INFORMATION SECURITY

ENHANCED SECURITY USING ENCRYPTION DECRYPTION

VERSION 1.0

A

Training Report

Submitted

In partial fulfillment

For the award of the Degree of

Bachelor of Technology

In Department Computer Science & Engineering

SUBMITTED BY –

PIYUSH KAMAL ANAND (16BCS1321)

B.E. CSE 4

CERTIFICATE

This is to certify **that PIYUSH KAMAL ANAND** of fourth Semester, B.E. (Computer Science) 2016-20, has presented a project report titled "**Enhanced security using encryption decryption"** in partial fulfillment for the award of the degree of Bachelor of Technology under Chandigarh University.

Date: …………………

ACKNOWLEDGEMENT

I have taken efforts in this project. However, it would not have been possible without the kind support and help of many individuals.

I would like to express our gratitude towards my parents & members of Chandigarh University for their kind co-operation and encouragement which help me in completion of this project.

I would like to express our special gratitude and thanks to all the resources from where I collected the information regarding project and all the books from where I gathered the information.

My thanks and appreciations also go to our colleague in developing the project and people who have willingly helped us out with their abilities.

PIYUSH KAMAL ANAND (16BCS1321)

B.E. CSE (SEMESTER 4)

ABSTRACT

Data sharing and networking, in today's date, forms the basis of computer science and technology. In today's competitive world, data security is more important than data sharing or generation as data is the most valuable resource one can possess. Be it public sector units or multinational companies, every organization has increased the needfor data security. Data integrity, authentication, security, and confidentiality are enhancing day by day to facilitate stronger security. To enable data security, various cryptography techniques are used. This project primarily focuses on implementing the existing encryption methods. This project is basically concerned about information security using cryptography, comparing the traditional and modern algorithms.

The purpose for developing this type of application suite is to facilitate the users who want to secure their data that is expected either to be stored locally or to be transmitted over network.

TABLE OF CONTENTS

INTRODUCTION

1.1 Purpose

This document provides all of the requirements for the “Enhanced Security using encryption and decryption”. The document primarily aims at enhancing the user’s and developer’s information about the various aspects of the project. This project is basically concerned about information security using cryptography, comparing the traditional and modern algorithms.

1.2. Problem Definition

Encryption and Decryption: In this aspect of the project, data security is facilitated. The data or files once encrypted cannot be accessed by illegitimate users. Only the authorized users with correct key can access the data. In the project, we have used two different methods for the same. First is the traditional cryptography algorithm like Caesar Shift Cipher and other is the modern symmetric cryptography AES (Advanced Encryption Standard).

1.3 Product Scope

Encryption and decryption are one of the tools providing reliable security mechanism to protect the data and information systems. The security level of these cryptosystems determines the extent to which data theft can be avoided.

1.4 Technique Involved

Encryption and Decryption: The techniques involved in this are DES, TripleDES, AES, RSA..

1.5 Overview

This document specifies SRS for “Enhanced security using encryption and decryption” which is a cryptographic application suite for Encryption/decryption of data, calculating various statistical characteristics of the algorithms and comparing the traditional and modern methods and securing user passwords using a master password in a password safe. The purpose for developing this type of application suite is to facilitate the users who want to secure their data that is expected either to be stored locally or to be transmitted over network and save their memory cost by compressing the data.

SOFTWARE REQUIREMENT SPECIFICATION

Software Requirements Specification (SRS) is the starting point of the software development activity. Little importance was given to this phases in the **early** days of software development. The emphasis was first on coding and then shifted to design.

As systems grew more complex, it become evident that the goal of the entire system cannot be easily comprehended. Hence need for the requirements analysis phase arose. Now, for large software systems, requirements analysis is perhaps the most difficult activity and also the most error prone.

Some of the difficulty is due to the scope of this phase. The software project is imitated by the client needs. In the beginning these needs are in the minds of various people in the client organization. The requirement analyst has to identify the requirements by tacking to these people and understanding their needs. In situations where the software is to automated a currently manuals process, most of the needs can be understood by observing the current practice.

The SRS is a means of translating the ideas in the minds of the clients (the output) into formal document (the output of the requirements phase). Thus the output of the phase is a set of formally specified requirements, which hopefully are complete and consistent, while the input has none of these properties.

