations were conducted to observe the functionality of the algorithm. Due to limited resources, the implementations were built on a desktop application using C++ programming on Microsoft Visual Studio 2008 and a mobile application using Android Studio development software.

9.2.1 Desktop Application

Desktop application is a software program that can be executed on a personal computer to perform a specific task by an end-user. Microsoft Visual Studio is selected as the programming software since it is a very convenient and powerful application development software that works on most operating systems such as Windows, Linux, Android, and iOS. Therefore, an encryption desktop application was developed by implementing LAO-3D lightweight block cipher.

The desktop application can be used to secure sensitive data before sending it through email or storing it in a database. Data is encrypted within the application and does not depend on the underlying transport. When data is stored or transferred over the network, it remains encrypted until it reaches the destination of the application user that holds the encryption key, therefore, the security of the data is guaranteed.

9.2.1.1 Encryption

Encryption is a method for securing digital data using a cryptographic algorithm, along with a password. The encryption process converts the information into unreadable data to protect it from the unintended receiver. In order to provide data security through encryption, LAO-3D algorithm was implemented on Microsoft Visual Studio using the source code from APPENDIX D as displayed in Figure 9.1. Three steps are required to perform the encryption application that includes entering the encryption key, entering the message, and executing the data encryption.

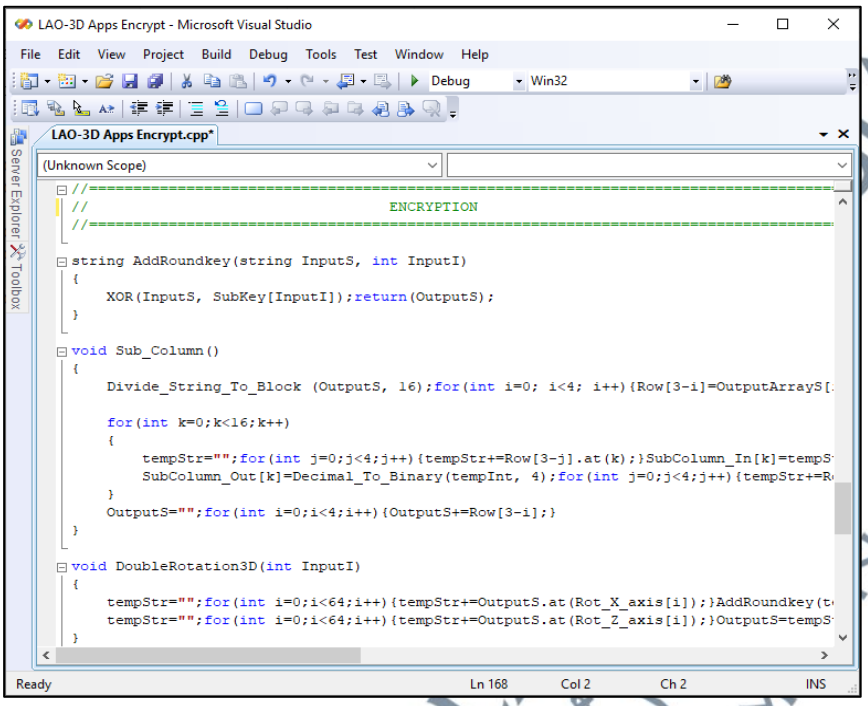
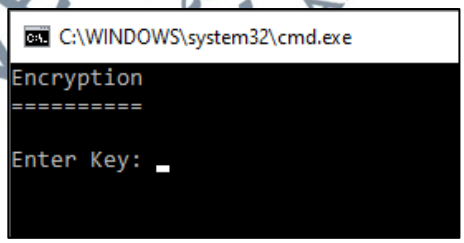


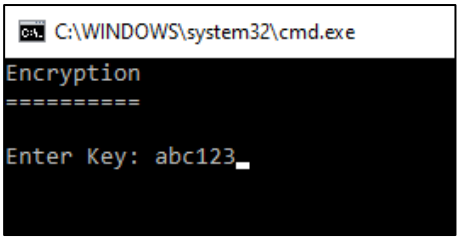
Figure 9.1: Encryption

i) **Step 1**

User is required to enter the encryption key as displayed in Figure 9.2. Encryption key is a secret word or phrase with a maximum of 16 characters long which is equal to the 128-bit key size of LAO-3D algorithm. The encryption key can be represented in form of letters, numbers, or special characters.



(i) Before entering the key

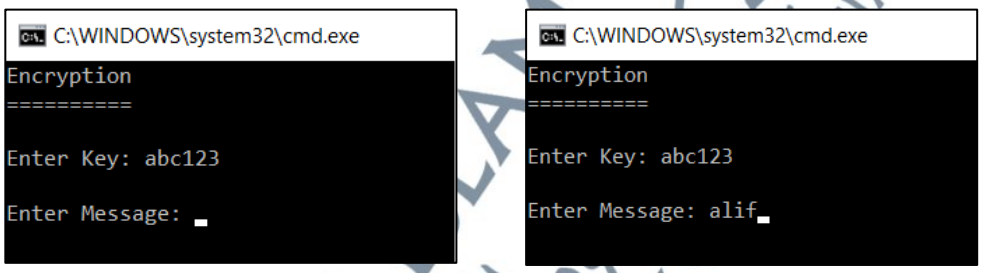


(ii) After entering the key

Figure 9.2: Input Encryption Key

ii) **Step 2**

User is required to enter the message as shown in Figure 9.3. Message is the information that needs to be protected through an encryption process. Similar to the encryption key, the message can be represented in form of letters, numbers, or special characters. The length of the message must not exceed 2,040 characters long or equal to 16,320 bits due to the limitation of the C++ programming of the Microsoft Visual Studio 2008.



