Table of Contents

CHAPTER 1

INTRODUCTION

1.1 Problem Definition.

ENCRYTON is a project developed to hide the important data from intruders or hackers. This application uses AES algorithm techniques to retrieve the encrypted data to the image. In any organization data is the most asset which must be kept protected and secure from unauthorized access. This application provides different techniques to hide and secure the data. This AES photo encryption application provides a user friendly and works efficiently in hiding the data.

1.2 Project Overview

In this software uses Cryptography for its security, security to the confidential data is provided in multilayer. All the personal files and private information like e-commerce transactions can be kept secret by using ENCRYTON technique. This system avoids misuse of data from the intruders. This algorithm for data hiding plays a major role when the confidential information is kept at service providers. It also helps to prevent data from damage.

Cryptography provides a number of security goals to ensure the privacy of data, non-alteration of data and so on. Due to the great security advantages of cryptography it is widely used today. Following are the various goals of cryptography.

- **Confidentiality**: Information in computer is transmitted and has to be accessed only by the authorized party and not by anyone else.
- **Authentication:** The information received by any system has to check the identity of the sender that whether the information is arriving from an authorized person or a false identity.
- **Integrity:** Only the authorized party is allowed to modify the transmitted information. No one in between the sender and receiver are allowed to alter the given message.
- **Non-Repudiation:** Ensures that neither the sender, nor the receiver of message should be able to deny the transmission.
- **Access Control:** Only the authorized parties are able to access the given information.

Cryptography technique is used when secret message are transferred from one party to another over a communication line. There are two main types of cryptography:

A. Symmetric key cryptography
B. Asymmetric key cryptography

a) **Symmetric key cryptography:** With this type of cryptography, both the sender and the receiver know the same secret code, called the key. Messages are encrypted by the sender using the key and decrypted by the receiver using the same key. The key plays a very important role in symmetric cryptography since their security directly depends on the nature of key i.e. the key length etc.

b) **Asymmetric key cryptography:** It used encryption and decryption algorithm pair. With public key cryptography, keys work in pairs of matched public and private keys.

1.3 Specification

Features:

- **Secure:** The primary purpose of encryption is to protect the confidentiality of digital data stored on computer systems or transmitted via the internet or any other.
- **Easy to use:** Encryption can protect information stored on your computer from unauthorized access - even from people who otherwise have access to your computer system. Encryption can protect information while it is in transit from one computer system to another.
- **Reliable and accurate:** This Encryption System can return the same data you that you encrypted that's why it is so Reliable and accurate
- **No need of examiner:** There is no need for the user to cross check the data that he/she encrypted on the time of decryption as the data is going to be the same as it encrypted.

Modules Overview:

- **Input:** Plain text or confidential data is given to the application. The data consist of lines of text that can be entered in the text area.
- **Encryption:** The entered text will be encrypted after generating the security key. The process of encryption will be done in multiple layers. After entering the security key, the text will be sent to the decryption process.
- **Image Decryption:** Transformation of cipher text to plain text is called Decryption. By applying the decryption process, the text obtained is the plain text. The plain text is displayed in text area provided. To retrieve the correct information, secret key is to be generated using the random matrix. By using the encryption algorithm, the plain text will open the image which is decrypted without any data misuse or loss.

1.4 Hardware Specification

- **Hard Disk: min 20MB -** For the best functioning of the software
- **Monitor** - For viewing the outputs windows.
- **Keyboard -** For Giving the input to the software.
- **Mouse -** For Giving the input to the software.

1.5 Software Specification:

- Operating System: Platform independent.
- Language: Java SE and Java EE.
- NetBeans IDE 7.4.
- IDE- Eclipse Java 2018-12.

CHAPTER 2

LITERATURE SURVEY

2.1 Existing System:

In the existing system when original message is encrypted some of the information may lose. There is no robustness in retrieving the data. All the secured information may be opened by intruders by using the decryption technique. There is no safety for the information. The algorithm used in the existing system is not efficient. Data may be damaged or lost when receiver is trying to retrieve the original information

2.2 Proposed System:

In the proposed system, security to the confidential data is provided in multilayer. All the personal files and private information like e-commerce transactions can be kept secret by using ENCRYTON encryption technique. This system avoids misuse of data from the intruders. This algorithm for data hiding plays a major role when the confidential information is kept at service providers. It also helps to prevent data from damage.

2.3 Feasibility Study:

Feasibility study refers to the overall idea of the package which we are designing. Software feasibility has four solid dimensions. Technical- is a project technically feasible? Is it within the state of the art? Can defects be reduced to a level matching the application's needs? Economical- is it financially feasible? Can development be completed at a cost the Software organization, its client, or the market can afford? Operational- Will the project's time-to-market beat the competition?

This study tells about how this package is useful to the users and its advantages and disadvantages, and also it tells whether this package is cost effective are not. There are three types of feasibility study, they are

- Economic Feasibility.
- Technical Feasibility.
- Operational Feasibility

2.3.1 Economical Feasibility

In this project the JAVA language is used for developing the piracy protection software, it is provided for free of cost. So, it is bought without spending money. Can be download this and use it. directly from the Internet itself. So, it is not needed to look from any third party or in the market. It is freely download it from the Internet. This Exact Knowledge Hiding through Database Extension Software will be cost effective. So, there is no problem of getting licensed and to pay money and get the package that is needed as it is concerned can be bought for free of cost

2.3.2 Technical Feasibility

Technical feasibility is important, but business need is even more important. It does no good to build a high-tech system or product that no one really wants. The Exact Knowledge Hiding through Database Extension Software is developed using for hiding database knowledge for the End user and is readily available with everyone so no need to search for any requirements and this software will work in any Operating System not like only in windows XP environment in order to pick up speed and also it is the advanced version of windows which available with everyone. The technical requirements like hardware and software requirements are available so it easily worked by other users.