- **Hardware interfaces**

This project is intended to be platform independent. Therefore no specific hardware is excluded. But it will at least work on x86 systems without any additional porting efforts. Moreover, no special hardware is needed for software operation. The hardware specifications on which the project has been developed:

Processor: Intel i5 7200U (Minimum - Pentium processor and above)
x86 compatible processor
RAM: 8 GB (Minimum - 512 MB and above)
HDD: 1 TB (Minimum - 80 GB or above)

- **Software interfaces**

This project is intended to work on any operating system as it has been programmed in java which is a platform independent language. We have tested the software to run on windows and android platforms. The software specifications on which the project has been developed :

Operating System: Windows 10

Front End: Java (Eclipse Java Oxygen)
Android studio (IDE 171.4443003)

Back End: Java (Eclipse Java Oxygen)
Android studio (IDE 171.4443003)
Oracle database (Express 11g edition)

- **User interfaces**

GUI (Graphical User Interface) will be used in this application.

- **Communication interfaces**

• Network protocols for program update information.

• System I/O protocols for local file access.

- **Memory constraints**

The project is expected to use 512 MB of RAM or more and 4 GB of external storage or more.

- **Other Nonfunctional Requirements**

✓ **Performance Requirements**

Most public key ciphers rely on high computational cost operations. Therefore, keeping performance considerations in mind, we have used symmetric key encryption for data encryption/decryption. Also, Huffman's coding algorithm is faster in comparison to other compression algorithms and more efficient too. Hence, we have used the mentioned algorithm.

✓ **Safety and Security Requirements**

User is required to remember his password that he/she used to encrypt data (or lock password safe) because most of secure cryptographic algorithms implemented in this suite are secure enough so that no algorithms better than brute-force can be used to recover lost password.

✓ **Software Quality Attributes**

  ➢ **Adaptability and reusability:** The suite is simple (and intuitive) enough that it should not be difficult to adapt it to user's needs. The code is standards compliant and is therefore easily reusable in other applications.

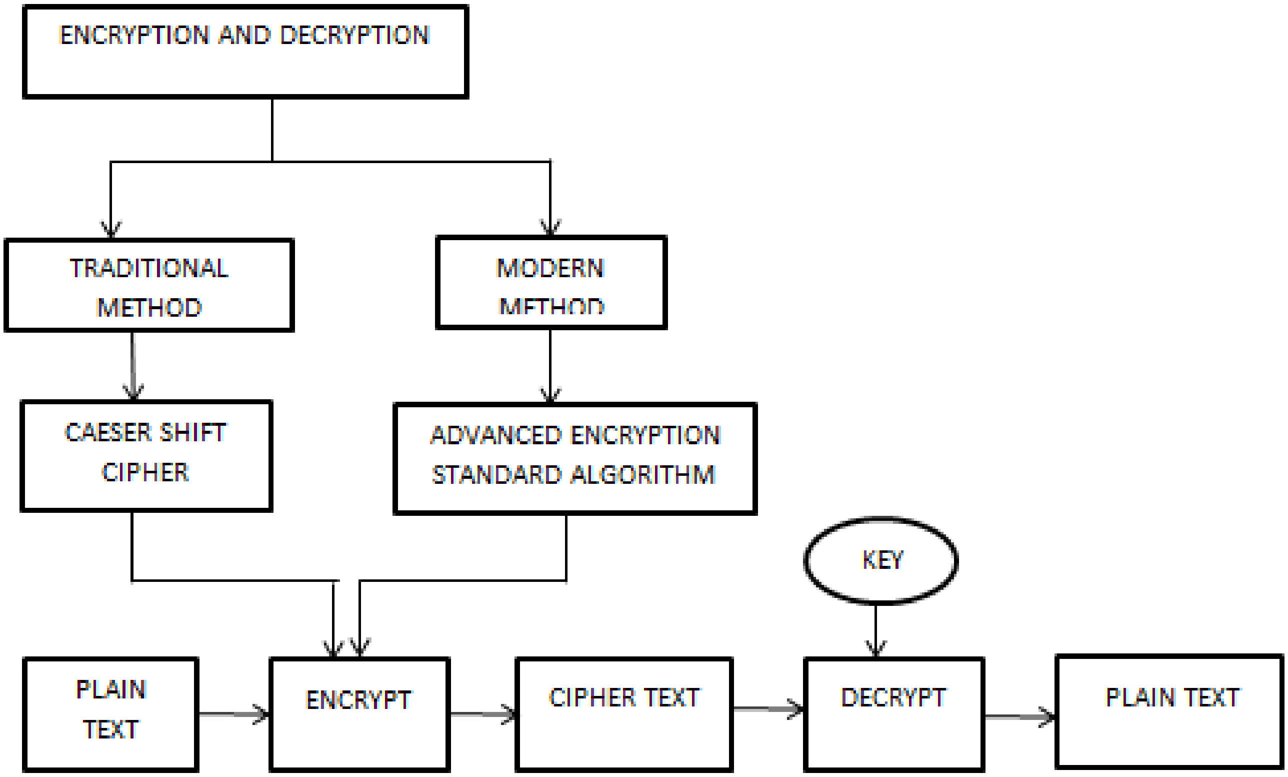
- **Portability:** The code is platform independent; it should be easily portable to different architectures and operating systems.
- **Reliability:** Serious attempts are made to make sure code is reliable and of enterprise quality.
- **Usability:** The project is still in planning stage.