(i) Before entering the message (ii) After entering the message

Figure 9.3: Input Message

iii) **Step 3**

After entering the encryption key and message, the application will execute an encryption process to generate the ciphertext as presented in Figure 9.4. The ciphertext is transformed into hexadecimal characters.

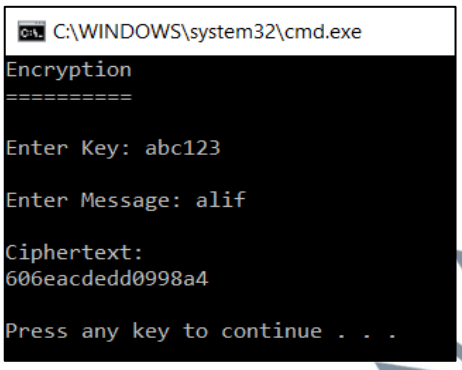


Figure 9.4: Output Ciphertext

9.2.1.2 Decryption

Decryption is a method of converting encrypted data into its original form using a cryptographic algorithm and a password. In general, decryption is a reverse process of an encryption method. The encrypted data is decoded to allow the authorized receiver to read the information. Similar to the encryption process implemented in the desktop application, LAO-3D algorithm was applied to Microsoft Visual Studio using the source code provided in APPENDIX E as displayed in Figure 9.5. Three steps are required to perform the decryption process which include entering the decryption key, entering the ciphertext, and executing the data decryption.

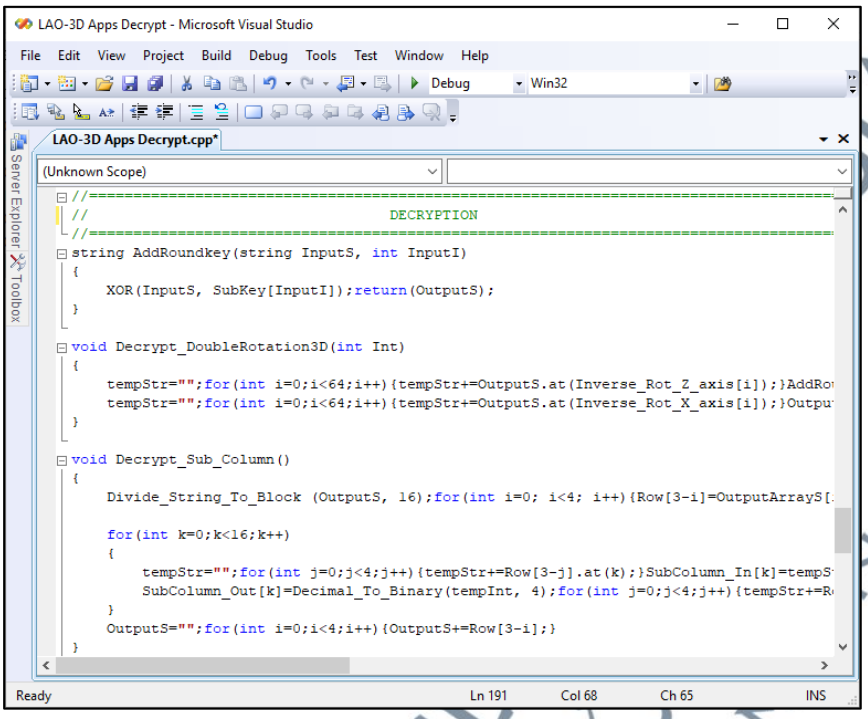
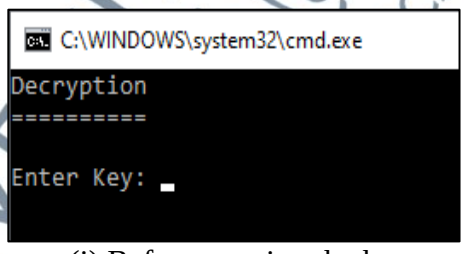


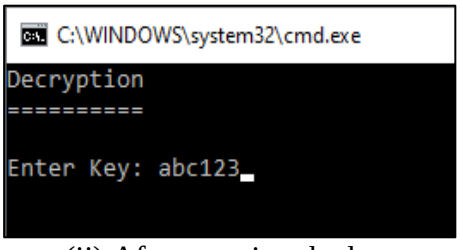
Figure 9.5: Decryption

i) **Step 1**

User is required to enter the decryption key as displayed in Figure 9.6. Decryption key is a secret word or phrase with a maximum of 16 characters long that can be represented in form of letters, numbers, or special characters.