2.3.3 Operational Feasibility

The Software that is developed is very user friendly. The user needs not to be a computer programmer. Even a computer literate who knows very basic things about the computer can work with this piracy protection software. Because this software itself will assist us in working with multimedia contents. This software is developed in fast growing language with updated features.

CHAPTER 3

SYSTEM ANALYSIS & DESIGN

3.1 Requirement Specification:

Hardware Specification

- **Hard Disk: min 20MB -** For the best functioning of the software
- **Monitor** - For viewing the outputs windows.
- **Keyboard -** For Giving the input to the software.
- **Mouse -** For Giving the input to the software.

Software Specification:

- Operating System: Platform independent.
- Language: Java SE and Java EE.
- NetBeans IDE.
- IDE- Eclipse.

3.2 Pseudo Code:

```
void encrypt(String srcPath, String destPath) {
     File rawFile = new File(srcPath);
    File encryptedFile = new File(destPath);
    InputStream inStream = null;
    OutputStream outStream = null;
    try {
      cipher.init(Cipher.ENCRYPT_MODE, secretKey);
      inStream = new FileInputStream(rawFile);
      outStream = new FileOutputStream(encryptedFile);
      byte[] buffer = new byte[1024];
      int len;
      while ((len = inStream.read(buffer)) > 0) {
        outStream.write(cipher.update(buffer, 0, len));
        outStream.flush(); }
      outStream.write(cipher.doFinal());
      inStream.close();
```

```
            outStream.close();
        } catch (InvalidKeyException ex) {
            System.out.println(ex);
        } catch (FileNotFoundException ex) {
            System.out.println(ex);
        } catch (IOException ex) {
            System.out.println(ex);
        } }
    void decrypt(String srcPath, String destPath) {
        File encryptedFile = new File(srcPath);
        File decryptedFile = new File(destPath);
        InputStream inStream = null;
        OutputStream outStream = null;
        try {
            cipher.init(Cipher.DECRYPT_MODE, secretKey);
            inStream = new FileInputStream(encryptedFile);
            outStream = new FileOutputStream(decryptedFile);
            byte[] buffer = new byte[1024];
            int len;
            while ((len = inStream.read(buffer)) > 0) {
                outStream.write(cipher.update(buffer, 0, len));
                outStream.flush();}
            outStream.write(cipher.doFinal());
            inStream.close();
            outStream.close();
        } catch (InvalidKeyException ex) {
            System.out.println(ex);
        } catch (FileNotFoundException ex) {
            System.out.println(ex);
        } catch (IOException ex) {
            System.out.println(ex);
} }
```