✓ **Database Requirements**

Oracle database will be used for password safe and data file repository. The user will store their login information for various accounts in a table in a database. Also, the data files to be encrypted and images to be compressed may be stored in the database.

SYSTEM DESIGN

1. DATA FLOW DIAGRAM



PROJECT METHODOLOGY

1. **Operations**

- Encrypt and decrypt data.
- Password safe locked with a master password.
- Comparing the traditional and modern cryptographic algorithms
- Generating a key to decrypt information

2. **Cryptographic function: Encryption**

▪ **Description and Priority**

This system feature involves encrypting the data using symmetric cryptographic ciphers for data security.

Priority: High

▪ **Stimulus/Response Sequences**

User selects the cipher used to encrypt data.

User selects data to be encrypted

User confirms encryption to be performed by program.

▪ **Functional requirements**

1. User selects the button corresponding to cipher he wants to be used
to encrypt data.

2. User assigns master key to lock file.

3. User selects the file (input) that is to be encrypted.

4. User clicks on 'Encrypt' button to apply changes.

4. Output encrypted file with cipher text is automatically created in input file directory.

3. **Cryptographic function: Decryption**

▪ **Description and Priority**

This system feature involves decrypting the data using symmetric cryptographic ciphers for data security.

Priority: High

▪ **Stimulus/Response Sequences**

User selects the cipher used to decrypt data.

User selects data to be decrypted

User confirms decryption to be performed by program.

- **Functional requirements**

1. User selects the button corresponding to cipher he wants to be used to decrypt data.

2. User assigns master key to lock file.

3. User selects the file (input) that is to be decrypted.

2. User clicks on 'Decrypt' button to apply changes.

3. Output decrypted file with plain text is automatically created in input file directory.

4. Password safe

- **Description and Priority**

This system feature involves securing a set of user's login info (i.e. username/password + additional useful info) by storing them in a table in DB.

Priority: Medium

- **Stimulus/Response Sequences**

User inputs login info (i.e. username/password + additional useful info) into table using program GUI.

- **Functional requirements**

1. User selects the button corresponding to which he wants to be used to apply password.

2. User inputs the data to be stored in table.

3. User clicks on ‘Apply’ button and the username and password are set.

SCREENSHOTS

ENCRYPTION AND DECRYPTION

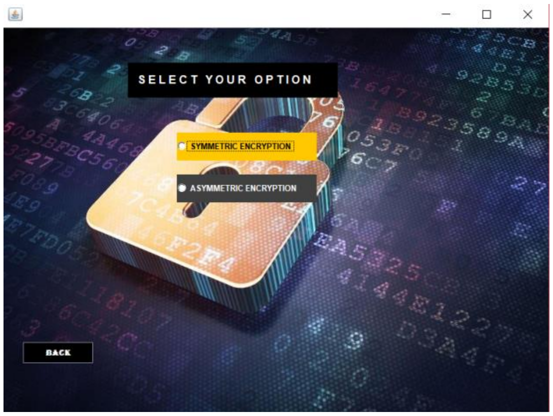


Fig 1.i) The user is asked to select between symmetric and asymmetric encryption.