(i) Before entering the key

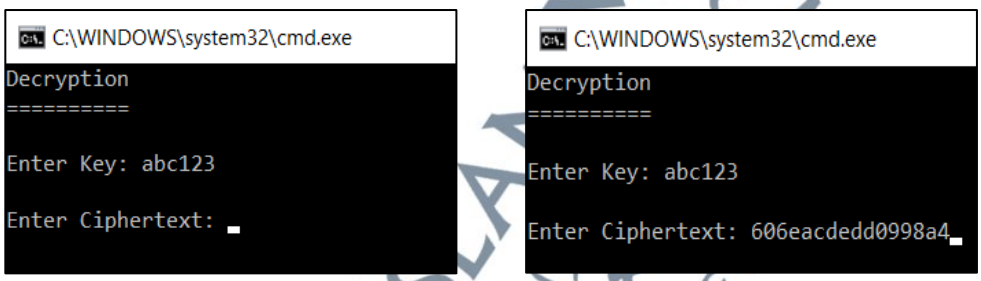


(ii) After entering the key

Figure 9.6: Input Decryption Key

ii) **Step 2**

User is required to enter the ciphertext as shown in Figure 9.7. Ciphertext is the data that needs to be recovered to reveal the message through a decryption process which is represented in form of hexadecimal characters. The length of the ciphertext must not exceed 4,080 hexadecimal characters long which equal 16,320 bits of data.



(i) Before entering the ciphertext (ii) After entering the ciphertext

Figure 9.7: Input Ciphertext

iii) **Step 3**

After entering the decryption key and ciphertext, the application will execute a decryption process to generate the plaintext as presented in Figure 9.8.

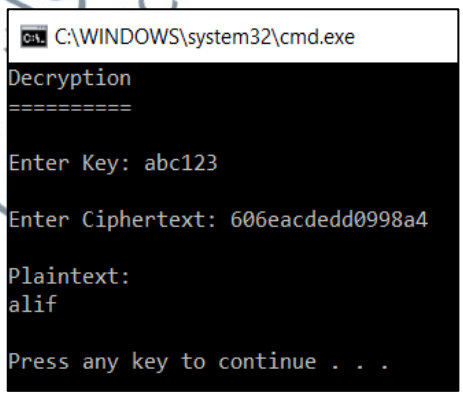
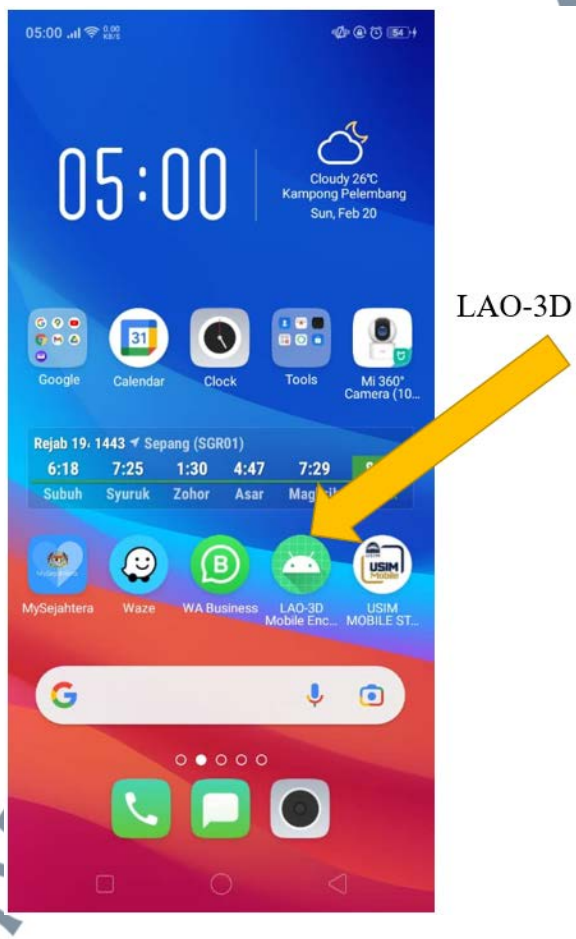


Figure 9.8: Output Plaintext

9.2.2 Mobile Application

Mobile application is a computer program or software application designed to run on a mobile device such as a smartphone, tablet, or watch. As the world's leading mobile operating system, a mobile encryption application was developed on Android by implementing LAO-3D lightweight block cipher as shown in Figure 9.9. Android Studio is selected as the development software due to its capability in building market-leading apps on every type of Android device.



LAO-3D Mobile Encryption App

Figure 9.9: Mobile Encryption Application

The mobile application was developed for data at rest encryption in which the encryption of the data (plaintext) is stored in the smartphone and is not moving through the internet. Only the encrypted data (ciphertext) will be transferred through the internet using any available instant messaging application (WhatsApp, Telegram, etc.) as shown in Figure 9.10. The application was designed specifically for offline data encryption to protect data from unauthorized access that can occur in online data encryption applications.