3.3 Flowchart:

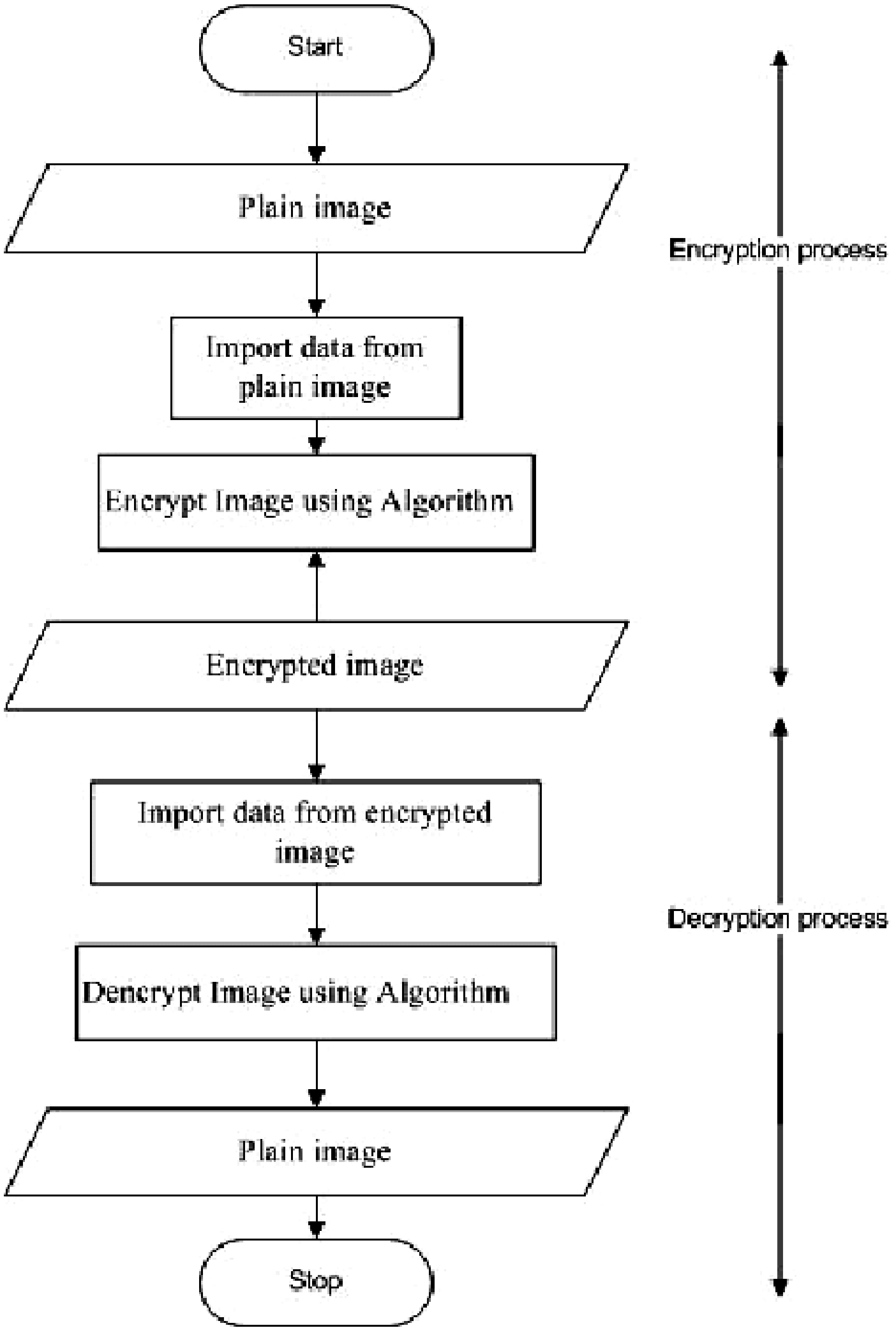

Start
Plain image
Import data from plain image
Encrypt Image using Algorithm
Encrypted image
Import data from encrypted image
Dencrypt Image using Algorithm
Plain image
Stop
Encryption process
Decryption process

Fig 3.3.1: Flowchart for IMAGE encryption and dencryption

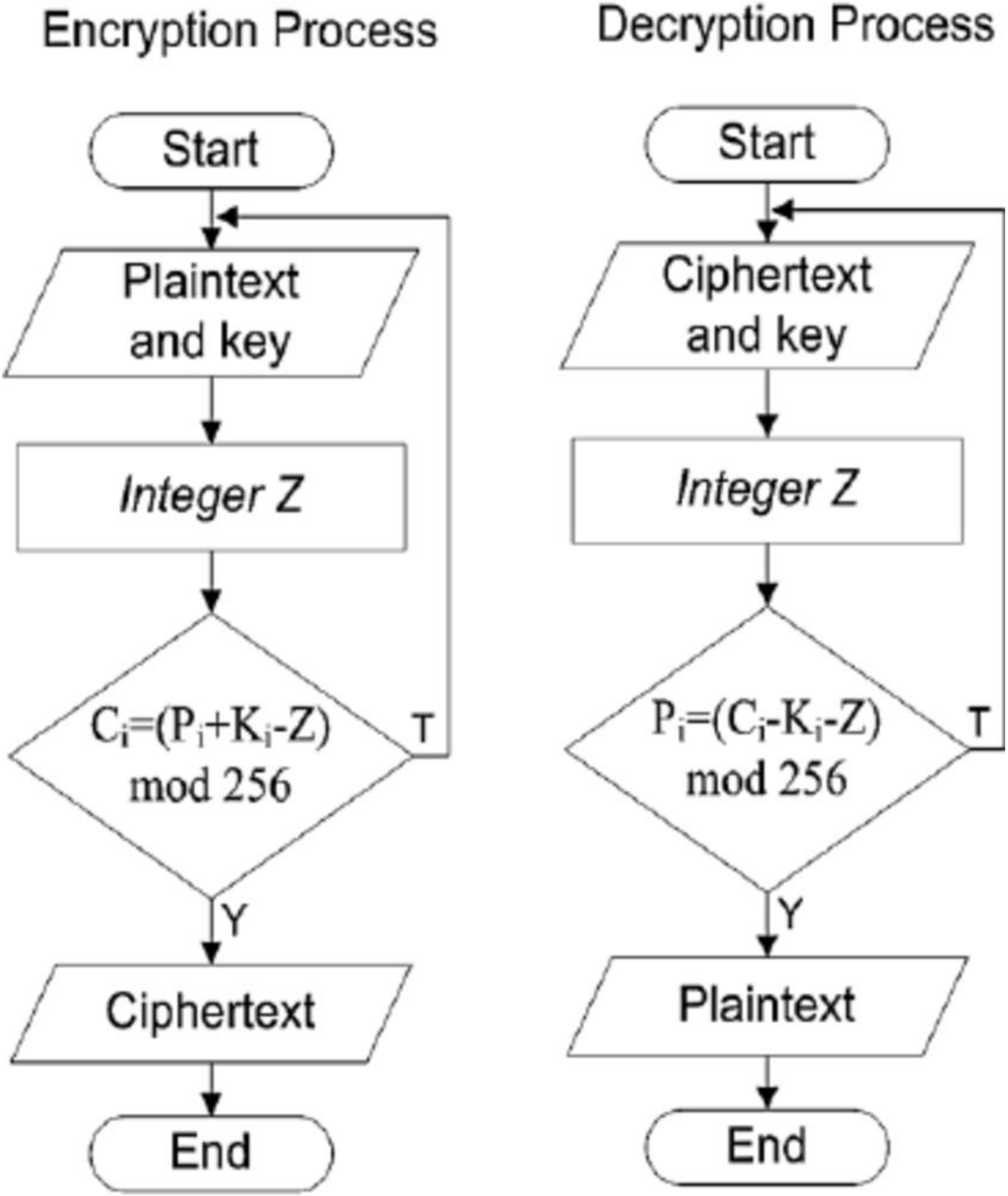


Fig 3.3.1: Flowchart for TEXT encryption and dencryption

HAPTER 4

OUTPUTS

Splash Screen:

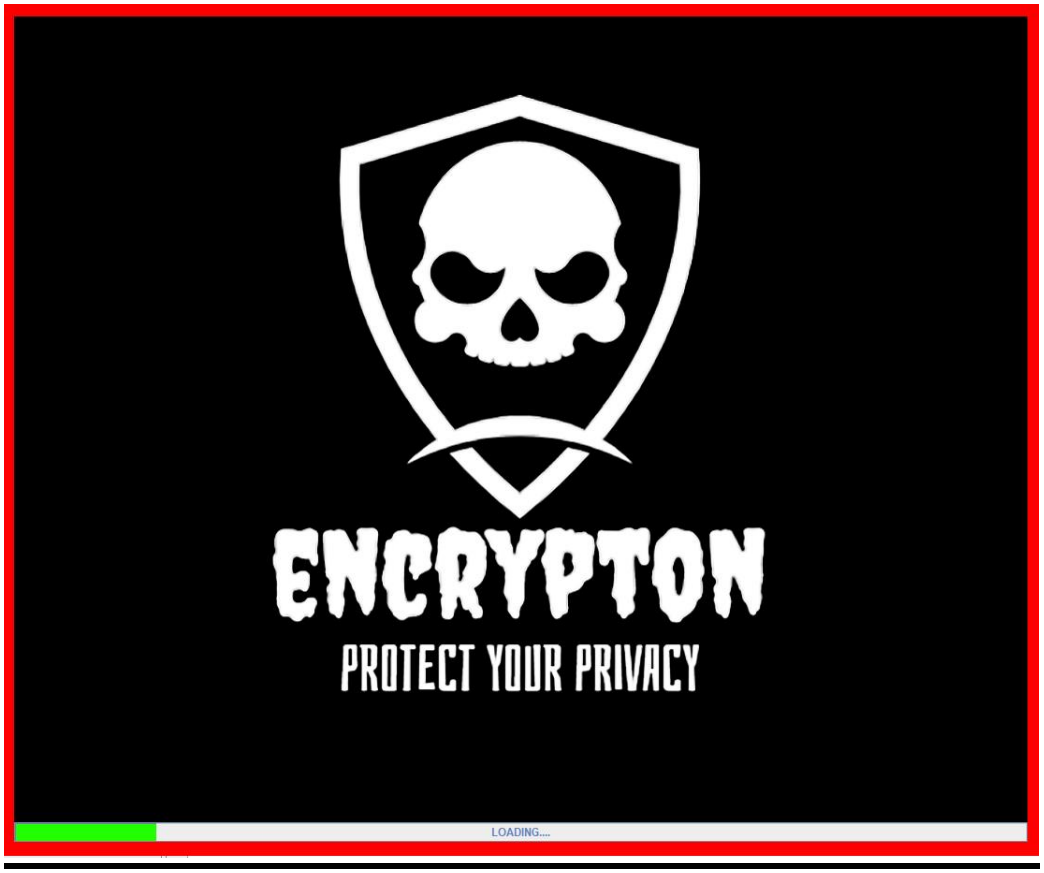


Fig 4.1: Splash Screen

HOME PAGE:

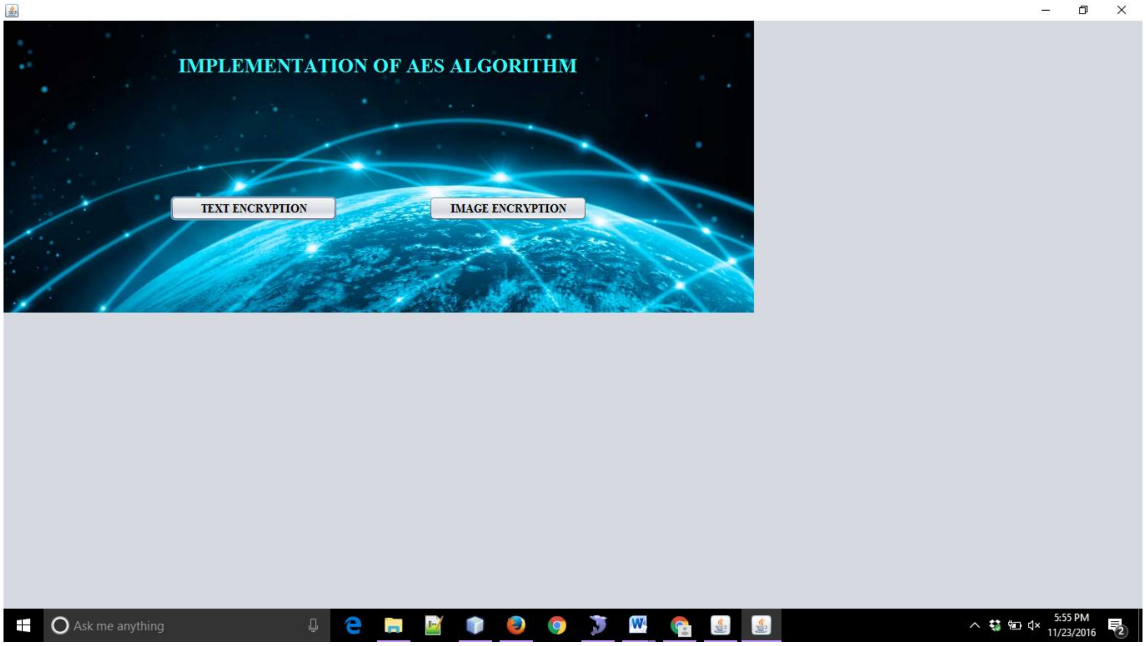
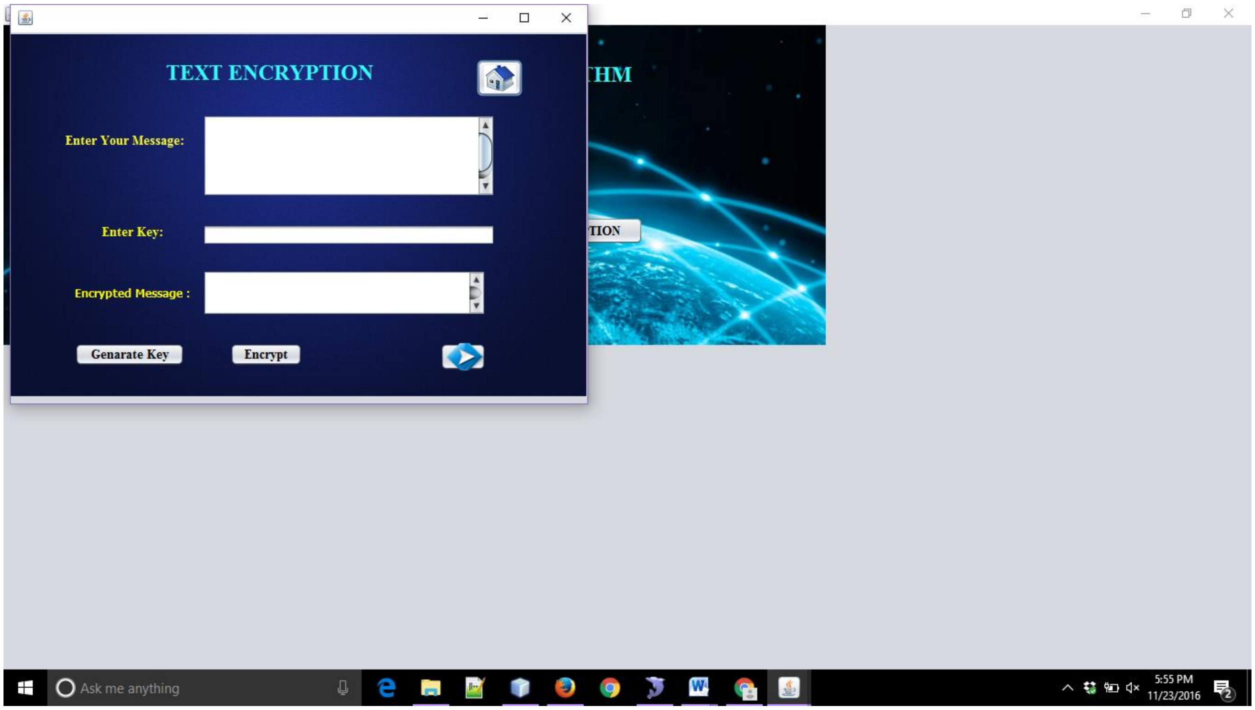
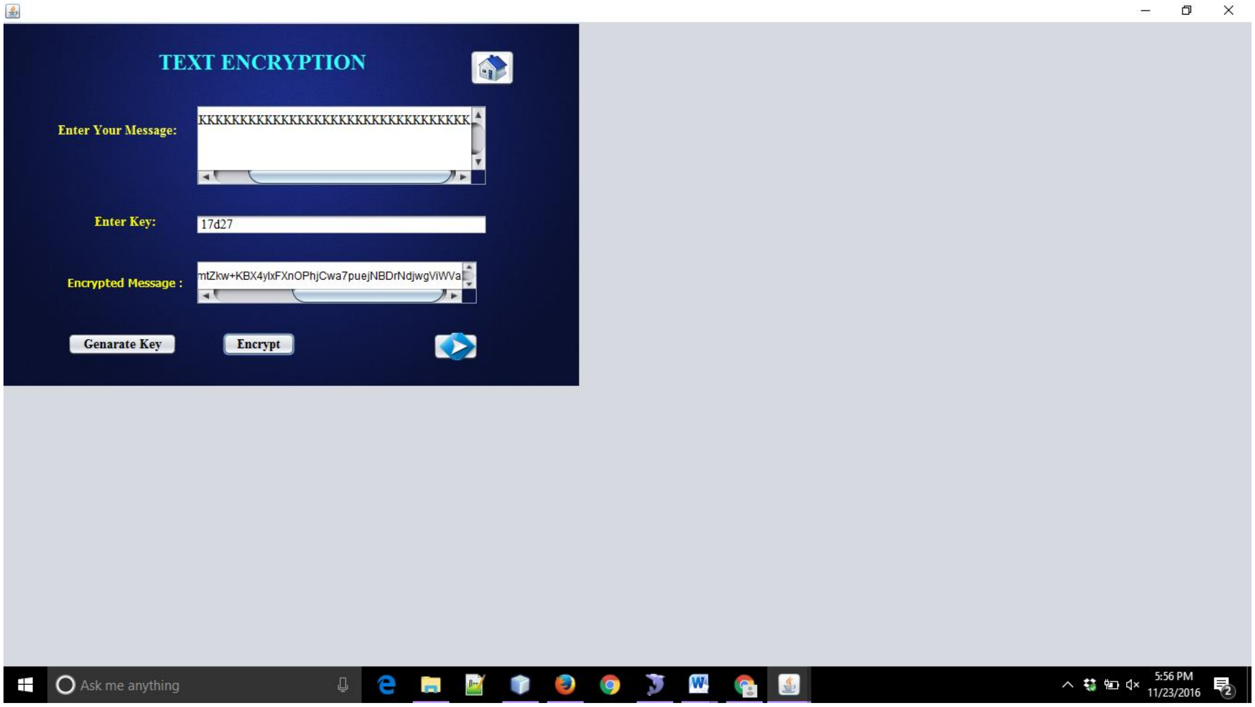