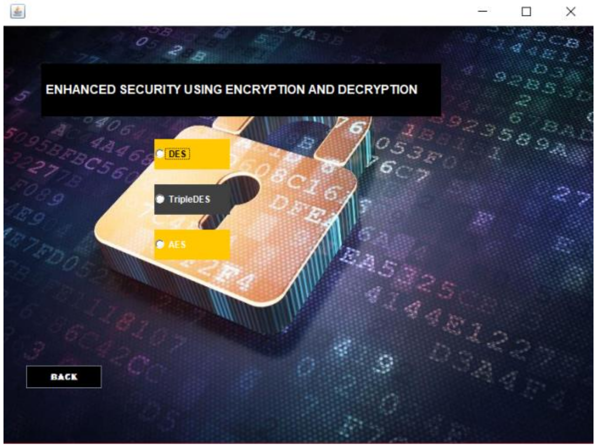
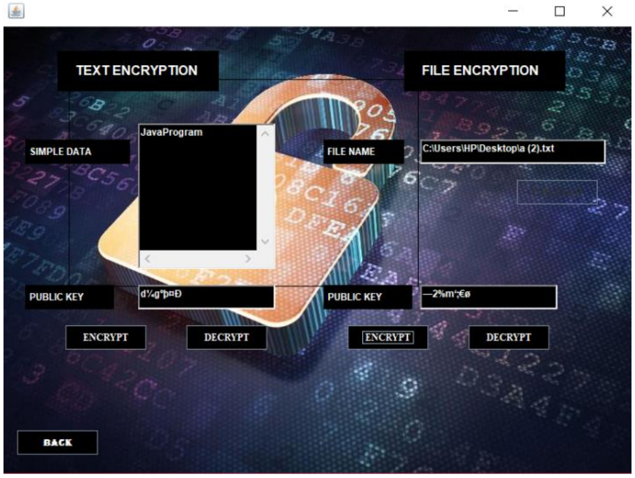


Fig 1.ii) If the user selects symmetric encryption, a list of different algorithms is displayed to select.



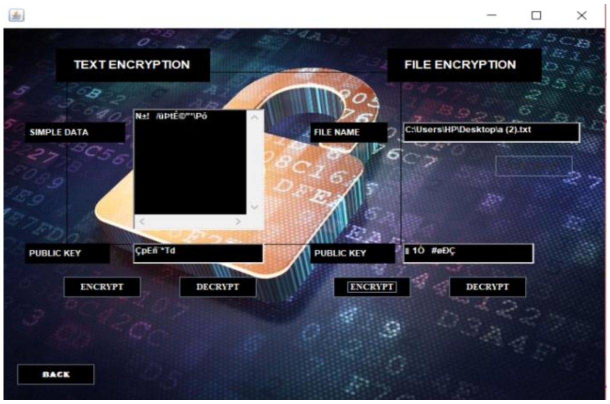
SIMPLE DATA: JavaProgram

FILE NAME: C:\Users\HP\Desktop\a (2).txt

PUBLIC KEY: d¼g°þ¤Ð

PUBLIC KEY: —2‰m';€ø

Fig 1.iii) On selecting DES and entering text or file to be encrypted.