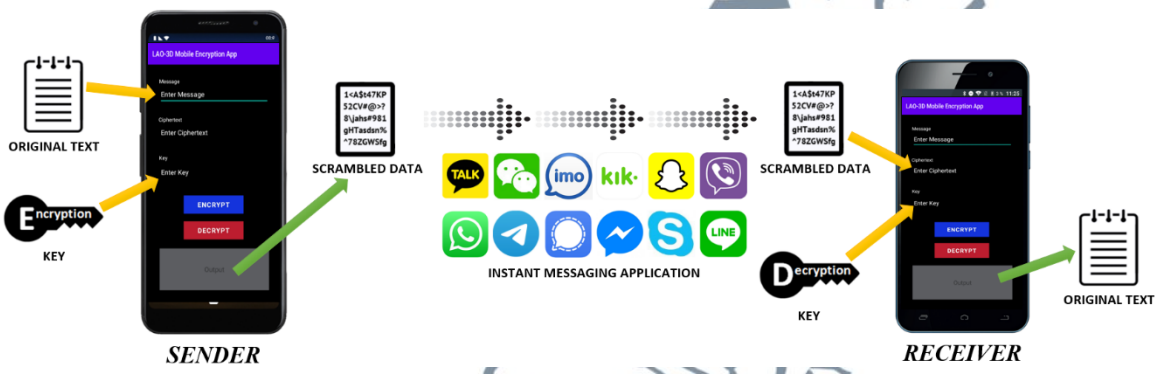


Figure 9.10: Encryption and Decryption Process

9.2.2.1 Encryption

In order to provide data security in mobile applications, LAO-3D lightweight block cipher was implemented on Android Studio (Bumblebee 2021.1.1) using the source code from APPENDIX D as displayed in Figure 9.11. Three steps are required to use the application that includes entering the encryption key, entering the message, and executing the data encryption in the mobile encryption application.

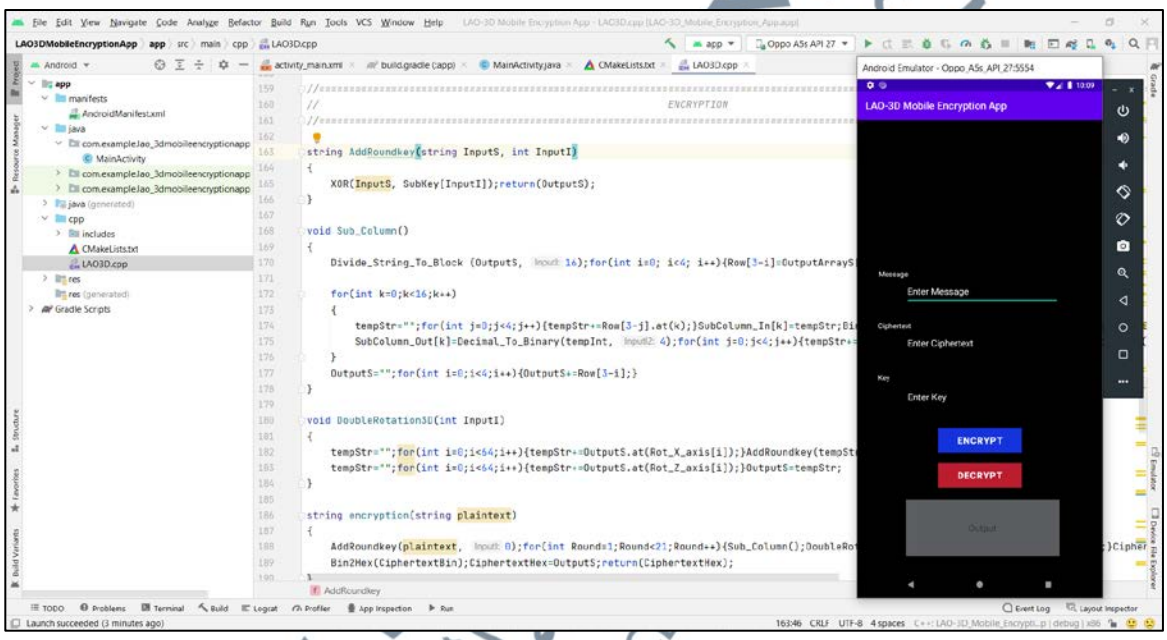
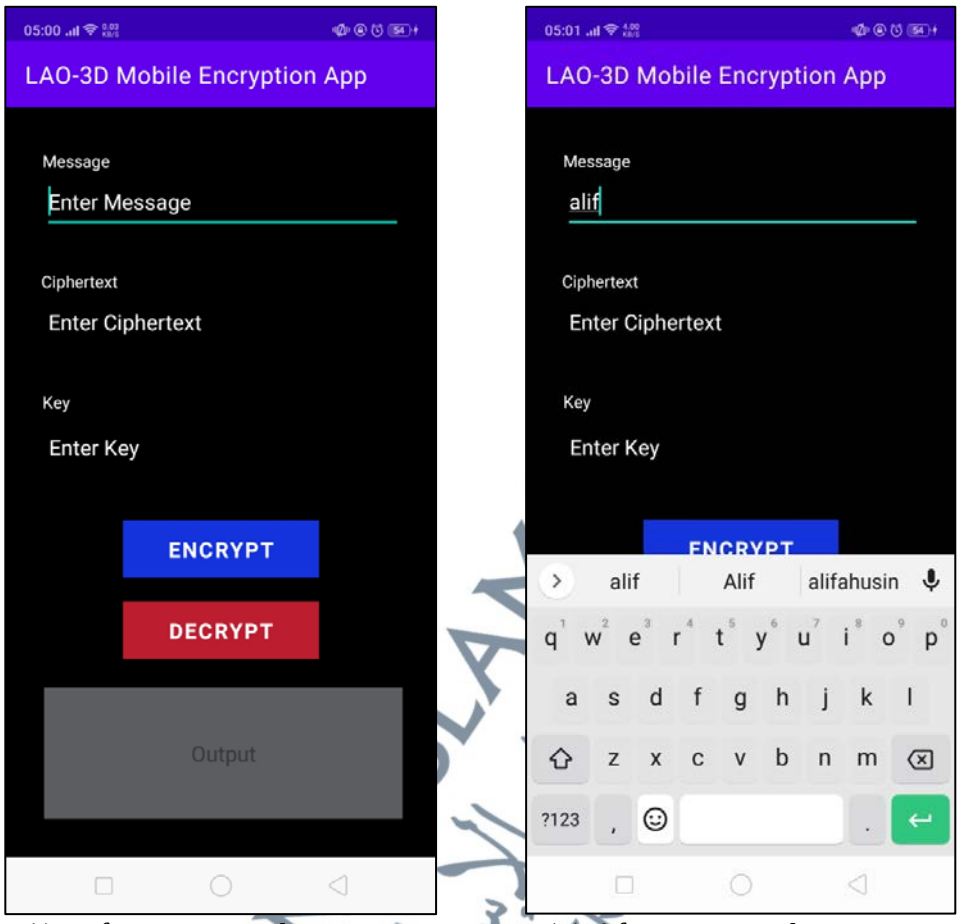