Fig 4.2 Home page

TEXT ENCRYPTION PAGE:





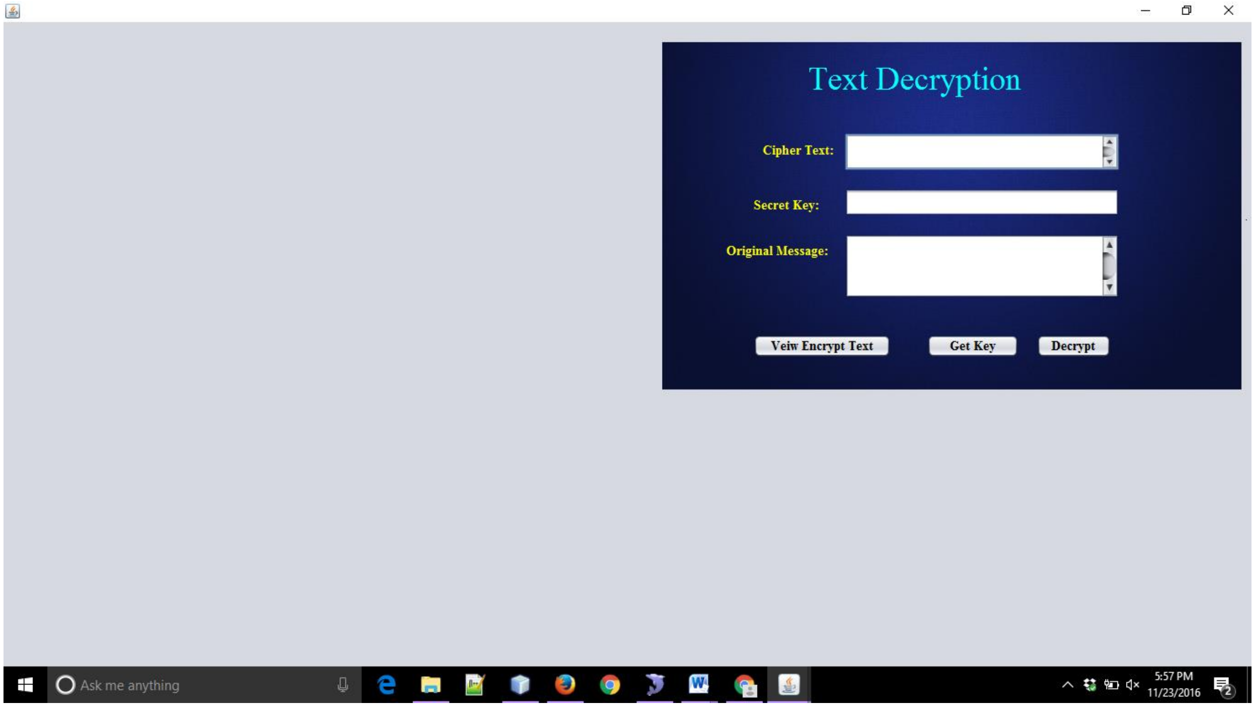
Enter Your Message: KKKKKKKKKKKKKKKKKKKKKKKKKKKKKKKK