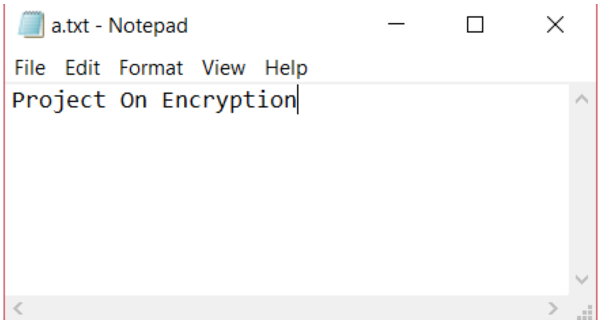
N±! /ûPtÉ©""\Pó

C:\Users\HP\Desktop\a (2).txt

ÇpEñ˚*Td

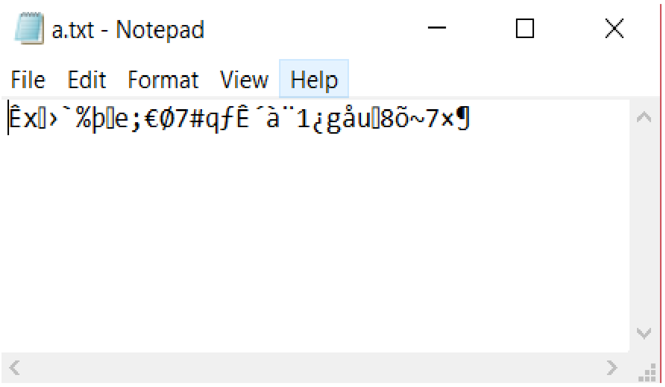
▮1Ò #øÐÇ

Fig 1.iv) After pressing Encrypt button.



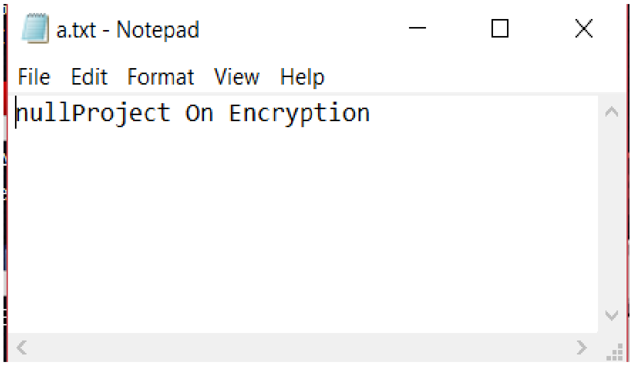
```
Project On Encryption
```

Fig 1.v)The original plaintext file.



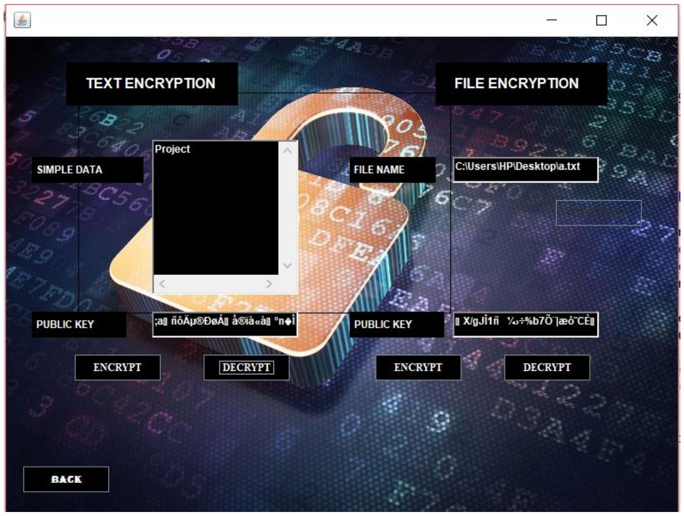
```
Êx▯›`%þ▯e;€Ø7#qƒÊ´à¨1¿gåu▯8õ~7x¶
```

Fig 1.vi) The encrypted text file.



```
nullProject On Encryption
```

Fig 1.vii) After pressing the decrypt button.



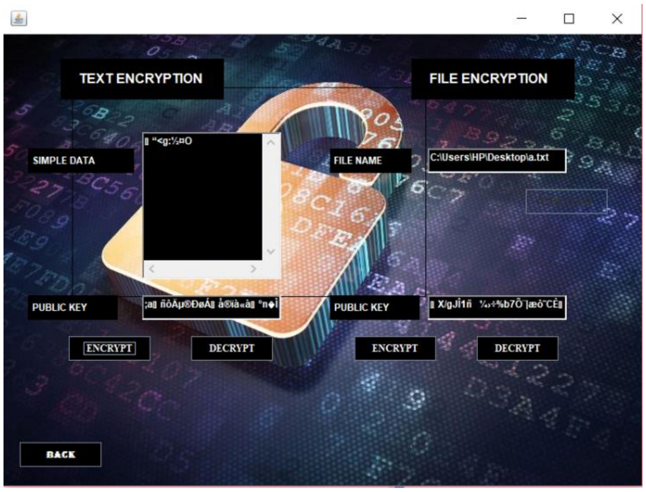
SIMPLE DATA: Project

FILE NAME: C:\Users\HP\Desktop\a.txt

PUBLIC KEY: ;a▯ ñôÄµ®ÐøÁ▯ å®ïà«à▯ °n◆Î

PUBLIC KEY: ▯ X/gJÎ1ñ ¼›÷%b7Õ¨|æô˝CÈ▯

Fig 1.viii) On selecting TripleDES algorithm and entering text or file to be encrypted.