Figure 9.11: Encryption

i) **Step 1**

User is required to enter the message in the text box as shown in Figure 9.12. The message can be represented in form of letters, numbers, or special characters.

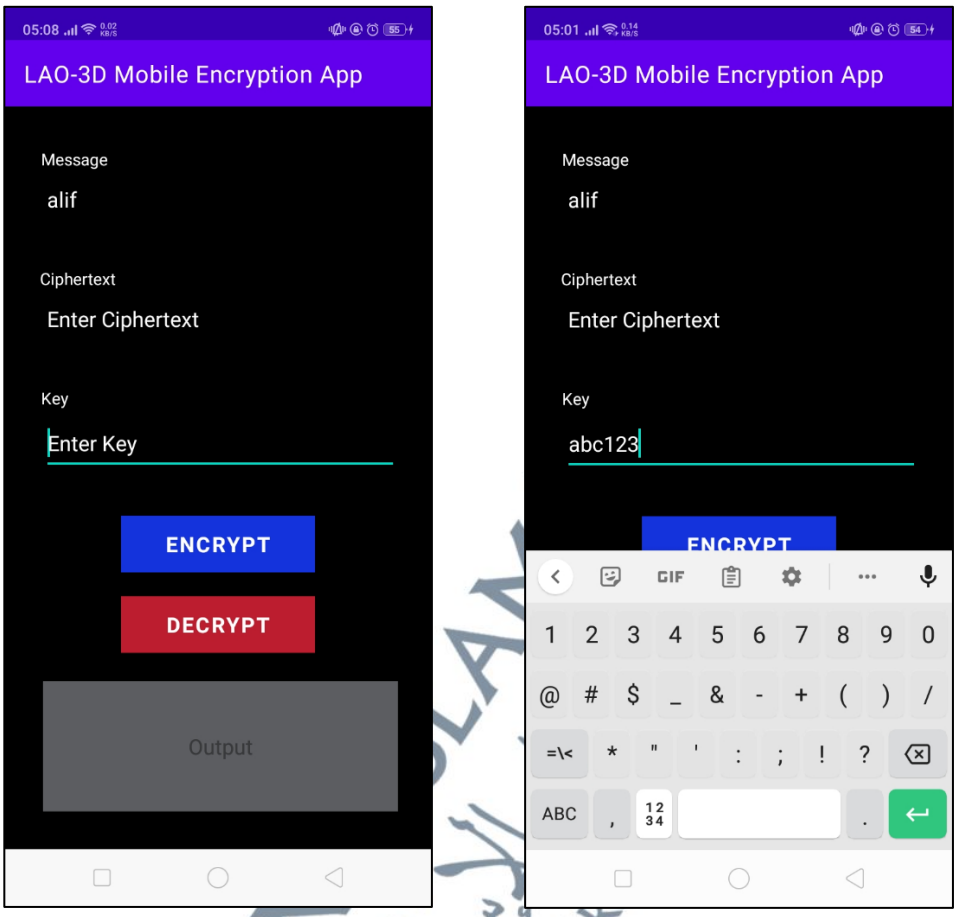


(i) Before entering the message (ii) After entering the message

Figure 9.12: Input Message

ii) **Step 2**

User is required to enter the encryption key in the text box as displayed in Figure 9.13. Similar to the message, the encryption key can be represented in form of letters, numbers, or special characters.