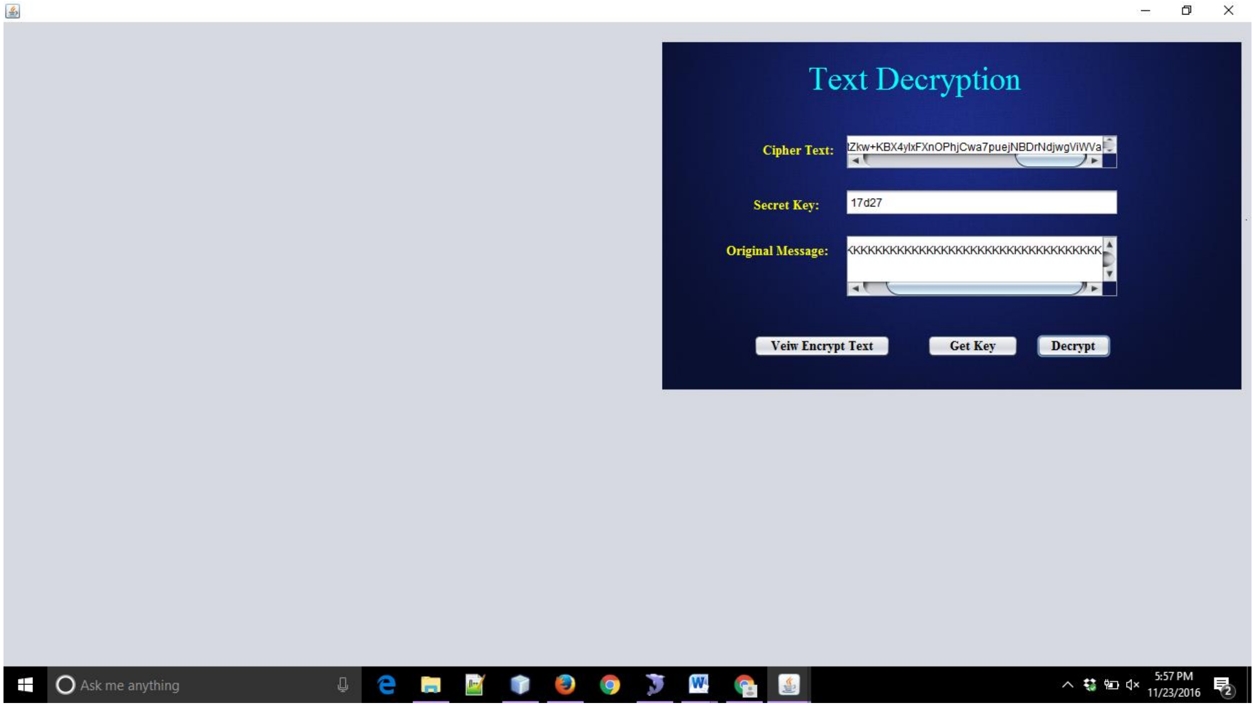
Enter Key: 17d27

Encrypted Message : mtZkw+KBX4ylxFXnOPhjCwa7puejNBDrNdjwgViWVa

Fig 4.3: TEXT ENCRYPTION PAGE

TEXT DECRYPTION PAGE:





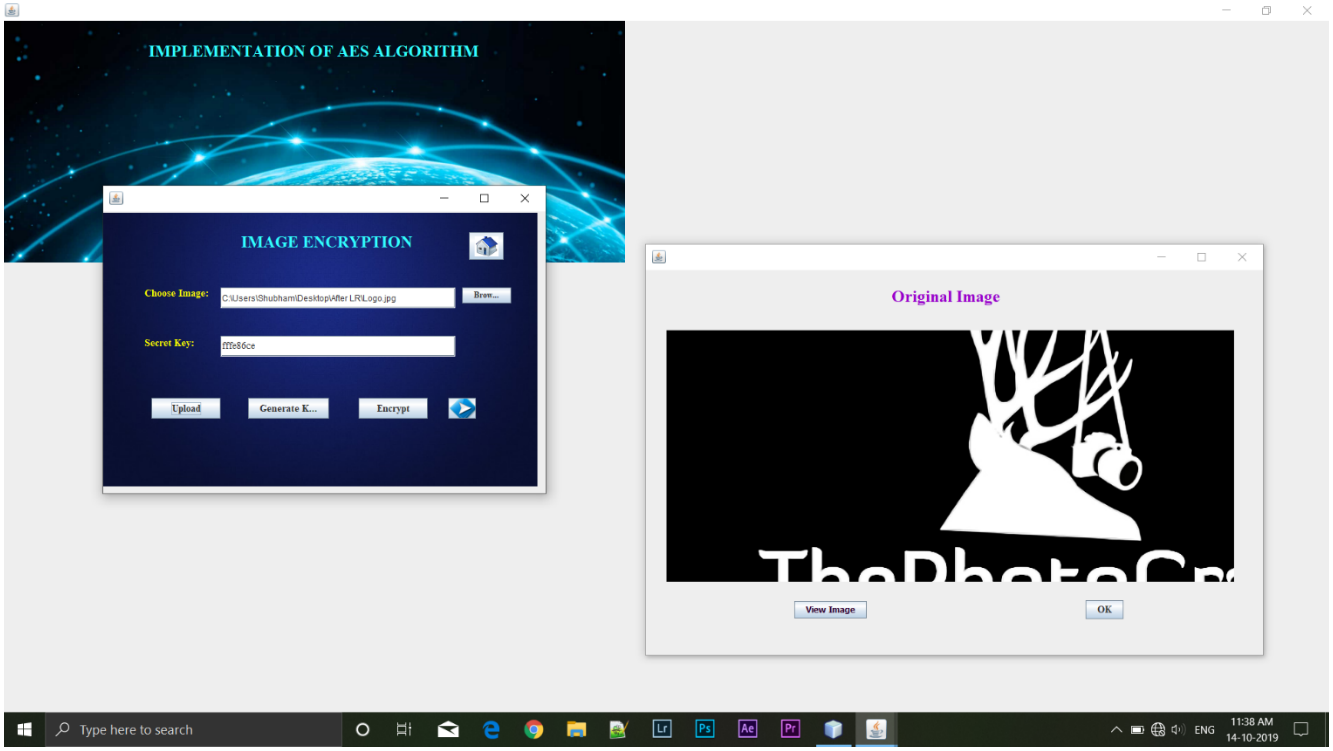
Cipher Text: tZkw+KBX4ylxFXnOPhjCwa7puejNBDrNdjwgViWVa

Secret Key: 17d27

Original Message: KKKKKKKKKKKKKKKKKKKKKKKKKKKKKKKKKKKKK

Fig 4.4: TEXT DENCRYPTION PAGE

IMAGE ECRYPTION PAGE:

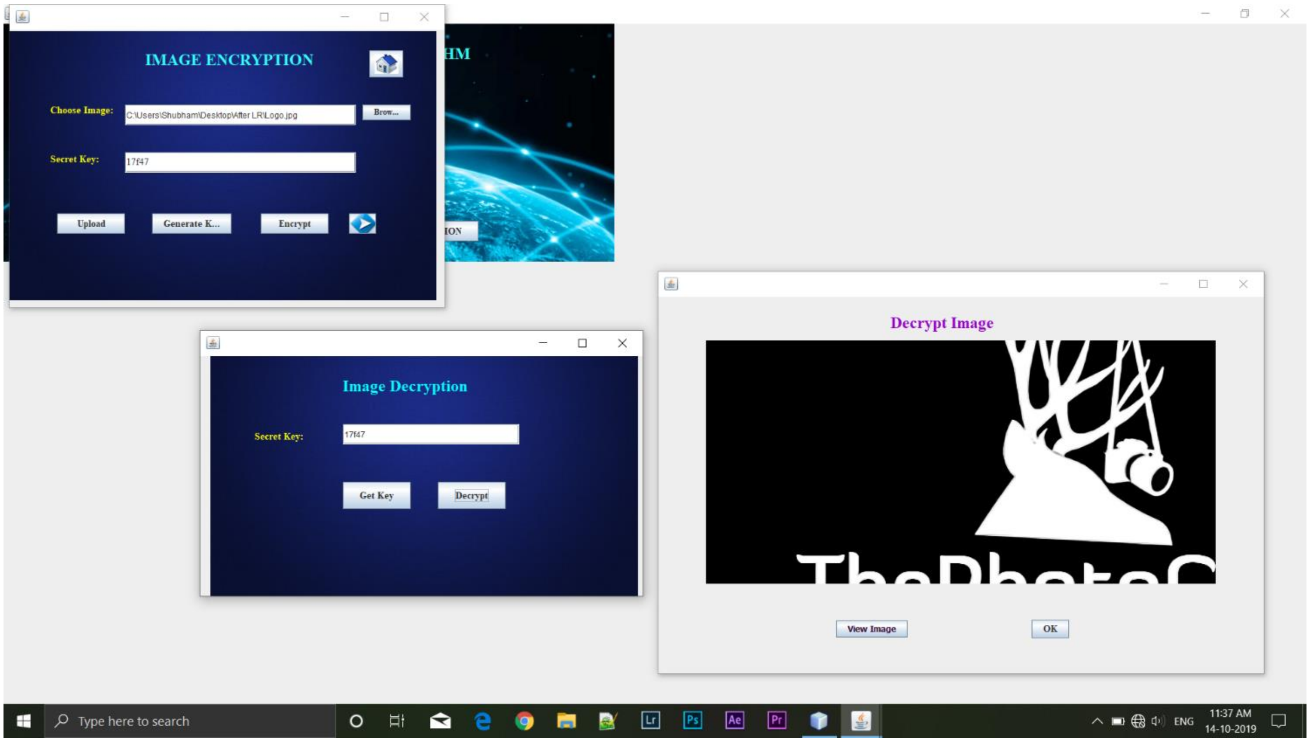


Choose Image: C:\Users\Shubham\Desktop\After LR\Logo.jpg Brow...

Secret Key: fffe86ce

Fig 4.5: IMAGE ENCRYPTION PAGE

IMAGE DECRYPTION PAGE



Choose Image: C:\Users\Shubham\Desktop\After LR\Logo.jpg Brow...

Secret Key: 17f47

Secret Key: 17f47

Fig 4.6: IMAGE DENCRYPTION PAGE

CHAPTER 5

CONCLUSIONS

Conclusion:

This application has been successful in retrieving the image by using algorithm. This application works efficiently in transforming the cipher text into plain text. By using a simple algorithm encrypted image can be retrieved. This application has been successful in encrypting photos even there are few disadvantages. All the defects in the previous system has been defeated by this application.

REFERENCES/BIBLIOGRAPHY

Bibliography

Books:

1. The Complete Reference Java by Herbert Scheldt **(**Tata McGraw-Hill)
2. Head First Java by Kathy Sierra & Bert Bates.

Websites:

1. www.sun.java.com
2. http://www.edutechlearners.com/
3. http://en.wikipedia.org/wiki/Encryption
4. http://en.wikipedia.org/wiki/Plaintext
5. http://en.wikipedia.org/wiki/Ciphertext
6. http://en.wikipedia.org/wiki/Decryption
7. http://en.wikipedia.org/wiki/Cryptography

Papers:

1. Chang-Mok Shin, Dong-Hoan Seo, Kyu-Bo Chol, Ha-Wmn Lee, and SmJmng Kim, " Multilevel Image Encryption by Binary Phase XOR Operations ", IEEE Proceeding in the year 2003.
2. N.K. Pareek, Vinod Patidar, "Image encryption using chaotic logistic map", Elsevier, Image and Vision Computing 24 (2006) 926–934.
3. Saroj Kumar Panigrahy, Bibhudendra Acharya and Debasish Jen, Image Encryption Using Self-Invertible Key Matrix of Hill Cipher Algorithm 1st t International Conference on Advances in Computing, Chikhli, India, 21-22 February 2008.
4. Mohammad Ali Bani Younes and Aman Jantan, An Image Encryption Approach Using a Combination of Permutation Technique Followed by Encryption, IJCSNS International Journal of Computer Science and Network Security, VOL.8, April 2008.
5. Mohammad Ali Bani Younes and Aman Jantan Image Encryption Using Block-Based Transformation Algorithm IAENG International Journal of Computer Science, 35,200