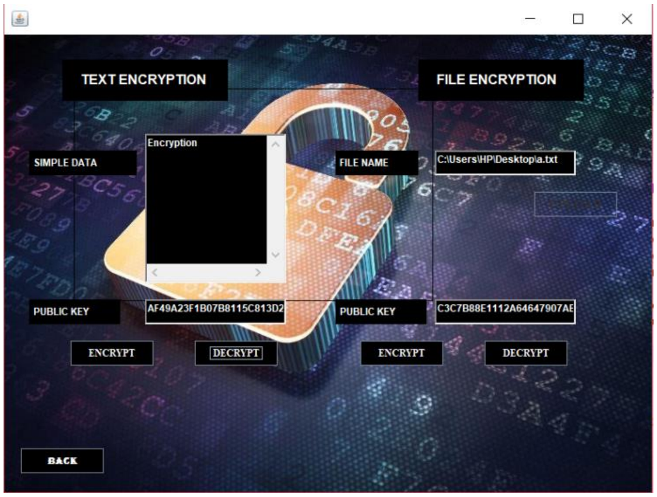
SIMPLE DATA: ▯ "<g:½¤O

FILE NAME: C:\Users\HP\Desktop\a.txt

PUBLIC KEY: ;a▯ ñôÄµ®ÐøÁ▯ å®ïà«à▯ °n◆Î

PUBLIC KEY: ▯ X/gJÎ1ñ ¼›÷%b7Õ¨|æô˝CÈ▯

Fig 1.ix) On pressing encrypt button in TripleDES algorithm



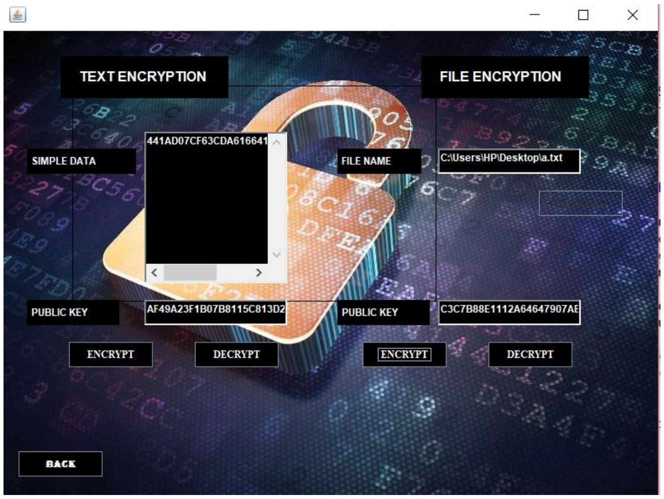
SIMPLE DATA: Encryption

FILE NAME: C:\Users\HP\Desktop\a.txt

PUBLIC KEY: AF49A23F1B07B8115C813D2

PUBLIC KEY: C3C7B88E1112A64647907AE

Fig 1.x) On selecting AES algorithmand entering text or file to be encrypted



441AD07CF63CDA616641

C:\Users\HP\Desktop\a.txt

AF49A23F1B07B8115C813D2

C3C7B88E1112A64647907AE

Fig 1.xi) On pressing encrypt button in AES algorithm

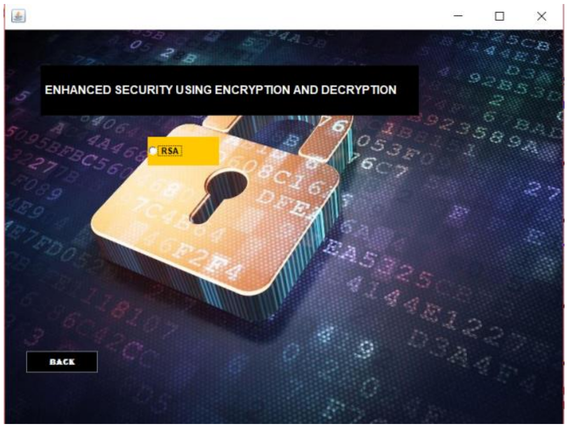
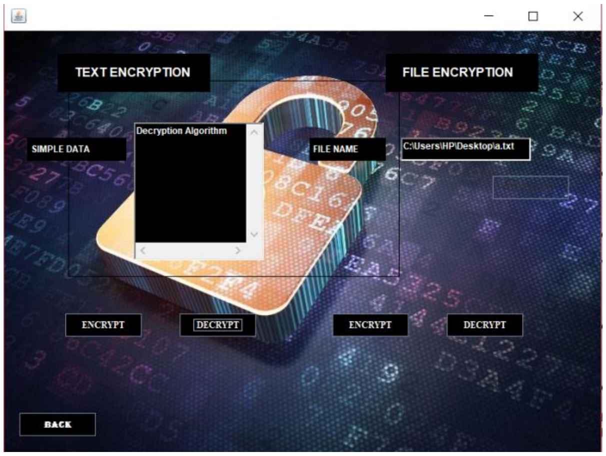


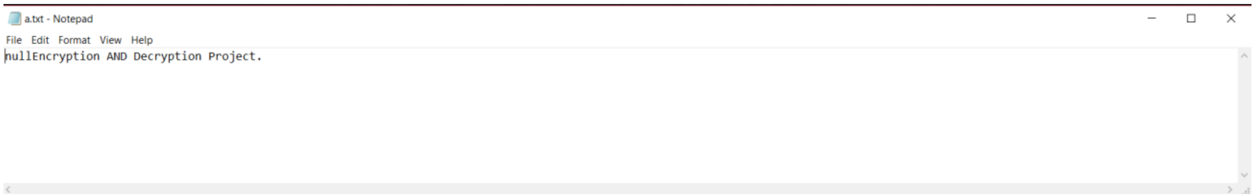
Fig 1.xii) On selecting asymmetric encryption technique



Decryption Algorithm

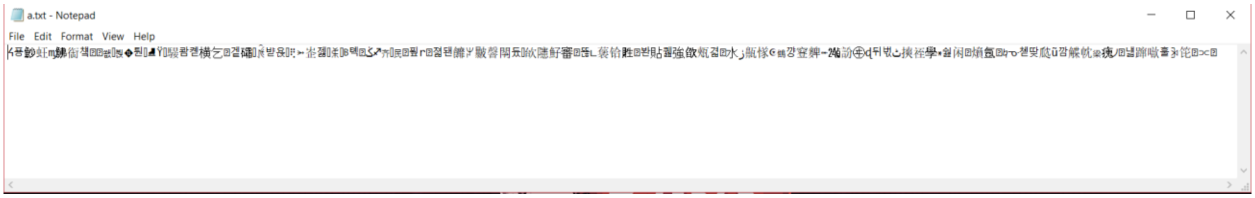
C:\Users\HP\Desktop\a.txt

Fig 1.xiii) On selecting RSA algorithm



```
nullEncryption AND Decryption Project.
```

Fig 1.xiv) The original plaintext file



```
[illegible]
```

Fig 1.xv) The encrypted text file

CONCLUSION AND FUTURE SCOPE

This project on “Enhanced security using encryption & decryption and Image Compression” is a user friendly application that will find its scope in the data security and efficient memory management. The developed software will secure data and files by encrypting them using AES algorithm and Caesar Shift Cipher algorithms and help provide data security

Every application has its own merits and demerits. The project has covered almost all the requirements. Further requirements and improvements can easily be done since the coding is mainly structured or modular in nature. Changing the existing modules or adding new modules can append improvements. Further enhancements can be made to the application, so that the web site functions very attractive and useful manner than the present one.

REFERENCES

1. https://www.tutorialspoint.com/cryptography/index.htm
2. https://www.garykessler.net/library/crypto.html
3. https://www.researchgate.net/figure/276230307_fig1_Figure-2-The-flow-chart-diagram-for-the-encryption-and-decryption-process
4. https://en.wikipedia.org/wiki/Triple_DES#Algorithm
5. http://slideplayer.com/slide/7897399/
6. https://www.researchgate.net/figure/AES-flowchart_fig11_282817937
7. Cryptography and Network Security" Seventh Edition by William Stallings.
8. https://www.google.com/images