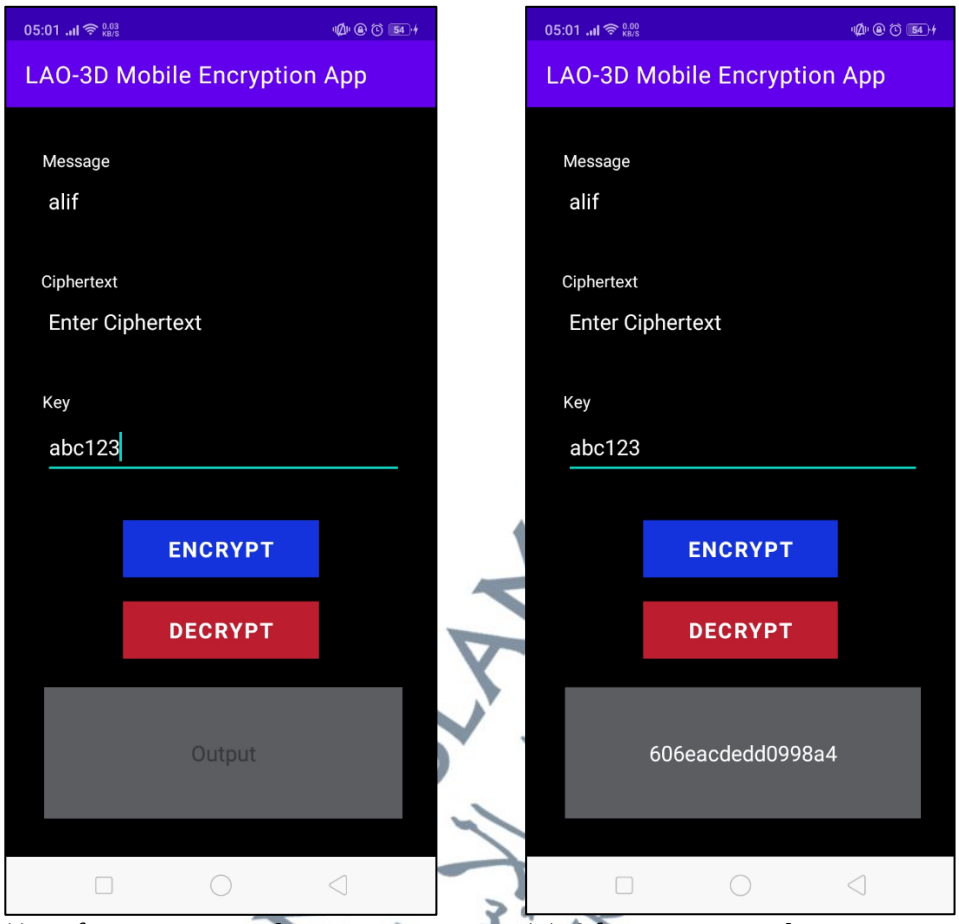


(i) Before entering the key (ii) After entering the key

Figure 9.13: Input Encryption Key

iii) **Step 3**

After entering the message and encryption key, the user is required to press the "Encrypt" button to generate the ciphertext. The ciphertext is transformed into hexadecimal characters as displayed in Figure 9.14.



(i) Before executing the encryption (ii) After executing the encryption

Figure 9.14: Output Ciphertext

9.2.2.2 Decryption

Similar to the encryption process implemented in the mobile application, LAO-3D lightweight block cipher was applied on Android Studio using the source code provided in APPENDIX E as displayed in Figure 9.15. Three steps are required to perform the decryption process which include entering the decryption key, entering the ciphertext, and executing the data decryption in the mobile encryption application.

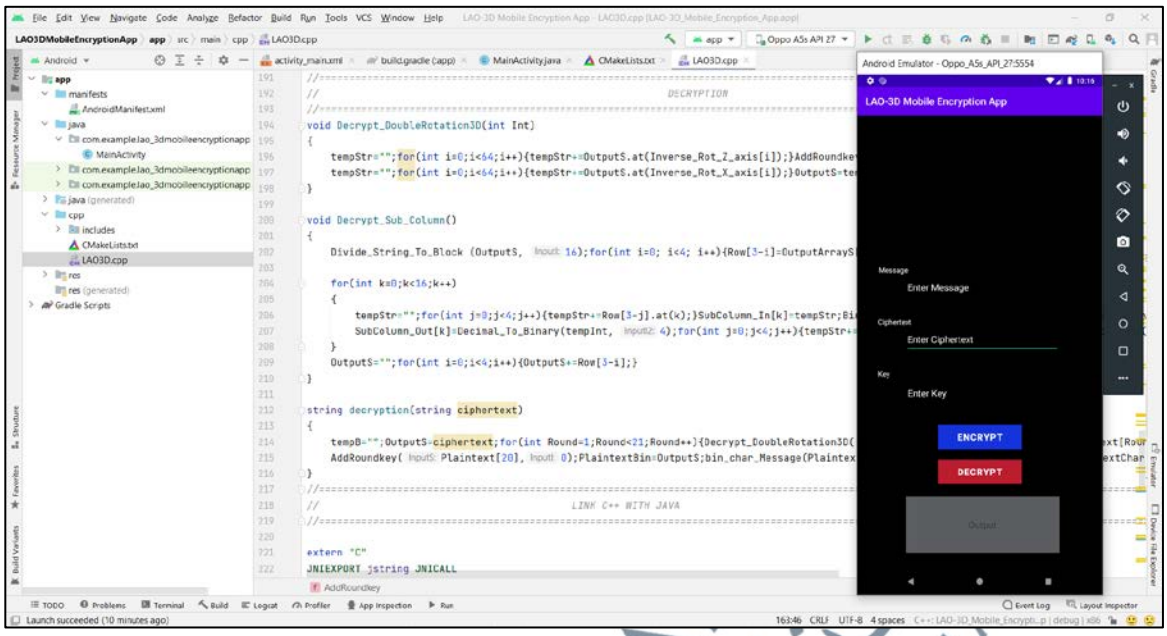
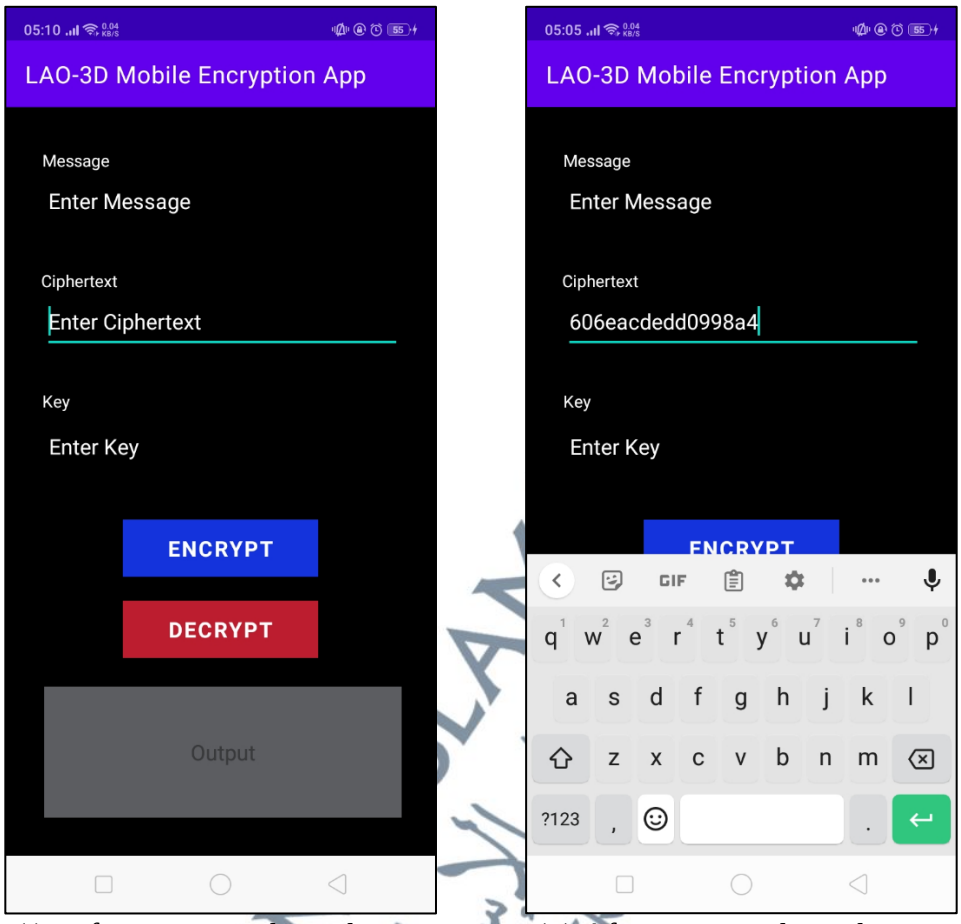


Figure 9.15: Decryption

i) Step 1

User is required to enter the ciphertext in the text box as shown in Figure 9.16.

The ciphertext is represented in the form of hexadecimal characters.

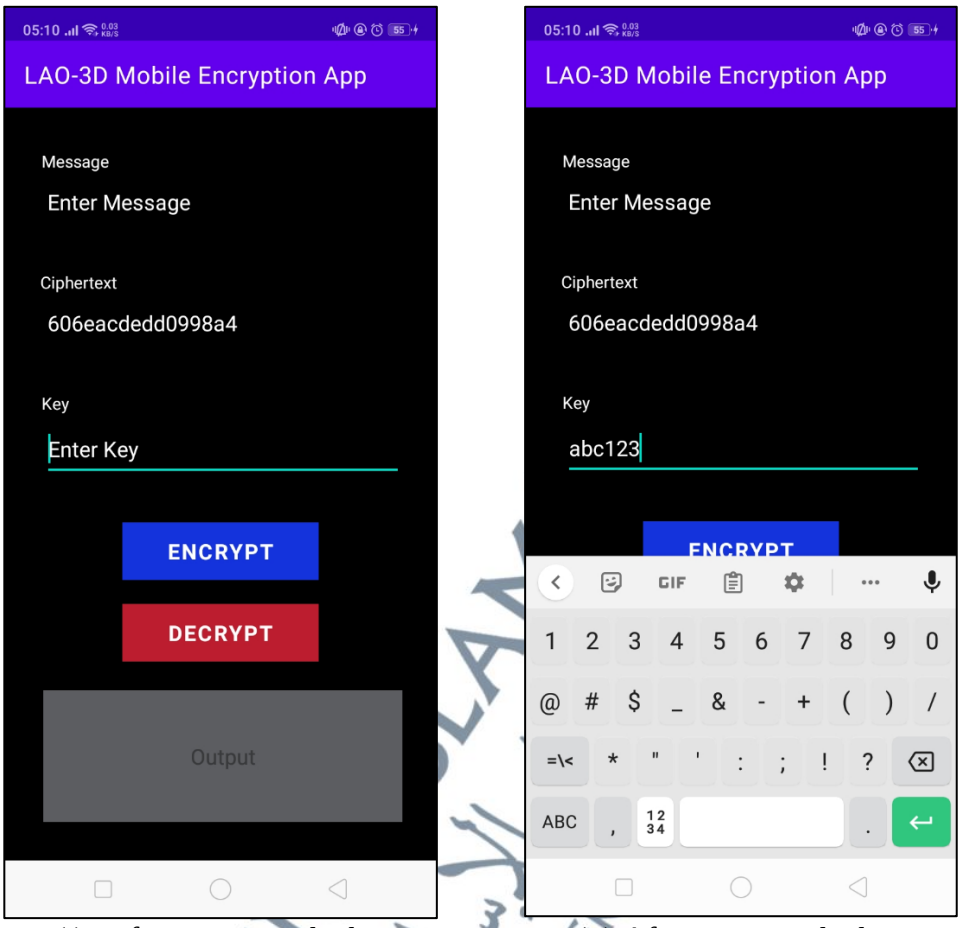


(i) Before entering the ciphertext (ii) After entering the ciphertext

Figure 9.16: Input Ciphertext

ii) **Step 2**

User is required to enter the decryption key in the text box as displayed in Figure 9.17. The decryption key can be represented in the form of letters, numbers, or special characters.

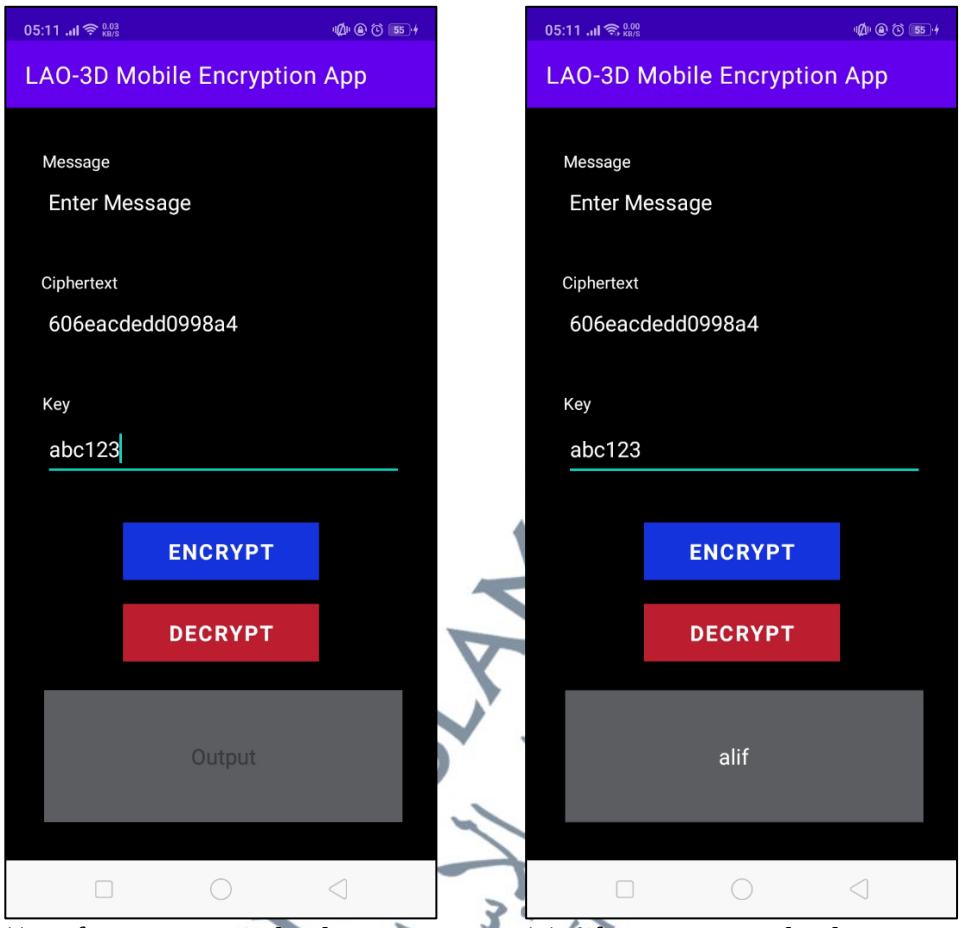


(i) Before entering the key (ii) After entering the key

Figure 9.17: Input Decryption Key

iii) **Step 3**

After entering the ciphertext and decryption key, the user is required to press the “Decrypt” button to generate the plaintext through a decryption process as displayed in Figure 9.18.



(i) Before executing the decryption (ii) After executing the decryption

Figure 9.18: Output Plaintext

9.3 Chapter Summary

Apart from the theoretical representation of the new algorithm design, two software implementations of LAO-3D lightweight block cipher were presented in the chapter. Firstly, a desktop application was developed by implementing the new lightweight block cipher to show the usefulness of the algorithm in a real application. The output from the application shows that the design, source code, and functionality of the LAO-3D works well as claimed in the thesis.

On the other hand, a mobile encryption application using Android Studio development software was established. This application gives users hands-on experience in using the data encryption application on their smartphones. For users with zero knowledge of cryptography, this mobile application can increase users' interest in knowing how actually encryption works. In addition, this approach can increase users' awareness of information security especially in protecting confidential data.